The Next Generation of BGP Data Collection Platforms

Thomas Holterbach University of Strasbourg

RIPE 90 May 15, 2025 Lisbon

Joint work with: Thomas Alfroy Cristel Pelsser



The BGP data collected by platforms like <u>RIS</u>, <u>RouteViews</u> and <u>PCH</u> is essential for understanding and monitoring Internet routing

anangements between ASes.					
AS Rank 🔺	AS Number v	Organization		cone size (ASes) ⊽	
1	3356	Level 3 Parent, LLC		53982	
2	1299	Arelion Sweden AB		41919	
3	174 Cogent Communications			37559	
4	3257	GTT Communications Inc.		36334	
5	2914	NTT America, Inc.		26976	
6	6 6939 Hurricane Electric LLC			21697	
7	6762	Telecom Italia S.p.A.		20271	
8	6453	TATA COMMUNICATIONS (AMERICA) INC		19334	
9	6461	Zayo Bandwidth		18116	
10	3491	PCCW Global, Inc.		11530	

CAIDA's AS rank



Catchpoint's BGP map



BGPlay

Routers that share their BGP routes are like satellites observing the Earth's surface

Each router (or "vantage point") provides a partial view

But together they allow monitoring at larger scale



bgproutes.i

Our new next-gen BGP route collection platform





bgproutes.i

Our new next-gen BGP route collection platform We just launched our new website!







Our new next-gen BGP route collection platform

Collection: High coverage



Distribution: Fast API with high granularity







% of ASes sharing their BGP data (RIS+RouteViews)



8

% of ASes sharing their BGP data (RIS+RouteViews)



And it is unlikely to improve anytime soon: RIS and RouteViews have recently adopted a selective a peering policy



RouteViews Peering Policy



sted by RouteViews Peering Coordinato Nina Bargisen

Most of us will know that the Internet, true to its name, is a network of networks. Each network, whether a local ISP or a global content provider, must connect with others to enable the worldwide flow of data we know as the Internet. We have two ways to interconnect: transit, where one network pays another for connectivity to the rest of the Internet, and peering, where networks agree to exchange traffic directly.

Peering Policies

As a network operator, your willingness to peer is stated in your peering policy. There are three types of policies:

- 1. Open the network peers with everyone,
- 2. Selective the network has defined a set of rules that describes who they peer with and how,
- 3. Restrictive these networks have very little interest in expanding their peering.







But is a 1.2% coverage really bad?



It is hard to know without ground truth But it likely depends on the use case

But is a 1.2% coverage really bad?



<u>Use case #1: Peer-to-peer link observation</u>

Use case #2: Forged-origin hijack detection



Use case #1: Peer-to-peer link observation We miss 84% of the links

Use case #2: Forged-origin hijack detection



Use case #1: Peer-to-peer link observation We miss 84% of the links

Use case #2: Forged-origin hijack detection We miss 24% of the Type-1 hijacks



<u>Use case #1: Peer-to-peer link observation</u> We miss 84% of the links

Use case #2: Forged-origin hijack detection We miss 24% of the Type-1 hijacks

For more details and use cases see our SIGCOMM'24 paper





Our new next-gen BGP route collection platform

<u>Collection:</u> High coverage



Distribution: Fast API with high granularity



https://bgproutes.io



bgproutes.i

Our new next-gen BGP route collection platform

<u>Collection:</u> High coverage \checkmark Storage: Low data management cost

Distribution: Fast API with high granularity



https://bgproutes.io



bgproutes.io simplifies, automates and opens BGP data contribution to every ASN

Network operators can authenticate using peeringDB

Network operators just have to fill a form to start peering with bgproutes.io

	Step #1: Submit your connection details
Selec	t the VM with whom you want to connect.
185.	216.75.11 (USA) ~
i	We recommend selecting the VM with the lowest latency to your router for more accuratimestamps.
Tell u	s with which IP address we should start peering.
Your	IP address (v4 or v6)
Tell u: 220 Our A	s with which AS number we should start peering. 0 ~ S number is 65000.
Tell u: 220 Our A i	s with which AS number we should start peering. 0 ~ S number is 65000. We will soon make iBGP sessions possible. They will be recommended as updates with the NO_EXPORT community will still be forwarded to our platform through iBGP.
Tell u: 220 Our A (i) Sub	s with which AS number we should start peering. 0 ~ S number is 65000. We will soon make iBGP sessions possible. They will be recommended as updates with NO_EXPORT community will still be forwarded to our platform through iBGP.

bgproutes.io/contribute



Our goal is not to compete against existing platforms Each existing platform has its strengths and weaknesses



5	RouteViews	PCH	CGTF RIS
			?
			?

Our goal is not to compete against existing platforms Each existing platform has its strengths and weaknesses



5	RouteViews	PCH	CGTF RIS
			?
			?

Our goal is not to compete against existing platforms Each existing platform has its strengths and weaknesses



5	RouteViews	PCH	CGTF RIS	bgproutes
			?	
			?	
				?



bgproutes.io embraces all existing platforms by centralizing their data in one unified repository

bgproutes.io already stores data for more than 5000 vantage points

Data providers				
Name	Number of vantage points			
bgroutes.io	v4: 32 v6: 2			
RIPE RIS	v4: 833 v6: 686			
RouteViews	v4: 735 v6: 695			
PCH	v4: 2129 v6: 390			
CGTF RIS Soon	v4: 0 v6: 0			

bgproutes.io/vantage_points



bgproutes.i

Our new next-gen BGP route collection platform

Collection: High coverage



Distribution: Fast API with high granularity



https://bgproutes.io



bgproutes.io lowers data management costs thanks to new BGP compression algorithms

Lossless compression e.g., for recent data



Lossy compression e.g., for old data

The Next Generation of BGP Data Collection Platforms

`omas Alfroy*, Thomas Holterbach*, Krenc[†], KC Claffy[†], Cristel Pelsser*[‡] sbourg, [†]CAIDA/UC San Diego, [‡]UCLouvain

The

active .

peers, RL

bgproutes.io

ABSTRACT

BGP data collection platforms as cu damental challenges that threaten the. Inspired by recent work, we analyze, p. new optimization paradigm for BGP collect. data collection with two components: analya tween BGP updates and using it to optimize same ing streams of BGP data. An appropriate definition. across updates depends on the analysis objective. Our include: a survey, measurements, and simulations to d the limitations of current systems; a general framework . rithms to assess and remove redundancy in BGP observation. quantitative analysis of the benefit of our approach in terms of a racy and coverage for several canonical BGP routing analyses su∖ as hijack detection and topology mapping. Finally, we implement and deploy a new BGP peering collection system that automates peering expansion using our redundancy analytics, which provides a path forward for more thorough evaluation of this approach.

CCS CONCEPTS

 $\bullet \, \mathbf{Networks} \rightarrow \mathbf{Network} \, \mathbf{measurement}.$

KEYWORDS

Internet measurement, BGP, Routing Security

ACM Reference Format:

Thomas Alfroy, Thomas Holterbach, Thomas Krenc, KC Claffy, Cristel Pelsser. 2024. The Next Generation of BGP Data Collection Platforms. In ACM SIGCOMM 2024 Conference (ACM SIGCOMM '24), August 4–8, 2024, Sydney, NSW, Australia. ACM, New York, NY, USA, 19 pages. https: //doi.org/10.1145/3651890.3672251

1 INTRODUCTION

The study of the global Internet infrastructure relies on BGP data collection platforms (RouteViews [61] and RIPE RIS [49]) that maintain BGP peering sessions with network operators who volunteer to share (sometimes portions of) their routing tables. Originally

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the established decades ago to support operational troubleshooting ("How do others reach my network?"), these systems have become a cornerstone for scientific and operational analysis of the Internet. Collecting this data faces a fundamental cost-benefit trade-off. information-hiding character of BGP requires collecting routes 's many BGP routers, *a.k.a* Vantage Points (VPs), as possible. 'actice the BGP protocol extensively propagates connectiv-'es, leading to highly redundant (along with significant coming from each peer. The result is a data set with 'ndancy and yet dangerous visibility gaps [34].

policies to store a snapshot of the aggregated vrs, as well as every BGP update received in 'vots, exacerbates the storage of redundant of the Internet (≈ 75k ASes [14] and ≈ 1M 's) and increasing connectivity between collection and use [1, 28]. Users often 's, using only a sample of the VPs, vely visible to other VPs. Finally, 'vo strains platform scalability. only ≈1% of the observably c. Despite continued addition of an terms of fraction of ASes they are a flat for two decades.

peering wit. A flat for two decades. These grove a ssures coincide with regulatory concerns about slow progests in deployment of routing security protections [62]. The ensuing public debate has highlighted the importance of these platforms for detecting both accidental and malicious transgressions in the routing system. While significant investment in data collection could accommodate gathering, retention, and sharing orders of magnitude more routing data, current constraints motivate us to consider a more strategic approach. We propose a data collection scheme that scales at least an order of magnitude in the number of VPs feeding public collection systems while limiting the increase in human effort and data volume.

Vision. We explore a fundamentally new way to collect BGP data: an overshoot-and-discard strategy. Akin to CERN's Large Hadron Collider (LHC) which generates millions of collisions just to see a few interesting particles (e.g., Higgs boson), overshooting BGP data collection will maximize the chance to see interesting routing events, e.g., BGP hijacks. We imagine a world where public BGP data providers could automate deployment of a division LMD.

bgproutes.io lowers data management costs thanks to new BGP compression algorithms

Lossless compression e.g., for recent data



Lossy compression e.g., for old data

The Next Generation of BGP Data Collection Platforms

`omas Alfroy*, Thomas Holterbach*, Krenc[†], KC Claffy[†], Cristel Pelsser*[‡] sbourg, [†]CAIDA/UC San Diego, [‡]UCLouvain

The

active .

peers, RL

bgproutes.io

ABSTRACT

BGP data collection platforms as cu damental challenges that threaten the. Inspired by recent work, we analyze, p. new optimization paradigm for BGP collect. data collection with two components: analya tween BGP updates and using it to optimize same ing streams of BGP data. An appropriate definition. across updates depends on the analysis objective. Our include: a survey, measurements, and simulations to d the limitations of current systems; a general framework . rithms to assess and remove redundancy in BGP observation. quantitative analysis of the benefit of our approach in terms of a racy and coverage for several canonical BGP routing analyses su∖ as hijack detection and topology mapping. Finally, we implement and deploy a new BGP peering collection system that automates peering expansion using our redundancy analytics, which provides a path forward for more thorough evaluation of this approach.

CCS CONCEPTS

 $\bullet \, \mathbf{Networks} \rightarrow \mathbf{Network} \, \mathbf{measurement}.$

KEYWORDS

Internet measurement, BGP, Routing Security

ACM Reference Format:

Thomas Alfroy, Thomas Holterbach, Thomas Krenc, KC Claffy, Cristel Pelsser. 2024. The Next Generation of BGP Data Collection Platforms. In ACM SIGCOMM 2024 Conference (ACM SIGCOMM '24), August 4–8, 2024 Sudney NSW Australia ACM New York, NY USA 19 pages https:// established decades ago to support operational troubleshooting (*How do others reach my network?*), these systems have become a cornerstone for scientific and operational analysis of the Internet. Collecting this data faces a fundamental cost-benefit trade-off. information-hiding character of BGP requires collecting routes `s many BGP routers, *a.k.a* Vantage Points (VPs), as possible. `actice the BGP protocol extensively propagates connectiv-`es, leading to highly redundant (along with significant coming from each peer. The result is a data set with `vdancy and yet dangerous visibility gaps [34].

policies to store a snapshot of the aggregated vrs, as well as every BGP update received in `ots, exacerbates the storage of redundant of the Internet (≈ 75k ASes [14] and ≈ 1M `s) and increasing connectivity between collection and use [1, 28]. Users often `., using only a sample of the VPs, vely visible to other VPs. Finally, `so strains platform scalability. only ≈1% of the observably ... Despite continued addition of an terms of fraction of ASes they are a flat for two decades.

peering wit. A flat for two decades. These grov ssures coincide with regulatory concerns about slow prog. ss in deployment of routing security protections [62]. The ensuing public debate has highlighted the importance of these platforms for detecting both accidental and malicious transgressions in the routing system. While significant investment in data collection could accommodate gathering, retention, and shar-

Partially funded by a RIPE community fund

For now, bgproutes.io only uses lossless compression

Lossless compression e.g., for recent data



Lossy compression e.g., for old data

The Next Generation of BGP Data Collection Platforms

Thomas Alfroy*, Thomas Holterbach*, Thomas Krenc[†], KC Claffy[†], Cristel Pelsser*[‡] *University of Strasbourg, [†]CAIDA/UC San Diego, [‡]UCLouvain

bgproutes.io

ABSTRACT

BGP data collection platforms as curr damental challenges that threaten Inspired by recent work, we analyze new optimization paradigm for BGP colle data collection with two component tween BGP updates and using it to optimize ing streams of BGP data. An appropriate defin across updates depends on the analysis objective include: a survey, measurements, and simulation: the limitations of current systems; a general framew rithms to assess and remove redundancy in BGP observ quantitative analysis of the benefit of our approach in terms racy and coverage for several canonical BGP routing analyses as hijack detection and topology mapping. Finally, we implem and deploy a new BGP peering collection system that automate peering expansion using our redundancy analytics, which provides a path forward for more thorough evaluation of this approach

CCS CONCEPTS

 \cdot Networks \rightarrow Network measurement

KEYWORDS

Internet measurement, BGP, Routing Security

ACM Reference Format:

Thomas Alfroy, Thomas Holterbach, Thomas Krenc, KC Claffy, Cristel Pelsser. 2024. The Next Generation of BGP Data Collection Platforms. In ACM SIGCOMM 2024 Conference (ACM SIGCOMM '24), August 4–8, 2024, Sydney, NSW, Australia. ACM, New York, NY, USA, 19 pages. https: //doi.org/10.1145/3651890.3672251

1 INTRODUCTION

The study of the global Internet infrastructure relies on BGP data collection platforms (RouteViews [61] and RIPE RIS [49]) that maintain BGP peering sessions with network operators who volunteer to share (sometimes portions of) their routing tables. Originally

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the established decades ago to support operational troubleshooting ("How do others reach my network?"), these systems have become a cornerstone for scientific and operational analysis of the Internet.

Collecting this data faces a fundamental cost-benefit trade-off. The information-hiding character of BGP requires collecting routes from as many BGP routers, *a.k.a* Vantage Points (VPs), as possible. But in practice the BGP protocol extensively propagates connectivity messages, leading to highly redundant (along with significant unique) data coming from each peer. The result is a data set with enormous redundancy and yet dangerous visibility gaps [34].

The platforms' policies to store a snapshot of the aggregated the every few hours, as well as every BGP update received in the every few hours, as well as every BGP update received in the every few hours, as well as every BGP update received in the event these snapshots, exacerbates the storage of redundant the continued growth of the Internet (\approx 75k ASes [14] and \approx 1M obally announced prefixes) and increasing connectivity between two rks further burden data collection and use [1, 28]. Users often the result of the data, e.g., using only a sample of the VPs, growing the connectivity uniquely visible to other VPs. Finally, annual vetting of new peers also strains platform scalability, the platforms connectively peer with only \approx 1% of the observably the continued addition of the ers, RIS and RV's coverage in terms of fraction of ASes they are there with how ers and of flat for two decades.

These growin pressures coincide with regulatory concerns about slow progress in deployment of routing security protections [62]. The ensuing public debate has highlighted the importance of these platforms for detecting both accidental and malicious transgressions in the routing system. While significant investment in data collection could accommodate gathering, retention, and sharing orders of magnitude more routing data, current constraints motivate us to consider a more strategic approach. We propose a data collection scheme that scales at least an order of magnitude in the number of VPs feeding public collection systems while limiting the increase in human effort and data volume.

Vision. We explore a fundamentally new way to collect BGP data: an overshoot-and-discard strategy. Akin to CERN's Large Hadron Collider (LHC) which generates millions of collisions just to see a few interesting particles (e.g., Higgs boson), overshooting BGP data collection will maximize the chance to see interesting routing events, e.g., BGP hijacks. We imagine a world where public BGP data providers could automate deployment of additional VPs. targeting

bgproutes.i

Our new next-gen BGP route collection platform

Collection: High coverage



Distribution: Fast API with high granularity



https://bgproutes.io



Collecting more data is useful But not when users cannot effectively process it

Collecting more data is useful But not when users cannot effectively process it

Current MRT archives consist of 1000+ compressed files for updates and RIB dumps

The BGP data is intermingled across all these files

Index of /handete

<u>Name</u>	Last modified	Size Descr	<u>iption</u>				
Parent Directo	<u>ory</u>	-		- 1			
<u>2001.10/</u>	2004-02-23 20:19	9 -					
<u>2001.11/</u>	2004-02-23 20:20	0 -					
<u>2001.12/</u>	2004-02-23 20:2	7 -					
<u>2002.01/</u>	2004-02-23 20:30	6 -					
<u>2002.02/</u>	2004-02-23 20:40	6 -					
<u>2002.03/</u>	2004-02-23 20:50	6 -		a/2	202	5.05	5/RIBS
<u>2002.04/</u>	2004-02-23 21:02	8 -					
<u>2002.05/</u>	2004-02-23 21:19	9 -		nodi	ified	<u>Size</u> D	escription
<u>2002.06/</u>	2004-02-23 21:29	9 -					
<u>2002.07/</u>	2004-02-23 21:40	0 -				-	
	2	rib.20250501	<u>1.0000.bz2</u> 2	2025-05-01	00:00	85M	
	?	rib.20250501	1 <u>.0200.bz2</u> 2	2025-05-01	02:00	85M	
	?	rib.20250501	<u>1.0400.bz2</u> 2	2025-05-01	04:00	85M	
	?	rib.20250501	1 <u>.0600.bz2</u> 2	2025-05-01	06:00	85M	
	?	rib.20250501	1.0800.bz2	2025-05-01	08:00	85M	
	?	rib.20250501	1.1000.bz2	2025-05-01	10:00	87M	
	?	rib.20250501	1.1200.bz2	2025-05-01	12:00	88M	
	?	rib.20250501	1.1400.bz2	2025-05-01	14:00	88M	
	?	rib.20250501	1.1600.bz2	2025-05-01	16:00	88M	
	?	rib.20250501	1.1800.bz2	2025-05-01	18:00	88M	
	21	rib.20250501	1.2000.bz2 2	2025-05-01	20:00	88M	

RouteViews MRT archive





What the user need

KBs of data





KBs of data



RouteViews MRT archive (10+TBs)

GBs of data

What the user will download, uncompress and process



Today, researchers often regretfully resort to sampling Results of our survey in our SIGCOMM'24 paper

What the user need





Today, researchers often regretfully resort to sampling Results of our survey in our SIGCOMM'24 paper





Today, researchers often regretfully resort to sampling Results of our survey in our SIGCOMM'24 paper





bgproutes.io comes with a simple and fast API that provides high-granularity access to BGP data

The API offers three endpoints:

vantage_points updates rib



bgproutes.io/data_api

Let's use our Python client to retrieve the data from pybgproutesapi import vantage_points, updates

Let's use our Python client to retrieve the data from pybgproutesapi import vantage_points, updates

Let's retrieve the vantage points we want to use vps = vantage_points(source=['bgproutes.io', 'ris'])

Let's use our Python client to retrieve the data from pybgproutesapi import vantage_points, updates

Let's retrieve the vantage points we want to use vps = vantage_points(source=['bgproutes.io', 'ris'])

Finally, we retrieve the updates and print them for every VP for vp in vps: vp_upd = updates(vp_ip=vp, start_date="2025-05-14T00:00:00", end_date="2025-05-15T00:00:00", aspath_regexp="^3333 | 3333 | 3333\$" print (vp_upd)







Our new next-gen BGP route collection platform

Collection: High coverage



Distribution: Fast API with high granularity



