Toward Detecting Hidden Broken Pieces of the Internet

Cristel Pelsser

In collaboration with:

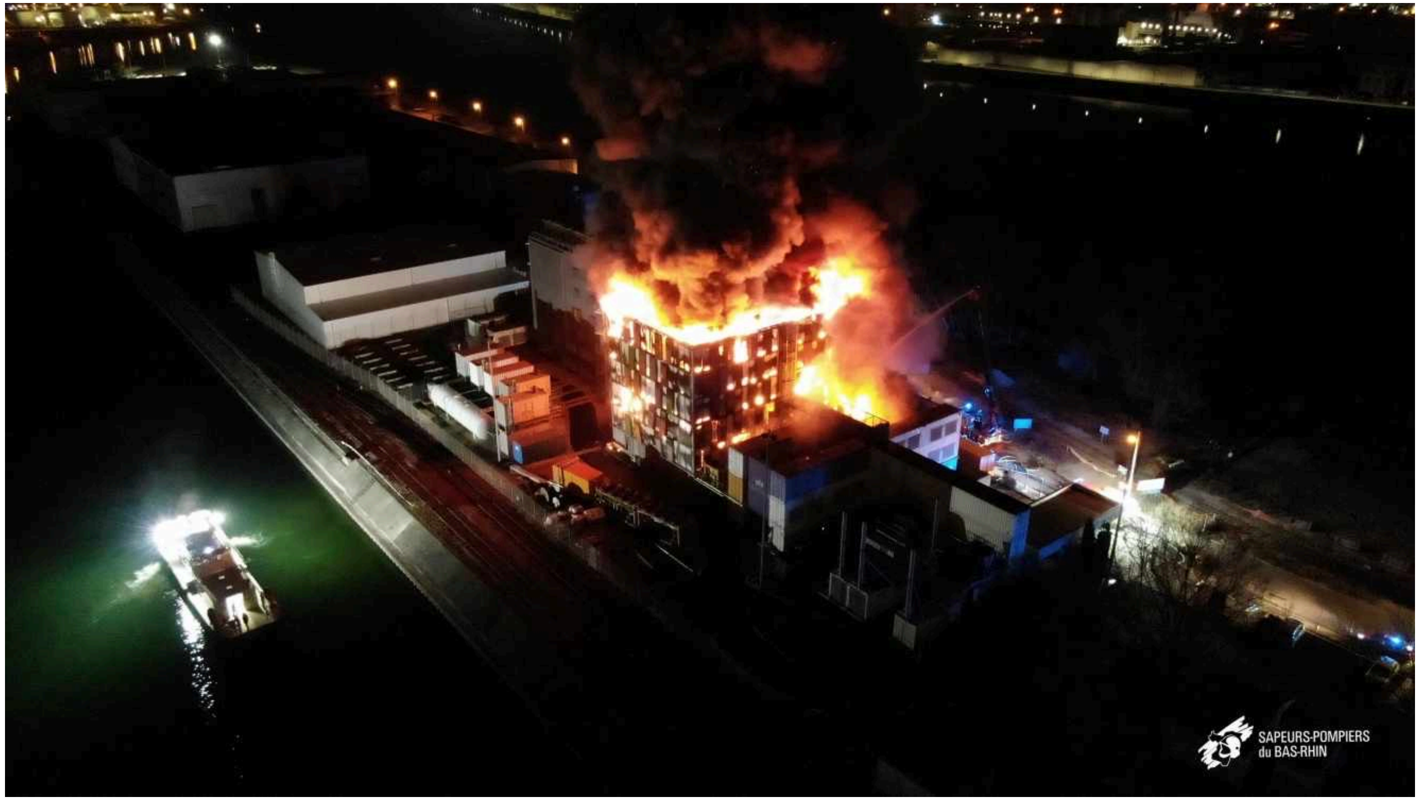
Julian Del Fiore (main contributor)

Valerio Persico

Pascal Mérindol

Antonio Pescapé

There are big outages …

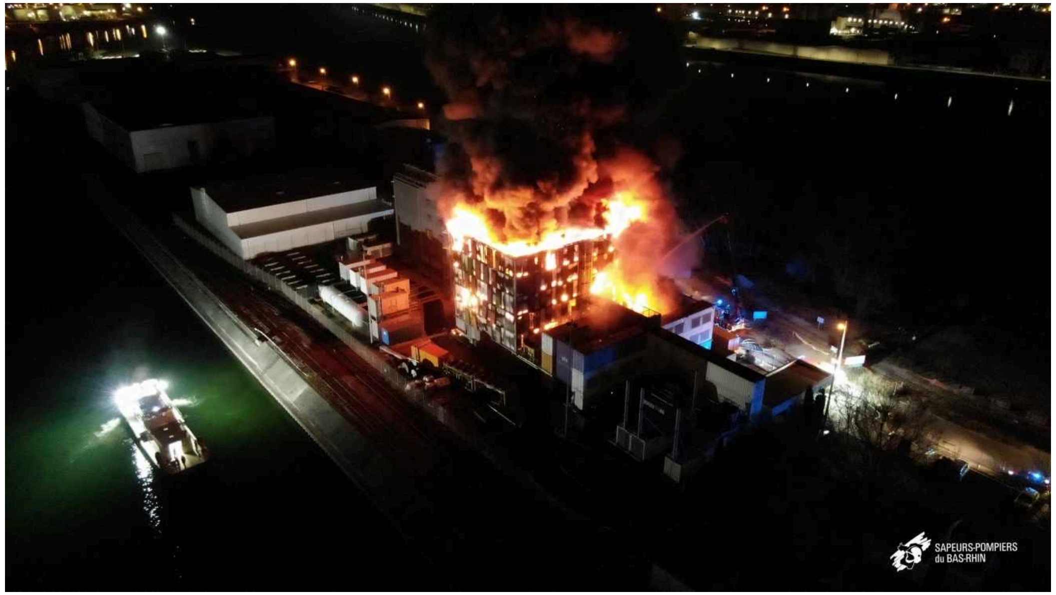


Strasbourg – where DCs go into flames

4 buildings in the same location (29,000 servers)

- SGB1 partially impacted,
- **SGB2 totally burned**,
- SGB3 is being progressively put back online and
- SGB4 needs to be checked

March 10, 2021



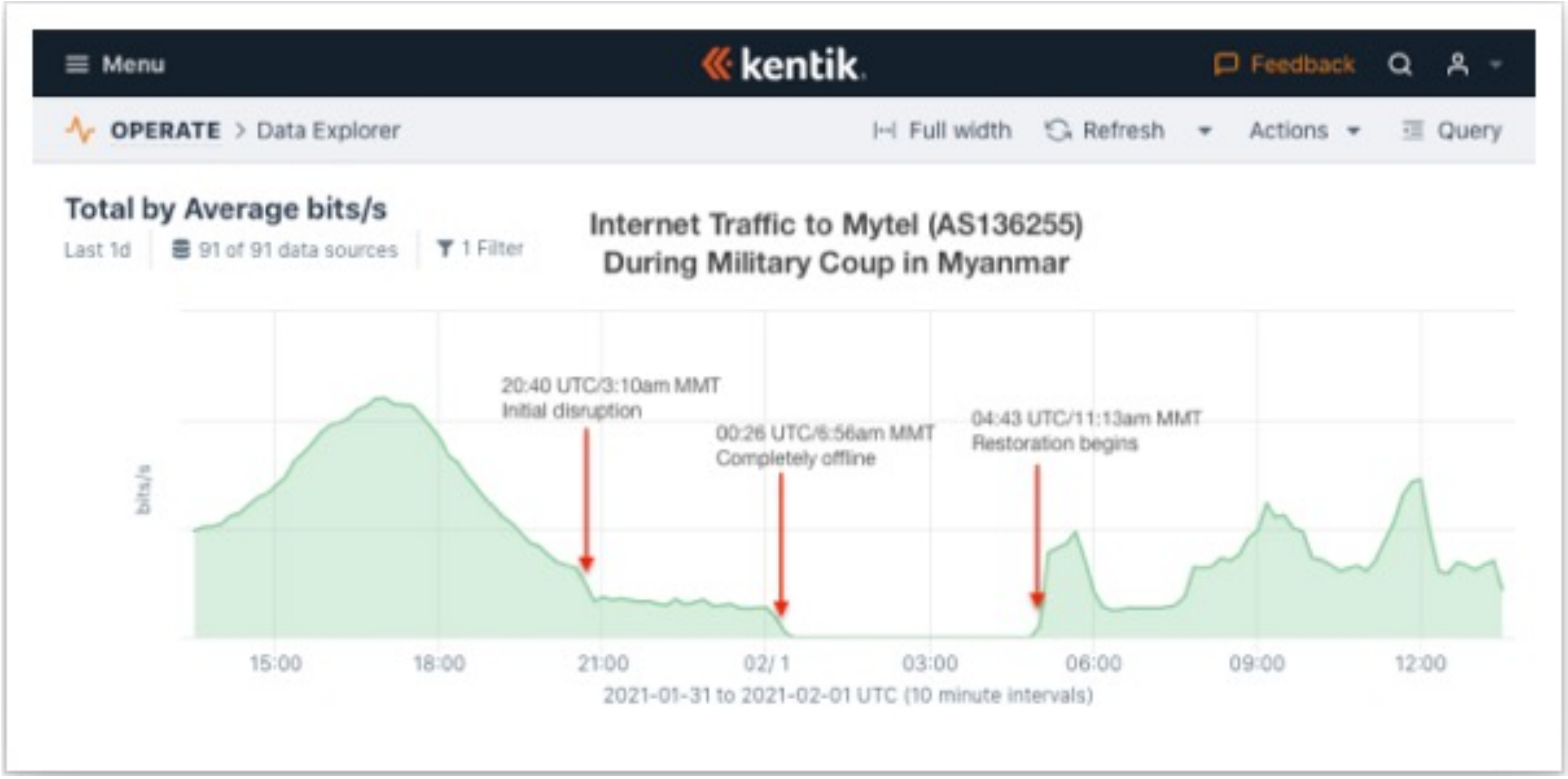
Many services are still down, data losses …

▶ Companies hopefully now understand the need for backups

Raises the question of the impact of a single hosting provider on the services we rely on

▶ With maybe some answers in upcoming measurement conferences ? 😉

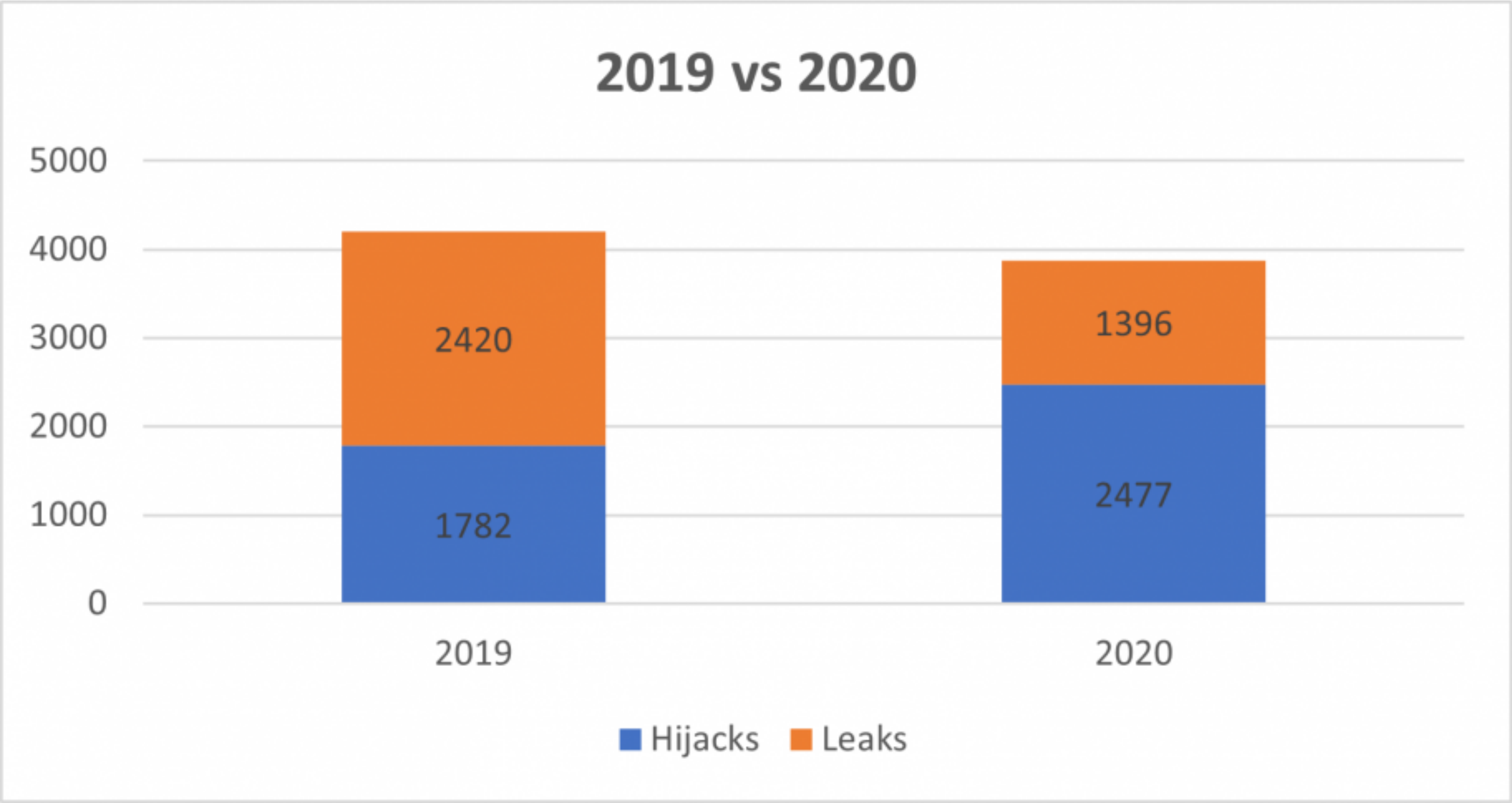
The Myanmar military coup – Jan 31, 2021



Doug Madory. https://www.kentik.com/blog/myanmar-goes-offline-during-military-coup/

And many more …

The ISOC reported around 4,000 BGP leaks and hijacks in 2019 and 2020



Source: https://www.manrs.org/2021/02/bgp-rpki-and-manrs-2020-in-review/

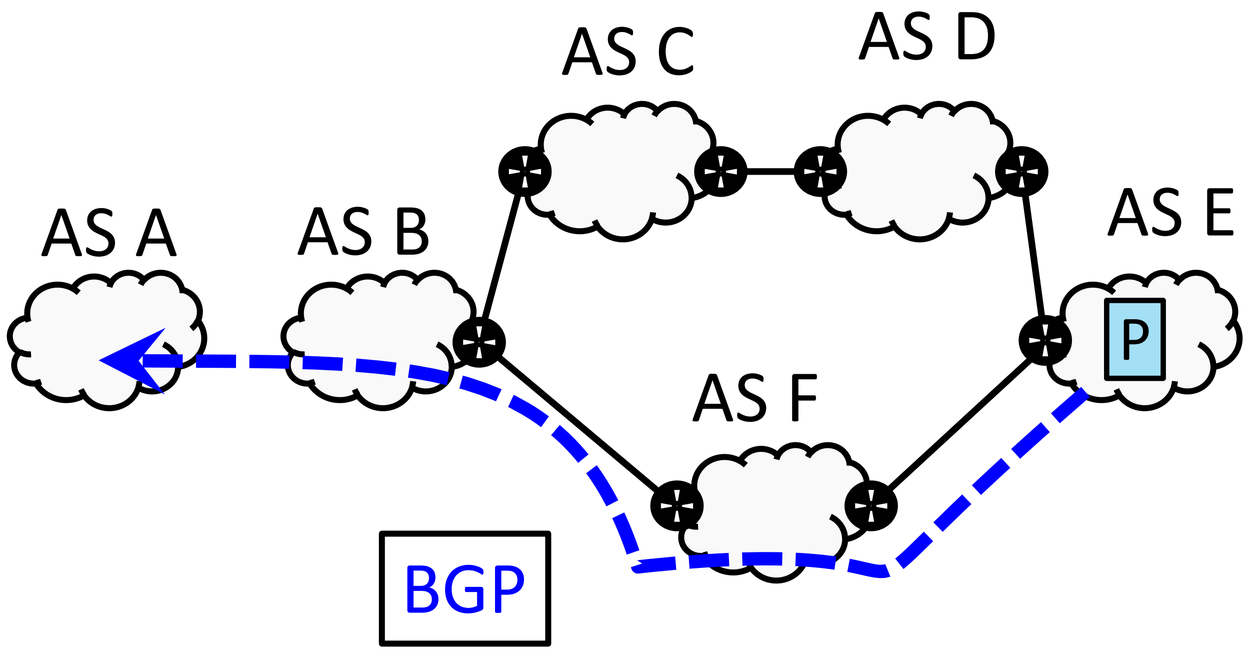
Some of my work on detecting such events

- R. Fontugne , E. Aben , C. Pelsser, R. Bush. *Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements*, IMC 2017.
- A. Guillot, R. Fontugne , P. Winter , P. Merindol, A. King , A. Dainotti , C. Pelsser. *Chocolatine: Outage Detection for Internet Background Radiation*, TMA 2019.
- Odnan Ref Sanchez , Simone Ferlin , Cristel Pelsser, Randy Bush. *Comparing Machine Learning Algorithms for BGP Anomaly Detection using Graph Features*. Big-DAMA'19: ACM CoNEXT Workshop 2019.
- Anant Shah , Romain Fontugne , Emile Aben , Cristel Pelsser, Randy Bush. *Disco: Fast, Good, and Cheap Outage Detection*. TMA 2017.

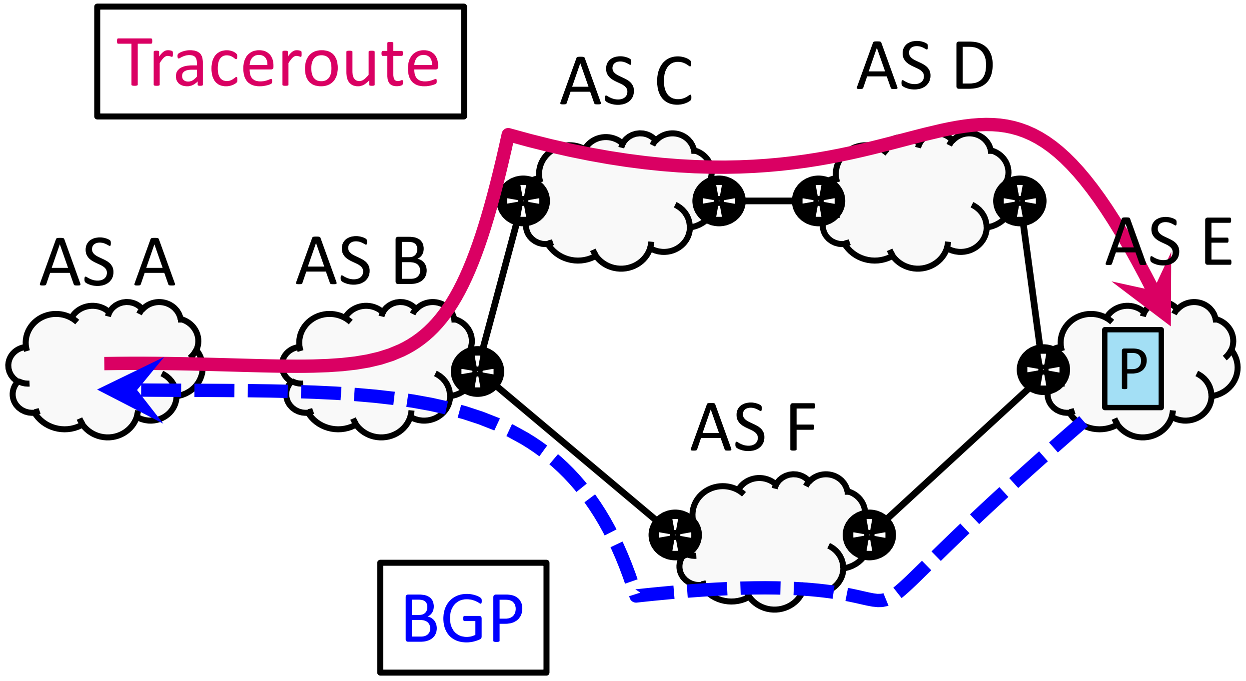
There are big outages …

and there are more subtle issues

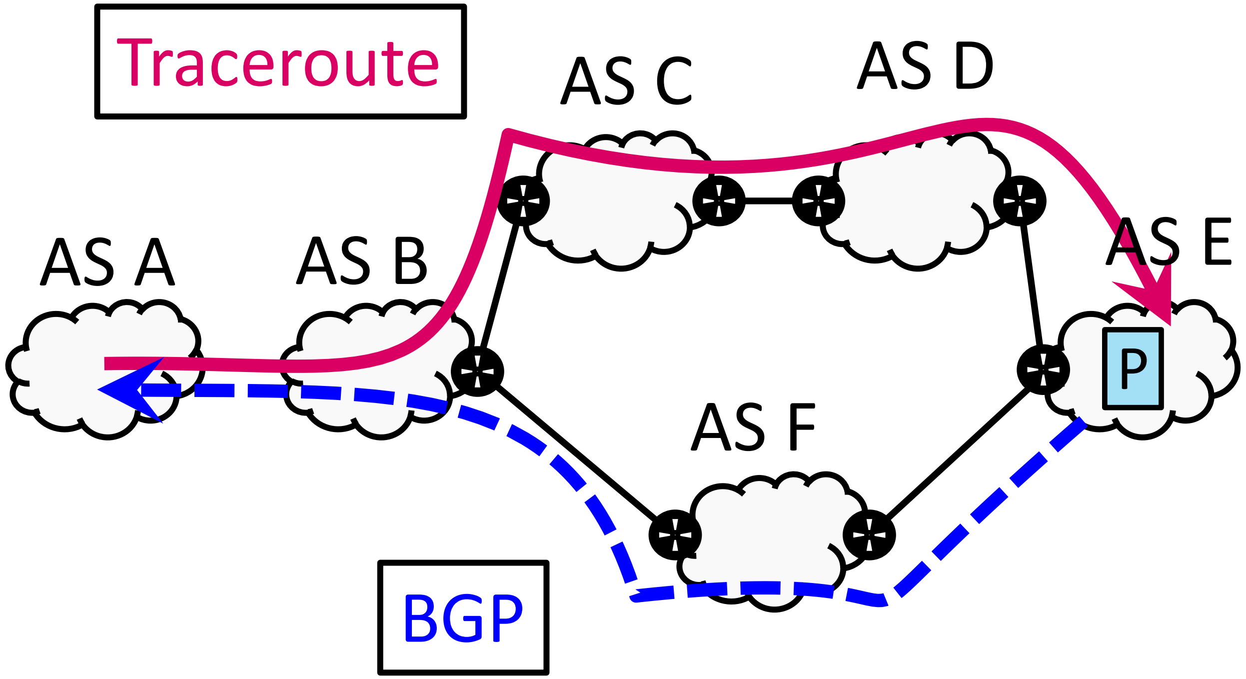
An ISP (AS B) announces a path in BGP but forwards packets along a different path



An ISP (AS B) announces a path in BGP but forwards packets along a different path



An ISP (AS B) announces a path in BGP but forwards packets along a different path



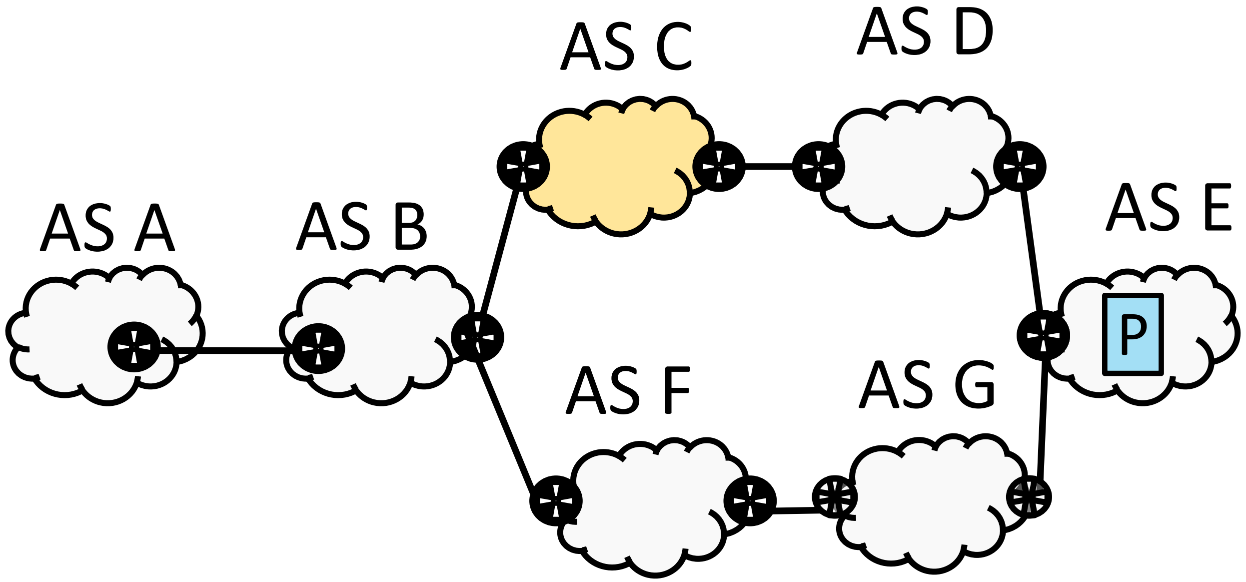
Because the peer C is cheaper

Or peer C pays B to access traffic data from AS A

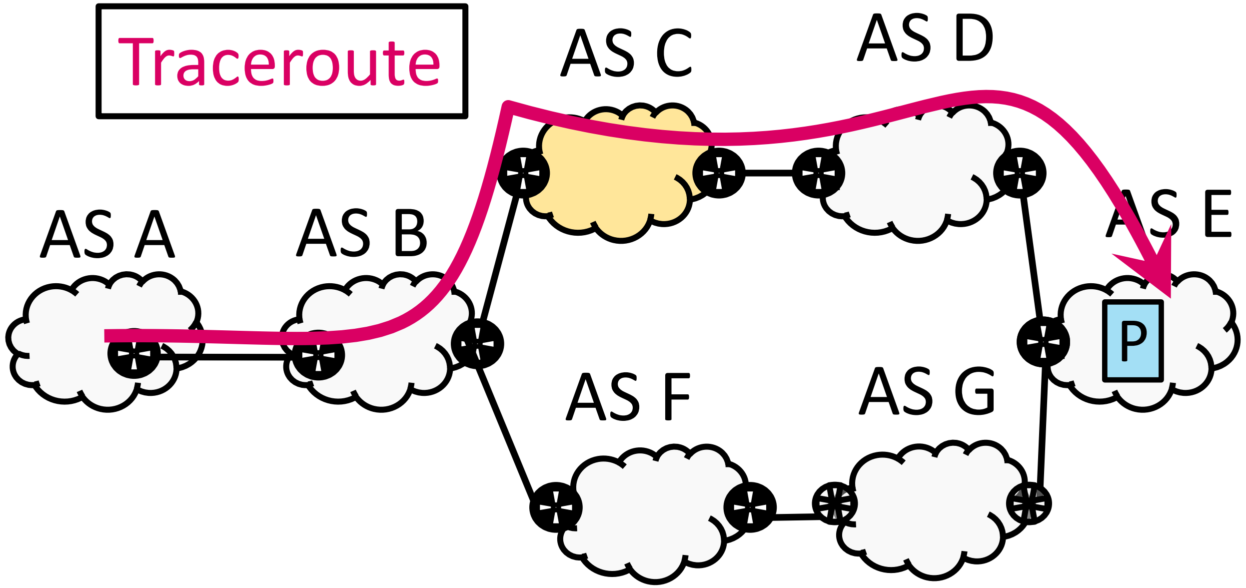
Or …

This difference in control and data paths may also be observed in the Kapela-Pilosov BGP monkey-in-the-middle attack

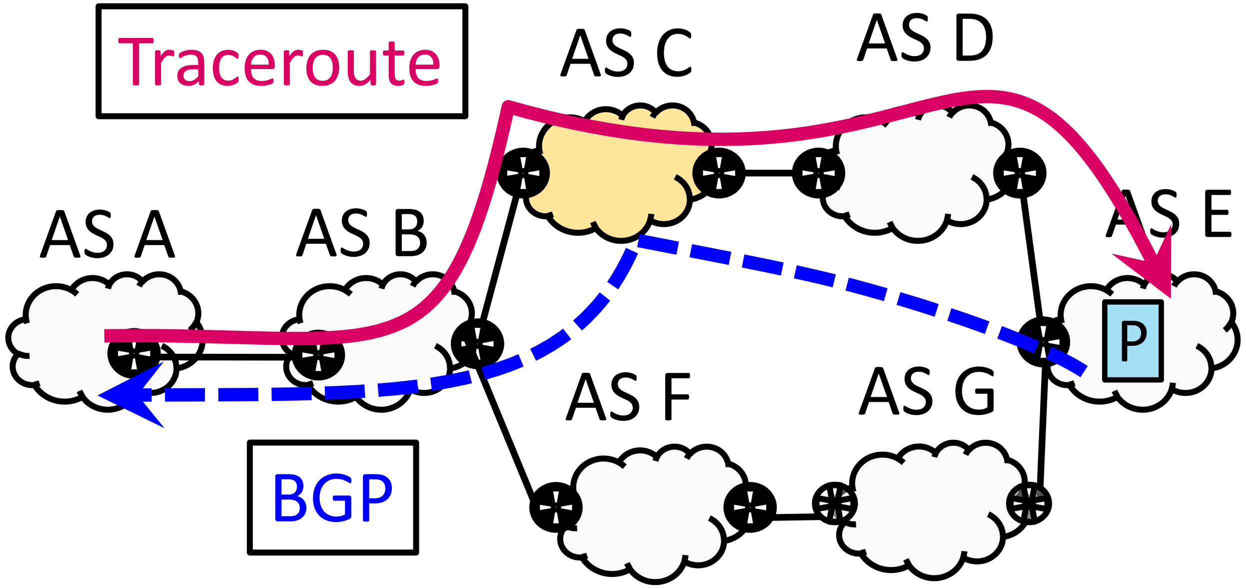
The topology



This difference in control and data paths may also be observed in the Kapela-Pilosov BGP monkey-in-the-middle attack



This difference in control and data paths may also be observed in the Kapela-Pilosov BGP monkey-in-the-middle attack

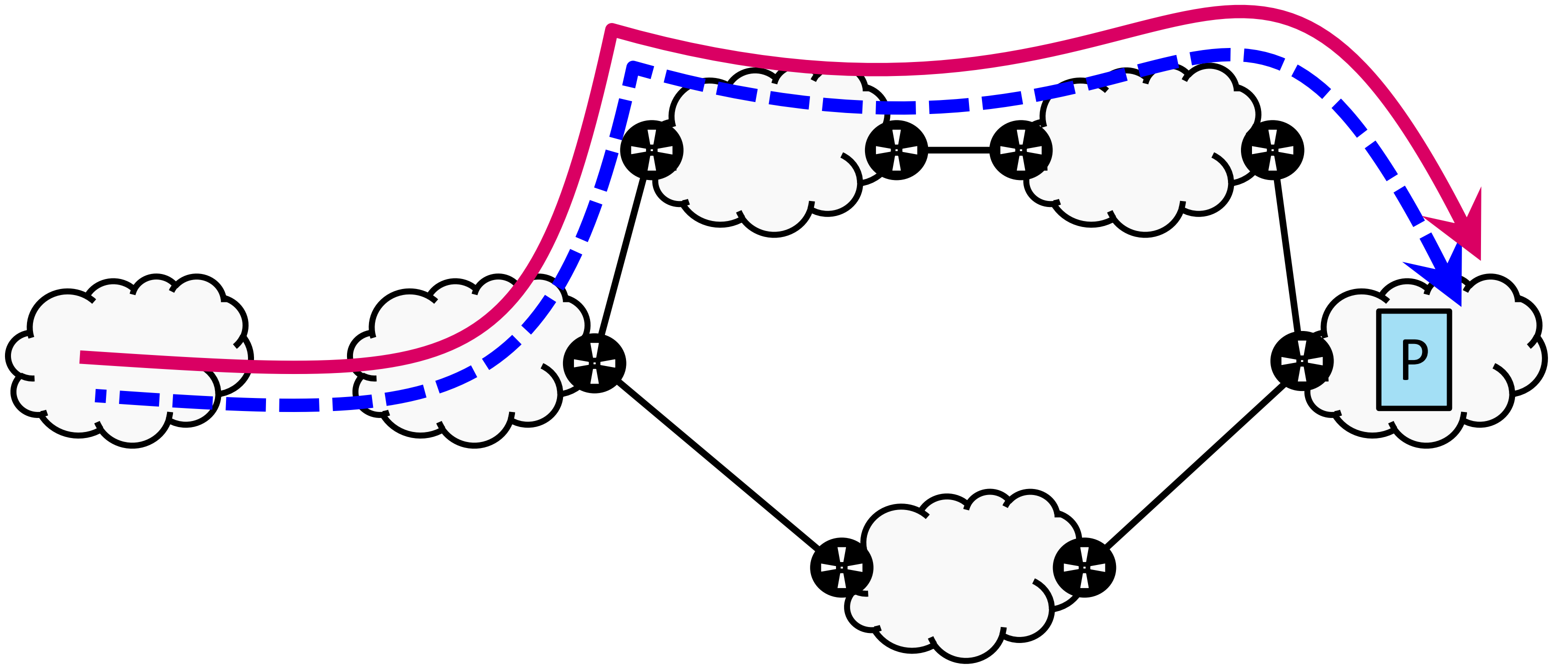


But for packets to follow the traceroute path, the yellow AS faked a direct link to the prefix origin

The general assumption is that

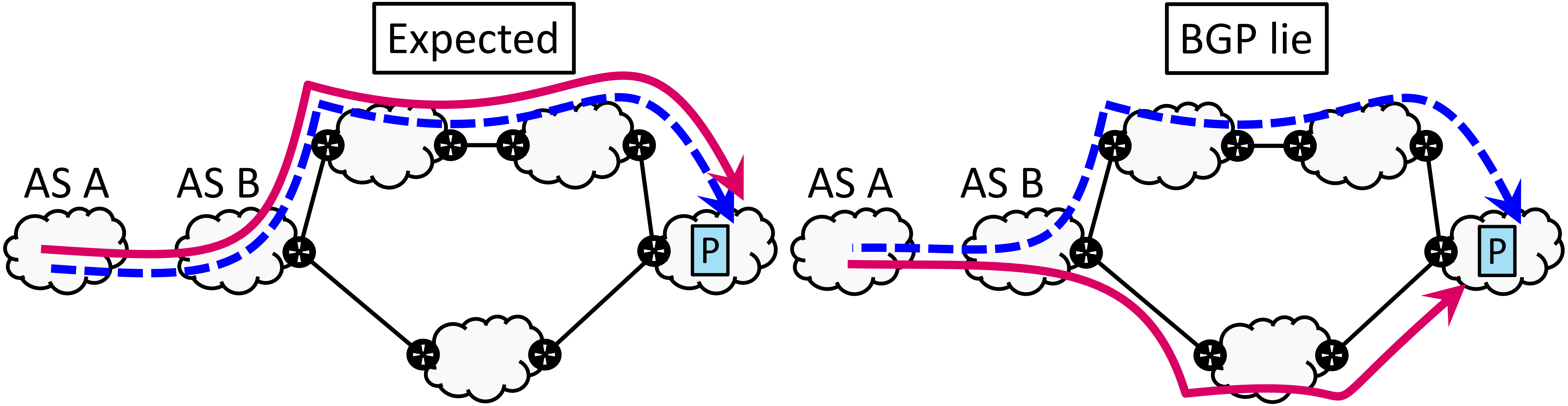
For each external prefix P...

- The control path (CP) advertised in BGP
- And the data path (DP) used in **practice** are the same

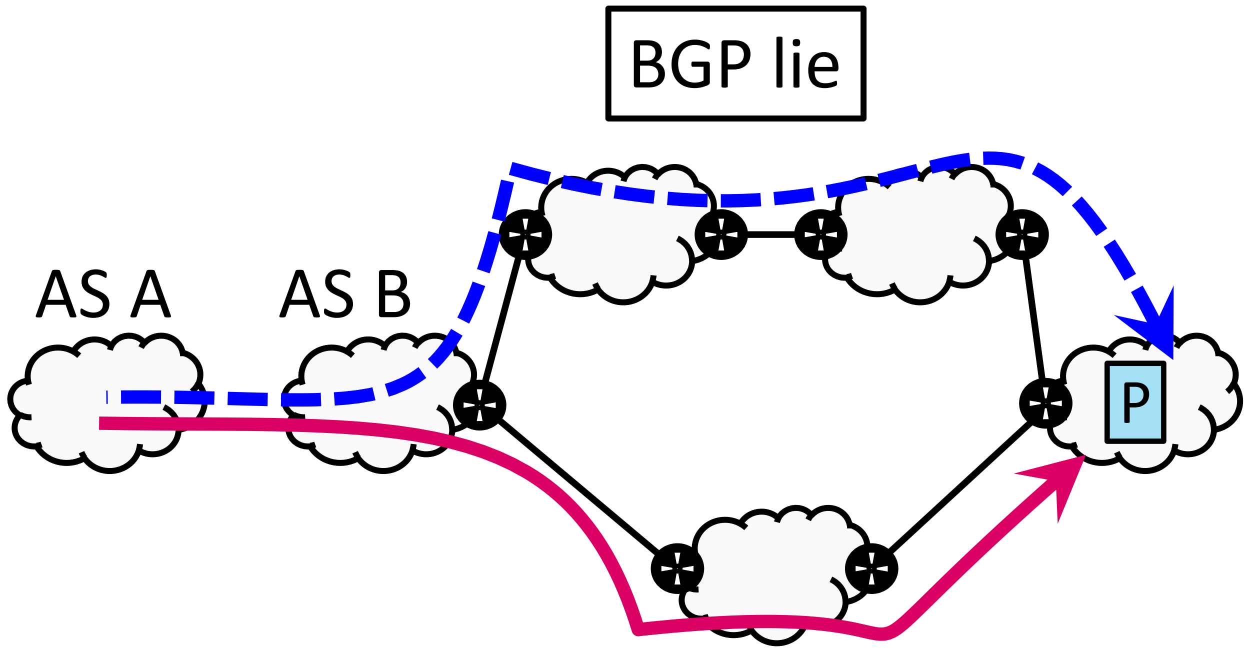


One form of BGP lie is

when the control path (CP) and data path (DP) for a prefix P do not match



Why detect BGP lies (CP ≠ DP)?

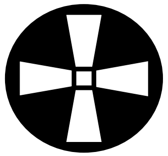


- If not, what is the point of using BGP?
- Allows us to detect possible malicious activities
- Would allow us to troubleshoot ASes

Detecting BGP lies

Required data

Control paths

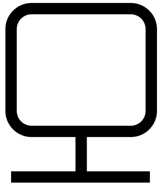


P	CP
P_Y	BCD
P_R	D
P_V	E

Data paths

Vantage Point (VP)

Traceroute per destination



Issues to consider

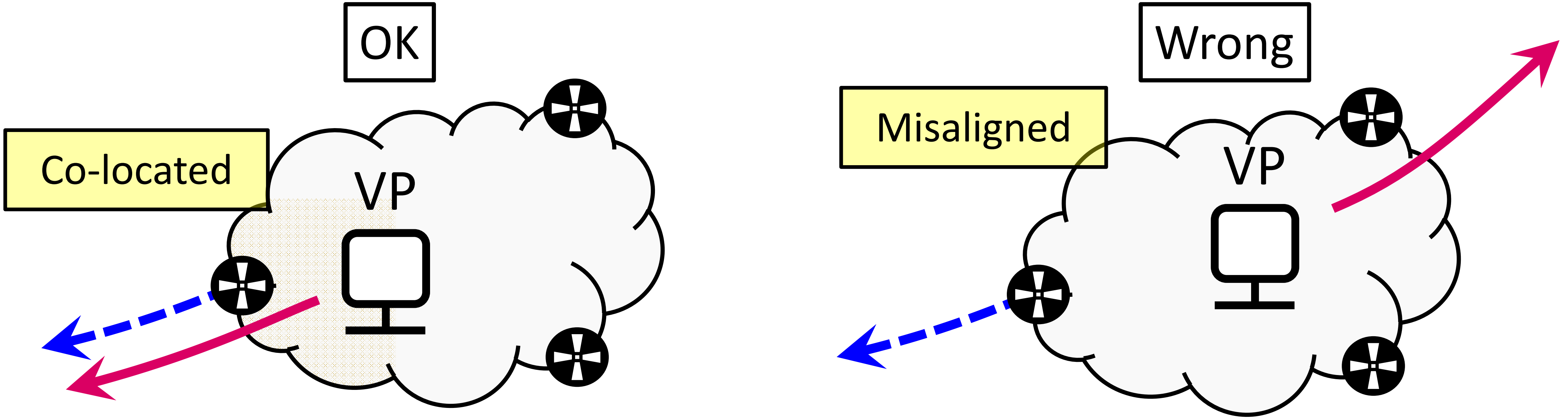
- Space-synchronization
  - Measurement platform
- Address space and time synchronization
  - Which DP should be compared with which CP
- IP-to-AS mapping
  - CPs come as AS-paths but DPs as IP-paths

Issues to consider

- Space-synchronization
  - Measurement platform
- Address space and time synchronization
  - Which DP should be compared with which CP
- IP-to-AS mapping
  - CPs come as AS-paths but DPs as IP-paths

Space-synchronization

- Control paths are obtained from a given router
- Data paths are gathered from a VP
- To be comparable, DPs need to go through the router that shared the CPs



IP-to-AS mapping

- While CPs are AS-paths, DPs are obtained as IP-paths

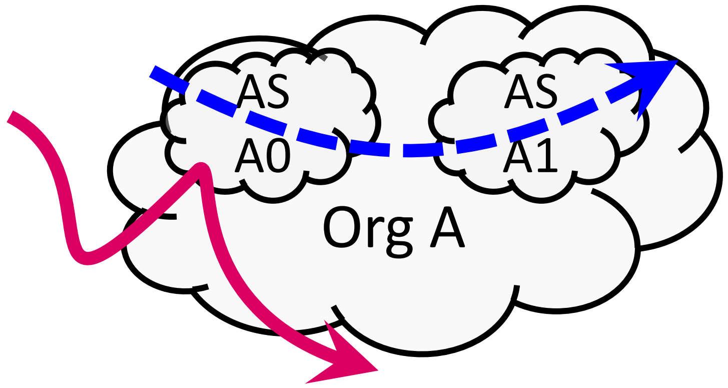
```
CP: AS A, AS B, AS C…
DP: IP1, IP2, IP3, IP4…
```

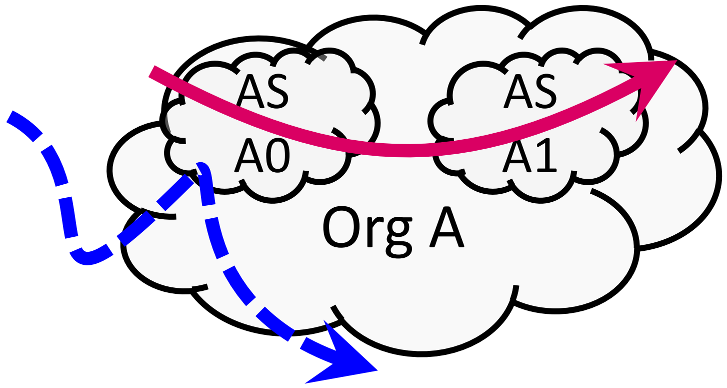
To compare them, an IP-to-AS mapping tool is needed !

The problem of IP-to-AS mapping

Noise or sources of errors

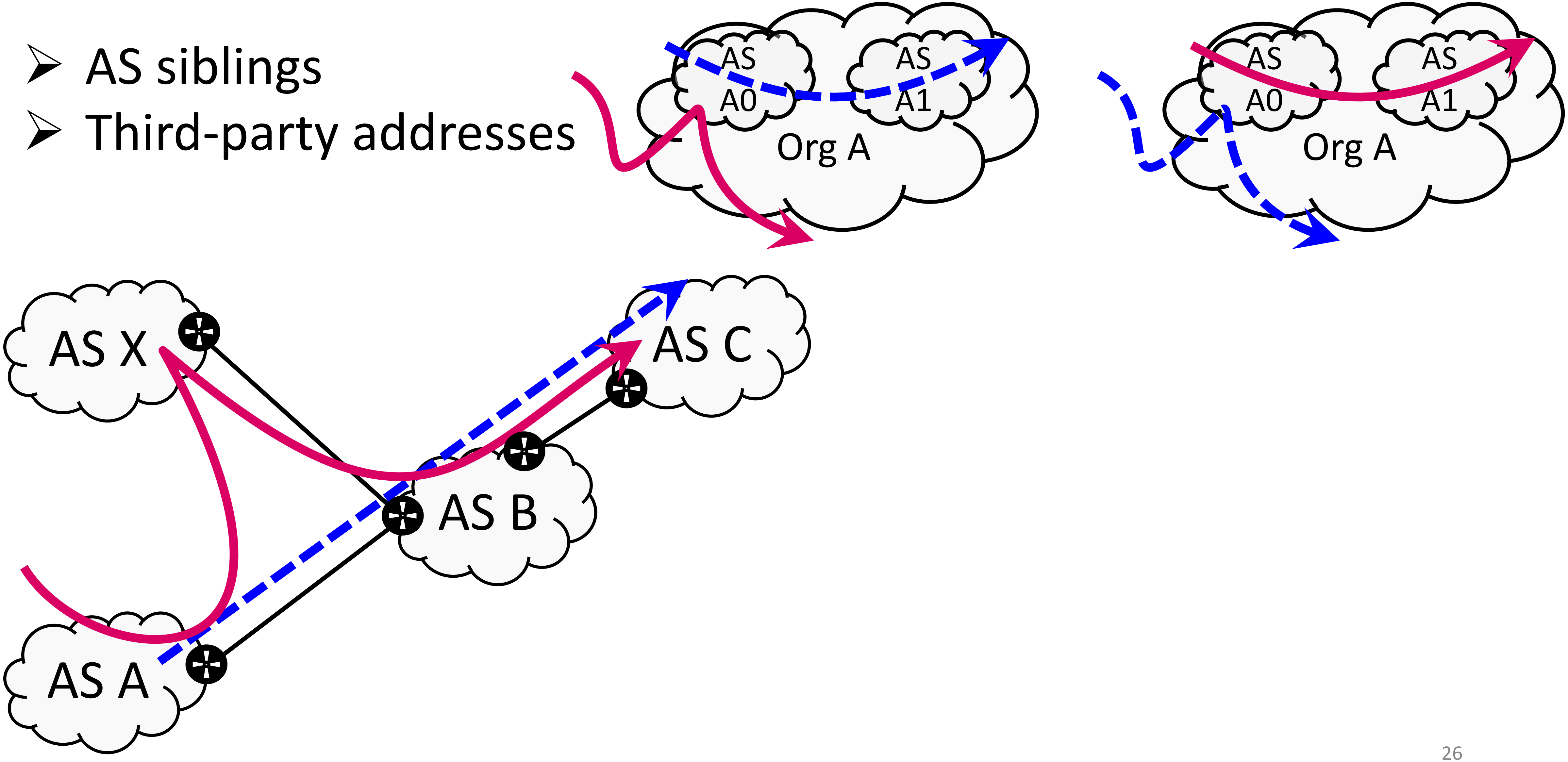
- AS siblings





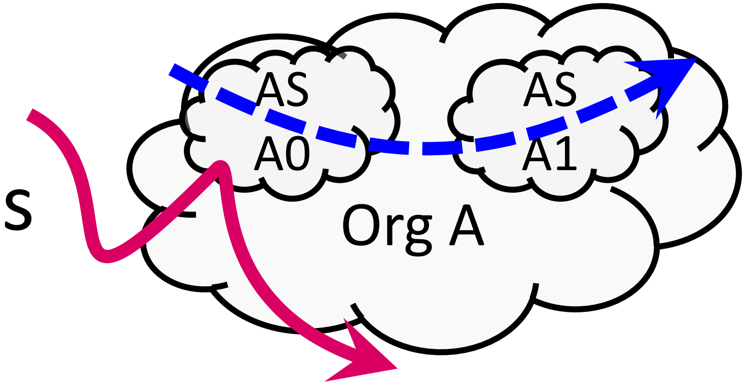
Noise or sources of errors

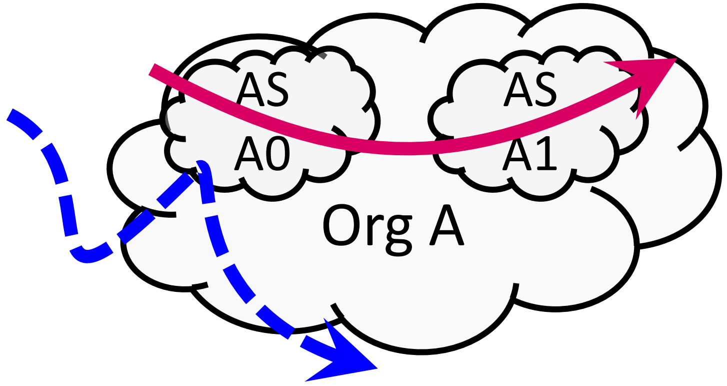
- AS siblings
- Third-party addresses

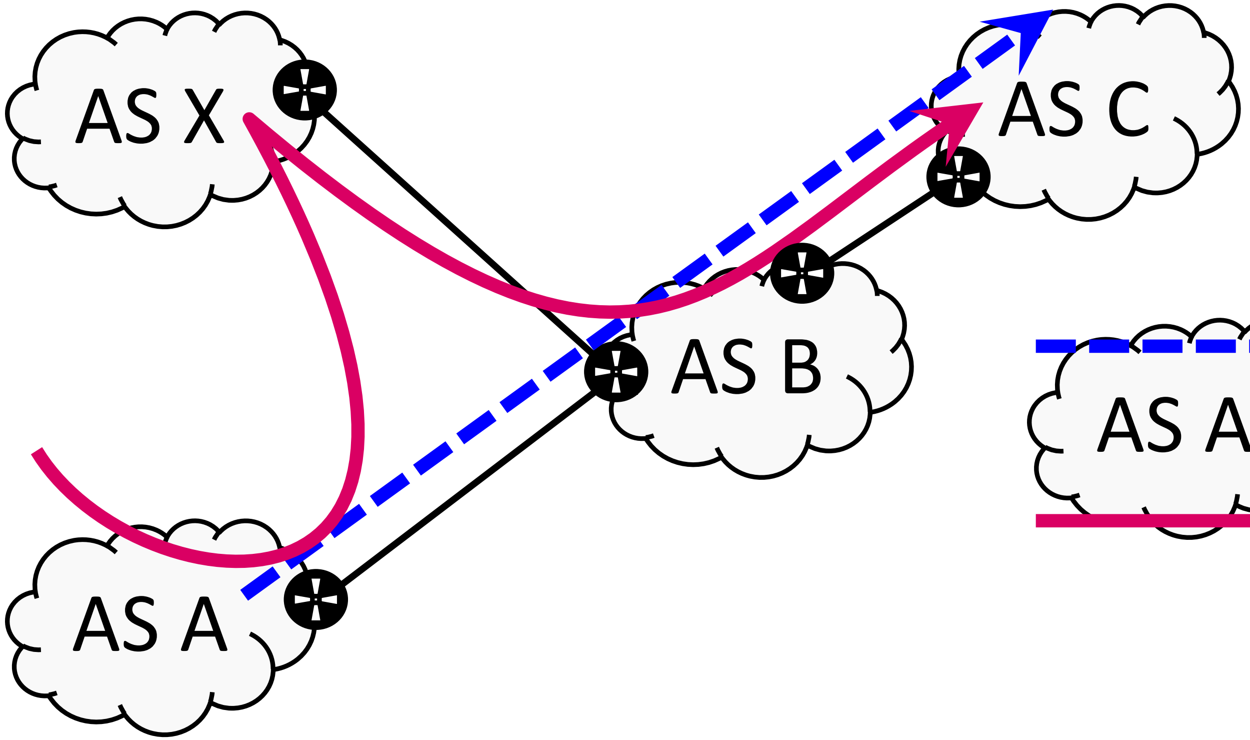


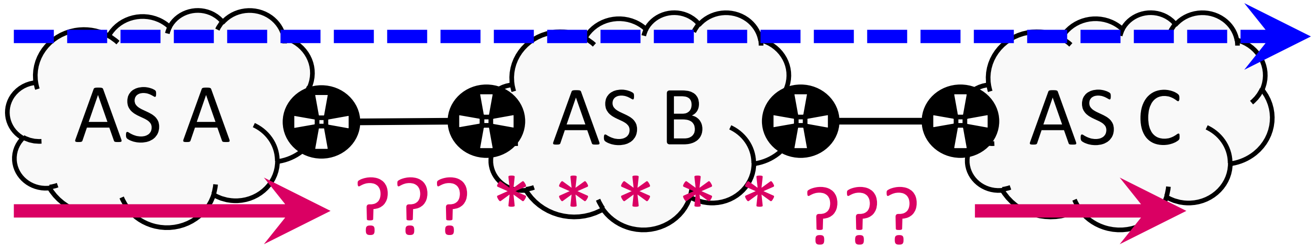
Noise or sources of errors

- AS siblings
- Third-party addresses
- Missing hops



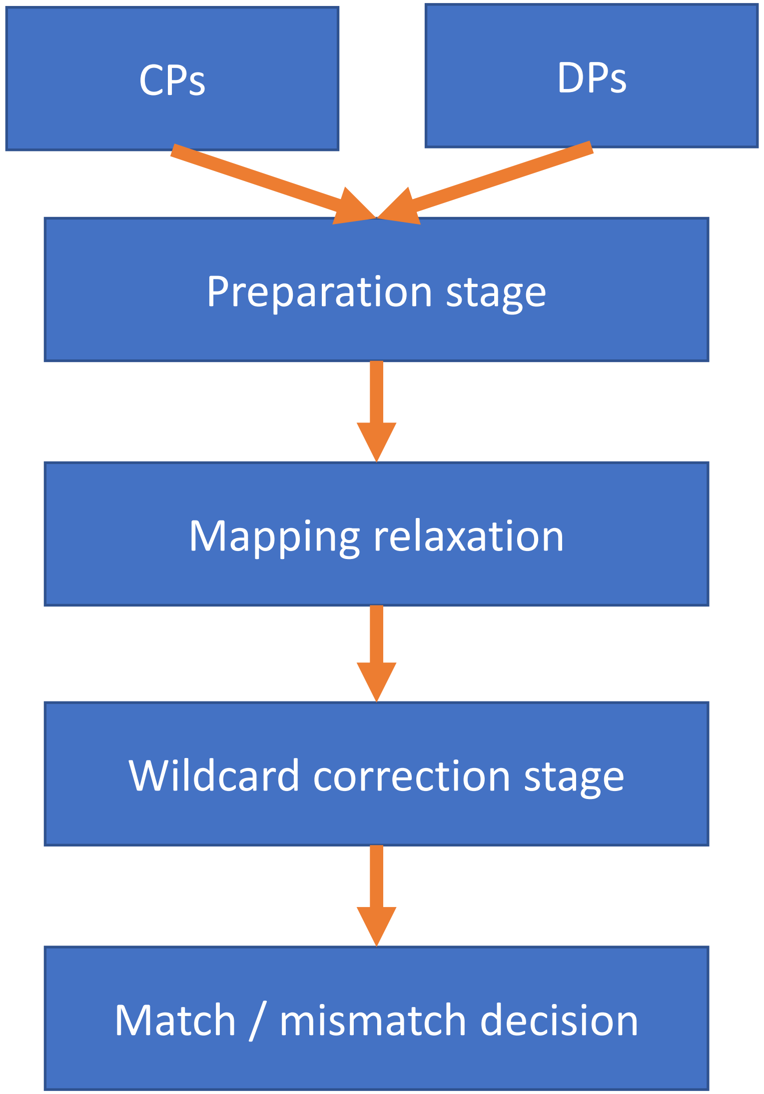






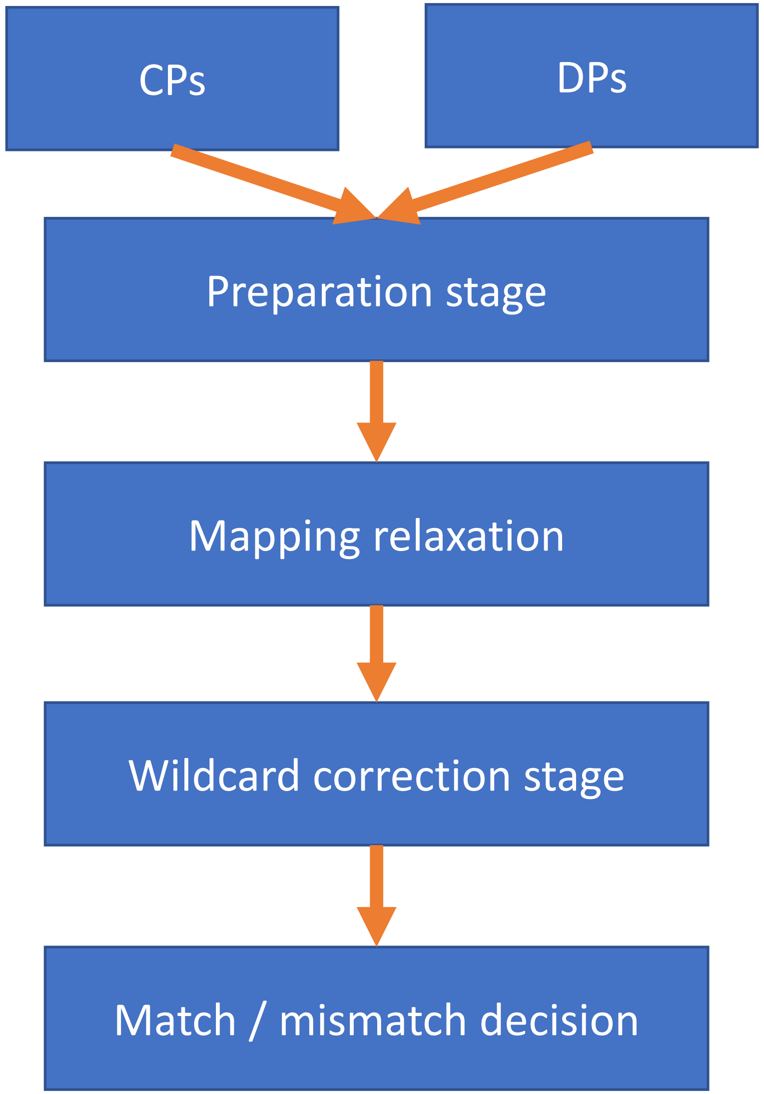
Our solution

A framework to detect BGP lies



- ✓ **Input:** CPs and DPs from a co-located VP
- ✓ **Output:** rate of BGP lies

A framework to detect BGP lies



✓ **Input:** CPs and DPs from a co-located VP

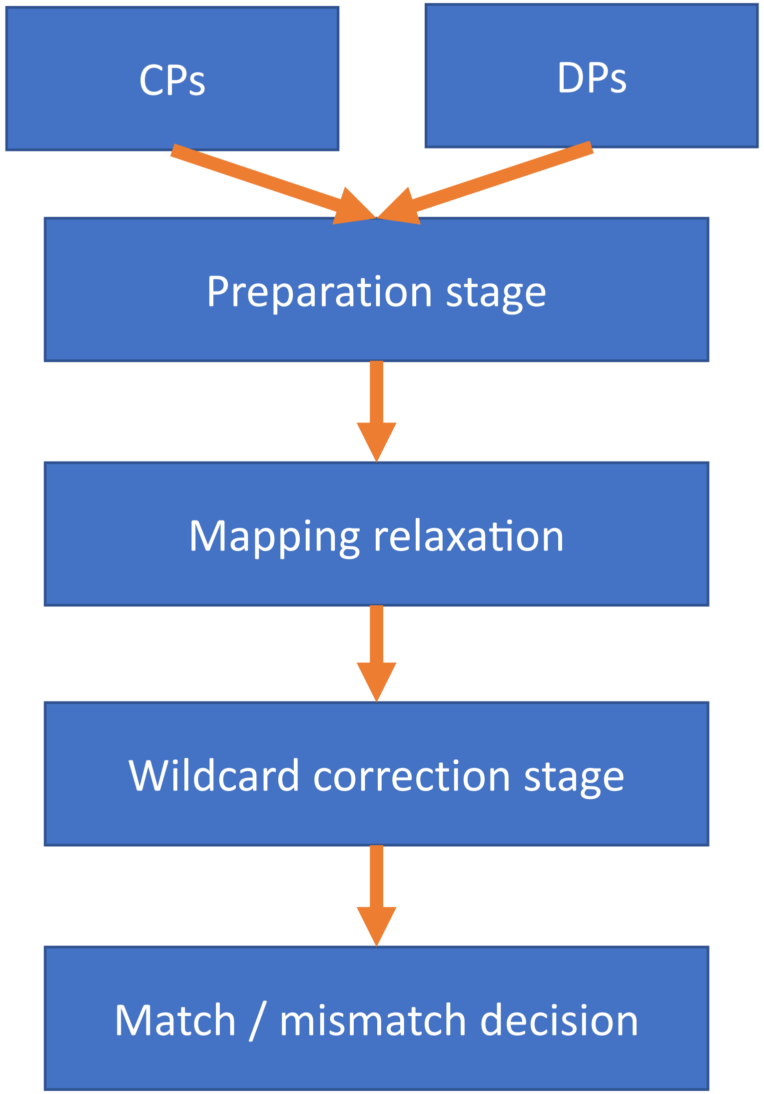
✓ **Output:** rate of BGP lies

❑ **Preparation stage:**
- Address space synchronization
- Time synchronization
- Basic IP-to-AS mapping

❑ **Mapping relaxation**
- AS siblings
- Third-party addresses

❑ **Wildcards correction stage**
- Missing hops

A framework to detect BGP lies



- ✓ **Input:** CPs and DPs from a co-located VP
- ✓ **Output:** rate of BGP lies

- ❑ **Preparation stage:**
  - Address space synchronization
  - Time synchronization
  - Basic IP-to-AS mapping
- ❑ **Mapping relaxation**
  - AS siblings
  - Third-party addresses
- ❑ **Wildcards correction stage**
  - Missing hops

...we are conservative!

Our measurements

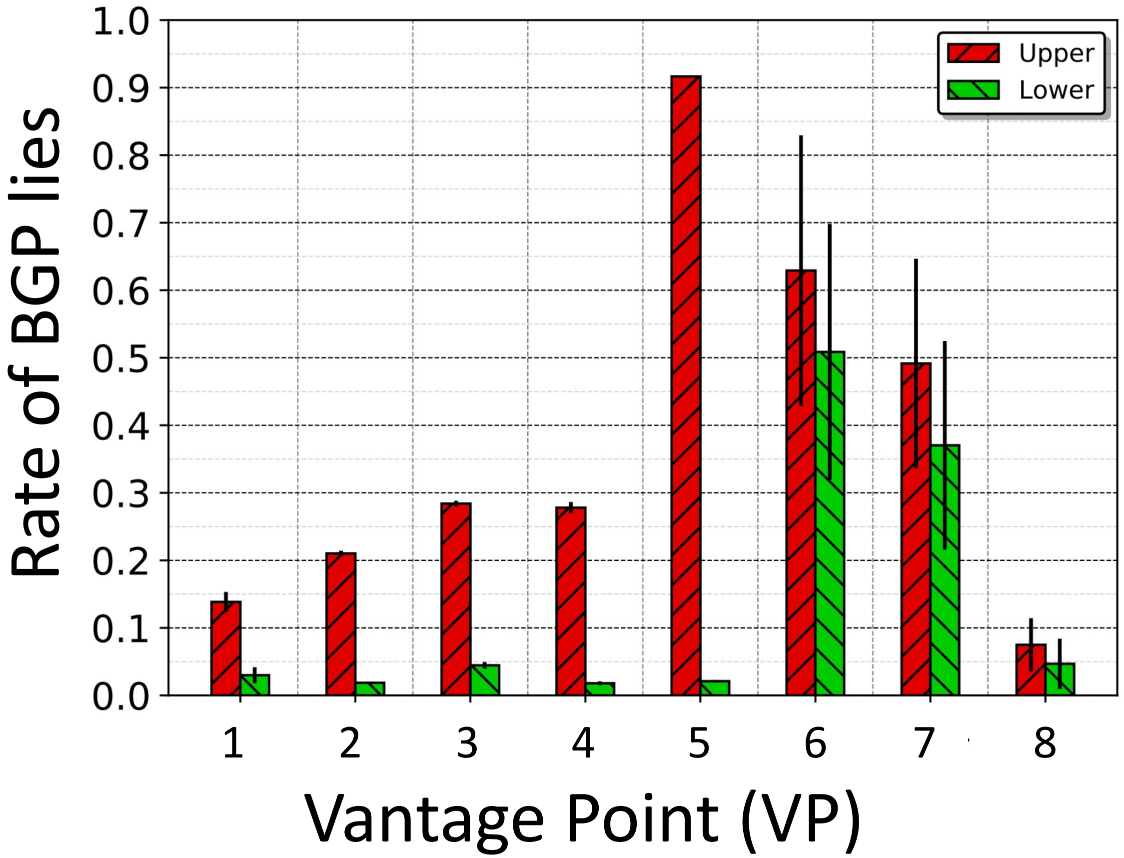
Experiment setup

- Deployed 8 co-located VPs
- CPs collected every two hours
- DPs gathered targeting 80K destinations per day
- We run measurements multiple days (at least 13 days)

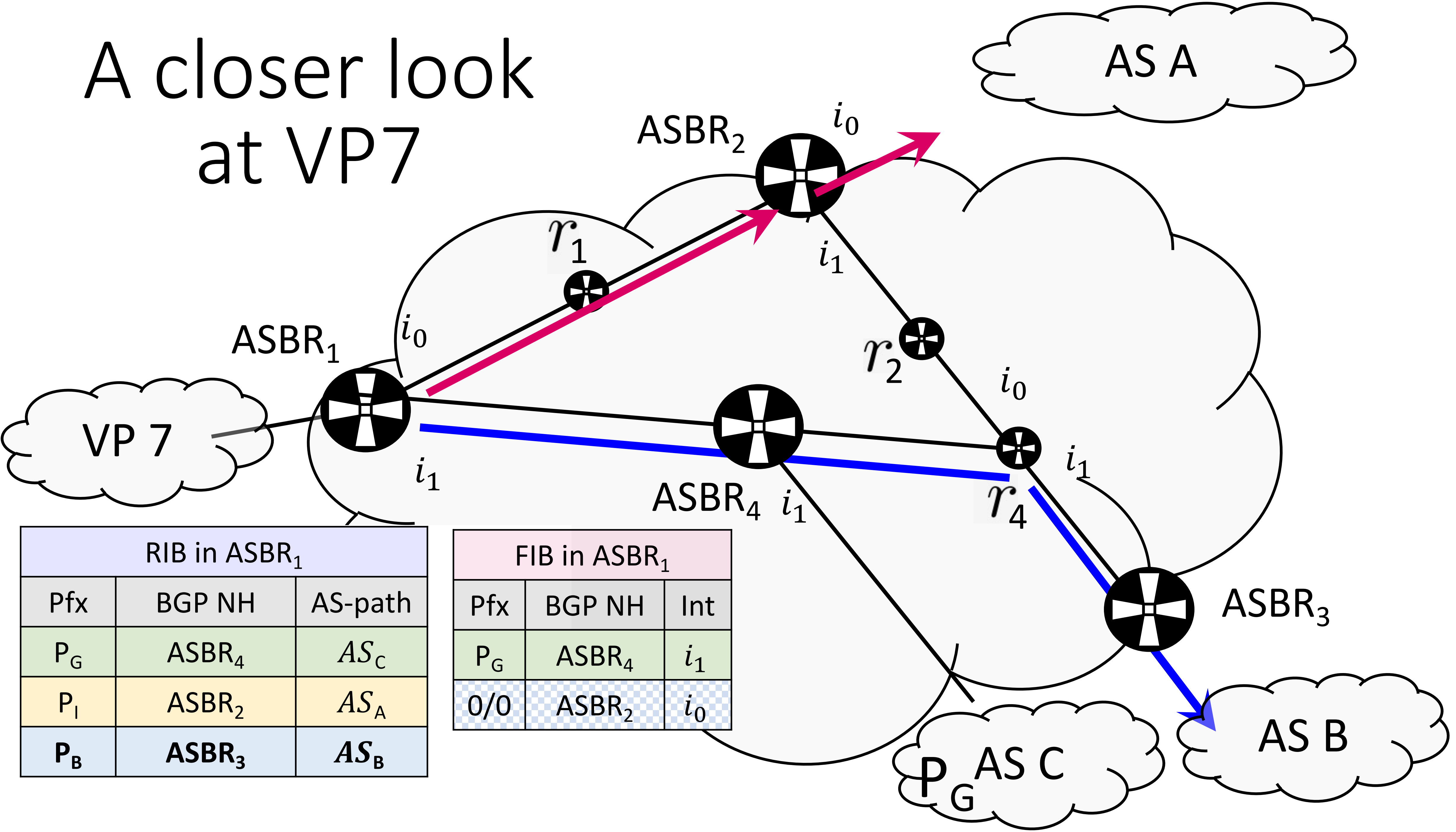
Low number of mismatches for most vantage points but they exist

At VP 7, the high number of ”lies” is due to patial forwarding tables in the provider AS.

These partial tables also create detours in the provider.



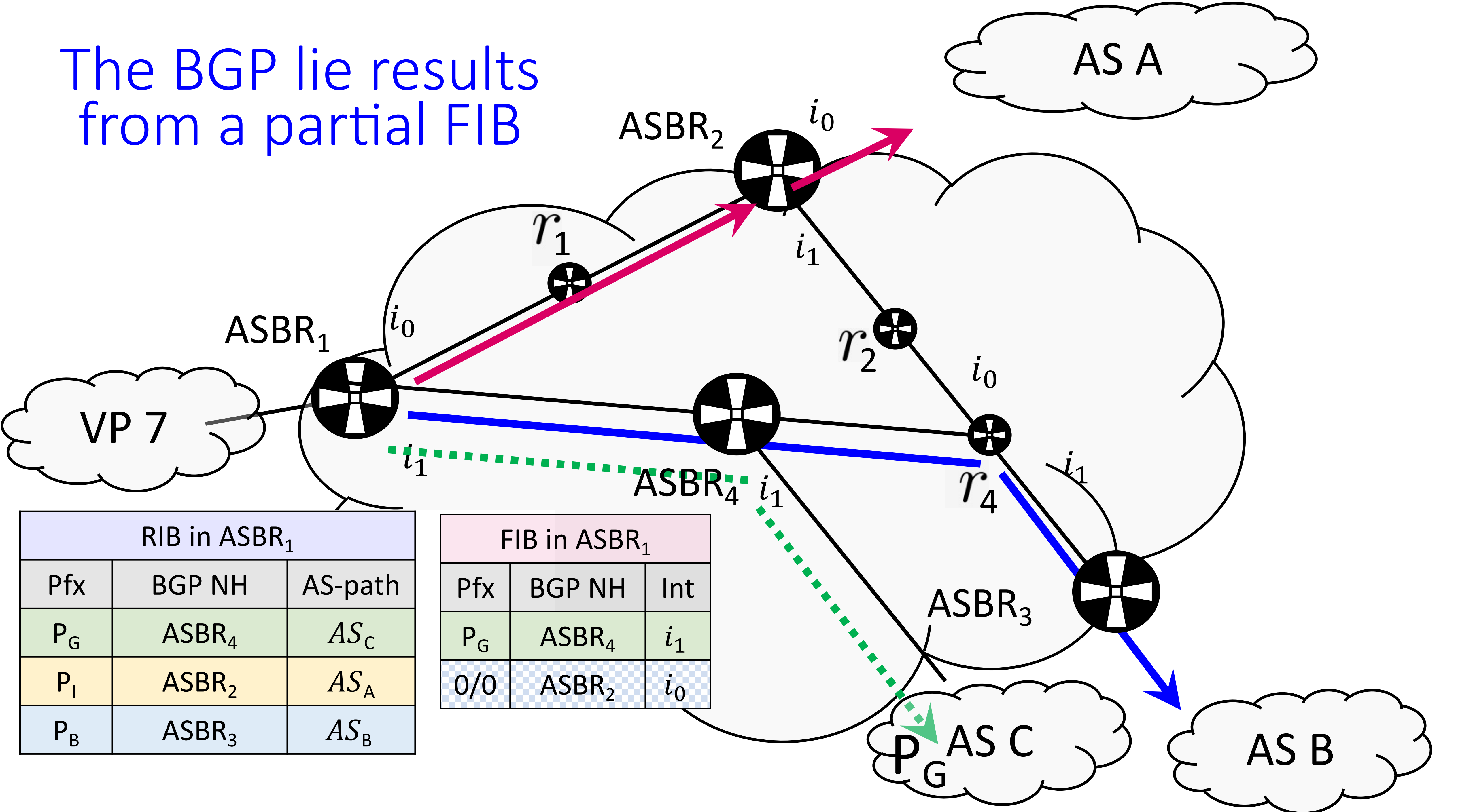
A closer look at VP7



RIB in $ASBR_1$		
Pfx	BGP NH	AS-path
P_G	$ASBR_4$	AS_C
P_I	$ASBR_2$	AS_A
P_B	**$ASBR_3$**	**AS_B**

FIB in $ASBR_1$		
Pfx	BGP NH	Int
P_G	$ASBR_4$	i_1
0/0	$ASBR_2$	i_0

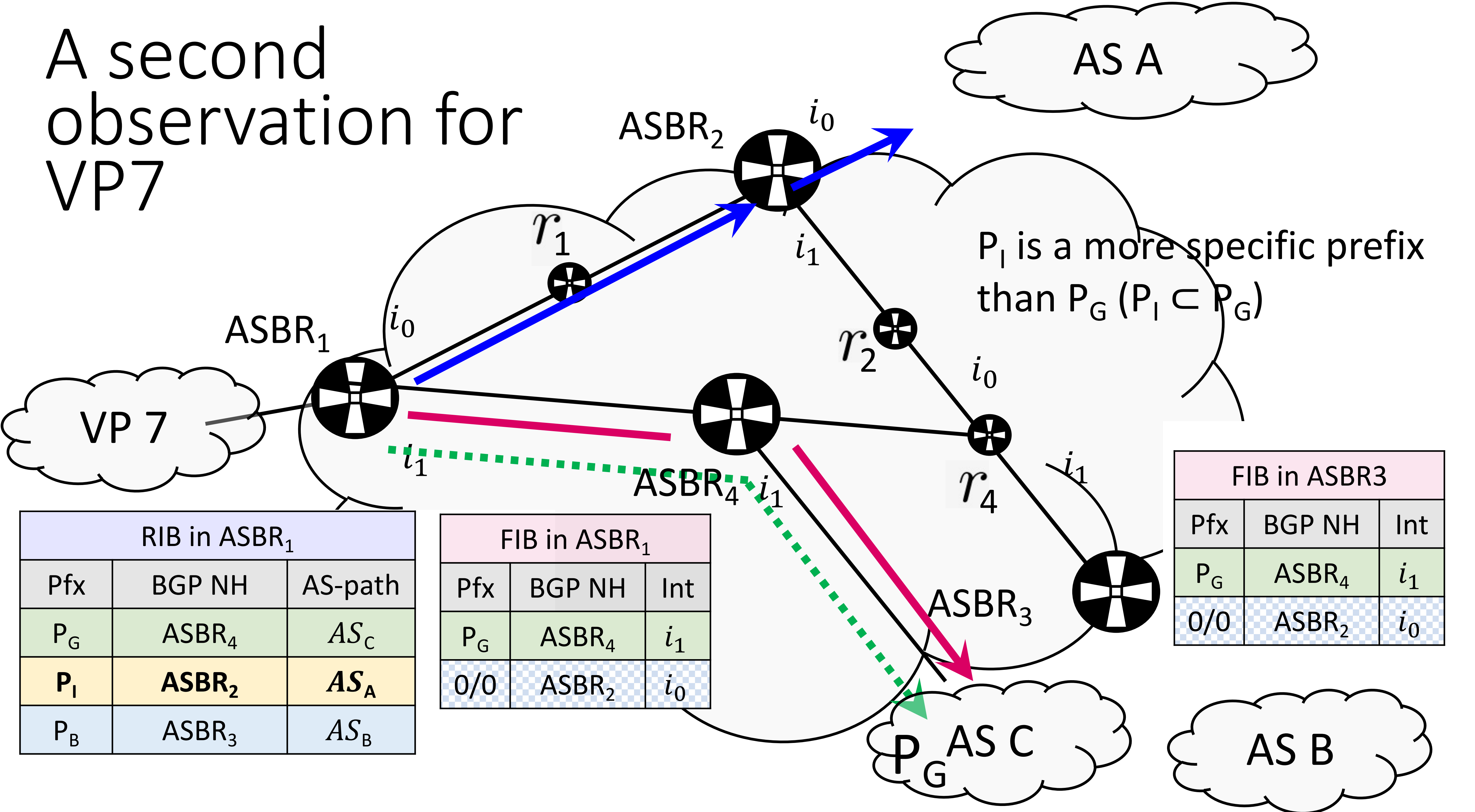
The BGP lie results from a partial FIB



RIB in ASBR$_1$		
Pfx	BGP NH	AS-path
P_G	ASBR$_4$	AS_C
P_I	ASBR$_2$	AS_A
P_B	ASBR$_3$	AS_B

FIB in ASBR$_1$		
Pfx	BGP NH	Int
P_G	ASBR$_4$	i_1
0/0	ASBR$_2$	i_0

A second observation for VP7

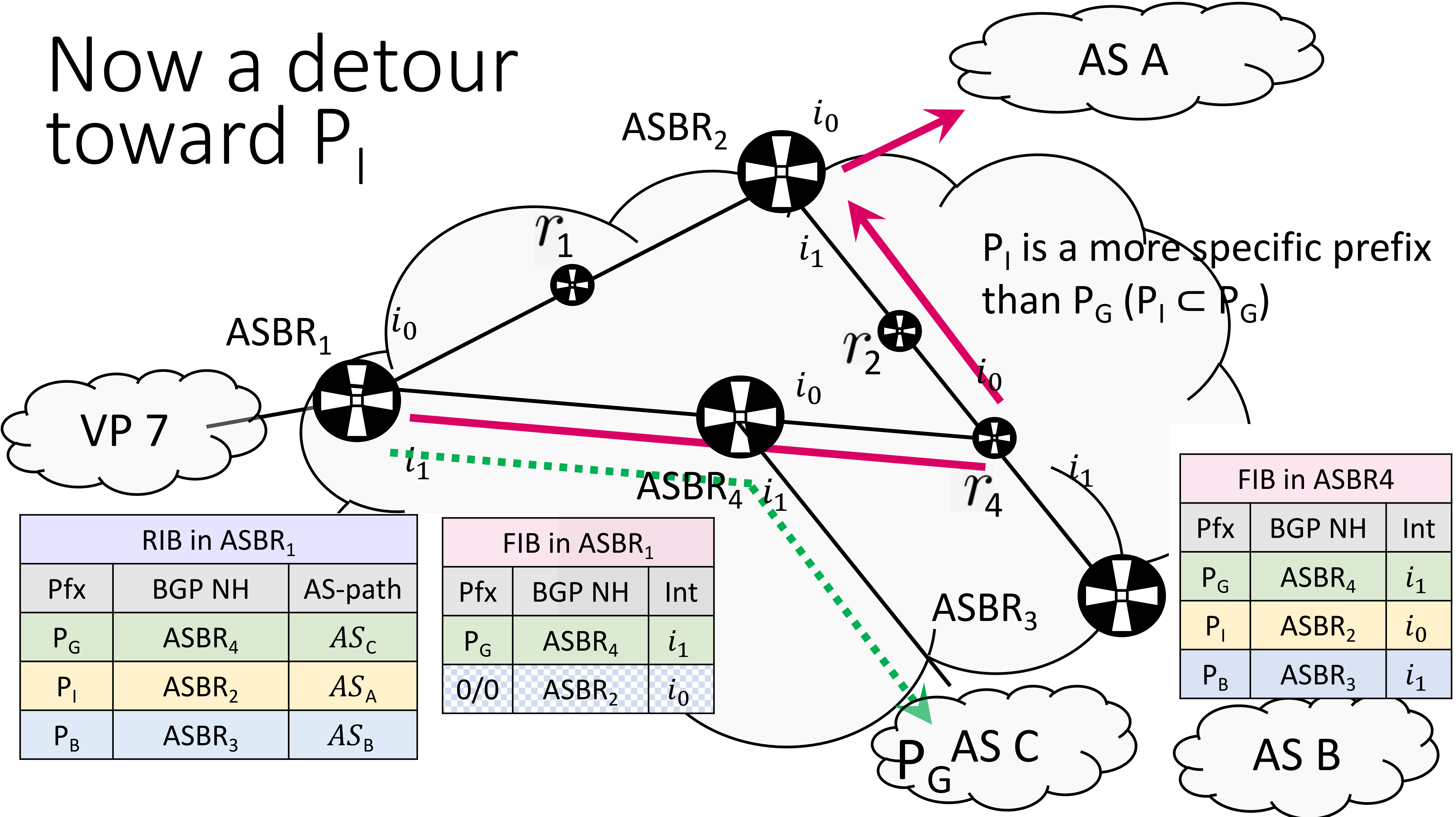


RIB in ASBR$_1$		
Pfx	BGP NH	AS-path
P_G	ASBR$_4$	AS_C
P_I	**ASBR$_2$**	**AS_A**
P_B	ASBR$_3$	AS_B

FIB in ASBR$_1$		
Pfx	BGP NH	Int
P_G	ASBR$_4$	i_1
0/0	ASBR$_2$	i_0

FIB in ASBR3		
Pfx	BGP NH	Int
P_G	ASBR$_4$	i_1
0/0	ASBR$_2$	i_0

Now a detour toward P_I



RIB in ASBR$_1$		
Pfx	BGP NH	AS-path
P_G	ASBR$_4$	AS_C
P_I	ASBR$_2$	AS_A
P_B	ASBR$_3$	AS_B

FIB in ASBR$_1$		
Pfx	BGP NH	Int
P_G	ASBR$_4$	i_1
0/0	ASBR$_2$	i_0

FIB in ASBR4		
Pfx	BGP NH	Int
P_G	ASBR$_4$	i_1
P_I	ASBR$_2$	i_0
P_B	ASBR$_3$	i_1

Take away on BGP lies

- A framework to detect BGP lies filtering the IP-to-AS mapping noise
- We care because lies have security implications, can mislead our measurements
- Patterns in results: technical limitations vs malicious ASs?

Lies and detours can be present in the same ASs

Both lead to unpredictable routing

Detecting both lies and detours can help debugging routing

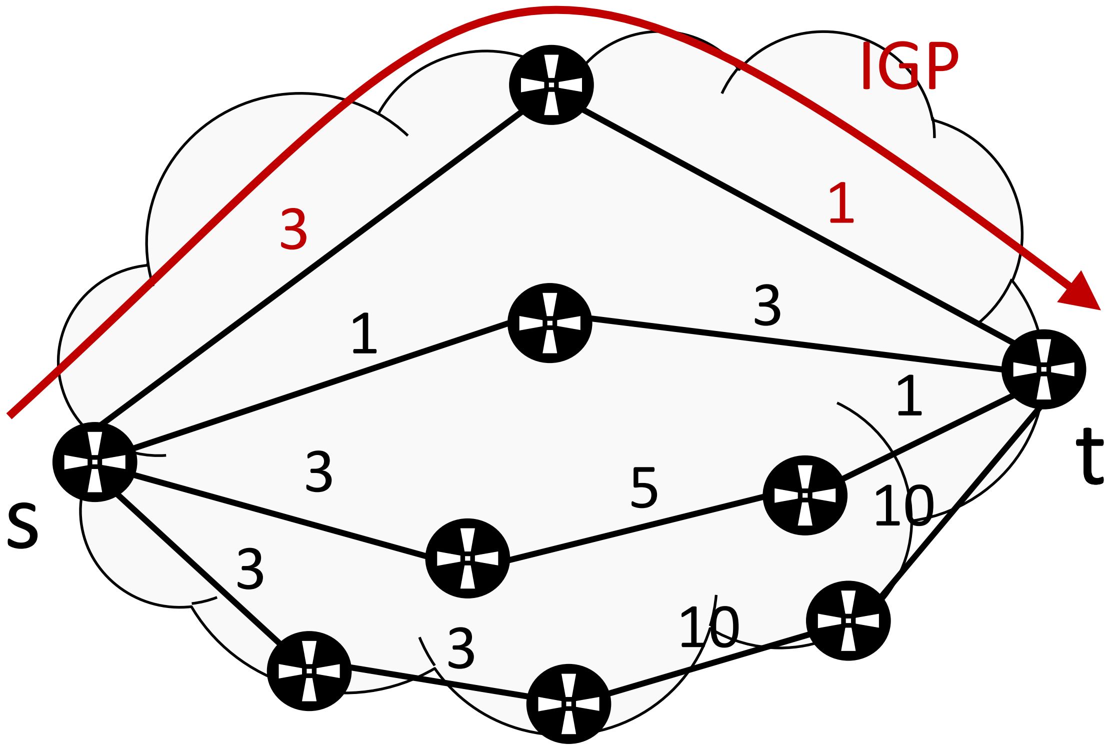
Detours likely have a negative impact on performance

Detecting detours can sometimes help explain the presence of lies

The art of detecting forwarding detours

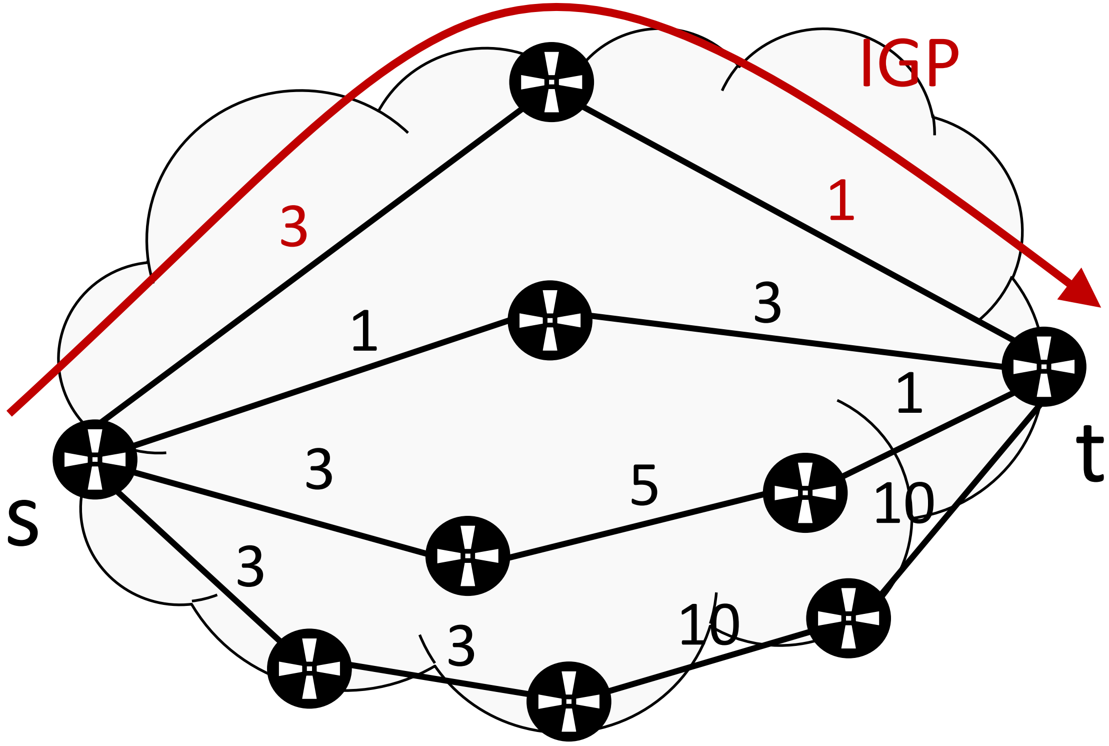
Inside an AS

- In the IGP, links have a cost according to some metric
- The path with minimum cost is used



Inside an AS

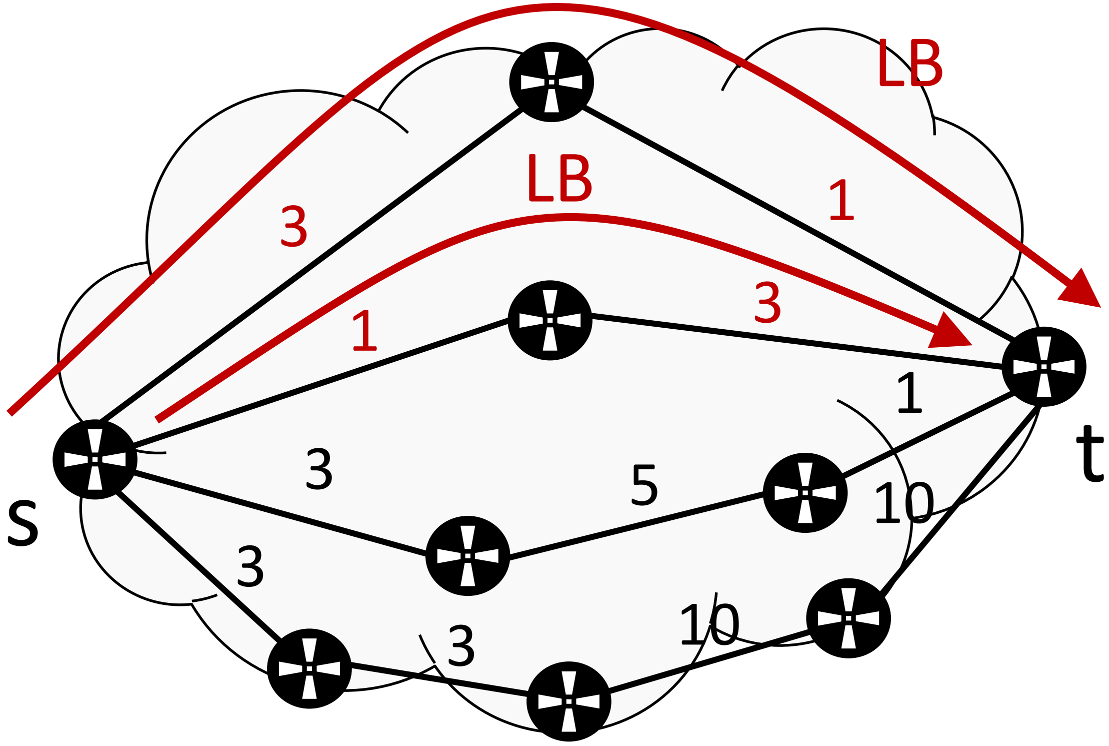
- In the IGP, links have a cost according to some metric
- The path with minimum cost is used



IGP		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1				
	P_2				
	P_3				
	P_4				
	P_5				
	P_6				
	P_7				
	P_8				

Load Balancing (LB)

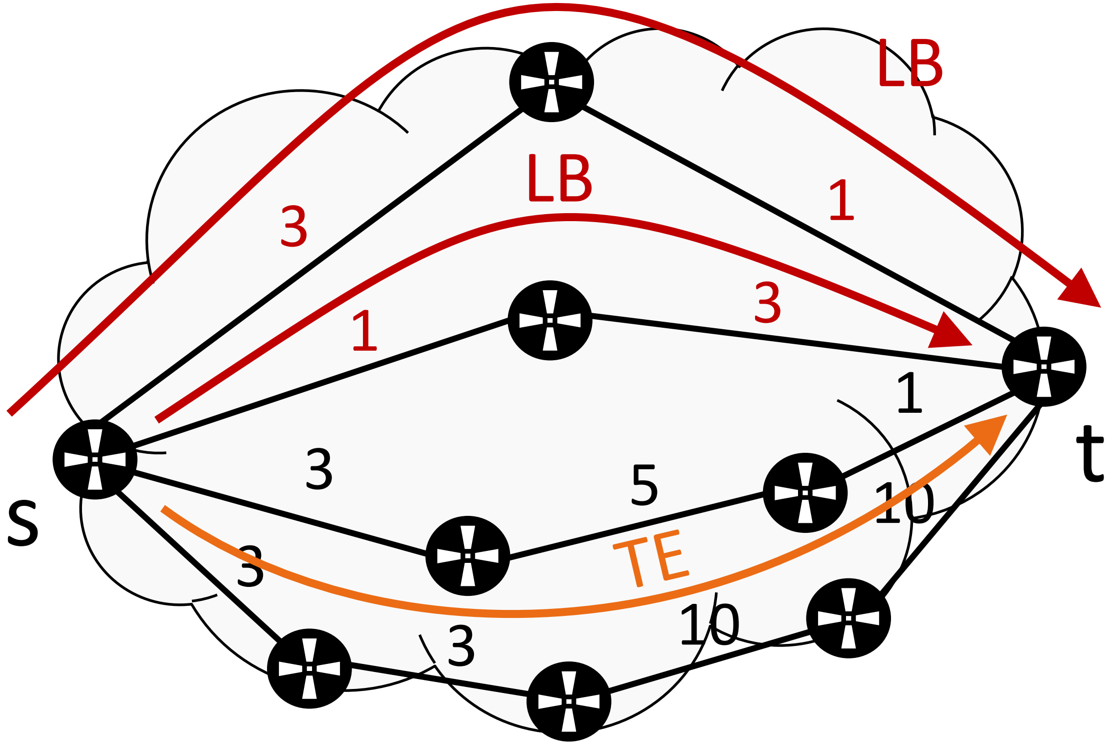
- From one to many best IGP paths
- Usually deployed with equal-cost multipath (ECMP)

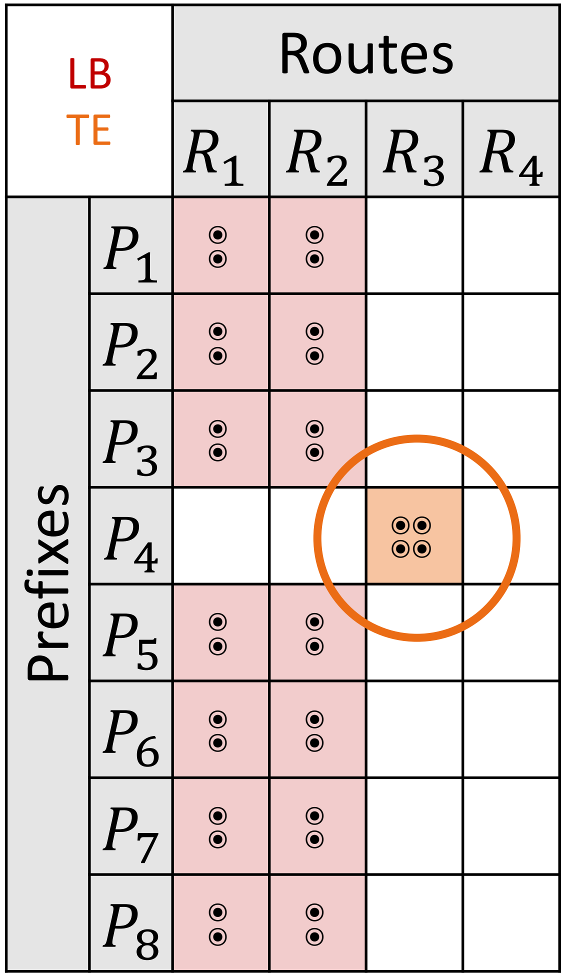


LB		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1				
	P_2				
	P_3				
	P_4				
	P_5				
	P_6				
	P_7				
	P_8				

Traffic Engineering (TE)

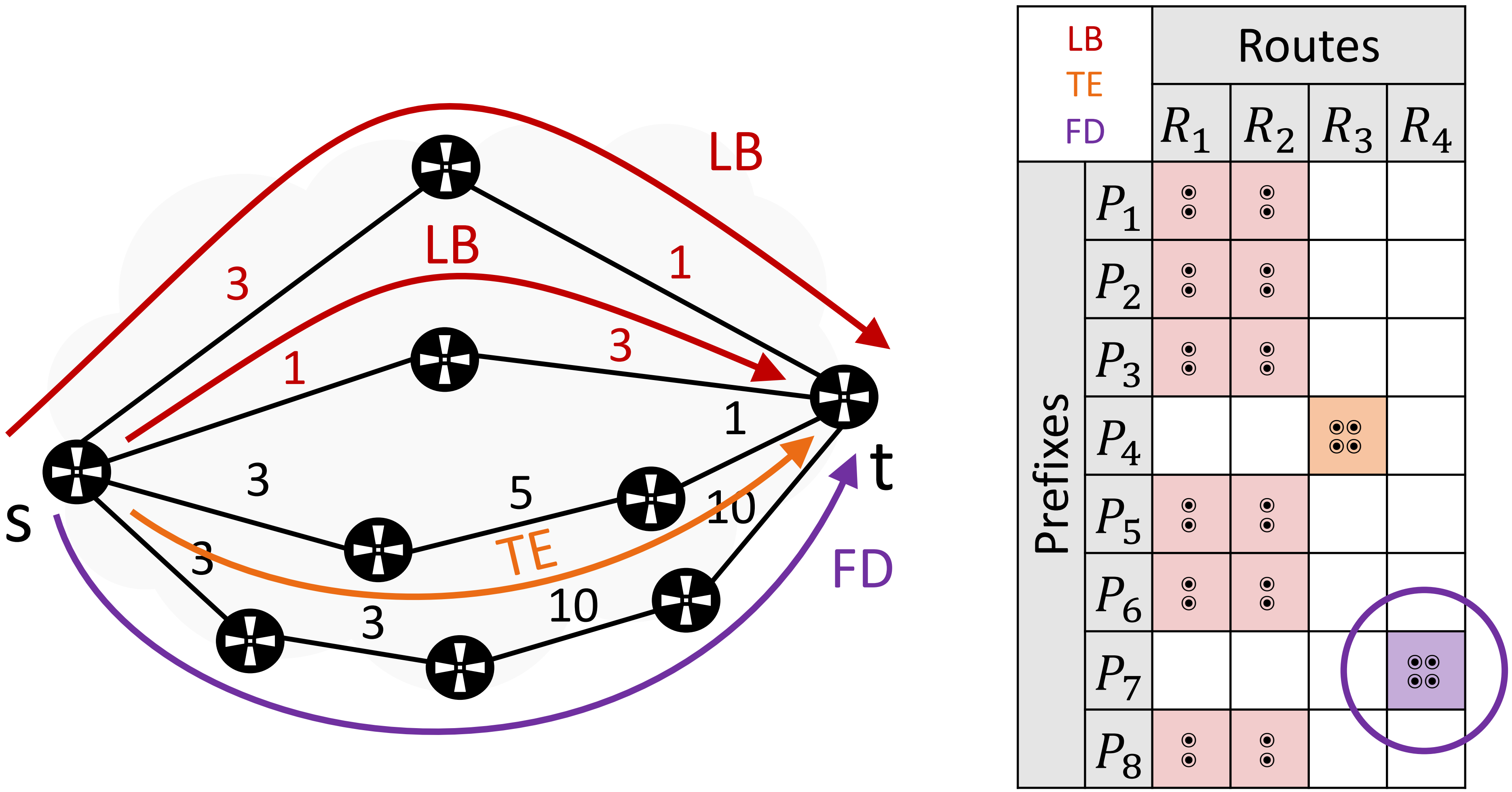
- Allows to craft paths “by hand”
- The crafted paths meet some requirements, e.g. low delay





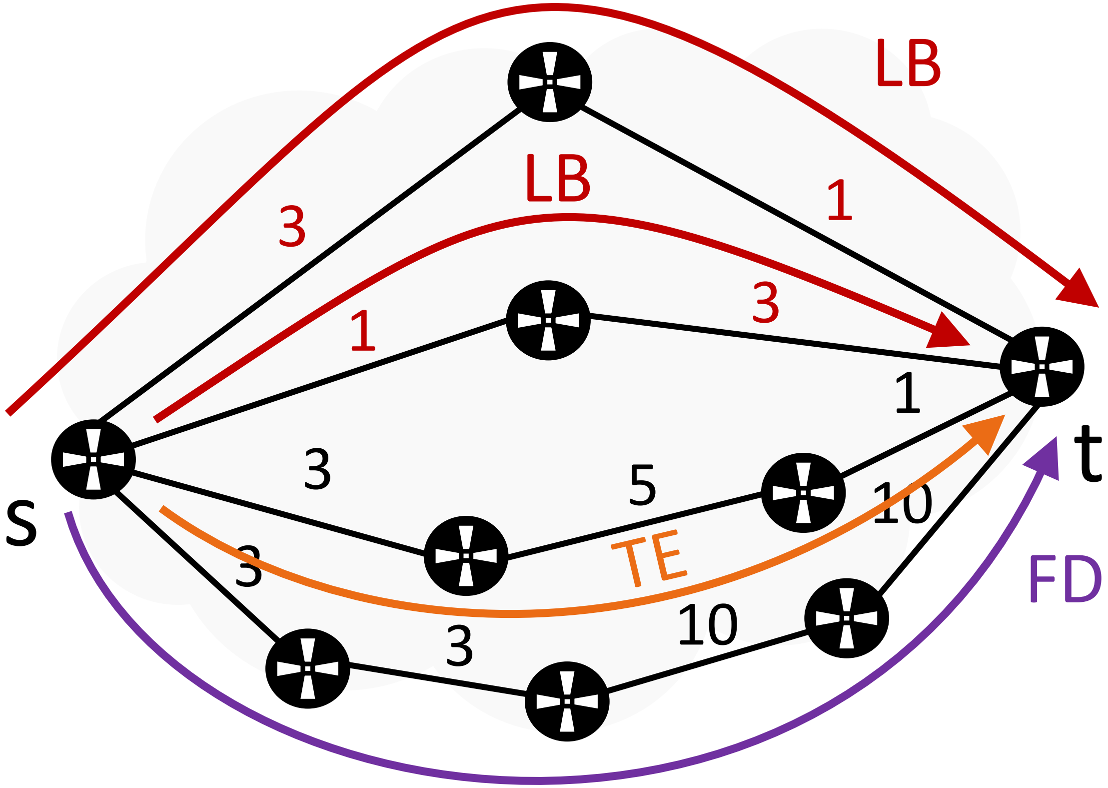
Forwarding Detours (FDs)

- When the forwarding route diverges from LB and TE paths



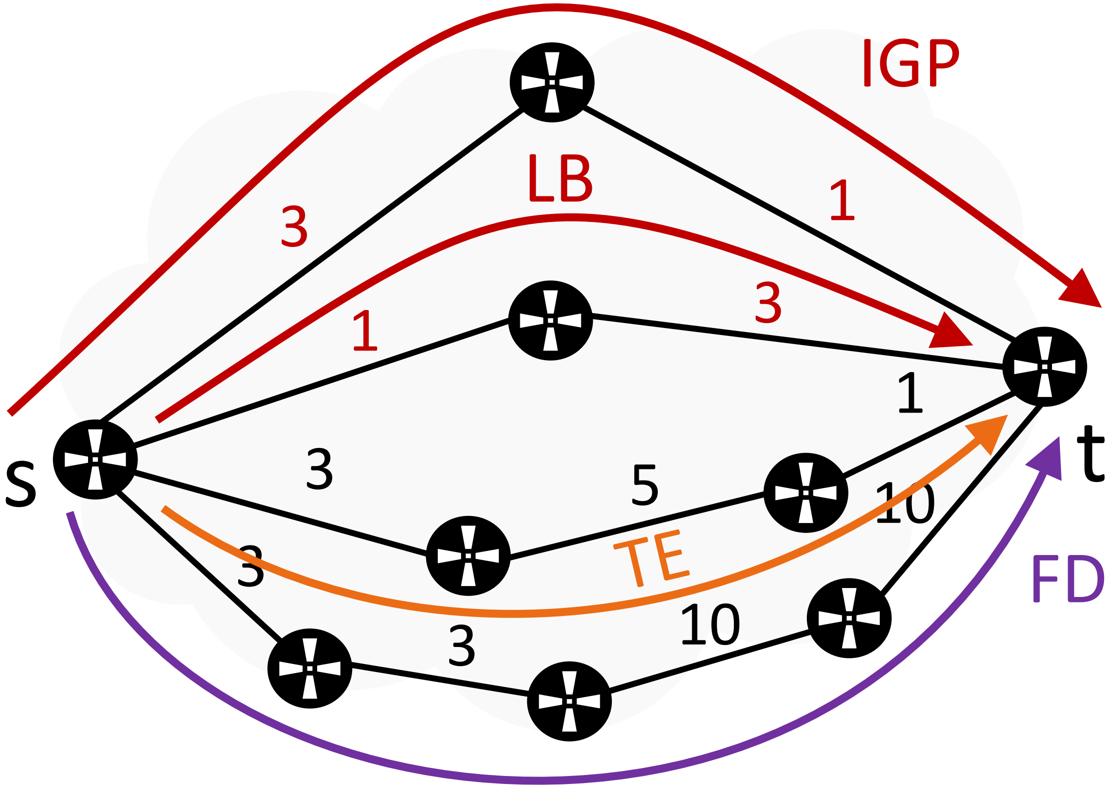
Why detecting Forwarding Detours?

- FDs relate to unexpected paths being used
- Possible negative impact on performance



Methodology to detect FDs

Forwarding Pattern - Run measurements and find the matrix



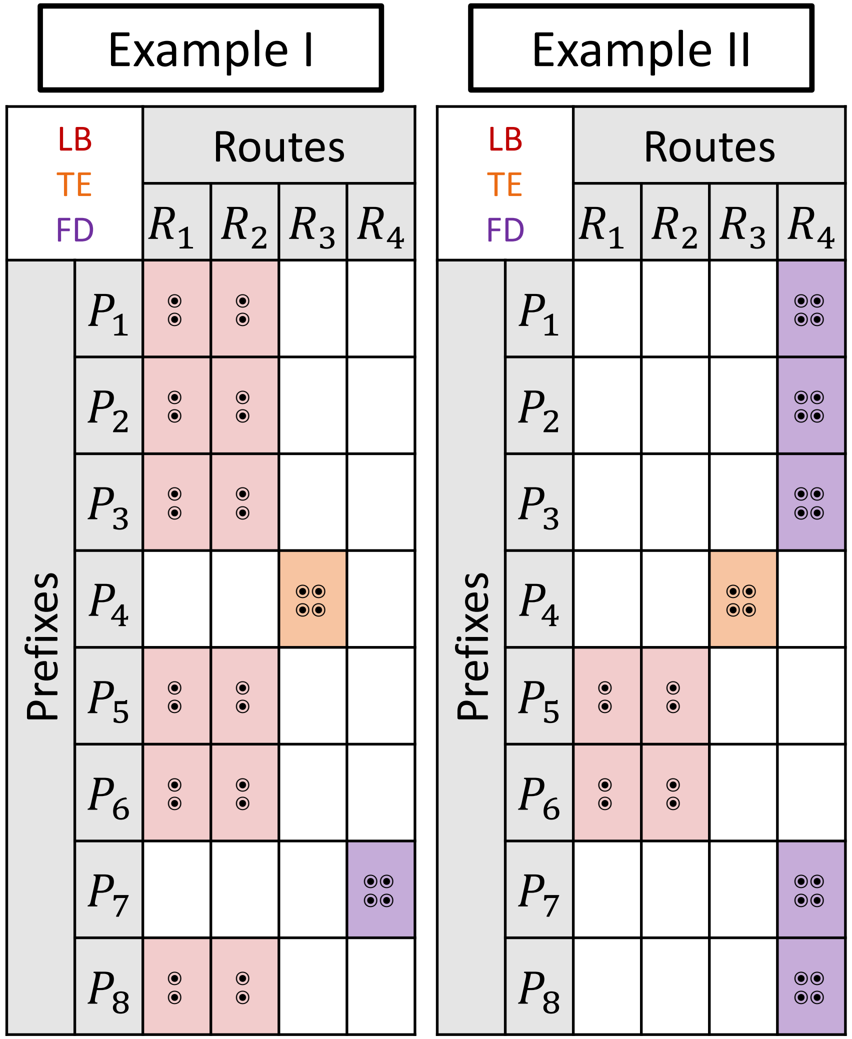
Example I

LB TE FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1	⦿ ⦿	⦿ ⦿		
	P_2	⦿ ⦿	⦿ ⦿		
	P_3	⦿ ⦿	⦿ ⦿		
	P_4			⦿⦿ ⦿⦿	
	P_5	⦿ ⦿	⦿ ⦿		
	P_6	⦿ ⦿	⦿ ⦿		
	P_7				⦿⦿ ⦿⦿
	P_8	⦿ ⦿	⦿ ⦿		

Example II

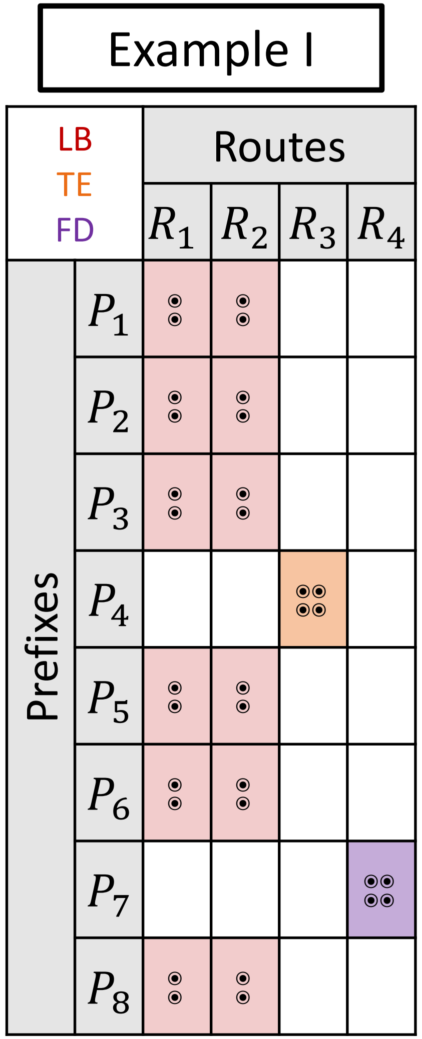
LB TE FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1				⦿⦿ ⦿⦿
	P_2				⦿⦿ ⦿⦿
	P_3				⦿⦿ ⦿⦿
	P_4			⦿⦿ ⦿⦿	
	P_5	⦿ ⦿	⦿ ⦿		
	P_6	⦿ ⦿	⦿ ⦿		
	P_7				⦿⦿ ⦿⦿
	P_8				⦿⦿ ⦿⦿

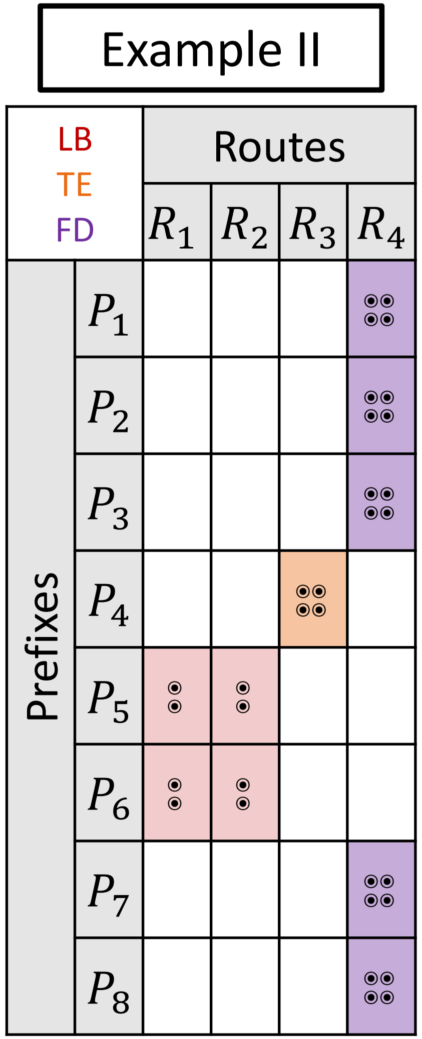
Concluding if FDs occur



Concluding if FDs occur

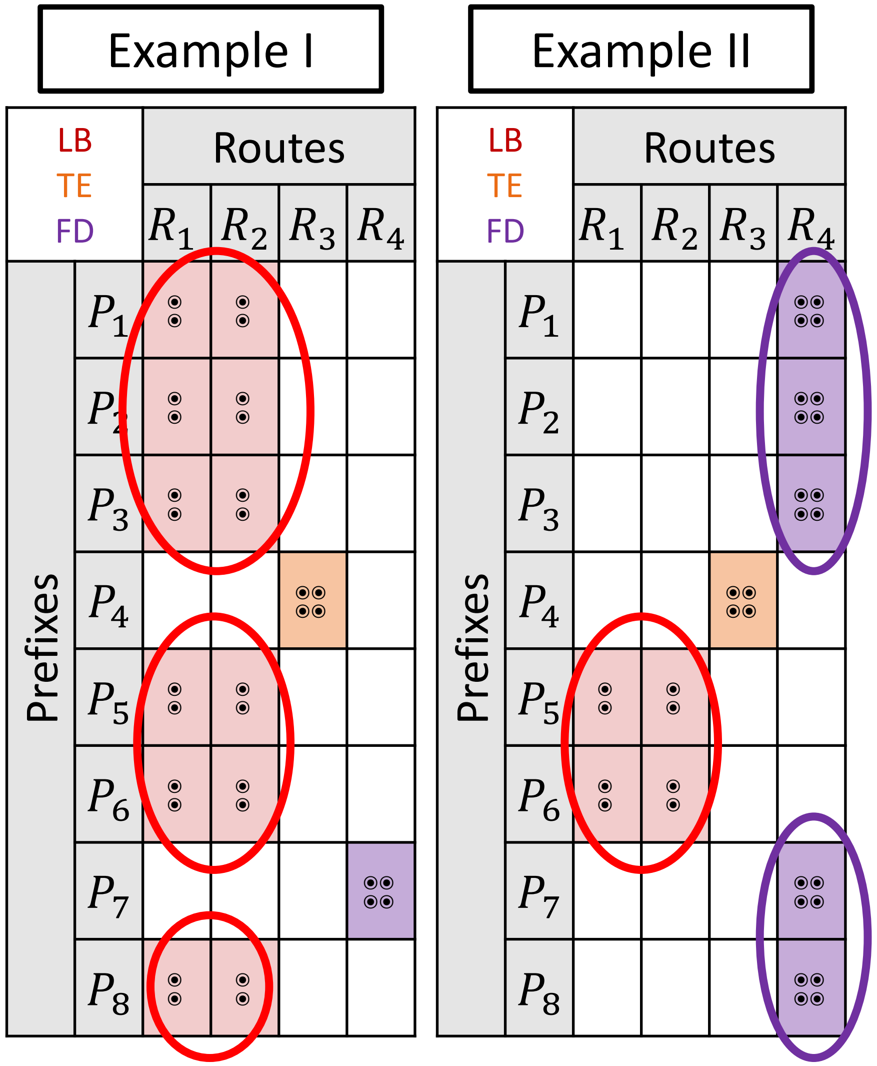
1. Identify prefixes related to the same routes





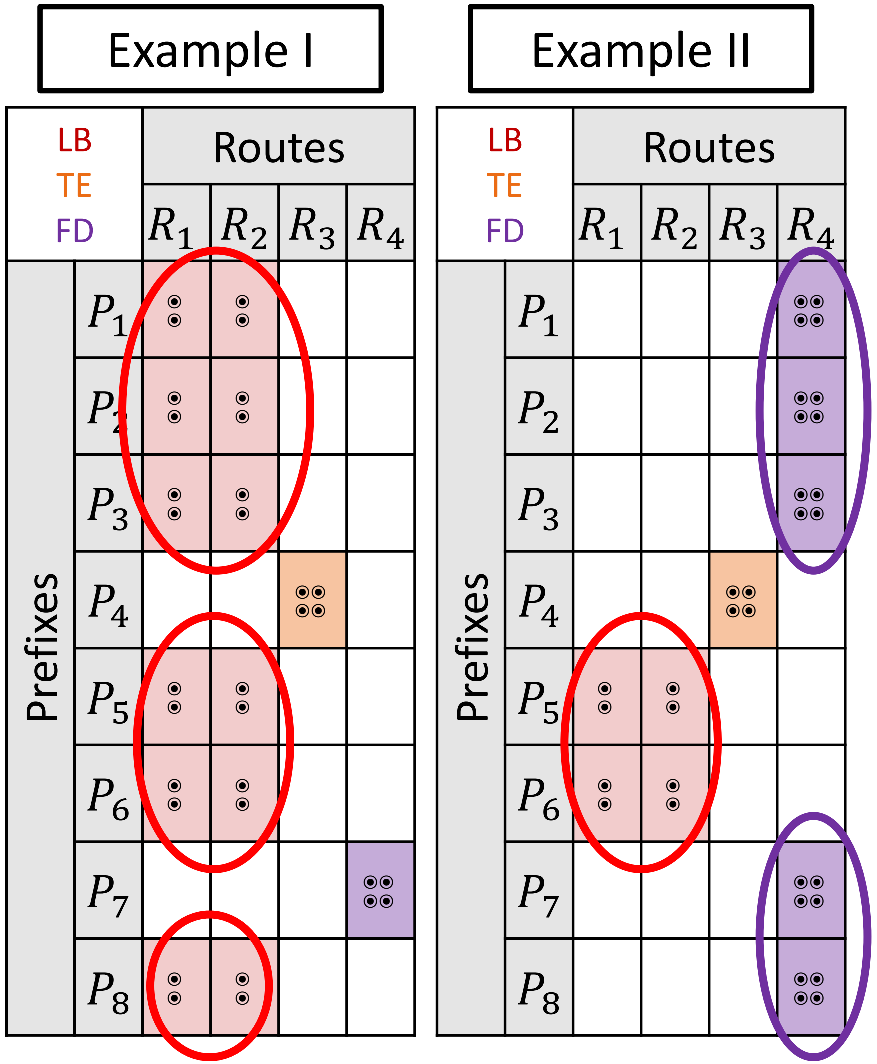
Concluding if FDs occur

1. Identify prefixes related to the same routes



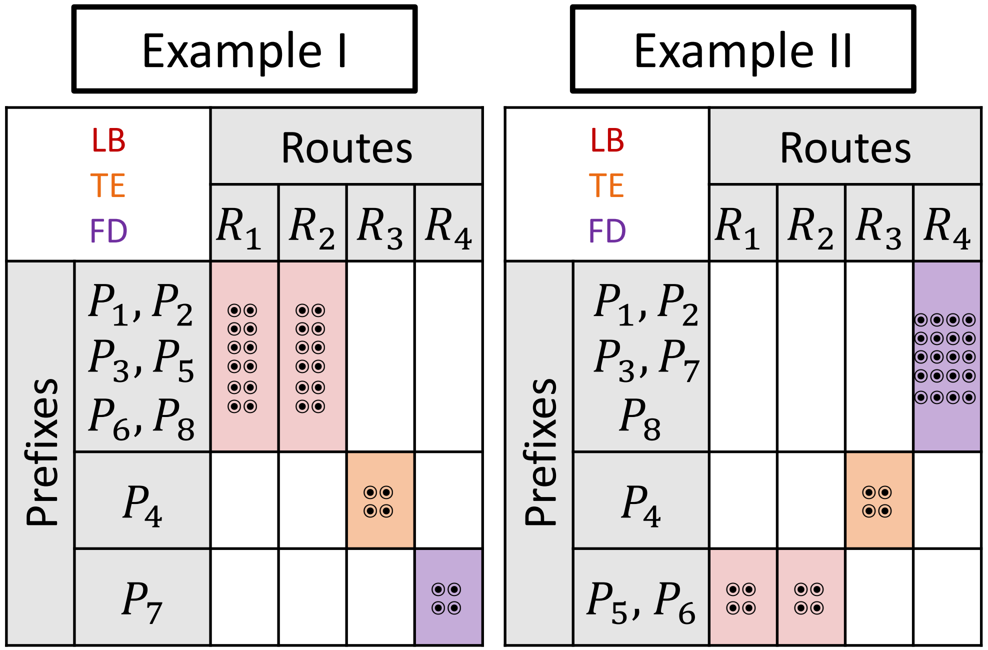
Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets



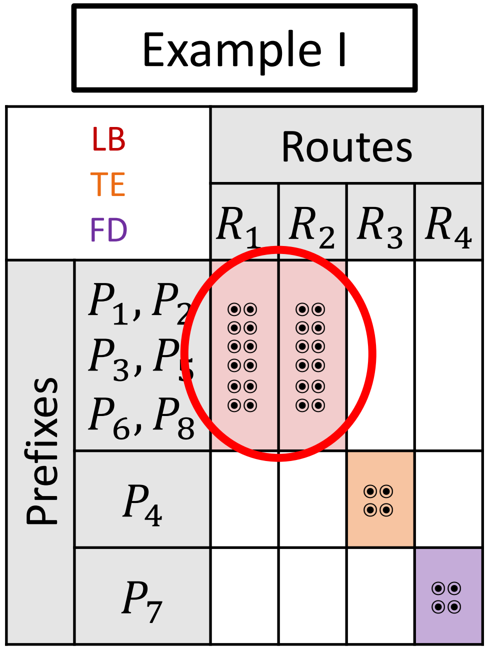
Concluding if FDs occur

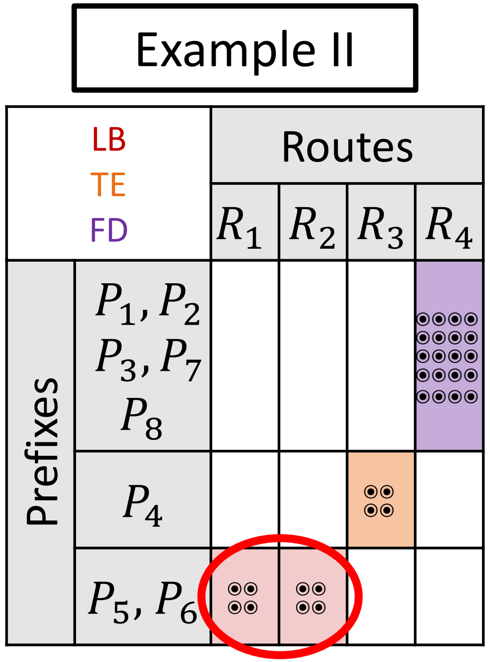
1. Identify prefixes related to the same routes
2. Group the related prefixes in sets



Concluding if FDs occur

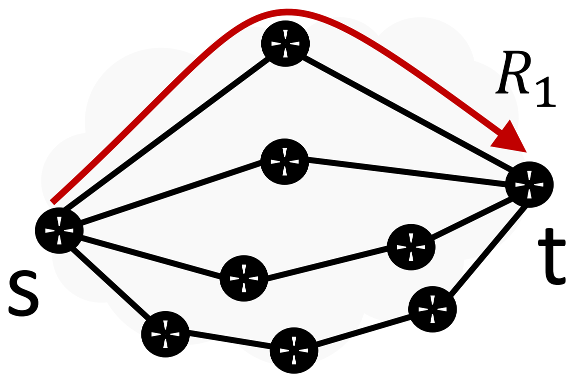
1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t

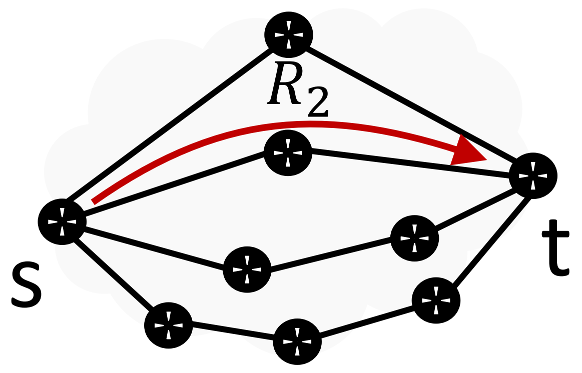




Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t





Example I

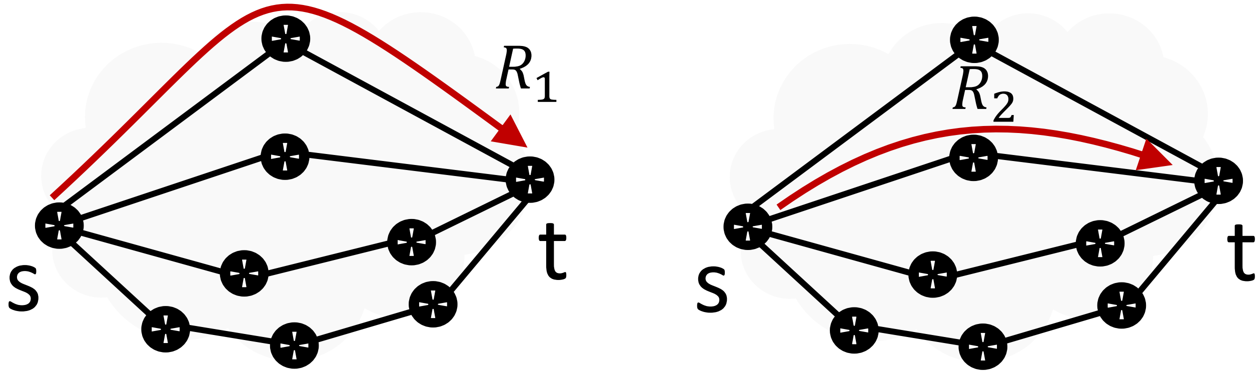
LB TE FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2, P_3, P_5, P_6, P_8				
	P_4				
	P_7				

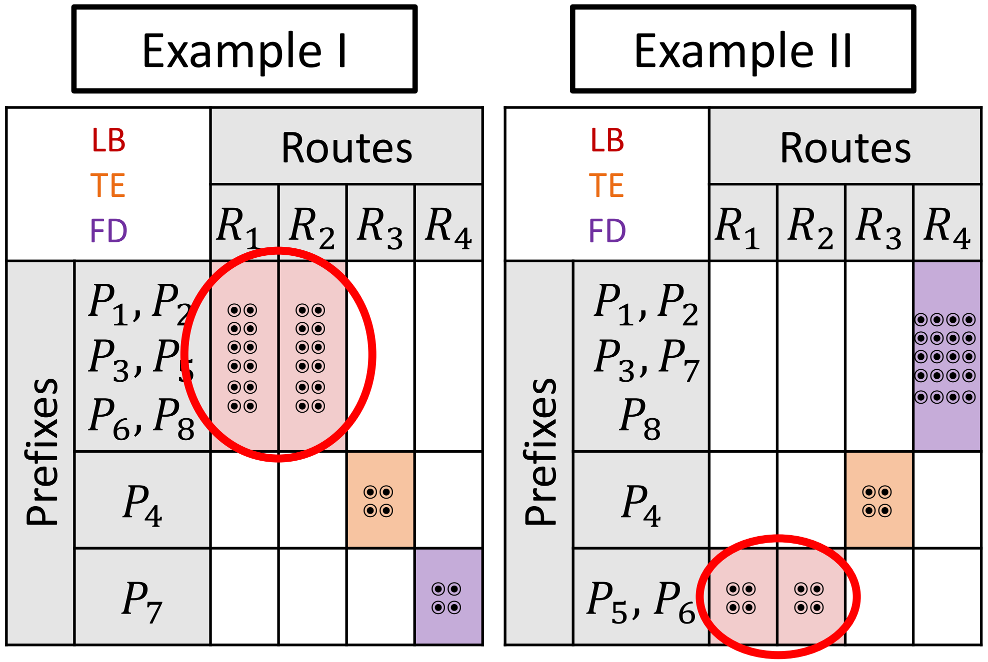
Example II

LB TE FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2, P_3, P_7, P_8				
	P_4				
	P_5, P_6				

Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t

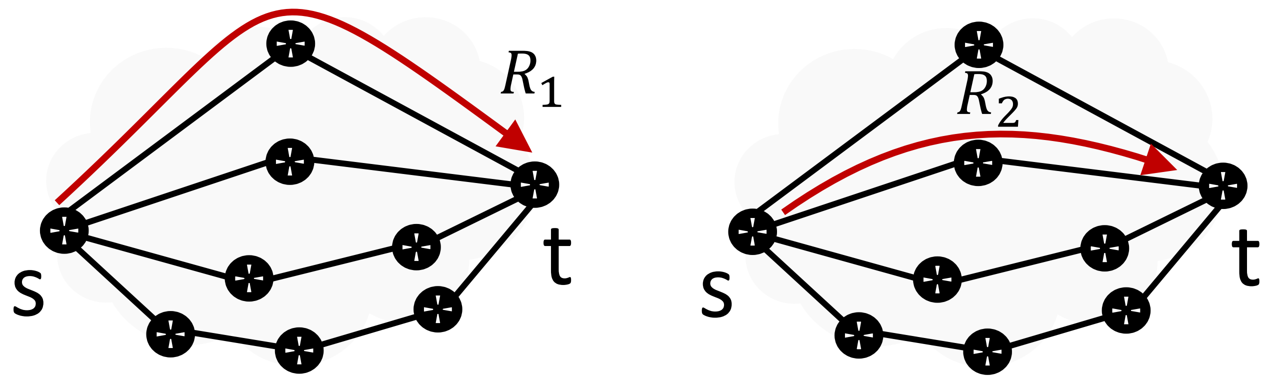


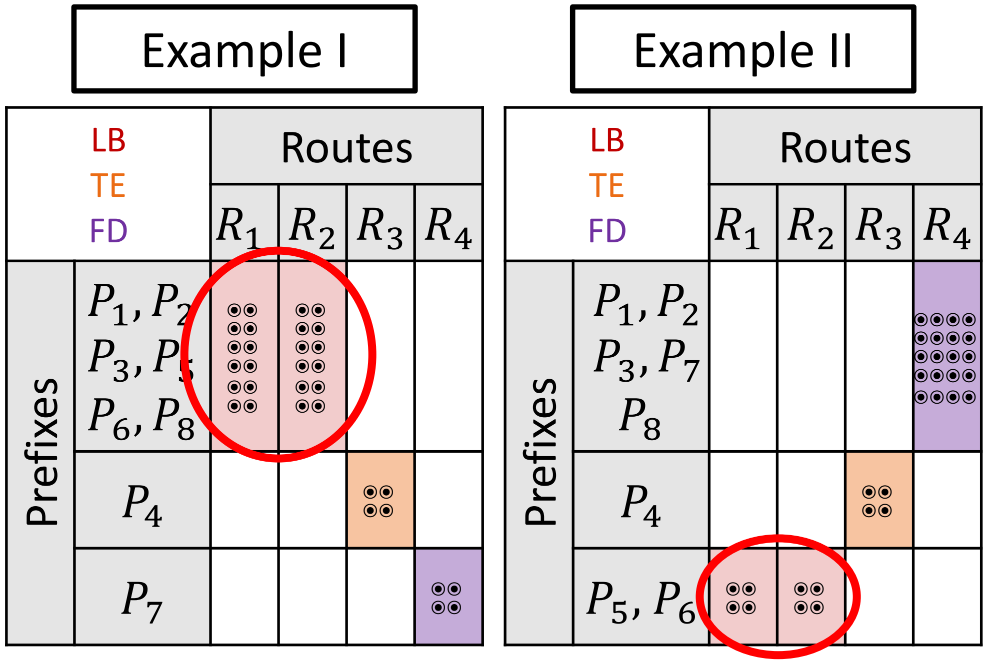


4. Compute #pfxs in each set: (6, 1, 1) and (5, 1, 2)

Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t

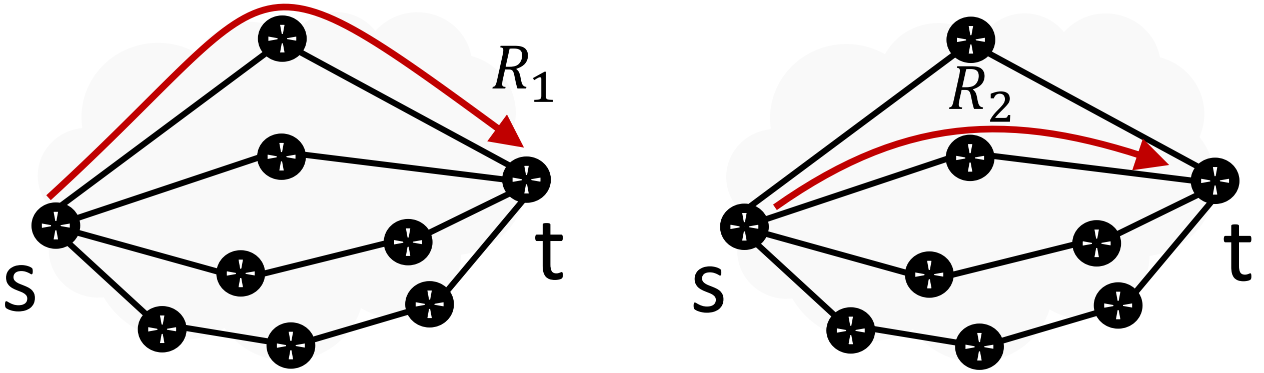


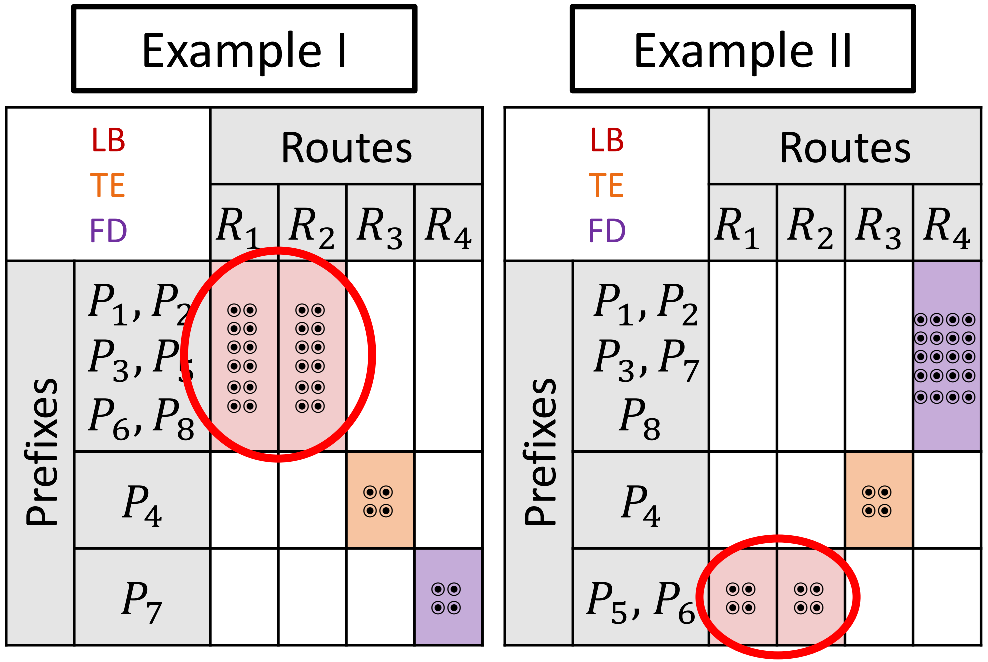


4. Compute #pfxs in each set: (6, 1, 1) and (5, 1, 2)
5. Turn it into proportions: (0.75, 0.125, 0.125) and (0.625, 0.125, 0.25)

Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t

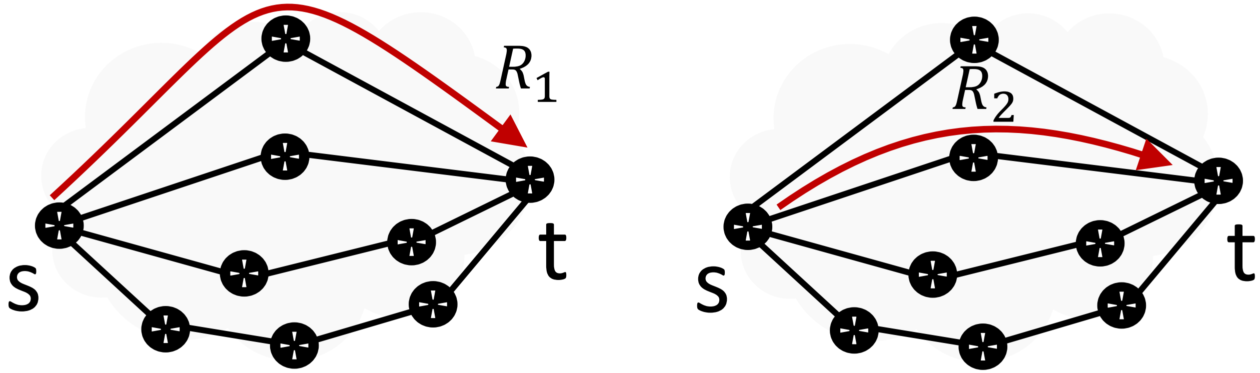


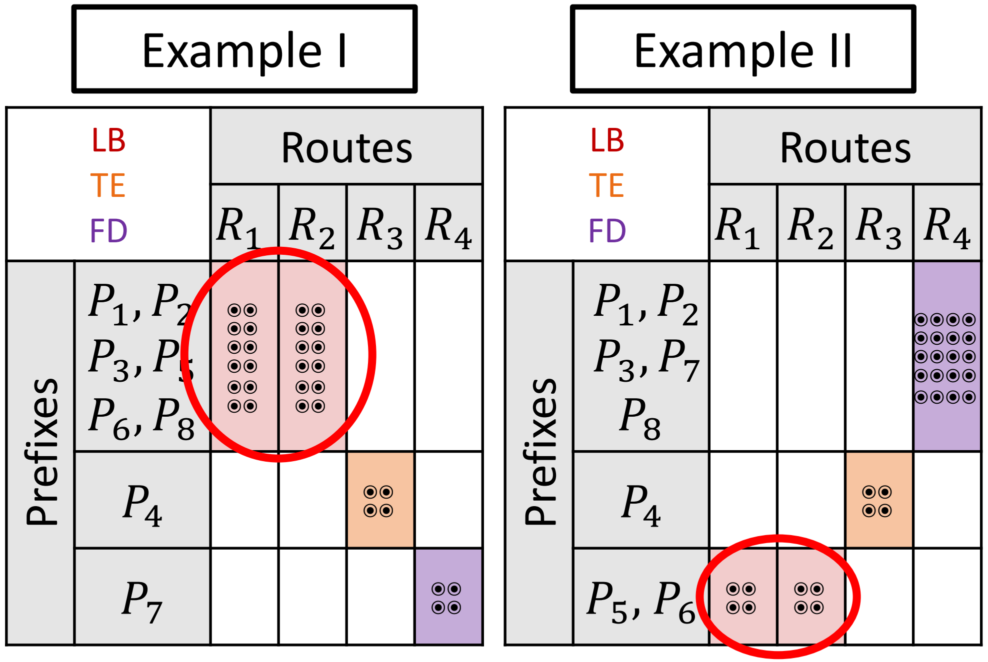


4. Compute #pfxs in each set: (6, 1, 1) and (5, 1, 2)
5. Turn it into proportions: (0.75, 0.125, 0.125) and (0.625, 0.125, 0.25)
6. Compute the n number of sets ... in this case $n = 3$ for both examples...

Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t

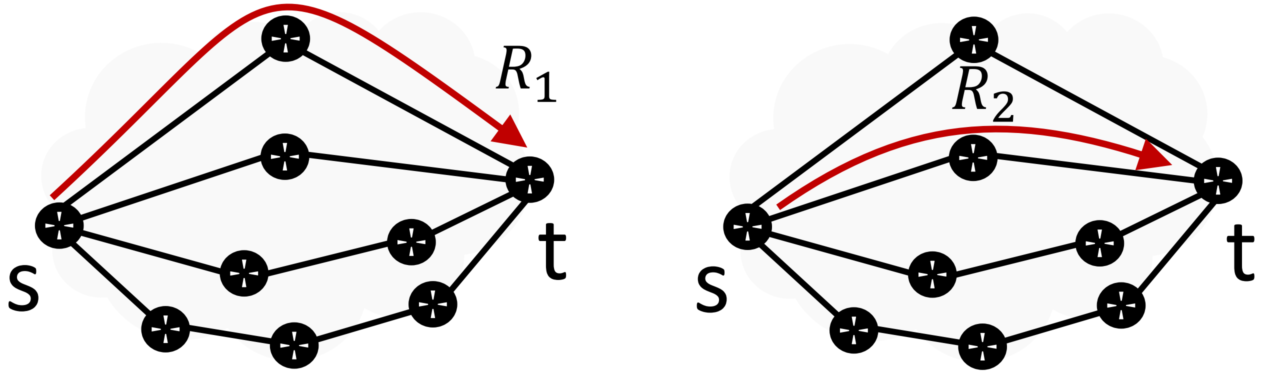


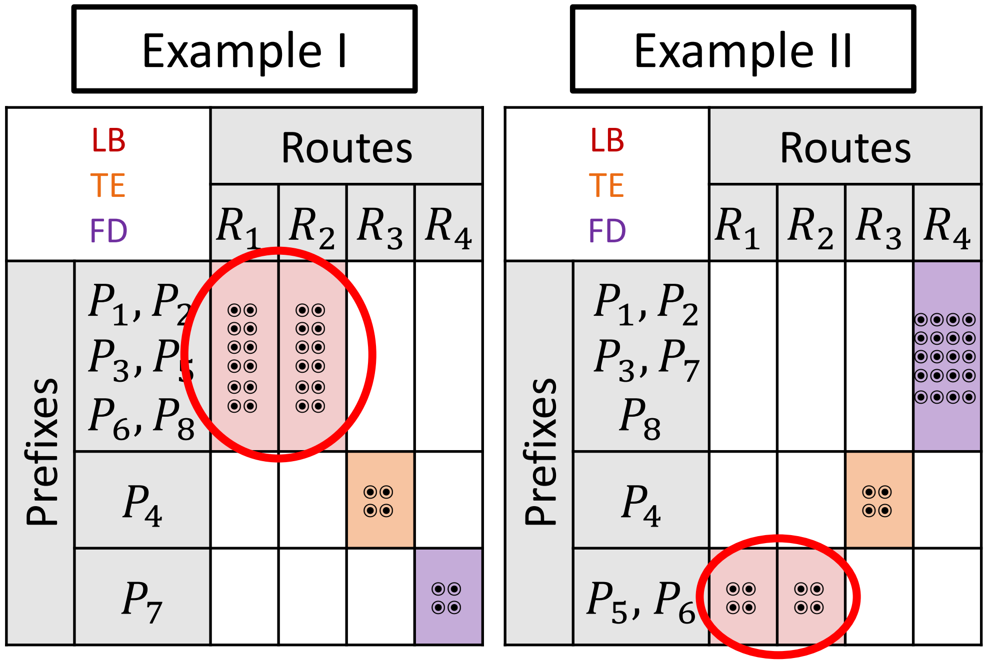


4. Compute #pfxs in each set: (6, 1, 1) and (5, 1, 2)
5. Turn it into proportions: (0.75, 0.125, 0.125) and (0.625, 0.125, 0.25)
6. Compute the n number of sets ... in this case $n = 3$ for both examples...
7. Conclude that FDs occur if LB is associated to less than $\frac{1}{n} = 0.33$ pfxs...

Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t



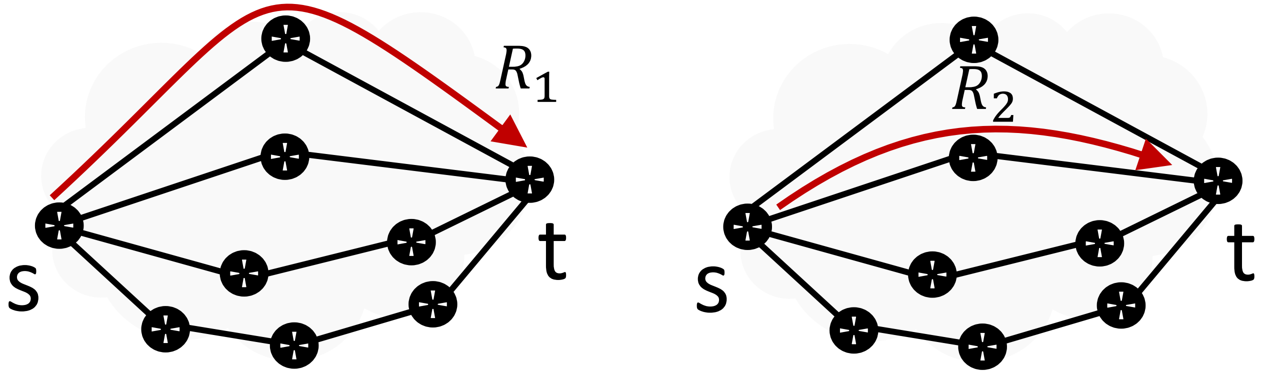


4. Compute #pfxs in each set: (6, 1, 1) and (5, 1, 2)
5. Turn it into proportions: (0.75, 0.125, 0.125) and (0.625, 0.125, 0.25)
6. Compute the n number of sets ... in this case $n = 3$ for both examples...
7. Conclude that FDs occur if LB is associated to less than $\frac{1}{n} = 0.33$ pfxs...

0.33 < 0.75 ... no FDs and 0.33 > 0.25 ... there are FDs

Concluding if FDs occur

1. Identify prefixes related to the same routes
2. Group the related prefixes in sets
3. Identify the LB set targeting router t



Example I

	LB TE FD	Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2 P_3, P_5 P_6, P_8				
	P_4				
	P_7				

Example II

	LB TE FD	Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2 P_3, P_7 P_8				
	P_4				
	P_5, P_6				

...we are conservative!

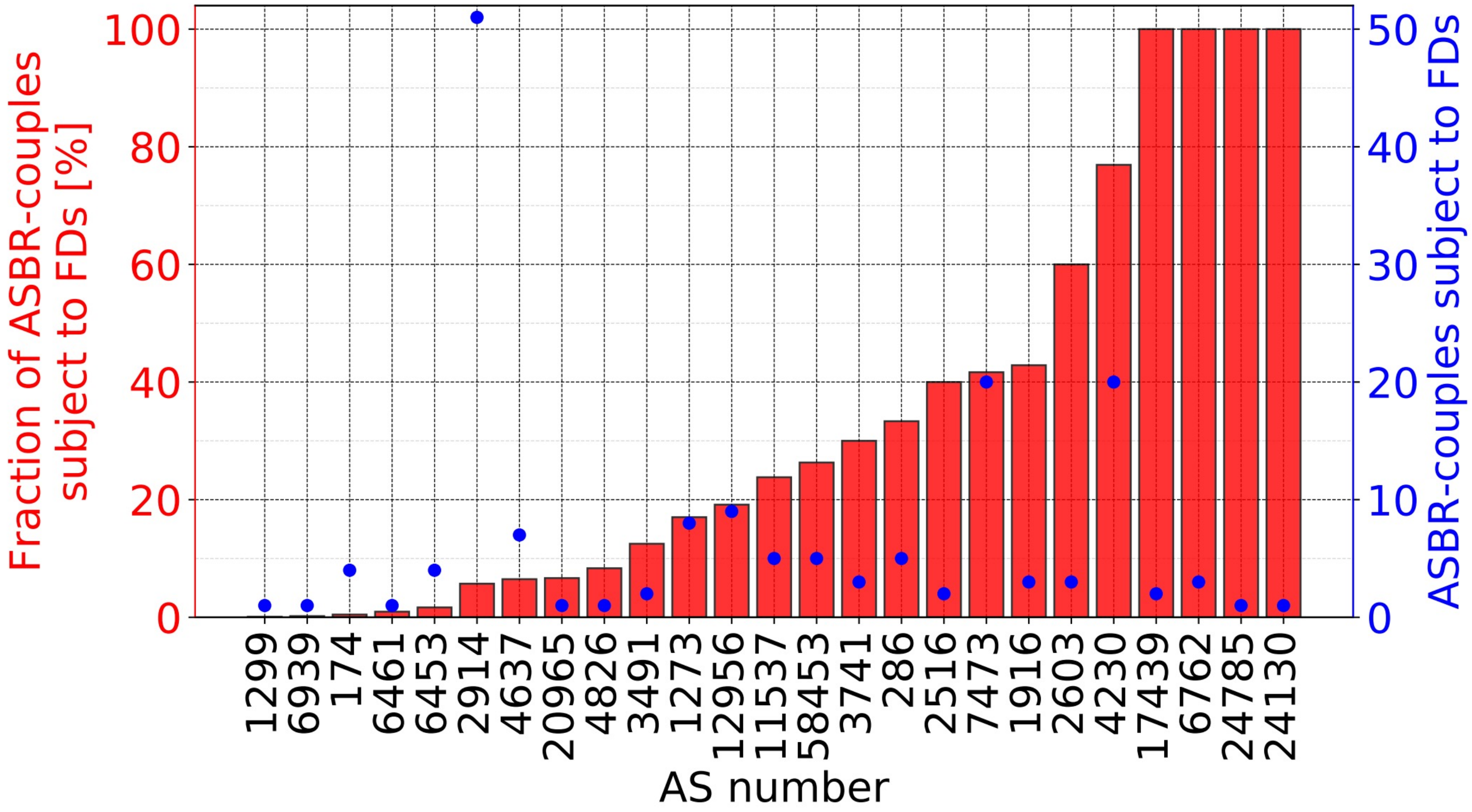
4. Compute #pfxs in each set: (6, 1, 1) and (5, 1, 2)
5. Turn it into proportions: (0.75, 0.125, 0.125) and (0.625, 0.125, 0.25)
6. Compute the n number of sets ... in this case $n = 3$ for both examples...
7. Conclude that FDs occur if LB is associated to less than $\frac{1}{n} = 0.33$ pfxs...

0.33 < 0.75 ... no FDs and 0.33 > 0.25 ... there are FDs

Our experiments

In the wild, FDs are a thing!

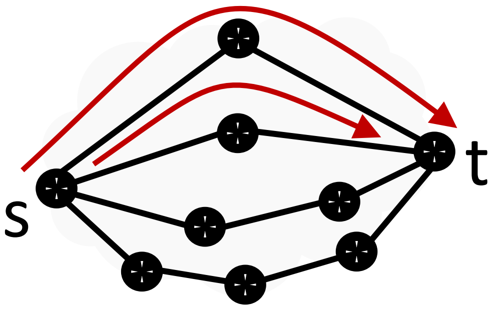
- We measure from 100 VPs
- We look for FDs between AS border routers (ASBRs) and request #pfxs > 100
- We find FDs in 25/54 ASs, with an heterogeneous distribution



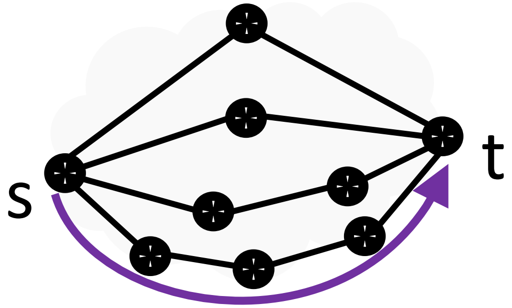
Digging into the results: a binary pattern

- According to the FDs we found, all traffic detours or none does

LB TE FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2 P_3, P_4 P_5, P_6 P_7, P_8				



LB TE FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2 P_3, P_4 P_5, P_6 P_7, P_8				



...in other words...

No cases like this!

LB TE, FD		Routes			
		R_1	R_2	R_3	R_4
Prefixes	P_1, P_2 P_3, P_5 P_6, P_8				
	P_4				
	P_7				

Take away on FDs

- ❖Routing inconsistencies produce FDs (and sometimes lies)
- ❖Our measurements show that FDs exist
- ❖FDs are distributed heterogeneously and have a binary pattern

Conclusion

- Many strange animals are still deployed on purpose or inadvertently
- Our tools have limitations to detect these animals

- Finding the appropriate measurement platform is a challenge

- For these studies, assumptions are made on how devices operate and how operators configure them. Validation of the latter is an open issue