Detecting BGP hijacks in 2014

Guillaume Valadon & Nicolas Vivet

Agence nationale de la sécurité des systèmes d'information

http://www.ssi.gouv.fr/en

NSC - November 21th, 2014

BGP Hijacking for Cryptocurrency Profit
Reported by Dell SecureWorks on August 7 2014

« From February to May 2014, an hijacker redirected cryptocurrency miners to his own mining pool, earning an estimated $83,000. »

Attack Requirements

- no authentication between a miner and its bitcoin pool
- traffic redirection using BGP prefixes hijacks

BGP 101

What is BGP (Border Gateway Protocol) ?

It is the routing protocol used by all Internet operators.

Some BGP facts

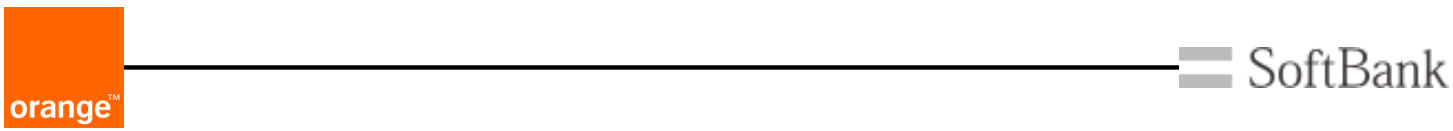
- it runs on 179/TCP
- it informs that an operator is in charge of IP prefixes
  - there is no guarantee that an operator is lying

What is BGP (Border Gateway Protocol) ?

It is the routing protocol used by all Internet operators.

Some BGP facts

- it runs on 179/TCP
- it informs that an operator is in charge of IP prefixes
  - there is no guarantee that an operator is lying
- it interconnects all Internet operators

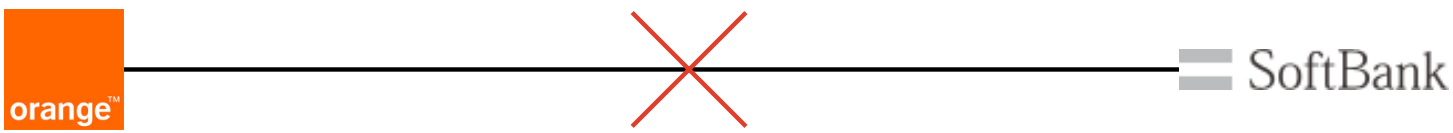


What is BGP (Border Gateway Protocol) ?

It is the routing protocol used by all Internet operators.

Some BGP facts

- it runs on 179/TCP
- it informs that an operator is in charge of IP prefixes
  - there is no guarantee that an operator is lying
- it interconnects all Internet operators

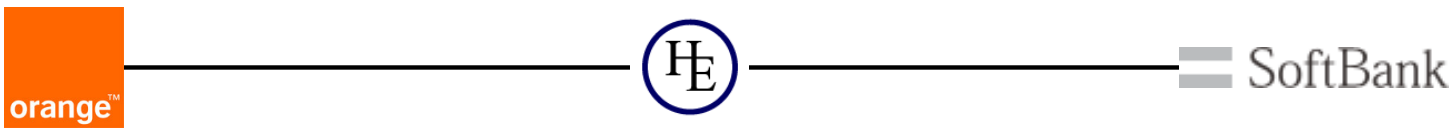


What is BGP (Border Gateway Protocol) ?

It is the routing protocol used by all Internet operators.

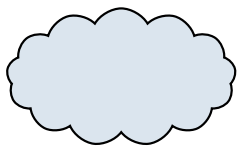
Some BGP facts

- it runs on 179/TCP
- it informs that an operator is in charge of IP prefixes
  - there is no guarantee that an operator is lying
- it interconnects all Internet operators



What Do You Need to Use BGP ?

- a network

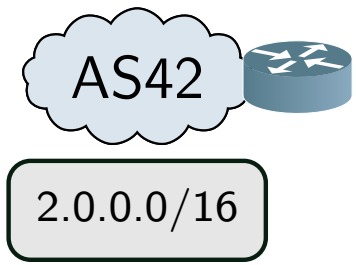


What Do You Need to Use BGP ?

- a network
- an AS number that identifies your network
- an IP prefix

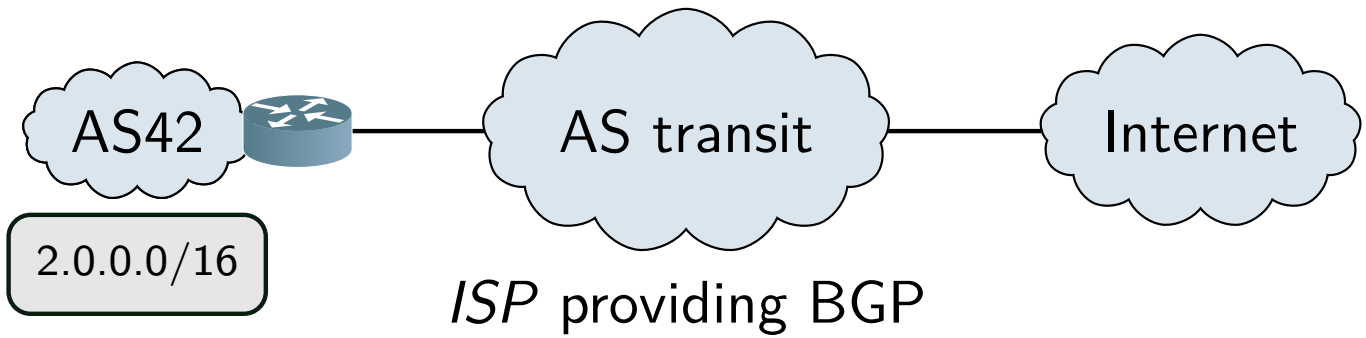
What Do You Need to Use BGP ?

- a network
- an AS number that identifies your network
- an IP prefix
- a BGP router



What Do You Need to Use BGP ?

- a network
- an AS number that identifies your network
- an IP prefix
- a BGP router
- a BGP interconnection



Internet Resources Allocation

AS & prefixes are allocated by Regional Internet Registry:

Europe

Asia

Africa

North America

Latin America & Caribbean

In Europe, per year, an ASN costs 50€ and a /22 50€.

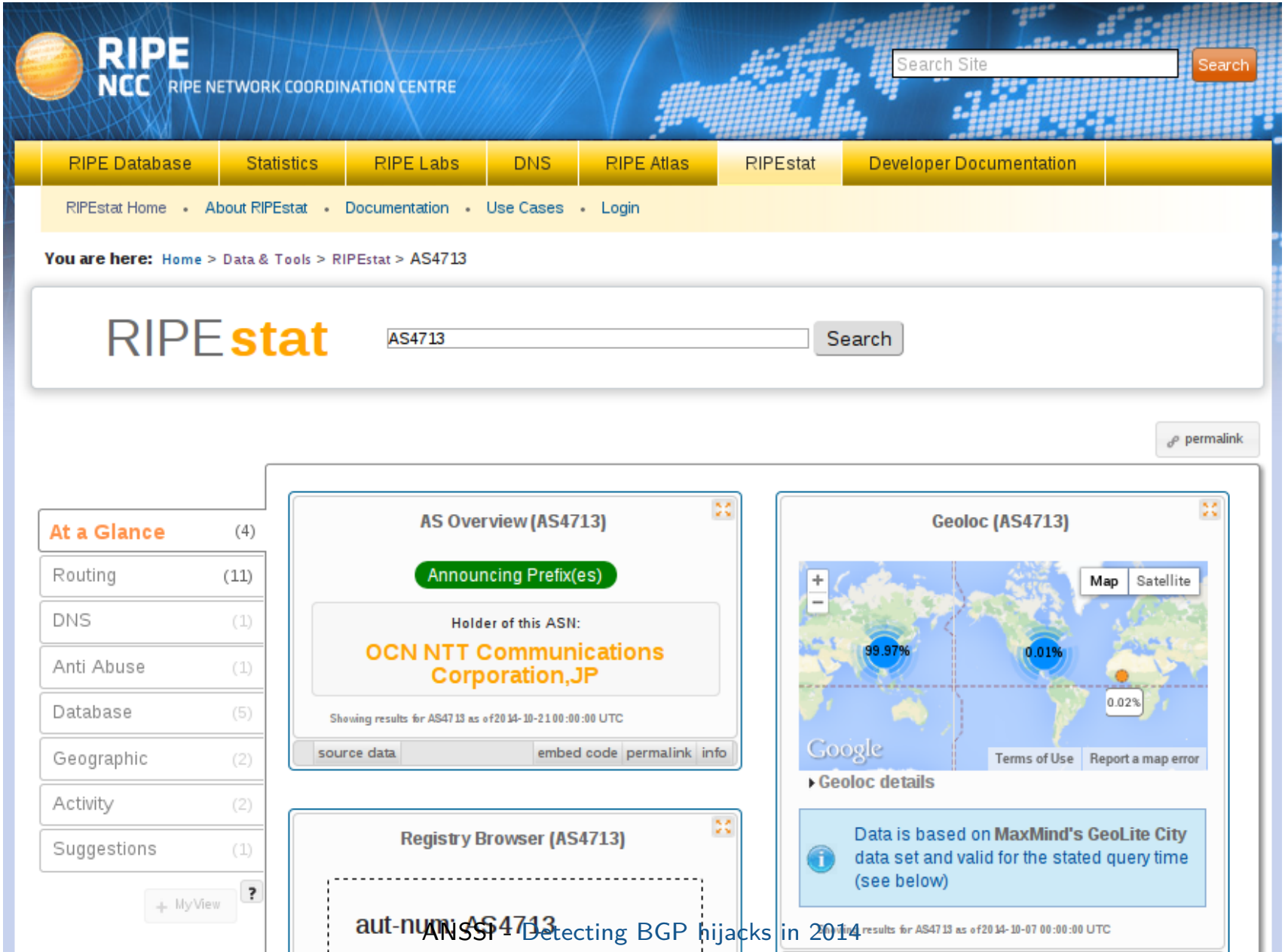
Access to Internet Resources Allocation

The WHOIS protocol

```
$ whois AS4713

aut-num:        AS4713
as-name:        OCN
descr:          NTT Communications Corporation
[..]
country:        JP
admin-c:        AY1361JP
tech-c:         TT10660JP
tech-c:         TT15086JP
changed:        apnic-ftp@nic.ad.jp 19960911
changed:        apnic-ftp@nic.ad.jp 20091113
source:         JPNIC
```

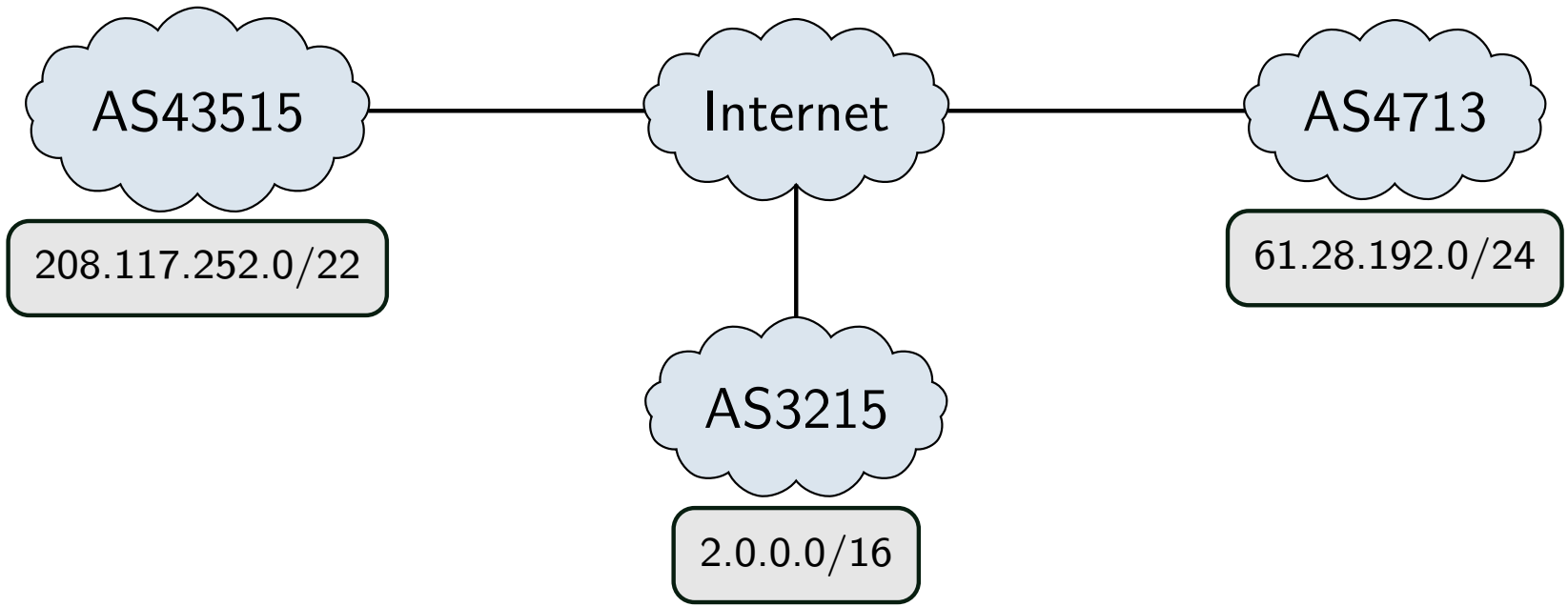
Access to Internet Resources Allocation

https://stat.ripe.net



AS Announces & Removes Prefixes

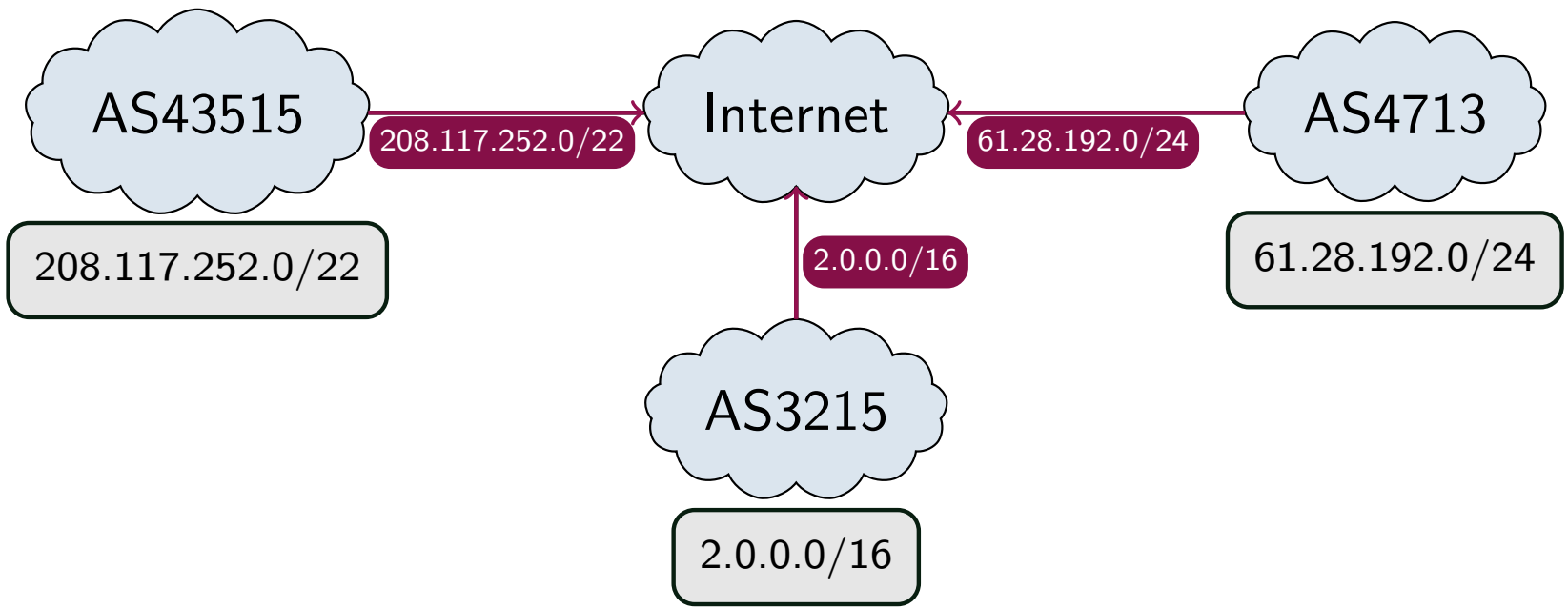
With BGP, an operator uses:



AS Announces & Removes Prefixes

With BGP, an operator uses:

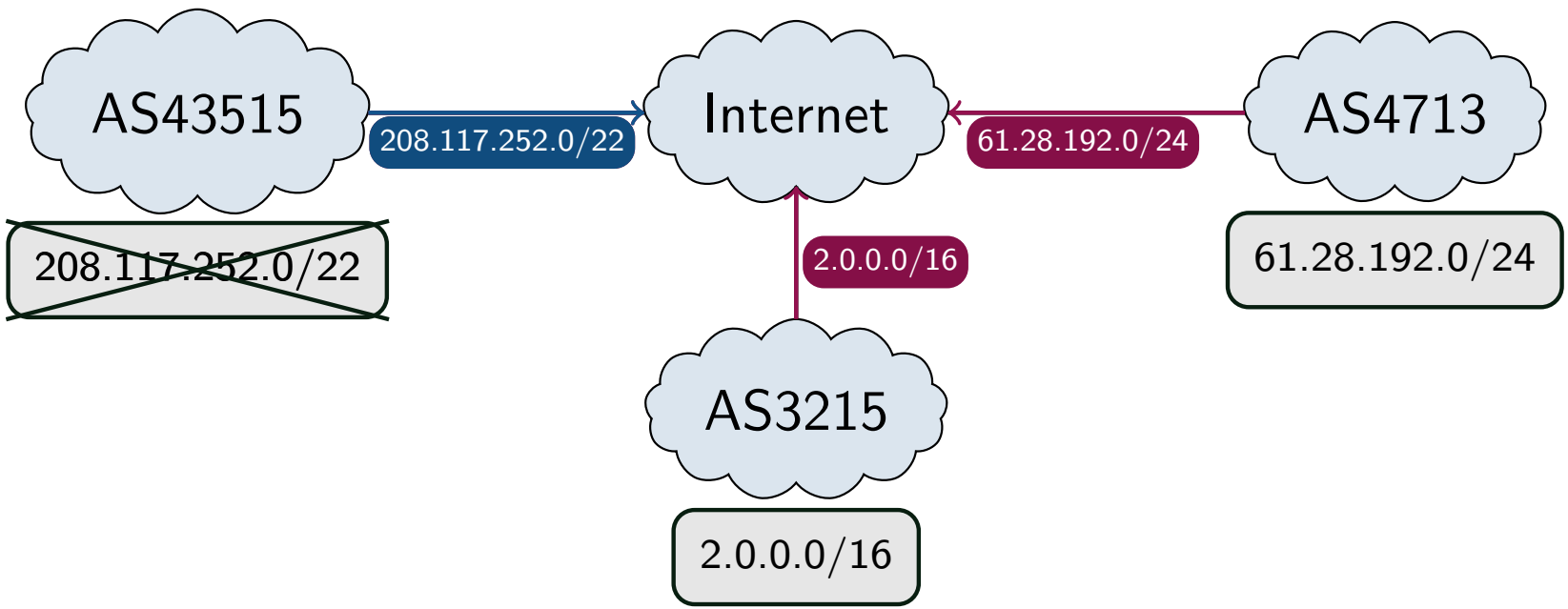
- UPDATE messages to announce its IP prefixes



AS Announces & Removes Prefixes

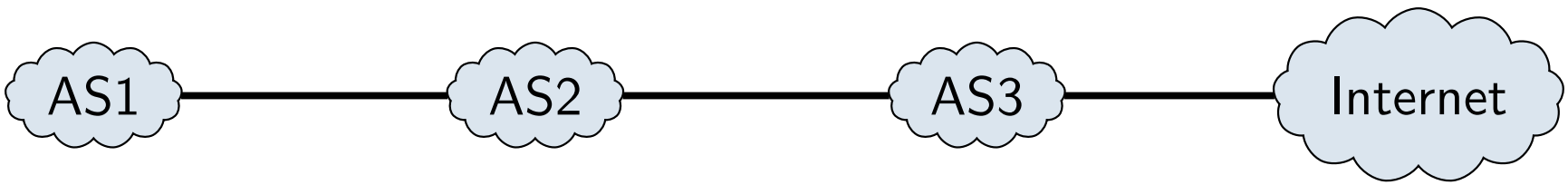
With BGP, an operator uses:

- UPDATE messages to announce its IP prefixes
- WITHDRAW messages to remove its IP prefixes



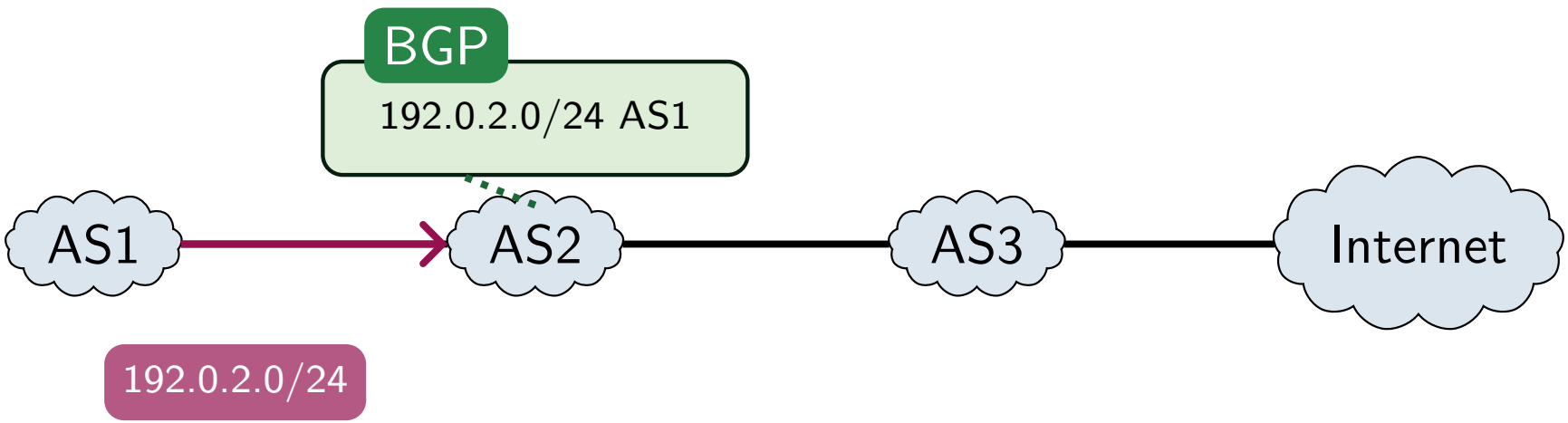
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



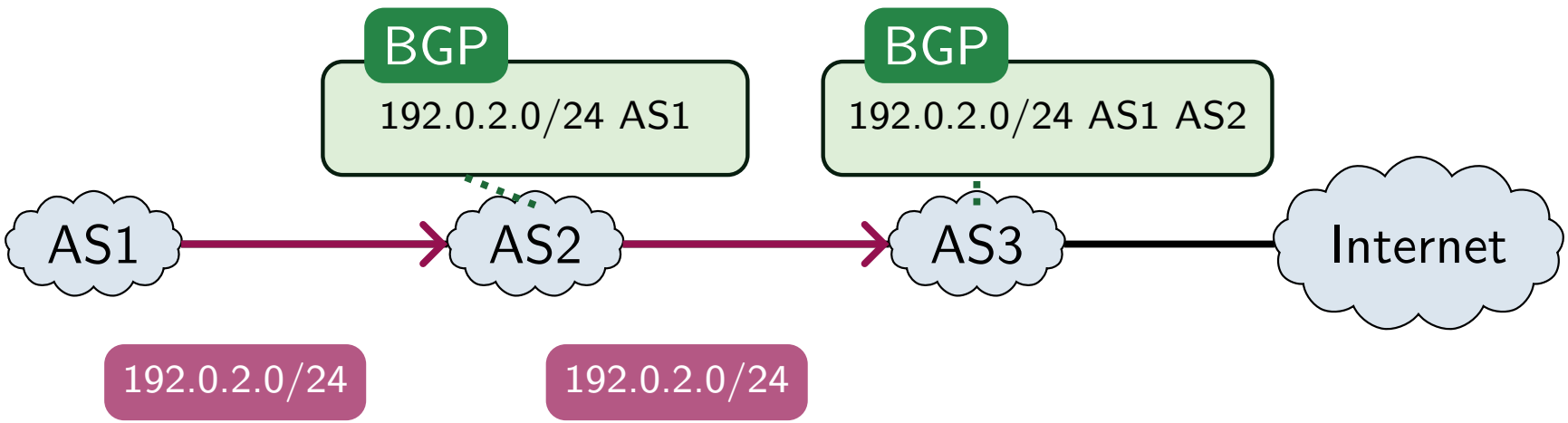
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



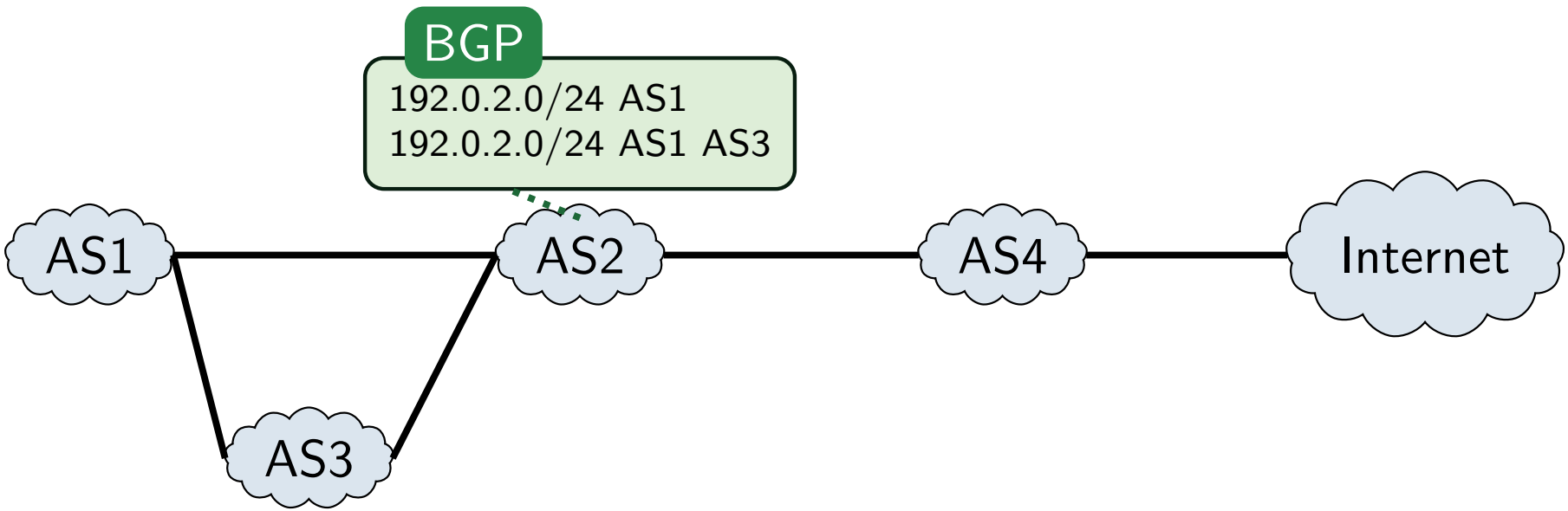
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



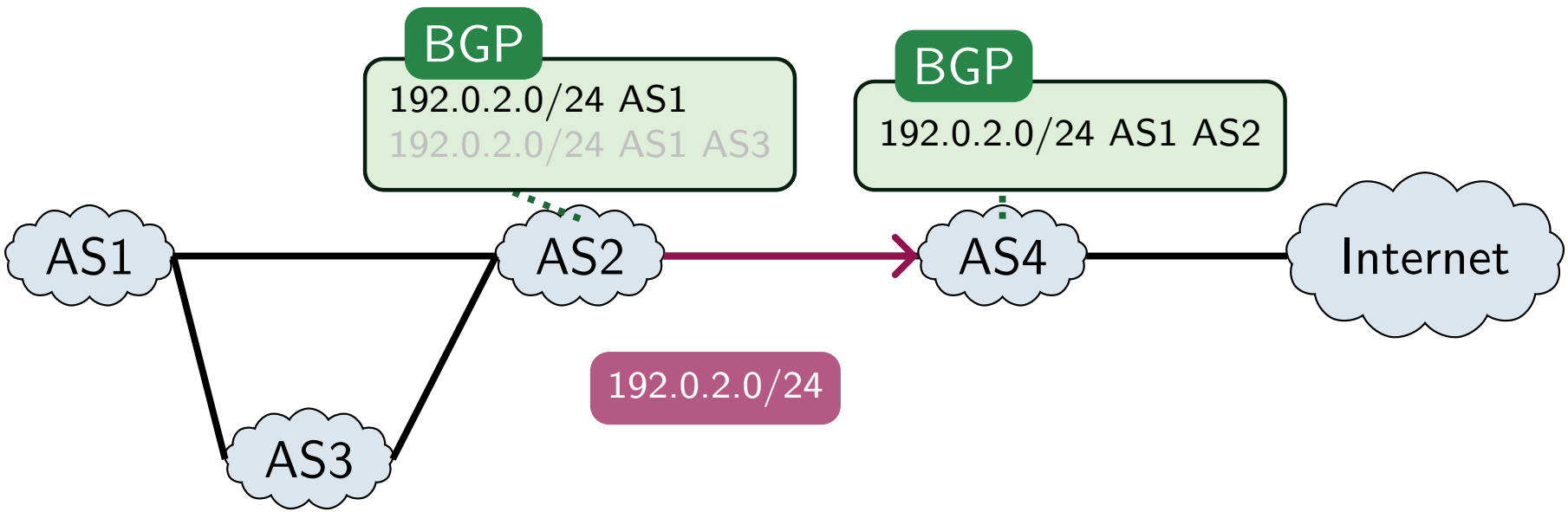
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



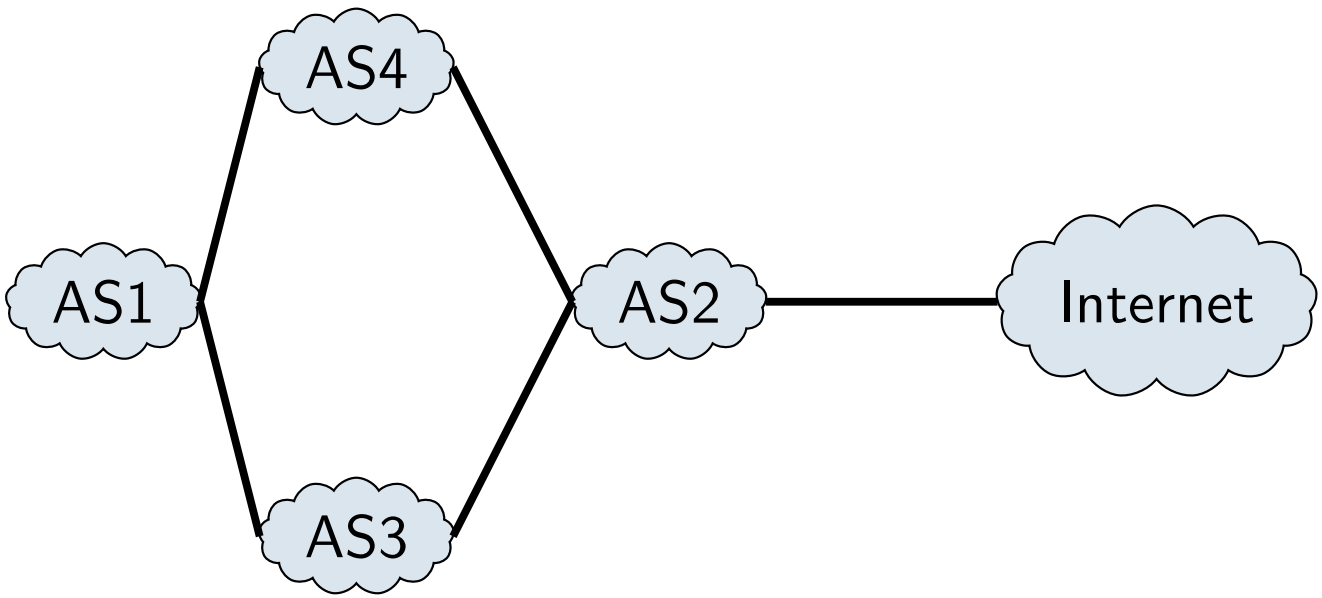
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



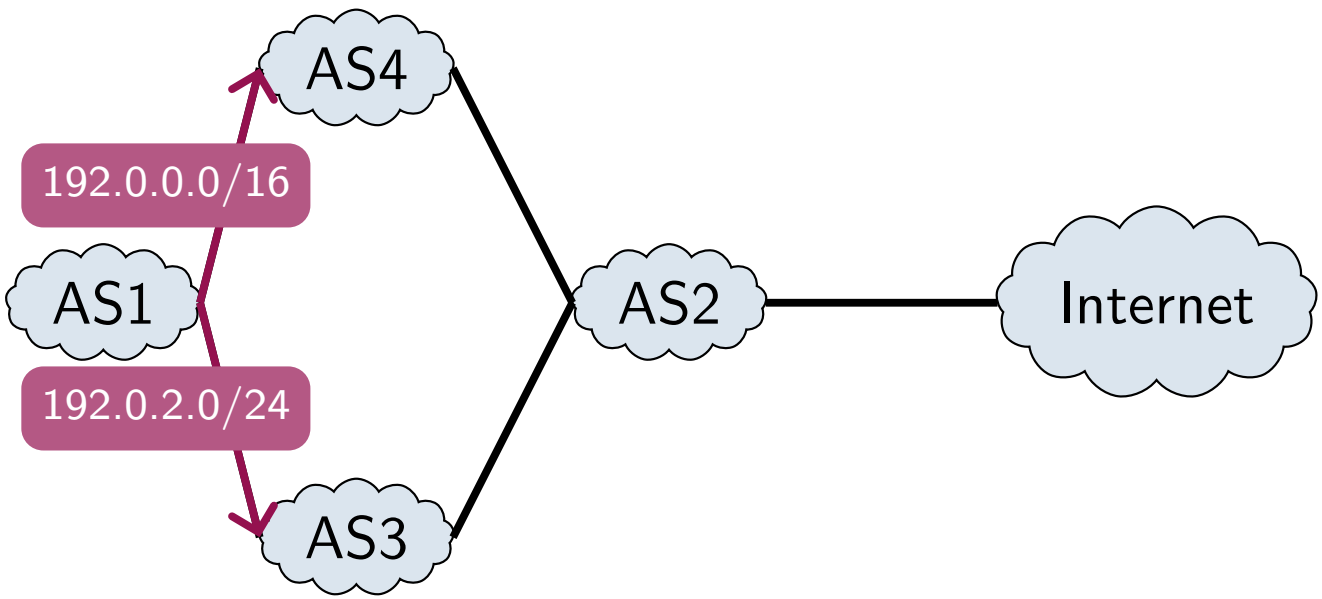
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



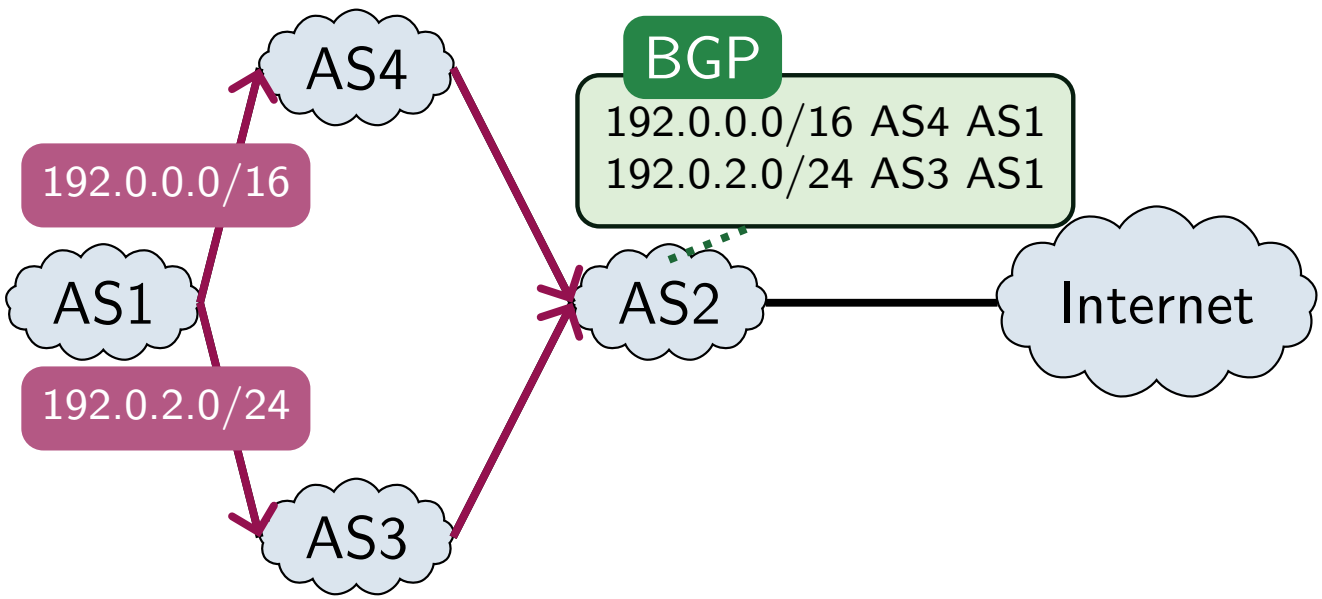
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



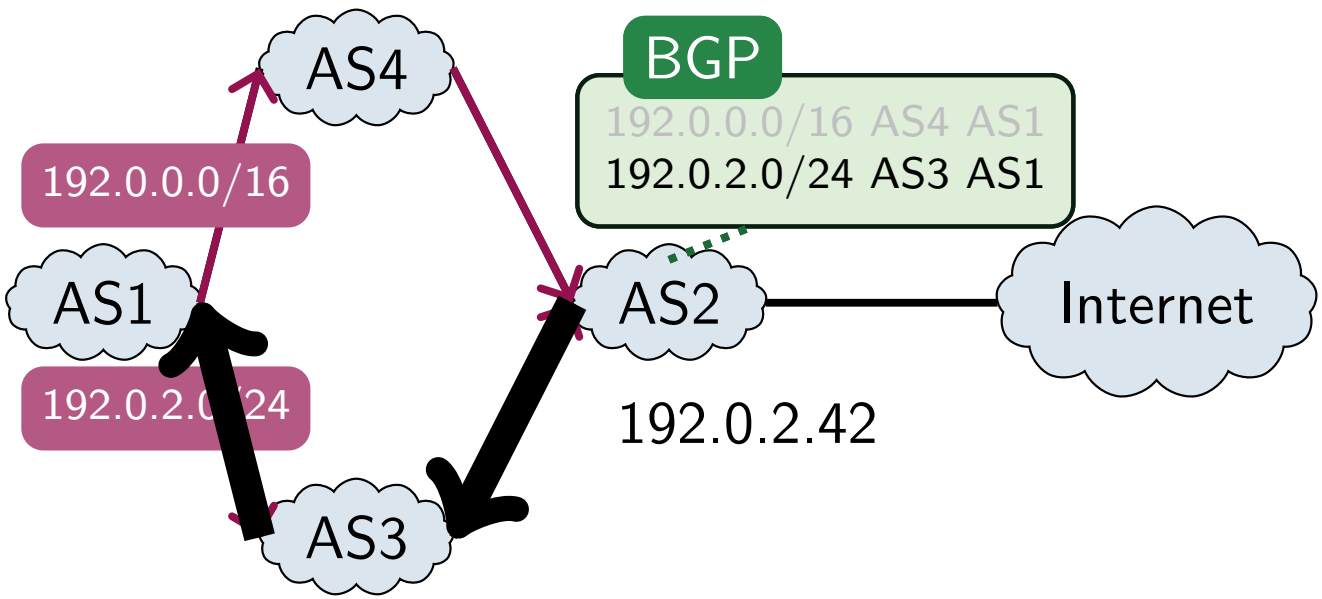
Three Simple BGP Rules

1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



Three Simple BGP Rules

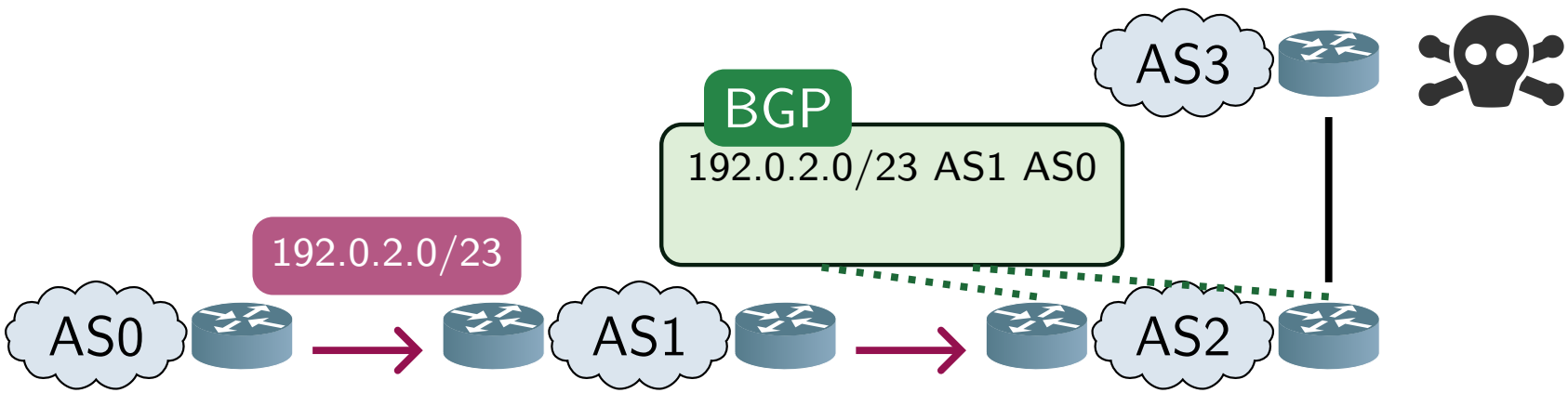
1. messages are forwarded to neighbors, after adding the ASN
2. only the shortest AS path is forwarded
3. packets are sent to the most specific prefix



Hijacks 101

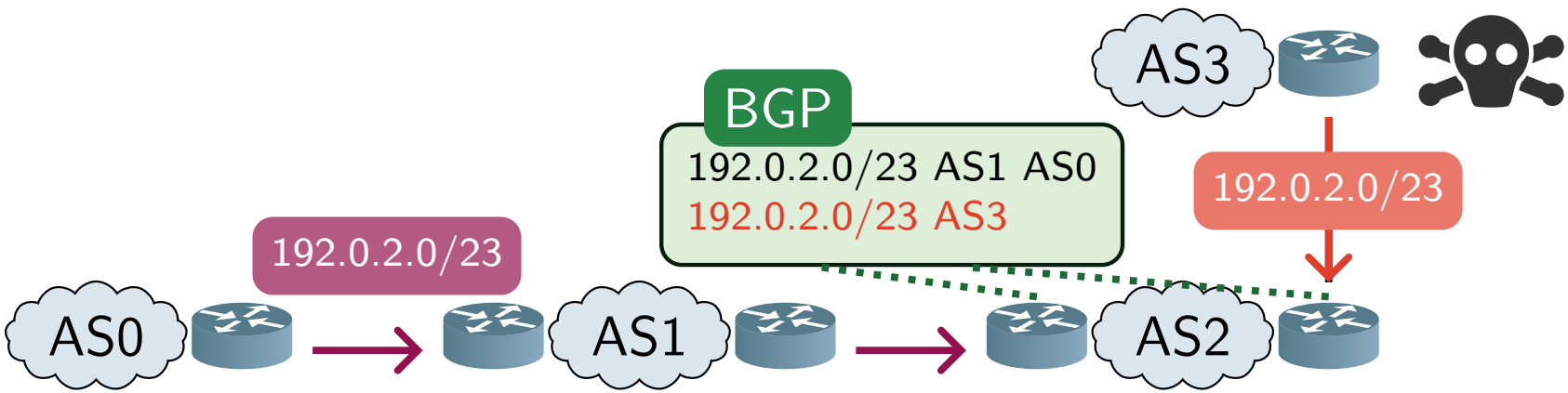
What is a Prefix Hijack?
BGP rule #2 in action

An hijack is a conflicting BGP announcement.



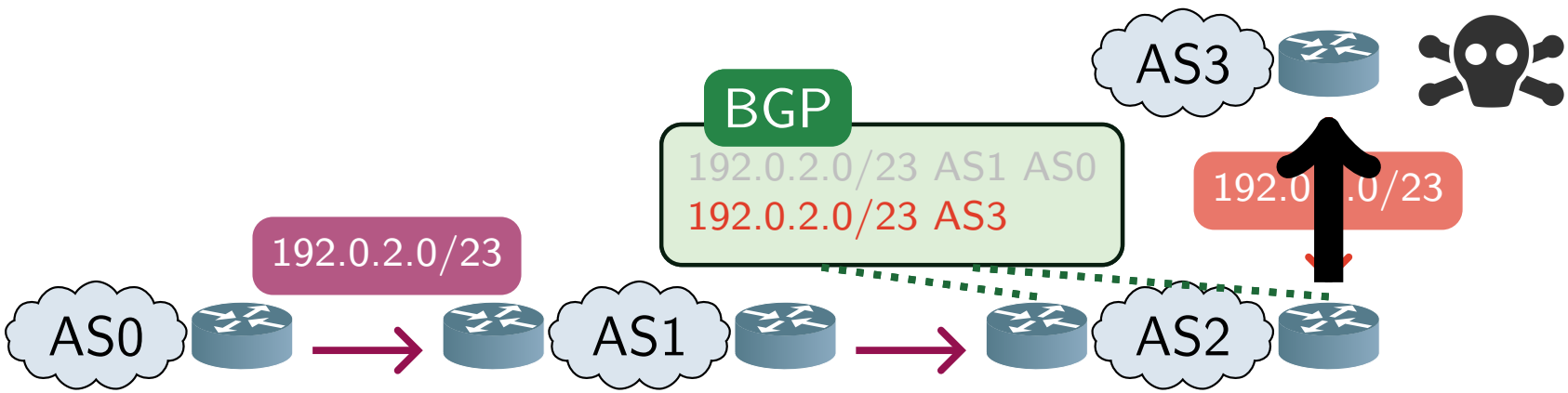
What is a Prefix Hijack?
BGP rule #2 in action

An hijack is a conflicting BGP announcement.



What is a Prefix Hijack?
BGP rule #2 in action

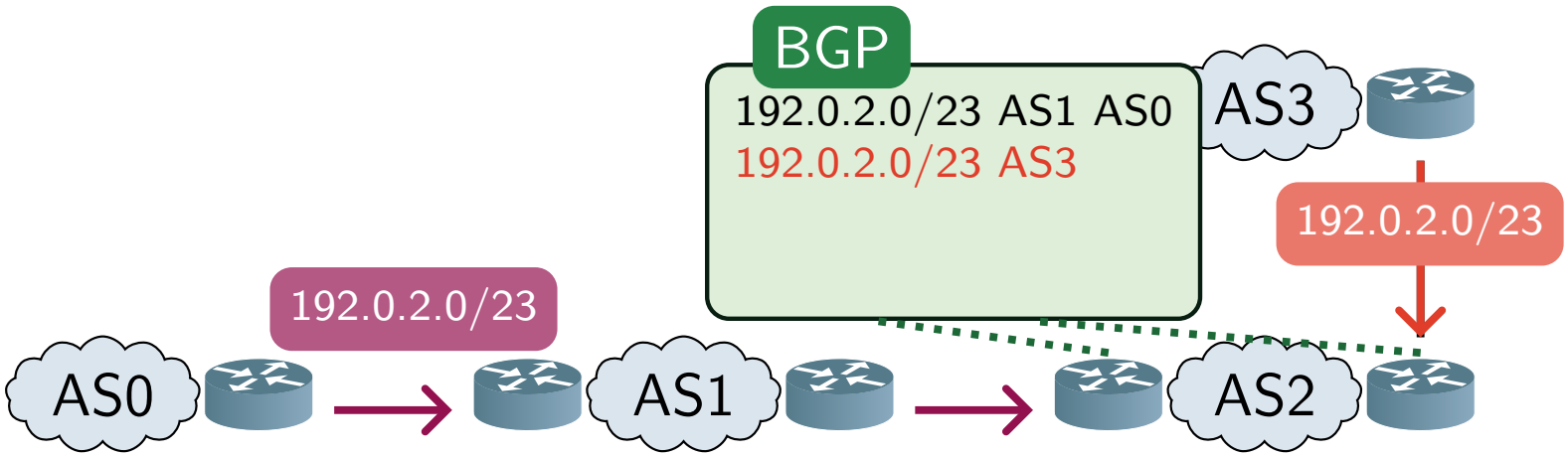
An hijack is a conflicting BGP announcement.



Rule #2 applies: traffic is redirected to AS3 !

Active Countermeasure

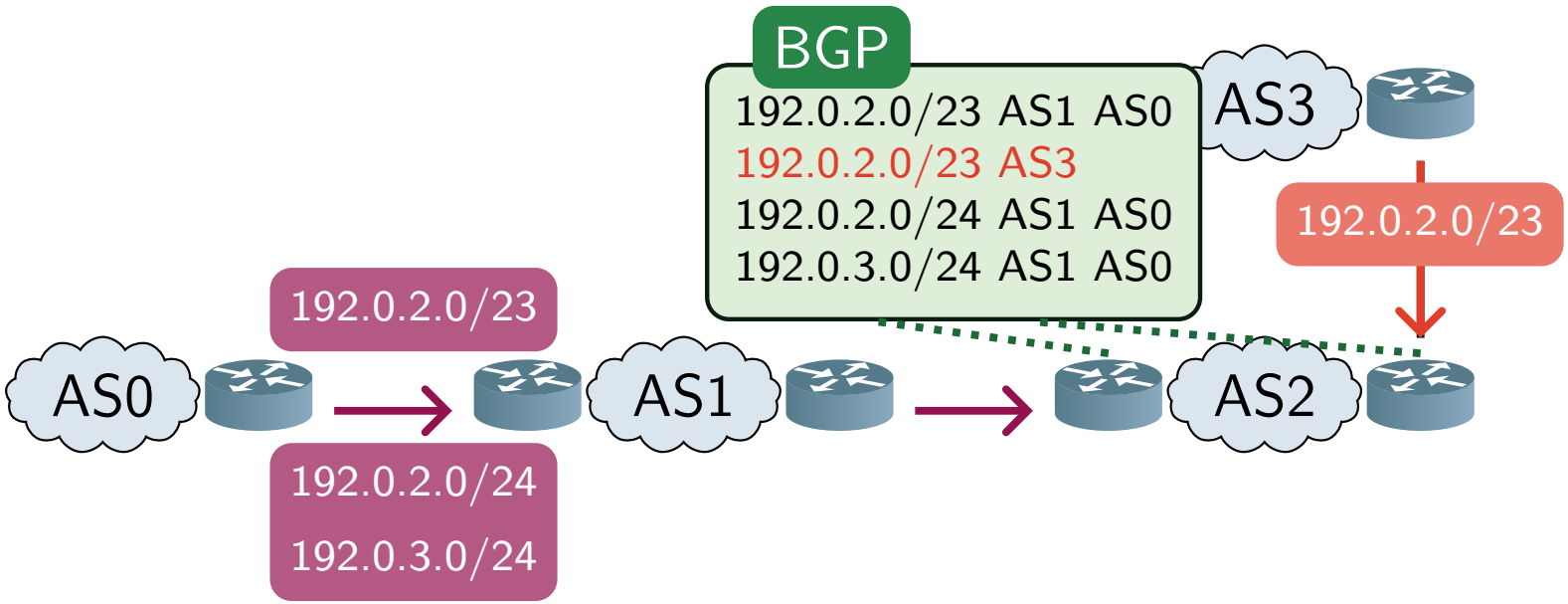
Use BGP rule #3 !



The origin AS announces more specific prefixes.

Active Countermeasure

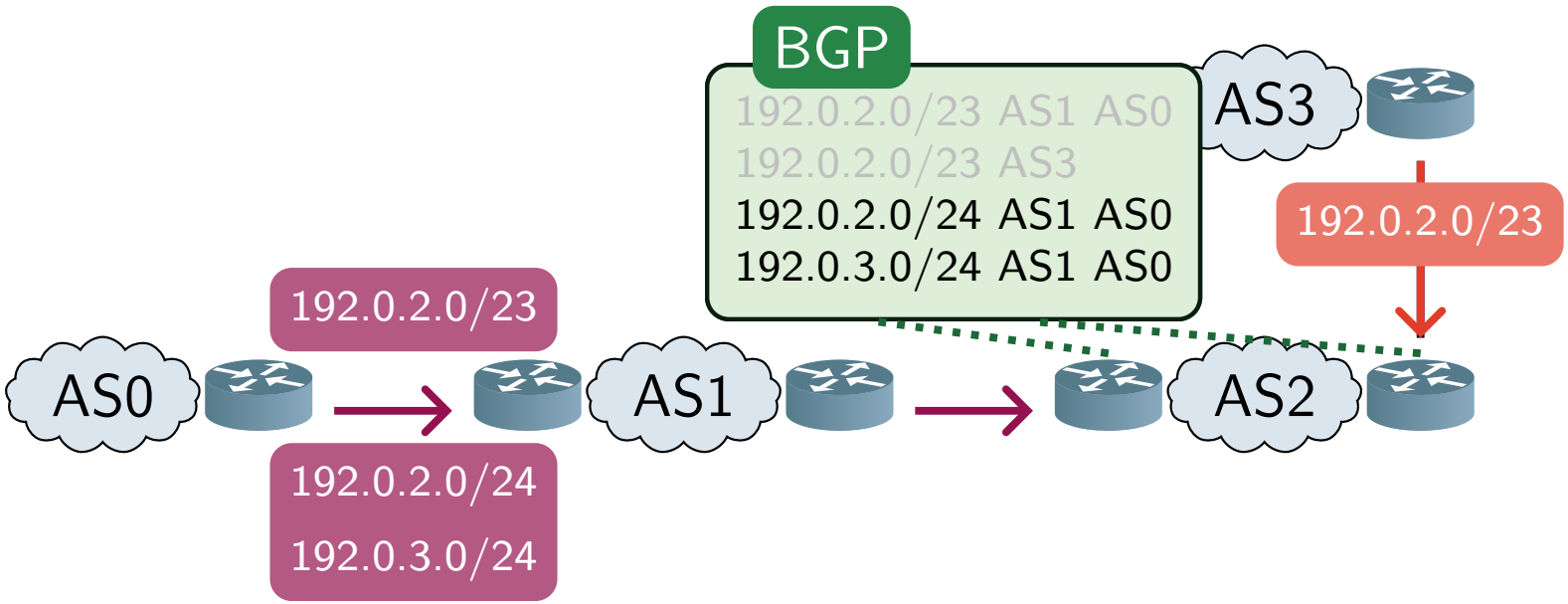
Use BGP rule #3 !



The origin AS announces more specific prefixes.

Active Countermeasure

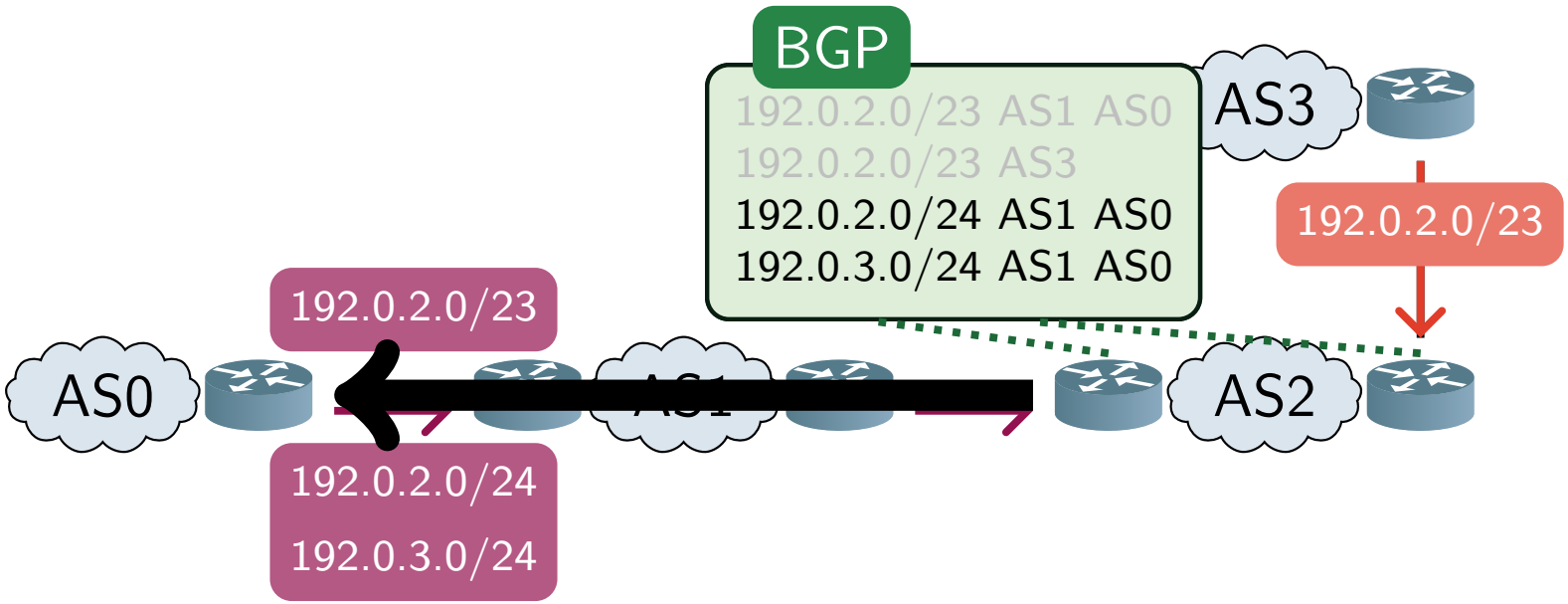
Use BGP rule #3 !



The origin AS announces more specific prefixes.

Active Countermeasure

Use BGP rule #3 !

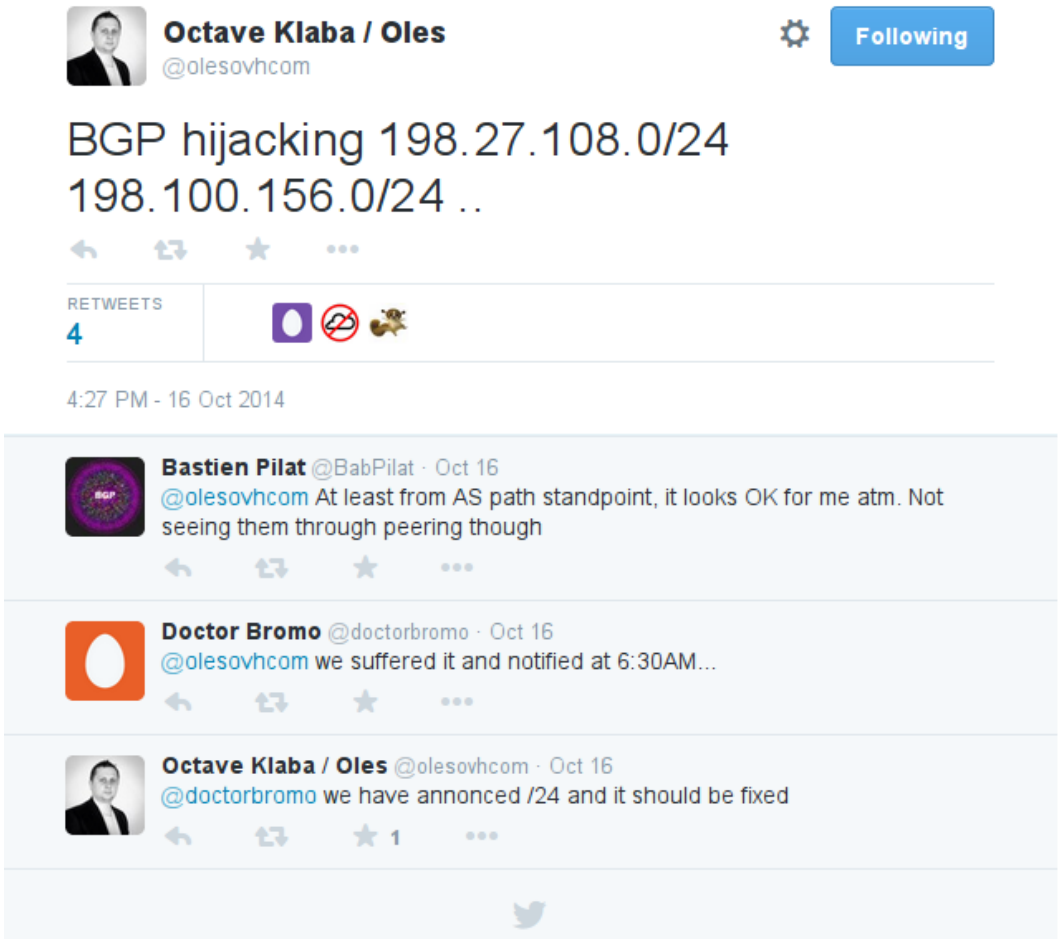


The origin AS announces more specific prefixes.

Rule #3 applies: traffic is sent to AS0 !

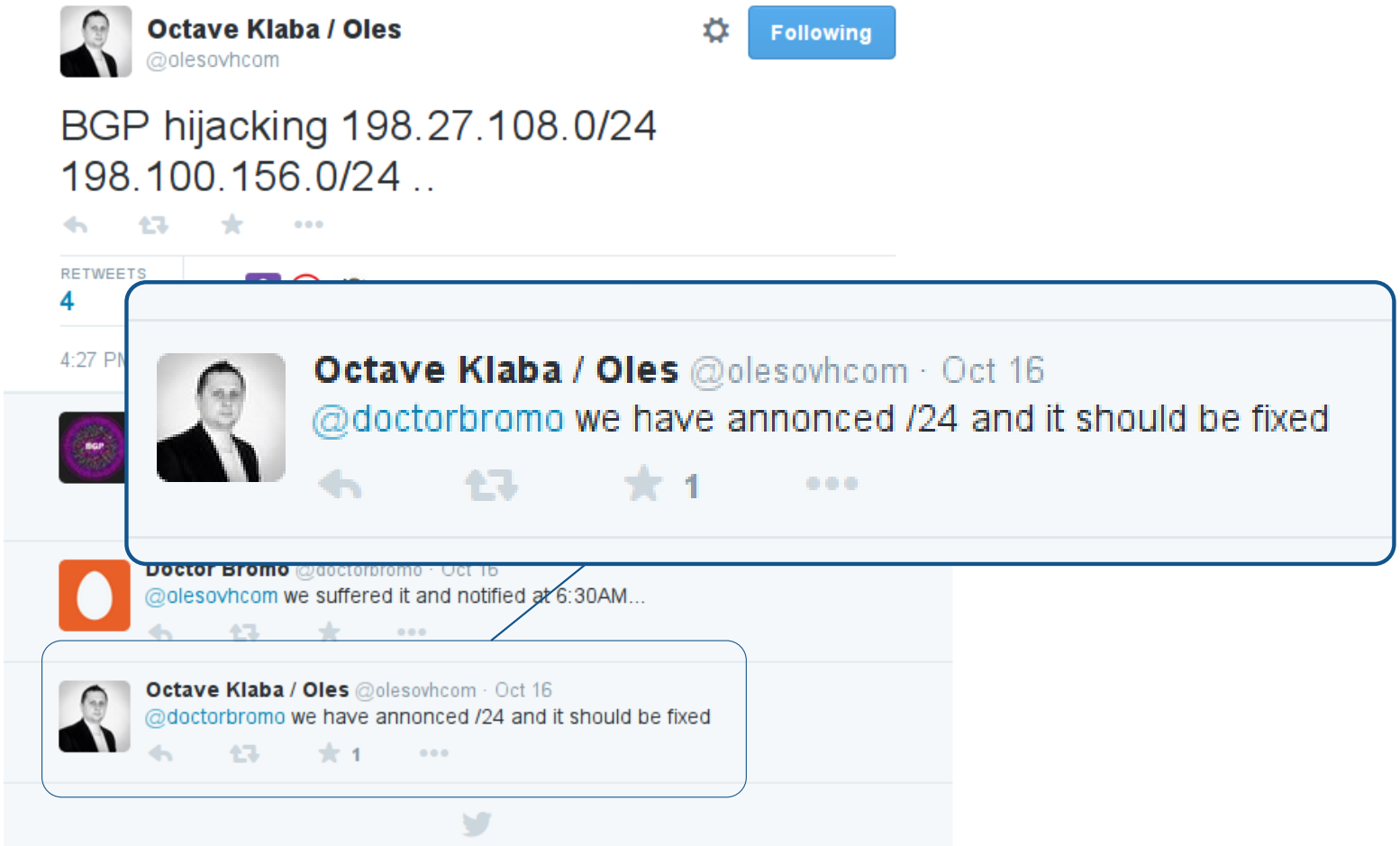
A Recent Example on October 16

Hijack against a French AS



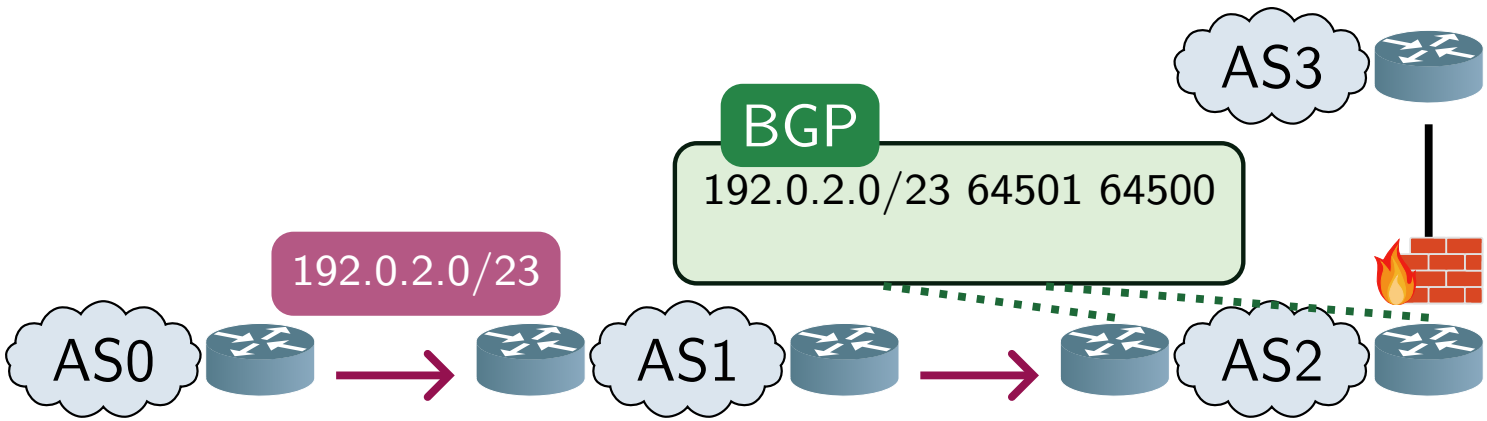
A Recent Example on October 16

Hijack against a French AS



Passive Countermeasure

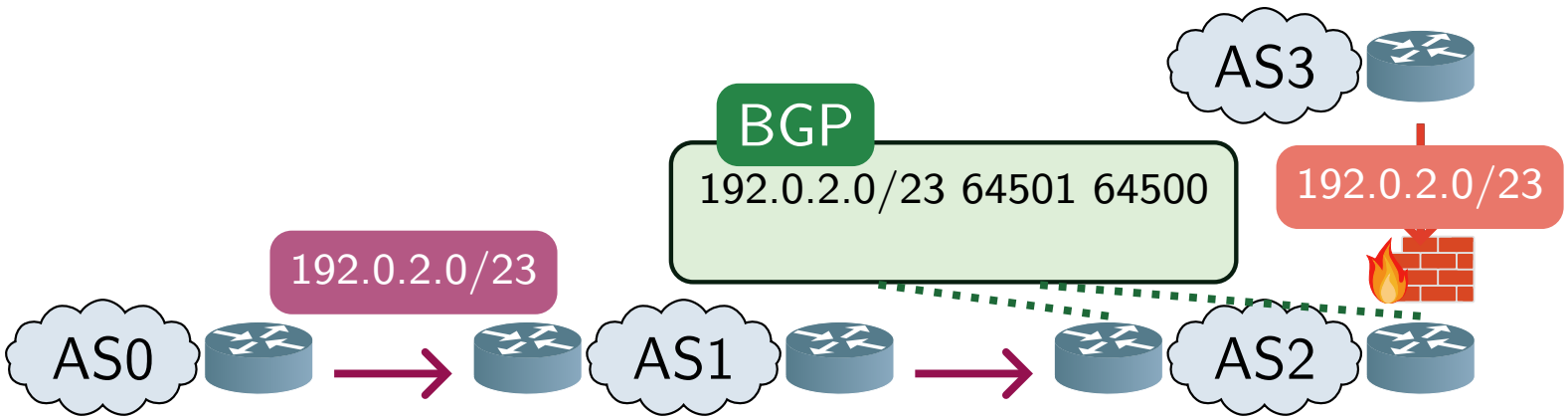
Strict filter on an interconnection



- a BGP router can filter prefix in UPDATE messages
- useful filtering can only be done by the upstream provider

Passive Countermeasure

Strict filter on an interconnection



- a BGP router can filter prefix in UPDATE messages
- useful filtering can only be done by the upstream provider

Passive Countermeasure

Automate filter maintenance

A route object:

- is declared by the AS in charge of an IP prefix
- tells who can announce the prefix with BGP
  - the operator, its DDoS mitigation provider, its clients, ...

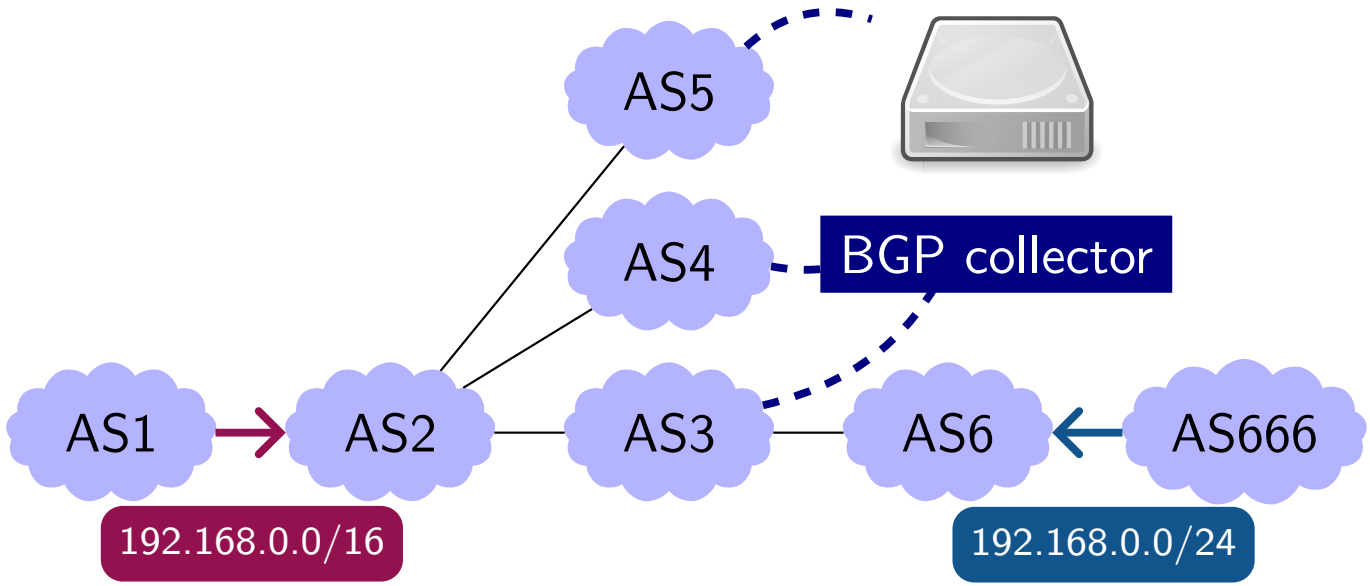
```
$ whois -T route 185.50.64.0/22

route:          185.50.64.0/22
descr:          Observatory IPv4 prefix.
origin:         AS202214
mnt-by:         ASOBS-MNT
source:         RIPE # Filtered
```

Offline Hijack Detection

BGP messages

Collecting BGP Archives

https://www.ris.ripe.net

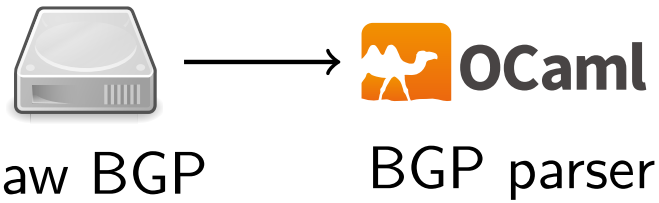


Routing Information Service (RIS)

- 13 BGP collectors all over the world
  - 263 BGP peers
- BGP messages dumped into binary files
  - 550 GB per year

Parsing BGP Archives

https://github.com/ANSSI-FR/parsifal



Need for a dedicated BGP parser

- fast & trusted parser
  - written in OCaml
- convert BGP messages to JSON
  - human readable / writable format

Parsing BGP Archives

https://github.com/ANSSI-FR/parsifal


```
{ "timestamp":1409750436, "collector": "rrc07",
  "as_path":"25152 6939 17922 7862 4761 9957 7500",
  "announce":["192.50.44.0/24"], "withdraw":[] }

{ "timestamp":1409782437, "collector": "rrc07",
  "as_path":"25152 6939 667 666",
  "announce":["192.50.44.0/24"], "withdraw":[] }
```


Need for a dedicated BGP parser

- fast & trusted parser
  - written in OCaml
- convert BGP messages to JSON
  - human readable / writable format

Parsing BGP Archives

https://github.com/ANSSI-FR/parsifal


```
{ "timestamp":1409750436, "collector": "rrc07",
  "as_path":"25152 6939 17922 7862 4761 9957 7500",
  "announce":["192.50.44.0/24"], "withdraw":[] }

{ "timestamp":1409782437, "collector": "rrc07",
  "as_path":"25152 6939 667 666",
  "announce":["192.50.44.0/24"], "withdraw":[] }
```


Need for a dedicated BGP parser

- fast & trusted parser
  - written in OCaml
- convert BGP messages to JSON
  - human readable / writable format

Parsing BGP Archives

https://github.com/ANSSI-FR/parsifal

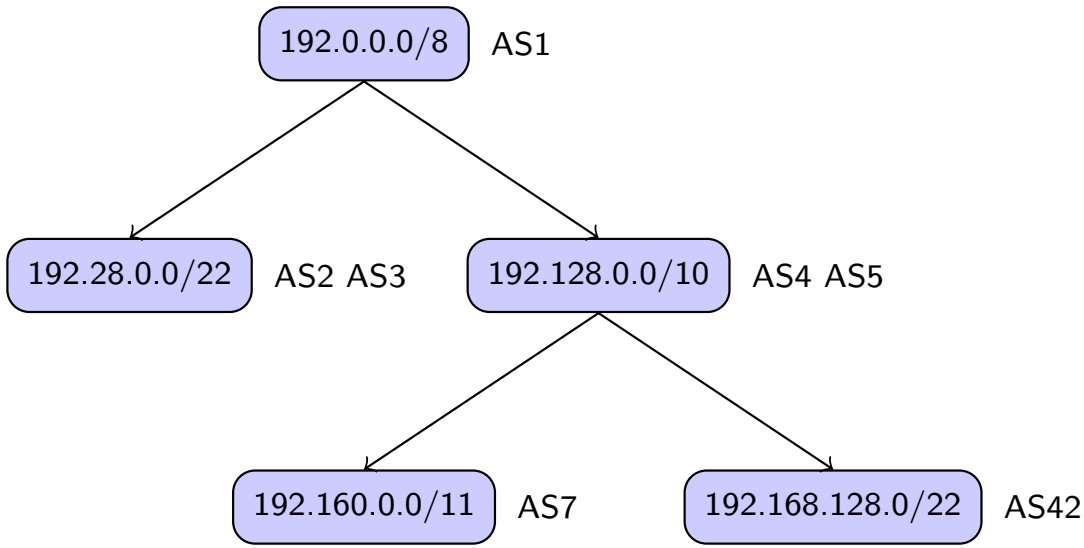

```
{ "timestamp":1409750436, "collector": "rrc07",
  "as_path":"25152 6939 17922 7862 4761 9957 7500",
  "announce":["192.50.44.0/24"], "withdraw":[] }

{ "timestamp":1409782437, "collector": "rrc07",
  "as_path":"25152 6939 667 666",
  "announce":["192.50.44.0/24"], "withdraw":[] }
```


Need for a dedicated BGP parser

- fast & trusted parser
  - written in OCaml
- convert BGP messages to JSON
  - human readable / writable format

Emulating a BGP Router

https://code.google.com/p/py-radix/

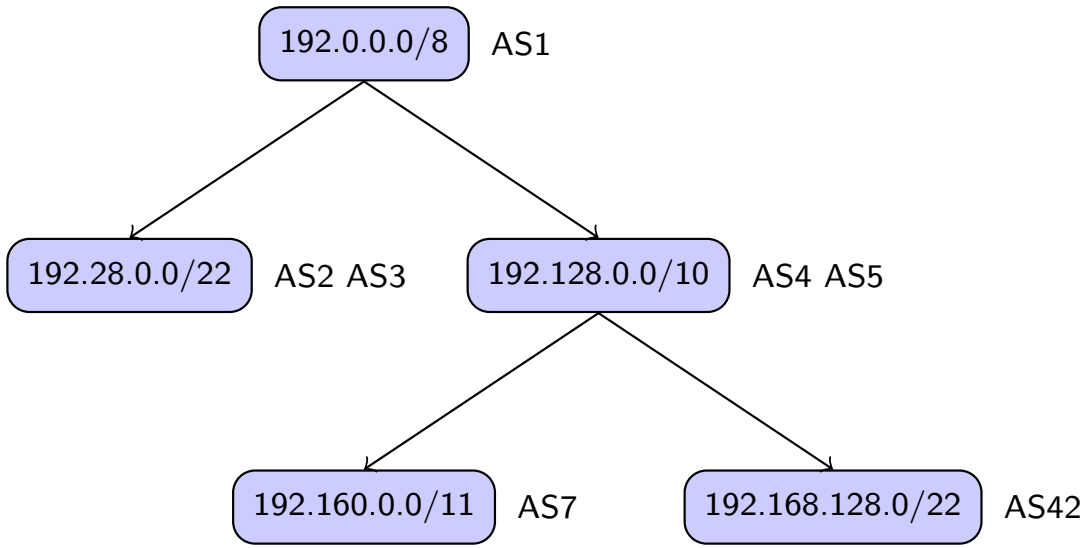


Build the routing table

- fast IP lookup library
  - similar to a router & the Linux kernel
- the tree is updated with each BGP messages
  - duplicated entries are conflicts

Emulating a BGP Router

https://code.google.com/p/py-radix/

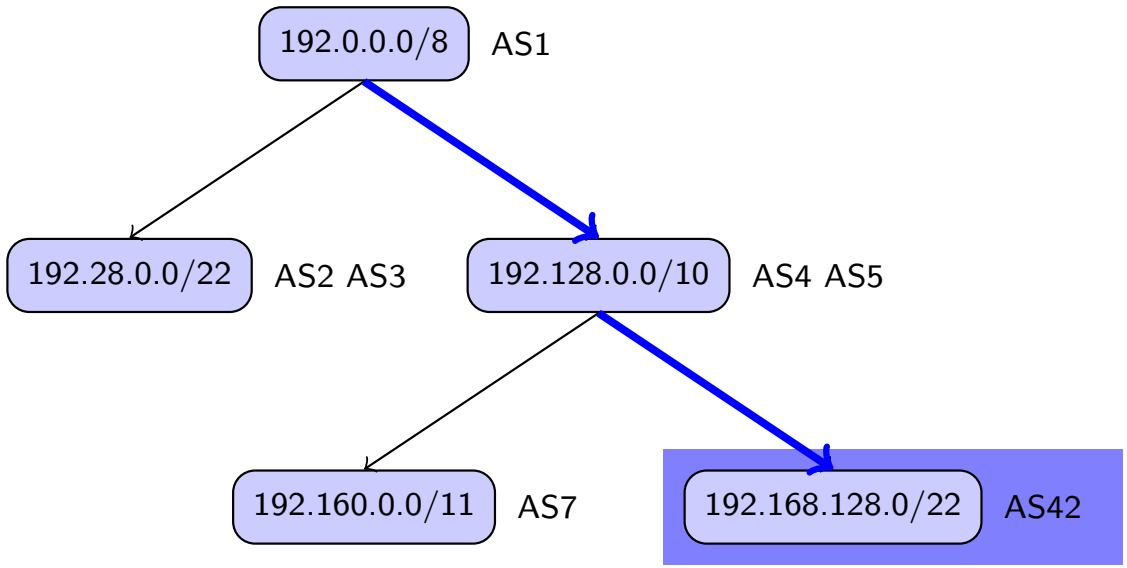


Processing an UPDATE message

```
{ "timestamp":1409750436, "peer_as":25152,
"as_path":"1234  666",
"announce":["192.168.128.0/24"], "withdraw":[] }
```

Emulating a BGP Router

https://code.google.com/p/py-radix/

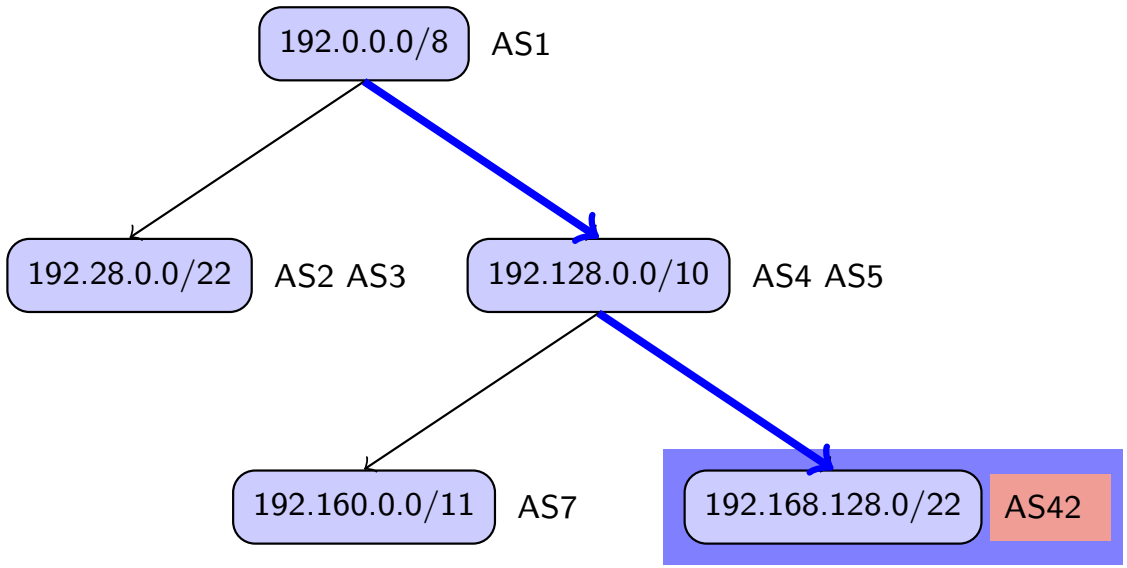


Processing an UPDATE message

```
{ "timestamp":1409750436, "peer_as":25152,
"as_path":"1234  666",
"announce":["192.168.128.0/24"], "withdraw":[] }
```

Emulating a BGP Router

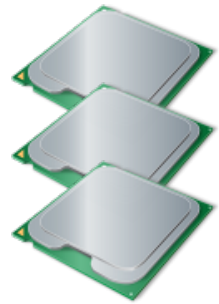
https://code.google.com/p/py-radix/

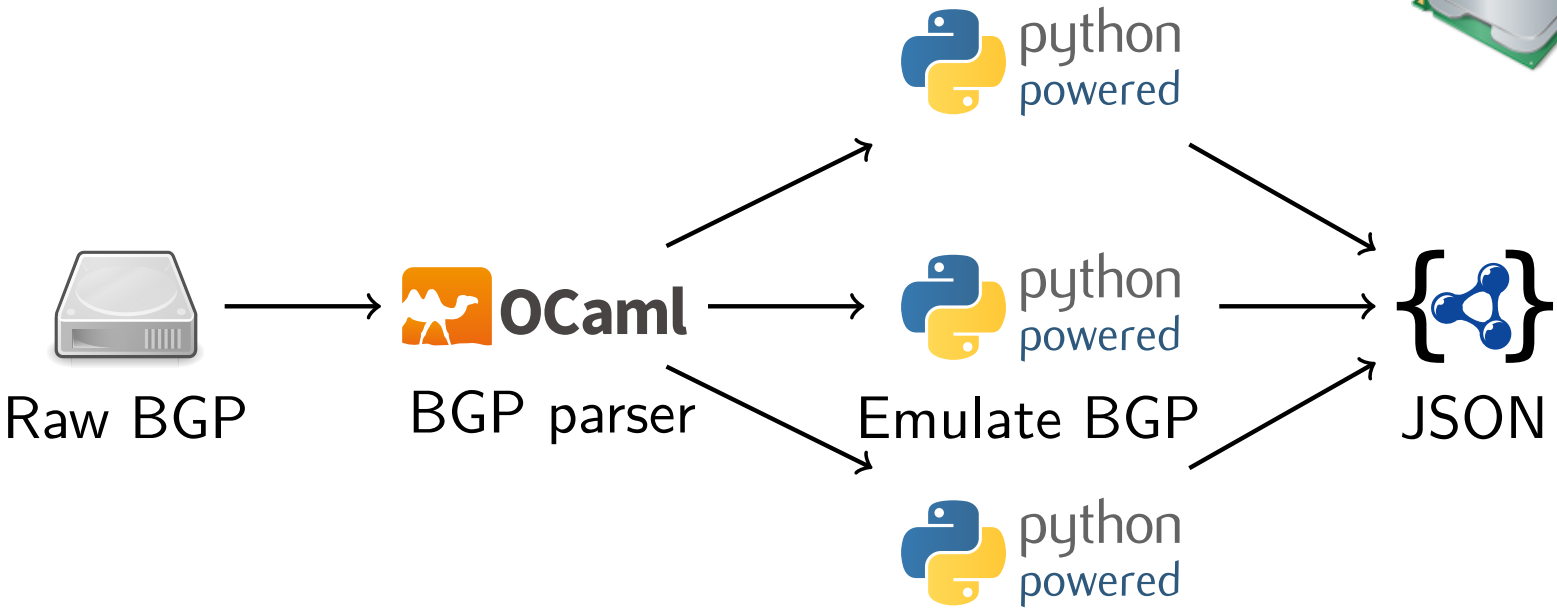


Processing an UPDATE message

```
{ "timestamp":1409750436, "peer_as":25152,
"as_path":"1234 666",
"announce":["192.168.128.0/24"], "withdraw":[] }
```

Putting Everything Together





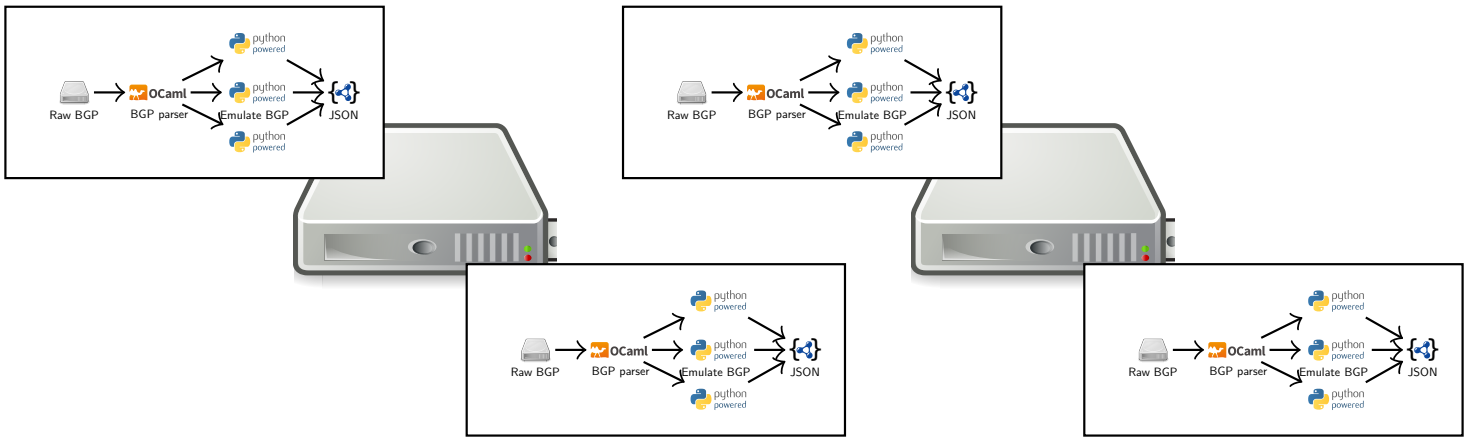
Processing 50k ASes

- emulated routers handle different AS
- with 8 cores, a month is processed in 10 hours

With 13 collectors, 156 months must be processed per year !

Faster Conflicts Detection

Scaling by adding cores

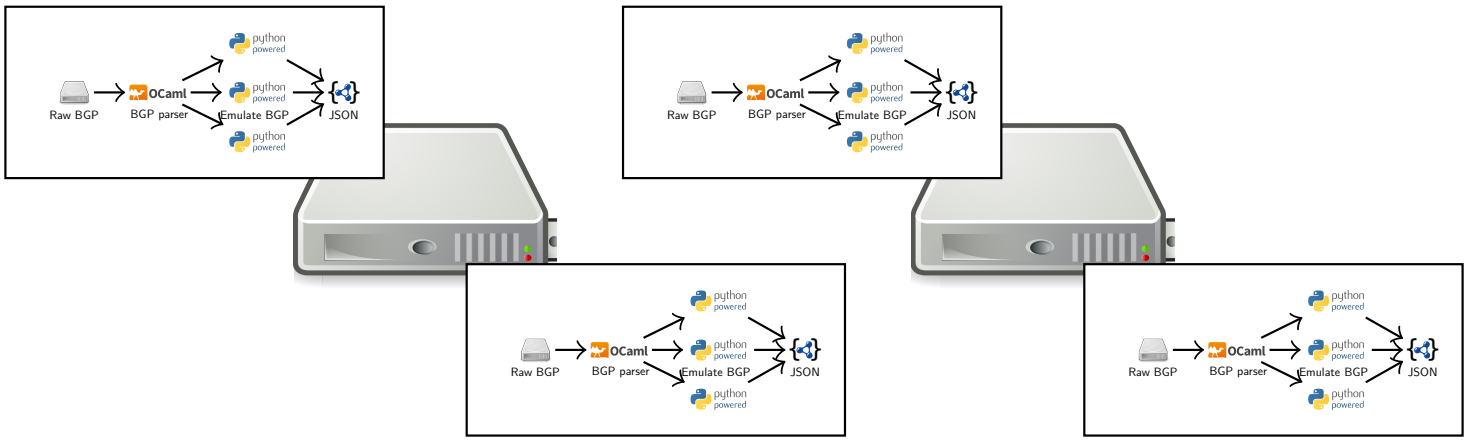


Conflicts detection

- completes in one week with 120 cores on 5 servers
  - generates 130 GB per year
- 11 536 345 959 conflicts
  - from January to October 2014

Faster Conflicts Detection

Scaling by adding cores

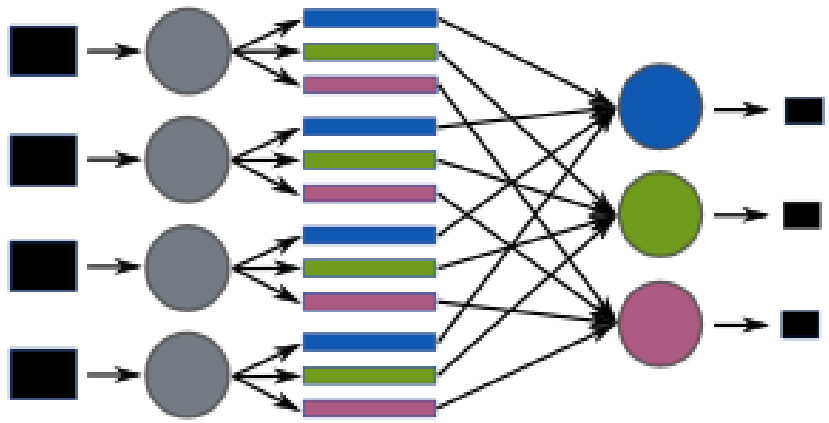


Conflict example

```
{ "timestamp":1409782437, "collector": "rrc07",
   "announce": { "prefix": "192.50.44.0/24", "asn": 666,
                 "as_path": "25152 6939 667 666"},
   "conflict_with": {"prefix": "192.50.44.0/24", "asn": 7500}}
```

Accessing The Data

`http://discoproject.org`



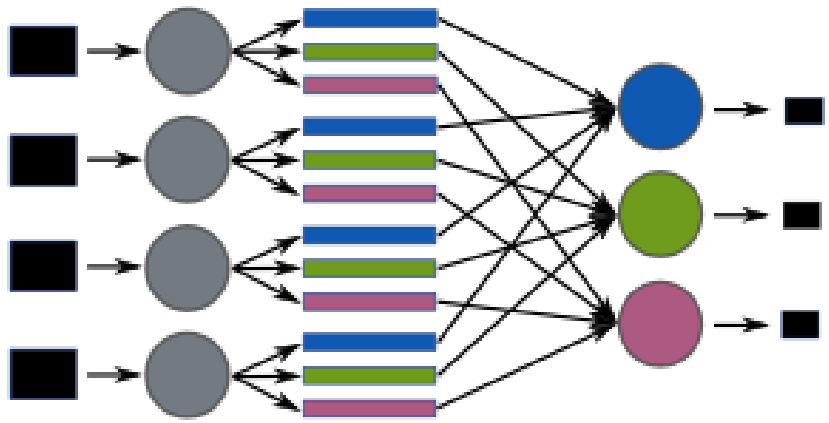
Disco?

- automatic data distribution & replication
  - like HDFS
- MapReduce framework in Python
  - like Hadoop

Accessing The Data

http://discoproject.org

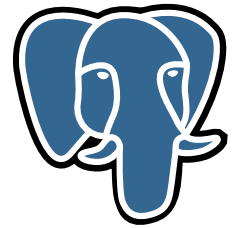
DISCO



From BIG DATA to small data

- one hour to extract conflicts targeting 1000 ASes
  - close to the number of French & Japanese ASes
- 70 millions conflicts per country
  - 200MB

Classifying Conflicts - 1/3
Using route objects

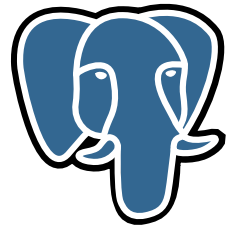


APNIC RIPE NCC

Validating a single conflict

```
{ "timestamp": 1409782437, "collector": "rrc07",
   "announce": { "prefix": "192.50.44.0/24", "asn": 666,
                 "as_path": "25152 6939 667 666"},
   "conflict_with": {"prefix": "192.50.44.0/24", "asn": 7500}}
```

Classifying Conflicts - 1/3
Using route objects



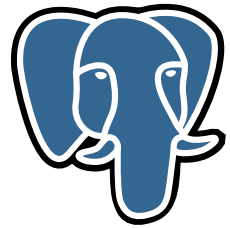
APNIC RIPE NCC

Validating a single conflict

```
{ "timestamp": 1409782437, "collector": "rrc07",
   "announce": { "prefix": "192.50.44.0/24", "asn": 666 ,
                 "as_path": "25152 6939 667 666"},
   "conflict_with": {"prefix": "192.50.44.0/24", "asn": 7500}}
```

```
$ whois -T route 192.50.44.0/24

route:          192.50.44.0/24
descr:          Example prefix
origin:         AS666
mnt-by:         AS666-MNT
```

Classifying Conflicts - 1/3
Using route objects



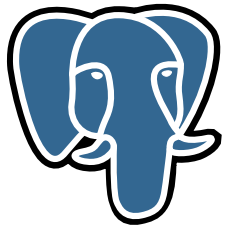
APNIC RIPE NCC

Validating a single conflict

```
{ "timestamp": 1409782437, "collector": "rrc07",
   "announce": { "prefix": "192.50.44.0/24", "asn": 666,
                 "as_path": "25152 6939 667 666"},
   "conflict_with": {"prefix": "192.50.44.0/24", "asn": 7500}}
```

```
$ whois -T route 192.50.44.0/24

route:          192.50.44.0/24
descr:          Example prefix
origin:         AS666
mnt-by:         AS666-MNT
```

Classifying Conflicts - 1/3
Using route objects



APNIC
RIPE NCC

Validating 70 millions conflicts

- all of them must be verified
- online queries are too slow
  - `WHOIS` databases are loaded daily into PostgreSQL
  - the `ip4r` type is used for fast prefix lookups

```
>>> client = Client("ripe")
>>> client.check("210.158.206.0/24", 17676, "2014/07/28")
True
```


0.01% conflicts removed

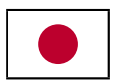

32% conflicts removed

Classifying Conflicts - 2/3

Using relations between AS objects

```
$ whois AS15557
aut-num:        AS15557
as-name:        LDCOMNET
descr:          SFR
org:            ORG-LA7-RIPE
admin-c:        LD699-RIPE
tech-c:         LDC76-RIPE
status:         ASSIGNED
mnt-by:         LDCOM-MNT
mnt-routes:     FMCF-MNT
mnt-routes:     LDCOM-MNT
source:         RIPE
```

```
$ whois AS41272
aut-num:        AS41272
as-name:        MOSELLE-TELE-AS
descr:          MOSELLE TELECOM
org:            ORG-MT18-RIPE
admin-c:        LD699-RIPE
tech-c:         LDC76-RIPE
status:         ASSIGNED
mnt-by:         MOSELLE-TELE-MNT

mnt-routes:     MOSELLE-TELE-MNT
source:         RIPE
```



2% conflicts removed

54% conflicts removed

Classifying Conflicts - 3/3

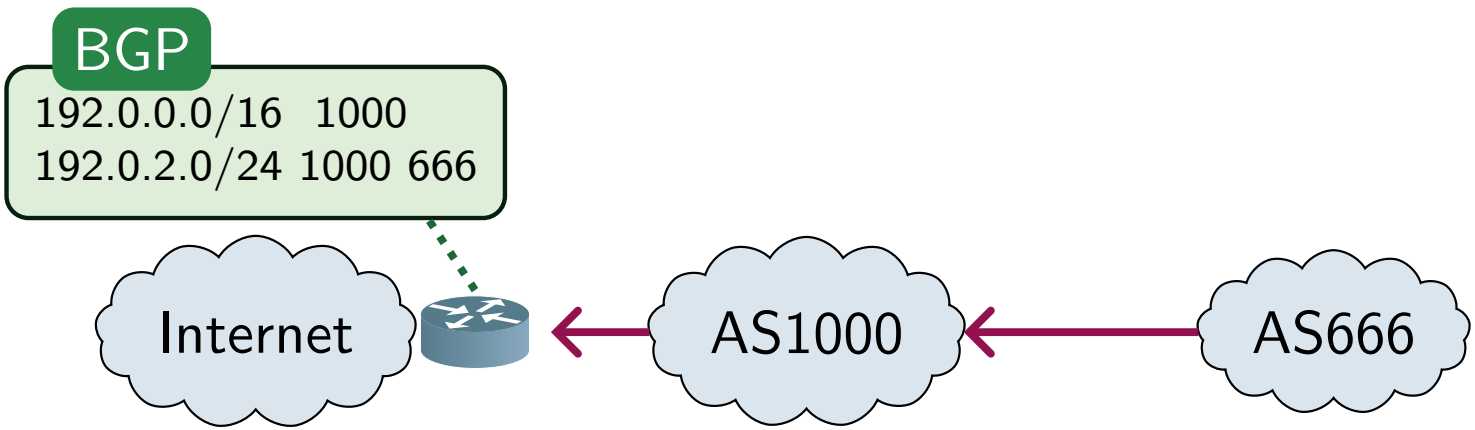
Using client/provider connectivity

```
{ "timestamp": 1409750436,
   "announce": { "prefix": "192.0.2.0/24", "asn": 666,
                 "as_path": "... 1000 666" },
   "conflict_with": {"prefix": "192.0.0.0/16", "asn": 1000 } }
```

Classifying Conflicts - 3/3

Using client/provider connectivity

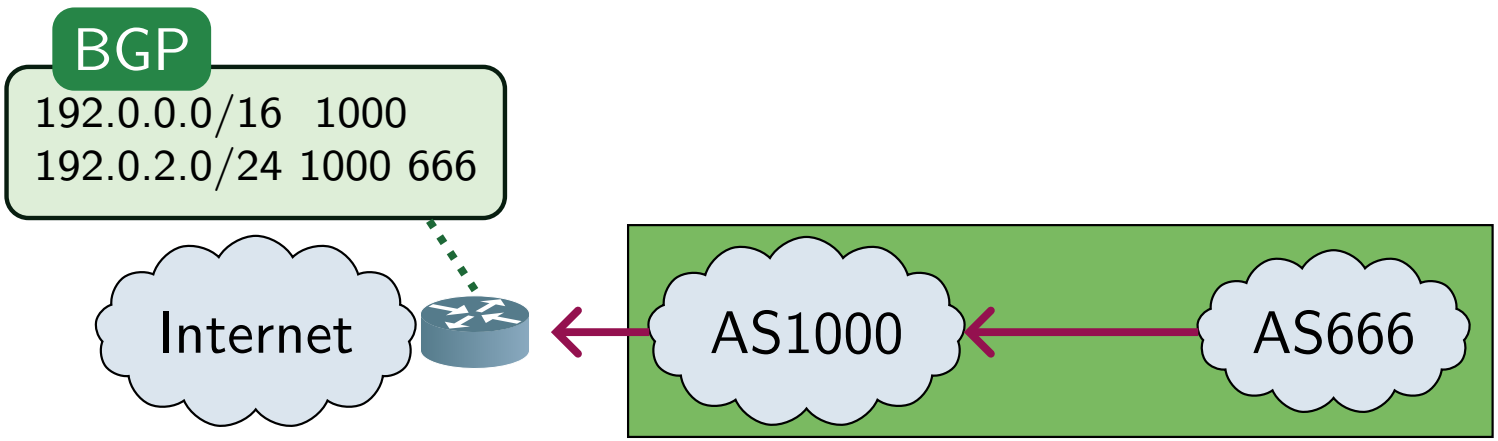
```
{ "timestamp": 1409750436,
   "announce": { "prefix": "192.0.2.0/24", "asn": 666,
                 "as_path": "... 1000 666" },
   "conflict_with": {"prefix": "192.0.0.0/16", "asn": 1000 } }
```



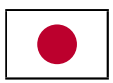
Classifying Conflicts - 3/3

Using client/provider connectivity

```
{ "timestamp": 1409750436,
   "announce": { "prefix": "192.0.2.0/24", "asn": 666,
                 "as_path": "... 1000 666" },
   "conflict_with": {"prefix": "192.0.0.0/16", "asn": 1000 } }
```



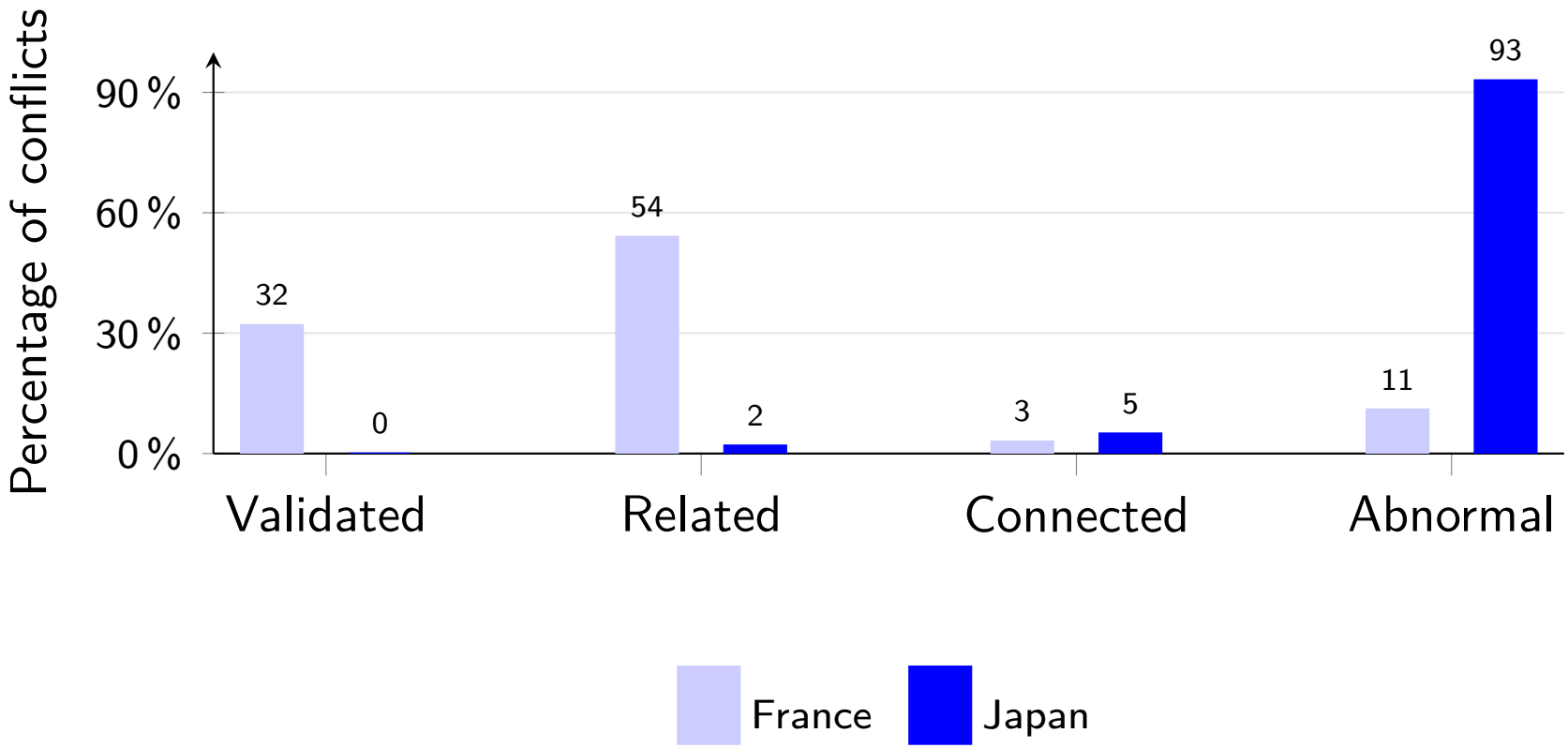
Client/Provider relation


5% conflicts removed


3% conflicts removed

Classifying conflicts

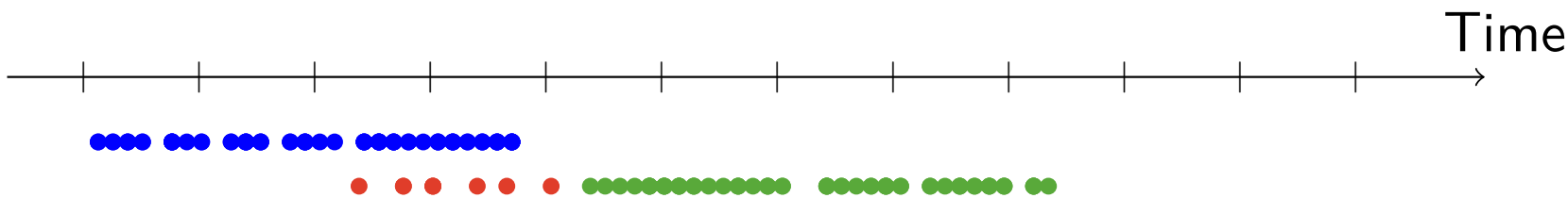
Summary



42 millions abnormal conflicts

8 millions abnormal conflicts

Computing durations
From conflicts to events



Before aggregation


```
{ "timestamp": 20141111.0, "collector": "rrc99" ,
   "type": "RELATION",
   "announce": { "prefix": "1.6.28.0/24", "asn": 666 }
   "conflict_with": {"prefix": "1.6.0.0/18", "asn": 1000 } }

{ "timestamp": 20141231.0, "collector": "rrc66" ,
    type": "RELATION",
   "announce": { "prefix": "1.6.28.0/24", "asn": 666 }
   "conflict_with": {"prefix": "1.6.0.0/18", "asn": 1000 } }
```


Computing durations

From conflicts to events

After aggregation

```
{ "conflict_with" : { "prefix" : "1.6.0.0/18",  "asn" : 1000 },
   "origin" :       { "prefix" : "1.6.28.0/24", "asn" :  666 },
   "begin": 20141111.0, "end" :  20141231.0,
   "peers" : [ "rrc99", "rrc66" ],
   "type" : "RELATION" }
```

 74 084 events

 73 902 events

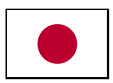
Events Visualization

A French AS

Reducing The Number of Events
Automatically

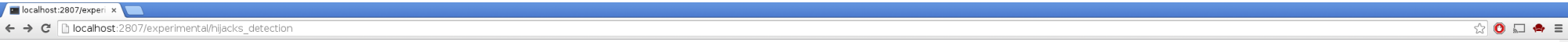
Simple rules

- remove events that change categories
- remove events if ASes belongs to the same country
- remove events longer than 6 months
- remove associated events


From 2154 prefixes in conflict to 557


From 4519 prefixes in conflict to 289

Looking For Hijacks



Hijacks targeting JP

#	origin.asn	origin.prefix	hijacker.asn	hijacker.prefix	total duration	real duration	# collectors	# peers
1	7543	103.248.44.0/22	133417	103.248.44.0/22	3 days, 4:43:41	0:00:58	4	8
2	44287	91.201.136.0/22	5580	91.201.137.0/24	0:02:13	0:02:13	2	2
3	44287	91.201.137.0/24	5580	91.201.137.0/24	0:02:13	0:02:13	2	2
4	44287	91.201.136.0/23	5580	91.201.137.0/24	0:02:13	0:02:13	2	2
5	2500	2001:200::/32	60983	2001:200:e103::/48	0:02:35	0:02:35	13	95
6	7660	2001:200:e000::/35	60983	2001:200:e103::/48	0:02:35	0:02:35	13	95
7	55902	103.247.88.0/22	17819	103.247.88.0/22	0:03:14	0:03:14	13	101
8	131073	46.102.174.0/24	61361	46.102.174.0/24	0:03:29	0:03:29	3	13
9	131074	46.102.174.0/24	61361	46.102.174.0/24	0:03:29	0:03:29	2	19
10	7514	211.13.192.0/19	13789	211.13.204.0/24	0:06:27	0:06:27	13	98
11	10001	177.74.153.0/24	263650	177.74.153.0/24	0:07:41	0:07:41	13	85
12	18097	216.179.196.0/23	21859	216.179.196.0/24	0:07:49	0:07:49	6	7
13	18097	216.179.196.0/23	37958	216.179.196.0/24	0:07:51	0:07:51	7	18
14	10000	103.234.136.0/24	1000	103.234.136.0/24	0:13:24	0:13:16	6	18
15	2516	23.10.32.0/20	4761	23.10.32.0/20	0:14:32	0:14:32	11	29
16	18144	1.0.64.0/18	28126	1.0.64.0/18	0:16:33	0:16:22	8	18
17	17676	126.0.0.0/8	3303	126.0.0.0/8	78 days, 1:44:00	0:17:59	1	2
18	132301	116.93.0.0/17	59325	116.93.58.0/24	0:21:06	0:21:06	1	15
19	132301	116.93.0.0/17	59325	116.93.59.0/24	0:21:56	0:21:56	1	15

Reducing The Number of Events
Manually

IP[y]: IPython

Interesting results

- similar AS names
  - `PACNET-MY Pacnet MY` and `PACNET Pacnet Global Ltd`
- AS under DDoS protection
  - the DDoS mitigation companies announces /24
- typos in AS numbers
  - 2208 and 208
- hijacks that were used to steal bitcoins
  - AS18863 was at the origin of some of these hijacks
- some events were never detected by operators
- ...

Closing Remarks

Since January 2014, there are:


69 suspicious events


102 suspicious events

Around 10 hijacks per year target French operators

Real-time BGP Hijack Detection

Targeted Internet Traffic Misdirection

Reported by Renesys on November, 2013

Real-time Detection Goals

BGP messages

python powered

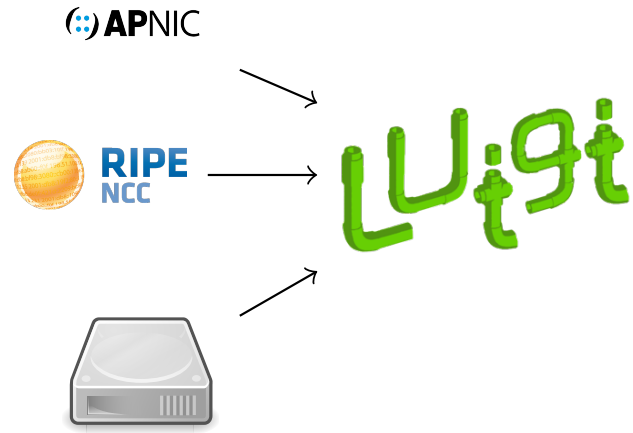
Hijacks

Alerts

Measurements

Detection Requirements

`https://github.com/spotify/luigi`

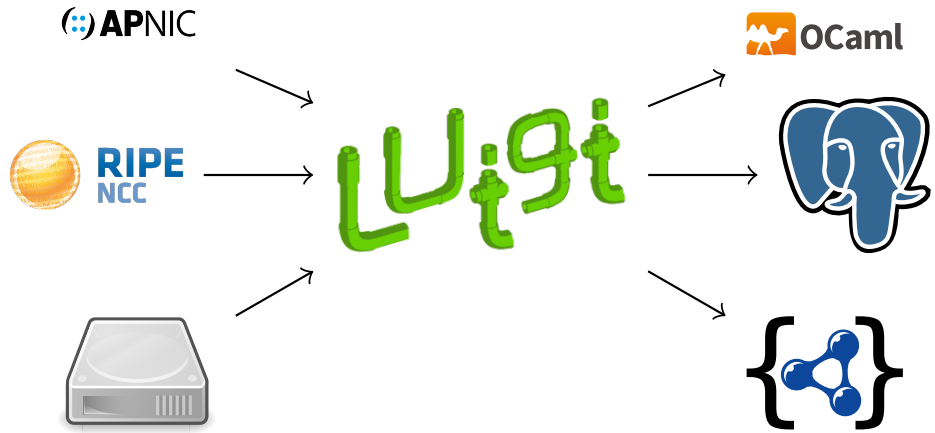


Fetching Tasks

- Internet registries
- raw BGP data

Detection Requirements

`https://github.com/spotify/luigi`



Fetching Tasks

- Internet registries
- raw BGP data

Processing Tasks

- synchronise whois databases
- parse BGP data to JSON
- create IP prefix to origin AS mapping

BGP Hijack Reporting

What must be reported

- only suspicious BGP hijacks
- about 50 events per week

BGP Hijack Reporting
IRC is so 2014

What must be reported

- only suspicious BGP hijacks
- about 50 events per week

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

```
$ whois 2a04:8000::/29
inet6num:    2a04:8000::/29
netname:     UA-UAHOSTING
descr:       Hosting Ukraine
country:     UA
org:         ORG-HUL6-RIPE
```

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

```
$ whois 2a04:8000::/29
inet6num:    2a04:8000::/29
netname:     UA-UAHOSTING
descr:       Hosting Ukraine
country:     UA
org:         ORG-HUL6-RIPE
```

```
$ whois -i org ORG-HUL6-RIPE
```

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

```
$ whois 2a04:8000::/29
inet6num:    2a04:8000::/29
netname:     UA-UAHOSTING
descr:       Hosting Ukraine
country:     UA
org:         ORG-HUL6-RIPE
```

```
$ whois -i org ORG-HUL6-RIPE
aut-num:     AS200000
as-name:     Ukraine-AS
descr:       Hosting Ukraine
org:         ORG-HUL6-RIPE
```

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

```
$ whois 2a04:8000::/29
inet6num:    2a04:8000::/29
netname:     UA-UAHOSTING
descr:       Hosting Ukraine
country:     UA
org:         ORG-HUL6-RIPE
```

```
$ whois -i org ORG-HUL6-RIPE
aut-num:     AS200000
as-name:     Ukraine-AS
descr:       Hosting Ukraine
org:         ORG-HUL6-RIPE
```

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

Analysis Result

- 2a04:8000::/29 belongs to the Ukrainian operator

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

Analysis Result

- 2a04:8000::/29 belongs to the Ukrainian operator
- 2a04:0800::/29 belongs to the French operator
- French operator made a mistake in its BGP configuration

BGP Hijack Troubleshooting

```
< hadron> 2a04:8000::/29 is announced from multiple origins:
< hadron>  SFR-BUSINESS-TEAM (AS12566)
< hadron>  Ukraine-AS (AS200000)
< hadron>  First originated from SFR-BUSINESS-TEAM (AS12566)
```

Analysis Result

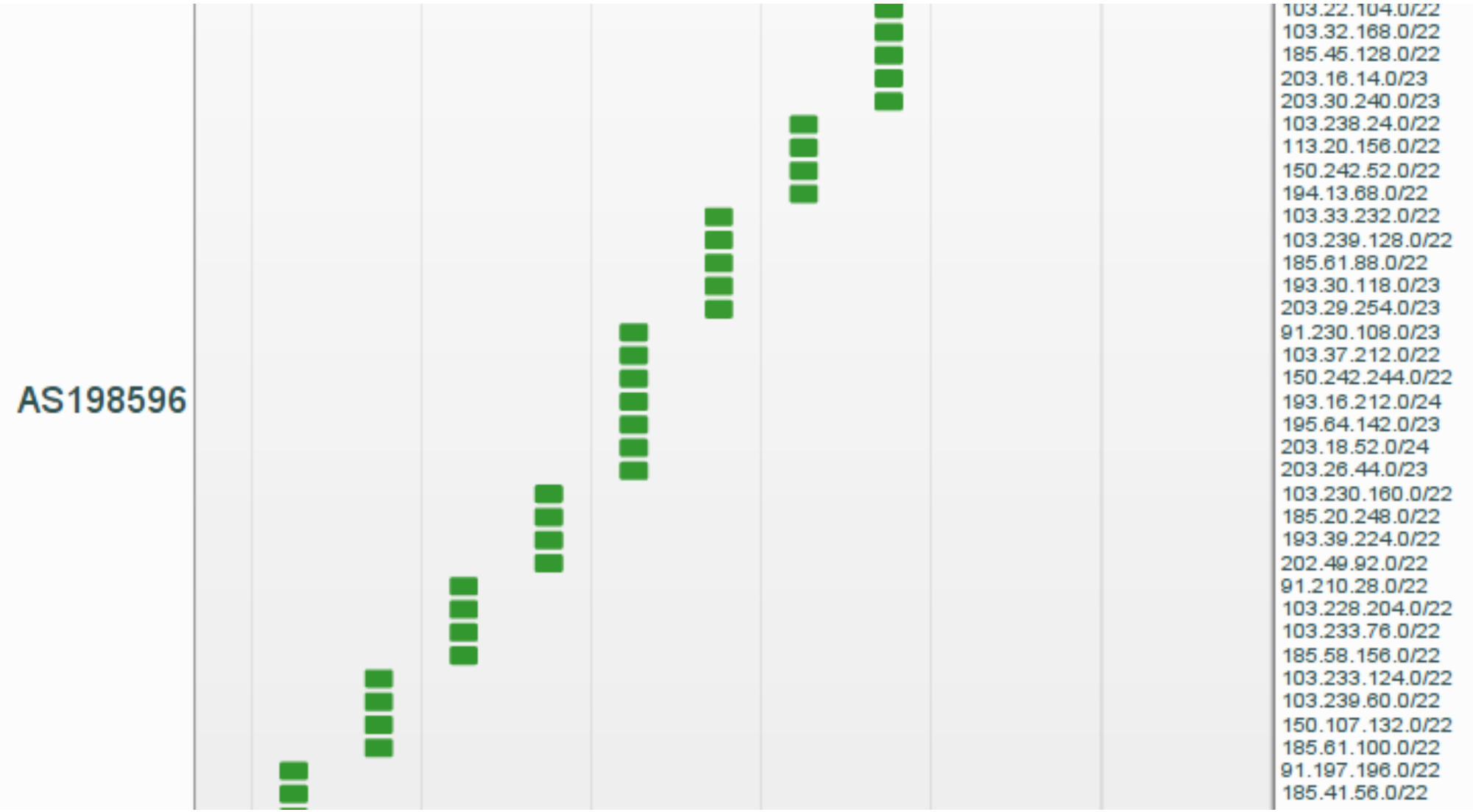
- 2a04:8000::/29 belongs to the Ukrainian operator
- 2a04:0800::/29 belongs to the French operator
- French operator made a mistake in its BGP configuration

It was a false positive, the route6 object was created a few days later by the Ukrainian operator.

Malicious BGP Hijack

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
```

https://stat.ripe.net/AS198596



Announces from September to October 2014

Malicious BGP Hijack

Infected AS_PATH

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Malicious BGP Hijack

Infected AS_PATH

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Definition

- infected ASes accepted the hijacking BGP update
- traffic to the hijacked prefix go to the hijacker's network

Malicious BGP Hijack

Infected AS_PATH

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Definition

- infected ASes accepted the hijacking BGP update
- traffic to the hijacked prefix go to the hijacker's network

How do we launch active measurements from these ASes?

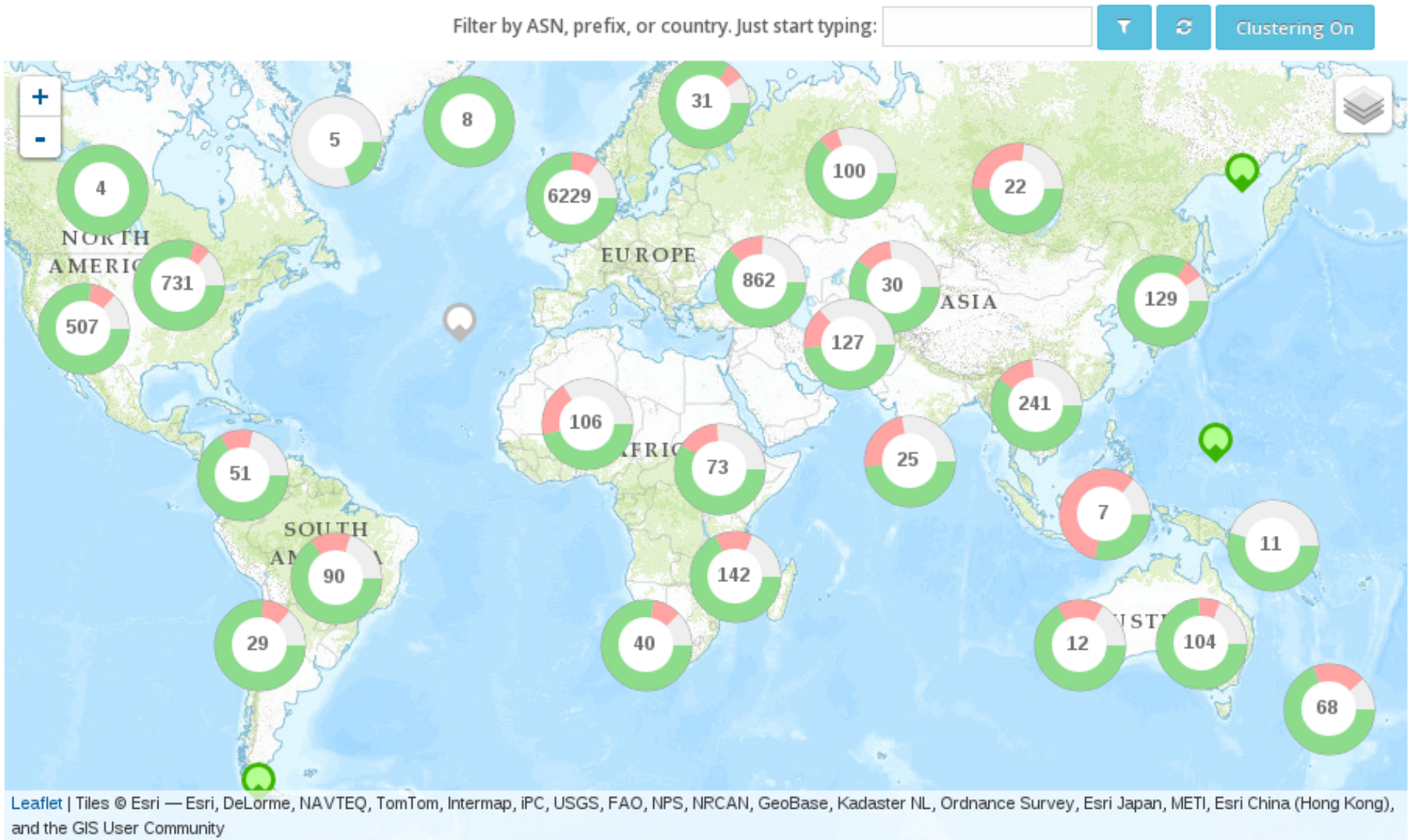
RIPE Atlas Measurement Project

https://atlas.ripe.net/

- 7100 probes in around 2000 ASes
- probes hosted by the community
- user-defined measurements
- ping, traceroute, HTTP, TLS and DNS
- public API

Global RIPE Atlas Network Coverage

This map shows the locations of all RIPE Atlas probes, including those that are connected, disconnected and abandoned (meaning they have not been connected for a long period of time).



Connected Disconnected Abandoned

Atlas Meets Our Needs

We always found a probe to launch our measurements!

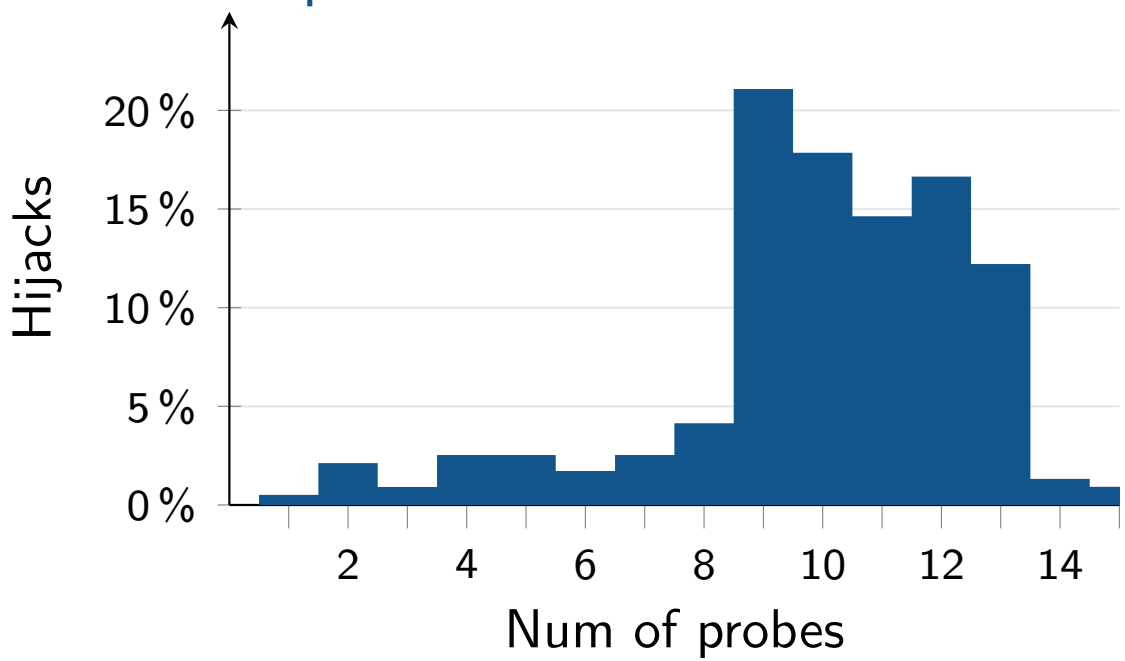
- 250 possible hijacks from september to november 2014
- `AS_PATH` are from the London based RIPE collector

Atlas Meets Our Needs

We always found a probe to launch our measurements!

- 250 possible hijacks from september to november 2014
- `AS_PATH` are from the London based RIPE collector

Number of probes found in infected ASes:



Traceroute Example

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Traceroute Example

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Traceroute Example

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Traceroute to
185.73.204.1

Traceroute Example

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Traceroute to
185.73.204.1

Traceroute Example

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```


```
1. 10.10.10.1
2. 82.118.96.1
3. 188.124.228.1
4. 95.215.3.78
5. * * *
```

Traceroute Example

```
< hadron> 185.73.204.0/22 is announced from multiple origins:
< hadron>  ALPHALINK-AS (AS25540)
< hadron>  TEHNOGRUP (AS198596)
< hadron> AS_PATH: 8607 39792 44050 131788 198596
```

Closing Remarks

- traceroute stops at AS44050 (PIN-AS)
- AS131788 and AS198596 are most certainly placeholders
- AS44050 (PIN-AS) is already known for previous hijacks

Conclusion

Conclusion

- wide scale BGP hijacks automatic detection
- only a few real hijacks per year regarding France and Japan
- early detection and reporting
- on-going work to identify traffic redirection

Take away messages

1. packets can be redirected on the Internet
2. traffic must be encrypted and authenticated
3. monitor prefixes and be ready to send more specific ones
4. networking Best Current Practices must be enforced

Questions?

A question == A Japanese Kit Kat

Related publication

- BGP configuration best practices (English & French)