



Università
degli Studi
della Campania
Luigi Vanvitelli

Reti di Calcolatori e Cybersecurity

DNS – Domain Name System

Ing. Vincenzo Abate

Protocollo che risolve problemi differenti

Ogni elemento ha un indirizzo

Nomi simbolici e indirizzi

Indirizzi numerici

- I computer e i router sono identificati in rete grazie ai loro indirizzi IP
- Indirizzi numerici codificati con 32 bit nel caso di IPv4, con 128 bit nel caso di IPv6
- Difficile da ricordare per gli umani...

Nomi simbolici

- I computer, le reti, i servizi di rete possono essere identificati anche mediante nomi logici
 - www.google.com
 - www.rai.it
 - pippo@unicampania.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
- Come semplifico vita? Sono mapping tra ip address e nome simbolico.

Ma allora serve qualcosa che dice: a questo nome corrisponde questo IP.

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 un indirizzo IP 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

DNS: Funzionalità

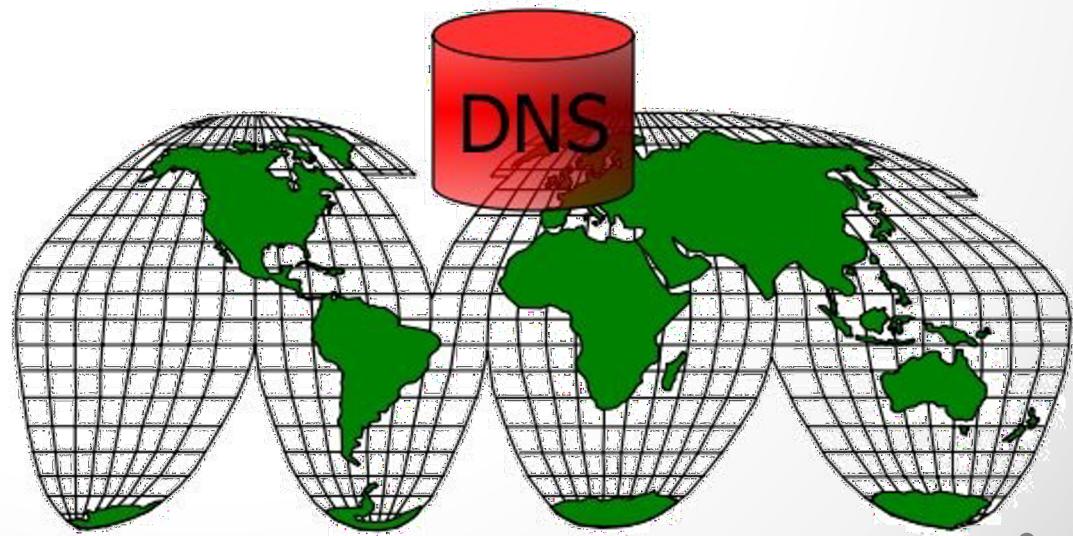
- **Alias degli hostname:**
 - ad una macchina con un nome complicato può essere associato un “soprannome” più piccolo e semplice da ricordare. P.es.: rcsn1.roma.rai.it
www.rai.it
 - L, URL
- **Alias dei server di posta:**
 - permette di associare un server di posta al nome di un dominio per facilitare la memorizzazione dell'indirizzo di posta
 - Es.: pippo@unicampania.it identifica l'utente pippo sulla macchina dove risiede il mailserver. L'associazione @unicampania.it al mailserver 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
 - il browser usa il primo che riceve quando riceve il pool casualmente

DNS: Soluzione centralizzata

- Un solo server dei nomi che contiene tutte le correlazioni: i client indirizzano le richieste al server che risponde direttamente ai client.
Impensabile oggi

- Problemi:

- Un punto singolo di guasto
- Volume di traffico
- Database centralizzato distante (world wide wait)
- Manutenzione



DNS: Soluzione decentrata

- L'archivio dei nomi simbolici è distribuito tra più server situati in diverse località e collegati tra loro. Ciascuno ha la responsabilità di raccogliere, gestire, aggiornare e divulgare le informazioni che lo riguardano
- Il client invia il nome simbolico ad uno di questi server.
- Se il server non è in grado di stabilire la corrispondenza tra nome simbolico e indirizzo IP diventa client nei confronti di un altro server e così via fino a trovare l'indirizzo IP cercato
- 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

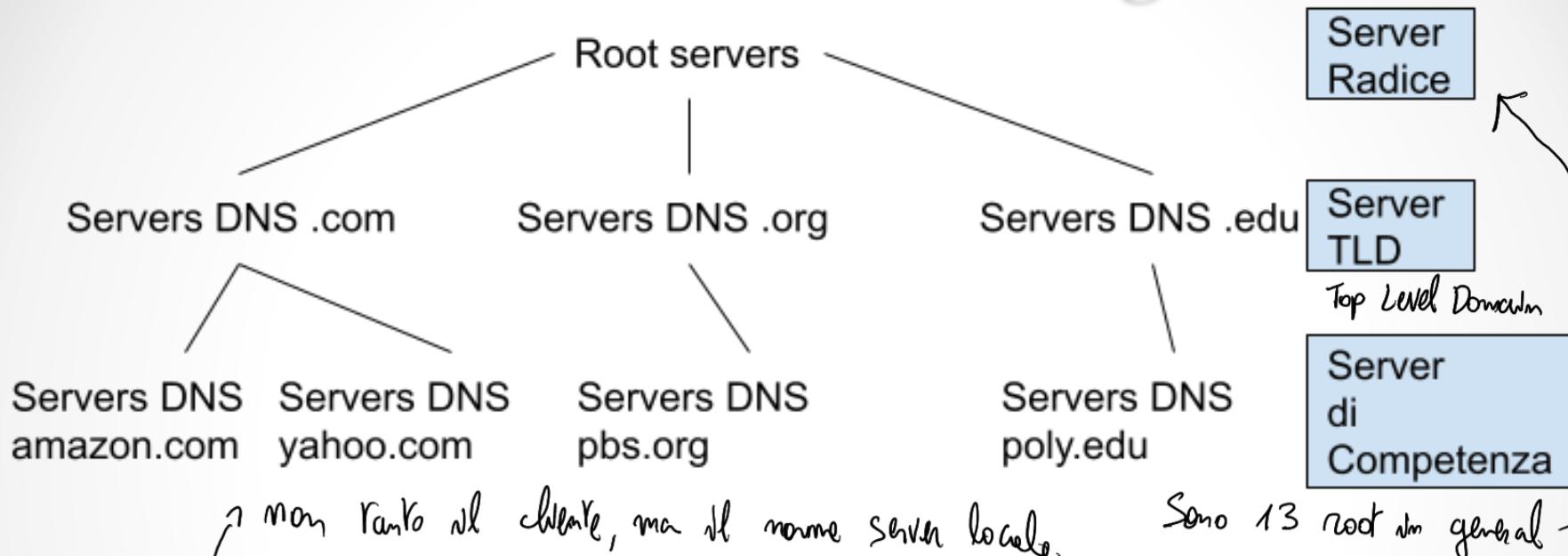
Il tutto è trasparente all'utente!

Funzionamento DNS

Prospettiva del client: DNS come «black-box».

- Il client invia un messaggio di richiesta DNS specificando l'hostname che deve essere trasformato in indirizzo IP
- Dopo un ritardo che va da msec a decine di secondi il client riceve un messaggio di risposta DNS che fornisce la correlazione desiderata.
- Questa «Black-box» è molto complessa e consiste di un gran numero di server dei nomi distribuiti sul globo.

Funzionamento DNS: DB gerarchico



Un Client richiede l'IP di www.amazon.com:

- 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 – Name server Locale

Local Name Server

↗ qualche anche ISP

- Ciascun operatore di rete ne installa uno nella propria rete
- Gli host di una rete sono configurati con l'indirizzo del DNS server locale ↗ collega il pc => indirizzo IP e DNS
 - 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 singoli host di fare una sola query DNS verso di essi: sarà poi il DNS server locale a fare la sequenza di interrogazioni descritta nella slide precedente

DNS – Root Server

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 centinaia di 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

DNS – Top Level Domain

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

TLD (Top Level Domain): quattro categorie principali:

1. Codici ISO 3165 identificativi delle singole nazioni (ccTLD)
country code TLD .it, .fr
2. Tre TLD che esistono solo negli Stati Uniti (usTLD): mil, edu, gov
3. TLD generici (gTLD) utilizzabili da soggetti in qualunque nazione: org, com, net,...
4. Suffisso int riservato alle organizzazioni nate in seguito a trattati internazionali

w dove esse qualcuno che viene invocata

DNS – Top Level Domain

In Italia la R.A (Registration Authority) è l’Istituto di Informatica e Telematica del CNR (IIT-CNR).

Ha il compito di gestire i domini del ccTLD (country code Top Level Domain) it. (www.nic.it/RA).

Funzioni:

- Contratti con i provider (ISP)
- Registrazione domini
- Gestione database

Associaz. nome-indirizzo. Le risorse sono mte.

DNS – Top Level Domain

Gli enti registrati presso un dominio possono decidere se adottare ulteriori gerarchie nella denominazione dei loro calcolatori.

Esempio: `lia.deis.unibo.it`

- `unibo` è registrato nel dominio `it`
- `deis` è registrato nel dominio `unibo`
- `lia` è registrato nel dominio `deis`

Tutti i siti che ricadono sotto `unibo.it` sono gestiti da `unibo.it`.

Autonomia concessa agli enti: per cambiare o assegnare i nomi dei calcolatori non è necessario informare alcuna autorità centrale.

Es: l'Università di Bologna non ha vincoli nell'assegnare o modificare nomi che terminano per `unibo.it`

DNS – Authoritative server

Authoritative Name Server

- 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 unicampania.it deve essere capace di risolvere tutti i nomi del tipo xyz.unicampania.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

DNS – risoluzione

Risoluzione ricorsiva *Si intende qualcosa livello di prima*

Quando un host o un server dei nomi A fa una richiesta ricorsiva a un server dei nomi B, allora B ottiene la correlazione richiesta a nome di A e quindi la invia ad A.

Risoluzione iterativa

Quando un host o un server dei nomi A fa una richiesta iterativa ad un server dei nomi B, se questo non ha la correlazione richiesta, esso invia immediatamente una risposta DNS ad A che indica l'indirizzo IP del server successivo nella catena, cioè del server dei nomi C. Il server A invia allora una richiesta a C.

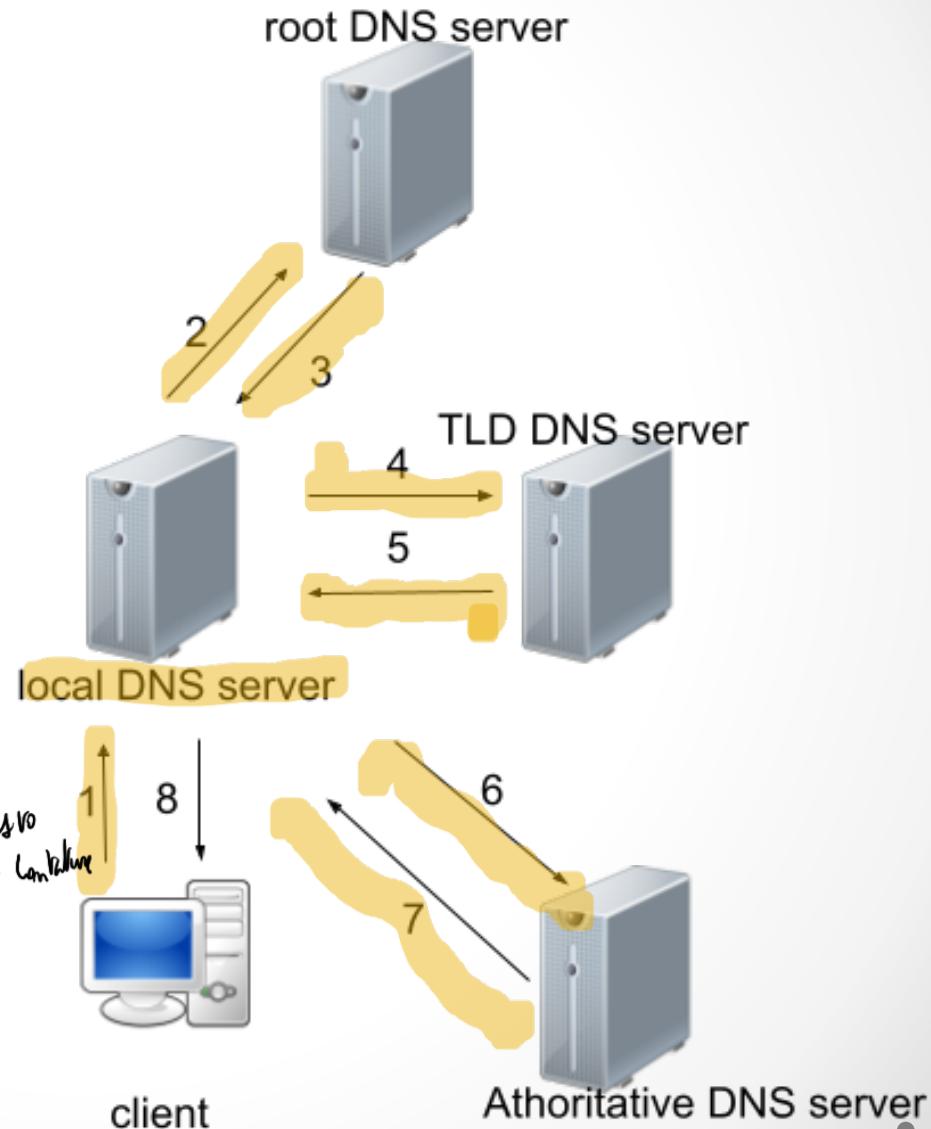
DNS – risoluzione Iterativa

Il server contattato risponde con il nome del server da contattare

- La logica: non conosco questo nome, ma conosco il nome di qualcuno a cui poter chiedere

Il TLD potrebbe non contattare necessariamente l'Authoritative Name Server finale, ma un Authoritative Name Server intermediario → così *so che è il successivo* —> *com'è*

- Sarà il server intermedio a fornire il nome del server di competenza
- In questi casi il numero di messaggi DNS aumenta

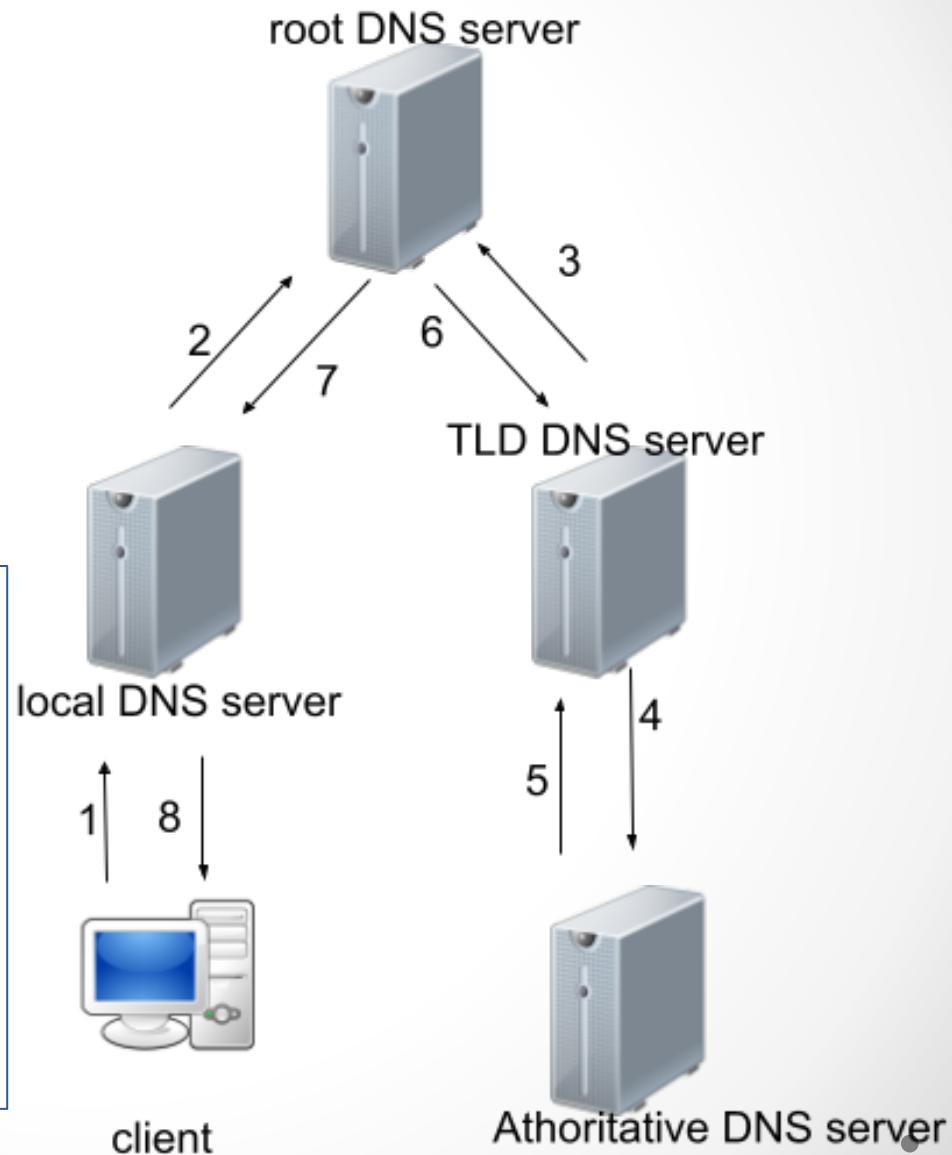


DNS – risoluzione Ricorsiva

- Sposta il carico della risoluzione dei nomi sul server contattato, delegando al NS contattato la responsabilità di risolvere l'indirizzo
- Troppo carico

Il TLD potrebbe non contattare necessariamente l'Authoritative Name Server finale, ma un Authoritative Name Server intermediario

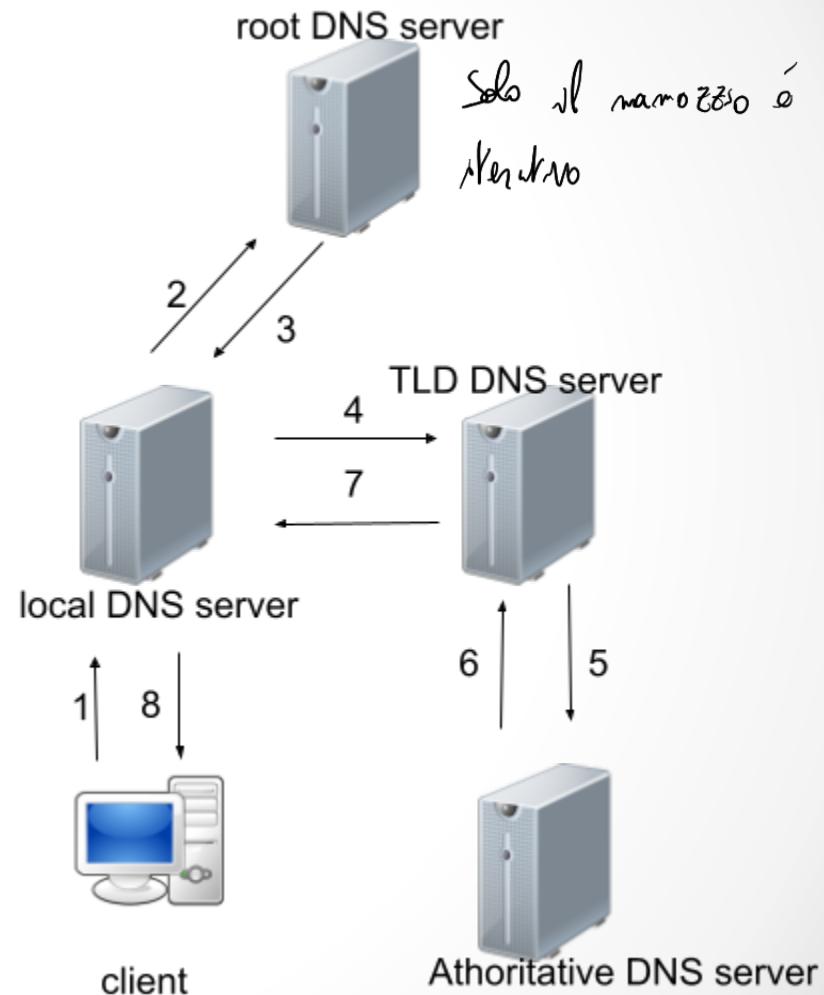
- Sarà il server intermediario a fornire il nome del server di competenza
- In questi casi il numero di messaggi DNS aumenta



DNS – risoluzione Mista

Tutte le richieste nella catena sono ricorsive ad eccezione di quella fatta dal server dei nomi locale a quello radice , che è di tipo iterativo.

Questo è dovuto al fatto che il server dei nomi radice riceve molte richieste e quindi è preferibile per esso usare le richieste iterative che sono “meno pesanti”.



DNS – Load Balancing

Server web replicati

I siti con molto carico sono replicati su più server ciascuno con un indirizzo IP.

A ciascun hostname canonico (nome del server web) è associato un gruppo di indirizzi IP.

Il database del DNS contiene il gruppo di indirizzi IP associati ad un hostname canonico.

A fronte di una richiesta da un client DNS il server DNS risponde con tutti gli indirizzi IP, ma ruota l'ordine all'interno di ogni risposta.

I client utilizzano il primo. La rotazione imposta dal DNS distribuisce il traffico tra tutte le repliche dei server.

DNS – Caching dei nomi

Per esigenze di efficienza un server DNS memorizza localmente un certo numero di corrispondenze

Non faccio nulla la prima volta → per le secon 3 che

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

↳ es. Authoritative cache
association

DNS – richieste

Ogni elemento di un data-base DNS (**resource record - RR**) consiste dei seguenti campi principali:

(**Name, Value, Type, TTL**)

Name è il nome del dominio.

Type è il tipo dell'elemento e specifica come il campo value deve essere interpretato.

TTL è il tempo di vita del record; determina il momento in cui una risorsa dovrà essere rimossa dalla cache.

La richiesta al DNS è costituita da un nome di dominio e da un tipo.

Richieste DNS: tipi principali

Tipo = A

Nome = hostname

Valore = indirizzo IP

Tipo = NS Name Server

Nome = dominio (es.: unicampania.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'hostname di un mailserver associato a nome

→ www, mail, ...

DNS: formato messaggi

Header di messaggio identification:

numero a 16 bit per la richiesta, la risposta usa lo stesso numero

↳ identifies the request

flag:

- Richiesta o risposta
- Chiede la ricorsione (Q)
- Ricorsione disponibile (R)
- Il server che risponde è di riferimento per la richiesta (R)

Nota: richiesta e risposta hanno lo stesso formato

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs
questions (variable number of questions)	
answers (variable number of resource records)	
authority (variable number of resource records)	
additional information (variable number of resource records)	

12 bytes

DNS: formato messaggi

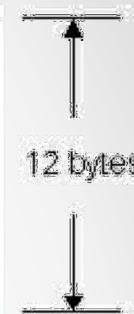
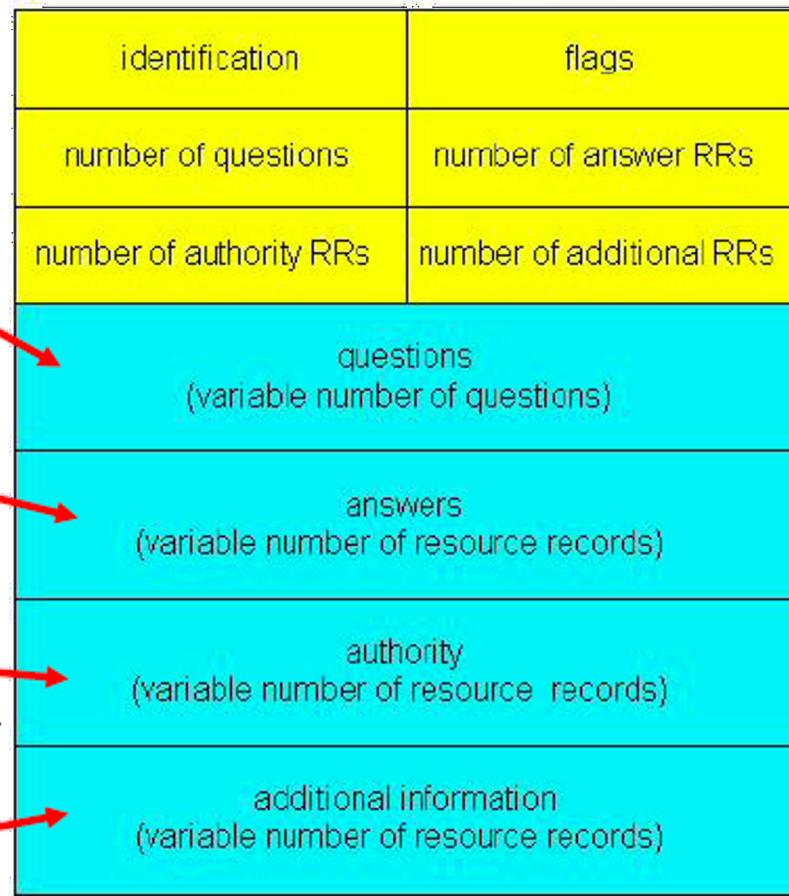
Nome, campi tipo per una richiesta

RR in risposta a una richiesta

Record per server di riferimento

Informazioni addizionali

Es.: RR di tipo A contenente indirizzo IP di un mail server il cui nome canonico è contenuto nella answer section



Payload

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



Contiene le info relative ad un Namespace \Rightarrow un computer, sì

File di configuraz.

BIND - esempio

Serial: numero seriale progressivo utilizzato per rilevare aggiornamenti del file. Di solito usa il formato: aaaammggxx

→ File dove configura

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 ritene 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

Zona: domino.s
parte di domino

```
; $ORIGIN .
$TTL 3600      ; 1 hour
@           IN SOA NAVA1.uniparthenope.it. postmaster.uniparthenope.it. (
                      2020271473 ; serial
                      2017080367 ; serial
                      3600       ; refresh (2 hours)
                      3600       ; retry (2 hours)
                      2419200   ; expire (4 weeks 2 days)
                      72800     ; minimum (5 days)
)
$TTL 3600      ; 1 week
```

- * **SOA:** Start of Authority: indica al nameserver le informazioni autorevoli importanti inerenti al namespace per il nameserver

BIND – direttive

\$INCLUDE — indica a `named` di includere un file zone in un altro file nel punto in cui viene usata la direttiva.

\$ORIGIN — imposta il nome del dominio da accodare a qualsiasi record non qualificato, come quelli che specificano solo l'host e nient'altro. Per esempio, un file zone potrebbe contenere una riga seguente:

`$ORIGIN example.com.`

qualsiasi nome utilizzato nei record della risorsa, che non termina con un punto (.), presenterà `example.com`.

\$TTL — imposta il valore predefinito Time to Live (TTL) in secondi, assegnato ai server dei nomi che indica il periodo di validità dei record di risorsa della zona. Un record di risorsa può avere un valore TTL proprio, che annulla quindi quello impostato da questa direttiva. Impostando un valore più alto si indica ai server dei nomi di conservare in memoria queste informazioni di zona per un periodo di tempo maggiore. Ciò riduce il numero di richieste relative a questa zona, ma allunga anche il tempo necessario per modificare il record di risorse.

BIND – record

A — informazioni sull'indirizzo che specifica un indirizzo IP da assegnare al nome

```
<host>      IN      A      <IP-address>
```

CNAME — record di nome tipico che mappa un nome all'altro, conosciuto anche come un alias.

```
<alias-name>    IN      CNAME     <real-name>
```

```
server1      IN      A      10.0.1.5  
www          IN      CNAME    server1
```

MX — si tratta del record "Mail eXchange", che indica dove va inoltrata la posta inviata a un particolare spazio dei nomi controllato da questa zona.

```
IN      MX      <preference-value>  <email-server-name>
```

→ Priority 10>20

```
IN      MX      10      mail.example.com.  
IN      MX      20      mail2.example.com.
```

NS — record Name Server che annuncia i server dei nomi autorevoli per una determinata zona

```
IN      NS      <nameserver-name>
```

```
IN      NS      dns1.example.com.  
IN      NS      dns2.example.com.
```

BIND – reverse DNS

Un file zone per la risoluzione inversa dei nomi viene utilizzato per tradurre un indirizzo IP in uno spazio particolare in un FQDN. Somiglia molto a un file zone standard, tranne per il fatto che i record di risorsa PTR, vengono utilizzati per collegare gli indirizzi IP a un nome del dominio qualificato.

	<i><last-IP-digit></i>	IN	PTR	<i><FQDN-of-system></i>
\$ORIGIN	1.0.10.in-addr.arpa.	→ da	1.0.10.20 a 1.0.10.25	
\$TTL	86400			↳ indirizzo impostato da chi gestisce i domini
@	IN SOA			dns1.example.com. hostmaster.example.com. (
				2001062501 ; serial
				21600 ; refresh after 6 hours
				3600 ; retry after 1 hour
				604800 ; expire after 1 week
				86400) ; minimum TTL of 1 day
		IN NS		dns1.example.com.
		IN NS		dns2.example.com.
20	IN PTR			alice.example.com.
21	IN PTR			betty.example.com.
22	IN PTR			charlie.example.com.
23	IN PTR			doug.example.com.
24	IN PTR			ernest.example.com.
25	IN PTR			fanny.example.com.

DNS – autoritativi e non

Server DNS autoritativi: un server DNS viene indicato come **autoritativo**, se sono salvate nel suo database informazioni di dominio su una specifica zona del Domain Name Space. Il DNS è strutturato di modo che per ogni zona esista almeno un **name server autoritativo**. Un sistema simile viene generalmente realizzato come cluster di server, dove i dati di zona identici **vengono salvati su un sistema con architettura master-slave**. In questo caso si parla anche di **name server primario** e **secondario**. Questo tipo di **ridondanza aumenta la stabilità e la disponibilità di un name server autoritativo**.

Server DNS non autoritativi: se le informazioni DNS di un name server non provengono dal proprio file di **zona**, ma sono di seconda o terza mano, questo server per le informazioni richieste svolge la funzione di **name server non autoritativo**. Una situazione simile si verifica quando un **name server non può rispondere ad una richiesta basandosi sul suo database e raccoglie quindi le informazioni da un altro name server (ricorsione)**. I dati DNS vengono **immagazzinati temporaneamente nella memoria locale (caching)** e **forniti se la richiesta viene effettuata nuovamente**.

NB: Le informazioni DNS dei name server non autoritativi risultano poco affidabili perché le voci del file di zona vero e proprio **possono essere nel frattempo modificate**.

DNS - nslookup

- nslookup è uno strumento da riga di comando molto pratico che viene usato soprattutto per risalire:
 - all'indirizzo IP assegnato a un determinato host
 - al nome di dominio collegato a un determinato indirizzo IP (Reverse DNS Lookup)
- Con nslookup si ottengono le informazioni relative all'indirizzo direttamente dalla cache DNS dei name server

Parametro di nslookup	Tipo di query
A	Indirizzo IPv4
AAAA	Indirizzo IPv6
MX	Mail server del/i nome/i di dominio (Mail Exchanger)
NS	Name server del nome di dominio

DNS - nslookup

```
C:\Users\Vincenzo>nslookup  
Server predefinito: UnKnown  
Address: 192.167.9.1 DNS locale  
  
> www.ingegneria.unicampania.it  
Server: UnKnown  
Address: 192.167.9.1  
  
Risposta da un server non autorevole:  
Nome: hosting-new.cressi.unicampania.it  
Address: 193.206.103.135  
Aliases: www.ingegneria.unicampania.it
```

```
> set ty=ns  
> unicampania.it  
Server: UnKnown  
Address: 192.167.9.1  
  
Risposta da un server non autorevole:  
unicampania.it nameserver = ns1.cressi.unicampania.it  
unicampania.it nameserver = u2dns1.unina2.it  
unicampania.it nameserver = ns1.unicampania.it  
unicampania.it nameserver = ns1.univan.it  
unicampania.it nameserver = ns2.cressi.unicampania.it  
  
ns1.cressi.unicampania.it      internet address = 193.206.103.215  
ns1.unicampania.it      internet address = 193.206.100.10
```

```
> server ns1.cressi.unicampania.it  
Server predefinito: ns1.cressi.unicampania.it  
Address: 193.206.103.215  
  
> www.ingegneria.unicampania.it  
Server: ns1.cressi.unicampania.it  
Address: 193.206.103.215  
  
www.ingegneria.unicampania.it canonical name = hosting-new.cressi.unicampania.it  
cressi.unicampania.it  
    primary name server = ns1.cressi.unicampania.it  
    responsible mail addr = hostmaster.cressi.unicampania.it  
    serial = 2022090900  
    refresh = 43200 (12 hours)  
    retry = 7200 (2 hours)  
    expire = 1209600 (14 days)  
    default TTL = 7200 (2 hours) → Sovrascrivere info
```

DNS - dig

Dig (Domain Information Groper) è uno strumento da riga di comando per l'interrogazione di Domain Name System (DNS) name server. È utile per verificare e risolvere i problemi di DNS e anche per eseguire ricerche DNS e visualizza le risposte che vengono restituite dal server dei nomi interrogato

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

DNS - dig

QUESTION SECTION: The query made to the DNS. In this example, we asked for the first available A record for the hostname, dyn.com.

ANSWER SECTION: The first available answer for the query made to the DNS.

AUTHORITY SECTION: The authoritative nameservers from which the answer to the query was received.

ADDITIONAL SECTION: Additional information the resolver may need but not the answer to the query.

```
$ dig dnsimple.com

; <>> DiG 9.8.3-P1 <>> dnsimple.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60554
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
dnsimple.com.           IN      A

;; ANSWER SECTION:
dnsimple.com.      59      IN      A      50.31.213.210

;; Query time: 294 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Feb  3 11:17:13 2015
;; MSG SIZE  rcvd: 46
```

DNS - dig

```
$ dig @ns1.dnsimple.com dnsimple.com

; <>> DiG 9.8.3-P1 <>> @ns1.dnsimple.com dnsimple.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35081
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
dnsimple.com.           IN      A

;; ANSWER SECTION:          TTL
dnsimple.com.       60      IN      A      50.31.213.210

;; Query time: 145 msec
;; SERVER: 198.241.10.53#53(198.241.10.53)
;; WHEN: Tue Feb  3 11:28:02 2015
;; MSG SIZE  rcvd: 46
```

<https://support.dnsimple.com/articles/how-dig/>