The Collateral Damage of Internet Censorship by DNS Injection

Anonymous <zion.vlab@gmail.com>

presented by Philip Levis

Basic Summary

- Great Firewall of China injects DNS responses to restrict access to domain names
- This affects traffic originating outside China
  - 26.4% of open resolvers affected
  - .de is the most affected TLD (70% of open resolvers in kr)
- Explain how, where, and why this happens
- Present several possible solutions

Just To Be Clear

This talk assumes that the Great Firewall of China is not designed to restrict Internet access to computers outside of China.

"Collateral damage" means restricting access to computers outside China.

DNS Overview

root
.

top level domain (TLD)
.com, .edu, .cn, .de

domain (authoritative)
stanford.edu, baidu.cn

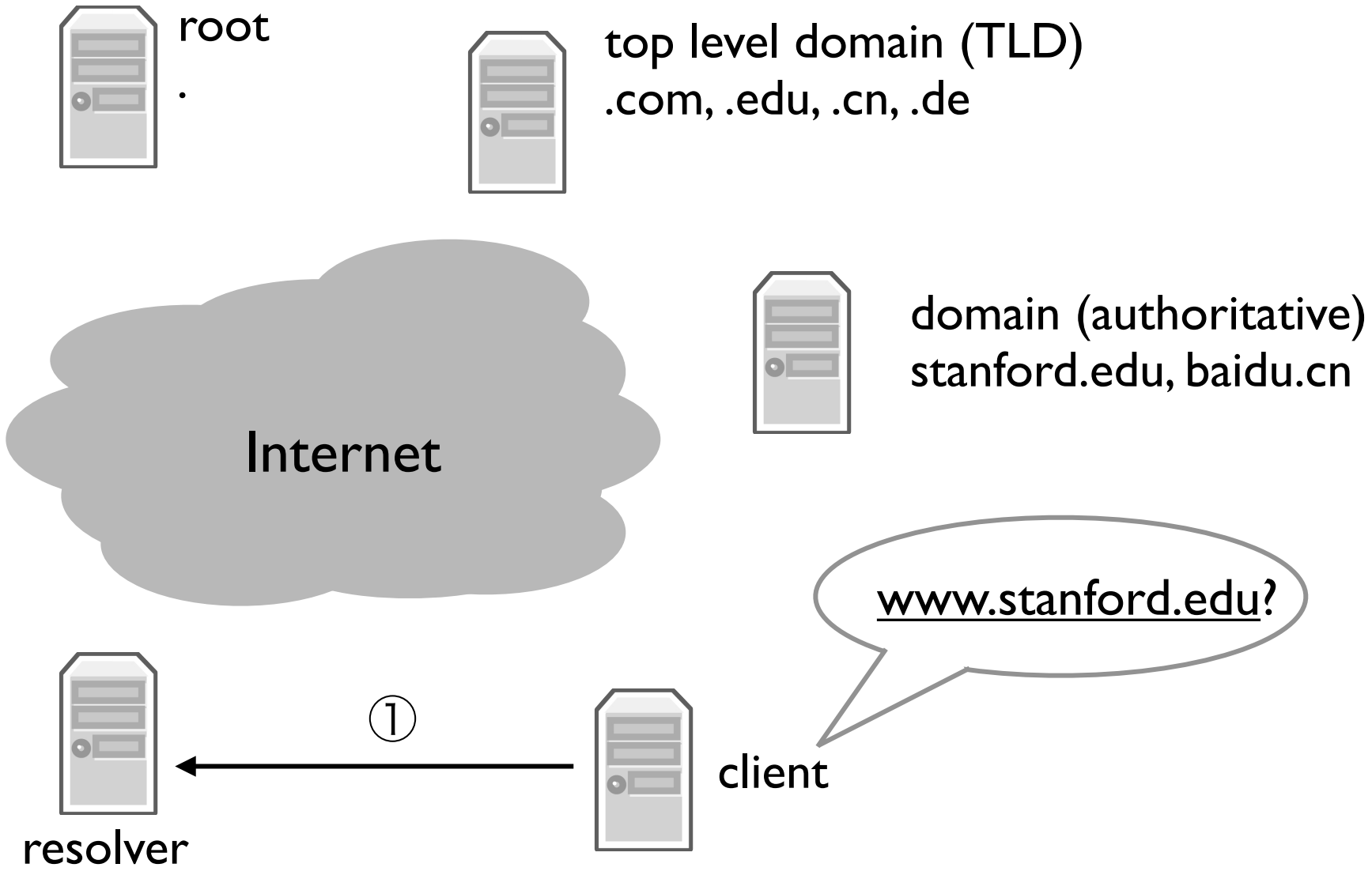
Internet

www.stanford.edu?

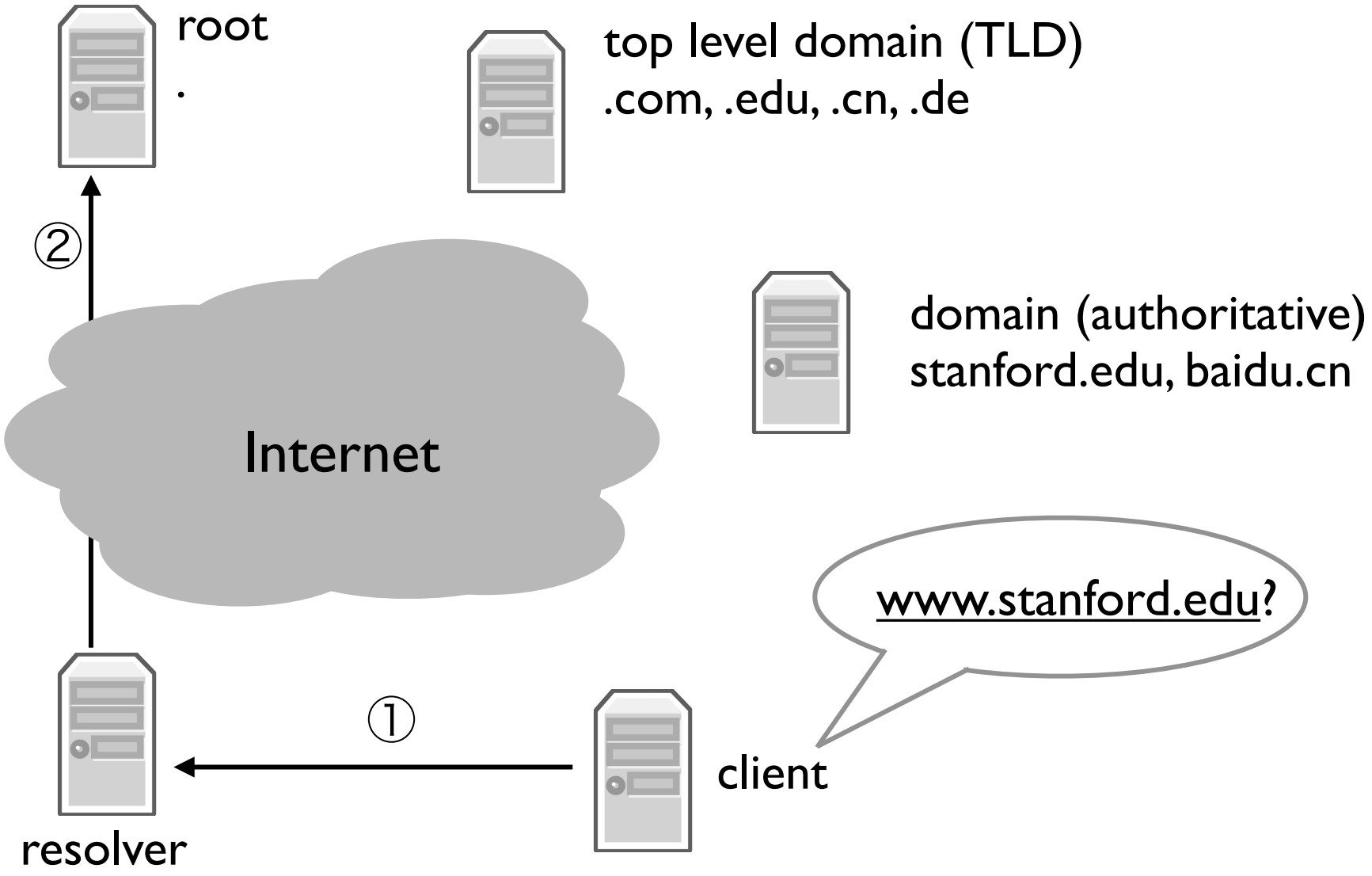
resolver

client

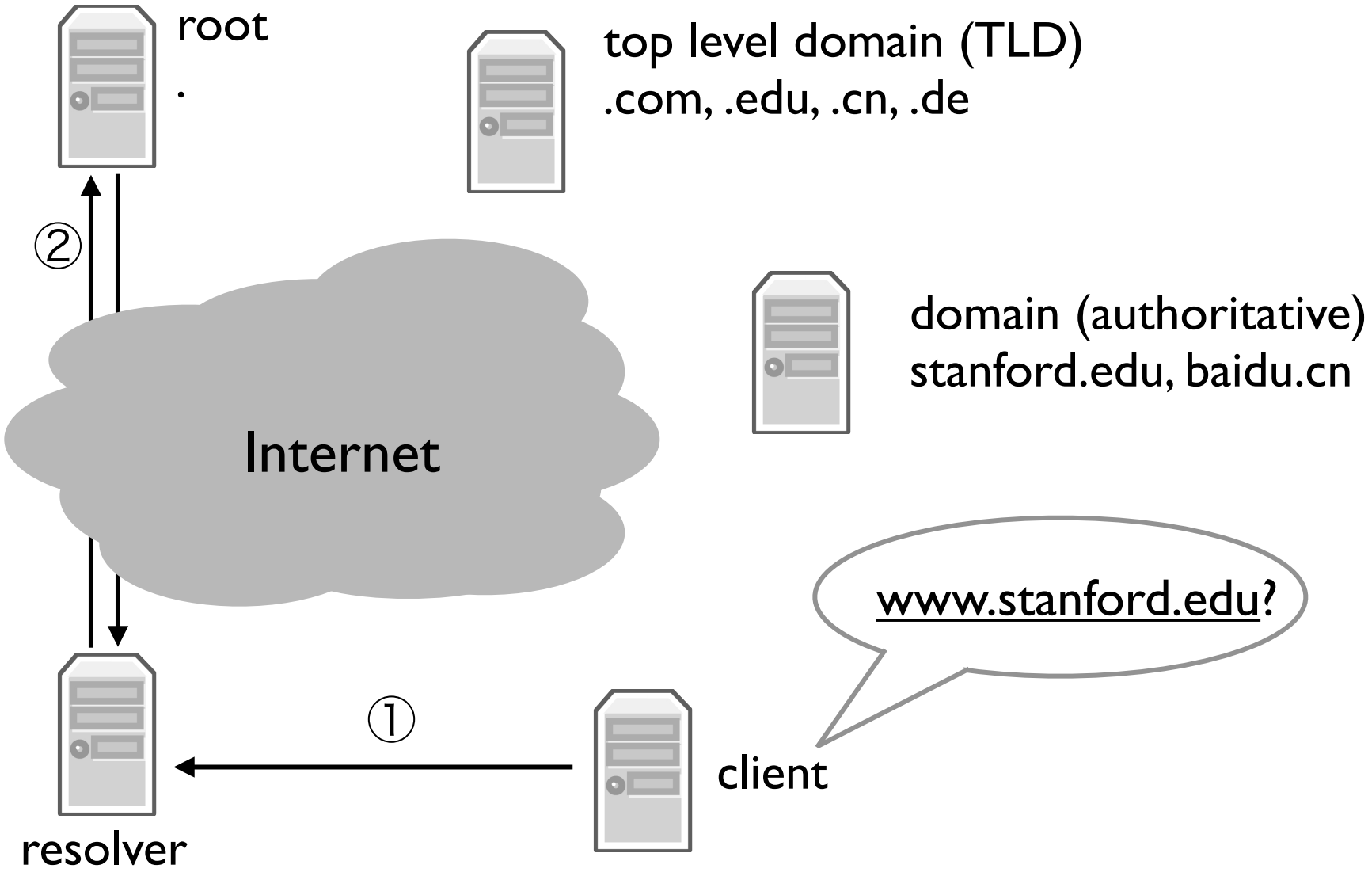
DNS Overview



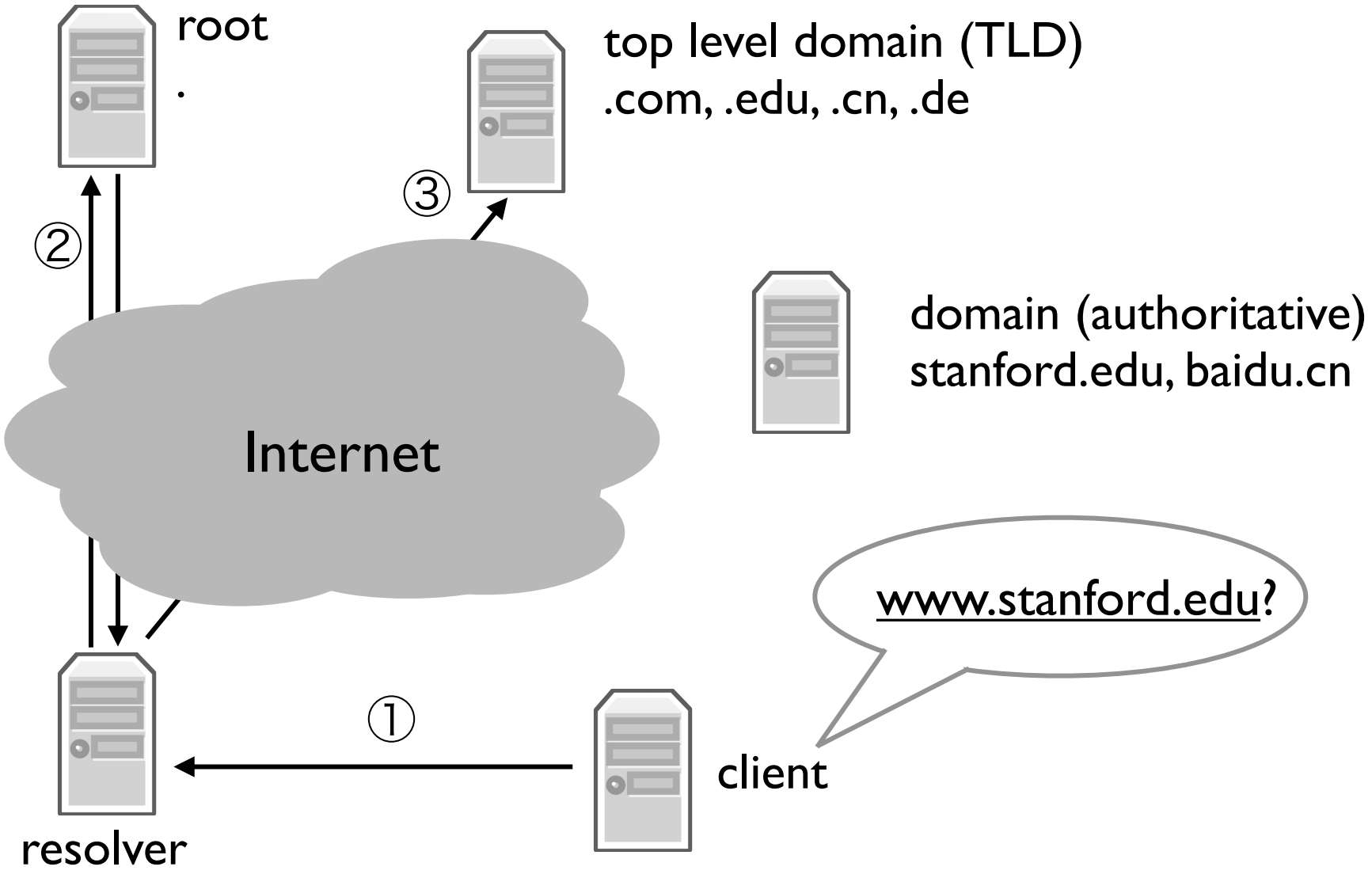
DNS Overview



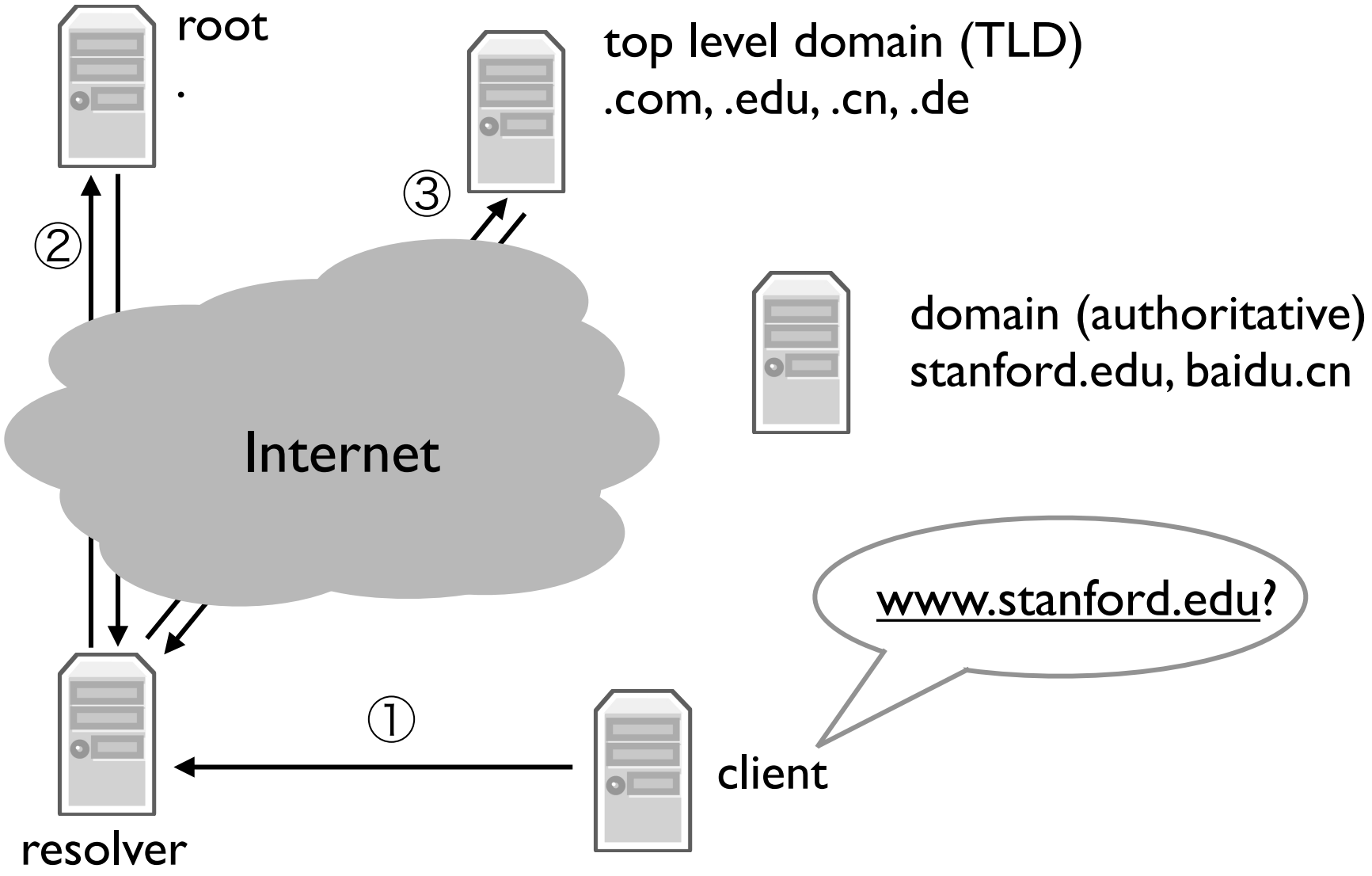
DNS Overview



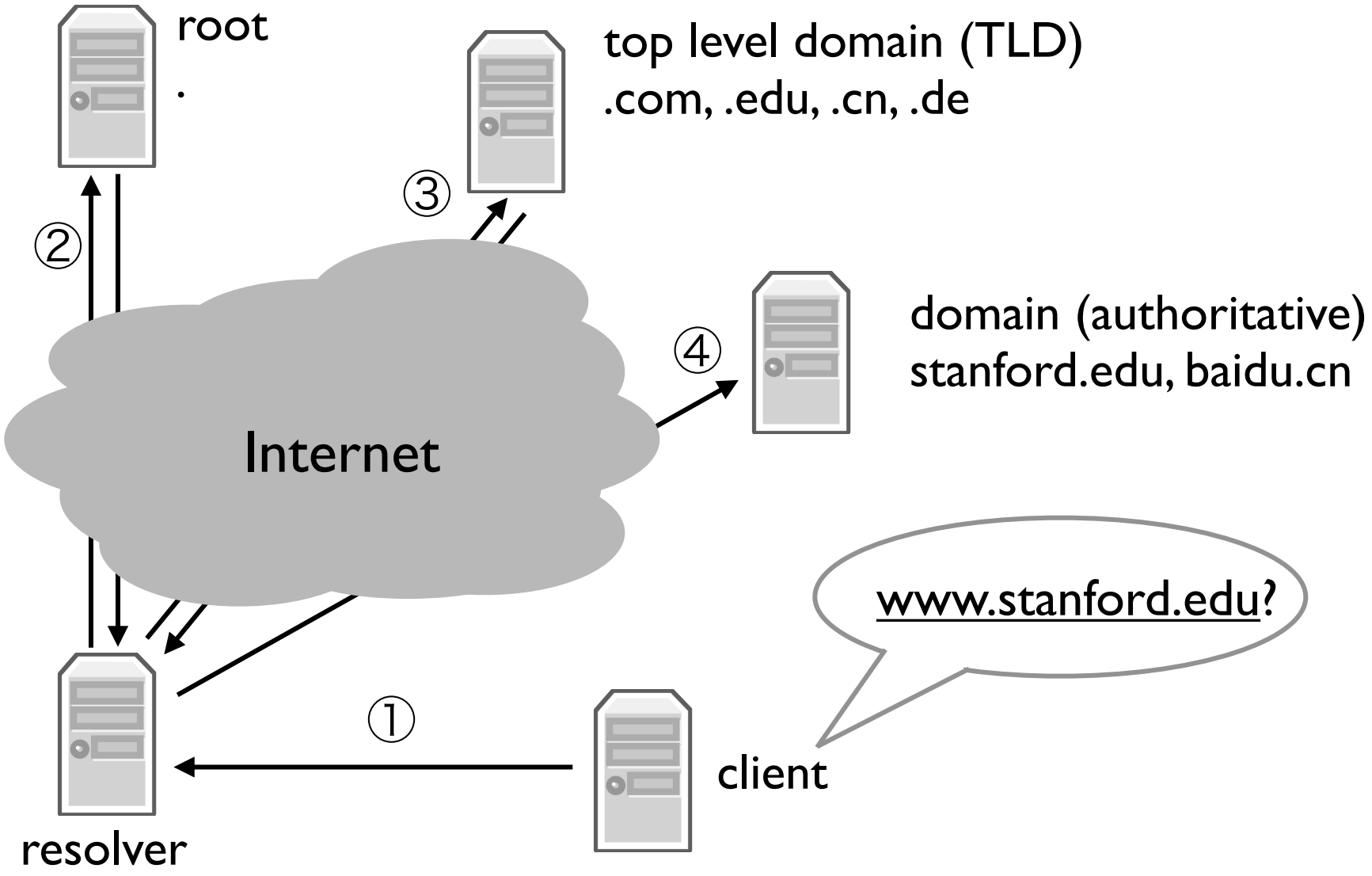
DNS Overview



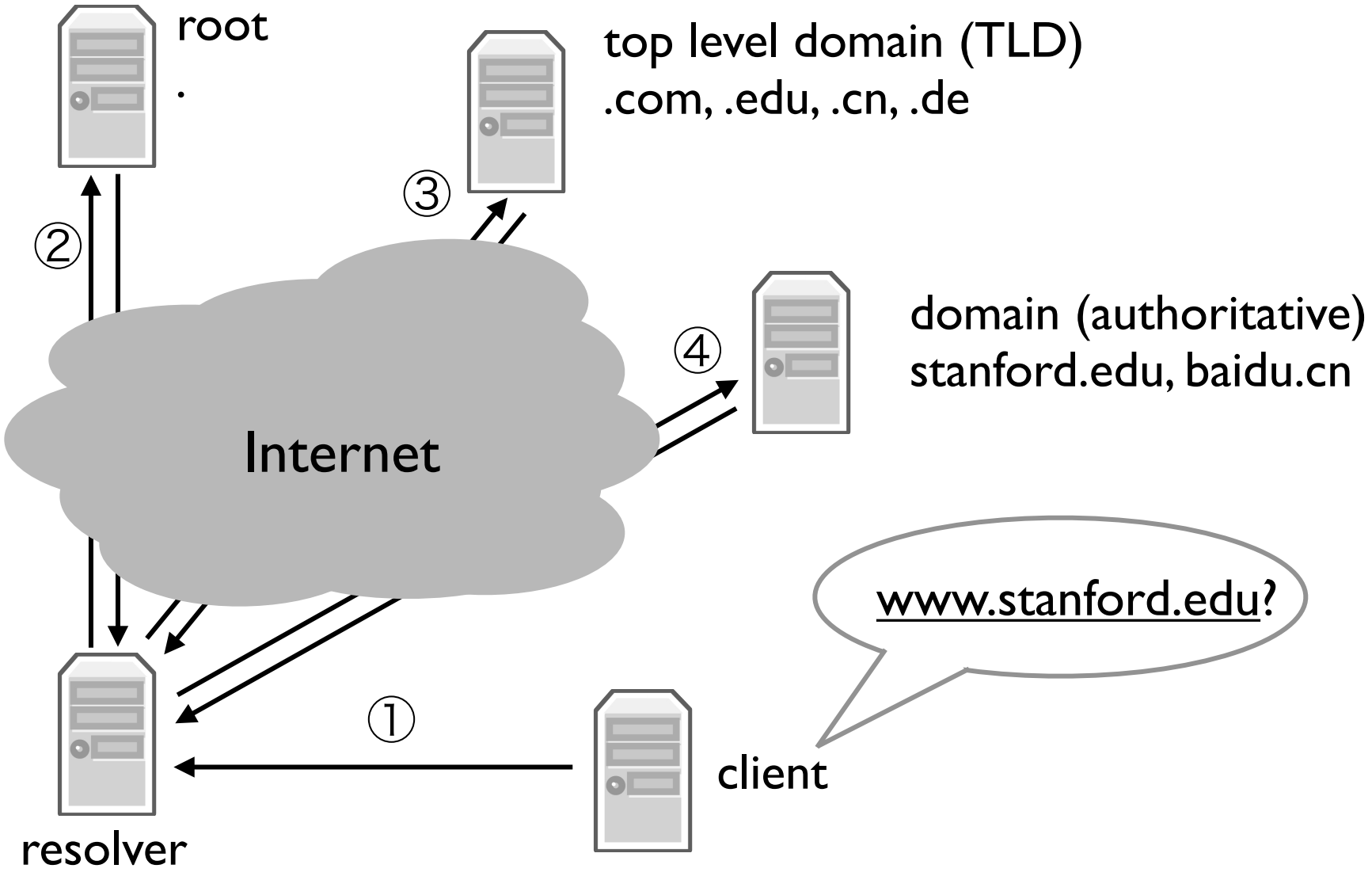
DNS Overview



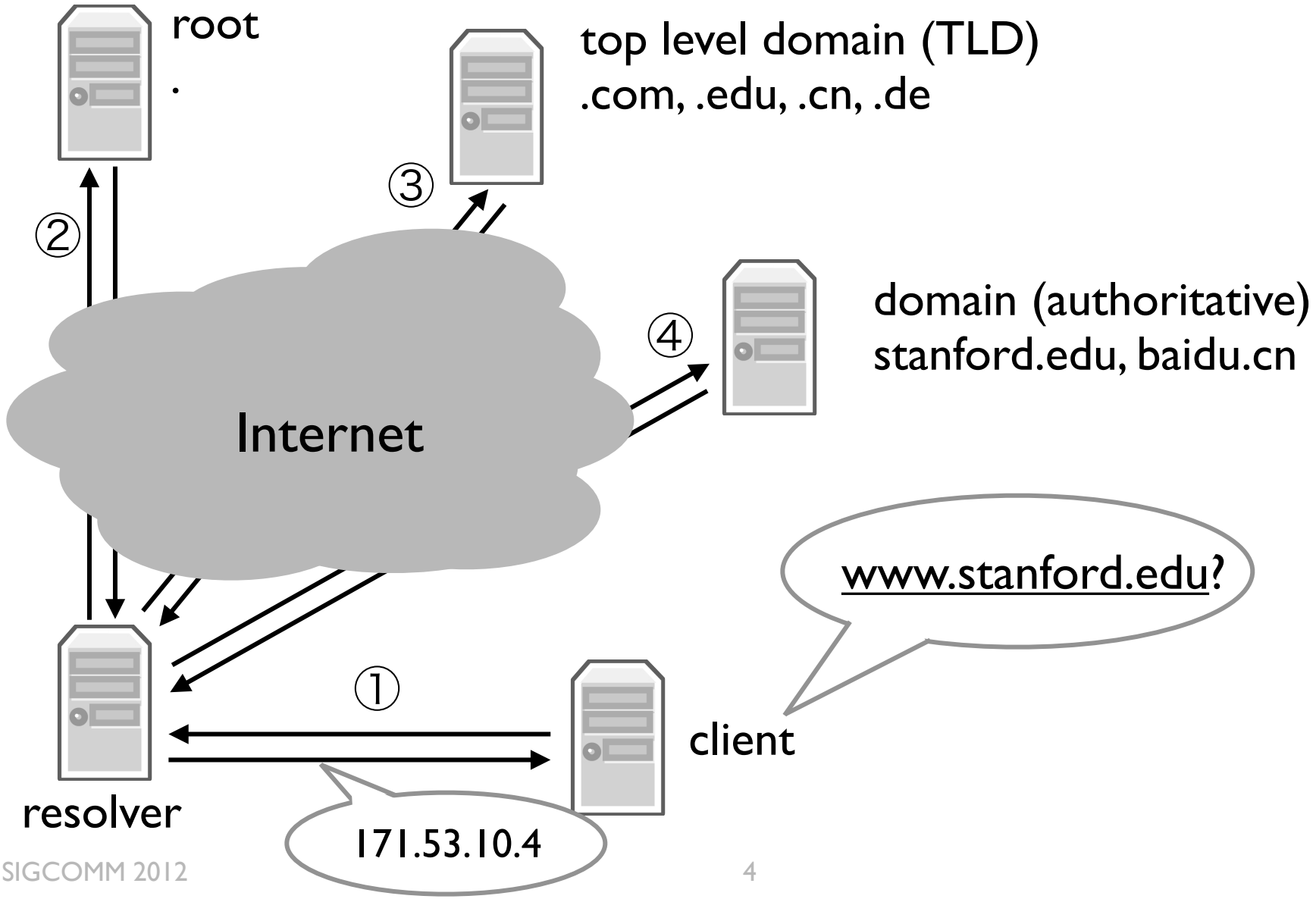
DNS Overview



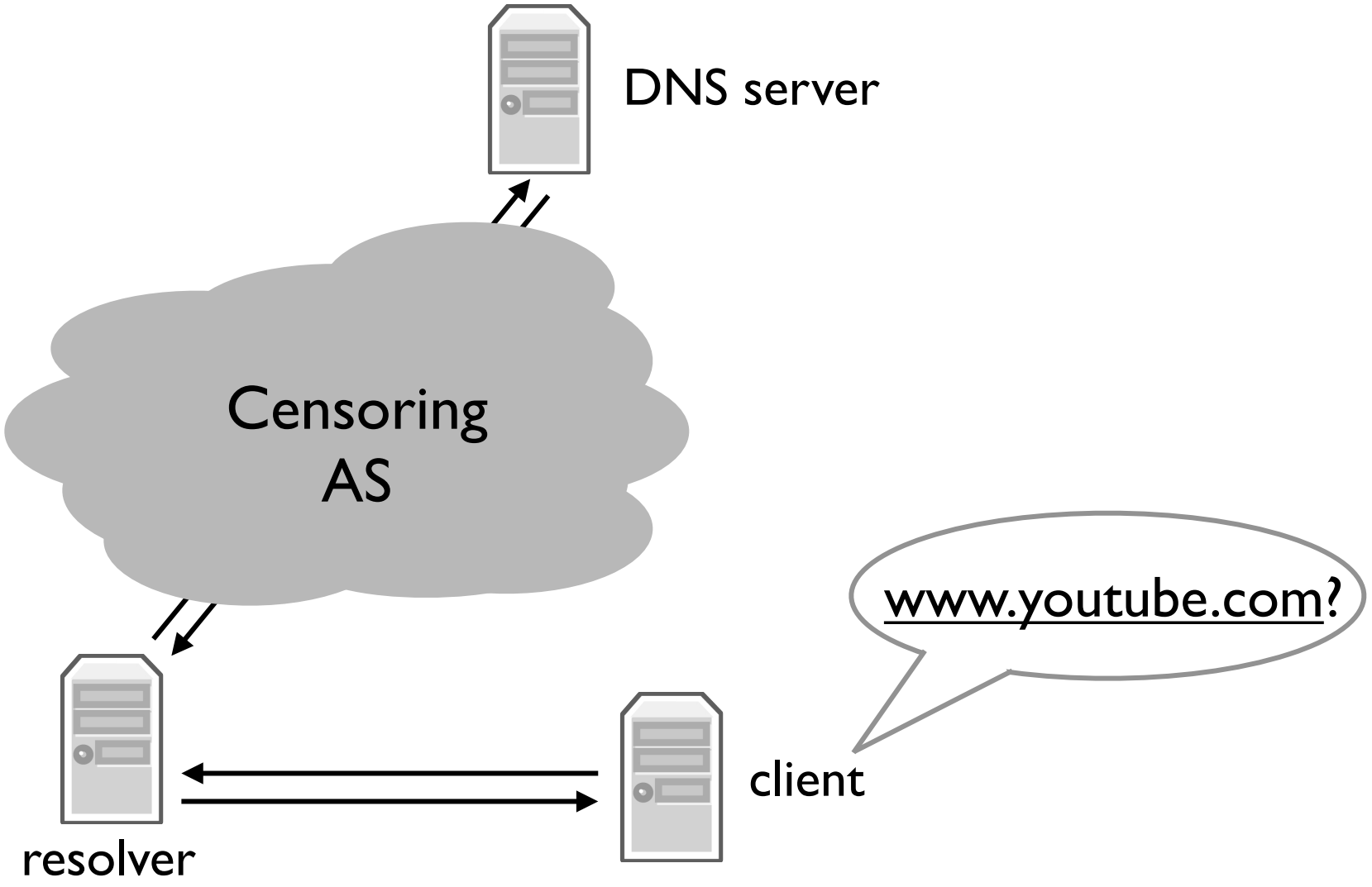
DNS Overview



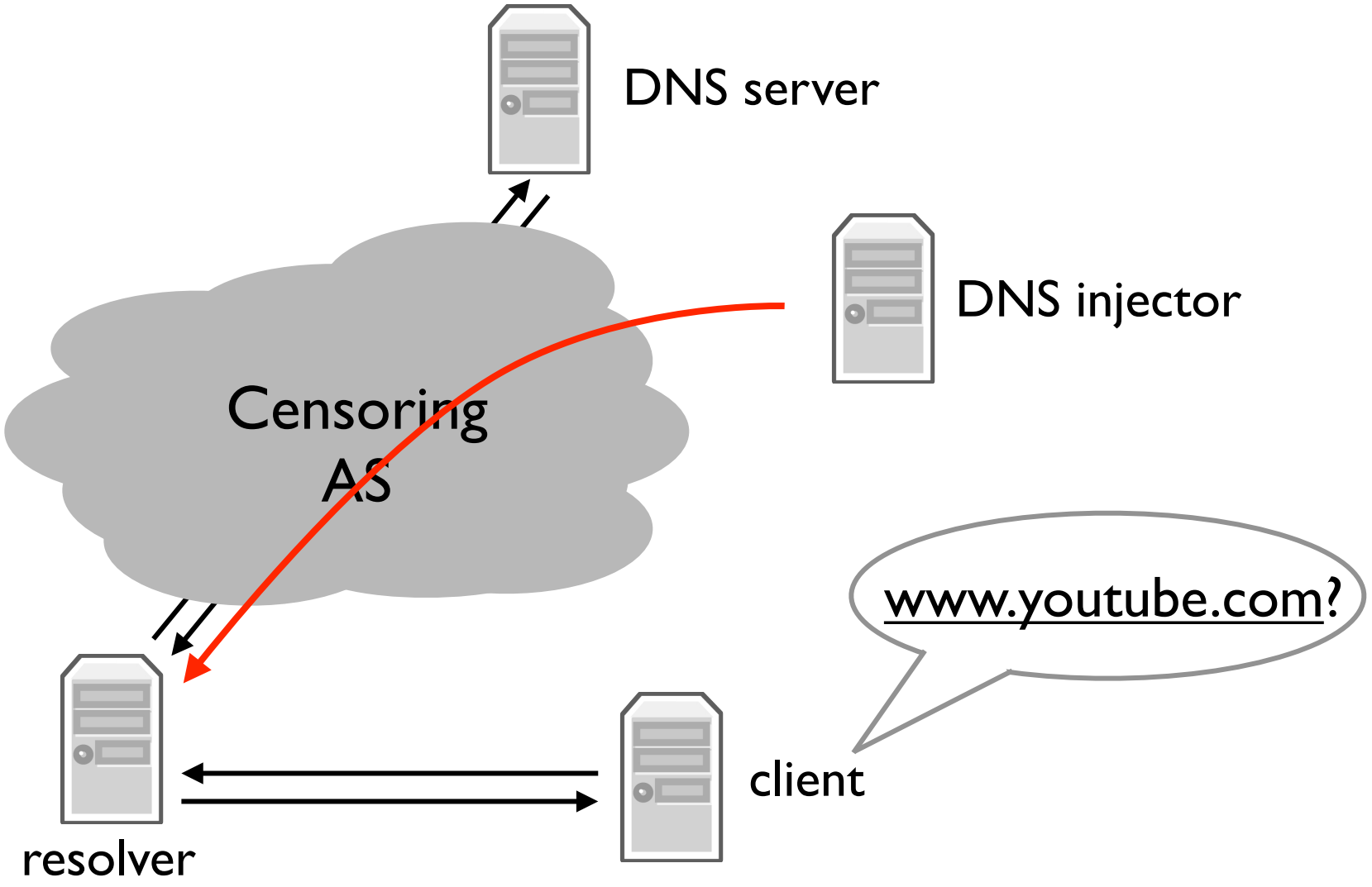
DNS Overview



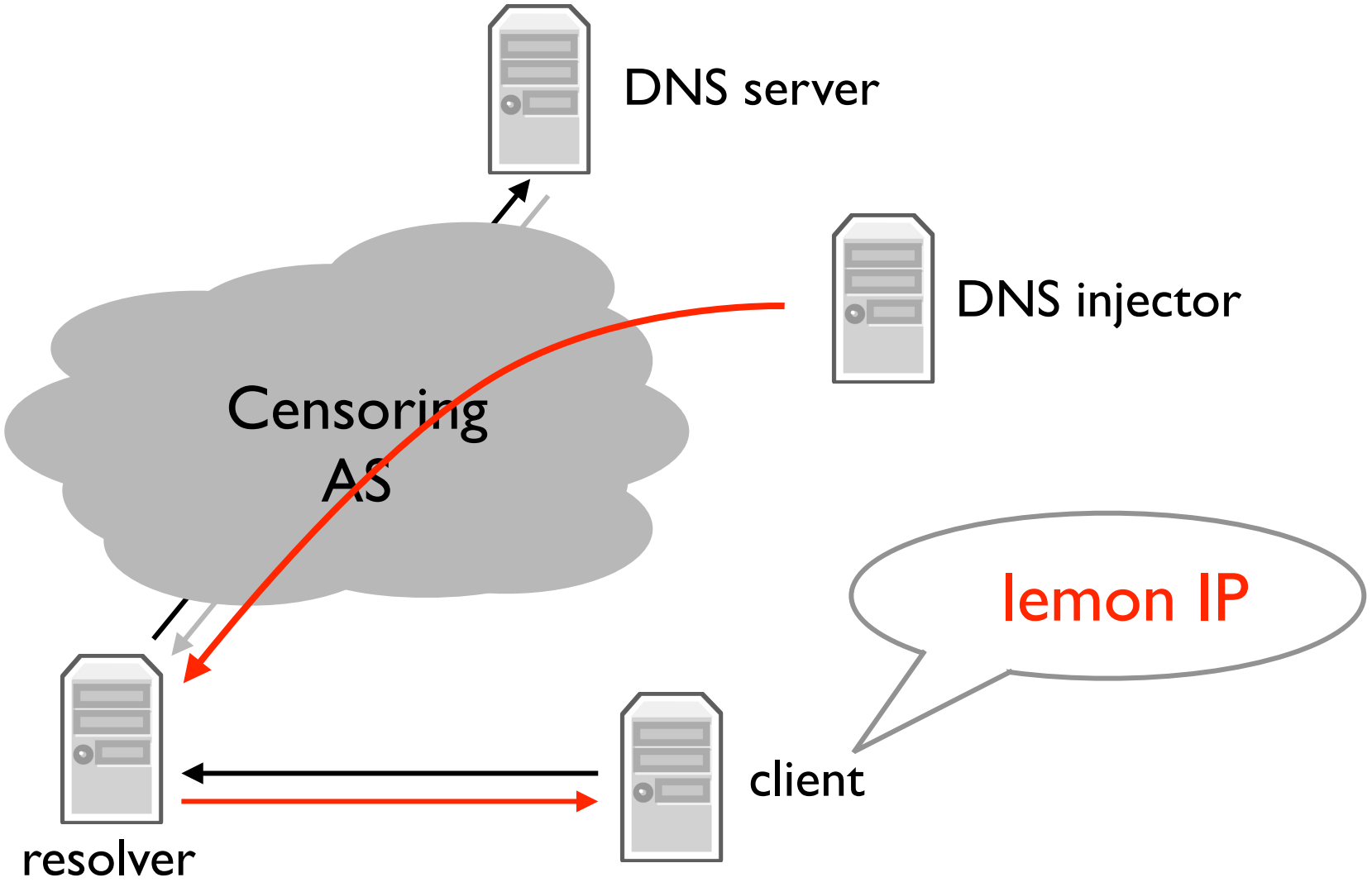
DNS Injection



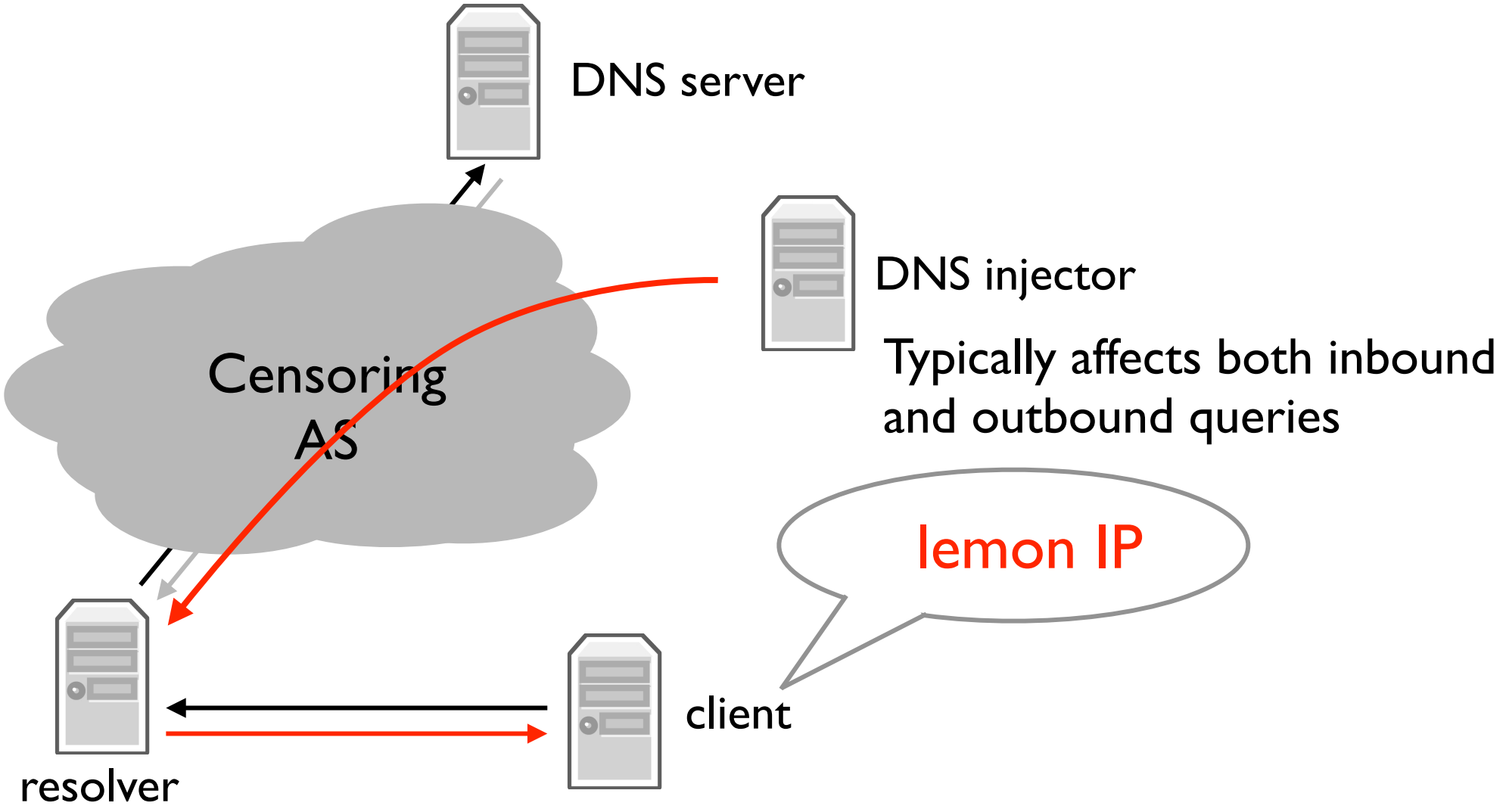
DNS Injection



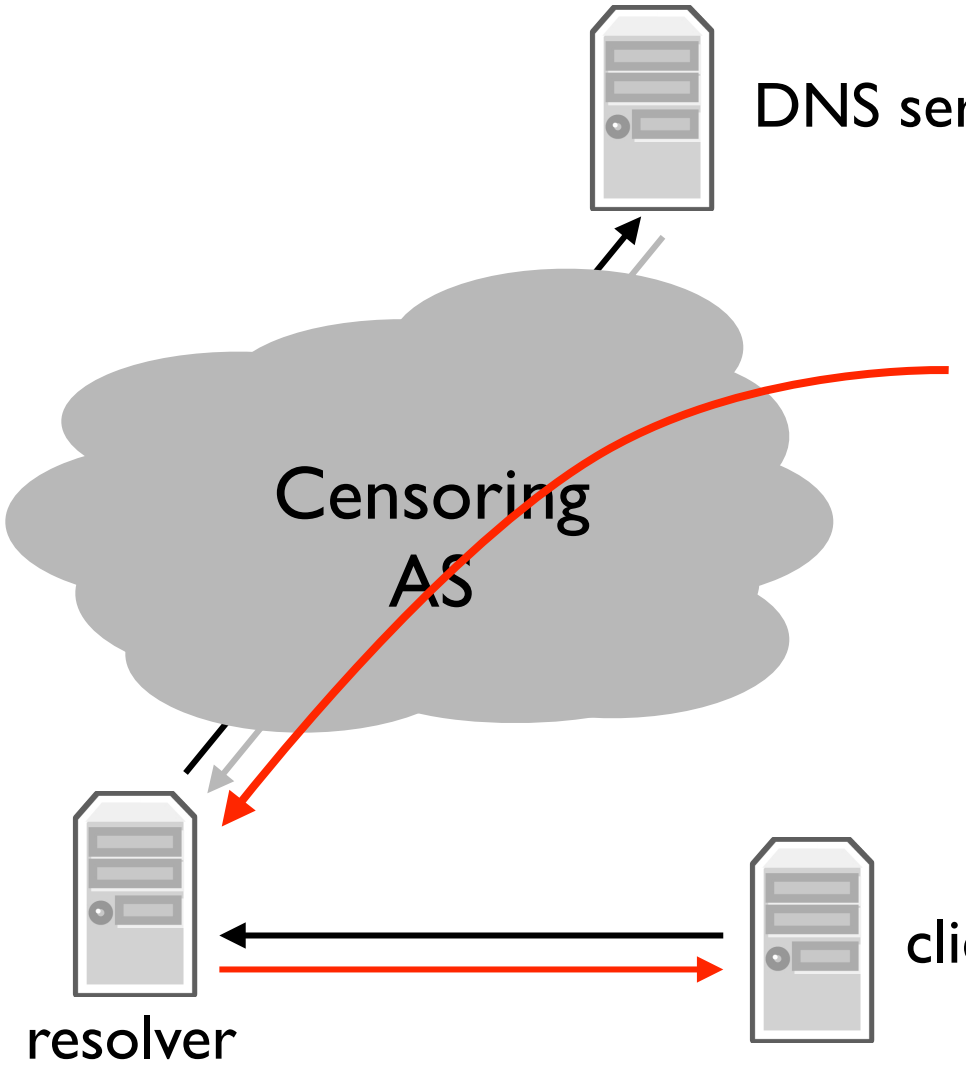
DNS Injection



DNS Injection



DNS Injection



Typically affects both inbound and outbound queries.

Typically does not suppress "correct" response, just wins race to respond.

Methodology

- *HoneyQueries* to detect autonomous systems paths to whom see DNS injection
- *TraceQueries* to identify location of injectors on affected paths
- *StepNXQueries* to measure collateral damage of DNS injection

HoneyQuery

- HoneyQuery: DNS query to sensitive domains, sent to unresponsive IP
  - Assumption: all observed DNS responses are from DNS injectors
- Send from a single vantage point (AS 40676)
  - 14 million IPs that cover all /24 subnets
  - Paths spread to discover all injecting autonomous systems
- Record IPs in responses: lemon IPs

Probed Domain Names

Domain	Category
www.google.com	Search Engine
www.facebook.com	Social Network
www.twitter.com	Social Network
www.youtube.com	Streaming Media
www.yahoo.com	Portal
www.appspot.com	Web Hosting
www.xxx.com	Pornography
www.urltrends.com	Site Ranking
www.live.com	Portal
www.wikipedia.com	Reference

Blacklisted Domains

Domain	Category
www.google.com	Search Engine
www.facebook.com	Social Network
www.twitter.com	Social Network
www.youtube.com	Streaming Media
www.yahoo.com	Portal
www.appspot.com	Web Hosting
www.xxx.com	Pornography
www.urltrends.com	Site Ranking
www.live.com	Portal
www.wikipedia.com	Reference

HoneyQuery Results

- 28 lemon IPs found
  - Use later to detect injected responses
- 388,988 (2.7%) of HoneyQueries responded
  - Use to generate poisoned path list

Destination	Count	Percentage
CN	388,206	99.80%
CA	363	0.09%
US	127	0.03%
HK	111	0.03%
IN	94	0.02%

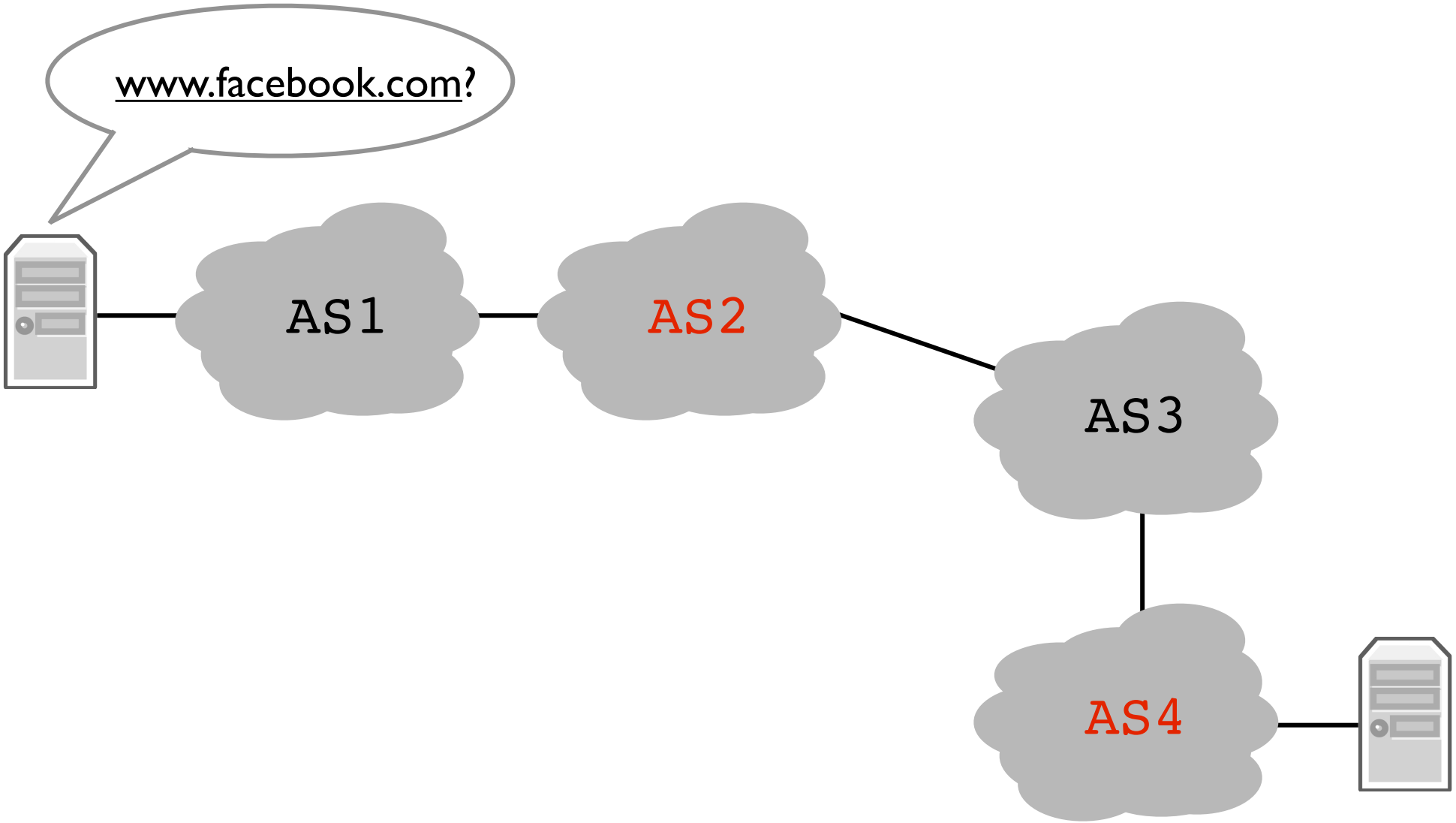
Top 5 of 16 regions

- Why are paths to IP addresses outside of China experiencing DNS injection?

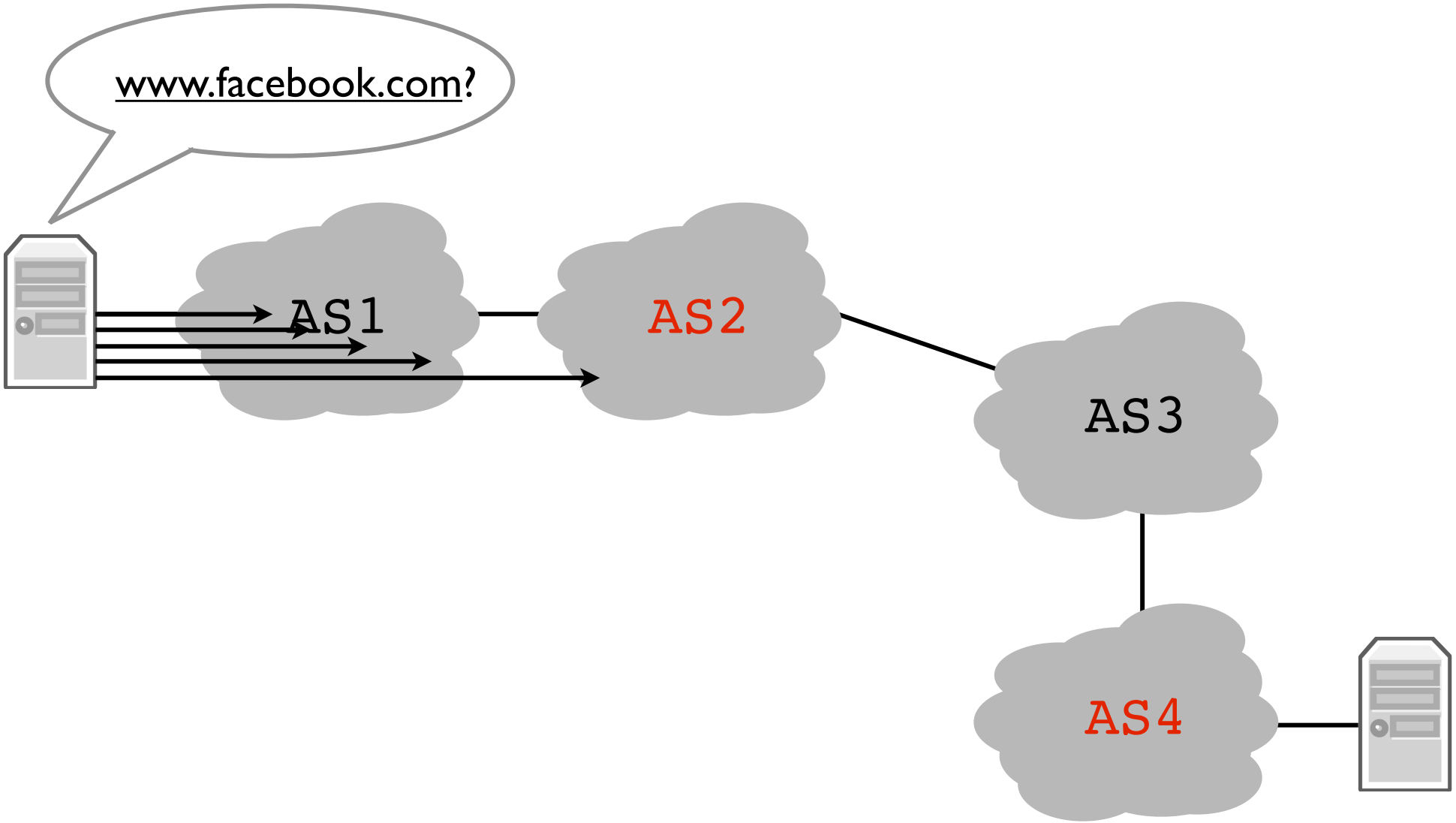
TraceQuery

- For each IP address in the poisoned path list, send a DNS query to a blacklisted domain with increasing TTL
  - Queries which reach an injector will trigger a response
- Mark IP address and autonomous system of router for TTL that triggers response
  - Sometimes queries trigger multiple responses, from multiple injectors

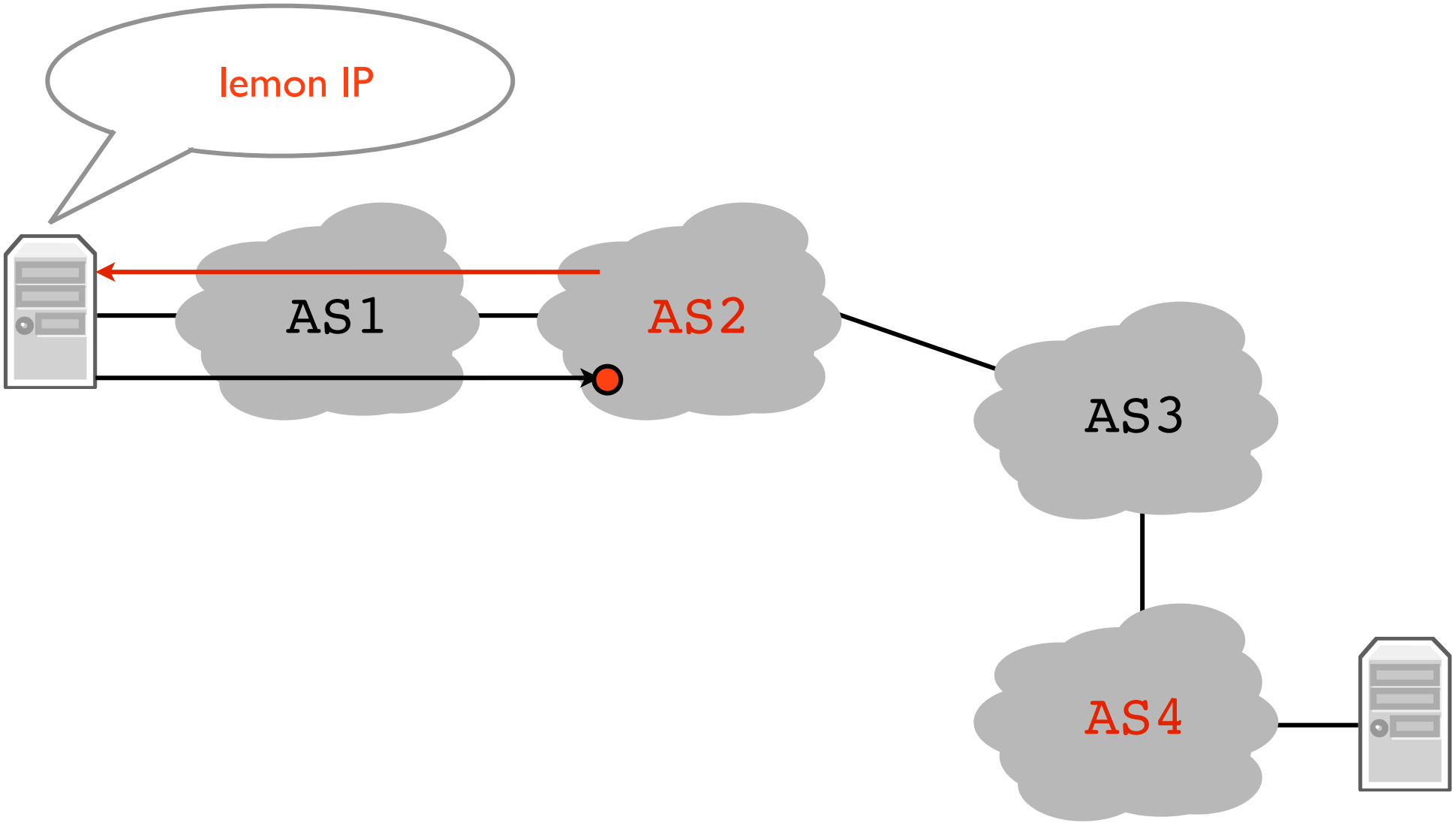
Example



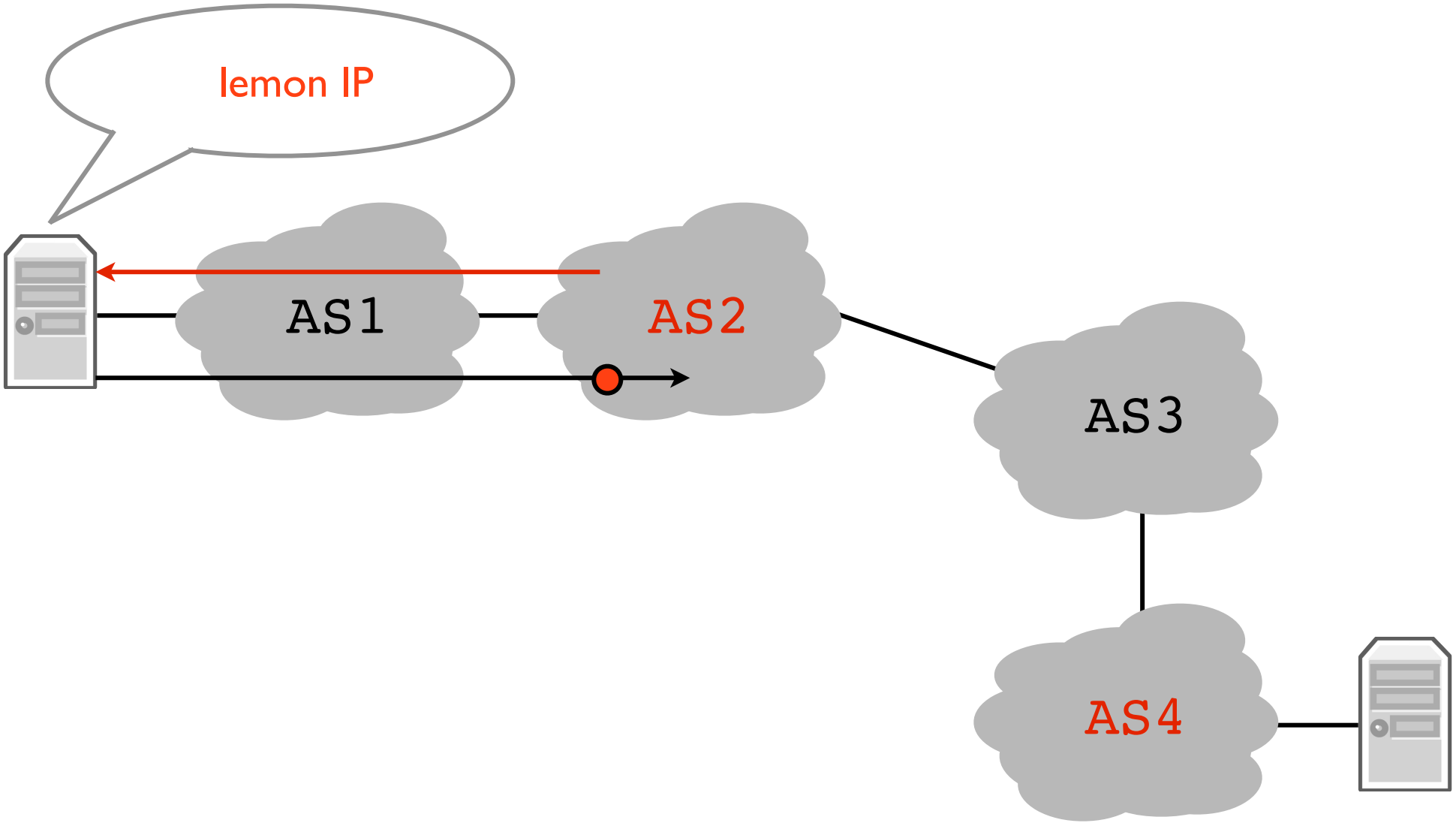
Example



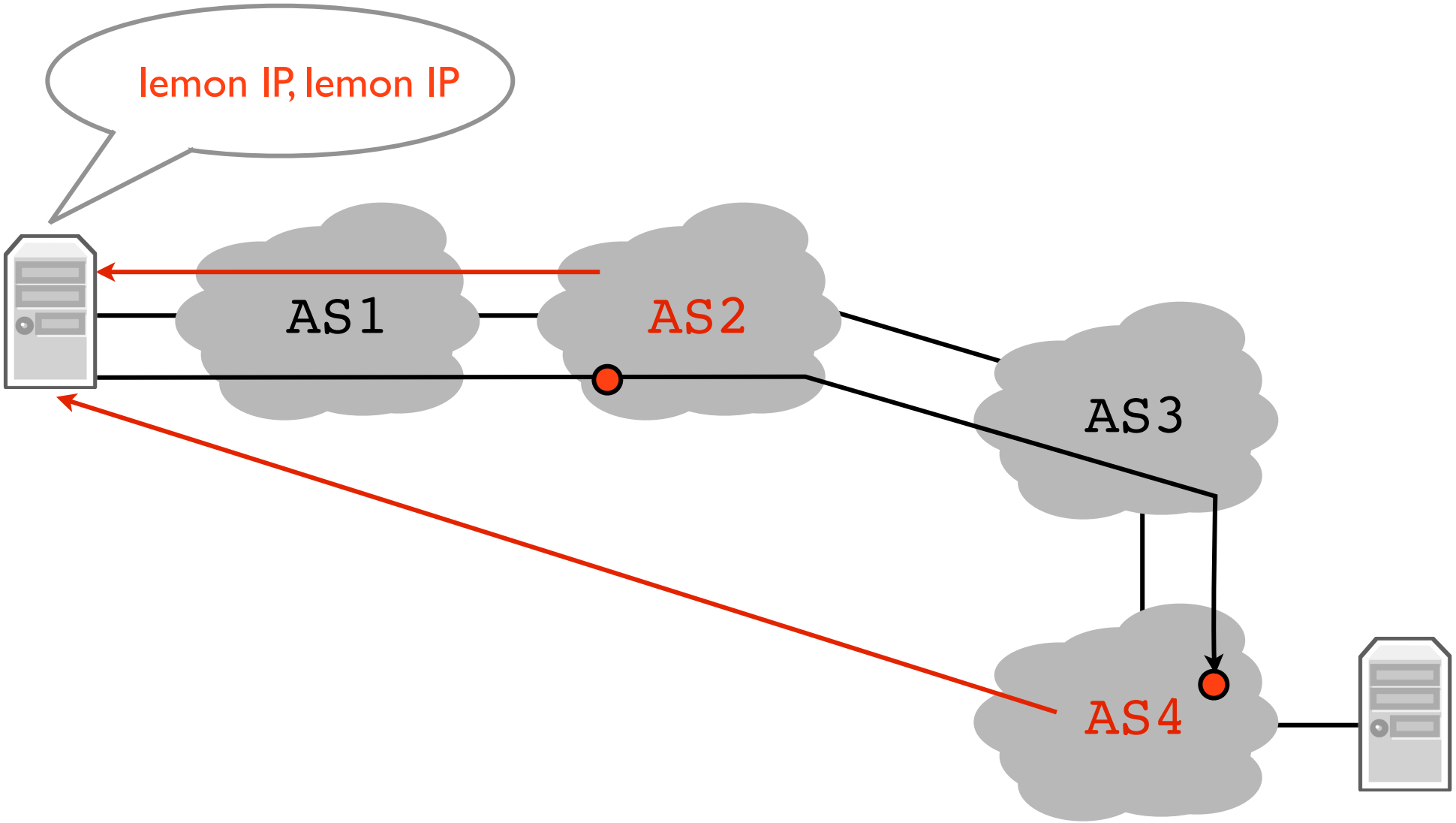
Example



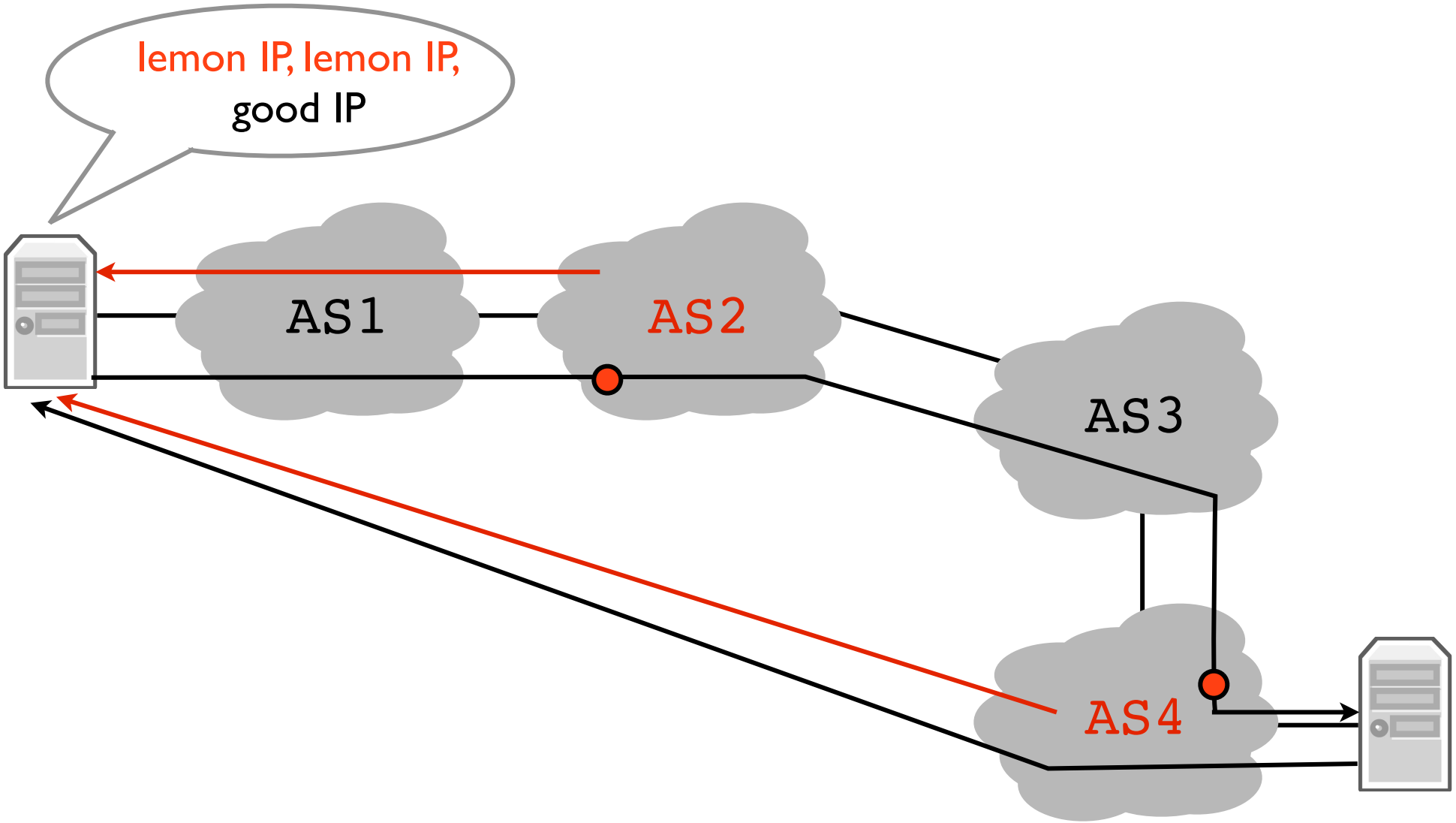
Example



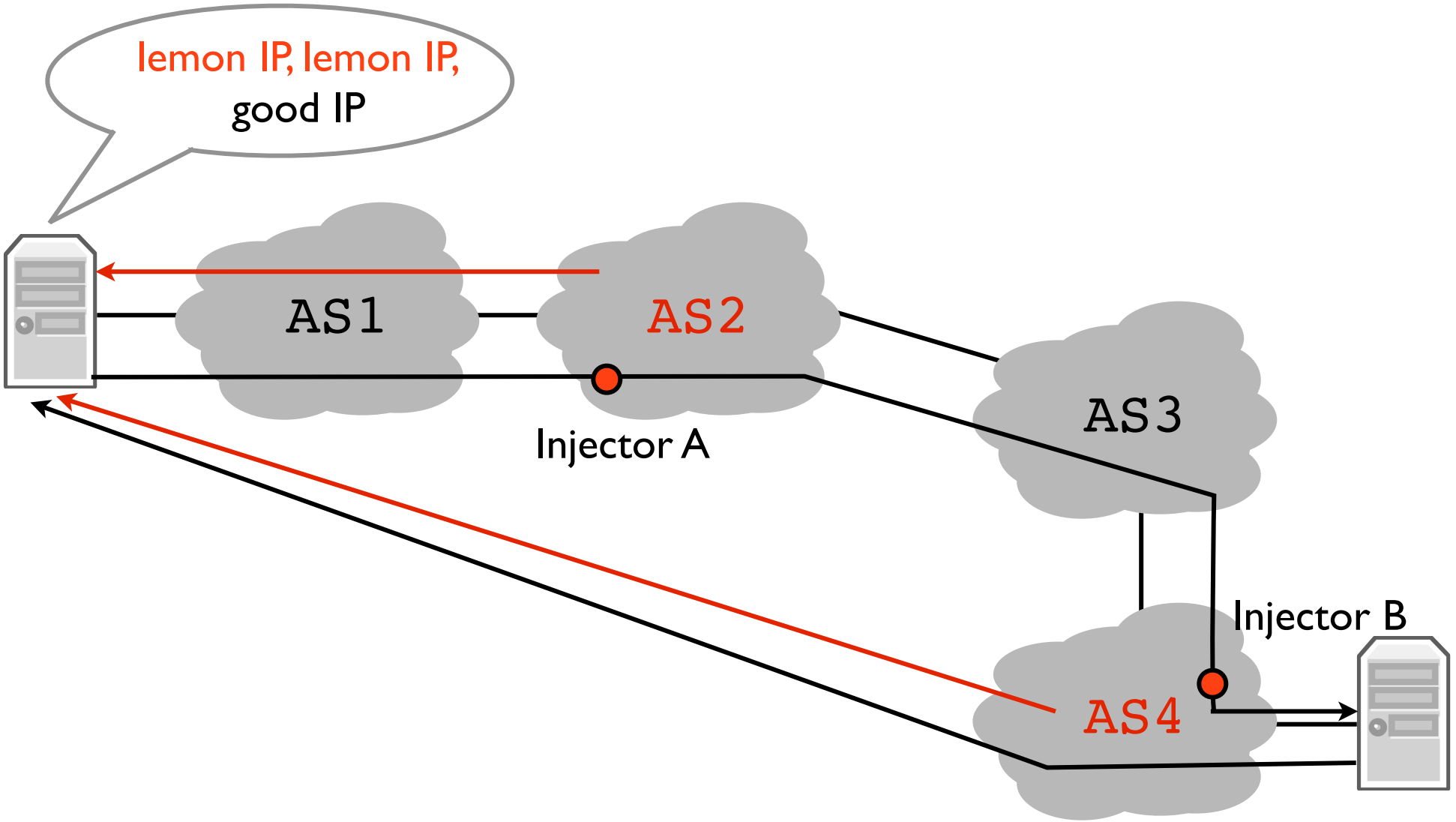
Example



Example



Example


lemon IP, lemon IP,
good IP
AS1
AS2
Injector A
AS3
Injector B
AS4

TraceQuery Results

- Found 3,120 router IP addresses associated with DNS injection
- All 3,120 IP addresses belong to 39 Chinese autonomous systems

AS Name	AS Number	IPs
Chinanet	4134	1952
CNCGroup China169 Backbone	4837	489
China Telecom (Group)	4812	289
CHINA RAILWAY Internet (CRNEt)	9394	78
China Netcom Corp.	9929	67

Top 5 ASes by router IP count

- How much does this affect the Internet?

Methodology

- Tested 43,842 open DNS resolvers in 173 countries outside of China
  - List from probing DNS servers of Alexa 1M top websites
  - Supplemented by lists from researchers
- Query for blacklisted domain from vantage point, check if response is lemon IP
  - Test blacklisted name for all 312 TLDs
  - Also, check against TCP-based DNS queries (injectors do not target DNS queries over TCP)

StepNX Query

- To identify *where* injection occurs, inject random strings into domain name
  - Injectors use very liberal pattern matching
  - Generate invalid names, expect NXDOMAIN response
  - www.facebook.com.{INVALID}: path to root server
  - www.facebook.com.{INVALID}.com: path to TLD server
  - Repeat 200 times to try different servers/paths

DNS Level	Affected Resolvers	Affected Rate
Root	1	0.002%
TLD	11573	26.4%
Authoritative	99	0.23%

Which resolution step sees injection

StepNX Query

- To identify *where* injection occurs, inject random strings into domain name
  - Injectors use very liberal pattern matching
  - Generate invalid names, expect NXDOMAIN response
  - www.facebook.com.{INVALID}: path to root server
  - www.facebook.com.{INVALID}.com: path to TLD server
  - Repeat 200 times to try different servers/paths

DNS Level	Affected Resolvers	Affected Rate
Root	1	0.002%
TLD	11573	26.4%
Authoritative	99	0.23%

Which resolution step sees injection

Who's Affected?

- 3 TLDs affected almost completely (99.53%)
  - cn, xn--fiqs8s, xn--fiqz9s
  - Expected: domains from within Great Firewall of China
- 11,573 (26.4%) of resolvers affected for one or more of 16 unexpected TLDs

TLD	Affected Resolvers
de	8192
xn--3e0b707e	5641
kr	4842
kp	384
co	90
travel	90
pl	90
no	90
iq	90
hk	90
fi	90
uk	90
xn--j6w193g	90
jp	90
nz	90
ca	90

16 unexpected TLDs affected by DNS injection on path from an open resolver

Whose Resolvers?

Open resolvers in 109 regions affected

Region	Affected Resolvers	Percentage
Iran	157	88%
Myanmar	163	85%
Korea	198	79%
Hong Kong	403	75%
Taiwan	1146	66%
India	250	60%

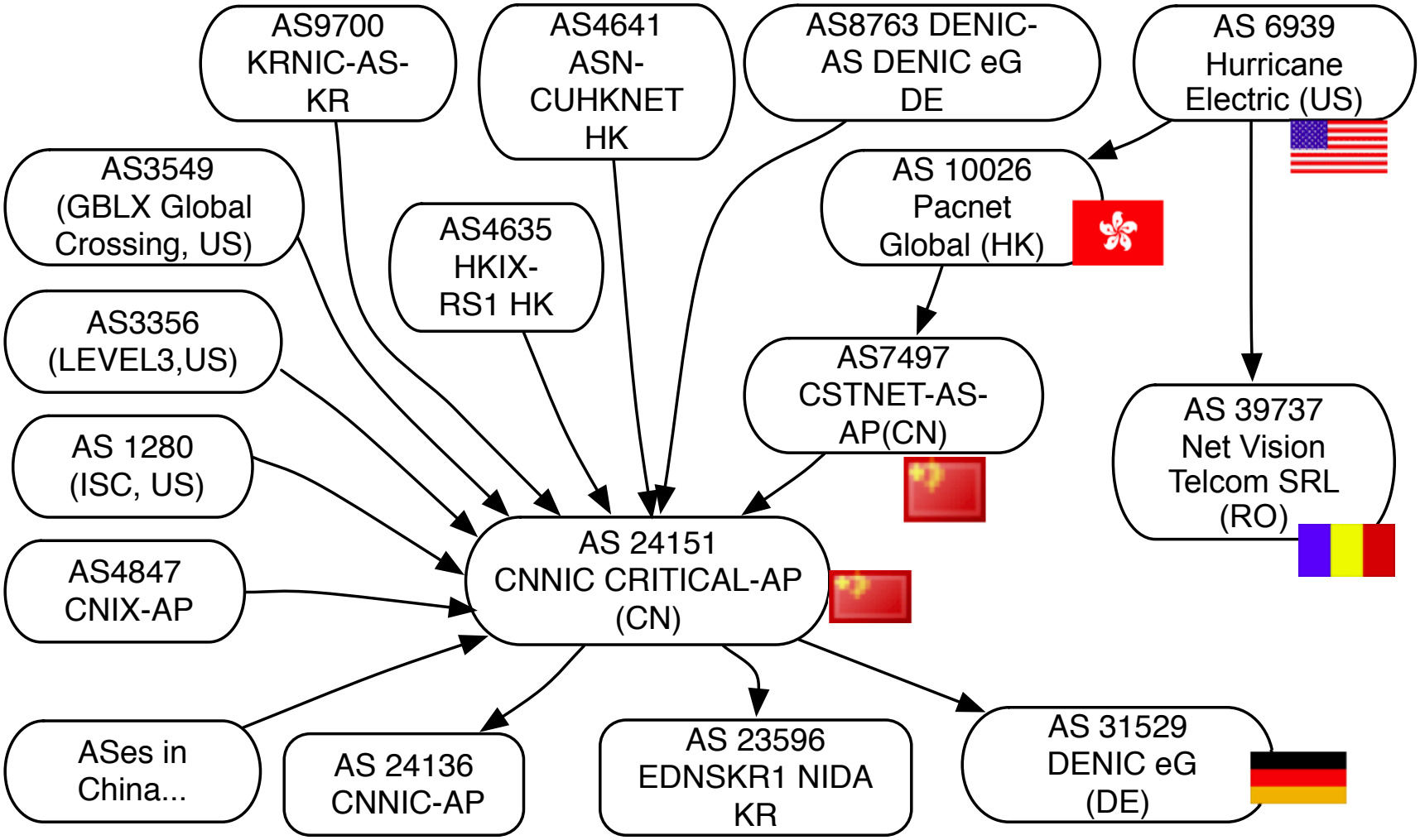
Top 6 regions by affected open resolver percentage

Details: .de

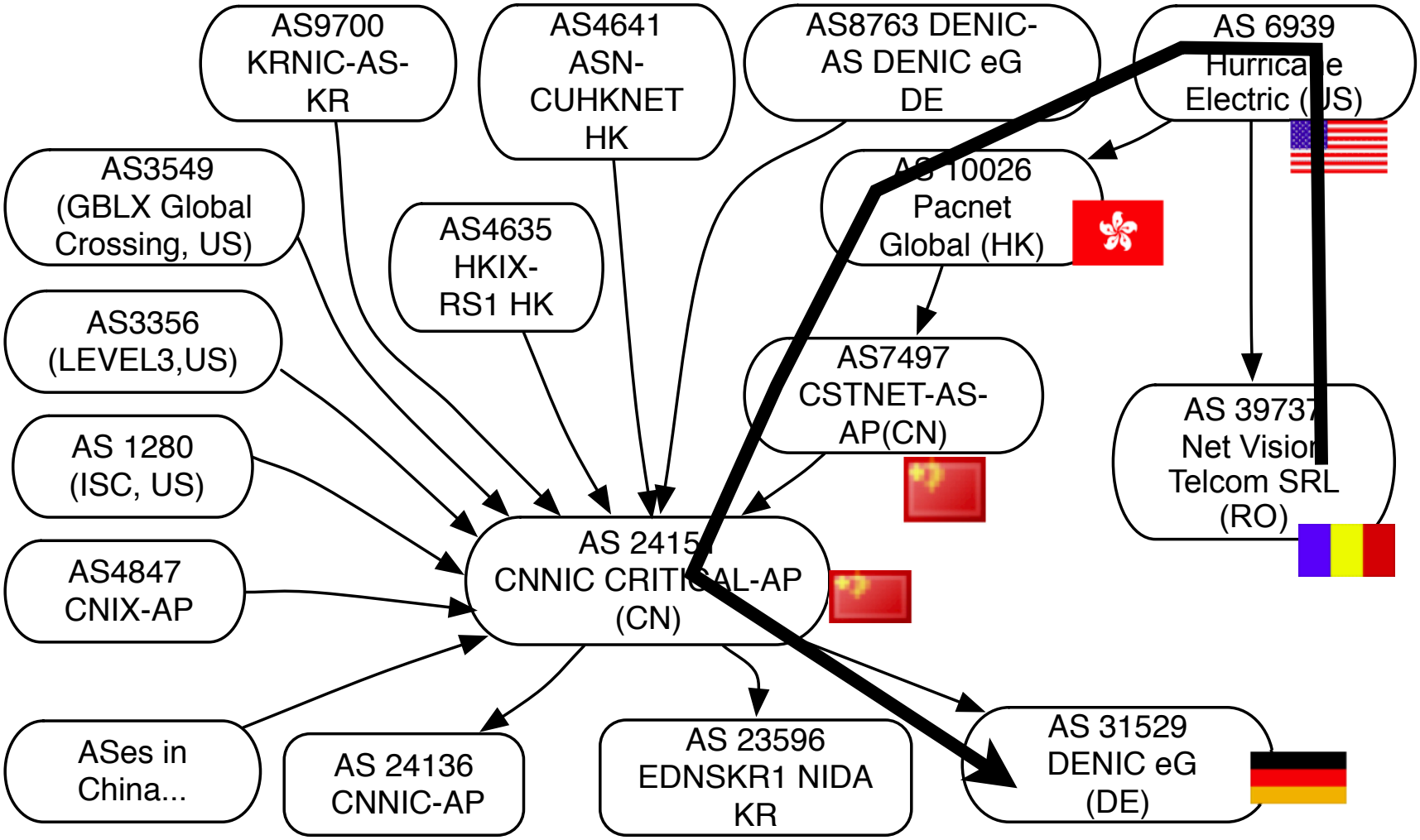
Region	Resolvers Affected
kr	76%
my	66%
hk	54%
ar	44%
il	42%
ir	36%
tw	36%
bg	31%
jp	28%
ro	25%

10 regions whose open resolvers are most greatly affected for .de queries

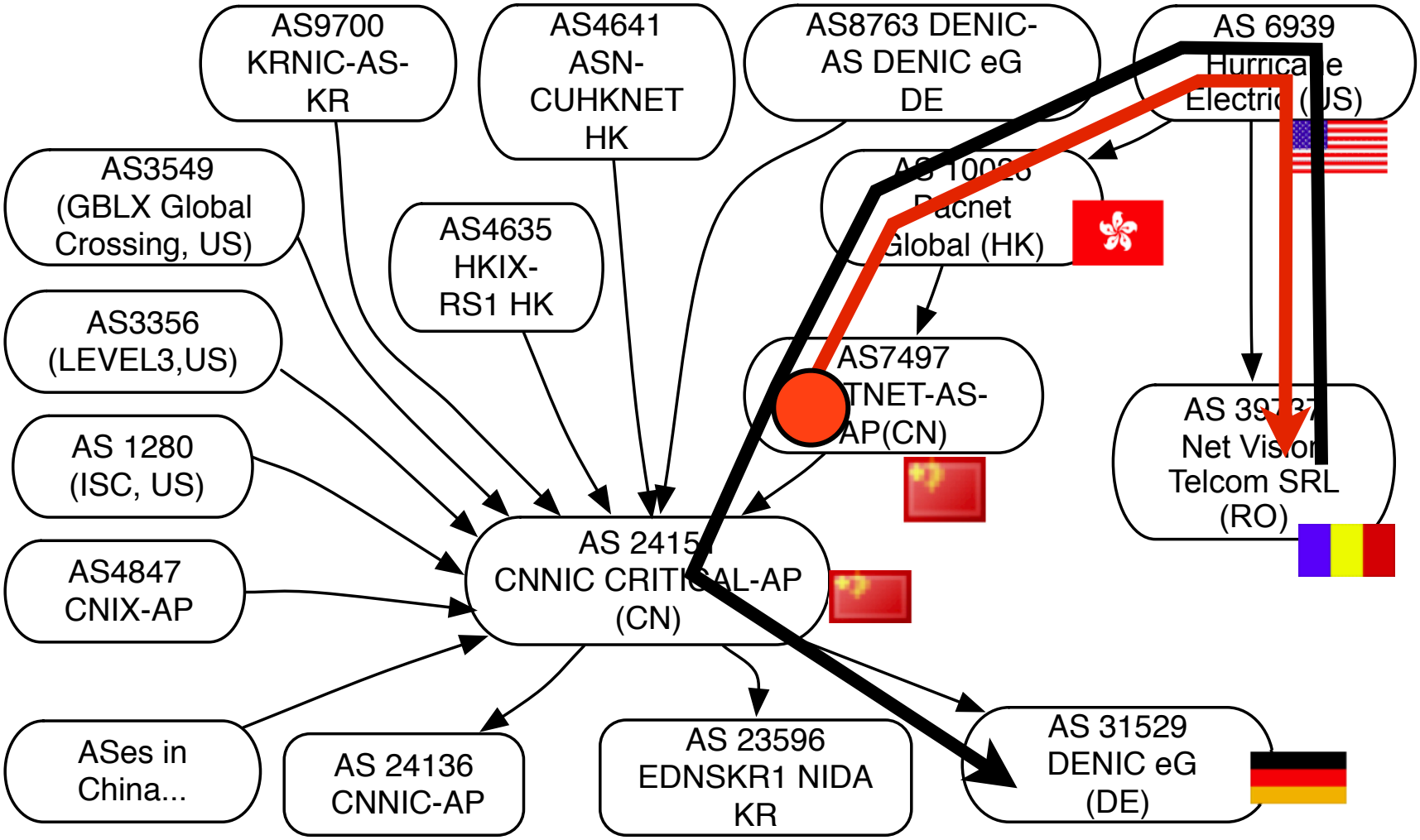
Example .de Injection



Example .de Injection



Example .de Injection



Solutions

- DNS injectors could filter out transit queries
- Autonomous systems could avoid transit through injecting neighbors
  - Particularly, TLD operators could monitor peering paths
- Security extensions for DNS (DNSSEC) prevent injection
  - DNSSEC has signed responses
  - Resolvers would reject injected responses, accept slower ones from authoritative servers
  - .de and .kr both support DNSSEC

Conclusion

- Great Firewall of China's DNS injection is affecting lookups originating outside China
  - Caused by queries traversing Chinese ASes
  - Effect is greatest at routes between resolvers and TLDs
- Suggestions on preventing collateral damage
- Some recent changes...

Questions

please contact

Anonymous <zion.vlab@gmail.com>