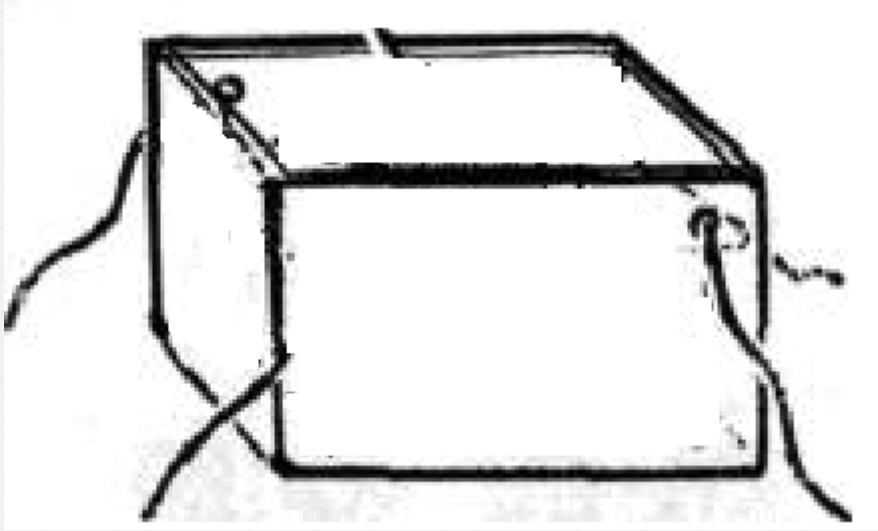
# Detecting Autonomous Systems Relationships

Alexander Asimov
<aa@highloadlab.com>
Highload Lab

# Our Goals

1. Traffic flow engineering
2. AS architecture design
3. BGP loop prediction

# Traffic flow: prepend

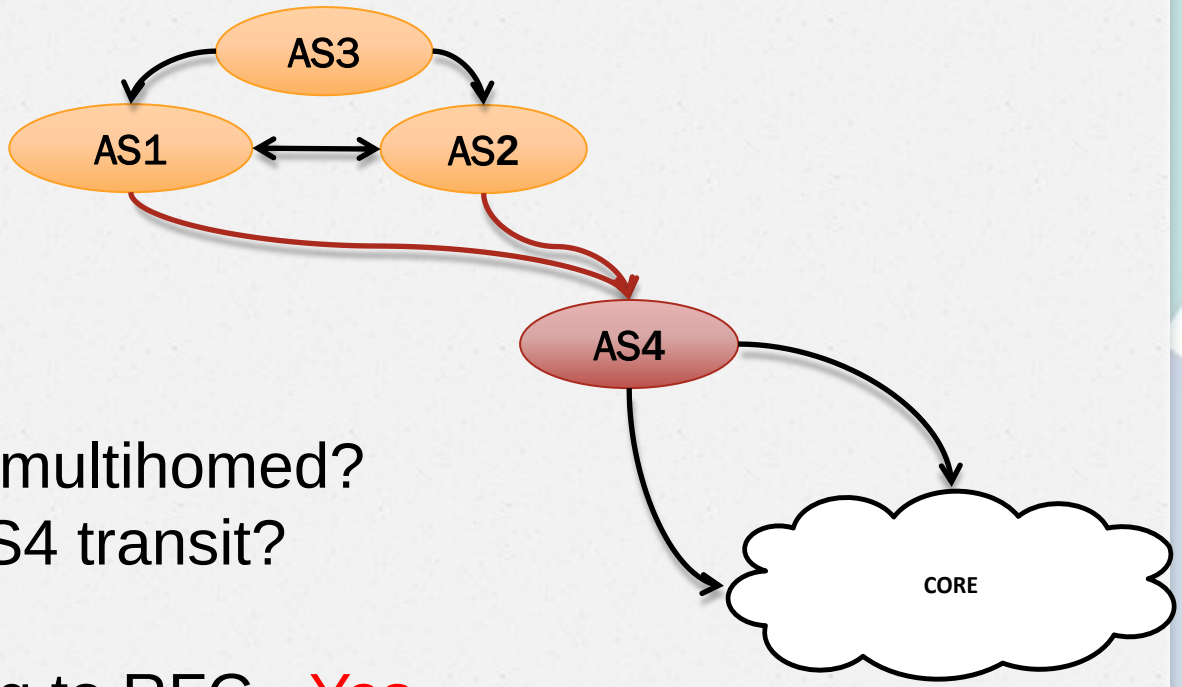


«Дерни за веревочку, дверка откроется»… а может быть, и нет

# AS architecture design

1. Where to place next point of presence?
2. How to forecast the vector/amount of traffic flow?

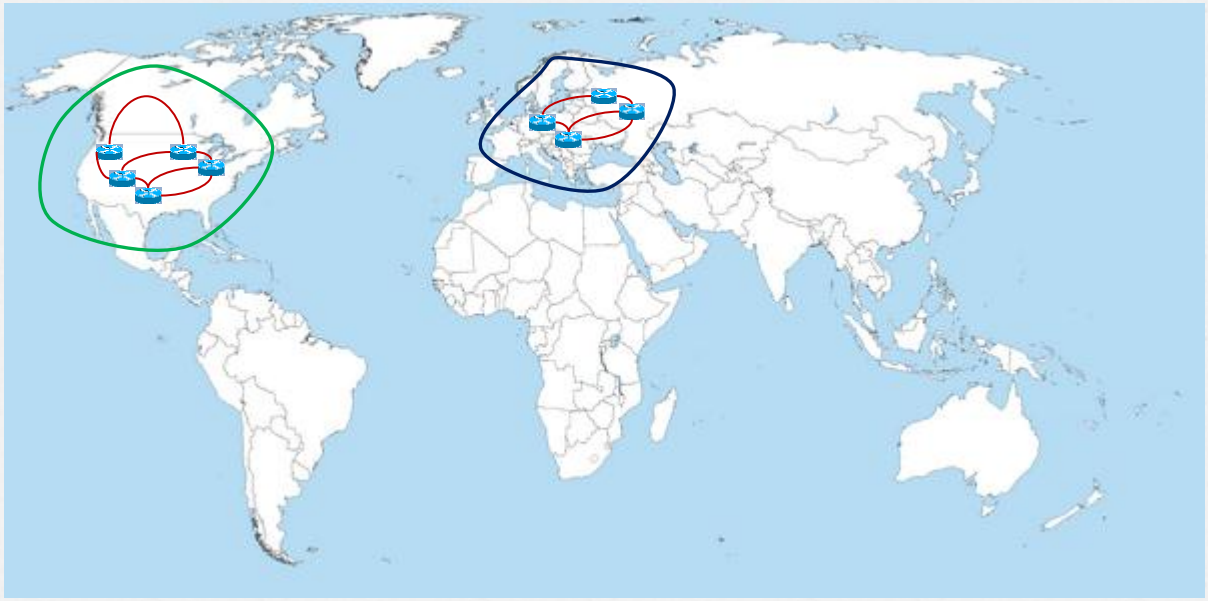
# AS types




Is AS3 multihomed?
Is AS4 transit?

According to RFC - Yes

# AS with separate parts



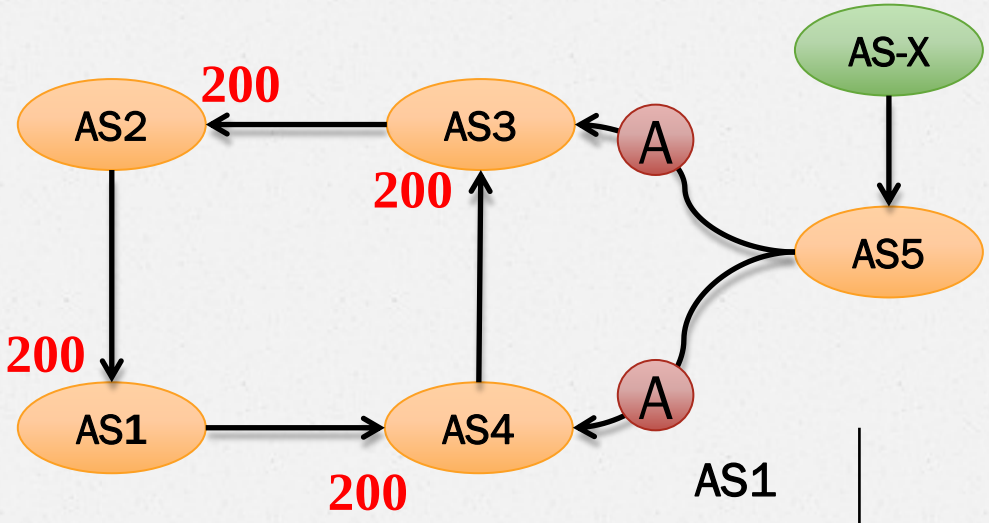
Two ASes with different route policy under one AS number! Transnational?

# BGP Route Loops

Built-in defense for static loops

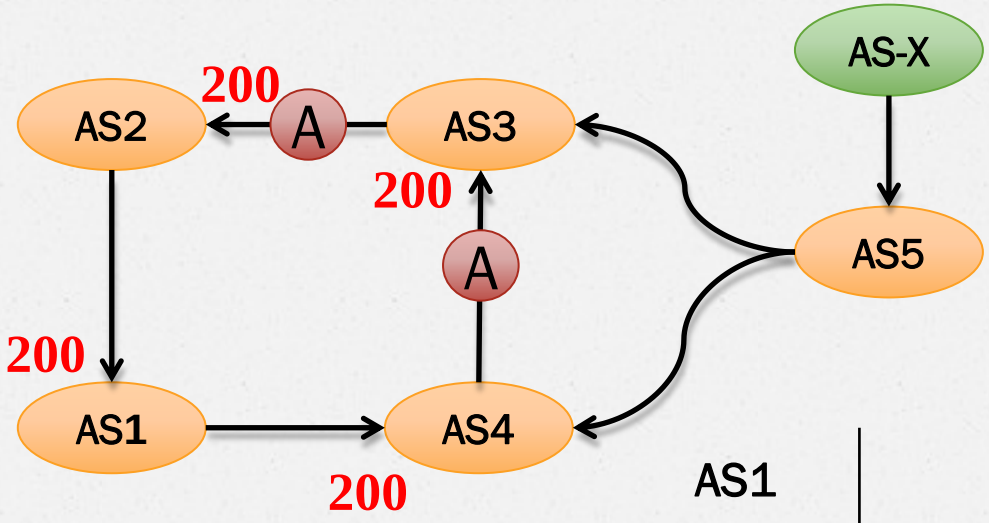
Dynamic loops!

# BGP Route Loops



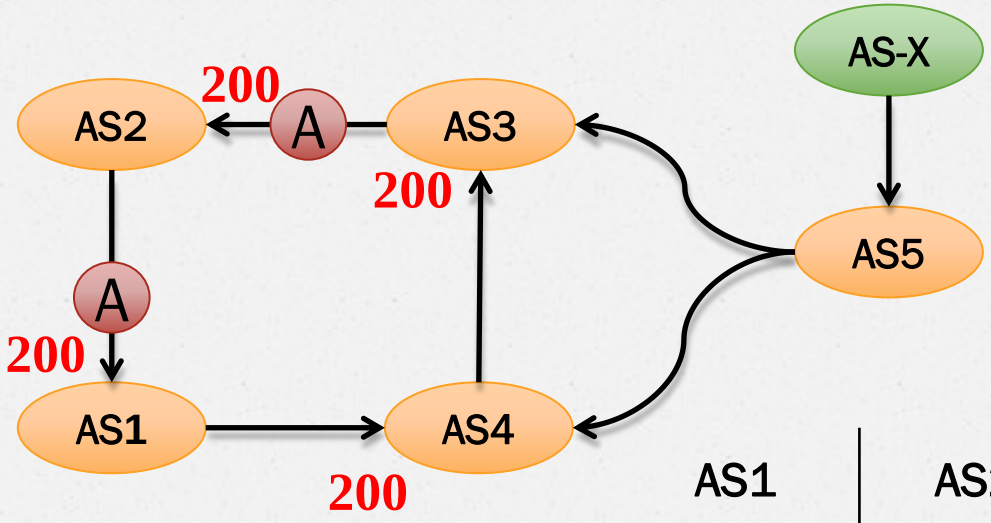

| | |
|---|---|
| AS1 | -- |
| AS2 | -- |
| AS3 | AS5 AS-X |
| AS4 | AS5 AS-X |

# BGP Route Loops



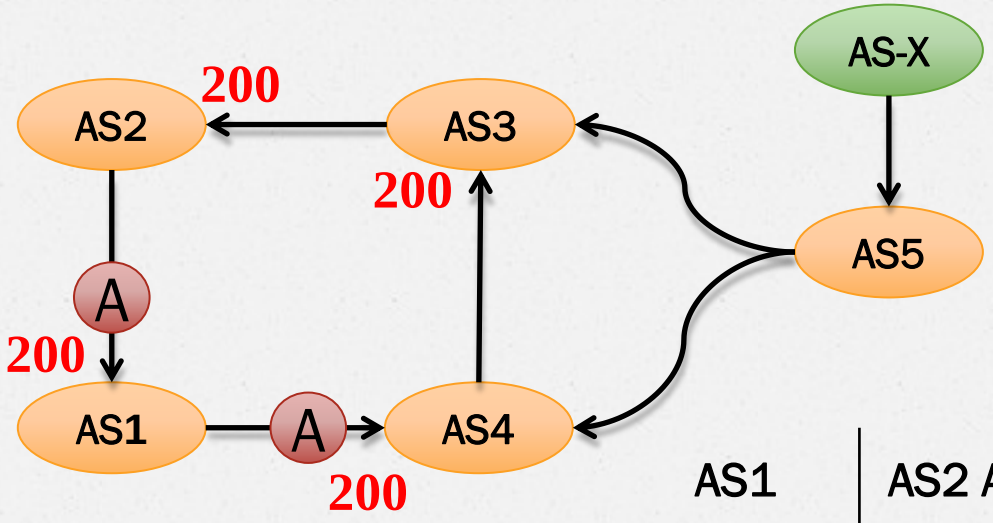

| | |
|---|---|
| AS1 | -- |
| AS2 | AS3 AS5 AS-X |
| AS3 | AS4 AS5 AS-X |
| AS4 | AS5 AS-X |

# BGP Route Loops



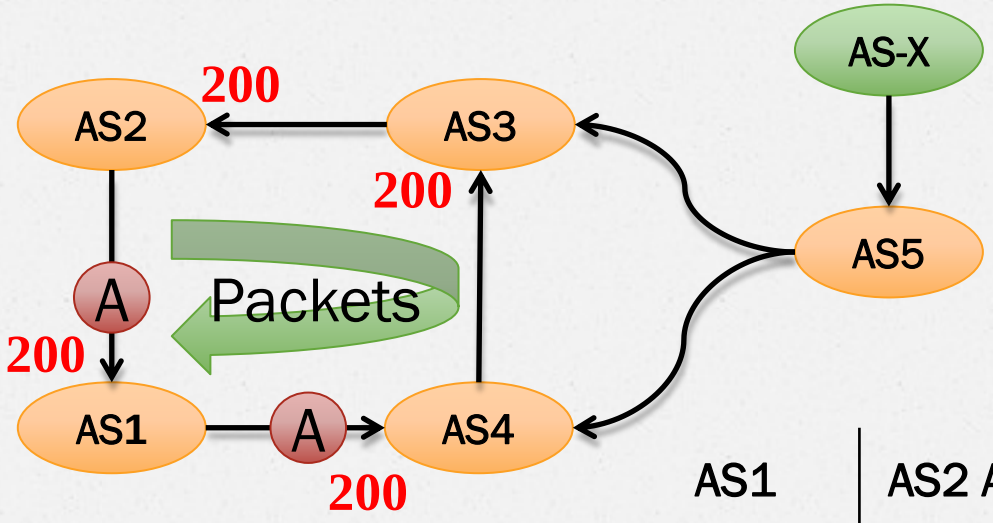

| | |
|---|---|
| AS1 | AS2 AS3 AS5 AS-X |
| AS2 | AS3 AS4 AS5 AS-X |
| AS3 | AS4 AS5 AS-X |
| AS4 | AS5 AS-X |

# BGP Route Loops



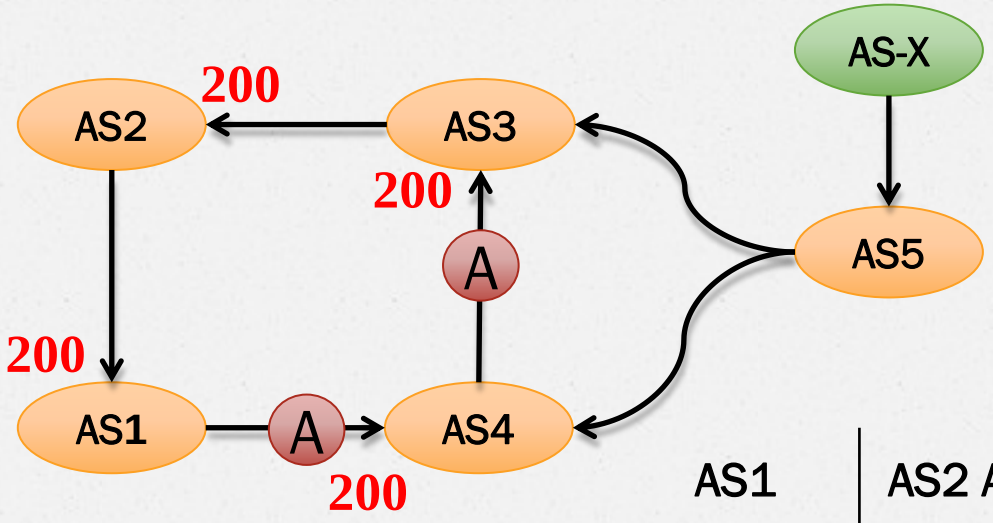

| | |
|---|---|
| AS1 | AS2 AS3 AS4 AS5 AS-X |
| AS2 | AS3 AS4 AS5 AS-X |
| AS3 | AS4 AS5 AS-X |
| AS4 | AS1 AS2 AS3 AS5 AS-X |

# BGP Route Loops




| | |
|---|---|
| AS1 | AS2 AS3 AS4 AS5 AS-X |
| AS2 | AS3 AS4 AS5 AS-X |
| AS3 | AS4 AS5 AS-X |
| AS4 | AS1 AS2 AS3 AS5 AS-X |

# BGP Route Loops




| | |
|---|---|
| AS1 | AS2 AS3 AS4 AS5 AS-X |
| AS2 | AS3 AS4 AS5 AS-X |
| AS3 | AS5 AS-X |
| AS4 | AS5 AS-X |

Again!

# BGP Route Loops

Built-in defense for static loops

Dynamic loops!

- Packet loss
- BGP Announce noise

# Breaking down

1. Route flap
2. Change prepend policy

   AS-X AS-X
3. Prepend one of ASes in loop

   AS-X AS2 AS-X

   Makes AS2 ignore your route

# Breaking down

1. Route flap
2. Change prepend policy

   AS-X AS-X
3. Prepend one of ASes in loop

   AS-X AS2 AS-X

   Makes AS2 ignore your route

How not to fall into another loop?

# One “killer” feature

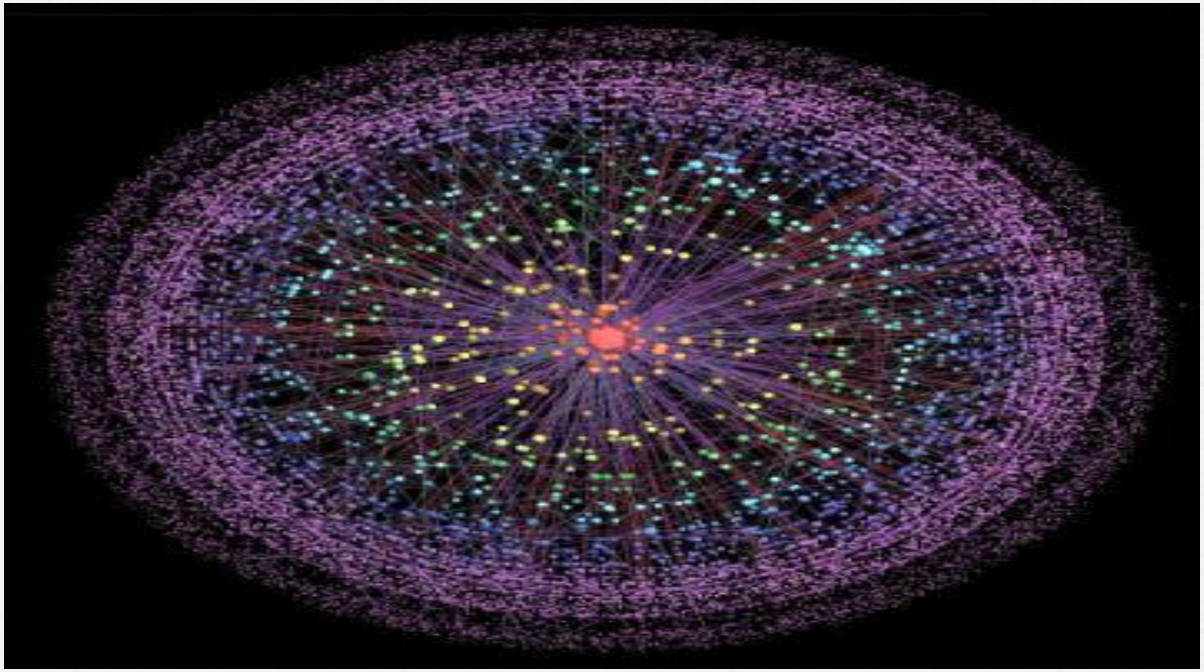
## Autonomous Systems Reverse Map

And there are multiple projects…

# Opte Project

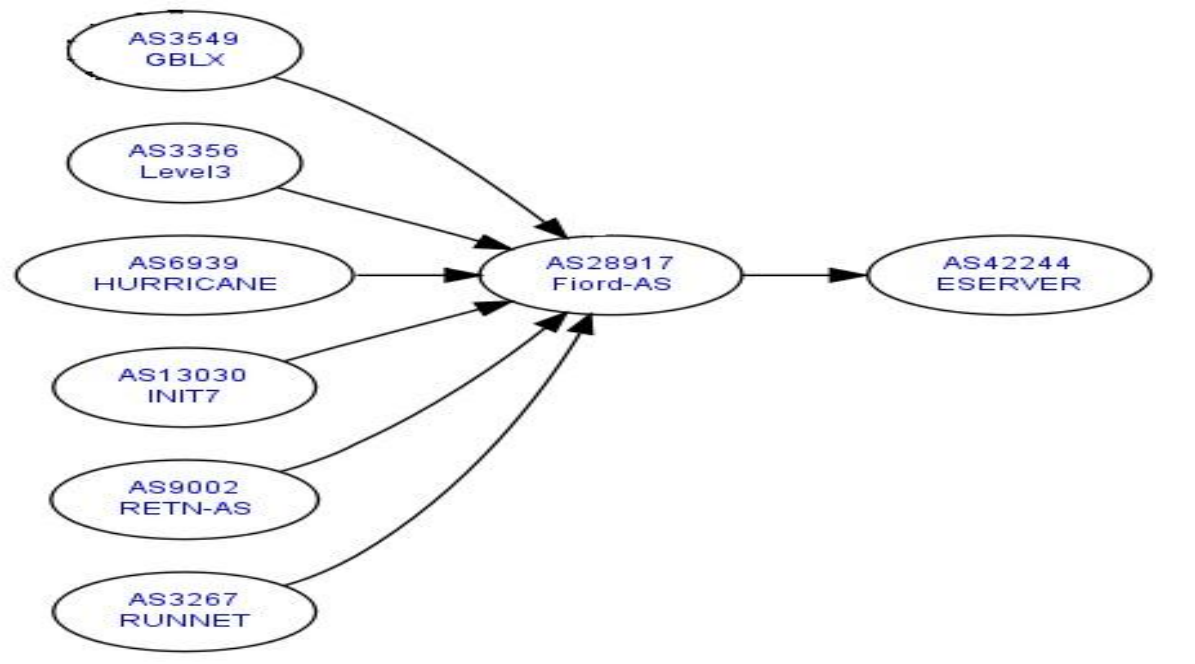

Beautiful!

# DIMES



Interesting!

# ROBTEX




Ok. But what will be used by my AS?

# Missing features

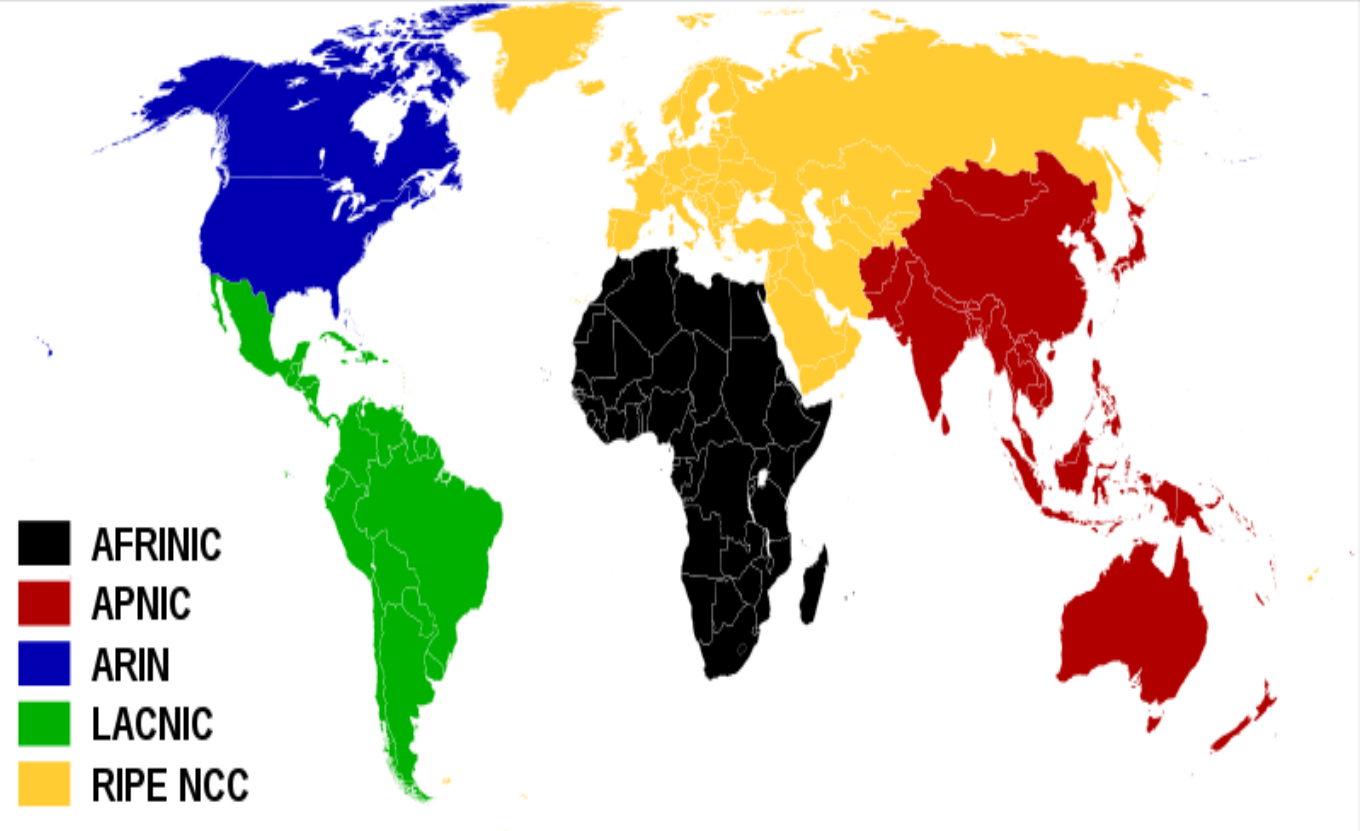
- Physical links discovery

No use of route policy

- Macro map

Show links that are used by somebody, not by your AS.

# WHOIS services



# Incompleteness

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

# Inconsistency

From RIPE DB

aut-num: AS42366

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

# Missing features

- Physical links discovery

No use of route policy;

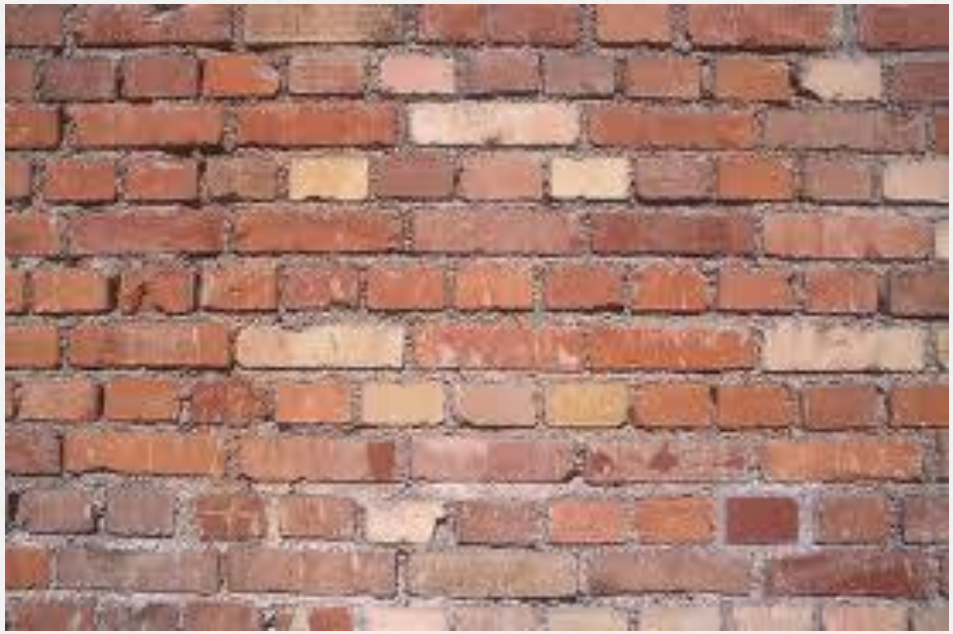
- Macro map

Shows links that are used by somebody, not by your AS;

- Route policy data

Outdated, incomplete.

# Deadlock?



No opportunity for route policy recovery!

# Project goals

- There are more then 400k physical links at interdomain level;
- Only 40k links are used at every moment by each AS;
- The goal is to find out links, that could be used by single AS.

# Route policy model

| | |
|---|---|
| Accept Filters | Local Pref |
| Local Pref | |
| AS_PATH | Prepend model |
| ORIGIN | Priority |
| MED | |
| eBGP vs iBGP | |
| IGP | |
| Router_ID | |

# Route policy model

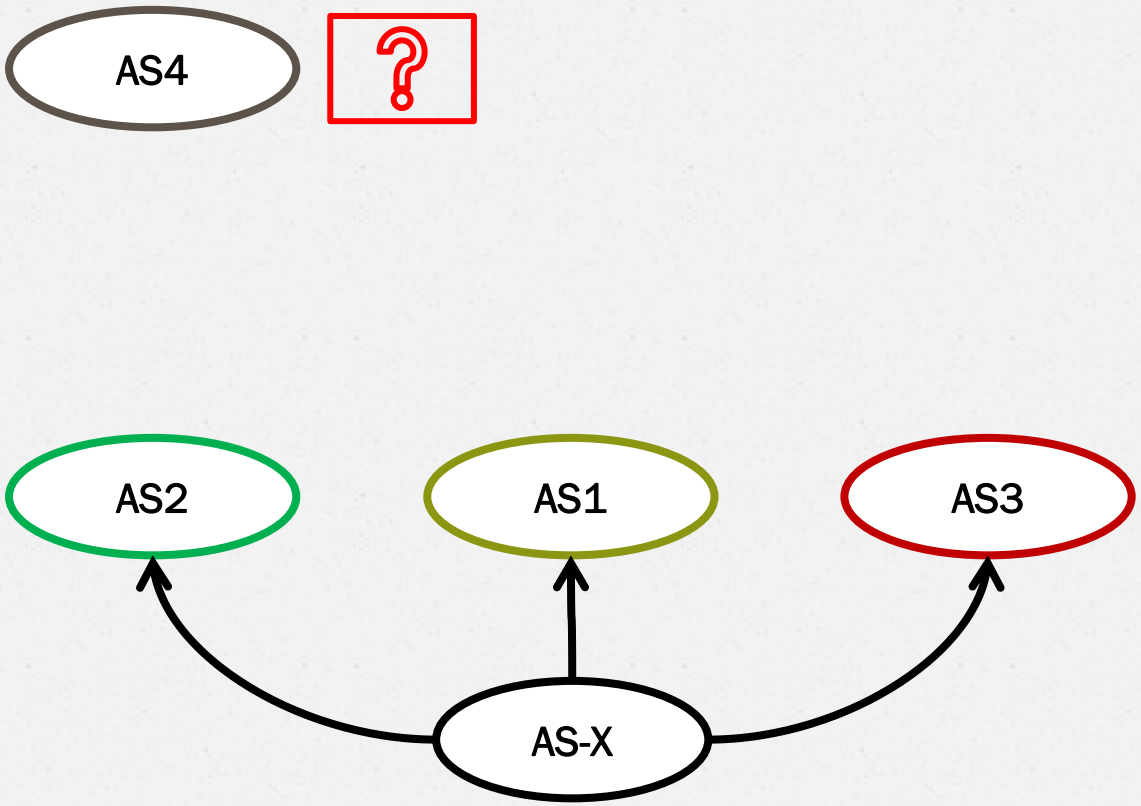
| | |
|---|---|
| Accept Filters | Local Pref |
| Local Pref | |
| AS_PATH | Prepend model |
| ORIGIN | Priority |
| MED | |
| eBGP vs iBGP | |
| IGP | |
| Router_ID | |

Discover every route policy level!

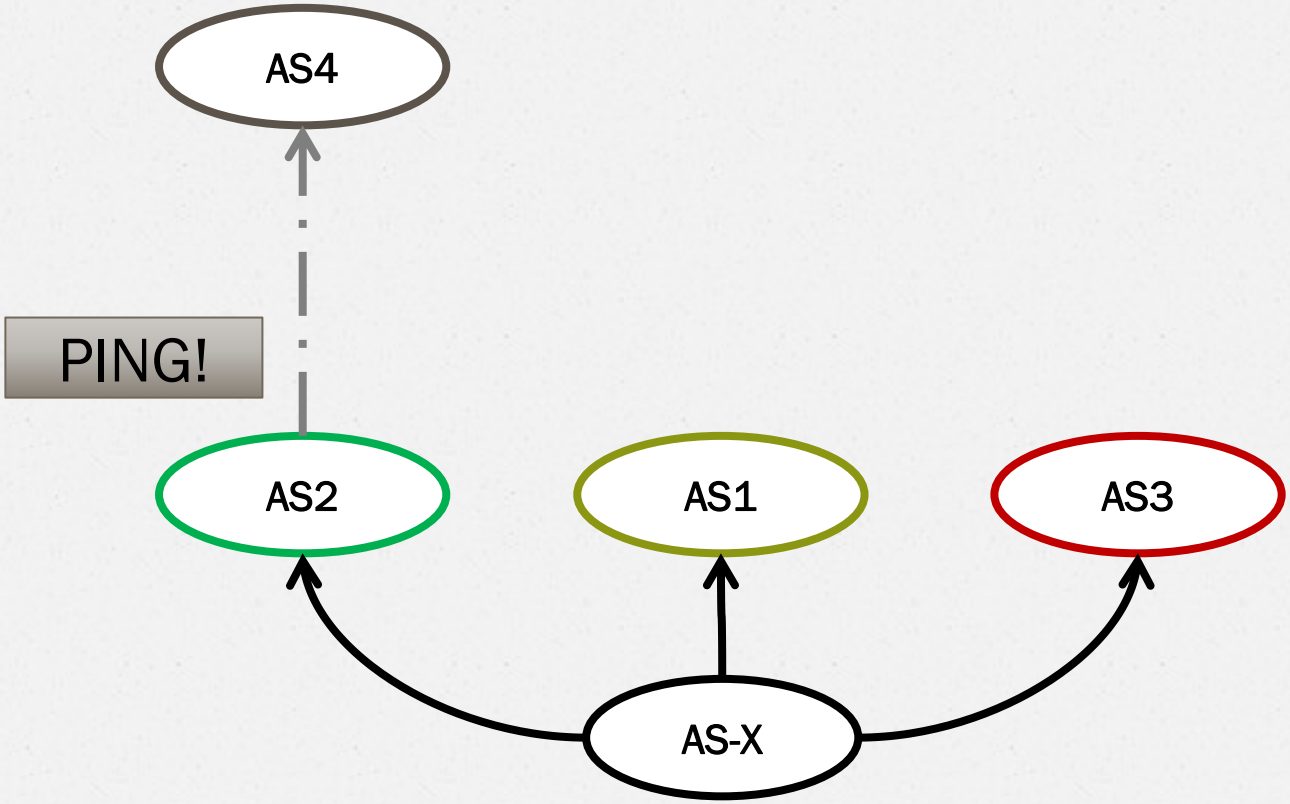
# Active policy discovery

1. Colored AS map
2. Traceroute
3. ping –R (spoofed)

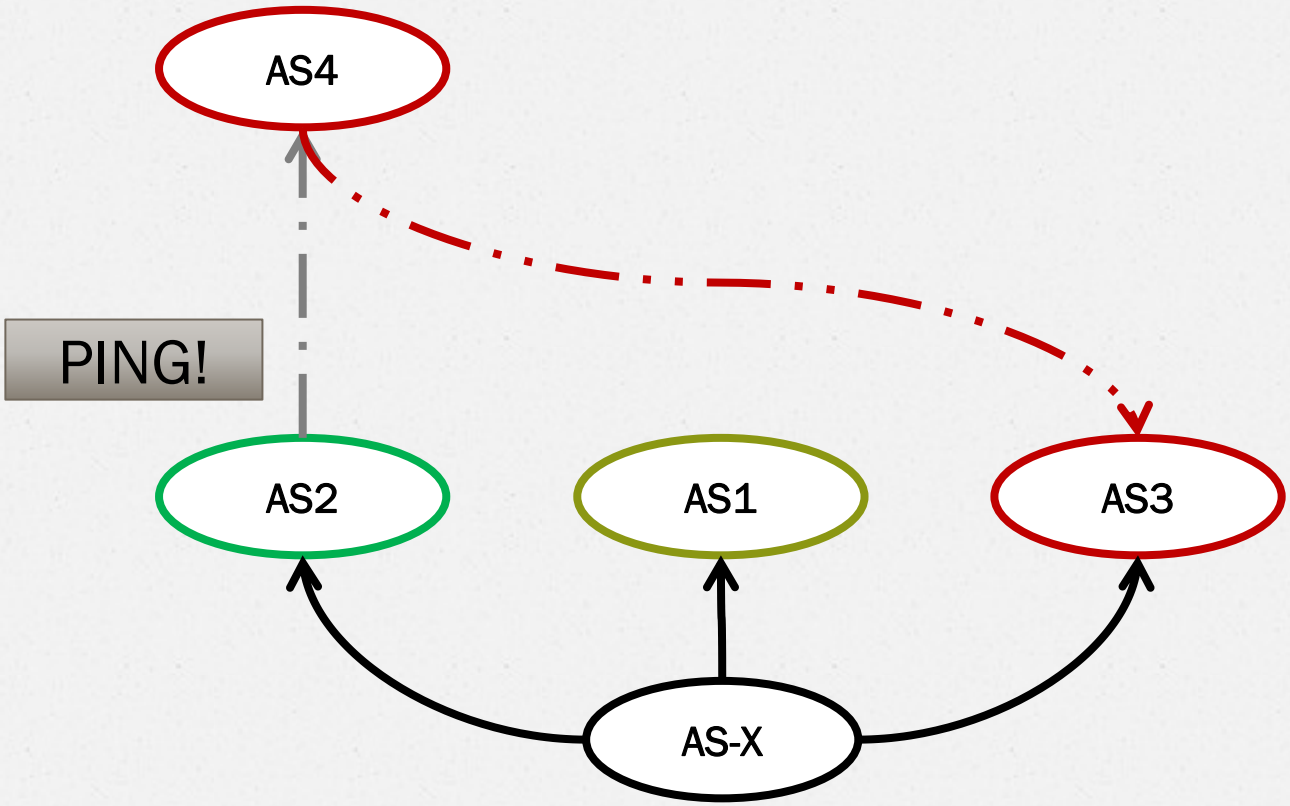
# Colored AS Map



# Colored AS Map



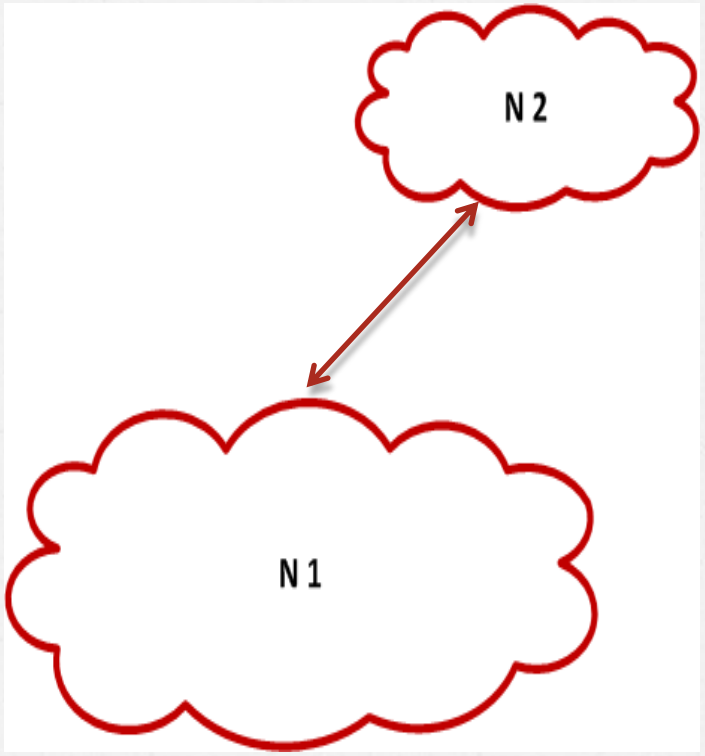
# Colored AS Map



# AS graph properties

BGP router announces only what is used.

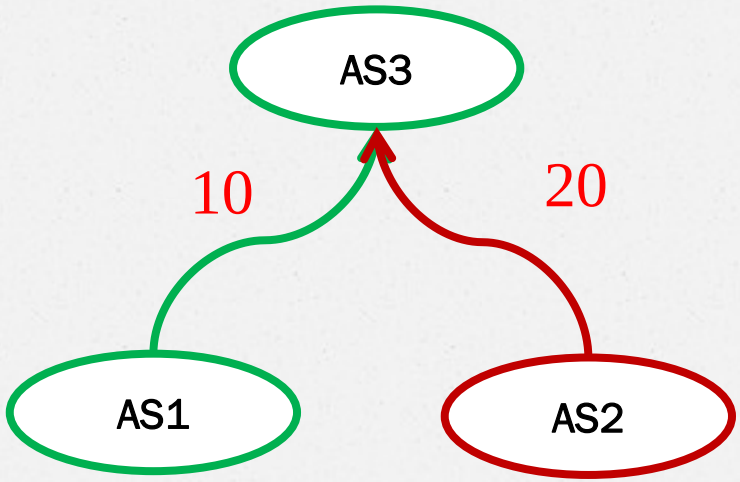
AS graph must be connected by each color!



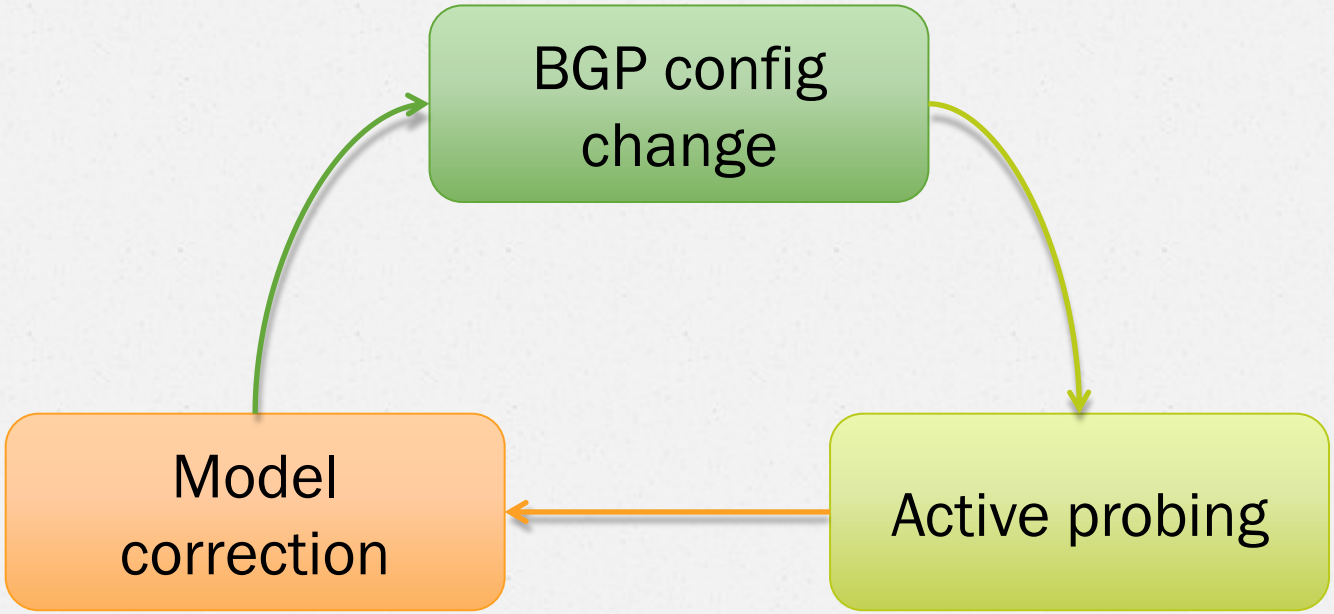
# Model Correction

Increase localpref

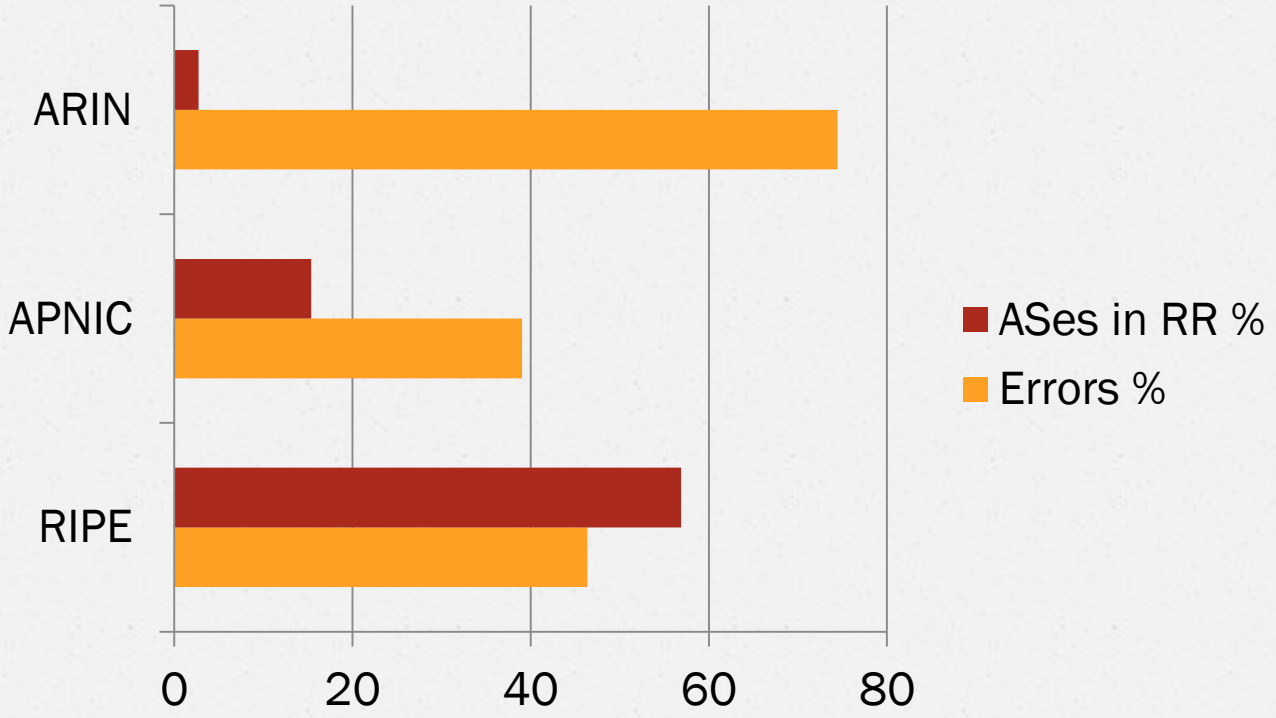
AS1 → AS2



# Verification Process



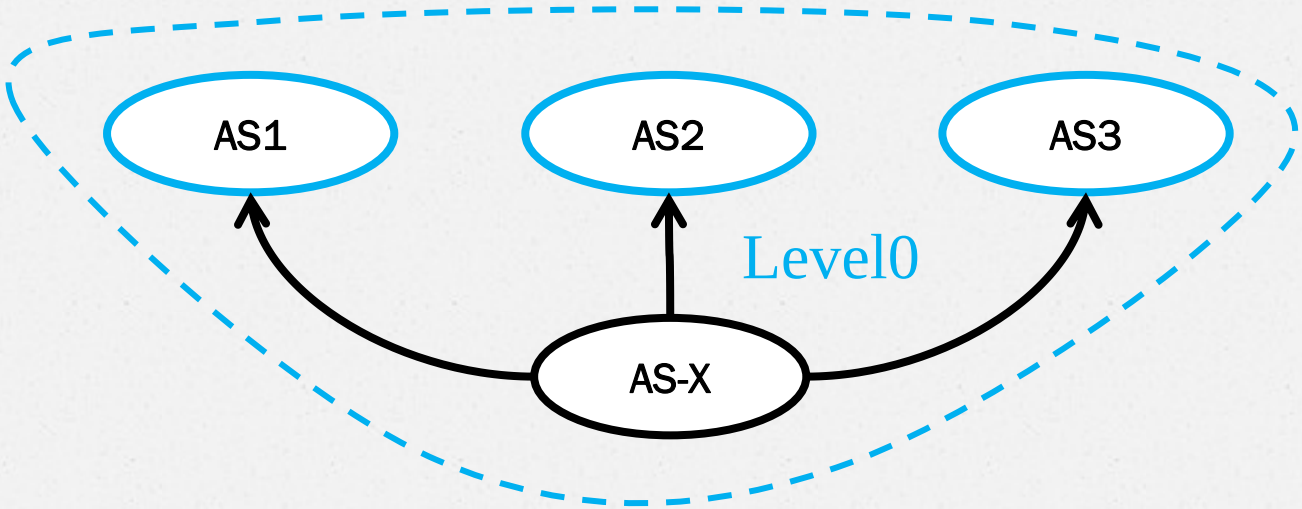
# WHOIS services check



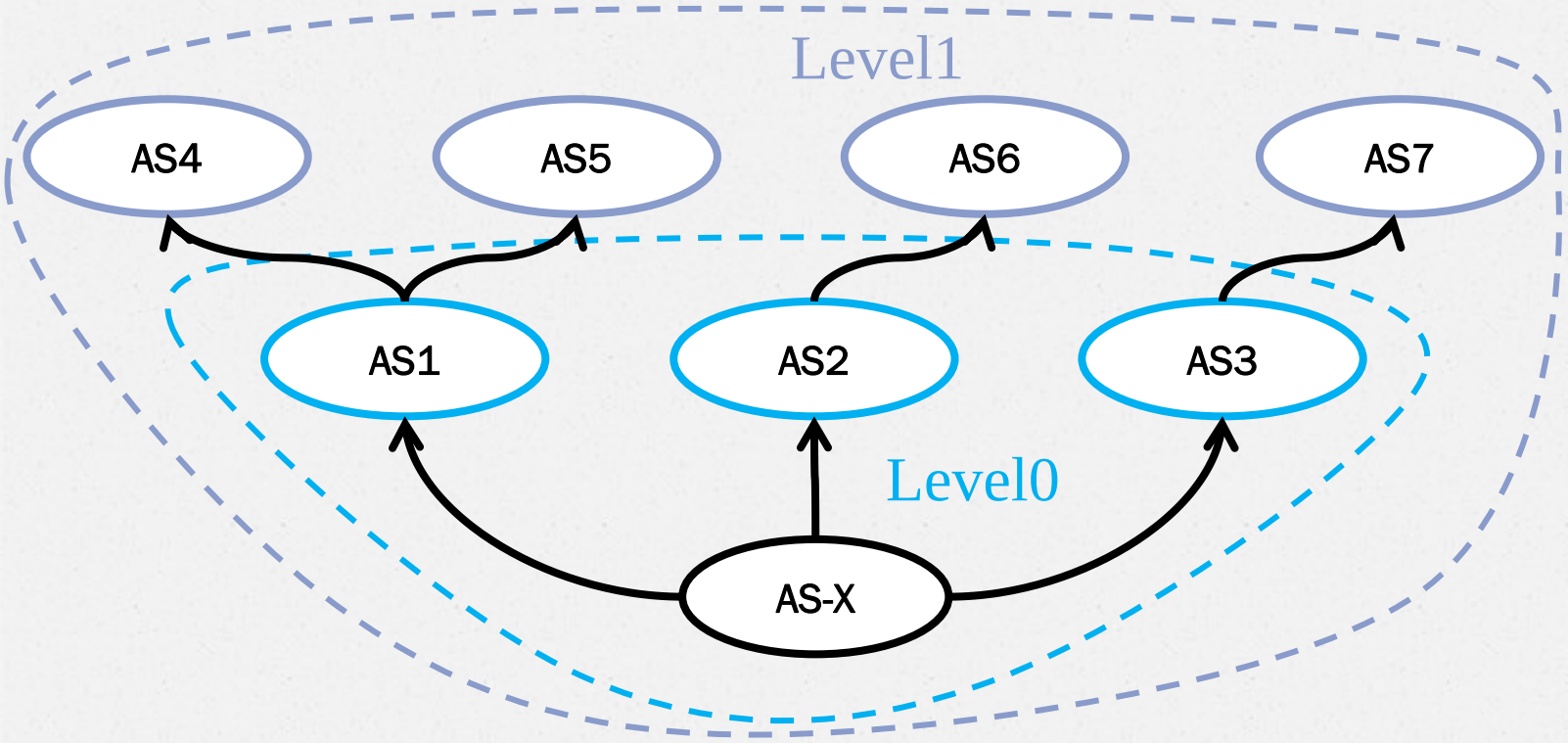
# Amount of neighbours

| AS Number | Description |
|---|---|
| 12389 | ROSTELECOM |
| 9002 | RETN |
| 20485 | TRANSTELECOM |
| 6854 | SYNTERRA |
| 3216 | SOVAM |
| 8732 | COMCOR |
| 31133 | MegaFon |
| 2854 | ROSPRINT |
| 39792 | ANDERS |

# AS connectivity

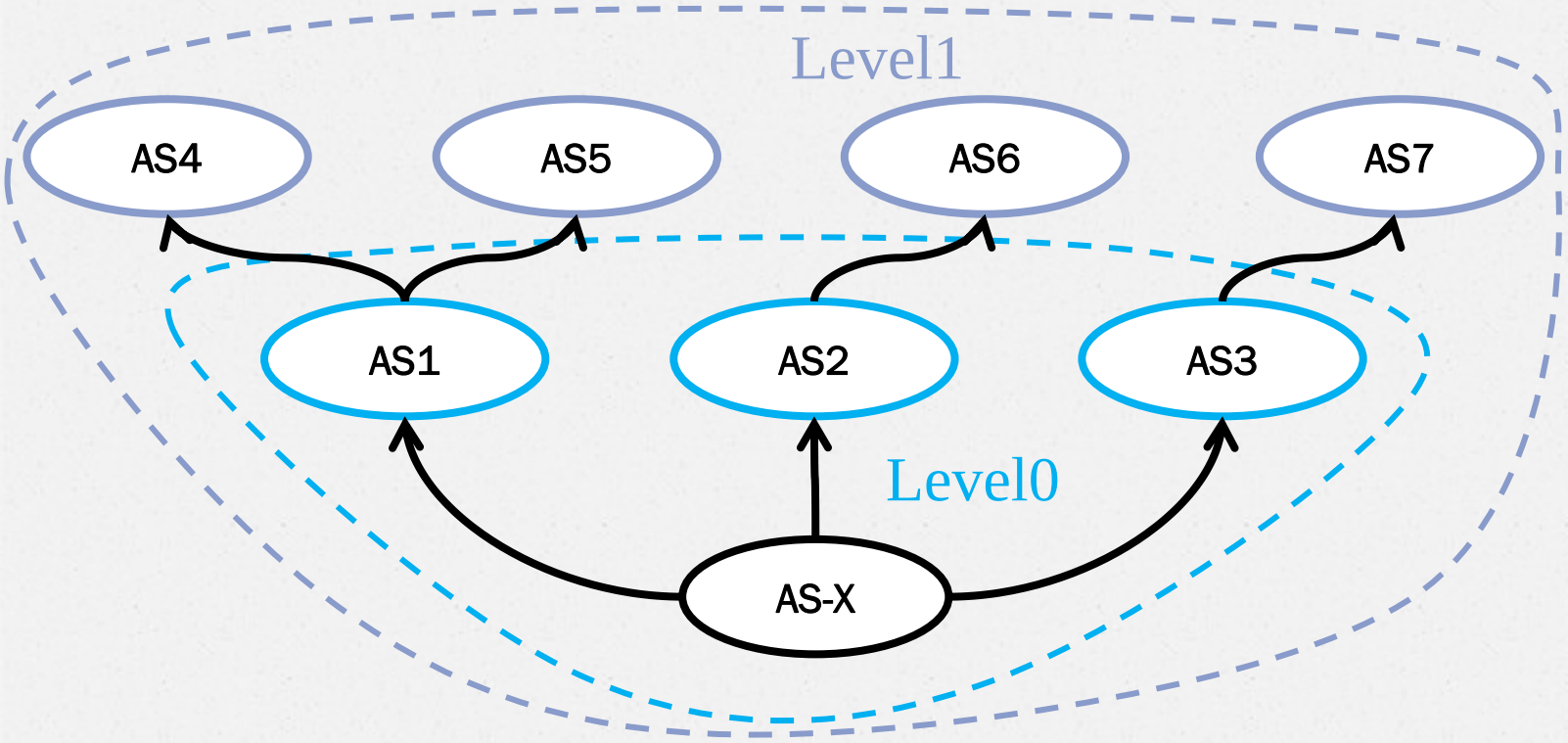


# AS connectivity



# AS connectivity

$$Degree(ASX) = \sum SizeOf(Level_i) * i$$



# Top AS connectivity

| AS Number | Description |
|---|---|
| 12389 | ROSTELECOM |
| 9002 | RETN |
| 20485 | TRANSTELECOM |
| 31133 | MegaFon |
| 3216 | SOVAM |
| 6854 | SYNTERRA |
| 8744 | STARTTELECOM |
| 39792 | ANDERS |
| 8732 | COMCOR |

# AS-QRATOR

| | Neighbours | Connectivity |
|---|---|---|
| 39792 | 9 | 8 |
| 41095 | 70 | 520 |
| 9002 | 2 | 2 |

It is balanced!

# Results

- Policy recovery is impossible;
- Active policy discovery is possible;
- There is unique graph for every AS;
- The only opportunity for engineering at interdomain routing level.

# Keep your WHOIS records up to date

Pretty please…

# Thank you for listening!

Questions?