

Università di Genova  
Facoltà di Ingegneria

---

*Livello di Applicazione in Internet*  
**2. DNS (Domain Name System)**

Prof. Raffaele Bolla  
Ing. Matteo Repetto

---



### Identificazione degli host

---

- Ogni *host* è identificabile in due differenti modalità:
  - Indirizzo IP (ad es. 121.7.106.83)
  - *Hostname* (ad es. www.google.com)

L'identificazione tramite *hostname* (URL) è normalmente preferita dall'utenza in quanto maggiormente mnemonica rispetto ad un indirizzo IP.

Gli indirizzi IP, caratterizzati da una lunghezza e da una strutturazione gerarchica fissa, sono invece più efficacemente utilizzabili nel routing rispetto agli *hostname*

- Il meccanismo che realizza la traduzione tra *hostname* e Indirizzo IP e viceversa è detto *Domain Name System* (DNS)

2.2

## DNS: introduzione

---

- Il DNS è un'entità del Livello di Applicazione, infatti fra l'altro:
  - funziona tra terminali comunicanti che usano il paradigma *Client-Server*,
  - si appoggia a un protocollo di trasporto *end-to-end* per trasferire i messaggi DNS tra i due terminali,
- Normalmente, però, non viene utilizzato direttamente dall'utente ma viene richiamato da altre applicazioni (Web,E-mail...).

2.3

## DNS: introduzione

---

- Il DNS è in generale:
  - Un database distribuito implementato in una gerarchia di *Name Server*.
  - Un protocollo dello strato di applicazione che permette agli *host* di comunicare con i *Name Server* ed ai *Name Server* di interagire fra loro, in modo da fornire il servizio di traduzione.
- I *Name Server* operano prevalentemente su macchine Unix usando l'implementazione software "*Berkeley Internet Name Domain*" (BIND)
- Il protocollo DNS utilizza UDP e la porta 53 (in casi particolari può operare su TCP)

2.4

## DNS: introduzione

---

- Il DNS, inoltre, fornisce altri servizi molto importanti:
  - **Alias degli *hostname***: un *hostname* può avere più di un alias del nome. L'*hostname* originale è detto canonico. Gli alias sono solitamente più mnemonici (www ,ftp , smtp) dell'*hostname* canonico.
  - **Identificazione server di posta**: usato per legare un dominio all'indirizzo di un server di posta. E' possibile indicare eventuali *Server* di posta aggiuntivi da utilizzare in caso di guasto del principale.
  - **Distribuzione del carico**: il DNS è utilizzato anche per ripartire il carico di traffico tra diverse repliche di uno stesso *Server* (ciascuna replica di *Server* su un *host* diverso).

2.5

## Name Server

---

- Il database distribuito è realizzato tramite una gerarchia di molti *Name Server*
- Nessun *Name Server* possiede nel proprio *database* tutte le possibili traduzioni *hostname*/indirizzo IP
- Perché il DNS non è centralizzato?
  - Volume di traffico
  - Il database centralizzato potrebbe essere troppo distante dagli *host*
  - Struttura distribuita più ridondante, quindi più robusta ai guasti e di manutenzione più agevole

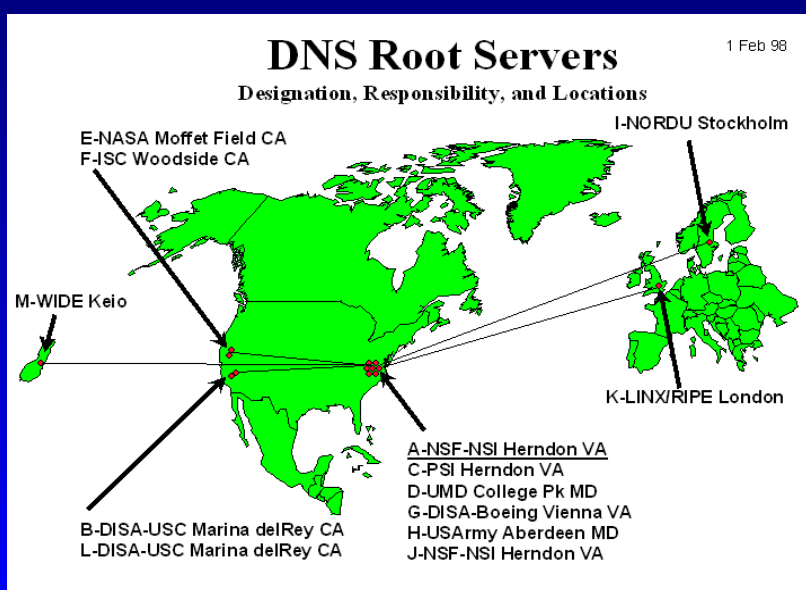
2.6

## Name Server

- Local Name Servers:
  - ogni ISP ha un *local (default) name server*
  - le richieste di DNS di ogni host vengono inizialmente sempre indirizzate al *local name server*
- Root Name Servers:
  - Quando un *local name server* non riesce a soddisfare la richiesta, esso si comporta come un *Client DNS* e inoltra tale richiesta al *Root Name Server* (ne esistono alcune dozzine)
  - Se il R.N.S. non possiede la traduzione dell'*hostname* risponde inviando l'indirizzo di un *Authoritative Name Server* che ha la corrispondenza di quel particolare *hostname*

2.7

## Name Server



2.8

## Name Server

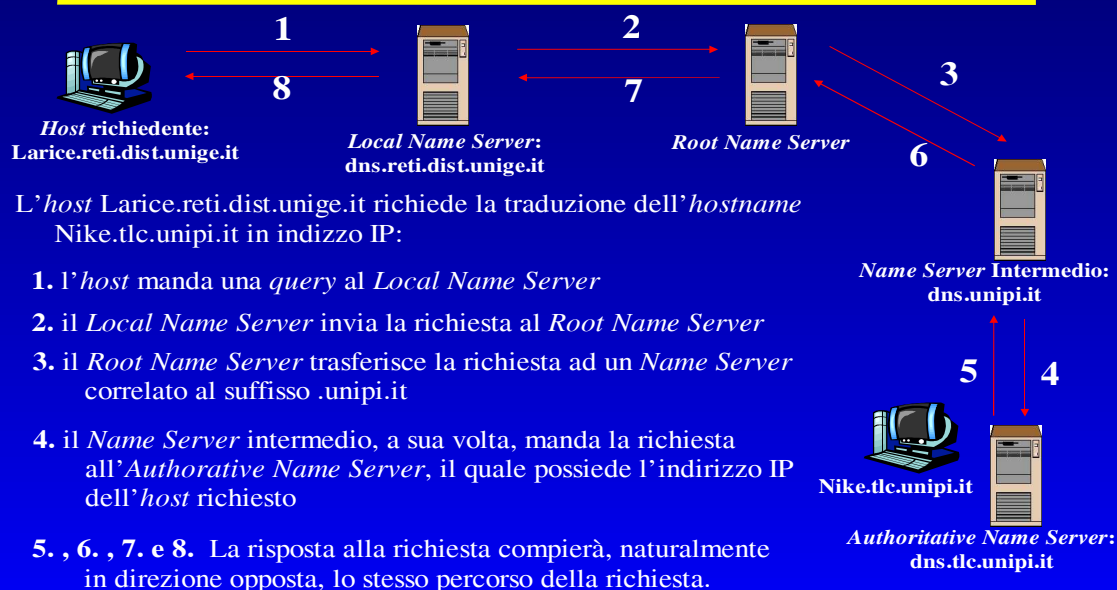
- Authoritative Name Server:

Ciascun *host* è registrato presso un *Authoritative Name Server* che, tipicamente, per ogni *host* è il *Name Server* situato presso il suo ISP locale.

Quando un *Authoritative Name Server* riceve una richiesta da un *Root Name Server*, esso risponde con la “traduzione” richiesta. Il *Root Name Server*, a sua volta, invierà la “traduzione” al *Local Name Server*, il quale, infine la girerà all’*host* richiedente.

2.9

## DNS: Esempio



2.10

## Meccanismi per aumentare l'efficienza

---

- **Iteratives query**
  - Ogni Server lungo la catena, se non ha la corrispondenza memorizzata direttamente, può fornire l'indirizzo IP del successivo Server della catena (riducendo la lunghezza del cammino di ritorno).
- **Caching**
  - Ogni Server mantiene le ultime traduzioni in una memoria temporanea per un periodo di tempo configurabile
- **Forwarding**
  - Invece che rivolgersi al *Root Server*, il *Local Server* può delegare un Server intermedio che conosce essere particolarmente “capace”

2.11

## Esempio di configurazione di un DNS

---

- Sistema Operativo: *Linux*
- Distribuzione: *Debian (sid)*
- Software DNS: *Bind 9.2.3-2*
- Software di interrogazione: *nslookup*

2.12

## Configurazione di bind 9.x

---

- La configurazione di bind avviene modificando due tipi di file
  - *named.conf*, nel quale si trovano le impostazioni di carattere generale;
  - i *file di zona*, ognuno dei quali è relativo ad un particolare dominio Internet di competenza del name server.

2.13

## named.conf

---

- *Options*
  - *directory*: la directory base;
  - *forwarders*: individua i server DNS utilizzati per la risoluzione di nomi di cui non si è authoritative;
  - *allow-query*: permette di fornire il servizio di risoluzione solo a determinati host o sottoreti;
  - *forward only*: individua un servizio di risoluzione solo di tipo slave, ossia rinvia sistematicamente ogni richiesta ai forwarders (*caching-only name server*).
- *Zone*
  - *type*: master, slave, hint;
  - *file*: file contenente i Resource Records;
  - *masters*: solo per i server di tipo slave;
  - *allow-transfer*: solo per i server di tipo master: chi può trasferire per intero i dati relativi ad un dominio.

2.14

## Memoria cache del dominio principale

---

- zone “.” {
 

```

          type hint;
          file “<nome_file>”;
      };
      
```
- In questo modo si indica il file contenente le informazioni necessarie a raggiungere i DNS del dominio principale.
- Il DNS locale conserva una memoria cache delle informazioni ottenute, in modo da ridurre le interrogazioni ai server principali.
- Senza questa direttiva il DNS non è in grado di risolvere nomi al di fuori del suo ambito di competenza. Questo può essere utile
  - nel caso si gestiscano reti locali “chiuso”;
  - nel caso si utilizzino i *forwarder*.

2.15

## Zone su cui si ha autorità

---

- zone “<dominio>” {
 

```

          type master;
          file “<nome_file_di_zona>”;
          allow-transfer {
              <host_abilitato>;
          };
      };
      
```
- *master* indica che le informazioni relative al dominio devono essere estratte direttamente dal file specificato;
- esistono zone per i domini normali (o diretti) e per gli *in-addr.arpa* (o inversi).

2.16



## Riproduzione delle informazioni di un altro DNS

---

- zone “<dominio>” {  
     type slave;  
     file “<nome\_file\_di\_zona>”;  
     masters {  
         <indirizzo\_ip\_del\_master>;  
     };  
 };
- Il DNS locale può fornire risposte autorevoli insieme ad altri da cui trae periodicamente le informazioni;
- Il file specificato viene creato ed aggiornato automaticamente, in base alle informazioni recuperate dal master;
- Le informazioni vengono eliminate se il master non risulta raggiungibile per un certo periodo di tempo.

2.17

## File di zona

---

- I file di zona costituiscono il database del dominio per cui il DNS è *authoritative*.
- Sono costituiti da un insieme di *Resource Record*, con la seguente sintassi:

```
[dominio] [TTL] [classe] tipo_dati_della_risorsa
```

- Ogni file di zona è associato al **dominio di origine** definito in *named.conf*.
- Il simbolo @ indica il dominio di origine  
 – di solito viene utilizzato solo per i record di tipo SOA.

2.18

## Resource Record

- **[dominio]** indica il nome a cui gli altri campi fanno riferimento
  - se non è indicato si fa riferimento al record precedente;
  - i nomi assoluti terminano con un punto; quelli relativi sono completati con il nome del dominio di origine.
- **[TTL]** rappresenta la validità dell'informazione nella cache di altri server
  - espressa in secondi;
  - solitamente è la stessa per tutti i record e non viene ripetuta.
- **[classe]** è la classe di indirizzamento
  - IN (internet) per le reti TCP/IP.
- **tipo** del record: SOA, MX, NS, A, PTR, CNAME, ecc.
- l'ultimo record rappresenta il contenuto del record stesso
  - spesso consiste in un nome od un indirizzo.

2.19

## SOA – Start Of Authority

- `@ IN SOA timo.lai.reti.dist.unige.it. postmaster.lai.reti.dist.unige.it (`  
`2003022401 ; Serial number`  
`86400 ; Refresh`  
`1800 ; Retry`  
`2592000 ; Expire`  
`172800 ) ; Negative Cache TTL`
- `timo.lai.reti.dist.unige.it` è il nome canonico dell'elaboratore che svolge la funzione di server primario per il dominio indicato;
- `postmaster.lai.reti.dist.unige.it` indica l'indirizzo di posta elettronica del responsabile della gestione del servizio di risoluzione dei nomi;
- il **numero seriale** serve ai server secondari per riconoscere gli aggiornamenti del database;
- il tempo di **refresh** indica l'intervallo di interrogazione da parte del DNS secondario;
- il tempo di **retry** è intervallo tra successive interrogazione da parte del DNS secondario in caso di irraggiungibilità del server primario;
- le informazioni nel server secondario nel caso il primario non sia raggiungibile rimangono valide per un periodo di tempo indicato da **expire**;
- le “risposte negative” da parte di server authoritative rimangono valide nei DNS in cui sono transitate per un periodo di tempo pari al **negative cache TTL**.

2.20

## TTL – *Time To Live*

---

- Normalmente la validità dei RR nelle cache dei DNS è la stessa per tutti i record.
- Il valore TTL non viene normalmente indicato esplicitamente per ogni record
  - di solito si specifica un valore di default.
- Le versioni di bind antecedenti alla 8.2 utilizzavano il campo *minimum* del record SOA
  - attualmente tale valore viene utilizzato per la negative cache.
- Il TTL di default viene attualmente indicato con la direttiva **\$TTL** all'inizio del file di zona.

2.21

## NS – *Name Server*

---

- **@** **IN** **NS** **timo.lai.reti.dist.unige.it.**
- Possono essere presenti più server per la stessa zona.
- Andrebbero utilizzati nomi canonici (quelli per cui esiste un corrispondente record A).

2.22

## **MX – Mail Exchanger**

---

- @ IN MX 10 mail.lai.reti.dist.unige.it.  
20 mail2.lai.reti.dist.unige.it.  
30 mail.dist.unige.it.
- I record MX indicano i nomi dei server per lo scambio della posta (SMTP server).
- Il numero indica la precedenza del relativo server di posta
- Vengono contattati prima i server con numero di precedenza più basso.

2.23

## **A – Address**

---

- dns 86400 IN A 192.168.8.39
- Permettono di associare il nome degli host agli indirizzi.
- I nomi possono essere indicati in forma abbreviata o assoluta
  - nel secondo caso devono terminare con un punto.
- Diversi nomi possono essere tradotti nello stesso indirizzo.
- È possibile specificare un valore di validità diverso da quello di default.

2.24

## CNAME – Canonical Name

---

- `www CNAME server.lai.reti.dist.unige.it.`
- Permettono di definire degli alias per i nomi canonici.
- Si potrebbe fare la stessa utilizzando più record di tipo A.
- Utilizzando i CNAME è più semplice cambiare l'indirizzo di una macchina (un solo record A da aggiornare).
- L'utilizzo degli alias definiti con CNAME è altamente sconsigliabile nella maggior parte delle situazioni (es. record SOA, NS, MX e CNAME).
- L'utilizzo andrebbe limitato solo alla definizione di nomi standard per le applicazioni (www, ftp, smtp, mail, ntp, dns, ecc.)
  - nei record SOA è assolutamente vietato utilizzare alias.

2.25

## Il dominio speciale *in-addr.arpa*

---

- Il dominio *in-addr.arpa* è utilizzato per associare un nome ad un indirizzo IP.
- *in-addr.arpa* rappresenta un dominio speciale che permette di esprimere gli indirizzi IP in una gerarchia simile a quella utilizzata per i nomi degli host.
- Le zone sono indicate con *x.x.x.in-addr.arpa*, dove le cifre che precedono *in-addr.arpa* rappresentano un frammento di un indirizzo IP rovesciato.
- Il file di zona contiene i record SOA, NS e PTR.
- Non bisogna specificare i server root per questo dominio.
  - vi si risale con la risoluzione diretta dalla zona “.”

2.26

## **PTR – Pointer**

---

- **30 PTR server.lai.reti.dist.unige.it.**
- I record PTR mantengono la corrispondenza tra indirizzo IP e nome dell'host (detta a volte “inversa”).
- Nell'esempio, 30 è l'abbreviazione del nome di dominio 30.8.168.192.in-addr.arpa.
- In pratica questi record rappresentano un collegamento tra un nome di dominio e un altro
  - solo così è possibile risolvere gli indirizzi numerici in nome di dominio.
- Si può abbinare un indirizzo ad un solo nome di dominio
  - anche nel caso ci fossero più record A per lo stesso indirizzo.

2.27

## **Bilanciamento del carico**

---

- È possibile che lo stesso servizio sia attivo su più host, allo scopo di suddividere il carico di richieste (es. server www, ftp).
- Il DNS permette di utilizzare lo stesso nome per diversi server, inserendo più record di tipo A per lo stesso nome.
- I server DNS rispondono alle richieste cambiando l'ordine dei server.
- I client in genere utilizzano solo il primo record della risposta.

2.28

## Messaggi DNS

L'intestazione del messaggio ha una dimensione fissa di 12 *byte* e sono previsti i seguenti campi:

- **Identificativo (16bit)**: per identificare la richiesta
- **Flag(16bit)**: i più significativi sono:
  - Domanda o risposta
  - Richiesta di ripetizione
  - Disponibilità del campo di ripetizione
  - Risposta da *Authoritative Server*
- **N°domande(16bit)**: dimensione del campo di domande RR
- **N°risposte(16bit)**: dimensione del campo di risposte RR
- **N°authorityRR(16bit)**: dimensione campo di *Authority Name Server RR*
- **N°RR aggiuntivi(16bit)**: dimensione del campo di Informazioni Aggiuntive.

identificativo	flag
N° domande	N° risposte RR
N° <i>authority RR</i>	N° RR aggiuntivi
Domande RR	
Risposte RR	
<i>Authority Name Server RR</i>	
Informazioni aggiuntive	

2.29

## Messaggi DNS

- Il campo dati è così strutturato:
  - **Domande RR**: contiene informazioni sulle domande inoltrate. Ha due sotto-campi:
    - » Nome: nome che è stato richiesto;
    - » Tipo: tipo di richiesta inoltrata (A, SOA, NS, ...).
  - **Risposte RR**: contiene le informazioni in risposta e, quindi contiene il *record* desiderato:
    - » *<Nome ,TTL,Classe,Tipo,Dato>*
    - » *possono essere presenti più record*
  - **Authoritative Name Server RR**: contiene l'indicazione sugli *Authoritative Name Server* per l'*host* richiesto.
  - **Informazioni Aggiuntive**: contiene altri *record* utili come per esempio nel caso di risposta ad una *query* MX conterrà l'*hostname* di un *server* di posta associato con l'*alias-name*

2.30

## Il DNS è molto di più...

---

- *DDNS, Dynamic DNS* – RFC 2136;
- *Split DNS*, per rendere visibile all'esterno solo una parte della propria rete;
- *DNSSEC* - RFC 2535, garantisce l'autenticità delle informazioni ricevute dai DNS;
- *IPv6* e record *A6*;
- altri RR record: *SRV*, *SIG*, *CERT*, *A6*...

2.31