Distributing Root Name Servers via Shared Unicast Addresses

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This memo describes an operational guideline for root name servers to share unicast addresses.

1. Motivation

For the stability of the Internet, it is critical that there are sufficiently many DNS root servers operating at various places of the Internet.

For the stability of the domestic Internet, it is critical for each country that there are sufficiently many DNS root servers operating at various places of the Internet in the country.

However, the number of unicast IP addresses of root servers is limited. Thus, for the internationally fair operation of DNS, the number of root servers in each country (including US) must be equal to the number of unicast IP addresses of root servers divided by the

number of countries (some weight may be given according to the number of Internet hosts in each country).

Given the current number of countries and IP addresses of root servers, each country (again, including US) will be able to have 1/20 root servers, which definitely is not sufficiently many.

Thus, it is necessary to somehow increase the number of root servers. This memo proposes administrative scoping of the routing ranges of unicast addresses of root servers.

With administratively scoped unicast addresses, any entity, including a country, can use the addresses for its local root servers and set the scope of the routing ranges of the addresses appropriately.

Note that operations similar to that described in this memo are possible today locally without global coordination by any operator who may be irritated by the lack of his control on (sufficiently many) root servers, which may be a source of some operational problems. This memo is an attempt to document the way to solve the problem in a least harmful manner.

Similar operation described in this memo may be applicable to gTLD servers but it is outside the scope of this memo.

2. Suggested Operation

As is demonstrated by the proliferated private use addresses, it is easy to set up routers to let unicast addresses have local scopes. It is also easy to let the unicast addresses have nested local scopes. The important difference between the addresses for privae use and root servers is in their semantics that the root servers sharing an address share the globally unique semantics of the address. The root servers may share a globally unique DNS host name, too.

A possible problem of such addresses is that the shared addresses can not be used for global communication. So, it is suggested that the root name servers with the administratively scoped shared unicast addresses have additional globally unique unicast addresses, which may be used for global communication such as zone transfer.

The other possible problem of such addresses is that the shared addresses are not managed by a single entity that the mapping from the shared address of a root server to some operational entity is impossible. However, if the routers near the root server has a global addresses, it is possible to map from the global address to an operational entity, which is expected to be operating the root server. That is, tools like traceroute works to find the operational

entity of the root servers.

To be compatible with the current practice that a single address belong to a single AS, each administratively scoped shared unicast address is assigned its own AS number. There will be multiple ASes of the AS number containing the same address ranges.

ASes, still, can be identified by adjacent ASes. For example, network operators may choose their favorite root server based on the AS numbers of the next hop ASes with, for example, AS path and BGP policy.

It is required that operators of an AS adjacent to the root servers' AS be fully responsible to the operation of the root servers. If a root server's AS is adjacent to multiple ASes, operators of all the ASes must be fully responsible to the operation of the root server. Thus, if there is a routing problem related a root server, operators of the next hop AS(es) should be contacted.

3. Assignment

Considering that each country is likely to need a considerable number of root servers, it is reasonable to make most, if not all, of the IP addresses of the root servers administratively scoped and shared.

Note that given the large number of root servers in the Internet, it is impossible that all the servers use a single server as the primary source of zone transfer. That is, the name and the IP address of the current primary server may also be shared.

Considering the huge effort to change the file containing the IP addresses of the root servers all around the Internet, the IP addresses of the root servers should better stay same as that of today. Organizations running the current root servers are requested to release the current class B or C address blocks containing the current IP addresses of the root server for the public use.

The AS numbers assigned to root server addresses are:

Name	IP Address/Mask	AS Number
A.ROOT-SERVERS.NET	198.41.0.4/8	(to be assigned by IANA)
B.ROOT-SERVERS.NET	128.9.0.107/16	(to be assigned by IANA)
C.ROOT-SERVERS.NET	192.33.4.12/8	(to be assigned by IANA)
D.ROOT-SERVERS.NET	128.8.10.90/16	(to be assigned by IANA)
E.ROOT-SERVERS.NET	192.203.230.10/8	(to be assigned by IANA)
F.ROOT-SERVERS.NET	192.5.5.241/8	(to be assigned by IANA)
G.ROOT-SERVERS.NET	192.112.36.4/8	(to be assigned by IANA)

H.ROOT-SERVERS.NET	128.63.2.53/16	(to be assigned by IANA)
I.ROOT-SERVERS.NET	192.36.148.17/8	(to be assigned by IANA)
J.ROOT-SERVERS.NET	198.41.0.10/24	(to be assigned by IANA)
K.ROOT-SERVERS.NET	193.0.14.129/24	(to be assigned by IANA)
L.ROOT-SERVERS.NET	198.32.64.12/24	(to be assigned by IANA)
M.ROOT-SERVERS.NET	202.12.27.33/24	(to be assigned by IANA)

4. Security Considerations

This memo describes just an operational guideline with no protocol change. As such, the guideline does not introduce any security issues of the protocol level.

As the route forgery to the root servers can be implemented today without this memo by anyone including local intruders, the guideline does not introduce any security issues of the operational level, either.

A guideline to track down and verify valid or forged route or AS path to the root servers is described in section 2.

5. Authors' Addresses

Masataka Ohta
Computer Center
Tokyo Institute of Technology
2-12-1, O-okayama, Meguro-ku
Tokyo 152-8550, JAPAN

Phone: +81-3-5734-3299
Fax: +81-3-5734-3415
EMail: mohta@necom830.hpcl.titech.ac.jp