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

G. Chen
China Mobile

February 25, 2013

Analysis of NAT64 Port Allocation Method
draft-chen-sunset4-cgn-port-allocation-01

Abstract

The document enumerated methods of port assignment in CGN contexts, more focused on NAT64 environments. The analysis categorized the different methods with several key features. Corresponding to those features, the uses of existing protocols are also described. The potential concerns and workaround have been discussed. It's expected the document could provide a informative base line to help operators choosing a proper method.

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.

Table of Contents

1. Introduction

With the depletion of IPv4 address, CGN has been adopted by ISPs to expand IPv4 spaces. Relying upon the mechanism of multiplexing multiple subscribers' connections over a smaller number of shared IPv4 addresses, CGN mapped IP addresses from one address realm to another, providing transparent routing to end hosts. [I-D.ietf-behave-lsn-requirements] defined the term of CGN. Several proposals including DS-Lite[RFC6333], NAT64[RFC6145], [RFC6146], NAT444 would likely fall into the scope. Focusing on the topic of IPv6 migration, the memo elaborate the considerations in NAT64 environment, where there IPv6-only nodes are connected.

[RFC6269] has provided a thoughtful analysis on the issues of IP sharing. It was point out that IP sharing may bring the impacts to law enforcement since the information of source address would be lost during the translation. Network administrators have to log the mapping status for each connection in order to identify a specific user associated with an IP address. It would post a challenge to operators, since it requires additional storage resource and data inspection process for indentifying the real users. It's desirable to compact the logging information by a rational port allocation. Those allocation policies should consider the tradeoff between port utilization and log storage compression. The document is trying to enumerate the several dimensions for assigning the port information. It's expected administrator could use those factors to determine their own properties.

2. Port Allocation Management

This section lists several factors to allocate the port information in NAT64 equipments. It's likely that each allocation model would have an exemplified case. The relevant issues and potential workarounds have also been described for each aspect.

2.1. NAT vs NAPT

NAT64 may not do Network Address Port Translation (NAPT), but only Network Address Translation (NAT). In those cases, there is no concern about port assignment. Those translation methods would relieve the demands of log information storage, since NAT does not have to administer address management with session flows. Furthermore, there is no requirement to maintain log when NAT64 performing stateless translations. Some existing practices are listed below from two aspects.

o Stateful NAT

The stateful NAT can be implemented either by static address translation or dynamic address translation.

In the case of static address assignment, one-to-one address mapping for hosts between a IPv6 network address and an IPv4 network address would be pre-configured on the NAT operation. Those cases normally occurred when a server deployed in a IPv6 domain. The static configuration ensure the stable inbound connectivity. The static method is also easier for Lawful interception system to derive the mapped address, since the mapping didn't change with time.

Dynamic address assignment would periodically free the binding so that the global address could be recycled for later uses. Addresses could be more efficiently used by time-division manner. It only requires systems maintaining mappings for per-customer, other than per-session flow. This method is usually adopted to reduce the log burden in some protocols.

o Stateless NAT

The stateless NAT is performed in compliant with [RFC6145]. Public IPv4 address is required to be inserted in IPv6 address. Therefore, NAT64 could directly extract the address and no need to record mapping states. The lawful interception could likely identify the IPv4 address through received IPv6 address. It's a protocol to eliminate the log information storage. There are two potential concerns for those technologies. First off, the static one-to-one mapping may didn't address the issue of IPv4 depletion. Secondly, it introduced the dependency of IPv4/IPv6. That would create new limitations since the change of IPv4 address would cause renumbering of IPv6 addresses. Whereas, that is useful for the IDC migration where there is IPv6 servers pools to receive inbound connections from IPv4 users externally[I-D.anderson-siit-dc].

2.2. Dynamic vs Static

When the case comes to port assignment, there are two methods for port allocations.

o Dynamic assignment

NAT64 normally do the dynamic assignment. In respect to the received connections, ports can be allocated to each sessions. NAT64 would do the dynamic approach by default, since it achieves maximum port utilization. One downside for this approach is the gateway has to record log information for each session. That would potentially

increase the log volume. There is a statistic from field trials that the average number of connections per customer per day at approximately 10,000 connections. If log system is required to store information for 180 days, the testing shown that the amount of data records would achieve 20T.

o Static assignment

The static assignment make a bulk of port reservation for a specific address. The bulk of port could be either a contiguous or non-contiguous port range for sake of attacks defense. [I-D.donley-behave-deterministic-cgn]has described a deterministic NAT to reserve a port range for each specific IP address. That is a significant improvement for lightening log volume. However, a trade-off should be made when administor has to consider the port utilization. For the administor who prioritize the port utilization, dynamic assignment maybe a suitable solution for them. Another consideration is using Address-Dependent Mapping or Address and Port-Dependent Mapping[RFC4787] to increase the port utilization. This feature has already been implemented as vendor-specific features. Whereas, it should be noted that REQ-7, REQ-12 in[I-D.ietf-behave-lsn-requirements] may reduce the incentivesr.

2.3. Centralized vs Distributed

There are increasing needs to connect NAT64 with downstream NAT46-capable CE devices to support IPv4 hosts/applications in a IPv6-only access. Several solutions have been proposed in this area, e.g. 464xlat[I-D.ietf-v6ops-464xlat], MAP-T[I-D.ietf-softwire-map-t] and 4rd[I-D.ietf-softwire-4rd]. With the feature of double-translation, the port allocation can be managed as a centralized way on NAT64 or distributed to downstream devices(e.g, CPE connected with NAT64) .

o Centralized Assignment

A centralized method would make port assignments when traffic come to NAT64. The allocation policy is enforced on a centralized gateway. Either a dynamic or static port assignment is made for received sessions.

o Distributed Assignment

NAT64 could also delegate the pre-allocated port range to customer edge devices. That can be achieved through additional out-band provisioning signals(e.g.[I-D.ietf-pcp-base] ,[I-D.tsou-pcp-natcoord][I-D.ietf-softwire-map-dhcp]). The distributed model normally performed A+P style for static port assignment. NAT64 should hold the corresponding mapping in

accordance with assigned ports. Those methods could shift NAT64 port computation/states into downstream devices. The detailed benefits was documented in [I-D.ietf-softwire-stateless-4v6-motivation].

3. Discussions

With demands of reducing log volume, there are several approaches of port assignment described in the aforementioned sections. It could be found that a trade-off between maximum port utilization and log volume always exist to justify the use of different solutions. In respect to difference of port assignment, the granularity of log could be ranked as per-session, per-port-bulk, per-customer and None. With the reduction of log volume, port utilization ratio is likely decreased. Therefore, the decision should be made if there is a quantitative statistic to evaluate what is gain from reducing log volume and loss from decreasing port utilization. Those data analysis is planned to be added after further lab testing. Operators could choose the proper method considering following:

- Average connectivities per customer per day
- Peak connectivities per day
- The amount of public IPv4 address in NAT64
- Application demands for specific ports
- The parallel processing capabilities of NAT64
- The tolerance of Log volume

Apart from above, the port allocation can be tuned corresponding to the phase of IPv6 migration. The use of NAT64 would advance IPv6, because it provides everyone incentives to use IPv6, and eventually the result is an end-to-end IPv6-only networks with no needs for IPv4. As more content providers and service are available over IPv6, the utilization on NAT64 goes down since fewer destinations require translation progressing. In the trend of decreased IPv4 connections, NAT64 could relax the multiplexing ratio of shared IPv4 address by either a delivered message or a centralized control . A load for log system can also be relieved due to simplified mapping states.

4. Security Considerations

TBD

5. IANA Considerations

This document makes no request of IANA.

6. References

6.1. Normative References

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", draft-ietf-pcp-base-29 (work in progress), November 2012.

[I-D.ietf-softwire-map-dhcp]
Mrugalski, T., Troan, O., Bao, C., Dec, W., Yeh, L., and X. Deng, "DHCPv6 Options for Mapping of Address and Port", draft-ietf-softwire-map-dhcp-02 (work in progress), February 2013.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[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.

6.2. Informative References

[I-D.anderson-siit-dc]
Anderson, T., "Stateless IP/ICMP Translation in IPv6 Data Centre Environments", draft-anderson-siit-dc-00 (work in progress), November 2012.

[I-D.donley-behave-deterministic-cgn]
Donley, C., Grundemann, C., Sarawat, V., Sundaresan, K., and O. Vautrin, "Deterministic Address Mapping to Reduce Logging in Carrier Grade NAT Deployments", draft-donley-behave-deterministic-cgn-05 (work in progress), January 2013.

[I-D.ietf-behave-lsn-requirements]
Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", draft-ietf-behave-lsn-requirements-10 (work in progress), December 2012.

[I-D.ietf-softwire-4rd]
Jiang, S., Despres, R., Penno, R., Lee, Y., Chen, G., and M. Chen, "IPv4 Residual Deployment via IPv6 - a Stateless Solution (4rd)", draft-ietf-softwire-4rd-04 (work in progress), October 2012.

[I-D.ietf-softwire-map-t]
Li, X., Bao, C., Dec, W., Troan, O., Matsushima, S., and T. Murakami, "Mapping of Address and Port using Translation (MAP-T)", draft-ietf-softwire-map-t-01 (work in progress), February 2013.

[I-D.ietf-softwire-stateless-4v6-motivation]
Boucadair, M., Matsushima, S., Lee, Y., Bonness, O., Borges, I., and G. Chen, "Motivations for Carrier-side Stateless IPv4 over IPv6 Migration Solutions", draft-ietf-softwire-stateless-4v6-motivation-05 (work in progress), November 2012.

[I-D.ietf-v6ops-464xlat]
Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", draft-ietf-v6ops-464xlat-10 (work in progress), February 2013.

[I-D.tsou-pcp-natcoord]
Sun, Q., Boucadair, M., Deng, X., Zhou, C., Tsou, T., and S. Perreault, "Using PCP To Coordinate Between the CGN and Home Gateway", draft-tsou-pcp-natcoord-09 (work in progress), November 2012.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

Author's Address

Gang Chen
China Mobile
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China

Email: phdgang@gmail.com