Keep your Communities Clean: Exploring the Routing Message Impact of BGP Communities

Thomas Krenc  
Naval Postgraduate School  
tkrenc@nps.edu

Robert Beverly  
Naval Postgraduate School  
rbeverly@nps.edu

Georgios Smaragdakis  
TU Berlin  
georgios@inet.tu-berlin.de

ABSTRACT

BGP communities are widely used to tag prefix aggregates in order to efficiently implement policy, traffic engineering, and inter-AS signaling. Because each individual AS defines its own community semantics, many ASes blindly propagate communities they do not recognize in routing announcements. Prior research has shown the potential security vulnerabilities possible when communities are not properly filtered. In this work, we shed light on a second unintended side-effect of communities and open propagation policies: an increase in unnecessary BGP routing messages. We examine 10 years of BGP messages observed at two route collector systems. In 2020, around 25% of all announcements update the community attribute, but not the AS path. Further 25% update neither. Using beacon prefixes, we find that communities can lead to an increase in number of update messages, at the tagging AS, but also at neighboring ASes that neither add nor filter communities — primarily geolocation communities during path exploration events: On a single day, 63% of all unique community attributes are revealed exclusively due to global withdrawals. While it is well-recognized that intra-AS next-hop or MED changes can cause spurious updates, we show in controlled laboratory experiments that they can be due to communities only, and transitively through the AS path. We show that different router implementations contribute to this behavior - per default - violating BGP specifications.

1 INTRODUCTION

Border Gateway Protocol (BGP), the Internet’s inter-domain routing protocol, is fundamental to the operation, policies, and economics of the network. Unsurprisingly, the real-world behavior of BGP has been subject to intense research scrutiny [13, 23, 27]. As an extensible protocol, BGP and its usage have evolved in response to network policies, and beholden to BGP implementation behaviors. The BGP decision process is complicated, in- volving iBGP, eBGP and IGP interaction, is governed by individual AS paths and communities in billions of update messages at 500+ peers over 10 years. We find that updates with no path change are common throughout the entire measurement period and are rooted in widespread community deployment, increasingly interconnected networks, and lack of community filtering. More specifically, we find:

(1) Around 50% of announcements in March 2020 signal no path change, while half of them show a change in communities.
(2) In laboratory experiments and in the wild, we show that community geo-tagging in combination with missing or ineffective cleaning can lead to an increase of update messages.
(3) We find that while all tested routers, i.e., Cisco IOS, Junos OS, and BIRD generate updates without AS path change by default, Junos OS at least prevents duplicates.
(4) By utilizing beacon prefixes we show that more than 60% of all encoded information in community attributes is revealed during global withdrawals, as a result of path exploration.

Our findings afford a better understanding of routing instabilities in the Internet, and may help foster detection of anomalous communities in the future. We provide a discussion on the implications of our findings and suggest future work.

2 BACKGROUND AND RELATED WORK

In this section, we provide details of BGP relevant to understanding our work on communities, as well as a summary of prior relevant research. We assume working familiarity with BGP; see [27] for a broad overview.

Path Exploration: The BGP decision process is complicated, involving iBGP, eBGP and IGP interaction, is governed by individual network policies, and beholden to BGP implementation behaviors. There is a basic tension between propagating reachability information quickly and sending it before the AS has converged on a new best state. Thus, updates often occur in bursts.

Several prior works analyze network stability, path exploration, and the tradeoff in withholding updates. Mechanisms such as route dampening and MRAI timers [3] have been explored, but may offer suboptimal performance in reacting to routing events [32].
Thus, these mechanisms are selectively deployed. Indeed, we show that path exploration, combined with BGP community use, is a significant contributor to BGP update traffic.

**Duplicate Updates**: As with the protocol itself, BGP update behavior has been extensively studied, for instance to understand routing dynamics [18], understand convergence and forwarding behavior [20], quantify path performance [33], and locate origins of instabilities [6]. Of most relevance to our present study are so-called “duplicate” BGP updates, superfluous messages that do not update routing state, first identified by Labovitz in 1998 [16]. Originally believed to be due to buggy implementations, Park et al. subsequently demonstrated that I/BGP/eBGP interaction was the primary cause of these duplicates [22]. As we also find, when a router receives an internal update with a changed attribute, that attribute may be removed prior to the induced message to an eBGP peer. Hauweele et al. later demonstrated in both real and lab experiments that MED and next-hop attribute changes induce these duplicates [14].

While duplicate updates have been a recognized issue for decades, we first show via controlled lab experiments in §3 the propagation and update implications of adding communities to BGP announcements. Second, our work highlights the effects of increased BGP community use on duplicates. We show that BGP geolocation communities are a primary source of unnecessary updates, and induce inter-AS message traffic even when communities are filtered.

**Communities**: BGP messages are relatively simple and include prefix updates (often termed an “announcement”) as well as prefix withdrawals (indicating that the prefix should be removed from the routing table). In addition, BGP messages can include multiple optional attributes, among them the next-hop, MED, and community. Among these, BGP communities are notable because they are transitive – meaning that they are an optional attribute that must be propagated. Thus, communities are focus of our study. As we will show, not only are BGP communities in common use, but they are a primary contributor to overall BGP message traffic.

Benoit et al. provides a taxonomy of BGP communities in [5]. As a contemporary convention, BGP communities can be broadly divided into informational communities and action communities [29]. Informational communities are typically added to ingress routing announcements to tag aggregates of routes in a common way in order for an AS to make internal policy and routing decisions. For instance, a common informational community used by large ASes is to encode the physical geolocation, e.g. “North America, Dallas, TX”, where a prefix is received.

In contrast, action communities are frequently added to egress routing announcements in order to implement in-band signaling to the next AS. For instance, a common use of action communities is the blackhole community which indicates that a provider should stanch traffic for a particular IP or prefix that is experiencing a DoS attack.

With the growth in BGP community adoption, researchers have in recent years explored community prevalence and security [5, 30], as well as the information they leak about connectivity, attacks, and outages [7, 9]. However, less attention has been given to the unintended impacts of communities on the volume of BGP message traffic in general, and updates in particular – these are the focus of the present research.

![Figure 1: Laboratory topology to understand conditions generating BGP update messages](image-url)

### 3 Controlled Experiments

To validate our findings and inferences, as well as to afford a deeper understanding of the root causes of the BGP update phenomenon we observe in the wild, we conduct a series of experiments in a controlled laboratory setting.

For each run of the experiments, we configure all routers that are depicted in Figure 1 to use one of the following routing software: Cisco IOS (12.4(20)T and XR 6.0.1), Juniper Junos OS (Olive 12.1R1.9), as well as the BIRD routing daemon (v1.6.6 and v2.0.7). By using real router images, we can gain insight into real-world BGP implementation behavior. Because we find identical behaviors for most of the experiments, we report only on the common behavior and where it deviates.

The lab topology is crafted to test several scenarios, with and without communities, to understand the conditions that generate BGP update messages and when those update messages are propagated. The topology consists of four autonomous systems: X, Y, Z and C. Router C1 mimics a route collector, while Z1 originates the prefix p. The links in the topology correspond to both physical connections and eBGP and iBGP sessions. AS Y has three routers within its network; both Y2 and Y3 peer with AS Z.

Prior to running our experiments, we verify that only BGP keepalive messages are sent once the network has converged. We are interested only in BGP update and withdrawal messages in this work; keepalives are pairwise heartbeat messages to test liveness.

**Exp1**: We begin without any BGP communities to characterize default behavior. Note that border router Y1 has two paths to reach p. In the absence of any policy, the BGP tie breaker selects Y1 as the next hop. Therefore, to induce BGP updates, we disable the Y1 to Y2 link, and perform a packet capture of all messages arriving at the collector C1 and between Y1 and Y3.

Without BGP communities, when Y1 chooses a new next hop of Y3, it sends an update message to X1 even though the AS path has not changed (Note: Junos does not generate duplicates). However, this update message does not propagate further – no update message is observed at the collector.

**Exp2**: Next, we consider the common scenario where AS Y implements communities that geographically tag incoming advertisements. Y2 adds community Y: 300 on ingress while Y1 adds Y: 400. Because Y2 is preferred, and no community filtering is implemented in this network, the collector sees p with Y: 300. We again disable the Y1 to Y2 link.

Again, this induces an update message from Y1 to X1. While the AS path is unchanged, this update includes a changed community...
value of $Y: 400$. Because the community value changed, $X_1$ also sends an update which is seen at the collector. Note that while updates sent by $Y_1$ can be due to an internal next-hop change (as in Exp1), in the case of $X_1$ the next-hop does not change. Thus, a change in the community attribute can be the sole trigger for an update.

**Exp3:** We implement community filtering on $X_1$ by configuring it to remove all communities on egress. We again flap the $Y_1$ to $Y_2$ link to generate the update message. Surprisingly, even though $X_1$ is removing communities, it still sends an update to the collector (Again, Junos does not generate duplicates). Note that this update has an unchanged AS path and includes no communities – i.e. it is an arguably unnecessary message.

**Exp4:** We then repeat experiment 3, but modify $X_2$ to filter communities on ingress from $Y_1$. In this case, the spurious update message is not sent as the communities are not contained in the router’s RIB. This shows that we can differentiate between ingress and egress community cleaning.

**Summary:** From the tested routing software, by default, only Junos prevents duplicates from being generated by, e.g., internal changes or community filtering on egress. We note that sending updates with no changes contradicts BGP specifications. Furthermore, all routers generate updates that are triggered only due a change in the community attribute, if communities are not filtered at ingress. Our findings imply that this behavior is transitive.

### 4 DATA SETS

To study the impact of BGP communities on update message propagation, we use publicly available archived routing traffic from RouteViews [28] and RIPE RIS [26] collectors. We obtain all updates, inclusive of both IPv4 and IPv6 prefixes, for a full day every 3 months (2019-03-15, 2019-06-15, 2019-09-15, etc.) across a ten-year span (2010 to 2020).

Prior to analyzing our update message data, we first perform basic filtering, cleaning, and normalization. Using current and historical allocation information from the regional registries, we remove BGP messages that contain an unallocated ASN or prefix at the time of the message. We did not aggregate overlapping prefixes, and we keep prefixes with length smaller than /24. Next, we note that many of the route collector peers are IXP route servers, some of which do not include their own ASN in the announcements. To avoid overcounting peer ASes and avoid ambiguity when processing the data, we add the ASN of the route server to the AS path. Finally, some BGP collectors only record messages at the single second granularity. When multiple messages arrive in the same second for these collectors, we preserve the message ordering and assume that each subsequent message arrives 0.01ms after the last. In the remainder of this paper, we refer to the resulting data set as $d_{hist}$. We use $d_{mar20}$ to point to the most recent data in our measurements, which is March 15, 2020. Table 1 provides an overview of $d_{mar20}$. There are approximately 1.5k sessions across nearly 600 unique AS peers. The number of BGP sessions at these two collector projects has roughly doubled over this time.

**Routing Beacons:** Routing beacons are prefixes with the only purpose to announce and withdraw particular routes at periodic intervals. This can help network operators and researchers investigate the behavior of the routing system as well as anomalies. RIPE operates such routing beacons [25] with an update pattern of a single announcement every 4 hours, starting at 00:00 UTC, and a single withdrawal every 4 hours, starting at 02:00 UTC. One specific beacon prefix is announced per route collector.

From $d_{hist}$, we select all updates that contain one of 15 selected beacon prefixes in March 15, 2020. We observe 307,984 announcements and 56,640 withdrawals spread over all sessions (577), peers (340), and collectors (34) in $d_{beacon}$. We refer to this subset as $d_{beacon}$.

### 5 ANNOUNCEMENT TYPES

To better understand those announcements, we first group them by the prefix and the BGP session of a peer AS / next-hop, in arriving order. Then, we look for changes in the AS path, AS path prepending, and the community attribute from one announcement to the next. Since these attributes can change independently of each other, we define six different combinations of two letters to label the announcement type. The first letter indicates a path change and the second letter indicates a change in the community attribute: $pc$, $pn$, $nc$, $nn$, $x$, $xn$.

An announcement with a path change only is in the category $pc$. If the path change is only due to path prepending (the set of ASes are equal), it is in $xn$. In, in addition to the AS path also the community attribute deviates, the announcement is in $pc$ (or $xc$ in case of path prepending). While we intuitively expect $pn$, $pc$, $x$, $xn$ updates, we also see updates without a path change: $nc$ and $nn$ cover all announcements with no path change, while the former also includes changes in the community attribute. We note that $nn$ and $nc$ – the only types that do not include

---

**Table 1: Overview $d_{mar20}$**

| IPv4 prefixes | IPv6 prefixes | Announcements w/ communities | unic. 16 bits | unic. AS paths | Withdrawals |
|---------------|---------------|-----------------------------|---------------|---------------|-------------|
| 1,071,150     | 99,141        | 1,008M                      | 737.0M        | 5,778         | 38.5M       |

**Table 2: Announcement types overview (share in $d_{mar20}$ and $d_{beacon}$)**

| type     | observed changes | $d_{mar20}$ | $d_{beacon}$ |
|----------|------------------|-------------|--------------|
| $pc$     | path + community | 33.7%       | 44.6%        |
| $pn$     | path only        | 15.1%       | 29.9%        |
| $nc$     | community only   | 24.5%       | 13.8%        |
| $nn$     | no change        | 25.7%       | 11.2%        |
| $xc$     | path prepending + comm. | 0.3%   | 0.2%        |
| $xn$     | path prepending only | 0.7%   | 0.3%        |
a path change - make up more than half of all announcements (24.5% and 25.7% respectively). The largest group of announcements is of type $pc$ with a share of 33.7%, while $pn$ announcements constitute 15.1%. Interestingly, the number of announcements with path prepending is negligibly small, contributing around 1%. For comparison, we also provide the share of types in $d_{\text{beacon}}$. Here, we see a different distribution. While $nc$ and $nn$ together contribute 25% to all announcements, $pc$ is the most dominant type with a share of 44.6%, followed by $pn$ with 29.9% share. Again, $xn$ and $xc$ are low in numbers. We remind that beacon prefixes provide us with a more controlled view on the update behavior since they are announced and withdrawn at stated intervals. In the wild, however, unpredictable changes at the origin AS can add to the dynamics of update propagation at all downstream paths.

Next, we investigate the longitudinal behavior of announcement types. In Figure 2, we highlight the evolution of the individual constituents. While in the first 5 years, the ratios of types are comparable, in the second 5 years the numbers drift apart. Most notable are the types $pc$ and $nn$. Not only are they historically the most dominant of all types, they are also responsible for the high variations of announcements over time. Although not as dynamically evolving, the number of $nc$ and $pn$ announcements is constantly high. We note that despite increased community usage, the share of all types is relatively stable. We can also confirm a similar stability on a daily basis.

6 UNNECESSARY UPDATES

Next, we study communities in announcements with no path change and their impact on update propagation. We focus on announcements for individual beacon prefixes ($d_{\text{beacon}}$) visible in BGP sessions over 24 hours.

**BGP Sessions.** We begin by investigating how each peer AS perceives announcement types, i.e., $pc$, $pn$, $nc$, $nn$, $xc$, and $xn$. The stacked bar plot in Figure 3 shows all the BGP sessions that are visible in collector rrc00. They are sorted by number of announcements visible for prefix 84.205.64.0/24 $\in d_{\text{beacon}}$. Further, the colors indicate the announcement type, see legend. We observe that each session shows a different number of announcements. But more interesting is the fact that each session shows a diverse distribution of announcements types, despite looking only at a single beacon prefix. To this end, the root causes, i.e., why $nc$ and $nn$ announcements are sent in the first place, remain unclear. Thus, in the following we take a close look at those announcement types.

**Community Exploration.** In order to study the root causes for $nc$ announcements, we consider a single BGP session. In Figure 4 we plot the cumulative sum of announcements over 24 hours of March 15, 2020. We plot all announcements for the same prefix 84.205.64.0/24 $\in d_{\text{beacon}}$ via a single AS path (28205 3356 174 12654). Vertical yellow lines indicate the arrival of a withdrawal message for that prefix, confirming the withdrawal interval for routing beacons.

All announcements for this particular route and day show up only during the withdrawal phases, i.e., at around 02:00, 06:00, 10:00, etc. We deduce that this particular route was never a best path during that day (all time best path: 28205 6939 50304 12654). During the withdrawal events we observe a total of 19 announcements: Starting with a $pc$ update (6 total), i.e., an announcement with changed path and community, followed by multiple (13 total) $nc$’s, announcements with changing community only. A quick look at the data shows that the peer AS20205 does not set any communities. However, it does not clean communities from its neighbor either: The changing communities in $nc$ announcements represent encoded ingress locations set presumably by AS3356. We observe a total of 9 locations encoded in 19 announcements: 9 city communities, two country and two geographical regions, i.e., Europe and North America. Per withdrawal phase, the location communities are mostly unique.

Due to distinct location communities attached to a single route, multiple $nc$ announcements occur (comparable to Exp2 in §3). Analogously to path exploration, we refer to this behavior as community exploration. Instead of multiple paths being announced, multiple...
communities for a single path are announced. Also, the example demonstrates that setting communities by one AS, can impact the update behavior of a different AS, if no proper filtering is in place (comparable to Exp4).

**Duplicate Announcements.** Next, we explore a possible reason for the occurrence of nn updates. Therefore, we choose a route similar to the previous community exploration example. However, we replace the peer AS with one that removes all communities (in >99% of the cases). Figure 5 shows the cumulative sum of announcements over the day of March 15, 2020. We plot announcements for the same prefix (84.205.64.0/24), but via a different AS path (20811 3356 174 12654). Vertical yellow lines represent withdrawal messages for that prefix, again in accordance with the predefined intervals. Again, all 31 announcements occur during the withdrawal events. Also, the phases begin with a path change (6 total), here pn, followed by a series of nn announcements (25 total).

Deduced from our previous observations, we speculate that during the withdrawal phase AS 20811 simply reannounces multiple nc’s from 3356 (as a implicit withdrawal) and remove the existing communities prior to announcing, thus inducing nn announcements. Note, we have demonstrated the possibility for such a behavior in the lab experiments (Exp3). Also, we manually re-visit the raw BGP data and confirm that no attribute, e.g., the MED, has changed and no other prefix is included in the updates towards the collector. Since our observations are limited to inter-AS changes, we do not exclude the possibility for other reasons we observe nn announcements, e.g., streams of updates due to intra-AS changes, misconfiguration, or rate limiting.

**Revealed Information.** We have shown that geo-tagging can lead to bursts of announcements just updating the community attribute, which can lead to re-announcements by neighboring ASes, in a lab experiment and in the wild.

Next, we investigate the amount of information that is revealed as a result of community exploration. Therefore, we utilize the fixed announcement and withdrawal phases of the beacon prefixes. We label all announcements \( a_{\text{beacon}} \) according to their appearances in any of the predefined phases, or outside them. We consider all announcements that appear withing 15 minutes of the respective phase begins, e.g., between 2:00 to 2:15 UTC for the first withdrawal phase.

In March 15, 2020, we identify a total of 21398 unique community attributes. 62% of all community attributes are revealed exclusively during the withdrawal phases. Only 17% are revealed during the announcement phases and <1% outside both phases. The remaining attributes show up ambiguously. Historically, this distribution is stable, as can be seen in Figure 6. While the number of unique community attributes per day during withdrawal phases increased multifold in the last ten years, so did the total number, resulting in a stable ratio of about 60%.

7 DISCUSSION

As the Internet’s core interdomain routing protocol, the BGP has been extensively studied. While previous work has found duplicate updates in the wild [16] and identified potential causes [14, 22], we show that BGP communities play a large role in the generation of unnecessary updates. First, as a transitive property of BGP messages, communities can induce updates to propagate through the entire routing system even when the path information is unchanged, the routing decision algorithm is unaffected, and the receiving AS does not recognize the community. Second, even when communities are filtered by an intermediate AS, common implementations still generate a duplicate update, just without the community. While duplicate updates without communities do not continue to propagate, we show that they represent a sizable fraction of BGP messages seen at route collectors and are unnecessary traffic.

Prior work has shown that the lack of filtering and widespread propagation of BGP communities can leak information about networks’ operation and practices [7, 9] and peering [8, 10], and can even be exploited to attack the routing system [30]. Our findings in this work demonstrate an additional motivation for more rigorous community filtering: reducing unnecessary duplicate update traffic. Not only does the unnecessary traffic impact router load and convergence times [1], it increases the load and storage requirements of systems that monitor BGP traffic including route collectors.

Further, as the global use of communities increases and ASes become increasingly interconnected, the impact of that filtering will place even more strain on the system. As such, our primary recommendation in this work is to add yet another motivation for operators to properly filter BGP communities.

However, we note several other implications of our findings that we plan to study in future work. First, communities are somewhat paradoxical to BGP’s emphasis on scalability and information hiding. For instance, the updates we observe often allow us to remotely infer the number of interconnections between two ASes and the...
location where they peer. Second, from observing updates and lack of updates at multiple points in the network, we can make rough guesses as to the way different ASes handle communities. Using more sophisticated network tomography techniques, we plan to classify per-AS community behavior, for instance those that tag, filter, and ignore. In future work we will use this information to estimate the impact of unnecessary communities per-AS. Finally, we believe that communities can enrich our understanding of anomalous behavior in the routing system beyond existing approaches. By characterizing the way individual ASes observe and process communities, our work provides a first step toward predicting anomalous communities.

REFERENCES

[1] Sharad Agarwal, Chen-Nee Chua, Supratik Bhattacharyya, and Christophe Diot. 2004. Impact of BGP dynamics on router CPU utilization. In International Workshop on Passive and Active Network Measurement. Springer, 278–288.

[2] CISCO 2005. Remotely Triggered Black Hole Filtering - Destination Based and Source Based. Cisco White Paper. http://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf.

[3] Shivani Deshpande and Biplob Sibarat 2004. On the impact of route processing on BGP convergence times. In IEEE Global Telecommunications Conference. 2004. GLOBECOM’04, Vol. 2. IEEE, 1147–1151.

[4] C. Dietzel, A. Feldmann, and T. King. 2016. Blackholing at IXPs: On the Effectiveness of DDoS Mitigation in the Wild.

[5] Benoit Donnet and Olivier Bonaventure. 2008. On BGP Communities. SIGCOMM Comput. Commun. Rev. 38, 2 (March 2008), 55–59. https://doi.org/10.1145/1355734.1355743

[6] Anja Feldmann, Olaf Maennel, Z. Morley Man, Arthur Berger, and Bruce Maggs. 2004. Locating Internet Routing Instabilities. In Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (Portland, Oregon, USA) (SIGCOMM ’04). Association for Computing Machinery, New York, NY, USA, 205–218. https://doi.org/10.1145/1015491.

[7] V. Giotsas, C. Dietzel, G. Smaragdakis, A. Feldmann, A. Berger, and E. Aben. 2017. Detecting Peering Infrastructure Outages in the Wild. In ACM SIGCOMM.

[8] V. Giotsas, M. Luckie, B. Huffaker, and kc claffy. 2014. Inferring Complex AS Relationships. In ACM IMC.

[9] V. Giotsas, G. Smaragdakis, C. Dietzel, P. Richter, A. Feldmann, and A. Berger. 2017. Inferring BGP Blackholing Activity in the Internet. In ACM IMC.

[10] V. Giotsas, G. Smaragdakis, B. Huffaker, M. Luckie, and k. claffy. 2015. Mapping Peering Interconnections at the Facility Level. In ACM CoNEXT.

[11] V. Giotsas and S. Zhou. 2013. Improving the Discovery of IXP Peering Links through Passive BGP Measurements.

[12] V. Giotsas, S. Zhou, M. Luckie, and kc claffy. 2013. Inferring Multilateral Peering. In ACM CoNEXT.

[13] Timothy G Griffin and Gordon Wilfong. 1999. An analysis of BGP convergence properties. ACM SIGCOMM Computer Communication Review 29, 4 (1999), 277–288.

[14] David Hauweele, Bruno Quoitin, Cristel Pelsser, Georgios Smaragdakis, and Randy Bush. 2018. BGP Communities: Even More Worms in the Routing Can. In ACM IMC.

[15] Florian Streibelt, Franziska Lichtblau, Robert Beverley, Anja Feldmann, Cristel Pelser, Georgios Smaragdakis, and Randy Bush. 2018. BGP Communities: Even More Worms in the Routing Can. In Proceedings of the Internet Measurement Conference 2018 (Boston, MA, USA) (IMC ’18). Association for Computing Machinery, New York, NY, USA, 279–292. https://doi.org/10.1145/3278532.3278557.

[16] Feng Wang, Zhuoqing Morley Mao, Jia Wang, Lixin Gao, and Randy Bush. 2006. A measurement study on the impact of routing events on end-to-end internet path performance. ACM SIGCOMM Computer Communication Review 36, 4 (2006), 375–386.

[17] Feng Wang, Zhuoqing Morley Mao, Jia Wang, Lixin Gao, and Randy Bush. 2006. A Measurement Study on the Impact of Routing Events on End-to-End Internet Path Performance. In Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (Pisa, Italy) (SIGCOMM ’06). Association for Computing Machinery, New York, NY, USA, 375–386. https://doi.org/10.1145/1159913.1159956.