MAP-IT: Multipass Accurate Passive Inferences from Traceroute

Alexander Marder and Jonathan M. Smith
University of Pennsylvania

Funding: DARPA, NSF, & ONR

Problem: Identify Inter-AS Link IP Addresses

- Scalable – no vantage point in AS
- For use with *existing* datasets

MAP-IT Algorithm

1: Create interface-level graph from traceroutes
2: **repeat**
3: Add inter-AS link inferences
4: Refine graph
5: **until** there are no more changes left to make
6: Infer links to stub ASes with single address

MAP-IT Algorithm

1: **Create interface-level graph from traceroutes**
2: **repeat**
3: Add inter-AS link inferences
4: Refine graph
5: **until** there are no more changes left to make
6: Infer links to stub ASes with single address

Interface-Level Graph

Trace 1:

109.105.98.10

198.71.45.2

198.71.46.172

216.249.136.198

Trace 2:

109.105.98.10

198.71.46.180

205.233.255.36

Trace 3:

198.71.45.236

198.71.46.180

216.249.136.198

Trace 4:

198.71.45.236

198.71.45.2

198.71.46.172

205.233.255.36

Interface-Level Graph

Trace 1:

109.105.98.10

198.71.45.2

198.71.46.172

216.249.136.198

Trace 2:

109.105.98.10

198.71.46.180

205.233.255.36

Trace 3:

198.71.45.236

198.71.46.180

216.249.136.198

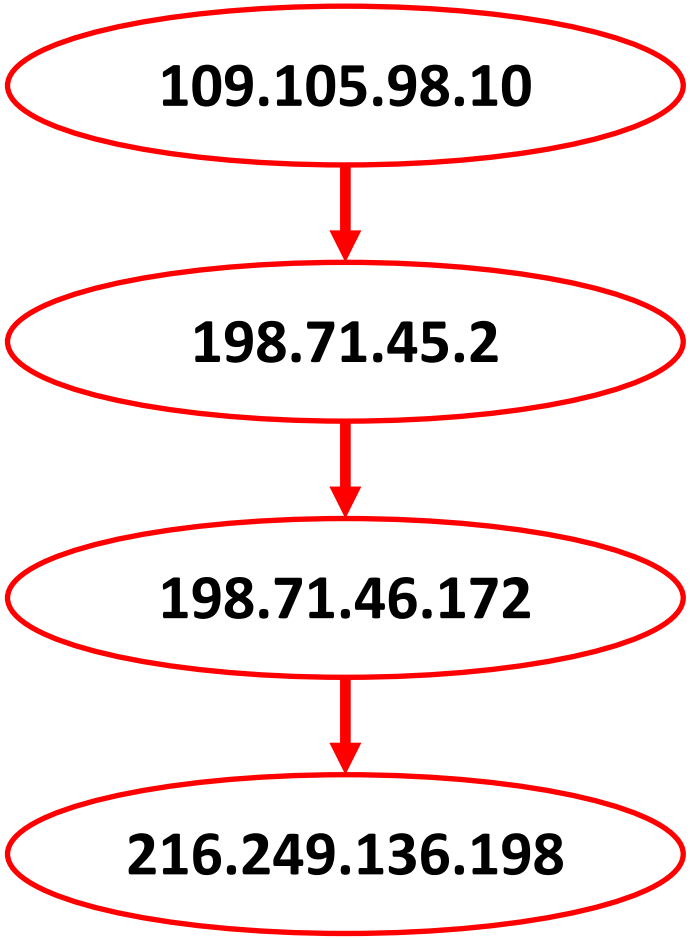
Trace 4:

198.71.45.236

198.71.45.2

198.71.46.172

205.233.255.36



Interface-Level Graph

Trace 1:

109.105.98.10

198.71.45.2

198.71.46.172

216.249.136.198

Trace 2:

109.105.98.10

198.71.46.180

205.233.255.36

Trace 3:

198.71.45.236

198.71.46.180

216.249.136.198

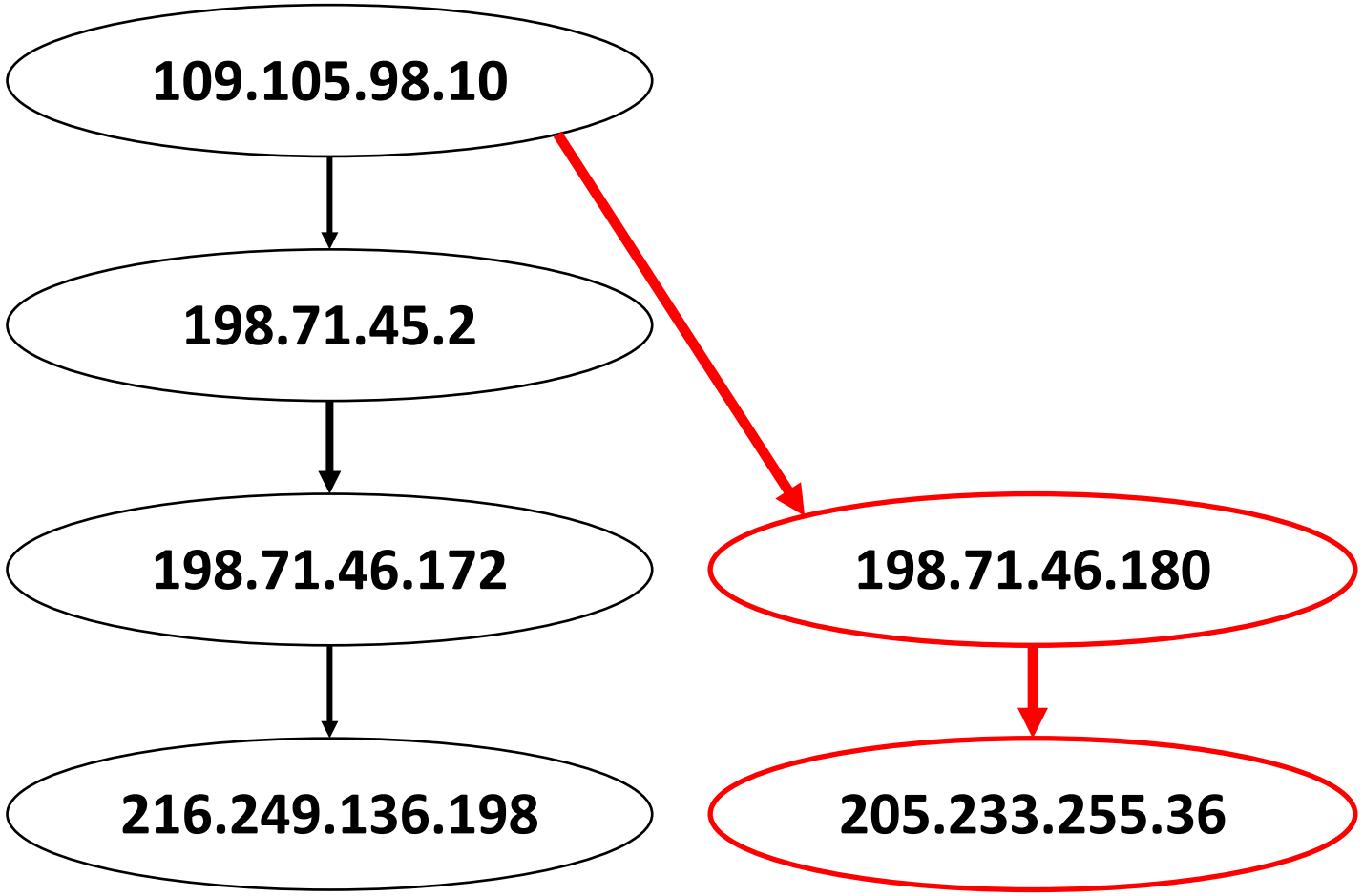
Trace 4:

198.71.45.236

198.71.45.2

198.71.46.172

205.233.255.36



Interface-Level Graph

Trace 1:

109.105.98.10

198.71.45.2

198.71.46.172

216.249.136.198

Trace 2:

109.105.98.10

198.71.46.180

205.233.255.36

Trace 3:

198.71.45.236

198.71.46.180

216.249.136.198

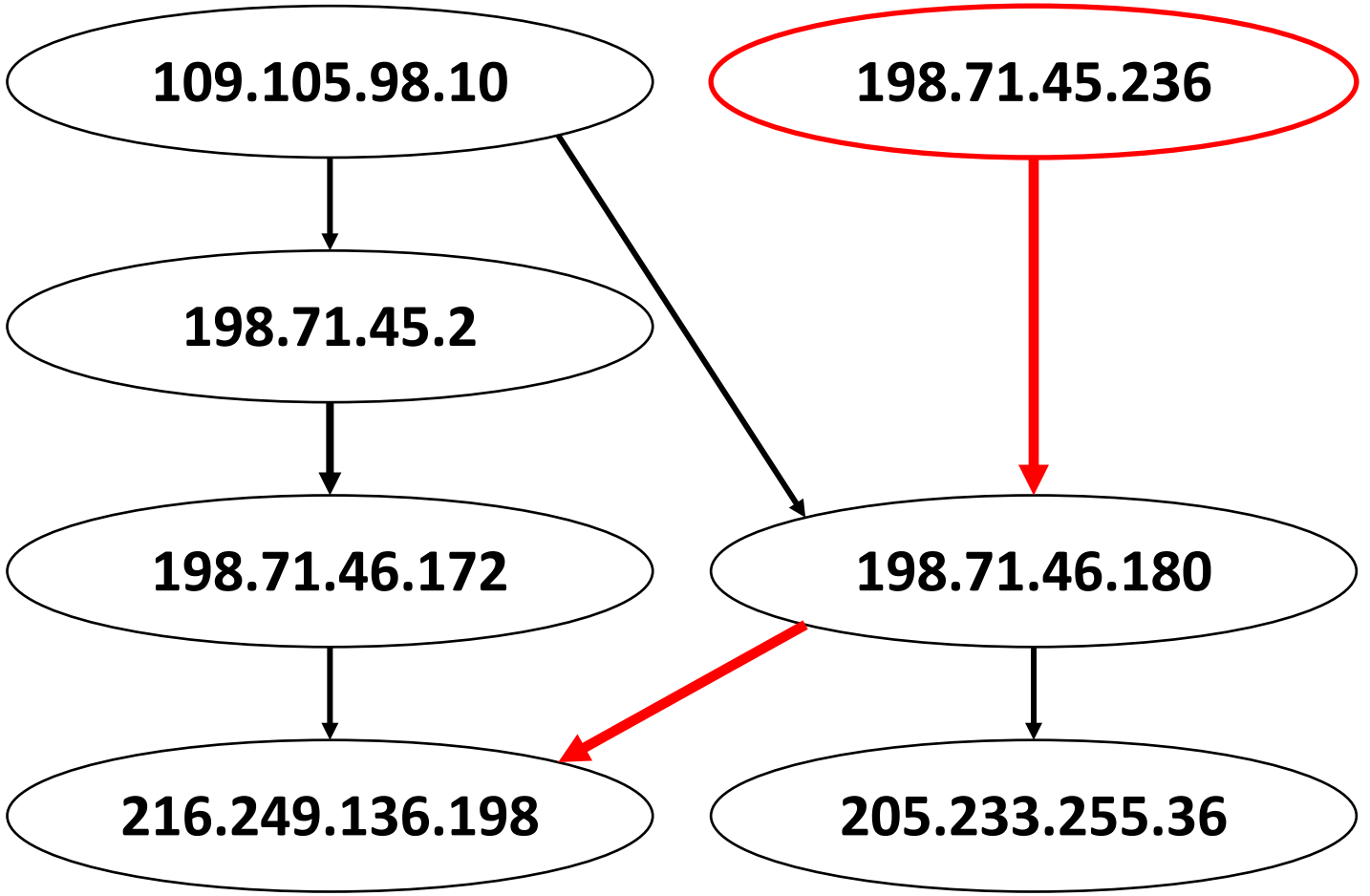
Trace 4:

198.71.45.236

198.71.45.2

198.71.46.172

205.233.255.36



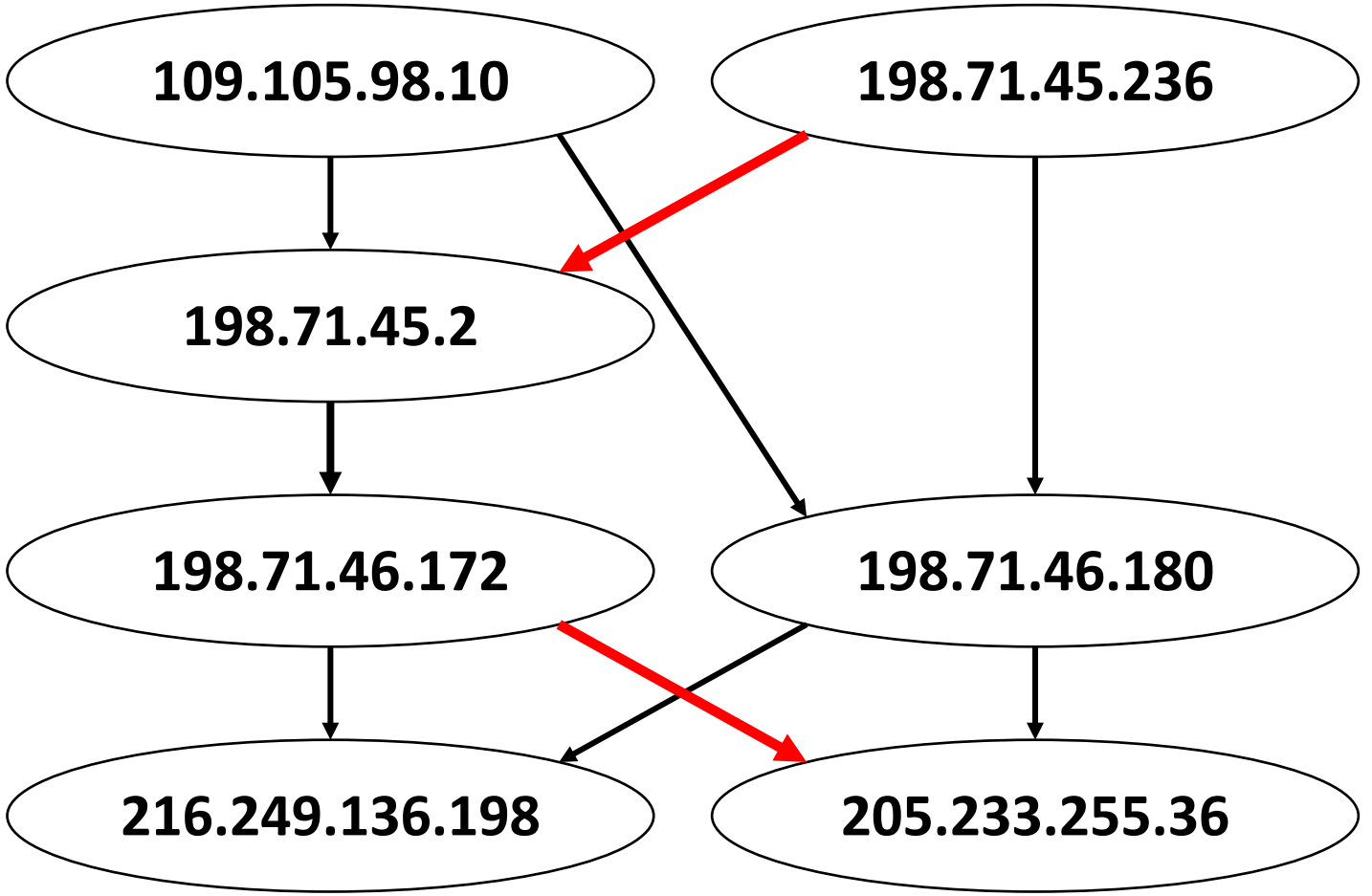
Interface-Level Graph

Trace 1:
109.105.98.10
198.71.45.2
198.71.46.172
216.249.136.198

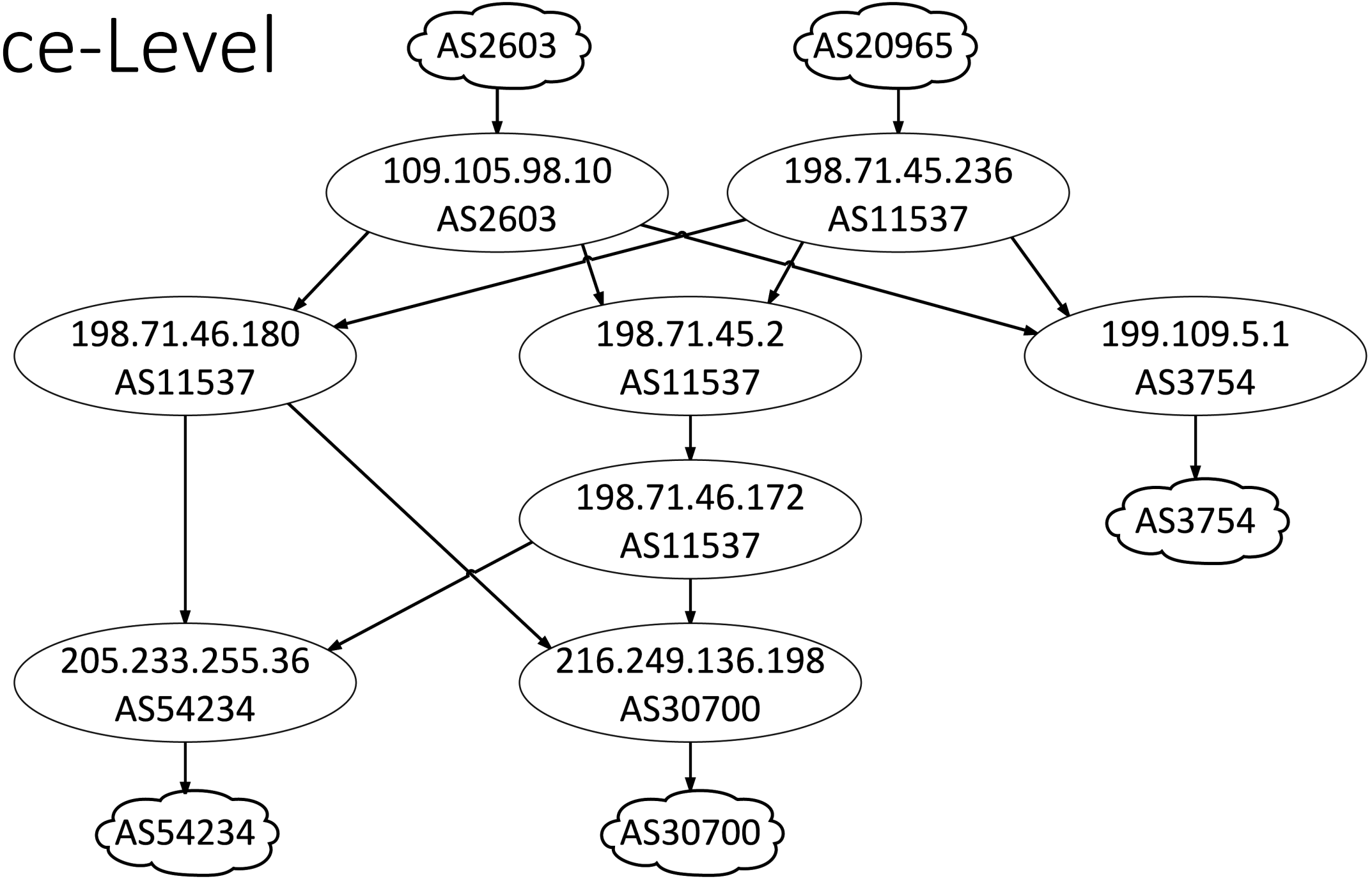
Trace 2:
109.105.98.10
198.71.46.180
205.233.255.36

Trace 3:
198.71.45.236
198.71.46.180
216.249.136.198

Trace 4:
198.71.45.236
198.71.45.2
198.71.46.172
205.233.255.36



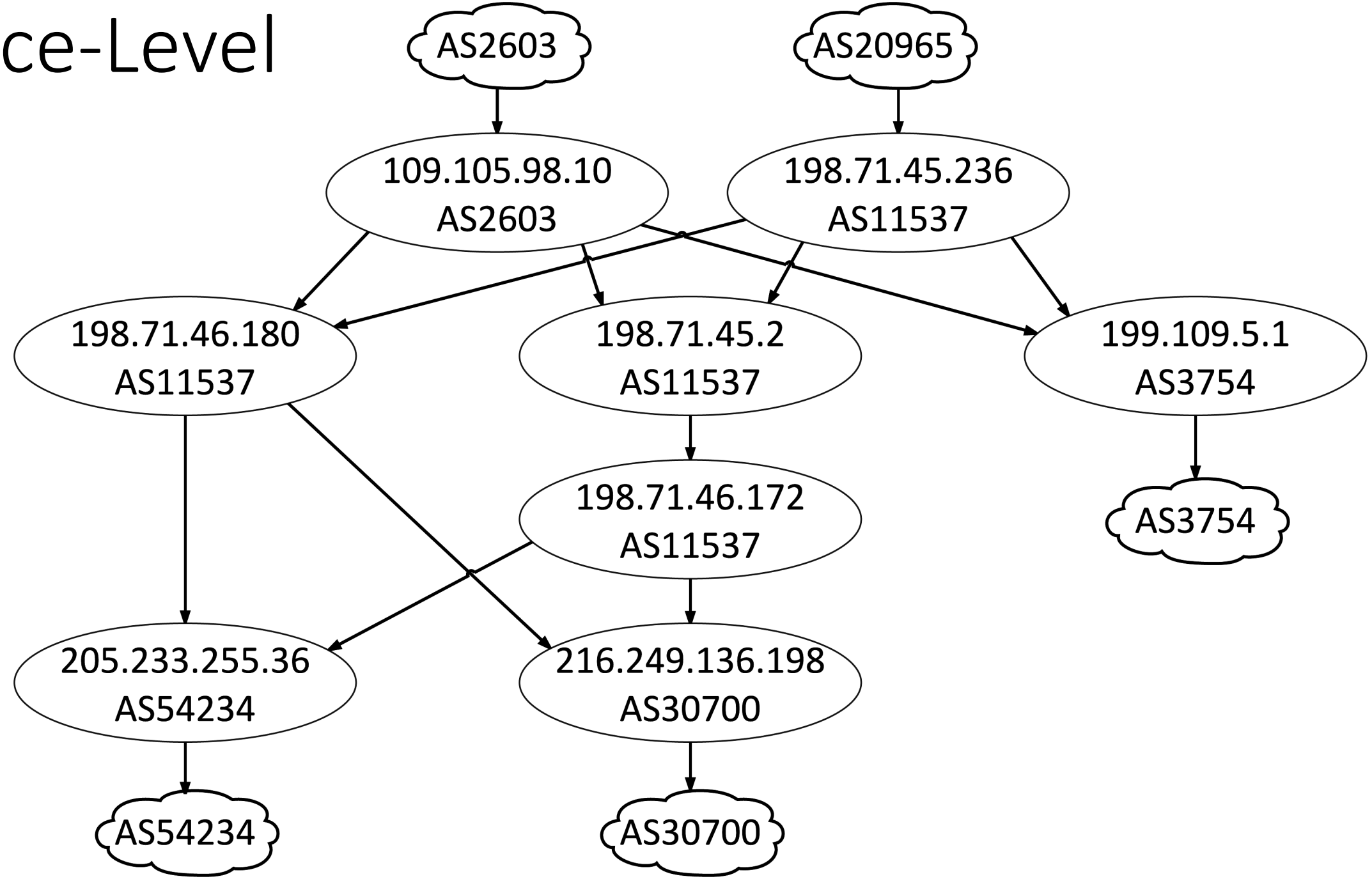
Interface-Level Graph



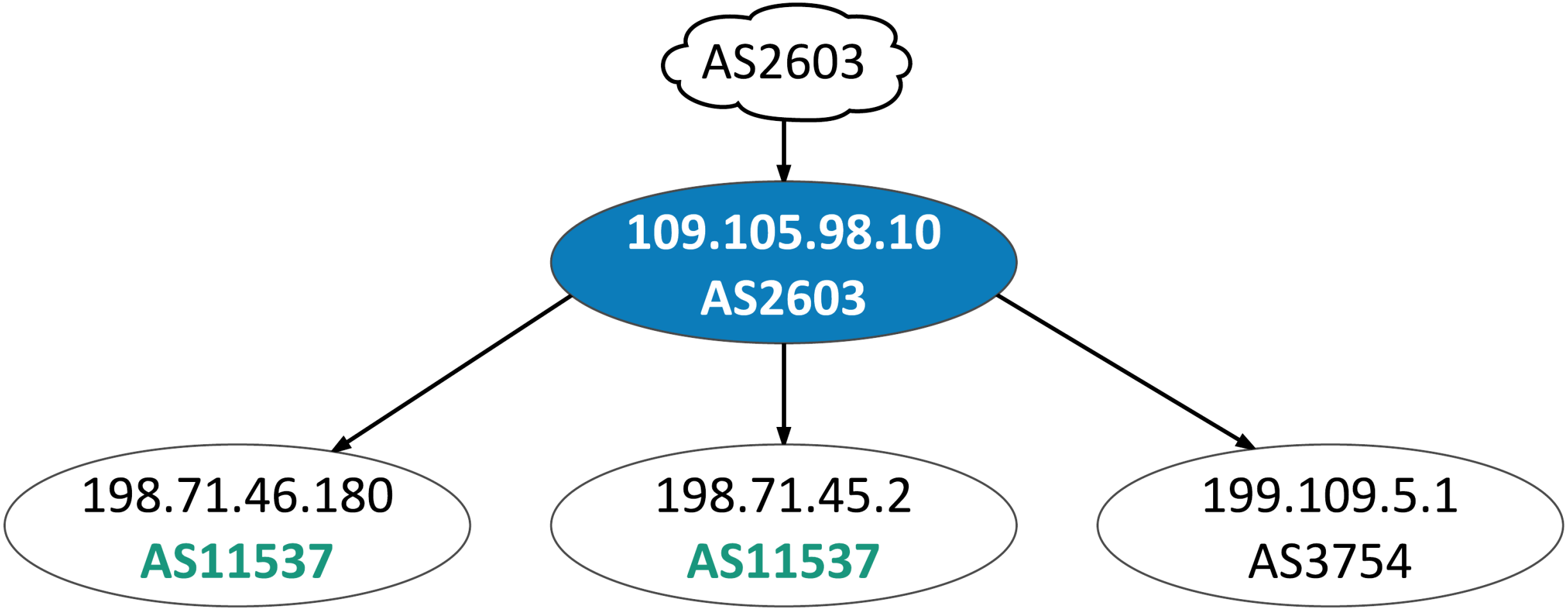
MAP-IT Algorithm

1: Create interface-level graph from traceroutes
2: **repeat**
3: Add inter-AS link inferences
4: Refine graph
5: **until** there are no more changes left to make
6: Infer links to stub ASes with single address

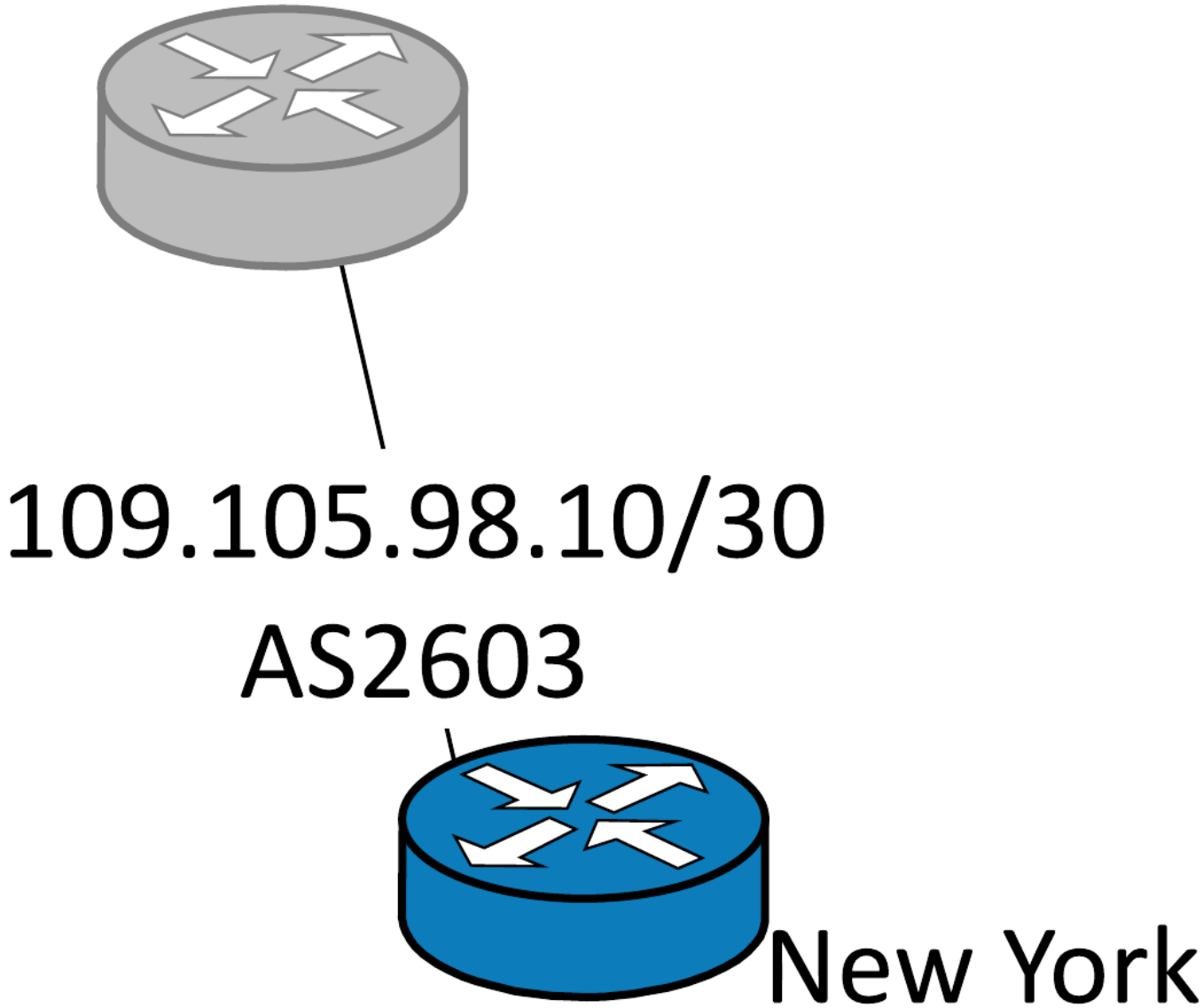
Interface-Level Graph



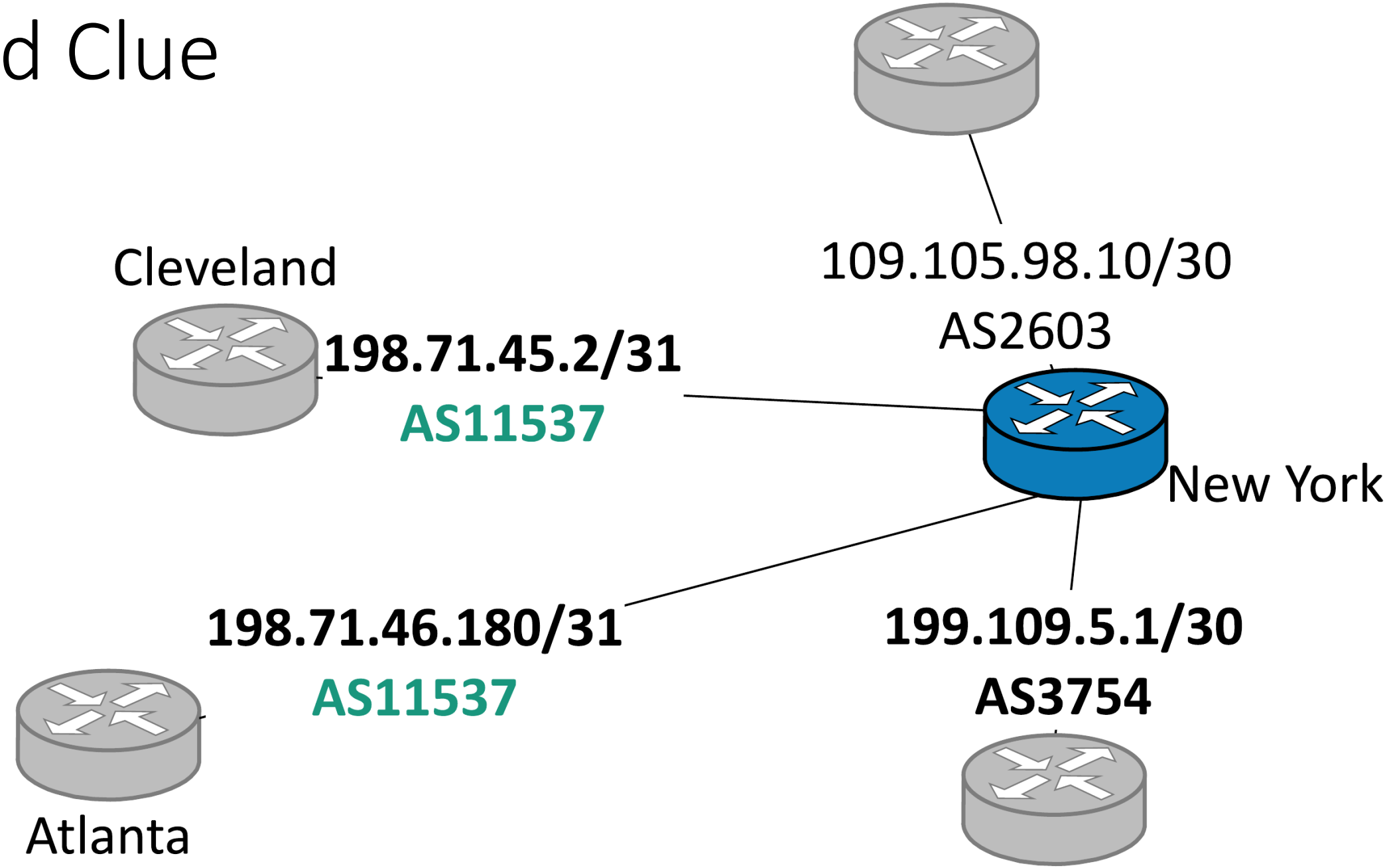
Forward Clue



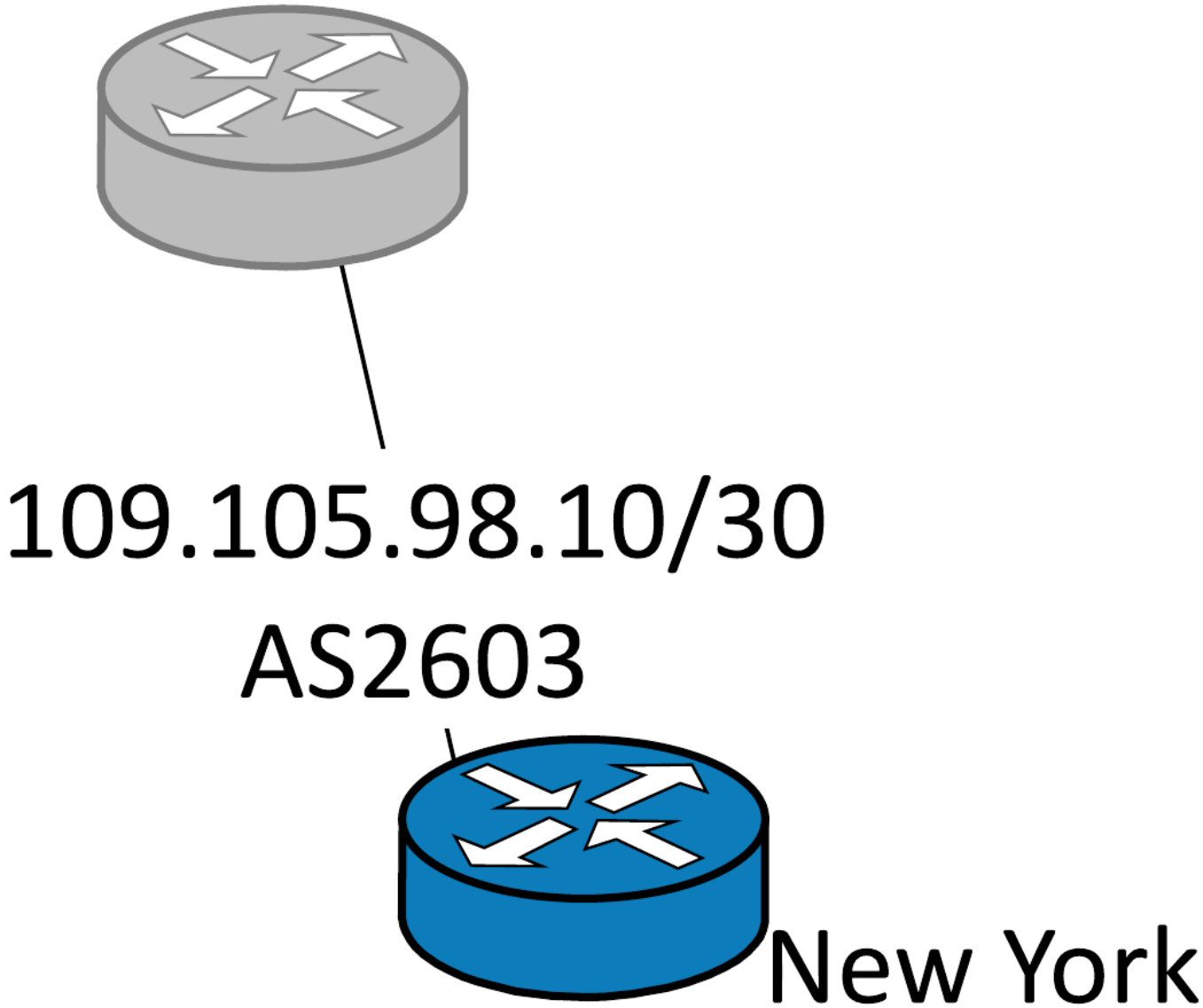
Forward Clue



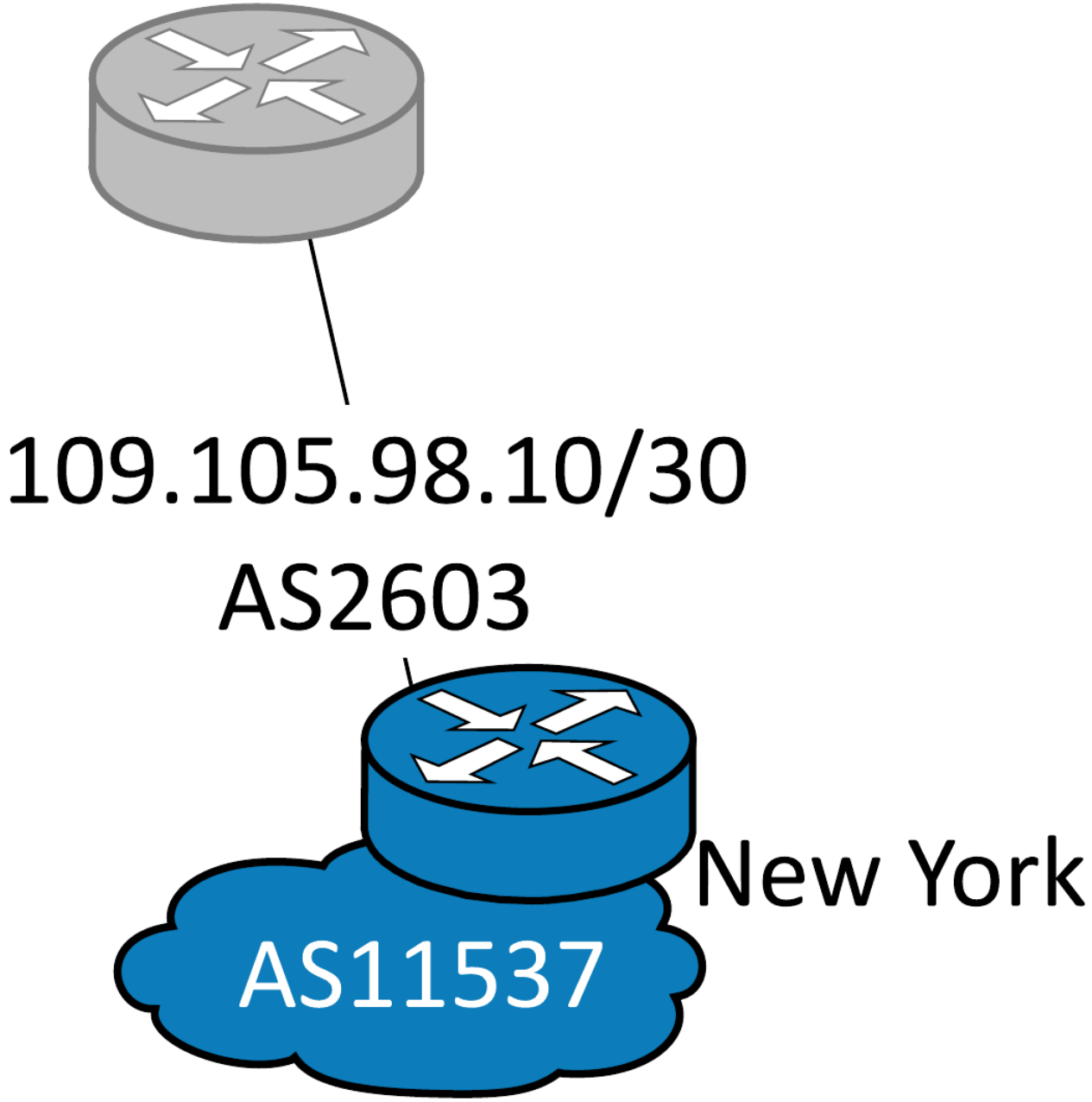
Forward Clue



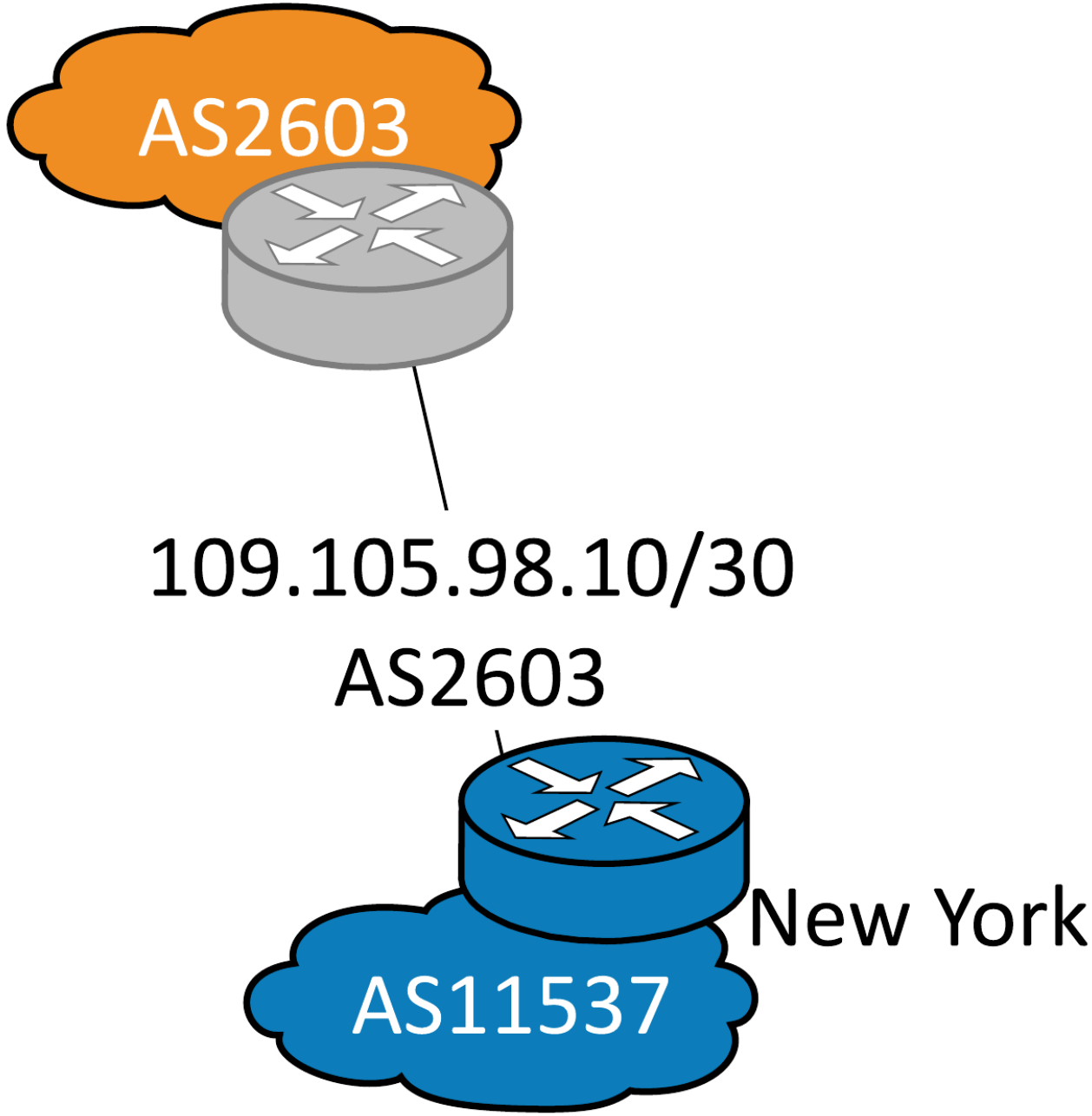
Forward Clue



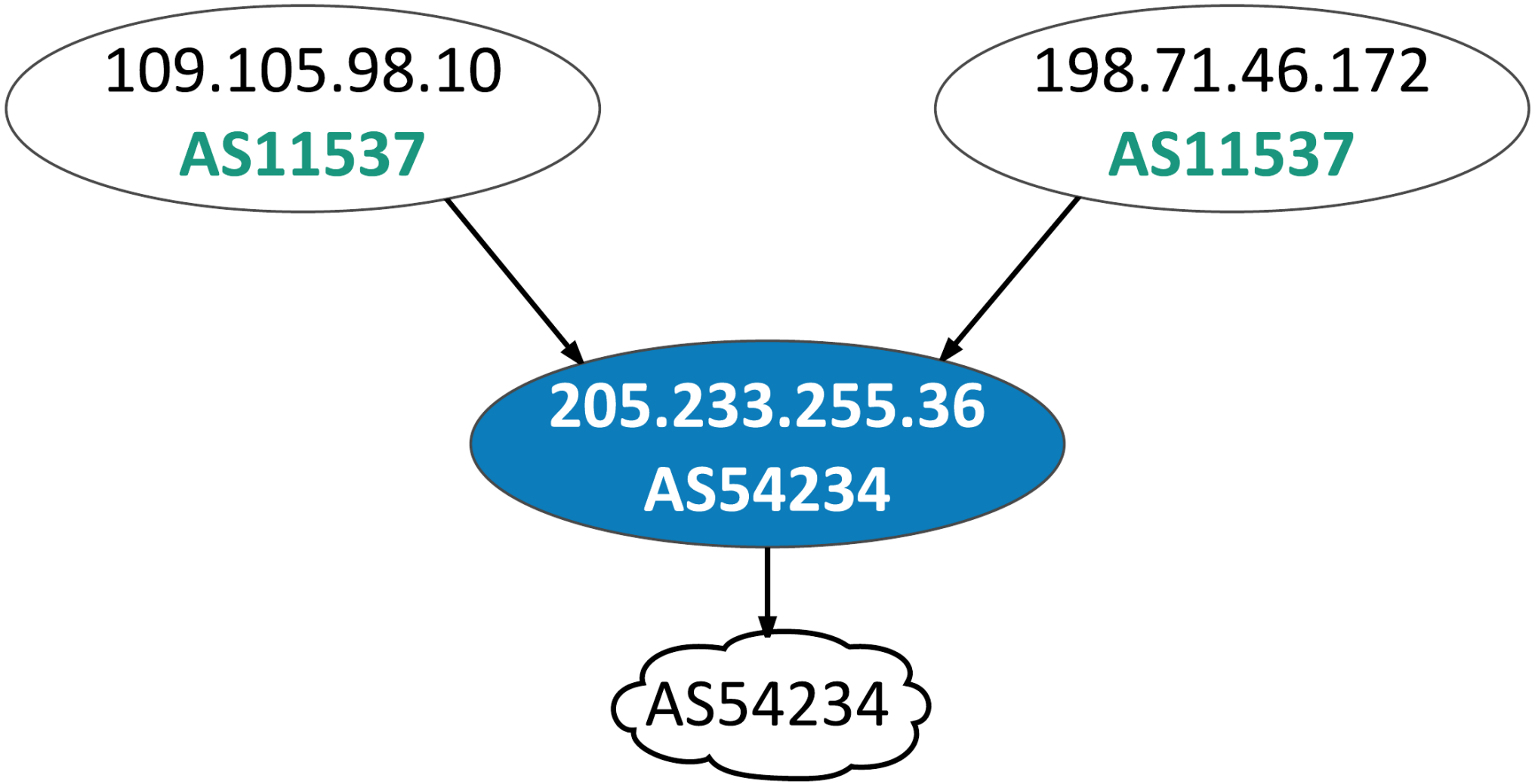
Forward Clue



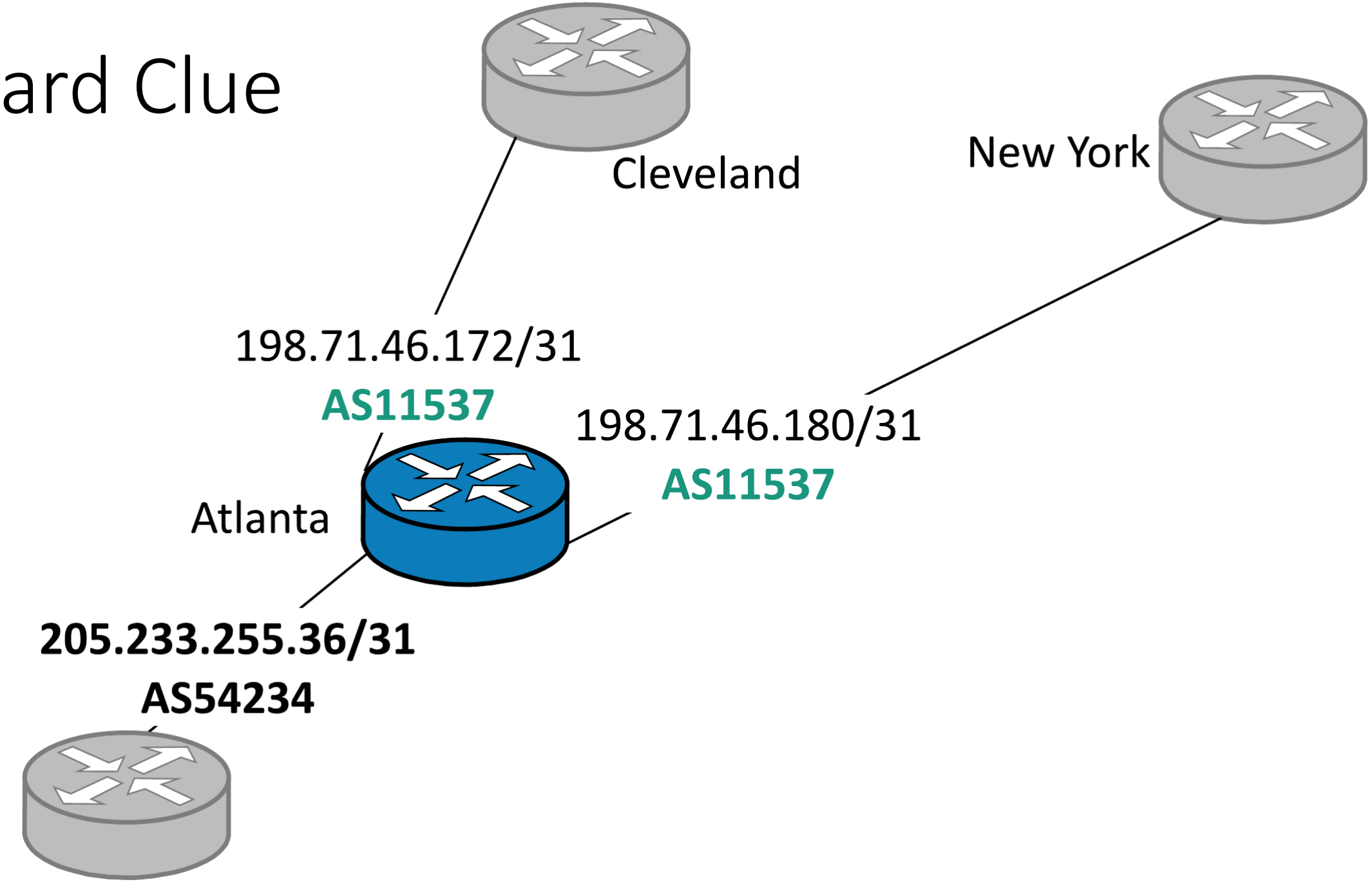
Forward Clue



Backward Clue



Backward Clue

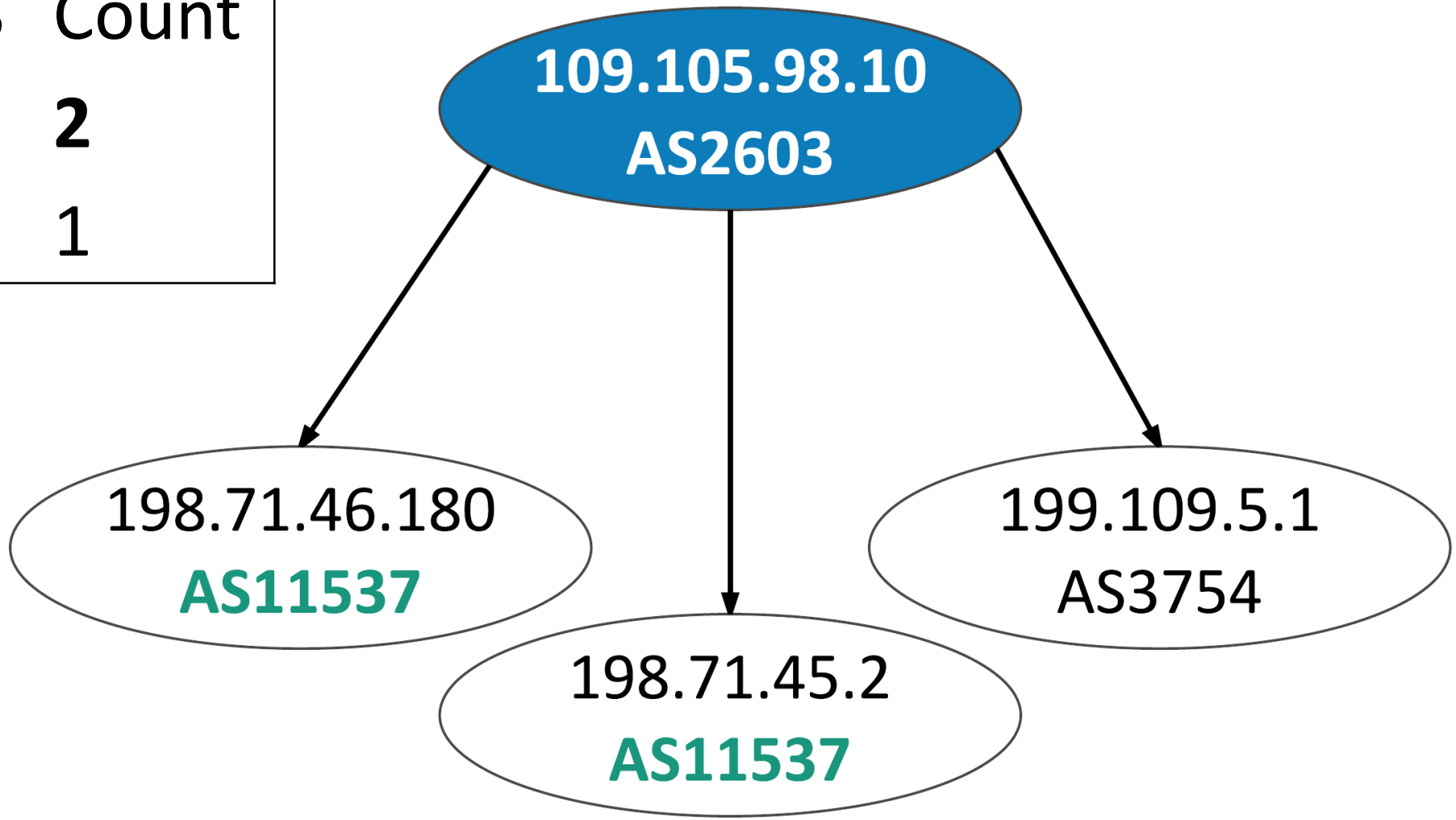


MAP-IT Algorithm

1: **Create interface-level graph from traceroutes**
2: **repeat**
3: **Add inter-AS link inferences**
4: **Refine graph**
5: **until there are no more changes left to make**
6: Infer links to stub ASes with single address

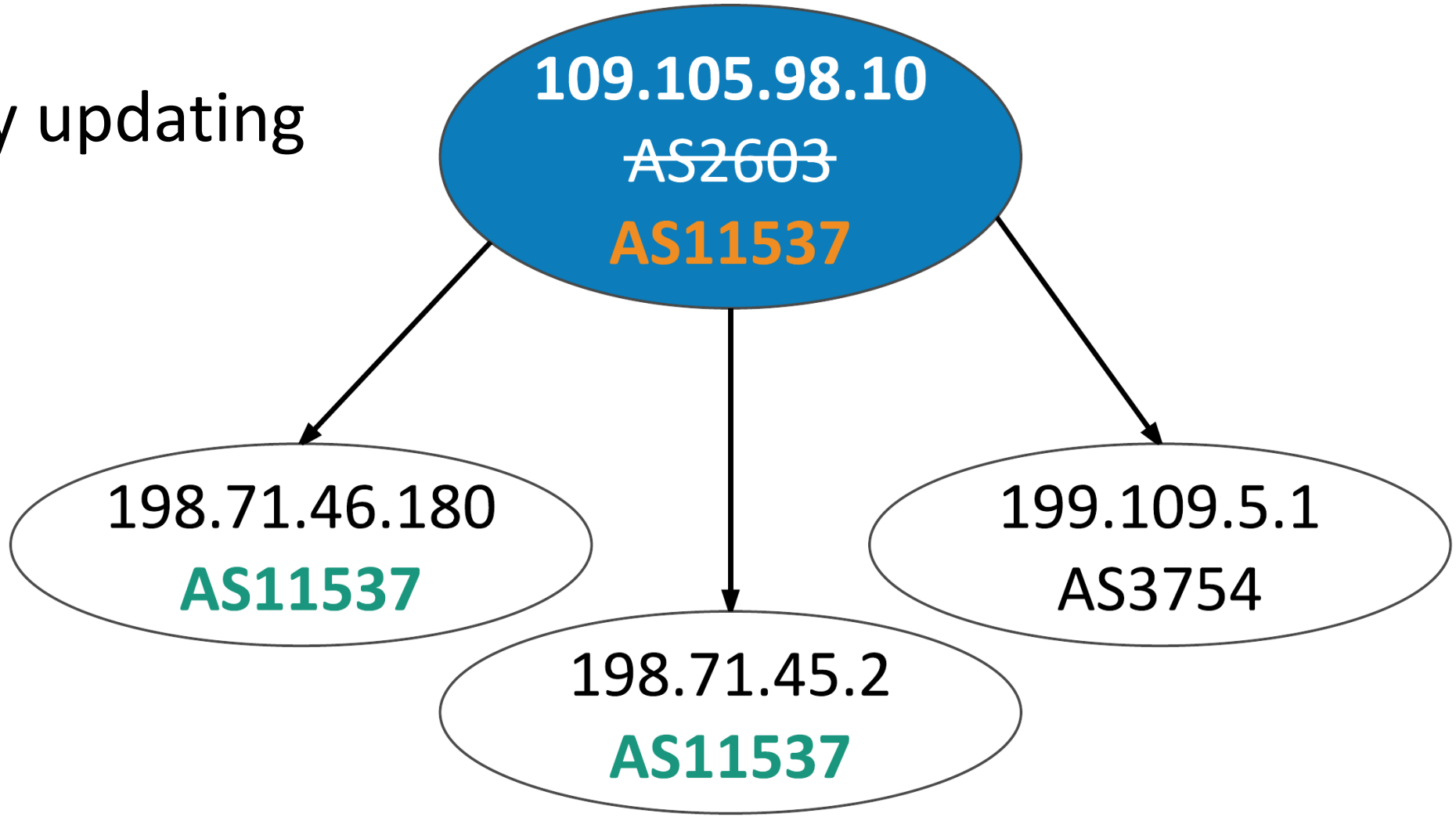
Infer Inter-AS Link

Neighboring AS	Count
11537	**2**
3754	1

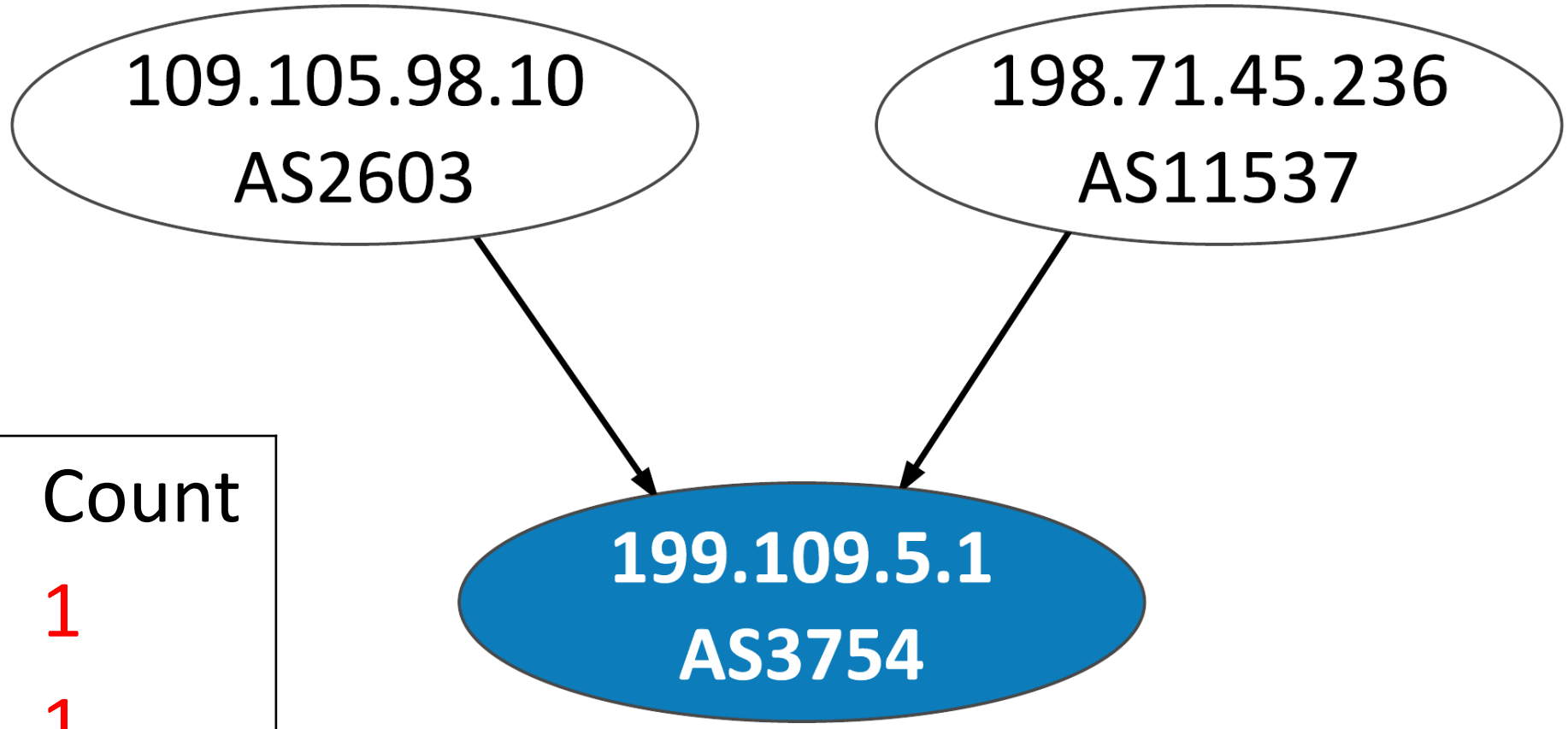


Refine Graph

Refine graph by updating IP2AS mapping

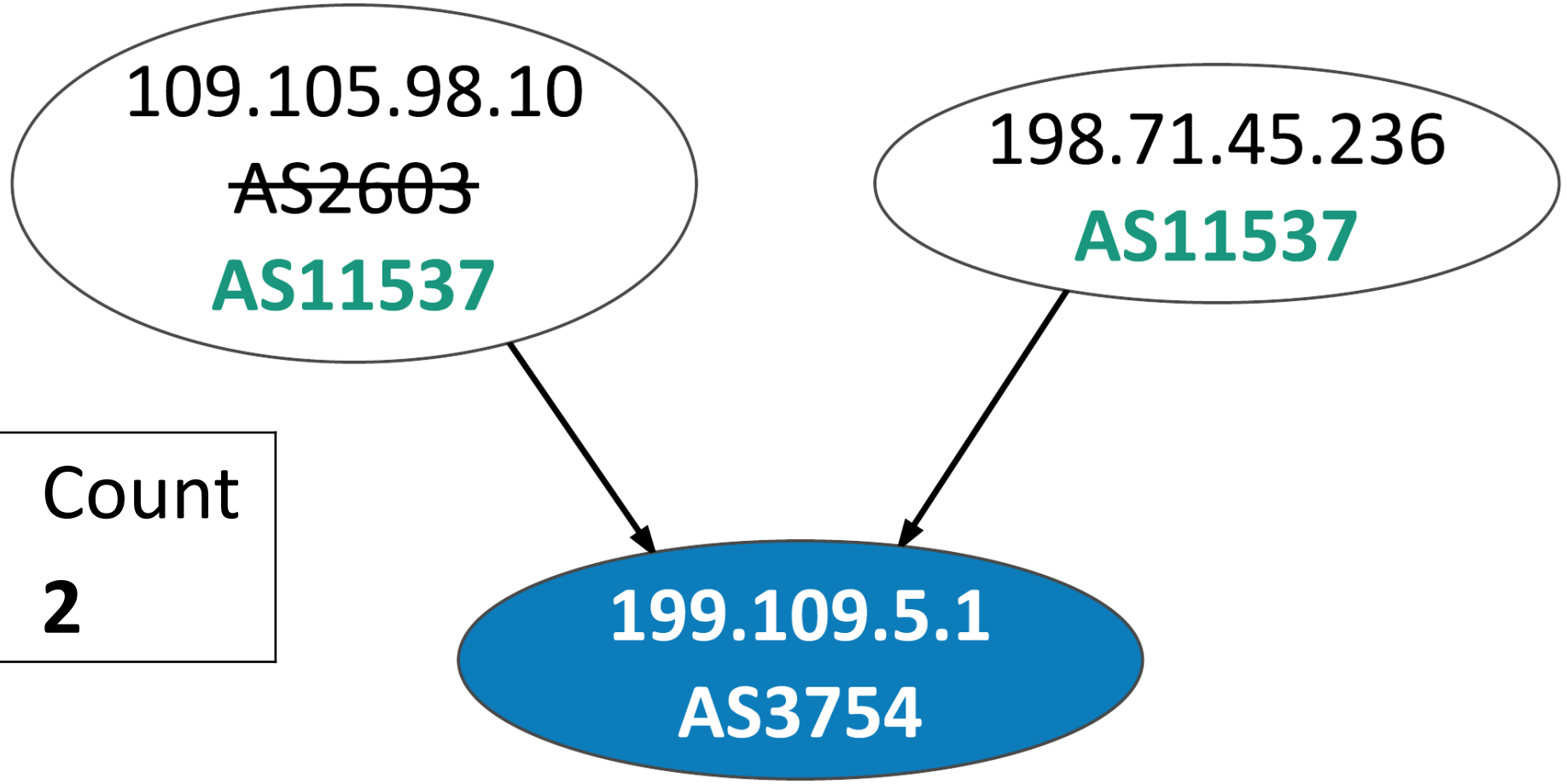


Multiple Passes: First Pass



Neighboring AS	Count
11537	1
2603	1

Multiple Passes: Second Pass



Neighboring AS	Count
11537	**2**

More Detail in the Paper

- Graph diminishes impact of artifacts
- Third party addresses
- Remove incorrect inferences
- ISP -> stub AS links with a single address
- Limitations

Experiments

- Traceroute datasets from CAIDA's website for 10/2015*
- Verification data:
  - Interface info provided by Internet2's NOC*
  - DNS hostnames for Level 3 and TeliaSonera

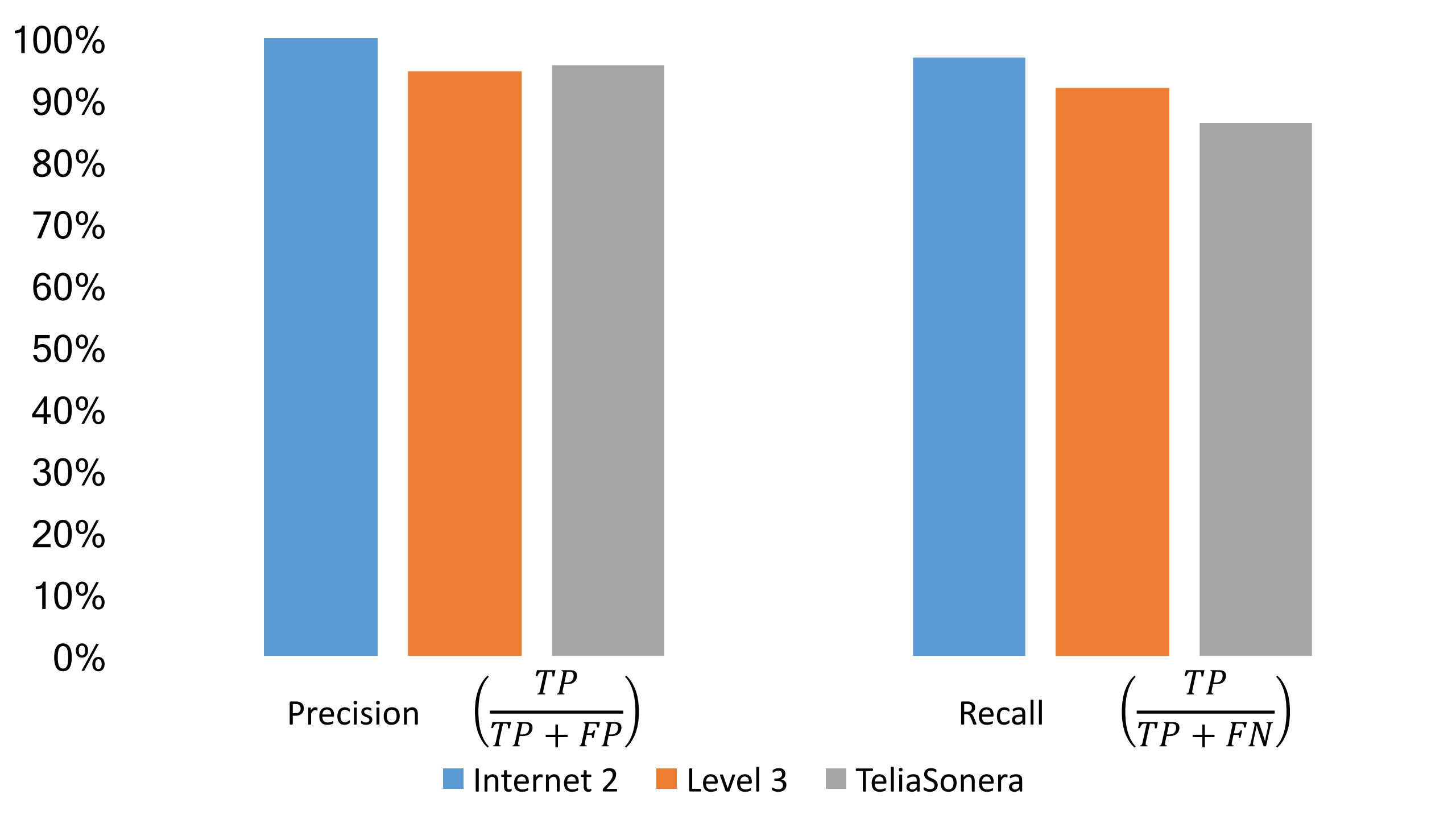
*Restricted, but available from source upon request

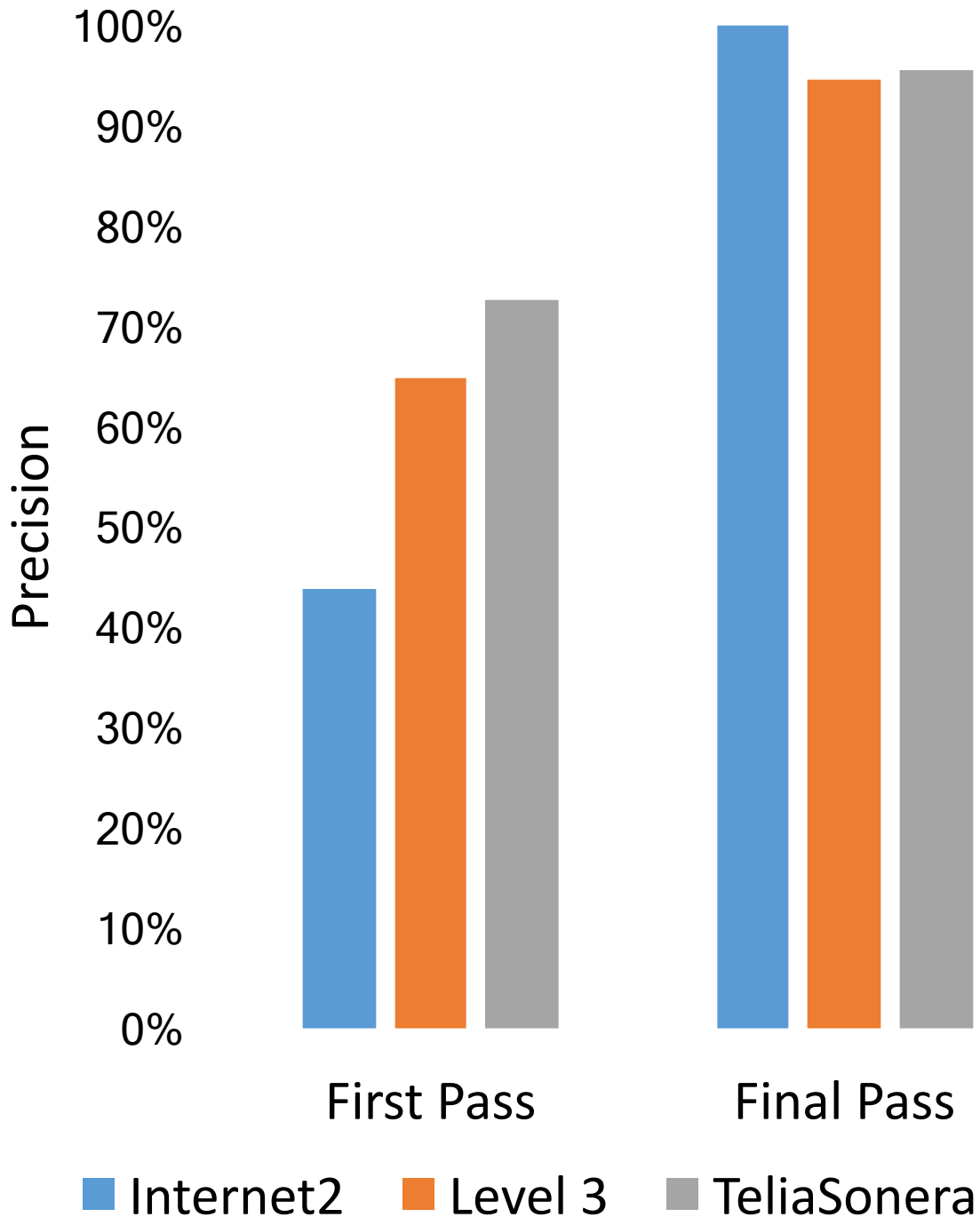
Internet2 (AS11537)

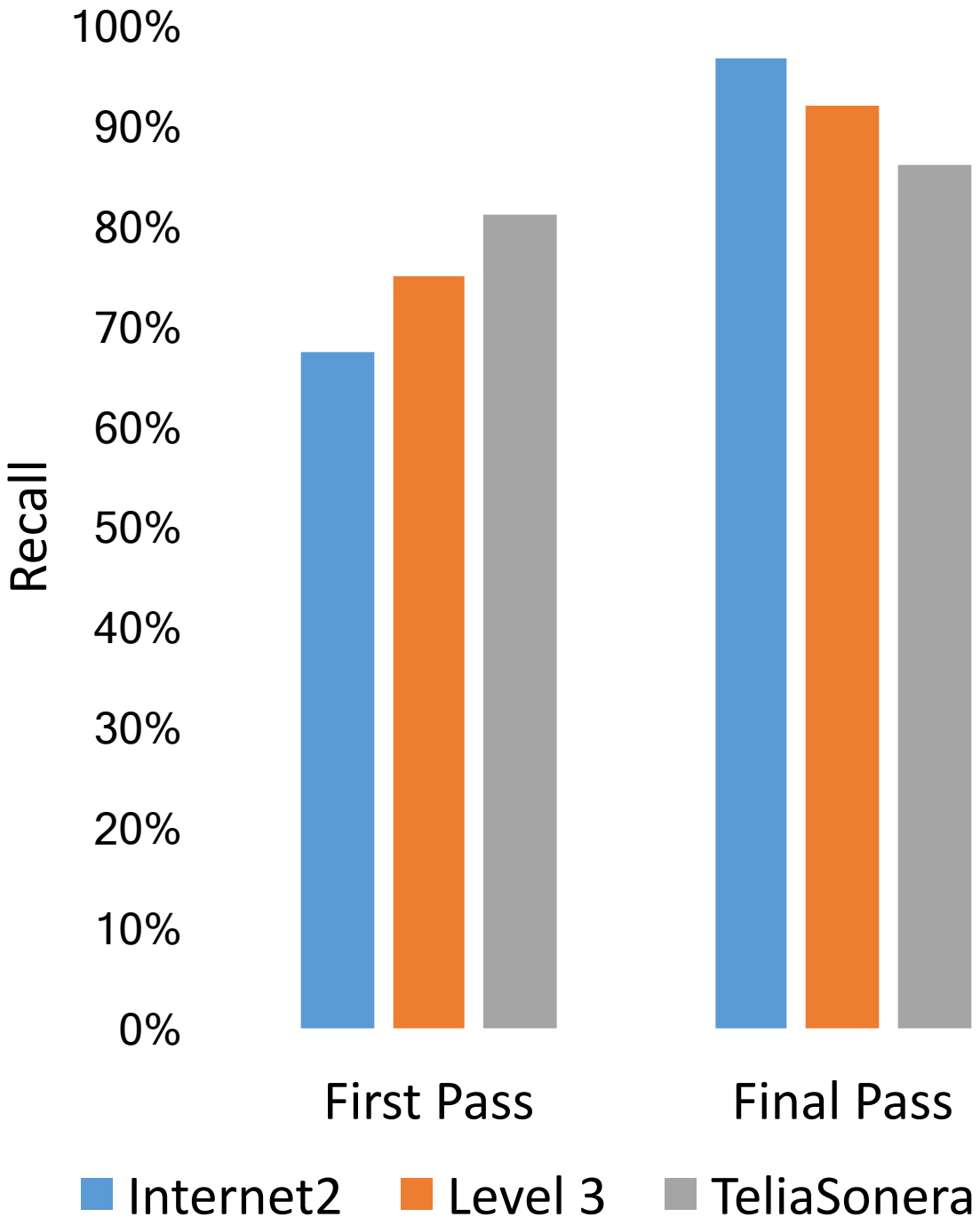
- XML interface-level information
- 192.122.175.12/31: **UVM** via **AL2S/ALBA**

Level 3 (AS3356) and TeliaSonera (AS1299)

- DNS hostnames often contain tags
- 4442 inter-AS links
  - **cogent**-ic-309423-den-b1.c.telia.net
- 3599 internal link pairs
  - 4.69.201.118: **ae-41-41**.ebr1.berlin1.level3.net
  - 4.69.201.117: **ae-41-41**.ebr2.budapest1.level3.net


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Precision $\left(\frac{TP}{TP + FP}\right)$
Recall $\left(\frac{TP}{TP + FN}\right)$
Internet 2
Level 3
TeliaSonera


Precision
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
First Pass
Final Pass
Internet2
Level 3
TeliaSonera


Recall
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
First Pass
Final Pass
Internet2
Level 3
TeliaSonera

Conclusion and Future Work

- MAP-IT is scalable and accurate
- Code is online (link in paper)
- Continue to refine as new datasets become available
- Explore tradeoffs with bdrmap

Questions?