Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 13 November 2026

N. Karstens
Garmin
S. Cheshire
Apple Inc.
M. McBride
Futurewei

12 May 2026

The Multicast Application Port
draft-ietf-intarea-multicast-application-port-05

Abstract

This document discusses the drawbacks of the current practice of assigning a UDP port to each multicast application. Such assignments are redundant because the multicast address already uniquely identifies the data. The document proposes assigning a UDP port specifically for use with multicast applications and lists requirements for using this port. This approach provides immediate compatibility with existing protocol stacks, while also requiring improvements to make the port easier to use.

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/.

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."

This Internet-Draft will expire on 13 November 2026.

Copyright Notice

Table of Contents

1. Introduction

The Internet community has recognized the need to be judicious when assigning port numbers (see [RFC7605], Section 6). With unicast applications, the need for explicit port assignment has been reduced by techniques such as locally assigning a dynamic port, combined with some mechanism for advertising that port (see [RFC7605], Section 7.1). Dynamic assignment does not work with multicast applications because it is impossible to guarantee that the port remains unused by all hosts that may want to join a given multicast group. The result is that each multicast application-layer protocol has had to have its own dedicated port assignment. Even worse, each different use of that multicast application-layer protocol has had to have a different unique port assigned.

In the TCP/IP model, the port number in the transport layer multiplexes applications within a host (see [RFC1122], Section 4.1.1 and [RFC7605], Section 5). With Any-Source Multicast (ASM), the use of a port number to multiplex applications is unnecessary because the destination multicast address already provides a unique identifier for the application. The same applies to Source-Specific Multicast (SSM) if both source address and destination multicast address are considered.

Because of the desire to conserve port numbers and the fact that a port is not necessary to multiplex multicast applications, this document assigns a UDP port that may be used with multicast applications: the Multicast Application Port.

Assigning a UDP port for multicast applications (as opposed to other methods) provides immediate compatibility with existing network protocol stacks. Section 3 contains requirements that facilitate use of the port on a given platform, but incorporating these requirements into existing platforms is expected to be a gradual process.

Use of this port is optional because there may be circumstances where assigning a port is preferred, such as when participants cannot meet the requirements in Section 3 and Section 4, or when a firewall blocks a traffic pattern used by the application (see Section 5).

An application may use this port in conjunction with a unicast port to balance out deficiencies related to multicast distribution (see [RFC9119], for example).

1.1. Requirements Language

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.

2. Assignment

This document _requests_ assignment of UDP port 8738 (0x2222) and gives it the service name "mcast-app-port".

Applications using the Multicast Application Port are identified by the destination multicast address (ASM) or by the combination of source address and destination multicast address (SSM). As such, the Multicast Application Port SHALL NOT be used as either a source port or destination port for any non-multicast messages.

The Multicast Application Port MAY be used as a source port by an application that exclusively uses multicast messages. If any application messages are unicast, then a different port SHOULD be used for the source port. This allows receivers to know which port to send replies to. Such arrangements would likely require receivers to use multiple sockets, as the application would need to bind to multiple ports.

3. Host Requirements

Hosts SHALL require applications using this port to use it non-exclusively. In practice, this means hosts using POSIX-like socket APIs would require applications to set the SO_REUSEADDR and/or SO_REUSEPORT socket options before binding the socket [POSIX]. This ensures that applications developed on a conformant host will also work on a non-conformant host.

Hosts SHALL prevent use of the port with the wildcard address (see [RFC3493], Section 3.8) by having the socket bind operation return an error code.

Hosts SHALL prevent applications from sending non-multicast packets using the Multicast Application Port as either a source or destination port by having the send operation return an error code.

Hosts SHALL discard all incoming, non-multicast packets that use the Multicast Application Port as either a source or destination port.

4. Application Requirements

Applications running on non-conformant hosts can ensure compatibility with conformant hosts by meeting the requirements in this section.

Applications running on a non-conformant host SHALL NOT prevent other applications from using this port. In practice, this means that applications using POSIX-like socket APIs would enable the SO_REUSEADDR and/or SO_REUSEPORT socket options before binding the socket [POSIX].

Applications running on a non-conformant host SHALL discard all datagrams received on the Multicast Application Port that do not have the multicast address used by the application.

5. Firewall Considerations

Many network firewalls (which operate on network infrastructure) and host firewalls (which operate on individual hosts) are configured to accept incoming messages as long as there was first an outgoing message using the same set of ports (see [RFC7288] for more discussion). Consider the following sequence of messages:

1. (Multicast) Host A to group containing Host B
   Source Port: 50000 (Dynamic)
   Dest Port: 8738

2. (Unicast) Host B to Host A
   Source Port: 60000 (Dynamic)
   Dest Port: 50000

3. (Unicast) Host A to Host B
   Source Port: 50000
   Dest Port: 60000

A host firewall running on Host A (or a network firewall between Host A and Host B) may block Message 2 because it uses a different set of ports than Message 1 uses.

While a firewall could be configured to accept Message 2, this configuration would have to be automated because the use of dynamic ports makes manual configuration too costly even in small deployments. However, this automation leads to unacceptable security risks. For example, if a firewall were to respond to Message 1 by opening up the source port used in the message, a malicious application running on the host could open large holes in the firewall by repeatedly sending variations of Message 1 using different source ports.

Host firewalls could be configured to allow messages associated with a given application (instead of specific ports), but this approach would not work with a network firewall.

Ultimately, the current practice of assigning a multicast application its own port is more practical for any application that uses both multicast and unicast messages and could be deployed in an environment using firewalls. Firewall configuration with an assigned port is straightforward: allow all messages using that port.

6. Security Considerations

Firewall rules referencing ports are typically intended to match specific applications. Because applications using the Multicast Application Port are identified by both port and destination multicast address, rules referencing the Multicast Application Port SHOULD also consider the destination multicast address.

Applications running on non-conformant hosts are vulnerable to a denial of service attack if another application claims exclusive access to the port.

Systems that use POSIX-like socket APIs typically have restrictions on binding multiple sockets to the same port. This can serve as a rudimentary security mechanism in that other local applications cannot eavesdrop on the multicast stream. A necessary side-effect of

using the Multicast Application Port is that applications can no longer rely on these security mechanisms. These applications may want to incorporate additional security measures into their protocol. Note that the problem of local eavesdropping is typically no worse than eavesdropping in-flight, so it is likely that both attack vectors can be resolved by the same security measure.

7. IANA Considerations

IANA is _requested_ to assign the following port:

Service Name	mcast-app-port
Transport Protocol	UDP
Assignee	IESG <iesg@ietf.org>
Contact	IETF Chair <chair@ietf.org>
Description	Multicast Application Port
Reference	This document
Port Number	8738

IANA is requested to update its "Application for Service Names and User Port Numbers" [IANA-APP] to reference this document and ask if the Multicast Application Port may be used.

8. Acknowledgement

Special thanks to the National Marine Electronics Association for their contributions in developing marine industry standards and their support for this research.

The authors are grateful to the members of the PIM and INT-AREA working groups for their review of this draft, and to the following individuals specifically:

* Dr. Joe Touch for consulting on port assignment

* Lorenzo Colitti for his suggestions for host requirements

* David Schinazi for pointing out likely port conflicts with several major OSes

* Juliusz Chroboczek for suggestions on the source port used for unicast

* Dave Thaler for insightful discussion on how the Multicast Application Port would operate in the presence of a firewall

9. References

9.1. Normative References

[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/info/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/info/rfc8174>.

9.2. Informative References

[IANA-APP] Internet Assigned Numbers Authority, "Application for Service Names and User Port Numbers", <https://www.iana.org/form/ports-services>.

[POSIX] The Open Group, ""The Open Group Base Specifications", Issue 7, 2018 edition", December 2001, <https://pubs.opengroup.org/onlinepubs/9699919799/>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <https://www.rfc-editor.org/info/rfc1122>.

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, DOI 10.17487/RFC3493, February 2003, <https://www.rfc-editor.org/info/rfc3493>.

[RFC7288] Thaler, D., "Reflections on Host Firewalls", RFC 7288, DOI 10.17487/RFC7288, June 2014, <https://www.rfc-editor.org/info/rfc7288>.

[RFC7605] Touch, J., "Recommendations on Using Assigned Transport Port Numbers", BCP 165, RFC 7605, DOI 10.17487/RFC7605, August 2015, <https://www.rfc-editor.org/info/rfc7605>.

[RFC9119] Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Z炭単iga, "Multicast Considerations over IEEE 802 Wireless Media", RFC 9119, DOI 10.17487/RFC9119, October 2021, <https://www.rfc-editor.org/info/rfc9119>.

Authors' Addresses

Nate Karstens
Garmin International, Inc.
1200 E. 151st St.
Olathe, KS 66062-3426
United States of America
Email: nate.karstens@gmail.com

Stuart Cheshire
Apple Inc.
Email: cheshire@apple.com

Mike McBride
Futurewei
United States of America
Email: michael.mcbride@futurewei.com