NETLINK S.a.s.

# Servizi di Rete: Il DNS
## Domain Name System

**Dott. Paolo PAVAN**

*Netlink S.A.S*

*Via Alpignano, 27*

*10093 collegno (TO)*

*pavan@netlink.it - http://www.netlink.it*

# Funzionamento DNS

Quando un client DNS **ha la necessità di ricercare un nome utilizzato in un programma, interroga i server DNS per risolvere il nome**. Ogni messaggio di interrogazione inviato dal client contiene tre tipi di informazioni, che specificano la domanda alla quale il server dovrà rispondere:

- Un nome di dominio DNS, specificato come nome di dominio completo (FQDN, Fully Qualified Domain Name)
- Un determinato tipo di interrogazione, che può specificare un record di risorsa per tipo o un tipo particolare di operazione relativa all'interrogazione
- Una determinata classe per il nome di dominio DNS.

Ad esempio, il nome specificato potrebbe essere l'FQDN relativo a un computer, ad esempio "host.dominio.com" e il tipo di interrogazione specificato potrebbe essere di cercare il record di risorsa di un indirizzo (A) tramite quel nome. Si consideri un'interrogazione DNS come una domanda composta di due parti che un client pone a un server, vale a dire "Sono disponibili dei record di risorse A per un computer denominato host.dominio.com?". Quando il client riceve una risposta dal server, legge e interpreta il record di risorsa A contenuto nella risposta, memorizzando l'indirizzo IP relativo al computer che aveva richiesto in forma di nome.

# Cosa è il DNS

- Domain Name System (DNS) è un servizio di nomi standard TCP/IP e per Internet, che consente ai computer client della rete di registrarsi e risolvere i nomi di dominio DNS
- Questo vuol dire che ad un dato IP (ad es 192.168.17.10) corrisponderà un nome univoco di host (ad es client01) di un determinato dominio (ad es dominio.com)

# Il Processo d'interrogazione

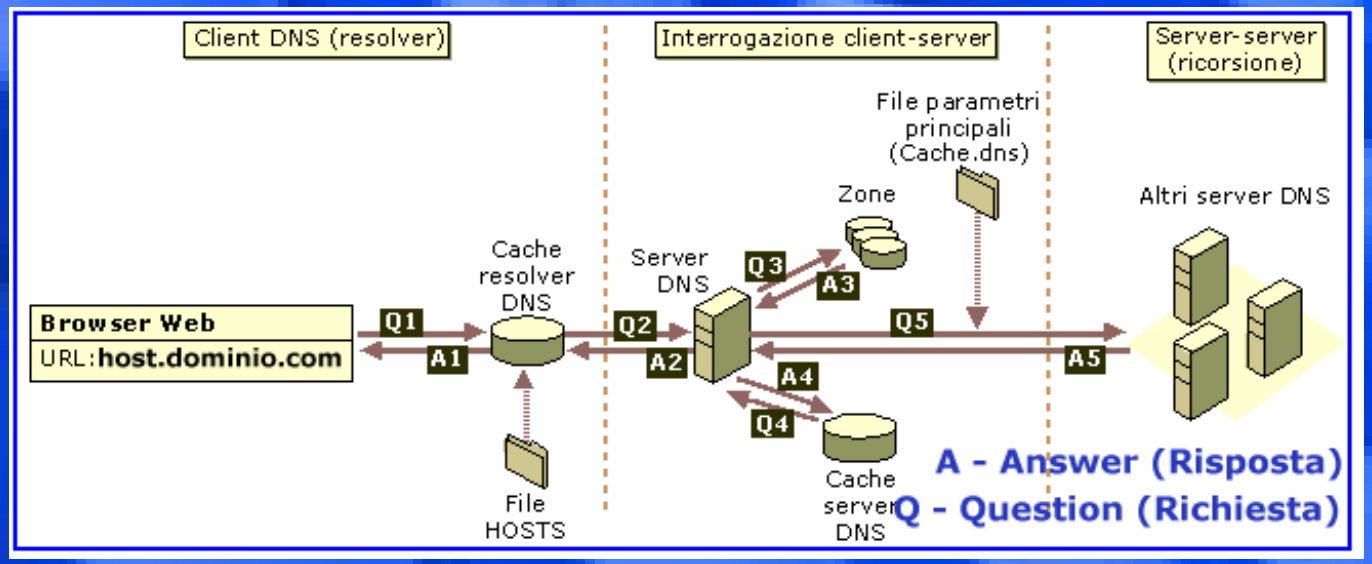
- In genere, il processo dell'interrogazione DNS si compone di due parti:
  - L'interrogazione relativa a un nome inizia sul computer client e viene passata a un resolver, il servizio **Client DNS**, per la risoluzione.
  - Quando non è possibile risolvere l'interrogazione localmente, la risoluzione del nome può essere richiesta ai **server DNS**.

# Metodologie di risoluzione

Le interrogazioni DNS possono essere risolte in svariati modi.

- Talvolta un client può rispondere a un'interrogazione **localmente,** mediante informazioni memorizzate nella cache e ottenute in seguito a un'interrogazione precedente. Per rispondere a un'interrogazione, il server DNS può utilizzare la **propria cache** di informazioni sui record di risorsa.
- Oppure un **server DNS può anche interrogare o contattare altri server DNS** per conto del client richiedente, in modo da risolvere il nome completamente e quindi inviare una risposta al client. Questo processo è noto come **ricorsione**.
- Inoltre, **lo stesso client** può tentare di connettersi con **altri server DNS** per risolvere un nome. In questo caso, il client utilizza interrogazioni aggiuntive e distinte, basate su risposte di riferimento ricevute dai server. Questo processo è noto come **iterazione.**

# Resolver Locale: Schema




- Lo schema prevede prima la richiesta alla cache locale (Client DNS) poi al DNS server della rete (File di Zona e Cache)

# Resolver Locale

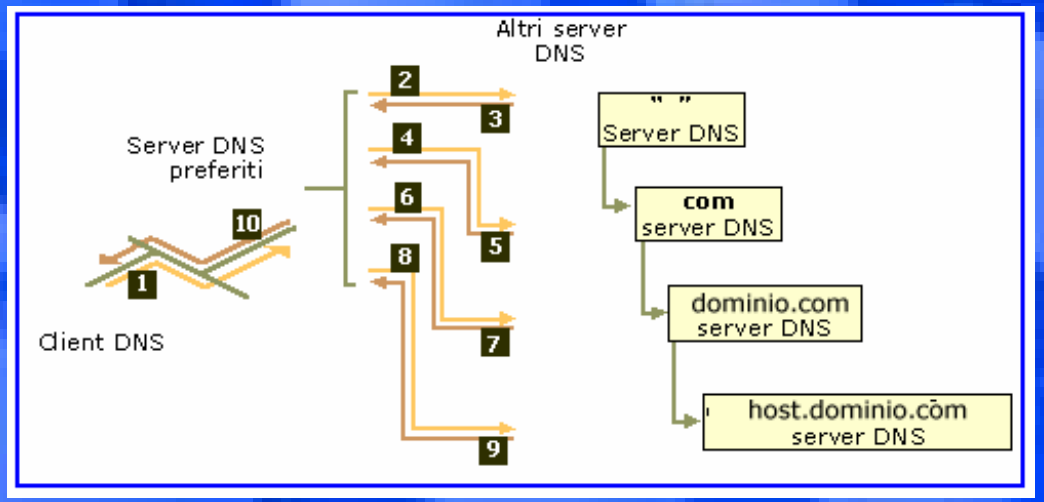
- La richiesta viene quindi passata al servizio Client DNS per la risoluzione, utilizzando informazioni memorizzate nella cache locale. Se il nome richiesto può essere risolto, l'interrogazione ottiene una risposta e il processo è completo.
- La cache del resolver locale può anche includere informazioni sul nome ottenute da due possibili fonti:
  - Se esiste un **file Hosts** configurato localmente, tutti i mapping del nome/indirizzo IP dell'host provenienti da quel file verranno precaricati nella cache all'avvio del servizio Client DNS.
  - I record di risorse ottenuti con le risposte alle interrogazioni DNS precedenti vengono aggiunti alla cache e conservati per un certo periodo.
- Se l'interrogazione non trova corrispondenza con una voce presente nella cache, il processo di risoluzione prosegue e il client chiede a un **server DNS di risolvere il nome**.

# Interrogazione del server DNS

Quando il server DNS riceve un'interrogazione, utilizza questo schema sequenziale per rispondere all'interrogazione:

- Verifica innanzitutto se è in grado di dare all'interrogazione una **risposta autorevole** in base alle informazioni sui record di risorse contenuti in una **zona configurata localmente sul server**. Se il nome richiesto individua un record di risorsa corrispondente nelle informazioni locali di zona, il server dà una **risposta autorevole (autoritativa)** utilizzando queste informazioni per risolvere il nome richiesto.
- Se non esistono informazioni di zona relative al nome richiesto, il server verifica allora se è in grado di risolvere il nome mediante informazioni **memorizzate nella cache** locale in seguito a interrogazioni precedenti. Se viene trovata una corrispondenza, il server risponderà con queste informazioni. Anche in questo caso, se il server preferito può inviare al client richiedente una risposta positiva in base a una corrispondenza trovata dalla relativa cache, l'interrogazione è completa ma la risposta sarà **non autorevole (autoritativa)**.
- Se invece il nome richiesto non trova sul server preferito — né nella relativa cache né nelle informazioni di zona — una corrispondenza valida per inviare la risposta, **il processo di interrogazione prosegue**, utilizzando la **ricorsione** per risolvere il nome completamente. Ciò comporta **l'intervento di altri server DNS per** consentire la risoluzione del nome.

# Interrogazione ad un DNS: Schema




- Lo schema prevede il passaggio della richiesta ad altri DNS attraverso un **schema gerarchico ricorsivo** fino ad arrivare ad un DNS in grado di dare una risposta autoritativa.
- A questo punto il server DNS locale sa a quale server DNS di livello superiore fare la rischiesta per ottenere una risposta positiva.

# La Ricorsione

- Si consideri l'uso del processo di ricorsione per individuare il nome "host.dominio.com." quando il client interroga un singolo server DNS. Il processo ha luogo quando un server e un client DNS vengono avviati per la prima volta e non dispongono nella cache locale di informazioni utili a favorire la risoluzione di un nome. *Si presuppone che il nome richiesto dal client riguardi un nome di dominio di cui il server non possiede informazioni memorizzate localmente*, vale a dire nelle relative zone configurate.
- In primo luogo, il server preferito analizza il nome completo e determina che è necessario conoscere la posizione del server autorevole per il dominio di primo livello, "**.com**". Il server utilizza quindi un'interrogazione iterativa indirizzata al server DNS di "com", per ottenere un riferimento al server di "**dominio.com**". Poi dal server di "dominio.com" ottiene una risposta di riferimento al server DNS di "**host.dominio.com**".
- Infine viene stabilita la connessione con il server di "host.dominio.com". Poiché questo server contiene il nome richiesto come parte della relativa zona configurata, **fornisce una risposta autorevole** al server di origine che ha avviato la ricorsione. Quando il server di origine riceve la risposta indicante che l'interrogazione effettuata ha ottenuto una risposta da un server autorevole, esso inoltra questa risposta al client richiedente, completando così il processo di interrogazione ricorsiva.
- Sebbene il processo di interrogazione ricorsiva comporti un notevole sfruttamento delle risorse, esso offre alcuni vantaggi relativi alle prestazioni del server DNS. Ad esempio, durante il processo di ricorsione, il server DNS che effettua la ricerca ricorsiva ottiene informazioni sullo spazio dei nomi di dominio DNS. Queste informazioni vengono memorizzate dal server nella cache e potranno essere riutilizzate per velocizzare la risposta a interrogazioni successive che le utilizzano o che trovano in esse una corrispondenza. Queste informazioni memorizzate nella cache possono aumentare anche di molto, *sebbene esse vengano cancellate ogni volta che il servizio DNS viene avviato e arrestato.*

# Iterazione

- L'iterazione è il tipo di risoluzione del nome utilizzato tra i client e i server DNS quando si verificano le seguenti condizioni:
  - Il client richiede l'uso della ricorsione, ma questa è disabilitata sul server DNS.
  - Il client non richiede l'uso della ricorsione nell'interrogare il server DNS.
- Una richiesta iterativa proveniente da un client comunica al server DNS che il client attende la migliore risposta che il server DNS possa fornire sul momento, **senza contattare altri server DNS (no ricorsione)**.
- Quando si utilizza un'iterazione, un server DNS risponde a un client unicamente in base alle informazioni specifiche riguardanti lo spazio dei nomi e attinenti ai dati sui nomi interrogati. Utilizzerà per questo la sua cache o i suoi file di zona.
- Quando viene effettuato un riferimento, il client DNS si assume la responsabilità di **continuare le interrogazioni iterative verso altri server DNS** configurati per risolvere il nome, fino ad una ipotetica richiesta diretta al server DNS autoritativo per quella richiesta.
- Nella maggior parte delle interrogazioni iterative, un client **utilizza il proprio elenco di server DNS configurato localmente** per contattare altri server dei nomi nello spazio dei nomi DNS se il suo server DNS primario non può risolvere l'interrogazione.

# Memorizzazione nella cache

- La memorizzazione delle informazioni nella cache velocizza le prestazioni della risoluzione DNS per le successive interrogazioni di nomi molto comuni, mentre riduce notevolmente il traffico delle interrogazioni relative al DNS sulla rete.
- Nell'effettuare le interrogazioni ricorsive per conto dei client, i server DNS memorizzano temporaneamente nella cache i **Record di Risorse (RR).** Gli RR memorizzati nella cache contengono informazioni ottenute dai server DNS autorevole per i nomi di dominio DNS acquisiti con le interrogazioni iterative, durante ricerche effettuate allo scopo di dare una risposta completa a un'interrogazione ricorsiva per conto di un client. Successivamente, quando altri client effettuano nuove interrogazioni che richiedono informazioni sugli RR corrispondenti agli RR memorizzati nella cache, il server DNS può rispondere utilizzando le informazioni RR già memorizzate nella cache.
- Quando le informazioni vengono memorizzate nella cache, a tutti gli RR presenti nella cache viene applicato un valore di durata predefinito **(TTL, Time-To-Live).** Finché il valore di durata predefinito TTL, relativo a un RR memorizzato nella cache non scade, un server DNS può continuare a tenerne i dati nella cache e utilizzare nuovamente l'RR per rispondere alle interrogazioni dei client che corrispondono a questi RR. Nella maggior parte delle configurazioni di zona viene assegnato ai valori TTL relativi alla cache e utilizzati dagli RR il **TTL minimo (predefinito)**, che viene impostato nel record di risorsa della zona denominato Origine di autorità (SOA). In base all'impostazione predefinita, il TTL minimo è di 3.600 secondi (1 ora), ma è possibile regolarlo oppure, se necessario, impostare per ciascun RR uno specifico TTL relativo alla cache.

# Risposte di un DNS

La precedente discussione sulle interrogazioni DNS presuppone che il processo termini con l'invio al client di una risposta positiva. Tuttavia, le interrogazioni possono anche inviare altre risposte. Sono riportate di seguito le risposte più comuni:

**Risposta autorevole**

- Una risposta autorevole è una risposta positiva inviata al client e recapitata con il bit authority del messaggio DNS impostato per indicare che la risposta è **stata ottenuta da un server che ha autorità diretta sul nome richiesto.**

**Risposta positiva**

- La risposta positiva può consistere nell'RR o nell'elenco di RR per i quali è stata effettuata l'interrogazione (noto anche come RRset), che coincidono con il nome di dominio DNS interrogato e con il tipo di record specificato nel messaggio dell'interrogazione.

**Risposta di riferimento**

- La risposta di riferimento contiene altri record di risorse non specificati per nome o tipo nell'interrogazione. Questo tipo di risposta viene inviata al client se non è supportato il processo di ricorsione. In genere questi record dovrebbero rappresentare un utile riferimento che il client può utilizzare per continuare l'interrogazione mediante l'iterazione
  Una risposta di riferimento contiene dati aggiuntivi quali record di risorse (RR) diversi dal tipo interrogato. Ad esempio, se il nome host interrogato è "www" e nella zona non è stato trovato nessun RR A per questo nome, ma è stato trovato invece un record CNAME per "www", il server DNS può includere tali informazioni nella risposta al client..

**Risposta negativa**

- Una risposta negativa del server può indicare che in seguito al tentativo da parte del server di elaborare e risolvere ricorsivamente l'interrogazione in modo completo e con una risposta autorevole, si è determinata una di queste due possibilità:

- Un server autorevole ha riportato che il nome richiesto non esiste nello spazio dei nomi DNS.

- Un server autorevole ha riportato che il nome richiesto esiste, ma che non esistono, per quel nome, i record del

  tipo specificato.