Network Working Group
Internet-Draft
Expires: April 26, 2006

C. Alexander, Ed.
J. Babiarz
Nortel

October 23, 2005

# RTP Payload Format for ECN Probing
## draft-alexander-rtp-payload-for-ecn-probing-02.txt

Status of this Memo



This Internet-Draft will expire on April 26, 2006.

Copyright Notice



Abstract

This memo defines a Real Time Transport Protocol (RTP) payload format for use when probing for congestion using Explicit Congestion Detection (ECN). This payload format is intended for use with the probing mechanisms described in draft "Real-time ECN Use Cases". While defined in terms of the specific application of admission control, it is desirable to overlay this format with other probing mechanisms so as to reduce the number of probing packet formats.

Table of Contents

## 1. Introduction

This memo defines a new RTP payload format for use with applications requiring congestion detection along the data path and verification of data path connectivity, for example, admission control of a real-time session. The format described herein is intended for use with the mechanisms described in "Congestion Notification Process for Real-Time Traffic" [2], which defines the use of the Explicit Congestion Notification (ECN) bits in the Internet Protocol (IP) header as a means to detect congestion in the network for real-time inelastic flows. The new format can be used to provide the capabilities described in "Real-time ECN Use Cases" [3], although it may also be used in other contexts.

The new RTP payload format defined herein is called "ecnprobe". Packets utilizing this payload are carried as RTP traffic through the IP network. Packets carrying this payload are treated the same as any other RTP packet with the exception of play-back by the receiving device.

The advantages of using this payload format are:

1. congestion detection can be performed using a simple probing mechanism without having to extend other protocols;

2. the payload format allows for limited detection of devices making inappropriate changes to the ECN markings in the network;

3. the packet carrying the payload can vary in size from the minimum necessary to carry the payload, to a size padded to mimic a specific codec.

Applications will use this payload format to create and send RTP probe packets through the IP network to determine the highest state of congestion along the path taken by the packets.

In all uses, applications receiving this payload MUST NOT attempt to play it as actual media.

This memo only defines the new payload format. Examples of its usage can be found in [3].

## 2. History

### 2.1 Version 00

Initial submission.

### 2.2 Version 01

Adding sections describing alternatives under investigation, as well as the reasons why we believe RTP is necessary. No other major content changes over -00 version.

## 3. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC2119 [7] and indicate requirement levels for compliant implementations.

## 4. Definitions

The following terms are used in this document:

Cheater: A device in the network that makes inappropriate changes to the ECN markings in the network. A cheating device might re-mark the ECN bits in the IP header in order to hide congestion from an endpoint (i.e., by lowering the ECN congestion marking), or might force an endpoint to think congestion is present when it is not (i.e., by raising the ECN congestion marking). Due to the nature of ECN and how conformant network devices mark ECN for real-time inelastic flows, it is possible to detect the presence of cheater devices which lower the ECN marking, but not those that raise it.

Probe Packet: The Probe Packet is an RTP packet utilizing the "ecnprobe" payload format defined herein.

Receiver: The Receiver is simply an endpoint device which receives one or more Probe Packets from the Sender. As defined here, the Responder does not respond directly to the Probe Packet.

Sender: The Sender is an endpoint device which generates one or more Probe Packets.

## 5. Alternatives Under Consideration

While we believe it is necessary to use RTP as the packet format for probing, there are other options. This section outlines the various options currently being investigated, including RTP.

### 5.1 Define New RTP Format

RTP is the mechanism we originally specified, and the overall content of this document still presumes RTP as the packet format for probing. What we have not adequately answered is why RTP? There is certainly no media content being delivered via the packets, resulting in the use of RTP for this coming into question.

RTP is preferred primarily because real media utilizes it and the underlying Real-time ECN mechanism for admission control of new sessions can benefit from it. The RTP probe flow has several other functions besides congestion monitoring. First, probing verifies the media path end-to-end, ensuring that both endpoints can reliably send RTP packets before alerting. An unreliable path can be detected via RTP mechanisms, allowing such flows to not be admitted.

Second, probing verifies that the measured traffic level is within the pre-engineered limits to provide good service. For this purpose, ECN metering and marking must be performed on the RTP probe flow packets along the same path that the RTP media packets will use. Within the network, routers must treat probe packets as close to real RTP media packets as possible. Using RTP for the probe packets should ensure this. It has been pointed out that routers can filter traffic based on traffic type, for example, routing RTP traffic one way and other traffic another, and if this were to occur when the probe packet were not using RTP, then the Real-time ECN mechanism would not function as intended. While acknowledging again that the probes would carry no media, RTP is necessary to ensure appropriate treatment of the probe packets in the network.

Third, since endpoints already utilize RTP, there is a minimal development effort to add ECN capabilities to RTP.

By using RTP, we are also able to leverage use of the RTP sequence number field during conformance verification, as described in "Congestion Notification Process for Real-Time Traffic" [2]. We do acknowledge that there are other alternatives to accomplishing this particular aspect of the mechanism, but it is a piece of RTP that can be re-used.

### 5.2 UDP

UDP has long been an alternative to using RTP. While everything necessary can certainly be built with a new protocol or packet format on top of UDP, what is lost with this approach is the assurance that the probe packets will be treated as expected in the network.

### 5.3 ICE/STUN

ICE/STUN is another suggested alternative that is still being investigated.

### 5.4 Re-use Existing RTP Format

This alternative is preferred at this time if the need for ECN-specific payload is dissolved. In such a case, another RTP packet format could be leveraged for use as the probe packet format.

## 6. RTP Payload Format for Real-Time ECN Admission Control

The "ecnprobe" payload is transported in RTP packets. However, it is not part of an RTP stream. It therefore has no requirements to use similar properties of the media it represents.

### 6.1 Registration

The new RTP payload format is defined as "ecnprobe", with a MIME type of "audio/ecnprobe" for audio and a MIME type of "video/ecnprobe" for video. The payload type for RTP packets carrying this payload is determined dynamically through methods outside the scope of this document.

### 6.2 IP Header Fields

DSCP: The DSCP set in the IP header is a critical component of the ECN method as outlined in [2]. It should be set appropriately for the session media for which admission control is being performed.

ECN: Unless attempting to detect for the presence of Cheaters along the media path, an application MUST set the two-bit ECN field in the IP header to '10', which indicates that it is an ECN-capable transport, with no congestion experienced. If attempting to detect for the presence of Cheaters, the ECN field SHOULD be set as required by the detection method being used.

### 6.3 RTP Header Fields

Payload Type: The payload type field MUST be filled with a value determined dynamically.

### 6.4 Payload Format

The "ecnprobe" payload format is shown in Figure 1.

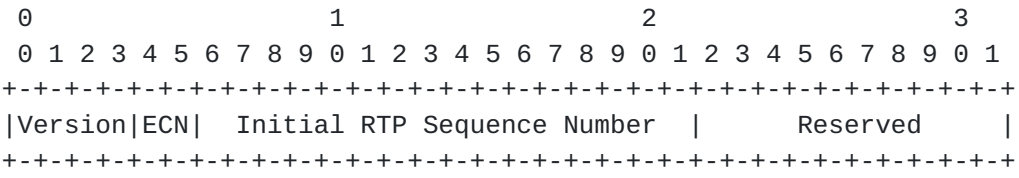


Figure 1: ecnprobe Payload Format

It consists of five fields: Version, ECN, Initial RTP Sequence Number (ISRN), and Reserved.

### 6.4.1 Version

The Version field designates the version of the payload format. This field is provided for future extensibility of the payload to carry additional information. The following value is defined by this document for the Version field:

0: Initial version defined by this document.

### 6.4.2 Explicit Congestion Notification (ECN)

This field contains a two-bit ECN value. If an application is trying to detect Cheaters, the Sender SHOULD set this field to the two-bit ECN value used in the IP header when sending the Probe Packet.

### 6.4.3 Initial RTP Sequence Number (IRSN)

In order to perform cheater detection and/or compliance testing in a unidirectional fashion, the receiving endsystem needs to know which packets to use for cheater detection and/or compliance testing. During probing, this is less important as the probe payload will contain the actual ECN value set in the IP header. But during media exchange, the receiver must know exactly which packets are intended for cheater detection and/or compliance testing. The IRSN value represents the initial sequence number used on the outgoing probe and/or media packets. This value is used as described in [2] to allow both ends to know which packets in the media stream are marked for cheater detection. In the event of lost or out-of-order packets, the receiver needs only to check the sequence number of the incoming packet against the calculated sequence number that it expects to find in packets being used for cheater detection and/or compliance testing.

### 6.4.4 Reserved

This field contains 10 bits reserved for future use.

## 7. Considerations for Payload Format

There were two main considerations driving the new payload format defined in this memo: extensibility and flexibility.

### 7.1 Extensibility Considerations

While the intended use for this payload format is for admission control using ECN, the payload format need not be limited to that application. Even for admission control applications which will use it, the payload format also need not be limited to the mechanisms described in this memo. With that in mind, the four-bit Version field is included to allow for extensibility for future applications/ implementations.

### 7.2 Flexibility Considerations

In addition to extensibility, another consideration is the flexibility to allow the initial definition of the payload to be used in as wide a range of implementations as possible.

While the default and minimum size of the payload is 4 octets, an application MAY pad to the payload in order to simulate a specific codec. In this case, the application needs to ensure that the packets carrying the padded payload are sent at the appropriate rate corresponding to the codec being simulated.

## 8. Considerations for Direct Feedback

The payload format is currently defined with no explicit mechanism to provide feedback on the Probe Packet(s) from the Receiver to the Sender. This section discusses the options that have been considered, and describes why they are not included along with the payload format definition.

### 8.1 Feedback via RTP

The payload format was originally envisioned to be used with either a unidirectional probe or a bidirectional probe.

This document specifies a unidirectional probe.

A bidirectional probe flows from the Sender to the Receiver, with the Receiver then generating its own probe in response, with the payload additionally carrying the ECN value from the IP header of the received probe packet. While this is feasible, the unidirectional probing model results in a simpler implementation.

### 8.2 Feedback via RTCP

Also considered was an approach whereby feedback is provided via RTCP from the Receiver to the Sender. While possible, implementing feedback via RTCP in real time as described in "Admission Control Use Case for Real-time ECN" [3] would necessitate violation of the rules governing the RTCP transmission interval described in RFC3550 [1]. The RTCP transmission interval deliberately paces RTCP transmissions to be no more frequent than every 5 seconds, but for an admission control application, the transmission interval would potentially need to be much shorter.

## 9. MIME Registration

This section registeres MIME types for audio/ecnprobe and video/ecnprobe.

### 9.1 audio/ecnprobe

MIME media type name: audio

MIME subtype name: ecnprobe

Required Parameters: none

Optional Parameters: none

Encoding considerations: This type is only defined for transfer via RTP [1] or Secure RTP [5].

Security considerations: See "Security Considerations" (Section 10).

Interoperability considerations: none

Published specification: This document.

Applications which use this media: The "ecnprobe" application subtype is used to perform ECN probing and data path connectivity for admission control, although it is not limited solely to this application.

Additional information:

1. Magic number(s): N/A

2. File extensions(s): N/A

3. Macintosh file type code(s): N/A

### 9.2 video/ecnprobe

MIME media type name: video

MIME subtype name: ecnprobe

Required Parameters: none

Optional Parameters: none

Encoding considerations: This type is only defined for transfer via RTP [1] or Secure RTP [5].

Security considerations: See "Security Considerations" (Section 10).

Interoperability considerations: none

Published specification: This document.

Applications which use this media: The "ecnprobe" application subtype is used to perform ECN probing and data path connectivity for admission control, although it is not limited solely to this application.

Additional information:

1. Magic number(s): N/A

2. File extensions(s): N/A

3. Macintosh file type code(s): N/A

## 10. Security Considerations

Security considerations for the use of ECN for real-time inelastic flows is covered in [2]. The main consideration to account for here is that when the payload is carrying any relevant information for admission control, the payload SHOULD be secured, e.g., using "The Secure Real-time Transport Protocol (SRTP)" [5] or "Security Architecture for the Internet Protocol" [6]. If an application is attempting to detect Cheaters and the payload is not secured, a cheating device will be able to inspect and modify the ECN field in the payload, thereby circumventing the detection method.

## 11. IANA Considerations

The Version field described in "Version" (Section 6.4.1) will need to be administered. This field should be administered on a first come, first served basis.

IANA is requested to make MIME type registrations as specified above in "MIME Registration" (Section 9).

## 12. Acknowledgements

The authors acknowledge a great many inputs, including the following: Francois Audet, Amy Pendleton, Tom Taylor, John Rutledge, Jeremy Matthews, Marvin Krym, Stephen Dudley, and Kwok Ho Chan.

## 13. References

### 13.1 Normative References

[1] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, July 2003.

[2] Babiarz, J., Chan, K., and V. Firoiu, "Congestion Notification Process for Real-Time Traffic", Internet-Draft draft-babiarz-tsvwg-rtecn-04.txt (Work in Progress), July 2005.

[3] Alexander, C., Ed., Babiarz, J., and J. Matthews, "Real-time ECN Use Cases", Internet-Draft draft-alexander-rtecn-use-cases-00.txt (Work in Progress), July 2005.

### 13.2 Informative References

[4] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[5] Baugher, M., Carrara, E., McGrew, D., Naslund, M., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[6] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

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

## Authors' Addresses

Corey W. Alexander (editor)
Nortel
MS 08704A30
2370 Performance Drive
Richardson, TX 75082
US

Phone: +1 972 684-8320
Fax: +1 972 684-1838
Email: coreya@nortel.com

Jozef Babiarz
Nortel
MS 04331C04
3500 Carling Avenue
Ottawa, Ontario K2H 8E9
CA

Phone: +1 613 763-6098
Fax: +1 613 763-2231
Email: babiarz@nortel.com

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.