Detecting Autonomous Systems Relationships

Alexander Azimov
<aa@highloadlab.com>
Highload Lab

Quiz!

1. Why We need AS relation and policy discovery?

BGP Route Prediction, AS Design

2. What have been already done?

Physical link discovery, classterization

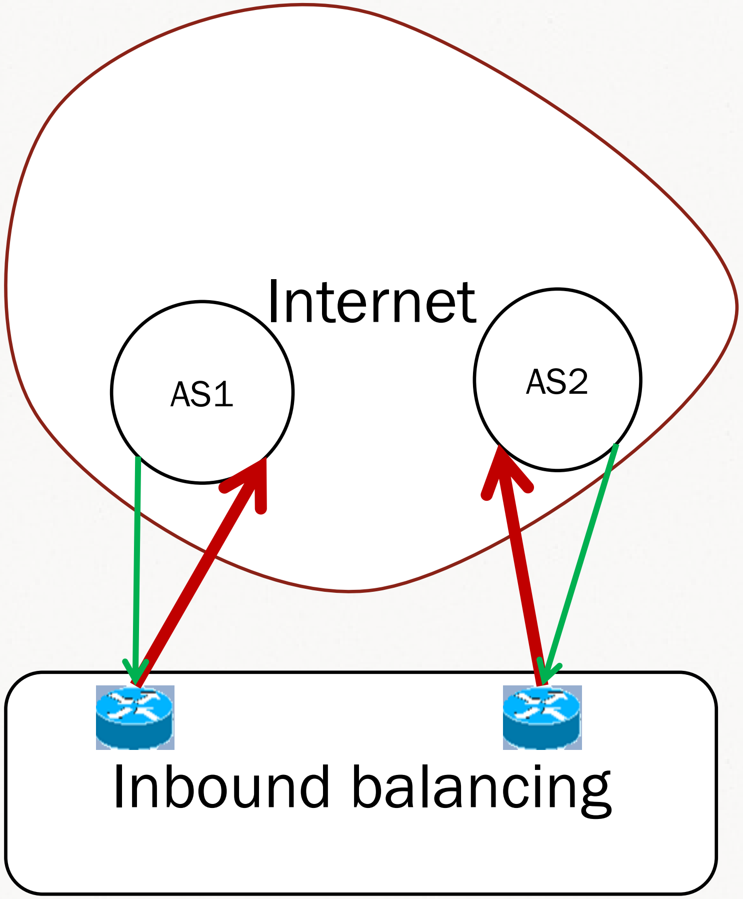
3. What have we done?

Active route policy discovery

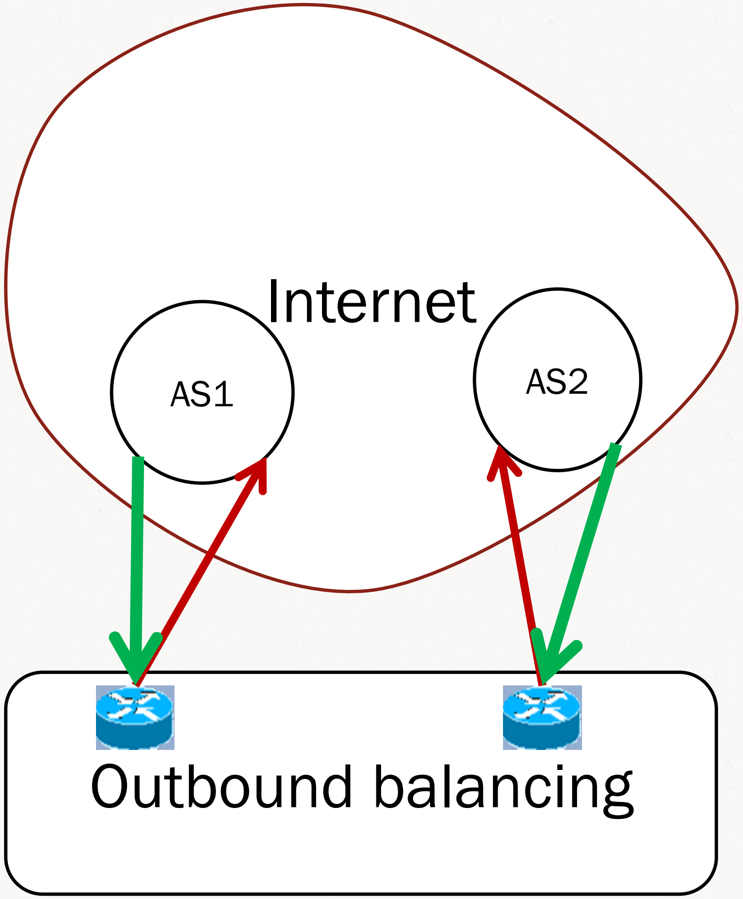
4. What opportunities does it give?

BGP Route Prediction, AS Design

Traffic generators

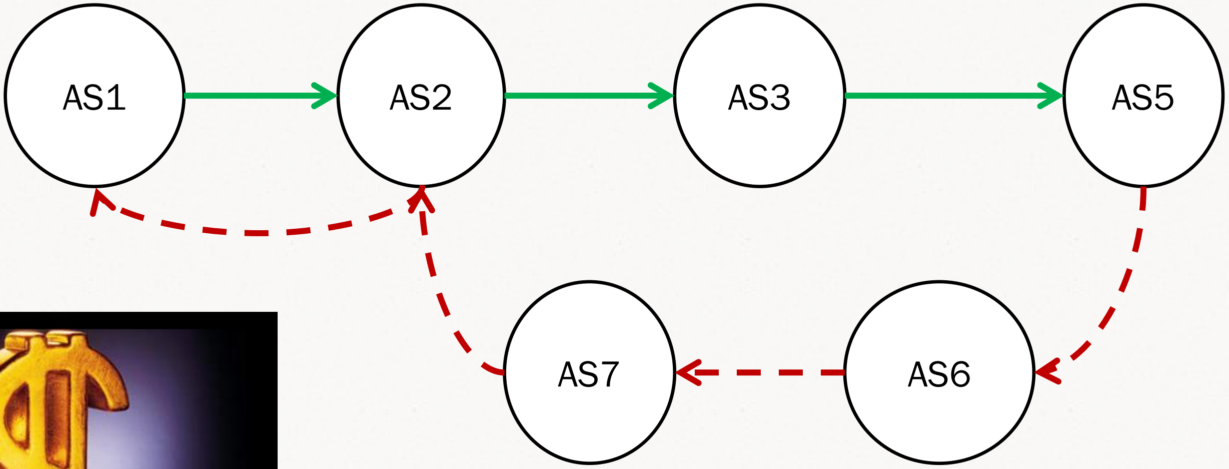


Traffic consumers



Traffic vector

Asymmetric!



Quiz!

1. Why We need AS relation and policy discovery?

BGP Route Prediction, AS Design

2. What have been already done?

Physical link discovery, classterization

3. What have we done?

Active route policy discovery

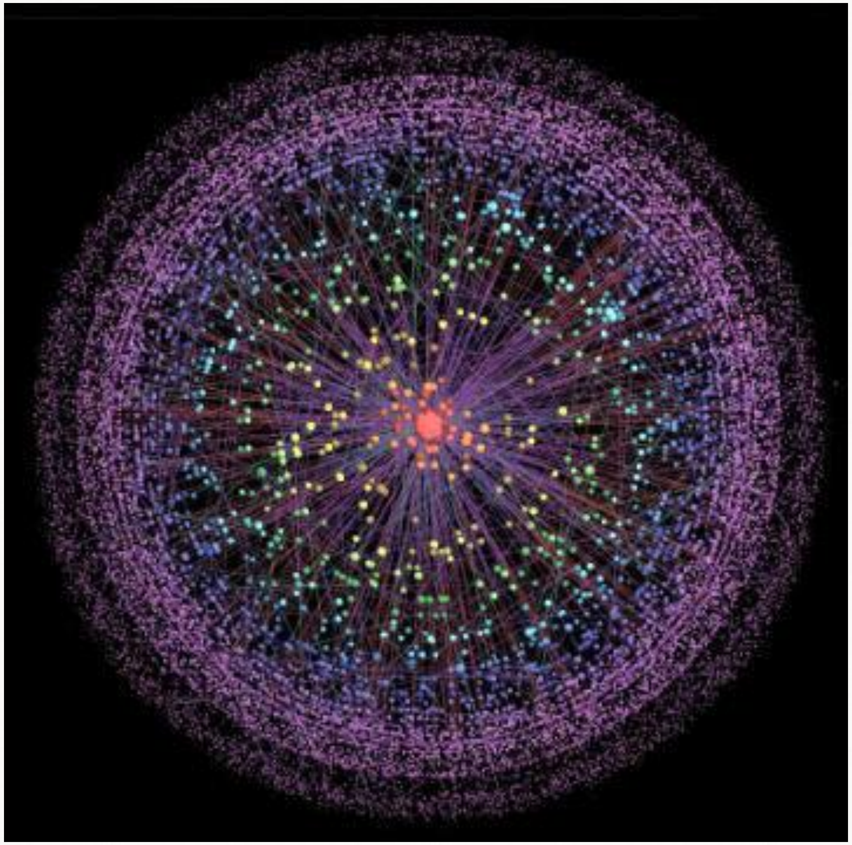
4. What opportunities does it give?

BGP Route Prediction, AS Design

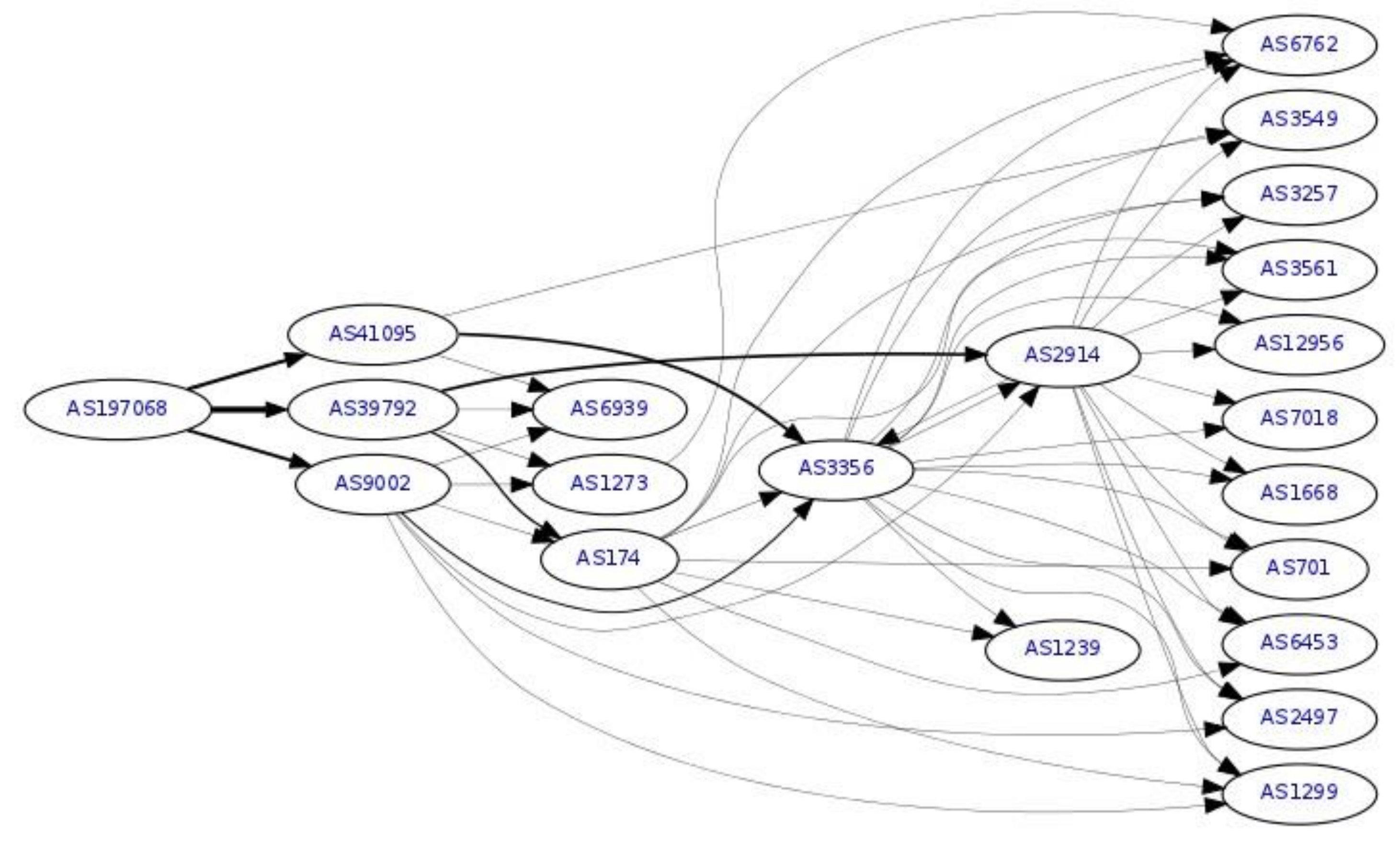
Physical Link Discovery

Map of the Internet, The Opte Project, www.opte.org

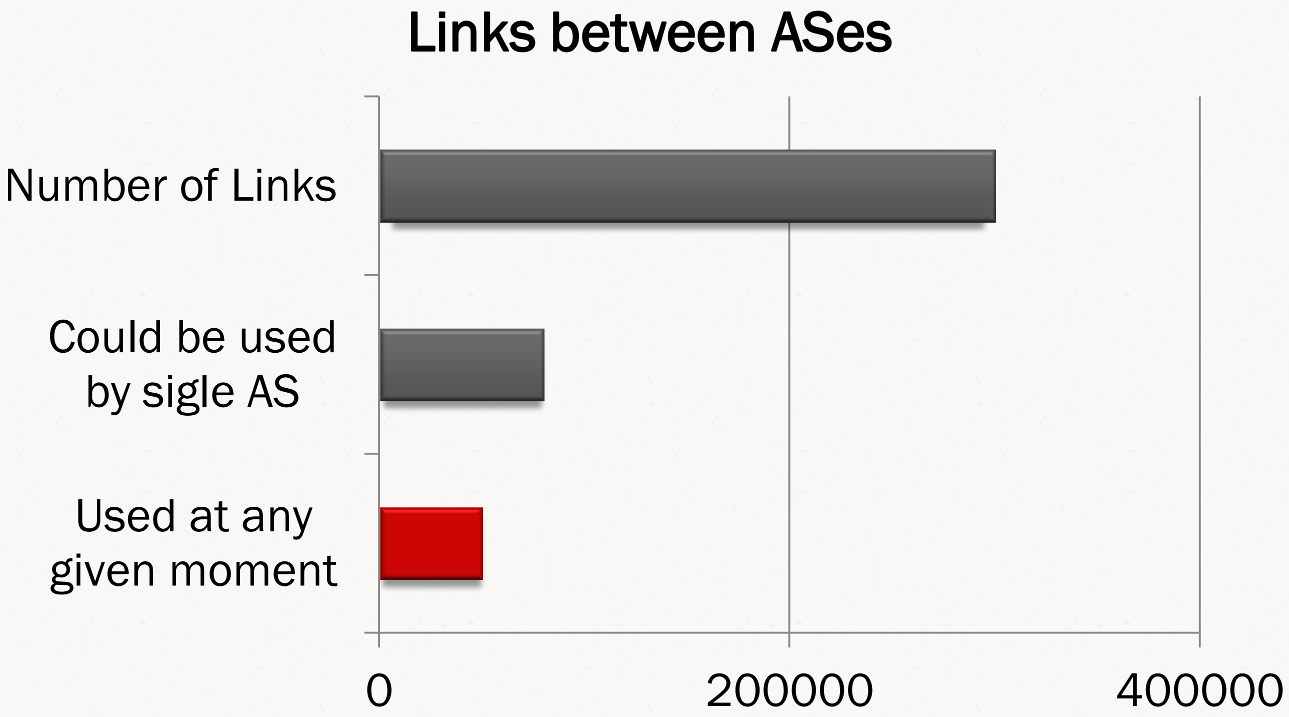
Classterization



BGP AS Paths


AS197068
AS41095
AS39792
AS9002
AS6939
AS1273
AS174
AS3356
AS2914
AS1239
AS6762
AS3549
AS3257
AS3561
AS12956
AS7018
AS1668
AS701
AS6453
AS2497
AS1299

Core of the problem



Route Policy in RR

Outdated or incomplete

Deadlock

1. Physical link discovery;
2. No registry of current route policies.

=

No opportunity for traffic flow prediction

Quiz!

1. Why We need AS relation and policy discovery?

BGP Route Prediction, AS Design

2. What have been already done?

Physical link discovery, classterization

3. What have we done?

Active route policy discovery

4. What opportunities does it give?

BGP Route Prediction, AS Design

AS Design

×

I did it my way…

×

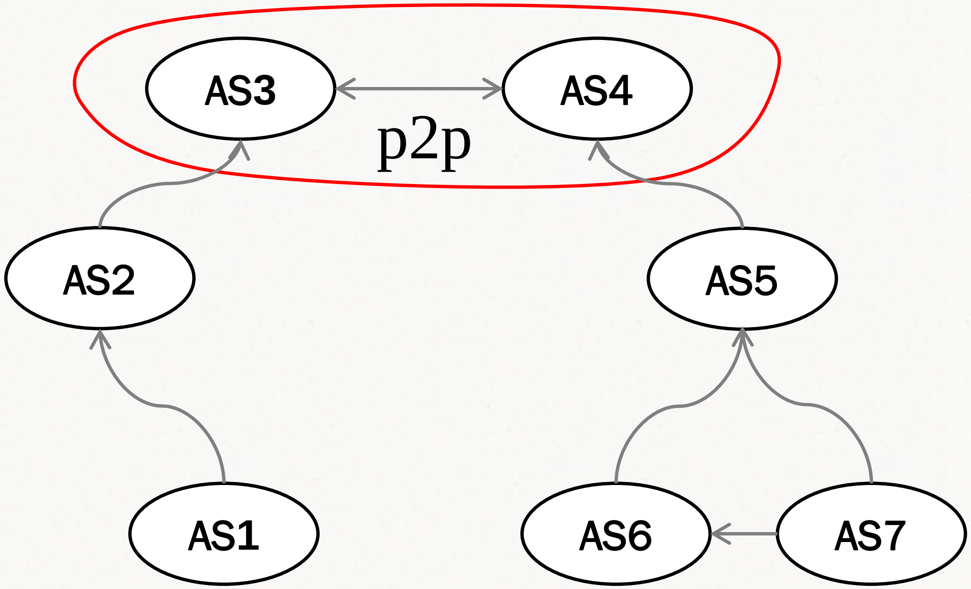
12
1
2
3
4
5
6
7
8
9
10
11

2

Route Policy Recovery

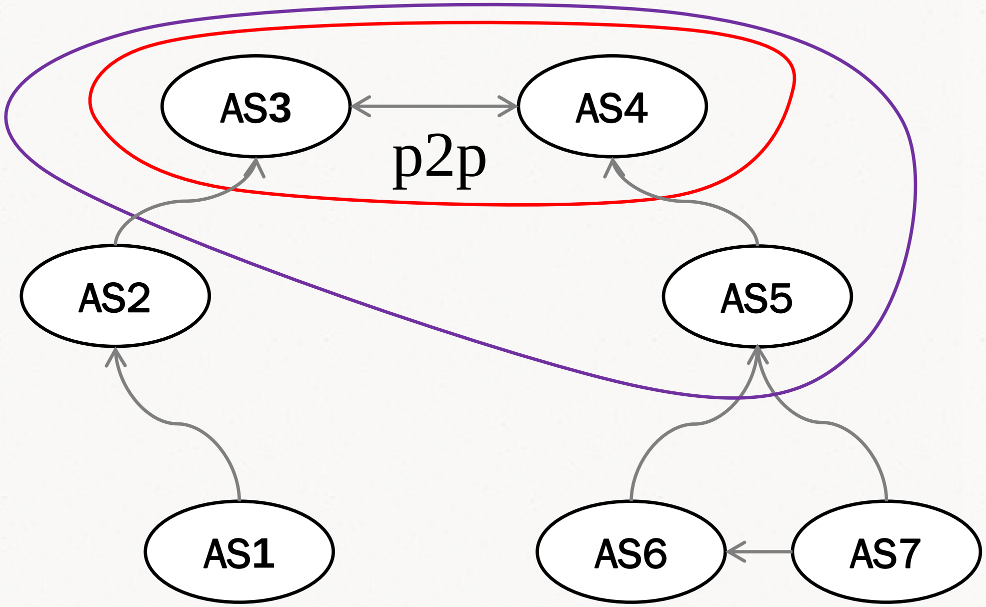
1. AS relations
2. Active verification
3. Priority at every level of BGP decision process
4. Mathematical Equations
5. ....

AS Relations : example



Relations:
p2p = {AS3, AS4}
c2p = {(AS2, AS23, (AS5,AS4),
(AS1,, AS2), (AS6, AS5), (AS7,AS5)}

AS Relations : example

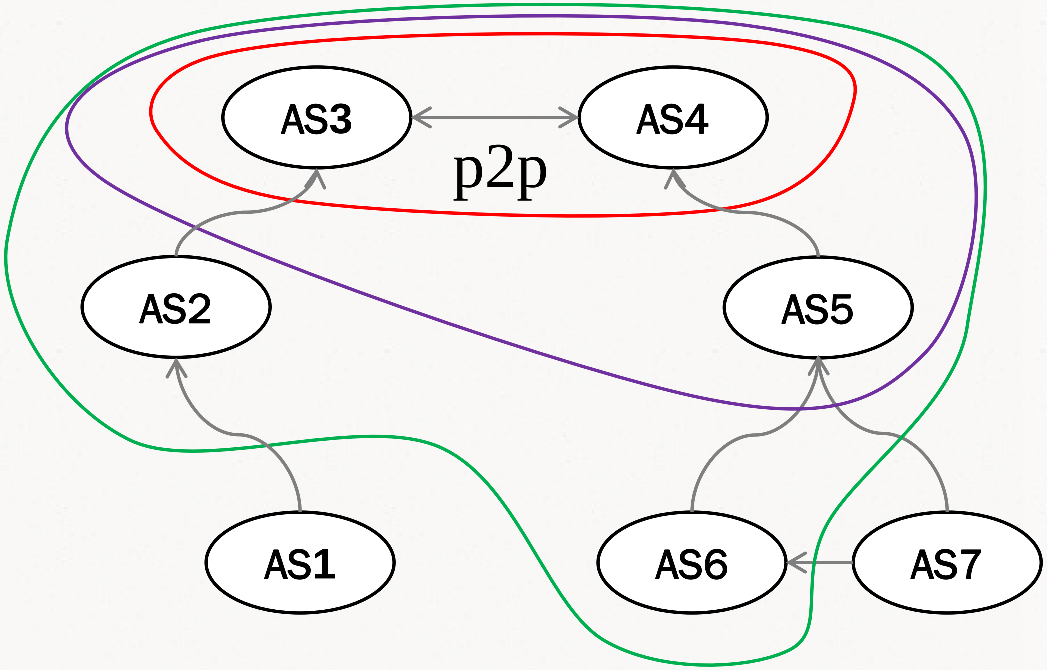


Relations:

p2p = {AS3, AS4}

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

AS Relations : example

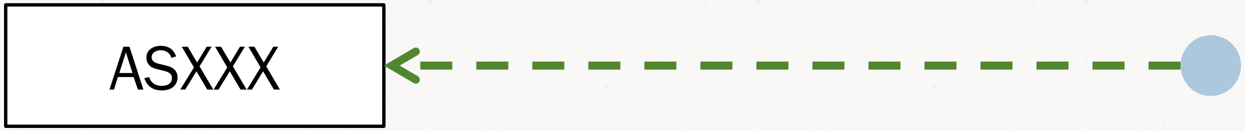


Relations:

p2p = {AS3, AS4}

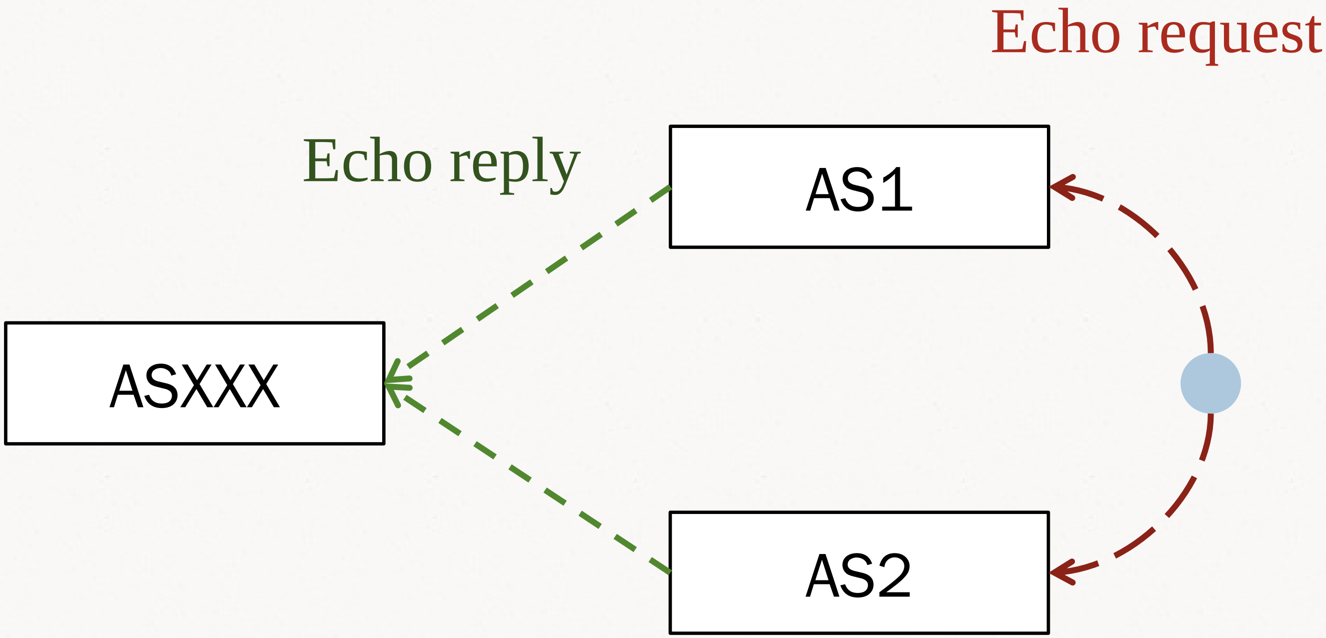
c2p = {(AS5, AS4, (AS2,AS3), (AS1, AS2), (AS6, AS5), (AS7,AS5)}

Active Verification : example



Traceroute
One remote node – one path

Active Verification : example



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

Quiz!

1. Why We need AS relation and policy discovery?

BGP Route Prediction, AS Design

2. What have been already done?

Physical link discovery, classterization

3. What opportunities does it give?

Active route policy discovery

4. What opportunities does it give?

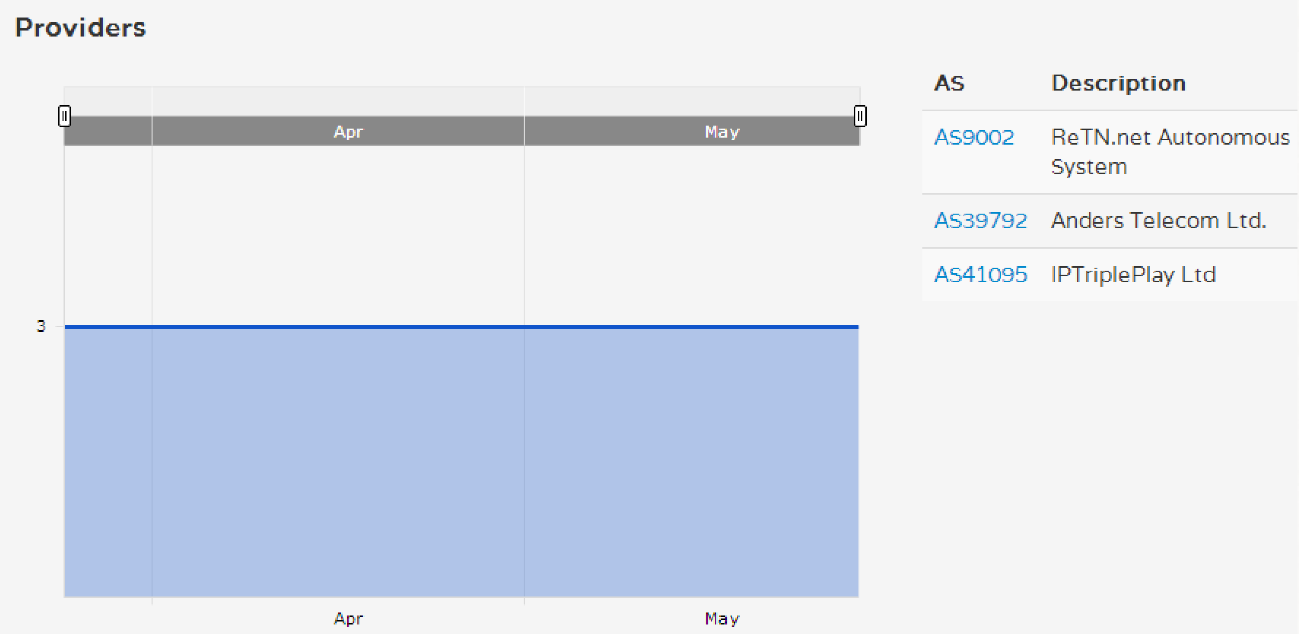
BGP Route Prediction, AS Design

How to make You interested in my results?

Qrator Radar

1. AS Relations
2. BGP Route Prediction
3. AS Design
4. Security Issues
5. Rates

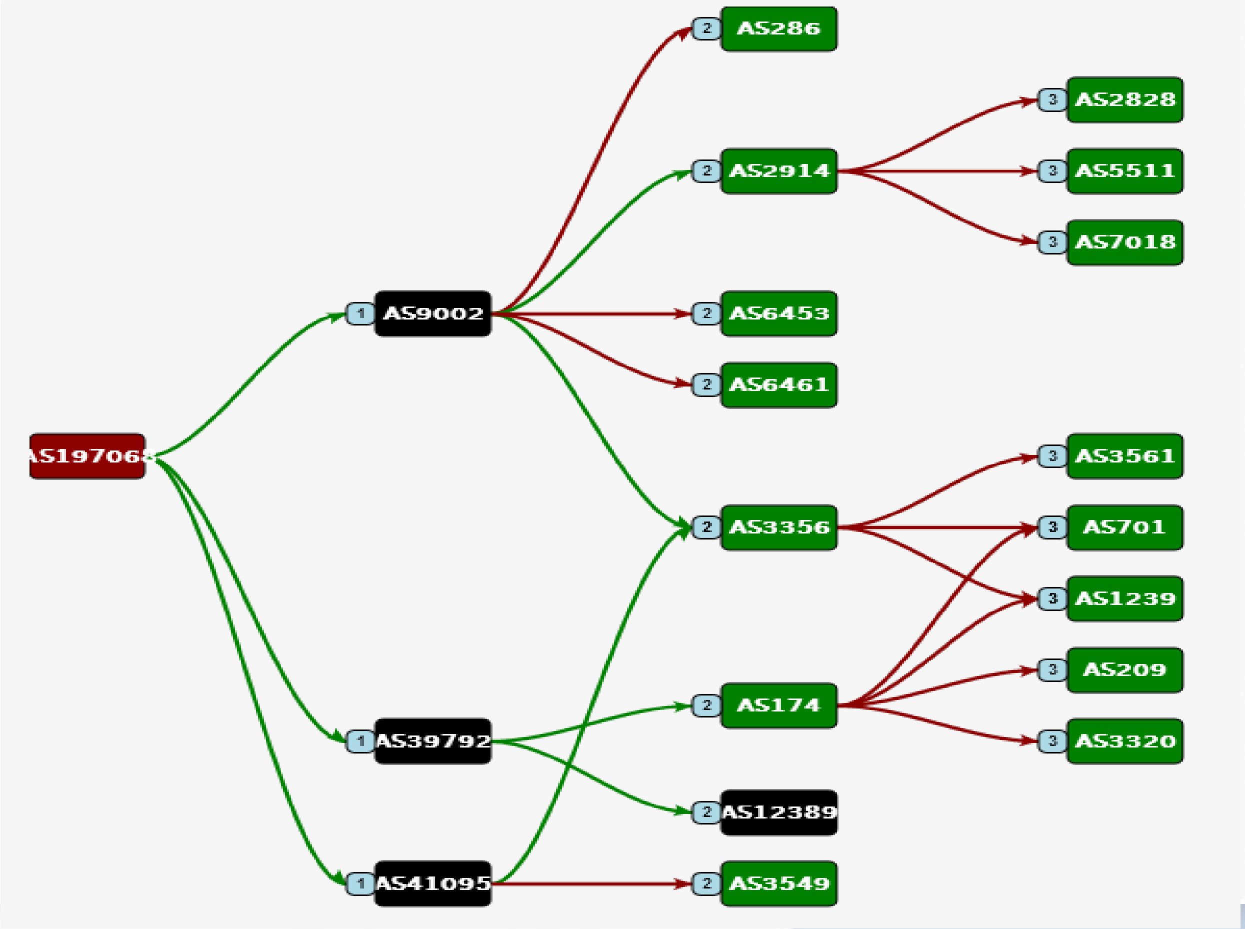
AS Relations

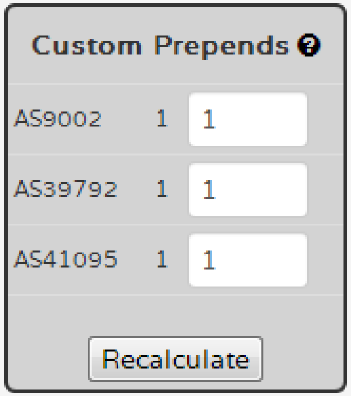


AS	Description
AS9002	ReTN.net Autonomous System
AS39792	Anders Telecom Ltd.
AS41095	IPTriplePlay Ltd

Rates: peering, customers, providers

BGP Route Prediction

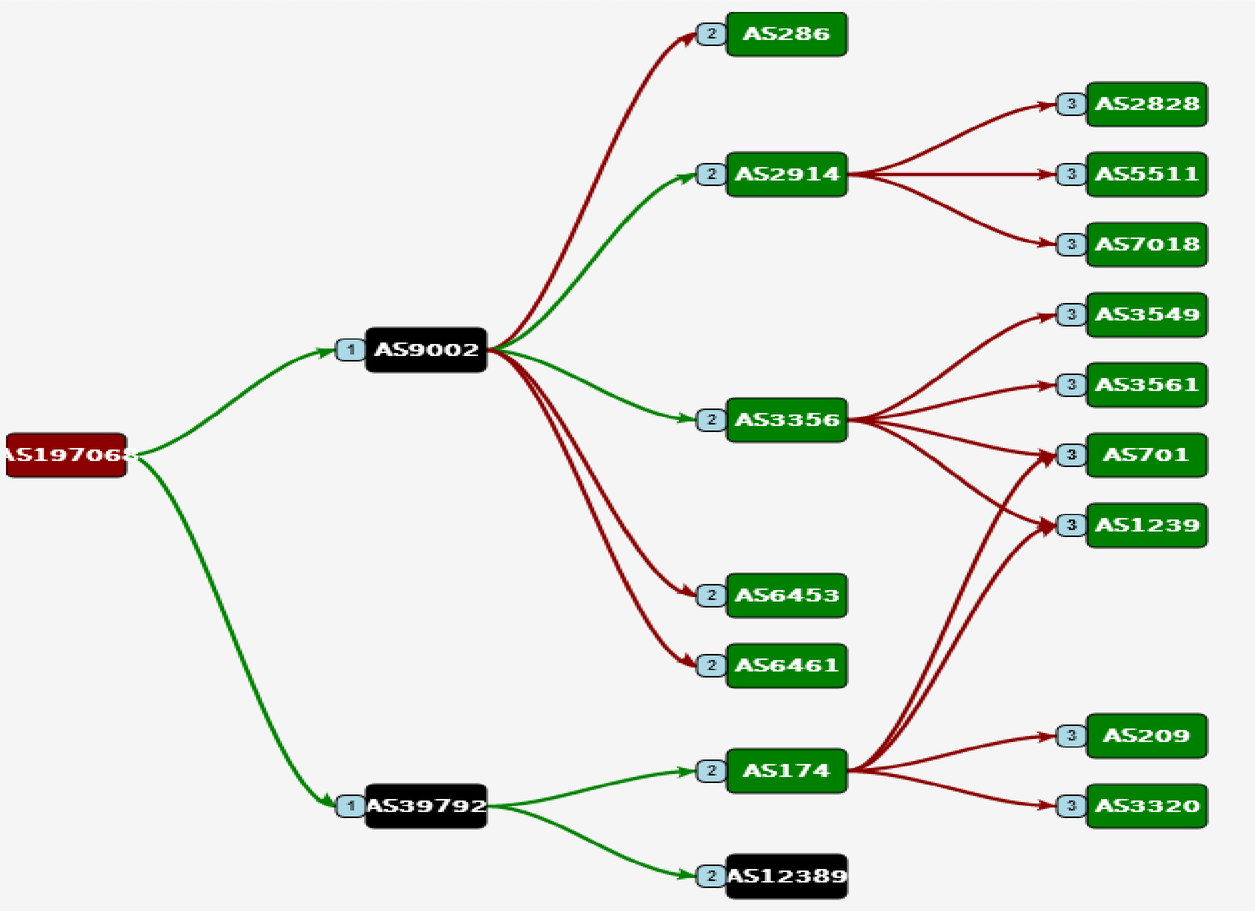


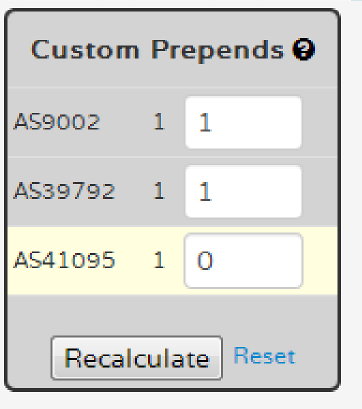


Custom Prepends

AS9002	1	1
AS39792	1	1
AS41095	1	1

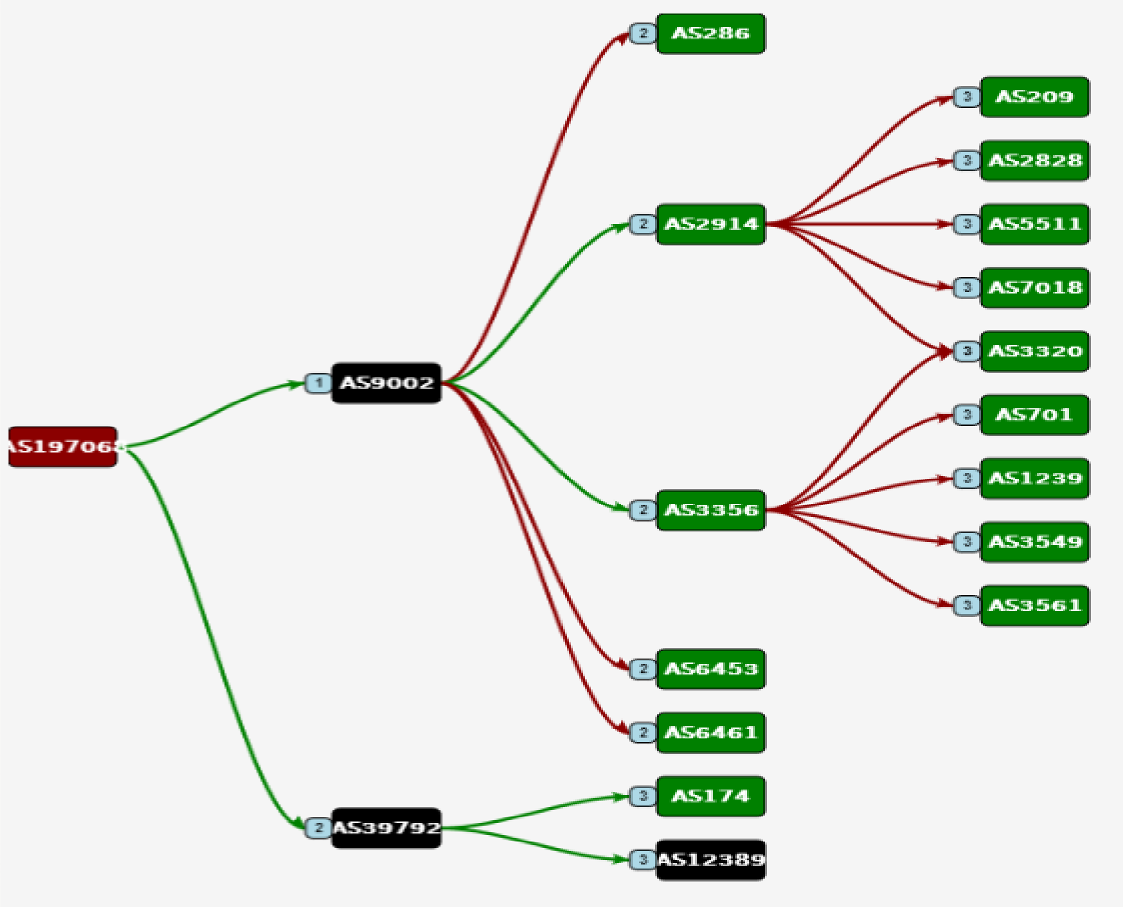
Route Withdraw

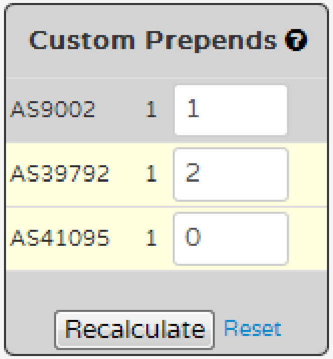



Custom Prepends ❓

AS9002	1	1
AS39792	1	1
AS41095	1	0

Prepend Policy

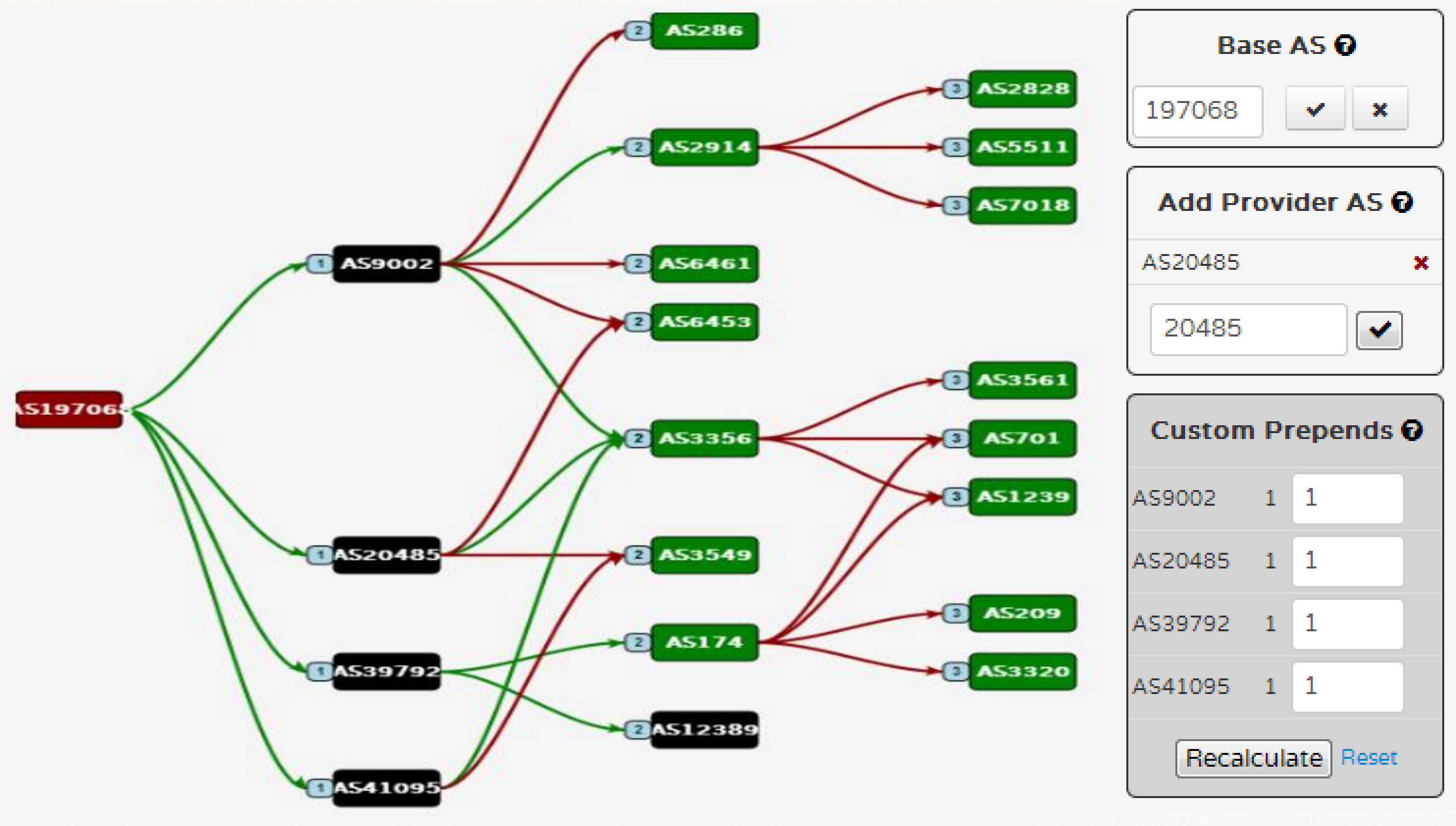




Custom Prepends

AS9002	1	1
AS39792	1	2
AS41095	1	0

AS Design



Base AS

197068 ✓ ✗

Add Provider AS

AS20485 ✗

20485 ✓

Custom Prepends

AS9002	1	1
AS20485	1	1
AS39792	1	1
AS41095	1	1

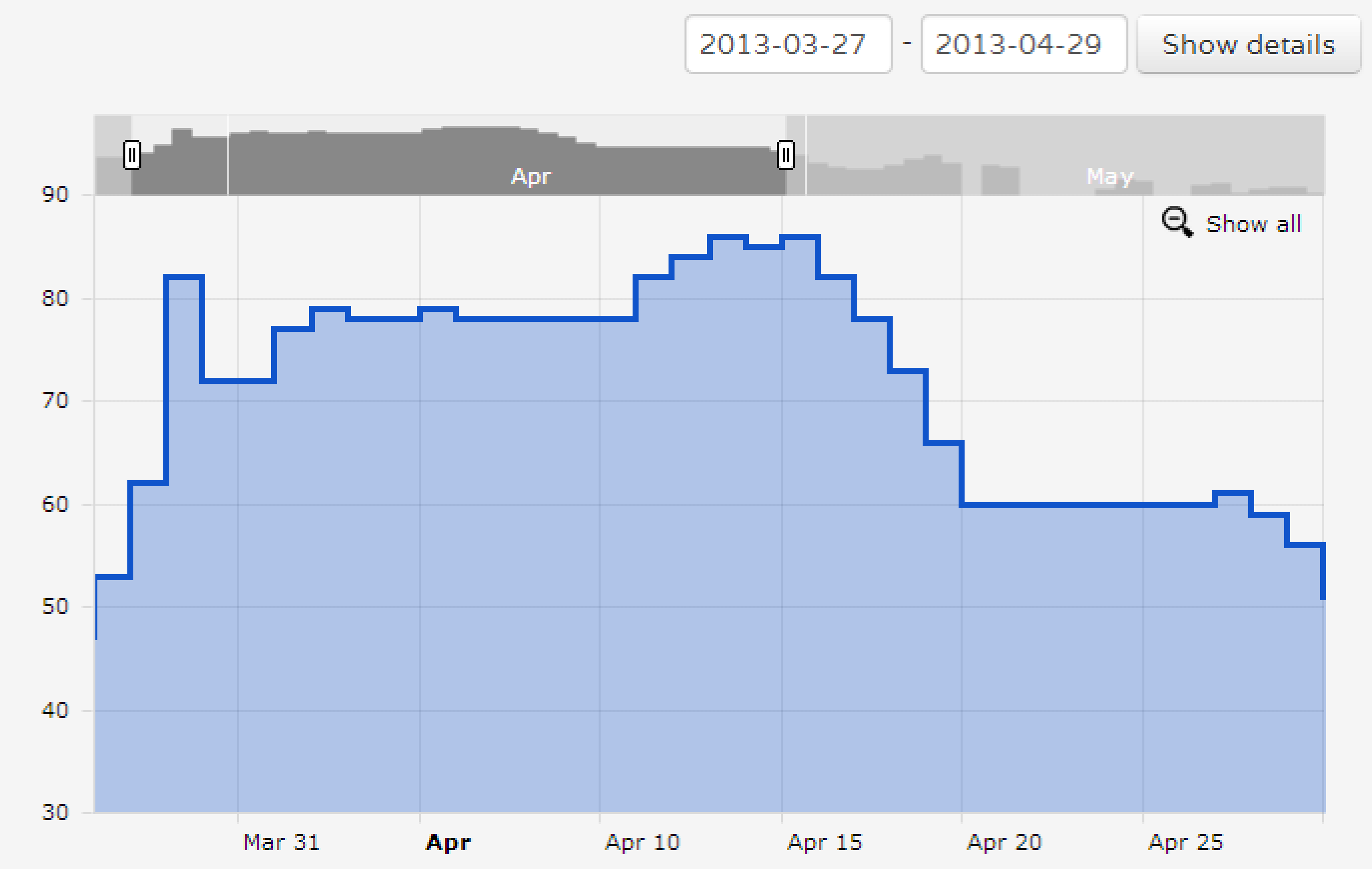
Recalculate Reset

Security Issues

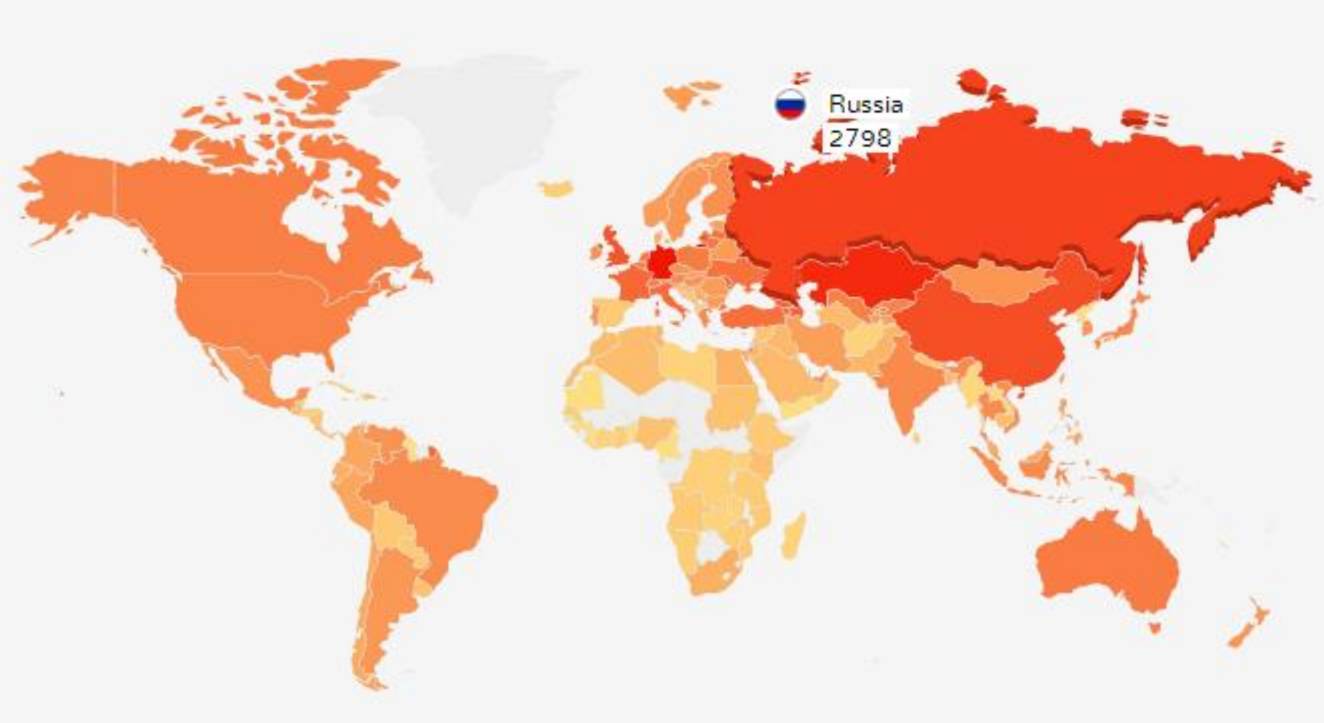
1. Default Route Errors
2. BGP Route Loops
3. DDoS Amplifires
4. Bots

> 30 % of ASes are affected!

Security Issues



Botnet map



Quiz!

1. Why We need AS relation and policy discovery?

BGP Route Prediction, AS Design

2. What have been already done?

Physical link discovery, classterization

3. What have we done?

Active route policy discovery

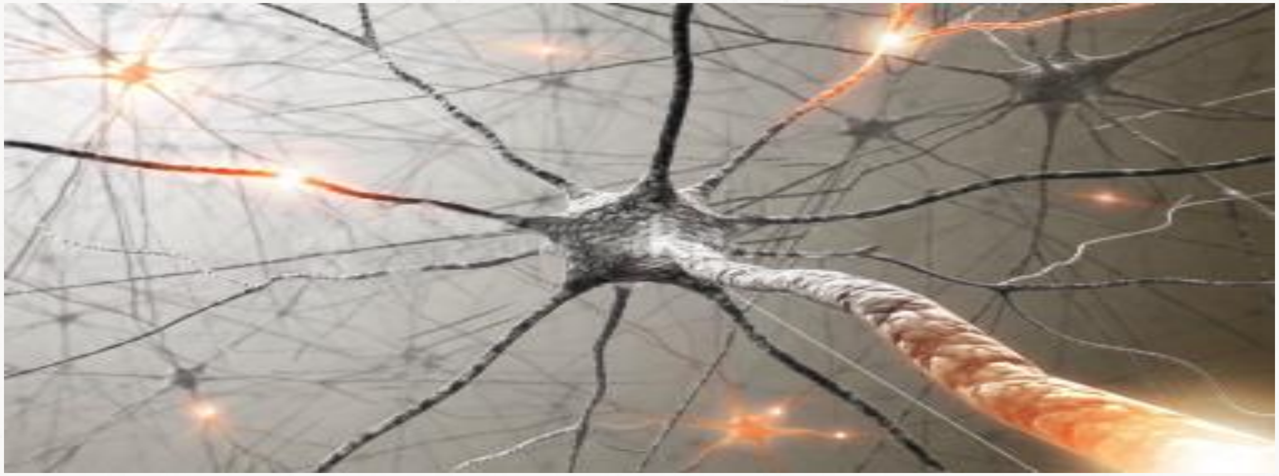
4. What opportunities does it give?

BGP Route Prediction, AS Design

Future Work

Drop detection ->

Prediction how to overcome it using prepend policy



Qrator Radar

radar.qrator.net