6 IL DNS (DOMAIN NAME SYSTEM)

6.1 La risoluzione dei nomi

L'applicazione **DNS (Domain Name System)** consente agli utenti della rete di usare dei nomi per identificare un computer con funzioni di server al posto del suo indirizzo IP. Le specifiche del DNS si trovano negli RFC 1034 e RFC 1035 e successivi aggiornamenti. Questo sistema è basato su un **database distribuito**, organizzato gerarchicamente e che segue il modello Client/Server.

Il DNS è formato da 3 componenti principali.

- **Domain Name Space**, specifica la struttura ad albero dei nomi di dominio. Il Name Space risulta diviso in 3 tipi di domini:
  1. **domini radice**: sono i domini di primo livello (Top Level Domain, TLD);
  2. **domini intermedi**: sono domini che hanno a loro volta dei sottodomini;
  3. **domini foglia**: sono domini privi di sottodomini e contengono solo host.
- **Name Server**, è un processo applicativo con il ruolo di server che contiene informazioni su alcune parti del Name Space chiamate **zone**. Il Name Server costituisce una *authority* per tali zone (viene detto *authoritative Name Server*). Un Name Server contiene anche i puntatori ad altri Name Server che possono essere usati per ricavare informazioni su altre zone. La zona dei TLD è detta **root zone** e i Name Server che ne rispondono sono i **root Name Server**. Questi conoscono anche gli indirizzi degli authoritative Name Server per ciascun dominio TLD.
- **Resolver**, è un programma con il ruolo di client che ottiene informazioni dal Name Server. Tipicamente viene realizzato da procedure del Sistema Operativo. Per esempio in Unix per accedere al resolver si richiamano le routine gethostbyname e gethostbyaddr.

#prendinota

La gestione dei nomi di dominio di primo livello è effettuata dall'organizzazione **IANA** (*Internet Assigned Numbers Authority*).
Un elenco aggiornato dei Top Level Domain si trova all'indirizzo: *www.iana.org/domains root/db/*.
IANA collabora con **ICANN** (*Internet Corporation for Assigned Names and Numbers*) l'ente che gestisce il DNS a livello mondiale e coordina le attività dei root Name Server.

Il sistema DNS è usato anche all'interno delle reti locali private per risolvere i nomi dei computer (hostname). Infatti, grazie al DNS, si possono associare alle macchine dei nomi facili da ricordare; i nomi possono rimanere gli stessi anche se cambia l'indirizzo IP; gli utenti possono connettersi ai server locali usando le stesse convenzioni usate su Internet (URL).

Per comporre il nome completo di un dominio si percorre il cammino dalla foglia (che rappresenta l'host) alla radice, rappresentata da un punto (.), separando le varie componenti con un punto.
Per esempio: www.ietf.org è il nome di dominio dell'host che offre il servizio web per l'organizzazione IETF (Internet Engineering Task Force). Infatti www è il nome del server web che si trova nel dominio *ietf* che a sua volta è contenuto nel dominio *org* il quale discende dal dominio radice.
Da notare che per il DNS i nomi "www.ietf.org" e "www.ietf.org." sono uguali in quanto il punto finale (che indica il dominio radice) è implicito in ogni nome di dominio, quindi può essere omesso.

Valgono poi le seguenti regole:

- i nomi delle singole componenti del cammino completo non devono superare i 63 caratteri, inclusi i punti (sono preferibili i nomi facili da ricordare);

- un cammino completo non deve superare i 255 caratteri, quindi meglio limitare il numero di livelli usati (non più di 5) e scegliere dei nomi brevi, per non renderne troppo complessa l'amministrazione;
- i nomi sono *case-unsensitive*, quindi è indifferente scrivere .it oppure .IT, perché entrambi individuano lo stesso dominio;
- ogni dominio controlla i suoi sottodomini, quindi se si vuole creare un nuovo sottodominio è necessario il permesso del dominio *padre*, mentre non si deve chiedere alcun permesso ai livelli superiori dell'albero.

6.2 Il formato dei pacchetti DNS

Il formato dei pacchetti DNS consente a un client di porre più richieste (**query**) in un singolo messaggio (**DNS request**). Ogni query consiste nel nome di dominio del quale il client cerca l'indirizzo IP e il tipo di oggetto desiderato (per esempio l'indirizzo). Il server risponde restituendo un messaggio simile (**DNS reply**) che contiene le risposte (**answer**) alle query. Se non può soddisfare tutte le query, il server indica nel messaggio di risposta altri Name Server che il client può contattare per ottenere le risposte. In FIGURA 14 è mostrato il formato delle PDU DNS, dove RR indica il **Resource Record.**

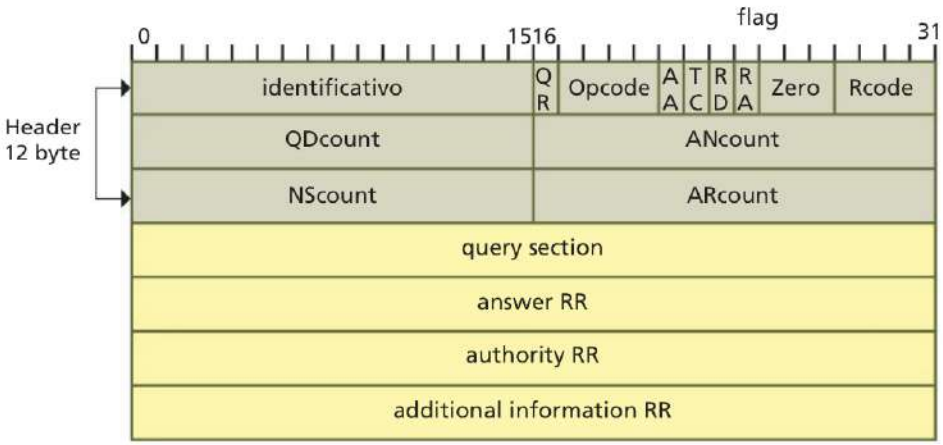


FIGURA 14 Formato delle PDU DNS

Il pacchetto è formato da una parte di header fissa di 12 byte e da 4 campi a lunghezza variabile.

I campi hanno il seguente significato:

- **identificativo**: è deciso dal client e inserito nelle risposte del server, permette di far corrispondere le reply alle request;
- **flag**: è un campo a 16 bit così suddiviso:
  - **QR** indica se il messaggio è una query (0) o una risposta (1);
  - **Opcode** indica il tipo di request:
    0 = Query Standard
    1 = Query Inversa
    2 = Richiesta di Stato del Server
    dal 3 al 15 non sono attualmente utilizzati;
  - **AA** se vale 1 indica una risposta authoritative del server;
  - **TC** se vale 1 indica che la reply eccedeva i 512 byte e il messaggio è stato troncato;

- **RD** se vale 1 indica che si desidera una ricerca ricorsiva, altrimenti la ricerca sarà iterativa, è impostato dal **#local resolver**;
- **RA** Ricorsione Disponibile (Available), impostato dal server;
- **Zero** deve essere 0, è riservato per usi futuri;
- **RCod** Codice di ritorno:
  0 = Nessun errore
  1 = Errore nella costruzione della query
  2 = Errore interno nel server dei nomi
  3 = Ricevuto da un server di autorità, indica che il nome specificato nella query non esiste nel dominio
  4 = Il server dei nomi non implementa quel tipo di query
  5 = Il server si rifiuta di eseguire l'operazione per motivi di impostazioni
  Dal 6 al 15 sono riservati per usi futuri;
- i 4 campi successivi specificano il numero di occorrenze presenti in ciascuno dei 4 campi che si trovano dopo l'header (query, answer, authority, additional information). Per esempio, per una query, **QDcount** è di solito 1 e i contatori degli altri campi sono 0; per una answer, **ANcount** è almeno 1, mentre gli altri contatori possono essere 0 o maggiori;

- **query section**: di solito in questa sezione si trova la domanda; contiene un numero di entry, con nome, tipo e classe della query, pari al valore QDcount specificato;
- le 3 sezioni successive sono tutte costituite nello stesso modo: ogni sezione ha un numero variabile di Resource Record.

#techwords

Local resolver
È l'applicazione client che risiede sull'host e, a fronte di un nome, restituisce un valore, solitamente un indirizzo IP.

6.3 I Resource Record (RR)

Ogni dominio, o meglio, ogni zona mantiene le informazioni in strutture dette **Resource Record** (letteralmente: descrittore di risorsa).
L'uso più frequente di queste strutture è per ottenere un indirizzo IP: dato il nome di un host, il DNS trova il Resource Record che mantiene l'associazione tra quel nome e l'indirizzo IP.
In realtà, questi record, come si vedrà in seguito, possono contenere altri dati oltre all'indirizzo IP.

Name	Type	Class	TTL	RDLength	RData

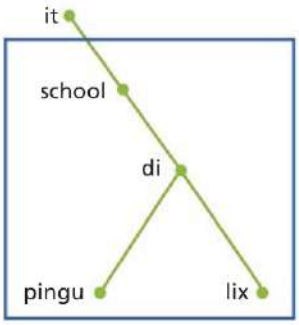
FIGURA 15 Tracciato di un Resource Record

La FIGURA 15 mostra il formato di un Resource Record, definito in RFC 1035, in cui:

- **Name** (DN, Domain Name) è il nome del dominio a cui il record appartiene;
- **Type** identifica il tipo di informazione contenuta nel campo RData;
- **Class** indica se le informazioni del record fanno riferimento a Internet o ad altro. La classe Internet è indicata con IN;
- **TTL** (Time To Live) indica la stabilità del record; più il valore è alto, più il record è stabile e sarà memorizzato nella cache del DNS. Un valore zero indica che il RR non deve essere memorizzato nella cache (per esempio i RR SOA sono sempre distribuiti con TTL = 0);
- **RDLength** specifica la lunghezza in ottetti del campo RData;
- **RData** è il valore restituito dal DNS, può contenere un numero, una stringa ASCII o un nome di dominio, dipende da quanto scritto nel campo Type.

Alcuni tipi di Resource Record sono diventati obsoleti, elenchiamo quindi di seguito solo quelli attualmente utilizzati.
Per gli esempi riportati in ogni voce dell'elenco, si fa riferimento alla parte di albero evidenziata in FIGURA 16 dove, con nomi del tutto inventati, il Domain Name è una macchina (chiamata pingu) del dipartimento di informatica (di) di una scuola (school) che si trova in Italia (it).

FIGURA 16 Tracciato di un Resource Record



dominio school.it

Contenuto del campo Type (identifica il tipo di informazione contenuta nel campo RData):

- **A** (Address): indica che nel campo RData si trova l'indirizzo IPv4 dell'host, quindi un numero binario di 32 bit.
  Per esempio:

  ```
  pingu.di.school.it. A IN 86400 198.45.30.165
  ```

  indica che l'host con DN = pingu.di.school.it. ha indirizzo IP 198.45.30.165 e questa informazione è stabile (TTL = 86.400 secondi è un valore alto).
- **AAAA**: come A ma riferito a indirizzi IPv6; questo tipo è stato introdotto in seguito nell'RFC 1886.
- **CNAME** (Canonical NAME): indica un nome di dominio e viene tipicamente usato per definire degli *alias*.
  Per esempio:

  ```
  www.di.school.it. CNAME IN pingu.di.school.it.
  ```

  definisce www.di.school.it. come un alias per l'host il cui nome canonico (cioè standard) è pingu.di.school.it. Quindi se in futuro l'host pingu verrà cambiato e il nome di dominio del nuovo web server sarà lix.di.school.it., si modificherà l'informazione nel Resource Record, ma non sarà necessario cambiare anche l'indirizzo web usato dagli utenti.
- **MX** (Mail eXchange): specifica una lista di server di posta elettronica ai quali inviare le e-mail destinate a uno specifico nome di dominio; nel campo RData si troverà il nome del dominio che accetta la posta per conto del dominio indicato nel campo Name.
  Per esempio:

  ```
  pingu.di.school.it. MX 1 IN istruzione.it.
  pingu.di.school.it. MX 2 IN education.it.
  ```

  Supponiamo che l'host pingu non sia inserito in Internet. Non può quindi ricevere la posta elettronica, e il Resource Record a lui associato indica che le e-mail destinate a pingu devono essere inviate ad altri domini che poi le ritrasmetteranno a pingu secondo gli accordi presi (per esempio via rete mobile). Nell'esempio, la posta viene inviata prima a istruzione.it. (il numero 1 indica la prima scelta) e nel caso questo server non sia in grado di riceverla, deve essere inviata a education.it. (numero 2).
- **NS** (Name Server): è l'authoritative Name Server per il dominio specificato. I Name Server usano i Resource Record di tipo NS per trovarsi l'un l'altro.
  Per esempio:

  ```
  di.school.it. NS IN name1.di.school.it.
  ```

  indica che il dominio di.school.it. ha come Name Server name1.di.school.it.

Si deve avere un NS record per ogni Name Server (primario o secondario) di un dominio.

- **PTR** (PoinTerR): è un puntatore a un'altra parte dello spazio dei nomi, ed è utilizzato soprattutto per associare un nome di dominio a un indirizzo IP nel dominio in-addr.arpa per la *risoluzione inversa* (trattata nelle pagine successive). Ci deve essere un solo PTR record per ciascun indirizzo IP.
  Per esempio:

```
165.30.45.198.in-addr.arpa. PTR IN pingu.di.school.it.
```

  indica che l'indirizzo IP = 198.45.30.165 appartiene all'host: pingu.di.school.it.
- **TXT** (TeXT): consente di associare un testo a un nome di dominio. Si possono avere più record TXT associati a un singolo Name.
  Per esempio:

```
pingu.di.school.it.
TXT IN "Server Linux del Dipartimento di Informatica"
TXT IN "Amministratore: marcot@di.school.it"
```

- **SOA** (Start Of Authority): fornisce il nome della fonte principale di informazioni sulla zona del Name Server. Esso contiene la versione attuale del database DNS, l'indirizzo di posta elettronica dell'amministratore e altri parametri. Questo record deve essere obbligatoriamente presente nel livello più alto del dominio e deve essere unico per ogni Name Server (o, meglio, per ogni zona a cui appartiene il Name Server).

6.4 Come funziona il DNS?

L'albero gerarchico del DNS è implementato mediante una **base di dati distribuita** in cui sono memorizzati i Resource Record. Il fatto che sia distribuita garantisce il funzionamento continuo della rete: se tutte le informazioni fossero memorizzate su un unico server e questo si guastasse, si fermerebbe tutta la rete Internet. Non solo, questo server sarebbe così sovraccarico per tutte le richieste da soddisfare da non essere in pratica utilizzabile.

> Quindi la soluzione è stata di suddividere lo spazio dei nomi del DNS in zone disgiunte, ognuna con un Name Server **principale** (**DNS primario**) e dei Name Server **secondari** (**DNS secondario**) che attingono al principale per avere le informazioni.

I client che accedono ai Name Server sono i **resolver**: quando un'applicazione necessita di informazioni dal DNS usa questa libreria per effettuare le interrogazioni (query). Se il Resource Record è authoritative per la zona richiesta, il server DNS risponderà direttamente in quanto dispone dell'informazione, mentre in caso contrario effettuerà una ricerca all'interno dello spazio dei nomi per trovare i dati richiesti.

Questo processo si chiama **risoluzione dei nomi**.
Ci sono due tipi di query DNS:

- **iterative**: richiedono a un server DNS la miglior risposta che già conosce;
- **ricorsive**: chiedono al server DNS di rispondere alla query in modo completo.

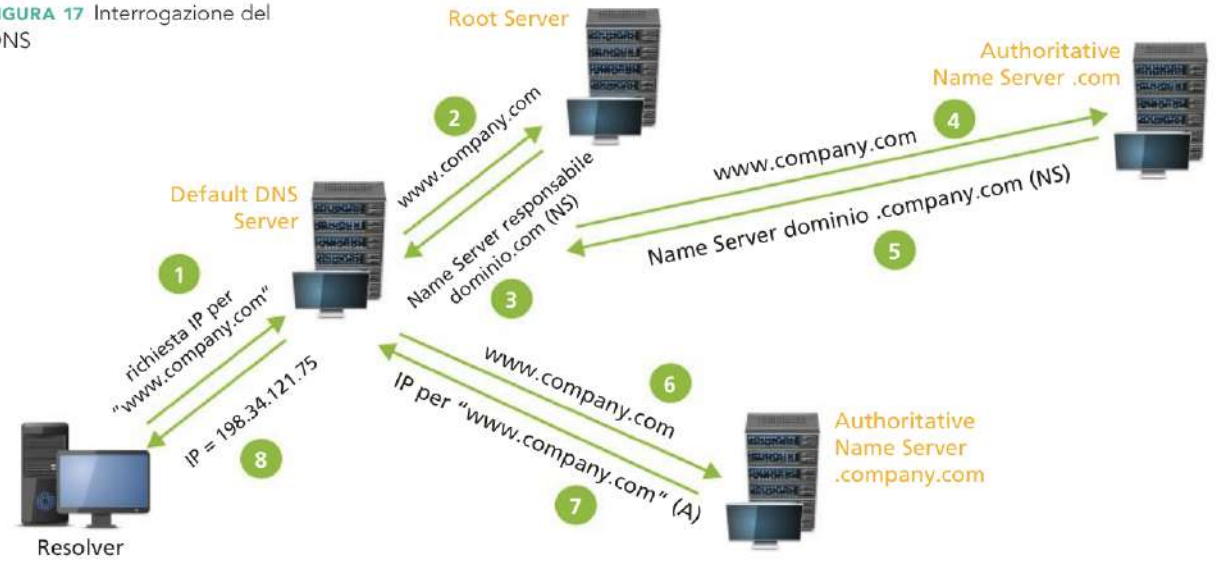
Di regola i resolver effettuano query ricorsive, lasciando così al Name Server il compito di risolvere il nome. I Name Server invece solitamente effettuano query iterative, seguendo via via i rimandi, finché non trovano la risposta.

Infatti un Name Server può inviare una query ricorsiva a un altro Name Server, ma spesso questi la rifiuta per evitare di essere sovraccaricato. Quando si verifica questa situazione, l'interrogazione diventa iterativa senza che l'utente finale se ne accorga.

esempio

In FIGURA 17 è illustrato il meccanismo di interrogazione del DNS nel caso di un utente che scrive l'indirizzo mnemonico del sito: *www.company.com*, nella barra degli indirizzi del browser.

FIGURA 17 Interrogazione del DNS



1) Il computer Resolver chiede al Default DNS Server di risolvere il nome fornito, inviando un messaggio DNS request con il tipo di richiesta (A) e la classe (IN) per ottenere così il corrispondente indirizzo IP, che successivamente sarà utilizzato per stabilire la connessione con la macchina remota che ospita il web server. Il Default DNS Server solitamente è il server del provider che fornisce la connessione a Internet, ma potrebbe anche essere un server DNS interno alla LAN se il computer è connesso a una rete locale. Il suo indirizzo IP si trova nel file di configurazione del protocollo TCP/IP sul computer.
2) Il Default DNS Server verifica prima di tutto se possiede l'indirizzo IP corrispondente al nome da risolvere. Potrebbe, infatti, essere in grado di risolvere autonomamente quel nome, perché ha nella cache le informazioni relative oppure perché tale nome è già stato risolto in precedenza. In caso contrario, esso interroga uno dei root server, dando inizio al processo di ricerca delle informazioni all'interno della gerarchia dei Domain Name. Le interrogazioni DNS request avvengono utilizzando un datagram UDP.
3) Il Root Server risponde con l'indicazione del server responsabile per lo spazio dei nomi .com.
4) Così il Default DNS Server può inoltrare la stessa richiesta all'authoritative Name Server di .com, il quale non è in grado di risolvere completamente il nome www.company.com, ma conosce il server che lo può fare (ossia il Name Server responsabile per la zona company.com).
5) Il Name Server del dominio .com invia al Default DNS Server l'indirizzo dell'authoritative Name Server della zona .company.com.

6) Il Default DNS Server invia la richiesta di risoluzione del nome all'indirizzo appena trovato del Name Server della zona company.com.
7) Il Name Server riconosce il nome www come facente parte della zona company.com e restituisce al Default DNS Server l'indirizzo IP corrispondente.
8) Con il messaggio DNS reply del Default DNS Server, il computer ottiene l'indirizzo IP.

Una volta ottenuto l'indirizzo IP del web server, il computer può inviargli la richiesta della pagina web con un messaggio di get che verrà instradato nella rete e, arrivato a destinazione, verrà letto dal server web. Questi risponderà inviando la pagina desiderata.

Alcune considerazioni:

- un Name Server intermedio potrebbe anche avere già soddisfatto una simile richiesta e memorizzato nella **cache** una copia della risposta. In questo caso il Name Server fornisce una risposta dichiarandola di tipo *non authoritative*. Questo tipo di risposta non è del tutto affidabile poiché se nel frattempo fossero intervenute delle modifiche, queste non verrebbero propagate agli altri Name Server che quindi manterrebbero nella loro cache il dato precedente, non più corretto. Di qui l'importanza del campo TTL (Time To Live) del Resource Record che sta a indicare la stabilità dell'informazione. Per esempio un hostname con un TTL molto alto indica che quell'host ha lo stesso indirizzo IP da molto tempo e quindi anche se l'informazione non è authoritative ha un'alta probabilità di essere corretta;
- ogni Name Server che ha autorità su un dominio è duplicato per motivi di affidabilità; si ha quindi un Name Server **primario** e un Name Server **secondario** che devono essere periodicamente sincronizzati così da avere le stesse informazioni memorizzate in entrambi. Per effettuare questo allineamento si usa una connessione TCP che consente di trasferire in modo affidabile notevoli quantità di dati (invece di usare UDP come nelle interrogazioni). Quindi di norma il Name Server è in ascolto sulla porta **53 TCP** e sulla porta **53 UDP**.

6.5 La risoluzione inversa

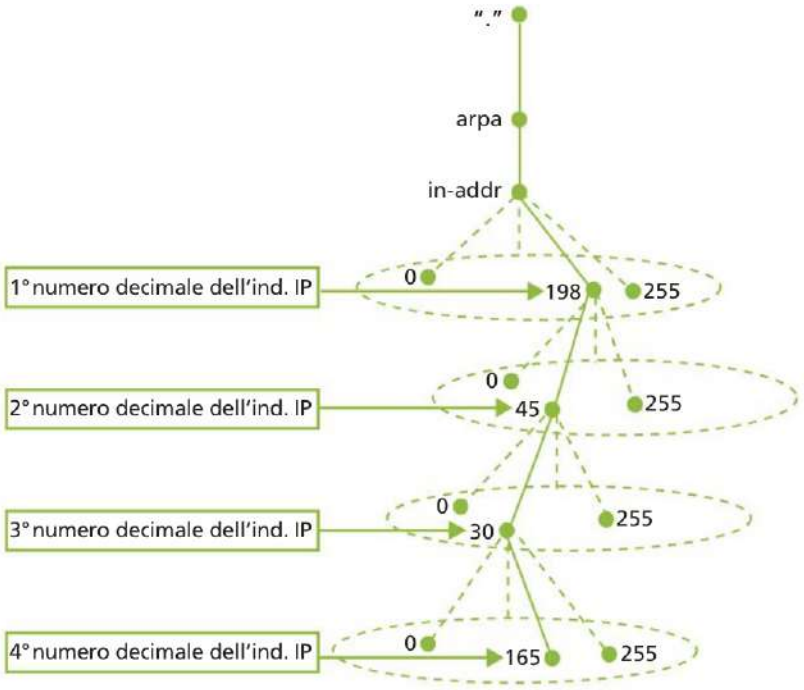
Quanto descritto nell'esempio precedente è il tipico **processo di risoluzione dei nomi**: dato un nome si deve trovare il corrispondente indirizzo IP.

> Esiste anche la possibilità di associare a un indirizzo IP il nome corrispondente e questo processo viene chiamato **risoluzione inversa**.

Di risoluzione inversa abbiamo già scritto a proposito del Resource Record PTR: infatti questo tipo di RR è usato per memorizzare l'associazione tra IP address e name, partendo dalla conoscenza dell'indirizzo IP (al contrario, quindi, degli RR di tipo A usati per la risoluzione, più frequente, dei nomi in indirizzi IP).
Questa ricerca viene resa semplice dal fatto che è stato creato un apposito dominio ***in-addr.arpa*** che usa la rappresentazione numerica degli indirizzi IP come etichette dei nodi (cioè come *name*). Questo speciale dominio può avere fino a 256 sottodomini di terzo livello (numerati da 0 a 255) corrispondenti ai possibili valori del primo

byte di un indirizzo IP; ognuno di questi a sua volta può avere fino a 256 sottodomini di quarto livello, anch'essi numerati da 0 a 255, che corrispondono ai possibili valori del secondo byte, e così via.
Quindi per risolvere un indirizzo IP richiesto, il resolver deve semplicemente chiedere al Name Server il Resource Record di tipo PTR del nodo corrispondente nel dominio *in-addr.arpa*. Per esempio, per ottenere il nome di dominio associato all'indirizzo IP 198.45.30.165, il resolver richiederà al DNS il Resource Record PTR del nome di dominio 165.30.45.198.in-addr.arpa (FIGURA 18).

FIGURA 18 Risoluzione inversa



Come si può notare, nel dominio *in-addr.arpa* gli indirizzi IP sono al contrario, in conseguenza della differente interpretazione della posizione degli elementi negli indirizzi IP e nei nomi di dominio. Infatti gli indirizzi IP diventano più specifici da sinistra verso destra, mentre i nomi di dominio diventano più specifici da destra verso sinistra. Quindi chiamare i nodi del dominio *in-addr.arpa* in questo modo permette agli indirizzi IP di riflettere correttamente la struttura gerarchica del DNS.

FISSA LE CONOSCENZE

- Qual è l'ente preposto alla gestione del DNS?
- Perché il database del DNS è distribuito?
- Descrivi il formato dei messaggi scambiati tra DNS Client e DNS Server.
- In quale struttura vengono mantenute le informazioni sui nomi di dominio?
- Sia l'RR di tipo A sia l'RR di tipo PTR contengono l'associazione tra un indirizzo IP e un nome; in che cosa, però, differiscono?
- Come è da interpretare una risposta di tipo non authoritative?

7 PROBLEMATICHE DI SICUREZZA

7.1 La non sicurezza di DHCP e DNS

Il **DHCP** utilizza i protocolli UDP e IP che sono intrinsecamente insicuri e nelle sue specifiche non si fa riferimento a possibili misure per la sicurezza.

Se ai tempi in cui è stato standardizzato questo protocollo il numero di utenti di Internet era limitato e si trattava per lo più di enti accademici e di ricerca, attualmente le problematiche di sicurezza sono di centrale importanza, soprattutto per un protocollo come DHCP che tratta informazioni di configurazione.

In particolare, ne individuiamo due derivanti da:

- **DHCP Server non autorizzati**: un DHCP Server abusivo potrebbe inserirsi e rispondere alle richieste del client fornendo informazioni false in modo da inibire gli host, oppure configurandoli per azioni fraudolente;
- **DHCP Client non autorizzati**: un host potrebbe ottenere le informazioni di configurazione destinate a un certo client con lo scopo di creare danni alla rete, oppure potrebbe usare un software che genera moltissime richieste DHCP così da esaurire gli indirizzi a disposizione del server e bloccare nuovi accessi alla rete.

Un modo per ovviare a questi inconvenienti è introdurre meccanismi di sicurezza nei livelli più bassi, per esempio evitando che un device non autorizzato possa inserirsi fisicamente nella rete.
Inoltre, si potrebbe usare **IPsec** per rendere sicuro il livello Network.

#prendinota

IP security protocol (IPsec) protegge i pacchetti IP scambiati tra host e router a livello Network, garantendone la confidenzialità.
Inoltre, offre i servizi di autenticazione del mittente e di integrità dei dati.

Il **DNS** è particolarmente critico dal punto di vista della sicurezza per vari motivi:

- non è autenticato: l'informazione richiesta potrebbe arrivare non dal DNS Server corretto ma da un'altra macchina;
- è molto lento, quindi è possibile che qualcuno intercetti la richiesta destinata a un DNS Server e risponda al suo posto (spoofing);
- il protocollo non offre meccanismi per proteggere l'integrità delle informazioni distribuite (basti pensare all'associazione tra hostname e indirizzo IP).

In passato si sono avuti casi di **DNS cache poisoning** volti a manomettere le informazioni contenute nei DNS Server, compromettendo la coerenza e l'integrità dei suoi dati.

IN ENGLISH PLEASE

DNS cache poisoning (or DNS spoofing) is a form of computer security hacking in which corrupt DNS data is introduced into the DNS resolver's cache, causing the Name Server to return an incorrect IP address. This results in traffic being diverted to another computer.

Nella precedente Lezione si è visto come un DNS Server mantenga in una memoria cache anche informazioni relative a domini non di sua competenza. Una risposta fornita sulla base di questi dati è detta **non authoritative** e il valore del campo TTL indica quanto sia attendibile (più è alto il TTL più è alta la probabilità che il dato sia corretto). Un attacco di tipo **cache poisoning** a un DNS Server comporta la modifica dei dati della sua cache, inserendovi un valore di TTL molto alto, così da rendere attendibile l'informazione modificata. Tipicamente, l'intervento consiste nell'associare a un nome l'indirizzo IP di un server malevolo. Per esempio, un utente scrive nel browser l'URL di un sito web ma viene poi direzionato, a sua insaputa, verso un sito clone costruito per effettuare furti di identità o di dati bancari. Questo succede perché nella cache del DNS Server l'indirizzo IP originale, associato a quel nome, è stato sostituito con quello del web server malevolo.

Per rimediare alle mancanze del protocollo originario in termini di sicurezza, in ambito IETF è stato creato un gruppo di lavoro che ha definito un'estensione al DNS denominata **DNSSEC** (Domain Name System Security Extensions).
Il compito di DNSSEC è di garantire all'utente che il sito web che sta visitando è quello originale e non una copia creata per scopi fraudolenti. A tal scopo si usano delle chiavi crittografiche per autenticare i dati nel DNS, a partire dalla root. Le chiavi per la root sono gestite da ICANN, l'ente responsabile dei Domain Name di primo livello (generici e nazionali).
Proprio per il ruolo particolarmente critico che il DNS riveste nell'attuale scenario di Internet, l'ICANN ha evidenziato la necessità di stabilire metriche e modalità per il controllo del DNS, individuando 5 indicatori importanti: **coerenza**, **integrità**, **velocità**, **disponibilità** e **robustezza**.

7.2 La protezione dei client nelle reti Microsoft

In una rete interna Microsoft, un client può ottenere indirizzi IP differenti ogni volta che viene acceso, poiché utilizza il protocollo di configurazione dinamica DHCP. Di conseguenza la configurazione dei **Resource Record DNS** è automatica.
Tipicamente i PC con versioni recenti di Windows sono in grado di gestire l'aggiornamento dinamico del record DNS: quando ottengono un indirizzo IP dal DHCP Server, inviano la richiesta di aggiornamento del record A relativo al client.
La FIGURA 19 descrive le due fasi di aggiornamento dinamico del record DNS:

1. quando il computer viene acceso, lo scambio di messaggi con il DHCP Server fornisce indirizzo IP e altre informazioni di configurazione di TCP/IP (default gateway e indirizzo del DNS Server);
2. il client comunica con il DNS Server per creare un nuovo **record A** relativo all'hostname del computer e al suo indirizzo IP.

FIGURA 19 Processo di aggiornamento dinamico del record A di un client Windows

Quando il client tenta di registrare un record A e scopre che ne esiste già uno con lo stesso nome, ma indirizzo IP diverso, per default tenta di sostituirlo con quello nuovo. In questo modo, però, un qualunque computer della rete potrebbe modificare un record A sul DNS Server.
Il processo appena descritto può essere reso sicuro con due diversi procedimenti: **autenticazione del client** oppure **assegnazione dei permessi in base alle zone DNS**.
Le zone che sono configurate per aggiornamenti dinamici sicuri permettono solo ai client autorizzati di modificare i Resource Record.
Di norma, sono gestiti nel seguente modo: dapprima il DNS Client cerca di usare la modalità dinamica non sicura e se viene rifiutata dal server passa allora a usare la modalità sicura. Quando poi una zona è integrata in Active Directory, il DNS Server (configurato su Windows Server) per default consente solo aggiornamenti dinamici sicuri. La configurazione degli aggiornamenti dinamici sicuri richiede quindi l'impostazione di alcuni parametri sul DNS Server. In particolare, Microsoft raccomanda che esso venga installato su un **Domain Controller** e che le zone siano integrate in **Active Directory** (servizi che affronteremo nel quinto anno).

#prendinota

In alcuni ambiti di rete che richiedono un livello di sicurezza molto elevato può non essere sufficiente l'autenticazione del DNS Client per creare o modificare un record DNS. In questi casi una soluzione è la definizione di Access Control List (che verranno trattate nel corso del quinto anno) per definire i permessi degli utenti.

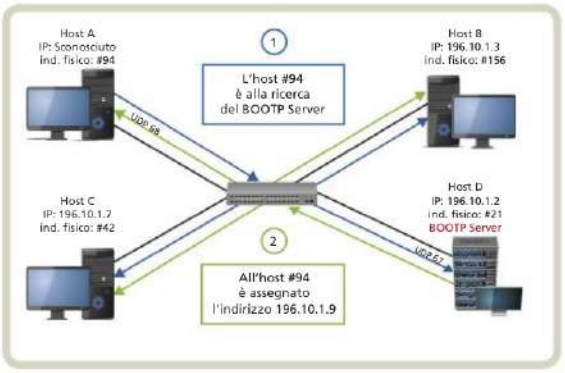
FISSA LE CONOSCENZE

- Descrivi come DHCP Server non autorizzati e DHCP Client non autorizzati possono creare problemi di funzionamento della rete.
- Spiega in che cosa consiste il DNS cache poisoning.
- Come può essere reso sicuro l'aggiornamento del DNS?

RIPASSIAMO INSIEME

1 La configurazione degli host

Per configurare in modo automatico gli host di una rete TCP/IP sono stati definiti in ambito IETF alcuni protocolli. Uno dei primi è stato BOOTP (BOOTstrap Protocol), che mette in comunicazione un computer privo di disco e un secondo host che gli fornisce le informazioni di rete. Poiché BOOTP poteva convogliare altre informazioni di configurazione, gli amministratori lo usavano anche per inviare un'installazione client preconfigurata ai computer nuovi da inserire nella rete aziendale.



2 Il DHCP (Dynamic Host Configuration Protocol)

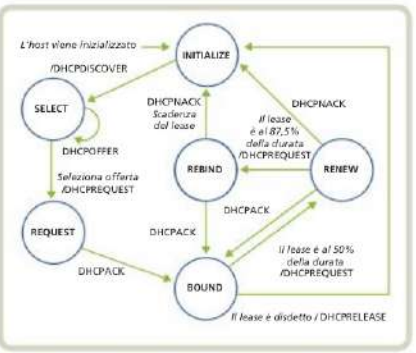
Quando nelle reti si diffusero i dispositivi mobili, BOOTP risultò troppo lento nell'aggiornare quei dispositivi che si spostavano da una rete a un'altra. Fu perciò necessario introdurre una nuova modalità di assegnazione dinamica, che consentisse di allocare velocemente gli indirizzi per un tempo limitato.

Il protocollo DHCP, evoluzione di BOOTP, soddisfa le esigenze di mobilità con l'assegnazione dinamica degli IP. Esso si basa sul concetto di lease, cioè affitto, degli indirizzi per un tempo limitato.

3 L'architettura Client/Server DHCP

Il DHCP Server utilizza un database nel quale sono memorizzati gli indirizzi IP a sua disposizione per l'allocazione ai DHCP Client presenti nella rete. DHCP usa il MAC address e il network address per identificare l'host. Quindi consulta il database e stabilisce se assegnare all'host un indirizzo IP permanente o temporaneo. Ogni volta che un host si connette a una rete, il suo DHCP Client richiede un indirizzo IP al DHCP Server, che lo sceglierà, in modo arbitrario, tra quelli disponibili nel suo address pool. Quando l'host lascerà la rete, il suo indirizzo ritornerà disponibile nel pool.

Quando un DHCP Server è responsabile dell'indirizzamento su una subnet diversa dalla propria è necessario introdurre un relay agent.



4 La comunicazione tra DHCP Client e DHCP Server

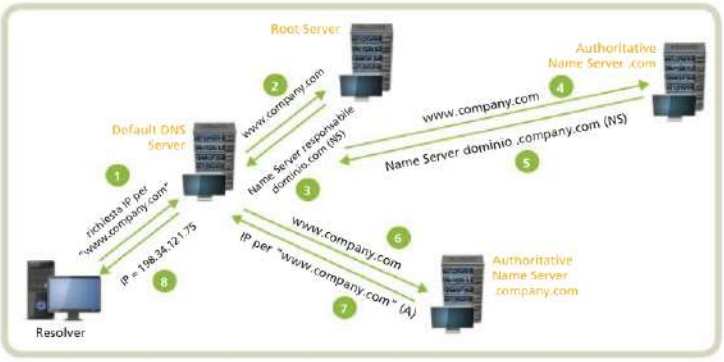
I messaggi scambiati tra DHCP Client e Server sono di tipo request/reply. Il processo di assegnazione di un indirizzo IP avviene in 4 fasi. Il DHCP Client può trovarsi in 6 stati.

DIDATTICA INCLUSIVA

5 Il DHCP per IPv6

A seguito della release di IPv6, il protocollo DHCP è stato aggiornato nella versione DHCPv6. Le configurazioni degli host IPv6 sono: stateless autoconfiguration e stateful autoconfiguration. DHCPv6 modalità *stateful* è usato per avere un controllo centralizzato degli host della rete, quindi nelle reti aziendali, mentre il metodo *stateless* è preferibile dove non c'è una gestione centrale, per esempio nelle reti domestiche.

6 Il DNS (Domain Name System)



Il Domain Name System (DNS) è un database distribuito usato dagli applicativi TCP/IP per il mapping dei nomi degli host e dei loro indirizzi IP. Gli applicativi accedono al DNS tramite un resolver che è un insieme di funzioni da usare per contattare il Name Server DNS. Il sistema DNS è usato anche all'interno delle reti locali private per risolvere i nomi dei computer (hostname). Infatti, grazie al DNS, si possono associare alle macchine dei nomi facili da ricordare; gli utenti possono connettersi ai server locali usando le stesse convenzioni usate su Internet (URL).

7 Problematiche di sicurezza

I problemi di sicurezza riguardano DHCP Server e Client non autorizzati. La vulnerabilità del DNS è data dal fatto che non è autenticato e che non è garantita l'integrità delle informazioni nei database distribuiti. Per il ruolo critico che il DNS riveste nello scenario di Internet, l'ICANN ha stabilito metriche e modalità per il controllo del DNS, individuando 5 indicatori importanti: coerenza, integrità, velocità, disponibilità e robustezza.

8 Il comando nslookup

Il comando nslookup è usato per interrogare il DNS. Si possono richiedere: la risoluzione di un nome o di un indirizzo IP, specifici Resource Record e di visionare il contenuto della memoria di un Name Server. Nslookup si può usare nella modalità interattiva e in quella non interattiva. Nella modalità interattiva si possono inviare più query e visualizzarne i singoli risultati, digitando solo nslookup senza opzioni. Nella modalità non interattiva si può inviare una sola query e visualizzarne il risultato. Di norma si usa quando si vuol interrogare un solo host e quindi si digita il nome dell'host dopo aver scritto nslookup.