

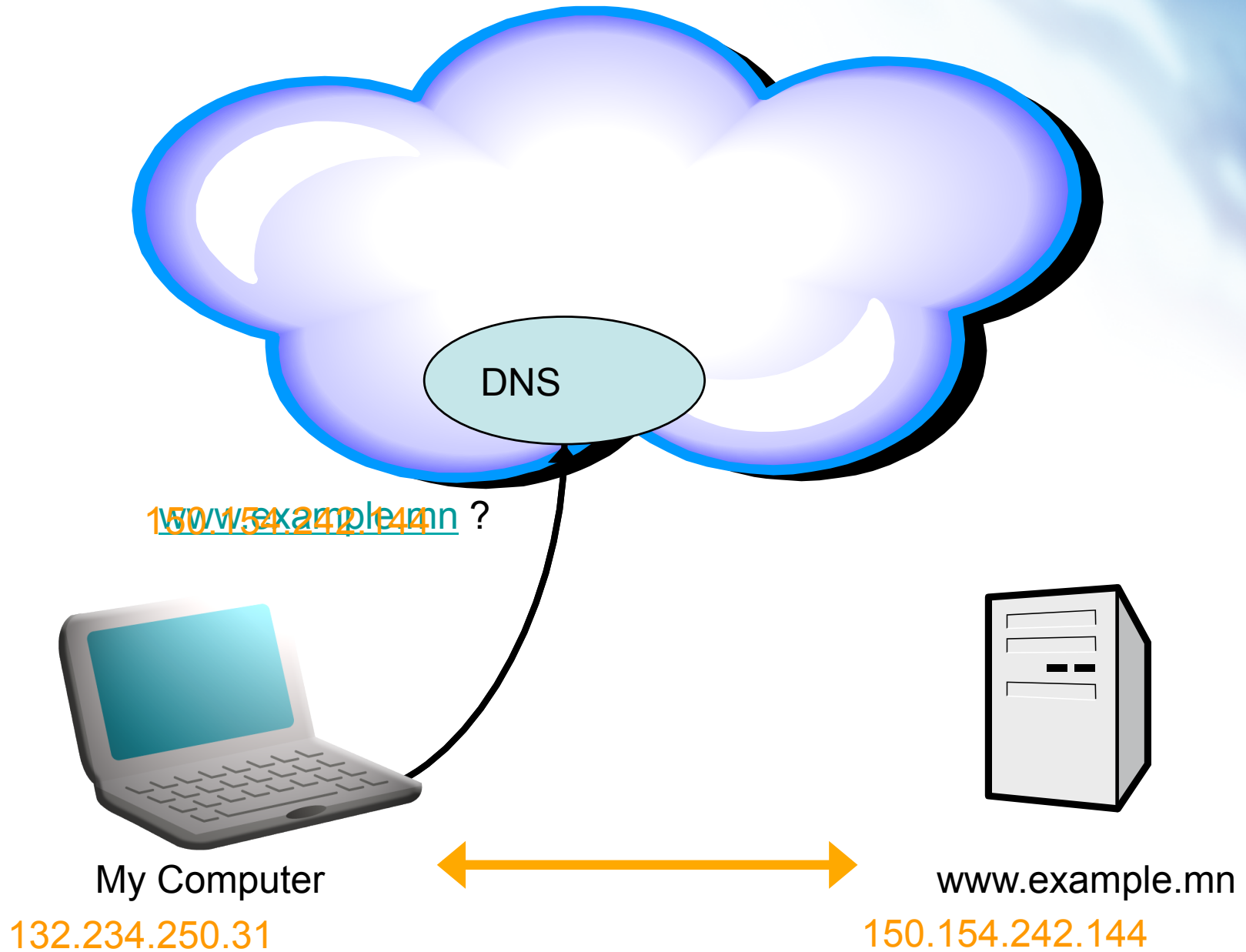
Future of the Internet in Mongolia

DNS Security

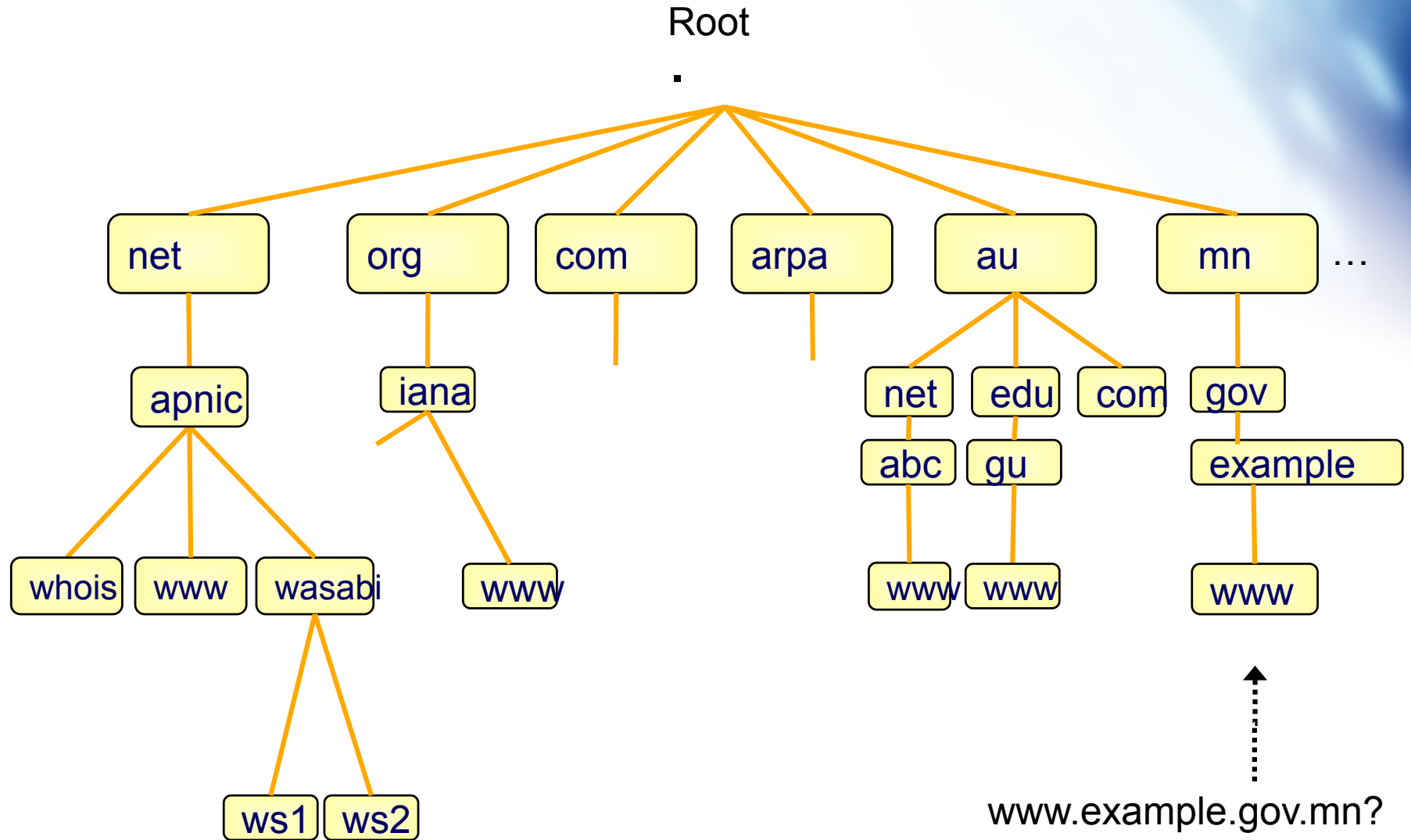
Champika Wijayatunga, APNIC
champika@apnic.net

Ulaanbaatar, Mongolia
21 October 2010

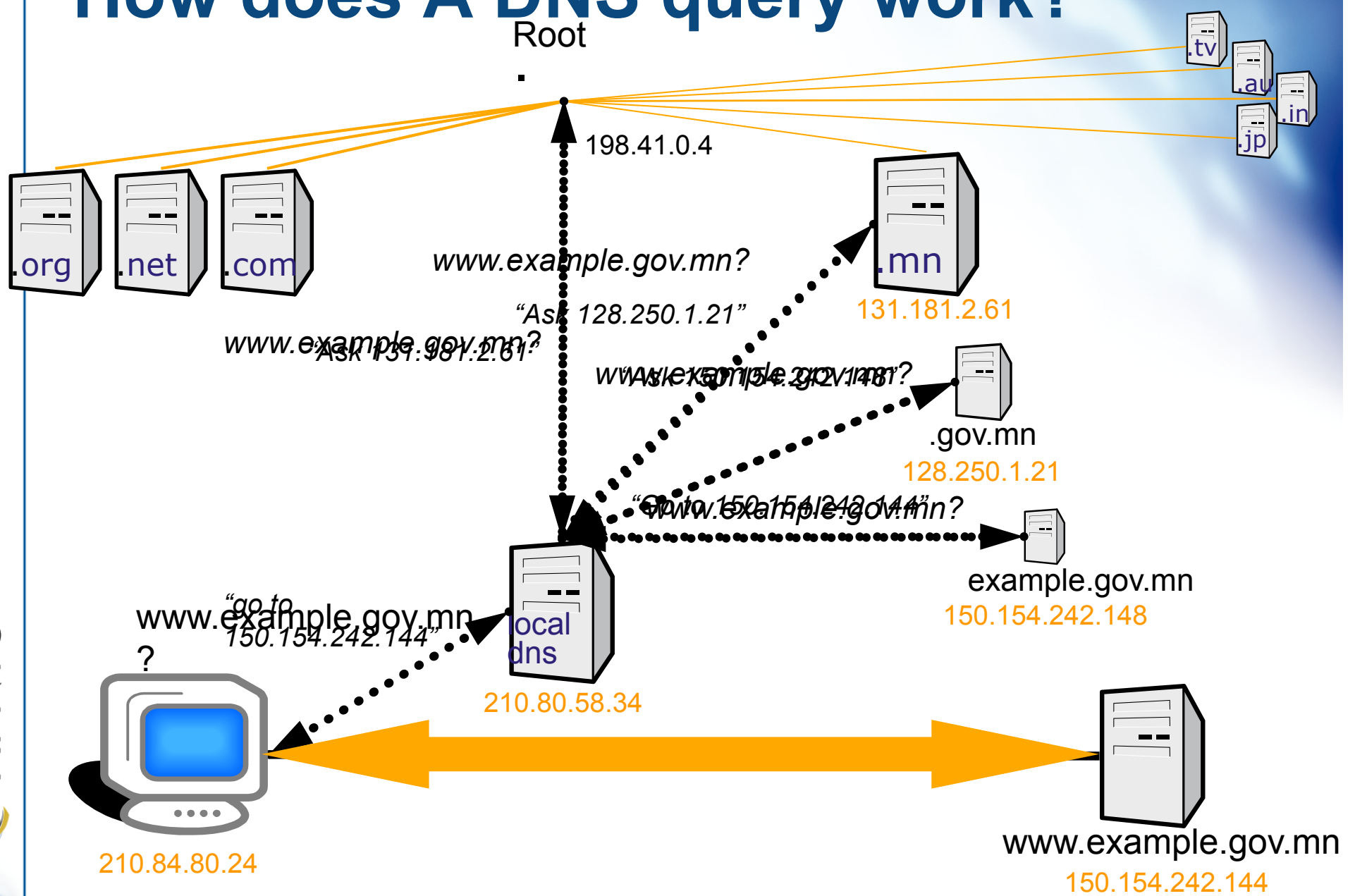
What is DNS ?



The DNS tree



How does A DNS query work?



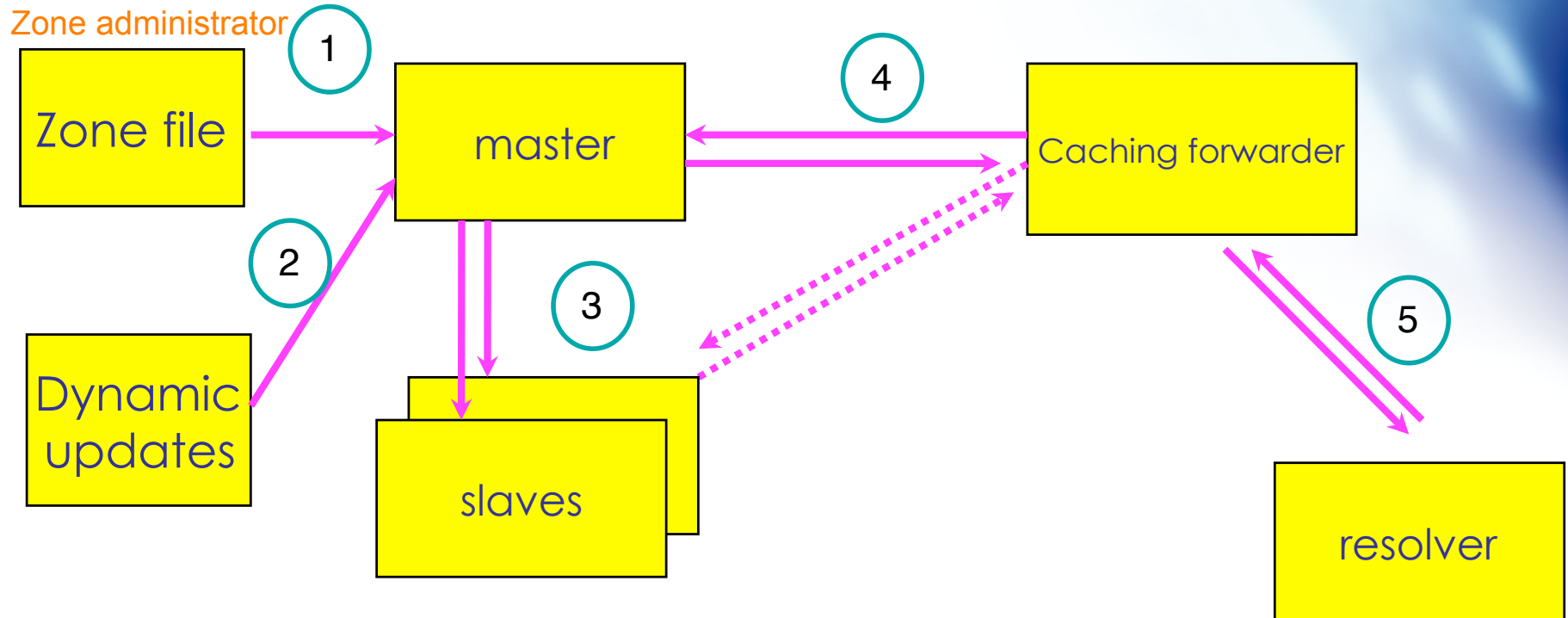
Can we make sure that DNS is secure?

- The original DNS protocol wasn't designed with security in mind
- It has very few built-in security mechanism
- As the Internet grew this would be a problem
 - For example DNS spoofing was to easy
- DNSSEC and TSIG were develop to help address this problem

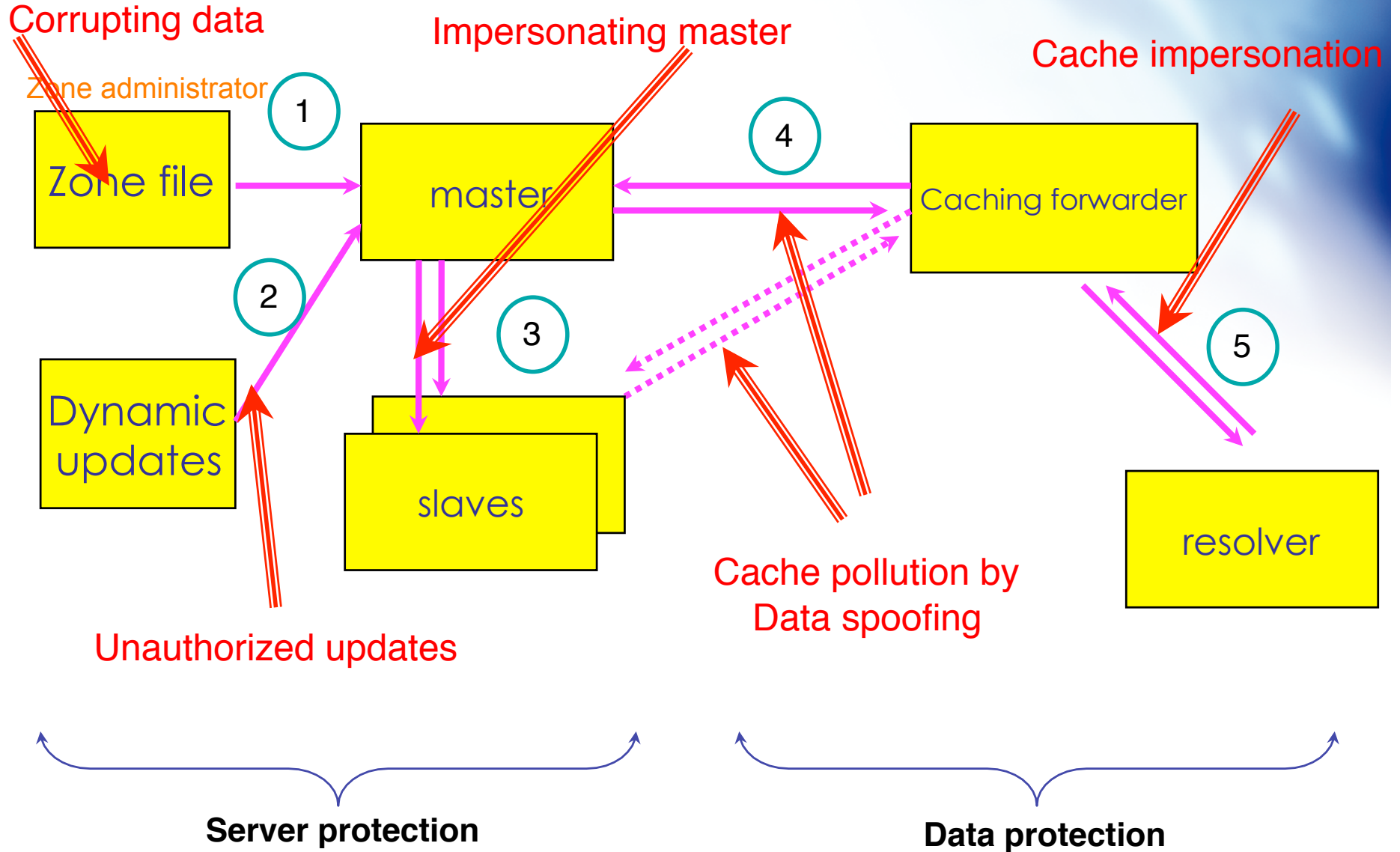
So why DNS Security?

- DNS is not secure
 - Applications depend on DNS
- TSIG protects the transactions between the Servers
- DNSSEC protects against data spoofing and corruption

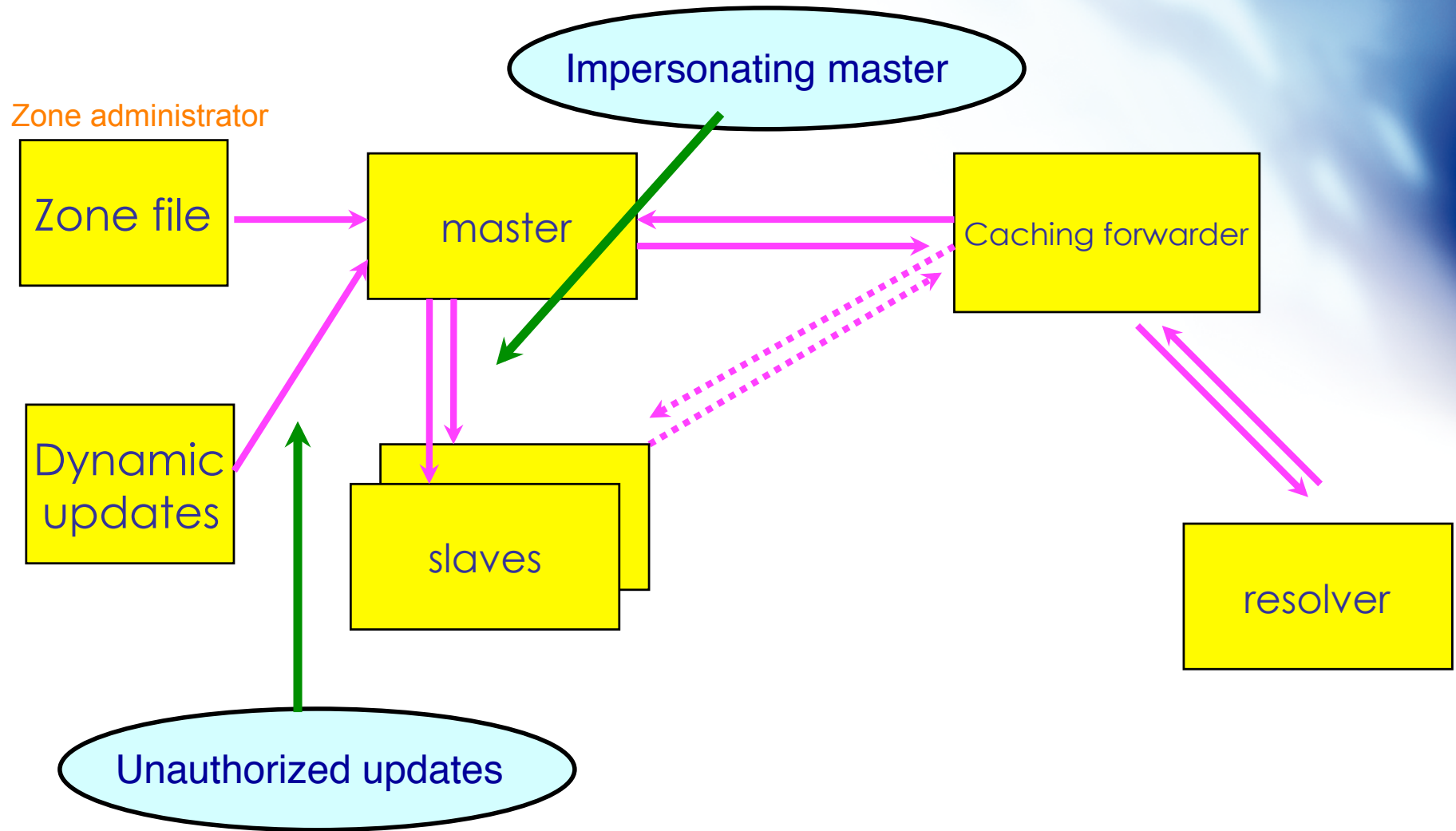
DNS: Data Flow



DNS Vulnerabilities

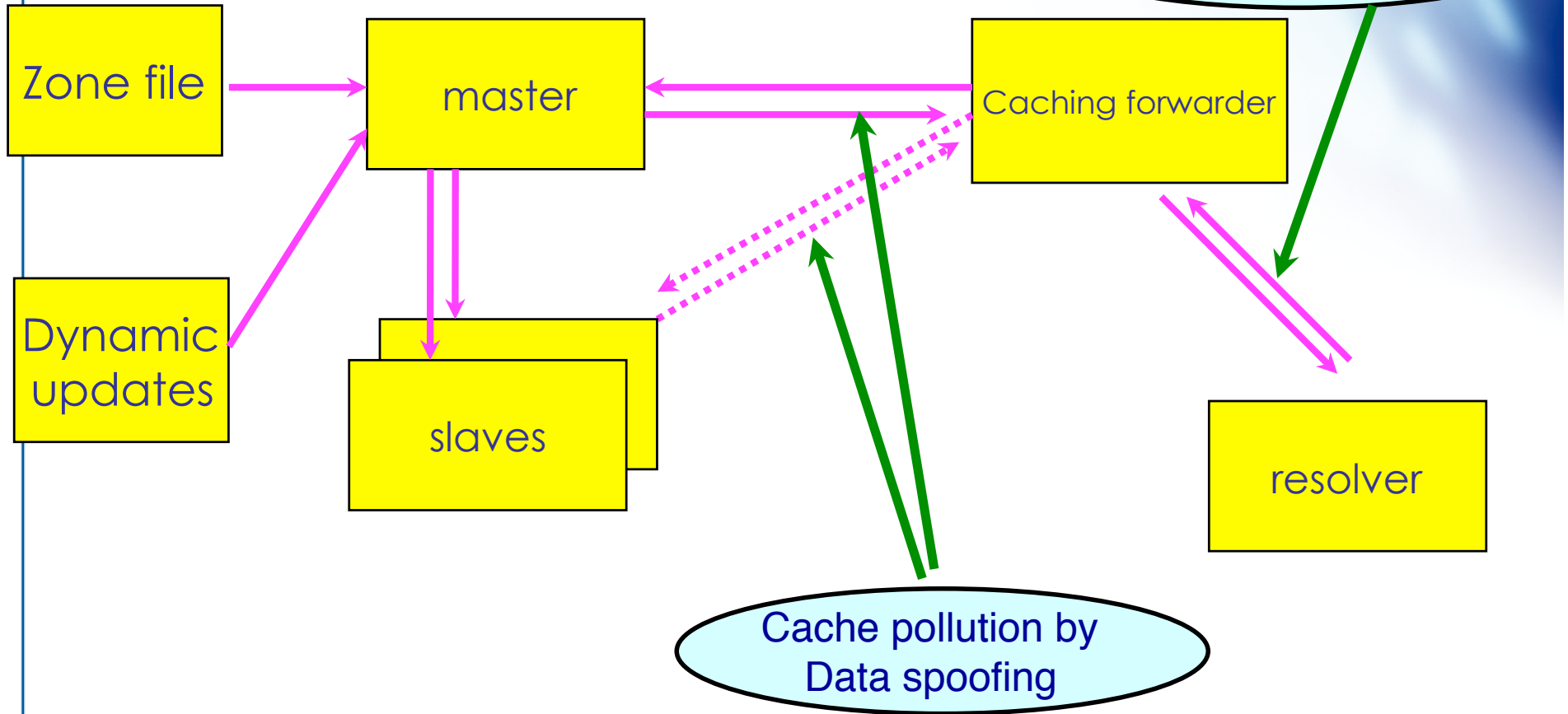


TSIG Protected Vulnerabilities



Vulnerabilities Protected by DNSSEC

Zone administrator



What is TSIG - Transaction Signature?

- A mechanism for protecting a message from a primary to secondary and vice versa
- A keyed-hash is applied (like a digital signature) so recipient can verify message
- Based on a shared secret - both sender and receiver are configured with it

What is DNSSEC ?

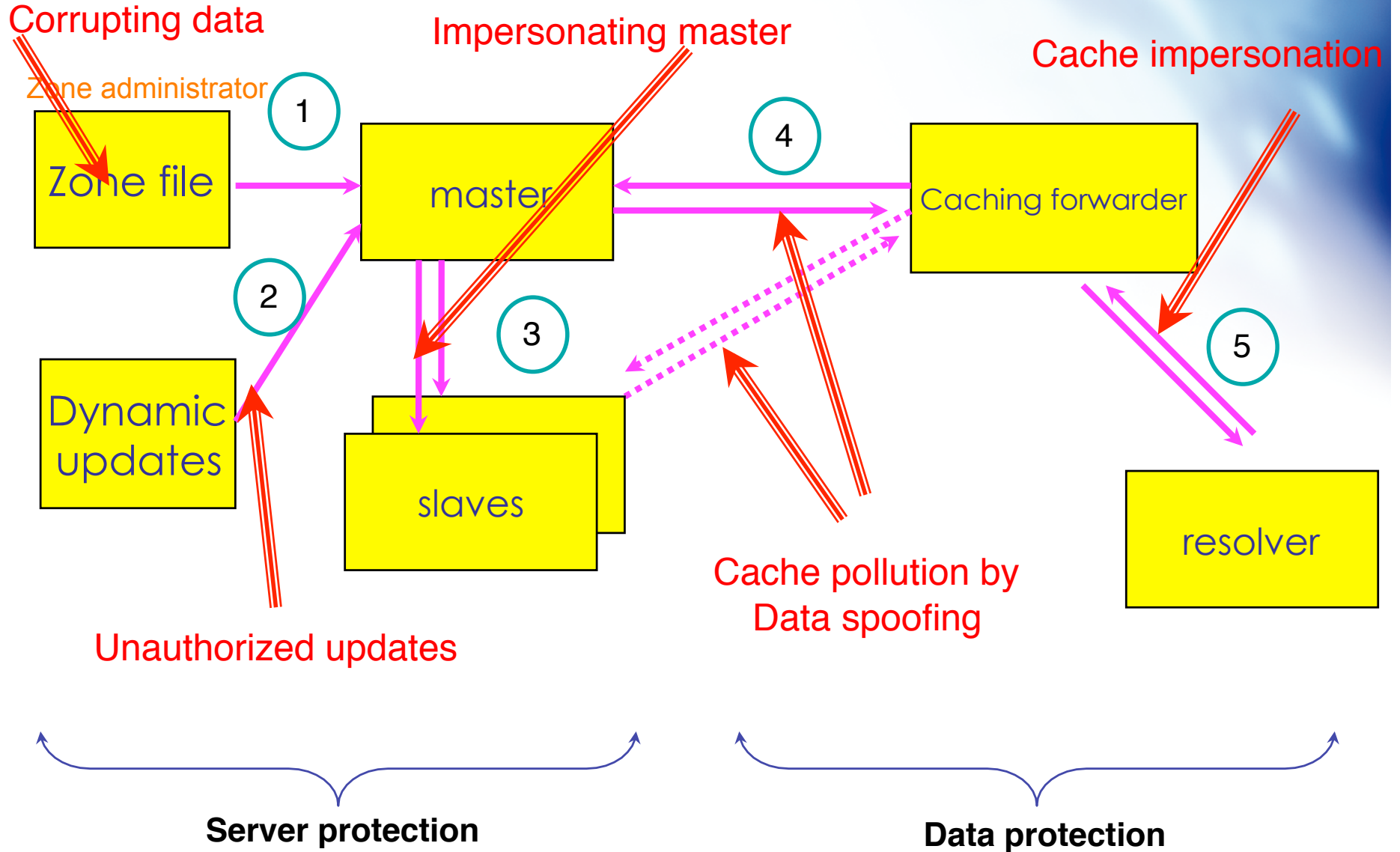
- DNSSEC protects against data spoofing and corruption
- DNSSEC also provides mechanisms to authenticate servers and requests
- DNSSEC provides mechanisms to establish authenticity and integrity



Protecting Transactions - TSIG steps

1. Generate secret
2. Communicate secret
3. Configure servers
4. Test

DNS Vulnerabilities



Securing your Zones - DNSSEC Steps

- Enable DNSSEC
- Create the Keys
- Sign the Zone
- Publish the signed zone
- Delegation process

Questions ?



Thank you 😊!
<champika@apnic.net>