Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 21, 2013

C. Xie
Q. Sun
China Telecom
S. Jiang
Huawei Technologies Co., Ltd
February 17, 2013

Use case of IPv6 prefix semantics for operators
draft-sun-v6ops-semantic-usecase-00

Abstract

Embedding certain semantics into IPv6 addresses will bring a lot of benifits for operators to simplify network management and apply operations accordingly[I-D.jiang-semantic-prefix]. This memo illustrates the use case of semantic bits from operator's point of view, and provides considerations on how to design the semantic bits in IPv6 address.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 21, 2013.

Table of Contents

1. Introduction

[I-D.jiang-semantic-prefix] introduces embedded semantics prefix solution in IPv6 context. With more and more differentiated requirements raising in the current Internet, service operators may want to apply more complicated policies for different kinds of customers and services. Policy control servers are introduced gradually in fixed network operator and mobile network operator. However, all of these policies can only take action based on efficient packet identification of different sematics.

Carrying semantic bits directly in IPv6 prefix is not only efficient for routers to do packet identification, but also suitable for operators. It provides an easy access and trustable fundamental for packet differentiated treatment.

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

1. Network Device management

In order to achieve easy management for network devices, operators will usually apply a simple and specific numbering policy for network devices. Besides, special-purpose security policies may be enforced for network devices other than for customers and service platforms. For example, when encountering a simple threat model from some subscribers' address block, operators may only filter the specific subscribers' address block other than the whole addresses network devices and service platforms. As a result, separated and specialized address space for network device will help to identify the network device among numerous addresses and apply policy accordingly.

2. Differentiated user management and service provisioning

In operator's network, different kinds of customers may have different requirements for service provisioning. For example, broadband access subscribers usually have lower priority than enterprise customers. And even for broadband access subscribers, different priorities can also be further divided to apply differentiated policy, e.g. bandwidth limit, etc.

3. High-priority service guarantee

Operators may provide their own ISP brokered services, .e.g. video streaming, IPTV, VOIP, etc, which usually have higher priority guarantee rent their IDC to third-party service platform, offering high priority services, .e.g. video streaming, VOIP, etc.

4. Service-based Routing

Service-based routing usually has close relationship with operator's network architecture. For example, some operators have distinct core networks for different kinds of services. As a result, operators may offer different routing policy for specific service platforms .e.g.video streaming, VOIP, etc. Different routing policies may also apply to high priority services. In this case, semantic embedded in the IPv6 address will be very helpful to implement service-based routing.

5. Security Control

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

6. 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.

2. How to design the semantic bits

The embedded semantic bits should be carefully designed for the followings reasons. Firstly, this kind of design should reflect the requirements and considerations of a given operator. Secondly, there are very limited bits which can be used to carry semantic information. In this section, we will discuss the guidelines for operators to define the semantic bits, typical types of semantics, considerations on the placement of semantics bits, and also give an example to further illustrate our considerations.

2.1. Guidelines to define the semantic bits

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

The following are some guidelines for operators to design the semantic bits:

- Determine the number of semantic bits. Typically, ISPs with millions subscribers would have /16 ~ /24 address space. It allows 40~48 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 22~40. Furthermore, within the arbitrary bits, 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, 24 bits for locator function is a minimum safe allocation. Hence, it is recommended to use 4~12 bits in prefix for embedded semantics.

- The number of semantics should be limited. According to the above analysis, the number of semantic bits left for operators is quite limited. Therefore, it is recommended that network operator only use necessary semantics when they can bring benefits to network operations, especially IP-layer policy, e.g. policy routing, access control and filtering, QoS, network measurement, etc. The network operators should be very careful to plan and manage the semantic field. The network operators should self-restrict NOT to put too many semantic into prefix. So that they may avoid trap themselves into very complicated management issues.

- For any packets, semantic overlap should be avoided. Any potential scenarios that a given address may be mapped two or more semantic prefixes are considered harmful. For a given device/ host, it is also recommended that either the source address or the destination address should be belonged to one semantic so as to simplify addressing selection process.

- The design of semantic bits should be scalable and stable from the long-term. It should reflect the general potential network strategy and policies in the future and should be defined in highly abstracted way since there might be quite a lot of unknown emerging services.

- Different size of addressing space should be planned carefully for different semantics. Since different semantics usually consumes different size of address space, operators should plan the size of address space according to the service model for different semantics.

3. Typical types of semantics

Operators may have multiple requirements to semantics. Generally speaking, these requirements can fall into two categories: the first one is related to the network features itself. For example, some semantics, like the network device type, etc., may be announced to

other carriers for network information exchange; while the second one is related to services types and subscriber types for operator itself.

The usage of the semantics of the two categories are quite different. For example, semantics in the first category does not need to carry QoS related information, and may reflect network architecture of the operator, while the semantics in the second category can reflect the QoS requirements of the given service.

With this in mind, we recommend that operators may define the semantics hierarchically, in which the first level is to define the function types of the prefixes, and the second level is to define the further usage within that specific prefix type.

3.1. Level-1 semantics

Level-1 semantics can be used to define the function types of the prefixes.

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

The following is the example of FT value.

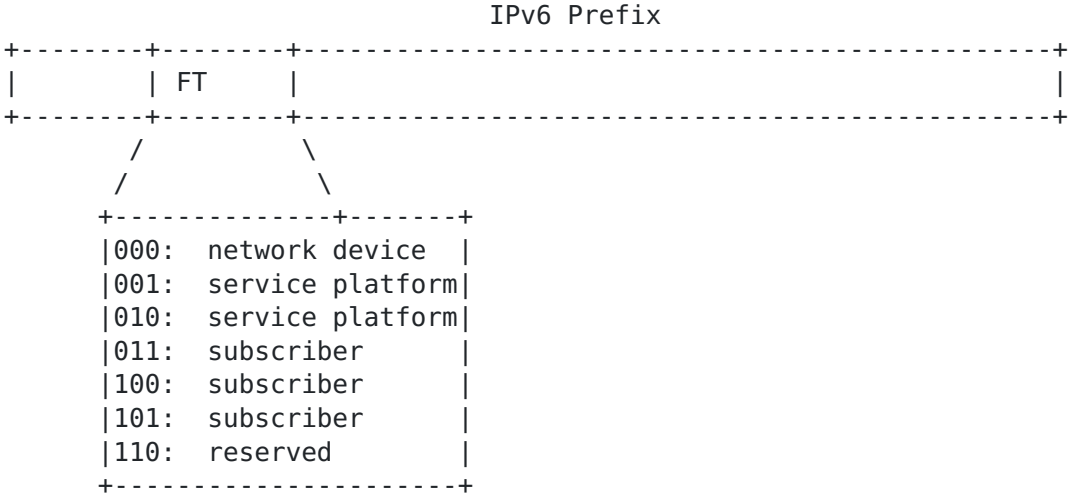

Figure 1: FT Value Example

In this case, one prefix type may have multiple FT values. For example, FT value of the subscriber prefix can be 010,011,100,101,110,111, The portion of each type should be estimated according to the accrual requirements for operators.

With this level-1 FT definition in hand, further classification can be applied to each type to define more detailed sub-types in level-2 semantics.

3.2. Level-2 semantics

Level-2 semantics is to define more detailed usage in different Function Types.

1. Network Device Type (NDT)

Network Device Type (NDT) is to indicate different types of network usage, e.g.,backbone network,metro network or network management, etc.

One example is shown in the following figure:

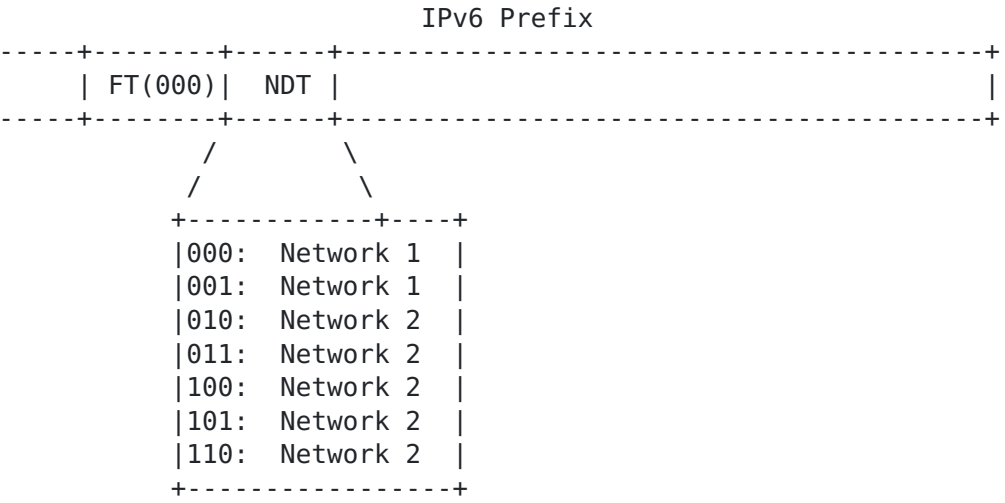

Figure 2: NDT Value Example

2. Subscriber type (ST)

Subscriber type is to indicate different types of subscribers, e.g. wireline broadband subscriber, mobile subscriber, enterprise, WiFi, etc. This type of prefix is allocated to end users. In particular, further divisions can be taken on subscriber's priorities features within one type, e.g. golden broadband subscriber, silver broadband subscriber and bronze broadband subscriber. This definition is based on operator's local service model.

One example is shown in the following figure:

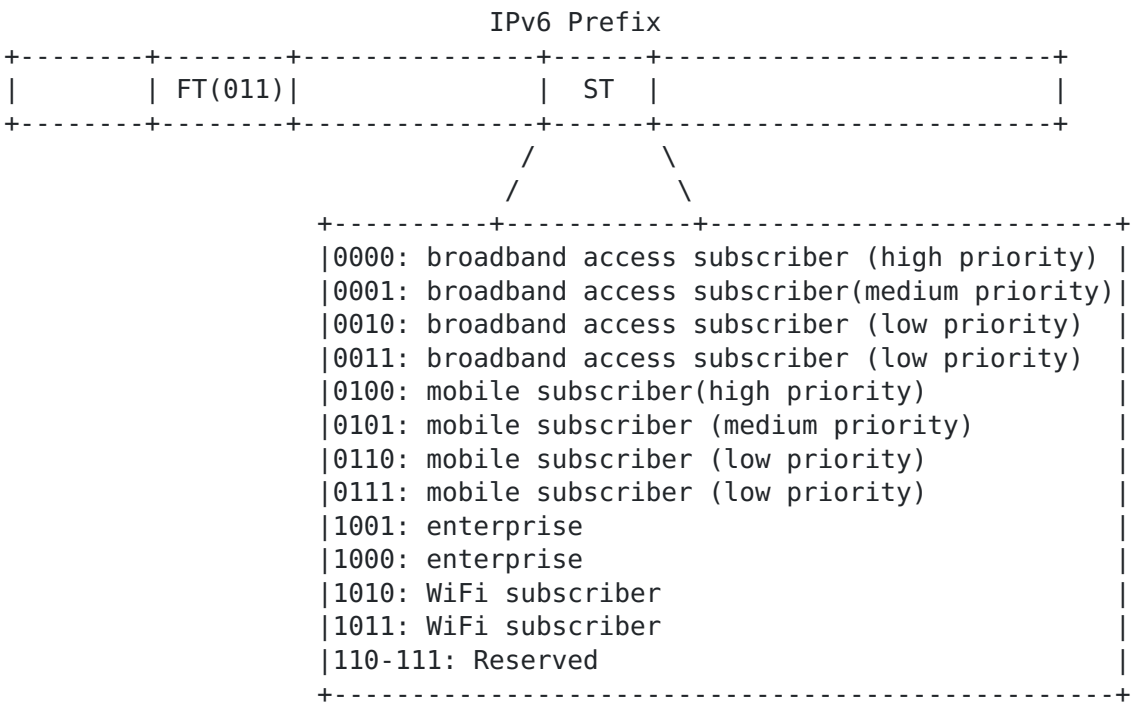

Figure 3: NDT Value Example

3. Platform Type(PT)

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

One example is shown in the following figure:

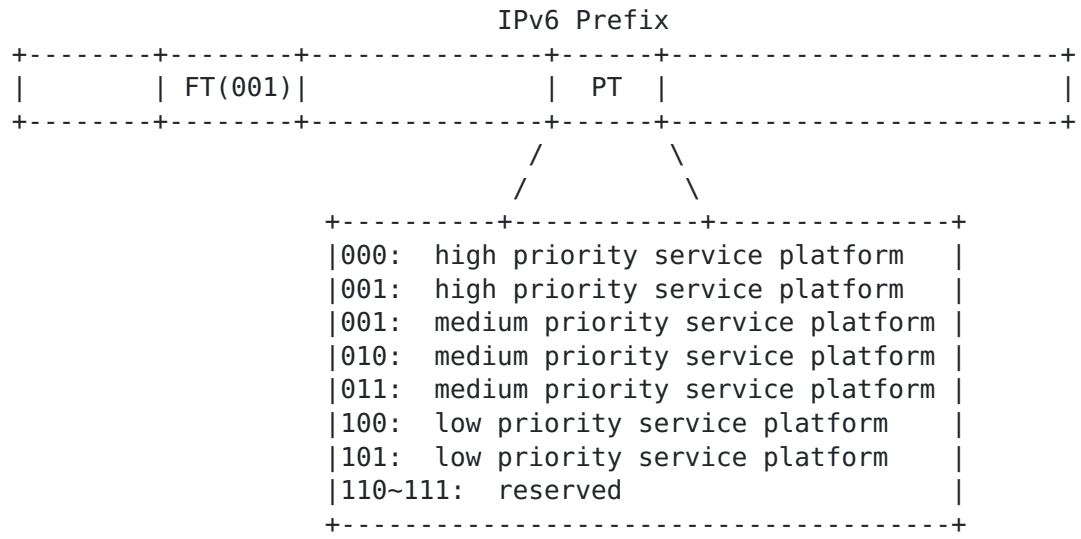

Figure 4: NDT Value Example

4. How to determine the placement of semantics bits

The placement of semantic bits should be carefully designed. For the different types of semantics mentioned above, since FT may be announced to different operators for intre-domain control support, it should be placed in the most left bits of the prefix. NDT may be followed by FT directly so that different device numbering policy can be taken afterwards. ST and PT is recommended be located in the lower place of the locator function , which is good to routing aggregation.

5. IANA Considerations

This document has no actions for IANA.

6. 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. When networks announce their local prefix semantics to their peer networks, it may increase the vulnerable risk.

7. Acknowledgements

TBD

8. References

8.1. Normative References

[I-D.jiang-semantic-prefix]
Jiang, S., Sun, Q., and I. Farrer, "A Framework for Semantic IPv6 Prefix and Gap Analysis", draft-jiang-semantic-prefix-04 (work in progress), January 2013.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

8.2. Informative References

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[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.

Authors' Addresses

Chongfeng Xie
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing 100084
P.R. China

Email: xiechf@ctbri.com.cn

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

Email: sunqiong@ctbri.com.cn

Sheng Jiang
Huawei Technologies Co., Ltd
No.156 Beiqing Road
Beijing 100095
P.R. China

Email: jiangsheng@huawei.com