

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 7, 2009

A. Morton
L. Ciavattone
AT&T Labs
July 6, 2008

TWAMP Reflect Padding Feature
draft-morton-ippm-twamp-reflect-padding-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 7, 2009.

Abstract

The IETF is completing its work on TWAMP - the Two-Way Active Measurement Protocol. This memo describes a proposed feature for TWAMP, intended for discussion in the IP Performance Metrics WG. The feature gives the reflector the ability to return some of the packet padding bits to the sender.

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](#)].

Internet-Draft

TWAMP Reflect Padding

July 2008

Table of Contents

1.	Introduction	3
2.	Purpose and Scope	3
3.	TWAMP Control Extensions	3
3.1.	Connection Setup with Reflect Padding Feature	4
3.2.	Request-TW-Session Packet Format	5
3.3.	Accept Session Packet Format	5
3.4.	Additional considerations	6
4.	Extended TWAMP Test	6
4.1.	Sender Behavior	7
4.1.1.	Packet Timings	7
4.1.2.	Packet Format and Content	7
4.2.	Reflector Behavior	8
5.	Security Considerations	9
6.	IANA Considerations	9
6.1.	Registry Specification	9
6.2.	Registry Management	9
6.3.	Experimental Numbers	9
6.4.	Registry Contents	9
7.	Acknowledgements	10
8.	References	10
8.1.	Normative References	10
8.2.	Informative References	11
	Authors' Addresses	11
	Intellectual Property and Copyright Statements	12

1. Introduction

The IETF is completing its work on TWAMP - the Two-Way Active Measurement Protocol [[I-D.ietf-ippm-twamp](#)], which is an extension to the One-way Active Measurement Protocol, OWAMP [[RFC4656](#)].

This memo describes a new proposed feature for TWAMP, so it can be discussed and interest to take-up the feature assessed. This feature adds the capability for the Session-Reflector to return a limited number of unassigned (padding) bits to the Server/Session-Sender. With this capability, the Control-Client/Session-Sender can information it deems useful and have the assurance that the corresponding test packet will contain the information when it is returned.

The relationship between this memo and TWAMP is intended to be an update to the TWAMP RFC when published.

2. Purpose and Scope

The purpose of this memo is to describe an additional function and feature for TWAMP [[I-D.ietf-ippm-twamp](#)]. The feature needs a clear description so it can be discussed and (hopefully) adopted in the IP Performance Metrics Charter.

The scope of the memo is currently limited to specifications of the following feature:

1. Extension of the modes of operation through assignment of new values in the Mode field (see [section 3.1 of \[RFC4656\]](#)), while retaining backward compatibility with TWAMP [[I-D.ietf-ippm-twamp](#)] implementations. These values identify the ability of the Server/Session-Reflector to reflect specific octets of Packet Padding back to the Client/Sender. The motivation for this extension is to permit the Sender to tag packets with a index for

simplified identification, or other uses.

(other items may be added)

When new features are discussed and reach consensus, they may become chartered work items in IETF IPPM (and may appear in a different memo).

[3.](#) TWAMP Control Extensions

TWAMP-Control protocol is a derivative of the OWAMP-Control protocol,

Morton & Ciavattone

Expires January 7, 2009

[Page 3]

Internet-Draft

TWAMP Reflect Padding

July 2008

and provides two-way measurement capability. TWAMP [\[I-D.ietf-ippm-twamp\]](#) uses the Mode field to identify and select specific communication capabilities, and this field is a recognized extension mechanism. The following sections describe one such extension.

[3.1.](#) Connection Setup with Reflect Padding Feature

TWAMP connection establishment follows the procedure defined in [section 3.1 of \[RFC4656\]](#). The Reflect Padding feature requires two new bit positions (and values) to identify the ability of the Server/Session-Reflector to reflect specific octets of Packet Padding back to the Client/Sender. With this added feature, the complete set of TWAMP mode values would be as follows:

Value	Description	Reference/Explanation
0	Reserved	
1	Unauthenticated	RFC4656, Section 3.1
2	Authenticated	RFC4656, Section 3.1
4	Encrypted	RFC4656, Section 3.1
8	Unauth. TEST protocol, Auth. CONTROL	draft-...-more-twamp (3)
16	Unauth. TEST protocol, Encrypted CONTROL	draft-...-more-twamp (4)
32	Auth. TEST protocol, Encrypted CONTROL	draft-...-more-twamp (5)

xx	Reflect Padding Capability	new bit position (X)

yyy	Reflect & Operate on Padding Bits	new bit position (Y)
-----	--------------------------------------	----------------------

In the original OWAMP mode field, setting bit positions 0, 1 or 2 indicated the security mode of the Control protocol, and the Test protocol inherited the same mode (see [section 4 of \[RFC4656\]](#)). In the [\[I-D.morton-ippm-more-twamp\]](#) bit positions (3, 4 or 5) discontinue the inheritance of the security mode in the Test protocol.

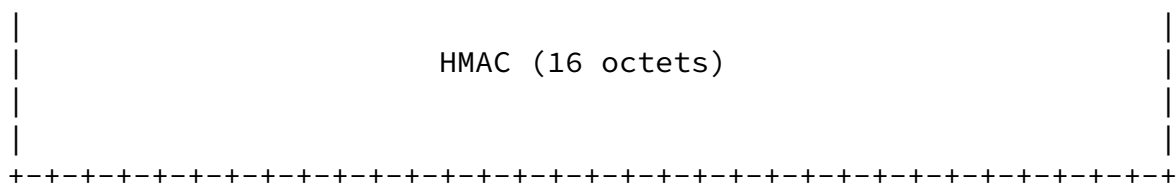
The Server sets one or both of the new bit positions (possibly 6 and/or 7) in the Server Greeting message to indicate its capabilities and willingness to operate in these modes if desired.

If the Control-Client intends to operate all test sessions under this control connection using one of the new modes, it **MUST** set one of mode bits corresponding to that mode in the Setup Response message.

3.2. Request-TW-Session Packet Format

The bits designated for the Reflect Padding feature in the Request-TW-Session command are as shown in the packet format below.

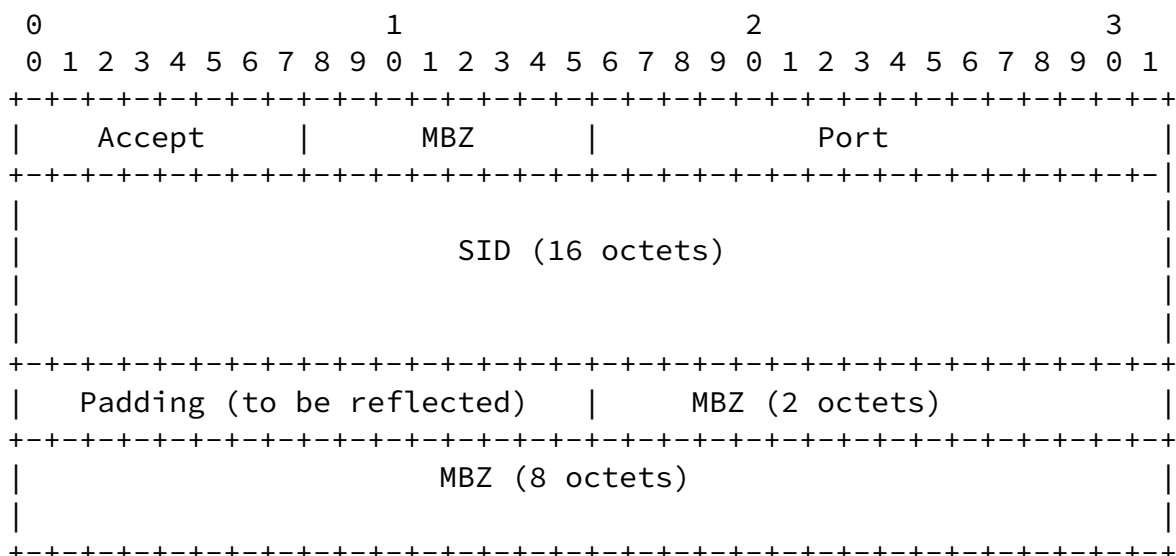
[illegible]

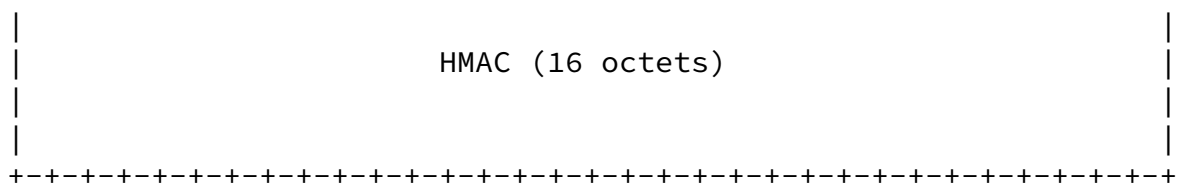


The "Packet Padding (to be reflected)" field SHALL be 2 octets long, as shown.

3.3. Accept Session Packet Format

The bits designated for the Reflect Padding feature in the Accept Session command are as shown in the packet format below.





The "Packet Padding (to be reflected)" field SHALL be 2 octets long, as shown.

[3.4.](#) Additional considerations

The value of the Modes field sent by the Server (in the Server Greeting message) is the bit-wise OR of the mode values that it is willing to support during this session.

If BOTH the above modes are adopted, the last eight bits of the Modes 32-bit field are used. The first 24 bits MUST be zero. A client conforming to this version of the specification MUST ignore the values in the first 24 bits of the Modes value. (This way, the bits are available for future protocol extensions.)

Other ways in which TWAMP extends OWAMP are described in [\[I-D.ietf-ippm-twamp\]](#).

[4.](#) Extended TWAMP Test

The TWAMP test protocol is similar to the OWAMP [\[RFC4656\]](#) test protocol with the exception that the Session-Reflector transmits test packets to the Session-Sender in response to each test packet it receives. TWAMP [\[I-D.ietf-ippm-twamp\]](#) [section 4](#) defines two additional test packet formats for packets transmitted by the

Session-Reflector. The appropriate format depends on the security mode chosen. This feature utilizes some of the bits within each test packet format.

[4.1.](#) Sender Behavior

This section describes extensions to the behavior of the TWAMP Session-Sender.

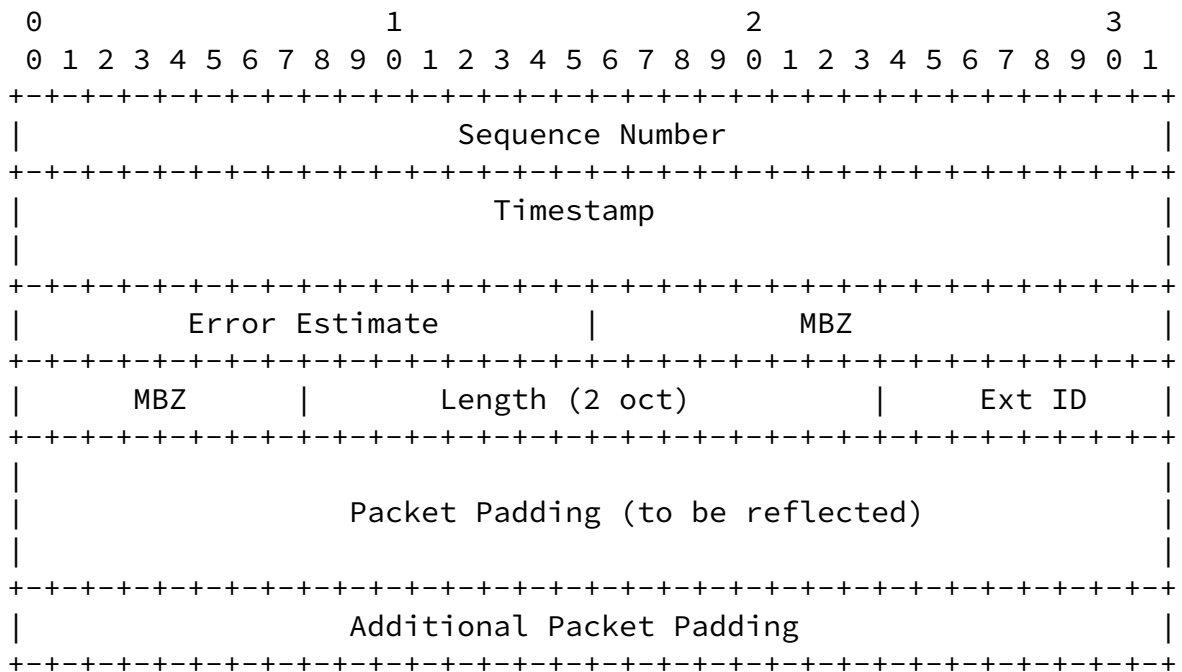
4.1.1. Packet Timings

The Send Schedule is not utilized in TWAMP, and this is unchanged in this memo.

4.1.2. Packet Format and Content

The Session-Sender packet format and content follow the same procedure and guidelines as defined in [section 4.1.2 of \[RFC4656\]](#) (as indicated in [section 4.1.2](#) of TWAMP [\[I-D.ietf-ippm-twamp\]](#)).

The Reflect Padding feature re-designates the packet padding field, as shown below for unauthenticated mode:



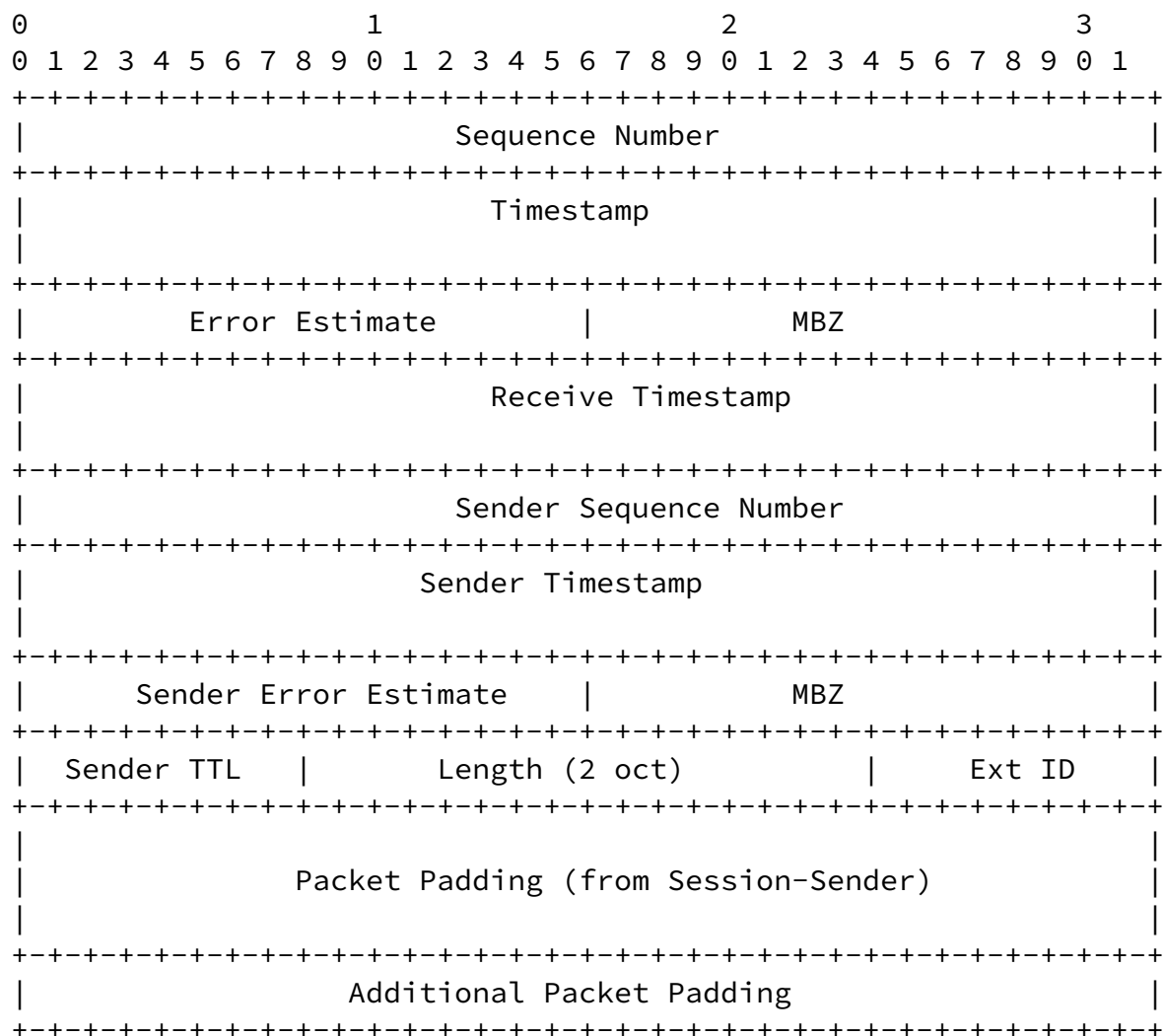
The "Packet Padding (to be reflected)" field MAY be as long as 12 octets, as shown. IF the test packet length is truncated within this field, THEN ALL packet padding MUST be reflected by Session-Reflectors using this feature.

4.2. Reflector Behavior

The TWAMP Reflector follows the procedures and guidelines in [section 4.2](#) of [I-D.ietf-ippm-twamp], with the following additional functions:

- o bits in the packet padding field of the Session-Sender's test packet MUST be inserted in the Session-Reflector's test packet.

The Reflect Padding feature re-designates the packet padding field, as shown below for unauthenticated mode:



The "Packet Padding (to be reflected)" field MAY be as long as 12 octets, as shown. IF the test packet length is truncated within this field, THEN ALL packet padding MUST be reflected by Session-Reflectors using this feature.

[5.](#) Security Considerations

These extended modes of operation permit stronger integrity protection on the TWAMP-Control protocol while simultaneously emphasizing accuracy or efficiency on the TWAMP-Test protocol, thus enhancing overall security when compared to the previous options.

The security considerations that apply to any active measurement of live networks are relevant here as well. See [\[RFC4656\]](#) and [\[I-D.ietf-ippm-twamp\]](#).

[6.](#) IANA Considerations

This memo adds two mode combinations to the IANA registry for the TWAMP Mode field, and describes behavior when the new modes are used. This field is a recognized extension mechanism for TWAMP.

[6.1.](#) Registry Specification

IANA has created a TWAMP-Modes registry (as requested in [\[I-D.morton-ippm-more-twamp\]](#)). TWAMP-Modes are specified in TWAMP Server Greeting messages and Set-up Response messages, as described in section 3.1 of [\[I-D.ietf-ippm-twamp\]](#), consistent with [section 3.1 of \[RFC4656\]](#), and extended by this memo. Modes are indicated by setting bits in the 32-bit Modes field. Thus, this registry can contain a total of 32 possible values.

[6.2.](#) Registry Management

Because the Modes registry can contain only thirty-two values, and because TWAMP is an IETF protocol, this registry must be updated only by "IETF Consensus" as specified in [\[RFC2434\]](#) (an RFC documenting registry use that is approved by the IESG). For the Modes registry, we expect that new features will be assigned using monotonically increasing bit positions and in the range [0-31] and the corresponding values, unless there is a good reason to do otherwise.

[6.3.](#) Experimental Numbers

No experimental values are currently assigned for the Modes Registry.

[6.4.](#) Registry Contents

TWAMP Modes Registry is recommended to be augmented as follows:

Internet-Draft

TWAMP Reflect Padding

July 2008

Value	Description	Semantics Definition
0	Reserved	
1	Unauthenticated	RFC4656, Section 3.1
2	Authenticated	RFC4656, Section 3.1
4	Encrypted	RFC4656, Section 3.1
8	Unauth. TEST protocol, Auth. CONTROL	draft-...-more-twamp (3)
16	Unauth. TEST protocol, Encrypted CONTROL	draft-...-more-twamp (4)
32	Auth. TEST protocol, Encrypted CONTROL	draft-...-more-twamp (5)

xx	Reflect Padding Capability	this memo, section 3.1 new bit position (X)
yyy	Reflect & Operate on Padding Bits	this memo, section 3.1 new bit position (Y)

[7.](#) Acknowledgements

The authors would like to thank future readers for helpful review and comments.

[8.](#) References

[8.1.](#) Normative References

[I-D.ietf-ippm-twamp]

Babiarz, J., "A Two-way Active Measurement Protocol (TWAMP)", [draft-ietf-ippm-twamp-08](#) (work in progress), June 2008.

[I-D.morton-ippm-more-twamp]

Morton, A. and K. Hedayat, "More Features for TWAMP",

[draft-morton-ippm-more-twamp-00](#) (work in progress),
February 2008.

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.

Morton & Ciavattone

Expires January 7, 2009

[Page 10]

Internet-Draft

TWAMP Reflect Padding

July 2008

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", [RFC 4656](#), September 2006.

[8.2](#). Informative References

[x] "".

Authors' Addresses

Al Morton
AT&T Labs
200 Laurel Avenue South
Middletown,, NJ 07748
USA

Phone: +1 732 420 1571
Fax: +1 732 368 1192
Email: acmorton@att.com
URI: <http://home.comcast.net/~acmacm/>

Len Ciavattone
AT&T Labs
200 Laurel Avenue South
Middletown,, NJ 07748
USA

Phone: +1 732 420 1239
Fax:
Email: lencia@att.com

URI:

Morton & Ciavattone

Expires January 7, 2009

[Page 11]

Internet-Draft

TWAMP Reflect Padding

July 2008

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.