

IPSECA: are we choosing
between security suites?

draft-osterweil-dane-ipsec-00

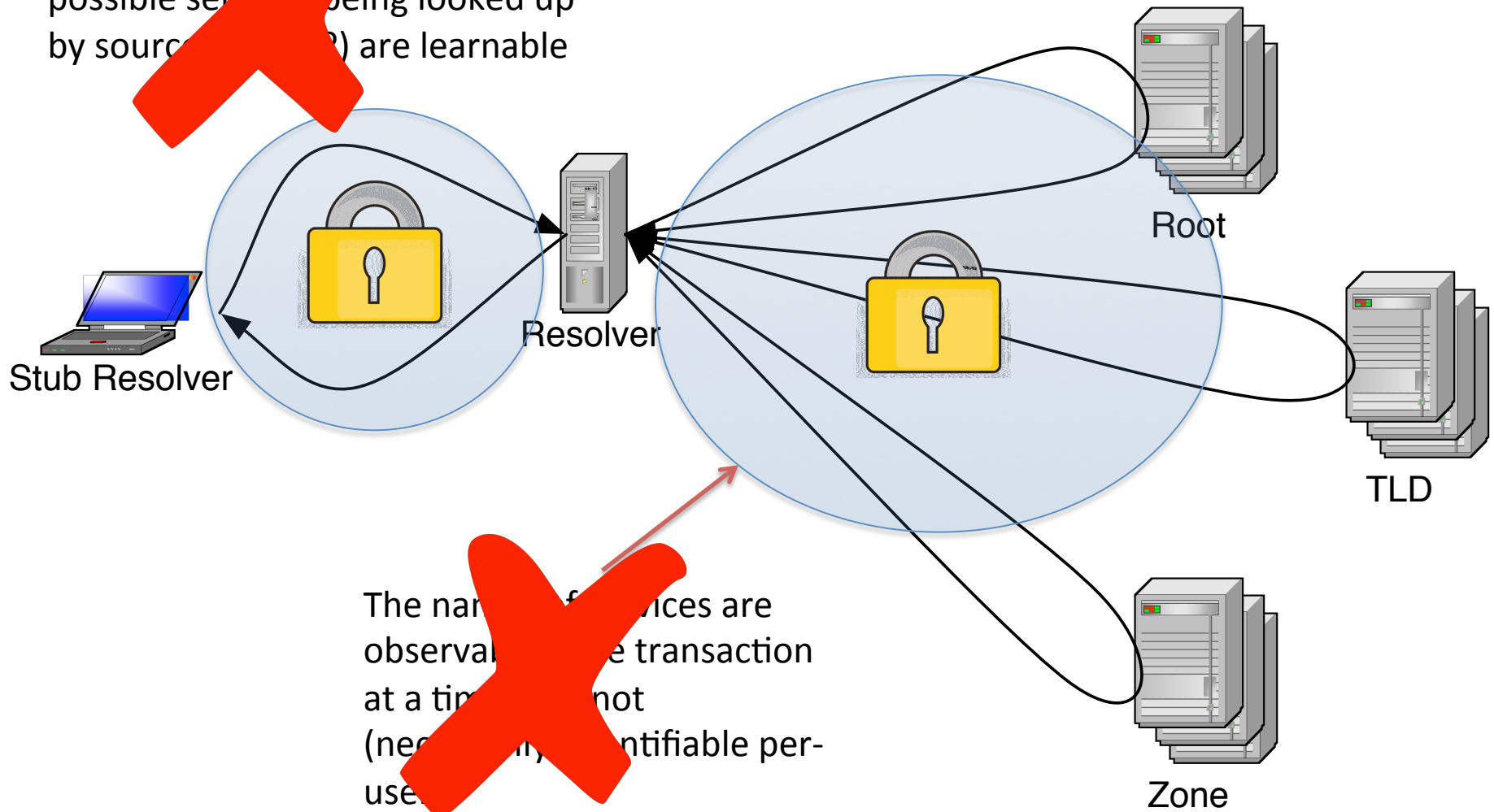
- DNSSEC is great, but doesn't try to offer privacy, transactional protections, etc.
- DNS can leak info... blah blah blah (see minutes from dnse)
 - We should worry about both the stub-to-resolver and resolver-to-name server hops [separately]

What's the point of this draft?

- Harmonize IPsec key learning with DANE
- Offer service-level transaction protections w/ IPsec (using OE)
- The idea: offering different security solutions to security practitioners allows us to effectuate the postures we need
 - Different deployments may benefit from different postures

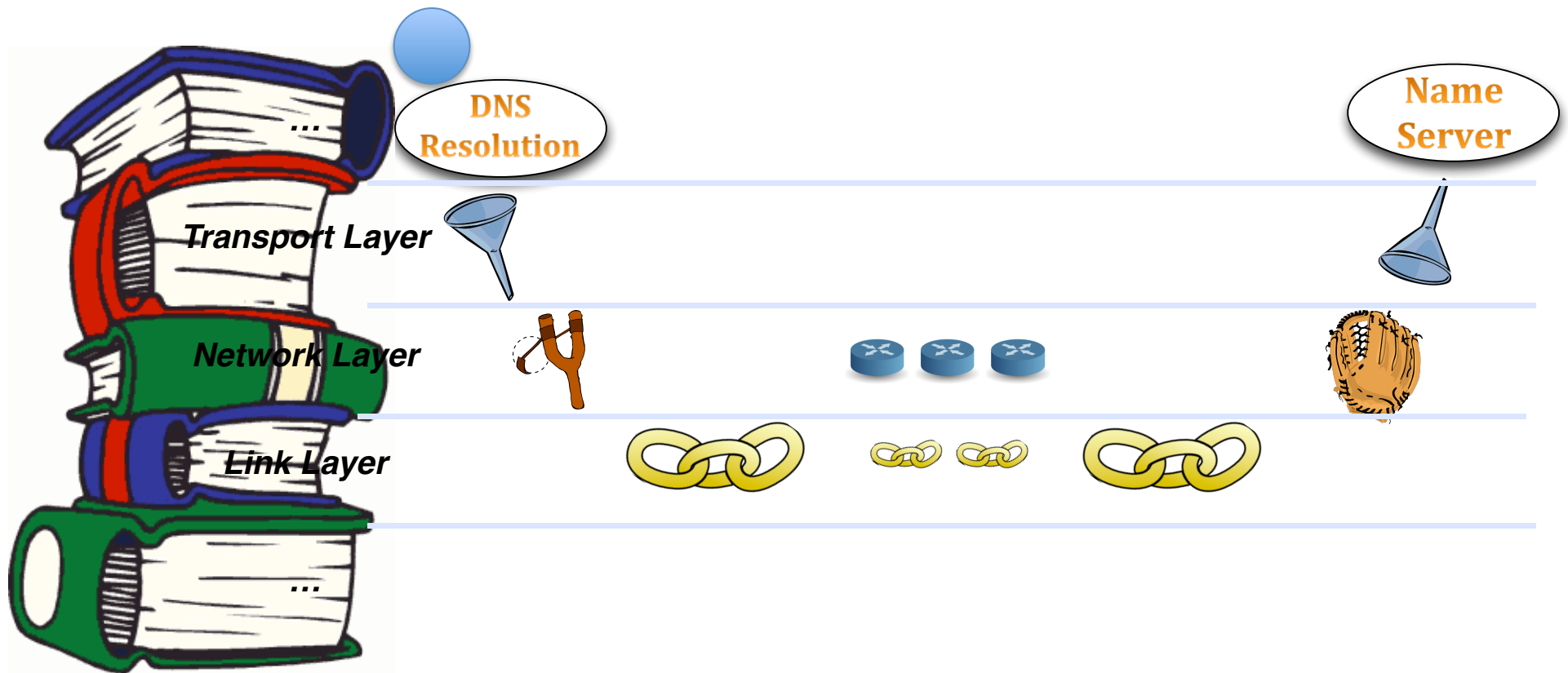
Well known stages of DNS

The names are associated with all possible services being looked up by source (IP) are learnable

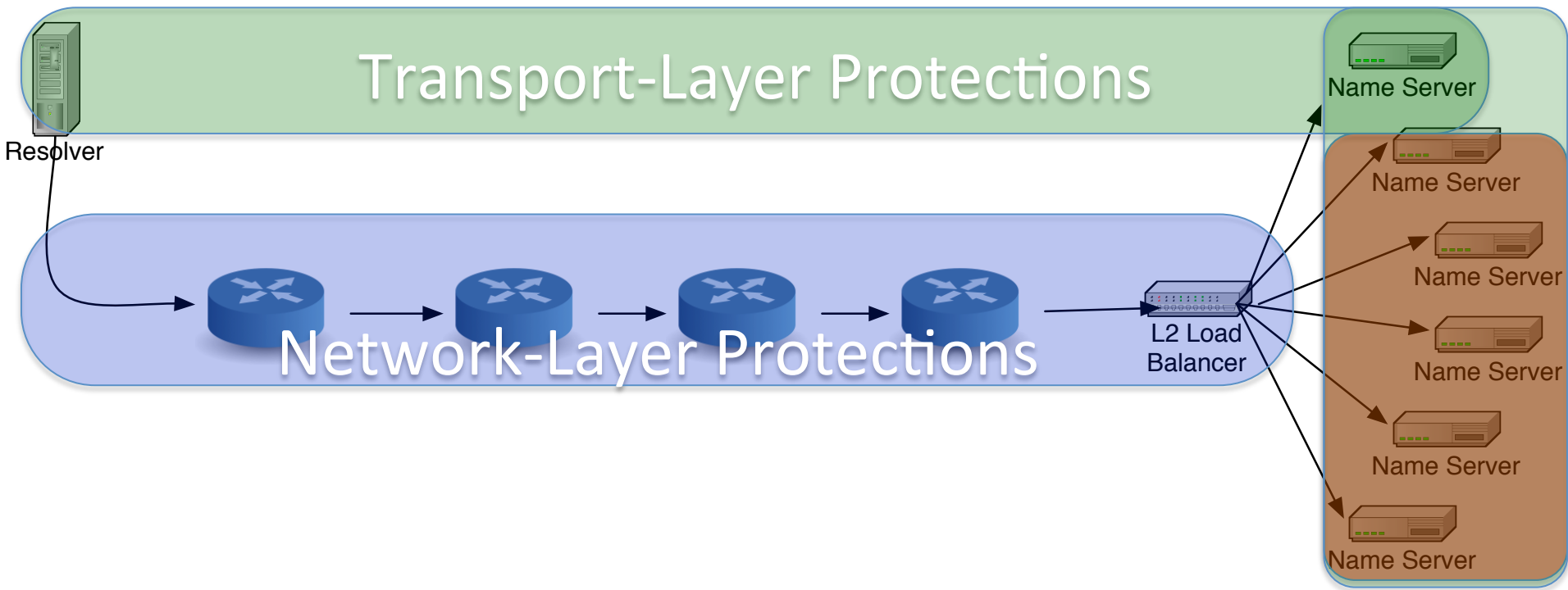


The names of services are observable in the transaction at a time, but not necessarily identifiable per-use

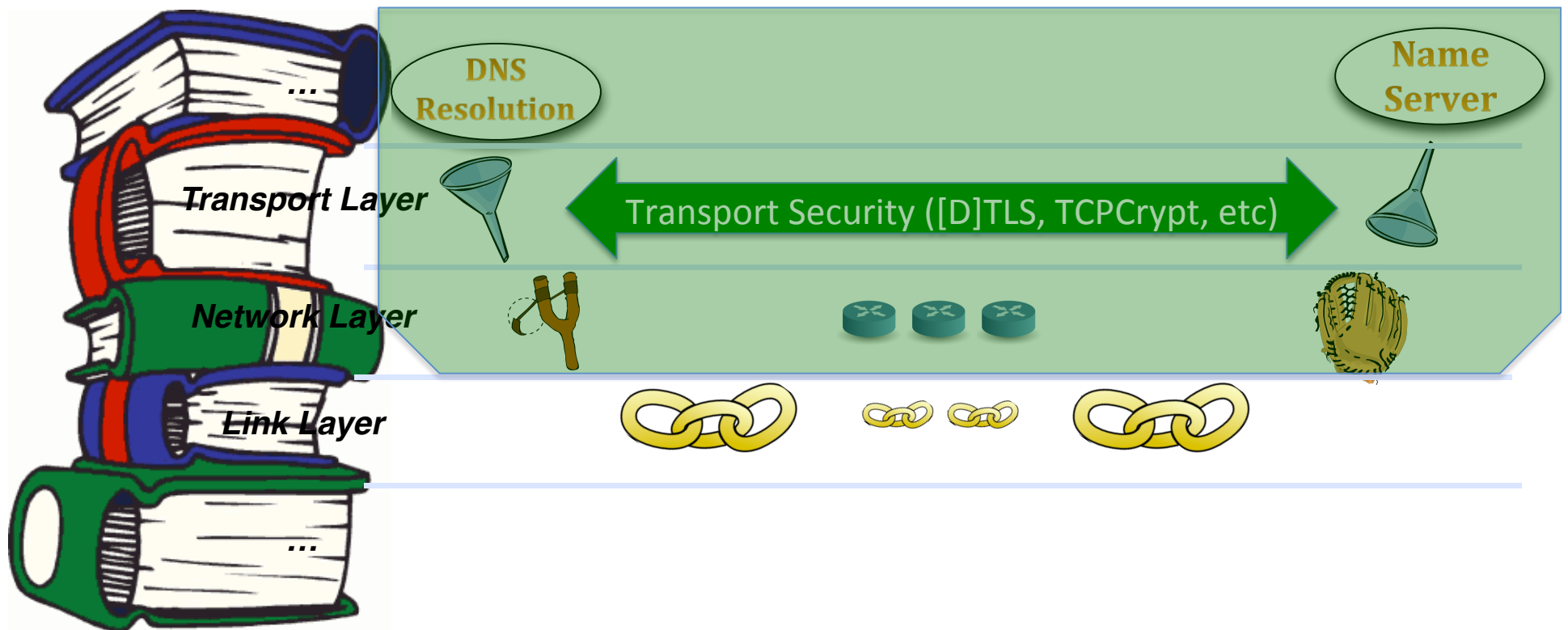
Passing DNS around the stack



Example solution scopes



Passing security up the stack



So?

- Well, figuring a practical usage of IPsec for DNS might teach us some lessons about *this type* of OE
- From this, maybe we can specify some things from this general utility
 - This was the motivation for starting with a DNS focus

Thanks!

Questions?