

# RIPE-210 Addendum

---

Stephen Gill  
E-mail: [gillsr@cymru.com](mailto:gillsr@cymru.com)  
Revision: 1.1, 09/20/2001

---

## Contents

Introduction .....	2
Root-servers exclusion .....	2
Staying Current.....	3
Finding Current DNS Netblocks.....	3
IOS Prefix-list Configuration.....	5
JUNOS Prefix-list Configuration.....	6
Conclusion .....	7
References .....	7

## Introduction

Route damping<sup>1</sup> is a mechanism for BGP enabled routers aimed at improving the overall stability of the Internet routing table and offloading routers' CPUs. Unstable routes may have a profound effect on the interdomain routing table; in many cases if the oscillation of a flapping route is small enough, it is considered good practice to withdraw the advertisement until it has stabilized. A well known publication by the RIPE organization released in May of 2000, known as [RIPE-210](#) [1], provided excellent guidelines and watermarks on which to base these parameters.

## Root-servers exclusion

The premise of the parameters defined in the white paper is simple: the degree of restrictions placed on prefixes should increase according to length, with the exception of the netblocks that pertain to the root name servers. Since DNS resolution is at the heart of how the Internet functions, and since humans are not in the regular practice of memorizing IP addresses, these netblocks should always be announced whether they oscillate or not. Several of the netblocks belonging to the DNS servers fall within RIPE-210's most restrictive damping parameters (24 bit prefixes); these prefixes would be quite susceptible to announcement withdrawal were they to fluctuate by even a small amount. Rather than improving Internet stability, the damping of any netblocks pertaining to the DNS servers would cut off access to the root name servers and effectively disable name resolution for many domains. Domain names that had not been cached requiring authoritative responses would not be resolvable. This would by far cause more harm than good.

A savvy network administrator implementing route-flap damping in his/her network should be keenly aware of the possibility of losing access to particular DNS netblocks due to route damping. The Internet routing table is quite a dynamic environment that requires constant care and observation in certain areas. Unfortunately, many individuals do not

---

<sup>1</sup> Also referred to as route dampening by certain vendors.

realize that the DNS prefixes listed in the RIPE publication are susceptible to change and should be reviewed on a regular basis. As an example, since the original publication of RIPE-210 in May of 2000, over half of the prefixes have changed and are no longer valid.

## Staying Current

The following table displays the original list of netblocks posted in RIPE-210 and whether they still serve the same purpose as of the time of this writing:

Table 1 - RIPE-210 Prefixes

ROOT SERVER	NETBLOCK	CURRENT (Y/N)
a.root-servers.net	198.41.0.0/24	YES
e.root-servers.net	192.203.230.0/24	YES
f.root-servers.net	192.5.4.0/23	YES
g.root-servers.net	192.112.36.0/24	YES
i.root-servers.net	192.36.148.0/24	YES
j.root-servers.net	198.41.0.0/24	REDUNDANT
	195.8.96.0/19	NO
	198.41.3.0/24	NO
	210.176.0.0/16	NO
	216.33.64.0/19	NO
	205.188.128.0/17	NO
	198.17.208.0/24	NO

As you can see, over half of the prefixes listed in RIPE-210 no longer house DNS root servers. One of them is even listed twice in the publication. This was likely an oversight since there appears to be another netblock missing (out of 13) that was possibly also redundant. Notice that many of the current prefixes will fall within the strictest category of the recommended damping parameters and would be more adversely affected than others.

Once the need for keeping the list of dampened DNS prefixes up to date has been internalized, it is important to learn how to perform independent verification of the DNS netblocks currently in use.

## Finding Current DNS Netblocks

First one must obtain the current list of DNS root servers. This can be accomplished through tools that perform standard name resolution such as *nslookup*, *ping*, or even *dig*. Perhaps the easiest and most precise method is to query one of the primary name servers for the complete list of all root name servers. For example, one may glean all of the IP addresses with one simple command:

```
dig . ns @a.root-servers.net | grep "IN A" | awk '{print $1,$5}' | sort
```

Of course this assumes that you have the 'dig', 'grep', 'sort', and 'awk' tools and that 'a.root-servers.net' is resolvable. The 'dig' utility can be found with the latest version of DNS 'bind'.

Once all of the current DNS root server IP addresses have been gathered, take a stroll over to a public looking glass site or a route server and search the BGP routing table for the netblocks associated with the IP addresses uncovered in the previous step. Alternatively, one may wish to look directly in their own router's BGP table and perform the same queries.

IOS syntax  
*show ip bgp [IP address]*

JUNOS syntax  
*show bgp [IP address]*

\* Note: [IP address] should be replaced with each DNS root server's IP address until all prefixes have been obtained.

A browsable list of looking glass servers can be found at: <http://nitrous.digex.net/>. Route servers also perform the same function.

The following is a partial list:

route-views.oregon-ix.net  
ner-routes.bbnplanet.net  
route-server.cerf.net  
route-server.ip.att.net  
route-server.cbbtier3.att.net  
route-server.gblx.net  
route-server.as5388.net  
route-server.exodus.net  
route-server-ap.exodus.net  
route-server-eu.exodus.net  
route-server.colt.net

Once the steps outlined above have been adhered to, one would arrive at the list of current DNS netblocks displayed in Table 2. These should be employed when adhering to RIPE-210's damping guidelines.

**Table 2 - Updated Prefixes**

ROOT SERVER	NETBLOCK	CURRENT (Y/N)
a.root-servers.net	198.41.0.0/24	YES

b.root-servers.net	128.9.0.0/16	YES
c.root-servers.net	192.33.4.0/24	YES
d.root-servers.net	128.8.0.0/16	YES
e.root-servers.net	192.203.230.0/24	YES
f.root-servers.net	192.5.4.0/23	YES
g.root-servers.net	192.112.36.0/24	YES
h.root-servers.net	128.63.0.0/16	YES
i.root-servers.net	192.36.148.0/24	YES
j.root-servers.net	198.41.0.0/24	REDUNDANT
k.root-servers.net	193.0.14.0/24	YES
l.root-servers.net	198.32.64.0/24	YES
m.root-servers.net	202.12.27.0/24	YES

In addition to following the steps prescribed above, some may find it helpful to join distribution lists that are focused on DNS. Unfortunately the signal to noise ratio on some lists can be minimal at best. With some careful coding, one could easily craft a script that would regularly watch for modifications of name server IP addresses and warn the administrator of any changes.

## IOS Prefix-list Configuration

Updating the DNS prefix-lists on routers is quite straightforward and takes very little effort. The commands necessary to do so for Cisco have been included here for clarity and completeness, and to serve as an update to the original RIPE-210 publication.

```
ip prefix-list rootservers description DNS root server netblocks.
! a.root-servers.net, j.root-servers.net
ip prefix-list rootservers seq 5 permit 198.41.0.0/24
! b.root-servers.net
ip prefix-list rootservers seq 10 permit 128.9.0.0/16
! c.root-servers.net
ip prefix-list rootservers seq 15 permit 192.33.4.0/24
! d.root-servers.net
ip prefix-list rootservers seq 20 permit 128.8.0.0/16
! e.root-servers.net
ip prefix-list rootservers seq 25 permit 192.203.230.0/24
! f.root-servers.net
ip prefix-list rootservers seq 30 permit 192.5.4.0/23
! g.root-servers.net
ip prefix-list rootservers seq 35 permit 192.112.36.0/24
! h.root-servers.net
ip prefix-list rootservers seq 40 permit 128.63.0.0/16
! i.root-servers.net
ip prefix-list rootservers seq 45 permit 192.36.148.0/24
! k.root-servers.net
ip prefix-list rootservers seq 50 permit 193.0.14.0/24
```

```
! l.root-servers.net
ip prefix-list rootservers seq 55 permit 198.32.64.0/24
! m.root-servers.net
ip prefix-list rootservers seq 60 permit 202.12.27.0/24
```

A more complete Cisco BGP damping configuration that follows RIPE-210 and contains the updated DNS netblocks is available in the [Cisco Secure BGP Template](#) [2]. Similarly, these updated prefixes can be defined on a Juniper router by entering the following commands:

## JUNOS Prefix-list Configuration

In addition to Cisco, the commands necessary to update DNS prefixes on Juniper routers have been included here as well.

```
[edit policy-options prefix-list root-servers.net]
set 198.41.0.0/24
annotate 198.41.0.0/24 "a.root-servers.net, j.root-servers.net"
set 128.9.0.0/16
annotate 128.9.0.0/16 "b.root-servers.net"
set 192.33.4.0/24
annotate 192.33.4.0/24 "c.root-servers.net"
set 128.8.0.0/16
annotate 128.8.0.0/16 "d.root-servers.net"
set 192.203.230.0/24
annotate 192.203.230.0/24 "e.root-servers.net"
set 192.5.4.0/23
annotate 192.5.4.0/23 "f.root-servers.net"
set 112.36.0/24
annotate 112.36.0/24 "g.root-servers.net"
set 128.63.0.0/16
annotate 128.63.0.0/16 "h.root-servers.net"
set 192.36.148.0/24
annotate 192.36.148.0/24 "i.root-servers.net"
set 193.0.14.0/24
annotate 193.0.14.0/24 "k.root-servers.net"
set 198.32.64.0/24
annotate 198.32.64.0/24 "l.root-servers.net"
set 202.12.27.0/24
annotate 202.12.27.0/24 "m.root-servers.net"
```

For a full synopsis on how to configure BGP damping in accordance with RIPE-210 specifications and the updated DNS netblocks, please refer to the [JUNOS Secure BGP Template](#) [3].

## Conclusion

When dealing with BGP route damping, it behooves the network administrator to follow the well established parameters defined in RIPE-210 with the knowledge that the DNS netblocks listed within are out of date requiring further inspection and constant care. Please note that this article is not affiliated with the original authors of the RIPE-210 document or RIPE organization in any way. It was written and developed independently to provide supplementary information from a third party.

## References

[1] RIPE, "Recommendation for Coordinated Route-flap Damping Parameters", May 2000.

<http://www.ripe.net/ripe/docs/ripe-210.html>

[2] Thomas, Rob, "Cisco Secure BGP Template", June 2001.

<http://www.cymru.com/~robt/Docs/Articles/secure-bgp-template.html>

[3] Gill, Stephen, "JUNOS Secure BGP Template", October 2001.

<http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf>