This memo reclassifies the address block 240.0.0.0/4 as usable address space. While the community has not concluded whether the block should be considered public or private, given the current consumption rate, it is clear that the block should not be left unused. This document also makes several recommendations on ways that current implementations of the IP protocol stack will need to be modified to make this address space usable.
1. Introduction

Recent estimates [1] indicate that the Internet Assigned Numbers Authority (IANA) will exhaust the unallocated pool of 32-bit IPv4 addresses some time sometime between 2008 and 2010. As that time rapidly approaches, the Internet community must consider what it should do with address space currently reserved for future use. [RFC3330] states that the address range 240.0.0.0/4 is reserved for future use. There are several possible uses of this block. One would be to reclassify the block as private address space, as defined in [RFC1918], so that large private organizations that have outgrown the other private blocks have additional room for network expansion. Another possibility is for the address space to be made available for public Internet use. A decision on which of these alternatives (if either) is chosen requires additional analysis and debate; what is clear, though, is that today’s IP protocol stack implementations will need to be modified to support any use of the currently-reserved space as most today return errors when such addresses are used.

This memo requires implementors to make the changes necessary to receive, transmit, and forward packets that contain addresses in this block as if they were within any other unicast address block.

It is envisioned that the utility of this block will grow over time. Some devices may never be able to use it as their IP implementations have no update mechanism. This is not to say that the block will find no use. For example, home implementations that make use of network address translation [RFC2766] can also make use of this range as their public facing address once the resources that people wish to access have been updated. Similarly, an organization building a new, private network (one with no need to communicate with other parts of the Internet), may benefit from the availability of this address space.

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 [RFC2119].

2. Implementation considerations

At the present time, most IP implementations consider any IP address in the range 240.0.0.0 through 255.255.255.255 to be invalid as the source or destination of a datagram. The check for such "illegal" addresses may occur in many places, including at datagram receipt, before IP datagram transmission, when an IP address is assigned to a network interface, or even by router and firewall configuration parsers. Because 240.0.0.0/4 is henceforth reclassified as usable
address space, implementations MUST treat this range as they would any other unicast address range. Implementors should review their implementation for these and other restrictions on the use of 240.0.0.0/4 and remove as appropriate.

How the check is implemented may vary, but a common method is to treat the IP address as a 32-bit quantity in network byte order, performing a logical AND operation with the value hexadecimal F0000000, and testing to see if the result is hexadecimal F0000000. If the test succeeds, the address is rejected.

Note that the broadcast address, 255.255.255.255, still must be treated specially in each case: it is illegal as a source IP address, it is illegal as an network interface address, and it matches the local system when used as the destination address in a received datagram.

3. Implementation status

As of the release of the second version of this draft, Apple OSX has been confirmed to support the use of 240.0.0.0/4 as unicast address space. Changes have been incorporated into recent versions of Sun Solaris and have been submitted for inclusion in the Linux kernel tree. No plans have been announced for modifications to any version of Microsoft Windows, in part because of uncertainty over how to perform 6-to-4 tunneling in the absence of a definitive statement on whether 240.0.0.0/4 is "public" or "private" space.

4. Security Considerations

The reclassification of 240.0.0.0/4 as a unicast block presents the same security issues as any other unicast block, with the possible addition that attackers may attempt to exploit poorly developed security software that cannot handle the change. The authors have not explored whether such implementations exist.

5. IANA Considerations

Although this memo requires implementations to treat addresses in the range 240.0.0.0/4 the same as any other unicast addresses, it does not change the "reserved" status of the 240.0.0.0/4 address block. The IANA is requested to continue to reserve this block for future use, with the understanding that future standards action will define how it is to be allocated.
6. References

6.1. Normative References


6.2. Informative References


URIs


Appendix A.  Changes

Authors' Addresses

Vince Fuller
Cisco Systems
Tasman Drive
San Jose, CA  95134
USA
Email: vaf@cisco.com

Eliot Lear
Cisco Systems
Glatt-com, 2nd Floor
Glattzentrum, Zurich  8301
Switzerland
Email: lear@cisco.com
David Meyer
Cisco Systems
Tasman Drive
San Jose, CA 95134
USA
Email: dmm@cisco.com