EIL
Dealing with the Privacy Problem of ECS

潘蓝兰 Pan Lanlan

abbypan@gmail.com

CNNIC

Agenda

- CDN , ECS and DNS Privacy
- EIL : Structure
- EIL : Deployment Model
- EIL: Privacy and Security
- Future Work

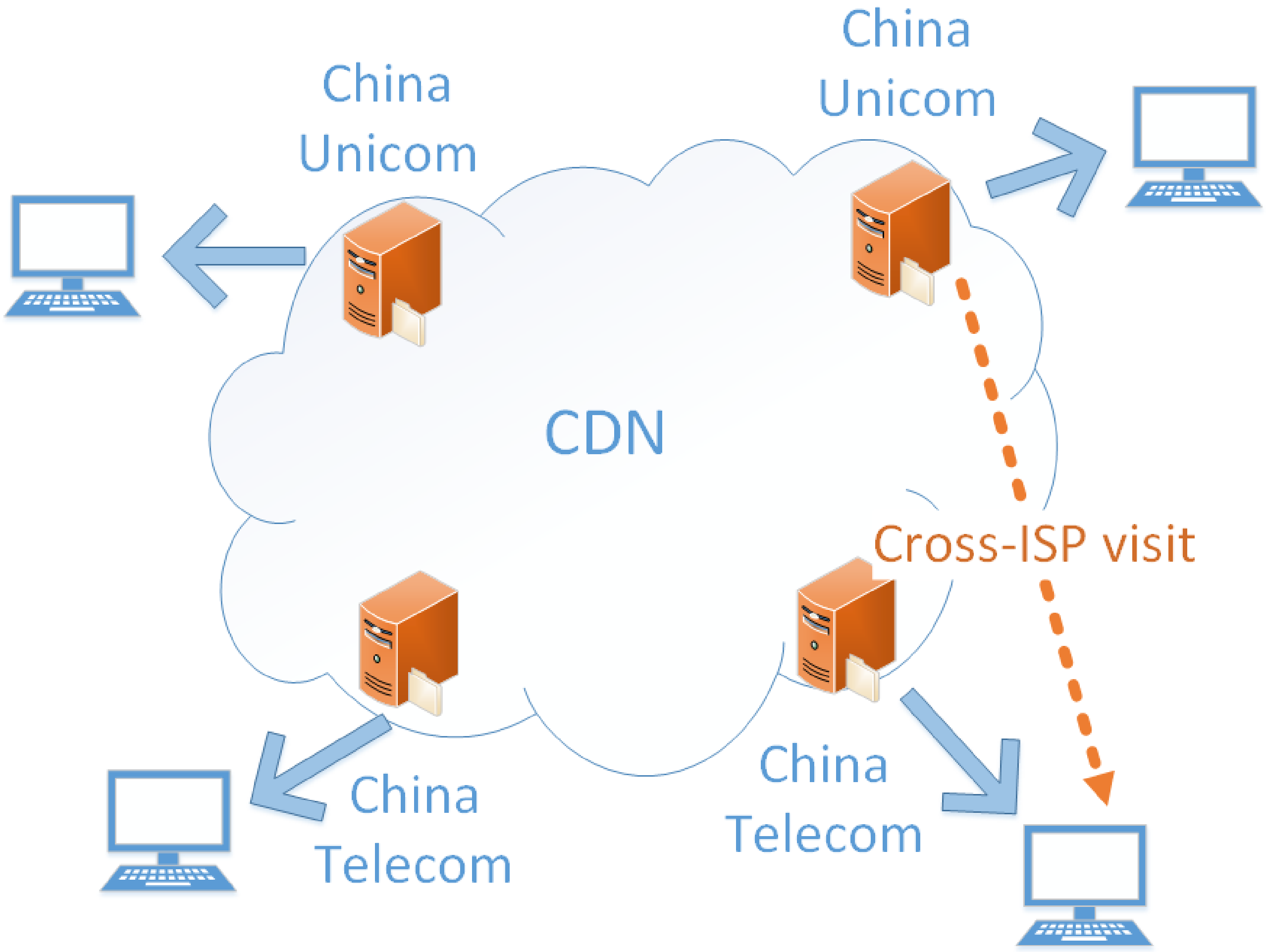
CDN , ECS and DNS Privacy

CDN

- CDN : make end user to visit the closest edge server.
- IP anycast is expensive.

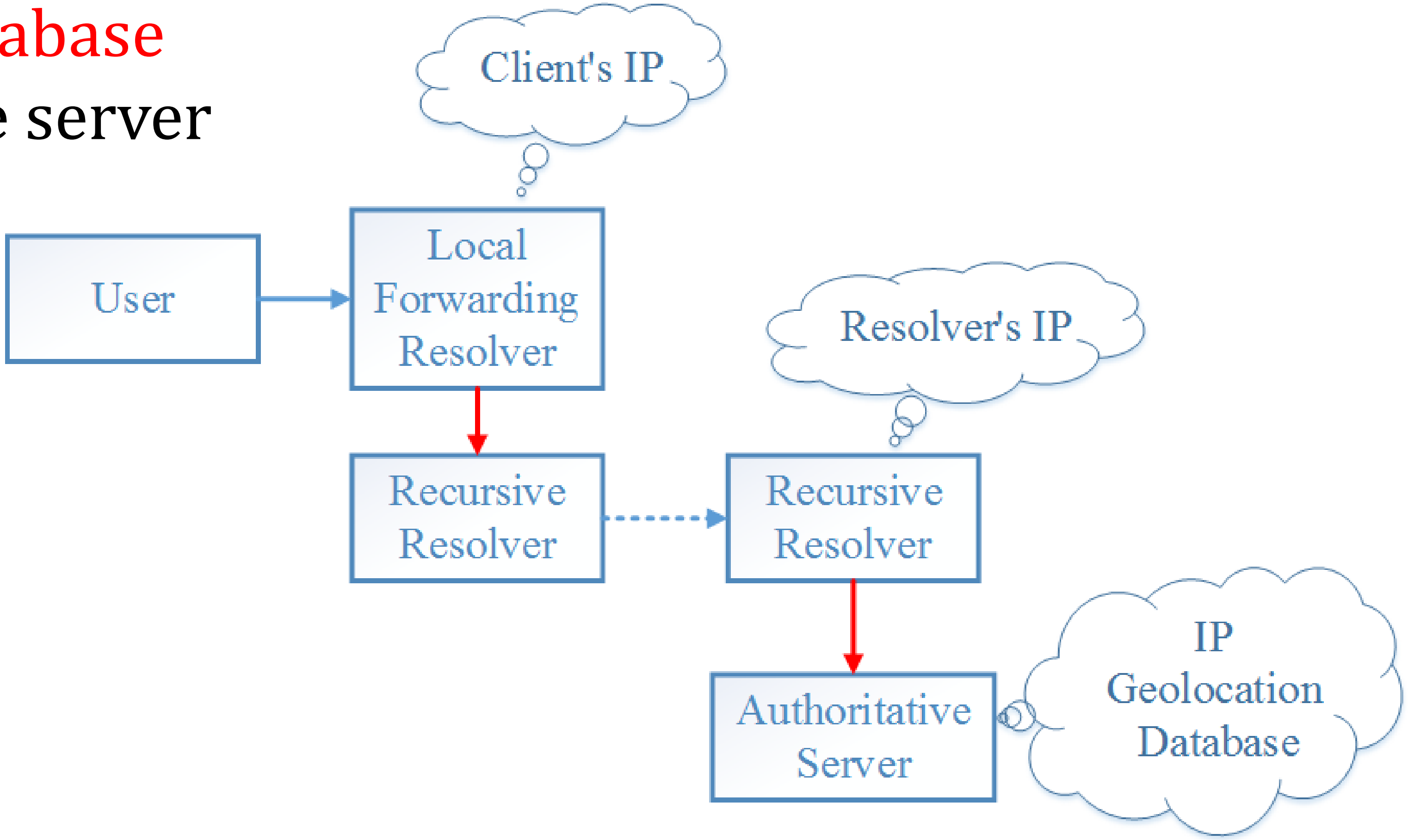
  Use DNS load balancing.
- IP transit is expensive.

  Avoid cross-ISP visit.



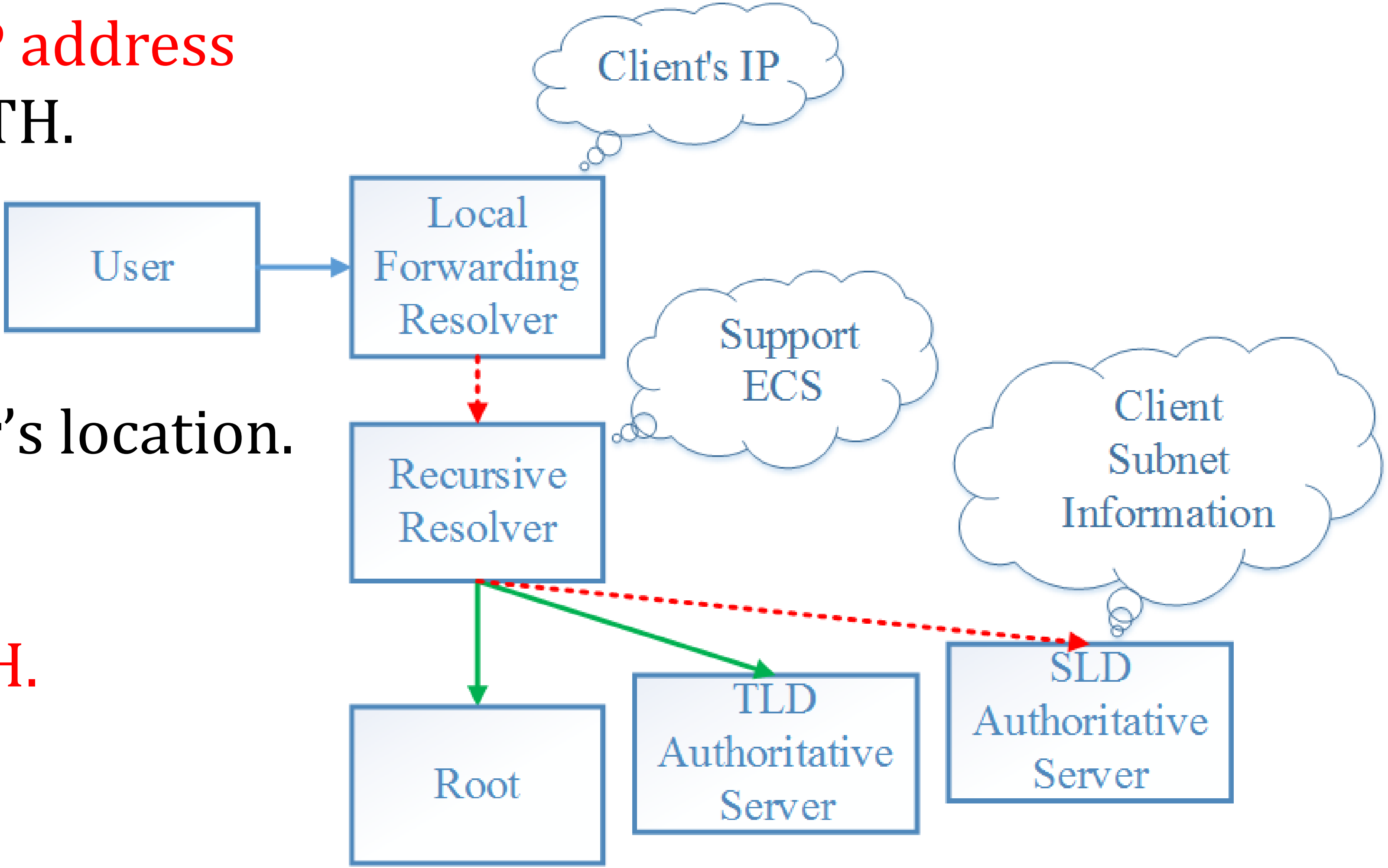
Quality of DNS Load Balancing

- Is the resolver's IP address close to the client's IP address?
- Is the IP geolocation database used by the authoritative server with high quality?



ECS

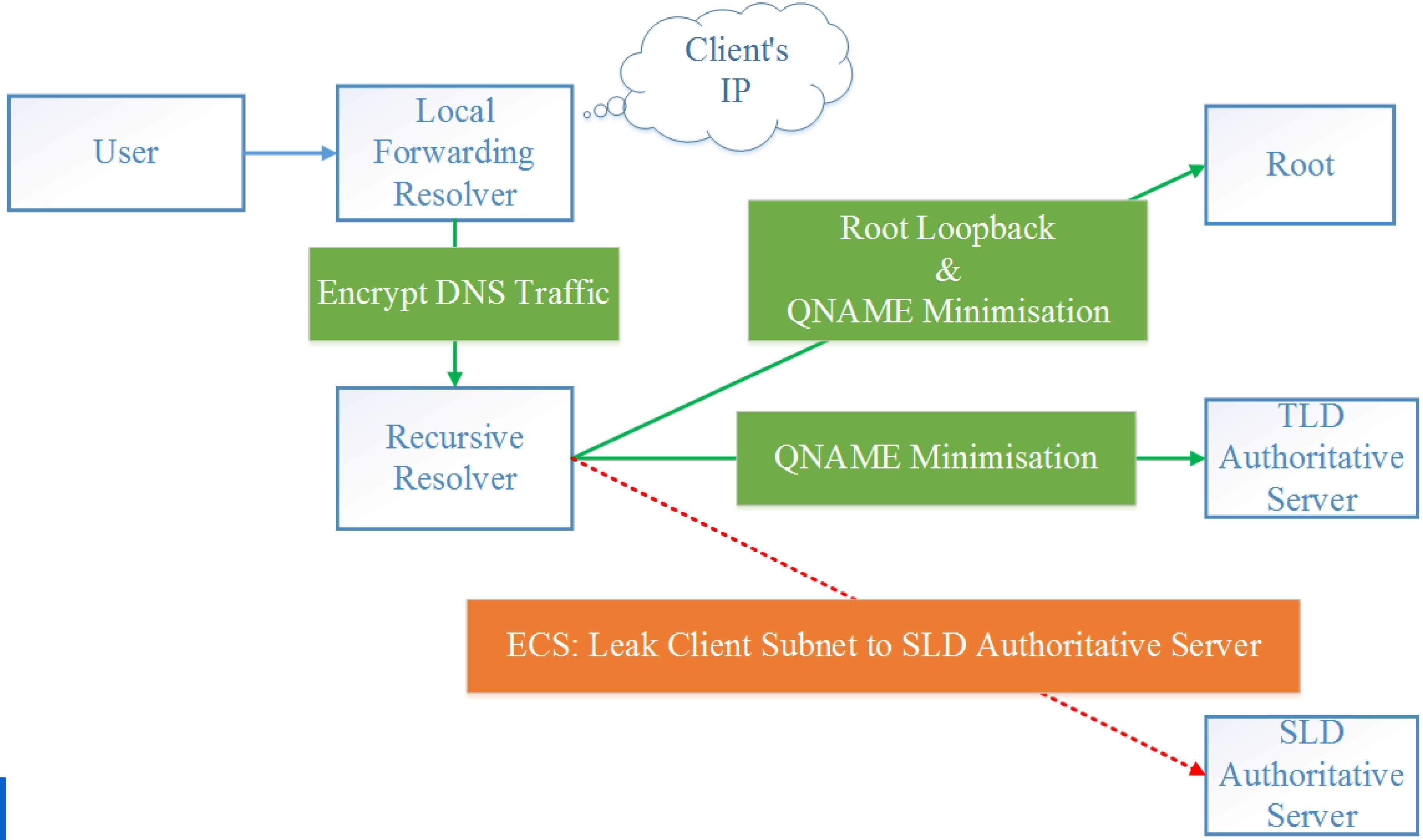
RFC7871 proposes ECS to
carry part of the client's IP address
in the DNS packets for AUTH.



Good:
Better determine end user's location.

Bad:
Leak client subnet to AUTH.

Who (client's IP) has visited Which (QNAME) domain?



User

Local Forwarding Resolver

Client's IP

Encrypt DNS Traffic

Recursive Resolver

Root Loopback & QNAME Minimisation

Root

QNAME Minimisation

TLD Authoritative Server

ECS: Leak Client Subnet to SLD Authoritative Server

SLD Authoritative Server

EIL：Structure

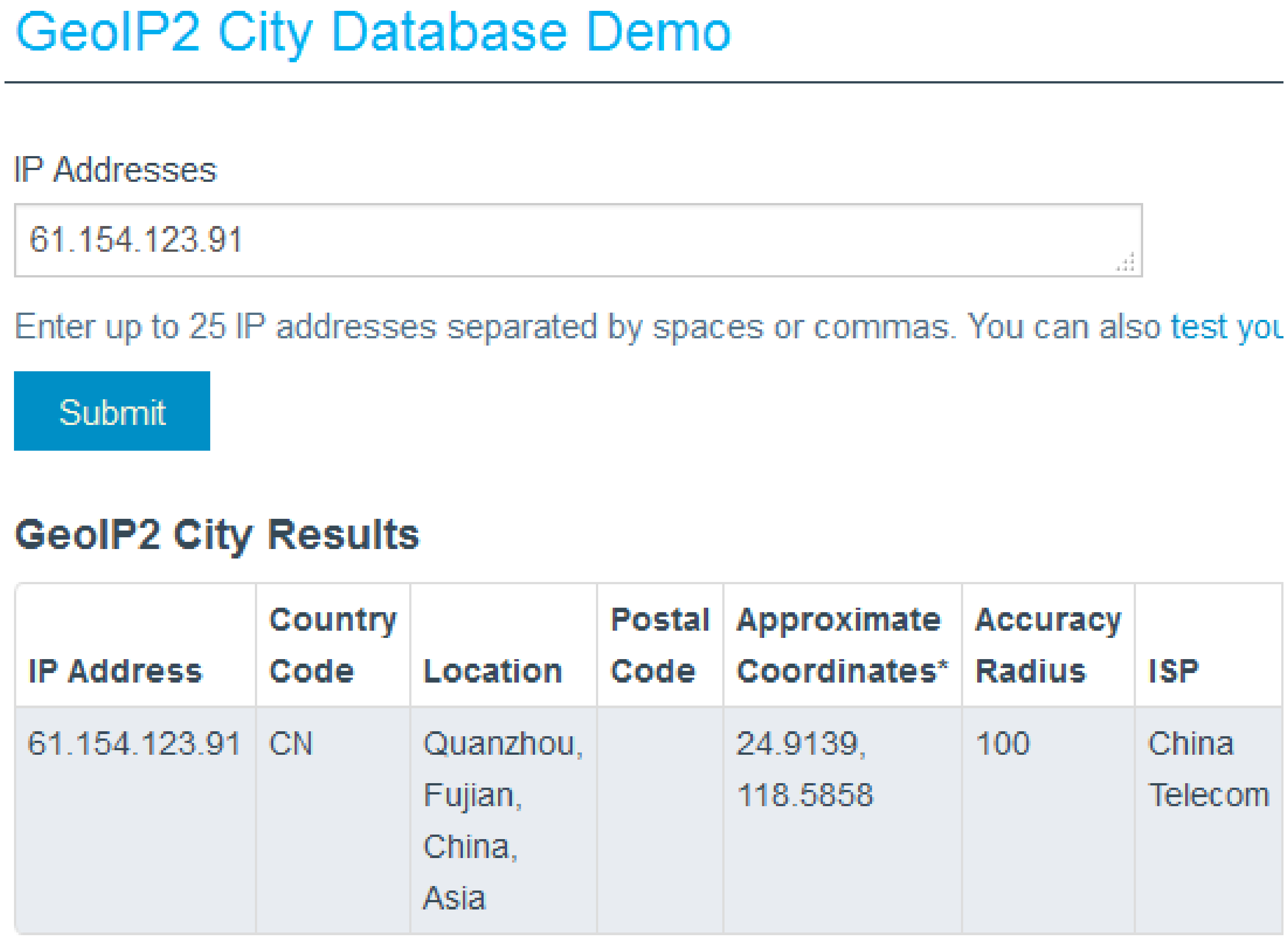
Maxmind Geolocation

client IP 61.154.123.91

Location: Quanzhou, Fujian, China, Asia

Quanzhou is a city in Fujian province.

ISP name: China Telecom



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

EIL: <COUNTRY-CODE, AREA-CODE, ISP>

COUNTRY-CODE: 2 octets

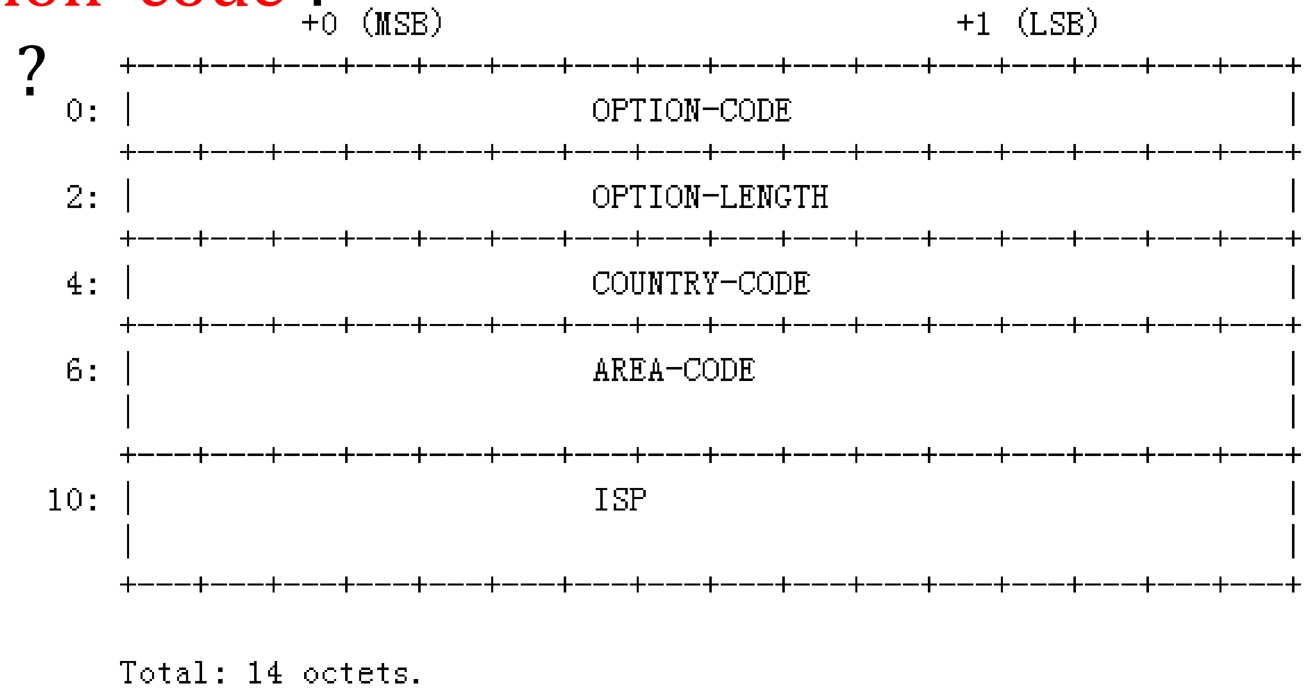
- defined in ISO3166

AREA-CODE: 4 octets （or 6 octets?)

- ISO 3166-2’s country subdivision code ?
- Area code of the phone number ?

ISP: 4 octets

- using shortcut names
- unique in COUNTRY



```
                      +0 (MSB)                          +1 (LSB)
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
   0: |                          OPTION-CODE                          |
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
   2: |                          OPTION-LENGTH                        |
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
   4: |                          COUNTRY-CODE                         |
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
   6: |                          AREA-CODE                            |
      |                                                               |
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  10: |                          ISP                                  |
      |                                                               |
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

      Total: 14 octets.
```

EIL: <COUNTRY-CODE, AREA-CODE, ISP>

Client IP	ECS	EIL
61.154.123.91	61.154.0.0/16	ISO3166: <CN, 35, TEL> Phone Number: <CN, 0591, TEL>
	61.154.123.0/24	Phone Number: <CN, 0595, TEL>

AREA-CODE: ISO 3166-2's country subdivision code ?

- <CN, 35, TEL> indicates <China, Fujian, China Telecom>
- province level precision, ISO standard

AREA-CODE: the phone number ?

- <CN, 0595, TEL> indicates <CHINA, Quanzhou, China Telecom>
- <CN, 0591, TEL> indicates <CHINA, Fujian, China Telecom>
- city level precision, numeric string fuzzy matching(059x)

Response

EIL contains a whitelist for COUNTRY-CODE, AREA-CODE and ISP. maintained by the DNSOP working group ?
https://github.com/abbypan/dns_test_eil/blob/master/eil_loc.json

Authoritative servers that supporting EIL must only response the EIL queries matched the whitelist.

Recursive resolver that supporting EIL must only cache the EIL responses matched the whitelist.

Not-EIL option

Similar to ECS, if all fields in EIL are set to null (0x20) value, means that client doesn’t want to use EIL.

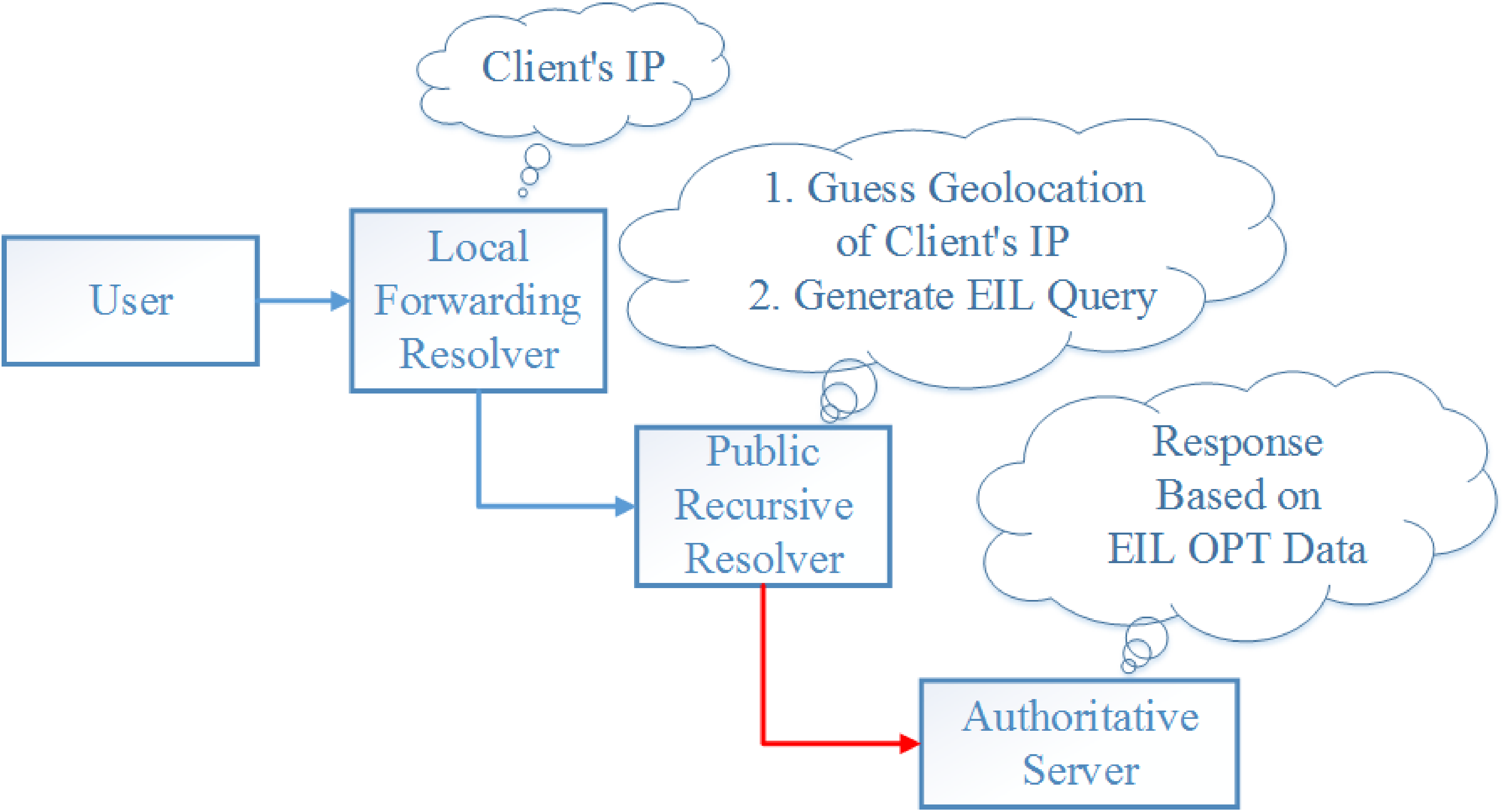
Problem, if the user doesn’t want ECS/EIL:

- not EIL indicates not ECS ?
- a new EDNS option, to ask next-hop recursive resolver not to add any extension like ECS/EIL ?

EIL : Deployment Model

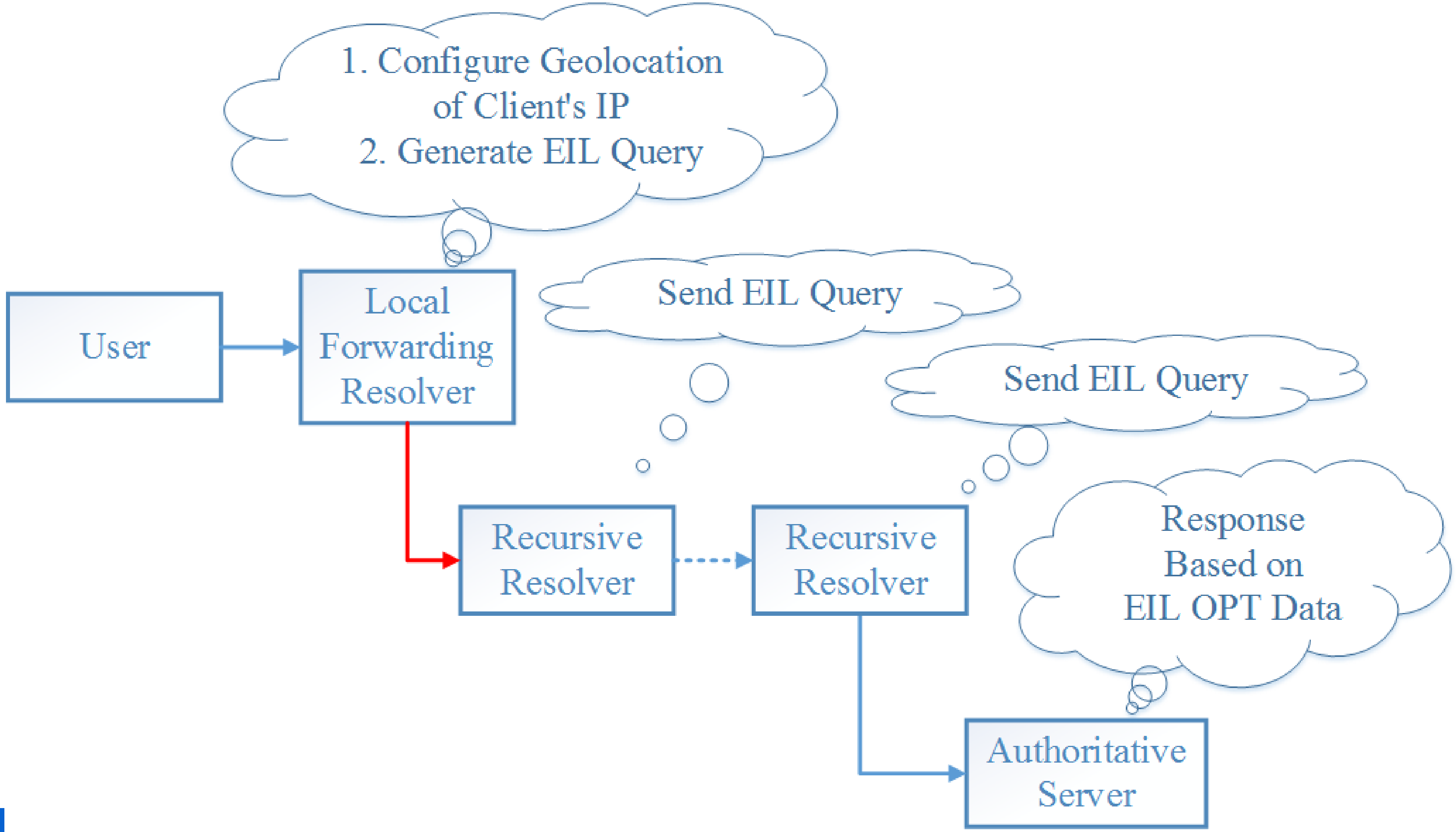
P-model: EIL initiated at public recursive resolver

P-model is close to ECS.


Client's IP
User
Local Forwarding Resolver
1. Guess Geolocation of Client's IP
2. Generate EIL Query
Public Recursive Resolver
Response Based on EIL OPT Data
Authoritative Server

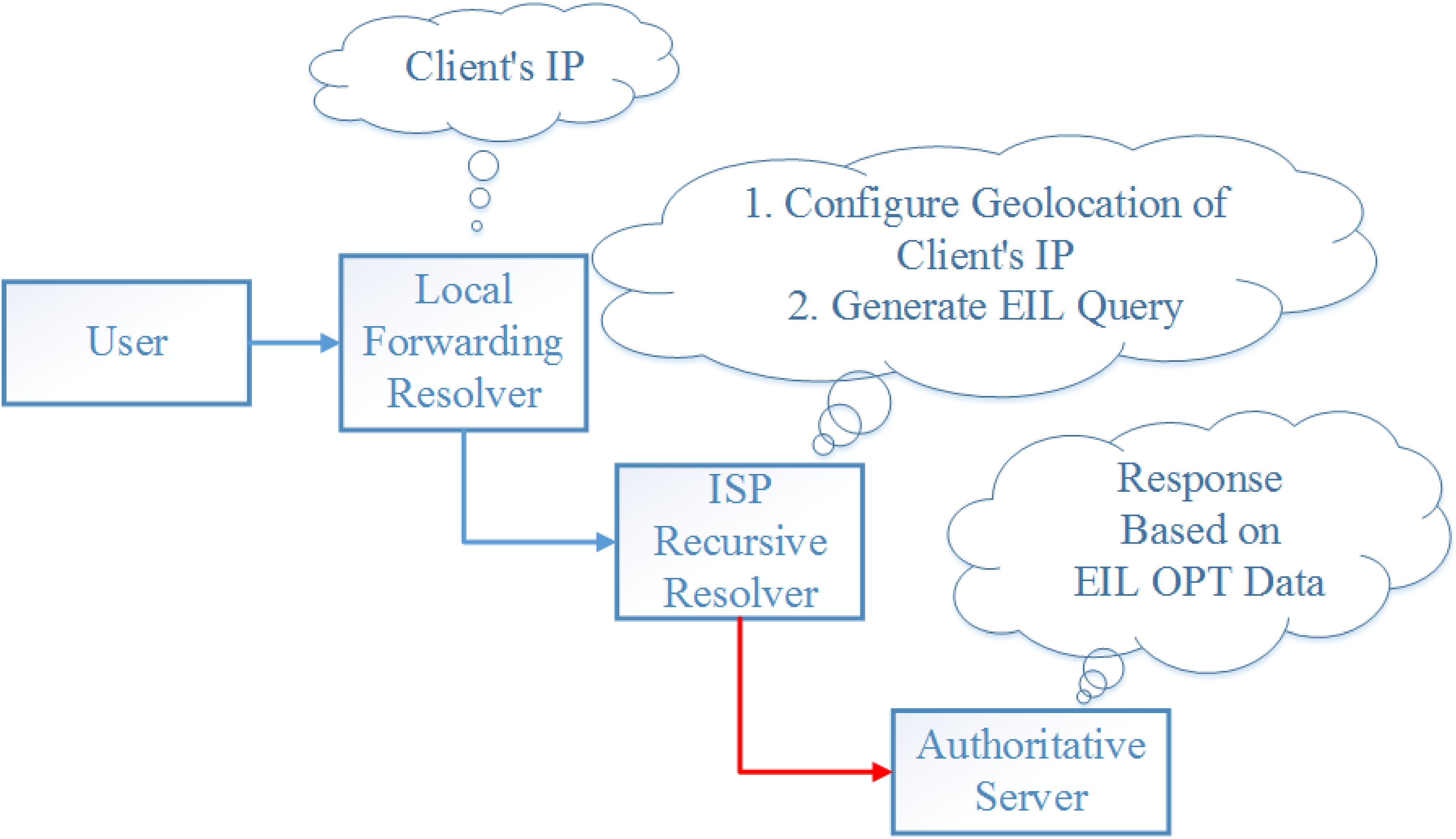
L-model: EIL initiated at local forwarding resolver

L-model has the most precisely geolocation.



I-model: EIL initiated at ISP recursive resolver

I-model will benefit if the authoritative server could not find the approximate geolocation of ISP recursive resolver.



Client's IP

User

Local Forwarding Resolver

1. Configure Geolocation of Client's IP
2. Generate EIL Query

ISP Recursive Resolver

Response Based on EIL OPT Data

Authoritative Server

Trade-off of the three deployment models

P-model is the most recommended.

Model	Cost	Geolocation quality	Deployment Effort
P-model	High	Depend on GeoIP database	Low
L-model	Low	High	High
I-model	Low	High	Middle

L-model requires firmware upgrade EIL support on the first-hop router.

Support ECS and EIL at the same time

Recursive resolvers can cache both ECS response and EIL response.

- Receive EIL query

search in EIL cache, send EIL query

- Receive ECS query

search in ECS cache, send ECS query

- Receive DNS query without EDNS option

search in ECS、EIL cache, send EIL query？

- Receive DNS query with not-ECS/not-EIL option

search in normal cache, send origin DNS query

- Receive ECS query, improve user privacy

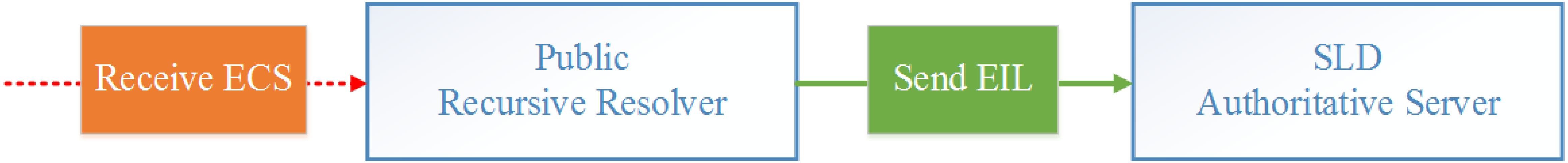
build EIL from ECS information, search in EIL cache, send EIL query？

EIL: Privacy and Security

User Privacy

Client IP	ECS	EIL
61.154.123.91	61.154.0.0/16	<CN, 35, TEL> <CN, 0591, TEL>
	61.154.123.0/24	<CN, 0595, TEL>

P-Model：Improve user privacy



Target Censorship

Target Cersorship is usually applied on domain (QNAME).

EIL covers bigger area than ECS.
Compared to ECS in plain text condition, EIL is weaker at blocking record attack, but stronger at targeted DNS poisoning attack.

Solution:

- Encrypt the dns traffic
- Use some proxy tunnel

Cache Size

Local forwarding resolver and ISP recursive resolver:

- cache EIL response in normal DNS response style ？
- Their customers have a static geolocation.

Public recursive resolver:

- The cache size of EIL is related to the row count in the <COUNTRY-CODE, AREA-CODE, ISP> geolocation whitelist.

DDoS Attack

Like pseudo-random sub-domain attack, name servers may encounter error EIL queries padding with some random error string.

As we have limited the data size of EIL, the defense cost will be smaller than sub-domain attack.

Authoritative server should refuse all error EIL query for security.

Recursive resolver could choose to make a better EIL query instead of refusing if it thinks itself can afford.

Future Work

Future Work

Demo code: https://github.com/abbypan/dns_test_eil
do more experiments in China network environment.

Bring it to the IETF.
https://github.com/abbypan/dns_test_eil/blob/master/ietf_draft/draft.txt

Apply the EIL to real DNS traffic.

Finally

Question ?

Many thanks to Sara for stand-in presentation.