Route Policy Verification

Alexander Azimov
<aa@highloadlab.com>
Highload Lab

BIG BROTHER
IS WATCHING
YOU!

Plan

1. Why we need route policy data?

   BGP Route Prediction, AS Design

2. What is wrong with Route Policy from RR?

   Physical link discovery, classterization

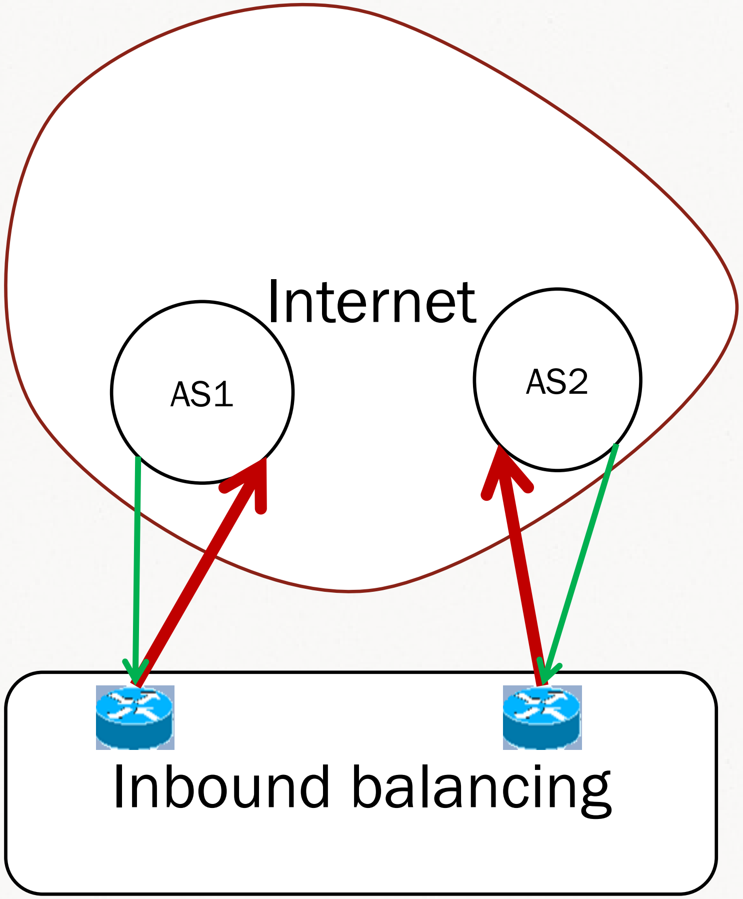
3. How have we made verification?

   Active route policy discovery

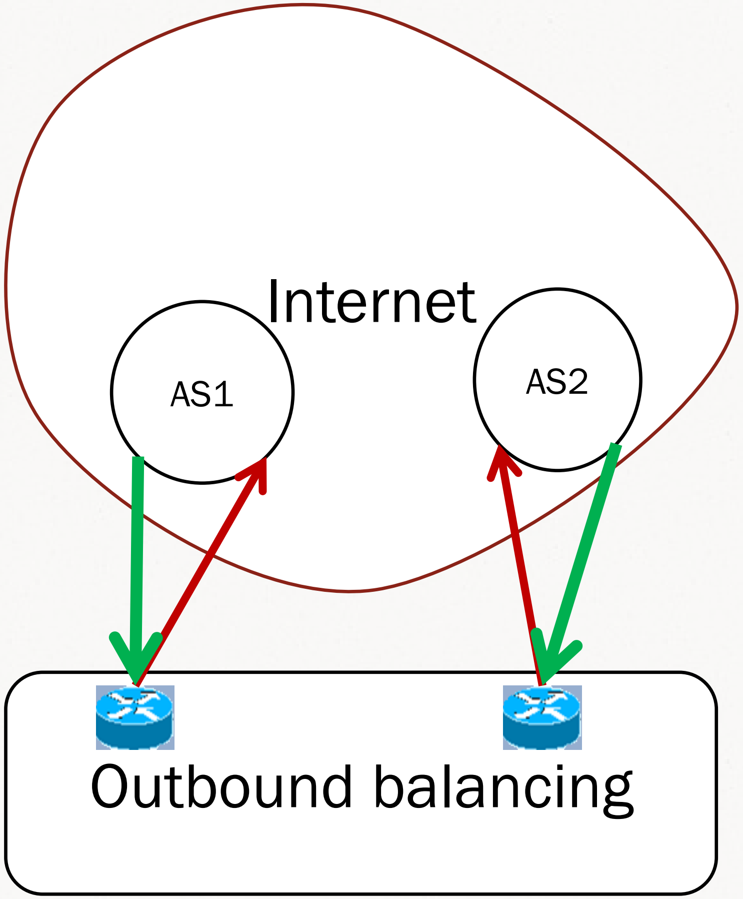
4. Results

   BGP Route Prediction, AS Design

Traffic generators

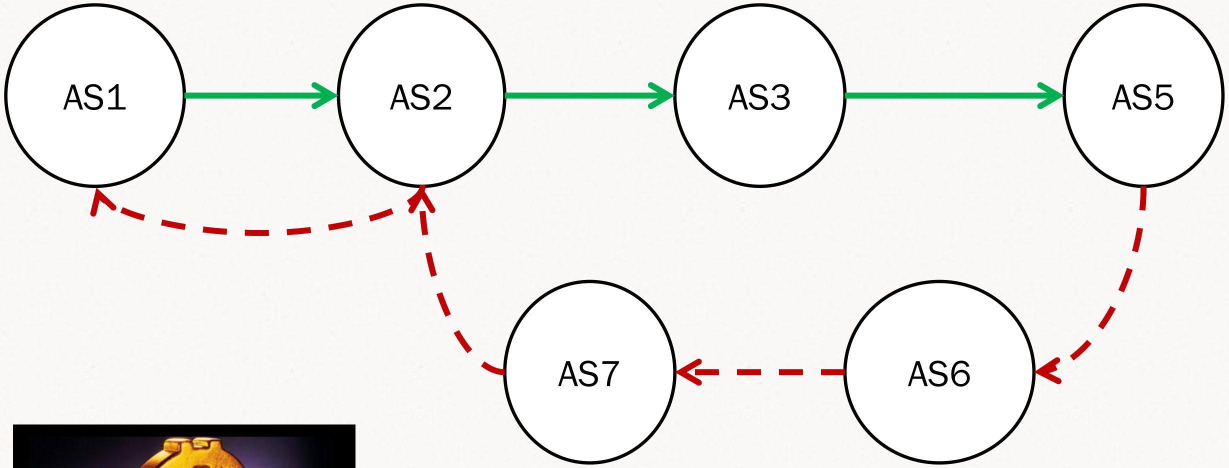


Traffic consumers



Traffic vector

Asymmetric!



AS1

AS2

AS3

AS5

AS7

AS6

= Route Policy

Plan

1. Why we need route policy data?

BGP Route Prediction, AS Design

2. What is wrong with Route Policy from RR?

Physical link discovery, classterization

3. How we made verification?

Active route policy discovery

4. Results

BGP Route Prediction, AS Design

Outdated

From RIPE DB

aut-num: AS42366

remarks: Due to major changes this object is outdated at moment

Erroneous

Incompleteness

Often	Sometimes	Never
Accept Fliters	Prepend	ORIGIN
		EBGP vs IBGP
Local Pref	Med	IGP
		Route ID

Plan

1. Why we need route policy data?

BGP Route Prediction, AS Design

2. What is wrong with Route Policy RR?

Outdated, errorneous and incomplete

3. How have we made verification?

Active route policy discovery

4. Results

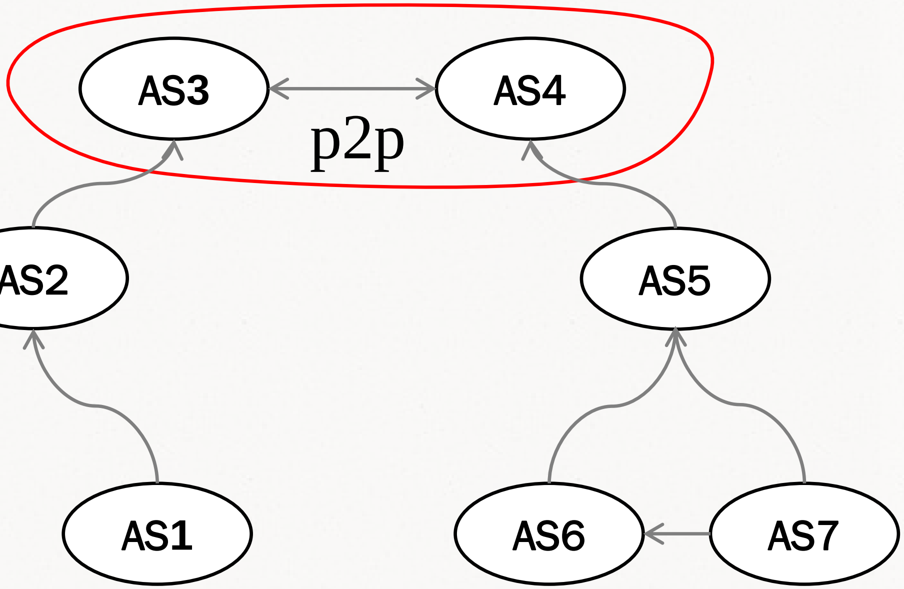
BGP Route Prediction, AS Design

Route Policy Recovery

1. Imitation model of BGP decision process
2. AS relations tagging
3. Active verification

Result: Priority at every level of BGP decision process

AS Relations tagging

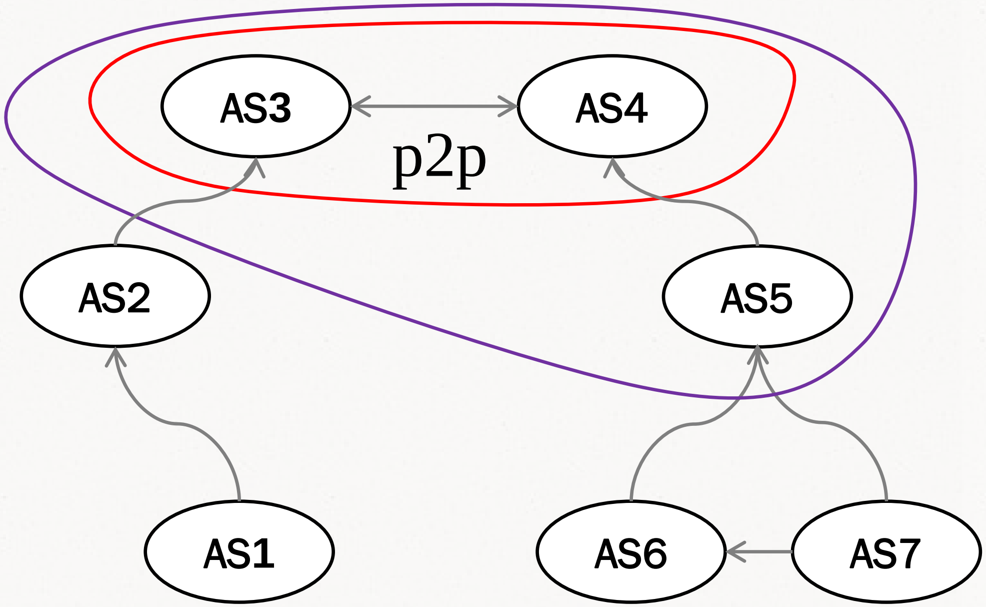


Relations:

p2p = {AS3, AS4}

c2p = {(AS2, AS23, (AS5,AS4),
(AS1, AS2), (AS6, AS5), (AS7,AS5)}

AS Relations tagging

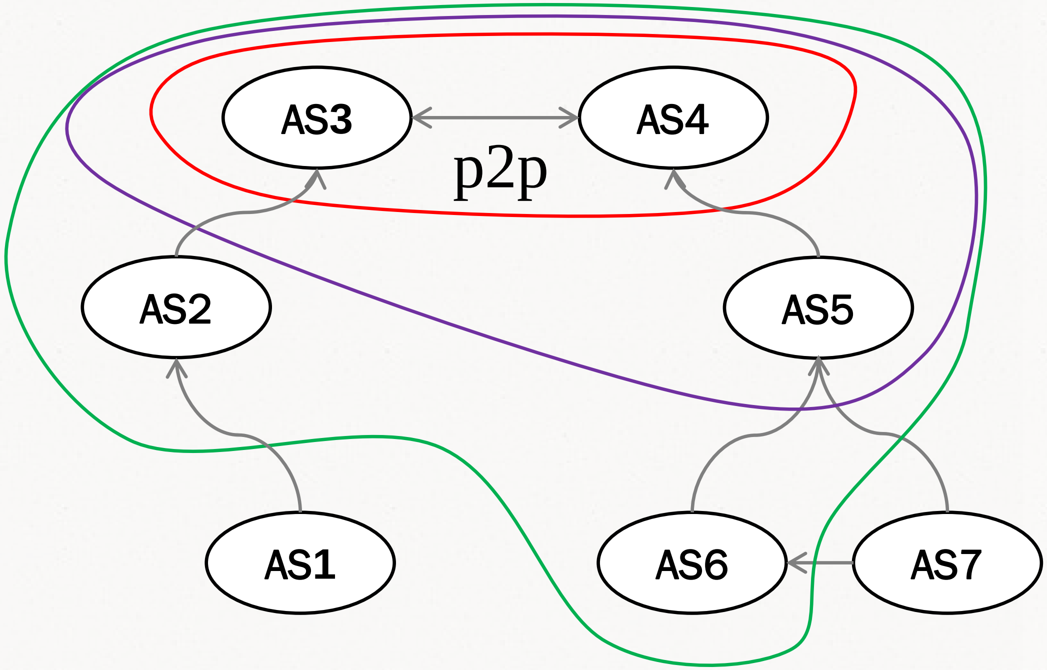


Relations:

p2p = {AS3, AS4}

c2p = {(AS5, AS4} (AS2,AS3) (AS1, AS2), (AS6, AS5), (AS7,AS5)}

AS Relations tagging

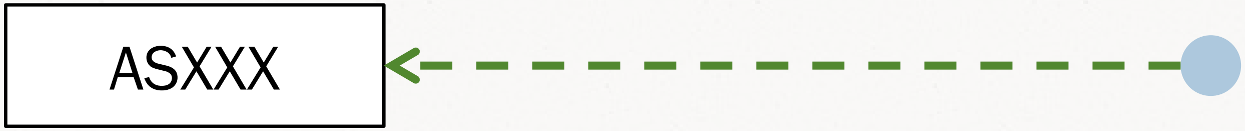


Relations:

p2p = {AS3, AS4}

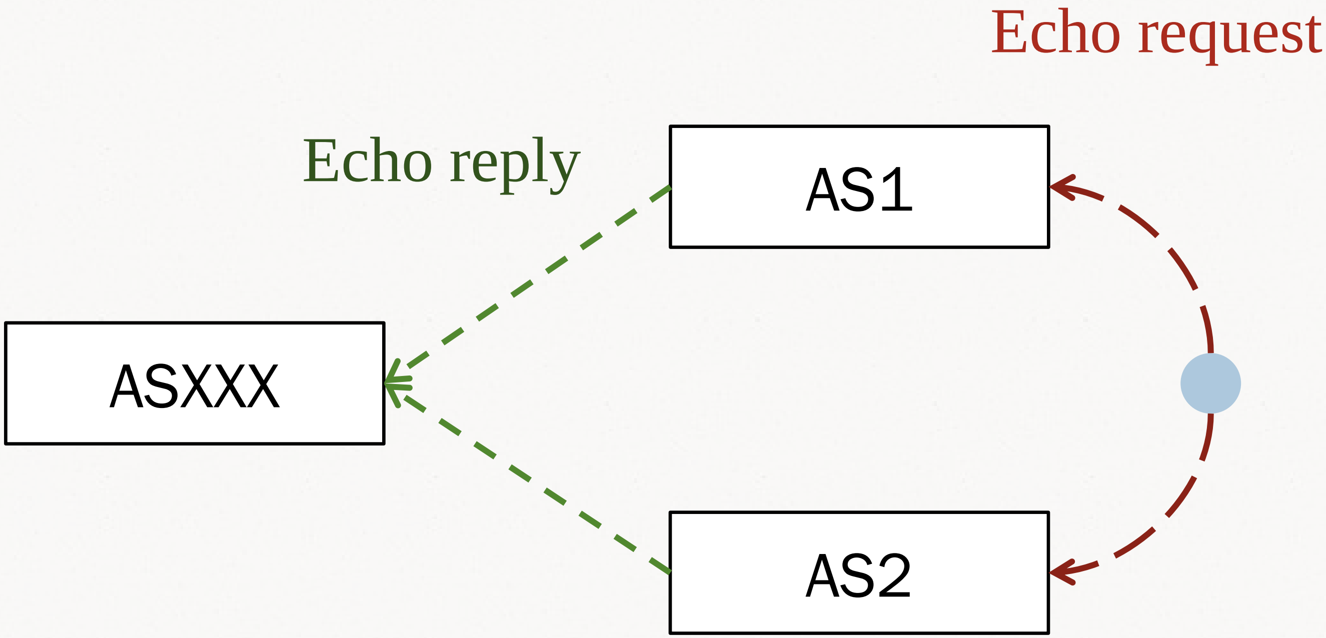
c2p = {(AS5, AS4, (AS2,AS3), (AS1, AS2), (AS6, AS5), (AS7,AS5)}

Active Verification : example



Traceroute
One remote node – one path

Active Verification : example

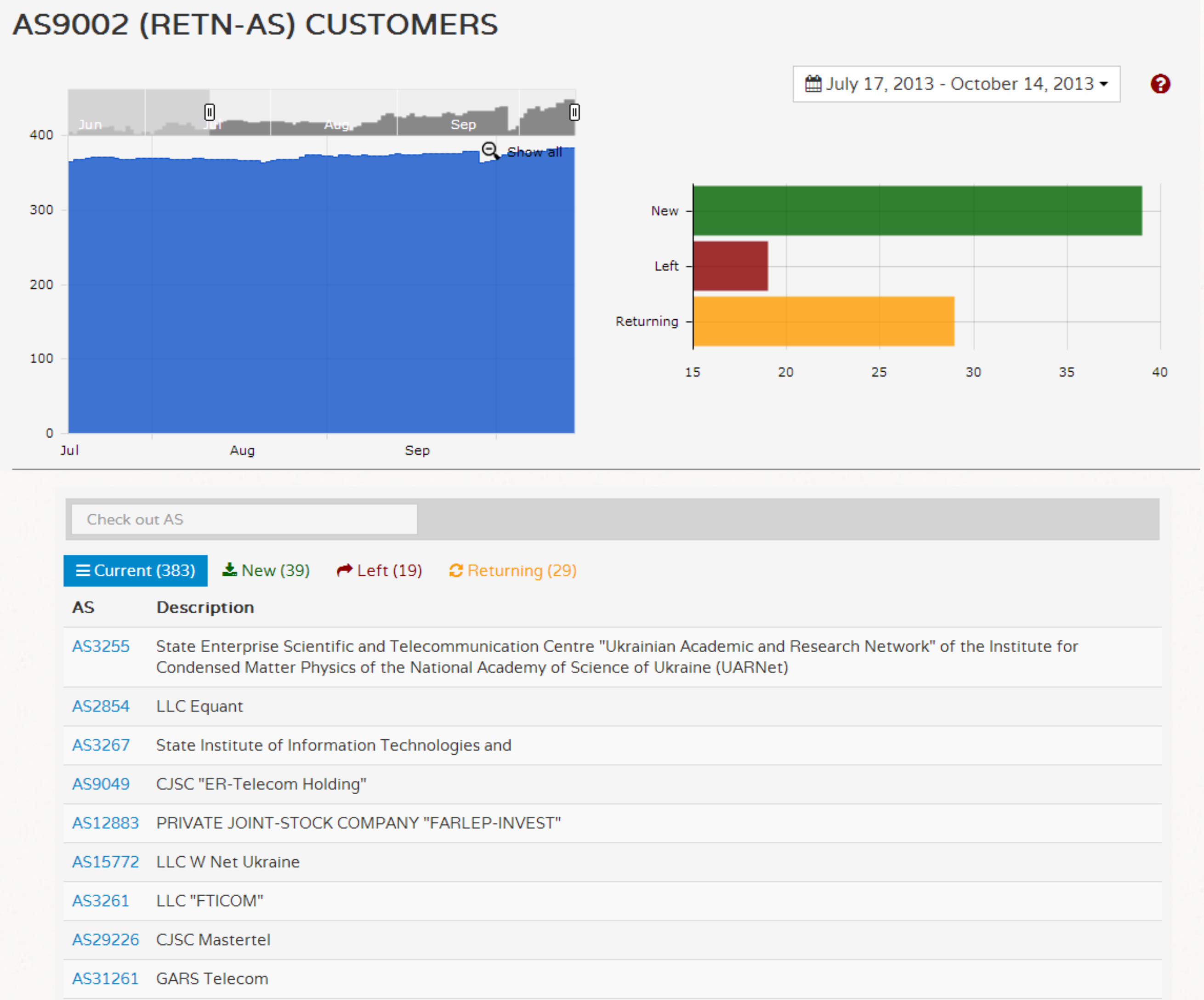


Ping –R with source from ASXXX
One remote node – count(neighbors) * path

Verification Data

radar.qrator.net

1. AS Relation typing;
2. Traffic flow prediction from Tier-1 providers;
3. Radar Monitor: static and dynamic route loops, DoS amplifires, botnet amps.



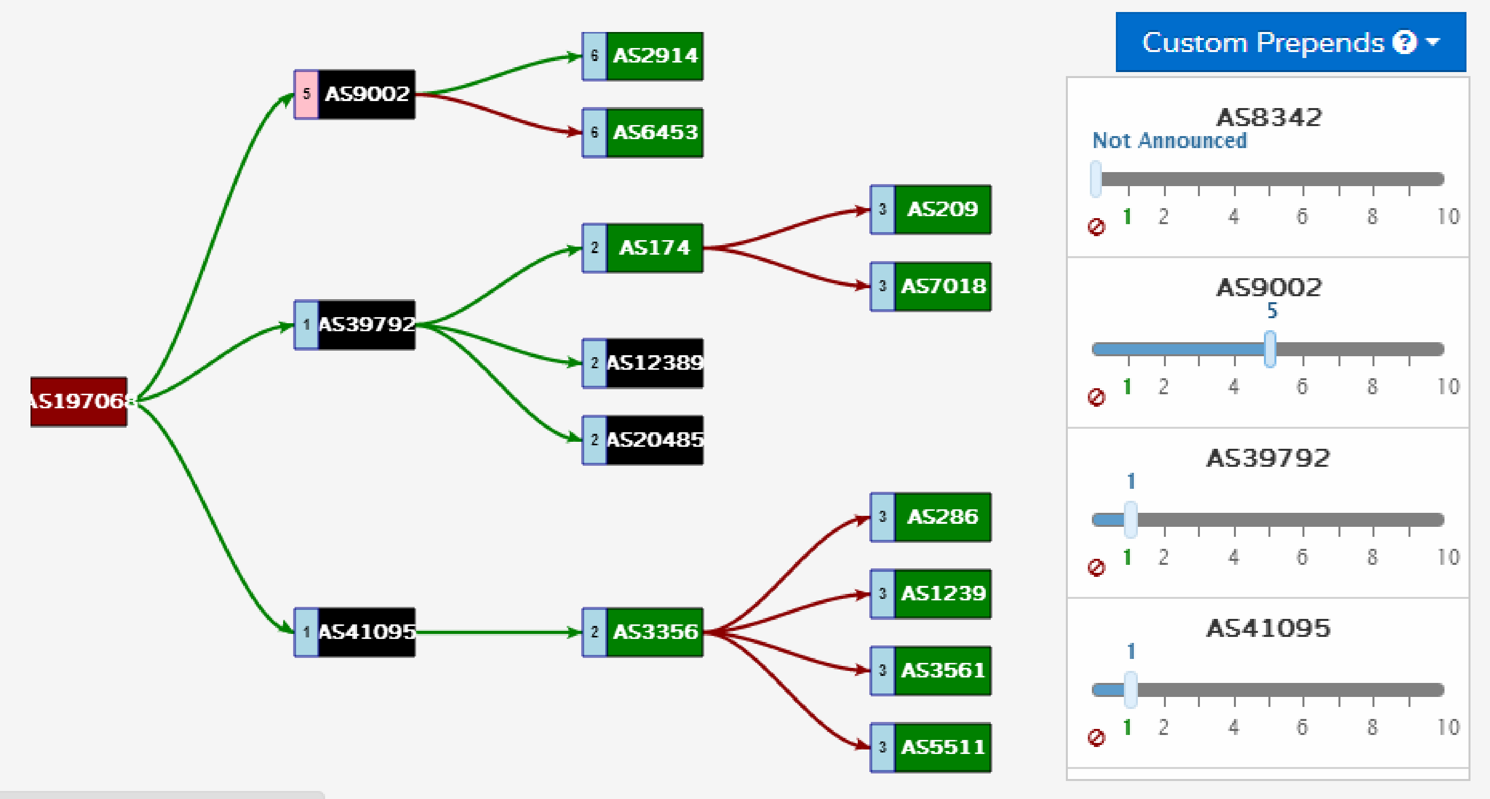
AS9002 (RETN-AS) CUSTOMERS

July 17, 2013 - October 14, 2013 ▾

Check out AS

☰ Current (383) New (39) Left (19) Returning (29)

AS	Description
AS3255	State Enterprise Scientific and Telecommunication Centre "Ukrainian Academic and Research Network" of the Institute for Condensed Matter Physics of the National Academy of Science of Ukraine (UARNet)
AS2854	LLC Equant
AS3267	State Institute of Information Technologies and
AS9049	CJSC "ER-Telecom Holding"
AS12883	PRIVATE JOINT-STOCK COMPANY "FARLEP-INVEST"
AS15772	LLC W Net Ukraine
AS3261	LLC "FTICOM"
AS29226	CJSC Mastertel
AS31261	GARS Telecom

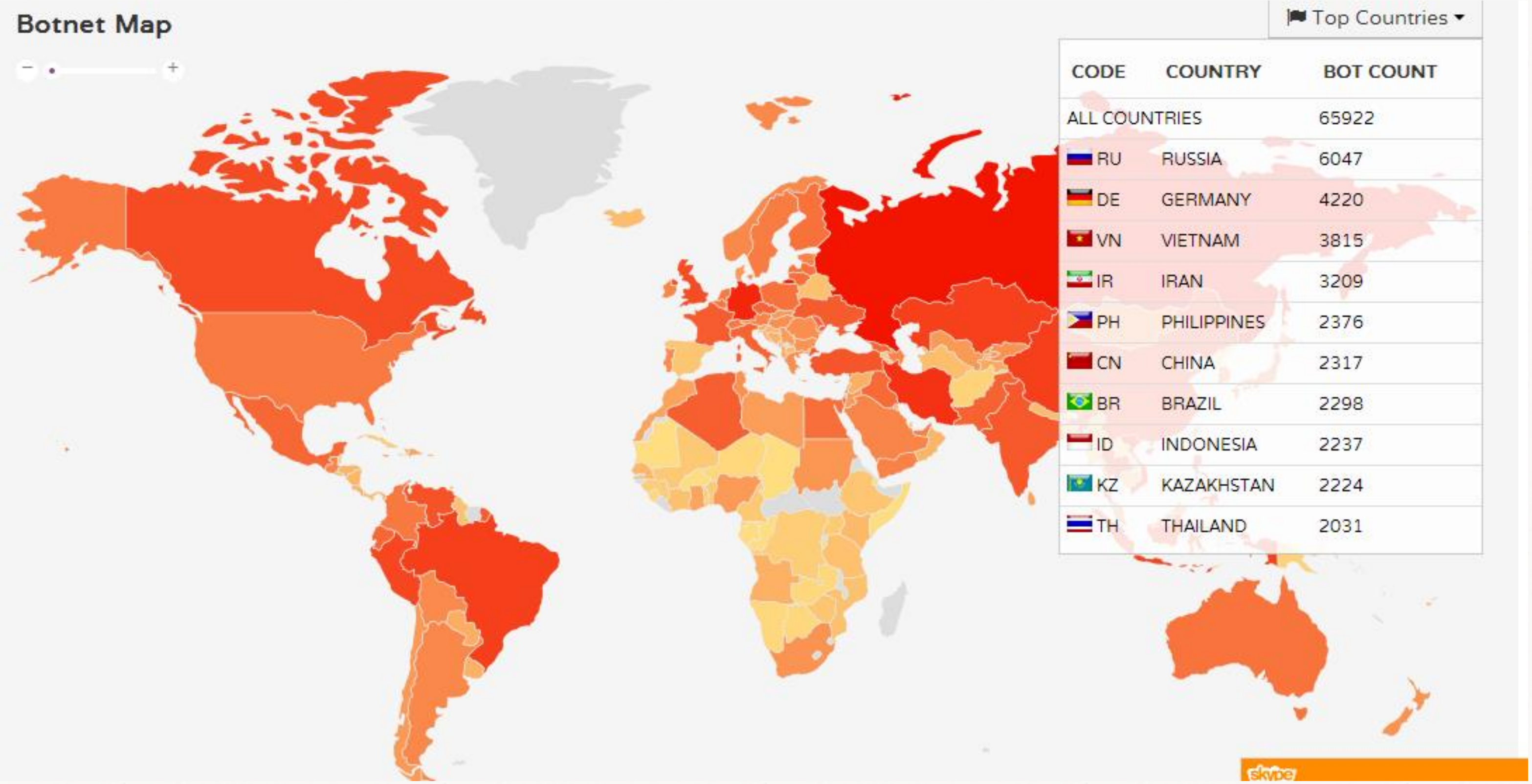


AS8342
Not Announced

AS9002
5

AS39792
1

AS41095
1



Botnet Map

CODE	COUNTRY	BOT COUNT
ALL COUNTRIES		65922
RU	RUSSIA	6047
DE	GERMANY	4220
VN	VIETNAM	3815
IR	IRAN	3209
PH	PHILIPPINES	2376
CN	CHINA	2317
BR	BRAZIL	2298
ID	INDONESIA	2237
KZ	KAZAKHSTAN	2224
TH	THAILAND	2031

Plan

1. Why we need route policy data?

BGP Route Prediction, AS Design

2. What is wrong with Route Policy data?

Outdated, erroneous and incomplete

3. How we made verification?

Active route policy discovery

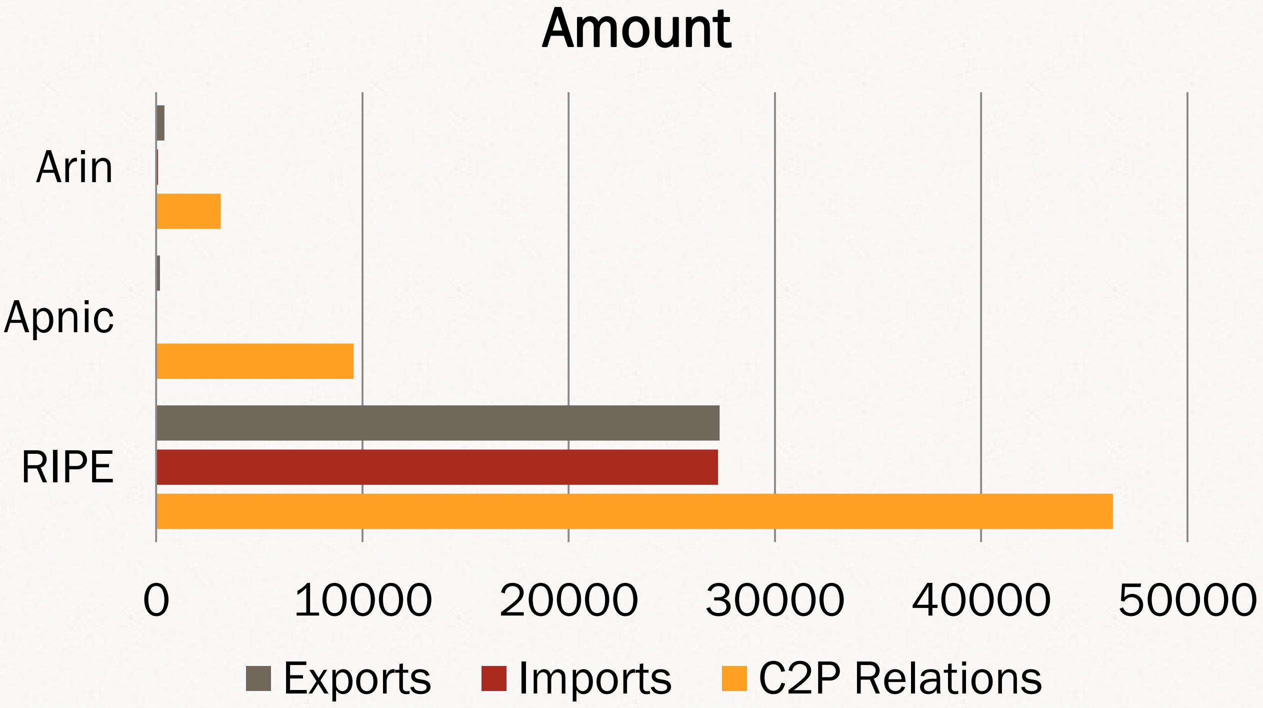
4. Verification Results

BGP Route Prediction, AS Design

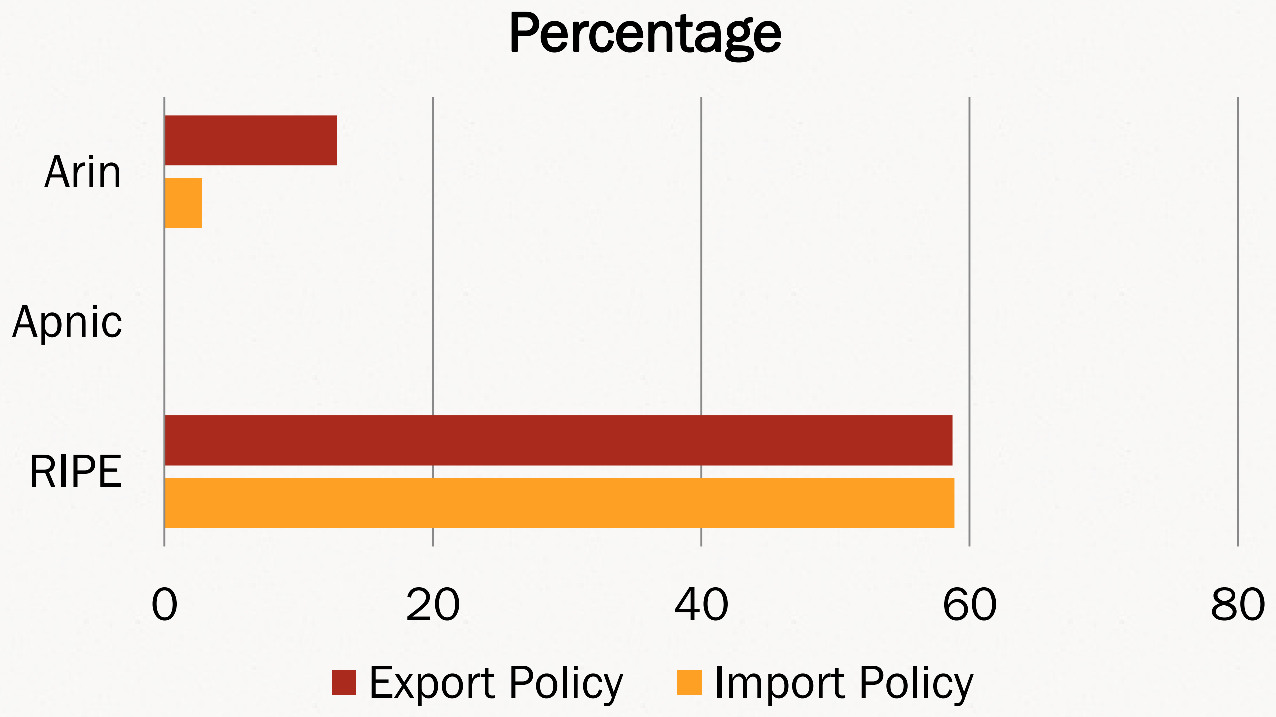
Customers as Criterion

1. Customers has global visibility unlike peering relations
2. Pref(customer) > Pref(not_customer)

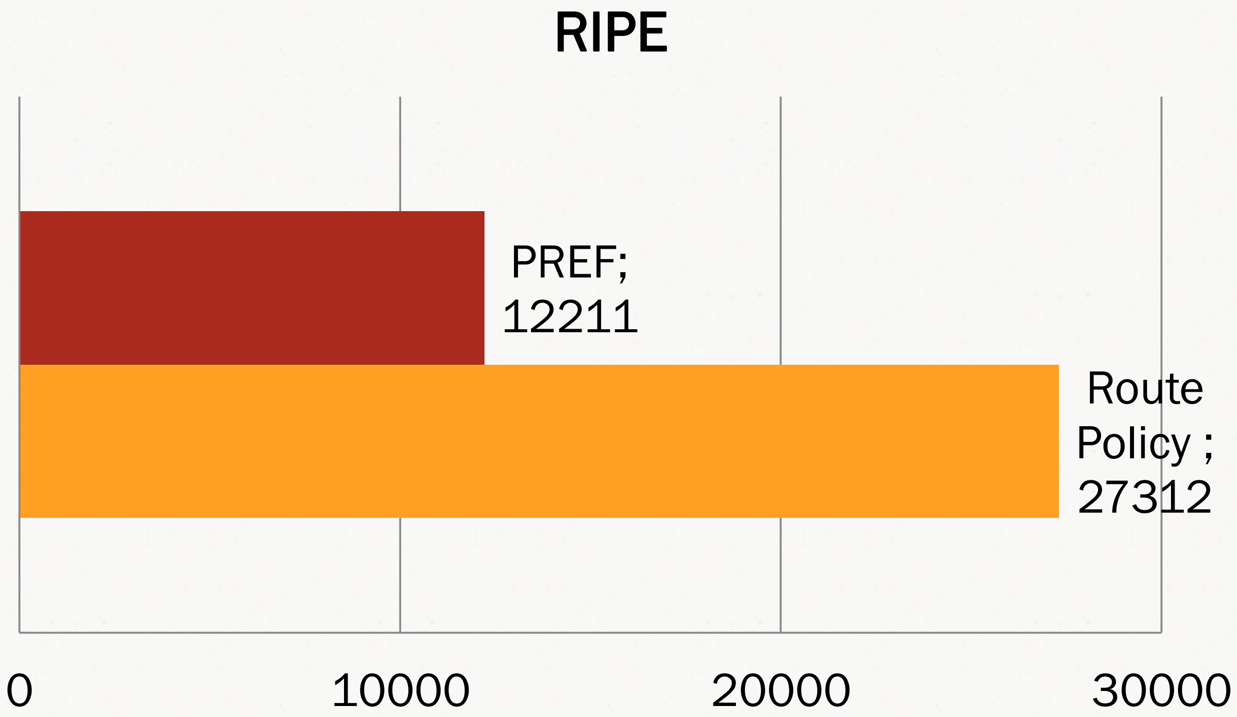
Completeness: links



Completeness: links



Completeness: pref

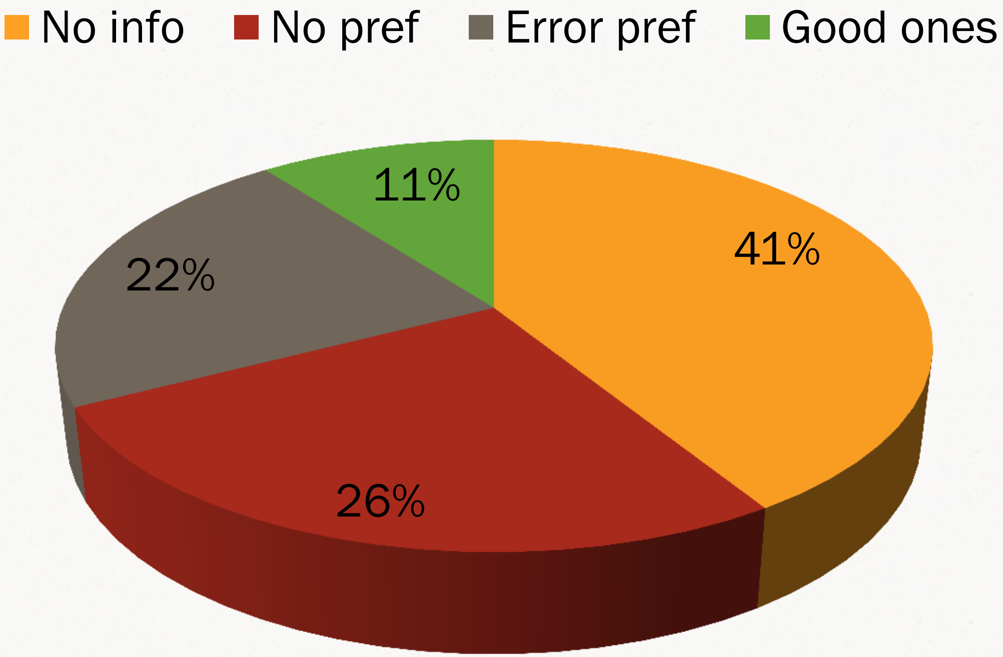


Erroneous: pref

$$good = count\big(pref(customer) > pref(!\,customer)\big)$$
$$bad = count\big(pref(customer) < pref(!\,customer)\big)$$

$$\frac{\sum_{AS} \frac{bad}{good + bad}}{count(AS)} = 68\%$$

C2P description



Results

1. Route Policy data from RR is greatly outdated, incomplete and full of errors. It can’t be used for AS Design or for traffic engineering purposes;
2. Mathematical models could be used for route policy recovery with high precision.

Qrator Radar

radar.qrator.net