Mic!

Domain Name System (DNS)

SCC. 203 – Computer Networks

Geoff Coulson

Week 14 Lecture 2

Contents

Outline

- Naming Principles
  - Internet Names vs. IP addresses
  - History
    - host.txt
- DNS Service Structure
  - Distributed database
  - DNS Hierarchy
- DNS Operation
  - Name resolution
- DNS Records & Messages
- DNS Security

Basic Principles of Naming

…or "What's in a name"
Act II, Scene II, Romeo & Juliet

Naming & Addressing

- Names & Addresses
  - To call someone, you need to ask for his/her phone number
  - To mail someone, you need to get their address
- How does naming and addressing work in the Internet?
  - If you need to reach Google do you need their IP
    - Does anyone know Google's IP?
  - Problem:
    - People can't remember IP addresses
    - Need human readable names that map to IP addresses

Internet Names & Addresses

- IP Addresses, e.g. 148.88.2.80
  - Computer usable labels for machines
  - Conform to structure of the network
- Names, e.g. www.lancaster.ac.uk
  - Human usable labels for machines
  - Conform to organizational structure
- How do you map from one to the other?
  - ➔ Domain Name System (DNS)

Internet Names & Addresses

- **Indirection** is the ability to reference objects (such as data) using a name (identity) instead of the value of the object (such as an address)
- Quite simply, it means not direct
  - If there is a direct connection between two things, indirection means that something is placed in the middle so that another level of indirection is created

> ***All problems in computer science can be solved by another level of indirection.***
>
> *– David Wheeler*

History

- Before DNS, all mappings were in **`hosts.txt`**
  - /etc/hosts on Linux
  - C:\Windows\System32\drivers\etc\hosts on Windows
- Process
  - Centralised, manual system
  - Changes were submitted to SRI via email
  - Machines periodically FTP new copies of `hosts.txt`
  - Administrators could pick names at their discretion
  - Any name was allowed
    - You could name your server as:
      - "best_server_in_the_world"

The Need for Something Better

- System administrators had to update hosts file on every machine to include every host their users might access

- Any machine not in hosts file could only be accessed using IP address

ping 148.88.65.80

and not ping www.lancs.ac.uk

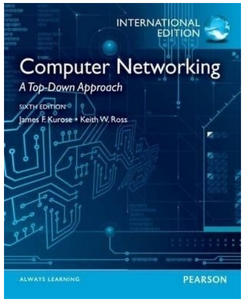
Hosts Files Today

- Used mainly to bypass DNS
  - … not suited to Internet scale
- Error prone
  - **No trigger for updates**
    - Name to IP mappings change
  - **No guarantee of network wide consistency**
- Can ‘guarantee’ access to important local servers
  - Beware over use due to above problems

From `host.txt` to DNS

- `host.txt`
  - Not scalable
    ➔ need for scalable system
    - SRI cannot handle load
  - **Hard to enforce uniqueness of names**
    ➔ need for unique naming system
    - e.g UCL
      = University College London
      = Université Catholique de Louvain
  - Many machines had inaccurate copies of `hosts.txt`
    ➔ need for system to provide real-time updates
    - Stanford-Research-Institute: Network-Information-Center (NIC) updated `hosts.txt` periodically
- Hence, DNS was born
  - Paul Mockapetris released the first version in 1984
  - RFCs 882 and 883
    - Superseded by 1034 and 1035

Chapter 2.5.1



DNS Service Structure

How can we identify and address Internet hosts?

DNS: domain name system

- People: many identifiers:
  - Name, passport #, National Insurance Number, etc.
- Internet hosts, routers:
  - IPv4 address (32 bit) - used for addressing datagrams
  - "name", e.g., www.yahoo.com - used by humans

Q: how to map between IP address and name, and vice versa?

- Domain Name System:
  - Distributed database implemented as a **hierarchy** of many name servers
  - Hosts and name servers communicate to resolve names (address/name translation) using Application-layer protocol
    - Note: core Internet function, implemented as application-layer protocol
    - Complexity at network's "edge"

DNS: services, structure

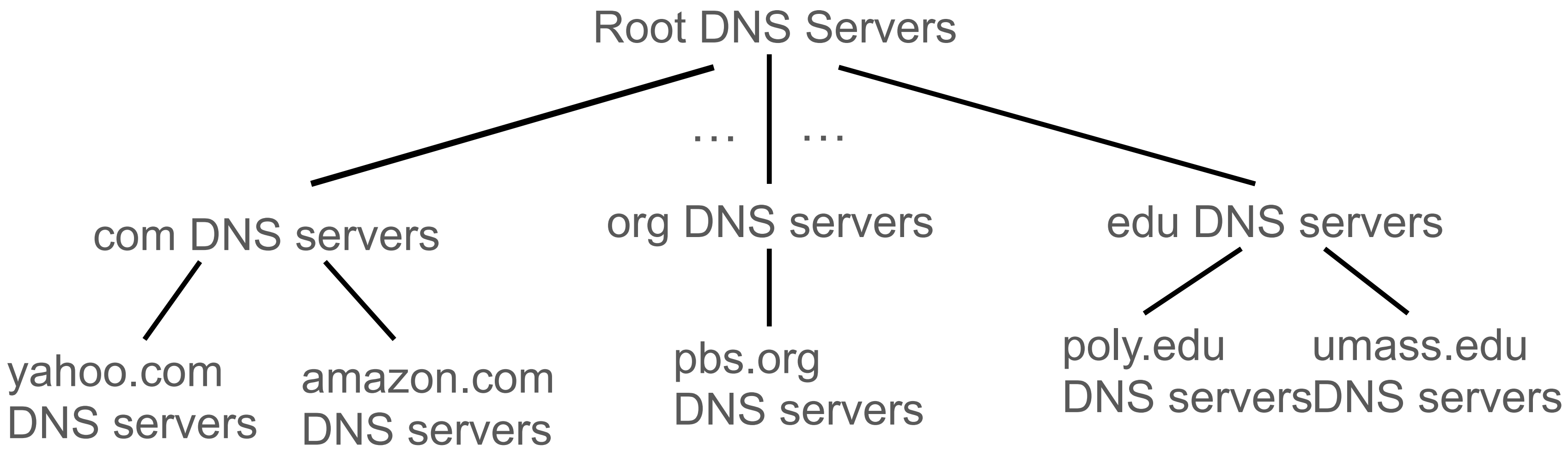
- DNS services
  - Hostname to IP address translation
  - Host aliasing
    - Alias names➔canonical
    - www.fb.com -> www.facebook.com
  - Mail server support
  - Load distribution
    - Replicated Web servers: many IP addresses correspond to one name

- Why not centralise DNS?
  - Single point of failure
  - Traffic volume
  - Maintenance

Basic answer: it wouldn’t scale!

DNS handles billions of queries per day!

DNS: a distributed, hierarchical database



Root DNS Servers

… …

com DNS servers

org DNS servers

edu DNS servers

yahoo.com DNS servers

amazon.com DNS servers

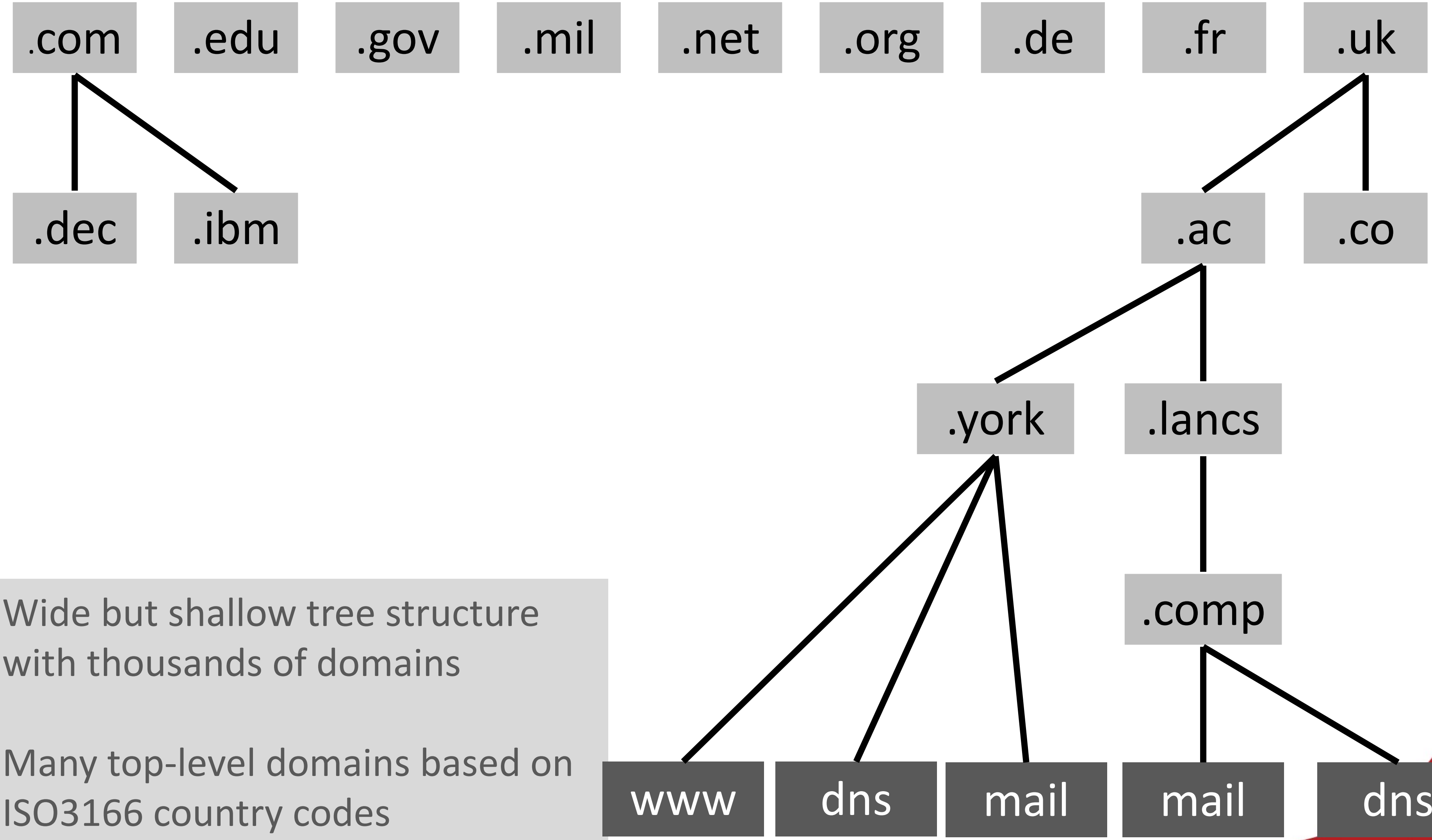
pbs.org DNS servers

poly.edu DNS servers

umass.edu DNS servers

- Client wants IP for www.amazon.com; 1st approximation:
  - Client queries root server to find .com DNS server
  - Client queries .com DNS server to get amazon.com DNS server
  - Client queries amazon.com DNS server to get IP address for www.amazon.com

Internet Domain Names



Wide but shallow tree structure with thousands of domains

Many top-level domains based on ISO3166 country codes

Subdomains

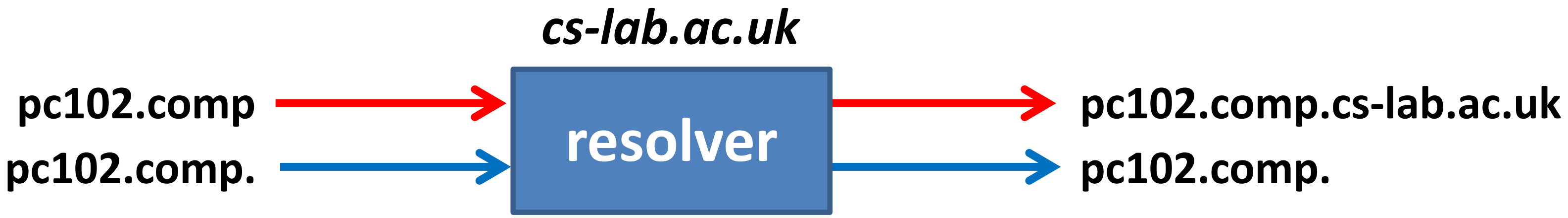
- A domain is a **subdomain** of another domain if its name ends in the other's name
  - So comp.lancs.ac.uk is a subdomain of
    - lancs.ac.uk

    which is sub-domain of
    - ac.uk

    which is sub-domain of
    - uk

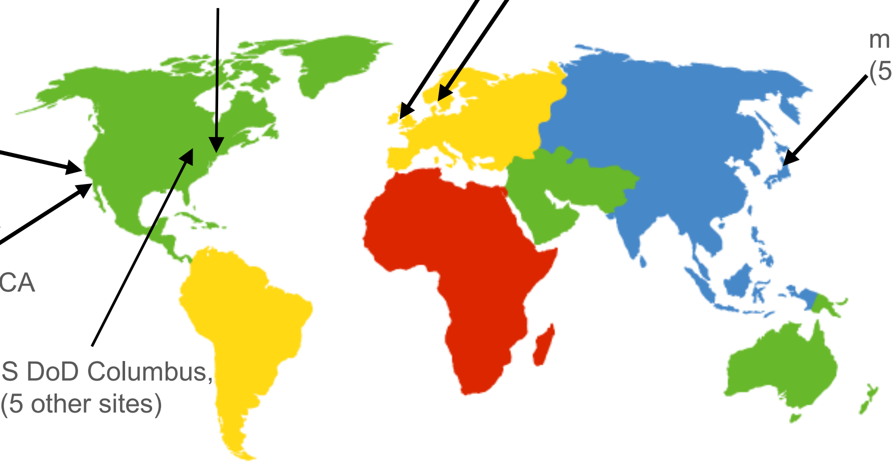
Fully Qualified Domain Names (FQDN)

- FQDNs end with a dot
  - – Implies rooted at top of DNS hierarchy
  - – No further resolution needed
  - – cs-lab.co.uk.
- Names without a dot can be extended toward root



Root name servers

- Contacted by local name server that cannot resolve a name



c. Cogent, Herndon, VA (5 other sites)
d. U Maryland College Park, MD
h. ARL Aberdeen, MD
j. Verisign, Dulles VA (69 other sites)

k. RIPE London (17 other sites)

i. Netnod, Stockholm (37 other sites)

e. NASA Mt View, CA
f. Internet Software C.
Palo Alto, CA (and 48 other sites)

m. WIDE Tokyo
(5 other sites)

a. Verisign, Los Angeles CA
(5 other sites)
b. USC-ISI Marina del Rey, CA
l. ICANN Los Angeles, CA
(41 other sites)

g. US DoD Columbus, OH (5 other sites)

13 logical root name “servers ” worldwide

- *actually, each “server” is replicated many times*

’13’ Root Servers

The magical few

a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

The '13' Root Servers

- Updated twice a day from non-public registry file server*
- Each server has a redundant backup
- They are also replicated across the globe
  - Many more than 13 physical machines!
  - Clients access closest servers
  - Addresses for one of each server hard-coded into resolvers etc.

** Currently performed by Verisign*

TLD, authoritative servers

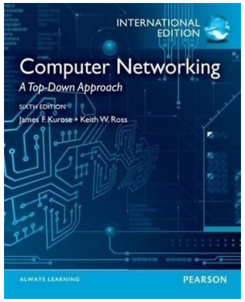
- Top-level domain (TLD) servers:
  - Responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
    - Network Solutions maintains servers for .com TLD
    - Educause for .edu TLD
- Authoritative DNS servers:
  - Organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts
  - Can be maintained by organization or service provider

Local DNS name server

- Does not strictly belong to hierarchy
- Each ISP (residential ISP, company, university) has one
  - Also called "default name server"
- When host makes DNS query, query is sent to its **local DNS server**
  - Has local cache of recent name-to-address translation pairs (but may be out of date!)
  - Acts as proxy, forwards query into hierarchy

Chapter 2.5.2

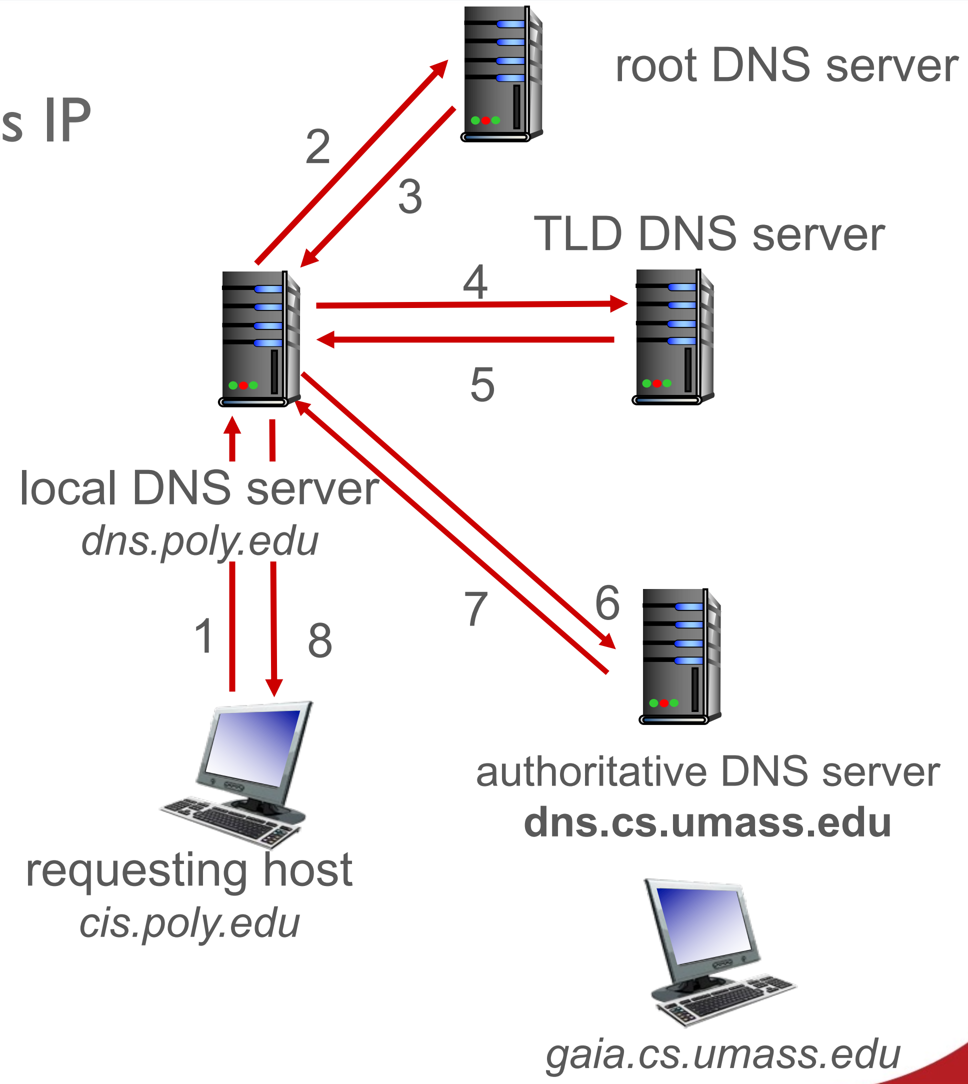
DNS: How does it work



Name resolution and other DNS services

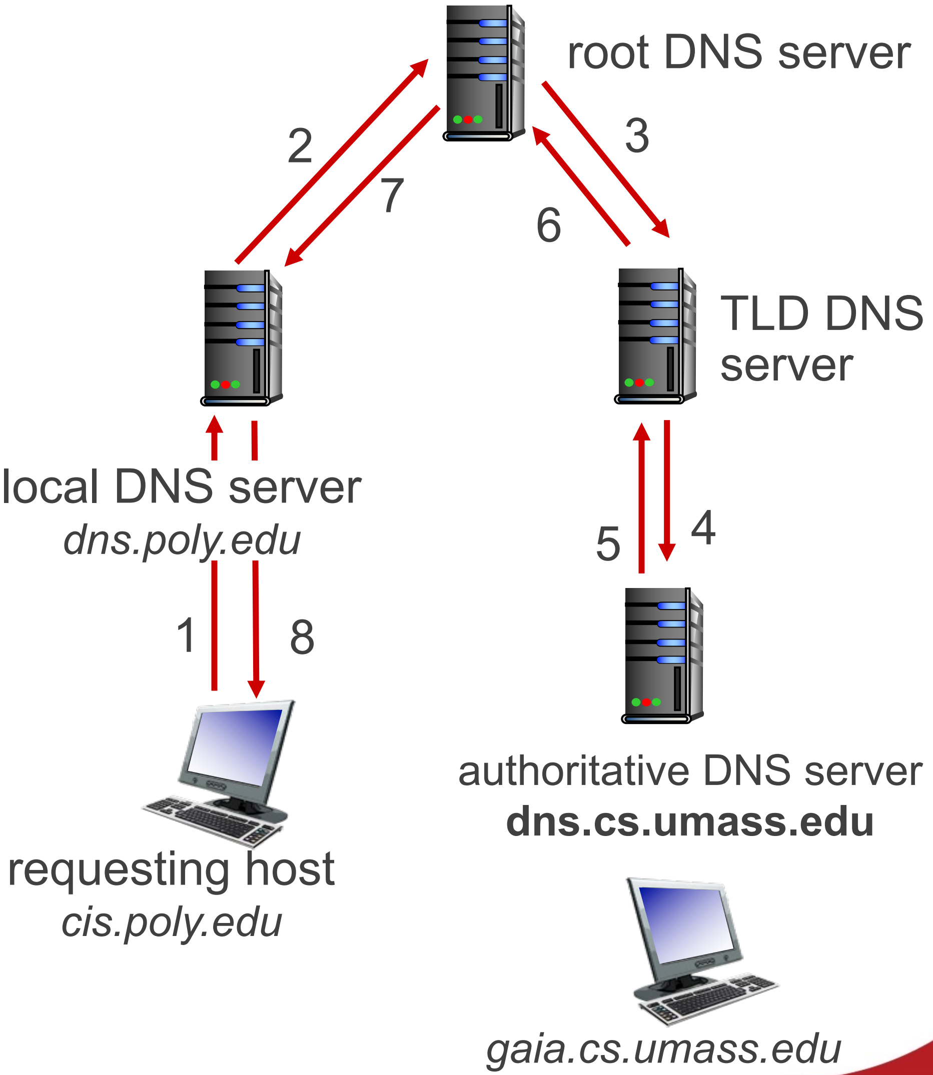
DNS name resolution example

- Host at cis.poly.edu wants IP address for gaia.cs.umass.edu
- *Iterative* query:
  - Contacted server replies with name of server to contact
  - "I don't know this name, but ask this server"



DNS name resolution example

- Recursive query:
  - Puts burden of name resolution on contacted name server
  - **Heavy load at upper levels of hierarchy?**

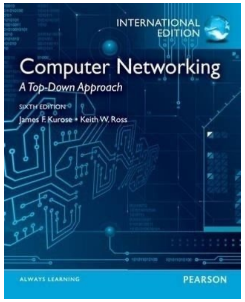


DNS: caching, updating records

- Once (any) name server learns a mapping, it *caches* it
  - Cache entries timeout (disappear) after some time (TTL)
  - TLD server content is typically cached in local name servers
    - Thus root name servers are not often visited
- But, cached entries may become *out-of-date* (best effort name-to-address translation!)
  - If name host changes IP address, may not be known Internet-wide until all TTLs expire
- Update/notify mechanisms proposed IETF standard
  - RFC 2136

Chapter 2.5.3

DNS Records and Messages



How DNS represents what it knows and exchange what it knows

DNS records

DNS servers store *resource records* (RRs)

RR format: `(name, value, type, ttl)`

type=A

- **`name`** is hostname
- **`value`** is IP address

type=NS

- **`name`** is domain (e.g., foo.com)
- **`value`** is hostname of authoritative name server for this domain

type=CNAME

- **`name`** is an alias for some "canonical" (the real) name
  - e.g. **`www.lancaster.ac.uk`** is really **`www.lancs.ac.uk`**
- **`value`** is canonical name

type=MX

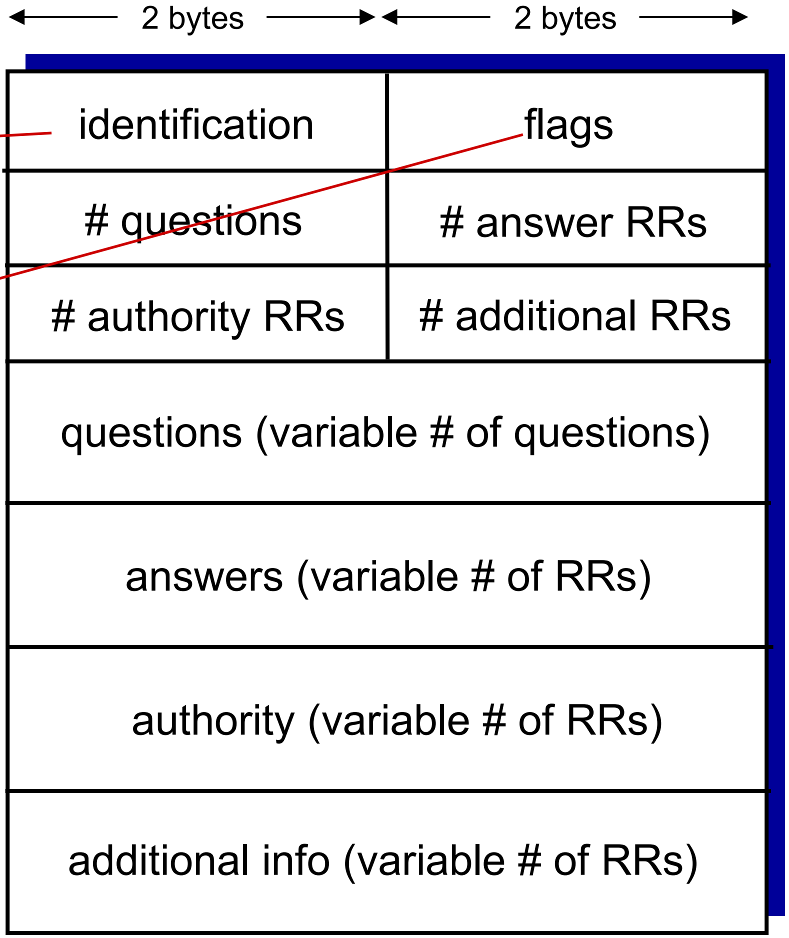
- **`value`** is name of mailserver associated with **`name`**

DNS protocol, messages

- Query and reply messages: both have same format

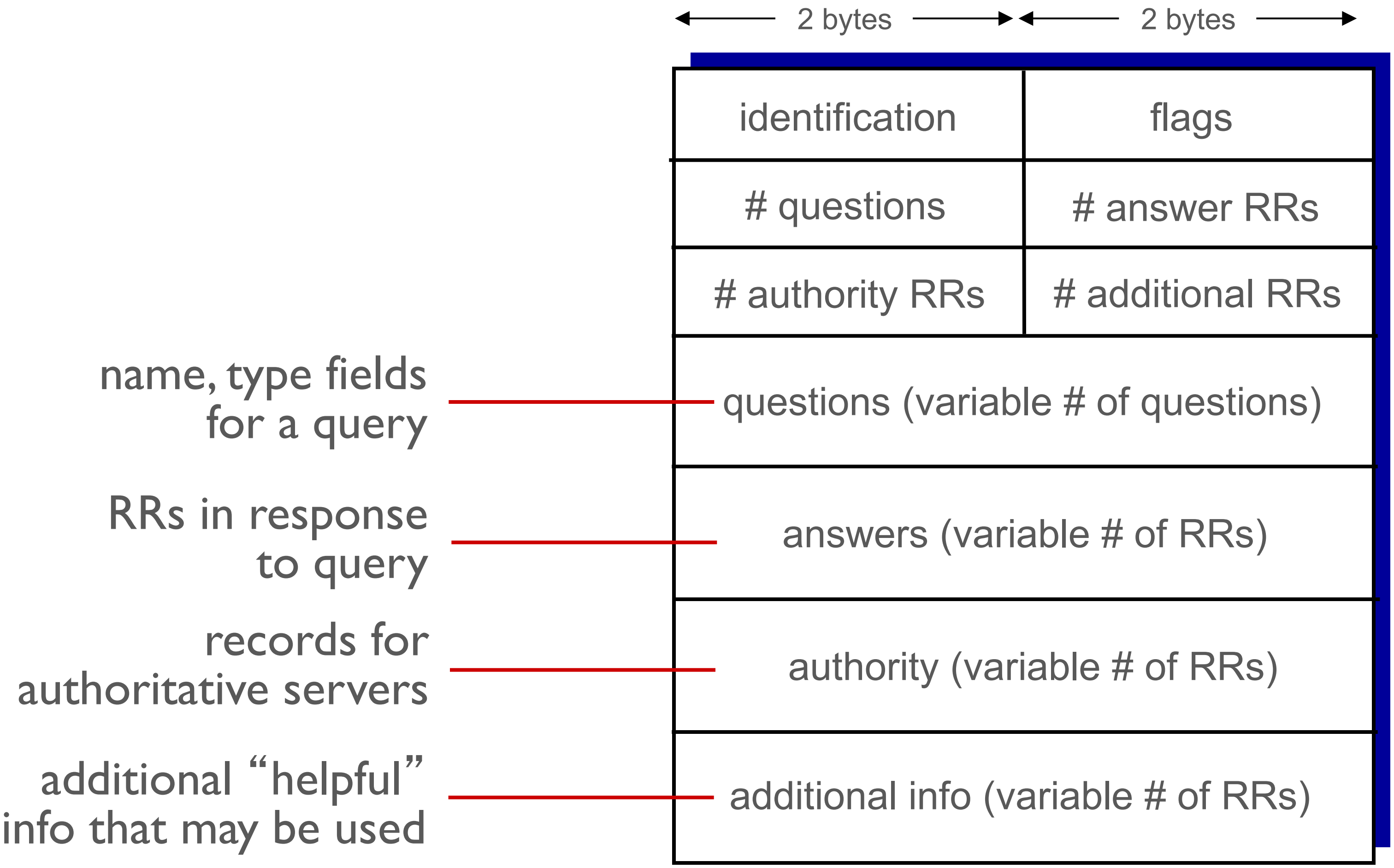
Message header

- Identification: 16 bit # for query, reply to query uses same #
- Flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative



2 bytes	2 bytes
identification	flags
# questions	# answer RRs
# authority RRs	# additional RRs
questions (variable # of questions)	
answers (variable # of RRs)	
authority (variable # of RRs)	
additional info (variable # of RRs)	

DNS protocol, messages



2 bytes

2 bytes

identification	flags
# questions	# answer RRs
# authority RRs	# additional RRs

questions (variable # of questions)

answers (variable # of RRs)

authority (variable # of RRs)

additional info (variable # of RRs)

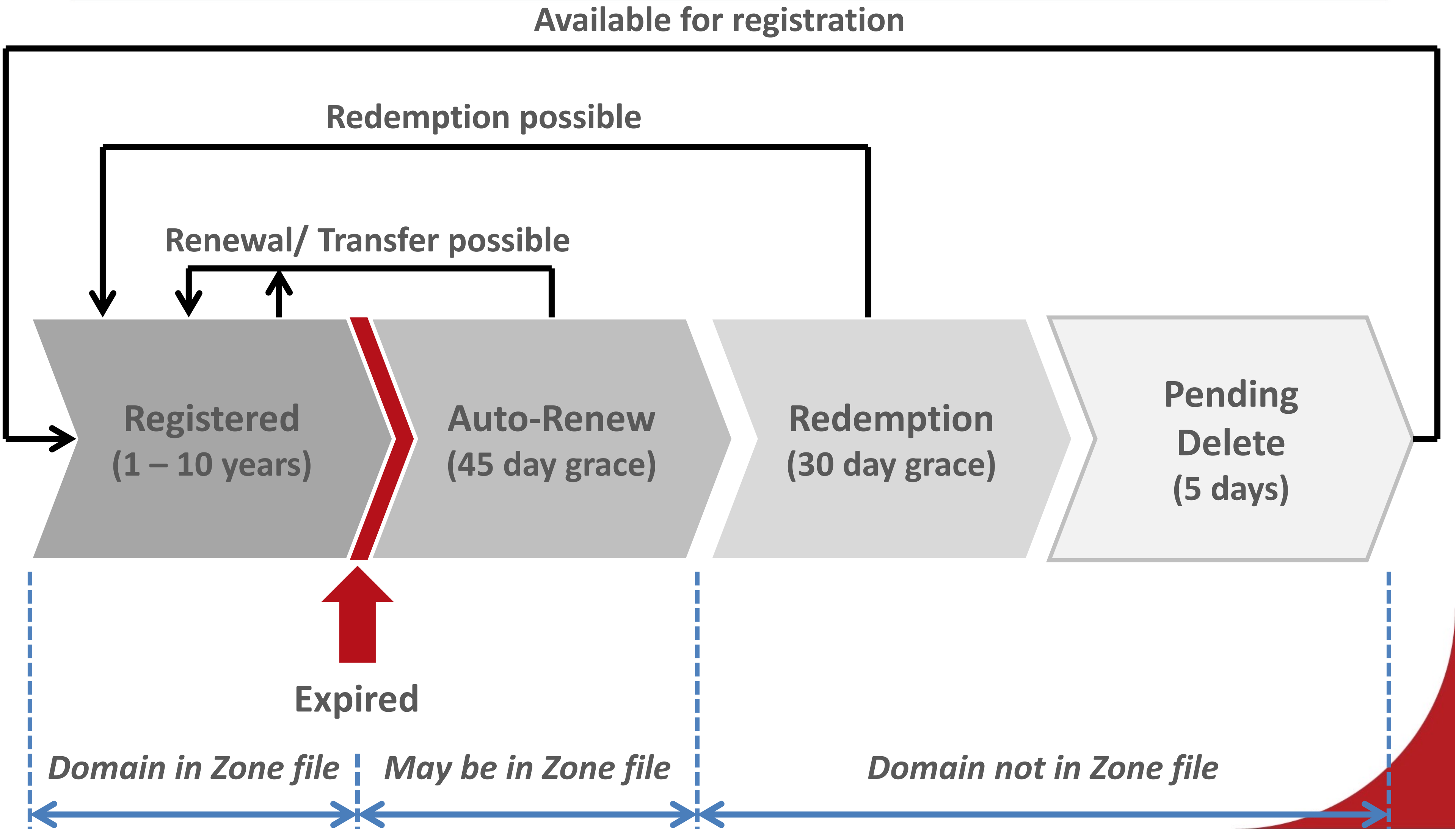
name, type fields for a query

RRs in response to query

records for authoritative servers

additional "helpful" info that may be used

Life of a DNS Registration



Available for registration

Redemption possible

Renewal/ Transfer possible

Registered
(1 – 10 years)

Auto-Renew
(45 day grace)

Redemption
(30 day grace)

Pending
Delete
(5 days)

Expired

Domain in Zone file

May be in Zone file

Domain not in Zone file

Inserting records into DNS

- Example: new startup "***Network Utopia***"
- Register name networkuptopia.com at *DNS registrar* (e.g., Network Solutions)
  - Provide names and IP addresses of authoritative name servers (primary and secondary)
  - Registrar inserts two RRs into .com TLD server:

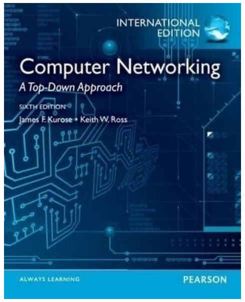
    ```
    (networkutopia.com, dns1.networkutopia.com, NS)
    (dns1.networkutopia.com, 212.212.212.1, A)
    ```
- Create authoritative server and insert:
  - type A record for www.networkuptopia.com
  - type MX record for networkutopia.com

What happens if DNS is slow or unreliable?

- Really depends…
- Can induce significantly delay to a request
  - Already 1 RTT
  - Usually *ms* (could be longer depending on resolution and local DNS state)
  - A blocking operation!
- If the target RR is cached at the host, then we don't need to look up
  - Valid until the cache expires

Chapter 2.5.3

DNS Security



Excursion on DNS Vulnerabilities

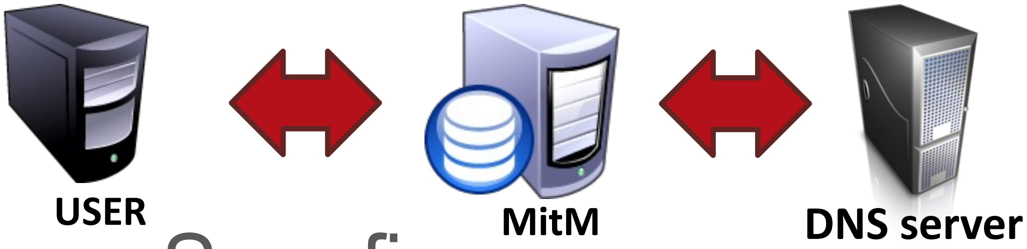
Attacking DNS

- DDoS attacks
  - Bombard root servers with traffic
    - Not successful to date
      - October 2002: massive DDoS against the root name servers
      - What was the effect?
        - » … users didn't even notice
      - Root zone file is cached almost everywhere

- Bombard TLD servers
  - Potentially more dangerous
- Redirect attacks
  - Man-in-middle
    - Intercept queries
  - DNS poisoning
    - Send bogus replies to DNS server, which caches
- Exploit DNS for DDoS
  - Send queries with spoofed source address: target IP
  - Requires amplification

DNS Hijacking

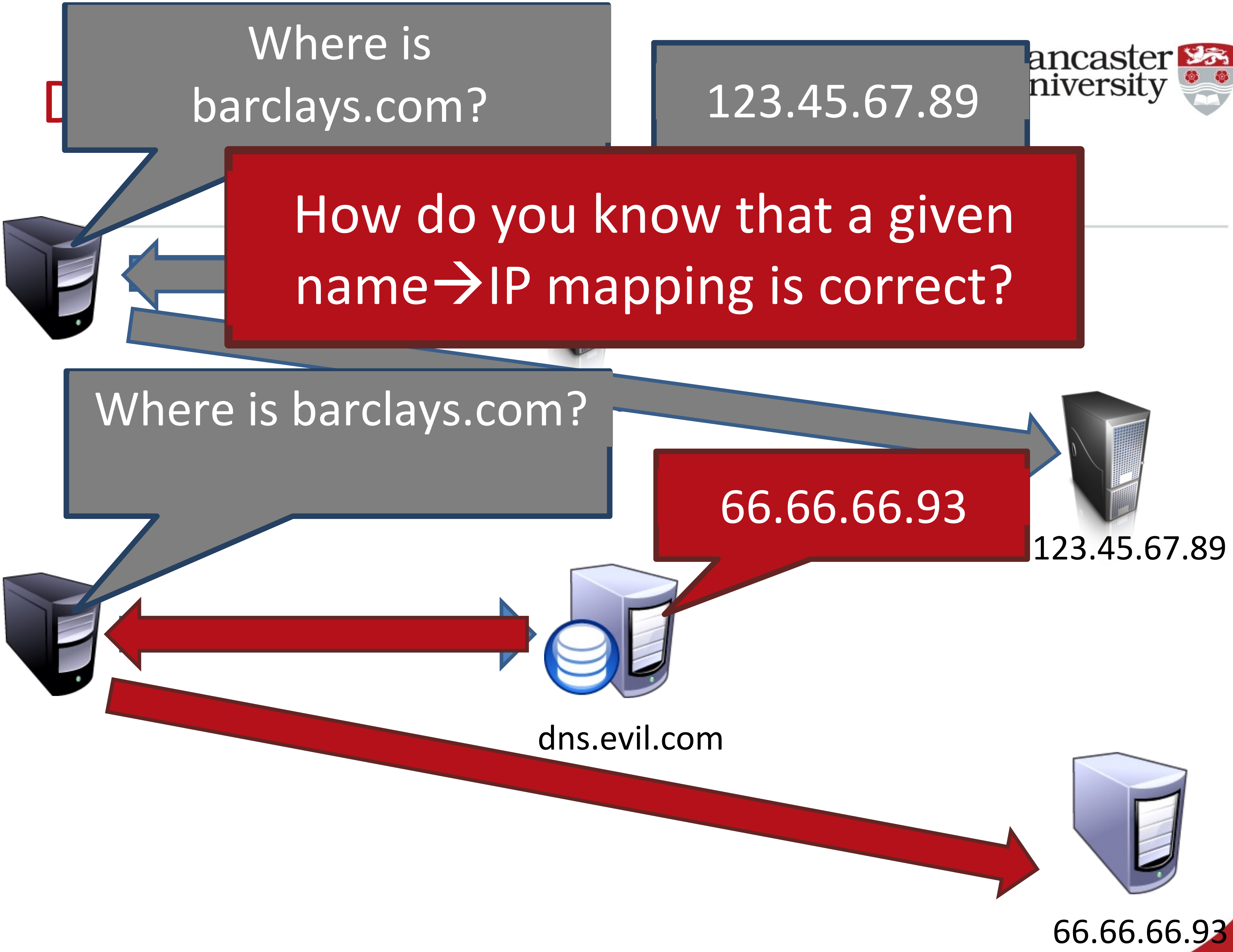
- Infect OS or browser with a virus/trojan
  - e.g. Many trojans change entries in /etc/hosts
  - *.bankofamerica.com → evilbank.com
- Man-in-the-middle



- Response Spoofing
  - Eavesdrop on requests
  - Outrace the servers response

DNS Hijacks: *ID Prediction*

- Requester will believe first response it sees
  - Dangerous if query for server A record
  - Disaster if query for Name Server (use this for subsequent queries)
  - Response must
    - Have correct query ID
    - Be to requester’s port number
  - On many early systems these could be predicted
- We now randomise
  - Query IDs
  - Source ports for queries



Where is barclays.com?

123.45.67.89

How do you know that a given name→IP mapping is correct?

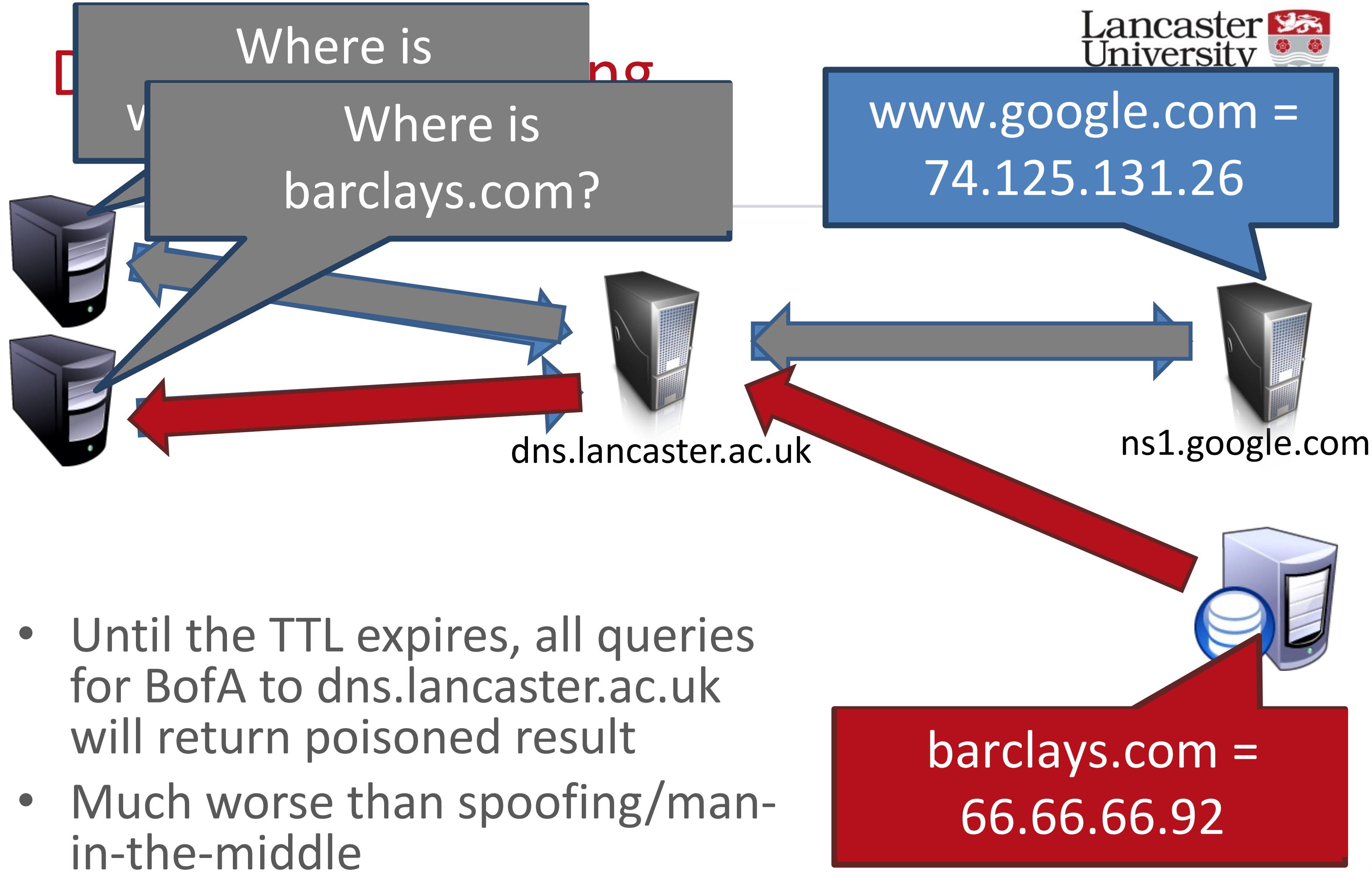
Where is barclays.com?

66.66.66.93

123.45.67.89

dns.evil.com

66.66.66.93



- Until the TTL expires, all queries for BofA to dns.lancaster.ac.uk will return poisoned result
- Much worse than spoofing/man-in-the-middle
    - Whole ISPs can be impacted!

Solution: DNSSEC

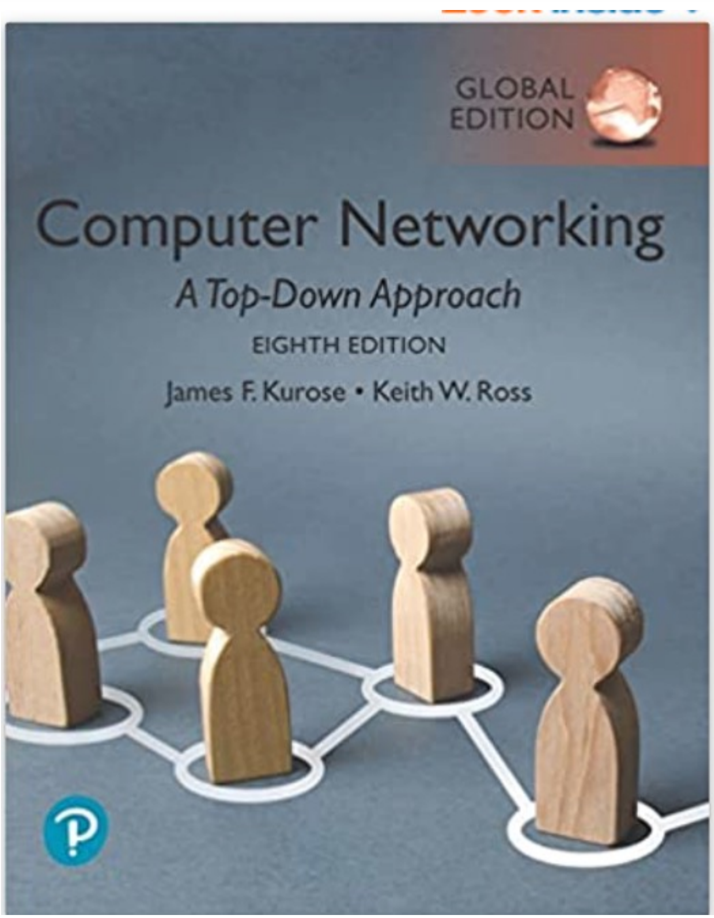
- Cryptographically sign critical resource records
  - Resolver can verify the cryptographic signature
- Two new resource types
  - Type = DNSKEY
    - Name = Zone domain name
    - Value = Public key for the zone
  - Type = RRSIG
    - Name = (type, name) tuple, i.e. the query itself
    - Value = Cryptographic signature of the query results
- Deployment
  - On the roots since July 2010
  - Verisign enabled it on .com and .net in January 2011
  - Comcast is the first major ISP to support it (January 2012)

Summary

- Naming & Addressing
  - Internet Domain Names vs. Addresses
  - History of Naming & Address resolution
  - Domain Name System Basics
- Domains & Name Allocation
    - DNS Names Space & Structure
    - Name resolution
- DNS Protocol & Service
  - Query resolution
  - DNS message format
  - Service handling
- DNS Security Issues

Reading Material

- □ Section 2.4 in Chapter 2



GLOBAL EDITION

Computer Networking

A Top-Down Approach

EIGHTH EDITION

James F. Kurose • Keith W. Ross

Thanks for listening!

Any questions?