IETF Criteria For Evaluating Reliable Multicast Transport and Application Protocols

Status of this Memo

This document is an Internet Draft. 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. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the internet-drafts Shadow Directories on:

- ftp.is.co.za (Africa)
- nic.nordu.net (Europe)
- ds.internic.net (US East Coast)
- ftp.isi.edu (US West Coast)
- munnari.oz.au (Pacific Rim)

Abstract

This memo describes the procedures for reviewing reliable multicast protocols within the Transport Area (TSV) of the IETF. They are temporary procedures. The Area Directors expect to be able to charter one or more WGs for standards track reliable multicast within a year or 18 months, as the procedures described herein help the transport and applications communities to identify and resolve the most serious technical problems with reliable multicast.

Within today's Internet, important applications exist for a reliable multicast service. Some examples that are pulling reliable multicast technology are collaborative workspaces (such as whiteboard), data and software distribution, and (more speculatively) web caching protocols. However, the technology for accomplishing
reliable multicast in the Internet is not well-understood at the current
time. Due to the nature of the technical issues, a single commonly
accepted technical solution that solves all the demands for reliable
multicast is infeasible.

A number of reliable multicast protocols have already been
invented to solve a variety of problems for various types
of applications (See Bibliography). How should these protocols
be treated within the IETF and how should the IETF guide
the development of reliable multicast in a direction beneficial
for the general Internet?

The TSV Area Directors and their Directorate have outlined a set of
review procedures that address these questions and set criteria
and processes for the publication as RFCs of internet-drafts on
reliable multicast transport or reliable multicast applications.

1.0 Background on IETF Processes and Procedures

In the IETF, work in an area is directed and managed by the Area
Directors (ADs), who have authority over the chartering of
working groups (WGs).

In addition, ADs review individually submitted (not by WGs)
internet-drafts about work that is relevant to their area
prior to publication as RFCs (Experimental,
Informational or, in rare cases, Standards Track). The review
is done according to the guidelines set out in the Internet
Standards Process, RFC 2026 [InetStdProc96].

The purpose of this Internet-Draft is to present
in advance the criteria that will be used by the
TSV ADs in reviewing reliable multicast internet-drafts.

2.0 Introduction

There is a strong application pull for reliable multicast.
Widespread use of the Internet makes the economy of multicast
transport important. Current Internet multicast offers
a best-effort many-to-many delivery
service and offers no guarantees. While many types of
applications lend themselves to the group-delivery model of
multicast, they require some kind of reliability, which is not
offered by IP multicast. Applications wishing to use a
reliable multicast include collaborative applications,
distributed interactive simulations, and distribution services
(e.g. netnews).

To meet the growing demand for reliable multicast, many reliable
multicast protocols have been proposed [Obraczka96, Multicast
Transport Protocols, Reliable Multicast Protocols, Overview of RM].

However, as we discuss in Section 3, the issues raised by reliable
multicast are considerably more complex than those related to
reliable unicast. In particular, reliable multicast protocols can
do damage in the Internet, through causing congestion disasters
if they are used popularly before they are well-engineered. Because
of the complexity of the technical issues, and the abundance of
proposed solutions, we are putting in place more well-defined review
procedures than usual. We compare this action with an IESG action
taken in 1991, RFC 1264 [], when community experience with standard
Internet dynamic routing protocols was still limited, and extra
review was deemed necessary to assure that the protocols introduced
would be effective, correct and robust.

Section 3 describes in detail the nature of the particular challenges
posed by reliable multicast. Section 4 describes the process for
considering reliable multicast solutions. Section 5 details the
additional requirements that need to be met by proposals to be advanced
to RFC status.

3.0 Issues in Reliable Multicast

Two aspects of reliable multicast make standardization particularly
challenging. First, the meaning of reliability varies in the context of
different applications. Secondly, if special care is not taken, reliable
multicast protocols can cause a particular threat to the operation
of the global Internet. These issues are discussed in detail in this
section.

3.1 One or Many Reliable Multicast Protocols or Frameworks?

Unlike reliable unicast, where a single transport protocol (TCP) is
currently used to meet the reliable delivery needs of a wide range of
applications, reliable multicast does not necessarily lend itself to
a single application interface or to a single underlying set of
mechanisms. For unicast transport, the requirements for reliable,
sequenced data delivery are fairly general. TCP, the primary
transport protocol for reliable unicast, is a mature protocol with
delivery semantics that suit a wide range of applications.

In contrast, different multicast applications have widely different
requirements for reliability. For example, some applications
require that message delivery obey a total ordering while others do
not. Some applications have many or all the members sending data
while others have only one data source. Some applications have
replicated data, for example in an n-redundant file store, so that
several members are capable of transmitting a data item while for
others all data originates at a single source. Some applications
are restricted to small fixed-membership multicast groups, while
other applications need to scale dynamically to thousands or tens of
thousands of members (or possibly more). Some applications have
stringent delay requirements, while others do not. Some
applications such as file-transfer are high-bandwidth, while other
applications such as interactive collaboration tools are more likely
to be bursty but use low bandwidth overall. These requirements each
impact the design of a reliable multicast protocol in a different
way.

In addition, even for a specific application where the application’s
requirements for reliable multicast are well understood, there are
many open questions about the underlying mechanisms for providing
reliable multicast. A key question concerns the robustness of the
underlying reliable multicast mechanisms as the number of senders or
the membership of the multicast group grows.

One challenge to the IETF is to end up with the right match between
applications’ requirements and reliable multicast mechanisms. While
there is general agreement that a single reliable multicast protocol
or framework is not likely to meet the needs of all Internet applications, there is less understanding and agreement about the exact relationship between application-specific requirements and more generic underlying reliable multicast protocols or mechanisms. There are also open questions about the appropriate integration between an application and an underlying reliable multicast framework, and potential generality of a single applications interface for that framework.

3.2 Congestion Control

A particular concern for the IETF (and a dominant concern for the Transport Services Area) is the impact of reliable multicast traffic on other traffic in the Internet in times of congestion (more specifically, the effect of reliable multicast traffic on competing TCP traffic). The success of the Internet relies on the fact that best-effort traffic responds to congestion on a link (as currently indicated by packet drops) by reducing the load presented on that link. Congestion collapse in today’s Internet is prevented only by the congestion control mechanisms in TCP [Jacobson88, HostReq89, Stevens96].

There are a number of reasons to be particularly attentive to the congestion-related issues raised by reliable multicast proposals. Multicast applications in general have the potential to do more congestion-related damage to the Internet than do unicast applications. This is because a single multicast flow can be distributed along a large, global multicast tree reaching throughout the entire Internet.

Further, reliable multicast applications have the potential to do more congestion-related damage than do unreliable multicast applications. First, unreliable multicast applications such as audio and video are, at the moment, usually accompanied by a person at the receiving end, and people typically unsubscribe from a multicast group if congestion is so heavy that the audio or video stream is unintelligible. Reliable multicast applications such as group file transfer applications, on the other hand, are likely to be between computers, with no humans in attendance monitoring congestion levels.

In addition, reliable multicast applications do not necessarily have the natural time limitations typical of current unreliable multicast applications. For a file transfer application, for example, the data transfer might continue until all of the data is transferred to all of the intended receivers, resulting in a potentially-unlimited duration for an individual flow. Reliable multicast applications also have to contend with a potential explosion of control traffic (e.g., ACKs, NACKs, status messages), and with control traffic issues in general that may be more complex than for unreliable multicast traffic.

The design of congestion control mechanisms for reliable multicast for large multicast groups is currently an area of active research. The challenge to the IETF is to encourage research and implementations of reliable multicast, and to enable the needs of applications for reliable multicast to be met as expeditiously as possible, while at the same time protecting the Internet from the congestion disaster or collapse that could result from the widespread use of applications with inappropriate reliable multicast
mechanisms. Because of the setbacks and costs that could result from the widespread deployment of reliable multicast with inadequate congestion control, the IETF must exercise care in the standardization of a reliable multicast protocol that might see widespread use.

The careful review and cautious acceptance procedures for proposals submitted as internet-drafts reflects our concern to meet the challenges described here.

4. IETF Process for Review and Publication of Reliable Multicast Protocol Specifications

In the general case of individually submitted internet-drafts (proposals not produced by an IETF WG), the process of publication as some type of RFC is described in RFC 2026 (4.2.3) [InetStdProc96]. This specifies that if the submitted internet-draft is closely related to work being done or expected to be done in the IETF, the ADs may recommend that the document be brought within the IETF and progressed in the IETF context. Otherwise, the ADs may recommend that the Internet-Draft be published as an Experimental or Informational RFC, with or without an IESG annotation of its relationship to the IETF context.

The procedure for Reliable Multicast proposal publication will have as its default RFC status Experimental, when the technical criteria listed in Section 5 are deemed to be fulfilled. Both the criteria and the procedure reflect the ADs’s technical assessment of the current state of reliable multicast technology. It does not reflect the origins of the proposals, which we expect will be equally from commercial vendors with initial products and from researchers.

Work on the development and engineering of protocols that may eventually meet the review criteria could take place either in an IRTF Research Group or a focused short IETF WG with an Experimental product.

When the work in reliable multicast technology has matured enough to be considered for standardization within the IETF, the TSV Area will charter appropriate standards track WGs. The criteria for evaluation of standards track products will be at least as stringent as those described herein (next section).

5. Technical Criteria for Reliable Multicast

The internet-draft must:

a. Analyze the behavior of the protocol.

The vulnerabilities and performance problems must be shown through analysis. Especially the protocol behavior must be explained in detail with respect to scalability, congestion control, error recovery, and robustness.

For example the following questions should be answered:

How scalable is the protocol to the number of users in a group, number of groups, wide dispersion of group members? If appropriate, how scalable is the protocol to the number of senders?
Identify the mechanisms which limit scalability and estimate those limits.

How does the protocol protect the Internet from congestion? How well does it perform? When does it fail?

Under what circumstances will the protocol fail to perform the functions needed by the applications it serves?

Is there a congestion control mechanism? How well does it perform? When does it fail?

b. Include a description of trials and/or simulations which support the development of the protocol and the answers to the above questions.

c. Include an analysis of whether the protocol has congestion avoidance mechanisms strong enough to cope with deployment in the Global Internet, and if not, clearly document the circumstances in which congestion harm can occur. How are these circumstances to be prevented?

d. Include a description of any mechanisms which contain the protocol within limited network environments. It is likely that some answers to a. and c. will mean that such mechanisms are required. We recognize that the confinement of internet applications is an open research area.

e. Show that the protocol can use IPSEC or other mechanisms for secure operation. (General requirement with specific ramifications for reliable multicast that are outside the scope of this memo).

Comments on these criteria, additions to them, or refinements are welcome, and should be sent to the Transport Services Area (trans-area@isi.edu).

6. References


