Network Working Group   S. Jiang, Ed.
Internet-Draft   Huawei Technologies Co., Ltd
Intended status: Informational   Q. Sun
Expires: January 16, 2014   China Telecom
                                                              I. Farrer
                                                      Deutsche Telekom AG
                                                                  Y. Bo
                                             Huawei Technologies Co., Ltd
                                                               T. Yang
                                                          China Mobile
                                                         July 15, 2013

             Analysis of Semantic Embedded IPv6 Address Schemas
                    draft-jiang-semantic-prefix-06

Abstract

   This informational document discusses the use of embedded semantics
   within IPv6 address schemas. Network operators who have large IPv6
   address space may choose to embed some semantics into their IPv6
   addressing by assigning additional significance to specific bits
   within the prefix. By embedding semantics into IPv6 prefixes, the
   semantics of packets can be easily inspected. This can simplify the
   packet differentiation process. However, semantic embedded IPv6
   address schemas have their own operational cost and even potential
   pitfalls. Some complex semantic embedded IPv6 address schemas may
   also require new technologies in addition to existing Internet
   protocols.

   The document aims to understand the usage of semantic embedded IPv6
   address schemas, and neutrally analyze on the associated advantages,
   drawbacks and technical gaps for more complex address schemas.

   This Internet-Draft will expire on January 16, 2014.

Copyright Notice

Table of Contents

1. Introduction

   As the global Internet expands, it is being used for an increasingly
   diverse range of services. These services place differentiated
   requirements upon packet delivery networks meaning that Internet
   Service Providers and enterprises need to be aware of more
   information about each packet in order to best meet a specific
   service's needs. Dividing a network into different subnets according
   to different semantics is already widely existing today, mostly
   motivated by either topological aspects, logical user/device groups,
   and/or trust/security domains.

   In order to inspect the semantics of packets so that they can be
   treated differently, some network operators have chosen to embed
   semantics into IPv6 prefixes. Routers and other intermediary devices
   can easily apply relevant policies as required. User types, service
   types, applications, security requirements, traffic identity types,
   quality requirements and other criteria may be used according to how
   a network operator may want to differentiate its services. Packet-
   level differentiation can also enable flow-level and user-level
   differentiation. Consequently, the network operators can treat
   network packets differently and efficiently. It is believed this
   mechanism can simplify the management and maintenance of networks.

   However, semantic embedded IPv6 address schemas come with their own
   operational cost and even pitfalls. Some complex semantic embedded
   IPv6 address schemas may also require technologies additional to
   existing Internet protocols.

   While network operators, who already have large IPv6 address space
   allocations, are free to plan and deploy addressing in their
   preferred way (including semantic embedded IPv6 address schemas), it
   is useful to analyze the benefits and drawbacks of a semantic
   approach to addressing.

   The document only discusses the usage of semantics within a single
   network, or group of interconnected networks which share a common
   addressing policy, referred to as a Semantic Prefix Domain.

This document does not intend to suggest the standardization of any
common global semantics. It does not intend to draw any conclusions,
either recommending this kind of address schemas or not. It aims to
provide network operators with relevant information to use in the
creation of their own addressing policy.

2. Terminology

The following terms are used throughout this document:

Semantic Prefix: A flexible-length IPv6 prefix which embeds certain
   semantics.

Semantic Prefix Domain: A portion of the Internet over which a
   consistent semantic-prefix based policy is in operation.

Semantic Prefix Policy: A policy based on the embedded semantics
   within IPv6 prefix.

3. Understanding of Semantic IPv6 Prefix Address Schema

Some network operators (either ISPs or enterprise network operators),
who have large IPv6 address space, have chosen to embed certain pre-
defined semantics into their IPv6 address schemas by assigning
additional significance to specific bits within the prefix. The IPv6
addresses of each packet can then explicitly express semantics.
Consequently, intermediate devices can easily apply relevant packet
differentiating operations accordingly. This mechanism may divert
much network complexity to the planning and management of IPv6
addressing and IP address based policies.

For illustrations of how semantic prefixes could be applied in real-
world scenarios, Appendix A describes an ISP example semantic IPv6
prefix address schema; Appendix B introduces an enterprise semantic
IPv6 prefix example; and Appendix C introduces an enterprise example
in which a multiple-site enterprise network with several prefixes of
different lengths is organized as a single, contiguous Semantic
Prefix Domain.

3.1. Overview of Semantic IPv6 Prefix Address Schema

A network operator first plans their IPv6 address schema, in which
useful semantics (see Section 3.5) are embedded into prefix. They
then delegate prefixes with the corresponding semantics to users.
The users generate their IPv6 addresses based on assigned prefixes.
Then, when the IPv6 stack on the user devices forms packets, the
source addresses comprise compliance semantics. For trust reasons,
the filters on the edge router may drop packets which are not
compliant with assigned prefixes.

The embedded semantics are only meaningful within a network domain
which implements a single policy (see Section 3.4). Different
service providers may make very different choices regarding the
specific semantics which are relevant to their networks. Therefore,
it is not possible or even desirable to attempt to standardize a
general semantic prefix policy.

Forwarding policies, access control lists, policy-based routing,
security isolation and other network operations (see Section 3.6) can
be easily applied according to semantics, which are self-expressed by
the source address of every packet. Also, the semantics of the
destination address may be taken in account if the destination is in
the same Semantic Prefix Domain or the peer Semantic Prefix Domain
whose semantics has been notified.

3.2. Existing Approaches to Traffic Differentiation

There are several existing approaches which have been developed that
can assist operators in identifying and marking traffic. These
solutions were mainly developed in the IPv4 era, where the IP address
is used as a host locator and little else. The limited capacity of a
32-bit IPv4 address provides very little room for encoding additional
information. Correspondingly, these approaches are indirect,
inefficient and expensive for operators.

3.2.1. Differentiated Services

Quality of Service (QoS) based on and Differentiated Services
[RFC2474] is a widely deployed framework specifying a simple and
scalable coarse-grained mechanism for classifying and managing
network traffic. But in a service provider's network, DiffServ
codepoint (DSCP) values cannot be trusted when they are set by the
customer as these are arbitrary values.

In real-world scenarios, ISPs deploy "remarking" points at the
customer edge of their network, re-classifying received packets by
rewriting the DSCP field according to local policy using information
such as the source/destination address, IP protocol number and
transport layer source/destination ports.

The traffic classification process leads to increased packet
processing overhead and complexity at the edge of the service
provider's network.

DSCP mechanism abstracts all the semantics into a single-dimension
service classes. This abstract processing has lost a lot of semantic
information, which providers want to inspect for every packet, then
process the packet accordingly.

The DSCP in the IPv6 header traffic class field allows 6-bits for
encoding service provider specific information related to the
contents of the packet. Whilst this is a useful part of an overall
packet differentiation architecture, the relative small number of
available bits (when compared to the available number of bits within
the service providers prefix) means that it cannot be used in
isolation.

3.2.2. Deep Packet Inspection

Deep Packet Inspection (DPI) may also be used by ISPs to learn the
characteristics of users packets. This involves looking into the
packet well beyond the network-layer header to identify the specific
application traffic type. Once identified, the traffic type can be
used as an input for setting the packet's DSCP or other actions.

But DPI is expensive both in processing costs and latency. The
processing costs means that dedicated infrastructure is necessary to
carry out the function. The incurred latency may be too much for use
with any delay/jitter sensitive applications. As a result, DPI is
difficult for large-scale deployment and it's usage is usually
limited to small and specific functions in the network. In short, it
is not scalable, and cannot support realtime network operations.

3.3. Justification for Semantics with the IPv6 Prefix

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

With proper access control filters deployed, the prefix can be
trusted by the network operators and is simple to inspect in the IP
header of a packet. The packets with the noncompliance source
addresses should be filtered. The prefix is delegated by the network
and therefore the network is able to detect any undesired

modifications and filter the packet accordingly. This also makes it
possible for the service provider to increase the level of trust in a
customer-generated packet. If the packet has an source or
destination address which is outside of the network operator's policy
then a session will simply fail to establish.

3.4. The Semantic Prefix Domain

A Semantic Prefix Domain is a portion of the Internet over which a
consistent set of semantic-prefix-based policies are administered in
a coordinated fashion. It is analogous to a Differentiated Services
Domain [RFC2474]. Some of the characteristics that a single Semantic
Prefix Domain could represent include:

a. Administrative domains

b. Autonomous systems

c. Trust regions

d. Network technologies

e. Hosts

f. Routers

g. User groups

h. Services

i. Traffic groups

j. Applications

A Semantic Prefix Domain has a set of pre-defined semantic
definitions, which are only meaningful locally. Without an efficient
semantics notification, exchanging mechanism or service agreement,
the definitions of semantics are only meaningful within local
Semantic Prefix Domain. Agreements on definitions between network
operators could be made. However, this may involve trust models
among network operators. Sharing semantic definition among Semantic
Prefix Domains enables more semantic based network operations.

An enterprise Semantic Prefix Domain may span several physical
networks and traverse ISP networks. However, when an interim network
is traversed (such as when an intermediary ISP is used for
interconnectivity), the relevance of the semantics is limited to
network domains that share a common Semantic Prefix Policy.

If an ISP has several non-contiguous address blocks, they may be
organized as a single Semantic Prefix Domain if the same Semantic
Prefix Policy is shared across these non-contiguous address blocks.

3.5. The Embedded Semantics

The size of the operator assigned prefix means that there is
potentially much more scope for embedding semantics than has
previously been possible. The following list describes some
suggested semantics which may be useful to network operators besides
source/destination location:

a. User types

b. Applications

c. Security domain

d. Traffic identity types

e. Quality requirements

f. Geo-location

The selection of semantics varies among different network operators.
They may choose one or more semantics to be embedded into their IPv6
address schemas, depending on what is important for them and what may
trigger packet differentiation processes in their networks. The
selection criterion and the impact of each choice are out of scope of
this document.

3.6. Network Operations Based on Semantic Prefixes

From the explicit semantics contained within the addresses of each
packet, many network operations can be applied. Compared with
traditional operations, these operations are easier to realize and
stable. Although detailed operation vary depending on various
embedded semantics, the network operations based on semantic prefix
can be abstracted into following categories:

a. Statistic based on certain semantic. Any embedded semantic can
    be set as a statistic condition. In other words, any embedded
    semantic can be measured independently.

b. Differentiate packet processing. Many packet processing
    operations can be applied based on the semantic differentiation,
    such as queueing, path selection, forwarding to certain process
    devices, etc.

   c. Security isolation. A set of packet filters that are based on
       semantic can fulfil network security isolation.

   d. Access control. Resource access, authentication, service access
       can be directly based on semantics.

   e. Resource allocation. Resources, such as bandwidth, fast queue,
       caching, etc., can be allocated or reserved for certain semantic
       users/packets.

   f. Virtualization. Within a Semantic Prefix Domain, organizing
       virtual networks is simplified by assigning all the nodes the
       same semantic identifier so that the packets from them can be
       distinguished from other virtual networks.

   It should also be noticed that these operations do not have to be
   processed on the same single device. They may be separated among
   network devices. In other words, if there are multiple semantics in
   a Semantics Prefix Domain, various semantics may be understood and
   treated on different network devices. It is not necessary for all
   network devices in such domain to capable of understanding all
   semantics.

[4](#). Potential Benefits

   Depending on various embedded semantics, different beneficial
   scenarios can be expected.

   a. Semantic prefix address schema provides a directly and explicitly
       mechanism for packet inspection. It improves the inspecting
       efficiency on IPv6 network devices.

   b. Simplified measurement and statistics gathering: the semantic
       prefix provides explicit identifiers which can be used for
       measurement and statistical information collection. This can be
       achieved by checking certain bits of the source and/or
       destination address in each packet.

   c. Simplified flow control: by applying policies according to
       certain bit values, packets carrying the same semantics in their
       source/destination addresses can.

   d. Service segregation: when service related information is encoded
       within the semantic prefix, this can be used to create simple
       access-control lists which can be applied uniformly across all
       network devices. Security zones are such typical services that
       need to be segregated.

   e. Policy aggregation: the semantic prefix allows many policies to
       be aggregated according to the same semantics within the policy
       based routing system [RFC1104].

   f. Easy dynamic reconfiguration of semantic oriented policy: network
       operators may want to dynamically change the policy actions that
       are operated on certain semantic packets. The semantic prefix
       allows such changes be operated easily, as only a small number of
       consistent policy rules need to be updated on all devices within
       the semantic prefix domain.

   g. Application-aware routing: embedding application information into
       IP addresses is the simplest way to realize application aware
       routing.

   h. Easy user behavior management: based on the user type reading
       from the addresses, any improper user behaviors can be easy
       detected and automatically handle by network policies.

   i. Easy network resources access rights management: the
       authentication of access right may already be embedded into the
       addresses. Simple matching policies can filter improper access
       requests.

   j. Easy virtualization: virtual network based on any semantics can
       be easily deployed using the semantic prefix mechanism.

5. Potential Drawbacks

   a. Address consumption caused by lower address utility rate.
       Embedding semantics into IPv6 addresses causes the network to use
       more of the address space that it normally would. The wastage
       comes from aligning. 1) A small addressing requirement for a
       separate type may get the same large address space as a large
       addressing requirement. 2) The number of types in each semantic
       has to align to 2^n, for example, 5 types uses to take 3 bits in
       the prefix.

       Network operators should be aware they may not get more addresses
       because they have allocated their assigned address block(s) for
       semantic use without the addresses actually being in use -
       leading to a lower address utility rate. Although the current
       Regional Internet Registry (RIR) policies do not disallow such
       address usage, such usage has not been taken into account in
       calculating reasonable addressing quotients.

   b. Complexity that is created within the semantic prefix policy.
       Encoding too many semantics into prefixes can come at the expense

of future addressing flexibility. At the same time, embedding
too many semantics may induce semantic overlap. Careful
consideration should be taken with semantics definition.

c. The risk of privacy/information leakage. The semantics in the
address may be guessable, or leaked to outside the organisation.
Therefore, some information of either subscribers or networks may
be leaked, too.

d. Burdening the host OS. In some complex semantic prefix
scenarios, the semantics prefix mechanism puts extra burden on
the originator. In such scenarios, host devices are given
multiple IPv6 prefixes and required to choose correctly. When
forming a packet, the originator of packets (normally the host
OS) has to pick the right address/prefix according to the
semantics to access a service.

e. In order to perform policies based on trusted user/prefix, tight/
strict access control filter linked with prefix assignment is
requested. It is the filter who makes sure the prefix right.
The filter should link back to other states of the user, like
user authentication, etc, in order to match the packet to its
properties and check whether it is mapped to right semantics or
not.

6. Gaps for complex semantic prefix scenarios

The simplest semantic prefix model is to embed only abstracted user
type semantics into the prefix. Current network architectures can
support this semantic prefix model, in which each subscriber is still
assigned a single prefix, while they are not notified the semantic
embedded in the prefix.

In order to fulfill more benefits of the semantic prefix design,
additional functions are needed to allow semantic relevant operations
in networks and semantic relevant interactions with hosts.

IPv6 provides a facility for multiple addresses to be configured on a
single interface. This creates a precondition for the approach that
user chooses addresses differently for different purposes/usages.

6.1. Semantic Notification in the Network

In order to manage semantic prefixes and their relevant network
actions, the network should be able to notify semantics along with
prefix delegation.

When an prefix is delegated using a DHCPv6 IA_PD [RFC3633], the
associated semantics should also be propagated to the requesting
router. This is particularly useful for autonomic process when a new
device is connected.

6.2. Semantic Relevant Interactions between Hosts and the Network

The more that semantics are embedded into a prefix, the more
complicated functions are needed for semantic relevant interactions
between hosts and the network, such as prefix delegation, host
notification, address selections, etc.

In practice, a single host may belong to multiple semantics. This
means that several IPv6 addresses are configured on a single physical
interface and should be selected for use depending on the service
that a host wishes to access. A certain packet would only serve a
certain semantic.

The host's IPv6 stack must have a mechanism for understanding these
semantics in order to select the right source address when forming a
packet. If the embedded semantic is application relevant,
applications on the hosts should also be involved in the address
choosing process: the host IPv6 stack reports multiple available
addresses to the application through socket API (one example is "IPv6
Socket API for Source Address Selection" [RFC5014]). The application
then needs to apply the semantic logic so that it can correctly
select from the offered candidate addresses.

Although [RFC6724] provides an algorithm for source address
selection, some semantic prefix policies may conflict with this
algorithm. In this case, source address selection mechanisms may
need further supporting functions to be developed.

6.3. Additional Technical Extensions

There are several areas in which the semantic prefix could be
extended in order to increase the usefulness and applicability of the
semantic prefix address schema. They are listed here for future
study. Currently, their feasibility, usefulness and applicability
are not carefully studied yet.

- Dynamic Policy Configuration

Dynamic policy configuration would simplify the distribution of
policy across devices in the semantic prefix domain. New functions
or protocol extension are needed to enable dynamic changes to the
policy actions in operation on certain semantic packets.

   - Semantics Announcements to peer networks

   A network may announce all, or some of its Semantic Prefix Policy to
   connected peer networks. This could be used to enable more dynamic
   configuration and enable traffic from different semantic prefix
   domains to traverse different networks whilst having the same
   semantic prefix policy applied. To achieve this automatically by
   message exchanging would require new functions or protocol
   extensions.

   - Extension of Prefix Semantics beyond the left-most 64 bits

   The prefix concept refers here to the left-most bits in the IP
   addresses delegated by the network management plane. The prefix
   could be longer than 64-bits 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 - SLAAC [RFC4862] cannot be used).

   - Organizing consumer/home networks according to semantics

   Consumers or subscribers are currently assigned /48 or /56 prefixes.
   They have bits, which may also count the right-most 64 bits too, to
   organize their networks into subnets. These subnets may be organized
   according to some semantics that are meaningful for the user himself.
   In such scenario, the user acts as the network operator for his own
   network. Some additional tecnologies/functions may be needed to make
   such organizing and follow-up management efficient.

7. IANA Considerations

   This document has no IANA considerations.

8. Change Log (removed by RFC editor)

   draft-jiang-semantic-prefix-04: add new pitfalls section; restructure
   to be a neatrul analysis document; 2013-07-15.

draft-jiang-semantic-prefix-05: reword to emphasis this mechanism is a (not the) method that network operators use their addresses; add text to clarify the increased trust is actually from the deployment of source address filter, which is a compliance requirement by semantic prefix; restructure the document, move examples and gap analysis into appendixes, reorganize most content into a frame section; add summarized description for framework at the beginning of Section 3; add description for network operations based on semantic prefix; add a new coauthor who contributes an enterprise semantic prefix network example; combine most of draft-sun-v6ops-semantic-usecase into the draft as ISP example in appendix; 2013-5-28.

draft-jiang-semantic-prefix-04: add new coauthor, re-organize the content, and refine the English, 2013-1-31.

draft-jiang-semantic-prefix-03: add the concept of hierarchical Semantic Prefix Domain and more gap analysis, 2012-10-22.

draft-jiang-semantic-prefix-02: resubmitted to v6ops WG. Removed detailed examples and recommendations for semantics bits, 2012-10-15.

draft-jiang-semantic-prefix-01: added enterprise considerations and scenarios, emphasizing semantics only for local meaning and no intend to standardize any common global semantics, 2012-07-16.

9. Security Considerations

Embedding semantics in prefix is actually exposing more information of packets explicit. These informations may also provide convenient for malicious attackers to track or attack certain type of packets. If networks announce their local prefix semantics to their peer networks, it may also increase the vulnerable risk.

Prefix-based filters should be deployed, in order to protect against address spoofing attacks or denial of service for packets with forged source addresses.

10. Acknowledgements

Useful comments were made by Erik Nygren, Dan Wing, Nick Hilliard, Ray Hunter, David Farmer, Fred Baker, Joel Jaeggli, John Curran, Tim Chown, Ted Lemon, Owen DeLong, Lorenzo Colitti, George Michaelson, Joel Halpern, Vizdal Ales, Bless Roland, Manning Bill, Manfred Albert and other participants in the V6OPS working group.

11. References

[11.1](#). Normative References

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

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

[RFC3315]   Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,
            and M. Carney, "Dynamic Host Configuration Protocol for
            IPv6 (DHCPv6)", [RFC 3315](#), July 2003.

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

[RFC4291]   Hinden, R. and S. Deering, "IP Version 6 Addressing
            Architecture", [RFC 4291](#), February 2006.

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

[RFC6724]   Thaler, D., Draves, R., Matsumoto, A., and T. Chown,
            "Default Address Selection for Internet Protocol Version 6
            (IPv6)", [RFC 6724](#), September 2012.

[11.2](#). Informative References

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

[Appendix A](#). An ISP Semantic Prefix Example

This ISP semantic prefix example is abstracted from a real ISP
address architecture design.

Note: for now, this example only covers unicast address within IP
Version 6 Addressing Architecture [[RFC4291](#)].

For ISPs, several motivations to use semantic prefixes are as
follows:

a. Network Device management: Separated and specialized address
    space for network device will help to identify the network device
    among numerous addresses and apply policy accordingly.

   b. Differentiated user management: In ISPs' network, different kinds
       of customers may have different requirements for service
       provisioning.

   c. High-priority service guarantee: Different priorities may be
       divided into apply differentiated policy.

   d. Service-based Routing: ISPs may offer different routing policy
       for specific service platforms .e.g.video streaming, VOIP, etc.

   e. Security Control: For security requirement, operators need to
       take control and identify of certain devices/customers in a quick
       manner.

   f. Easy measurement and statistic: The semantic prefix provides
       explicit identifiers for measurement and statistic.

   These requirements are largely falling into two categories: some is
   regarding to the network device features, and the others are related
   to services provision and subscriber identification. The functional
   usage of the semantics for the two categories are quite different.
   Therefore, an ISP semantic IPv6 prefix example is designed as a two-
   level hierarchical architecture, in which the first level is the
   function types of prefixes, and the second level is the further usage
   within an specific prefix type.

A.1. **Function Type Semantic Bits**

   Function Type (FT): the value of this field is to indicate the
   functional usage of this prefix. The typical types for operators
   include network device, subscriber and service platform.

```
   +--------+--------+------------------------------------------------+
   |        | FT     |                                                |
   +--------+--------+------------------------------------------------+
        /          \
        +------------+------------+
        |000:     network device  |
        |000~010: service platform|
        |011~101: subscriber      |
        |110:     reserved        |
        +-------------------------+
```
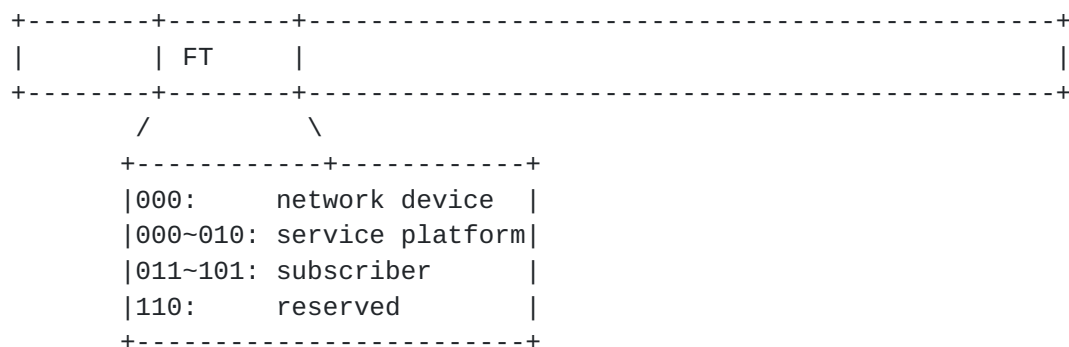
                        Function Type Bits Example

                              Figure 1

   The portion of each type should be estimated according to the actual
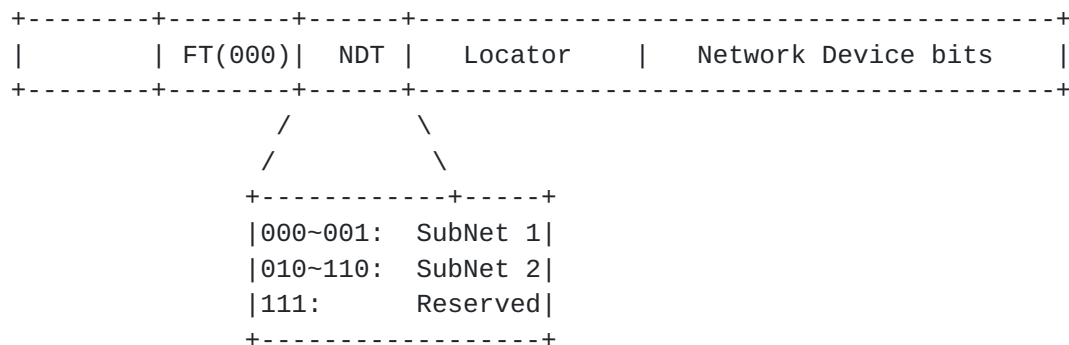   requirements for operators, in order to use the address space most
   efficiently. Within the above FT design, the whole ISP IPv6 address
   space is divided into four parts: the network device address space (1
   /8 of total address space), the service platform address space (2/8
   of total address space), the subscriber address space (3/8 of total
   address space), and a reserved address space (1/8 of total address
   space) for future usage.

A.2. **Network Device Type Bits within Network Device Address Space**

   Network Device Type (NDT) indicates different types of network
   devices. Normally, one operator may have multiple networks,
   e.g.backbone network, mobile network, ISP brokered service network,
   etc. Using NDT field to indicate specific network within an operator
   may help to apply some routing policies. Locating NDT bits in the
   left-most bits means that a single, simple access- control list
   implemented across all networking devices would be enough to enforce
   effective traffic segregation. The Locator field is followed behind
   NDT.

```
   +--------+--------+------+----------------------------------------+
   |        | FT(000)|  NDT |   Locator    |   Network Device bits    |
   +--------+--------+------+----------------------------------------+
                /         \
               /           \
         +------------+-----+
         |000~001:  SubNet 1|
         |010~110:  SubNet 2|
         |111:      Reserved|
         +------------------+
```

                  Network Device Type Bits Example

                             Figure 2

   The portion of each subnet type should be estimated according to the
   actual requirements for operators, in order to use the address space
   most efficiently. Within the above NDT design, SubNet 1 is assigned
   2/8 of the network device address space, SubNet 2 is assigned 5/8,
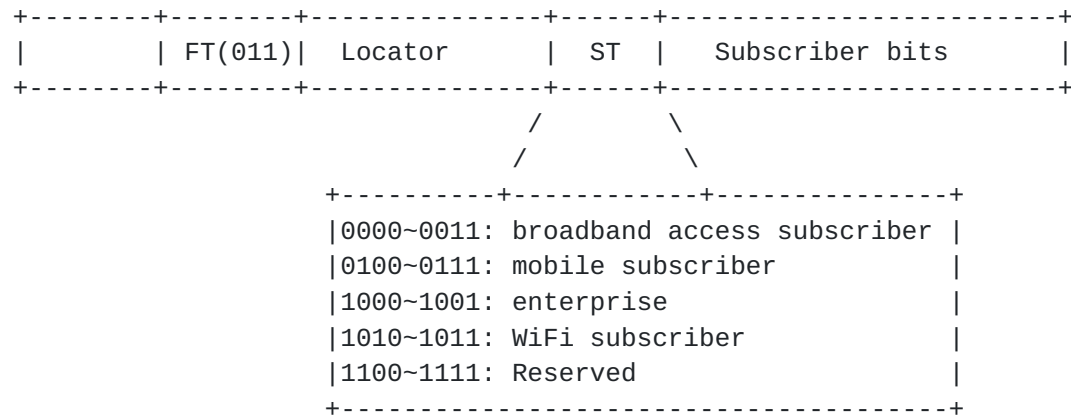   and 1/8 is reserved.

A.3. **Subscriber Type Bits within Subscriber Address Space**

Subscriber Type (ST) indicates different types of subscribers, e.g.
wireline broadband subscriber, mobile subscriber, enterprise, WiFi,
etc. This type of prefix is allocated to end users. Further,
division may be taken on subscriber's priorities within a certain
subscriber type.

The Locator field within subscriber address space is put before ST
for better routing aggregation.

```
+--------+--------+---------------+------+------------------------+
|        | FT(011)|  Locator      |  ST  |   Subscriber bits      |
+--------+--------+---------------+------+------------------------+
                              /        \
                             /          \
                +----------+-----------+---------------+
                |0000~0011: broadband access subscriber |
                |0100~0111: mobile subscriber           |
                |1000~1001: enterprise                  |
                |1010~1011: WiFi subscriber             |
                |1100~1111: Reserved                    |
                +---------------------------------------+
```
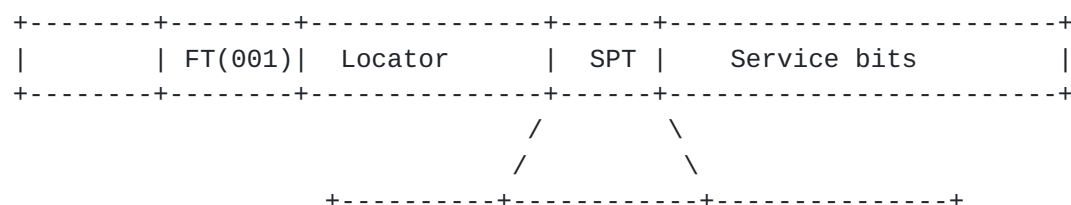
Subscriber Type Bits Example

Figure 3

The portion of each subscriber type should be estimated according to
the actual requirements for operators, in order to use the address
space most efficiently. Within the above ST design, the broadband
access subscriber type is assigned 4/16 of the subscriber address
space, the mobile subscriber is assigned 4/16, enterprise type and
WiFi subscriber type are assigned 2/16 each, and 2/16 is reserved.

A.4. Service Platform Type Bits within Service Platform Address Space

Service Platform Type (SPT) indicates typical service platforms
offered by operators. This field may have scalability problem since
there are numerous types of services . It is recommended that only
aggregated service platform types should be defined in this field.
This type of prefix is usually allocated to service platforms in
operator's data center.

```
+--------+--------+---------------+------+------------------------+
|        | FT(001)|  Locator      | SPT  |    Service bits        |
+--------+--------+---------------+------+------------------------+
                              /        \
                             /          \
                +----------+-----------+---------------+
```

```
                    |000~001: Self-running service platform |
                    |001~011: Tenant service platform      |
                    |100~101: Independent service platform |
                    |110~111: Reserved                     |
                    +--------------------------------------+
```

                     Service Platform Type Bits Example

                                  Figure 4

   The portion of each subnet type should be estimated according to the
   actual requirements for operators, in order to use the address space
   most efficiently.

Appendix B. An Enterprise Semantic Prefix example

   This enterprise semantic prefix example is also abstracted from an
   ongoing enterprise address architecture design. This example is
   designed for a realtime video monitor network across a city region.
   The semantic prefix solution is planning to be deployed along with a
   strict authorization system.

   Note: this example only covers unicast address within IP Version 6
   Addressing Architecture [RFC4291].

   For this example, the below semantics are important for the network
   operation and require different network behaviors.

   a. Terminal type: there are two terminal types only: monitor cameras
       or video receivers. They are estimated to have similar number.
       Network devices use another different address space.

   b. Geographic location: the city has been managed in a three-level
       hierarchical regionalism: district, area and street. Each level
       has less than 28 sub-regions. This can also be considered as a
       replacement of topology locator within this specific network.

   c. Authorization level: the network operator is planning to
       administrate the authorization in three or four levels. An
       receiver can access the cameras that are the same or lower
       authorization level.

   d. Civilian or police/government.

   e. Device attribute: this indicates the attribute of a camera
       device. The attribute is expressed in an abstract way, such as
       road traffic, hospital, nursery, bank, airport, etc. The
       abstracted attribute type is designed to be less than 64.

   f. Receiver Attribute: this indicates the attribute of a video
       receiver. The attribute is based on the receiver group, such as
       police, firefighter, local security, etc. The attribute/receiver
       group type is designed to be less than 128.

   This example enterprise network has obtained a /32 address block from
   ISP. There is another /48 dedicated for network devices.

   The first bit is Terminal type, which indicates terminal type.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        ISP assigned block                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |T|    Geographic   Locator    | AL|C|Device Attr|  Device Bit |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

             A semantic prefix design example for cameras

                            Figure 5

   3-level hierarchical geographic locator takes 15 bits (each level 5
   bits, 32 sub-regions). Authorization level takes 2 bits and 1 bit
   differentiates civilian or police/government. 6 bits is assigned for
   device attribute.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        ISP assigned block                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |T| GeoLoc  | AL|C|Receiver Attr|  Topology Locator |ReceiverBit|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

           An semantic prefix design example for video receivers

                            Figure 6

   The receiver is not as much as geographically distributed as cameras.
   Therefore, Geographic locator is only detailed to district level.
   Topology locator is needed for network forwarding and aggregation
   within a district. It is assigned 10 bits. Authorization level bits
   and civilian bit are the same with camera address space. Receive
   attribute takes 7 bits, giving it is designed to be up to 128.

Appendix C. A Multi-Prefix Semantic example

   A multiple-site enterprise may have been assigned several prefixes of
   different lengths by its upstream ISPs. In this situation, in order

to create a single, contiguous Semantic Prefix Domain, it is
necessary to base the semantic prefix policy on the longest assigned
prefix to ensure that there in enough addressing space to encode a
consistent set of semantics across all of the assigned prefixes.

In this example, an enterprise has received a /38 address block for
one site (A) and a /44 for a second site (B) . They can be organized
in the same Semantic Prefix Domain. The most-left 18 (site A) and 12
(site B) bits are allocated as locator. It provides topology based
network aggregation. The 8 right-most bits (from bits 56 to 63) are
assigned as the semantic field. In this design, the multiple-site
enterprise that has been assigned two prefixes of different lengths
can be organized as the same Semantic Prefix Domain. The semantic
and the Semantic Prefix Domain can traverse the intermediate ISP
networks, or even public networks.

The similar situation may happen on ISPs in the future, when an ISP
used up its assigned address space, or built up multiple networks in
different places.

Authors' Addresses

   Sheng Jiang (editor)
   Huawei Technologies Co., Ltd
   Q14, Huawei Campus, No.156 BeiQing Road
   Hai-Dian District, Beijing 100095
   P.R. China

   Email: jiangsheng@huawei.com

   Qiong Sun
   China Telecom
   Room 708, No.118, Xizhimennei Street
   Beijing 100084
   P.R. China

   Email: sunqiong@ctbri.com.cn

   Ian Farrer
   Deutsche Telekom AG
   Bonn 53227
   Germany

   Email: ian.farrer@telekom.de

Yang Bo
Huawei Technologies Co., Ltd
Q21, Huawei Campus, No.156 BeiQing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: boyang.bo@huawei.com

Tianle Yang
China Mobile
32, Xuanwumenxi Ave. Xicheng District
Beijing 100053
China

Email: yangtianle@chinamobile.com