IPv6 Address/Mask Notation
draft-lubashev-ipv6-addr-mask-00

Abstract

With significantly longer IPv6 address prefixes assigned to ISPs, operators sometimes find opportunities to assign special meaning to lower-order bit patterns. Often, these bit patterns cannot be expressed as an address prefix.

This RFC introduces IPv6 Address/Mask notation that allows one to express address groupings beyond "all addresses that share a single prefix". The notation is similar to the IPv4 Address/Mask notation in its expressiveness, but its syntax is derived from the traditional Address/Prefix-length notation. The traditional Address/Prefix-length notation is a special case of the Address/Mask notation.

For example, using this notation, both 2001:db8::/32 and 2001:db8::ffff:ffff:: have the same meaning. However, the following requires the new notation: 2001:db8::1234/ffff:ffff::ffff or, equivalently, 2001:db8::1234/32+::ffff.

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 http://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 September 28, 2017.

Copyright Notice
1. Introduction

In the days of IPv4, we have learned to think of IP address groupings in terms of CIDR blocks, because virtually all logical address groupings fit that model well: IP address allocations, subnets, routing announcements, etc.

With the move to IPv6, the primary mechanism for matching on addresses remains matching by prefix length, albeit with longer prefix lengths. This only allows for strictly hierarchical address groupings. The longer address lengths, however, provide opportunities for assigning semantics to bit strings within addresses beyond the prefix. Here we define a syntax for specifying groupings (matching rules) of IPv6 addresses where a set of less-significant bits have a particular value. For example, 2001:dba8::1234/ffff:ffff:ffff would match on any addresses starting with 2001:dba8::/32 and ending with the last 16 bits being ::1234.
1.1. Netmask and Prefix Length Notations

There are two common notations for identifying groups of addresses (networks, subnets, internet routing blocks). These notations can also be used to identify a single host and its subnet.

The netmask notation described by [RFC0950] is commonly used for IPv4. It consists of a tuple of a network address and a network mask. For example: 198.51.100.4 netmask 255.255.255.0.

The prefix-length notation described by [RFC4632] is commonly used for both IPv4 and IPv6. It consists of a tuple of a network address and a prefix length. For example: 198.51.100.4/24 or 2001:db8::1234/32.

Depending on the context, netmask and prefix length notations can specify either a "group of addresses" or "a group of addresses and a specific address within that group". If the network address contains one or more set bits not selected by the network mask or prefix length, then network address specifies a host address in addition to the subnet. For example: 198.51.100.4/24 means "host 198.51.100.4 within a group of hosts 198.51.100.0 - 198.51.100.255".

2. Problem Description

The problem with the prefix length notation for IPv6 is that it is not sufficiently expressive of IPv6 address groupings for a growing number of applications.

IPv6 allocation guidelines [RFC6177] guarantee at least /48 allocation to network operators. Because these address blocks are orders of magnitude larger than any imaginable number of physical hosts, network operators are managing those addresses in new and creative ways. Sometimes, useful address grouping are not "all addresses that share a prefix of a certain length". Additionally, within an administrative scope, there are use-cases where semantics are assigned to individual bits or series of bits.

Consider these examples:

1. Allocating a block of addresses to each host and using the least significant bits to specify traffic class or prioritization information. These operators may need a way to express a rule that applies to all traffic of a particular traffic class. For example, an operator may route an address prefix to a physical server or virtual machine host and then use less significant bits to indicate an application, virtual machine guest, or TLS certificate.
2. Using "middle" bits of IPv6 addresses to specify traffic class or prioritization information, leaving less significant bits to identify sites and individual hosts. While only applicable with an administrative scope, these operators need a way to express both rules that apply to particular hosts as well as to particular traffic classes. For example, a corporate network environment may use a prefix per-site but then use the next bits to indicate whether a subnet is a lab, guest wireless, production environment, or other.

3. Network operators managing multiple similar data centers may have different prefixes routed to those data centers but desire a unified set of rules for assigning, managing, and routing IPv6 addresses within those data centers. These operators need to express rules that do not depend on the prefixes of the addresses to which the rules apply.

3. Notational Conventions

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].

4. IPv6 Address/Mask Notation

This RFC extends prefix-length notation of [RFC4632] in a way that is reminiscent of the IPv4 netmask notation of [RFC0950]. The proposed notation would allow specifying IPv6 mask instead of the prefix length after "/". For example: 2001:db8::1234/ffff:ffff::ffff.

The mask indicates which bits of the address are relevant for the address grouping. Note that the mask may be sparse and is not strictly a prefix.

4.1. Constraints and Validation

To be a valid definition for just a group of addresses, the address part MUST NOT have any bits outside of the mask set. Otherwise, the notation identifies an individual address and a group of addresses it belongs to.

4.2. Examples: groups of addresses

1. 2001:db8::1234/ffff:ffff::ffff

This specifies IPv6 addresses that look like 2001:db8::1234 when you ignore bits 16-95.
2. ::aa00:1234/::ff00:ffff
   This specifies IPv6 addresses that have "aa" in bits 24-31 and
   "1234" in bits 0-15.

3. 2001:db8::/ffff:ffff::
   This is equivalent to 2001:db8::/32.

4.3. Examples: specific addresses and groups they belong to

1. 2001:db8::1:1234/ffff:ffff::ffff
   This specifies IPv6 address 2001:db8::1:1234 that belongs to a
group of addresses that look like 2001:db8::1234 when you ignore
bits 16-95.

2. 2001:db8::aa00:1234/::ff00:ffff
   This specifies IPv6 address 2001:db8::aa00:1234 that belongs to a
group of addresses that have "aa" in bits 24-31 and "1234" in
bits 0-15.

3. 2001:db8::1/ffff:ffff::
   This is equivalent to 2001:db8::1/32.

4.4. Textual representation of the IPv6 Address/Mask notation

   When IPv6 mask is used after "/", both the network address and mask
parts MUST be formatted as IPv6 addresses and, therefore, their
canonical textual representation is dictated by [RFC5952].

4.5. Use prefix length instead of mask

   The canonical representation of a group of IPv6 addresses MUST use a
prefix length instead of a mask if possible. That is, if the mask
has all its most-significant bits set, up to some bit, followed by
all clear bits, then the canonical representation MUST use a prefix
length.

5. Scoped Mask/Value specifications

   A common use-case is to specify an address/mask filter within a
prefix scope. For example, specifying all addresses ending with
::1234 within 2001:db8::/32 can be specified as 2001:db8::1234/
ffff:ffff::ffff.
To make these easier to operationally manage and validate, it helps to have an explicit convention for representing these. For example: 2001:db8::1234/32+::ffff.

This is specified as:

ADDRESS / PFX_LEN + SCOPED_MASK

These can be canonicalized into an ADDRESS / MASK specification. The canonical MASK is constructed by performing the bitwise-or of SCOPED_MASK and the mask derived from an address with the PFX_LEN most-significant bits set.

The the PFX_LEN most-significant bits MUST NOT be set in SCOPED_MASK.

6. Security Considerations

This document only specifies IPv6 address grouping notation and its meaning and does not intend to specify when matching based on bit substrings is applicable or appropriate. IP addresses can be spoofed or attacker-controlled. This is especially true of IPv6 addresses differing only in less-significant bits and belonging to different administrative domains. As such, care must be taken when applying any semantic meaning to bits in addresses. Guidance for this applicability is outside the scope of this document.

7. Acknowledgments

The Acknowledgments will come here.

8. Normative References


RFC5952, August 2010,  


Authors’ Addresses

Igor Lubashev  
Akamai Technologies  
EMail: igorlord@alum.mit.edu

Erik Nygren  
Akamai Technologies  
EMail: erik+ietf@nygren.org  
URI: http://erik.nygren.org/