Computer Communications 109 (2017) 162–175

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Benchmarking methodology for DNS64 servers

Gábor Lencse [a,*], Marius Georgescu [b], Youki Kadobayashi [c]

[a] Department of Networked Systems and Services, Budapest University of Technology and Economics, Magyar tudósok körútja 2, Budapest, H-1117, Hungary
[b] IP/MPLS Backbone Department of RCS&RDS, Str. Dr. Nicolae D. Staicovici 71-75, Bucharest 030167, Romania
[c] Internet Engineering Laboratory of Nara Institute of Science and Technology, Takayama-cho, 8916-5, Nara, 630-0192 Japan

ARTICLE INFO

Article history:
Received 17 November 2016
Revised 29 April 2017
Accepted 15 June 2017
Available online 16 June 2017

Keywords:
Benchmarking
DNS64
Internet
IPv6
IPv6 transition
Performance analysis

ABSTRACT

DNS64 is an important IPv6 transition technology used in convergence with NAT64 to enable IPv6-only clients to communicate with IPv4-only servers. Several DNS64 implementations have been proposed as a solution. Their performance is an important decision factor for network operators with regard to choosing the most appropriate one among them. To that end, this article proposes a methodology for measuring their performance. The number of resolved queries per second is proposed as performance metric and a step by step procedure is given for its measurement. The design considerations behind the method are also disclosed and the performance requirements for the tester device are specified. The feasibility of our method is proven and its execution is demonstrated in two case studies, which include an empirical analysis of the tester as well as that of three open-source DNS64 implementations. The influence of the rate of existing AAAA records on the performance of the DNS64 server, as well as the influence of the cache hit rate of the DNS64 server on the performance of the DNS64 server are also measured and modeled. Our results and their precision may serve as a reference for further tests.

1. Introduction

DNS64 [1] servers together with NAT64 [2] gateways play an important role in the IPv6 transition by enabling an IPv6-only client to communicate with an IPv4-only server. We expect this scenario to be very common in the upcoming years because the ISPs (Internet Service Providers) cannot provide public IPv4 addresses to their ever increasing number of new clients, due to the depletion of the public IPv4 address pool. They could distribute private IPv4 addresses and use CGN (Carrier Grade NAT), but the forward-looking procedure is to deploy global IPv6 addresses to the new clients. However, the majority of the servers on the Internet still have IPv4 addresses only. We believe that the NAT64/DNS64 tool suite [3] is one of the best solutions for this problem. NAT64 is mentioned as the only "feasible stateful translation mechanism" in [4]. Reference [5] gives an up to date survey of the IPv4 address sharing methods, and concludes that: "The only actual address sharing mechanism that really pushes forward the transition to IPv6 is Stateful NAT64 (Class 4). All other (classes of) mechanisms are more tolerant to IPv4."

Several implementations exist for both DNS64 and NAT64. When selecting from among them, performance is a decisive factor for network operators. Having performance data produced by using standardized benchmarking methods enables network operators to compare different implementations. RFC 2544 [6] aims to define such methods. IPv6 specificities were later addressed in [7], but this document explicitly excluded IPv6 transition mechanisms from its scope. The internet draft [8] aims to cover them. There are several IPv6 transition methods and the draft attempts to be general enough to cover most of them. To that end, several categories were defined (e.g. encapsulation, single or double translation) and a specific benchmarking setup is recommended for each category. DNS64 is a solution which does not fit in these categories, and therefore requires "individual attention".

In this article, we focus on the methodology for benchmarking DNS64 servers. Our aim is threefold. We would like to give an insight into our considerations which resulted in the method specified in [8], Section 9. We also provide a detailed example of how to carry out the measurement procedure described in the draft. And last but not least we would like to receive feedback from the scientific community about the proposed benchmarking method.

The remainder of this paper is organized as follows. In Section 2, the relevance of the DNS64 performance is stated and a brief introduction to the operation of the DNS64 plus NAT64 IPv6 transition solution is given. In Section 3, a short survey of other methodologies for the performance analysis of DNS64 servers is

* Corresponding author.
E-mail addresses: lencse@hit.bme.hu (G. Lencse), marius.georgescu@rcs-rds.ro (M. Georgescu), youki-k@is.aist-nara.ac.jp (Y. Kadobayashi).

http://dx.doi.org/10.1016/j.comcom.2017.06.004
0140-3664/

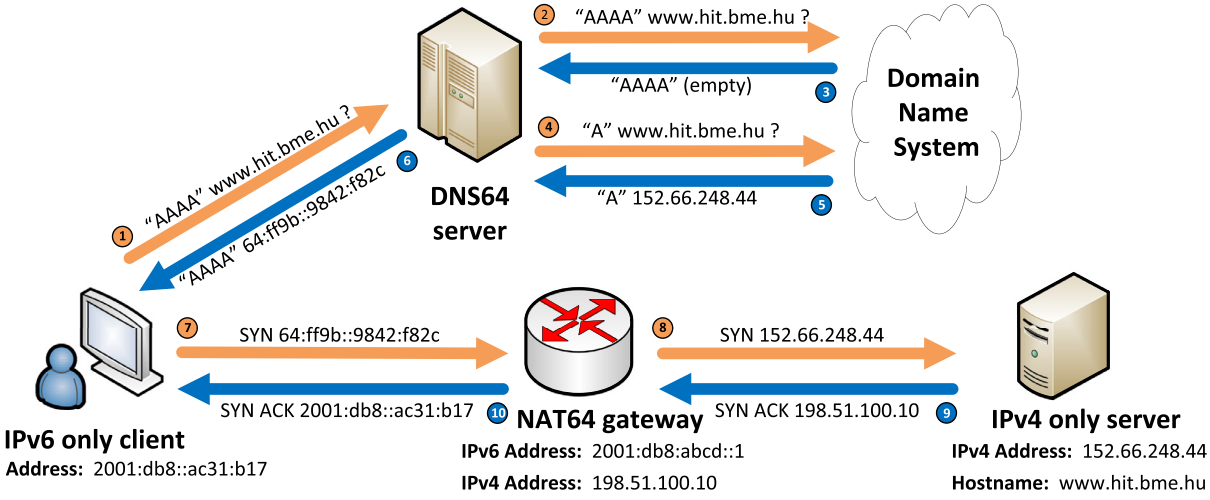

Fig. 1. The operation of the DNS64+NAT64 solution: an IPv6-only client communicates with and IPv4-only server [10].

presented. In Section 4, the proposed benchmarking methodology is described. In Section 5, performance requirements for the tester device are formulated. Section 6 is a general case study for demonstrating how to carry out the proposed tests and giving a deeper insight into the methods, as well as providing a reference concerning the expected accuracy of the results. Section 7 is a supplementary case study for examining different test and traffic setups. In Section 8, our plans for future research are outlined. Finally, in Section 9, the conclusions are stated.

2. Background information: relevance of DNS64

We examine the relevance of the DNS64 performance in the first subsection, and for those not familiar with the operation of DNS64 and NAT64, we present the operation of these important IPv6 transition solutions in the second subsection.

2.1. Relevance of DNS64 performance

A large ISP needs to resolve several hundred thousands of DNS requests per second. For example, RCS&RDS, the current employer of the second author, does about 300,000 qps (queries per second), whereas Google Public DNS did a daily average of 810,000 qps in 2012 [9].

As for DNS64, it is used only by the IPv6-only clients. Their number is usually low in the beginning at all ISPs, but it is expected to rise due to the depletion of the public IPv4 address pool. We cannot see into the future, but if the transition to IPv6 will use mainly the DNS64+NAT64 technology and there will be a time when the majority of the clients will be already IPv6-only and they still need to be able to connect to IPv4-only servers, then the DNS64 servers will be faced with a load of the above mentioned magnitude. Practically it means that a delay in the DNS64 resolution will have an immediate negative effect on the user experience of the high number of IPv6-only clients.

We believe that the science of computer communication needs a proper benchmarking methodology for DNS64 servers so that the performance of the different DNS64 implementations may be accurately measured and compared by using standardized performance metrics and researchers may adequately qualify the different DNS64 implementations by obtaining reasonable and comparable performance characteristics.

2.2. Operation of DNS64 and NAT64

We demonstrate the operation of DNS64 and NAT64 on the example of an IPv6-only client and an IPv4-only web server taken verbatim from our conference paper [10]. Fig. 1 shows a scenario where an IPv6-only client communicates with an IPv4-only web server. The DNS64 server uses the 64:ff9b::/96 *NAT64 Well-Known Prefix* [11] for generating *IPv4-embedded IPv6 addresses* [11]. There are two prerequisites for the proper operation:

1. A DNS64 server should be set as the DNS server of the IPv6-only client.
2. Packets towards the 64:ff9b::/96 network are routed to the NAT64 gateway (routing must be configured that way).

Let us follow the steps of the communication:

1. The client asks its DNS server (which one is actually a DNS64 server) about the IPv6 address of the www.hit.bme.hu web server.
2. The DNS64 server asks the DNS system about the IPv6 address of www.hit.bme.hu.
3. No IPv6 address is returned.
4. The DNS64 server then asks the DNS system for the IPv4 address of www.hit.bme.hu.
5. The 152.66.148.44 IPv4 address is returned.
6. The DNS64 server synthesizes an *IPv4-embedded IPv6 address* by placing the 32 bits of the received 152.66.148.44 IPv4 address after the 64:ff9b::/96 prefix and sends the result back to the client.
7. The IPv6 only client sends a TCP SYN segment using the received 64:ff9b::9842:f82c IPv6 address and it arrives to the IPv6 interface of the NAT64 gateway (since the route towards the 64ff9b::/96 network is set so in all the routers along the path).
8. The NAT64 gateway constructs an IPv4 packet using the last 32 bits (0x9842f82c) of the destination IPv6 address as the destination IPv4 address (this is exactly 152.66.248.44), its own public IPv4 address (198.51.100.10) as the source IPv4 address and some other fields from the IPv6 packet plus the payload of the IPv6 packet. It also registers the connection into its connection tracking table (and replaces the source port number by a unique one if necessary). Finally it sends out the IPv4 packet to the IPv4 only server.
9. The server receives the TCP SYN segment and sends a SYN ACK reply back to the public IPv4 address of the NAT64 gateway.