Reti di Calcolatori

Prof. Roberto Canonico
Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

Corso di Laurea in Ingegneria Informatica

Il sistema DNS

I lucidi presentati al corso sono uno strumento didattico che NON sostituisce i testi indicati nel programma del corso

Nota di copyright per le slide COMICS

Nota di Copyright

Autori:
Simon Pietro Romano, Antonio Pescapè, Stefano Avallone,
Marcello Esposito, Roberto Canonico, Giorgio Ventre

Università degli Studi di Napoli
Federico II

Domain Name System (DNS)

- Tutti noi siamo oggi abituati a raggiungere un servizio (e quindi il calcolatore che lo offre) utilizzando nomi simbolici di facile memorizzazione:
  - www.google.com
  - www.rai.it
  - pippo@unina.it
- Questi nomi non sono immediatamente adatti ad essere compresi dai dispositivi che costituiscono la rete Internet
- Un nome di questo tipo, infatti, non dà informazioni esatte sulla dislocazione sul territorio della macchina che si desidera contattare
- I router, di conseguenza, non saprebbero come instradare i dati in maniera tale da raggiungere la destinazione

Nomi simbolici vs Indirizzi IP

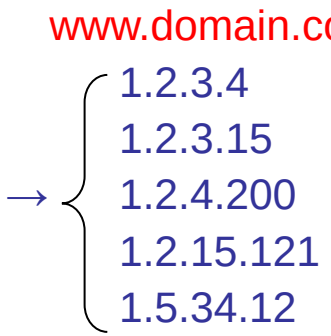
- La rete Internet è stata progettata invece per lavorare con indirizzi di diversa natura. Per es.:
  - 143.225.229.3
  - 217.9.64.225
- Questi indirizzi, detti indirizzi IP, sono formati da 4 numeri che vanno da 0 a 255 separati da un punto.
- Ogni dispositivo nella rete Internet ha un tale indirizzo; esso permette l'identificazione univoca a livello globale e la localizzazione
- A differenza dei nomi simbolici, essendo gli indirizzi IP di lunghezza fissa, sono più facilmente gestibili dalle macchine

Il servizio DNS

- Non volendo rinunciare alla comodità di lavorare con nomi simbolici, è stato necessario progettare un servizio di risoluzione dei nomi simbolici in indirizzi IP
- Tale servizio associa ad un nome simbolico univoco (www.grid.unina.it) un indirizzo IP (143.225.229.3) permettendo così di raggiungere la macchina
- Questo servizio si chiama Domain Name System (DNS) ed è definito in RFC1034 e RFC1035
  - Ideato nel 1983 da Paul Mockapetris
- Esso si basa sullo scambio di messaggi UDP sul porto 53

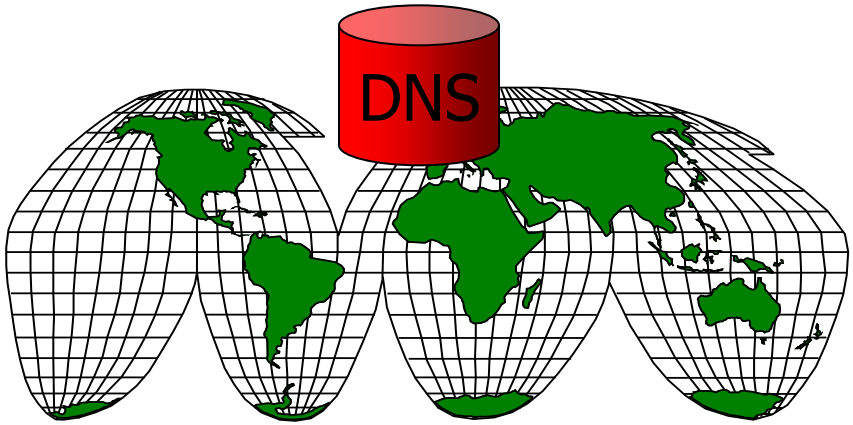
Altre funzionalità offerte

- Alias degli hostname:
  - ad una macchina con un nome complicato può essere associato un “soprannome” più piccolo e semplice da ricordare.
    P.es.: rcsn1.roma.rai.it → www.rai.it
- Alias dei server di posta:
  - permette di associare un server di posta al nome di un dominio per facilitare la memorizzazione dell’indirizzo di posta
  - Es.: pippo@unina.it identifica l’utente pippo sulla macchina mailsrv1.cds.unina.it.
    L’associazione @unina.it → mailsrv1.cds.unina.it
    è realizzata dal servizio DNS
- Distribuzione del carico:
  - quando un server gestisce un carico troppo elevato si suole replicare il suo contenuto su molte macchine differenti. Il servizio DNS distribuisce il carico tra le macchine rilasciando ciclicamente indirizzi appartenenti all’intero pool, senza che gli utenti si accorgano di nulla



DNS centralizzato?

- Si potrebbe pensare di risolvere il problema piazzando in un unico punto della terra una macchina che realizzi la risoluzione di tutti i nomi

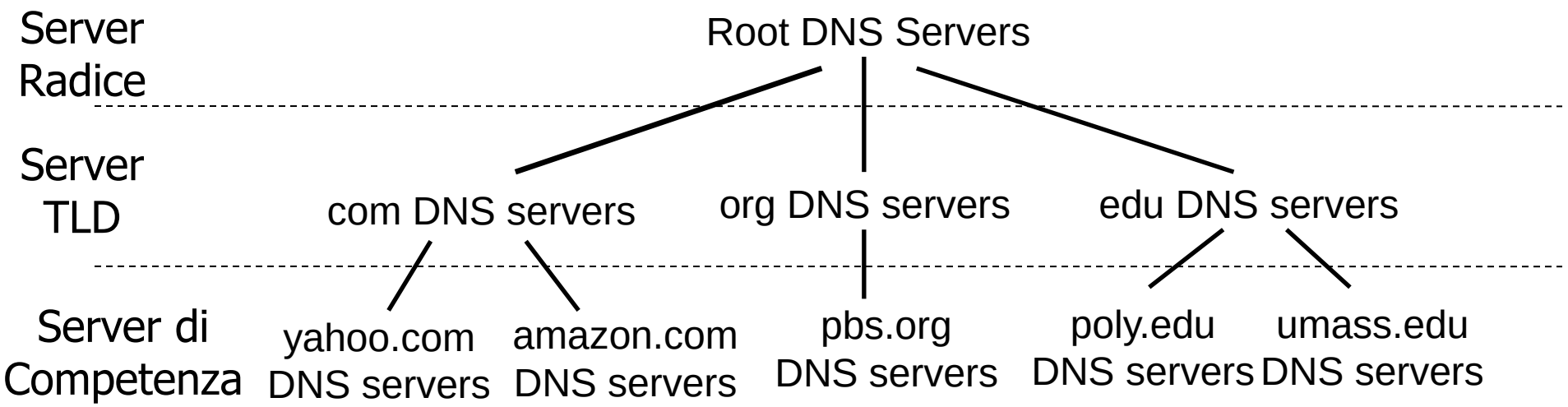


- Questa soluzione, sebbene teoricamente realizzabile, ha così tanti svantaggi da risultare impraticabile:
  - Single Point of Failure
  - Volume di traffico
  - Database distante
  - Manutenzione

DNS distribuito!

- Si distribuiscono le informazioni tra varie entità server
- Ciascuna ha la responsabilità di raccogliere, gestire, aggiornare e divulgare le informazioni che la riguardano
- In particolare l'approccio è di tipo gerarchico:
  - gli elementi più alti nella gerarchia contengono molte informazioni non dettagliate
  - gli elementi più bassi nella gerarchia contengono poche informazioni dettagliate
- Attraverso un colloquio concertato tra le entità (di cui gli utenti non hanno percezione) si riesce a fornire il servizio di risoluzione

DNS: un database gerarchico e distribuito



Un Client richiede l'IP di www.amazon.com (1st approx):

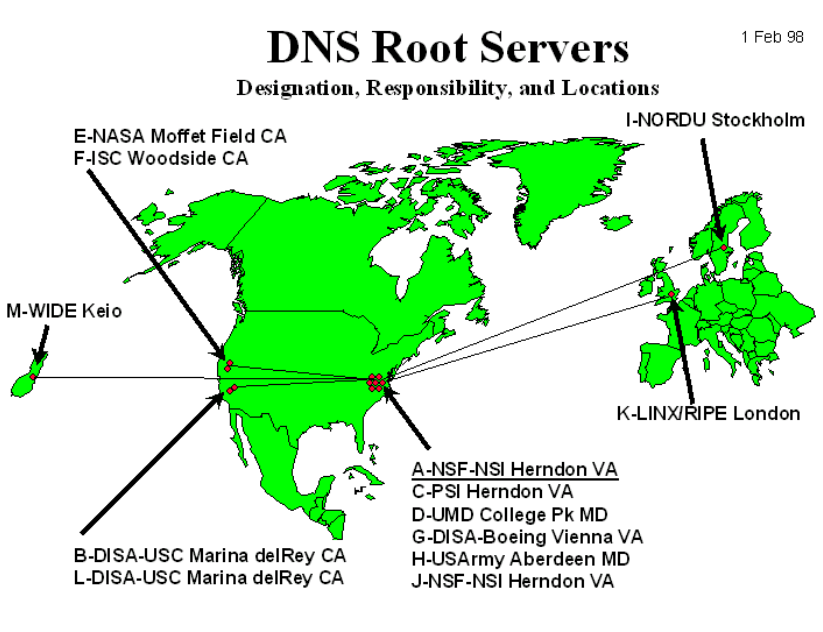
- Il client dapprima contatta uno dei root server per avere la lista degli indirizzi IP dei TLD per il dominio com
- Il client contatta uno dei TLD server che gli restituisce l'indirizzo IP del server autorizzato per amazon.com
- Infine il client contatta il server autorizzato per amazon.com che gli restituisce l'indirizzo IP di www.amazon.com

DNS: attori

- Resolver
  - È il client da cui parte la richiesta di risoluzione al sistema DNS
  - È una funzionalità user-level del sistema operativo dell'end system
- Registry
  - È titolare della risoluzione di un determinato name space
  - È l'organizzazione abilitata a fare modifiche al database dei nomi di un determinato dominio
  - Mantiene in esercizio i server autoritativi per un determinato dominio
- Registrar
  - È l'agente che sottomette al registry le richieste di modifica di risoluzione per conto del registrant
- Registrant
  - È l'entità che "possiede" l'uso di un determinato dominio

Tipologie di server DNS (Root)

- Root Name Server
  - 13 root server logici in Internet (etichettati da A ad M) i cui indirizzi IP sono ben noti alla comunità
  - In realtà si tratta di 376 diversi server fisici (vedi http://www.root-servers.org/)
  - Ad essi si riferiscono i Local Name Server che non possono soddisfare immediatamente una richiesta di risoluzione
  - Il Local Name Server si comporta come client DNS ed invia una richiesta di risoluzione al Root Name Server



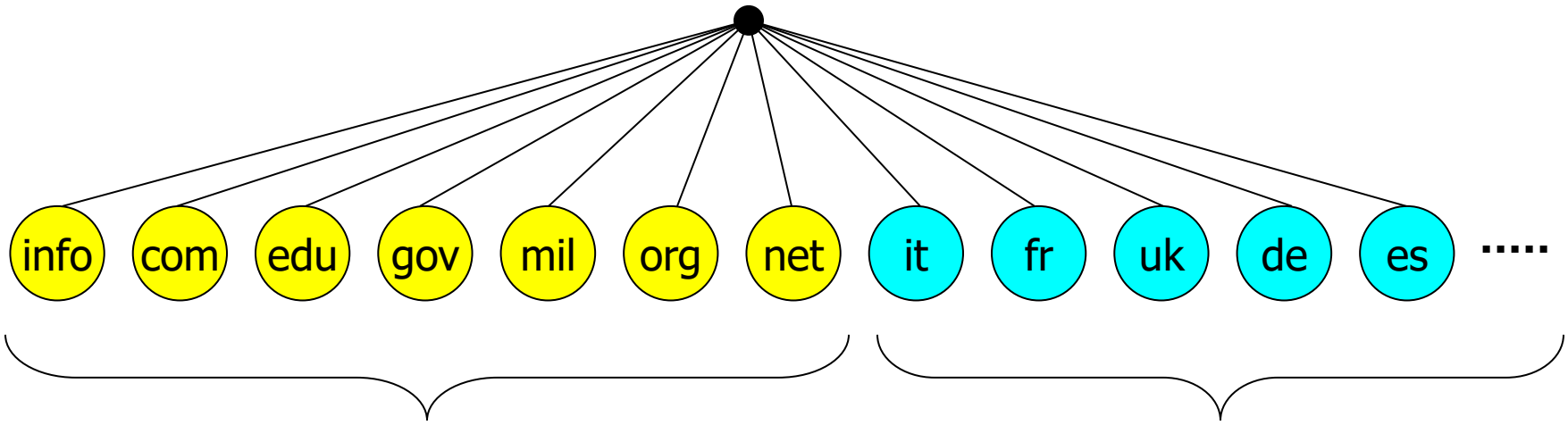
List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
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, Information Sciences Institute
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

Fonte: https://www.iana.org/domains/root/servers

I "top-level domain" server (TLD)

- Questi server si occupano dei domini di alto livello (generici e geografici)



Domini TLD: 20 generici (gTLD) + 248 geografici (ccTLD)

Tipologie di server DNS (Authoritative)

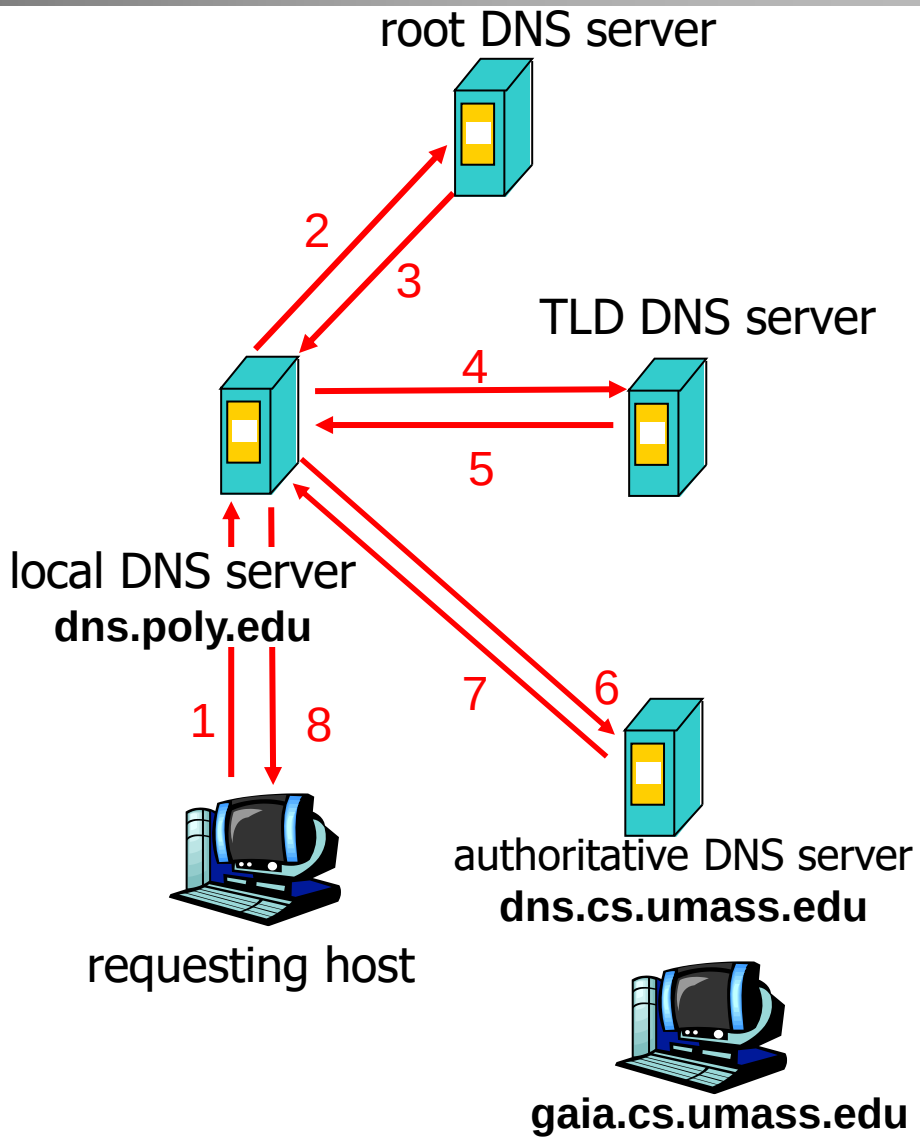
- Authoritative Name Server (Assoluto)
  - È un server dei nomi capace di risolvere tutti i nomi all'interno di un determinato dominio
    - Es.: un server dei nomi assoluto per il dominio **unina.it** deve essere capace di risolvere tutti i nomi del tipo ***xyz.unina.it***
  - Ad esso si riferiscono i Name Server TLD quando devono risolvere un indirizzo del dominio
  - Può essere mantenuto dall'organizzazione che ha titolo all'uso del dominio o da un provider che gestisce il servizio di risoluzione dei nomi per conto del proprietario del dominio

Local Name Server

- Local Name Server
  - Ciascun operatore di rete ne installa uno nella propria rete
  - Gli host di una rete sono configurati con l'indirizzo del DNS server locale
    - Questa configurazione può avvenire o manualmente o in maniera automatica
    - Tutti gli host della rete richiedono a questo server il servizio di risoluzione
  - Un Local Name Server non appartiene alla gerarchia di server
    - Un Local Name Server opera da proxy ed invia la query alla gerarchia di server DNS restituendo ai client le risposte finali
  - L'uso di un server DNS locale consente ai client di fare una sola query DNS verso di essi
    - il local DNS server interroga i server della gerarchia secondo una sequenza descritta nelle slide successive
    - i local DNS server sono anche detti *recursive name servers*
      - Il motivo sarà chiaro nelle slide successive
  - Alcuni operatori over-the-top gestiscono server pubblici con funzione di "DNS server locale"
    - Google: 8.8.8.8 ed 8.8.4.4
    - Cloudflare: 1.1.1.1 ed 1.0.0.1

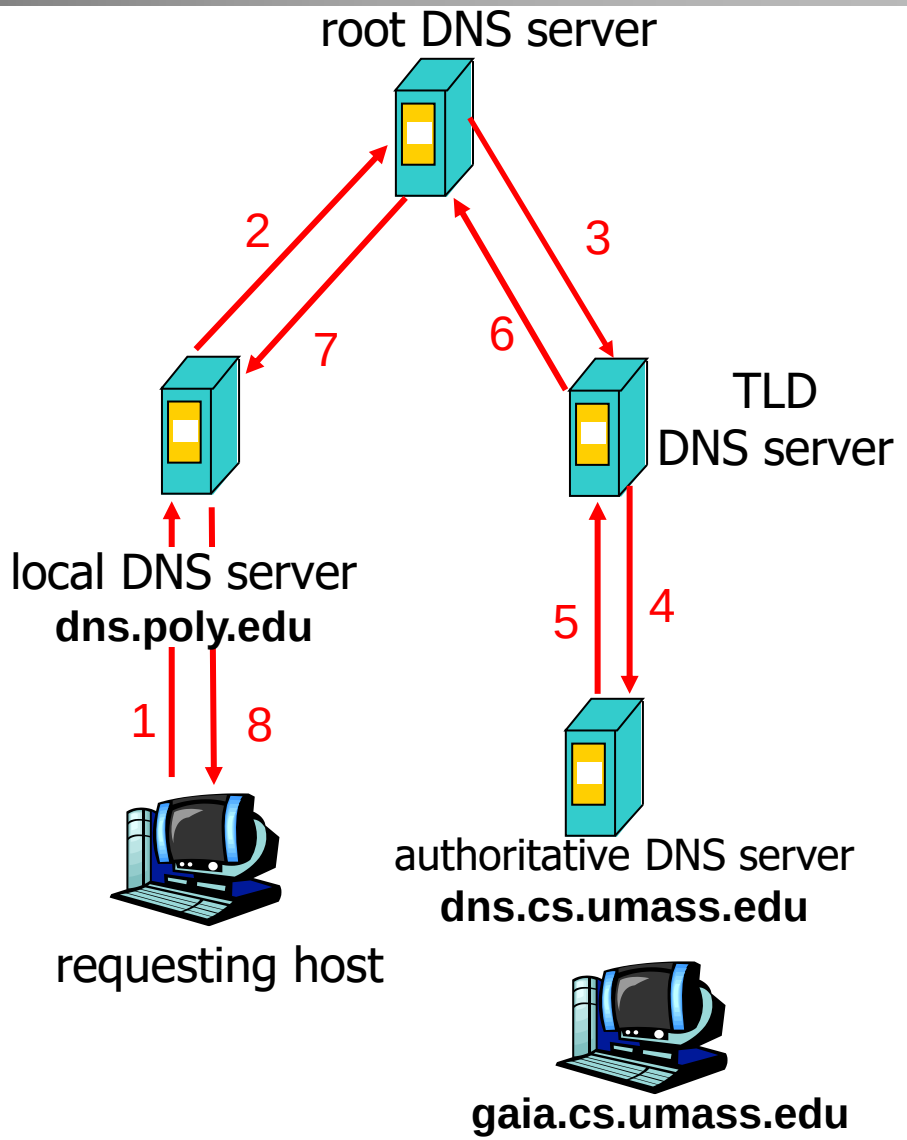
Risoluzione con query iterative

- Un host richiede al server DNS locale della rete poly.edu l'indirizzo IP di ***gaia.cs.umass.edu***
- ***1° caso: il server DNS locale genera*** *query iterative*:
  - Il server contattato risponde con il nome del server da contattare
  - Logica: *non conosco questo nome, ma conosco il nome di qualcuno a cui poter chiedere*



Risoluzione con query ricorsive

- Un host richiede al server DNS locale della rete poly.edu l'indirizzo IP di ***gaia.cs.umass.edu***
- ***2° caso: il server DNS locale e gli altri generano*** *query ricorsive*:
  - Si chiede al server contattato di fornire la risoluzione completa
  - Problema: *carico eccessivo sui server al vertice della gerarchia*
- **NOTA:** anche nel caso precedente, la query inviata dal client al server DNS locale era di tipo ricorsivo
- Per questo motivo, i server DNS locali sono detti server ricorsivi
- Non tutti i server accettano query ricorsive

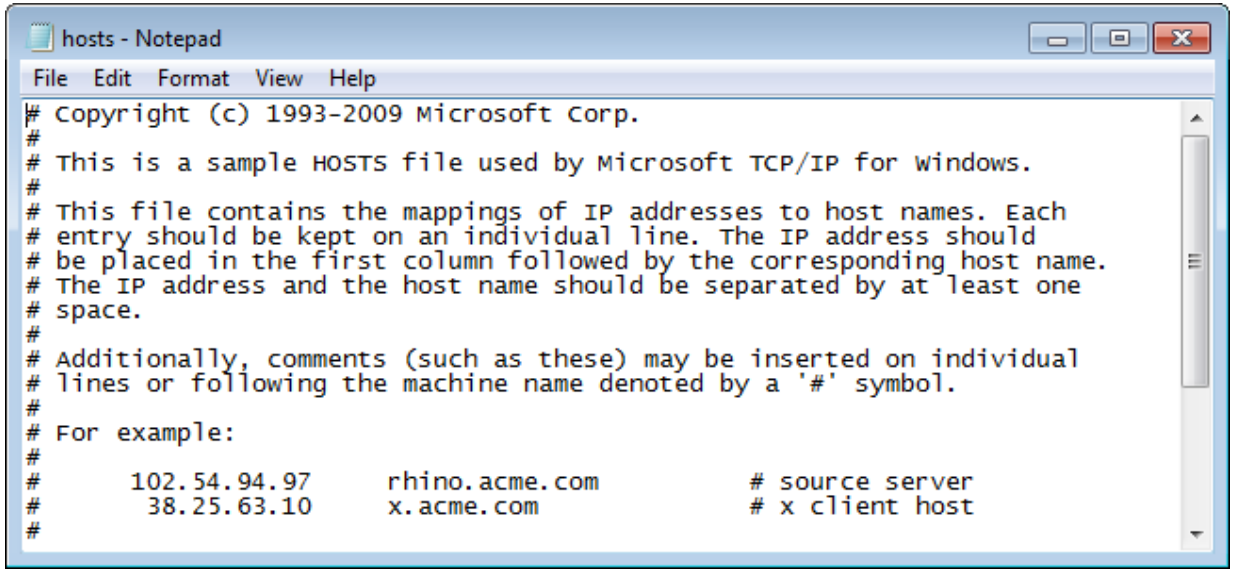


Un esempio a più livelli

- Il TLD potrebbe non contattare necessariamente l'Authoritative Name Server finale, ma un Authoritative Name Server intermediario
- Sarà il server intermedio a fornire il nome del server di competenza
- In questi casi il numero di messaggi DNS aumenta

Il file hosts

- Prima di interrogare il sistema DNS, il DNS resolver presente negli end-system controlla una eventuale corrispondenza:
  `indirizzo-IP  nome`
  presente nel file di sistema hosts
- In Unix/Linux è il file: /etc/hosts
- In Windows è il file: C:\Windows\System32\Drivers\Etc\hosts



Il caching dei nomi

- Per esigenze di efficienza sia il client DNS presente negli end-system che i server DNS memorizzano localmente un certo numero di corrispondenze
- Per evitare che informazioni non aggiornate restino nella rete, dopo un certo tempo (circa un giorno), le associazioni vengono eliminate dalla cache
- Ad es. un server locale può memorizzare associazioni IP/nomi non di sua competenza e/o gli indirizzi dei server TLD in modo da aggirare i server root

Cosa memorizza un DNS

Resource records (RR)

Formato RR: **(Nome, Valore, Tipo, TTL)**

- TTL: tempo di vita residuo di un record scaduto il quale viene eliminato dalla cache
- Il significato di Nome e Valore dipende da Tipo:

- Tipo=A
  - **nome**=hostname
  - **valore**= indirizzo IPv4
- Tipo=AAAA
  - **nome**=hostname
  - **valore**= indirizzo IPv6
- Tipo=NS
  - **nome**=dominio (es.: unina.it)
  - **valore**=ind. IP dell'Authoritative NS
- Tipo=CNAME
  - **nome**=alias per il nome canonico (reale)
  - **valore**=nome canonico
- Tipo=MX
  - **nome=**dominio di posta (es. libero.it)
  - **valore**=nome dell'host mailserver associato a **nome**

Esempi di RR

- Type A
  - relay.bar.foo.com, 145.37.93.126, A
- Type NS
  - foo.com, dns.foo.com, NS
- Type CNAME
  - foo.com, relay.bar.foo.com, CNAME
- Type MX
  - foo.com, mail.bar.foo.com, MX
- Type AAAA
  - www.bar.com, 2001:734:3403:fffa::7, AAAA

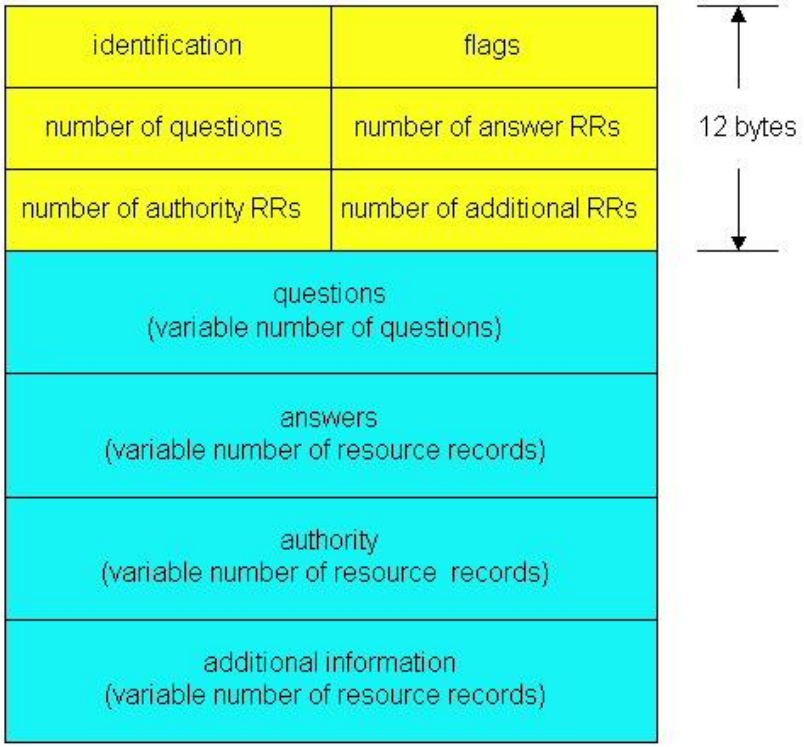
* Negli esempi non è mostrato il valore del campo TTL

Il formato dei messaggi (1)

Protocollo DNS : *richieste e risposte*, entrambe con lo stesso formato di messaggio

Header del mess.:

- identification: diverso numero di 16bit per ogni richiesta. Le risposte usano lo stesso identificativo
- flags:
  - risposta a richiesta
  - ricorsione desiderata
  - ricorsione disponibile
  - risposta authoritative



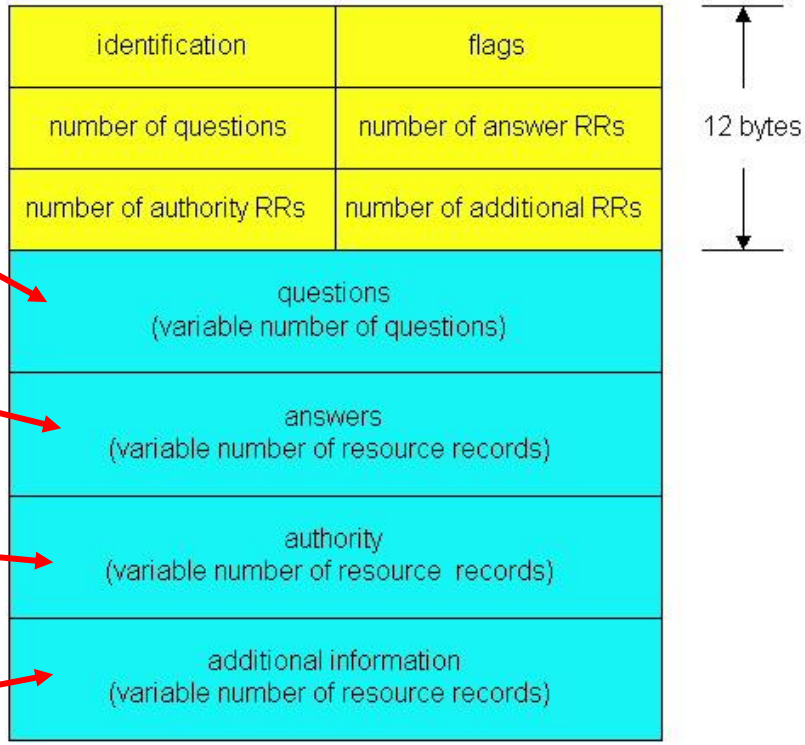
Il formato dei messaggi (2)

Nome e tipo per una richiesta

RR in risposta ad una richiesta

records per server authoritative

informazioni addizionali utili che possono essere utilizzate



Il software BIND

- BIND (Berkeley Internet Name Domain) è una implementazione dei protocolli Domain Name System (DNS)
- È liberamente re-distribuibile
- È costituito dai seguenti componenti:
  - Un server DNS (named)
  - Una libreria per la risoluzione dei nomi di dominio
  - Strumenti di diagnostica
- Questa implementazione è la più utilizzata in Internet su sistemi Unix-like

Configurazione di BIND: un esempio di file di zona

```
$TTL 3600
@       IN SOA grid.grid.unina.it. root.grid.grid.unina.it. (
                        2004020901      ; Serial
                        10800           ; Refresh
                        3600            ; Retry
                        604800          ; Expire
                        86400 )         ; Minimum TTL
; Machine Name
localhost       A       127.0.0.1

vesuvio         A       143.225.229.1
grid            A       143.225.229.3
honolulu        A       143.225.229.111
comicserver     A       143.225.229.112
...
; Aliases
www         CNAME   grid
ftp         CNAME   grid
news        CNAME   grid
tesisti     CNAME   vesuvio
www.tesisti CNAME   vesuvio

; MX Record
            MX      10      grid.grid.unina.it.
```

* SOA: Start of Authority

Significato di alcuni parametri

- **Serial**: numero seriale progressivo utilizzato per rilevare aggiornamenti del file. Di solito usa il formato: aaaammggxx
- **Refresh**: intervallo in secondi tra due successivi prelievi del file di zone da parte di un DNS server
- **Retry**: intervallo in secondi tra tentativi successivi di recuperare una zona in caso di fallimento
- **Expire**: tempo in secondi che deve trascorrere per ritenere scadute le informazioni di una zona che non si riesce ad aggiornare
- **Minimum TTL**: tempo di durata di default delle singole entry del file di zona

Un esempio: configurazione del Reverse DNS

```
$TTL 3600

@       IN SOA  grid.grid.unina.it. root.grid.grid.unina.it. (
                        2004020901      ; Serial
                        10800           ; Refresh
                        3600            ; Retry
                        604800          ; Expire
                        86400 )         ; Minimum TTL
; DNS Servers
                NS      grid.grid.unina.it.

; Machine Name
1               PTR     vesuvio.grid.unina.it.
3               PTR     grid.grid.unina.it.
111             PTR     honolulu.grid.unina.it.
112             PTR     comicserver.grid.unina.it.
```

Il file named.root

```
.                        3600000   IN   NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000        A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000        NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000        A     128.9.0.107
;
; formerly C.PSI.NET

...

.                        3600000        NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000        A     198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                        3600000        NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000        A     202.12.27.33
; End of File
```

Un esempio di uso di nslookup

```
> nslookup
> www.cisco.com
Server:         143.225.229.3
Address:        143.225.229.3#53
Non-authoritative answer:
Name:   www.cisco.com
Address: 198.133.219.25
> set ty=ns
> cisco.com
Server:         143.225.229.3
Address:        143.225.229.3#53
Non-authoritative answer:
cisco.com       nameserver = ns1.cisco.com.
cisco.com       nameserver = ns2.cisco.com.
Authoritative answers can be found from:
ns1.cisco.com   internet address = 128.107.241.185
ns2.cisco.com   internet address = 64.102.255.44
> server ns1.cisco.com
Default server: ns1.cisco.com
Address: 128.107.241.185#53
> set ty=a
> www.cisco.com
Server:         ns1.cisco.com
Address:        128.107.241.185#53

Name:   www.cisco.com
Address: 198.133.219.25
```

Chiedo di risolvere l'host

Indirizzo del local DNS che serve la richiesta

Ecco la risposta, che non proviene da un server

Imposto nslookup per l'invio di query di tipo NS: restituirà i name server authoritative di un dominio specificato

Chiedo il Name Server authoritative per il dominio cisco.com

Eccoli: sono due

E questi sono i loro indirizzi IP

Imposto nslookup per l'invio delle successive query al NS ns1.cisco.com

Reimposto nslookup per l'invio di query di tipo A (risoluzione di nomi di host) e richiedo la risoluzione del nome di host www.cisco.com

Questa volta la risposta è authoritative.
La entry non-authoritative memorizzata in cache era valida.

MX server con nslookup

```
> nslookup
> set ty=mx
> unina.it
Server:         143.225.229.3
Address:        143.225.229.3#53

Non-authoritative answer:
unina.it        mail exchanger = 10 pmx1.unina.it.
unina.it        mail exchanger = 10 pmx2.unina.it.

Authoritative answers can be found from:
unina.it        nameserver = dscna1.unina.it.
unina.it        nameserver = dscna2.unina.it.
pmx1.unina.it   internet address = 192.132.34.28
pmx2.unina.it   internet address = 192.132.34.29
dscna1.unina.it internet address = 192.133.28.1
dscna2.unina.it internet address = 192.133.28.7
```

Imposto nslookup per l'invio di query di tipo MX (Mail eXchanger): server SMTP di dominio

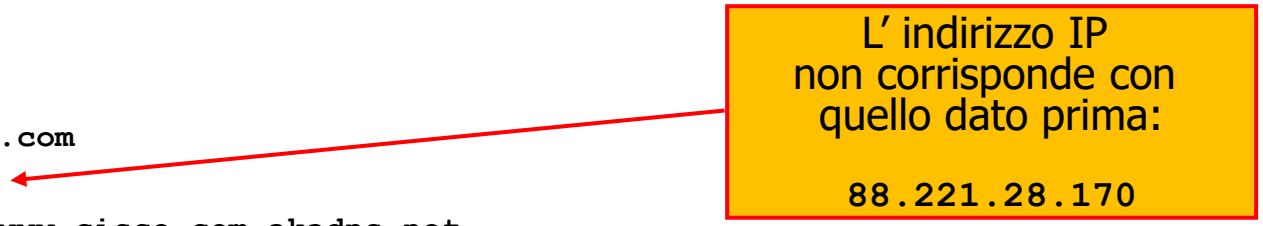
Chiedo i mail server del dominio "@unina.it"

Nslookup: esempio (1)

```
C:\Documents and Settings\User>nslookup
*** Impossibile trovare nome server per l'indirizzo 85.37.17.11: Non-existent domain
Server predefinito:  host69-28-static.38-85-b.business.telecomitalia.it
Address:  85.38.28.69

> www.cisco.com
Server:  host69-28-static.38-85-b.business.telecomitalia.it
Address:  85.38.28.69

Risposta da un server non di fiducia:
Nome:    e144.cd.akamaiedge.net
Address:  88.221.28.170
Aliases:  www.cisco.com, www.cisco.com.akadns.net
          geoprod.cisco.com.akadns.net, www.cisco.com.edgekey.net
          www.cisco.com.edgekey.net.globalredir.akadns.net
> set ty=ns
> cisco.com
Server:  host69-28-static.38-85-b.business.telecomitalia.it
Address:  85.38.28.69

Risposta da un server non di fiducia:
cisco.com       nameserver = ns2.cisco.com
cisco.com       nameserver = ns1.cisco.com
```

Nslookup: esempio (2)

```
> server ns1.cisco.com
Server predefinito:  ns1.cisco.com
Address:  128.107.241.185

> set ty=a
> www.cisco.com
Server:  ns1.cisco.com
Address:  128.107.241.185

Nome:    origin-www.cisco.com
Address:  198.133.219.25
Aliases:  www.cisco.com, www.cisco.com.akadns.net
```



Un sito che mostra come funziona DNS

- https://dns-lookup.jvns.ca/trace.html

Il tool DIG

- "dig" is a robust command-line tool developed by BIND for querying DNS nameservers

dig Commands

COMMAND	DESCRIPTION	EXAMPLE
`dig [hostname]`	Returns any A record found within the queried hostname's zone.	`dig dyn.com`
`dig [hostname] [record type]`	Returns the records of that type found within the queried hostname's zone. List of Record Types.	`dig dyn.com MX`
`dig [hostname] +short`	Provides a terse answer, usually just an IP address.	`dig dyn.com +short`
`dig @[nameserver address] [hostname]`	Queries the nameserver directly instead of your ISP's resolver.	`dig @ns2.p01.dynect.net dyn.com`
`dig [hostname] +trace`	Adding `+trace` instructs dig to resolve the query from the root nameserver downwards and to report the results from each query step.	`dig dyn.com +trace`
`dig -X [IP address]`	Reverse lookup for IP addresses.	`dig -X 204.13.248.106`
`dig [hostname] any`	Returns all records for a hostname.	`dig dyn.com any`