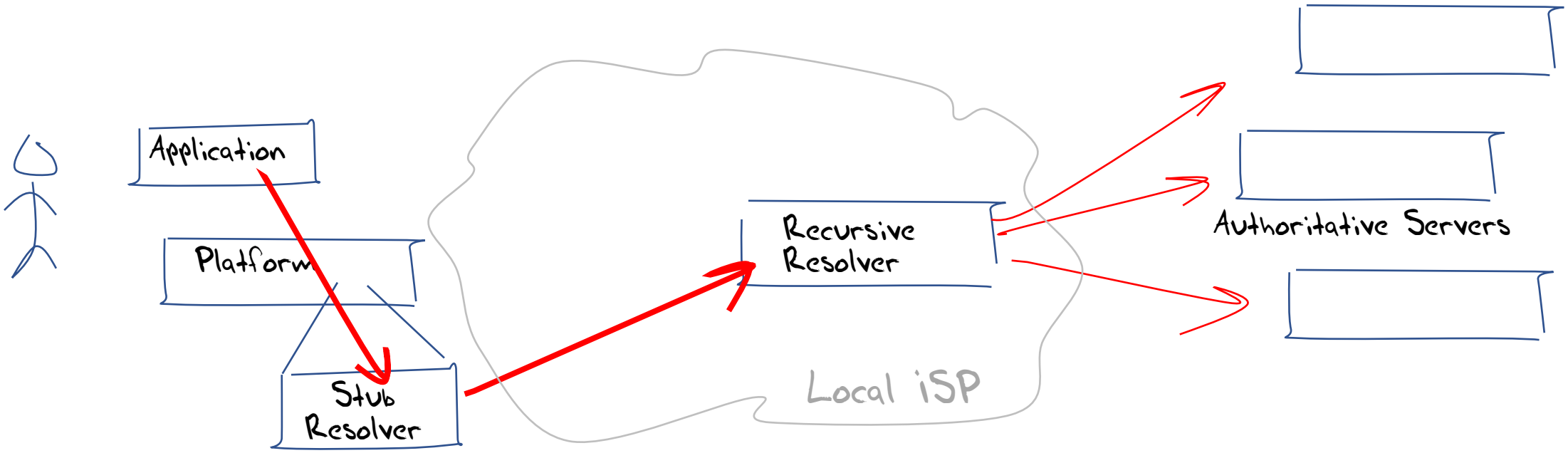
Implications of DNS Encryption

Geoff Huston
APNIC Labs

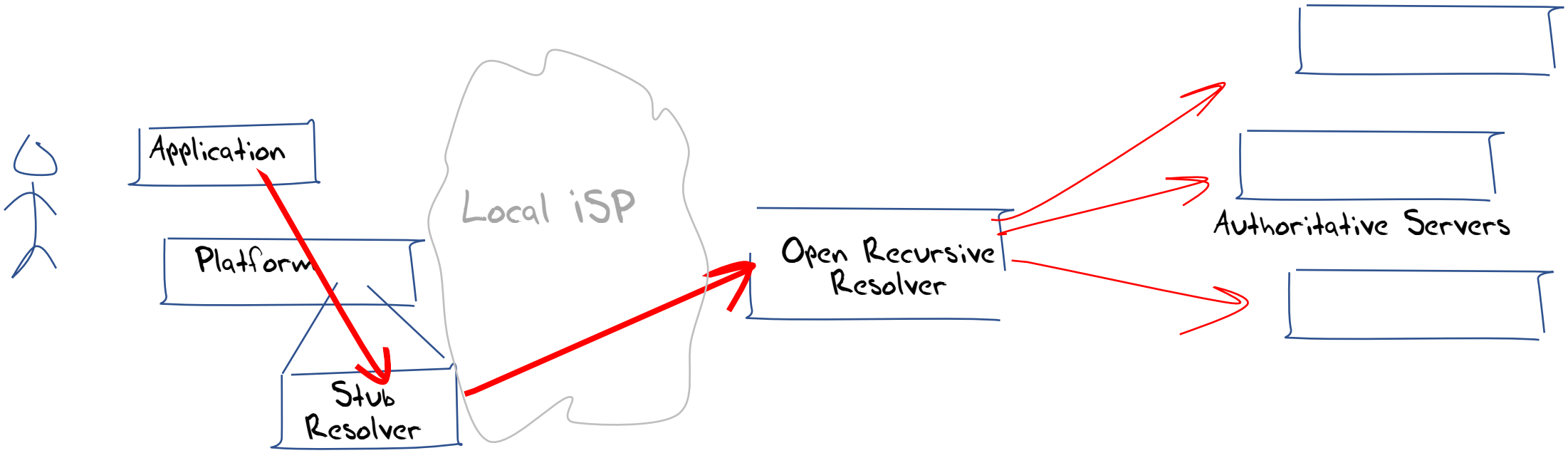
A Traditional View of the DNS

The DNS is part of shared common infrastructure services

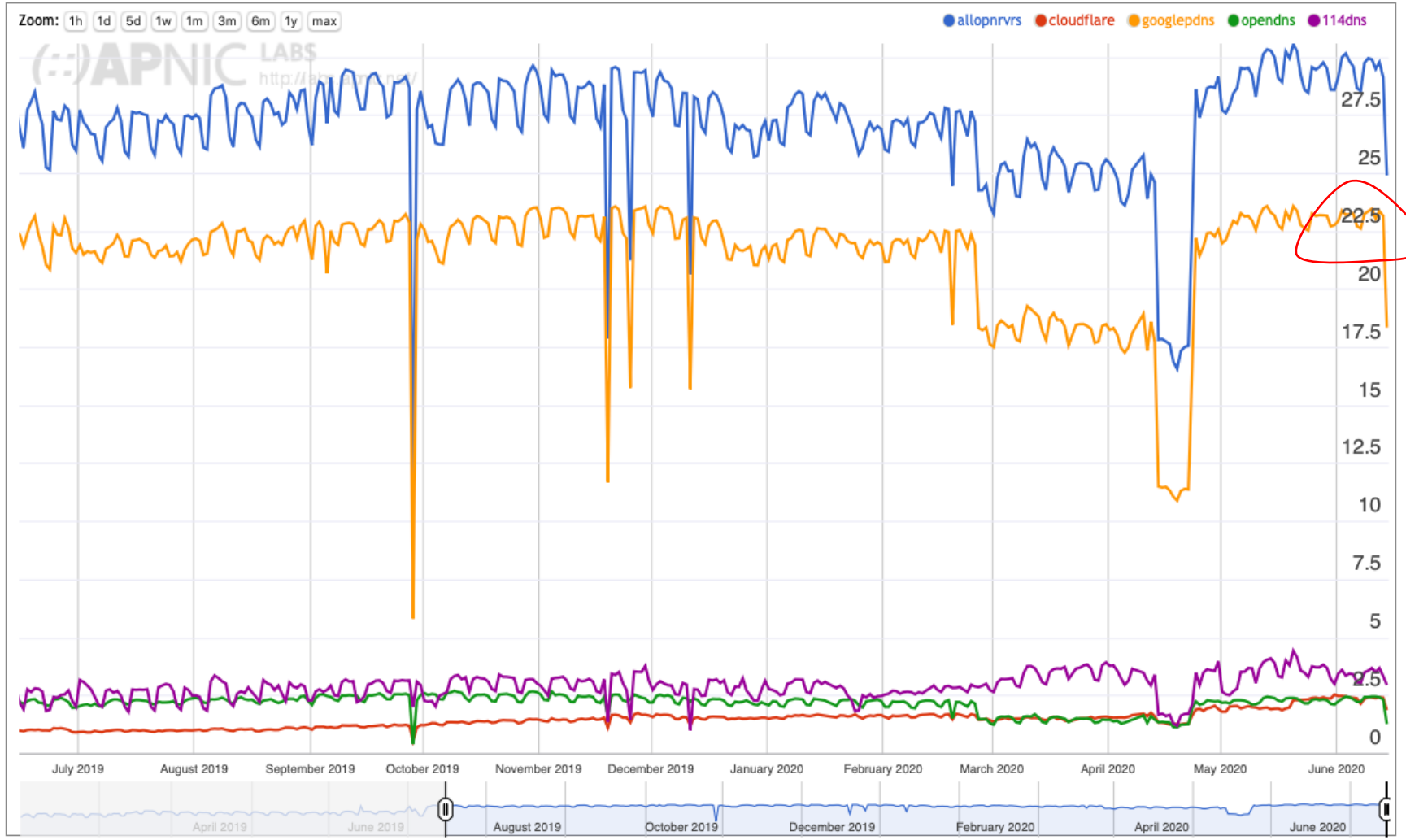


The Rise of Open Resolvers

The DNS is a service overlay



Use of Open Resolvers



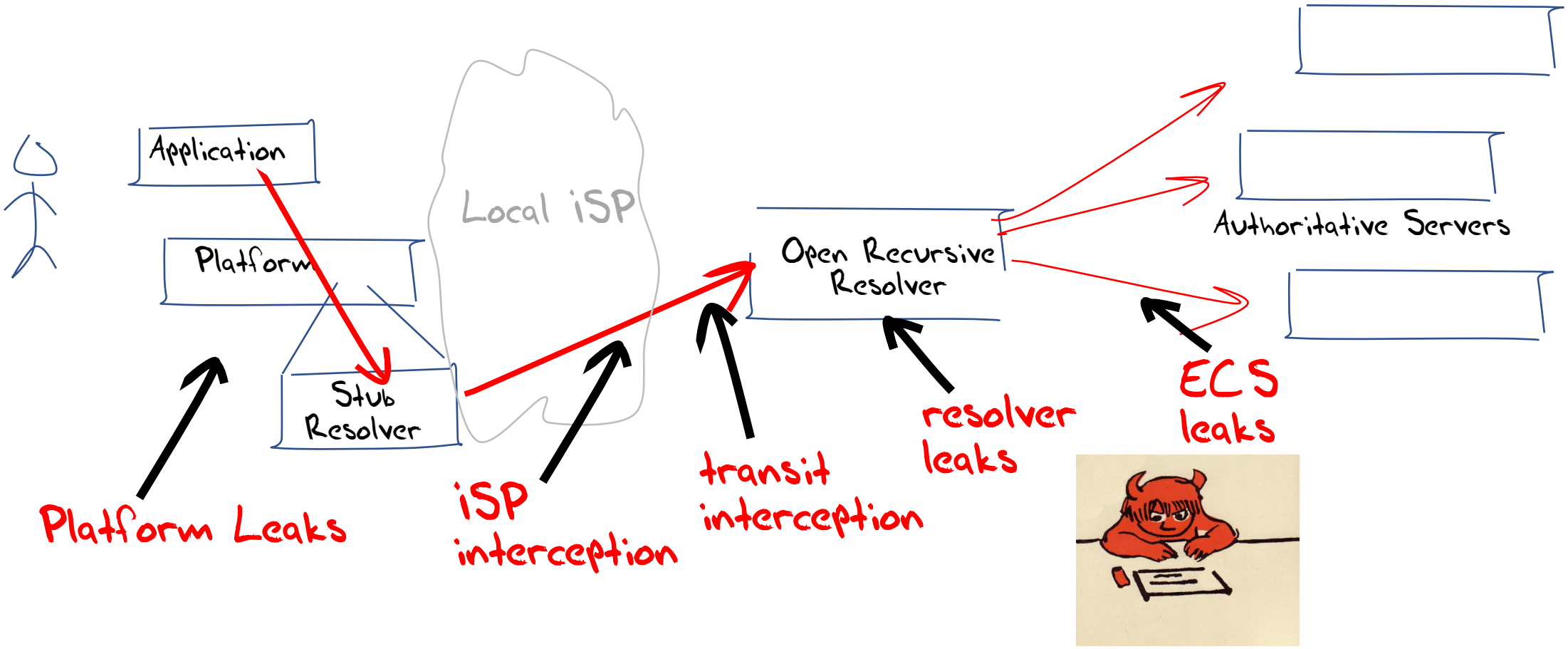
More than a quarter of the Internet's users send queries to open resolvers

Google is the dominant provider with 22÷ market share

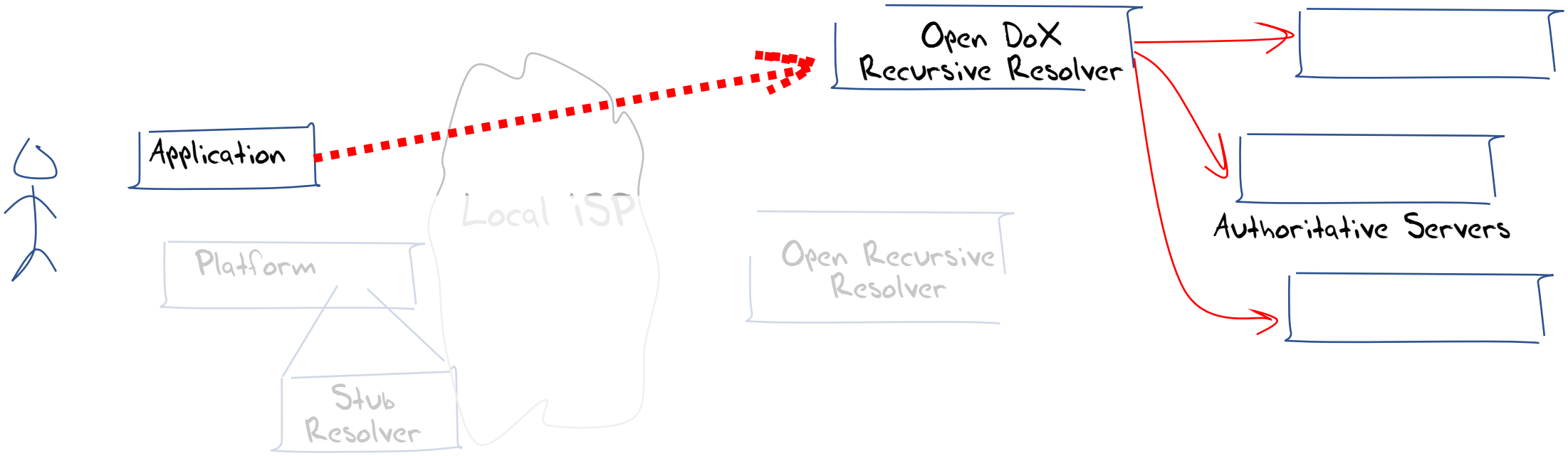
https://stats.labs.apnic.net/rvrs

Opportunities for Interception

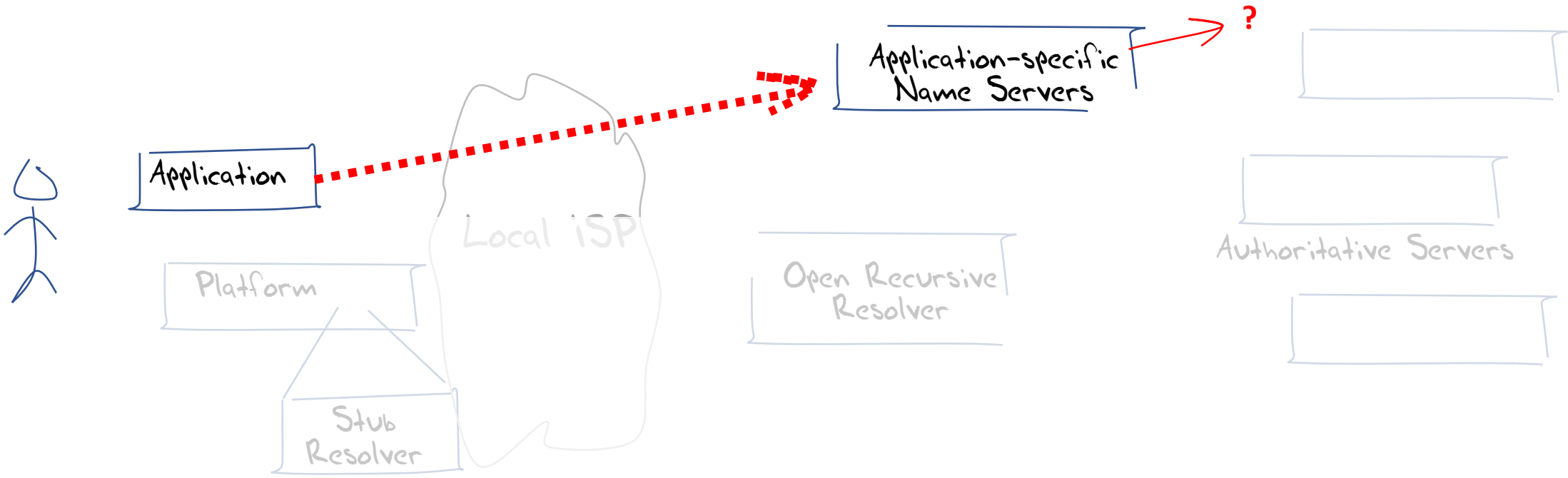
The DNS is a service overlay



Sealing it up



Application Specific Name Services?



Futures?

- The DNS appears to be receding as a common infrastructure
- DoH / DoQ are pushing the name space to become an application capability
- It’s possible that the other end of the encrypted tunnel becomes an application-specific name service rather than generic DNS
- From such application-specific platforms its possible that application-specific name services are used
  - Name “pushing”
  - Customised “names”
  - Other bright ideas!
- At that point the coherency of the name system is placed under pressure and fragmentation of this space becomes more likely