AN Use Case BOF
Internet-Draft
Intended status: Informational
Expires: October 30, 2014

S. Jiang, Ed.
Huawei Technologies Co., Ltd
B. Carpenter
Univ. of Auckland
Q. Sun
China Telecom
April 28, 2014

Autonomic Networking Use Case for Auto Address Management
draft-jiang-auto-addr-management-00

Abstract

This document describes a use case for autonomic address management in large-scale networks. It is one of a series of use cases intended to illustrate requirements for autonomic networking.

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 October 30, 2014.

Table of Contents

1. Introduction

This document is one of a set of use cases being developed to clarify the requirements for discovery and negotiation protocols for autonomic networking (AN). The background to AN is described in [I-D.irtf-nmrg-autonomic-network-definitions] and [I-D.irtf-nmrg-an-gap-analysis]. A problem statement and outline requirements for the negotiation protocol are given in [I-D.jiang-config-negotiation-ps].

This document is dedicated to how to make IP address management in large-scale networks as autonomic as possible, including operator (ISP) networks and large enterprise networks. Although this document is targeting pure IPv6 networks, autonomically sharing public IPv4 addresses among the Address Family Transition Routers (AFTRs) [RFC6333] or NAT64 [RFC6146] devices is also discussed.

Note in draft: This version is preliminary. In particular, opinions may vary about how concrete vs how abstract a use case should be.

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, the prefix management is still largely depending on human planning. In other words, there is no basic information or policies 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.

Additionally, the management of public IPv4 addresses on AFTRs or NAT64 devices is similarly rigid and static. The utilisation rate of addresses depends on the initial plan. Efficient utilisation of public IPv4 addresses is the most important requirement since they are a limited resource during the IPv4 exhaustion period.

The problem to be solved by AN is how to dynamically and autonomically manage IPv6 address space and public IPv4 addresses on AFTRs or NAT64 devices in large-scale networks, so that IP addresses can be used efficiently. The AN approach discussed in this document is based on the assumption that there was a generic dicovery and negotiation protocol that enables direct negotiation between intelligent IP routers. [I-D.jiang-config-negotiation-protocol] is one of the attempts at such a protocol.

3. 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 most 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.

Where applicable, another intended experience is dynamically and autonomically sharing public IPv4 addresses on AFTRs or NAT64 devices without human intervention. The administrator only has to configure the total available IPv4 address range.

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

4. 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:

- Identity of this device. It can be verified by the certification authority (CA) that is maintained by the network administrator(s).
- Identity of a trust anchor which is certification authority (CA) that is maintained by the network administrator(s).
- Role of this device.
- An IPv6 prefix length for this device.
- An IPv6 prefix that is assigned to this device and its downstream devices.
- A public IPv4 address pool if the device acts as an AFTR or NAT64 device.

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

- Identity of a trust anchor which is a certification authority (CA) that is maintained by the network administrator(s).
- Total IPv6 address space. It is one (or several) IPv6 prefix(es).
- A public IPv4 address pool if the network provides IPv4 over IPv6 access or IPv4/IPv6 transition services.
- The initial prefix length for each device role.

4.1. 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:

- Role of this device, this includes whether this device acts as an AFTR or NAT64 device.
- Default IPv6 prefix length for this device.
- Identity of this device.

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

4.2. 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.

- Non-default value for the IPv6 prefix length for this device. This needs to be decided based on the role of this device.
- The initial prefix length for each device role.
- Identity of a trust anchor.
- Whether to allow the device request more address space.
- Whether to allow the device to request or share public IPv4 address.
- The policy when to request more address space, for example, the address usage reaches a certain limit or percentage.

5. Interaction with other devices

5.1. 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 optimise them.

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

- The device may require to be assigned more IPv6 address space, if it used up its assigned IPv6 address space.

- An AFTR or NAT64 device will need to request and acquire an initial public IPv4 address pool.

- An AFTR or NAT64 device will need to discover its neighbors, from which it may acquire spare public IPv4 addresses.

- An AFTR or NAT64 device may acquire spare public IPv4 addresses with their associated available period.

5.2. Monitoring, diagnostics and reporting

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

- The actual address assignments need to be logged for the potential offline management operations.

- 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.

- A forecast of address exhaustion should be reported.

6. 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, such as dynamically negotiating the sharing of public IPv4 addresses.

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.

7. Security Considerations

Relevant security issues are discussed in [I-D.irtf-nmrg-autonomic-network-definitions], [I-D.jiang-config-negotiation-ps]. The security mechanism in this document is established on a Public Key Infrastructure (PKI) system [RFC3647] that is maintained by the network administrator(s).

8. IANA Considerations

This document requests no action by IANA.

9. Acknowledgements

Valuable comments were received from Michael Behringer and Chongfeng Xie.

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

10. Change log [RFC Editor: Please remove]

draft-jiang-auto-addr-management-00: original version, 2014-04-28.

11. References

[I-D.irtf-nmrg-an-gap-analysis]
Behringer, M., Carpenter, B., and S. Jiang, "Gap Analysis for Autonomic Networking", draft-irtf-nmrg-an-gap-analysis-00 (work in progress), April 2014.

[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-00 (work in progress), December 2013.

[I-D.jiang-config-negotiation-protocol]
Jiang, S., Carpenter, B., Liu, B., and Y. Yin, "Configuration Negotiation Protocol for Network Devices", draft-jiang-config-negotiation-protocol-01 (work in progress), April 2014.

[I-D.jiang-config-negotiation-ps]
Jiang, S., Yin, Y., and B. Carpenter, "Network Configuration Negotiation Problem Statement and Requirements", draft-jiang-config-negotiation-ps-02 (work in progress), January 2014.

[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.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

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

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

Email: brian.e.carpenter@gmail.com

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

Email: sunqiong@ctbri.com.cn