

Internet Draft
Document: [draft-ietf-mboned-ipv4-mcast-
unusable-01.txt](#)
Expires: June 2004

B. Nickless
Argonne National
Laboratory
December 2003

IPv4 Multicast Unusable Group And Source Addresses

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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>.

2. Abstract

Some IPv4 multicast datagrams should not be routed, either within an administrative domain or between administrative domains. A list of those restrictions is supplied here. These restrictions SHOULD be respected by IPv4 multicast applications and included in network device access control lists. IANA should permanently reserve certain address ranges.

3. Table of Contents

<u>1.</u> Status of this Memo.....	<u>1</u>
<u>2.</u> Abstract.....	<u>1</u>
<u>4.</u> Conventions used in this document.....	<u>2</u>
<u>5.</u> Background.....	<u>2</u>
<u>6.</u> Specific (Source,Group) Restrictions.....	<u>2</u>
<u>7.</u> Unusable Locally.....	<u>4</u>
<u>8.</u> Unusable Inter-domain.....	<u>4</u>
<u>9.</u> No Flooding of Knowledge of Active Sources.....	<u>5</u>

10.	IANA Considerations.....	6
11.	Security Considerations.....	6
Nickless	Informational - Expires June 2004	1
	IPv4 Multicast Unusable Group	December 2003
	And Source Addresses	
12.	Acknowledgements.....	6
13.	References.....	6
12.	Author's Address.....	7

[4.](#) Conventions used in this document

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](#)].

[5.](#) Background

IPv4 multicast [[MCAST](#)] is an internetwork service that allows IPv4 datagrams sent from a source to be delivered to one or more interested receiver(s). That is, a given source sends a packet the network with a destination address 224/4 CIDR [[CIDR](#)] range. The network transports this packet to all receivers (replicated where necessary) that have registered their interest in receiving these packets.

Some combinations of Source Address and Group Address SHOULD NOT be routed for various reasons. This note describes those restrictions so they can be:

- Avoided by applications, especially those that choose multicast groups on a random or ad-hoc basis.
- Properly reflected in network device restriction lists.
- Reserved by IANA.

[6.](#) Specific (Source,Group) Restrictions

Following is a list of (Source,Group) ranges that should not be used or routed in certain circumstances. Each range is associated with a brief explanation and a cross-reference to a fuller explanation to be found in following sections of this note.

(*,224.0.1.2/32)	SGI-Dogfight	Section 8.4
(*,224.0.1.3/32)	Rwhod	Section 8.5
(*,224.0.1.22/32)	SVRLOC	Section 8.4
(*,224.0.1.24/32)	Microsoft-DS	Section 8.4
(*,224.0.1.35/32)	SVRLOC-DA	Section 8.5

(* ,224.0.1.39/32)	CISCO-RP-ANNOUNCE	Section 8.5
(* ,224.0.1.40/32)	CISCO-RP-DISCOVERY	Section 8.5
(* ,224.0.1.60/32)	HP-DEVICE-DISC	Section 8.5
(* ,224.0.2.2/32)	SUN-RPC	Section 8.4
(* ,224.77.0.0/16)	Norton Ghost	Section 8.3
(* ,224.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,225.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,225.1.2.3/32)	Altiris	Section 8.3

Nickless Informational - Expires June 2004 2
 IPv4 Multicast Unusable Group December 2003
 And Source Addresses

(* ,225.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,226.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,226.77.0.0/16)	Norton Ghost	Section 8.3
(* ,226.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,227.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,227.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,228.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,228.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,229.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,229.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,230.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,230.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,231.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,231.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,232.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,232.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,232.0.0.0/8)	Source-Specific Multicast	Section 9.1
(* ,233.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,233.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,234.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,234.42.42.42/32)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,234.142.142.42/31)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.44/30)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.48/28)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.64/26)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.128/29)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.136/30)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.140/31)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,234.142.142.142/32)	Phoenix/StorageSoft ImageCast	Section 8.3
(* ,235.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,235.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,236.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,236.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,237.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,237.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,238.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(* ,238.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1

(*,239.0.0.0/8)	Administratively Scoped Groups	Section 8.1
(*,239.0.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(*,239.128.0.0/24)	Control plane of IGMP snoopers	Section 7.1
(0.0.0.0/0,*)	Link Local Addresses	Section 8.2
(10.0.0.0/8,*)	Private Address Space	Section 8.2
(127.0.0.0/8,*)	Loopback Address Space	Section 8.2
(169.254.0.0/8,*)	Link Local Addresses	Section 8.2
(172.16.0.0/12,*)	Private Address Space	Section 8.2
(192.0.2.0/24,*)	Documentation/Example	Section 8.2
(192.168.0.0/16,*)	Private Address Space	Section 8.2

Nickless Informational - Expires June 2004 3
 IPv4 Multicast Unusable Group December 2003
 And Source Addresses

[7.](#) Unusable Locally

Multicast datagrams that match the criteria in this section SHOULD NOT be used, even on local, unrouted subnetworks.

7.1 Groups processed in the control plane of IGMP-snooping switches.

[MCAST] describes the mapping of IPv4 Multicast Group addresses to Ethernet MAC addresses, as follows:

An IP host group address is mapped to an Ethernet multicast address by placing the low-order 23-bits of the IP address into the low-order 23 bits of the Ethernet multicast address 01-00-5E-00-00-00 (hex). Because there are 28 significant bits in an IP host group address, more than one host group address may map to the same Ethernet multicast address.

Multicast group addresses in the 224.0.0.0/24 range are used for local subnetwork control. This maps to the Ethernet multicast address range 01-00-5E-00-00-XX, where XX is 00 through FF. Ethernet frames within this range are always processed in the control plane of many popular network devices, such as IGMP-snooping switches.

Because of the many-to-one mapping of IPv4 Multicast Group Addresses to Ethernet MAC addresses, it is possible to overwhelm the control plane of network devices by sending to group addresses that map into the 01-00-5E-00-00-XX (hex) range.

IGMP-snooping network devices must also flood these frames to all outgoing ports, so the damage may extend to end systems and routers.

[8.](#) Unusable Inter-domain

Multicast datagrams that match the criteria in this section SHOULD NOT be routed between administrative domains.

[Section 7](#) (Unusable Locally) is incorporated here by reference.

8.1 Administratively Scoped Addresses

[RFC 2366](#) [[ADMIN](#)] defines 239.0.0.0/8 for use within an administrative domain. As such, datagrams with group addresses that match 239.0.0.0/8 SHOULD NOT be passed between administrative domains.

8.2 Special Use IPv4 Source Addresses

[RFC 1918](#) [[PRIVATE](#)] defines certain ranges of IPv4 unicast addresses that can be used within an administrative domain. Multicast datagrams are no exception to the rule that datagrams addressed within these ranges SHOULD NOT be passed between administrative domains.

Nickless	Informational - Expires June 2004	4
	IPv4 Multicast Unusable Group	December 2003
	And Source Addresses	

127.0.0.0/8 is widely used for internal host addressing, and is generally not valid on datagrams passed between hosts.

0.0.0.0/8 and 169.254.0.0/16 are valid only in the context of local links. Such source addresses are not valid for datagrams passed between networks. [[RFC 1700](#)] [[RFC 3330](#)]

192.0.2.0/24 is reserved for documentation and example code. [[RFC 3330](#)]

8.3 Personal Computer Deployment and Control Applications

The Norton Ghost [[GHOST](#)], Phoenix/StorageSoft ImageCast [[IMCAST](#)], and Altiris [[ALTIRIS](#)] applications are used to duplicate files and filesystems from servers to clients, and to otherwise maintain groups of Personal Computers. They are intended to be used on a local subnet or within an administrative domain, but the default addresses used by the software are not within the administratively-scoped range 239.0.0.0/8 (see [Section 8.1](#) above).

8.4 Known Insecure Services

Applications that use certain multicast group addresses have been demonstrated to be vulnerable to exploitation, leading to serious security problems.

8.5 Internal Resource Discovery

Applications that use certain multicast group addresses are used to discover resources within an administrative domain.

9. No Flooding of Knowledge of Active Sources

In the absence of explicit requests by interested receivers, multicast datagrams that match the criteria in this section SHOULD NOT be transmitted across administrative domain boundaries.

The knowledge of active sources that match the criteria in this section SHOULD NOT be passed between administrative domains, for example through the operation of the Multicast Source Discovery Protocol (MSDP) [[MSDP](#)].

Sections [7](#) and [8](#) are incorporated here by reference.

9.1 Source-Specific Multicast

Multicast datagrams addressed within 232.0.0.0/8 (See [[IANA](#)]) are used in the Source-Specific Multicast regime. Interested recipients request traffic from specific sources using specific group addresses. Knowledge of active sources is not flooded throughout

Nickless	Informational - Expires June 2004	5
	IPv4 Multicast Unusable Group	December 2003
	And Source Addresses	

the Internet, as it is the responsibility of the application to discover the active sources.

10. IANA Considerations

Due to the issue outlined in [Section 7.1](#) with 233.0.0.0/24 and 233.128.0.0/24 above, IANA SHOULD NOT allocate AS 0 nor AS 32768 to any Autonomous System or Registry.

IANA SHOULD reserve the 31 address blocks referenced in [Section 7](#).

11. Security Considerations

Low to moderate multicast traffic levels, using addresses within these [Section 7.1](#) Multicast Group Address ranges, can result in severe denial of service on network devices that process frames with Ethernet MAC addresses in the 01-00-5E-00-00-XX (hex) range in the control plane.

Interdomain forwarding of multicast traffic generated by certain

multicast applications (see [Section 8.3](#)) can result in internal enterprise data being replicated far beyond that which was intended.

Interdomain forwarding of multicast traffic on certain multicast groups (see [Section 8.4](#)) can lead to compromise of host systems.

[12.](#) Acknowledgements

The author relied heavily on a list of problematic groups maintained by Cisco Systems, especially Beau Williamson and his colleagues.

Jay Ford and Alan Croswell provided references for the Norton Ghost restriction.

Leonard Giuliano, John Kristoff, Alastair Matthews, Pekka Savola, and Beau Williamson provided helpful comments, corrections, and suggestions.

This work was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

[13.](#) References

[RFC2119] [RFC 2119](#): Key Words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997.

Nickless	Informational - Expires June 2004	6
	IPv4 Multicast Unusable Group	December 2003
	And Source Addresses	

[MCAST] [RFC 1112](#): Host extensions for IP multicasting. S.E. Deering. Aug-01-1989.

[CIDR] [RFC 1519](#): Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. V. Fuller, T. Li, J. Yu, K. Varadhan. September 1993.

[ADMIN] [RFC 2365](#): Administratively Scoped IP Multicast. D. Meyer. July 1998.

[PRIVATE] [RFC 1918](#): Address Allocation for Private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear. February 1996.

[RFC 1700] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2,

[RFC 1700](#), October 1994.

[RFC 3330] "Special-Use IPv4 Addresses", IANA, [RFC 3330](#), September 2002.

[GHOST] Symantec.

<http://service2.symantec.com/SUPPORT/ghost.nsf/docid/1999033015222425>

[IMCAST] Phoenix Technologies.

<http://www.storagesoft.com/products/imagecast>

[ALTIRIS] Altiris

<http://www.altiris.com/support/docs/altirisexpress/axtechref41.pdf>

[MSDP] Multicast Source Discovery Protocol. Bill Fenner and David Meyer, Editors. Work in Progress. [draft-ietf-msdp-spec-20.txt](#)

[IANA] Internet Assigned Numbers Authority.

<http://www.iana.org/assignments/multicast-addresses>

14. Author's Address

Bill Nickless

Argonne National Laboratory

9700 South Cass Avenue #221

Argonne, IL 60439

Phone: +1 630 252 7390

Email: nickless@mcs.anl.gov

Nickless Informational - Expires June 2004

7