DHC Working Group                                Sheng Jiang
Internet Draft                      Huawei Technologies Co., Ltd
Intended status: Informational                   July 09, 2012
Expires: January 05, 2013

**Semantic IPv6 Prefix**
**draft-jiang-semantic-prefix-00.txt**


Status of this Memo

Copyright Notice

Abstract

   Some Internet Service Providers desire to be aware of more
   information about each packet, so that packets can be treated
   differently and efficiently. IPv6, with a large address space, allows
   semantics to be embedded into addresses. Routers can easily apply
   relevant operations accordingly. This document provides analysis on
   how to form semantic prefix and corresponding use cases, and
   identifies the technical requirements to maximize the benefits of the
   semantic prefix approach. It is recommended to use 4~12 bits in
   prefix for embedded semantics.

Table of Contents

## 1. Introduction

   While the global Internet increases explosively, more and more
   differentiated requirements are raised for the packet delivery of
   networks. Internet Service Providers desire to be aware of more
   information about each packet, such as destination location, user
   types, service types, applications, security requirments, quality
   requirements, etc. Based on the information, network operators could
   treat packets differently and efficiently.

   However, except for destination location, almost of abovementioned
   information is not expressed explicitly. Hence, it is difficult for
   network operators to identify.

   Two passive and indirect technologies are already developed to
   distinguish the packets. Deep Packet Inspection (DPI) has been used
   by ISPs to learn the characters of packets. But DPI is expensive for
   both operational costs and process latency. Its time delay is too
   much to be able to be used for real time traffic control. Overlay
   networks are constructed in order to permit routing of packets to
   destinations not specified by IP addresses. But still, the overlay
   has no control over how packets are routed in the underlying network
   between two overlay nodes. Although tunnel or label forwarding may
   operate the traffic path, they introduce extra overhead while they
   depend on indirect information sources.

   An initiative solution, Quality of Service (QoS) and DiffServ
   [RFC2474] was also developed. It specifies a simple, scalable and
   coarse-grained mechanism for classifying and managing network
   traffic. However, the DiffServ fields set by the packet senders are
   not trustable by the network operators. In the real user case, ISPs
   deploy "remarking" points at the edge network, which classify each
   received packet and rewrite its DiffServ field according to user
   information learned from AAA or VLAN.

   The abovementioned solutions are mainly developed in IPv4 era, in
   which IP address is only locator, nothing else, giving the limited
   space. Although DiffServ was developed identically for IPv4 and IPv6,
   it did not inherit the same limitation.

   IPv6 has broken such limitation with its very large address space. It
   allows certain semantics to be embedded into addresses. Applications
   or ISPs can proactively embed pre-defined information into addresses
   so that intermediate devices can easily apply relevant operations on
   packet since addresses are the most explicit element in a packet. It
   provides an easy access and trustable fundamental for packet
   differentiated treatment.

The technical fact that IPv6 allow multiple addresses on a single
interface also provides precondition for the approach that user
chooses application-associated address differently.

This approach transfers much network complexity to the planning and
management of IPv6 address and IP address based policies. It indeed
simplifies the management of ISP networks.

This document provides analysis on how to form semantic prefix and
its user cases. It is recommended to use 4~12 bits in prefix for
embedded semantics. This document also analyzes the technical gaps to
maximum the benefits of semantics prefix approach.

## 2. Why Prefix

Although interface identifier of IPv6 address has arbitrary bits and
extension header can carry much more information, they are not
trustable by network operators. Selfish users may easily change the
setting of interface identifier or extension header in order to
obtain undeserved priorities/privileges, while servers or enterprise
users may be much more self-restricted since they are charged
accordingly.

Prefix is almost the only thing an operator can trust in an IP packet
because it is delegated by the network and the network can detect any
undesired modifications, then filter the packet.

The prefix concept here refers the most left bits in IP addresses,
that are delegated by the network management plane. It could be
longer than 64, if the network operators strictly manage the address
assignment by using Dynamic Host Configuration Protocol for IPv6
(DHCPv6) [RFC3315] (but in this case standard Stateless Address
Autoconfiguration - SLACC [RFC4862] cannot be used).

Two major arguments against this approach should be considered. One
of them is practical: although IPv6 address space is plentiful, it
should not be wasted. This argument can be dealt with by ensuring
that only a small number of traffic classes are identified within a
given user's traffic, so only a few bits in the prefix are needed.
The second argument is that addresses should not, as a matter of
principle, contain application semantics, because this violates the
layering structure of protocols. This argument can be answered by
ensuring that the only impact of the approach on the routing and
forwarding system is to modestly increase the number of internal
routes handled by the ISP concerned; there should be no impact on
aggregated routes that the ISP announces to other ISPs.

**3**. **The Semantic Prefix Domain**

A Semantic Prefix domain, analagous to a Differentiated Services
Domain [RFC2474], is a contiguous portion of the Internet over which
a consistent set of semantic prefix policies are administered in a
coordinated fashion.  A Semantic Prefix domain can represent
different administrative domains or autonomous systems, different
trust regions, different network technologies, hosts and routers,
different user groups, different services, different traffic groups,
different applications, etc.

The selections of semantics are various among different Semantic
Prefix Domains. Network operators should choose semantics according
to their needs for network management and services management. If an
ISP has several discontinuous address blocks, it may be organized as
a single semantic Prefix domain if the same semantic definition
shared among these discontinuous address blocks. If these blocks have
different sizes, their semantic prefix domains may be distinguished
each other by minimum differences of semantic definition.

A Semantic Prefix domain has a set of pre-defined semantic
definitions. Without an efficient semantics notification or
exchanging mechanism, the definitions of semantics are only
meaningful within local semantic prefix domain. The semantics
notification or exchanging does not have to through protocols. Manual
interactions between network operators may also work out. However,
this may involve trust models among network operators.

Sharing semantic definition among Semantic Prefix domains enables
more semantic based network operations.

**4**. **The Embedded Semantics**

As mentioned in Section 1, much information regarding to packets is
useful for network operators, such as destination location, user
types, service types, applications, security requires, quality
requirements, etc. But, the prefix bits that can be used for embedded
semantics are very limited. Therefore, only the selected, most useful
semantics can be embedded in the prefix. Note, however, that DiffServ
provides a very rich QoS semantic with only 6 bits. The available
bits increase largely in the strictly managed network by DHCPv6.

The following are some semantics may be useful by network operators:
user types, service types, security information, traffic identity
types, applications or application types, etc. When used, all of them
should be restricted in a highly abstracted way.

In a given Semantic Prefix Domain, multiple semantics can be used
combinatorially. They may be organized by using semantic type bits in

prefix or any pre-defined arbitrary way. However, the former is preferred.

To use the limited bits efficiently, bits semantics should be pre-defined very carefully. Some formation recommendations are introduced below.

## 5. Formation of Semantic prefix

Depending on the IPv6 address space that network operators received from IANA, the number of arbitrary bits in prefix is different. For now, this document only discusses unicast address within IP Version 6 Addressing Architecture [RFC4291].

Typically, network operators would have /13 ~ /20 address space according to its user scale. It allows 51~44 arbitrary bits in prefix to be set by network operators (assuming the network is not strictly managed by DHCPv6). However, many ISPs plan to assign /56 or even /48 for subscribers, the arbitrary bits are reduced to 43~32.

The locator function of IP address should be ensured first. Enough consideration should be given for future expanding. Some address space may be wasted in aggregation. For a Semantic Prefix Domain that organizes several millions subscribers with a continuous IPv6 address block, 28 bits for locator function is a minimum safe allocation. Several bits may be good for safety margin.
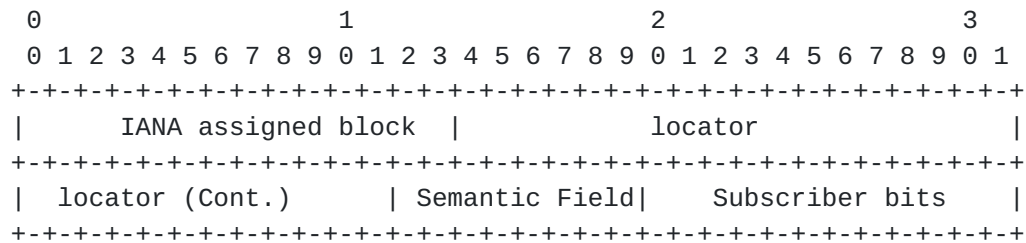
The current network is mainly aggregated according to locator. Hence, it is recommended using the most left bits of prefix for locator function and lower bits for semantics. However, if the network operator would like to organize network aggregation by semantic prior, using higher bits for semantics is also possible. Mixed aggregation model can be reached by put semantics or part of semantics bits in the middle of locator bits.

According to the above analysis, it is recommended to use 4~12 bits in prefix for embedded semantics. It is recommended network operator only use necessary semantics when they can bring benefits to network operations.

The network operator should be very careful to plan and manage the semantic field. The first and most important principle is to avoid semantic overlap. Any potential scenarios that a given packet may be mapped two or more semantic prefixes are considered harmful.

While assigning all these bits on a separated subfield mechanism is considered inefficient and lack of flexibility, it is recommended to assign in low granularity, such as bit by bit.

## 5.1. An example of semantic prefix

```
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |      IANA assigned block  |              locator              |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  locator (Cont.)      | Semantic Field|    Subscriber bits    |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The above figure represents an example of semantic prefix.

In this example, the semantic prefix domain have a /14 IPv6 address
space. The 30 most-left bits are allocated as locator. It serves
network aggregation of topology based. The 12 most-right bits are
subscriber bits. It means /52 prefix is assigned to subscribers. 8
bits (from bit 44 to 51) are assigned as semantic field. It may be
assigned further for semantic combinations.

A further detailed example, combing user type, service type, VPNs,
and application virtual overlay networks, the semantic field can be
assigned like blow (presented in octet):

```
  00   Normal individual user with normal internet access services
  01   High-end individual user with normal internet access
         services
  02   High-end individual user with secure internet access
         services
  03~07 Reserved
  08   Enterprise user with normal internet access services
  09   Enterprise user with secure internet access services
  0A~0F Reserved
  10~3F VPNs (with 48 sub-IDs)
  40~7F Application virtual overlay networks (with 64 sub-IDs)
  80~FF Reserved
```

In practice, a host may belong to several semantics. It means several
IPv6 addresses are available on a single physical interface. A
certain packet would only serve a certain semantic. The stack or
applications on that host must know and understand these semantics
and its correspondent bits in order to choose right source address
when forming a packet.

## 6. Benefits

This section presents some, definitely not all, benefits. Depending
on embedded semantics, various beneficial scenarios can be expected.

- Easy measurement and statistic

The semantic prefix provides explicit identifiers for measurement and statistic. They are as simple as checking certain bits of address in each packets.

- Easy flow control

By applying policies according to certain bit value, it is easy to control packets that have the same semantics.

- Policy aggregation

Semantic prefix allows many policies to be aggregated according to the same semantics in the policy based routing system [RFC1104].

- Application-aware routing

Embedding application information into IP addresses is the simplest way to realize application aware routing.

## 7. Gaps

The simplest model of semantic prefix is only embedded abstracted user type semantic into the prefix. It can be supported with the current network architecture because each subscribe still assigned one prefix, while they are not notified the semantic within it.

The more semantics embedded into prefix, the more complicated functions are needed for prefix delegation, host notification and address selections.

- Associate semantics with prefix delegation

When DHCPv6-PD [RFC3633] delegates a prefix, the associated semantics should be bounded.

- Notify prefix semantics to hosts

When a host connects to network, it should be assign a short prefix locator with some enabled semantics rules.

- Address selection according to semantics on hosts

In this architecture, hosts have to be intelligent enough to choose its source address according to its given information. It may also receive address select information from the applications. In some complicated scenarios, choosing destination address may also need further supporting functions.

The current address selection algorithms and address selection API [RFC5014] are too simple to support this architecture.

8. Security Considerations

   This document provides no new security features.

9. IANA Considerations

   This document has no IANA considerations.

10. References

10.1. Normative References

   [RFC1104] H.W. Braun, "Models of policy based routing", RFC 1104,
             June 1989.

   [RFC2474] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition
             of the Differentiated Services Field (DS Field) in the IPv4
             and IPv6 Headers", RFC 2474, December 1998

   [RFC3315] R. Droms, et al., "Dynamic Host Configure Protocol for
             IPv6", RFC 3315, July 2003.

   [RFC3633] O. Troan, and R. Droms, "IPv6 Prefix Options for Dynamic
             Host Configuration Protocol (DHCP) version 6", RFC 3633,
             December 2003.

   [RFC4862] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless
             Address Autoconfiguration", RFC 4862, September 2007.

   [RFC4291] R. Hinden, and S. Deering, "IP Version 6 Addressing
             Architecture", RFC4291, February 2006.

10.2. Informative References

   [RFC5014] E. Nordmark, S. Chakrabarti, J. Laganier, "IPv6 Socket API
             for Source Address Selection", RFC 5014, September 2007.


   Author's Addresses

   Sheng Jiang
   Huawei Technologies Co., Ltd
   Q14, Huawei Campus
   No.156 Beiqing Road
   Hai-Dian District, Beijing  100095
   P.R. China
   EMail: jiangsheng@huawei.com