

Revisiting Recommended BGP Route Flap Damping Configurations

Clemens Mosig, Randy Bush, Cristel Pelsser, Thomas C. Schmidt, Matthias Wählisch

BGP Route Flap Damping

Route

10.20.30.0/24

Flap



Damping



Last year at RIPE ...



Lessons learned



RFD is used on the Internet.

Tier1 provider as well as small ISPs
deploy RFD.

Most vendors provide deprecated,
harmful default configurations. Most
ASs use them.

Last year at RIPE ...



Recommendations to you!




1. Check the **configurations of your routers** whether you have unpurposely enabled RFD.
2. Check whether your **whois entries** are up to date.
3. Consider using **recommended parameters** (adjusting suppress-threshold) or disabling RFD.

See <https://www.ripe.net/publications/docs/ripe-580>


IETF/RIPE Recommendations are based on ...

Measurement	Pelsser <i>et al.</i> [5]
Year	2010
IP version	IPv4
RFD implementation	Cisco
Vantage point ASes	NTT, Equinix
Damping duration	estimated
RFD impact on BGP churn	✓
Collateral damage	✗
Sweet spot analysis	✗


IETF/RIPE Recommendations are based on ...

Measurement	Pelsser <i>et al.</i> [5]
Year	2010 
IP version	IPv4
RFD implementation	Cisco
Vantage point ASes	NTT, Equinix
Damping duration	estimated
RFD impact on BGP churn	✓
Collateral damage	✗
Sweet spot analysis	✗

IETF/RIPE Recommendations are based on ...

Measurement	Pelsser <i>et al.</i> [5]
Year	2010
IP version	IPv4 
RFD implementation	Cisco
Vantage point ASes	NTT, Equinix
Damping duration	estimated
RFD impact on BGP churn	✓
Collateral damage	✗
Sweet spot analysis	✗

IETF/RIPE Recommendations are based on ...

Measurement	Pelsser <i>et al.</i> [5]
Year	2010
IP version	IPv4
RFD implementation	Cisco 
Vantage point ASes	NTT, Equinix
Damping duration	estimated
RFD impact on BGP churn	✓
Collateral damage	✗
Sweet spot analysis	✗

IETF/RIPE Recommendations are based on ...

Measurement	Pelsser <i>et al.</i> [5]
Year	2010
IP version	IPv4
RFD implementation	Cisco
Vantage point ASes	NTT, Equinix ←
Damping duration	estimated
RFD impact on BGP churn	✓
Collateral damage	✗
Sweet spot analysis	✗

We took a fresh look ...

Measurement	Pelsser <i>et al.</i> [5]	This work
Year	2010	2010, 2020
IP version	IPv4	IPv4, IPv6
RFD implementation	Cisco	Cisco, Juniper
Vantage point ASes	NTT, Equinix	5 Tier-1, 20 Random ASes
Damping duration	estimated	emulated
RFD impact on BGP churn	✓	✓
Collateral damage	✗	✓
Sweet spot analysis	✗	✓

We took a fresh look ...

Measurement	Pelsser <i>et al.</i> [5]	This work
Year	2010	2010, 2020
IP version	IPv4	IPv4, IPv6 ←
RFD implementation	Cisco	Cisco, Juniper
Vantage point ASes	NTT, Equinix	5 Tier-1, 20 Random ASes
Damping duration	estimated	emulated
RFD impact on BGP churn	✓	✓
Collateral damage	✗	✓
Sweet spot analysis	✗	✓

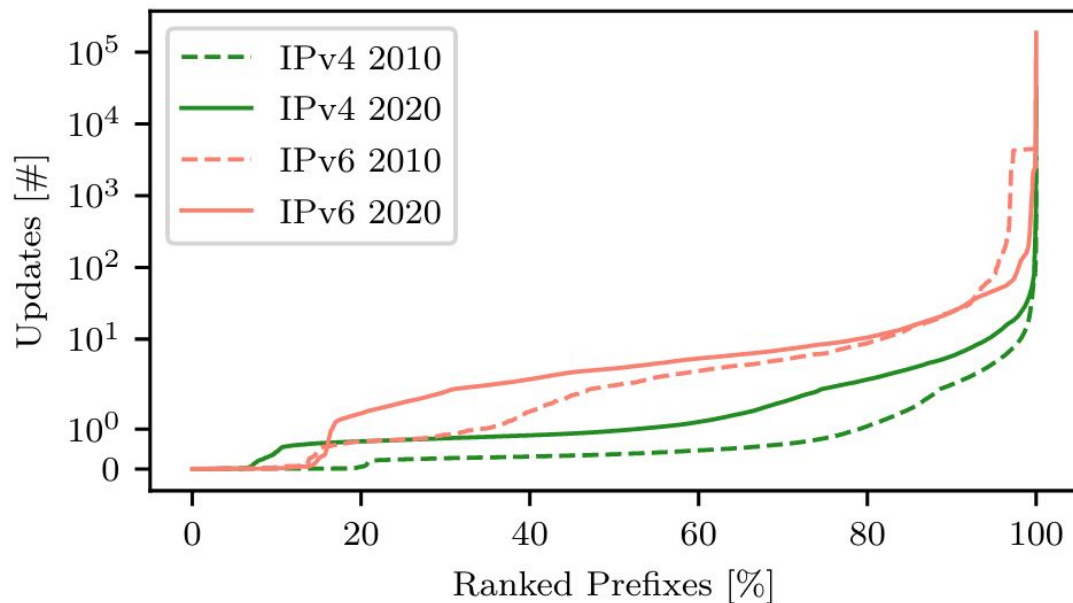
We took a fresh look ...

Measurement	Pelsser <i>et al.</i> [5]	This work
Year	2010	2010, 2020
IP version	IPv4	IPv4, IPv6
RFD implementation	Cisco	Cisco, Juniper ←
Vantage point ASes	NTT, Equinix	5 Tier-1, 20 Random ASes
Damping duration	estimated	emulated
RFD impact on BGP churn	✓	✓
Collateral damage	✗	✓
Sweet spot analysis	✗	✓

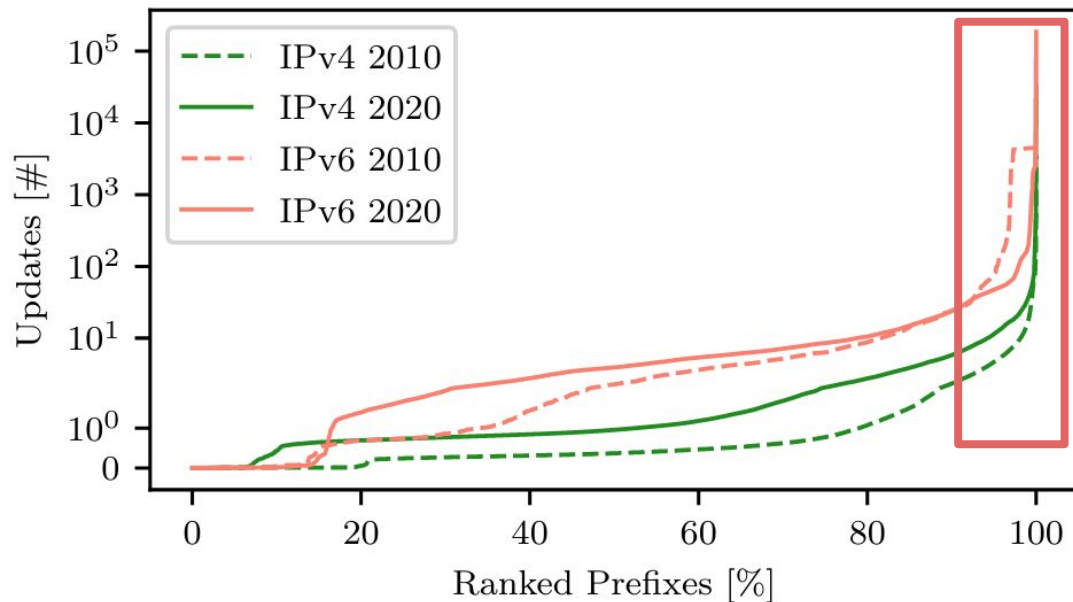
We took a fresh look ...

Measurement	Pelsser <i>et al.</i> [5]	This work
Year	2010	2010, 2020
IP version	IPv4	IPv4, IPv6
RFD implementation	Cisco	Cisco, Juniper
Vantage point ASes	NTT, Equinix	5 Tier-1, 20 Random ASes ←
Damping duration	estimated	emulated
RFD impact on BGP churn	✓	✓
Collateral damage	✗	✓
Sweet spot analysis	✗	✓

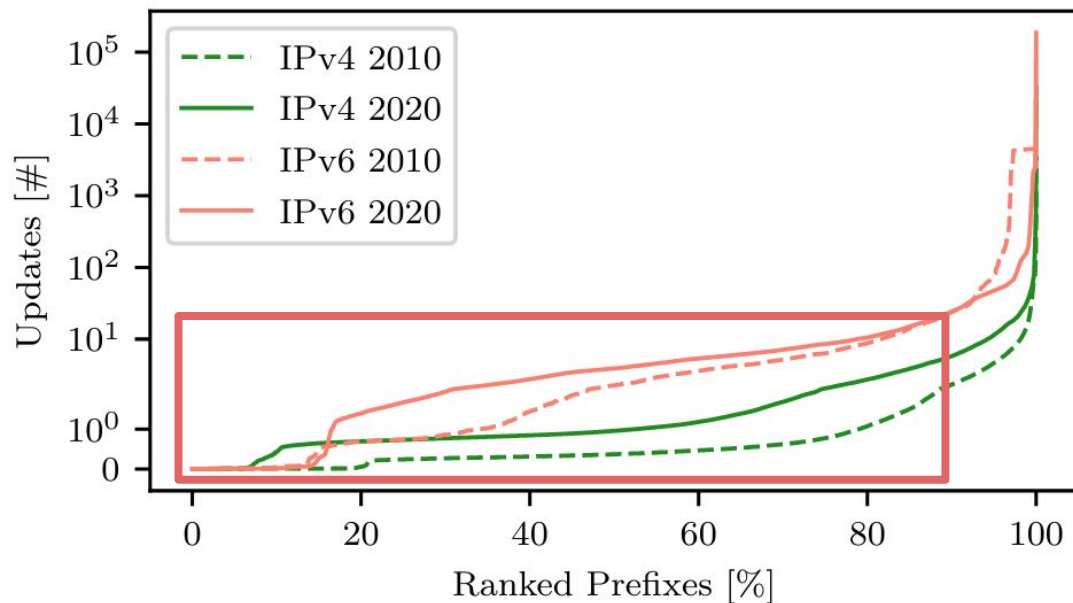
3% of all IPv4 prefixes cause **53.9%** of BGP updates



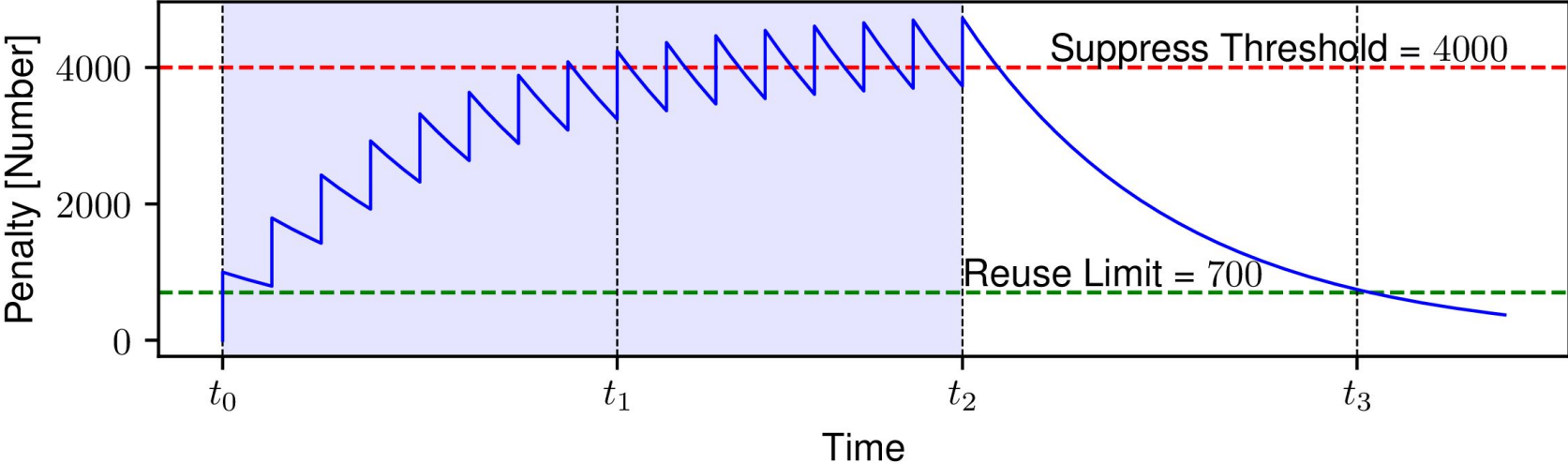
3% of all IPv4 prefixes cause **53.9%** of BGP updates



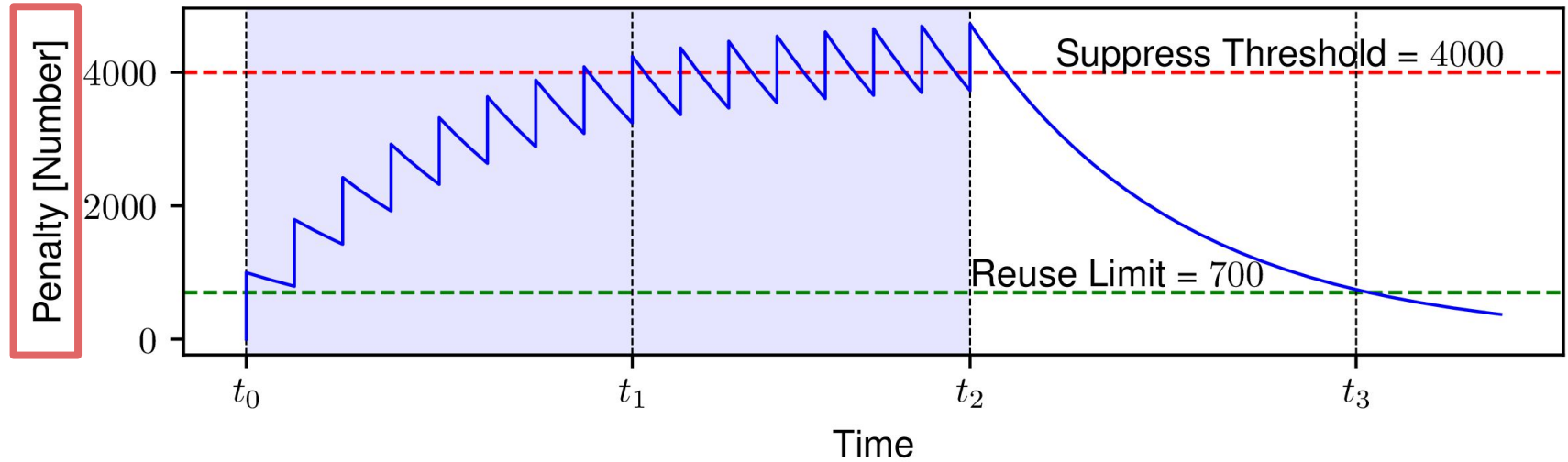
3% of all IPv4 prefixes cause **53.9%** of BGP updates



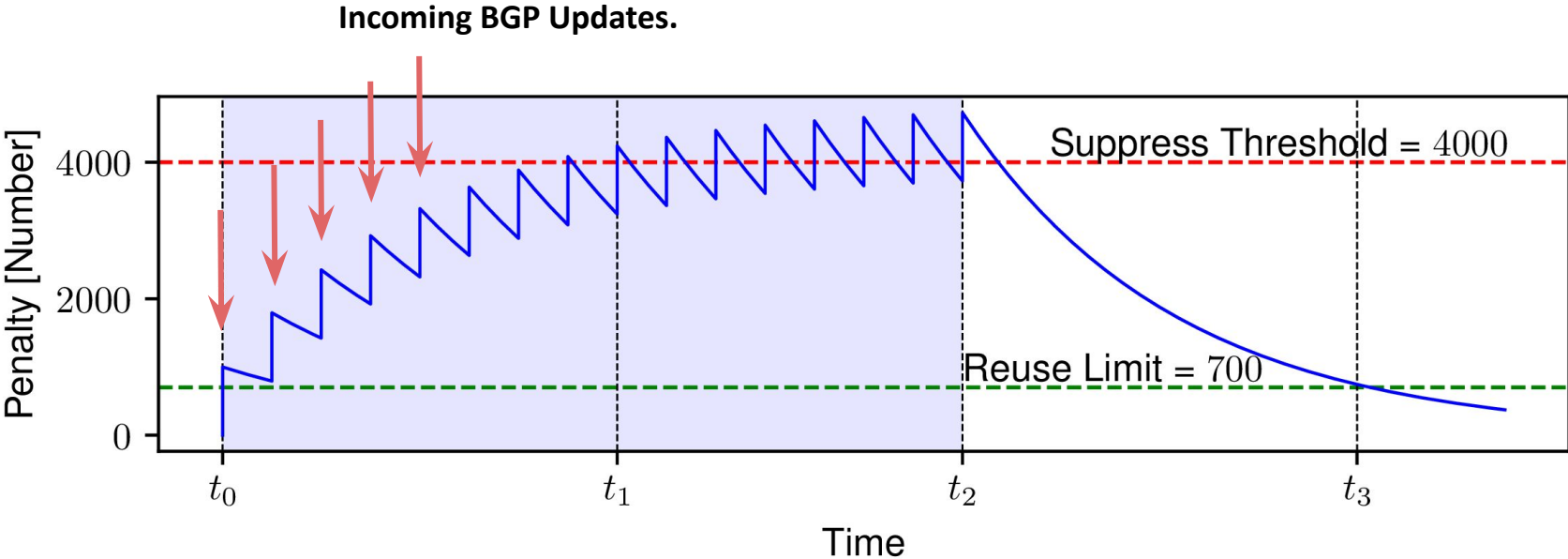
Route Flap Damping Mechanism



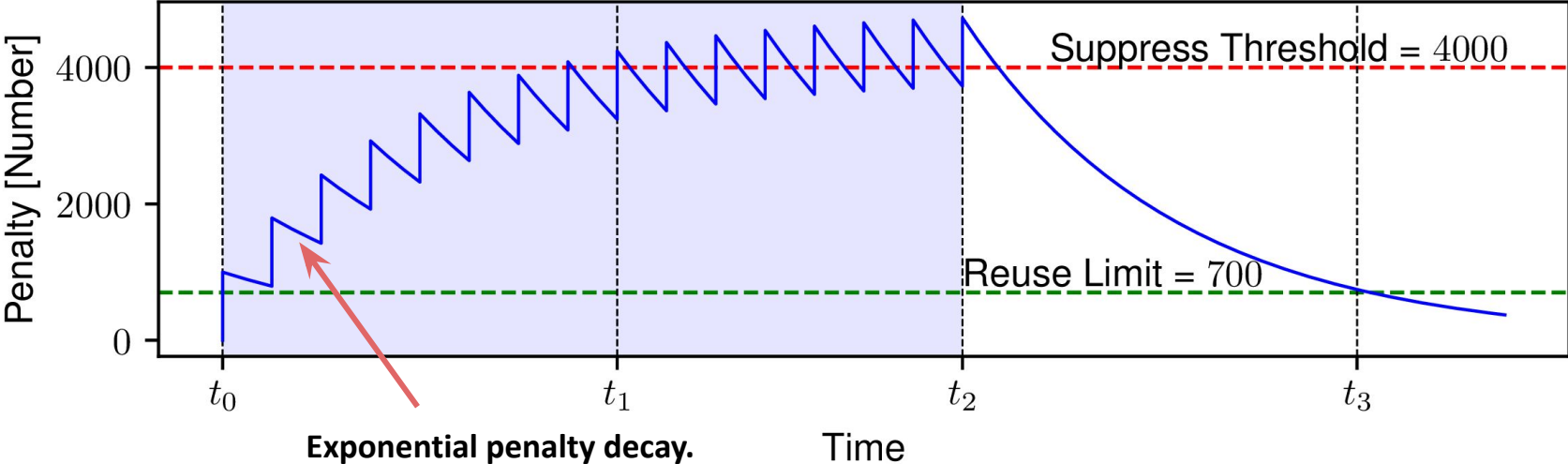
Route Flap Damping Mechanism



Route Flap Damping Mechanism

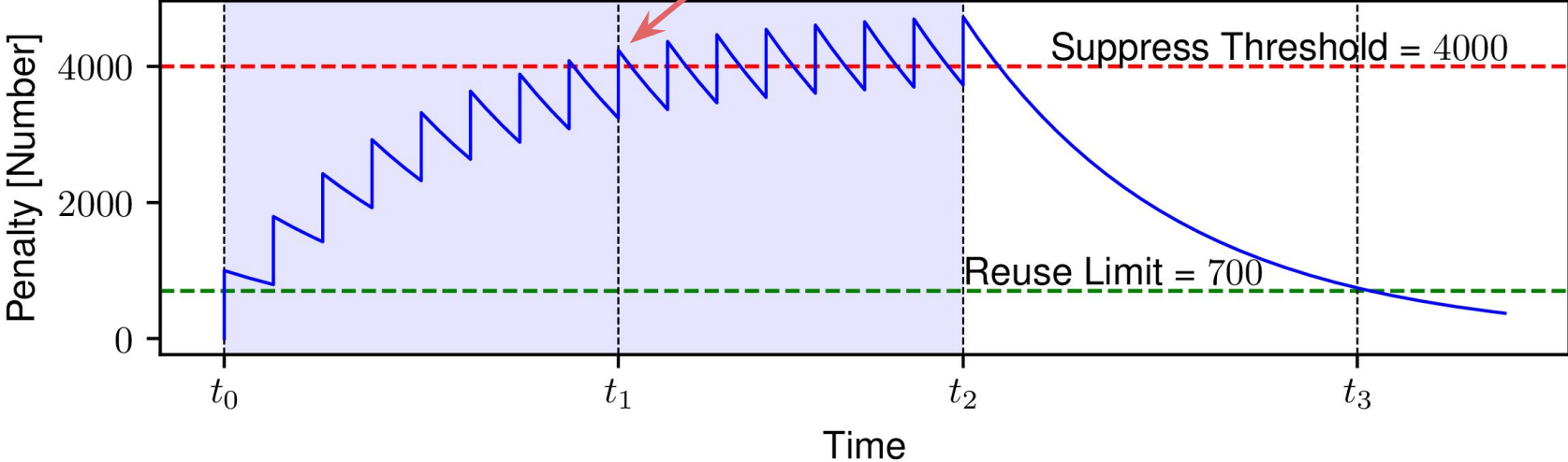


Route Flap Damping Mechanism

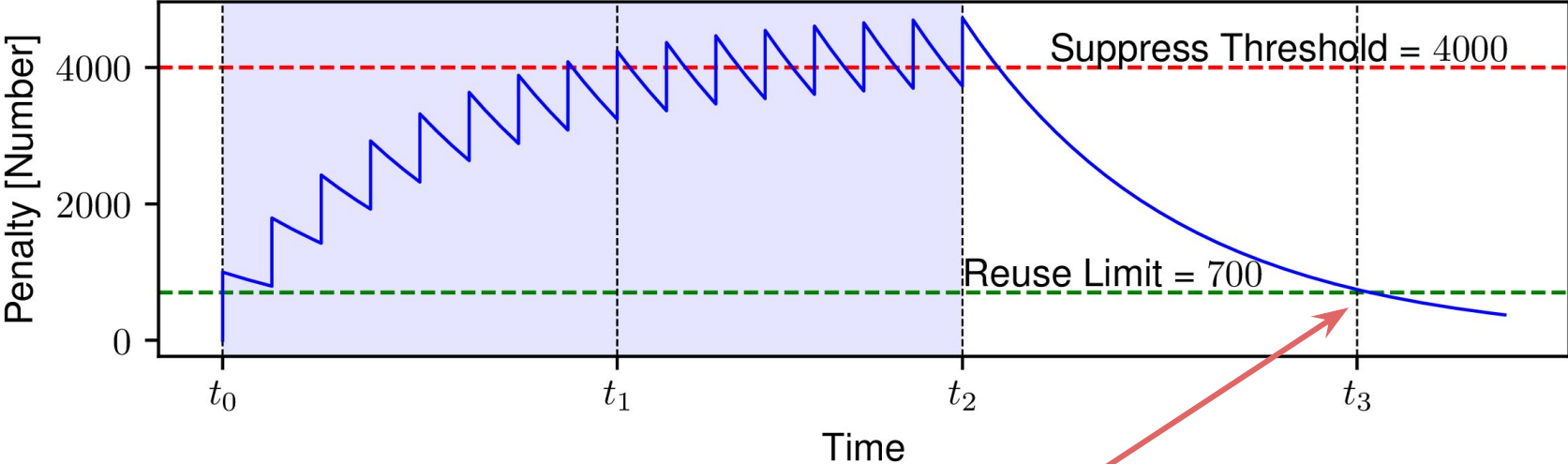


Route Flap Damping Mechanism

Suppress Threshold reached!

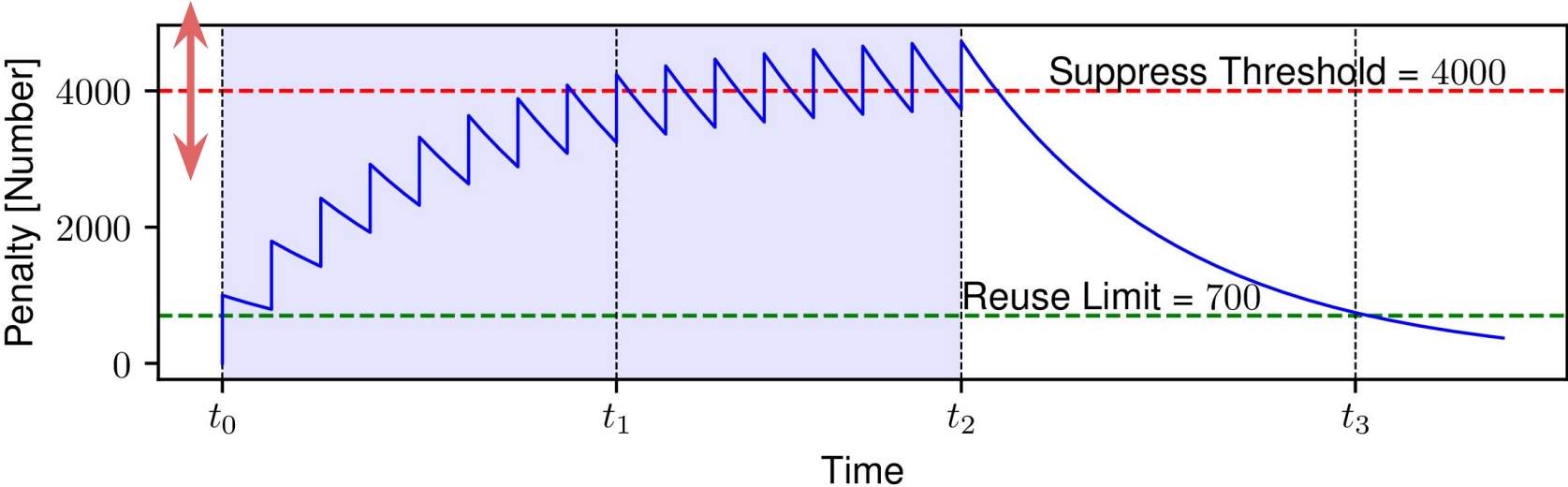


Route Flap Damping Mechanism

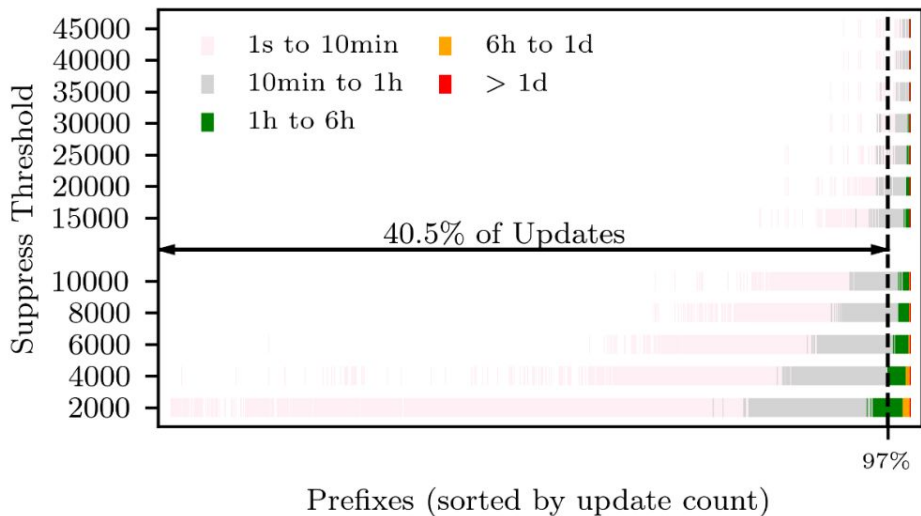


Prefix considered usable again.

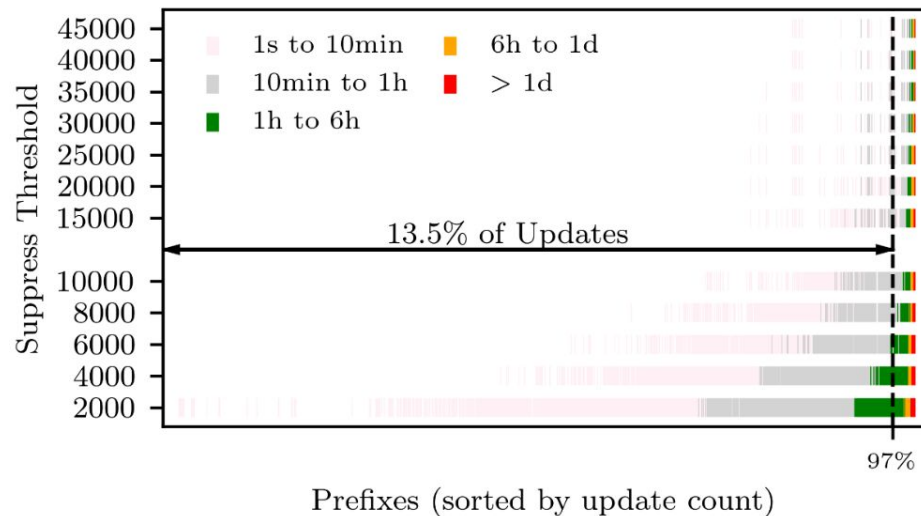
Route Flap Damping Configuration depends on the Suppress Threshold.



Suppress Duration for different thresholds

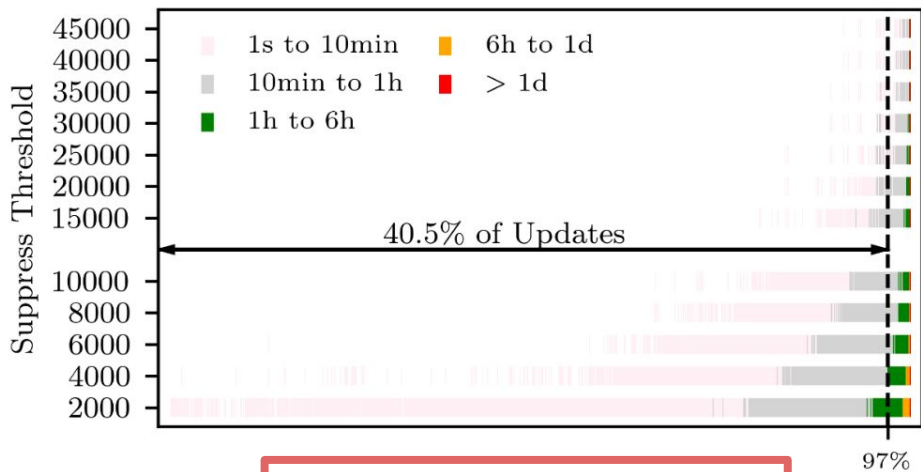


IPv4



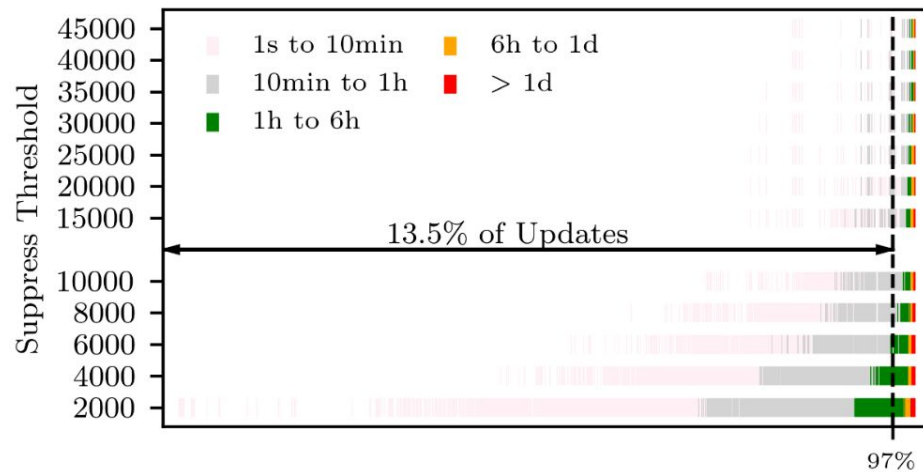
IPv6

Suppress Duration for different thresholds



Prefixes (sorted by update count)

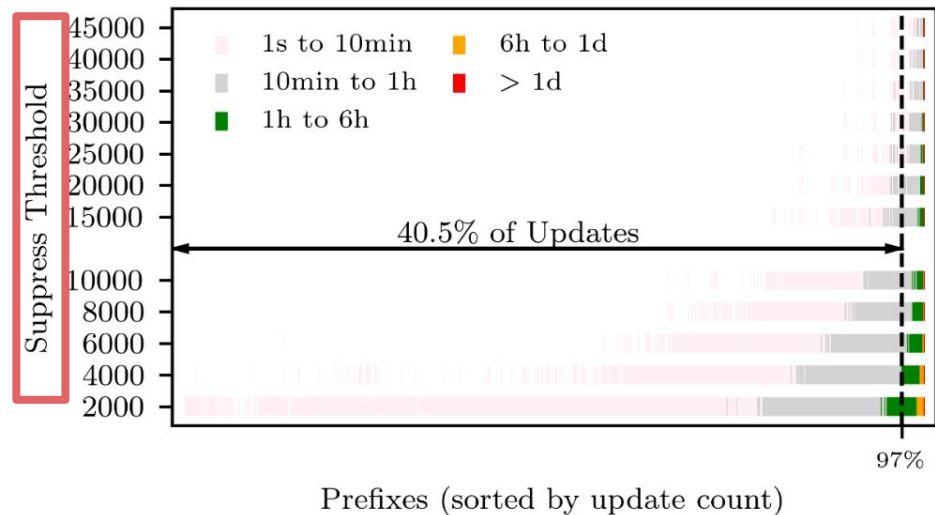
IPv4



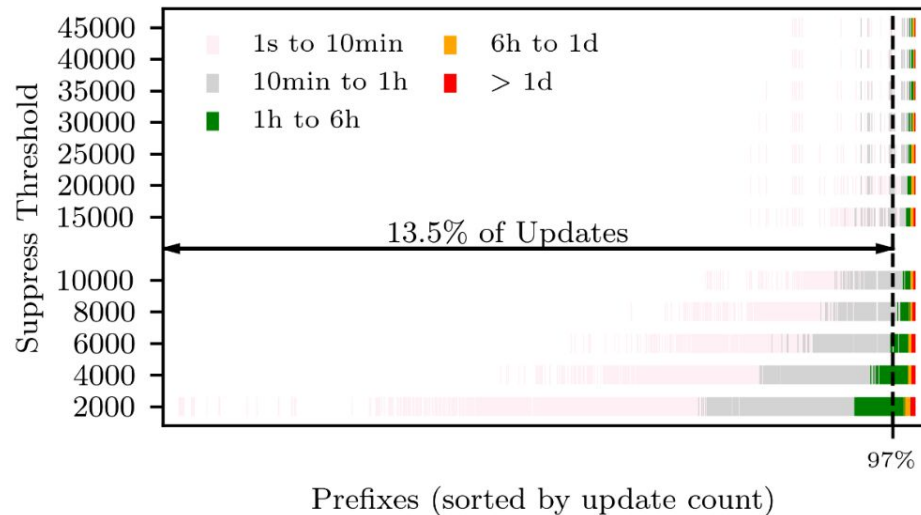
Prefixes (sorted by update count)

IPv6

Suppress Duration for different thresholds

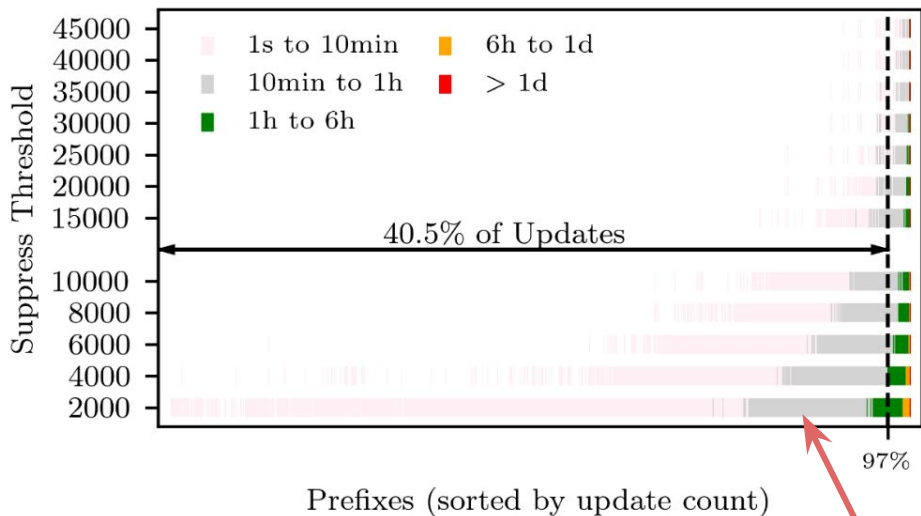


IPv4



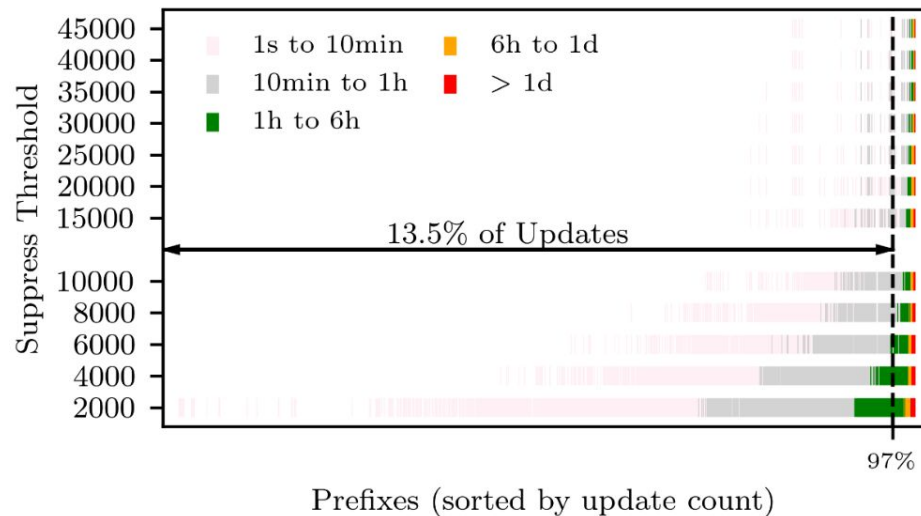
IPv6

Suppress Duration for different thresholds



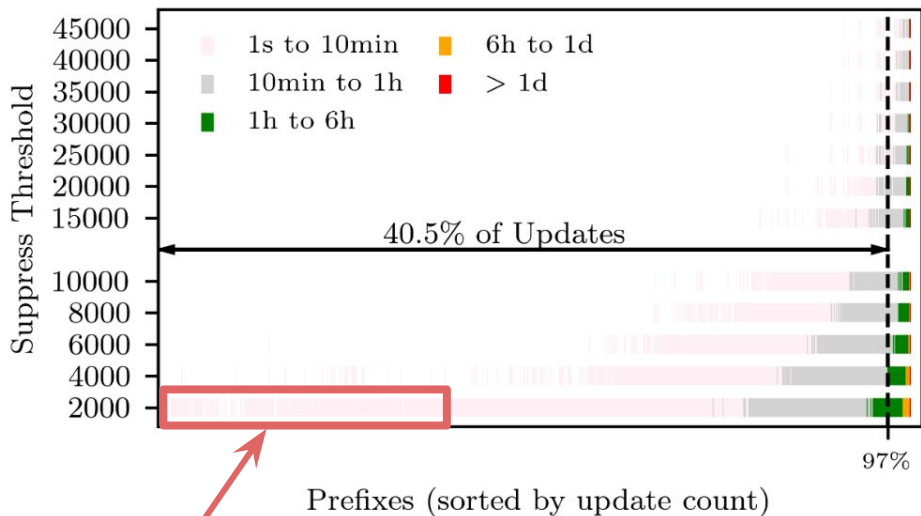
IPv4

Prefix X ranks at 80% and is suppressed between 10min to 1h during the 7 day measurement period.



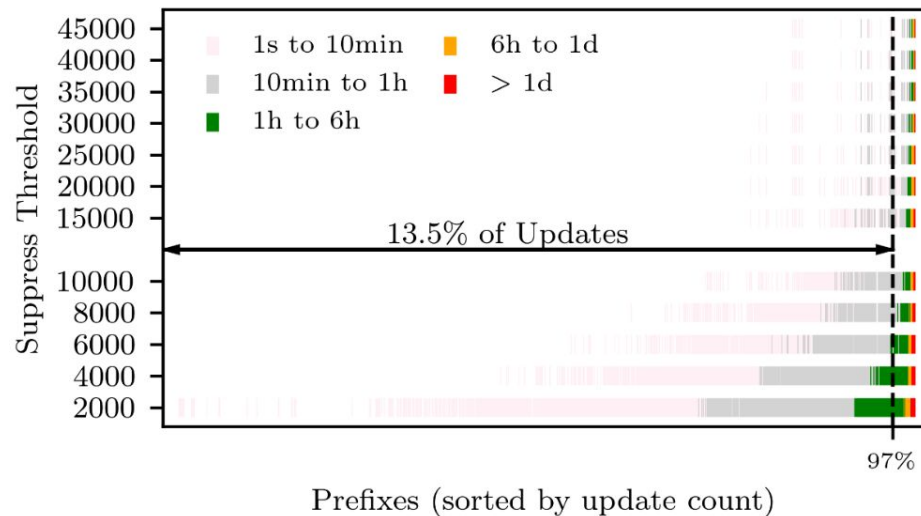
IPv6

Suppress Duration for different thresholds



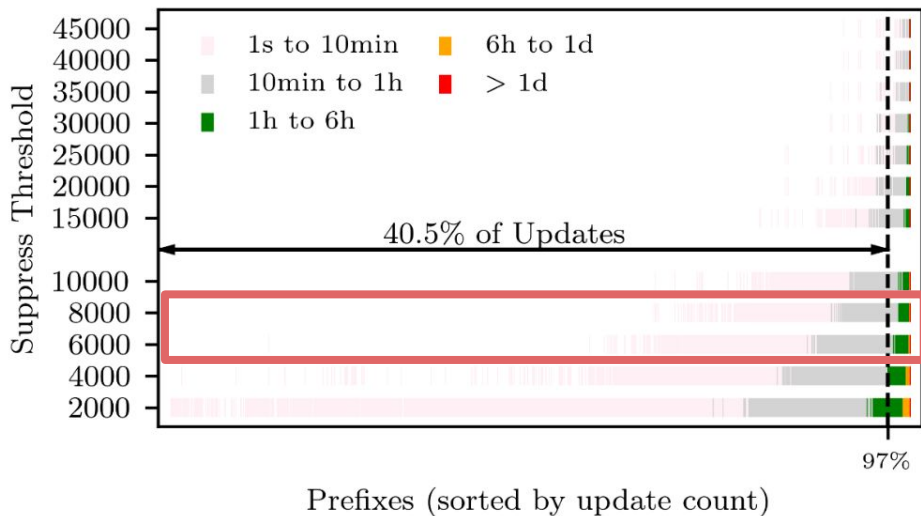
IPv4

**Even very quiet prefix
get suppressed.**

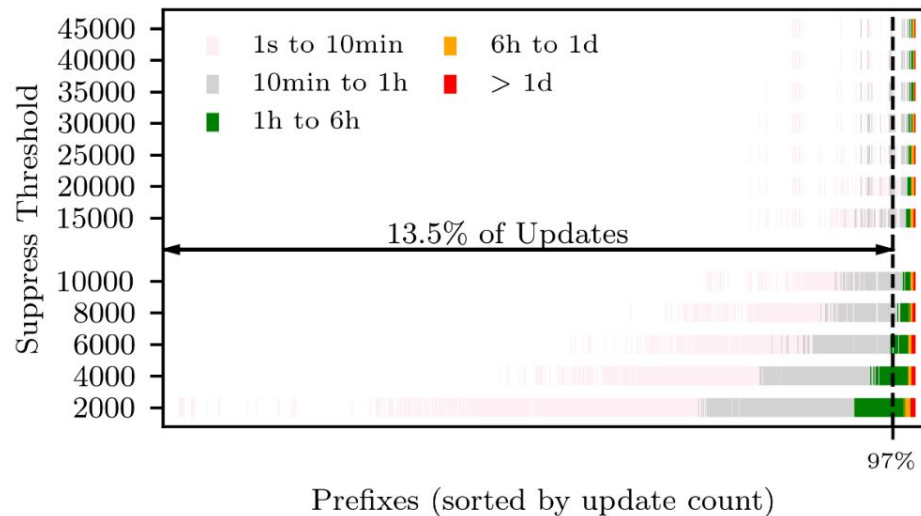


IPv6

Suppress Duration for different thresholds



IPv4



IPv6

Do we need new RFD recommendations?

Do we need new RFD recommendations?

NO.

Current recommendations are still valid

RFD parameter	Vendor Defaults		Recommendations
	Cisco	Juniper	RFC 7454
Withdrawal penalty	1000	1000	1000
Readvertisement penalty	0	1000	0/1000
Attributes change penalty	500	500	500
Suppress-threshold	2000	3000	6000
Half-life (min)	15	15	15
Reuse-threshold	750	750	750
Max suppress time (min)	60	60	60

Website (rfd.rg.net)

Revisiting Recommended BGP Route Flap Damping Configurations

Authors: Clemens Mosig, Randy Bush, Cristel Pelsser, Thomas C. Schmidt, Matthias Wählisch

In: Proc. of IEEE/IFIP Network Traffic Measurement and Analysis Conference (TMAN) 2021

Abstract: BGP Route Flap Damping (RFD) is recommended to suppress BGP churn. Current configuration recommendations for RFD, however, are based on a study from 2010. Since then, BGP churn increased by one order of magnitude, which may lead to outdated RFD parameters and introduce risks to reachability of stable networks. In this paper, we revisit current recommendations to configure RFD. First, we develop an accurate and scalable emulation of Cisco and Juniper RFD implementations and make it publicly available. Second, we successfully reproduce the 2010 measurement study that justified the current RFD recommendations using current data. Third, we consider the RFD implementation of an additional major router vendor (Juniper), which penalizes BGP churn differently compared to the previously studied Cisco implementation. Fourth, we include IPv6 data from 2020. Our results show that the recommended RFD configuration parameters from 2010, though seemingly rarely used, still hold today for IPv4 and IPv6 and across vendors, even though BGP churn increased significantly. Our study reviews metrics to assess the impact of differently configured RFD, discusses collateral damage, and gives insights into sweet spots when damping routes.

Contact: clemens.mosig@fu-berlin.de

[BibTeX](#) [Paper](#) [Articles](#) [Presentation \(video\)](#) [Presentation \(slides\)](#)

BGP Beacons, Network Tomography, and Bayesian Computation to Locate Route Flap Damping

Authors: Caitlin Gray, Clemens Mosig, Randy Bush, Cristel Pelsser, Matthew Roughan, Thomas C. Schmidt, Matthias Wählisch

In: Proc. of ACM Internet Measurement Conference (IMC) 2020

Abstract: Proprietary autonomous systems which deploy specific tracer-domain techniques such as Route Flap Damping (RFD) or Route Origin Validation (ROV) remain a challenge today. Previous approaches to detect per-AS behavior often relied on heuristic derived from passive and active measurements. Those heuristics, however, often lacked accuracy or imposed tight restrictions on the measurement methods. We introduce an algorithmic framework for network tomography (NetChisel), which implements Bayesian Computation for Autonomous Systems, using an original combination of active probing and stochastic simulation, we present the first study to expose the deployment of RFD. In contrast to the expectation of the Internet community, we find that at least 17% of measured ASes enable RFD, most using deprecated vendor default configuration parameters. To illustrate the power of computational Bayesian methods we compare NetChisel with free RFD heuristics. Thereafter, we successfully apply a generalization of the Bayesian method to a second challenge, measuring deployment of ROV.

Contact: caitlin.gray@student.adelaide.edu.au and clemens.mosig@fu-berlin.de

[BibTeX](#) [Paper](#) [Articles](#) [Articles list](#) [datahub \(top\)](#) [RFD deployment \(top\)](#) [Presentation \(video\)](#) [Presentation \(slides\)](#)



Paper

Revisiting Recommended BGP Route Flap Damping Configurations

Clemens Mosig¹, Randy Bush², Cristel Pelsser³, Thomas C. Schmidt⁴, Matthias Wählisch⁵

¹Fritz-Haber Center, ²Amazon / IU, ³Université de Strasbourg, ⁴HAW Hamburg, ⁵clemens.mosig, m.waehlich@fu-berlin.de, randy@rps.com, pelsser@unistra.fr, tcschmidt@haw-hamburg.de

Abstract—BGP Route Flap Damping (RFD) is recommended to suppress BGP churn. Current configuration recommendations for RFD, however, are based on a study from 2010. Since then, BGP churn increased by one order of magnitude, which may lead to outdated RFD parameters and introduce severe loss of reachability of stable networks. In this paper, we revisit current recommendations to configure RFD. First, we develop an accurate and scalable emulation of Cisco and Juniper RFD implementations and make it publicly available. Second, we successfully reproduce the 2010 measurement study that justified the current RFD recommendations using current data. Third, we consider the RFD implementation of an additional major router vendor (Juniper), which penalizes BGP churn differently compared to the previously studied Cisco implementation. Fourth, we include IPv6 data from 2020. Our results show that the recommended RFD configuration parameters from 2010, though seemingly rarely used, still hold today for IPv4 and IPv6 and across vendors, even though BGP churn increased significantly. Our study reviews metrics to assess the impact of differently configured RFD, discusses collateral damage, and gives insights into sweet spots when damping routes.

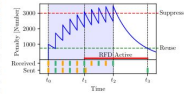


Fig. 1. RFD rate perspective. The penalty for a prefix that oscillates between advertisement (green) and withdrawal (orange). The dashed horizontal lines represent suppress and reset thresholds.

to trigger RFD. The current recommendation for the suppress-threshold [2], [3], the major knob to fine-tune RFD behavior in routers, is based on BGP data from 2010 [4], even though the Internet changed significantly during the last ten years. Those changes include more networks and higher churn in IPv4 and different BGP dynamics in IPv6.

A recent study [5] confirms RFD deployment in different types of networks, but the research and operator communities lack an up-to-date view on proper RFD configuration.

In this paper, we revisit parameter recommendations for RFD by making the following contributions:

- 1) We give an up-to-date view on BGP Churn from almost 2000 BGP vantage points.
- 2) We develop an accurate and scalable emulation of Cisco and Juniper RFD implementations and make it publicly available.
- 3) We reproduce the original study by Pelsser et al. [3] that justifies current RFD recommendations for IPv4 using a selected subset of vantage points.
- 4) We analyze IPv6, which shows a different churn signature compared to IPv4, and compare to recent data in 2020.
- 5) We incorporate an additional router vendor implementation (Juniper), which implements a different RFD behavior compared to the vendor studied in the past [4].

RIPE Labs Article

Should You Update Your Route Flap Damping Parameters?

Clemens Mosig — 16 Nov 2021
Contributors: Randy Bush, Cristel Pelsser, Thomas C. Schmidt, Matthias Wählisch

[Home](#) [Index](#) [RSS](#) [Feedback](#) [Contact](#)

BGP Route Flap Damping (RFD) is recommended to suppress BGP churn. Default RFD configurations in routers have been shown to be harmful. Current configuration recommendations by the IETF and RIPE, however, are based on a study from 2010 which focused on IPv4 only. This article presents our recent measurement study which shows that the old parameter recommendations are valid for today's Internet in both IPv4 and IPv6.

Route Flap Damping (RFD) is a mechanism to locally suppress BGP update churn on the Internet. RFD default configuration parameters in routers are too strict and cause unwanted prefix update suppression, which leads to reachability issues. In 2010, Pelsser et al. determined configuration parameters to avoid these issues.

This post presents results from a 2021 study in which my colleagues and I (from Freie Universität Berlin, IU/Arccus, Université de Strasbourg, and HAW Hamburg) reproduced and extended the study from 2010 in order to also consider IPv6 and one other router vendor (Juniper).

We found that the current recommendations - BCP 194 and ripe-380 - are still valid today and will be valid in the future if current trends continue, considering IPv4 and IPv6. We recommend network operators check their RFD configurations for harmful

Questions? Contact clemens.mosig@fu-berlin.de!