Redes de Computadores II

Universidade do Algarve

Semana 9

https://github.com/ncatanoc/redes_algarve

Néstor Cataño

nestor.catano@gmail.com

DNS (Domain Name Service)

Goal:

To understand the basic underpinnings of **DNS** and its relationship with IPs

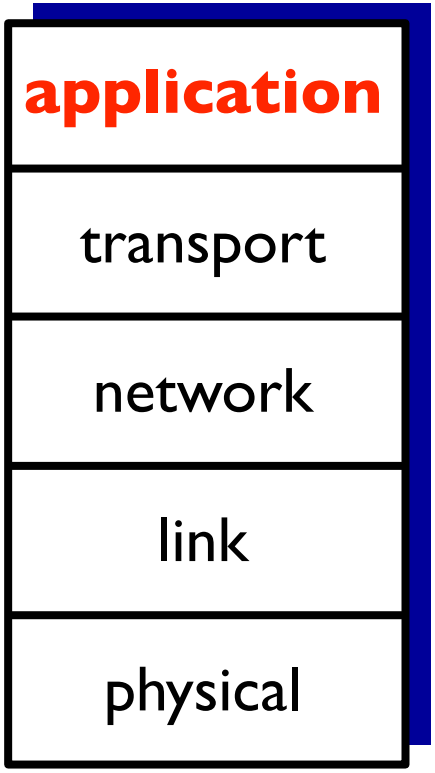
Roadmap

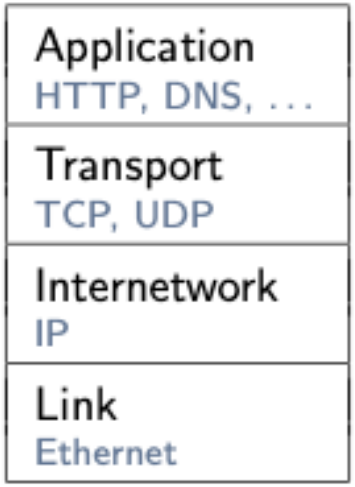
1. **DNS (domain name service)**
2. DNS security

DNS

Introducing the Domain Name Service

- How does the network know where to take us when we type www.ualg.pt?
- How does the network know where to send an email sent to someone@ualg.pt?





Hostname vs Domain name

Hostname

It refers to a particular device on a network. So, in the URL mail123.mybusiness.com, "mail123" is the hostname.

Domain name

It identifies the website. So, stick with the example website URL mail123.mybusiness.com. "mybusiness" is the domain name.

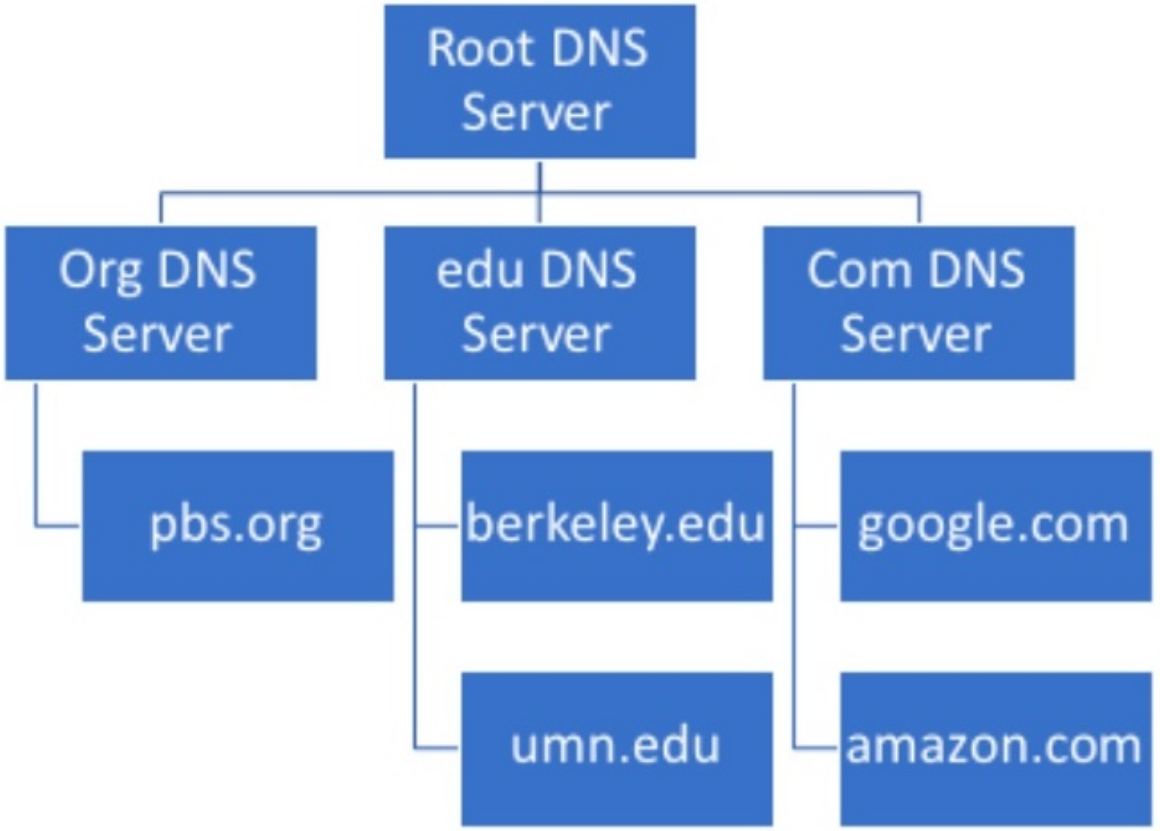
What is DNS?

Finding the best way to go 35.163.72.93 to www.ualg.pt

DNS provides host aliasing, mail server aliasing and load distribution.

DNS is a hierarchical, distributed system

Hierarchical distributed system



DNS runs over UDP

DNS records and messages

- Resource Records
  - Records stored in the DNS distributed Database
  - Including hostname-to-IP address mappings
- DNS Messages
  - Carries the resource records

DNS resource records

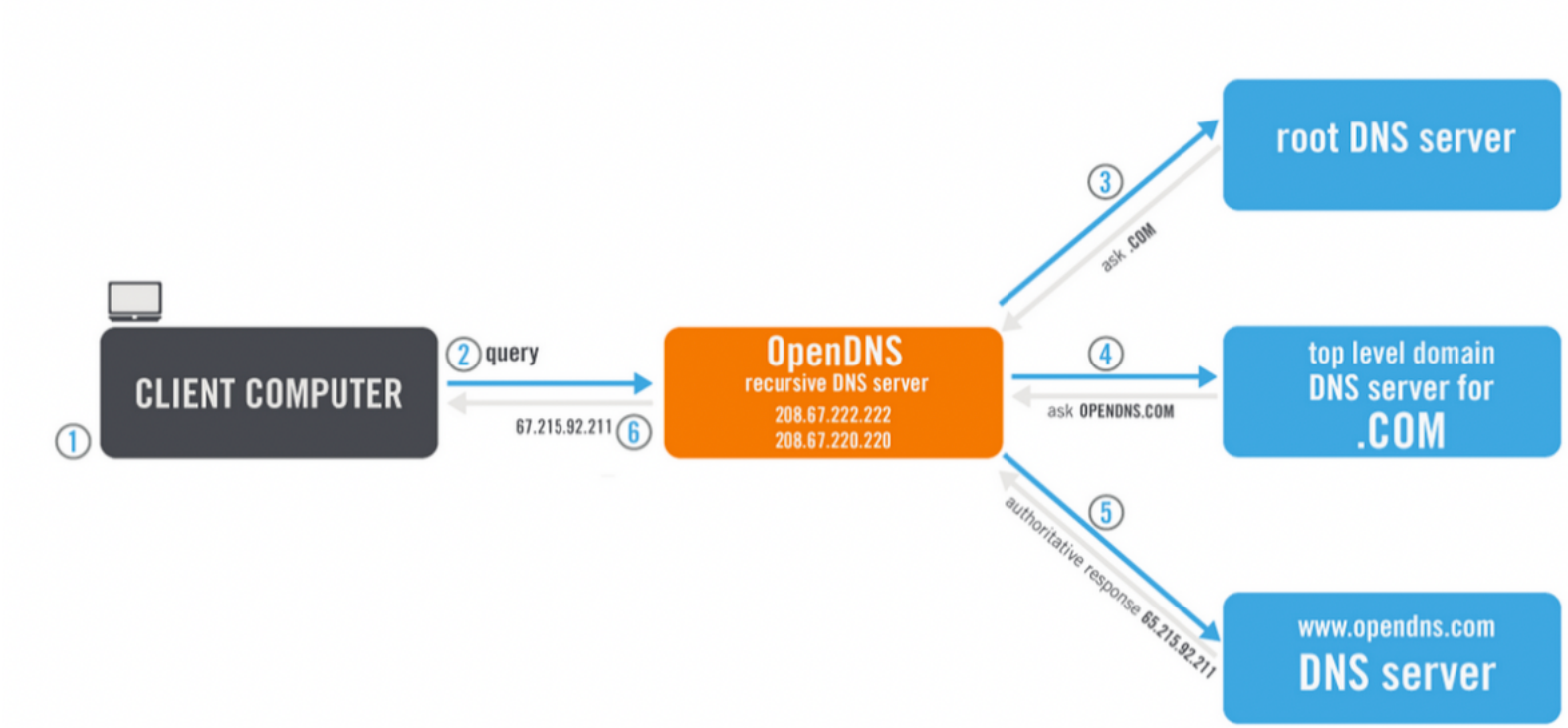
(Name, Value, Type, TTL)

- Meaning of Name Value depends on Type
- Types include A, NS, CNAME and MX
  - Type=A Name is hostname and the Value is the IP address
  - Type=NS Name is a domain and Value is a Name Server

DNS messages

- Messages transfer Resource Records
- Messages consist of queries and replies
- Message content consists of questions and answers
  - Example Question: berkeley.edu Type A
  - Example Answer: (berkeley.edu, 35.163.72.93, Type A, TTL)
- Messages can carry multiple questions and answers
- Messages can carry the records for authoratative servers

Recursive name resolution



Roadmap

1. DNS (domain name service)
2. **DNS security**

Traffic filtering

Traffic Filtering

- Using DNS to control domain access
  - Security Considerations
  - Parental Controls
  - Censorship

DNS security considerations

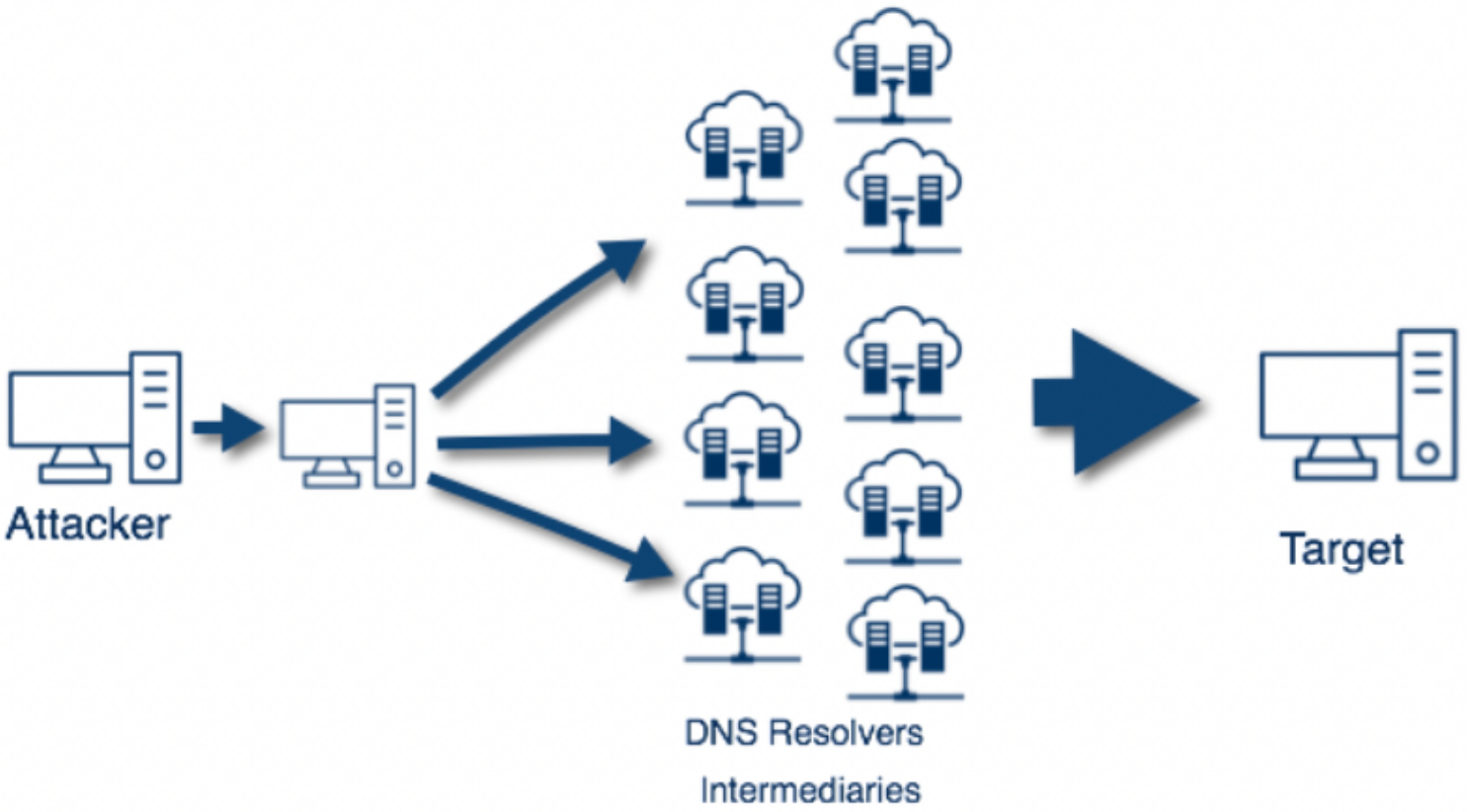
DNS Security Considerations

- Covert Channels
- DNS Poisoning
- DNS Sinkholing
- DNS Amplification Attacks

Cover channel

- Using DNS as a way to hide traffic
  - DNS traffic is essential so rarely restricted
  - By embedding data in the DNS message a client can circumvent filters
  - Bypass restrictions (wifi paywall, Tor, secure shells)
- DNS Covert Channel
  - Attacker sends DNS requests to a specifc covert channel DNS server
  - The covert channel DNS server acts as a proxy
  - Covert data piggybacks on DNS traffic

DNS amplification attack



DNS Sinkhole

https://www.youtube.com/watch?v=X2Y_MvzIUko&t=114s

DNS summary

DNS Summary

- UDP based protocol
- Resource Records and Messages
- Different Types of Records
- Distributed
  - Name Servers (recursive and authoritative)
  - Database
- Security Concerns
  - Using DNS to attack targets
  - Using DNS to bypass controls
  - Using DNS to censor
  - Using DNS to stop attacks