

Master thesis : Revisiting the BGP communities usage

Auteur : Razafindralambo, Noro

Promoteur(s) : Donnet, Benoît

Faculté : Faculté des Sciences appliquées

Diplôme : Master en sciences informatiques, à finalité spécialisée en "computer systems and networks"

Année académique : 2017-2018

URI/URL : <http://hdl.handle.net/2268.2/4507>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.



Revisiting the BGP communities usage

Master Thesis conducted for obtaining the Master's degree
in Computer Science by Noro Razafindralambo
under the supervision of Prof. Benoit Donnet

University of Liege - Faculty of Applied Sciences
Academic year 2017-2018

ABSTRACT

BGP is an interdomain routing protocol, used to learn and propagate prefixes in the Internet. It is used by ASes to exchange reachability information. To indicate the reachability of a subnet, an AS can send route advertisements to its neighbouring ASes. When multiple routes are available to join a given destination, the routing decision taken by BGP to select the best route relies on mechanisms that can be enforced by BGP attributes. This thesis focuses on one of these attributes: the BGP community. The BGP community attribute is a means to label a route to add information to it. Measurements and analyses spanning the history of BGP communities are used to evaluate the usage of that attribute. The results suggest that more and more ASes are using BGP communities over time, generalizing the usage of that attribute and making it more and more prevailing. The number of routes carrying BGP communities keeps on growing and this is impacting the size of BGP routing tables. A taxonomy refining the proposition made by Donnet and Bonaventure [1] ten years ago is proposed to enable the classification of the BGP communities. A quantification of the BGP communities based on that taxonomy contributes to uncover the recent trends ruling the usage of BGP communities. The results reflect that the vast majority of BGP communities are used for Traffic Engineering purposes. A website gathering information about the communities of the studied ASes is presented (http://www.montefiore.ulg.ac.be/~bgp_communities/). This website is updated on a regular basis and represents a significant step forward as it allows researchers to access communities information that are in general not easy to glean.

Keywords: *BGP, community, attribute, routing, taxonomy.*

ACKNOWLEDGEMENT

First of all, I would like to express my sincere gratitude to my supervisor **Benoit Donnet** for providing me with the opportunity to work on such an interesting topic and for his guidance. He was always available whenever I had a question and provided me with comments that allowed me to improve this document.

I am also grateful to **Guy Leduc** for lending me the book [2] which was really useful to me.

I would like to thank my entire family for their encouragement and support, and especially my uncle **Hary Razafindralambo**, who always believed in me.

TABLE OF CONTENTS

LIST OF FIGURES	v
LIST OF TABLES	vii
1 Introduction	1
2 BGP generalities	3
2.1 BGP basics	3
2.1.1 Notion of AS	3
2.1.2 Introducing BGP	3
2.1.3 Internal and External BGP	4
2.2 AS relationships and hierarchy	5
2.3 BGP attributes	7
2.3.1 Origin	7
2.3.2 AS path	8
2.3.3 Next hop	8
2.3.4 Local Preference	8
2.3.5 MED	9
2.3.6 Community	9
2.4 BGP Decision Process	10
3 BGP community attribute	12
3.1 Definition	12
3.2 Usage of BGP Communities	13
3.2.1 Well-known communities	15
3.2.2 Blackhole community	16
3.3 Evolution of BGP communities	17
3.3.1 BGP Extended community	17

3.3.2	BGP Large community	19
4	Methodology	20
4.1	Approach	20
4.2	Data collection	21
4.2.1	Tools	21
4.2.2	Data Selection Description	21
4.2.3	Data Collection Description	23
4.2.4	Data Processing Description	23
4.2.5	Deliverables	23
4.3	Web Scraping	24
4.3.1	Tools	24
4.3.2	Description	24
4.3.3	Deliverables	25
4.4	Communities classification	26
4.4.1	Description	26
4.4.2	Deliverables	26
4.5	Website building	26
4.5.1	Tools	26
4.5.2	Description	26
4.5.3	Deliverables	27
5	Results	28
5.1	The importance of BGP communities	28
5.1.1	General results	28
5.1.2	Specific results	32
5.2	Revisiting the taxonomy	34
5.3	BGP Community Classification: trends and tendencies	37
5.3.1	General classification	37
5.3.2	Classification per AS	38
5.4	BGP Community Browser: a website	41
6	Conclusion	43
	REFERENCES	44

LIST OF FIGURES

2.1	An example of connections between ASes	4
2.2	BGP peering session	5
2.3	AS relationships	5
2.4	Emerging new Internet logical topology (Labovitz et al. [3])	6
2.5	Classification of BGP attributes	7
2.6	Illustration of the <code>AS_PATH</code> attribute	8
2.7	Illustration of the <code>LOCAL_PREF</code> attribute	9
2.8	Illustration of the <code>MED</code> attribute	10
3.1	Setting the <code>LOCAL_PREF</code> with a community attribute	14
3.2	Illustration of the <code>NO_ADVERTISE</code> community value	15
3.3	Illustration of the <code>NO_EXPORT</code> community value	16
3.4	Illustration of the <code>NO_EXPORT_SUBCONFED</code> community value	17
3.5	Usage of BGP community for blackholing	18
	(a)	18
	(b)	18
	(c)	18
4.1	General structure of the project	21
5.1	Evolution of the number of ASes using BGP communities	29
5.2	Evolution of the number of ASes from [4]	29
5.3	Evolution of the number of different BGP communities	30
	(a) Tier 1	30
	(b) Tier 1	30
	(c) Tier 1	30
	(d) Tier 2	30
5.4	Evolution of the memory consumption due to BGP communities	31
	(a) Tier 1	31

(b)	Tier 1	31
(c)	Tier 1	31
(d)	Tier 2	31
5.5	BGP community list lengths	34
(a)	Tier 1	34
(b)	Tier 1	34
(c)	Tier 1	34
(d)	Tier 2	34
5.6	General classification of BGP communities	35
5.7	General classification of the BGP communities	37
(a)	High level classification	37
(b)	Traffic Engineering vs Route Tagging	37
(c)	Traffic Engineering classification	37
(d)	Route Tagging classification	37
5.8	Classification of BGP communities per AS	39
5.9	Classification of recognized BGP communities per AS	39
5.10	BGP community browser	42
(a)	Home page	42
(b)	AS result	42
(c)	AS result	42
(d)	AS result	42
(e)	Community result	42
(f)	Community result	42

LIST OF TABLES

3.1	Tagging communities published by AS3561 [5]	14
3.2	Some examples of BGP community usage from [6]	14
4.1	Tier 1 and their data providers	22
4.2	Tier 2 and their data providers	22
4.3	Pages used to get the semantic of BGP communities per AS	25
5.1	Size of RIBs tables per provider for the first dump of December 2017 . .	32
5.2	Proportion of routes carrying BGP communities for the Tier 1	33
5.3	Proportion of routes carrying BGP communities for the Tier 2	33
5.4	Average repartition of BGP communities corresponding to Figure 5.7 . .	38
5.5	Proportion of classified BGP communities per Tier 1	40
5.6	Proportion of classified BGP communities per Tier 2	41

CHAPTER 1

Introduction

An Autonomous System (AS) is a network or a group of networks under the control of a single administrative entity. In order to determine the optimal paths for source-destination pairs spanning multiple ASes, a protocol is needed to exchange reachability information. BGP is an interdomain routing protocol used to learn and propagate prefixes in the Internet. To indicate the reachability of a subnet, an AS can send route advertisements to its neighbouring ASes. When multiple routes are available to join a given destination, the routing decision taken by BGP to select the best route relies on mechanisms that can be enforced by BGP attributes. This thesis focuses on one of these attributes: the BGP community. The BGP community attribute provides a means to label a route, either to provide additional information about that route or to influence the routing policies.

Ten years ago, Donnet and Bonaventure [1] studied the usage of the BGP community attribute and proposed a taxonomy for a better classification of the various communities. They manually collected BGP communities information from ISPs websites and whois servers, and they built a database tagged using their taxonomy. However, no up-to-date classification is available today, underlining the need for a more modern insight on the usage of this attribute.

This document contributes to address this challenge by updating the study on the importance of BGP communities. This project investigates the evolution of the BGP communities usage throughout the years and the more recent trends it follows, on the basis of a subset of Tier 1 and Tier 2 networks. The study reveals that there is an increasing number of ASes using BGP communities, highlighting the prevalence of that attribute. More and more routes are carrying BGP communities and the number of different communities observed directly impacts the routing table size.

A revision of the taxonomy suggested by Donnet and Bonaventure [1] is proposed, and allows to better capture the intent behind the usage of BGP communities. A database making use of the revisited taxonomy is built. It is comprising data extracted programmatically from websites publicly documenting the communities semantic. Thanks to this revisited taxonomy, this project achieves to uncover the recent trends and tendencies ruling the usage of BGP communities and to quantify the communities belonging to a given category. It appears from the results that the most widespread motivation behind the usage of BGP communities concerns Traffic Engineering purposes.

The development of a website (http://www.montefiore.ulg.ac.be/~bgp_communities/) allowing researchers to obtain easily communities information that are in general not straightforward to glean represents a major step forward. The website is updated on a regular basis, which ensures the validity of the information presented. Moreover, it allows to gather communities information about multiple ASes at a single place and in a normalized format. This is an important achievement because the publicly available information are spread over different websites in a large variety of formats: data can be presented in tables, but also in plain text, and sometimes they can appear as a mix of tables and plain text, which is neither a straightforward nor an effective manner to research a community.

It is worth mentioning that this thesis does not provide a thorough and complete analysis of all existing BGP communities, but rather restricts the domain of study to a subset of ASes. Large communities are not studied in this project, because there was no mention of such communities in the available information documenting the semantic of the BGP communities. Moreover, the tool used to collect the communities does not support large communities yet, as Giotsas [7] stated.

This document is structured as follows. Chapter 2 introduces the key concepts around BGP, explaining not only the BGP attributes, but also the BGP decision process, used to select the best route towards a destination. Then, chapter 3 dives into the BGP community attribute and provides a documentation on the generalities of that attribute. Chapter 4 explores the approach followed to carry out this project, from the data collection to the analyses. The produced taxonomy and the results of this work are presented in chapter 5. Finally, a conclusion closes this document in chapter 6.

CHAPTER 2

BGP generalities

This chapter aims to give the reader an introduction to the basics of BGP for a better understanding of the overall context of this Master's Thesis. The section 2.1 will introduce BGP and the key concepts around that protocol. It will be followed by a section illustrating AS relationships and hierarchy. Afterwards we will dive into the BGP attributes. And we will end with an explanation of BGP decision process.

2.1 BGP basics

2.1.1 Notion of AS

An Autonomous System (AS) is a network or a group of networks under the control of a single administrative entity. That entity can be an ISP or a large organization. An ISP will run an IGP (Internal Gateway Protocol) within an AS to determine optimal paths internal to that AS. To determine paths for source-destination pairs spanning multiple ASes, an ISP will run an EGP (External Gateway Protocol). An EGP is a protocol used by two different ASes to exchange reachability information. It allows an AS to have full connectivity to the entire Internet [2]. The Internet de facto interdomain routing protocol is BGP 4 [8].

2.1.2 Introducing BGP

BGP is an interdomain routing protocol used to obtain and propagate reachability information between ASes (Rekhter et al. [8]). The destinations are advertised as prefixes which themselves represent a subnet or a collection of subnets. When there are multiple routes available to reach a given destination, the best route is selected on the basis of some attributes through a mechanism called BGP decision process, addressed by section 2.4 . There are 4 types of messages sent between BGP speakers (Stewart [2]):

- OPEN used to open a BGP peering session

- UPDATE used to communicate information between two BGP speakers. This is the message sent to advertise a prefix or to withdraw a previously advertised prefix. It is the message carrying the BGP attributes.
- NOTIFICATION which is sent when an error occurs
- KEEPALIVE sent between BGP peers to confirm that the connection between them is still active

2.1.3 Internal and External BGP

There are two possibilities to exchange reachability information. The information can be propagated between routers belonging to the same AS, through an Internal BGP (iBGP) session represented by the red dashed lines in figure 2.1. When the exchange is done by BGP peers belonging to different ASes, we talk about external BGP (eBGP), whose sessions are represented by the red continuous lines in figure 2.1. The red routers in figure 2.1 are called "AS border routers" and are mainly responsible for running both EGP as eBGP and iBGP, and IGP. The grey routers are "internal routers" as they are internal to an AS. Their main purpose is to run an IGP within that AS.

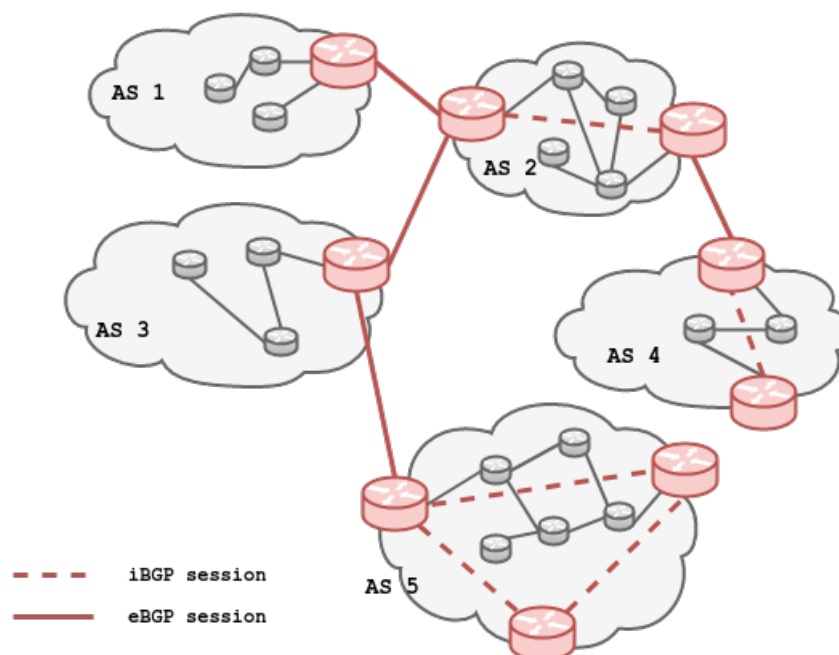


Fig. 2.1 An example of connections between ASes

Figure 2.2 shows how AS1 and AS2 can exchange reachability information. AS1 wants to advertise the prefix 132.45.9.0/24 to AS2. They must establish a BGP peering session between their border routers R1 and R2. It will be an eBGP session

because R1 and R2 belongs to different ASes. The border router R2 will then distribute the prefix that was learned to all the routers internal to AS2 through iBGP. The routers

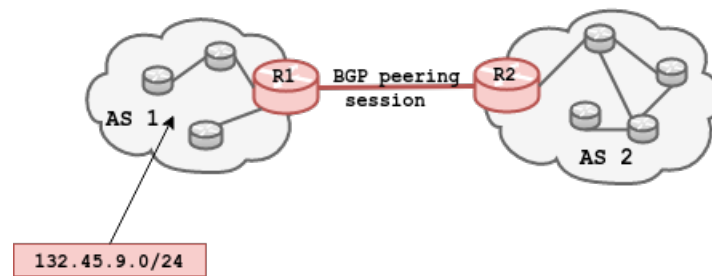


Fig. 2.2 BGP peering session

in an AS run an IGP to learn routes within the internal network. Then the BGP and IGP information will be combined by routers to construct a forwarding table (cf section 2.4) that maps each destination prefix to the outgoing links along the best path through the network towards the egress border router [9].

2.2 AS relationships and hierarchy

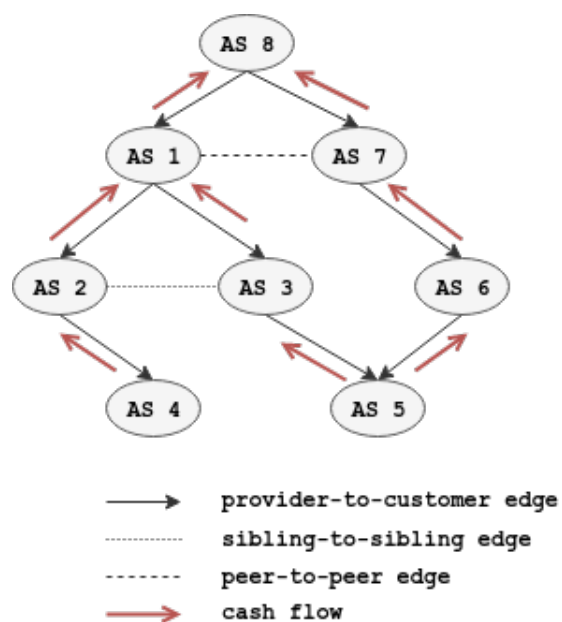


Fig. 2.3 AS relationships

BGP is used not only used to exchange routing information in the Internet but also to establish business relationships between ASes. The AS business relationships can be classified as (cf (Caesar and Rexford [9])):

- Transit relationship, which includes customer-to-provider (c2p) and provider-to-customer (p2c). In this relationship, a customer pays a provider to transit traffic in the Internet.
- Peering relationship, or peer-to-peer (p2p) allows two ASes to freely exchange traffic between themselves and their customers without transiting through a provider.
- Sibling relationship, in which two ASes under the same ownership are allowed to exchange traffic without any cost.

Figure 2.3 shows an example of AS relationships. For instance, this figure shows that AS8 is a provider for AS1 and AS7 who are customers, but also providers of ASes below. AS1 and AS7 have a peering relationship so they can exchange traffic without transiting through AS8. AS4 can be categorized as a stub autonomous system as it is connected only to AS2. AS5 has 2 providers: AS3 and AS6. AS5 is multi-homed.

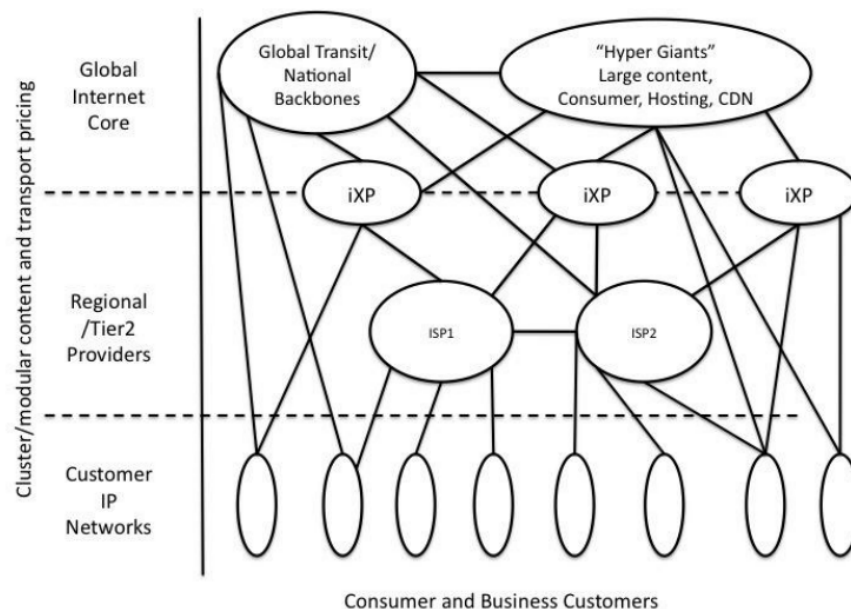


Fig. 2.4 Emerging new Internet logical topology (Labovitz et al. [3])

The hierarchy of transit providers generally seen in textbooks [3] involves:

- Tier 1 Service Provider : Those ISPs do not have to pay other ISPs for transit. They peer with all other Tier 1 ISP, to maintain global reachability.
- Tier 2 Service Provider : A network that needs to purchase transit service from Tier 1 Providers to reach some portion of the Internet. They can pair with other Tier 2 ISPs to alleviate concerns on the cost of transit relationships.
- Tier 3 Service Provider : Those ISPs generally buy transit services to Tier 2 ISPs.

But the interconnection strategies of the providers shifted towards what we can see in Figure 2.4 (Labovitz et al. [3]). Due to the decreasing cost of transit and the increasing demand towards content providers, Figure 2.4 emerges as a new Internet traffic pattern. In this pattern, large content providers, datacenter/CDNs and consumer networks see the majority of traffic (by volume) flowing directly between them.

2.3 BGP attributes

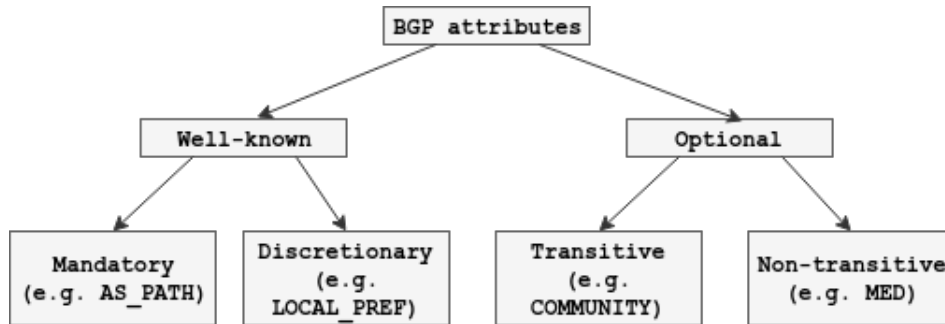


Fig. 2.5 Classification of BGP attributes

BGP attributes are pieces of information carried with a BGP update. The BGP attributes can be classified through the system presented in figure 2.5. As shown in the figure, some attributes are well-known, which means that they must be recognized by each router supporting BGP. When well-known attributes must figure in every announcement, they are said to be mandatory, otherwise they are said to be discretionary. Attributes that are not well-known are said to be optional, which means that a router supporting BGP does not have to know or to recognize the attribute. It will just have to forward the attribute if it is transitive, or drop it if it is non-transitive [8]. Now let us examine a subset of BGP attributes.

2.3.1 Origin

The BGP origin attribute is a well-known mandatory attribute. It provides information about the way a prefix was injected into BGP. There exist three different origin codes, listed by order of preference:

- IGP (value 0): The route was learned from an IGP. This value is the most preferred one, i-e a route with this origin value will be selected before routes with other codes.
- EGP (value 1): The prefix was learned through an EGP.
- incomplete (value 2): The prefix was learned by some other means [8].

2.3.2 AS path

The AS_PATH is a well-known and mandatory BGP attribute representing the list of each AS traversed by the announcement. When an AS creates or forward an announcement, it appends its AS number to the AS_PATH before sending the announcement. When selecting the best route, one of the criteria can be to pick the route having the shortest AS_PATH. Sometimes, one may want to force the selection of one route over the others even if it is a longer route, through a mechanism called AS path prepending. In order to achieve that, the AS will prepend its AS number a given number of times to the shorter routes, to make them artificially longer and less desirable than the route we want to select. Those routes will then become backup routes. For instance, AS1 could

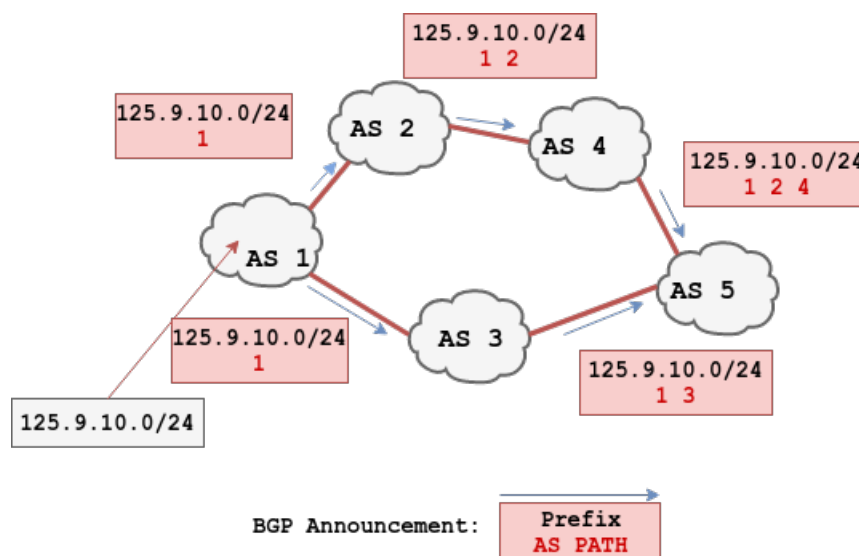


Fig. 2.6 Illustration of the AS_PATH attribute

prepend its ASN 3 times to the AS_PATH before sending it to AS 3 so that (1,2,4) would be shorter and then preferred over (1,1,1,3).

2.3.3 Next hop

The BGP next-hop attribute is well-known and mandatory. It specifies the IP address of the next hop for forwarding packets to reach a destination prefix.

2.3.4 Local Preference

The LOCAL_PREF is is well-known and discretionary. It is a metric attached to each route so that when several routes are available, the preferred route will be the one with the highest local preference.

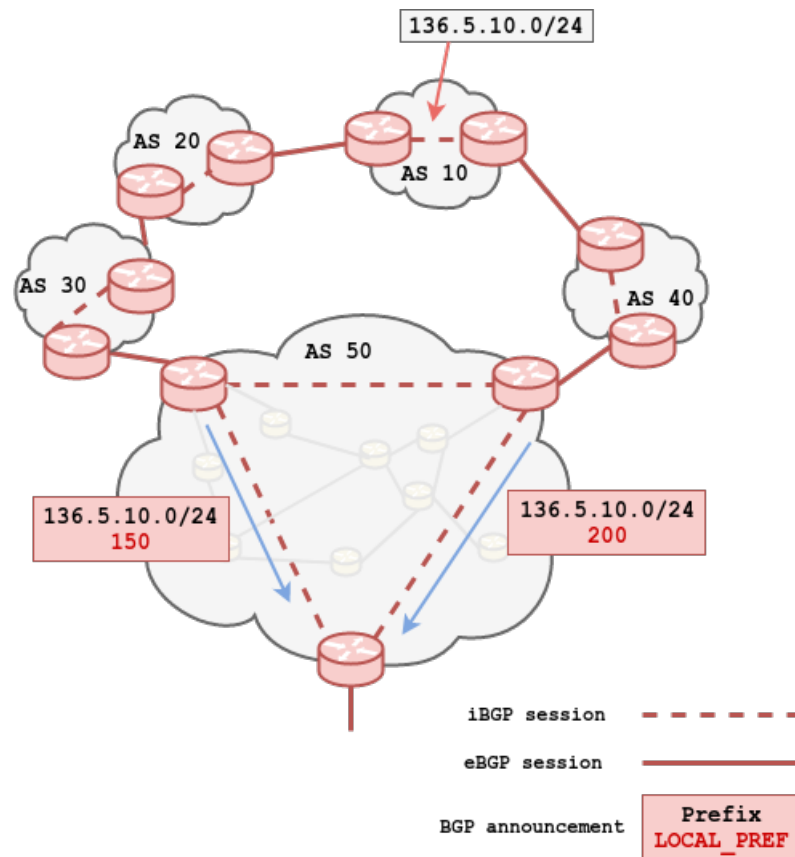


Fig. 2.7 Illustration of the `LOCAL_PREF` attribute

2.3.5 MED

The multi-exit discriminator (MED) 4 attribute is an optional non-transitive attribute. It is used to choose the optimal link to reach a particular prefix when several entry points are connected to a neighbor. The path with the lowest MED value will be preferred.

2.3.6 Community

From the figure 2.5 we can see that the community attribute is optional and non-transitive. It is not required to send it with every announcement and it can be exported even if it is not recognized by the router traversed by the announcement. And that makes the community attribute a good candidate for its main functionalities. It is used to add information to a given route or to take an action about that route [10] or to simplify the configuration of complex routing policies [2]. Moreover, multiple communities can be attached to one route. This attribute will be discussed in detail in chapter 3.

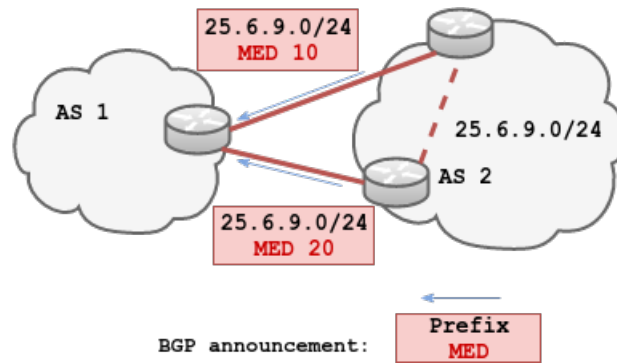


Fig. 2.8 Illustration of the MED attribute

2.4 BGP Decision Process

Whenever a new route is learned, the Routing Information Base (RIB), which stores all IP routing information, is updated. The best paths are selected from the RIB, then the Forwarding Information Base (FIB) is built and the forwarding information is distributed to the interface line-cards. The FIB is the table used for forwarding IP packets based on their destination IP address. The need for a FIB is justified by the fact that some entries in the RIB could have next hops that are not directly connected. The FIB is used to resolve the next hops and compute the outgoing interfaces. The size of the FIB can impact the forwarding performance of a router because a large FIB may take a longer time to be processed [11]. This separation between the Control Plane with the RIB and the Forwarding Plane with the FIB thus plays a role in the performance of routers. Let us describe how the BGP decision process is orchestrated to select the best route. If there is only one route toward a particular destination, the best path to reach that destination is obvious. But when there are multiple routes to reach a given destination, BGP has to choose the best one in order to put it in the FIB. The decision process is the following, if a step does not select exactly one route, go to the next step:

1. Choose the route with the highest LOCAL_PREF
2. Select the route with the shortest AS_PATH
3. Select the route with the lowest ORIGIN value
4. Select the route with the lowest MED
5. Prefer routes learned via eBGP. If there are more than one route, select the route with the lowest BGP identifier
6. If all the routes were learned via iBGP, the route that was learned from the iBGP neighbor with the lowest BGP identifier is selected

The BGP decision process and the addition and retrieval of forwarding entries directly impact the processing load resulting from BGP updates. The high routing update volume may lead to instability. Excessive updates may cause a BGP implementation to be unable to maintain its BGP or IGP sessions [12]. This effect of 'route oscillations' is called "route flap". In an effort to contain the routing instability, Villamizar et al. [12] introduces "route flap damping" which defines mechanisms to prevent the oscillations.

The next chapter will provide further explanations about the BGP community attribute.

CHAPTER 3

BGP community attribute

The BGP community attribute usage is a topic that interested many researchers. Giot-sas et al. [13] discussed the usage of the community attribute to infer AS relationships. Interdomain Routing can take profit of the BGP communities, as Quoitin et al. [14] showed, by proposing a use of communities for Interdomain traffic engineering. The BGP community attribute utilization was the topic of Quoitin and Bonaventure [15]. Donnet and Bonaventure [1] aimed to provide a taxonomy to classify the usage of the attribute and to study its importance. The usage of BGP community attribute for detecting peering infrastructure outages was also discussed by Giot-sas et al. [16]. The BGP community attribute was also studied for its use in DDoS mitigation techniques as Dietzel et al. [17] and Giot-sas et al. [18] explained. This chapter will introduce the BGP community attribute and give examples of usage for that attribute.

3.1 Definition

The BGP community attribute is documented in RFC 1997 [19]. It is an attribute that groups together destinations for which the same routing decisions can be applied. Therefore, performing an action on a group of destinations is simple, it only requires a knowledge of the identity of the group, and the community value that describes the desired action. There is no need to know the members of the group. The community attribute is a 32-bit value structured as follows: **ASN:value**.

- The leading 16 bits represent the AS number (ASN). It indicates the AS that originated the community.
- The remaining 16 bits represent the value of the community and its semantic can be defined by the AS.

The values between 1:0 through 65534:65535 can be used to define a community. The other communities (0:x and 65535:x where $x \in [0-65535]$) are reserved. Indeed, AS

number 0 is reserved and may be used to identify non-routed networks [20] and AS number 65535 is reserved [21] for use by well-known communities.

Communities makes it easier to identify the relations between ASes and it also makes traffic engineering simpler. The BGP community attribute confers more control, not only to the provider through a simplified configuration and management, but also to the customer [10]. For instance, the community attribute can be used to prepend n times an AS number to an AS path. It can also be applied in the multi-provider Internet, to simplify the customization of the local preference attribute, and such a configuration will be explained in section 3.2. Indeed, RFC 1998 [22] describes the 2 possible configurations of the `LOCAL_PREF`: it can be AS based or community based. The AS based configuration is done at the provider level and tends to be less efficient, because coordination and configuration are required each time there is a change in the network. Moreover it may be a source of additional complexity since keeping the configuration up-to-date can be problematic. The community based configuration removes the burden of configuring the `LOCAL_PREF` at the provider level. It rather gives control to the customer who is more likely to figure out better its requirements and its needs. The customer can then use the communities to gain more flexibility in the control of its own routing policy.

3.2 Usage of BGP Communities

BGP communities can be classified into two types (Steenbergen and Scholl [10]):

- The communities used to tag a route with the purpose of providing additional information to the customer about that route [15]. For instance, it can inform about:
 - the location where the route was learned. It may be a city, a country, a region and even a continent.
 - the type of peers from which the route was learned (customer, peering partner, transit provider)

This data can be used to shape or influence the policy decisions [10].

- The communities used to take action on the routing policies [15]. It can be about deciding whether or not a prefix is allowed to be exported (to control prefix announcements), or influencing other BGP attributes like the `AS_PATH` or the `LOCAL_PREF`. It is even possible to combine the action with an informational tag, so that a more specific behavior can be targeted. For instance, one can decide

to tag a route such that the prefix will never be forwarded to Japan.

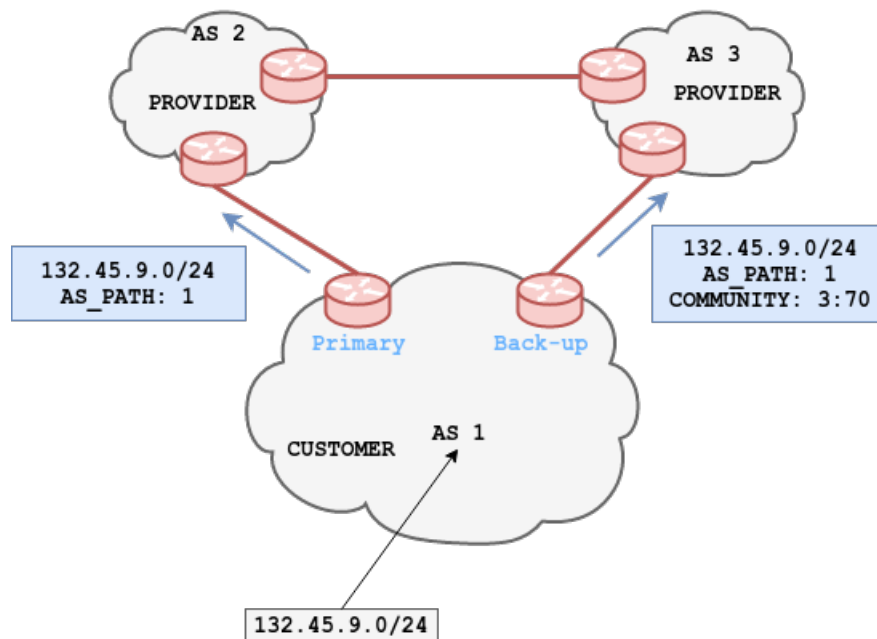


Fig. 3.1 Setting the LOCAL_PREF with a community attribute

Let us illustrate some of the various configurations of the community attribute:

- Below is an example of a possible configuration to indicate the location from where the route was learned.

3561:SRCCC	S is the source (peer or customer) R is the region CCC is the ISO3166 country code
------------	--

Table 3.1 Tagging communities published by AS3561 [5]

- Here are some examples of community configuration:

4436:50	Set local-pref to 50 (Backup Only)
4436:999	Do not export outside of current region
4436:1000	Prepend 1x globally
4436:2010	Prepend 2x in North America
4436:3111	Prepend 3x in Ashburn
65001:6020	No-export to transits in Europe

Table 3.2 Some examples of BGP community usage from [6]

Figure 3.1 shows an example of usage of the community attribute to set the local preference. In that configuration, AS2 and AS3 are providers while AS1 is a customer. The preferred path to reach AS3 traverses AS2 and the direct route between AS1 and AS3 is a backup path. Let us consider that for AS3, normal customer local preference is 100 and peer local preference is 90. The community value is set to 3:70 in the direct route using AS1 to AS3 peering session, so that path can become a back-up path, as the other route traversing AS2 was not tagged with a community attribute and has a default local preference of 100.

3.2.1 Well-known communities

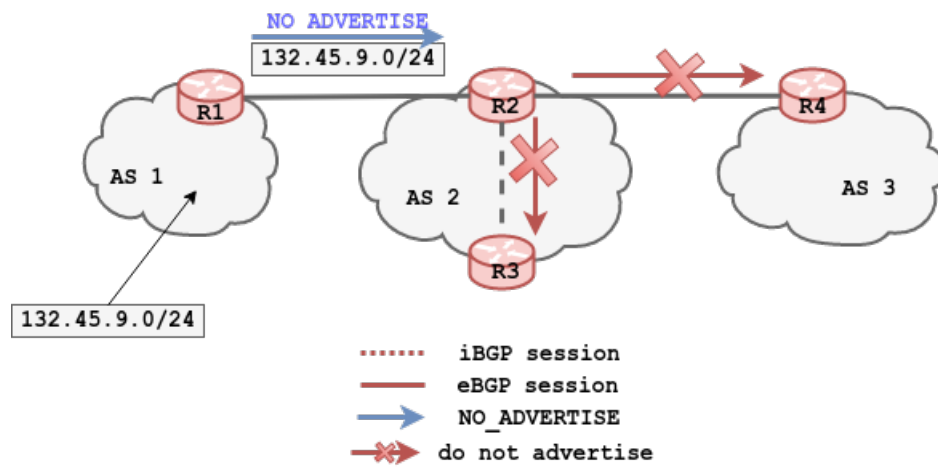


Fig. 3.2 Illustration of the NO_ADVERTISE community value

Some communities have pre-defined values, these are well-known communities supported by all BGP speakers such as:

- **NO_ADVERTISE**: it is used to tell the router that it should not advertise the prefix to any BGP peer [19]. Figure 3.2 shows that the advertisement from R1 reaches R2 but is not propagated to R3 or R4. This community can be used in the context of BGP blackholing, as indicated in [23], and it must tag any blackhole announcement. This is to ensure that the route is never readvertised using BGP.
- **NO_EXPORT**: routers receiving routes carrying that community attribute must not advertise the route outside the BGP confederation boundary [19]. Namely, the prefixes tagged with this community cannot be advertised through eBGP to external ASes. An AS confederation is a collection of autonomous systems advertised as a single AS number to BGP speakers that are not members of the confederation [24] and that are also called subconfederations. Figure 3.3 shows that the advertisements reaches every router of AS2 but is not propagated to AS3. A possible

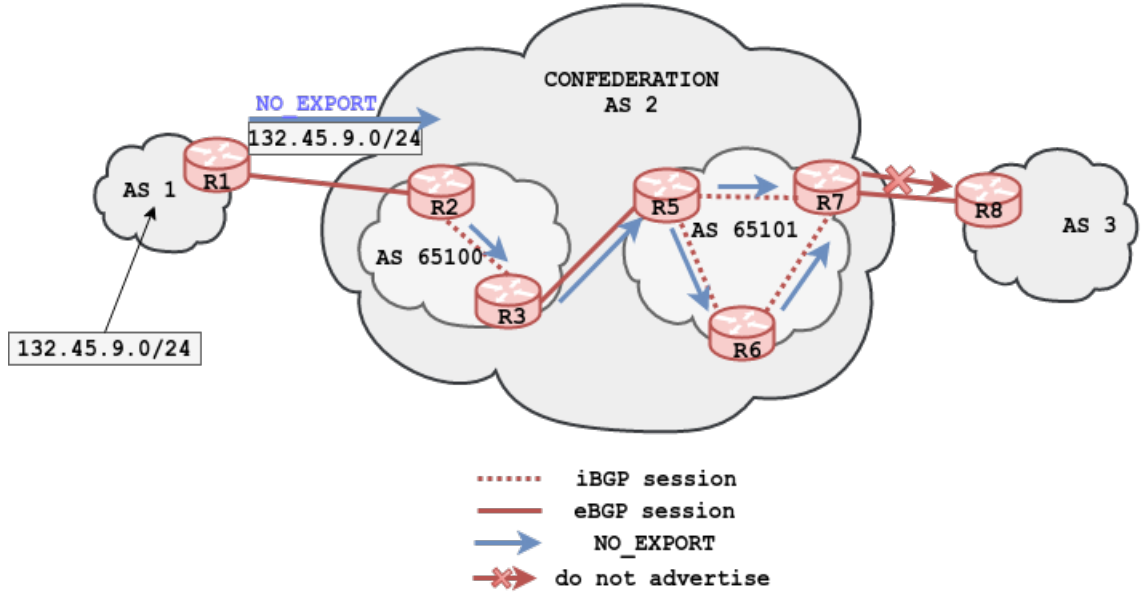


Fig. 3.3 Illustration of the NO_EXPORT community value

usage of this attribute is discussed in [18] in the context of BGP blackholing. Blackhole announcements must neither be propagated nor readvertised outside the local AS. Therefore, they have to be tagged with the NO_EXPORT community as shown in Figure 3.5.

- NO_EXPORT_SUBCONFED: routers receiving routes carrying that community must not advertise the route to eBGP peers, including eBGP peers between subconfederations [19]. This can be used to prevent a specific subnet to be advertised to its neighbors. Figure 3.4 shows that the advertisement reaches the subconfederation directly connected to R1 (AS 65100) in AS2 but is not propagated to the other subconfederation in AS2 (AS 65101).

3.2.2 Blackhole community

Another usage of the BGP community attributes is for blackholing purposes. When an AS announces a prefix to another AS, attaching a blackhole community to the advertisement means for the other AS that all the traffic towards this prefix has to be dropped. This technique can be used to restrict the reachability of a given prefix (Giotsas et al. [18]). It can also be used to mitigate DDoS by reducing the impact of the attack on the victim's infrastructure (Dietzel et al. [17]). The value commonly used by network operators to describe BGP blackholing is 666 (King et al. [23]). However, not all of them adopt this convention. Figure 3.5 shows how AS4 tries to protect itself against the DDoS represented by the thick red arrow. To do so, AS4 attaches a blackhole community to the announcement it sends to AS2 (cf fig. 3.5a). AS2 then understands that it

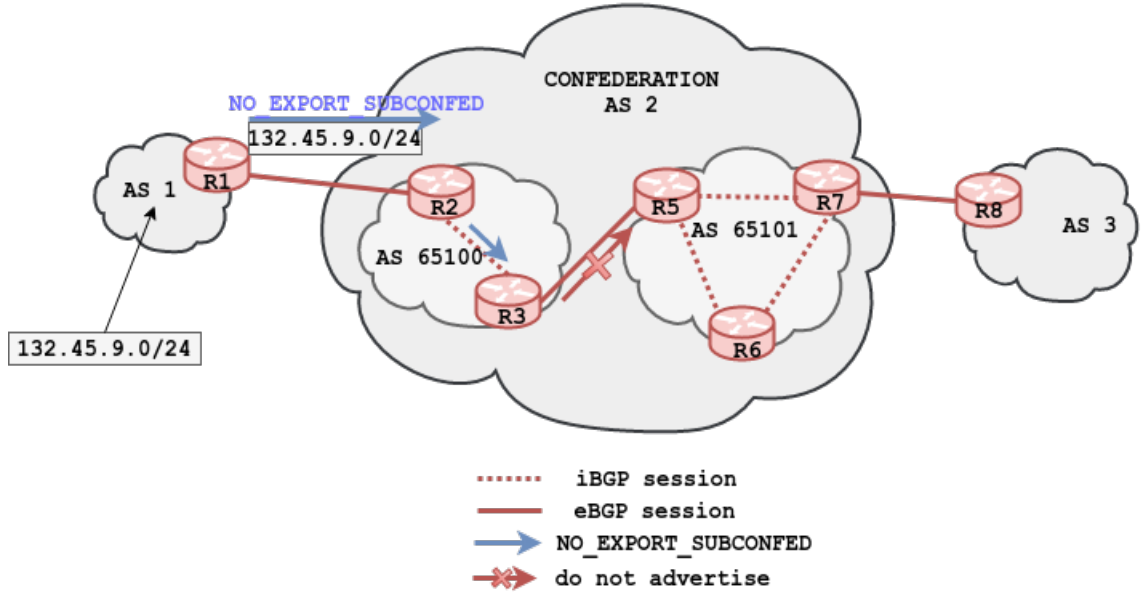


Fig. 3.4 Illustration of the NO_EXPORT_SUBCONFED community value

has to drop the traffic towards the blackholed prefix. RFC7999 (King et al. [23]) underlines that the prefix should not be propagated outside the local AS, thus AS2 adds the NO_EXPORT community to the announcement (cf fig. 3.5b). In figure 3.5c, we can see that the traffic towards the blackholed prefix is finally dropped at AS2 ingress point.

3.3 Evolution of BGP communities

3.3.1 BGP Extended community

MPLS VPNs exploit Virtual Routing and Forwarding (VRF) which allows a router to have multiple (virtual) routing tables. Moreover, there may be a separate virtual routing table for each network interface (either physical or logical). To control the import and export policies in a VPN, a "route target" is needed. Besides, in order to avoid routing loop, it is necessary to identify the site which originated the route, so that the routes learned from that site are not advertised back to it (Cittadini et al. [25]). The BGP community cannot accommodate those requirements. So, the BGP extended community was introduced by Sangli et al. [26]. Indeed, with its 8 bytes value, it is now large enough to allow the setting of a type value identifying a route target or a route origin. A route target is used to define where the routes should be exported and a route origin defines where the VPN IP address was learned.

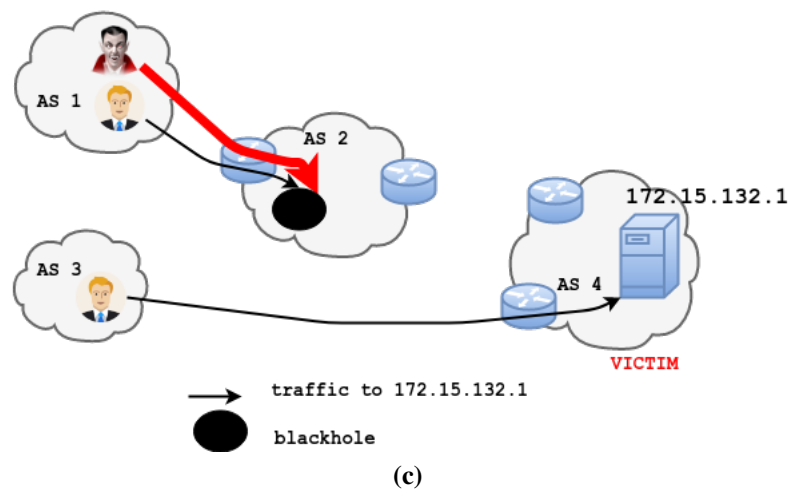
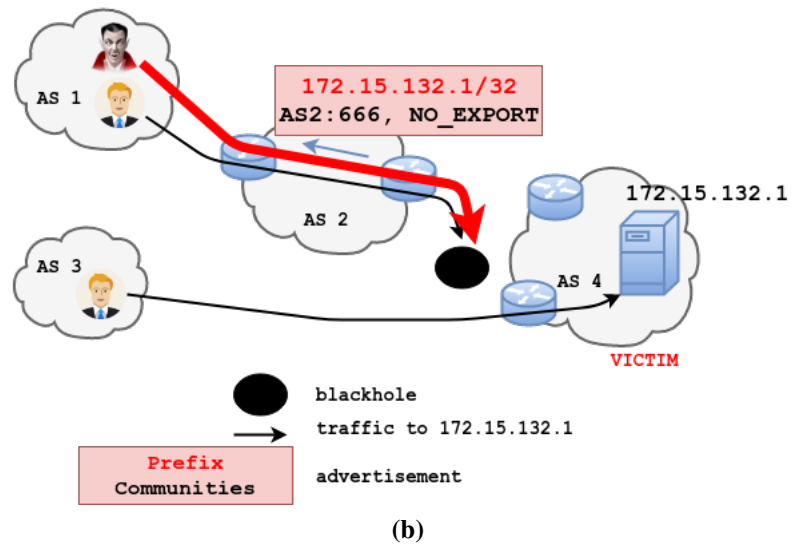
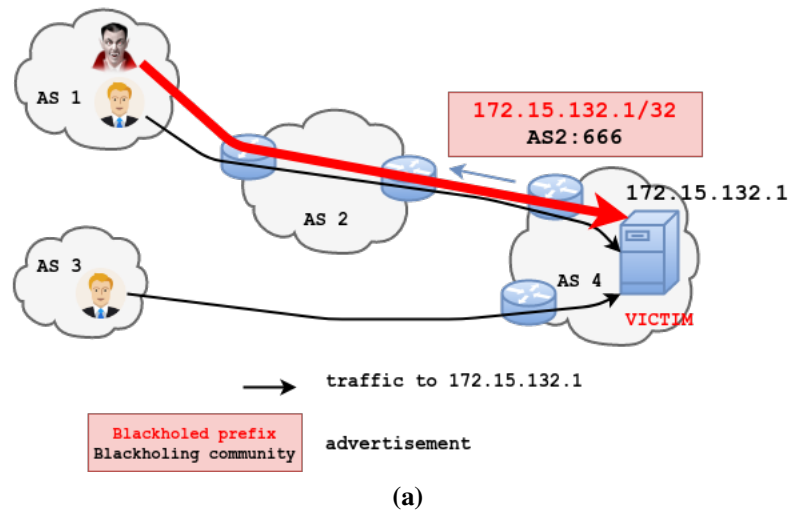


Fig. 3.5 Usage of BGP community for blackholing

3.3.2 BGP Large community

- **Motivations**

4 bytes AS numbers were defined in 2007 and specified by RFC 4893 (Vohra and Chen [27]), later obsoleted by RFC 6793 (Vohra and Chen [28]), and were introduced to prepare for the anticipated exhaustion of the 2 bytes AS numbers. However, neither the BGP community nor the BGP extended community is large enough to accommodate 4 bytes AS number. Thus, the 12 bytes BGP large community was introduced, then documented in 2017 in RFC 8092 (Heitz et al. [29]). It is more flexible and offers more capabilities. It has the following structure:

Global Administrator : Local data Part 1 : Local data Part 2

The first 32 bits (Global Administrator) represents an ASN, the next 32 bits represents a function and the remaining bits represents the parameter of this function. The usage we can make of these values will be explained right after.

- **Examples**

(Snijders et al. [30]) gives a variety of examples to explain the usage of the BGP Large community. Let us take the example of the large community used to pinpoint a particular geographic location from which an announcement can be received. There are multiple possible encodings for a given location, for instance:

- the ISO 3166-1 numeric country identifier (528 represents the Netherlands)
- the code published by the United Nations Statistics Division (145 is Western Asia)

The BGP Large community attribute allows a better classification of the communities as the type of encoding will be used as a function, and the code representing the geographic location will be used as a parameter. Let us take the attribute example: 64497:1:392. In this example, the function "1" indicates that the encoding used is ISO 3166-1 numeric country identifier, and the value 392 encodes Japan.

CHAPTER 4

Methodology

This project is strongly inspired by Donnet and Bonaventure [1] who attempted to devise a taxonomy to classify the BGP communities in 2007. This thesis aims at conducting a study on the BGP community attribute, to observe its evolution and to identify the trends it follows. Towards this end, a subset of tier 1 and tier 2 networks were selected as data source for measurements, collection and analysis. Their data were collected through data providers, then processed in order to make some analyses. The taxonomy presented in [1] is revisited, and the communities collected previously were classified according to the semantic obtained after a web scraping procedure. An analysis of the tendencies is then conducted and finally, a website is built with the idea of a BGP community browser in mind. Section 4.1 presents the structure adopted and the approach taken to reach these goals. The remaining sections will each detail a different building block of the project from the data collection to the development of a website.

4.1 Approach

In order to carry out this project, the approach taken is documented on Figure 4.1. Further subsections will dive into the details of this approach, but to summarize the main points, a `python` module will be responsible for collecting, processing and storing the data for later reuse. A `java` module will scrap the websites and save the communities, their semantic and their classification in `json` files. The `python` module will read the taxonomy documented in the `json` files and classify the communities stored previously. Finally, `php` will be used to load the relevant data and present them on a website. The project is open-source and available here:

<https://gitlab.com/rzelodie/Communities>

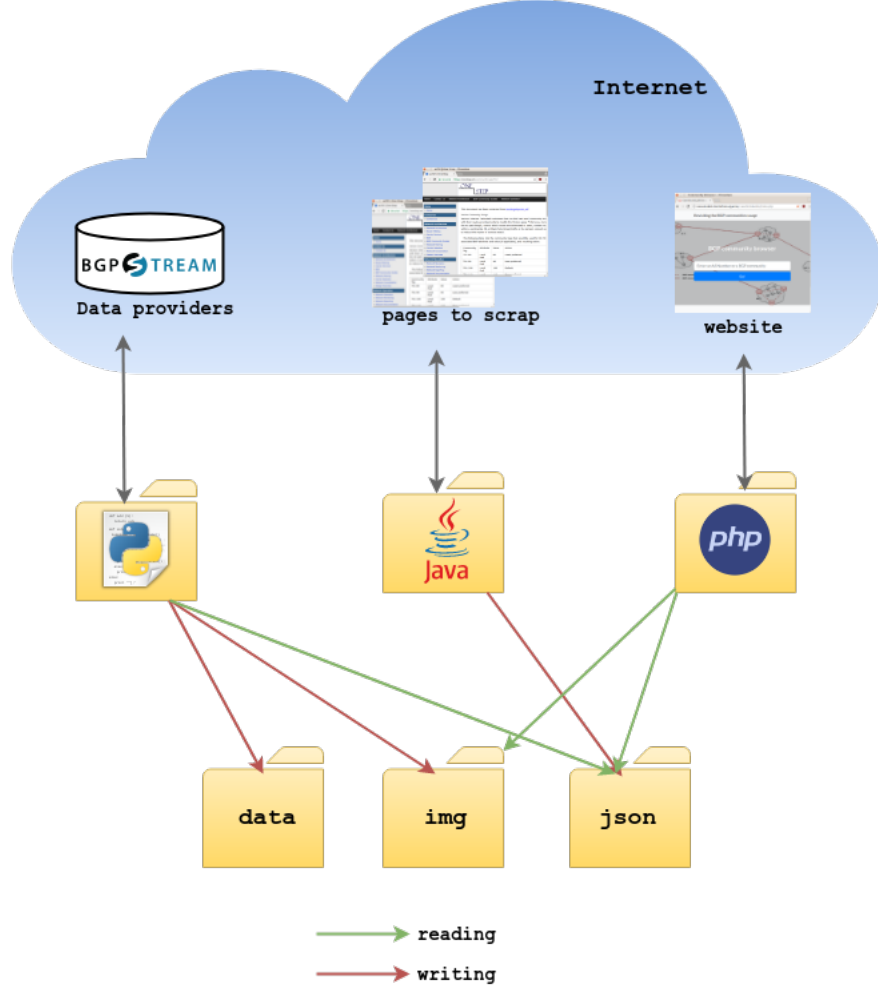


Fig. 4.1 General structure of the project

4.2 Data collection

4.2.1 Tools

BGPStream is an open-source framework for live and historical BGP data analysis [31]. `pyBGPstream`, which is a Python binding to the C BGPStream API, was used to configure and read a stream of BGP measurement data. The data were collected from BGPStream data providers which are listed here [32]. Then, Python `pickle` [33] module was used to serialize the collected data. Finally, `matplotlib` [34], a python library to produce figures, was used to generate plots for the collected data.

4.2.2 Data Selection Description

The first issue was to select the AS numbers to query to build the dataset. Table 4.1 and 4.2 display the list of selected AS numbers. Only tier 1 and tier 2 has been selected for the sake of ensuring the inclusion of an important load of BGP update messages in the

study. The tier 1 were selected from the list provided in [35] and the tier 2 were selected from [36]. The next issue was to determine the provider to query to get information about these AS numbers. Route Views [37] and Ripe [38] are both dispensing tools to get real-time and historical BGP information. The line of attack was to query the 20 providers from Route Views and the 20 providers from Ripe accessible from the list of BGPStream providers [32]. The results of the query showed that one AS can sometimes be found in several providers. Thus, the proportion of routes carrying BGP communities for each AS was calculated per provider and compared. The proportions were in general identical regardless of the chosen provider. The process followed to select the provider to associate with each AS was to try to minimize the number of providers queried by choosing the ones gathering data about the most important number of considered ASes. This gave the providers listed in table 4.1 for the selected Tier 1, and the providers listed in table 4.2 for the selected Tier 2.

ASN	AS name	Provider
209	Century Link	route-views6
286	KPN International	rrc01
701	Verizon	route-views6
1239	Sprint	route-views6
1299	Telia Carrier	route-views2
2914	NTT Communications	rrc01
3257	GTT	route-views2
3356	Century Link	route-views2
3491	PCCW Global	rrc19
5511	Orange	rrc01
6762	Telecom Italia Sparkle	route-views2
6453	Tata Communications	rrc03
6830	Liberty Global	rrc01
7018	AT & T	route-views6
12956	Telxius	rrc03

Table 4.1 Tier 1 and their data providers

ASN	AS name	Provider
1273	Vodafone	rrc03
4589	Easynet	rrc01
5400	British telecom	rrc01
6939	Hurricane Electric	rrc01
8928	Interoute	rrc03

Table 4.2 Tier 2 and their data providers

4.2.3 Data Collection Description

`pyBGPStream` was used to gather different types of information:

1. General Data

One part consisted in collecting general data that would enable the study of the evolution of BGP communities throughout the years. The goal is to be able to observe: the evolution of the number of ASes carrying BGP communities, the evolution of the number of different BGP communities, and the evolution of memory consumption due to the BGP community attribute.

Towards this end, `pyBGPStream` was used to collect the BGP information for every first dump of each month from the first dump available for a provider to a last dump set on January 2018.

2. Specific Data

The second part consisted in collecting more specific data that would enable the study of the proportion of routes carrying BGP communities per AS and the community list length per AS at a well-defined point in time. Therefore, a more specific dump was targeted to illustrate the tendencies: the first dump of December 2017.

In order to visualize the evolution, for each dump and for each AS, the BGP communities advertised by that AS and the memory consumption due to the usage of BGP communities are saved into files for later reuse (an example of reuse is for classification purposes). In addition to that, the proportion of routes carrying BGP communities and the community list length for a selected dump were also written to files.

4.2.4 Data Processing Description

The collected data was processed to produce various plots, with some presented in this report, and others meant to detail the results of a query on the BGP community browser (cf section 4.5) developed for this project.

4.2.5 Deliverables

At the end of this stage, the collected data is stored in a data folder. Data corresponding to ASes queried through the same data provider are saved in the same file. A folder `img` containing plots specific to each single AS was also produced for later manipulations by the BGP communities browser website.

4.3 Web Scraping

4.3.1 Tools

The tools that were used to carry out the web scraping stage were:

- `jsoup`[39], used to parse html
- `junit`[40], used to conduct unit tests
- `jackson`[41], used in the project as a json generator

4.3.2 Description

The pages to scrap in order to obtain the semantic of the BGP communities are listed in Table 4.3. The web scraping stage of the project was quite complex, principally due to the fact that all the web pages have different structures. Even though a vast majority of the pages comes from `onestep`, they are all different, and cannot be parsed using a unique general method. Indeed, some pages present their communities as plain text, some as tables, some as a mix of plain-text and tables. For some pages, the communities are classified according to their role and usage, while for others, the communities are just gathered without any structure indicating their meaning. Therefore, a different method has been written to scrap each of the pages in Table 4.3. However, it is worth mentioning that for AS12956, a page describing the meaning of its BGP communities could not be found. For AS6830, the communities and their semantic were registered manually because the only documentation that could be found was in russian and needed to be translated before being usable. The communities of AS6453 were also registered manually. The same was done for AS6939, because the documentation states that the only community used by Hurricane Electric is the blackhole community. Due to the inherent complexity of the scraping procedure, the approach followed was test-driven development. Unit tests have been written for each of the methods used to fetch the semantic of the communities.

This extraction of the communities semantic highlighted a pattern in the usage of BGP communities, which lead to a revisit of the taxonomy initially proposed by Donnet and Bonaventure [1]. A new taxonomy was then devised and will be documented in detail in section 5.2. But globally, the main idea is to simplify the classification of communities by focusing only on the intent motivating their usage. The extracted communities and their meaning are then classified according to that new taxonomy and serialized into json format through the use of `Jackson` library.

ASN	url to communities semantic
209	https://onestep.net/communities/as209/
286	https://as286.net/AS286-communities.html
701	https://onestep.net/communities/as701/
1239	https://onestep.net/communities/as1239/
1299	https://onestep.net/communities/as1299/
2914	https://onestep.net/communities/as2914/
3257	https://onestep.net/communities/as3257/
3356	https://onestep.net/communities/as3356/
3491	https://onestep.net/communities/as3491/
5511	https://bgp.he.net/AS5511#_whois
6762	https://etabeta.noc.seabone.net/communities.html
6453	https://www.sanog.org/resources/sanogl4/sanogl4-amit-tata-communities.pdf
6830	http://www.bgptools.ru/AS6830
7018	https://onestep.net/communities/as7018/
12956	No documentation found
1273	https://onestep.net/communities/as1273/
4589	https://onestep.net/communities/as4589/
5400	https://onestep.net/communities/as5400/
6939	https://www.he.net/adm/blackhole.html
8928	https://onestep.net/communities/as8928/

Table 4.3 Pages used to get the semantic of BGP communities per AS

The motivation behind scraping the websites rather than extracting all of the meanings of the communities by hand lies in the fact that the data in these websites are updated every once in a while. For instance, AS209, AS3356 and AS5400 seems to be updated every 15 days on onestep. Notice that the structure of the page stays the same, only the content is updated, which makes it possible to continue using the scraping methods to extract the communities.

4.3.3 Deliverables

At the end of this stage, a folder containing the json files holding the communities and their semantic along with their taxonomy is delivered. These json files are very important because they are going to be loaded by the website to provide documentation about an AS and its communities.

4.4 Communities classification

4.4.1 Description

This stage consists in reading the json files produced in the previous stage (cf section 4.3) and using it to classify the data collected in the first stage. An important point to notice is that there exists communities having several meanings at once. A good illustration is given by AS4589 communities.

The community "4589:2640" is defined as a prepend of length two on all IXPs in Germany. It is ambiguous as the meaning is not unique. This community can be used at the same time for traffic engineering, for Geographical annotation and for relationship annotation. It is an *hybrid* community. For the context of this Master's thesis, the classification of the collected BGP communities will never classify them as being hybrid. Whenever several meanings are attached to a community, the priority will be given to the traffic engineering semantic, and after that to the route tagging communities. In the route tagging communities, the priority will be given to the communities expressing relationships between ASes. Every unclassified community will be tagged as being "unknown".

Python `unittest` framework [42] was used to write unit tests for the classification procedure as it is a very sensitive issue.

4.4.2 Deliverables

At the end of this stage, plots and tables illustrating the trends and tendencies in the usage of BGP communities were produced and commented in section 5.3. Various calculations on the proportion of communities belonging to a category of the taxonomy were computed.

4.5 Website building

4.5.1 Tools

The website was developed using `php` and `Twitter Bootstrap`. `Bootstrap` is a front-end open source library to design websites. A template landing page from [43] was used as a basis for the website.

4.5.2 Description

The home page of the website is a form allowing to request information about either an AS number or a community. A regular expression is used to ensure that only valid

requests are executed:

- If the user inputs something else than an AS number or a community, the user will remain within the form view and an error message will be displayed.
- If the user requests one of the AS numbers studied for this thesis, the data about the communities linked to that AS and their classification will be loaded from the json files generated in the scraping phase (cf section 4.3) and displayed in tables. The communities defined by regular expression will appear differently than the plain communities. Graphs showing the evolution of the number of different BGP communities and the evolution of memory consumption for that AS will also be displayed. Those are the graphs generated during the data processing in the data collection stage of the project.
- If the user requests an AS number that was not studied for this thesis, a message indicating that this information is not available yet is displayed.
- If the user requests a community belonging to one of the studied AS numbers, the community will be displayed with its semantic and the category it belongs to in the taxonomy. It might happen that the community entered by the user is not a plain community but rather matches a community defined by a regular expression. In that case, the regular expression is displayed with the semantic and the category of the community according to the taxonomy.
- If the user requests a community that is not recognized, a message indicating that the information about the requested community is not available yet.

The content of the page showing the results of a query is generated on the fly. This dynamic website, originally intended to run on the montefiore `ms8xx` server, makes `php` the natural choice of language with regards to the technologies supported by the `ms8xx`.

4.5.3 Deliverables

This stage consists in the production of a website making use of the scraped communities semantic and the plots generated during the data collection to display information not only about ASes but also about communities. As it was mentioned in section 4.3, the pages that are being scraped are updated very often. So the json files must be updated often as well in order for the developed website to remain up-to-date. Following this idea, a script will launch the scraping every 15 days.

CHAPTER 5

Results

This chapter details the results of the analyses conducted on the BGP communities of the dataset introduced in chapter 4. Section 5.1 will investigate how the BGP communities affects routing tables. Then, section 5.2 will present the revisited taxonomy, which was used to classify the BGP communities of the dataset. The outcome of this classification will define the trends and tendencies that will be presented in section 5.3. Finally, a discussion on the BGP community browser will close the chapter.

5.1 The importance of BGP communities

5.1.1 General results

Figure 5.1 shows the evolution of the number of ASes using BGP communities throughout the years for the data providers selected for this project. The figure suggests that an increasing number of ASes are adopting the usage of BGP community. Indeed, since 2005, a steady growth was noticed. `route-views2` has seen the number of ASes multiplied by six between 2005 and 2018. `rrc19` has seen a tremendous growth from no AS using BGP communities in the latest months of 2016 to more than 2500 ASes in early 2017. At first glance, these results may seem quite impressive. However, when they are put in perspective with the overall number of ASes documented in Figure 5.2, this becomes less impressive. To summarize, more and more ASes seem to be relying on BGP communities, generalizing the usage of this attribute and making it more and more prevailing. Proportional results are provided in section 5.1.2. The figure also points out some cases where the number of ASes drops to 0, this might be due to errors occurring during the data collection stage with `BGPstream`: error messages were prompted indicating that for some specific dates `bgpstream` was unable to read the entire data because of *incomplete dump record*. Donnet and Bonaventure [1] also observed a growth in the number of ASes using BGP communities, but for different data providers than those selected for this work.

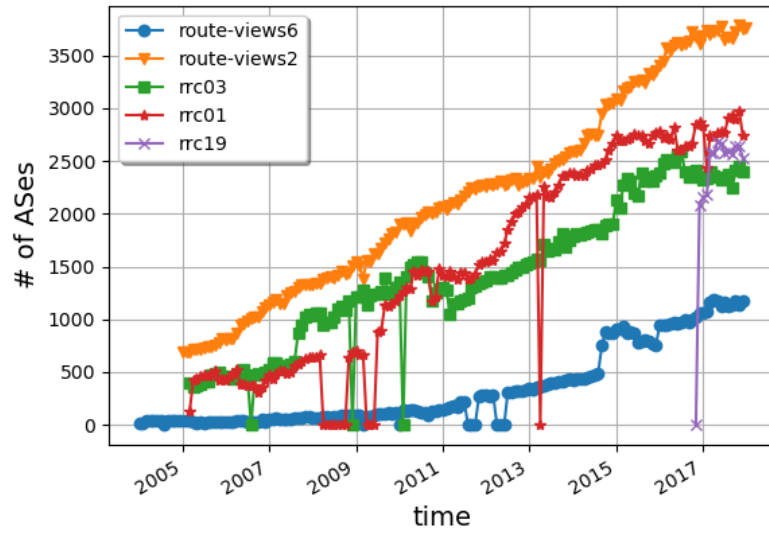


Fig. 5.1 Evolution of the number of ASes using BGP communities

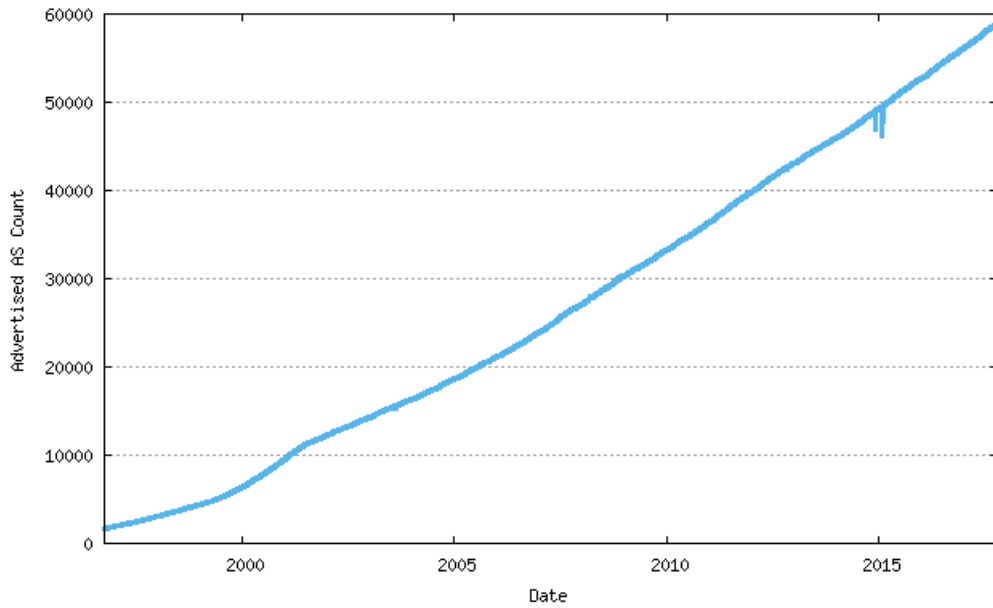
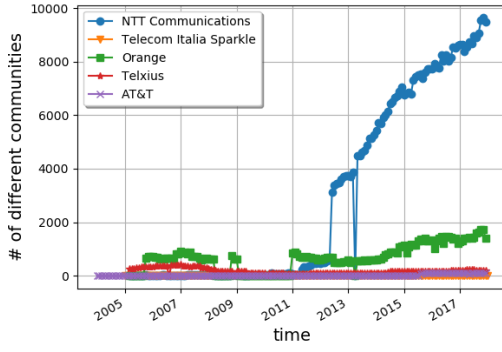
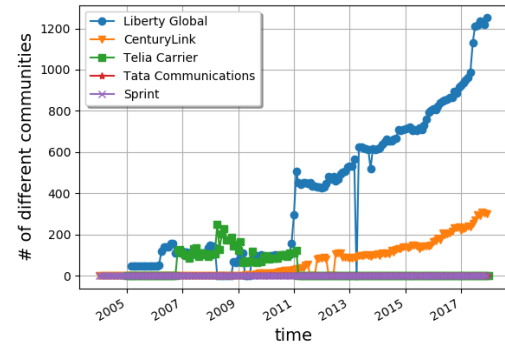


Fig. 5.2 Evolution of the number of ASes from [4]

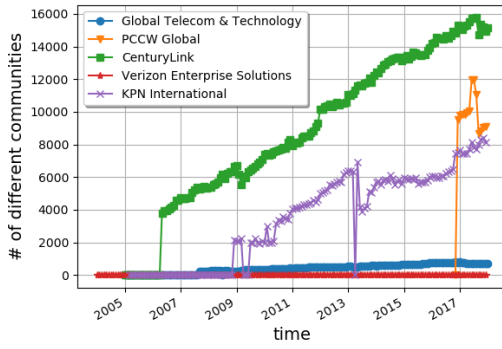
Observing the evolution at the scale of the data providers gave an interesting insight on the importance of BGP communities from a general point of view. But in order to get more details, it is also interesting to have a look at a smaller scale. Figure 5.3 is a visualization of the number of different BGP communities per AS of the dataset.



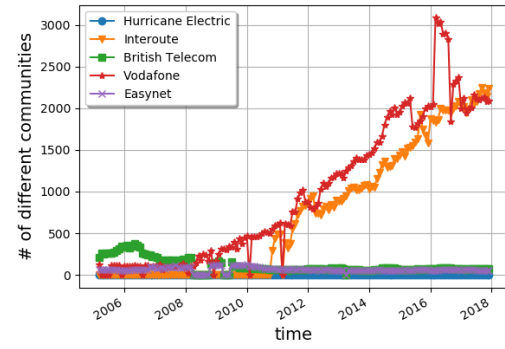
(a) Tier 1



(b) Tier 1



(c) Tier 1



(d) Tier 2

Fig. 5.3 Evolution of the number of different BGP communities

We can observe that even if there is a clear difference between ASes, the general pattern of evolution shows an increase in the different communities used per AS, with the biggest users in 2017 being NTT Communications (cf Figure 5.3a) with more than 9000 different BGP communities and Century Link (cf Figure 5.3c) with more than 15000 different BGP communities. Once again, there seems to be a steady growth in the usage of BGP communities. However, 4 ASes in the dataset seem to not follow this pattern. Telia Carrier appears to have used BGP communities between 2007 and 2011, but not anymore after that. Sprint, Tata Communications and Hurricane Electric appear to use no BGP communities at all. If we compare these numbers to the observation in [1], we can see that we were able to monitor more communities nowadays, while 10 years ago only about 7000 different communities at most were observed. However, it is important to note that [1] stays on the data provider scale, which means that their study took into account all the ASes advertising BGP communities available for these providers, while this work focuses only on a subset of ASes. Moreover, the providers selected for [1] are different from those selected for this project.

One more interesting point to study is the evolution of memory consumption due

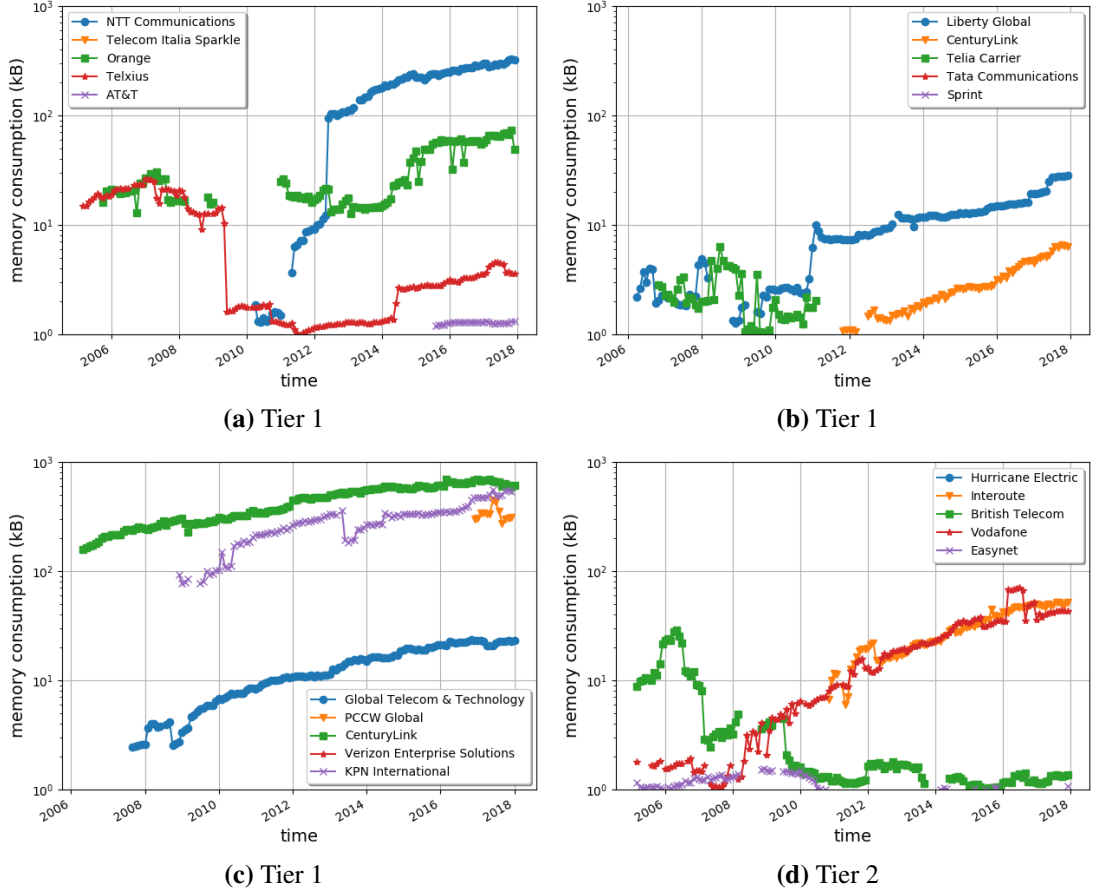


Fig. 5.4 Evolution of the memory consumption due to BGP communities

to the BGP communities, illustrated by Figure 5.4. In order to compute the memory consumption, the approach documented in [1] (which models the behavior of Quagga BGP daemon [44]) was followed. Quagga is a software suite providing BGP-4 (and other routing protocols) implementation for unix platforms. As a reminder, the BGP community attribute can either contain a unique 32 bits value or contain several 32 bits values, in which case they are called a BGP community list [1][45]. The approach followed consisted in sorting the BGP communities received so that the community values of each community list are sorted in numerical order. Then, each community list will be added to a set. The memory size will be the set of BGP community lists plus a 32 bits pointer for each prefix [1].

In [1], an increase in the memory consumption produced by the BGP communities usage was observed regardless of the data provider studied. If we examine Figure 5.4 in conjunction with Figure 5.3, we can see that whenever there is a growth in the number of different communities observed for an AS, a growth in the memory consumption due to the BGP communities usage is spotted as well. This is highlighted by the example of NTT Communications (cf Figure 5.4a) where an increase of a hundredfold was no-

ticed in the memory consumption between 2011 and 2018. Within the same period, the communities recorded for NTT Communications increased from hundreds of different communities in 2011 to more than 9000 different communities in 2018. A steady growth was also observed in Liberty Global, Century Link, KPN International, Interoute and Vodafone. Conversely, for ASes where a decrease in the number of different communities is observed, a decrease in the memory consumed by BGP communities is recorded as well. This is illustrated by the examples of Telxius (cf Figure 5.4a), Telia Carrier (cf Figure 5.4b) and British Telecom (cf Figure 5.4d) which have experienced a drop in the memory consumption resulting from the BGP communities usage. A general indication of the overall memory consumption in routing tables is given by Table 5.1. It is an overview of the size of the RIBs tables for the first dump of December 2017 for all the providers used to build the dataset. It is worth recalling that these providers contain data about thousands of ASes, which do not all use BGP communities.

Provider	Size (MB)
route-views2	132.3
route-views6	9.5
rrc01	415.4
rrc03	411.2
rrc19	462.7

Table 5.1 Size of RIBs tables per provider for the first dump of December 2017

5.1.2 Specific results

Tables 5.2 and 5.3 provide a side-by-side comparison of the percentage of routes carrying BGP communities for each AS of the dataset for the first dump of December 2006 and the first dump of December 2017. Table 5.2 lists the proportion for the tier 1 networks while Table 5.3 lists the tier 2 networks. These tables show that some ASes who did not use BGP communities in 2006 are now using BGP communities, such as Verizon or Interoute. We can generally observe an increase in the number of routes carrying BGP communities: for example Telxius went from 85.40% of routes in 2006 to 100% in 2017. It also appears that out of the 20 ASes, 4 did not use any BGP community, neither in 2006 nor in 2017: Sprint, Telia Carrier, Tata Communications and Hurricane Electric.

If we consider the routes carrying BGP communities, an example of interesting information to retrieve is the BGP community list length corresponding to each AS. Figure 5.5 shows that information for each AS of the dataset, for the first dump of

ASN	Type	Proportion (2006)	Proportion (2017)
209	Century Link	0.00%	100.00%
286	KPN International	0.00%	100.00%
701	Verizon	0.00%	99.99%
1239	Sprint	0.00%	0.00%
1299	Telia Carrier	0.00%	0.00%
2914	NTT Communications	100.00%	100.00%
3257	GTT	0.00%	100.00%
3356	Century Link	99.99%	99.99%
3491	PCCW Global	0.00%	99.99%
5511	Orange	94.82%	100.00%
6762	Telecom Italia Sparkle	100.00%	100.00%
6453	Tata Communications	0.00%	0.00%
6830	Liberty Global	100.00%	100.00%
7018	AT & T	0.00%	100.00%
12956	Telxius	85.40%	100.00%

Table 5.2 Proportion of routes carrying BGP communities for the Tier 1

ASN	AS name	Proportion (2006)	Proportion (2017)
1273	Vodafone	99.71%	100.00%
4589	Easynet	100.00%	100.00%
5400	British telecom	100.00%	99.99%
6939	Hurricane Electric	0.00%	0.00%
8928	Interoute	0.00%	100.00%

Table 5.3 Proportion of routes carrying BGP communities for the Tier 2

December 2017. This figure shows the cumulative distribution of the number of community values in each BGP community attribute in log-scale. We can see that apart from Telxius, Verizon, Telecom Italia Sparkle and AT & T, all the other ASes routes always carry more than 2 different 32 bits values. Figure 5.5a shows the examples of PCCW Global where more than 90% of the routes carry more than six 32 bits values, and NTT Communications, where 90% of the routes carry more than eight 32 bits values. Figure 5.5d shows that some routes carry more than thirty 32 bits values while in Figures 5.5a and 5.5c, community lists of length 60 are observed. Community lists of length 60 were already observed in 2007 for Linx data provider [1].

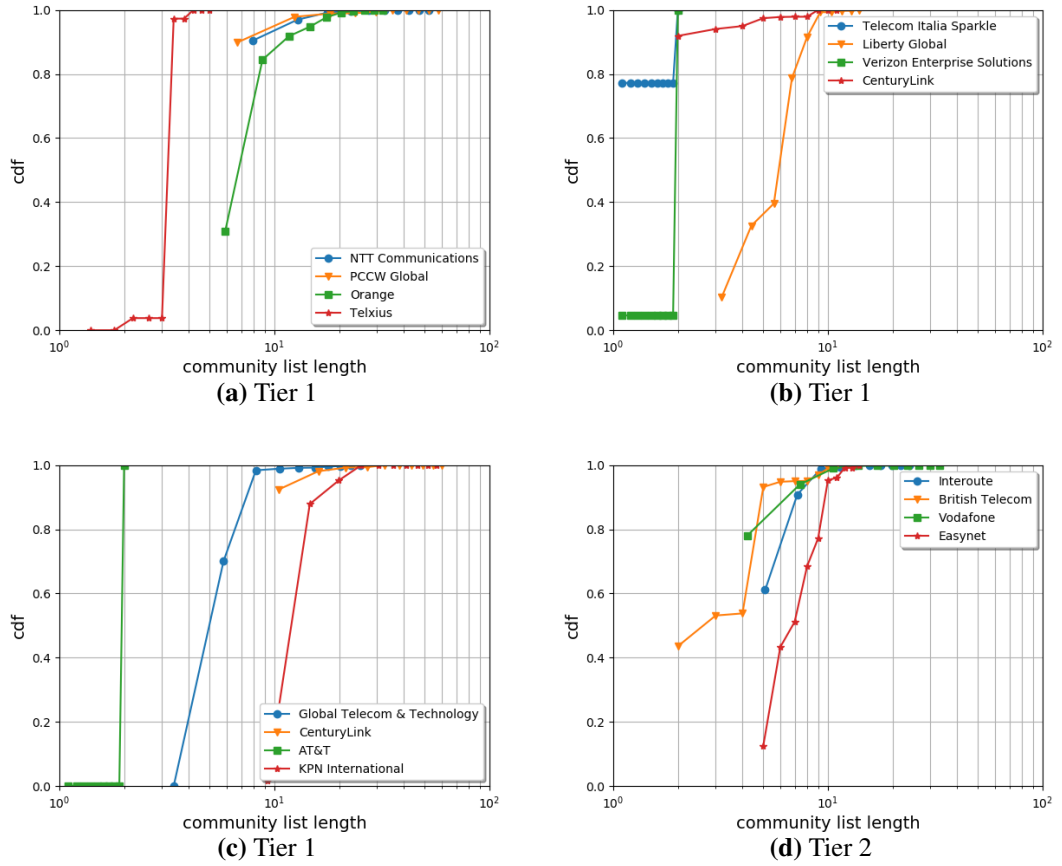


Fig. 5.5 BGP community list lengths

5.2 Revisiting the taxonomy

Donnet and Bonaventure [1] proposed a taxonomy back in 2007 to classify the usage of BGP communities. In a few words, the communities were organized in 3 main categories: the *inbound communities* (referring to communities used when a route is received on an eBGP session), the *blackhole communities* (referring to the communities used for blackholing [16]) and the *outbound communities* (inserted by the route origi-

nator for traffic engineering purposes).

However, that taxonomy highlights the way a community is introduced into a network before highlighting the motivation behind the usage of that community. Despite the fact that *Blackhole* communities, *Local Preference* communities, *Prepend* and *Announcement* communities are used for the same purpose: Traffic engineering, they belong to different categories. Local Preference communities were classified as inbound communities, while Blackhole communities had their own category. It can be interesting to revise this taxonomy to rather focus on enforcing the intent motivating their usage. The new taxonomy is presented in Figure 5.6 and it tries to put the communities used for the same purposes under a same category.

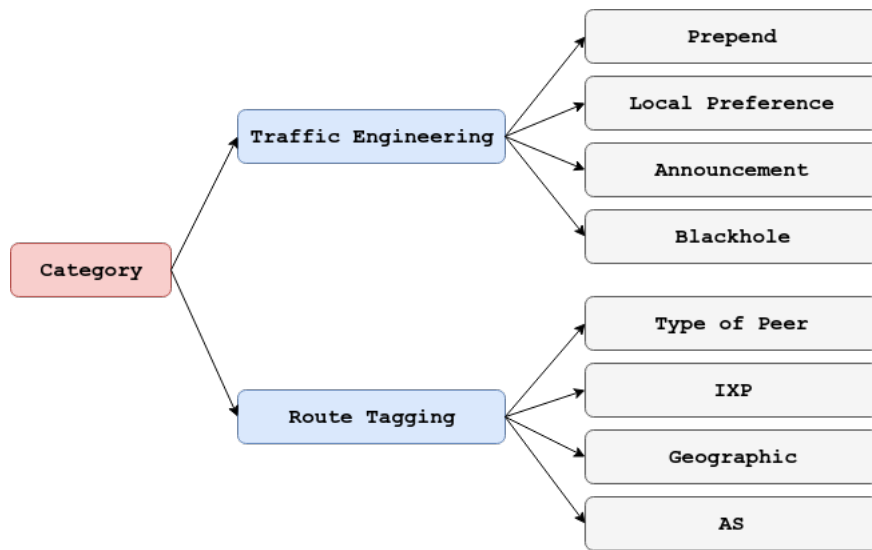


Fig. 5.6 General classification of BGP communities

As a reminder, the motivations behind the usage of BGP communities are either for *route tagging* purposes – it can be used for instance to identify the location where a route was learnt – or for *traffic engineering* purposes – to set up the local preference for example – (cf. section 3.2). It is only natural that these 2 usages become the main categories of the new taxonomy. The scraping of the websites holding the semantic of the BGP communities corresponding to the AS of the dataset revealed the subcategories of our main categories.

The Traffic Engineering category is divided into 4 subcategories:

- *Prepend*

This community is used for AS path prepending. For instance, the scraping revealed that 701:2 prepends Verizon AS number 2 times to the AS path.

- *Local Preference*

This community is used to set the local preference. For instance, 286:80 is used to lower the local preference of a route to 94. More details about how to set the local preference of a route with BGP communities can be found in section 3.2.

- *Announcement*

This community is used to filter the announcement of routes. For instance, the scraping revealed that 8928:65203 means "do not advertise to DE".

- *Blackhole*

This community is used for blackholing purposes. For instance, the scraping revealed that 3356:9999 blackholes the traffic.

The Route Tagging category is divided into 4 subcategories:

- *Type of Peer*

This community indicates the type of relationship between ASes (peer, customer, transit, provider). For instance, the scraping revealed that 3356:123 indicates a customer route.

- *IXP*

This community indicates the Internet Exchange Point where a route was learnt. For instance, the scraping revealed that 8928:65203 indicates that the route was learnt from LINX Internet Exchange.

- *Geographic*

This community indicates the geographical location where a route was learnt. For instance, the scraping revealed that 6762:15550 indicates that the route was learnt in Rio de Janeiro.

- *AS*

This community indicates the AS where a route was learnt. For instance, the scraping revealed that 209:64810 indicates that the route was learnt from Telecom Italia (AS 6762).

5.3 BGP Community Classification: trends and tendencies

5.3.1 General classification

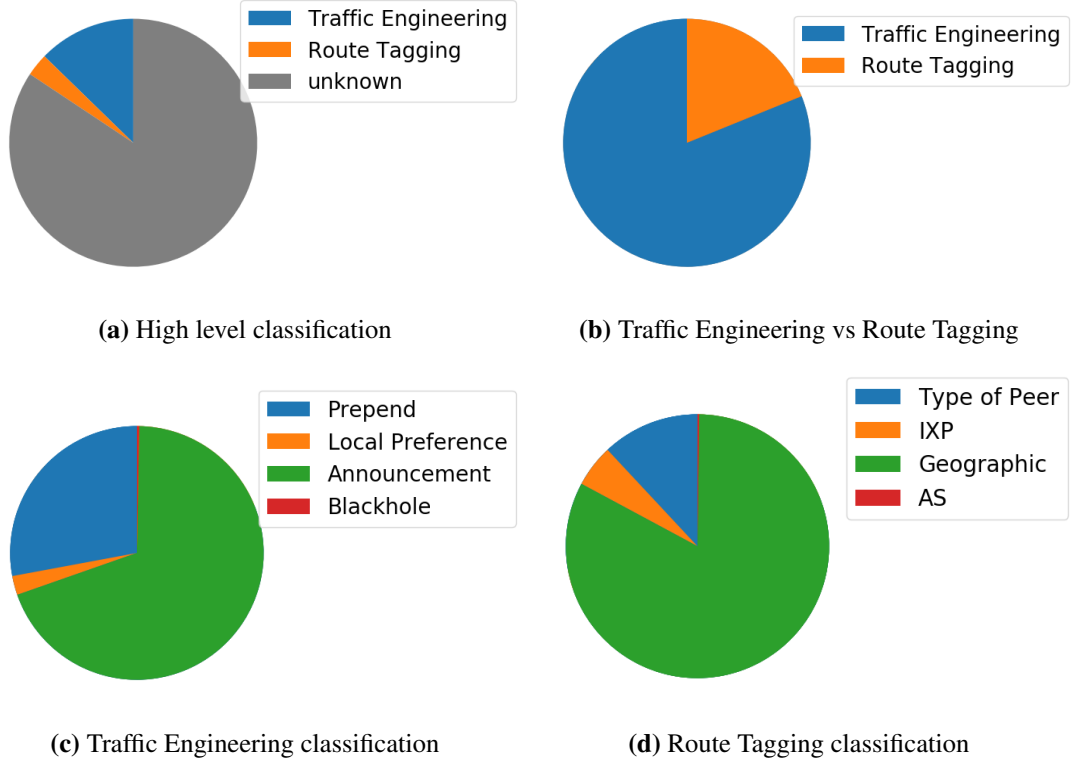


Fig. 5.7 General classification of the BGP communities

A classification of the BGP communities of the dataset using the new taxonomy was achieved and lead to the results displayed in Figure 5.7. Table 5.4 gives the measurements of the global proportion of BGP communities corresponding to this figure. The different pie charts presented in Figure 5.7 show the average proportion of BGP communities belonging to a category.

First, Figure 5.7a shows the high-level classification of the BGP communities. We can observe a predominant number of unclassified communities, accounting to 84.34% according to Table 5.4. This is due to the fact that there exists some communities whose semantic is unknown and which did not belong to the communities obtained through the scraping stage. An analysis of the classification of the BGP communities per AS will be provided thereafter in section 5.3.2 and will investigate these unclassified communities on the AS scale. If we consider the proportion of unclassified communities in [1] per data provider, we can see that compared to this project, only 78.20% of the communities were unclassified for routeviews data providers and 76.95% for ripe data providers. This can be explained by the fact that a large number of BGP community attribute

information corresponding to all of ASes of their selected providers were collected for [1]. Yet, for this project, only the information specific to a subset of ASes was collected.

Then, Figure 5.7b filters the unclassified communities to show only the proportion of *Route Tagging communities* and *Traffic Engineering communities*. We can see that more communities are used for Traffic Engineering than for Route Tagging. The results obtained in 2007 followed a similar pattern, with 23.37% of the total number of communities used for Route Tagging and 73.36% for route redistribution (Announcement and Prepending) in [1].

Figure 5.7c shows the low-level classification for the Traffic Engineering category, with the subcategories Announcement and Prepend being used the most with respectively 69.38% and 27.94% of the Traffic Engineering communities. In [1], more communities were used for Prepending rather than for Announcement purposes, with 47.43% of the total number of BGP communities used for Prepending and 25.9% for Announcement.

Figure 5.7d shows the low-level classification for the Route Tagging communities. It appears that the Geographic subcategory is the most widespread amongst the Route Tagging communities, reaching 82.64% of the Route Tagging communities. In [1], 9.11% of the total number of communities were used to specify a Geographic location.

Category	Proportion
Traffic Engineering	12.70%
<i>Prepend</i>	27.94%
<i>Local Preference</i>	2.44%
<i>Announcement</i>	69.38%
<i>Blackhole</i>	0.25%
Route Tagging	2.96%
<i>Type of Peer</i>	11.96%
<i>IXP</i>	5.20%
<i>Geographic</i>	82.64%
<i>AS</i>	0.20%
Unclassified	84.34%

Table 5.4 Average repartition of BGP communities corresponding to Figure 5.7

5.3.2 Classification per AS

Figures 5.8 and 5.9 show the classification of BGP communities per AS number belonging to the dataset. We can see that for AS1239, AS1299, AS6453 and AS6939 there is

no value because they do not use any BGP communities. Figures 5.8 takes into account the unclassified communities, while Figure 5.9 only considers the classified communities.

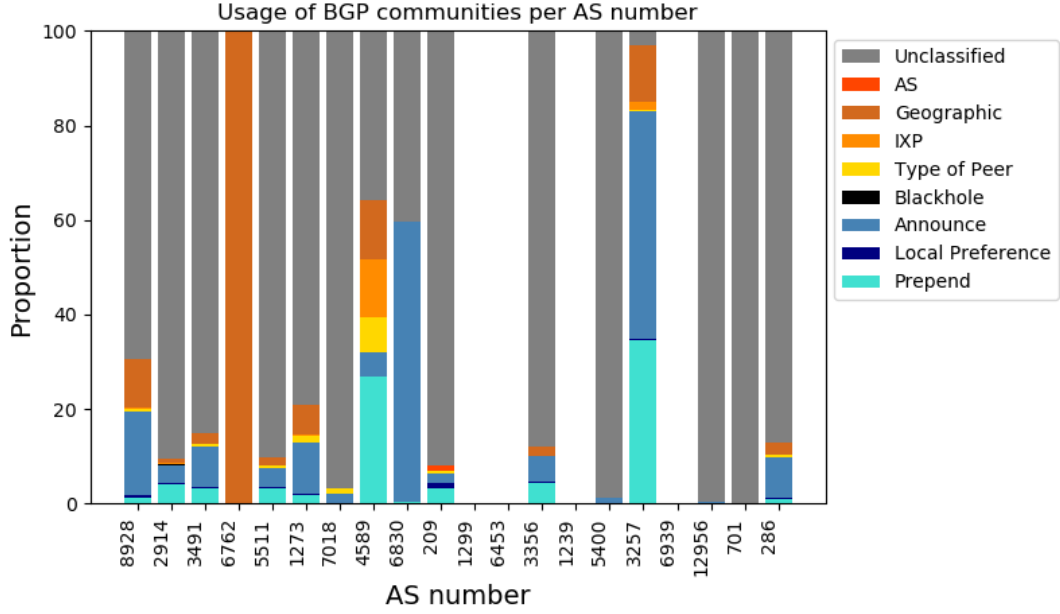


Fig. 5.8 Classification of BGP communities per AS

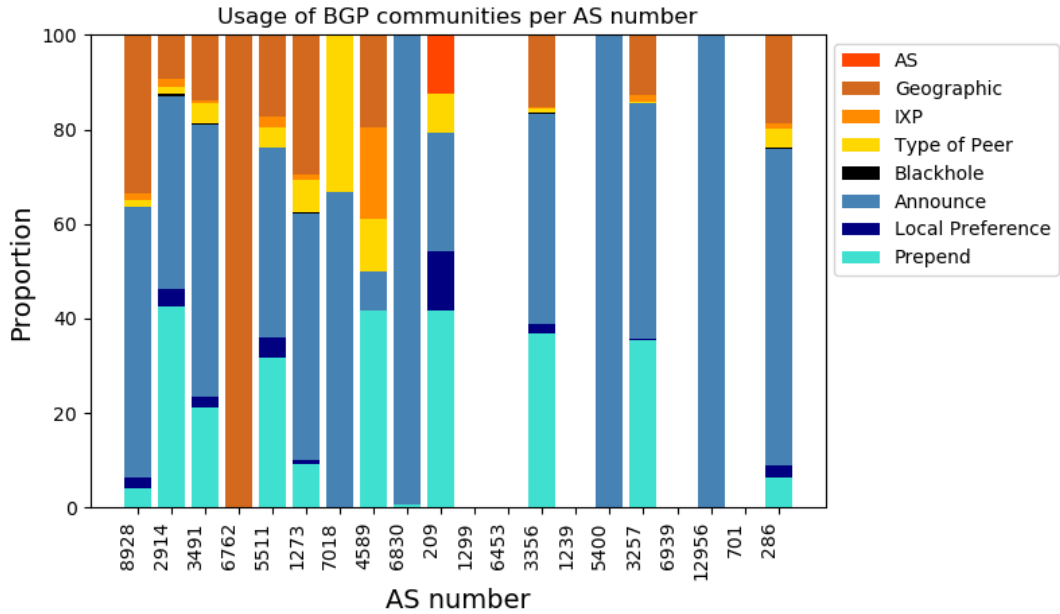


Fig. 5.9 Classification of recognized BGP communities per AS

Figures 5.9 and 5.8 indicate that for almost all ASes, the majority of communities are unclassified. None of the communities of AS 701 were recognized even though the scraping procedure extracted the semantic of all the documented communities of

that AS. Similarly, only a few communities of AS7018 could be classified. This suggests the existence of other communities than the communities scrapped in the previous stage attached to the routes of the ASes of the dataset. A closer look into their communities confirmed that assumption. The communities observed for AS701 for December 2017 were: 701:1020, 701:333, 701:444 which were not part of the information available about the communities of that AS. Similarly, the majority of AS7018 communities were not provided by the scrapped websites, such as 7018:35110, 7018:38001, 7018:39231. Besides, the communities observed in an AS might be coming from other ASes, but as we only scrapped websites documenting the communities of a limited number of ASes, we could not cover all existing communities. This can be illustrated by AS2914. Various communities were observed for that AS such as: 45896:63101, 54113:79, 6453:12000, 6762:1571, corresponding to different ASes and none of these communities are being documented on the scrapped websites. We can see that only AS6762 got 100% of its communities classified, and all of the communities observed for that AS belong to the Route Tagging Geographic category. Many observations can be made from Figure 5.9. For instance, we can see that the recognized communities from AS6830 and AS5400 are all used for announcement.

ASN	Classified(%)	Unclassified(%)
209	8.03%	91.97%
286	12.87%	87.13%
701	0.00%	100.00%
1239	-	-
1299	-	-
2914	9.41%	90.59%
3257	97.08%	2.92%
3356	11.92%	88.08%
3491	14.80%	85.20%
5511	9.88%	90.12%
6453	-	-
6762	100.00%	0.00%
6830	59.63%	40.37%
7018	3.30%	96.70%
12956	0.52%	99.48%

Table 5.5 Proportion of classified BGP communities per Tier 1

Table 5.5 and Table 5.6 give measurements on the proportion of classified and unclassified communities per AS belonging to the dataset. We can see from the tables that the most successful classifications were for AS6762 with 100% of the communities classified, which corroborates what Figure 5.8 already demonstrated, followed by

ASN	Classified(%)	Unclassified(%)
1273	20.84%	79.16%
4589	64.29%	35.71%
5400	1.33%	98.67%
6939	-	-
8928	30.71%	69.29%

Table 5.6 Proportion of classified BGP communities per Tier 2

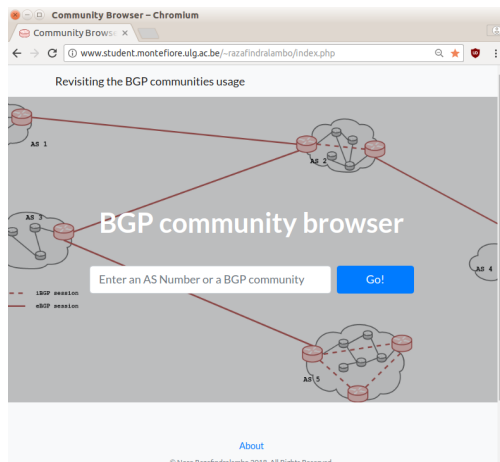
AS3257 with 97.08% of the communities being classified. In third position we have AS4589 with 64.29%. The less successful classifications were AS5400, with 1.33%, AS12956 with 0.52%, and AS701 with 0% of classified communities.

5.4 BGP Community Browser: a website

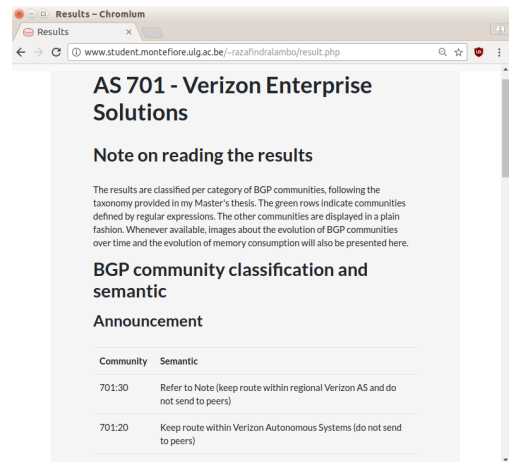
The final outcome of this project was the development of a website, meant to behave as a BGP community browser. The website has been developed and is available here:

http://www.montefiore.ulg.ac.be/~bgp_communities/

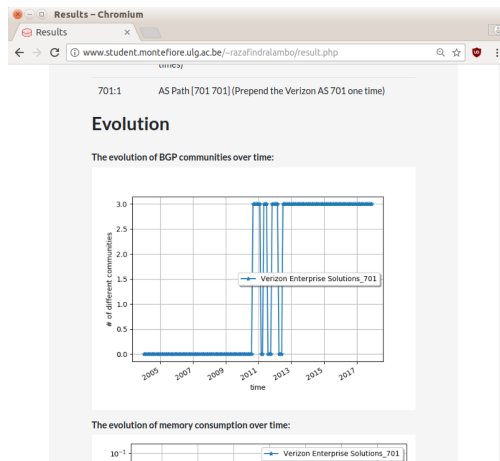
Figure 5.10 shows screenshots of the developed website. Figure 5.10a shows the home page of the website. A form allows to introduce a query for an AS number or a community. Figures 5.10b, 5.10c show a successful result for an AS query. The table of communities recognized by that AS is displayed along with a graph showing the evolution of the number of different BGP communities for that AS. Figure 5.10d shows an unsuccessful query. If the AS number is not available, the user will see that page. Figure 5.10e shows a successful result for a BGP community query. The community is displayed with its semantic and its classification. If the community was not found, the message in 5.10f is displayed.



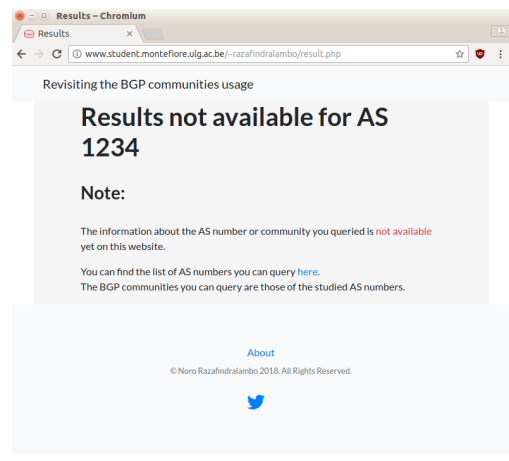
(a) Home page



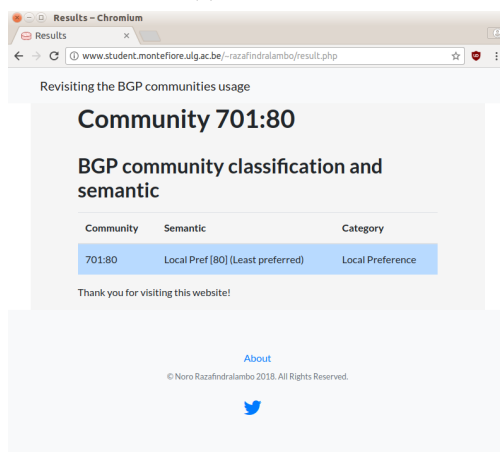
(b) AS result



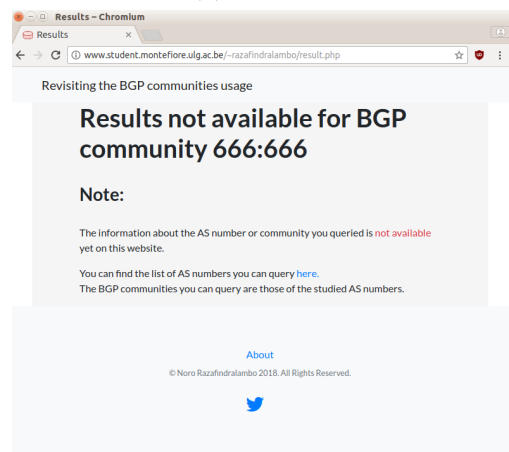
(c) AS result



(d) AS result



(e) Community result



(f) Community result

Fig. 5.10 BGP community browser

CHAPTER 6

Conclusion

This Master's thesis focused on the BGP community attribute. This attribute groups together destinations for which the same routing decisions can be applied. It can be used to add information to a given route, or to take action on the routing policies.

In 2007, Donnet and Bonaventure [1] studied the usage of the BGP community attribute and proposed a taxonomy as a structured way to describe the various communities. They manually collected BGP communities information that were publicly available, and they built a database tagged using their taxonomy. However, more than a decade has passed without any up-to-date report classifying the various BGP communities available today, underlining the need for a more modern insight on the usage of this attribute.

This document contributed to address this issue by underlining the importance of that attribute. The study showed that there is an increasing number of ASes using BGP communities. This attribute appears to be more and more pervasive as the study revealed that among the ASes using BGP communities, almost all the routes are carrying BGP communities today, while only a fraction of routes were carrying BGP communities in 2006. The study also exposed that the variation in the size of routing tables is impacted by the usage of BGP communities and can be linked with the number of different communities observed.

The taxonomy introduced by Donnet and Bonaventure [1] was revised to better capture the motivation behind the usage of BGP communities, by grouping together under a same category the communities that are used for the same general purpose. Information about the communities of the ASes selected for this project were extracted from different websites and centralized in a database tagged with the revised taxonomy. This database was a key factor leading to the classification of the BGP communities ob-

served in the dataset and contributing to the conception of a website documenting the BGP communities.

Thanks to this revisited taxonomy, this project achieved to uncover the recent trends and tendencies ruling the usage of BGP communities and to quantify the communities belonging to a given category. The results showed that more communities are used for Traffic Engineering than for Route Tagging, with 69.38% of the Traffic Engineering communities being used to influence the Announcement of the routes and 82.64% of the Route Tagging communities being used to indicate the Geographic Location where a route was learnt.

A significant step forward has been accomplished through the development of a website (http://www.montefiore.ulg.ac.be/~bgp_communities/) allowing researchers to obtain easily communities information that are in general not straightforward to glean. Indeed, the BGP communities information was extracted from different websites, each presenting their communities in a different format: sometimes in tables, sometimes in plain text, sometimes using the mix of both tables and plain text. In order to provide a more effective and straightforward way to research the communities, the developed website presents the information in a unique normalized format. Moreover, there is a further advantage in the usage of that website: the database constituting its basis is collected programmatically, in contrast to [1] where it was collected manually. As the information about BGP communities may change over time, the website is developed so that the content is updated on a regular basis. However, this website is in a sense incomplete, as it currently contains only information about the ASes studied for this work while there are still a large number of ASes publicly disclosing information about their communities. Being able to gather all the available information about the BGP communities of various ASes at a single place would considerably ease the usage of BGP communities and enhance the research.

Future work could focus on enriching the existing database in order to be able to identify more and more communities, and to reduce the proportion of unclassified communities. Towards this end, more ASes should be added to the dataset. Measurements and analyses following the approach described in this thesis could be conducted to study the usage of their communities. Another direction of research would be to study the large BGP community attribute.

REFERENCES

- [1] B. Donnet and O. Bonaventure, “On bgp communities,” *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 55–59, April 2008.
- [2] J. W. Stewart, III, *BGP4: Inter-Domain Routing in the Internet*. Addison-Wesley Longman Publishing Co., Inc., 1998.
- [3] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, “Internet inter-domain traffic,” *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 75–86, August 2010.
- [4] “The 16-bit as number report,” accessed: 2018-05-23. [Online]. Available: <http://www.potaroo.net/tools/asn16/>
- [5] “Savvis community attributes,” accessed: 2017-11-26. [Online]. Available: <https://onestep.net/communities/as3561/>
- [6] “Bgp communities,” accessed: 2017-11-26. [Online]. Available: <https://onestep.net/communities/as4436/>
- [7] V. Giotsas, “Bgpstream: Support for large bgp communities,” 2017, accessed: 2018-05-11. [Online]. Available: <https://github.com/CAIDA/bgpstream/issues/54>
- [8] Y. Rekhter, T. Li, and S. Hares, “A border gateway protocol 4 (bgp-4),” Internet Engineering Task Force, RFC 4271, January 2006.
- [9] M. Caesar and J. Rexford, “BGP routing policies in ISP networks,” vol. 19, pp. 5 – 11, 12 2005.
- [10] R. A. Steenbergen and T. Scholl, “Bgp communities: A guide for service provider networks,” 2013, accessed: 2017-10-07. [Online]. Available: <https://fr.slideshare.net/RichardSteenbergen/bgp-communities-a-guide-for-service-provider-networks>
- [11] G. M. Trotter, “Terminology for forwarding information base (FIB) based router performance,” Internet Engineering Task Force, RFC 3222, December 2001.

- [12] C. Villamizar, R. Chandra, and R. Govindan, “Bgp route flap damping,” Internet Engineering Task Force, RFC 2439, November 1998.
- [13] V. Giotsas, M. Luckie, B. Huffaker, and k. claffy, “Inferring complex ASrelationships,” in *Proc. ACM Internet Measurement Conference (IMC)*, November 2014.
- [14] B. Quoitin, S. Uhlig, and O. Bonaventure, “Using redistribution communities for interdomain traffic engineering,” October 2002.
- [15] B. Quoitin and O. Bonaventure, “A survey of the utilization of the BGP community attribute,” Internet Engineering Task Force, Internet Draft (work in progress) draft-quoitin-bgp-comm-survey-00, February 2002.
- [16] V. Giotsas, C. Dietzel, G. Smaragdakis, A. Feldmann, A. Berger, and E. Aben, “Detecting peering infrastructure outages in the wild,” in *ACM SIGCOMM*, August 2017.
- [17] C. Dietzel, A. Feldmann, and T. King, “Blackholing at IXPs: On the effectiveness of DDoS mitigation in the wild,” in *PAM*, 2016.
- [18] V. Giotsas, G. Smaragdakis, C. Dietzel, P. Richter, A. Feldmann, and A. Berger, “Inferring bgp blackholing activity in the internet,” in *Proceedings of ACM IMC 2017*, November 2017.
- [19] R. Chandra, P. Traina, and T. Li, “BGP communities attribute,” Internet Engineering Task Force, RFC 1997, August 1997.
- [20] W. Kumari, R. Bush, H. Schiller, and K. Patel, “Codification of AS 0 processing,” Internet Engineering Task Force, RFC 7607, August 2015.
- [21] J. Haas and J. Mitchell, “BGP support for four-octet autonomous system (AS) number space,” Internet Engineering Task Force, RFC 7300, July 2014.
- [22] E. Chen and T. Bates, “An application of the bgp community attribute in multi-home routing,” Internet Engineering Task Force, RFC 1998, August 1996.
- [23] T. King, C. Dietzel, J. Snijders, G. Doering, and G. Hankins, “Blackhole community,” Internet Engineering Task Force, Tech. Rep. 7999, October 2016.
- [24] P. Traina, “Autonomous system confederations for BGP,” Internet Engineering Task Force, RFC 1965, June 1996.
- [25] L. Cittadini, G. Di Battista, and M. Patrignani, “MPLS virtual private networks,” in *Recent Advances in Networking, Volume 1*, ser. ACM SIGCOMM eBook, H. Haddadi and O. Bonaventure, Eds. ACM, 2013, pp. 275–304. [Online]. Available: <http://www.sigcomm.org/content/ebook>

- [26] S. Sangli, D. Tappan, and Y. Rekhter, “Bgp extended communities attribute,” Internet Engineering Task Force, RFC 4360, February 2006.
- [27] Q. Vohra and E. Chen, “BGP support for four-octet AS number space,” Internet Engineering Task Force, RFC 4893, May 2007.
- [28] —, “BGP support for four-octet autonomous system (AS) number space,” Internet Engineering Task Force, RFC 6793, December 2012.
- [29] J. Heitz, J. Snijders, K. Patel, I. Bagdonas, and N. Hilliard, “Bgp large communities attribute,” Internet Engineering Task Force, RFC 8092, February 2017.
- [30] J. Snijders, J. Heasley, and M. Schmidt, “Use of bgp large communities,” Internet Engineering Task Force, RFC 8195, June 2017.
- [31] “Bgpstream - an open source framework,” accessed: 2018-05-11. [Online]. Available: <https://bgpstream.caida.org/>
- [32] “Bgpstream - data providers,” accessed: 2018-05-11. [Online]. Available: <https://bgpstream.caida.org/data>
- [33] “Pickle - python object serialization,” accessed: 2018-05-11. [Online]. Available: <https://docs.python.org/2/library/pickle.html>
- [34] “Matplotlib - a python plotting library,” accessed: 2018-05-11. [Online]. Available: <https://matplotlib.org/>
- [35] “Tier 1 network,” accessed: 2018-05-11. [Online]. Available: https://en.wikipedia.org/wiki/Tier_1_network
- [36] “Tier 2 network,” accessed: 2018-05-11. [Online]. Available: https://en.wikipedia.org/wiki/Tier_2_network
- [37] “University of oregon route views project,” accessed: 2018-05-11. [Online]. Available: <https://matplotlib.org/>
- [38] “Ripe network coordination centre,” accessed: 2018-05-11. [Online]. Available: <https://www.ripe.net/>
- [39] “Jsoup - a java html parser,” accessed: 2018-05-11. [Online]. Available: <https://jsoup.org/>
- [40] “JUnit - a unit testing framework,” accessed: 2018-05-11. [Online]. Available: <https://junit.org/junit4/>

- [41] “Jackson project - a json library for java,” accessed: 2018-05-11. [Online]. Available: <https://github.com/FasterXML/jackson>
- [42] “unittest - a unit testing framework for python,” accessed: 2018-05-11. [Online]. Available: <https://docs.python.org/2/library/unittest.html>
- [43] “Bootstrap - a landing page template,” accessed: 2018-05-11. [Online]. Available: <https://startbootstrap.com/template-overviews/landing-page/>
- [44] “Quagga routing suite,” accessed: 2018-05-25. [Online]. Available: <https://www.quagga.net/>
- [45] “Understanding bgp communities, extended communities, and large communities as routing policy match conditions,” accessed: 2017-10-07. [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-bgp-communities-extended-communities-match-conditions-overview.html
- [46] T. Kris Foster, “Application of bgp communities,” *The Internet Protocol Journal*, vol. 6, no. 2, pp. 2–9, June 2003.
- [47] G. Lixin, “On inferring autonomous system relationships in the internet,” *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, December 2001.
- [48] E. Karpilovsky, M. Caesar, J. Rexford, A. Shaikh, and J. van der Merwe, “Practical network-wide compression of ip routing tables,” *IEEE Transactions on Network and Service Management*, vol. 9, no. 4, pp. 446–458, December 2012.
- [49] V. Giotsas and S. Zhou, “Inferring AS relationships from BGP attributes,” *CoRR*, vol. abs/1106.2417, August 2011.