Internet Engineering Task Force
Internet-Draft
Updates: RFC4291, RFC4443, RFC6724 (if approved)
Intended status: Standards Track
Expires: 25 August 2024

M.R. Smith
22 February 2024

IPv6 Formal Anycast Addresses and Functional Anycast Addresses
draft-smith-6man-form-func-anycast-addresses-02

Abstract

Currently, IPv6 anycast addresses are chosen from within the existing IPv6 unicast address space, with the addresses nominated as anycast addresses through configuration. An alternative scheme would be to have a special class of addresses for use as anycast addresses. This memo proposes a distinct general anycast addressing class for IPv6, and a more specific scheme for functional anycast addresses.

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 25 August 2024.

Copyright Notice

Table of Contents

1. Introduction

[RFC1546] was the first description of host anycast services, and proposed two ways of supporting them in terms of addressing:

* using parts of the existing address space

* create a special class of addresses for anycast use

The first method of supporting anycast addresses, by using parts of the existing (unicast) address space, could be described as informal. From the address itself, it is not possible to determine that the apparent unicast address is actually being used as an anycast address.

As the second method would create a special class of addresses for anycast use, it could be described as formal. Encoded within the addresses would be a well known value that indicates they are anycast addresses, regardless of context.

In terms of a spectrum of packet delivery, ranging from delivery to a single destination (unicast), through to delivery to multiple destinations (multicast), anycast addresses are a distinct class of addresses when compared to unicast and multicast addresses.

Packets sent to a unicast destination are intended to be delivered to one and only one unique destination host. Packets sent to a multicast destination are intended to be delivered to a group of interested destination hosts, with the interested group consisting of one or more members, and the packets being duplicated by the network when and where necessary.

Packets sent to an anycast destination are intended to be delivered to only one host, however that host is a member a set of hosts sharing the same anycast address. As a type of address, anycast addresses can be imagined to fall between unicast and multicast address types on a packet delivery spectrum. Packet delivery to an anycast address shares characteristics of both unicast and multicast address packet delivery.

IPv6 anycast addresses [RFC4291] are currently from within the existing unicast address address space. Therefore, this memo gives these IPv6 anycast addresses the name "Informal Anycast" addresses.

This memo proposes a distinct and formal class of IPv6 addresses for anycast use, calling them "Formal Anycast" addresses.

The described IPv6 Formal Anycast address class can support a total of 16 sub-classes of anycast address formats and structures, allowing other semantics to be encoded in the anycast address. Following the definition of the Formal Anycast address class, this memo then proposes the first sub-class, called "Functional Anycast" addresses.

There are some existing reserved and well known anycast addresses within the existing Informal Anycast address space, that have been assigned by IANA [IANA-IPV6ANYC]. While well known, they do not have any of the formal attributes that the proposed formal Functional Anycast addresses have, other than having specified and well known values; they could be described as semi-formal. Well known Functional Anycast addresses are proposed that correspond to these existing semi-formal anycast addresses.

"MRS:" comments - points to consider further, to eventually be removed.

2. Terminology

Anycast Domain

Formal Anycast Address

Functional Anycast Address

Informal Anycast Address

Semi-Formal Anycast Address

3. Drawbacks of Informal Anycast Addresses

There are drawbacks and limitions of the existing IPv6 Informal Anycast addresses:

* As mentioned in the Introduction, there is nothing specifically encoded in an Informal Anycast address to distinguish it from a unicast address, such as being from within a well known address prefix. In some situations, this unintentional obfuscation may be of use, however in others, such as while troubleshooting, it can be detrimental. For example, duplicate routes for an address or prefix appearing in a route table with different announcing routers may be a fault if unintentional, meaning it is a duplicate unicast address assignment. Alternatively, it may be the intended configuration if the address or prefix routes are Informal Anycast routes i.e., the address or prefix from within the unicast address space is being used an anycast address or anycast prefix. The duplicate routes and the addresses or prefixes themselves provide no indication of whether the configuration is intentional or not.

* Constraining the visibility and reachability of an anycast provided service or function may be useful for security reasons, which can be fundamentally enforced by encoding and limiting the scope of or domain where packets are intended and able to be forwarded. Informal Anycast addresses can only have one of three fundamental forwarding scopes encoded in the address, matching those of the three types of IPv6 unicast addresses - limited to a link scope (Link-Local Address), limited to a local network scope (Unique Local Address) or having global Internet scope (Global Unicast Address) [RFC4291][RFC4193]. These scopes are coarse. More fine grained scopes, such as those used in IPv6 multicast [RFC7346], would provide much more control over anycast service or function visibility.

* Some transport layer protocols, such as SCTP [RFC3286] and Multipath TCP [RFC6824], and some applications, deal directly with IPv6 addresses, and supply them to their communications peer or peers. Currently, if these transport layer protocols or applications are dealing with both unicast and anycast addresses, and wish to provide only unicast or anycast types of address or set of addresses to their peer or peers during their communications transactions, it would be necessary to manually configure the transport protocol or application so that it can distinguish between unicast and anycast addresses. A well known address class that identifies anycast addresses would allow these transport layer protocols or applications to identify the different address types without any manual configuration.

4. Formal Anycast Addresses

4.1. Address Format

The following diagram shows the structure of an IPv6 Formal Anycast address.

DIAGRAM TO COME

4.2. Address Fields

4.2.1. Formal Anycast Prefix

A 8 bit prefix value of TBD (aa00::/8 preferred, indicating a Anycast Address; fa00::/8 an alternative, indicating a Formal Anycast address), identifying this address as a Formal Anycast address.

4.2.2. Visible Scope

A 4 bit Visible Scope field used to express and enforce visibility and assumed reachability of the Formal Anycast address. The values and meanings of the values of this field are the same as those for the IPv6 multicast address scope field [RFC4291][RFC7346].

When packets with a Formal Anycast destinaton address are being forwarded, this field's value takes precedence over a non-zero Hop Limit field value, meaning the packet MUST be discarded at the edge of the indicated visibility domain even though it may have a non-zero Hop Limit value. A specific ICMPv6 Destination Unreachable [RFC4443] message, described below, SHOULD be generated and returned to the packet's sender indicating the packet was discarded as it reached the edge of its Visible Scope.

4.2.3. Anycast Identifier Format

A 4 bit field identifying the format of the following Anycast Identifier field, holding digits in the range of 0x0 through 0xf in hexidecimal.

The first assigned value is 0, specifying that the following Anycast Identifier Format is that of a Functional Anycast addresses, which is described later in this memo.

Other values will be assigned by IANA as future Anycast Identifier Formats are specified.

4.2.4. Anycast Identifier

A 112 bit field holding the Anycast Identifier value. The format and structure of this field is encoded in the previous Anycast Identifier Format field.

4.3. Anycast Address Registration Protocol

Rather than having to manually configure a network's routing protocol to distribute a host's anycast address, or have a host participate in the network's routing protocol, a protocol for hosts to automatically register an anycast address for routing protocol distribution would be beneficial.

Development of this protocol is left for a later memo, however as the requirements of such an anycast address registration protocol are very similar to that of hosts' multicast address registration with a network, it is likely that an anycast address registration protocol could be modelled on and derived from the IPv6 Multicast Listener Discovery protocol [RFC2710][RFC3810].

4.4. Network Service Provider Visible Scope

A network service provider, such as an Internet Service Provider, may wish to use an anycast address to provide a service with a visibilility limited to all of its direct customers.

When using a Formal Anycast address for this service, that reuses IPv6 multicast scopes, this means the address needs to have a scope that is greater than the Organization-Local scope, yet smaller than the unlimited Global scope.

This memo defines a new scope called the Network Service Provider (NSP) scope, that falls between the Organization-Local and Global IPv6 multicast scopes. This NSP scope's hexidecimal value is B. This scope can be used with both Formal Anycast and IPv6 multicast addresses.

(MRS: perhaps this scope shouldn't be at B, but instead hard up against the Organization-Local scope i.e. at value 9? Could there be a need for any other future scopes between Organization-Local and Network Service Provider - which would be scopes within the Network Service Provider's network.)

4.5. Link-Local Visible Scope

One of the possible Visible Scope values is the Link-Local scope, specifying that the Formal Anycast address's visibility is limited to a link that the host is directly attached to.

Nodes on the link will need to consider Formal Anycast addresses with a Link-Local Visible Scope on-link, so that they perform Neighbor Discovery [RFC4861] for these addresses.

Similar to the unicast Link-Local prefix [RFC5942], IPv6 implementations SHOULD BE updated to consider the Formal Anycast prefix with a Link-Local Visible Scope on-link. Using the (preferred, IANA TBA) aa00::/8 Formal Anycast prefix, this means IPv6 implementations will consider aa20::/12 to be on-link.

Unlike the unicast Link-Local prefix, updated IPv6 implementations MUST NOT use SLAAC [RFC4862] to generate an automatic address from within this Formal Anycast Link-Local Visible Scope prefix.

(MRS: Need to further consider this constraint, and more generally the idea of host automatically generated dynamic anycast addresses, rather than either having well known or system administrator chosen and configured anycast addresses. If there is an anycast address registration protocol that hosts can use (suggested above), then hosts could possibly dynamically generate anycast addresses and then register them.)

Note that unlike the unicast Link-Local prefix, IPv6 nodes may not and typically would not have an address from within the Formal Anycast Link-Local Visible Scope prefix. One of the node's Link-Local addresses on the same link should be used as a source address when sending to a Formal Anycast Link-Local Visible Scope destination. This does not preclude using other greater scope unicast source addresses.

In the interrim IPv6 implementation update period, IPv6 nodes can be informed that the Formal Anycast Link-Local Visible Scope prefix is on-link in one of two ways:

* A manually configured entry in the host's Prefix List [RFC4861].

* A dynamic update to nodes' Prefix Lists using a Router Advertisement Prefix Information Option (PIO) [RFC4861]for the Formal Anycast Link-Local Visible Scope prefix of aa20::/12, with the 'L' or on-link flag set to on, and the 'A' or autonomous address-configuration flag set to off (as this prefix MUST NOT be used by the node to automatically generate an address for its use

within this prefix). The Valid and Preferred Lifetimes for the Formal Anycast Link-Local Visible Scope prefix in the PIO are set to infinity.

4.6. ICMPv6 Destination Unreachable Message

As mentioned prevously, if a packet with a Formal Anycast destination address reaches the edge of the Visible Scope for the address, a ICMPv6 Destination Unreachable [RFC4443] message SHOULD be generated and sent back to trigger packet's sender.

Note that if the router at the edge of the visibility domain is also assigned the Formal Anycast address, the packet is host processed locally rather than being discarded, and an ICMPv6 Destination Unreachable message IS NOT generated.

When a router implementation formally supports Formal Anycast addresses, the ICMPv6 Code for the Destination Unreachble message is IANA-TBD, indicating that the Edge of the Visible Scope [was] Reached.

If a router implementation does not formally support Formal Anycast addresses an operator should use packet filters to enforce the Visible Scope boundary. A packet failing to pass the packet filter should cause the router to generate a Destination Unreachable Communication with destination administratively prohibited message [RFC4443] (Code 1) message, which is semantically similar to the formal Edge of Visibile Scope Reached message.

Note that ICMPv6 messages are not sent reliably, so Formal Anycast packet senders will need to be able to handle not receiving a ICMPv6 Destination Unreachable message in response to a packet reaching the edge of the visibility domain.

There may be situations where silently discarding Formal Anycast packets at the Visible Scope boundary may be preferred. In this case, a packet discard route, covering the Visible Scope prefix can be installed in a router's forwarding table, saving router control plane resources.

4.7. Default Address Selection

4.7.1. Formal Anycast Scope Comparison

As the Formal Anycast address scopes are defined to be the same as Multicast address scopes, the same Multicast scope comparison methods, described in [RFC6724], are also used with Formal Anycast address scopes.

4.7.2. Source Address Selection

As mentioned in Appendix B. of [RFC6724], anycast addresses are candidates during source address selection.

4.7.3. Destination Address Selection

An IPv6 implementation may be presented with a candidate set of destination addresses that consists of both Formal Anycast and unicast addresses. The implementation needs to make a choice or choices as to which of these candidate addresses to attempt to use.

The decision to use a Formal Anycast address instead of a unicast address by the destination is an active and conscious one. Therefore, when a choice needs to be made between a Formal Anycast address and a unicast address, the Formal Anycast address should be preferred.

In terms of the Destinaton Address Selection algorithm described in [RFC6724], this preference of Formal Anycast over unicast addresses introduces a new rule between Rule 1 ("Avoid unusable destinations") and Rule 2 ("Prefer matching scope"), specifically (using "1.5" here to indicate the position):

> Rule 1.5: Prefer Formal Anycast addresses.
>
> If DA is a unicast address, and DB is a Formal Anycast address, then prefer DB.

Note that there may be instances where an application would prefer to use a unicast address over a Formal Anycast address. In this case, Formal Anycast addresses can be easily identified and ignored using the well known 8 bit Formal Anycast prefix.

4.8. Non-Local Anycast Forwarding

(MRS:This section is being left here for the moment, however this idea should probaby be moved to a different memo, as it is describing forwarding that isn’t unicast forwarding (unicast forwarding is used by conventional anycast))

One possible use for Formal Anycast addresses is to represent a function that is performed on the packet by the network that is beyond conventional destination address based unicast IPv6 forwarding, as the packet traverses the path towards its final delivery point.

Currently, hop-by-hop processing of an IPv6 packet as it traverses the network is indicated using the Hop-by-Hop Options (Extension) Header [RFC8200].

Drawbacks of using the Hop-by-Hop Option Header are that some high speed routers ignore them [RFC7045], and that packets with the Hop-by-Hop Options Header may be dropped by transit Autonomous System (AS) networks [RFC7872]. The dropping of these types of packets by transit ASes may be due to a default deny policy for Extention Header types other than those of TCP, UDP, ICMPv6 and possibly IPsec ESP.

Encoding the intent of hop-by-hop processing of a packet as an anycast IPv6 destination address has the advantage of the packet always being processed by all router implementations, including high speed implementations, as processing a packet's IPv6 destination address is required to perform IPv6 destination address based forwarding. As there is no explicit Hop-by-Hop Options Header in the packet, a transit AS is less likely to drop the packet, unless it explicitly implements IPv6 Destination Address packet filters that drop packets with Formal Anycast addresses.

Another advantage is that there may now be no need for the addition of an Extension Header to the IPv6 packet for hop-by-hop processing, increasing the packet's effective payload size.

Conventional unicast IPv6 forwarding based on destination address prioritises a node's local addresses over all others. This means that when a node originates a packet with one its own addresses as the destination, the node will deliver the packet internally for local processing, rather than sending it out one of the node's network interfaces.

The functional requirements for Non-Local Anycast Forwarding are:

* When being sent by the node, the packet is not delivered internally to the node's own instance of the Formal Anycast address.

* After being submitted to the network for forwarding, the packet must not be sent back towards its source, as this would potentially cause the packet to follow a loop in its forwarding path.

4.9. Advice on Structuring the Anycast Identifier Field Values

The Anycast Identifier Format field within a Formal Anycast address specifies the format and structure of the 112 bit Anycast Identifier field. The following is advice and guidelines to use when developing a new Anycast Identifier field format and structure.

Forwarding towards anycast addresses is the same as forwarding towards unicast addresses, which uses the longest match rule BCP 198 [RFC7608]. Longest match forwarding facilitates summarisation of forwarding information, where a single more general forwarding route can summarise a number of more specific forwarding routes. Summarisation saves entries in forwarding tables outside of the summarised forwarding domain, provides simpler destination based filtering for security purposes, and facilitates easier destination address based traffic analysis.

The use of route summarisation with anycast addresses effectively creates an anycast domain that is being identified and summarised by the anycast summary route. Outside of the anycast domain, a single summary route exists, covering all anycast addresses within the domain. Within the anycast domain, individual routes for individual anycast addresses exist.

When designing a new Anycast Identifier field format and structure, the following guidelines should be followed. These guidelines should allow a set of more specific anycast routes to be summarised as well as improving operator usability.

* The order of fields within the Anycast Identifier field should be from the most general to most specific, in the direction following the high order to low order bits of the Anycast Identifier field and the broader IPv6 address.

* The order of bits within fields should also be from the most general to most specific, matching the direction of high order to low order of bits within the Anycast Identifier field.

* The bits in fields holding bits that are matched exactly, such as flag fields or fields holding numeric values that are matched exactly, can be orded to suit the field’s use and application. However, a hierarchial order, from most significant to least significant bit, following Anycast Identifier field bit order, is suggested. Although initially defined hierarchially, the order of flags in flag fields may later deviate from this recommendation due to later flag bit definition.

* End-users of the functions and services being provided using Formal Anycast addresses are unlikely and ideally should never see these addresses. However, operators of these functions and services will deal with these addresses during planning, configuration and troubleshooting. Where possible, fields and their values should be ordered and structured to assist with these tasks. Field boundaries within the Anycast Identifier field should align with 16 bit word, 8 bit octet or 4 bit nibble positions within the whole IPv6 address. For example, if part of an IPv6 prefix is included in the Anycast Identifier, it should start at a 16 bit "piece" boundary, where colons appear [RFC4291], within the IPv6 address. Note that this guildeline should not take precedence over any previous measures to faciliate more specific anycast route summarisation.

* A further address usability recommendation is to set field and bit values to zero for the likely most common or likely most secure meaning for these fields or bit values. In IPv6 addresses zero field values can be compressed [RFC5952], resulting in a shorter address for an operator to type. A shorter address to enter naturally reduces the opportunities for and likelihood of errors in the address, and reduces the possibilities of security issues caused by errors in the Formal Anycast address.

5. Functional Anycast Addresses

The first defined sub-class or sub-format of Formal Anycast addresses is the Functional Anycast address sub-class.

5.1. Features

The following are the features of Functional Anycast addresses. In many cases they're inspired by and mirror IPv6 multicast address features [RFC4291][RFC3306].

* Provides separate globally well known and local network defined anycast function or service identifier spaces. Globally well known identifiers can be encoded in applications during their development as constants, avoiding the need for them to be specified and configured during deployment of the application.

* Provides a minimum of 24 bits for use as identifiers for anycast functions or services, supporting more than 16 million values.

* Provides 8 bits for the identification of up to 256 local instances, versions or revisions of the same function or service, assisting with function or service deployment or maintenance. These 8 bits can also be used to increase the size of the function or service identifier space to 32 bits where useful, increasing the range of values to more than 4 billion.

* Identifies an anycast function or service identifier space, known as an anycast domain, using an IPv6 unicast address prefix of up to 64 bits in length.

  A network can create multiple distinct anycast domains by using multiple of its IPv6 prefixes, from its Global [RFC4291] or Unique Local [RFC4193] address spaces (the Link-Local prefix could be used to create a distinct anycast domain, however it can only be used once, despite the network having many instances of the Link-Local prefix (as many as it has links)).

  A "unspecified" anycast domain is supported using an all zeros 64 bit IPv6 prefix.

  External to the anycast domain, the identifying 64 bit prefix can be used to create a single summary route for the anycast function or service identifier space, which will help routing scaling for anycast functions or services. The anycast domain boundary could also correspond to routing protocol scaling boundaries, such as OSPFv3 areas [RFC5340] or IS-IS level [RFC5308] boundaries, when useful.

5.2. Address Format

The format of Functional Anycast addresses is modelled on the IPv6 multicast address format [RFC4291].

The format of an Functional Anycast address is as follows:

DIAGRAM TO COME

The address fields are as follows:

* Anycast Domain Prefix - a 64 bit field holding a IPv6 unicast address prefix identifying the anycast domain that is either the provider and possible authority for the following Anycast Function Identifier space.

  The length of the prefix is specified in the following Prefix-Length field, with the remaining bits of the field set to zero.

An all zero Anycast Domain Prefix means an unspecified Anycast Function Identifier provider. An all zeros Prefix in effect means "this" provider, with "this" meaning the current anycast domain.

Link-Local, Unique-Local [RFC4193], Global and possible future other unicast prefixes [RFC4291] identify a specific Anycast Function Identifier provider (MRS: Need to think about more about using Link-Local prefix, as it really isn't specific - perhaps either prohibit, or make it all zeros "current" equivalent). Within an anycast function domain, this allows multiple anycast function sub-domains to be created, identified by different unicast prefixes in this field.

* Reserved - a 2 bit reserved field.

  Set to zero upon transmission, ignored upon receipt.

* Prefix-Length - An 6 bit field specifying the length of the previous Anycast Domain Prefix.

  A value of zero means a 64 bit length prefix, while prefix lengths of 1 through 63 (0x01 through 0x3f) are encoded natively.

  The unspecified Anycast Domain Prefix of all zeros is considered to be 64 bits in length, meaning a Prefix-Length value of 0 for this prefix.

  This is an informational field to assist with operation and troubleshooting.

  (MRS: This field is inspired by the equivlent field when IPv6 multicast addresses contain a unicast prefix per [RFC3306]. I'm not entirely sure it is necessary, as we don't embed prefix length in unicast addresses, and unicast routing protocols, also used for anycast, carry prefix length information separately.)

* Flags - A 8 bit flag field.

  The lower 6 flags are reserved and must be set to zero upon transmission, and ignored upon receipt.

  The high order flag is the 'T' or Transient flag. T=0 indicates that the later Anycast Function Identifier is well known and assigned by the Internet Assigned Numbers Authority (IANA). T=1 indicates that the Anycast Function Identifier is transient or dyamically assigned, and has been assigned by the Functonal Anycast domain's local authority.

The second most high order flag is the 'LI' or Last Instance flag. When a network supports hop-by-hop processing of packets using anycast addressing, this flag indicates whether anycast processing of the packet should cease at the first anycast instance encountered (LI=0), even though there may be further candidate anycast hops that suit, or whether the packet should continue to be sent to any subsequent anycast hops until the Last Instance of the matching anycast address is encountered (LI=1).

* Local Instance - An 8 bit field holding a identifier of the instance, version or revision of the function identified by the following Anycast Function Identifier field, local to the current anycast domain.

  The default value of this field is zero, indicating the default and first instance of the anycast function.

  Non-default values are chosen by the local anycast domain operator, even when the following Anycast Function Identifier is using a well-known IANA Anycast Function Identifier value.

  An anycast domain operator may chose to assign other semantics to this field, as long as they're both less significant than the previous fields and more sigificant than the following Anycast Function Identifier field.

  When the 'T' bit in the Flags field is set to 1, meaning transient Anycast Function Identifiers, this field could be used to effectively increase the size of the following Anycast Function Identifier field to 32 bits, increasing the value range of Anycast Function Identifiers from in the order of 16 million to in the order of 4 billion.

* Anycast Function Identifier - A 24 bit field identifying the anycast function to be performed on the packet when it arrives at a host that has been configured with the Functional Anycast address.

  When the 'T' bit in the Flags field is set to zero, the Anycast Function Identifiers values are from a well known Anycast Function Identifier registry maintained by IANA, with initial entries specified later in this memo.

  When the 'T'bit in the Flags field is set to 1, the values in the Anycast Function Identifier field are local to and assigned by the authority identified in the Prefix field in any manner that suits their purposes and requirements.

5.3. Assignment of Anycast Function Identifiers

In the history of the Internet, it has been common to conflate a function or service with a protocol.

For example, historically, the TELNET protocol [RFC0854] had been the most popular "Network Virtual Terminal" protocol. In more recent times, the SSH protocol [RFC4252] has become the de facto network virtual terminal protocol. Accessing the network virtual terminal service has either been referred to as "TELNETting in" or "SSHing in" to the host providing the service, using the protocol being used to refer to the service being accessed.

In either case, TELNET and SSH protocols are being used to access a remote network virtual terminal service. Functionally, from the perspective of network virtual terminal access, the differences are relatively minor; data security and integrity via encryption and authentication is where the primary differences between TELNET and SSH are – in TELNET authentication [RFC2941] and encryption [RFC2946] of the data stream is optional, where as with SSH it is mandatory.

When both IANA and local anycast domain operators assign Anycast Function Identifiers, it is recommended that they’re allocated and identified by protocol agnostic function or service type rather than to a specific protocol that provides that function or service. As the particular protocol being used to access the function or service will be encoded in the upper transport layer protocols and ports in the IPv6 packet, service or function based Anycast Function Identifers can support and stay constant across the use and evolution of different function or service access protocols.

For example, with a well-known Anycast Function Identifier specifically allocated to a Network Virtual Terminal (NVT) [RFC0318] service, the hosts providing the NVT service could initially support both TELNET (assuming TELNET is considered secure enough) and SSH. If both TELNET and SSH become deprecated, and a new NVT access protocol is developed, the same Anycast Function Identifier for the NVT service could be used to reach a node supporting this new access protocol.

Another example is the domain name service. Currently domain name resolution commonly takes place using the Domain Name Service protocol [RFC1035], carried directly over UDP and TCP, using port 53. More recently, work has been taking place to operate DNS over TLS [RFC7858] and HTTPS [RFC8484] to enhance the security of the domain name resolution function. The use of multiple protocols to access fundamentally the same domain name resolution function suggests a protocol agnostic domain name resolution Anycast Function Identifier.

This doesn't preclude Anycast Function Identifiers being used to support and identify specific protocols (examples of this occur later). There may be current and future cases where the allocation and use of an Anycast Function Identifier for a specific protocol is the better choice. This should be considered and evaluated on a case by case basis.

5.4. Assigned Anycast Function Identifiers

A number of past RFCs have reserved anycast addresses and identifiers. These addresses and indentifiers are mapped to the following corresponding and well known Anycast Function Identifiers, and are to be listed in the IANA Anycast Function Address Identifier registery if it is created.

[RFC2526] reserves the highest 127 values of a subnet prefix Interface Identifier for anycast addresses. The equivalent values for Functional Anycast addresses are the highest 127 values of the 32 bit Anycast Function Identifier, a range of (in IPv6 address format, excluding the high order 96 bits) :ffff:fff8 through :ffff:ffff. The IANA Internet Protocol Version 6 (IPv6) Anycast Addresses registry [IANA-IPV6ANYC] records assignments for subnet prefix anycast addresses within the Interface Identifier space. The current and future values of these anycast subnet prefix Interface Identifier values are to also be recorded in the Anycast Function Address Identifier registry.

[RFC4291] reserves an Interface Identifer of all zeros within a unicast prefix as the Subnet-Router anycast address. The equivalent 32 bit Anycast Function Identifier value for Functional Anycast addresses is also all-zeros.

[RFC7723] reserves the IPv6 address 2001:1::1/128 for the use as the Port Control Protocol Anycast address. The equivalent 32 bit Anycast Function Identifier value is (in IPv6 address format, excluding the high order 96 bits) :0001:0001.

[RFC8155] reserves the IPv6 address 2001:1::2/128 for the use as the Traversal Using Relays around NAT Anycast address. The equivalent 32 bit Anycast Function Identifier value is (in IPv6 address format, excluding the high order 96 bits) :0001:0002.

5.5. Sources of Inspiration for Anycast Function Identifiers

A future possible source of inspiraton for well known assigned Anycast Function Identifiers could be DHCPv6 [RFC8415] options that encode IPv6 addresses for services.

A number of these options encode multiple IPv6 addresses as candidates for access to the service (for example, the SIP Servers IPv6 Address List option [RFC3310]). The use of anycast for service resiliance would allow a single Anycast Function Identifier value to provide equivalent service, although this wouldn't preclude defining multiple different Anycast Function Identifiers to the service to provide the service client concurrent access to multiple service instances. For example, 3 Functional Anycast addresses could be allocated for DNS resolvers, providing a client with seperately verifiable DNS resolver services from up to 3 different resolvers, and allowing the client to distribute requests across all 3 resolvers.

Another source of inspiration for well known assigned Anycast Function Identifiers could be the IANA IPv6 Multicast Address Space [IANA-IPV6MCAST] registry, where some of the multicast addresses represent services that could also be useful when provided via anycast.

While using these possible source of inspiration, the recommendation to choose protocol agnostic function or service identifiers still stands. DHCPv6 or multicast groups can be used to inspire more generic function or service identifiers.

5.6. Global Scope Functional Anycast Addresses on the Internet

(MRS: Need to fully review this idea and section. An idea to help overcome the /48 prefix length constraint would be to have all Formal Anycast addresses that are going to be used on the Internet come from an IANA reserved prefix within the existing GUA address space e.g. 20e0::/12 (i.e. operators would accept a prefix announcement of length of up to /80 within 20e0::/12). aa::/8 would still be used for smaller than global scope anycast, because a prefix of "aa" is very helpful to identify anycast addresses.)

Functonal Anycast addresses could be used to provide anycast services across the Internet, by using the the Global scope.

When being used on the Internet, many of the possible values of the Prefix field are ambiguous, meaning that they wouldn't unambiguously identify the party using the Functional Anycast address to provide the service or function. Examples of ambiguous prefixes are the all-zeros unspecified prefix, any ULA [RFC4193] prefixes, and the Link-Local [RFC4291] prefix. Other ambiguous prefixes are those in the IPv6 reserved address registry [IANA-IPV6RESA] that are not valid on the Internet.

To overcome this ambiguity, if Global scope Functional Addresses are used over the Internet, the Prefix field MUST be set to a GUA [RFC4291] prefix value assigned to the party providing the anycast service to Internet clients. A network either accepting or originating a Global scope Functional Address prefix for announcement from a downstream stub autonomous system for announcement onto the Internet MUST only accept or originate a route announcement for a Global scope Functional Anycast prefix that includes an explicitly identified GUA prefix. All other Global scope Functional Anycast prefix announcements with ambiguous or non-explicitly identified GUA prefixes MUST be ignored.

As forwarding towards anycast addresses is functionally the same as forwarding towards unicast addresses, Functional Anycast prefixes would be announced into the Internet's unicast forwarding route table. These Functional Anycast prefixes SHOULD BE aggregate announcements with the aggregation boundary occurring directly after the Anycast Domain Prefix.

It is common practice today to limit the prefix length of unicast IPv6 Internet routes accepted to a length of no more than 48 bits i.e. a /48. This is a blunt and simple way to attempt to somewhat limit the number of IPv6 routes in the Internet route table. It is imposing this limit by enforcing a minimal level of aggregation at the /48 boundary. Networks using prefix lengths longer than /48 are expected to aggregate those networks into a route advertisement that is /48 or shorter.

This practice of limiting advertised unicast route prefix lengths to 48 bits will limit the size of the Prefix included in Global scope Functional Anycast announcements to 32 bits, as the high order 16 bits of the Functional Anycast prefix are used to encode the Functional Address type prefix and address scope. This would limit the use of Global scope Functional Anycast addresses to provide global Internet anycast services to those organisations who have a /32 or shorter assignment from an RIR.

As Functional Anycast addresses are a separate class of addresses, and are all identified by a unique /8 prefix, this /48 prefix length limit could be specifically relaxed for Functional Anycast routes. A /48 prefix, when included in a Functional Anycast, results in a Functional Anycast prefix length of /64. Imposing a /64 prefix length limit on Functional Anycast routes, identified by a high order prefix of aae0::/16, and a GUA anycast domain prefix, would achieve the same outcome of attempting to reducing the number of entries in the IPv6 Internet route table.

Wide acceptance of Functional Anycast prefixes of up to 64 bits in length on the Internet may take same time to occur. Use of Global scope Functional Anycast addresses by organisations who have RIR /32 assignments, which will be accepted by unicast /48 prefix filters present today, would raise awareness of Functional Anycast addresses. This increased awareness could be leveraged to motivate the changing of prefix filters to accept Global scope Functional Anycast prefixes up to 64 bits in length.

5.7. Example Use Cases

This section provides some example use cases of Functional Anycast addresses that would suit the described scenarios.

5.7.1. Devices Factory Configured with NTP Functional Anycast Addresses

Assume IANA has allocated a set of well-known Anycast Function Identifier values of 0x004440, 0x004441, 0x004442 and 0x004443 for use with the Network Time Protocol [RFC5905], to facilitate meeting the NTP best practice of having a minimum of 4 NTP time sources [RFC8633].

A device manufacturer uses this set of well-known Anycast Function Identifier to set factory default Functional Anycast addresses for access to a device customer's NTP servers.

The corresponding Functional Anycast address is constructed as follows:

* 8 bit Formal Anycast Prefix value (0xaa proposed).

* 4 bit Visible Scope value of 0x8, corresponding to Organization-Local [RFC7346], as the manufacturer is unlikely to have any knowledge of device customers' use of or preference for smaller scopes.

* 4 bit Anycast Identifier Format value of 0x0, corresponding to the Functional Anycast format.

* 112 bit Anycast Identifier in the Functional Anycast format:

* - 64 bit Anycast Domain Prefix value of the all zeros unspecified prefix.

  - 2 bit reserved field set to zero.

  - 6 bit Prefix-Length field set to zero, meaning a 64 bit length Anycast Domain Prefix value.

- 8 bit Flags field set to all zeros. The upper 7 bits are zero as they're served, while the lowest 'T' or Transcient flag is set to zero indicating an IANA assigned well known Anycast Function Identifier.

- 8 bit Local Instance flag set to the default value of zero.

- 24 bit Anycast Function Identifier field set to either 0x004440, 0x004441, 0x00442 or 0x004443; one of the IANA assigned well known Anycast Function Identifier values for the NTP protocol.

All of the above mean that the NTP server Functional Anycast addresses the device manufacturer sets as the defaults would be (in IPv6 address compressed format):

* aa80::4440

* aa80::4441

* aa80::4442

* aa80::4443

5.7.2. Branch Office DNS Resolvers

An enterprise network operator decides to use Functional Anycast addresses to provide DNS resolver service to end-user devices, located in various corporate offices.

Specifically for a single mid-sized branch office, with in the order of 200 staff, the operator decides to provide two DNS resolvers located in the office. This will provide lower latency DNS resolution through DNS caching, reducing perceiveable application response time [NORMNEIL]. Access to a third, geographically close, off-site DNS resolver is provided for redundancy. This off-site DNS resolver will be one of the other branch office's local DNS resolvers.

All three DNS resolvers will provide their services to clients via Functional Anycast addresses. Different clients will receive the on-site DNS resolver addresses in alternating order, both before the off-site DNS resolver address. This provides rudimentry on-site DNS resolver load balancing and keeps both DNS resolvers' lookup caches populated to reduce the client visible performance impact of the fail-over to the remaining on-site DNS resolver, should its sibling fail. The on-site DNS resolvers will watch each others' availablility, taking over its sibling's Functional Anycast address

if the sibling becomes unavailable. Should both on-site DNS resolvers become unavailable, clients will resort to using the remaining off-site DNS resolver.

Assume IANA have allocated the well known Anycast Function Identifier values of 5300, 5301 and 5302 for use with anycast DNS resolvers.

The operator allocates decimal identifiers of 703, 9556, 4739, 38809 and 2764 to the corporate offices, with the order reflecting geographic proximity. Each office will have its own unicast /48 from within a globally unique address space of 2001:db8::/32, meaning that the office prefixes are 2001:db8:2bf::/48, 2001:db8:2554::/48, 2001:db8:9779::/48 and 2001:db8:acc::/48.

The corresponding Functional Anycast address is constructed as follows:

The Visibiliity Scope for for these DNS resolvers' Functional Anycast addresses will be Organization-Local (8).

For office 9556, using offic 4739 as an off-site backup, the Functional Anycast addresses for the three DNS resolvers will be:

1. aa80:2001:db8:2554::5301

2. aa80:2001:db8:2554::5302

3. aa80:2001:db8:9779::5303

5.7.3. Automatic eBGP Session Establishment

Assume IANA has allocated a well-known Anycast Function Identifier value of 0x000179 for use with automatic eBGP [RFC4271] session establishement.

Smaller, stub site routers are preconfigured with a Functional Anycast address to attempt to automatically establish an eBGP session with a one or two upstream eBGP peer aggregation routers over one or two different designated ("WAN") links upon initialisation.

The eBGP Functional Anycast address would be a Link-Local Visible scope address. The stub router would use its link's, SLAAC generated [RFC4861] and link unique Link-Local address [RFC4291] as the source address to reach the eBGP Functional Anycast address. Using Link-Local scope Formal Anycast and unicast addresses for this eBGP session would provide a basic level of eBGP access security.

The stub site router will need to also be preconfigured or somehow automatically generate an Autonomous System Number (ASN) to use for establishing the eBGP session or sessions. How the ASN is preconfigured or generated is out of scope for this memo, and is left to future work.

Once the eBGP session is established, the peer eBGP routers trade routes. These traded routes could include the upstream eBGP providing a default route or other more specific routes, and the downstream stub site router providing a route to its downstream prefix or prefixes.

The downstream prefix or prefixes could be those the stub site router has learned via DHCPv6 Prefix Delegation (DHCPv6-PD) [RFC3633]. An advantage of having the stub site router inject DHCPv6-PD prefixes into the BGP routing domain is that the route information for this or these prefixes within the BGP routing domain would more accurately reflect the state and therefore the availability of the prefixes at the site they've been assigned and are being used it. Stub site routers announcing their own prefixes would also distribute the announcement processing load across the stub site routers rather than concentrating it at the upstream aggregation router(s). This also avoids the upstream aggregation router having to process the DHCPv6-PD response to determine the assigned delegated prefix for subsequent BGP announcement [RFC3633], meaning it can act as a much simpler and pure DHCPv6 relay [RFC8415].

The upstream link(s) that a stub site is attached to does not have to be limitied to being a true link-layer point-to-point link, meaning that the link only supports a single router pair of a stub and upstream aggregation router. The link could be a multi-access link, with the single link supporting many stub site routers and a number of upstream aggregation routers.

As the eBGP Functional Anycast address is a Link-Local Visible Scope address, the address is configured as an anycast address on the upstream aggregation routers' stub site facing network interface. This results in the receiver of the Neighbor Advertisements for this address using the information received in the first received Neighbor Advertisement to update its neighbor cache, rather than the last and most recently received Neighbor Advertisement. These types of Neighbor Advertisements are known as "Anycast Neighbor Advertisements" in [RFC4861].

[RFC4861] says that Anycast Neighbor Advertisements should be delayed a random amount of time between 0 and MAX_ANYCAST_DELAY_TIME, a variable with a default value of 1 second. This random delay is to reduce the probability of loss of the Neighbor Advertisement due to network congestion.

Specific to this eBGP use case, the Anycast Neighbor Advertisements delay could include other metrics in the calculation to more intelligently distribute the eBGP sessions across the set of upstream aggregation routers. For example, the number of existing eBGP sessions could be a metric, where an upstream aggregation router delays its Anycast Neighbor Advertisement longer when it has more established eBGP sessions.

An operator set router preference metric could be considered, allowing the operator to more gracefully phase out a legacy upstream aggregation router by setting it preference lower than the newer upstream aggregation routers. The operator would then manually terminate the eBGP sessions individually on the legacy upstream aggregation router, at a rate of something like one ever 3 seconds, causing them to be restablished on the higher preference and newer upstream aggregation routers. This would be more graceful than terminating all eBGP sessions at once on the legacy upstream aggregation router by, for example, switching it off.

Branch office stub router, automatically attempts to establish a BGP session with a well-known functional anycast address "out of the box" over the default WAN interface.

IANA assigned well-known BGP Anycast Function Identifier

Link-local scope Functional Anycast address. Provides a minimum level of security, as only possible to establish BGP sessions between direct link peers.

Use unspecified prefix (comment that fe80::/64 could be used, although unnecessary)

Well-known AS Number used by all stub routers. This makes the BGP sessions eBGP sessions. Routers will reject routes from other stub routers using the same ASN, however this is both fine and ideal as this is a stub router - default only plus announcing its local prefix(es).

Sub router acquires a delegated prefix via DHCPv6-PD

The delegated prefix is announced via the BGP session. Stops the upstream aggregation router needing to observe a DHCPv6 server's relayed response to then announce the delegated prefix into the network.

Upstrem router accepts and establishes BGP sessions with any link-local address from the well known ASN, to the Functional Anycast BGP address.

There are potential trust issues here. BGPsec? Use the first BGP session to bootstrap connectivity to then establish a more trusted connection of some sort via PKI. Requirement for being link-local peers adds a minimal level of security and trust, but not much.

5.7.4. An ISP's Anycast DNS Resolvers

ISPs' IPv4 DNS resolvers have been the target of Distributed Denial of Service attacks (DDoS) [REF], with the attacks launched from the Internet.

These attacks have been possible because ISPs' have assigned their DNS resolvers public IPv4 addresses, with the public IPv4 addresses being both globally unique and globally reachable.

The need for global uniqueness comes from the requirement for the DNS resolvers to have an addresses that are not present within the ISP's customers' networks. Inherent with global uniqueness of a public IPv4 address is global reachability. To protect the DNS resolvers from DDoS attacks, an ISP has to actively configure protection mechanisms such as packet filters that discard traffic from the Internet, while continuing to allow the ISP's customers to use the DNS resolver.

There are two drawbacks of having to use purposely configured protection mechanisms such as packet filters once the DNS resolver has a publically unique and reachable address. Firstly, as the public IPv4 address is normally reachable, an error in configuring the packet filter means a "fail unsafe" consequence.

Secondly, packet filters can only be applied within the local network. This means that the large volume of DDoS traffic will reach the local network before it can be discarded. This discarded DDoS traffic consumes network capacity on paths towards the network that should instead be available to legitimate traffic towards the network.

Ideally, the ISP could assign its DNS resolvers addresses that should be unique within both the ISP's network and all of its customers' networks. The addresses should be reachable from the customers' networks while not being reachable from the Internet. Inherently, these customer and ISP only visible addresses would protect the DNS resolvers from Internet launched DDoS attacks. There would be no need for the ISP to configure packet filters to protect the DNS resolvers from the Internet, and as the DNS resolvers addresses are unreachable from the Internet, it would not be possible to send large volumes of DDoS traffic towards them. The ISP's Internet transit capacity would be more available for legitimate traffic.

Unique Local Addresses (ULA) [RFC4193] would appear to be addresses that could be used for this purpose. They are intended to be globally unique, due to their embedded 41 bit random number, meaning that they should not collide with any of the ISP's customers network's addresses. They are also not intended to be reachable globally across the Internet.

However, the ISP's ULA addresses assigned to its DNS resolvers would be unlikely be realiably reachable from all of its customers' networks. The IPv6 source address selection algorithm tries to pick source addresses that have high order prefix address bits that match those of the destination [RFC6724]. Consequently, to reach an ISP's ULA addressed DNS resolvers, customers' hosts would pick their ULA source addresses, should they have them. These packets may reach the ISP's DNS resolvers, due to customers' default routes, however the DNS response return packets are unlikely to reach the customers' hosts as the ISP is unlikely to know customers' ULA routing prefixes, due to trading of ULA routing prefixes being prohibited by default [RFC4193].

So the source addresses that customers' hosts use when sending to the ISP's DNS resolvers need to be of greater scope and reachability than ULA addresses, while the ISP's DNS resolvers need to have addresses that have a greater scope and reachability than ULA addresses, yet are not IPv6 Globally Unique Addresses [RFC4291].

Customers' GUA addresses would meet this customer host source address requirement, while IPv6 Functional Anycast addresses with a Network Service Provider Visibility Scope would meet the ISP's DNS resolver address requirements.

5.7.5. Microservices Architecture Applications

(MRS: Any possible application here? Perhaps service redundancy and service anycast service addresses.

5.7.6. Global Time Distribution Network

We Have The Time Company (WHTT) are an enterprise who specialise in providing accurate time to global clients across the Internet, via the Network Time Protocol.

To provide robust time across they Internet, they provide access to their NTP servers via Functional Anycast addresses.

WHTT have a GUA /32 assignment from their Regional Internet Registry. They provide time to clients via the following Global scope Functional Anycast address, with a Global scope, an anycast domain prefix of 2001:db8::/32, a Prefix Length of 32 (0x20), and the well known NTP Anycast Function Identifier of 0x101.

* aae0:2001:db8:0:0:2000::101

5.7.7. Multipath Transport Layer Protocols

Multipath transport layer protocols, such as MPTCP [RFC6824] and SCTP [RFC3286], establish a full multipath session between hosts in three stages, using multiple connections.

Stage one involves establishing an initial connection between the hosts. During stage two, the hosts' remaining set of IP addresses are exchanged. Finally, in stage three, the full multipath session is established, with the hosts establishing further connections between the alternative IP addresses exchanged during stage two. Note that during the multipath session, any of the connections could fail or could be purposely torn down, and as long as at least one connection persists, the multipath session continues.

When multipath transport protocols are used for client-server applications, a single common IPv6 anycast address could be used by multiple servers, and then for the initial connection between the clients and servers during stage one.

During stage two, the server limits the set of alternative IP addresses it supplies to clients to its unicast addresses, excluding its one or more anycast addresses.

Subsequent connections that establish the full multipath session during stage three would then be limited to only being established between the unicast addresses of the clients and server.

Once any of these stage three unicast address connections is established, the server could actively tear down the initial connection to its anycast address, meaning that all of the now remaining connections are established with the individual server's unicast address or addresses.

Switching to using only unicast connections for the remainder of the multipath session overcomes one of the significant limitations of the use of anycast with connection oriented transport layer protocols [RFC1546]; the limitation that where the anycast address instance's packets are delivered to depends on the network's forwarding domains topology, and if the network topology changes, packets may be delivered to a different anycast instance that is unaware of and has not previously been involved in the transport layer connection.

With this use of both anycast and unicast addresses in combination with multipath transport protocols, the effects of this anycast limitation are reduced to the time between establishment of the initial client-server connection to the server's anycast address, and when the first client-server connection is established using exclusively unicast addresses. This is in contrast to this risk possibility existing for the entire duration of a single path transport layer protocol connection to an anycast address.

The benefit of the above use of anycast in combination with multipath transport layer protocols applies to all types of anycast addresses discussed in this memo.

There is a further advantage if Formal Anycast addresses are used. This is that as a Formal Anycast address is easily identified due to its well known prefix, the multipath transport layer protocol implementation does not have to be configured with which of the server's IPv6 addresses are its anycast addresses, so they can be excluded from the IPv6 address exchange that occurs during stage two.

6. Security Considerations

Functional Anycast addresses should not introduce any new security concerns in comparison to the use of addresses from within the unicast address space as anycast addresses. [RFC7094] provides considerable anycast related security discussion and references.

The ability to identify a Functional Anycast address using its well known 8 bit prefix, and the inclusion of forwarding scopes in the addresses, provide opportunies to enhance security of anycast services.

7. IANA Considerations

IANA are requested to register the aa00::/8 prefix in the Internet Protocol Version 6 Address Space registry for use with Formal Anycast addresses. If aa00::/8 is not chosen, then fa00::/8 is a proposed alternative.

IANA are requested to update the use of the IPv6 multicast scopes registry to also record use with Formal Anycast IPv6 addresses.

IANA are requested to record a new IPv6 multicast and Formal Anycast scope named the "Network Service Provider" scope, with a scope value of B in hexidecimal.

IANA are requested to register a new ICMPv6 Destination Unreachble code for Edge of Visible Scope Reached.

IANA are requested to establish a registry for the Flags field of Functional Anycast addresses, and to reserve the T flag to indicate transient Anycast Function Identifiers.

IANA are requested to establish a registry for well known Anycast Function Identifiers, and to reserve the values described previously in the "Assigned Anycast Function Identifers" section of this memo.

8. Acknowledgements

Gavin Owen prompted the lunch time conversation where the author joined together and immedidately recognised the benefits of using of anycast addresses in combination with multipath transport layer protocols to provide more robust anycast services.

Review and comments were provided by YOUR NAME HERE!

This memo was prepared using the xml2rfc tool.

9. Change Log [RFC Editor please remove]

draft-smith-6man-form-func-anycast-addresses-00, initial version, 2018-10-22

draft-smith-6man-form-func-anycast-addresses-01, updates, 2019-11-03

* Fixed scope location error in addresses used throughout
* Added section on the idea of an anycast address registration protocol

* Reference updates

draft-smith-6man-form-func-anycast-addresses-02, updates, 2024-02-23

* Last Instance flag

10. References

10.1. Normative References

[RFC0854] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD 8, RFC 854, DOI 10.17487/RFC0854, May 1983, <https://www.rfc-editor.org/info/rfc854>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

10.2. Informative References

[IANA-IPV6ANYC] "Internet Protocol Version 6 (IPv6) Anycast Addresses", <https://www.iana.org/assignments/ipv6-anycast-addresses/ipv6-anycast-addresses.xhtml>.

[IANA-IPV6MCAST] "IPv6 Multicast Address Space Registry", <https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml>.

[IANA-IPV6RESA] "IPv6 Multicast Address Space Registry", <https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml>.

[RFC0318] Postel, J., "Telnet Protocols", RFC 318, DOI 10.17487/RFC0318, April 1972, <https://www.rfc-editor.org/info/rfc318>.

[RFC1546] Partridge, C., Mendez, T., and W. Milliken, "Host Anycasting Service", RFC 1546, DOI 10.17487/RFC1546, November 1993, <https://www.rfc-editor.org/info/rfc1546>.

[RFC2526] Johnson, D. and S. Deering, "Reserved IPv6 Subnet Anycast Addresses", RFC 2526, DOI 10.17487/RFC2526, March 1999, <https://www.rfc-editor.org/info/rfc2526>.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <https://www.rfc-editor.org/info/rfc2710>.

[RFC2941] Ts'o, T., Ed. and J. Altman, "Telnet Authentication Option", RFC 2941, DOI 10.17487/RFC2941, September 2000, <https://www.rfc-editor.org/info/rfc2941>.

[RFC2946] Ts'o, T., "Telnet Data Encryption Option", RFC 2946, DOI 10.17487/RFC2946, September 2000, <https://www.rfc-editor.org/info/rfc2946>.

[RFC3286] Ong, L. and J. Yoakum, "An Introduction to the Stream Control Transmission Protocol (SCTP)", RFC 3286, DOI 10.17487/RFC3286, May 2002, <https://www.rfc-editor.org/info/rfc3286>.

[RFC3306] Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, DOI 10.17487/RFC3306, August 2002, <https://www.rfc-editor.org/info/rfc3306>.

[RFC3310] Niemi, A., Arkko, J., and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, DOI 10.17487/RFC3310, September 2002, <https://www.rfc-editor.org/info/rfc3310>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <https://www.rfc-editor.org/info/rfc3633>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/info/rfc4252>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <https://www.rfc-editor.org/info/rfc4786>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI 10.17487/RFC5308, October 2008, <https://www.rfc-editor.org/info/rfc5308>.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008, <https://www.rfc-editor.org/info/rfc5340>.

[RFC5505] Aboba, B., Thaler, D., Andersson, L., and S. Cheshire, "Principles of Internet Host Configuration", RFC 5505, DOI 10.17487/RFC5505, May 2009, <https://www.rfc-editor.org/info/rfc5505>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[RFC5942] Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, DOI 10.17487/RFC5942, July 2010, <https://www.rfc-editor.org/info/rfc5942>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <https://www.rfc-editor.org/info/rfc6724>.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, DOI 10.17487/RFC6824, January 2013, <https://www.rfc-editor.org/info/rfc6824>.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <https://www.rfc-editor.org/info/rfc7045>.

[RFC7094] McPherson, D., Oran, D., Thaler, D., and E. Osterweil, "Architectural Considerations of IP Anycast", RFC 7094, DOI 10.17487/RFC7094, January 2014, <https://www.rfc-editor.org/info/rfc7094>.

[RFC7346] Droms, R., "IPv6 Multicast Address Scopes", RFC 7346, DOI 10.17487/RFC7346, August 2014, <https://www.rfc-editor.org/info/rfc7346>.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix Length Recommendation for Forwarding", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015, <https://www.rfc-editor.org/info/rfc7608>.

[RFC7723] Kiesel, S. and R. Penno, "Port Control Protocol (PCP) Anycast Addresses", RFC 7723, DOI 10.17487/RFC7723, January 2016, <https://www.rfc-editor.org/info/rfc7723>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/info/rfc7872>.

[RFC8155] Patil, P., Reddy, T., and D. Wing, "Traversal Using Relays around NAT (TURN) Server Auto Discovery", RFC 8155, DOI 10.17487/RFC8155, April 2017, <https://www.rfc-editor.org/info/rfc8155>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8633] Reilly, D., Stenn, H., and D. Sibold, "Network Time Protocol Best Current Practices", BCP 223, RFC 8633, DOI 10.17487/RFC8633, July 2019, <https://www.rfc-editor.org/info/rfc8633>.

Author's Address

Mark Smith
PO BOX 521
HEIDELBERG VIC 3084
Australia
Email: markzzzsmith@gmail.com