Improving Privacy for GeoIP DNS Traffic

Pan Lanlan(潘蓝兰)

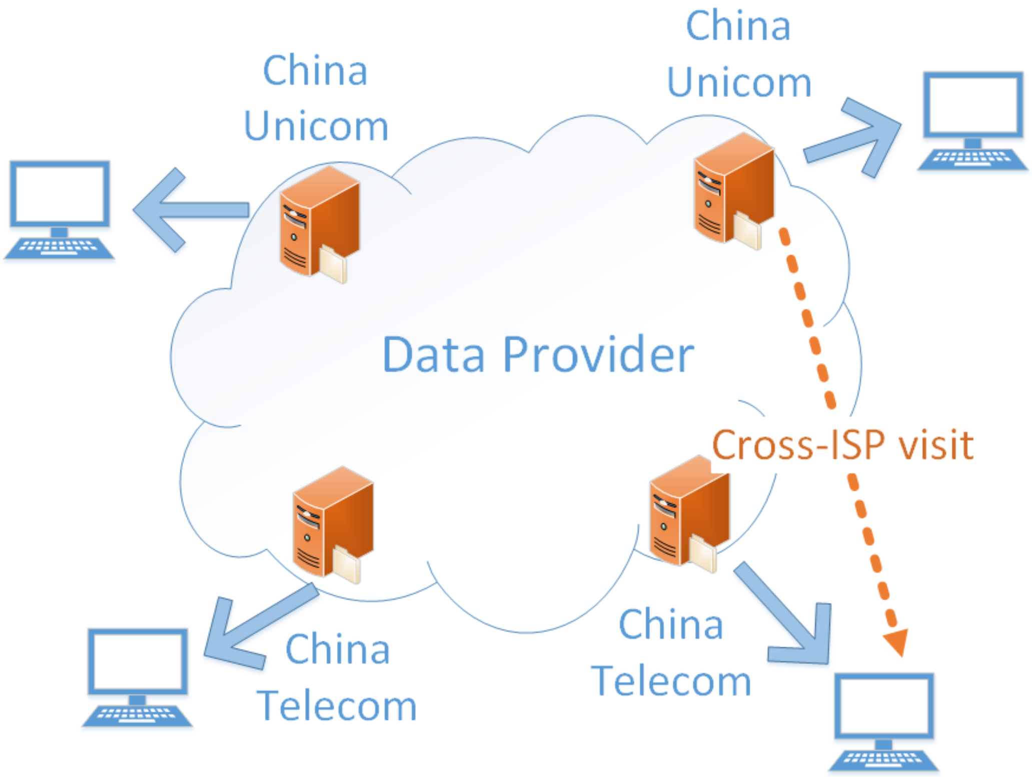
abbypan@gmail.com

Geely Automobile Research Institute, China

QSHINE 2018

Bring the content as close to the users as possible

Return tailor IP to users, avoid high latency cross-isp visit.

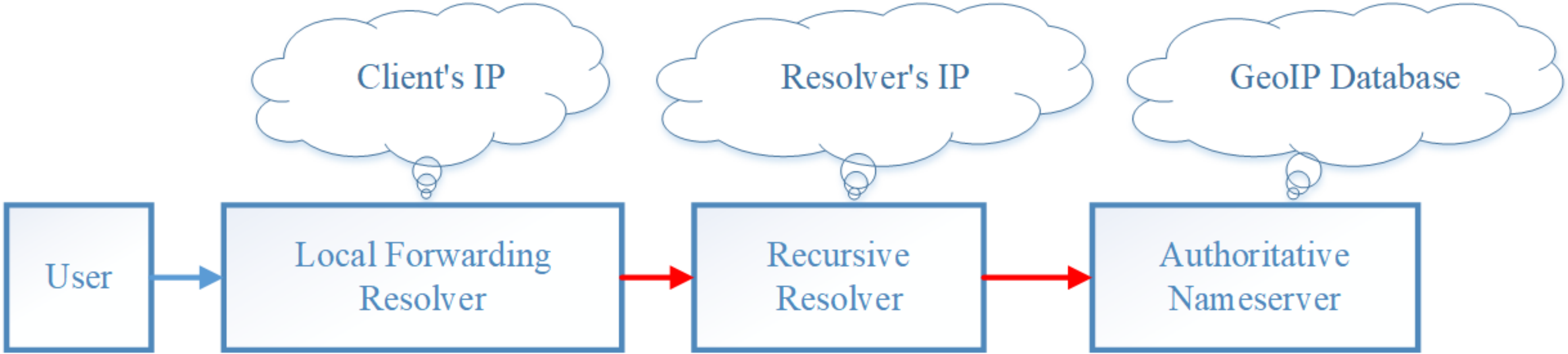


GeoIP DNS Traffic

Authoritative Nameserver return tailor IP based on perceived geographical location of the resolver’s IP address (Resolver’s GeoIP information).

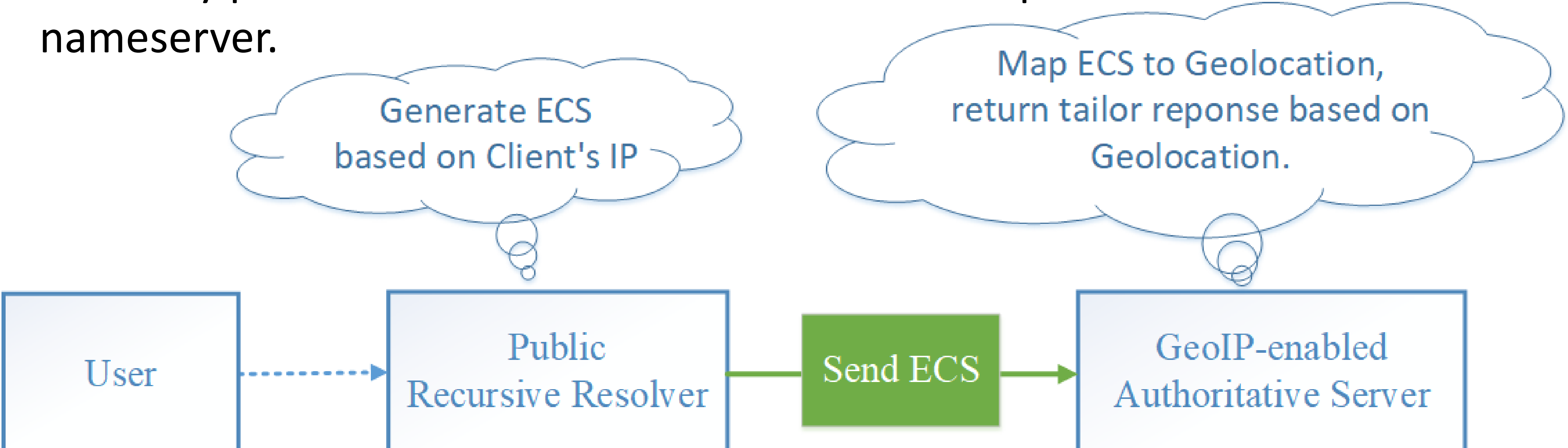
1) Proximity IP Problem: Is the resolver's IP address close enough to the client's IP address?

2) GeoIP Database Problem: Does the authoritative nameserver use an GeoIP database with high quality?



ECS extension : Client Subnet

Proximity IP Problem: Public recursive resolvers such as GoogleDNS and OpenDNS are not close enough to many users since they couldn't deploy servers among each country and each ISP's network.
ECS carry part of the client's IP address in the DNS packets for authoritative nameserver.

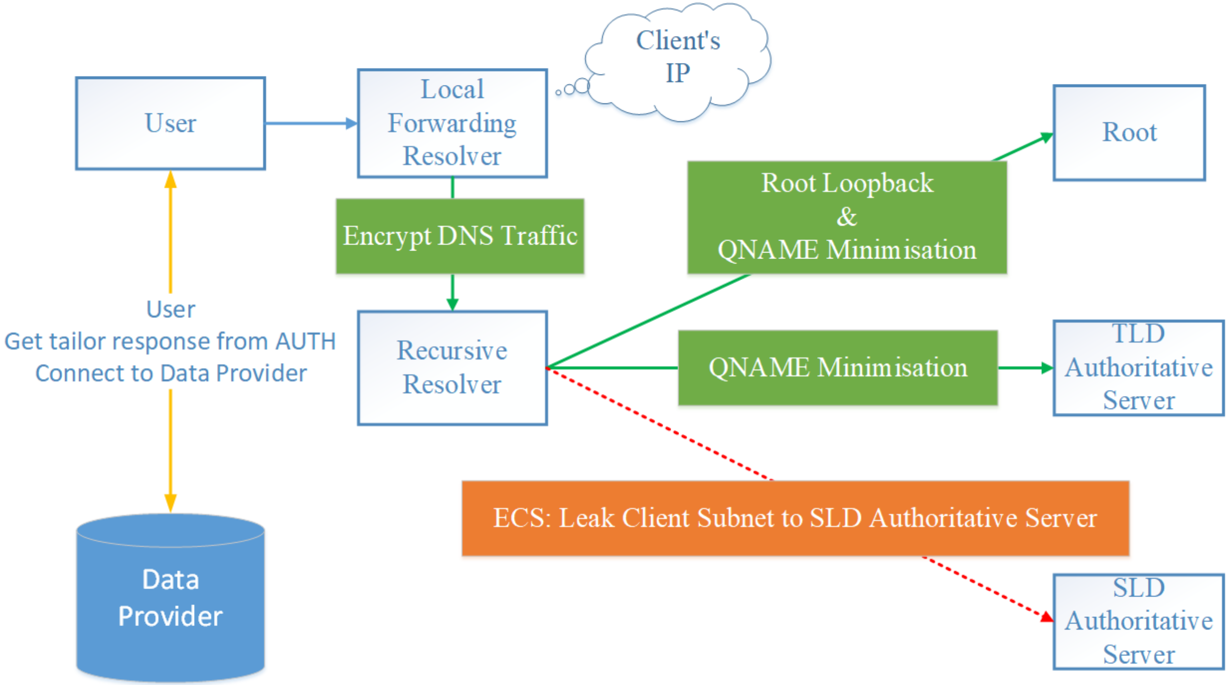


Generate ECS based on Client's IP
Map ECS to Geolocation, return tailor reponse based on Geolocation.
User
Public Recursive Resolver
Send ECS
GeoIP-enabled Authoritative Server

DNS Privacy, ECS(client subnet)

ECS mitigate Proximity IP Problem of public recursive resolver.

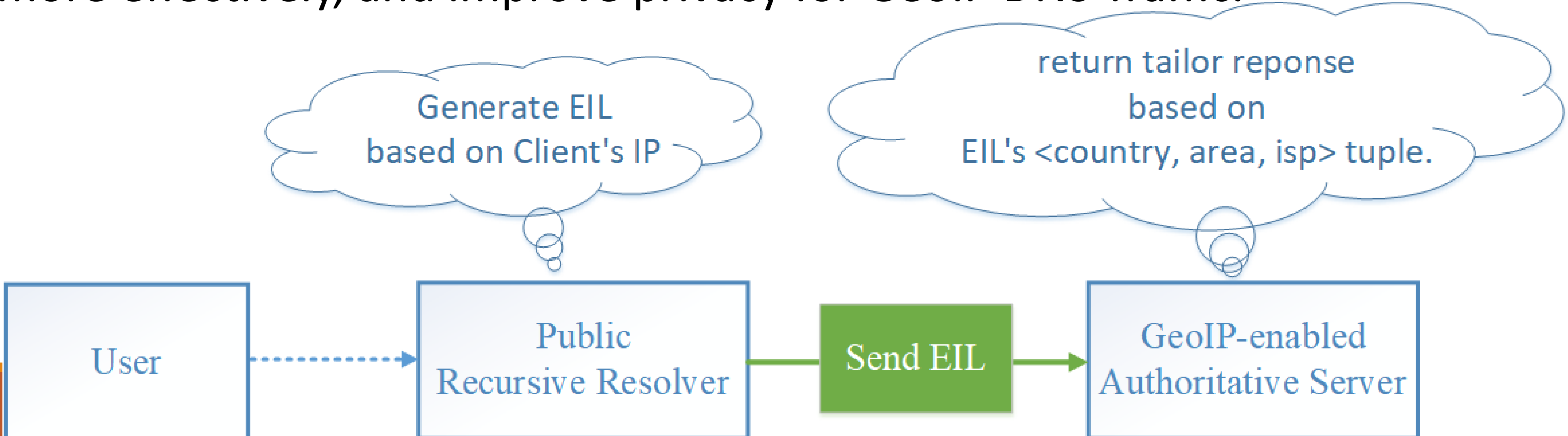
ECS leaks client subnet information on the resolution path to the authoritative nameserver.



EIL: <COUNTRY, AREA, ISP>

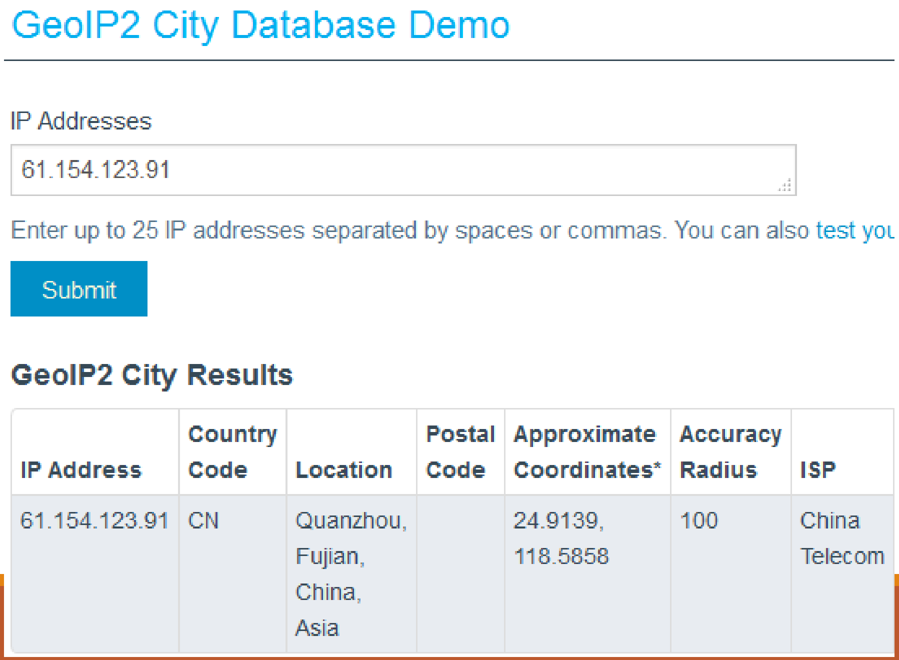
To find the right balance between privacy improvement and end-user experience optimization, EIL includes the GeoIP information of client’s IP in DNS packets, not client subnet information.

EIL can counter the proximity IP problem and GeoIP database problem more effectively, and improve privacy for GeoIP DNS Traffic.



EIL Structure: <COUNTRY, AREA, ISP>
<CN, 35, TEL> indicates <China, Fujian, China Telecom>

Compared to ECS’s client subnet such as 61.154.123.0/20,
EIL contains very few sensitive information because it is associated with a very broad geographic area.



GeoIP2 City Database Demo

IP Addresses

61.154.123.91

Enter up to 25 IP addresses separated by spaces or commas. You can also test you

GeoIP2 City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP
61.154.123.91	CN	Quanzhou, Fujian, China, Asia		24.9139, 118.5858	100	China Telecom

Privacy Improvement

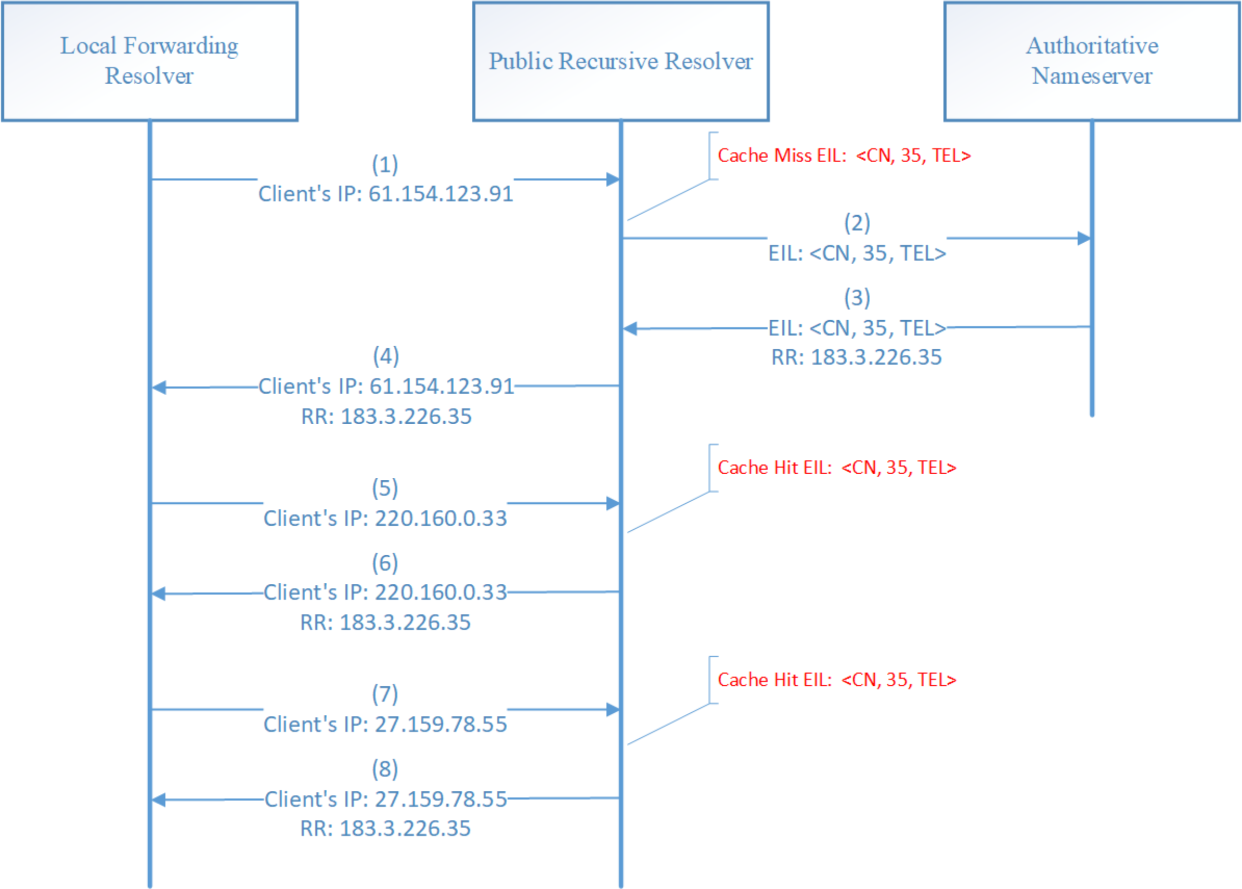
EIL replaces the sensitive client subnet information to aerial view GeoIP information for user privacy protection.

The GeoIP information is generated from Client's IP, not from user's physical geolocation.

Since EIL's GeoIP information covers much bigger area than ECS's client subnet information, EIL will be stronger at monitoring targeted DNS censorship attack.

Increase Cache-hit Rate of Recursive Resolver

Each EIL GeoIP information covers huge amounts of client subnets.



Local Forwarding Resolver

Public Recursive Resolver

Authoritative Nameserver

Cache Miss EIL: <CN, 35, TEL>

(1)
Client's IP: 61.154.123.91

(2)
EIL: <CN, 35, TEL>

(3)
EIL: <CN, 35, TEL>
RR: 183.3.226.35

(4)
Client's IP: 61.154.123.91
RR: 183.3.226.35

Cache Hit EIL: <CN, 35, TEL>

(5)
Client's IP: 220.160.0.33

(6)
Client's IP: 220.160.0.33
RR: 183.3.226.35

Cache Hit EIL: <CN, 35, TEL>

(7)
Client's IP: 27.159.78.55

(8)
Client's IP: 27.159.78.55
RR: 183.3.226.35

Experiment

We totally collect 910.9K Chinese IPv4 CIDR/24 subnets for experiment, which cover top 3 China ISPs and 31 Areas.
For each subnet, we send the ECS query for www.qq.com to authoritative nameserver 123.151.66.83, get the tailor response, and analyze the GeoIP information.

For TEL ISP, 28 areas can enable EIL, which covered 479.9K subnets, 96.40245%.
For UNI ISP, 26 areas can enable EIL, which covered 234.0K subnets, 85.92825%.
For MOB ISP, 27 areas can enable EIL, which covered 66.3K subnets, 47.10294%.
We can find that responses for MOB ISP are not as steady as TEL ISP and UNI ISP, in this case, 4 areas reserve ECS query can help for website traffic optimization. 11(Beijing), 32(Jiangsu), 31(Shanghai), 14(Shanxi).

Details

More details are shown in:
https://github.com/abbypan/dns_test_eil
https://datatracker.ietf.org/doc/draft-pan-dnsop-edns-isp-location/

Thank You

Questions ?