UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE ED INFORMATICHE
Corso di Laurea in Informatica

Il Livello Applicativo – Parte A

Applicativi UDP: TFTP e DNS

RETI DI CALCOLATORI - a.a. 2023/2024

Roberto Alfieri

Livello Applicativo: sommario

PARTE A

- Applicativi UDP: TFTP e DNS

PARTE B

- I servizi di posta elettronica: SMTP, POP e IMAP.

PARTE C

- Il World Wide Web

PARTE D

- Multimedia

TFTP e FTP

TFTP è la versione semplificata (Trivial) di FTP (File Transfer Protocol)
http://openskill.info/topic.php?ID=87
Per noi è interessante perché è un esempio di come viene gestito a livello applicativo il controllo del flusso.

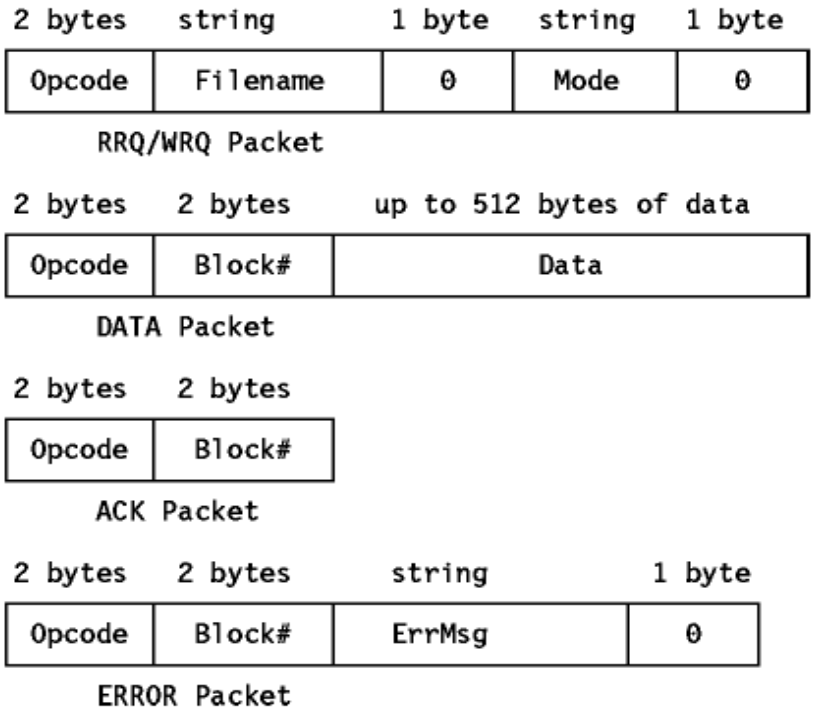
Il protocollo FTP *(RFC 959) è stato sviluppato per trasferimento affidabile ed efficiente dei dati, per questo motivo si basa TCP. Il server FTP offre anche un servizio di autenticazione per l'accesso al file-system, la gestione delle directory (navigazione, creazione, cancellazione) e dei file.*
Altra caratteristica peculiare è quella di usare due porte: la TCP/21 (comandi) e la TCP/20 (dati).
Le modalità di funzionamento sono due: attiva e passiva.
*Nella **modalità attiva** il client apre il canale comandi verso il server (porta 21 del server), mentre per la trasmissione dati il client svolge la funzione di server, ovvero rimane in ascolto sulla porta > 1024 mentre il server si comporta da client utilizzando la porta 20.*
In genere le politiche di sicurezza impediscono l'accesso alle porte dei client bloccando questa modalità.
*Nella **modalità passiva** il server indica al client la porta > 1024 da utilizzare per il trasferimento dei dati.*

TFTP non supporta l'autenticazione e utilizza UDP, con il server in ascolto sulla porta 69. Questo significa che la gestione del flusso (numerazione dei pacchetti, Ack, gestione degli errori) viene realizzata a livello applicativo, all'interno di TFTP.

Il protocollo TFTP

Ogni trasferimento inizia con una richiesta di read (comando get) o write (comando put) .
GET: Il server risponde con un file frammentato in datagrammi numerati.
Ogni datagramma deve essere riscontrato.
Il block-size di default è di 512 byte
Un pacchetto di dimensione inferiore rappresenta l'ultimo pacchetto trasmesso

Opcode (16 bit)
1 RRQ (Read Request)
2 WRQ (Write Request)
3 DATA
4 ACK
5 ERROR

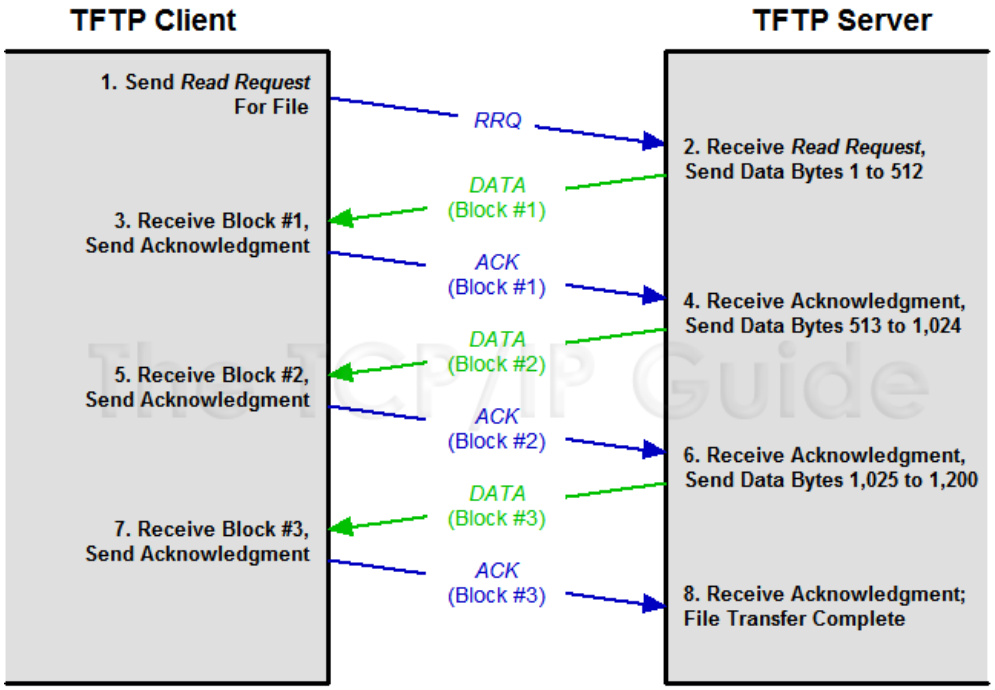


Le fasi di una sessione TFTP

- Il client contatta il server inviando un pacchetto di tipo RRQ o WRQ
- Il server risponde inviando/ricevendo pacchetti DATA di 512 byte.

Per ogni DATA inviato/ricevuto viene inviato/ricevuto un ACK (o un ERROR)

- I pacchetti vengono trasferiti finché la loro lunghezza non è inferiore a 512 byte;
- Termine della connessione;



Esempi:

```
> tftp -v <nome server>  -c put /etc/hosts hosts
> tftp -v <nome server>  -c get  hosts
```

DNS: Domain Name System

DNS è il protocollo applicativo più importante tra quelli che si appoggiano su UDP.

Scopo del sistema DNS:

- gestire uno spazio univoco dei nomi per i nodi della rete
- Fornire agli utenti di IP un servizio per la traduzione nome-numero e numero-nome

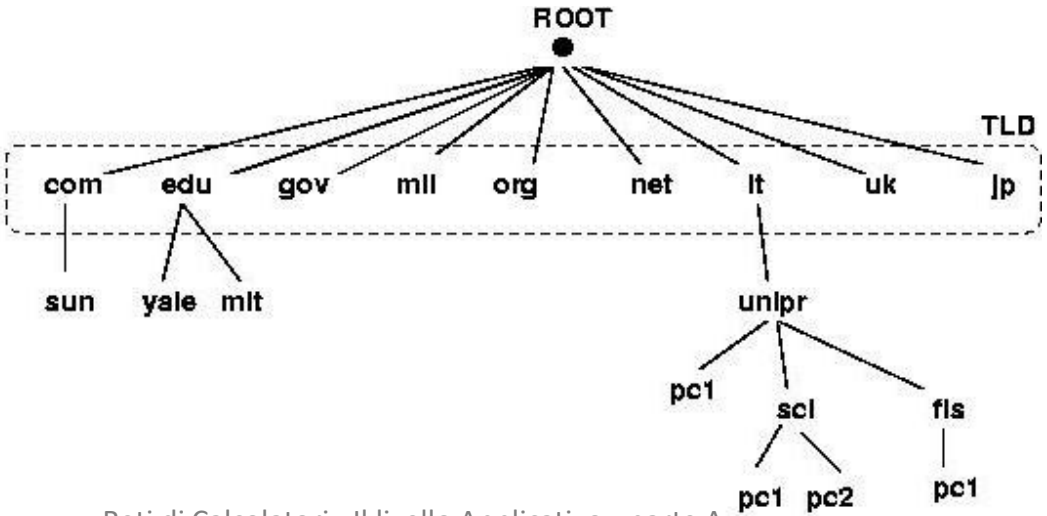
Lo spazio dei nomi è strutturato in modo gerarchico, come il file-system, ma la radice è a destra. *Esempio: didattica-linux.unipr.it.*
Il primo elemento è il nome locale del nodo, mentre gli elementi successivi (domini) rappresentano il percorso nella gerarchia e sono separati da punto ('.').

Un nome completo termina sempre con un punto, che rappresenta la radice della gerarchia.
Il dominio più a destra (**it** nell'esempio) è detto Top Level Domain (TLD).
I TLD sono gestiti dall'organismo internazionale ICANN (attraverso la sua emanazione IANA) che li assegna alle organizzazioni che ne fanno richiesta, mentre i livelli successivi sono gestiti in modo autonomo dalle organizzazioni assegnatarie.

DNS: i Top Level Domain

Inizialmente Internet era composta unicamente da nodi americani, per cui esistono alcuni TLD che rispecchiano la strutturazione Statunitense originale (1985):
com (commerciali), edu (istituzioni educative), gov (governo federale US), mil (forze armate US), net (provider di rete), org (organizzazioni no-profit).
Successivamente, con la diffusione di Internet, sono nati i TLD geografici nazionali:
it, es, fr, de, gr ca, at, au, be, nl, pt, ch, ecc
A partire dal 2000 ICANN ha approvato diversi nuovi nomi TLD generici quali:
biz (business), info (informazioni), name (nome di persona), pro (professionisti), coop (cooperative), museum (musei), travel (viaggi), aero (aerotrasporti)

Attualmente sono attivi seguenti TLD http://www.iana.org/domains/root/db/

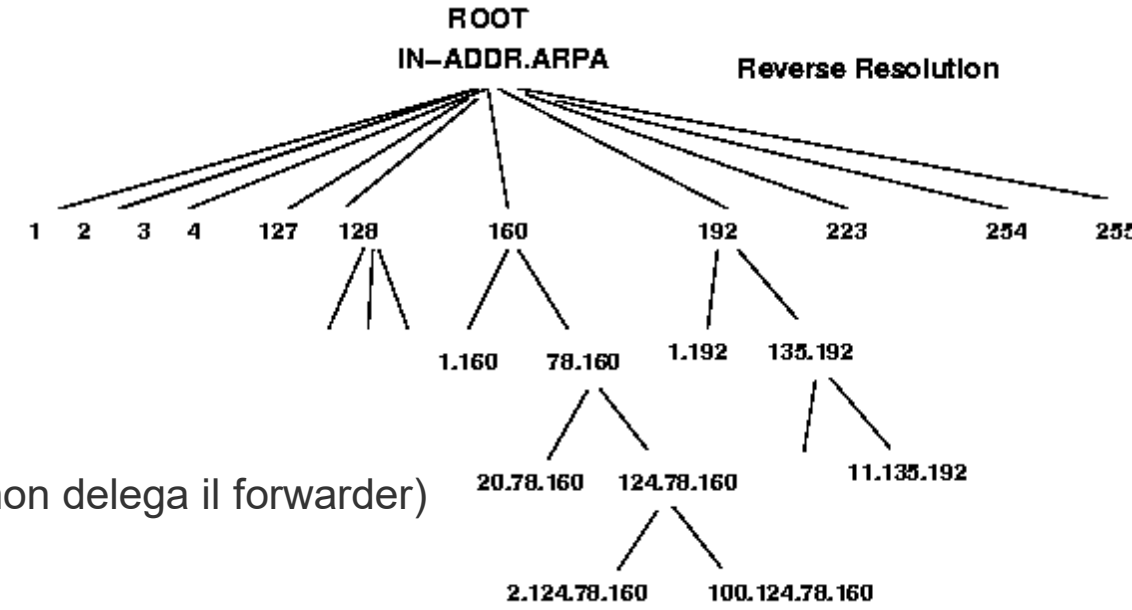


Risoluzione Inversa

La risoluzione inversa consiste nella risoluzione del nome a partire dall'indirizzo IP.
Viene usata ad esempio per produrre un output leggibile nei file di log, oppure per controlli di autenticazione (e.g. richiedere che il client sia registrato)
Il nome dei domini di Reverse è composto dai numeri della rete (in ordine rovesciato), seguiti dalla stringa "in-addr.arpa" (TLD per la risoluzione inversa).
Il rovesciamento del numero consente di ricercare i numeri nello stesso albero dei nomi, utilizzando lo stesso procedimento di parsing da destra verso sinistra.

Ad esempio:
10.48.78.160.in-addr.arpa
è il nome di
caio.cce.unipr.it
nel ramo della risoluzione inversa.

provare il comando:
dig PTR 10.48.78.160.in-addr.arpa
dig -x 160.78.48.10
dig -x 160.78.48.10 +trace
-x → semplifica il reverse search
+trace → dig esegue query iterative (non delega il forwarder)



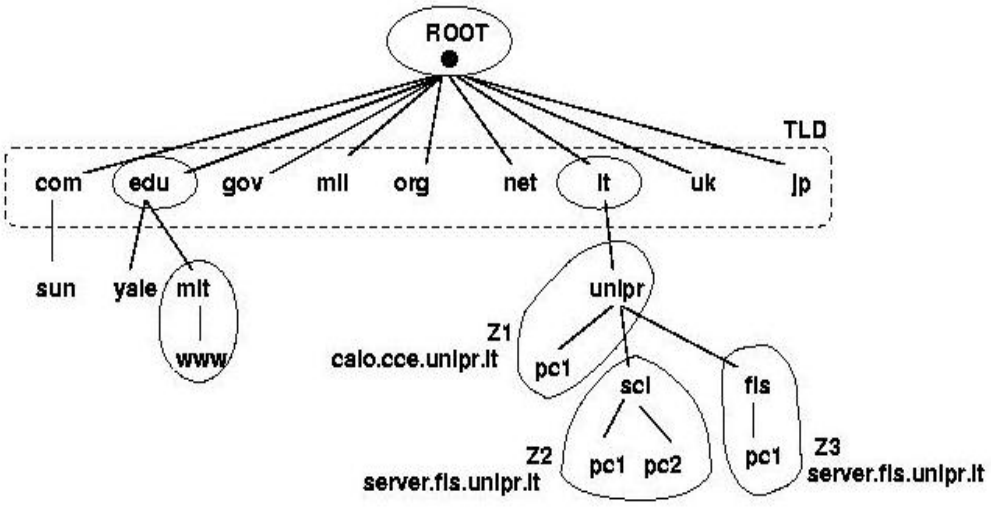
DNS client

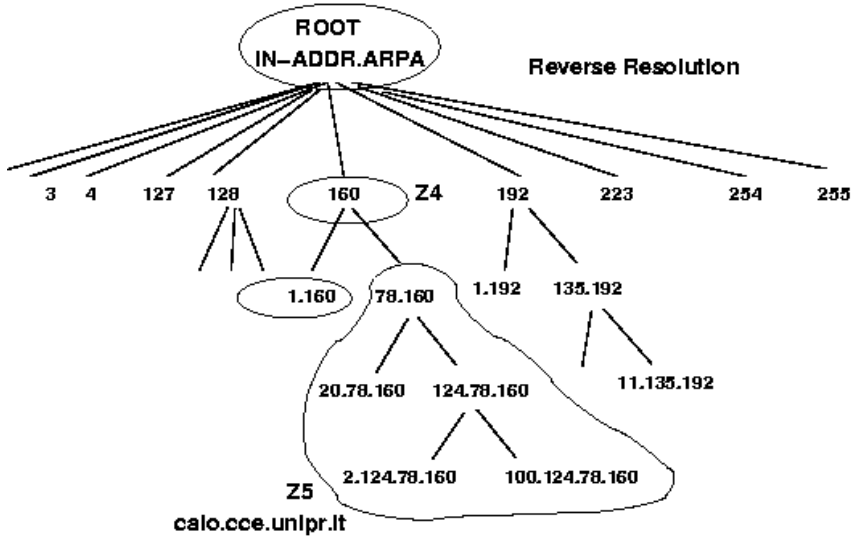
Un DNS client contiene un componente software, detto Resolver, che ha il compito di risolvere la richiesta. Il Resolver deve essere configurato con l'indicazione di almeno un **server DNS forwarder** a cui rivolgersi per le risoluzioni.
Il server DNS forwarder recupera l'informazione (interagendo eventualmente con gli altri server DNS) e la comunica al Resolver.
Nei sistemi Linux questa configurazione viene stabilita nel file /etc/resolv.conf.
Esempio: nameserver 160.78.48.10
la configurazione del DNS può essere impostata dinamicamente dal protocollo DHCP assieme alle altre informazioni di configurazione (indirizzo IP, Gateway, netmask, ..)
Vista la criticità del servizio DNS un client dichiara tipicamente almeno 2 DNS Forwarder per ridondanza.
In un programma applicativo il ruolo di Resolver è svolto dalla funzione **gethostbyname().**

Esistono anche specifici client a linea di comando come **nslookup e dig**

Le Zone del DNS

I TLD possono creare sottodomini di livello 2, i quali a loro volta possono gestire domini di livello 3 e così via. *Ad esempio il dominio a.b.com. può creare c.a.b.com*
Lo spazio dei nomi è gestito in modo distribuito suddividendolo in “Zone”. Ogni Zona include una porzione dell'albero che gestisce in modo autonomo con un DNS server Primario e uno o più DNS server Secondari che ne replicano i dati (per sicurezza e prestazioni).
Una Zona si forma attraverso la delega che il server della Zona superiore assegna mediante il record NS
Ogni nuovo host viene inserito tipicamente sia nella zona per la risoluzione diretta che nella zona per la risoluzione inversa.





Il servizio DNS: il server

Il **servizio DNS** è definito dall'RFC1034 e RFC1035
BIND è il nome del demone DNS più comunemente usato sui sistemi Unix/Linux.

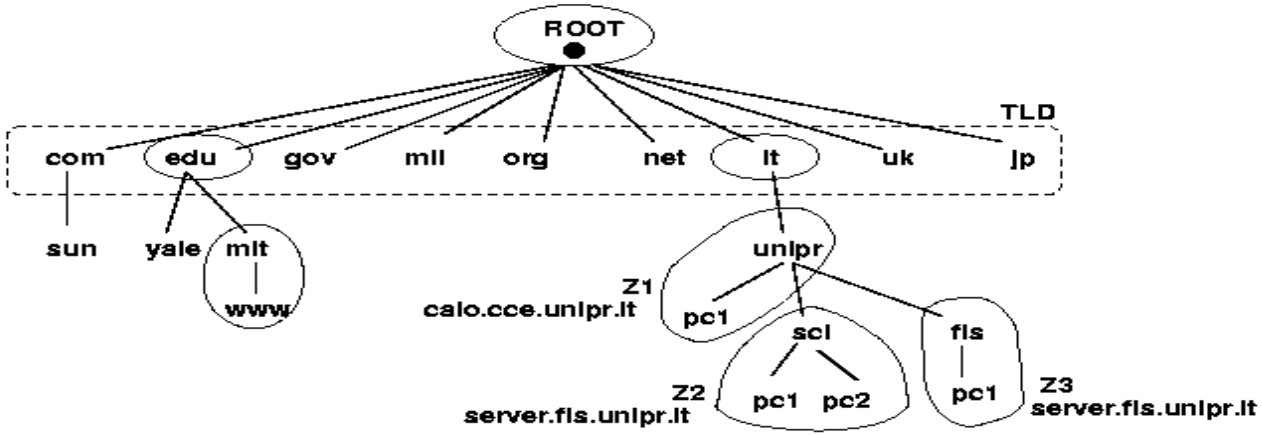
Un server può essere configurato per diversi tipi di funzionamento:

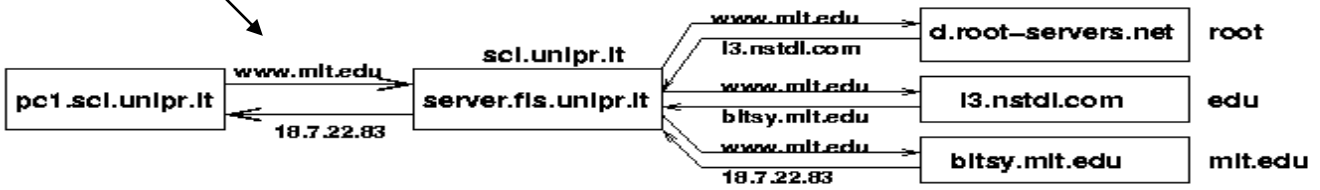
- **Server Autoritativo di Zona Primario o Secondario**
  - L'amministratore di Zona aggiorna i dati sul Primario.
  - I server Secondari si sincronizzano con il primario replicando tutta la Zona ("Zone Transfer") attraverso un Data-Pull sulla porta 53/TCP.
  - Risponde alle query che riceve (53/UDP).
  - Un server Autoritativo è generalmente anche Forwarder NS.
- **Server Forwarder (o Caching Name Server):**
  - Riceve query dai client (53/UDP)
  - Ottiene la risposta interrogando i Server Autoritativi
  - Mantiene copia locale in Cache delle risposte ottenute
  - Invia la risposta al client

La risoluzione Ricorsiva e Iterativa

Se il server che riceve a richiesta è autoritativo per il dato richiesto risponde direttamente, altrimenti occorre attraversare l'albero passando attraverso i server autoritativi coinvolti. L'attraversamento può essere ricorsivo o iterativo.
Modalità Ricorsiva: Se il server interrogato non è autoritativo per il dato richiesto, passa la richiesta al server successivo e così via in modo ricorsivo.
Modalità Iterativa: Il server restituisce al client l'indirizzo del server successivo. In questo modo è il DNS locale che contatta direttamente i server coinvolti.

Generalmente un server ammette query ricorsive solo per i client locali.

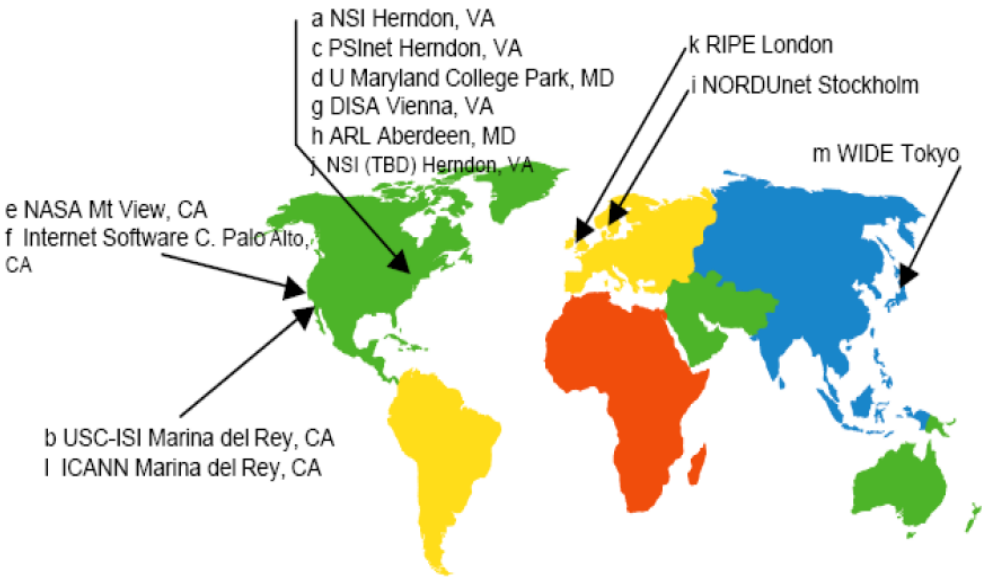




I Root Server

L'albero DNS possiede 13 **Root Server** che contengono le informazioni riguardo i domini di primo livello. Questi server vengono contattati ogni volta che un client chiede informazioni relative ad altri TLD, quindi ogni DNS Forwarder deve possedere una lista aggiornata dei Root Server (file named.ca di Bind).
I Root NS sono iterativi: se non hanno la risposta forniscono l'indirizzo del server del TLD da contattare.

A.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**198.41.0.4**
B.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.228.79.201**
C.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.33.4.12**
D.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**128.8.10.90**
E.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.203.230.10**
F.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.5.5.241**
G.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.112.36.4**
H.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**128.63.2.53**
I.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.36.148.17**
J.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**192.58.128.30**
K.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**193.0.14.129**
L.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**199.7.83.42**
M.ROOT-SERVERS.NET.	**3600000 IN**	**A**	**202.12.27.33**



Resource Record

Le informazioni relative alla zona vengono memorizzate come **Resource Record (RR)**.

Il formato generico di un RR dispone dei seguenti campi:

- **Nome**: Il nome di dominio a cui questo RR si riferisce.
- **TTL**: Tempo di vita del RR nella cache dei server DNS prima di essere scartato.
- **Classe**: Identifica la famiglia di protocollo. **IN** che indica il sistema Internet.
- **Tipo**: Il tipo di RR. I tipi principali sono:
  - ✓ **A**: Il più usato. Indica l'indirizzo IPv4 per il nome specificato.
  - ✓ **AAAA:** Indica l'indirizzo IPv6 (eventuale) associato al nome.
  - ✓ **CNAME:** Record Canonical Name, usato per indicare un nome di alias.
  - ✓ **MX**: Mail eXchanger, indica un host che gestisce la posta per il dominio.
  - ✓ **NS:** Un server DNS per il dominio specificato.
  - ✓ **PTR:** Usato nella risoluzione inversa per associare un indirizzo IP al nome.
  - ✓ **SOA:** Start of Authority, un RR che indica il server DNS dove risiedono i dati autoritativi per questo dominio ed alcuni dati amministrativi.

Esempio di Record

```
; Authoritative data for unipr.it. (Zone1)
;nome          classe    tipo      valore                    (serial  refresh retry expire min_life)
unipr.it            IN        SOA     caio.cce.unipr.it  manager  (20050818 8H  2H  1W  1D)
unipr.it            IN        TXT       “Univ Parma”
unipr.it            IN        MX        1          mail.unipr.it.
unipr.it            IN        MX        2          mail2.unipr.it.
fis                 IN        NS        server.fis.unipr.it.   ; Zone 2

dns                 IN        CNAME     server1.unipr.it.
mail                IN        CNAME     server2.unipr.it.
mail2               IN        CNAME     server1.unipr.it.
pop                 IN        CNAME     server2.unipr.it.
www                 IN        CNAME     server1.unipr.it.

server1             IN        A         160.78.124.1
                    IN        HINFO     Server1 Linux

server2             IN        A         160.78.124.2
                    IN        HINFO     Server2 Linux

pc1                 IN        A         160.78.124.101
                    IN        HINFO     Client1 Win2000

pc2                 IN        A         160.78.124.102
                    IN        HINFO     Client2 Win2000
```

DNS e la Posta elettronica

Per ogni dominio che è in grado di ricevere posta il DNS fornisce una lista di server SMTP a cui inviare il messaggio.
In questo modo, se il mail server principale del destinatario non è operativo, è possibile inviare il messaggio verso un server di backup in grado di gestire la posta del dominio.

Queste informazioni sono contenute nei record MX (Mail eXchanger).

```
unipr.it        IN      MX      1       icaro.cce.unipr.it.
unipr.it        IN      MX      2       ipruniv.cce.unipr.it.
```

Il campo numerico indica la priorità (il numero più basso ha maggiore priorità)

Provare il comando:

- `dig -t mx unipr.it +short`

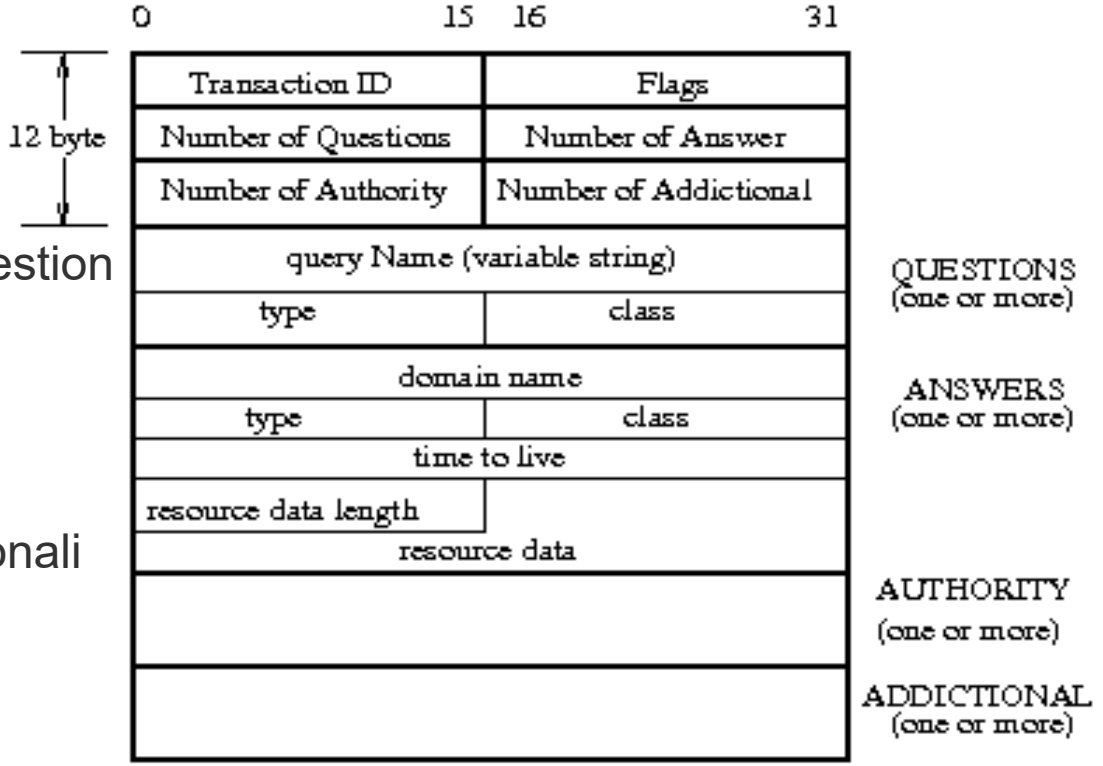
0 unipr-it.mail.protection.outlook.com.

Il formato del pacchetto DNS

Tutti i pacchetti DNS hanno lo stesso formato di figura, composto da:
Transaction ID: serve per associare domanda a risposta
16 Flags tra cui: QR (domanda (0) / risposta (1)) - OPCODE (4 bits, tipo di query) RD (Recursion Desired) - RA (Recursion Available) - RCODE (4 bits, esito della risposta)

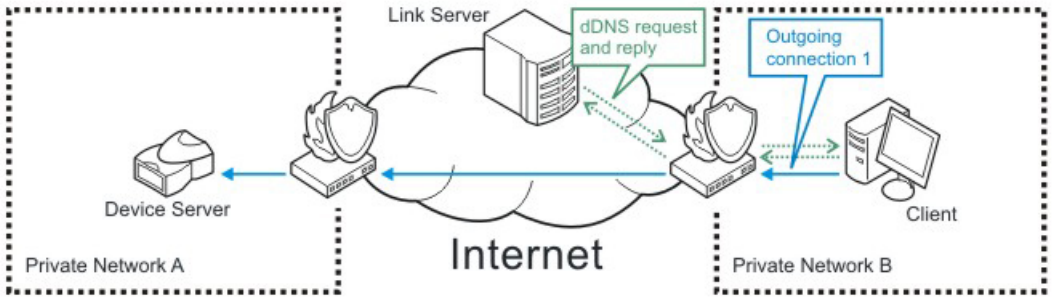
4 sezioni: QUESTIONS, ANSWERS, AUTHORITY e ADDITIONALS

QUESTIONS:
domande per il DNS.
ANSWERS:
elenco di RR che rispondono alla Question
AUTHORITY:
elenco di RR degli NS autoritativi
che portano più vicino alla risposta.
ADDITIONAL:
elenco di RR con informazioni addizionali



DNS dinamico (dDNS)

Il DNS Dinamico è una tecnologia che permette ad un nome DNS in Internet di essere sempre associato all'indirizzo IP di uno stesso host, anche se l'indirizzo cambia nel tempo (tipicamente computer portatili).
Il servizio è costituito da una popolazione di client dinamici (host con indirizzo IP dinamico che vogliono che il loro IP attuale sia registrato nel DNS), da uno o più server DNS dinamici e da un protocollo di comunicazione tra le due parti.
nsupdate è una utility disponibile ai client per l'aggiornamento del DNS.
L'aggiornamento dinamico del DNS può essere fatto direttamente dal server dhcp:
http://semicomplete.com/articles/dynamic-dns-with-dhcp



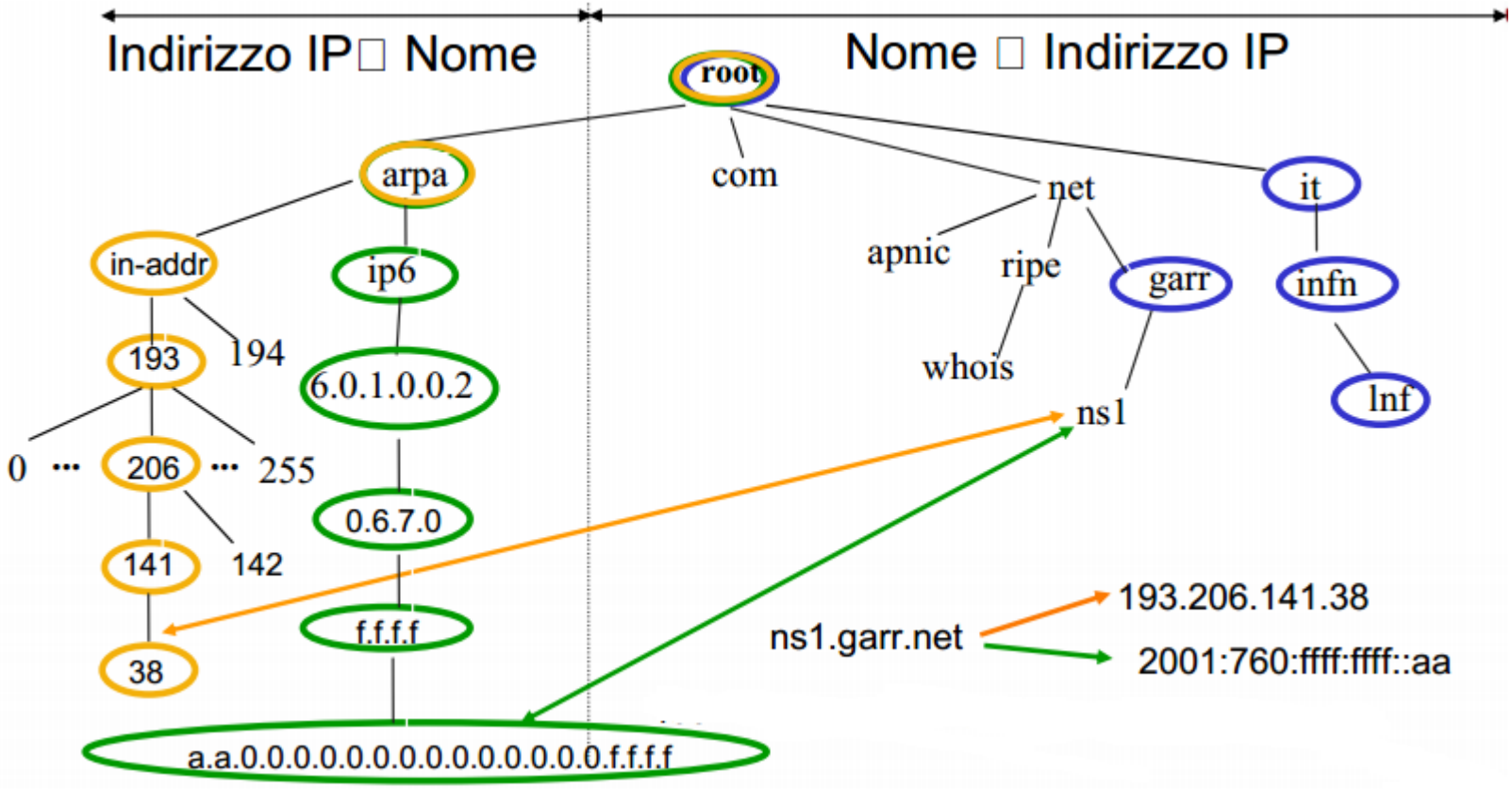
DNS e IPv6

L'utilizzo di IPv6 non modifica i meccanismi di base del DNS, ma è solo stato necessario introdurre alcuni nuovi elementi:

- Un nuovo Resource Record AAAA
- Un nuovo dominio per la risoluzione inversa : ip6.arpa (RFC 3152)

Riferimenti: Tutorial del GARR http://www.garr.it/eventiGARR/ws9/pdf/Gallo_Valli_pres.pdf

Il name space IPv4 e IPv6



Riferimenti: Tutorial del GARR: http://www.garr.it/eventiGARR/ws9/pdf/Gallo_Valli_pres.pdf

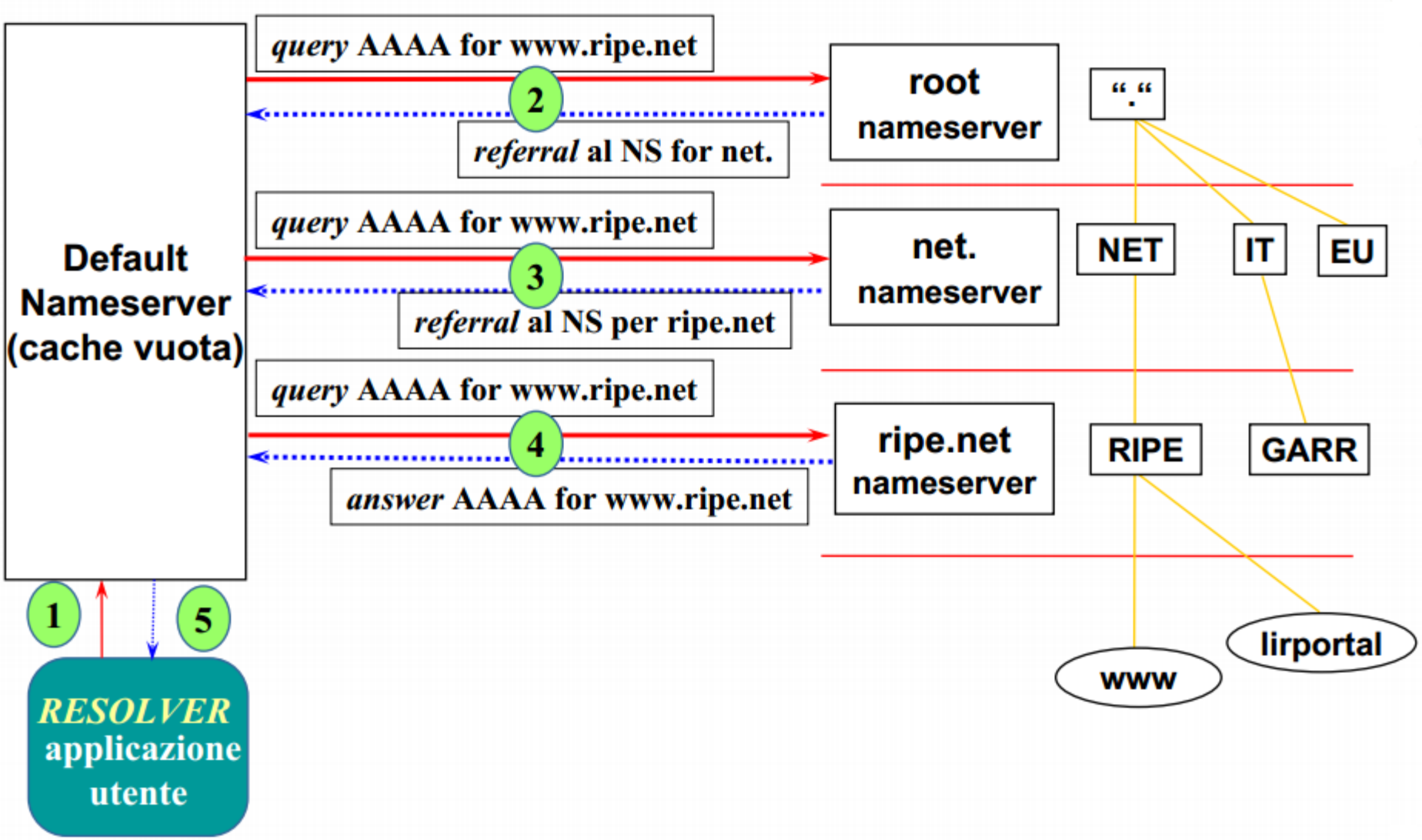
IPv6 e i root NS

Lettera	Vecchio nome	Indirizzo IPv6	Indirizzo IPv4	Operatore	Luogo geografico
A	ns.internic.net	2001:503:ba3e::2:30	198.41.0.4	VeriSign	Dulles, Virginia, USA
B	ns1.isi.edu	2001:500:84::b	192.228.79.201	USC Information Sciences Institute	Marina del Rey, California, USA
C	c.psi.net	2001:500:2::c	192.33.4.12	Cogent	distribuito in *anycast*
D	terp.umd.edu	2001:500:2d::d	199.7.91.13	University of Maryland	College Park, Maryland, USA
E	ns.nasa.gov	2001:500:a8::e	192.203.230.10	NASA	Mountain View, California, USA
F	ns.isc.org	2001:500:2f::f	192.5.5.241	ISC	distribuito in *anycast*
G	ns.nic.ddn.mil	2001:500:12::d0d	192.112.36.4	NIC del DoD USA	Vienna, Virginia, USA
H	aos.arl.army.mil	2001:500:1::53	128.63.2.53	U.S. Army Research Lab	Poligono di Aberdeen, Maryland, USA
I	nic.nordu.net	2001:7fe::53	192.36.148.17	Autonomica Archiviato il 1° maggio 2001 in Internet Archive.	distribuito in *anycast*
J	–	2001:503:c27::2:30	192.58.128.30	VeriSign	distribuito in *anycast*
K	–	2001:7fd::1	193.0.14.129	RIPE NCC	distribuito in *anycast*
L	–	2001:500:9f::42	198.32.64.12	ICANN	Los Angeles, California, USA
M	–	2001:dc3::35	202.12.27.33	Progetto WIDE	distribuito in *anycast*

Al momento non è possibile aggiungere altri nomi di server, a causa di un problema di ottimizzazione del protocollo: un pacchetto UDP deve poter contenere tutti i nomi dei server e con un quattordicesimo nome si supererebbe la dimensione massima del pacchetto.

Riferimenti: Wikipedia *https://it.wikipedia.org/wiki/Root_nameserver*

Processo iterativo per risoluzione dei nomi



Riferimenti: Tutorial del GARR http://www.garr.it/eventiGARR/ws9/pdf/Gallo_Valli_pres.pdf

Sicurezza del DNS

Le specifiche originali del DNS (RFC 882, 1034 e 1035) non prevedono autenticazione, integrità dei dati o cifratura e espongono il servizio a violazioni della sicurezza.
Il principale problema di sicurezza riguarda la possibilità di dirottare la richiesta di traduzione del nome di un server verso un IP fraudolento (DNS spoofing).

Una tecnica molto diffusa è il DNS cache poisoning (avvelenamento della cache).

L'attaccante gestisce un server DNS autoritativo per un dominio fake. Quando viene interrogato risponde includendo informazioni false (con un TTL molto grande) riguardo un dominio target, che vengono memorizzate in cache ed utilizzate quando successivamente vengono richieste traduzioni sul target, dirottando la richiesta verso un IP fraudolento.

La soluzione principale è stata l'introduzione del DNSSEC (RFC 9364).

DNS Security Extensions (DNSSEC)

I Domain Name System Security Extensions (DNSSEC) sono una serie di specifiche dell'IETF (RFC 9364) per garantire la sicurezza e affidabilità delle informazioni fornite dai sistemi DNS.

Servizi:
- Autenticazione: garanzia sull'origine dei dati DNS
- Integrità dei dati ricevuti (non la riservatezza)

Funzionamento:
Ogni server DNSSEC possiede una coppia di chiavi crittografiche, una pubblica e una privata. La chiave privata viene utilizzata per firmare ogni Resource Record (RRset) generando un nuovo Record type, il RRsig. Il server pubblica anche la chiava pubblica introducendo il nuovo record type DNSkey.
Il client, utilizzando la chiave pubblica DNSkey del server può verificare l'autenticità della firma RRsig.

Riferimenti:
https://www.cloudflare.com/dns/dnssec/how-dnssec-works/