

Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 29, 2013

C. Xie
Q. Sun
China Telecom
S. Jiang
Huawei Technologies Co., Ltd
February 25, 2013

Use case of IPv6 prefix semantics for operators
draft-sun-semantic-usecase-02

Abstract

Embedding certain semantics into IPv6 addresses will bring a lot of benefits 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 29, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

Semantic use case

February 2013

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	How to design the semantic bits	4
3.	A use case for Semantic Prefix	6
3.1.	Level-1 semantics	6
3.2.	Level-2 semantics	7
4.	Benifits of Semantic Use Case	10
5.	IANA Considerations	11
6.	Security Considerations	11
7.	Acknowledgements	11
8.	References	11
8.1.	Normative References	11
8.2.	Informative References	11
	Authors' Addresses	12

[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 semantics.

The semantics are mainly used in a local region within an operator. 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

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. In particular, semantic prefix would be quite useful for identifying subscriber's priority in downstream traffic across large-scale regions where subscriber's profile is difficult to synchronize.

3. High-priority service guarantee

Xie, et al.

Expires August 29, 2013

[Page 3]

Internet-Draft

Semantic use case

February 2013

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.

The semantic bits should be defined after an operator have got its IPv6 address pool. The embedded semantic bits should be carefully

designed. Firstly, the number of bits which can be used to carry semantic information. Secondly, some semantics may easily raise the implementation complexity on host and network devices. So careful considerations and tradeoff should be taken in semantic design.

[I-D.jiang-semantic-prefix] has listed some semantics which may be useful to network operators. In this document, we provide a use case to use some selected semantics, achieving enhanced network management and service provisioning ability with limited impact on existing network infrastructure.

[Note: Further use cases could be added to reflect other requirements and implementation possibility.]

2. How to design the semantic bits

Depending on the IPv6 address space that network operators received from IANA or upstream network service providers, the number of

Xie, et al.

Expires August 29, 2013

[Page 4]

Internet-Draft

Semantic use case

February 2013

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:

- o 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.
- o The number of semantics should be limited. According to the above

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

- o Semantic overlap should be largely avoided . Any potential scenarios that a given address may be mapped two or more semantic prefixes might be harmful. Otherwise, if one subscriber is allocated with multiple semantics, context-based semantic selection mechanism must been introduced which might increase the complexity in device/hosts. In our use case, either the source address or the destination address only belongs to one semantic so as to simplify address selection process.
- o 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.
- o 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.](#) A use case for Semantic Prefix

As mentioned in section one, operators may have multiple requirements to use semantics. These requirements are largely falling into two categories: the first one is related to the network device features, while the second one is related to services provision and subscriber identification.

The functional usage of the semantics for the two categories are quite different. For example, the semantics for the first category

does not need to carry QoS related information, but may need to reflect network architecture of the operator; while the semantics in the second category should reflect the QoS requirements of the given subscriber/service.

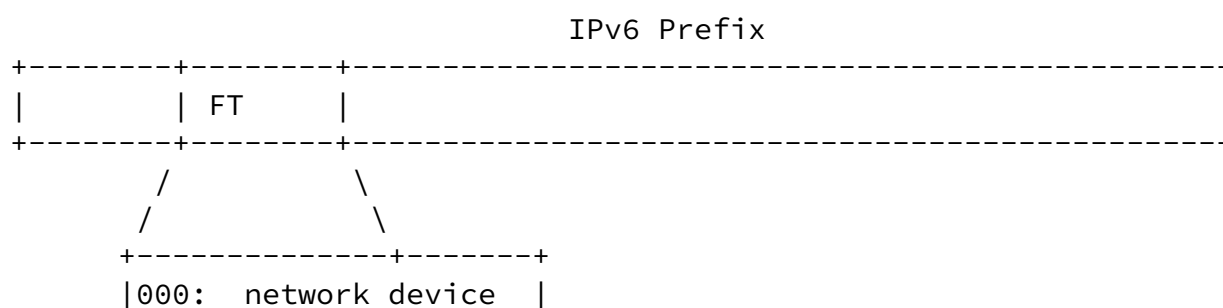
With this in mind, in our use case, the semantics are defined hierarchically, in which the first level is to define the function types of the prefixes, and the second level is to define the further usage within that specific prefix type.

[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 field 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.



001:	service platform
010:	service platform
011:	subscriber
100:	subscriber
101:	subscriber
110:	reserved
+-----+	

Figure 1: FT Value Example

In this example, 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 actual requirements for operators.

With the above FT definition, the whole IPv6 addressing space is firstly divided into three parts(as in the following figure).

+-----+			
IPv6 Addressing Space			
+-----+			
Subscriber	Service Platform	Network Device	
Addressing	Addressing	Addressing	
Space	Space	Space	
+-----+			

Figure 2: Addressing Space Division

3.2. Level-2 semantics

Level-2 semantics is to define more detailed usage in different Function Types (addressing space).

1. Network Device Type (NDT)

Network Device Type (NDT) is to indicate 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. Besides, implementing the

NDT field 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 put behind NDT to indicate the region of a certain device.

One example is shown in the following figure:

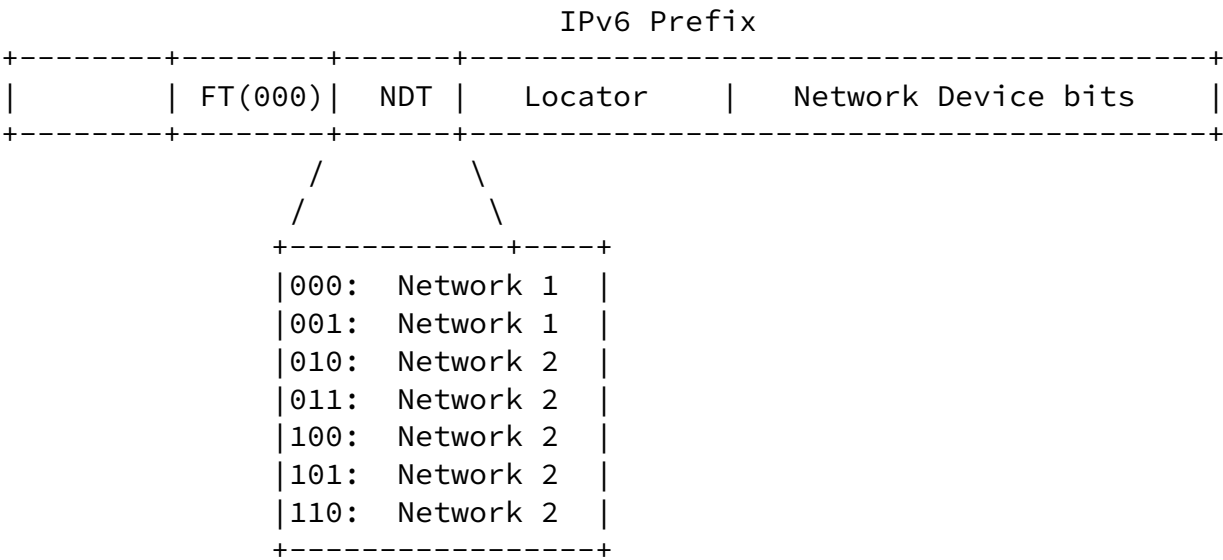


Figure 3: NDT Value Example

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 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.

Here, the Locator will reflect the different regions of a subscriber, and is put before ST for better routing aggregation.

One example is shown in the following figure:

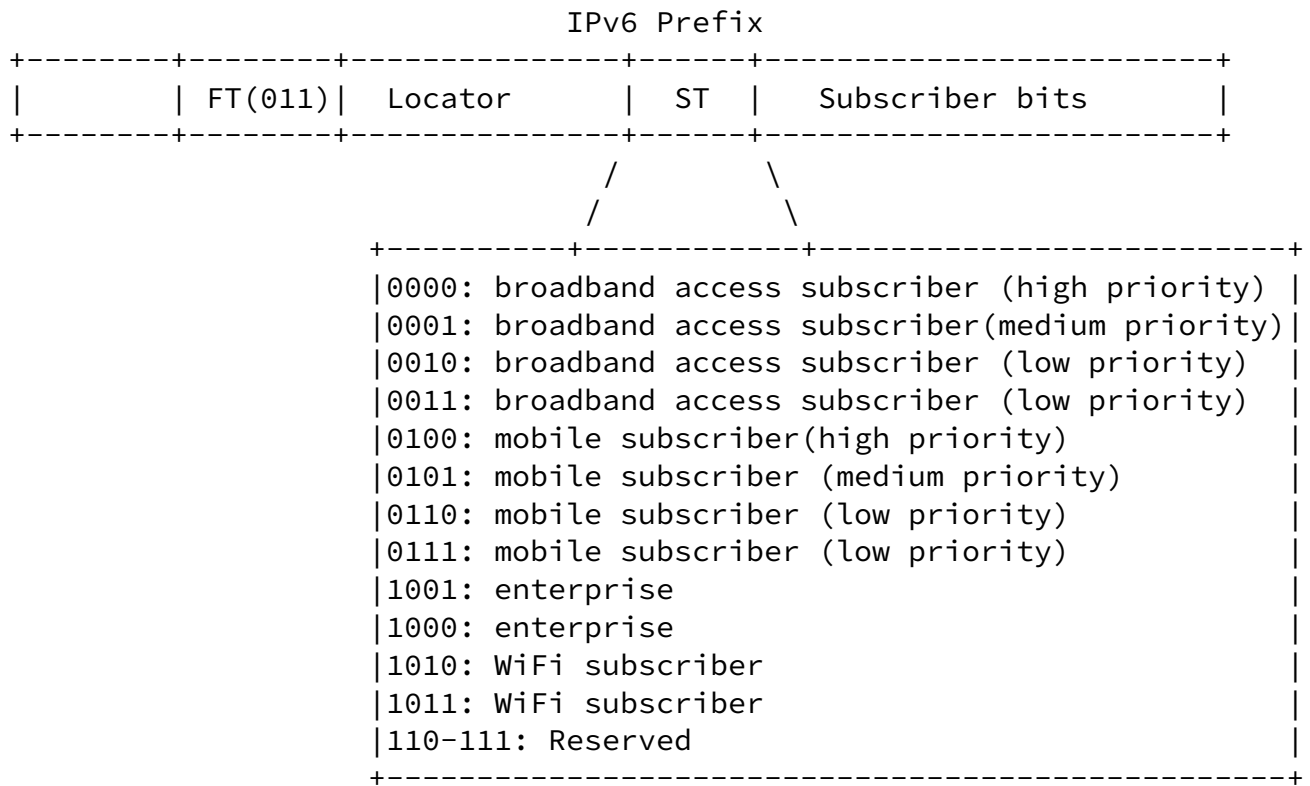


Figure 4: ST Value Example

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:

Internet-Draft

Semantic use case

February 2013

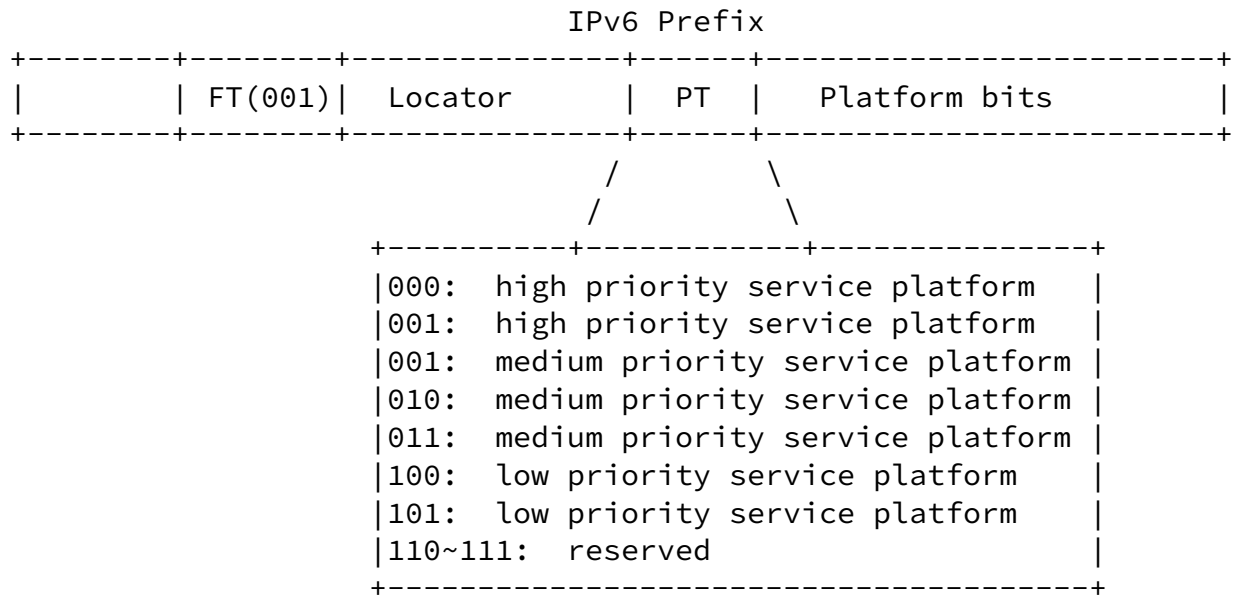


Figure 5: PT Value Example

4. Benifits of Semantic Use Case

The following describes a few benifits (and non-exhaustive) of above semantic use case for an operator:

1. Easy network device management. With the combination of FT, NDT and Locator, network devices from different regions can be easily identified. Besides, network-based routing policies can also be enforced with NDT.
2. Bi-directional subscriber quality of service guarantee. Since ST is consistent with the overall communication process for a subscriber, bi-directional quality of service guarantee can be easily achieved for cross-region communication.
3. Fine-Grained user and service control. Normally, ST is located in the source address of a subscriber, and PT is located in the destination address for upstream traffic. Therefore, with a simple combination of ST and PT, fine-Grained service control can

be applied to subscribers (e.g. high priority broadband access subscriber with high priority service platform).

4. Service-based Routing. With the definition of ST, different routing policies can be applied according to ST field.

Other requirements listed in section one can also be achieved in this use case.

[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

Authors would like to show sincere appreciation to Erik Nygren, Joel Jaeggli, Owen DeLong for their comments and suggestions.

[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.

Xie, et al. Expires August 29, 2013 [Page 11]

Internet-Draft Semantic use case February 2013

- [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: sunqiong@ctbri.com.cn

Qiong Sun

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

Email: bingxuere@gmail.com

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

Email: jiangsheng@huawei.com