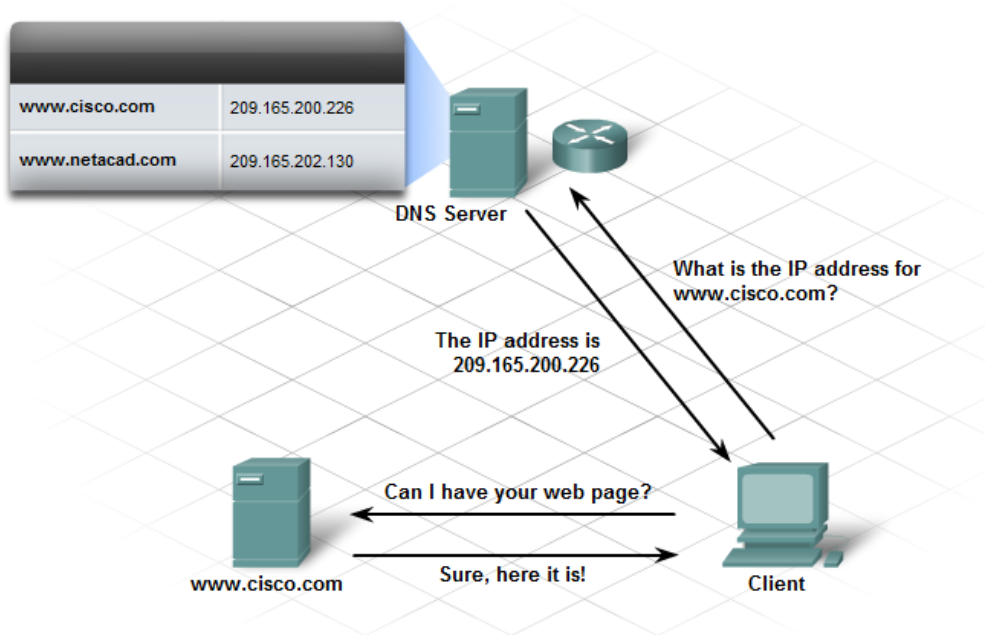
TESINA DI SISTEMI

DNS (Domain Name System)

Storia

Di tutti i servizi Internet, il Domain Name System (DNS) è uno tra i meno compresi ma allo stesso tempo uno tra i più importanti. Definito negli RFC 1034 e 1035, il DNS ha l'importante compito di convertire i nomi delle macchine collegate in rete in indirizzi IP e viceversa.
Ogni computer di Internet possiede un indirizzo numerico chiamato indirizzo IP, che identifica in modo unico solo quella macchina. I computer hanno bisogno di questi indirizzi per poter comunicare. Quando digitiamo nel browser l'URL *www.google.com* , il DNS dell'Internet Provider, o del server tramite cui accediamo ad Internet, traduce il nome mnemonico del sito nell'indirizzo IP 209.85.171.100



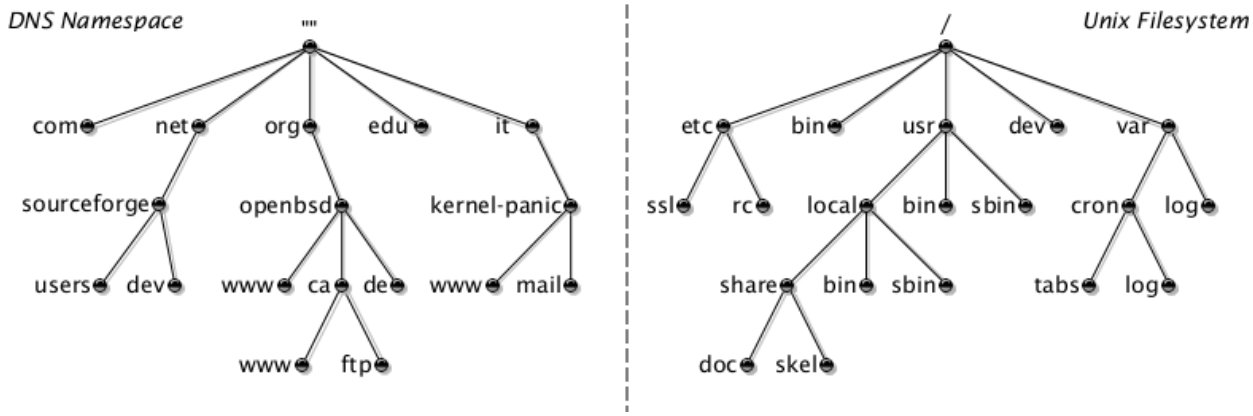
Quando Internet muoveva ancora i primi passi, il collegamento tra due macchine veniva effettuato solamente mediante gli indirizzi IP. Dato che gli indirizzi non sono certo facili da ricordare, si è deciso molto presto di adottare l'uso di nomi simbolici al posto di indirizzi numerici. Questo nuovo modo di identificare le macchine necessitava tuttavia di un qualche sistema in grado di tradurre gli indirizzi in nomi e viceversa. Inizialmente la gestione delle corrispondenze tra indirizzi IP e nomi mnemonici di tutte le macchine collegate, era affidata allo *Stanford Research Institute Network Information Center*(SRI-NIC) che si preoccupava di mantenere tutte le corrispondenze in un singolo file, chiamato HOSTS.TXT. Tutte le macchine periodicamente accedevano a questo file per ottenere una copia aggiornata.
Con la crescita esponenziale del numero di macchine collegate ad Internet, questo semplice sistema di traduzione è stato presto abbandonato in favore di un sistema più flessibile, il Domain Name System, o più semplicemente DNS.
E' importante notare che l'uso del file HOSTS non è scomparso del tutto. Trova ancora applicazione all'interno di reti di piccole dimensioni, dove l'uso un singolo file per mantenere le corrispondenze risulta spesso molto più pratico che installare un server DNS interno. Esso è utilizzato da molti

sistemi operativi per risolvere degli indirizzi IP senza dover ricorrere ad un server DNS(in windows esso è collocato nella cartella C:\Windows\System32\drivers\etc).
Nelle comunicazioni tra rete locale e rete Internet rimane comunque indispensabile affidarsi ad un DNS.
Il sistema DNS è stato concepito nel 1983 quando nessuno si sarebbe aspettato uno sviluppo di Internet pari a quello degli ultimi anni. Nonostante la sua età, ha dimostrato di essere un sistema dotato di una notevole *scalabilità*, ovvero in grado di adeguarsi facilmente all'aumento delle macchine collegate.
Le specifiche originali sono descritte nello standard RFC 882. Nel 1987 vennero pubblicati commenti allo standard RFC del DNS, con i nomi RFC 1034 e RFC 1035 rendendo obsolete le specifiche precedenti.

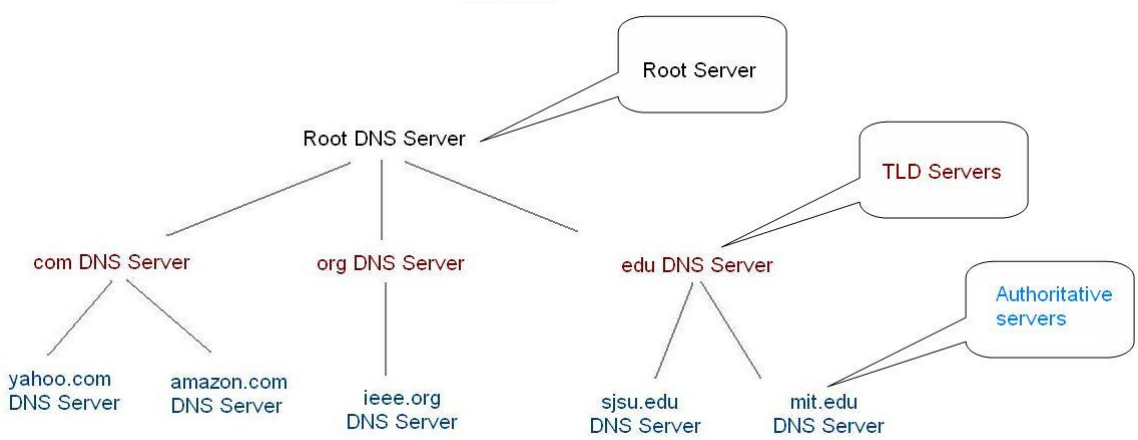
Albero dei domini

Il DNS è un grande database distribuito. Questo significa che non esiste un unico computer che conosce l'indirizzo IP di tutte le macchine collegate in Internet (come avveniva usando il file HOSTS). Le informazioni sono invece distribuite su migliaia di macchine, i server DNS. **Ognuno di questi server è responsabile di una certa porzione del nome, detta dominio. I server sono organizzati secondo una struttura gerarchica ad albero.**

Il suo nome è albero dei domini e la sua somiglianza alla struttura del file system UNIX è evidente.



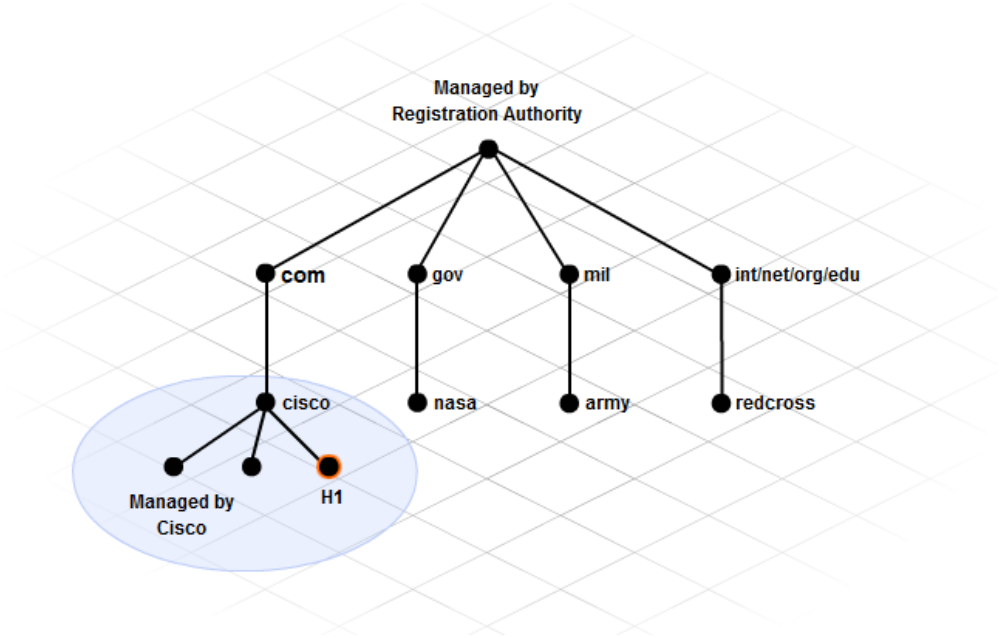
Si tratta di un albero inverso al cui capo troviamo il dominio radice (di solito denotato con un punto '.') e dove ogni nodo dell'albero corrisponde ad un dominio, ovvero al server DNS che lo gestisce.
Le foglie dell'albero sono i nomi delle macchine.



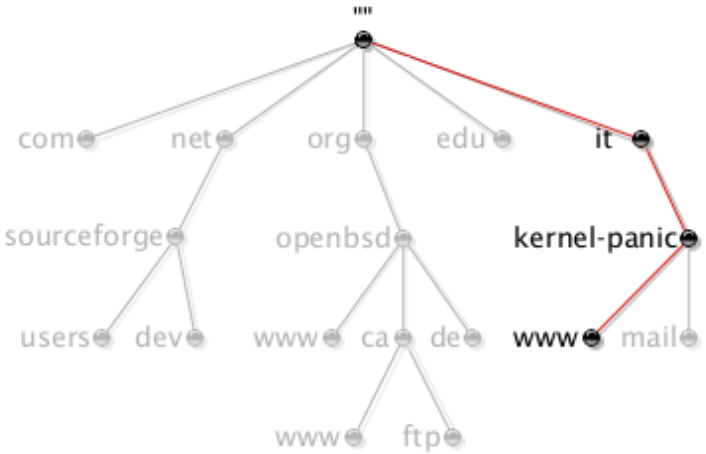
Un nome di dominio, come per esempio *it.wikipedia.org*, può essere parte di un URL, come *http://it.wikipedia.org/wiki/Treno*, o di un indirizzo e-mail, come per esempio *apache@it.wikipedia.org*.

Per fare un esempio prendiamo il sito *www.cisco.com*.

Il nome *www.cisco.com* è il dominio di livello più basso, al di sopra di esso troviamo *cisco.com*. Questo a sua volta è un sottodominio di *.com*.
"www" è per convenzione il nome della macchina che risponde alle richieste di pagine html.
In molti casi, ma non sempre, il nome privato del prefisso "www." porta comunque alla stessa pagina, come per esempio *trenitalia.it* o ancora *trenitalia*.



Per esempio, il nome di dominio evidenziato nella figura seguente è composto dalla sequenza *www*, *kernel-panic*, *it* e l'etichetta nulla della radice, e si scrive quindi *www.kernel-panic.it.* Con il punto finale(che indica appunto la radice).



Nome di dominio

Un nome a dominio è dunque costituito da una serie di stringhe separate da punti, ad esempio *it.wikipedia.org*.
A differenza degli indirizzi IP, dove la parte più importante del numero è la prima partendo da sinistra, in un nome DNS la parte più importante è la prima partendo da destra.
Questa è detta dominio di primo livello (o TLD, Top Level Domain), per esempio .org o .it.
Un dominio di secondo livello consiste in due parti, per esempio wikipedia.org, e così via. Ogni ulteriore elemento specifica un'ulteriore suddivisione. Quando un dominio di secondo livello viene registrato all'assegnatario, questo è autorizzato a usare i nomi di dominio relativi ai successivi livelli come it.wikipedia.org (dominio di terzo livello) e altri *some.other.stuff.wikipedia.org* (dominio di quinto livello) e così via.

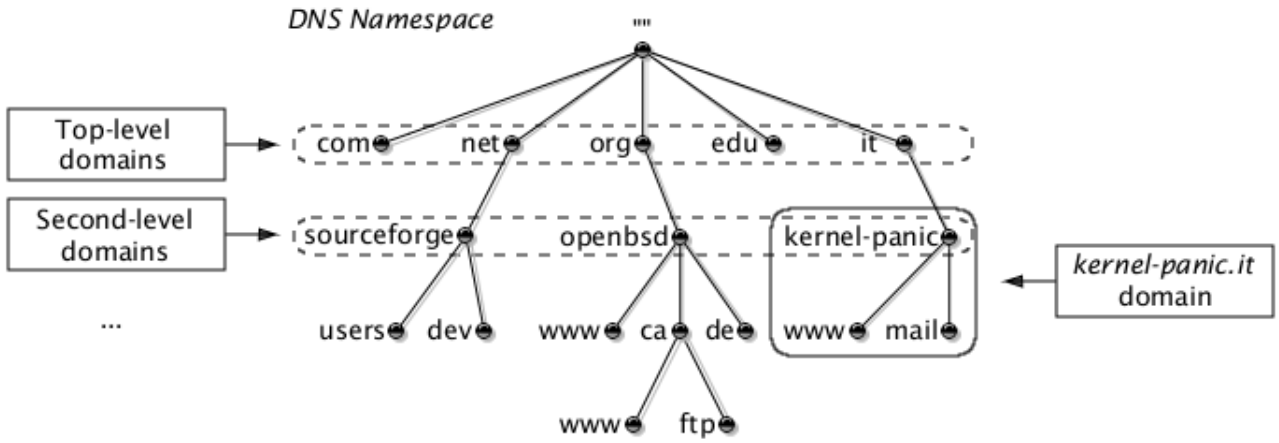
I nomi di dominio sono soggetti a determinate restrizioni: per esempio ogni parte del nome (quella cioè limitata dai punti nel nome) non può superare i 63 caratteri e il nome complessivo non può superare i 255 caratteri.
Si definisce *Fully Qualified Domain Name* (FQDN) un nome di dominio che include tutti i domini di livello superiore al suo.
Un FQDN è anche detto nome di dominio completo.
Se si pensa al DNS come ad un albero, il FQDN di un certo nodo è costituito dal nome del nodo seguito da quello di tutti gli altri nodi tra esso e la radice dell'albero. In sostanza si tratta di risalire l'albero fino alla radice leggendo via via tutti i nodi che si incontrano. Quindi il FQDN di una certa macchina comprende il nome di quella macchina, seguito da tutti i domini di cui l'host è parte fino al dominio di radice, compreso.

Un FQDN dunque è un **nome di dominio non ambiguo** che **specifica la posizione assoluta di un nodo all'interno della gerarchia dell'albero DNS**.

Per distinguere un FQDN da un nome di dominio standard si aggiunge il nome dell'host alla stringa del dominio, in modo da renderla assoluta.
Per esempio, dato un host con il nome *miopc* e un dominio *ciaomamma.it*, l'FQDN è:

MIOPC **.** CIAOMAMMA **.** IT **.**

Come è noto, quando un utente digita un nome di dominio, i nomi dei singoli nodi vengono separati dal punto '.'. Questi nomi vanno dal più specifico (più lontano dalla radice) verso il meno specifico (più vicino alla radice). Dato che un nome di dominio completo finisce con l'etichetta radice, e che questa è sempre rappresentata da una stringa nulla, un nome completo finisce sempre con un punto. Se non viene specificato il punto, quello che abbiamo è un nome incompleto. Di solito i nomi incompleti vengono completati automaticamente dal software, provando con il dominio locale e con alcuni domini predefiniti, tra cui il '.' della radice. Quindi se viene omesso il punto finale quando si digita un nome di dominio, questo viene facilmente riconosciuto come un nome da risolvere rispetto al dominio radice. Allo stesso modo la macchina *host1.networking.net.wind.it.* può comunicare con la macchina *host2.networking.net.wind.it.* usando solo la stringa '*host2*'.
Il dominio radice, o dominio di root, che troviamo a capo dell'albero contiene un elenco di tutti i server DNS dei domini di primo livello. Sparsi per Internet esistono una decina di DNS radice, ma sono usati solo per creare ridondanza e contengono tutti le stesse informazioni.



I domini di primo livello, detti anche TLD (*Top Level Domain*) sono di tre tipi:

- Domini organizzativi(rappresentano un tipo di organizzazione) detti anche i domini generici o **gTLD**(*general TLD*)
- Domini geografici(di soli due lettere, rappresentano una nazione es *.it,.us*) detti **ccTLD** (*Country Code TLD*)
- Dominio inverso: *in-addr.arpa* (un dominio speciale per la risoluzione inversa)

Domini organizzativi

I nomi di dominio organizzativi sono:

introdotti dal 1988:

- *com* Organizzazioni commerciali
- *edu* Istituzioni inerenti l'educazione
- *gov* Istituzioni governative
- *int* Organizzazioni internazionali
- *mil* Istituzioni militari
- *net* Organizzazioni inerenti le reti
- *org* Organizzazioni non-profit

approvati alla fine del 2000:

- *biz* Siti per il commercio(*Business Organizations*)
- *name* Pagine personali
- *info* Siti di informazione
- *aero* Società di trasporto aereo
- *coop* Cooperative
- *museum* Musei
- *pro* Professionisti

Tali domini vengono suddivisi in due classi: sponsored e unsponsored

- **sTLD** (sponsored TLD): sono i gTLDs gestiti da uno sponsor che rappresenta la comunità e che dimostra di avere con essa affinità. Fanno parte degli sTLD i suffissi:
  - **aereo,** per l'industra dei trasporti aerei
  - **asia,** per la comunità dell'Asia
  - **cat,** per la lingua e la cultura catalana
  - **coop,** per le cooperative
  - **jobs,** per siti sull'impiego
  - **museum,** per i musei
  - **mobi,** per siti dedicati ai dispositivi mobili
  - **travel,** per le agenzie di viaggio, gli uffici turistici, gli alberghi, ecc.
  - **tel,** per i servizi relativi a connessioni tra una rete telefonica a Internet
  - **edu,** per siti di educazione scolastica superiore
  - **gov,** per siti governativi e le loro agenzie in USA
  - **mil,** per le forze armate USA
  - **int,** per le organizzazioni internazionali
- **uTLD** (unsponsored TLD): sono quei gTLDs non sponsorizzati (uTLDs), che, come ad esempio ".com" o ".info", operano direttamente secondo le politiche stabilite dalla comunità Internet globale e più in particolare tramite le procedure di ICANN. Fanno parte degli uTLD i suffissi:
  - **com,** per le organizzazioni commerciali
  - **net,** per le infrastrutture di rete
  - **org,** per le organizzazioni
  - **info,** per i siti informativi
  - **biz,** per business
  - **name,** per le famiglie e i singoli
  - **pro,** per alcune professioni

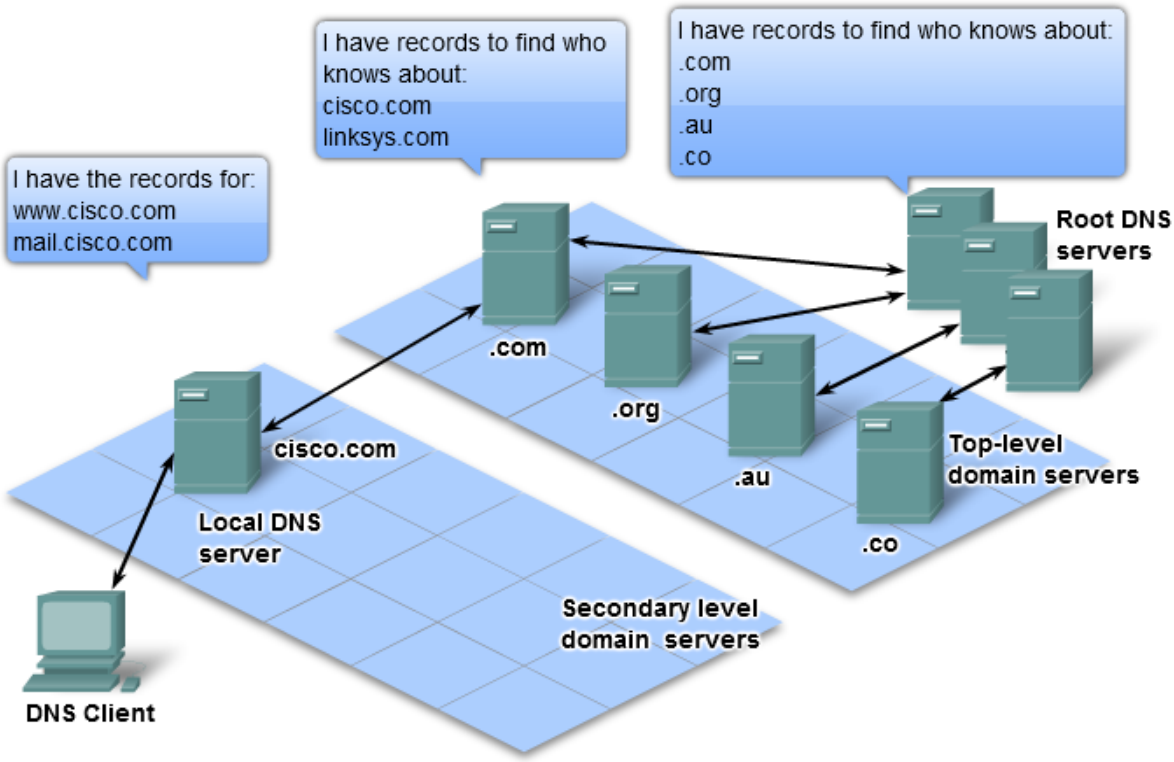
Domini geografici

Al di sotto dei domini di alcuni paesi esiste una gerarchia che rispecchia quella dei domini di primo livello. Ad esempio i nomi delle organizzazioni commerciali di Regno Unito (.UK) e Giappone (.jp) finiscono rispettivamente in *.co.uk* e *.co.jp*, mentre l'equivalente dei *.edu* sono *.ac.uk* e *.ac.jp* (dove ac è l'abbreviazione di academic).
Anche per gli Stati Uniti è stato previsto il codice *.us* ; viene usato in combinazione del codice di ogni stato (ad esempio *.ny.us* indica lo stato di New York).

Gerarchia dei domini

Ogni dominio può contenere host o sottodomini, che a loro volta possono essere suddivisi in sottodomini.
Un DNS che copre un dominio di primo livello conosce gli indirizzi di tutti i server DNS di secondo livello sottostanti ad esso. Quindi un DNS *.it* conosce tutti i domini del tipo *qualche-cosa.it* .
Un DNS di secondo livello di una certa organizzazione conosce a sua volta tutte le macchine il cui nome Internet finisca con *nome-organizzazione.it*. Tra queste, come già accennato, molto spesso

troviamo la macchina speciale "*www*", che identifica il server Web della società. Il suo compito consiste nel rispondere alle richieste di pagine Html.

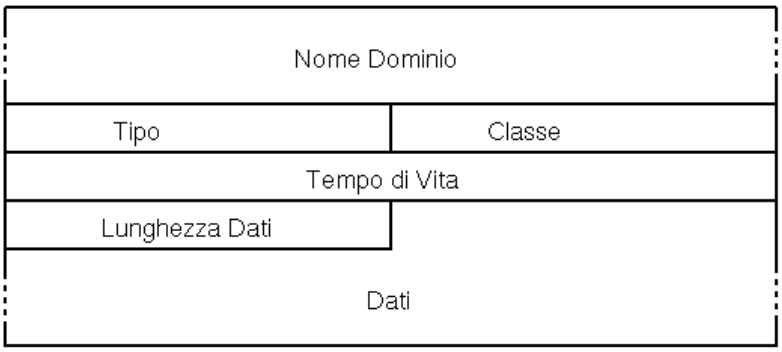


Ogni dominio viene amministrato da un'organizzazione.
I TLD sono gestiti dall'InterNIC(Internet Network Information Center) che delega l'amministrazione di ogni dominio ad altre autorità. Ad esempio il dominio .it è amministrato dalla *Registration Authority* Italiana ovvero dal NIC (www.nic.it).
Molto spesso queste organizzazioni delegano l'amministrazione dei loro sottodomini a terzi. Quindi ad esempio il dominio *wind.it* viene gestito da Wind per delega dalla *Registration Authority*, il dominio *net.wind.it* è gestito da Net per delega da Wind.

Resource Record

Tutte le informazioni relative alla zona coperta da un server DNS vengono memorizzate in un file sotto forma di *Resource Record* (RR) ovvero di un **descrittore di risorsa**.
Associato ad un nome di dominio possiamo trovare più RR, ciascuno contenente informazioni di vario tipo, ma relative sempre allo stesso nome.
Il descrittore di risorsa più comune è il record che contiene l'IP di un host, tuttavia esso può contenere anche altre informazioni quale per esempio il nome di un altro name server, etc….
Di seguito viene mostrata la struttura del descrittore di risorsa:

Resource Record DNS



Il formato generico di un RR dispone oltre ai dati (es. valore dell'IP) dei seguenti campi:

- *Nome Dominio*: Il nome di dominio a cui questo RR si riferisce: è la chiave di ricerca utilizzata per rispondere alle richieste,vengono restituiti tutti i descrittori di risorsa del dominio.
- *Tempo di vita*: Time-To-Live(TTL), indica in secondi quanto a lungo questo RR rimarrà nella cache dei server DNS prima di essere scartato.
- *Classe*: Identifica la famiglia di protocollo. Il valore usato è sempre IN che indica il sistema Internet.
- *Tipo*: Il tipo di RR. I tipi principali sono:
    - A: E' il tipo più usato. Indica che il RR contiene l'indirizzo IP per il dominio specificato. Usato nella normale risoluzione del nome.
    - CNAME: *Record Canonical Name*, usato per indicare un alias per un indirizzo IP
    - MX: Mail eXchanger, nome del server di posta per il dominio
    - NS: Un server DNS per il dominio specificato.
    - PTR: alias per un indirizzo IP. Usato nella risoluzione inversa.
    - SOA(*Start of Authority*) : un RR che indica il server DNS dove risiedono i dati autoritativi per questo dominio ed alcuni dati amministrativi.
    - Rdata: Contiene le informazioni per il tipo specificato.

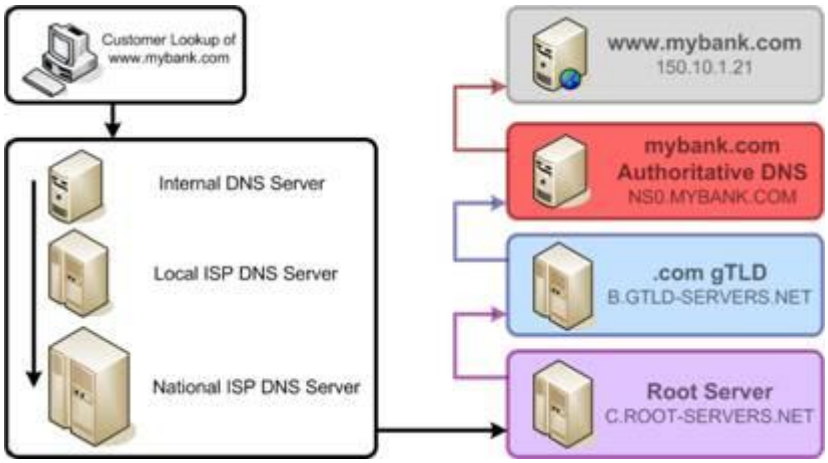
A seconda del valore di *Tipo* abbiamo i seguenti casi:

- A: Un indirizzo IP a 32 bit
- CNAME: nome di dominio
- MX: nome host.
- NS: nome host
- PTR: nome di dominio
- SOA: Comprende diversi campi(indirizzo di posta dell'amministratore,flag,…)

Risoluzione di un dominio

La ricerca di un indirizzo IP molto spesso non è un operazione diretta. Questo perché come già detto, il database DNS non è localizzato in una sola macchina.

La ricerca di un server non locale comporta l'interrogazione dei server DNS di livello superiore e poi di nuovo di quelli di livello inferiore finché non si individua un server DNS in possesso delle informazioni ricercate.
In questo processo si sale e si ridiscende la struttura ad albero, come mostrato nella seguente figura:



Si noti che non si chiede direttamente al server radice in quanto per via del *caching* l'informazione cercata potrebbe essere già disponibile nei server DNS di livello superiore come verrà illustrato in dettaglio più avanti.

Vediamo ora il meccanismo DNS al lavoro. Quando un utente desidera collegarsi con il sito www.networkingitalia.it vengono eseguiti i seguenti passi:

1. Sul computer dell'utente viene consultato il file HOSTS alla ricerca del server WWW di Networkingitalia.
2. Non trovandolo, viene effettuata una richiesta al proprio server DNS. Questo può essere il DNS del provider Internet, oppure, se il computer è installato in una rete collegata direttamente ad Internet, è probabile che il server DNS sia interno.
3. Dato che il server contattato si limita a coprire solo la sua zona (nel caso del DNS del provider si tratterà della zona al di sotto di nomeprovider.it, nel caso di un DNS interno la zona coperta sarà del tipo nome-organizzazione.it) la richiesta viene inoltrata ad un DNS radice.
4. Il DNS radice non conosce l'IP per www.networkingitalia.it ma conosce i Resource Record dei server DNS .it e li restituirà al primo DNS.
5. A questo punto il nostro DNS inoltra la stessa richiesta verso l'indirizzo di un DNS .it
6. Il DNS .it non conosce l'IP per www.networkingitalia.it ma conosce i RR relativi ai DNS che gestiscono il dominio networkingitalia.it e li restituirà al primo DNS.
7. Il nostro DNS ora contatta uno di questi DNS, il quale finalmente conosce l'IP per www.networkingitalia.it e lo restituisce al computer dell'utente.

In genere i sistemi operativi sono dotati di un comando nslookup che consente di interrogare direttamente i server DNS per risolvere un dominio.

Per utilizzare tale utility in Windows basta digitare al prompt dei comandi:

C:/> nslookup

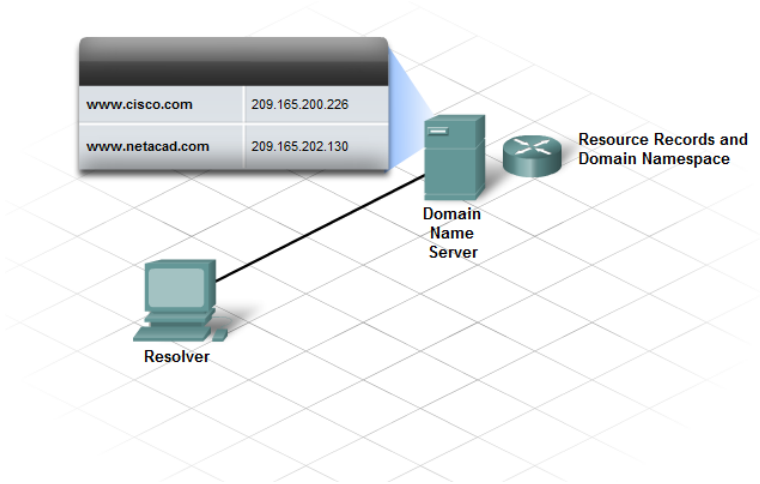
Viene mostrato il nome del DNS server di default e il suo IP.

Digitando i nomi dei domini da risolvere avremo come risposta gli IP corrispondenti:

```
C:\Users\Mario>nslookup
Server predefinito:  UnKnown
Address:  192.168.0.1

> www.google.com
Server:  UnKnown
Address:  192.168.0.1

Risposta da un server non autorevole:
Nome:    www.l.google.com
Addresses:  74.125.39.104
          74.125.39.147
          74.125.39.106
          74.125.39.99
          74.125.39.105
          74.125.39.103
Aliases:  www.google.com

> www.tiscali.it
Server:  UnKnown
Address:  192.168.0.1

Risposta da un server non autorevole:
Nome:    www.tiscali.it
Address:  213.205.32.10

>
```

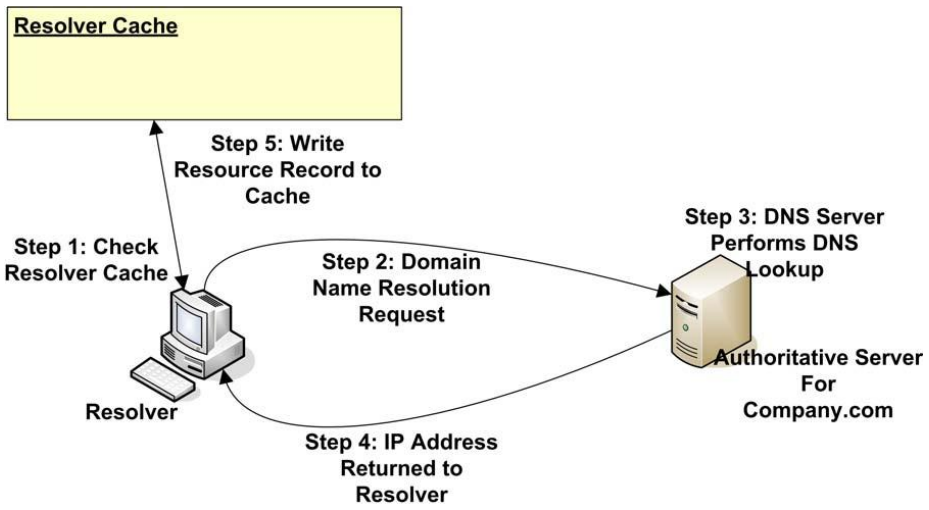
Il resolver

Si tratta di una procedura client server.
Il client (detto anche resolver) è in esecuzione sulle macchine collegate in rete e si occupa di effettuare al DNS le richieste di traduzione da indirizzi in nomi e viceversa.
Il server è il server DNS e si occupa di rispondere alle richieste del resolver seguendo i passi appena visti.
Data la brevità e la semplicità delle richieste e delle relative risposte, il protocollo usato è per lo più l'UDP, che ricordo, fornisce una comunicazione meno affidabile ma più veloce. Più raramente si usa il TCP. La porta usata dal servizio DNS è la numero 53.

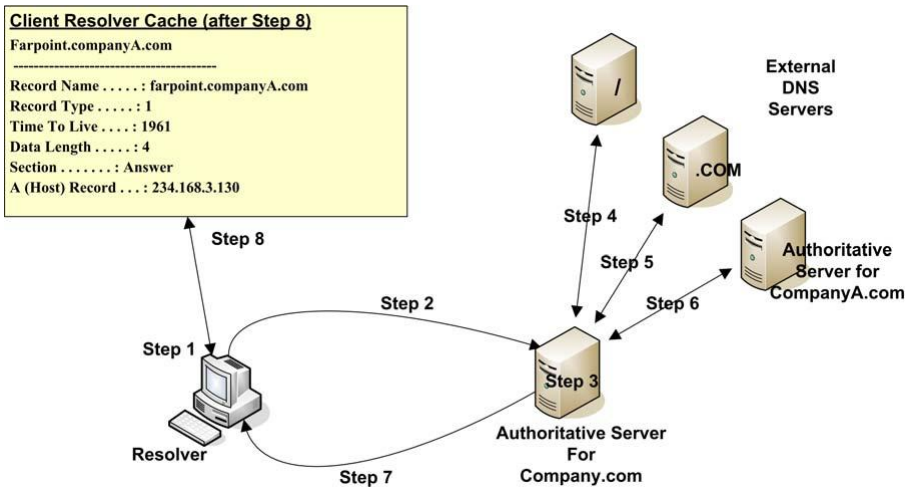


Il resolver come anche i vari server DNS locali sono dotati di una cache in cui vengono memorizzati i risultati delle interrogazioni effettuate in maniera da evitare di ripetere ogni volta la ricerca.

Nell' esempio mostrato nella seguente figura l'indirizzo IP è contenuto nella cache del Server DNS locale che fornisce al resolver i dati richiesti:



Di seguito viene invece mostrata una ricerca che coinvolge anche i livelli superiori, in particolare si noti come tali dati vengano memorizzati dal client nella sua cache:



Per osservare il contenuto della cache del resolver DNS relativa al proprio pc-windows basta digitare al Promt dei Comandi :

C:/ > ipconfig /displaydns

Questo è un esempio dell'output che si ottiene :

update.microsoft.com

 Nome record . . . . . : update.microsoft.com
 Tipo record . . . . . : 5
 Durata (TTL). . . . . : 74
 Lunghezza dati. . . . : 4
 Sezione . . . . . : Risposta
 Record CNAME . . . . : update.microsoft.com.nsatc.net

 10.33.205.213.in-addr.arpa

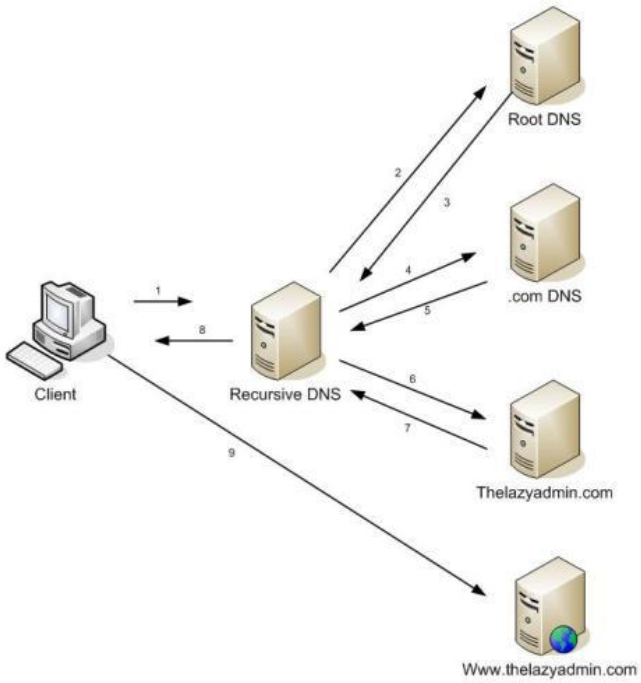
 Nome record . . . . . : 10.33.205.213.in-addr.arpa
 Tipo record . . . . . : 12
 Durata (TTL). . . . . : 38525
 Lunghezza dati. . . . : 4
 Sezione . . . . . : Risposta
 Record PTR . . . . . : pop.tiscali.it

 windowshelp.microsoft.com

 Nome record . . . . . : windowshelp.microsoft.com
 Tipo record . . . . . : 1
 Durata (TTL). . . . . : 1411
 Lunghezza dati. . . . : 4
 Sezione . . . . . : Risposta
 Record A (Host) . . . : 207.46.197.98

Risoluzione ricorsiva e iterativa

Il modo di procedere nella risoluzione del nome è detto **ricorsivo** se viene chiesto al **DNS di fare tutto il lavoro ed alla fine di restituire la risposta**.



E' non ricorsivo o iterativo se invece della risposta **può venire restituito un riferimento ad un altro DNS e sarà lo stesso server a dover effettuare l'interrogazione presso il nuovo DNS server**.
Un server DNS è in grado di gestire i riferimenti, quindi può usare entrambi i metodi per risolvere la richiesta. Il resolver usa invece il metodo ricorsivo perché non è in grado di seguire i riferimenti, quindi lascia tutto nelle mani del suo DNS. I server radice sono non ricorsivi: se non hanno la risposta, forniscono gli indirizzi di chi la possiede. I server DNS dei provider sono ricorsivi nei confronti dei computer dei propri utenti perché cercano la risposta e quando la trovano la restituiscono al client.
I server DNS sono in grado di effettuare *caching*, cioè possono ricordare le interrogazioni effettuate più di recente e le relative risposte. In questo modo la risoluzione di un nome molto richiesto può essere soddisfatta immediatamente, senza dover inoltrare la query ad un DNS radice. Nel nostro esempio il DNS dell'utente ha interpellato il DNS radice per conoscere uno dei DNS .it
In realtà è molto probabile che questa informazione si trovi già nella cache del server DNS.
Come abbiamo visto ogni RR contiene un campo TTL (Time To Live) che indica in secondi quanto a lungo i server DNS terranno l'RR in cache. Di solito il valore è di 86400 secondi (24 ore).

Struttura dei messaggi DNS

I pacchetti di richiesta e di risposta del DNS contengono i seguenti campi:

- *Header*: Indica se il messaggio è una richiesta o una risposta, contiene alcuni flag, i codici di errore ed altre informazioni relative al pacchetto.
- *Question*: contiene la domanda per il DNS.
- *Answer*: contiene un elenco di RR che rispondono alla domanda.
- Authority: contiene un elenco di RR NS di server DNS che portano più vicino alla risposta.
- *Additional*: contiene un elenco di RR con informazioni utili per rispondere alla domanda, anche se non si tratta della risposta.

Header	
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

Formato generale Messaggi DNS

Identificativo	Flag
Numero Richieste	Numero RR Risposte
Numero RR Autorita'	Numero RR Aggiuntivi
Richieste	
RR Risposta	
RR Autorita'	
RR Informazioni Aggiuntive	

Campo Flag DNS

QR	Codice	AA	TC	RD	RA	Zero	Ritorno

Nell'header troviamo tra le altre cose il flag AA (*Authoritative Answer*). Quando è attivo, nei messaggi di risposta, indica che il DNS che ha generato la risposta (direttamente o indirettamente) è il server autorevole per quella zona. Se la risposta viene memorizzata nella cache del nostro DNS, effettuando la stessa richiesta, otterremo la stessa risposta ma con il flag AA non attivo, ad indicare che la risposta non è autorevole.

Tipi Richiesta e Responso DNS

Nome	Valore	Descrizione	Responso	Richiesta
A	1	Indirizzo IP	■	■
NS	2	Name Server	■	■
CNAME	5	Nome Canonico	■	■
PTR	12	Record Puntatore	■	■
HINFO	13	Informazioni Host	■	■
MX	15	Record Mail Exchange	■	■
AXFR	252	Richiesta di Zone Transfer		■
* o ANY	255	Richiesta di Tutti i Record		■

Una particolarità dei messaggi di risposta è che il campo Authority, contenente i RR che portano verso i server autorevoli, viene riempito anche se il messaggio è la risposta. Se chiediamo un record A contenuto nella cache, la risposta come è stato detto è non autorevole. Tuttavia il campo Authority contiene ancora gli indirizzi autorevoli, cioè permette di sapere quali sono i server DNS a cui rivolgersi per avere la risposta autorevole.
Per il corretto funzionamento di tutto questo meccanismo ogni server DNS deve avere due tipi di informazione. Il primo tipo riguarda i domini direttamente coperti dal DNS. Il secondo tipo è l'indirizzo del DNS radice a cui rivolgersi nel caso una richiesta non possa essere risolta internamente. Si può trovare la lista ufficiale dei DNS radice al seguente indirizzo: ftp://ftp.rs.internic.net/domain/named.root
Inoltre ogni macchina in rete deve essere configurata in modo da conoscere l'indirizzo IP del DNS che dovrà usare (a meno che questa informazione non venga fornita automaticamente).

Bilanciamento del carico e tolleranza ai guasti

Un'altra peculiarità del DNS è la capacità di fornire servizi di *load balancing* e *fault tolerance*.
Per far questo vengono associati gli indirizzi IP di diverse macchine ad un solo nome. Il computer dell'utente sceglierà a caso uno di questi indirizzi. Server DNS più sofisticati sono in grado di restituire un solo indirizzo IP basandosi sul carico delle macchine e sulla loro disponibilità.
Per ottenere il nome di una macchina sapendo l'indirizzo IP le cose diventano più complesse. Sapere i nomi a partire da indirizzi IP torna utile per varie ragioni. Ad esempio, per produrre un output leggibile nei file di log, altre volte viene usato per controlli di autenticazione.
Per ricavare un indirizzo IP dato il nome, si può seguire la struttura gerarchica dell'albero dei domini nel modo visto in precedenza. Per effettuare l'operazione inversa non è più possibile seguire questa gerarchia.
Per rendere possibile questo servizio è stato riservato il dominio speciale "*in-addr.arpa*", chiamato anche dominio inverso. Termina in "arpa" perché Internet era originariamente denominata ARPAnet. Dato che i nomi dei domini sono organizzati in modo tale da avere la parte più significativa a destra, mentre gli indirizzi IP, nel formato decimale, hanno i byte più significativi a sinistra, è necessario creare il nome di dominio inverso mettendo i numeri dell'indirizzo IP in ordine inverso e aggiungendo *in-addr.arpa* alla fine. In questo modo viene rispettata la natura gerarchica del DNS. Un esempio di dominio *in-addr.arpa* può essere *34.16.1.151.in-addr.arpa* Quando viene effettuata una richiesta di traduzione da IP a nome, viene effettuata una normale ricerca del nome di dominio. Ad esempio se in Unix si digita il comando "*nslookup 151.1.16.34*" viene eseguita una ricerca per il nome di dominio "*34.16.1.151.in-addr.arpa*". Per poter funzionare sono presenti nei DNS i RR di tipo PTR il cui funzionamento ricalca a grandi linee quello dei record A.

Gestione Posta Elettronica

Il server DNS ha un'altra importante funzione oltre a quelle viste finora. Gioca infatti un ruolo molto importante nella gestione della posta elettronica. Normalmente quando si pensa alla posta elettronica si pensa che il mail server del computer mittente debba solo conoscere il mail server del dominio del destinatario per arrivare a destinazione. Se questo fosse vero il mail server del mittente si limiterebbe ad interrogare il proprio DNS per scoprire l'indirizzo IP del mail server del destinatario. In realtà il DNS non si limita a fornire un servizio di traduzione da indirizzi IP a nomi e viceversa.
E' infatti in grado di fornire alcune utili informazioni di routing per la posta al mail server mittente.
Per ogni dominio che è in grado di ricevere posta, il DNS è in grado di fornire una lista di computer a cui si può inviare il messaggio. In questo modo, se il mail server principale del destinatario non è operativo, è possibile inviare il messaggio verso un computer di backup in grado di gestire la posta altrettanto bene. Queste informazioni sono contenute nei record MX (Mail eXchanger). Il mail server deve sempre chiedere al proprio DNS quali host possono gestire la posta per un certo dominio. Inserendo informazioni appropriate nei record MX di un DNS si può informare il mail server associato a quel DNS che, per un certo dominio, esistono varie macchine che possono ricevere la posta. Ogni record MX restituito al mail server contiene tra le altre cose un valore di preferenza. Il valore di preferenza indica al mail server un ordine di scelta tra gli host MX a cui è possibile consegnare il messaggio per il dominio specificato.

Utilizzo di un server DNS

Quando si allaccia il proprio computer o la propria rete ad Internet è essenziale disporre di un servizio DNS in modo da trovare e farsi trovare sulla rete. Per far questo ci sono sostanzialmente due strade. La prima è di affidarsi ai server DNS di un provider Internet. La seconda è di installare un server DNS all'interno della propria rete.
Nel primo caso bisogna contattare un Internet Service Provider informandolo riguardo i record che si vogliono inserire per permettere l'accesso dall'esterno. L' ISP informerà la *Registration Authority* del fatto che esso fornisce servizi DNS per il o i computer che si vogliono allacciare ad Internet. Fatto questo si procede con il configurare le proprie macchine in modo che usino i DNS dell' ISP.
Se invece si vuole dotare la propria rete di un server DNS interno bisogna prima di tutto dotarsi di due server DNS, uno primario ed uno secondario, altrimenti l'InterNIC o la RA Italiana non acconsentiranno all'inserimento del nome di dominio nel database dei propri DNS. Fatto questo si procede alla registrazione di un dominio presso la *Registration Authority*. A questo punto si possono configurare i propri DNS per strutturare al meglio la propria rete.
Un secondo server DNS è sempre richiesto per ragioni di fault tolerance. Le informazioni contenute nel DNS secondario sono una copia del primario. Periodicamente (di solito ogni 6 ore, ma è possibile specificare qualsiasi intervallo) il DNS secondario interroga il primario per controllare se la tabella dei domini indirizzati è cambiata. In caso affermativo questa viene copiata nel secondario.
La Registration Authority varia a seconda del dominio di primo livello sotto cui si vuole inserire la propria organizzazione. Come abbiamo detto, per il dominio .it esiste la *Registration Authority* Italiana (http://www.nic.it/RA). Nel caso si usi uno dei domini generici .com, .edu, .gov, .org, .net bisogna rivolgersi all'InterNIC (http://www.internic.net).
L'autorità centrale al di sopra di queste organizzazioni e responsabile del coordinamento e della gestione del sistema DNS è l' *Internet Assigned Numbers Authority* (IANA).
Si può trovare una lista dei domini di primo livello e delle relative organizzazioni che li gestiscono al sito http://www.norid.no/domreg.html .

Avere il proprio server DNS comporta diversi vantaggi, tra cui una più veloce risoluzione dei nomi dato che il server DNS dell' ISP è di solito piuttosto caricato di traffico. Inoltre, nel caso ci siano frequenti cambiamenti nei nomi delle macchine della propria rete, si può effettuare l'aggiornamento dei propri DNS in modo diretto, mentre con un ISP bisogna aspettare un certo intervallo di tempo, di solito stabilito dall' ISP stesso.
Se ciò che vogliamo è solo risolvere i nomi più velocemente senza registrare alcun dominio e senza rivolgersi all' ISP o all'Authority, è sufficiente impostare un server DNS con semplici funzioni di caching. Questo sistema velocizza le richieste di risoluzione, specialmente se il DNS del proprio ISP è sovraccaricato. Inoltre questo sistema funziona senza problemi anche con gli indirizzi IP dinamici. Un DNS caching è un server non autorevole. Ottiene tutte le sue informazioni dai server DNS primario e secondario, non ha autorità su nessuna zona e richiede almeno un RR NS da cui poter ricavare inizialmente informazioni.
A questo punto è opportuno fare una precisazione. Ciò di cui abbiamo parlato è la registrazione di un nome di dominio. Non stiamo parlando dell'attribuzione di indirizzi IP per le proprie macchine. Per fare questo ci sono altre organizzazioni, come la RIPE per Europa, Medio Oriente e parte dell'Africa, l'ARIN per Nord e Sud America, Caraibi e Africa Sub-Sahariana, e l'APNIC per l'Asia del Pacifico. Diversamente dal caso dei nomi, per avere un indirizzo IP fisso rivolgersi al proprio ISP è spesso l'unica strada dato che gli indirizzi non vengono rilasciati direttamente agli utenti finali ma solo agli ISP e ad altre organizzazioni che fanno uso di un grande numero di indirizzi.
E' bene notare che i server DNS non producono nessun tipo di broadcast per rendersi visibili nella rete. E' necessario effettuare la registrazione presso l'autorità sotto la quale vogliamo comparire. Se si installasse un server DNS senza registrare il dominio che si intende coprire, questo non avrebbe effetto sulla rete perché il server DNS di livello superiore non lo indirizza (o ne indirizza un altro se il dominio è già stato registrato da un'altra organizzazione).
Per ottenere informazioni su un dominio e sul suo gestore esiste un sistema, il WHOIS che permette di collegarsi ed effettuare richieste ad un server NIC(è possibile ottenere lo stesso servizio andando sul sito www.whois.net).

Virtual Hosting

Uno dei vantaggi dell'utilizzo del DNS è quello di poter gestire più domini su uno stesso server.
In pratica registrando due domini *www.sito1.com* e *www.sito2.com* con lo stesso indirizzi IP sul DNS, le richieste verranno inoltrate allo stesso server che è in grado di distinguere il sito richiesto leggendo l'header HTTP (contente l'URL digitata).
Questa è una soluzione molto economica per gestire più siti senza dover acquistare più indirizzi IP.

Motivazioni utilizzo DNS

In conclusione elenchiamo di seguito una serie di ragioni che rendono vantaggioso l'utilizzo di questo sistema distribuito:

- La possibilità di attribuire un nome testuale facile da memorizzare a un server (ad esempio un sito world wide web) migliora di molto l'uso del servizio, in quanto gli esseri umani trovano più facile ricordare nomi testuali (mentre gli host e i router sono raggiungibili utilizzando gli indirizzi IP numerici). Per questo, il DNS è fondamentale per l'ampia diffusione di internet anche tra utenti non tecnici, ed è una delle sue caratteristiche più visibili.

- È possibile attribuire più nomi allo stesso indirizzo IP (o viceversa) per rappresentare diversi servizi o funzioni forniti da uno stesso host (o più host che erogano lo stesso servizio) Questa flessibilità risulta utile in molti casi:
    - Nel caso il server debba sostituire il server che ospita un servizio, o si debba modificare il suo indirizzo IP, è sufficiente modificare il record DNS, senza dover intervenire sui client.
    - *virtual hosting*
    - *re-direzione*: utilizzando nomi diversi per riferirsi ai diversi servizi erogati da un host, è possibile spostare una parte dei servizi su un altro host, e spostare i client su questo nuovo host modificando il suo record nel DNS.
    - *Bilanciamento carico e tolleranza ai guasti*: facendo corrispondere più indirizzi IP a un nome, *il carico dei client viene distribuito su diversi server*, ottenendo un aumento delle prestazioni complessive del servizio e una tolleranza ai guasti (ma è necessario assicurarsi che i diversi server siano sempre allineati, ovvero offrano esattamente lo stesso servizio ai client).
- La risoluzione inversa è utile per identificare l'identità di un host, o per leggere il risultato di un *traceroute*.