

ANIMA WG
Internet-Draft
Intended status: Informational
Expires: November 5, 2015

S. Jiang, Ed.
Z. Du
Huawei Technologies Co., Ltd
B. Carpenter
Univ. of Auckland
Q. Sun
China Telecom
May 4, 2015

**Autonomic Prefix Management in Large-scale Networks
draft-jiang-anima-prefix-management-01**

Abstract

This document describes an autonomic solution for prefix management in large-scale networks.

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 November 5, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) 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	2
2.	Problem Statement	3
2.1.	Intended User and Administrator Experience	3
2.2.	Analysis of Parameters and Information Involved	3
2.2.1.	Parameters each device can decide for itself	4
2.2.2.	Information needed from policy intent	4
2.2.3.	Comparison with current solutions	5
2.3.	Interaction with other devices	5
2.3.1.	Information needed from other devices	5
2.3.2.	Monitoring, diagnostics and reporting	6
3.	Autonomic Prefix Management Solution	6
3.1.	Behaviors to discover prefix providing device	6
3.2.	Behaviors on prefix providing device	6
3.3.	Prefix Requests Behaviors	7
3.4.	Prefix log	8
4.	Autonomic Prefix Management Options	8
4.1.	Prefix Objective option	8
5.	Prefix Management Intent	8
5.1.	Example of Prefix Management Intent	9
6.	Security Considerations	10
7.	IANA Considerations	10
8.	Acknowledgements	11
9.	Change log [RFC Editor: Please remove]	11
10.	References	11
	Authors' Addresses	12

[1.](#) Introduction

This document proposes an autonomic solution for prefix management in large-scale networks. The background to Autonomic Network (AN) is described in [[I-D.irtf-nmrg-autonomic-network-definitions](#)] and [[I-D.irtf-nmrg-an-gap-analysis](#)]. A generic discovery and negotiation protocol (GDN) is proposed by [[I-D.carpenter-anima-gdn-protocol](#)], which would be used by the proposed autonomic prefix management solution.

This document is dedicated to how to make IPv6 prefix management in pure IPv6 large-scale networks as autonomic as possible. This document for now is only considering service provider (ISP) networks. Although there are similarities with large enterprise networks, the requirements are a little different for the two use cases.

Note in draft: This version is preliminary. In particular, many design details may be subject to change until the anima specifications become agreed.

2. Problem Statement

The autonomic networking use case considered here is autonomic IP address management in large-scale networks.

Although DHCPv6 Prefix Delegation [[RFC3633](#)] has supported automated delegation of IPv6 prefixes, prefix management is still largely depending on human planning. In other words, there is no basic information or policy to support autonomic decisions on the prefix length that each router should request or be delegated, according to its role in the network. Roles could be locally defined or could be generic (edge router, interior router, etc.). Furthermore, the current IPv6 prefix management by humans is rigid and static after initial planning.

The problem to be solved by AN is how to dynamically and autonomically manage IPv6 address space in large-scale networks, so that IPv6 addresses can be used efficiently. The AN approach discussed in this document is based on the assumption that there is a generic discovery and negotiation protocol that enables direct negotiation between intelligent IP routers. [[I-D.carpenter-anima-gdn-protocol](#)] is one of the attempts at such a protocol.

2.1. Intended User and Administrator Experience

The intended experience is, for the administrator(s) of a large-scale network, that the management of IPv6 address space can be run with minimum efforts, for both the network and network device initiation stage and during running time. In the ideal scenario, the administrator(s) only have to configure a single IPv6 prefix for the whole network and the initial prefix length for each device role.

The actual address usage needs to be logged for potential offline management operations including audit and security incident tracing.

2.2. Analysis of Parameters and Information Involved

For specific purposes of address management, a few parameters are involved on each device (some of them can be pre-configured before they are connected). They include:

- o Identity of this device. It can be verified by the certification authority (CA) that is maintained by the network administrator(s).

- o Identity of a trust anchor which is certification authority (CA) that is maintained by the network administrator(s).
- o Role of this device.
- o An IPv6 prefix length for this device.
- o An IPv6 prefix that is assigned to this device and its downstream devices.

A few parameters are involved in the network as a whole. They are:

- o Identity of a trust anchor which is a certification authority (CA) that is maintained by the network administrator(s).
- o Total IPv6 address space. It is one (or several) IPv6 prefix(es).
- o The initial prefix length for each device role.

2.2.1. Parameters each device can decide for itself

This section identifies those of the above parameters that do not need external information in order for the devices concerned to set them to a reasonable value after bootstrap or after a network disruption. There are few of these:

- o Role of this device.
- o Default IPv6 prefix length for this device.
- o Identity of this device.

The device may be shipped from the manufacture with pre-configured role and default prefix length.

2.2.2. Information needed from policy intent

This section identifies those parameters that need external information about policy intent in order for the devices concerned to set them to a non-default value.

- o Non-default value for the IPv6 prefix length for this device.
This needs to be decided based on the role of this device.
- o The initial prefix length for each device role.
- o Identity of a trust anchor.

- o Whether to allow the device request more address space.
- o The policy when to request more address space, for example, the address usage reaches a certain limit or percentage.

2.2.3. Comparison with current solutions

This section briefly compares the above use case with current solutions. Currently, the address management is still largely depending on human planning. It is rigid and static after initial planning. The address requests will fail if the configured address space is used up.

Some functions, for autonomic and dynamic address management, may be achievable by extending the existing protocols, for example, extending DHCPv6-PD to request IPv6 address according to the device role. However, defining uniform device roles may not be a practical task. Some functions are not suitable to be achieved by any existing protocols.

However, using a generic autonomic discovery and negotiation protocol instead of specific solutions has the advantage that additional parameters can be included in the autonomic solution without creating new mechanisms. This is the principal argument for a generic approach.

2.3. Interaction with other devices

2.3.1. Information needed from other devices

This section identifies those of the above parameters that need external information from neighbor devices (including the upstream devices). In many cases, two-way dialogue with neighbor devices is needed to set or optimize them.

- o Identity of a trust anchor.
- o The device will need to discover a device, from which it can acquire IPv6 address space.
- o The initial prefix length for each device role, particularly for its own downstream devices.
- o The default value of the IPv6 prefix length may be overridden by a non-default value.
- o The device will need to request and acquire IPv6 prefix that is assigned to this device and its downstream devices.

- o The device may respond to prefix delegation request from its downstream devices.
- o The device may require to be assigned more IPv6 address space, if it used up its assigned IPv6 address space.

2.3.2. Monitoring, diagnostics and reporting

This section discusses what role devices should play in monitoring, fault diagnosis, and reporting.

- o The actual address assignments need to be logged for the potential offline management operations.
- o In general, the usage situation of address space should be reported to the network administrators, in an abstract way, for example, statistics or visualized report.
- o A forecast of address exhaustion should be reported.

3. Autonomic Prefix Management Solution

This section introduces an autonomic prefix management solution. It extends the generic discovery and negotiation protocol defined by [[I-D.carpenter-anima-gdn-protocol](#)]. The relevant options are defined in [Section 4](#).

3.1. Behaviors to discover prefix providing device

A device should decide the length of request prefix by the intent-based mechanism, described in [Section 5](#). If it used up its current address resource, it could request more, which is not necessary to be on the same scale as its initial resource.

A prefix requesting device that needs new or more address space should firstly discover peer devices that may be able to provide extra address space. The device should send out a GDN Discovery message that contains a Prefix Objective option [Section 4.1](#), in which the device also indicates whether it supports the DHCPv6 Prefix Delegation (PD) [[RFC3633](#)] function and the length of requested prefix.

3.2. Behaviors on prefix providing device

A peer device receiving a Discovery message with a Prefix Objective option, if it is able to provide such a prefix, should respond with a GDN Response message. The Response message also carries a Prefix Objective option, which also indicate whether the peer device

supports the PD function and the available prefix length matching the request. If the peer device does not have enough resource, it may silently drop the Discovery message or return a GDN Response message, which contains a longer prefix length (smaller address space) that it can provide. A divert option may also be added into the GDN Response message. This divert option indicates another device that may provide the prefix. The diverted device is typically an upstream gateway router, but it could in theory be any device that might have unused prefix space.

A gateway router in a hierarchical network topology is normally responsible to provide prefixes for routers within its subnet. In the case that it does not have enough resource for the downstream requesting router, it should return a GDN Response message, which contains a longer prefix length (smaller address space) that this gateway router may provide. In this case too, a divert option may be added into the GDN Response message. The diverted device is typically another upstream gateway router.

A resource shortage may cause the gateway router to request more resource from its upstream device. This would be another independent GDN discovery and negotiation process. During the processing time, the gateway router should send a Confirm-waiting Message to the initial requesting router. When the new resource becomes available, the gateway router responds with a GDN Response message with the prefix length matching the request.

The algorithm to choose which prefixes to assign on the prefix providing devices is an implementation choice out of document scope.

3.3. Prefix Requests Behaviors

Upon receiving the GDN Response message that indicates the requesting prefix length is accepted, the requesting device may request the prefix using DHCPv6 PD, if both itself and the response device support PD.

Upon receiving the GDN Response message that indicates the requesting prefix length is not possible, but a longer prefix length is available, the requesting device may request the longer prefix using DHCPv6 PD, if both itself and the response device support PD.

If the GDN Response message carries a divert option, the requesting device may send an unicast GDN Discovery message to the diverted device to find out whether that device can provide the requested length prefix.

[Author's note: undecided whether we should support prefix delegation using the GDN protocol. This would have some partial overlap with DHCPv6 PD. But it seems more consistent as a solution.]

3.4. Prefix log

Within the autonomic prefix management, all the prefix assignment is done by devices without human intervention. It is even more important to record all the prefix assignment history. However, the logging and reporting process is out of document scope.

4. Autonomic Prefix Management Options

This section defines the GDN options that are used to support autonomic prefix management.

4.1. Prefix Objective option

The Prefix Objective option carries the PD support flag and the prefix length. The format of the Prefix Objective option is described as follows:

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Prefix_Obj_Option      |      option-len      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|PD_Support_Flag| Prefix_Length |
+---+---+---+---+---+---+---+---+---+---+---+---+

```

option-code Prefix_Obj_Option (TBA1).

option-len 2, length of option content in octets.

PD_Support_Flag Indicates whether the message sender supports DHCPv6 Prefix Delegation function, 1 for support, 0 for no support, as client or server accordingly. This flag must not be set to any other values.

Prefix_Length Indicate the prefix length that the message sender requests or is willing to provide.

5. Prefix Management Intent

With in a single administrative domain, the network operator could manage all their devices with role set. If so, there is possibility to configure/manage the prefix length for every device in a simple way.

The network operator could only manage the default prefix length for each type of role. A prefix management intent, which contains all mapping information of device roles and their default prefix lengths, should be flooded in the network, through the Autonomic Control Plane (ACP) [[I-D.behringer-anima-autonomic-control-plane](#)]. The intent flooding mechanism is out of document scope.

Upon receiving the prefix management intent, every device can decide its default prefix length by matching its own role.

5.1. Example of Prefix Management Intent

The prefix management intent in this document is used to carry mapping information of device roles and their default prefix lengths in an autonomic domain. For example, an IPRAN operator wants to configure the prefix length of RNC Site Gateway (RSG) as 34, the prefix length of Aggregation Site Gateway (ASG) as 44, and the prefix length of Cell Site Gateway (CSG) as 56. She/he may input the following intent into the autonomic network:


```
<autonomic_intent>
  <protocol_version>1.0</protocol_version>
  <intent_type>Network management</intent_type>
  <autonomic_domain>CT_11</autonomic_domain>
  <intent_name>Prefix management</intent_name>
  <intent_version>1</intent_version>
  <intent_timestamp>2015-05-04 00:00:00</intent_timestamp>
  <intent_lifetime>Permanent</intent_lifetime>
  <content>
    <role>
      <role_name>RSG</role_name>
      <role_characteristic>
        <prefix_length>34</prefix_length>
      </role_characteristic>
    </role>
    <role>
      <role_name>ASG</role_name>
      <role_characteristic>
        <prefix_length>44</prefix_length>
      </role_characteristic>
    </role>
    <role>
      <role_name>CSG</role_name>
      <role_characteristic>
        <prefix_length>56</prefix_length>
      </role_characteristic>
    </role>
  </content>
</autonomic_intent>
```

6. Security Considerations

Relevant security issues are discussed in [\[I-D.carpenter-anima-gdn-protocol\]](#). The security mechanism in this document is established on a Public Key Infrastructure (PKI) system [\[RFC3647\]](#) that is maintained by the network administrator(s).

It is RECOMMENDED that DHCPv6 PD, if used, should be operated using DHCPv6 authentication or Secure DHCPv6.

7. IANA Considerations

This document defines one new GDN option. The IANA is requested to assign a value for this option from the GDN Option Codes table of the GDN Parameters registry as defined by [\[I-D.carpenter-anima-gdn-protocol\]](#) (if approved).

- o The Prefix Objective option (TBA1), described in [Section 4.1](#).

8. Acknowledgements

Valuable comments were received from Michael Behringer and Chongfeng Xie.

This document was produced using the xml2rfc tool [[RFC2629](#)].

9. Change log [RFC Editor: Please remove]

[draft-jiang-anima-prefix-management-00](#): original version, 2014-10-25.

[draft-jiang-anima-prefix-management-01](#): add intent example and coauthro Zongpeng Du, 2014-05-04.

10. References

- [I-D.behringer-anima-autonomic-control-plane]
Behringer, M., Bjarnason, S., BL, B., and T. Eckert, "An Autonomic Control Plane", [draft-behringer-anima-autonomic-control-plane-02](#) (work in progress), March 2015.
- [I-D.carpenter-anima-gdn-protocol]
Carpenter, B. and B. Liu, "A Generic Discovery and Negotiation Protocol for Autonomic Networking", [draft-carpenter-anima-gdn-protocol-03](#) (work in progress), April 2015.
- [I-D.irtf-nmrg-an-gap-analysis]
Jiang, S., Carpenter, B., and M. Behringer, "General Gap Analysis for Autonomic Networking", [draft-irtf-nmrg-an-gap-analysis-06](#) (work in progress), April 2015.
- [I-D.irtf-nmrg-autonomic-network-definitions]
Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking - Definitions and Design Goals", [draft-irtf-nmrg-autonomic-network-definitions-07](#) (work in progress), March 2015.
- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", [RFC 3647](#), November 2003.

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

Zongpeng Du
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: duzongpeng@huawei.com

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Qiong Sun
China Telecom
No.118, Xizhimennei Street
Beijing 100035
P. R. China

Email: sunqiong@ctbri.com.cn

