Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 10, 2013

C. Zhou
Huawei Technologies
T. Tsou
Huawei Technologies (USA)
C. Grundemann
Cablelabs

July 16, 2012

Scenarios of IPv4 sunsetting
draft-zhou-sunset4-scenarios-01

Abstract

This document describes scenarios at subscriber, carrier and enterprise sites during IPv4 sunsetting. In each site, there may be different requirements and issues. The aim of this document is to put forward some issues in these scenarios and to identify whether further specifications are needed to solve these issues to facilitate IPv4 sunsetting.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

There are already a set of documents in IETF which to some extent facilitate IPv6 transition. For example, [I-D.ietf-behave-lsn-requirements] describes the common requirements of CGN (NAT44). For devices which implement NAT, MIB module is introduced in [I-D.ietf-behave-nat-mib]. However, there are many scenarios and issues encountered at subscriber, carrier and enterprise sites, e.g., source trace, high availability, and ALG issues at carrier site scenario. In this document, these scenarios will be proposed in detail and some issues in these scenarios will be discussed.

2. Conventions

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.

3. Subscriber Site Scenario

Some subscribers have the need to run some servers at home, for example, web server, webcam, FTP server, etc. Sometimes when a subscriber equipment reboots it may be assigned a new IP address which is different from the previous one. To accomadate this IP address change, DDNS is used. If NAT is used in subscribe premise, static port-forwarding can be configured for a specific service so that DDNS can continue to work. But if CGN is deployed in the operator's network, one CGN will serve a lot of users, static port-forwarding configuration will require a lot of operational work, and there will be IP address and port conflict if multiple subscribers require a same purlic IP address and / or port. A traditional solution is to assign public IP address to scribers who needs to run a server at home, but this will also require extra operational work, make the network more complicated. In such a case, a possible solution is that DDNS system works together with some dynamic NAT traversal technologies, e.g. UPnP/PCP, or the CGN provide DDNS proxy.

4. Carrier Site Scenario

For carrier site case, we provide some scenarios and issues as below for the working group discussion.

4.1. Traceback

Before CGN is introduced, the servers use the source IPv4 address as an identifier to treat incoming packets differently. When the

address sharing scheme is proposed, the server could not identify which host sends the packet because the packets are from the same source address. [I-D.boucadair-intarea-nat-reveal-analysis] proposed solutions to identify each host sharing the same IP address with a unique host identifier. But there are at least two issues existing in the traceback solutions: logging architecture and port allocation algorithm.

As described in section 4 of [I-D.ietf-behave-lsn-requirements], the destination addresses or ports should not be logged in CGN in order to reduce the logs in CGN. [RFC6302]provides recommendations for Internet-facing servers logging incoming connections. But it does not provide any recommendations about logging on carrier-grade NAT. So, a logging architecture in CGN to maintain records of the relation between a customer's identity and IP/port resources is needed.

[RFC6431] provides port set options for port range allocation: contiguous, non-contiguous and random. In the random-based solution, the algorithm should be reversible in order to trace the host. But this may bring some security problems.

4.2. Stateless CGN

Carrier-grade NAT44 is one of the solutions to deal with the IPv4 address shortage problem. But the current NAT44 CGN(Carrier-grade NAT) is stateful and TCP/UDP session based, which makes the CGN complex. There have been a number of efforts at IETF moving the NAT function from a stateful carrier grade NAT to the CPEs by allocating port sets to each customer, e.g., MAP/4RD-U, LAFT6, and etc. There is also a requirement for NAT44 CGN to become completely stateless.

4.3. High Availability

In most ISP networks, one CGN device may serve large number of customers. For stateful NAT, if there is a single point of failure in the CGN, the service may be interrupted or degraded. Therefore, redundancy capabilities (including hot and cold standby) of the CGN devices are strongly needed to deliver highly available services to customers. [I-D.xu-behave-stateful-nat-standby] may be a possible way to solve this problem. In addition, pre-configuring a pool of public IPv4 addresses to the CGN device when it is in failure may also be a candidate solution.

4.4. ALG

Carrier-grade NAT44 performs NAT-44 and inherits the limitations of NAT. Some protocols require ALGs in the CGN to traverse through the NAT, e.g., FTP, RTP. However, in most ISP's network, CGN is a shared

network device which needs to support a large number of sessions. It is a huge work load for CGN to implement every ALGs, which will obviously bring bad performance for CGN. How to make CGN more efficiency under the pressure of ALG becomes an issue. One possible solution is to let the CPE or host implement ALG instead of CGN, or a flexible way to make ALG at either CPE or CGN is needed.

5. Enterprise Site Scenario

NAT is a basic feature of enterprise network. The firewall/NAT device is deployed at the entrance of the enterprise network, following by the web server and the terminal. Part of the web servers are required to open publically to provide one domian name and corresponding IP address (Two ways: the enterprise has its own DNS server; the enterprise has no DNS server and needs to publicize one public address). NAT device is required to support this specific case. In addition, the terminal or the web server following NAT device need to access Internet. There are requirements for the enterprise users to record the NAT translation information.

Some basic requirements of NAT device are also valid in enterprise scenarios, e.g., NAT traceback, port range allocation and NAT standby. NAT device needs to record the NAT translation log in traceback solutions. NAT server is required to support port range allocation. Two NAT devices should store the information of each other to guarantee normal operation when one device is in failure in enterprise scenarios.

6. IANA Considerations

No request to IANA.

7. Security Considerations

TBD

Authors' Addresses

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone:
EMail: cathy.zhou@huawei.com

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
EMail: tina.tsou.zouting@huawei.com

Chris Grundemann
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Phone: 303.661.3779
Email: c.grundemann@cablelabs.com

8. Normative References

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

[I-D.ietf-behave-nat-mib] Perreault, S., Tsou, I., and S. Sivakumar, "Additional Definitions of Managed Objects for Network Address Translators (NAT)", April 2012.

[I-D.boucadair-intarea-nat-reveal-analysis] Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Solution Candidates to Reveal a Host Identifier in Shared Address Deployments", September 2011.

[I-D.xu-behave-stateful-nat-standby] Xu, X., Boucadair, M., Lee, Y., and G. Chen, "Redundancy Requirements and Framework for Stateful Network Address Translators (NAT)", October 2010.