An Analysis of Interdomain Prefix Visibility

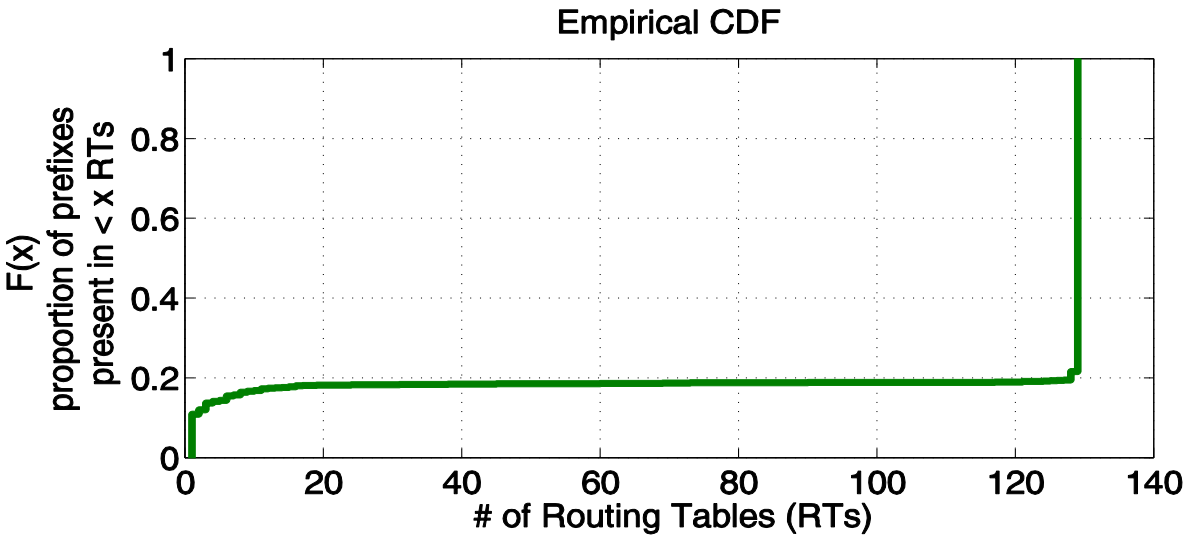
Andra Lutu[1,2] & Marcelo Bagnulo[2]
IMDEA Networks[1], University Carlos III Madrid[2], Spain

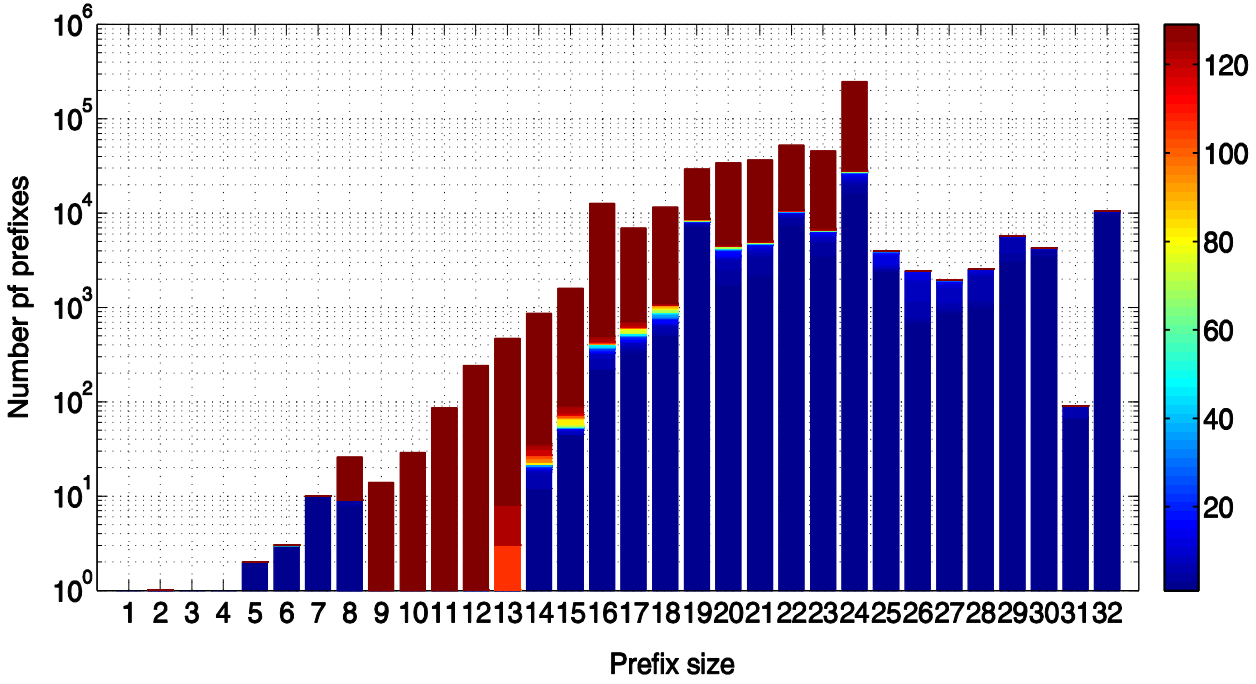
Interdomain prefix visibility – reality check

- Interdomain prefix reachability:
  - ***The naïve view:*** full global interconnection, every route is distributed to every router
  - ***Reality check:*** this is NOT what we can see in the routing tables
- **Questions: How many prefixes are in some but not all the ”full” routing tables? Can we characterize them?**
- Analyze all BGP routing data from ***RouteViews*** and ***RIPE Routing Information Service (RIS)*** projects
  - All together there are 24 different RT collection points
  - More than 130 different ASes periodically dump their *entire* routing tables

Interdomain Prefix Visibility – BGP Data

- Full Routing Table - Contains almost all the prefixes injected in the interdomain
- Polishing the full routing tables for our study
  - No bogons/martians present
    - Use up to date bogon filters
  - No MOAS prefixes
    - Check the Origin AS for each prefix identified
  - No Internal routes
    - Not considering prefixes only present in 1 RT with an AS-Path of length 1
  - No transient routes
    - Filter the prefixes that are not consistently appearing in time
      - Take two routing feeds 8hours apart and compare the prefix sets





Interdomain prefix visibility

- We find that not all the full RTs identified contain **all** the prefixes injected in the interdomain
- See **CDF** for prefix visibility in the RTs sample from 23.10.2012
- 129 unique monitors

BGP routing data analysis

- Sampling time 23.10.2012
  - 129 full RTs from RIPE RIS and RouteViews
  - ASes distributed over all the RIRs:
    - 9/129 ASes in LACNIC
    - 14/129 in APNIC
    - 37/129 in ARIN
    - 68/129 in RIPE NCC
- **Limited Visibility** prefix = present in *less than 95% of the monitors* in the sample
- A total of 512.000 prefixes identified
  - 415.576 High-Visibility prefixes (HV)
  - 98.253 Limited-Visibility prefixes (LV)

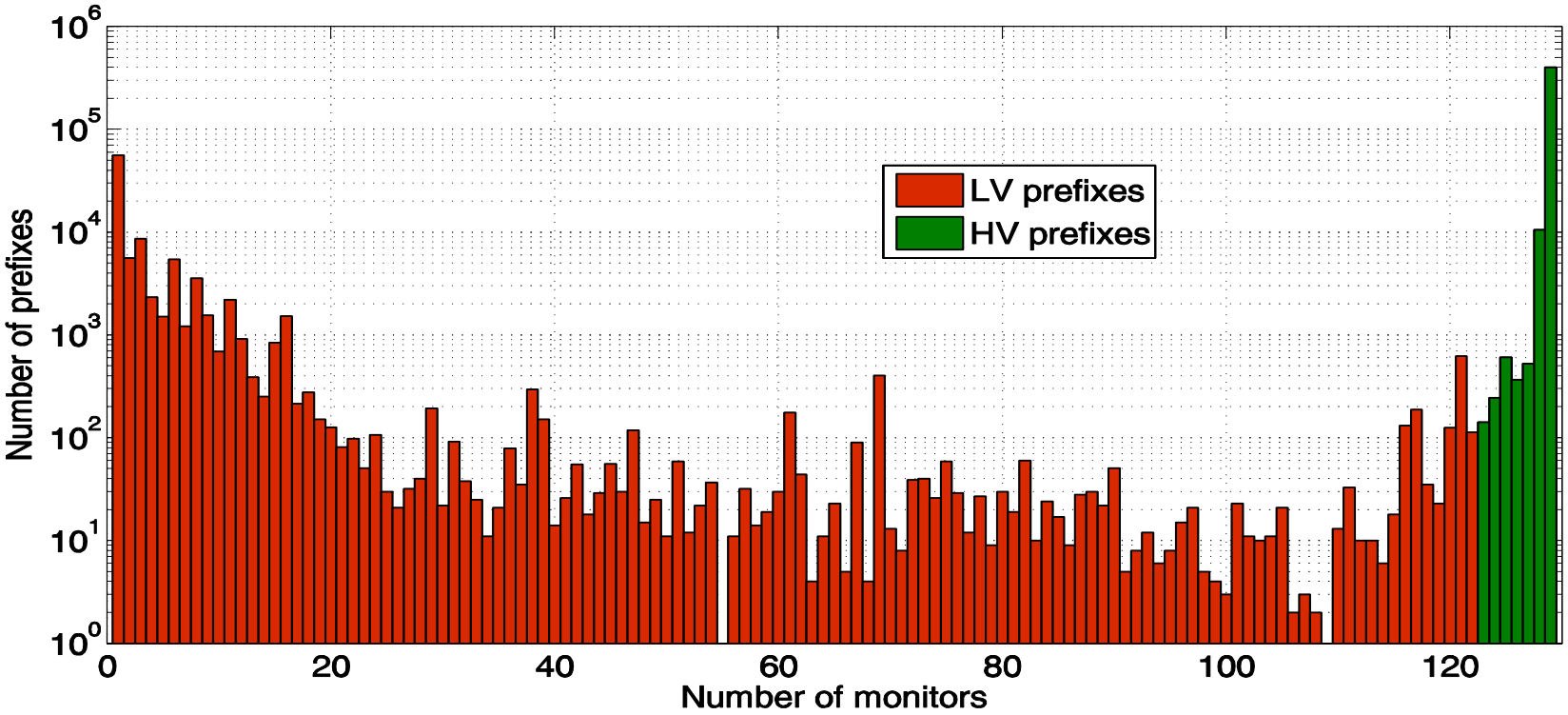
Dark Prefixes

- Dark prefixes are the LV prefixes that are not covered by any HV prefix
- This would constitute address space that is not globally reachable
  - In 2012.10.23 there were ~2.400 dark prefixes in the LV prefix set

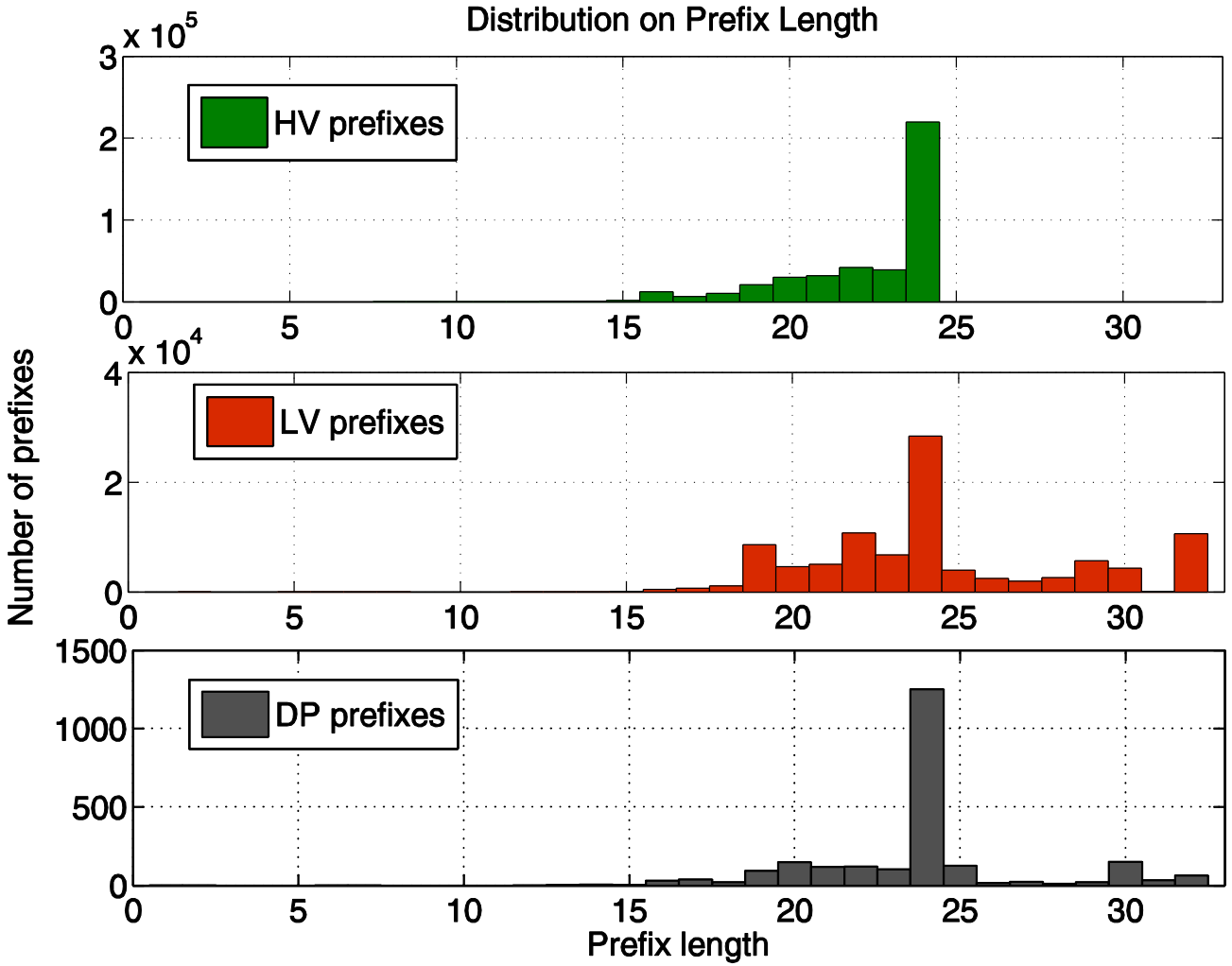
- We focus on these three prefix sets we identify:
  - High Visibility
  - Limited Visibility
  - Dark Prefixes

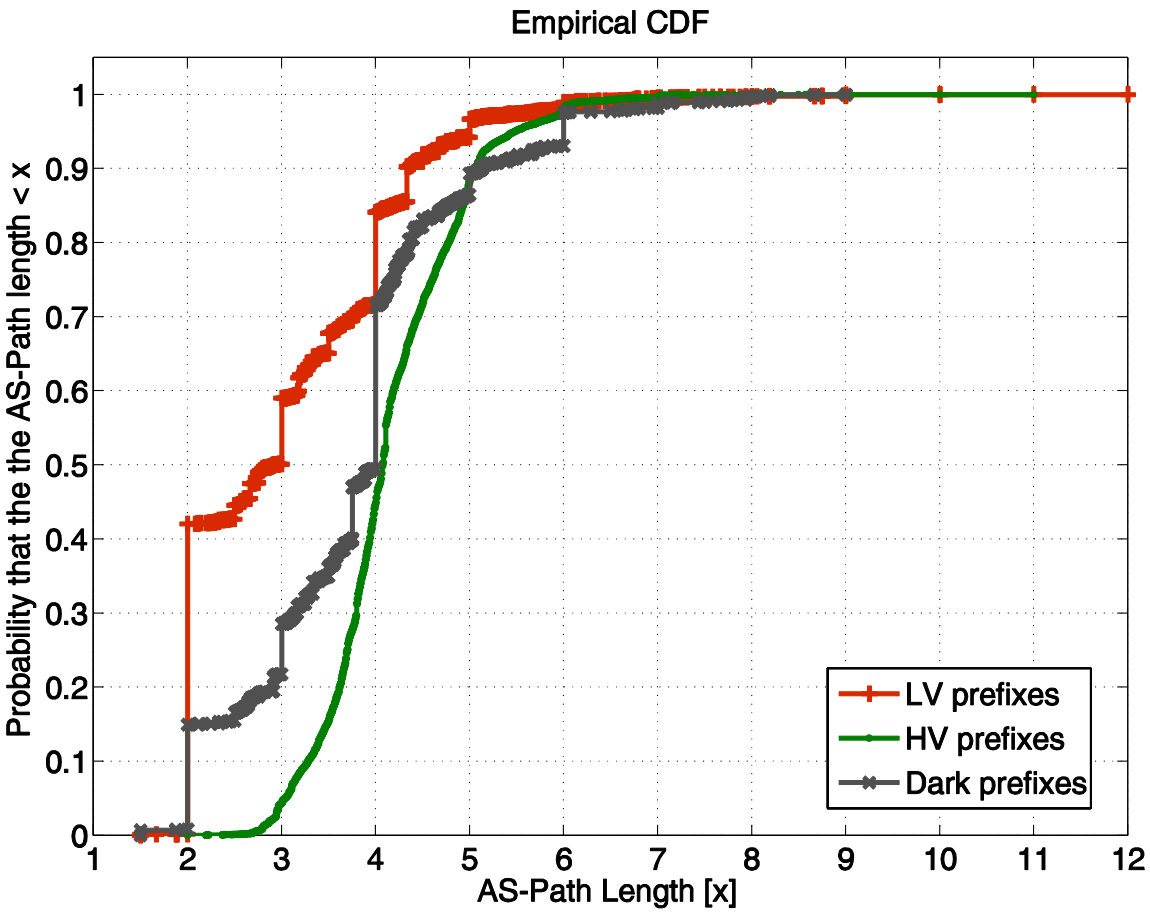
Prefix visibility as of 23.10.2012

- Visibility distribution: # of LV prefixes present in *n* monitors, where n = 1, … 129
  - Logscale on the Y axis



Prefix visibility – distribution on prefix length

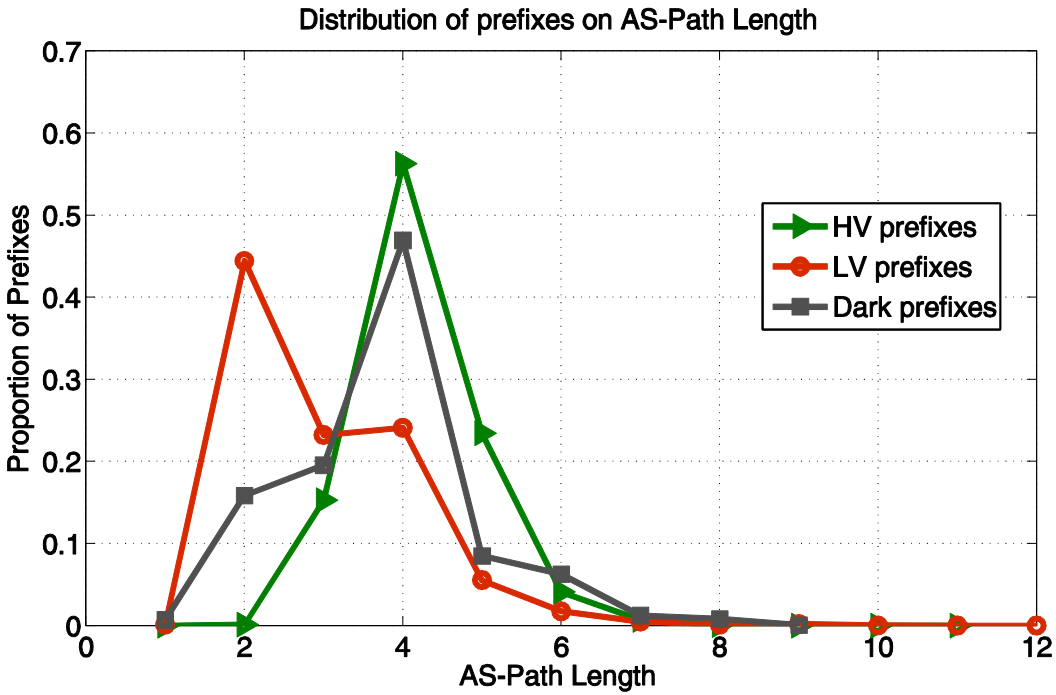




AS-Path length

- The per set mean AS-Path length (no prepending considered):
  - LV prefixes – 3.02
  - HV prefixes – 4.16
  - Dark prefixes – 3.75

AS-Path length



- Observe that for this data set, the AS-Path length for the LV prefixes is much smaller than the AS-Path length for the HV prefixes

Origin ASes for the LV prefixes

- Identified 3.570 different ASes originating the LV prefixes identified on 2012.10.23:
  - 14% in LACNIC (~493 ASes)
  - 30.5% in APNIC (~1.081 ASes)
  - 30.1% in RIPE (~1.068 ASes)
  - 22.4% in APNIC (~795 ASes)
  - 1.1% in AFRINIC (~42 ASes)

What are these prefixes?

- We are looking to explain this phenomena:
  - Is it something the origin AS intended or is it something that the AS is suffering?
- All the results of this study are made available online

visibility.it.uc3m.es

  - *Up to date information on LV announced by each AS*
  - *Check to see if an AS is originating LV prefixes*
  - *Retrieve those prefixes and see if there are any Dark prefixes within the set*
- Please provide feedback!
  - Short form that you can fill in and send

How does this work?

visibility.it.uc3m.es

Limited Visibility Prefixes

Retrieve the limited visibility prefixes per origin AS

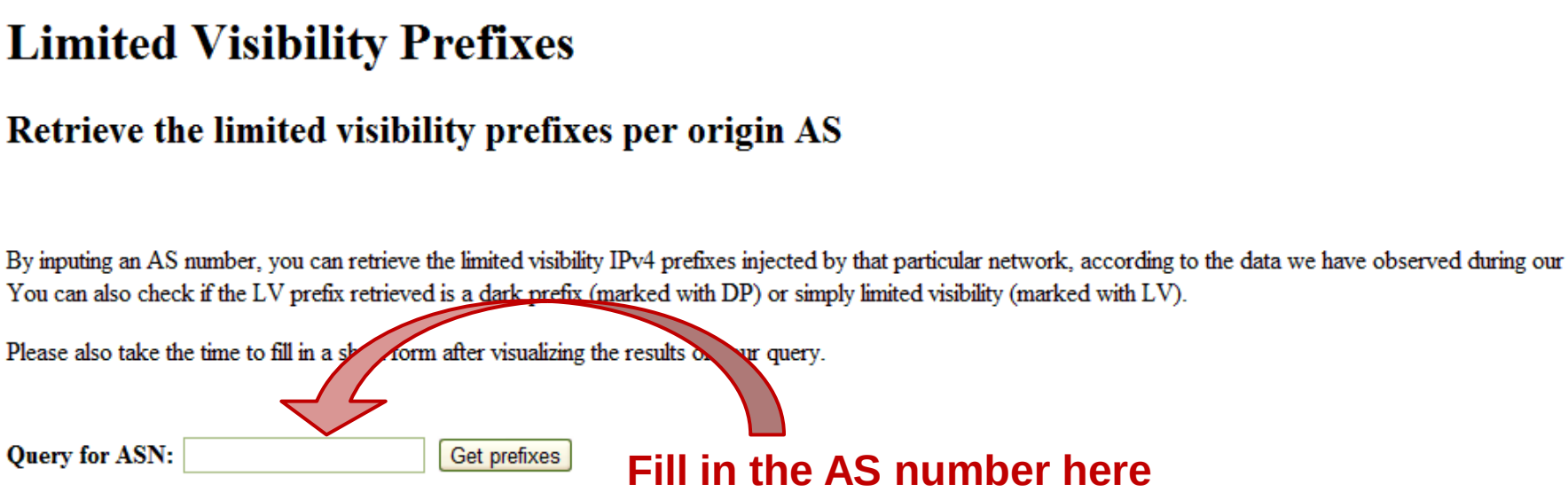
By inputing an AS number, you can retrieve the limited visibility IPv4 prefixes injected by that particular network, according to the data we have observed during our study. You can also check if the LV prefix retrieved is a dark prefix (marked with DP) or simply limited visibility (marked with LV).

Please also take the time to fill in a short form after visualizing the results of your query.

Query for ASN: Get prefixes

How does this work?

visibility.it.uc3m.es



How does it work?

visibility.it.uc3m.es

- Example of output:

Please take the time to fill in the form concerning the prefixes listed below!

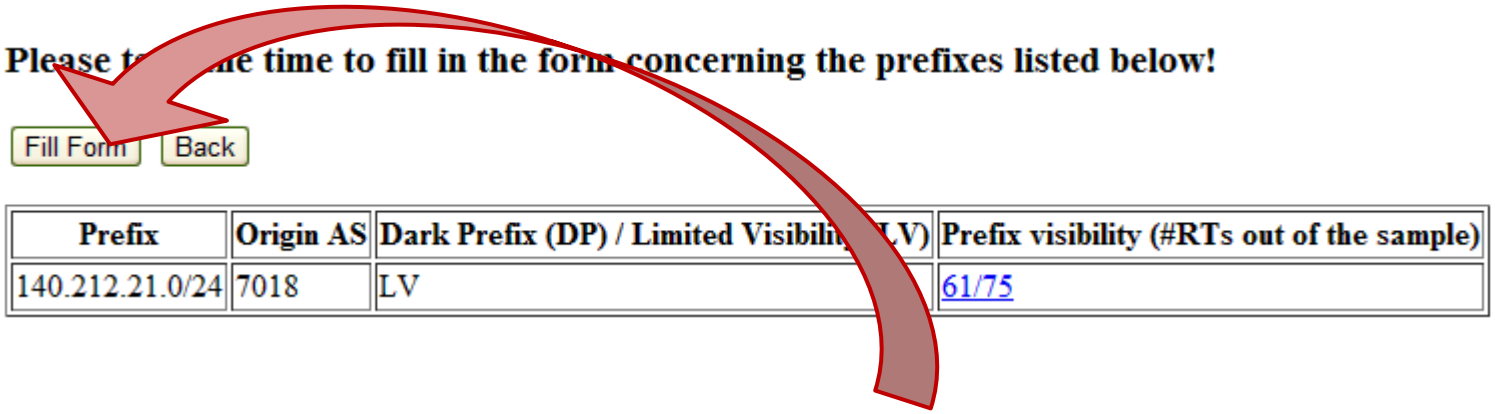
Fill Form | Back

Prefix	Origin AS	Dark Prefix (DP) / Limited Visibility (LV)	Prefix visibility (#RTs out of the sample)
140.212.21.0/24	7018	LV	61/75

How does it work?

visibility.it.uc3m.es

- Example of output:



Please t[illegible]e time to fill in the form concerning the prefixes listed below!

Fill Form | Back

Prefix	Origin AS	Dark Prefix (DP) / Limited Visibili[illegible]LV)	Prefix visibility (#RTs out of the sample)
140.212.21.0/24	7018	LV	61/75

Next step: fill in form!

How does it work?

- Form takes just a few minutes, we appreciate any level of information that can be provided!

- All the information on the LV prefixes queried in the webpage is updated on a daily bases, using the latest available routing information
- Plan to provide via email an anonymized report at the end of the survey

visibility.it.uc3m.es

QUESTIONS?

andra.lutu@imdea.org

marcelo@it.uc3m.es