

GARR

The Italian Academic & Research Network



www.garr.it

Tutorial IPv6 Avanzato

II DNS e IPv6

L'indirizzamento IPv6 per gli Enti GARR

Marco Gallo - Cristiano Valli

Workshop9, Roma, 15-18.06.2009



Indice degli argomenti

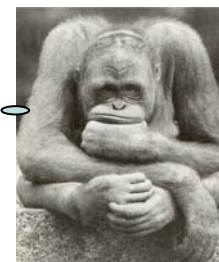
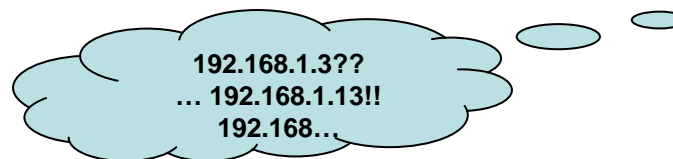
- I Parte: Il DNS e IPv6
 - Funzionamento del DNS su IPv6
 - L'IPv6 e la struttura gerarchica del DNS
 - Interazione tra IPv6 e IPv4 nel DNS
 - Configurazione del DNS per IPv6 su BIND
 - Tools per il troubleshooting
 - Conclusioni

- II Parte: l'IPv6 gestito dal GARR-LIR
 - Registrazione dello spazio IPv6 su RIPE
 - Piano di Indirizzamento e tools per il subnetting

DNS: obiettivo/esigenza

- Dare dei nomi ai calcolatori
- Associare un nome ***Human-readable*** ad un host, piu' semplice da ricordare di un indirizzo IP.

- ... Se in IPv4 questo era (e') l'obiettivo



- In IPv6 diventa un'esigenza...

2001:0b00:0c18:0001:0290:27ff:fe17:fc1d



- Un indirizzo e' formato da **8** campi di **16** bits ciascuno (**128** in tutto), ogni campo e' separato da ":" ed espresso in **notazione esadecimale**

IPv6 e il DNS: innovazioni

- L'utilizzo di IPv6 **non** modifica i meccanismi di base del *Domain Name System*
- Per gestire la risoluzione degli indirizzi IPv6 sono stati introdotti:
 - Un (due) **nuovo resource record** per associare un indirizzo IPv6 ad un nome
 - un (due) **nuovo dominio** per la risoluzione inversa degli indirizzi IPv6

Tipi di Indirizzi IPv6 [RFC 4291]

- **Anycast: uno al piu' vicino.** Indirizzo che si riferisce ad un insieme di interfacce. Un pacchetto inviato ad un indirizzo anycast, viene recapitato ad **una delle interfacce** che fanno parte dell'insieme da esso individuato (tipicamente da quella più "vicina", secondo la misura di "distanza" utilizzata dal protocollo di routing);
- **Multicast: uno a tanti.** Un pacchetto inviato ad un indirizzo multicast, viene recapitato a **tutte le interfacce** che fanno parte dell'insieme da esso individuato. Il **broadcast** in IPv6 **non esiste**. Il Multicast viene utilizzato al suo posto.
- **Unicast:** indirizzo che identifica **univocamente** un'interfaccia;

Indirizzi Unicast

- Gli indirizzi Unicast si distinguono in:
 - **Unspecified**: indica l'assenza di indirizzo quindi non e' assegnabile ad un host. Un esempio del suo utilizzo e' in DHCP quando viene inviato un pacchetto di inzializzazione ad un host prima che abbia "imparato" il suo indirizzo appartenente ad un determinato scope. Come "0.0.0.0" in Ipv4, l'indirizzo "::/0" indica la rotta di default.
 - **Loopback**: "::1" e' l'indirizzo locale di un host ed equivale a 127.0.0.1 in IPv4.
 - **Limited-Scope**:
 - **Link-local**: Configurati automaticamente sfruttando l'indirizzo Media Access Control (MAC) dell'interfaccia di rete. Non dovrebbero essere pubblicati su DNS perche' hanno un significato locale.
 - **Site-local**: Equivalenti agli indirizzi privati in IPv4 ma sono stati dichiarati deprecati [RFC 3879].
 - **Aggregatable Global**: indirizzi IPv6 pubblici routabili.

L'IPv6 e la struttura gerarchica del DNS

Risoluzione diretta e inversa

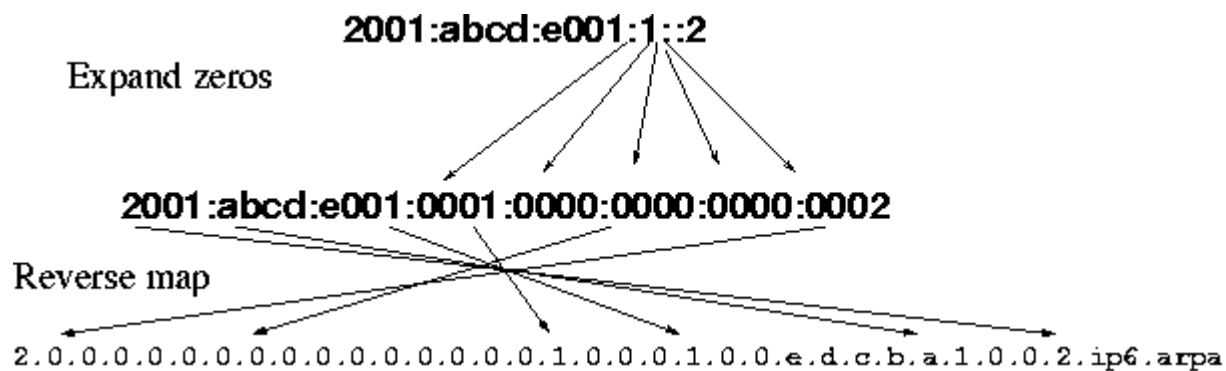
- Anche con IPv6, nel protocollo standard DNS, vengono individuate e distinte 2 tipologie di risoluzioni:
 - Risoluzione diretta:
 - Corrispondenza nome host – indirizzo IP
 - Risoluzione inversa:
 - Corrispondenza indirizzo IP – nome host

ip6.arpa o ip6.int?

- L' RFC 1886 indica l'ip6.int come dominio da utilizzare per la mappatura del reverse lookup in IPv6.
- L' RFC 3152 invece dice di usare l'ip6.arpa.
- Poiche' l'architettura gerarchica del DNS gia' usava il ".arpa" per IPv4, l'ip6.arpa e' stato preferito all'ip6.int (deprecato dall'IETF l 1 Giugno 2006 – RFC 4159) come dominio per il reverse in IPv6

Il reverse DNS lookup

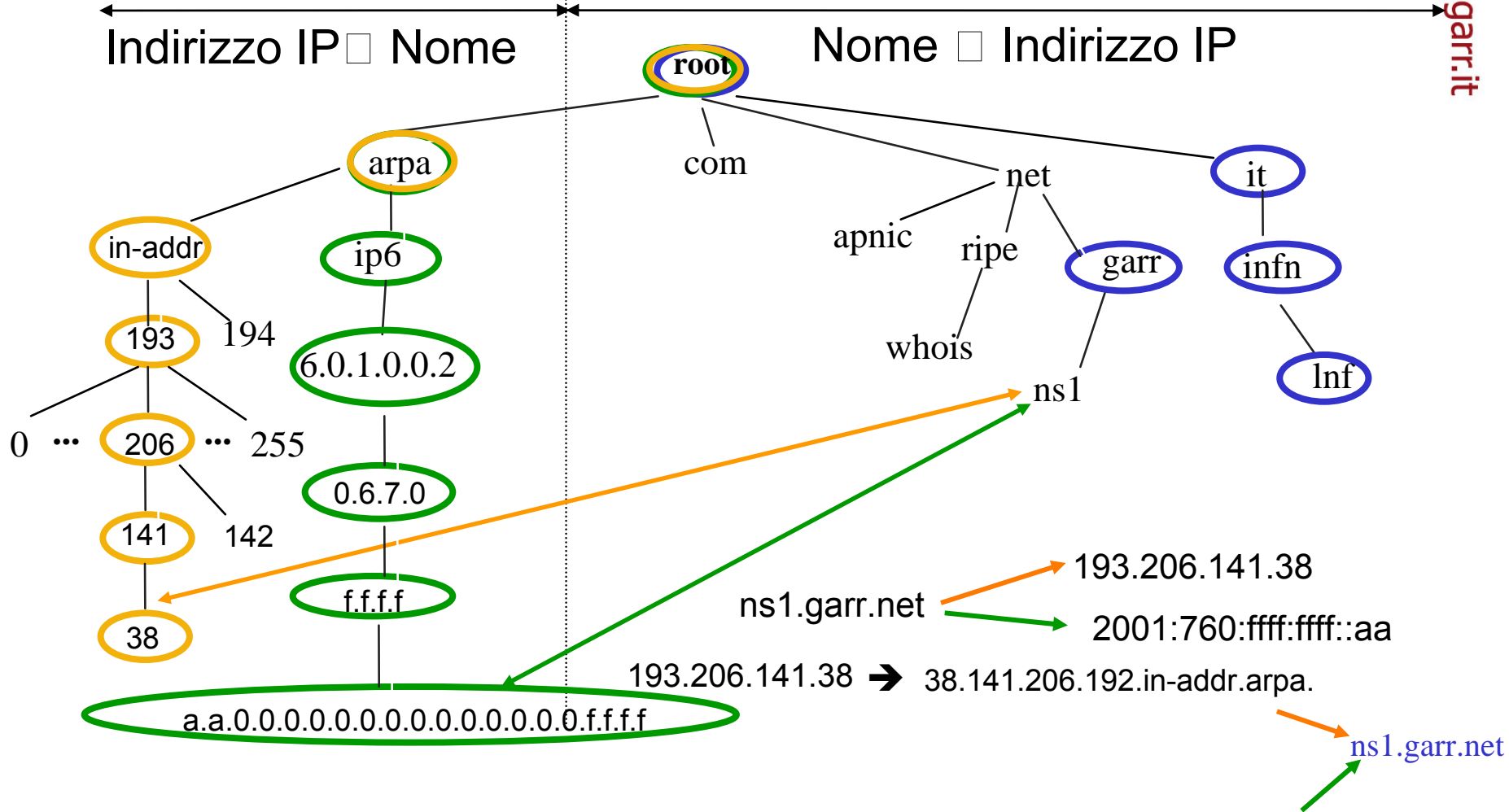
- Il reverse di un indirizzo IPv6 e' espresso, nel dominio "ip6.arpa", da una sequenza di otto cifre esadecimali scritte in ordine inverso; numeri e lettere sono separati da un punto



L'IPv6 nella gerarchica del DNS

- Suddivisione gerarchica delle zone dello spazio di indirizzamento
- Struttura ad albero rovesciato
- Localita' dell'informazione
 - ogni nodo detiene un database con le informazioni della propria network IPv6 e interroga gli altri nodi quando deve trovare le informazioni non locali
- Basato sul modello client/server
 - Le informazioni possono essere ottenute tramite interrogazioni ad una delle foglie dell'albero

Risoluzione diretta e inversa di un indirizzo IPv6 nell'albero dei nomi



2001:760:ffff:ffff::aa → a.a.0.f.f.f.f 12

IPv6 e i root nameserver

- I root nameserver sono i server responsabili (autoritativi) delle informazioni relative al dominio ".";
- Possiedono l'elenco dei server responsabili per ognuno dei domini di primo livello riconosciuti e lo forniscono in risposta a ciascuna richiesta.
- Contengono le informazioni per la risoluzione inversa (risoluzione indirizzo-nome)
- La lista aggiornata dei root-server è mantenuta da InterNIC
 - *ftp://ftp.rs.internic.net/domain/named.root*
 - *ftp://ftp.nic.it/pub/DNS/named.root*

IPv6 e i root nameservers

- I root nameserver sono risorse critiche, in particolare per IPv6.
- 13 roots in tutto il mondo (10 negli USA)
 - Non tutti i root NS hanno IPv6 attivo
 - A partire dal 4 febbraio 2008 sono stati introdotti records AAAA nella configurazione di 6 dei 13 root nameserver
 - <http://www.iana.org/reports/2008/root-aaaa-announcement.html>

Authority	IPv6 Address	Prefix Length
A.ROOT-SERVERS.NET	2001:503:ba3e::2:30	/48
F.ROOT-SERVERS.NET	2001:500:2f::f	/48
H.ROOT-SERVERS.NET	2001:500:1::803f:235	/48
J.ROOT-SERVERS.NET	2001:503:c27::2:30	/48
K.ROOT-SERVERS.NET	2001:7fd::1	/32
M.ROOT-SERVERS.NET	2001:dc3::35	/32

IPv6 e i root nameserver



Perche' solo 13 root nameserver (1)

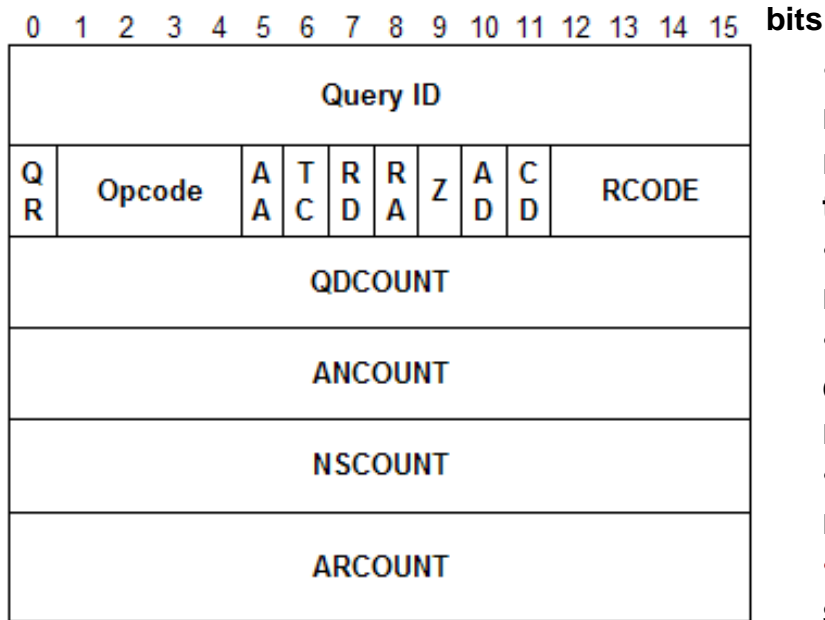
- Il numero (esiguo) dei root nameserver e' dovuto ai limiti definiti nelle specifiche del DNS sulla **grandezza del pacchetto** [RFC 1035].
- Il limite e' fissato a 512 byte su UDP.
- Piu' root NS attivi => Piu' resource records da includere nel pacchetto DNS che i root nameserver dovrebbero fornire in risposta nel corso del processo iterativo di risoluzione.
 - Con IPv6 questo problema e' ancor piu' evidente visto che nel pacchetto DNS oltre a records **A** devono essere inclusi anche records **AAAA**

Formato del pacchetto DNS [RFC 1035]

- I dati del DNS vengono scambiati tra i nameserver mediante un pacchetto, il “message”, che presenta la seguente struttura:
 - Il formato del “message” e' diviso in cinque sezioni, alcune delle quali sono vuote in alcuni casi

Header	Include campi con informazioni di controllo
Question	La query ad un certo nome
Answer	I RR per il nome richiesto
Authority	I RR degli NS autoritativi
Additional	RR che gestiscono informazioni aggiuntive

Formato dell'Header [RFC 1035]



- **Query ID**: identificativo a 16 bits assegnato del resolver che genera la query. Campo copiato nella risposta corrispondente e serve al match tra domanda e risposta alla query fatta
- **QR**: Campo a 1 bit che specifica se il messaggio e' una domanda(0) o una risposta (1)
- **OPcode**: campo a 4 bits specifica il tipo di query. Di solito settato a zero che significa risposta standard
- **AA**: Risposta autoritativa solo valido nelle risposte
- **TC**: troncamento, specifica che il message e' stato troncato perche' troppo lungo

- **RD**: Recursion Desired, predispone il nameserver a gestire la query in maniera ricorsiva
- **RA**: Recursion Available, indica che la gestione ricorsiva della query e' disponibile sul nameserver
- **Z**: riservato ad usi futuri. Deve essere zero in tutte le domande e risposte
- **RCODE**: definisce l'esito della risposta (no error, format error...)
- **QDCOUNT**: indica il numero di entries nella sezione Question
- **ANCOUNT**: indica il numero di RR presenti nella sezione Answer
- **NSCOUNT**: specifica il numero di NS indicati nella sezione Authority
- **ARCOUNT**: indica il numero di RR nella sezione Additional

Perche' solo 13 root nameserver (2)

- La condizione verso cui si tende:
 - tutti i 13 root nameserver rispondano in IPv6 e si assegni ad ognuno di essi un record AAAA.
 - Tutti i records (**A** e **AAAA**) dovranno essere inclusi nel pacchetto DNS superando il problema sul limite sulla grandezza
- Questo e' cio' che viene proposto nello studio presentato dall'ICANN Security and Stability Advisory Committee.
 - <http://www.icann.org/en/committees/security/sac018.pdf>

Utilizzo dell'EDNS0 [RFC 2671]

- L'EDNS0 (*Extension Mechanisms for DNS version 0*) e' il sistema introdotto dall'IETF per superare il limite sulla grandezza del pacchetto DNS.
- Mediante l'EDNS0 si definisce un **nuovo RR**, il record **OPT**, non visibile nel database distribuito del DNS.
 - Si tratta di uno "**pseudo-record**" che agisce al livello di trasporto.
 - E' gia' supportato sia dalla maggior parte dei resolver presenti sui sistemi operativi di piu' recente generazione sia da tutte le versioni di BIND 9

Come funziona l'EDNS0

- Un client dotato di resolver in grado di gestire l'EDNS, per pacchetti superiori ai 512 byte, invierà al nameserver un *message* contenente nella sezione "Additional" un record OPT.
- Se anche il server supporta l'EDNS risponderà al client con un message di grandezza pari a quella specificata dal client.
- I nameserver che non supportano ancora l'EDNS semplicemente rispondono con un "error code" se ricevono una query contenente il record OPT.
- Il client in tal caso ripeterà la query senza usare l'EDNS

Root nameserver replicati

- La ISC (Internet Software Consortium) ha adottato un sistema che permette di replicare i Root Name Server in modo da renderli più accessibili a località fisicamente lontane dai 13 Root Server globali.
- Obiettivo:
 - Configurare NS cloni da un master/primary server che contengano gli stessi dati (files);
 - che utilizzino lo stesso indirizzo IP (metodo Anycast).
 - Questo tipo di nameserver sono già stati installati:
 - <http://www.root-servers.org/>
 - Presso MIX: repliche di I-root, K-root e J-root di cui sia I che K rispondono anche in IPv6
 - Presso NAMEX: repliche di F.root, J.root di cui F risponde anche in IPv6
 - Vantaggi per gli ISP afferenti agli Internet Exchange: tempi di risposta più bassi per le richieste rivolte ai root NS.

IPv6 sui nameservers dei TLD

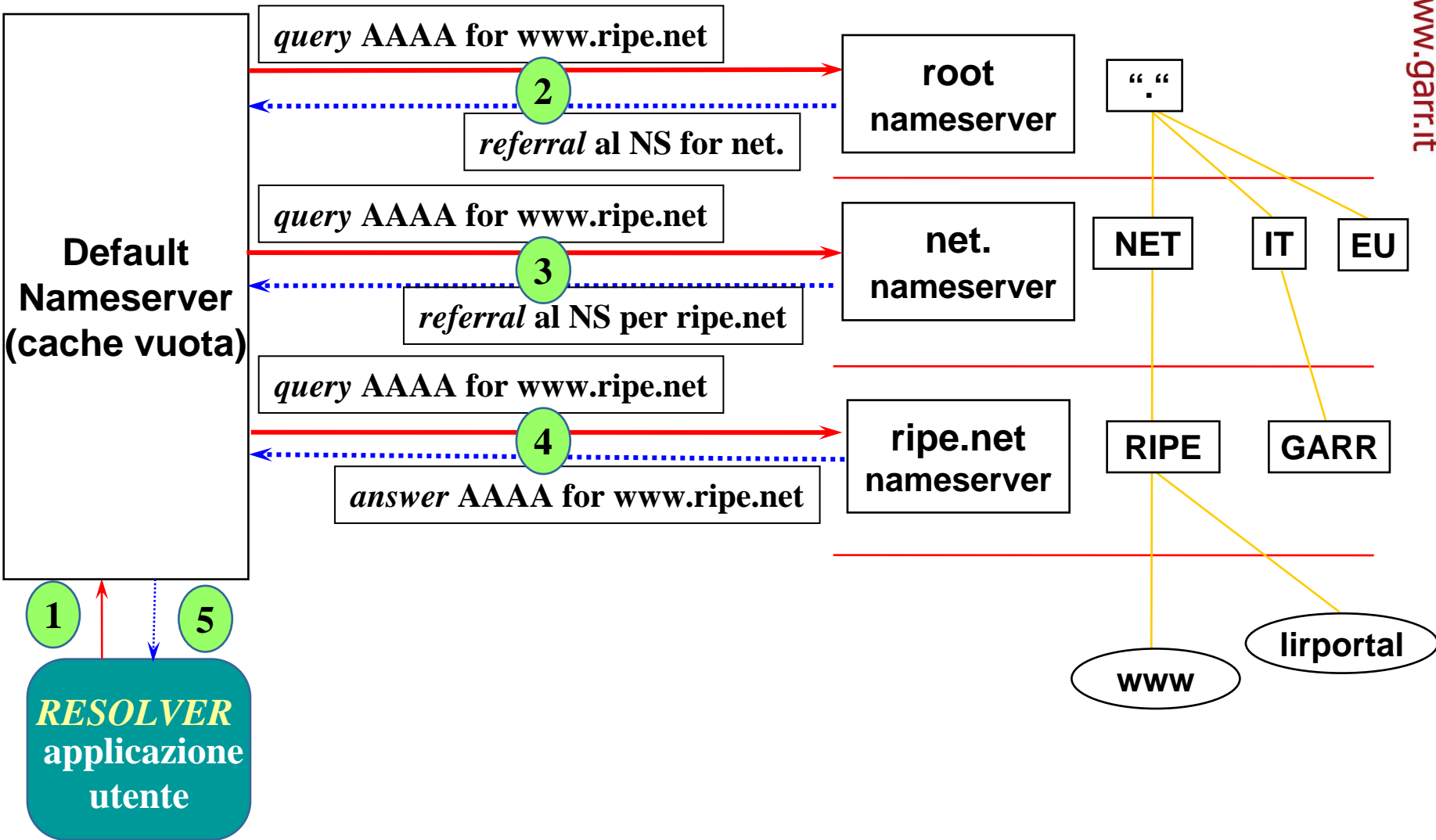
- Alcuni dei root nameserver sono configurati per rispondere a query IPv6.
- Diverse Authority di TLD hanno configurato IPv6 su alcuni dei nameserver autoritativi del dominio di primo livello che amministrano
 - Sia il Registro per il “.it” che EURid per il “.eu” hanno abilitato due nameserver a rispondere in IPv6
- Una volta attivato il trasporto IPv6 sull’infrastruttura di rete che amministrarete dovrete aggiungere dei records AAAA per la risoluzione diretta.

Interazione tra IPv6 e IPv4 nel DNS

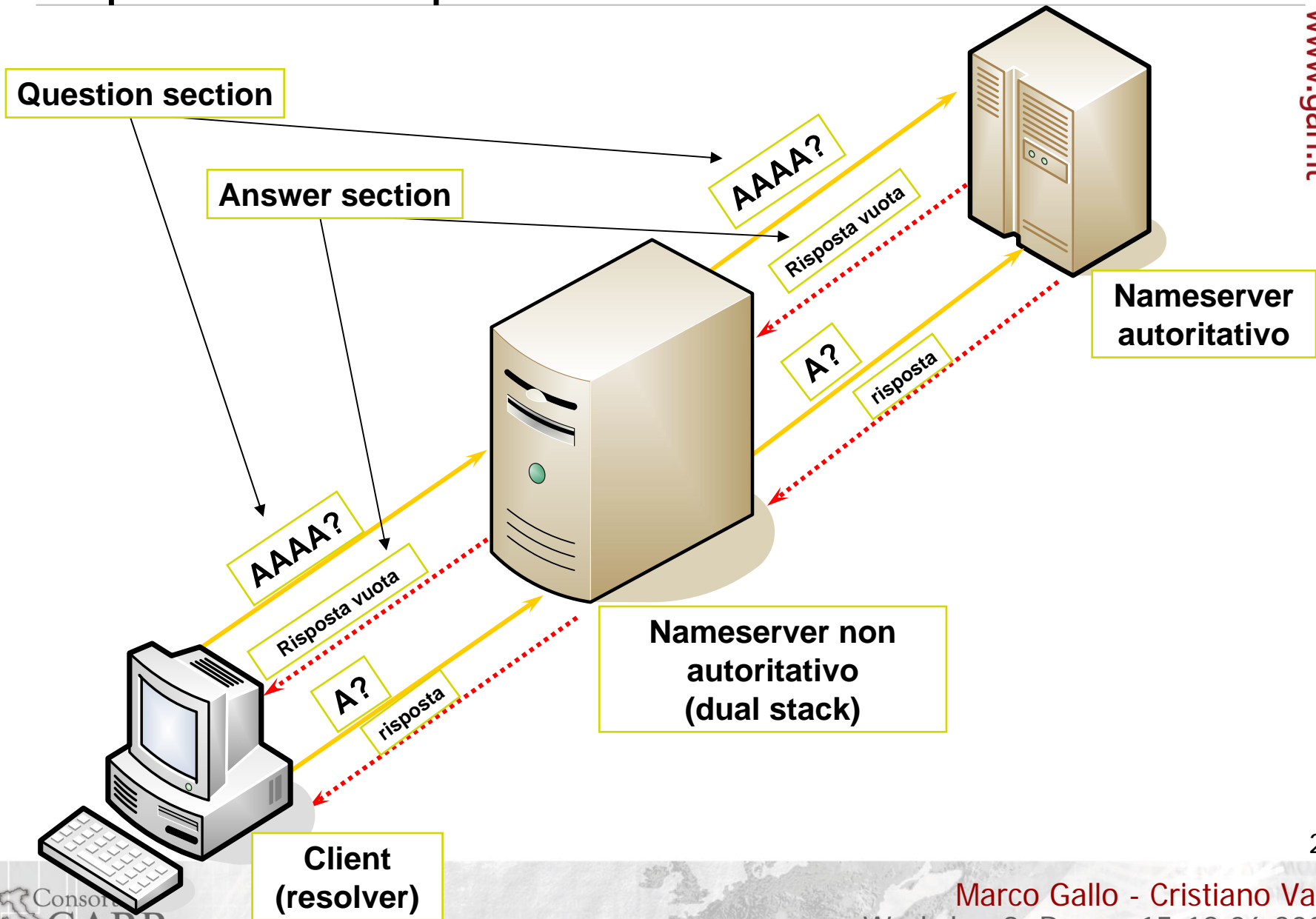
Risposta ai records AAAA nel processo iterativo

- Un nameserver IPv6 deve essere configurato in dual stack
 - Gran parte delle applicazioni di rete in dual stack tentano di risolvere indirizzi IPv4 e IPv6, inviando query al DNS sia su record A sia su record di tipo AAAA.
 - Ma cosa accade se nel processo iterativo di risoluzione dei nomi viene coinvolto un nameserver su cui non sono configurati records per IPv6?

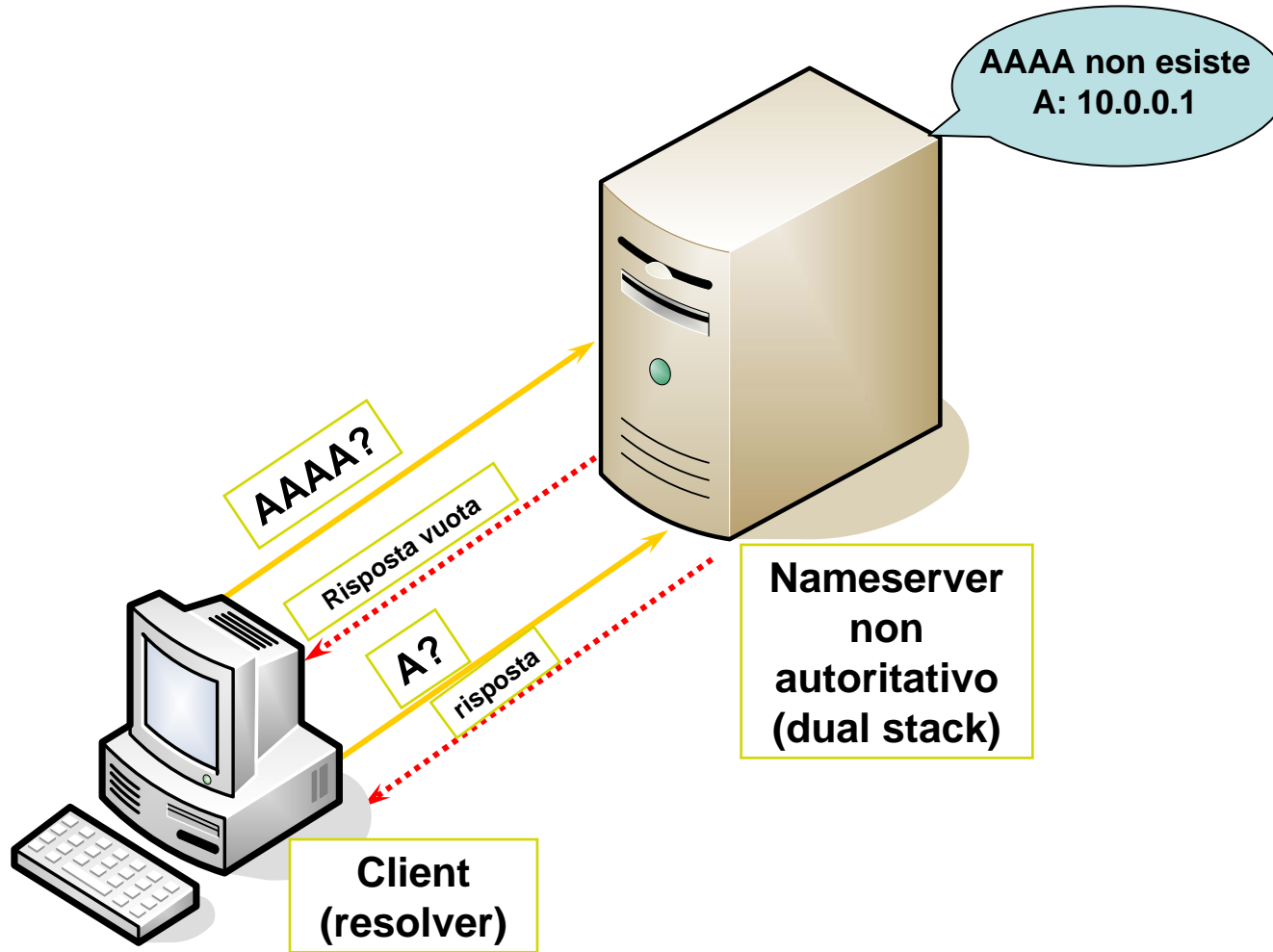
Il processo iterativo di risoluzione dei nomi



Risposta vuota per i records AAAA



Risposta vuota per i records AAAA



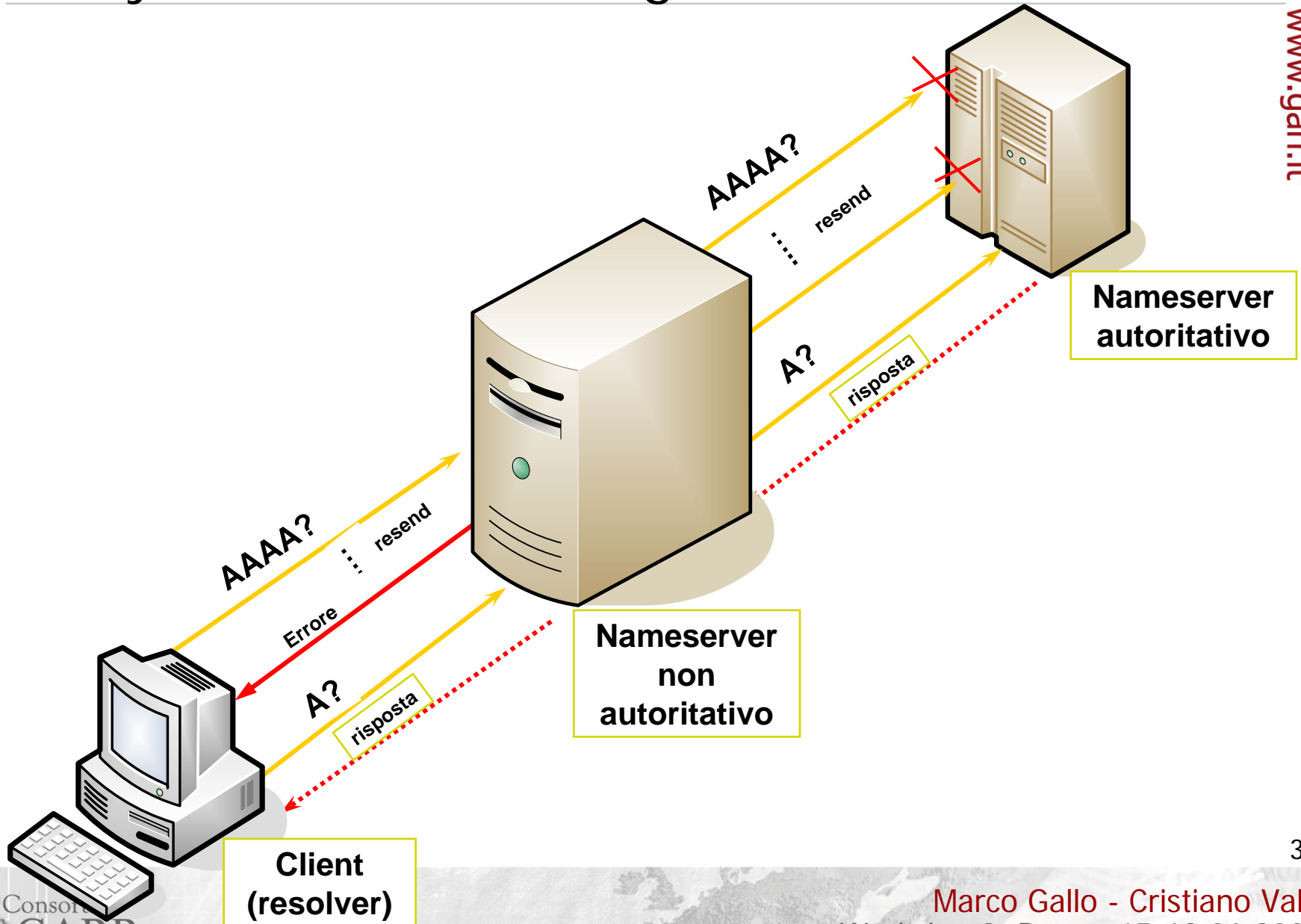
Interazione tra records A e AAAA

- Una query fatta su IPv6 non e' detto che interagisca solo con records di tipo AAAA
- L'indirizzo sorgente da cui parte la query indica solo il trasporto usato per interrogare il nameserver.
 - Un client che interroga un nameserver potrebbe utilizzare un **trasporto diverso** da quello usato dal nameserver a cui il client sottomette la query.
 - Importante: l'ideale e' che sul server sia configurato il dual stack
- Query su records di tipo AAAA potrebbero essere dirette verso zone i cui nameserver autoritativi hanno solo attivo IPv4

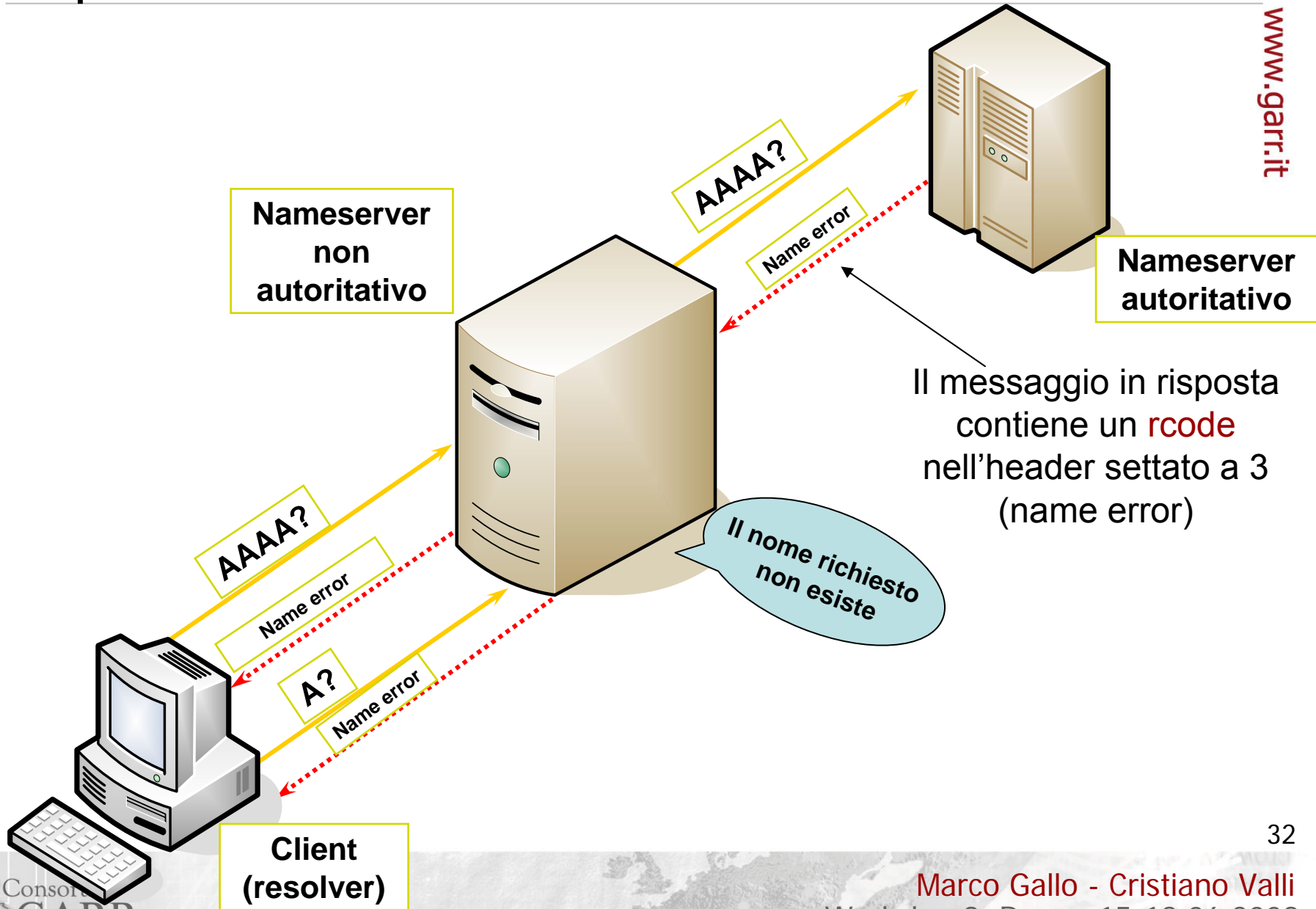
Risposte non corrette di alcuni NS su records AAAA [RFC 4074]

- Gli **AAAA** rappresentano lo **standard** in **IPv6** per la risoluzione diretta.
- Gran parte dei server DNS gestiscono correttamente questo tipo di records
- Vi sono alcuni nameserver che non trattano i records AAAA nel modo previsto
- L'RFC 4074 fornisce i dettagli di tali mal funzionamenti
 - I malfunzionamenti riportati nell'RFC 4074 non sono specifici in realta' solo del record AAAA visto che tali problemi sono stati osservati anche per altri tipi records comunemente usati per IPv4.

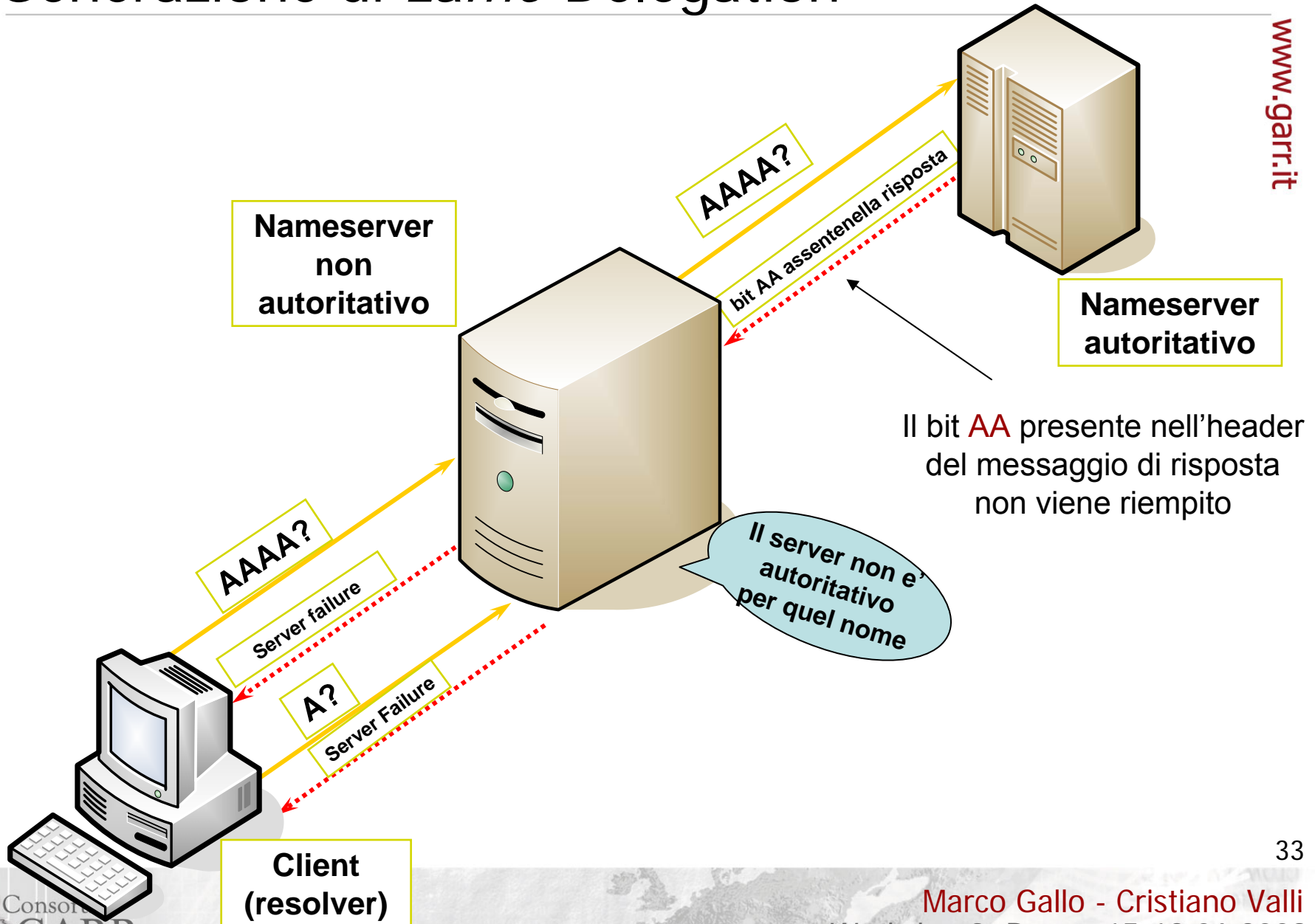
Query su records AAAA ignorata



Risposta di errore sul nome



Generazione di *Lame* Delegation



Workaround??

- Il problema del “name error” non riguarda BIND. Sul sito della **US-CERT** (**U**nited **S**tates **C**omputer **E**mergency **R**eadiness **T**eam) vengono elencati i sistemi vulnerabili a questo problema e viene consigliato di applicare le patch del vendor:
 - <http://www.kb.cert.org/vuls/id/714121>
- Gli **altri** malfunzionamenti **possono riguardare BIND** ma soprattutto per cache nameserver. Tali problemi **non sono** comunque **stati evidenziati su BIND** a partire **dalla v9.4** in poi.
 - **Tenere aggiornato BIND.**
- Anche se alcuni dei problemi descritti possono essere tenuti sotto controllo nella propria LAN configurando e aggiornando opportunamente i nameserver, si tratta comunque di “bug” che dovrebbero essere risolti sui nameserver autoritativi.

Configurazione del DNS per IPv6 su BIND 9

- BIND9 supporta tutti i tipi di records usati nel DNS
- Il **trasporto** IPv6 e' supportato ma e' fondamentale che lo sia anche dal sistema operativo su cui BIND viene installato.
 - La gestione del trasporto IPv6 e' stato particolarmente trattato e migliorato su BIND a partire dalla versione 9.2
- BIND9 puo' eseguire e ricevere query su IPv6 cosi' come rispondere agli strumenti di lookup per eseguire query su IPv6 per il troubleshooting

Installare BIND con IPv6 attivo

- Scaricare la versione piu' recente di BIND in /usr/src
- Decomprimere il pacchetto
 - `tar -xzf bind-9.x.y.tar.gz`
 - `cd bind-9.x.y`
- Anche se il trasporto di IPv6 e' ormai nativo su BIND lo si puo' esplicitamente specificare al momento dell'installazione:
 - `./configure --enable-ipv6`
 - Naturalmente se per qualche ragione si vuole disabilitare il trasporto IPv6:
 - `./configure --disable-ipv6`
- Infine compilare e installare come root:
 - `make`
 - `su`
 - `make install`

- Su BIND potrebbe essere disabilitato il trasporto IPv6 ma eventuali records AAAA configurati nei file di zona potrebbero essere comunque trasportati su IPv4 [RFCs **3901 - 4472**].
- Non confondere il trasporto con i dati!
- Le richieste di risoluzione di indirizzi IPv6, si possono ottenere sia mediante trasporto su pacchetti IPv4 sia IPv6. La versione (v4/v6) del protocollo con cui si esegue il trasporto e' indipendente dal tipo di dati (records) che vengono trasportati (A o AAAA).
 - *Bind 4-8* risponde alle richieste fatte **soltanto** su trasporto IPv4
 - *Bind 9* puo' rispondere alle richieste direttamente su trasporto IPv6
- Condizione ideale: la macchina che ospita il DNS deve essere DUAL-STACK!

Opzioni da linea di comando

- Su BIND9 e' possibile disabilitare uno dei due stack (v4/v6) anche se sono entrambi attivi di default.
 - **named -6 BIND 9.x.y**
 - Indica al processo named di utilizzare solo IPv6 anche se il sistema operativo del server e' in grado di gestire IPv4
 - **named -4 BIND 9.x.y**
 - Fa in modo che named utilizzi solo IPv4
- Le due opzioni si escludono a vicenda.

File di configurazione di BIND

- Di default i file di configurazione di BIND 9 verranno distribuiti nel file system in questo modo:
 - Il file di configurazione: `/etc/named.conf`
 - Il "named" si trovera' sotto `/usr/local/sbin`
 - Tutti gli altri file di configurazione in `/var/named`

Query ricorsive

- Per abilitare le query ricorsive sul proprio DNS agli host su cui e' stato configurato un IPv6 appartenente alla propria /48, su named.conf si configura:

```
options {  
    allow-recursion {  
        2001:760:1010::/48;  
    }  
}
```

Update dalla loopback

- Con l'allow-update e' possibile definire una lista di IP abilitati a sottomettere update di una determinata zona.
- Per consentire update provenienti dalla loopback IPv4 o IPv6

```
options {  
    allow-update { ::1; 127.0.0.1; };  
};
```

- L'istruzione allow-update puo' essere configurata anche in una zona o in una view oltre che tra le options.

Come abilitare l'EDNS

- All'interno della parte di configurazione dedicata a definire le caratteristiche specifiche del nameserver, viene aggiunta l'istruzione per abilitare l'EDNS:

```
server ip-addr {  
    edns yes | no ;  
};
```

- L'istruzione e' valida solo per le versioni di BIND 9 ed e' configurabile solo nella sezione "server" della configurazione globale.

Specifici controlli IPv6 su BIND

- BIND dispone di controlli specifici riguardanti il suo funzionamento su IPv6.
 - listen-on-v6
 - transfer-source-v6
 - alt-transfer-source-v6
 - avoid-v6-udp-ports
 - query-source-v6
 - preferred-glue

Accettare query IPv6

- Per rendere operativo il nameserver ad accettare query IPv6 (non abilitato di default), nelle options del named.conf si configura anche quanto segue:

```
options {  
    listen-on-v6 { any; };  
};
```

- Prima di BIND 9.3.0 l'istruzione listen-on-v6 accettava solo *any* o *none* come argomenti. Ora e' possibile, mediante il comando *port*, configurare anche una porta alternativa alla 53:

```
options {  
    listen-on-v6 port 1055 { any; };  
};
```

transfer-source-v6

- Istruzione valida solo per le zone di tipo *slave*
- E' possibile individuare quale indirizzo IPv6 il nameserver slave andra' ad utilizzare, su connessione TCP, come indirizzo sorgente per il trasferimento di zona:

```
options {  
    transfer-source-v6 2001:760:2521:1:210:4bff:fe10:d24;  
};
```

- E' possibile specificare anche la porta sorgente:

```
options {  
    transfer-source-v6 2001:760:2521:1:210:4bff:fe10:d24 port 53;  
};
```

alt-transfer-source-v6

- Istruzione che ha effetti solo per zone di tipo *slave*.
- Specifica un indirizzo IPv6 sorgente o numero di porta alternativo per lo **zone-transfer**, nel caso quello di default fallisse

`alt-transfer-source-v6 (ipv6_address | *) [port (integer | *)];`

E' indispensabile che l'istruzione

use-alt-transfer-source

sia configurata su "yes"

query-source-v6

- Predispone l'indirizzo IP e/o un determinato numero di porta ad essere utilizzato come sorgente per qualunque query in uscita che il nameserver trasmette su IPv6.
- E' un'istruzione che potrebbe essere utilizzata in una view o tra le global options

```
options {  
    query-source-v6 2001:760:0:2::13;  
};
```

```
options {  
    query-source-v6 * port 54321;  
};
```

- L'asterisco sta ad indicare l'IP di default del server

Preferred-glue

- Con questa opzione, valida a partire dalla v9.3 di BIND, e' possibile specificare la preferenza rispetto ai records che si vuole che vengano inclusi nel pacchetto DNS.
 - Con l'istruzione:
 - Preferred-glue A
 - Il message conterra' i records A e possibilmente eventuali record AAAA
 - Viceversa con l'istruzione:
 - Preferred-glue AAAA
 - Si da la preferenza ai record AAAA

File di zona del reverse name del localhost-v6

```
; From: @(#)localhost.rev 5.1 (Berkeley) 6/30/90
; $FreeBSD: src/etc/namedb/PROTO.localhost-v6.rev,v 1.1 2002/01/22 17:22:41 ume Exp $
;
; This file is automatically edited by the `make-localhost' script in
; the /etc/namedb directory.
;
```

```
$TTL 3600
```

```
@      IN      SOA      ns1.garr.net. root.ns1.garr.net. (
                2005063001      ; Serial
                3600      ; Refresh
                900      ; Retry
                3600000      ; Expire
                3600 ) ; Minimum

IN      NS      ns1.garr.net.
IN      PTR     localhost.garr.net.
```

Utilizzo delle view con IPv6

- L'istruzione view specifica diversi ambiti di visibilita' delle zone rispetto a porzioni di network

```
acl "internal" {
    2001:760:1010::/64;
    ::1;
};
view "internal" {
    match-clients { internal; };
    recursion yes;
    zone "intranet.prova.it" {
        type master;
        file "intranet.prova.it.int";
        allow-transfer { any; };
    };
};

view "external" {
    match-clients { any; };
    recursion no;
    zone "prova.it " {
        type master;
        file "prova.it.ext";
        allow-transfer { none; };
    };
};
```

- Le query provenienti da host appartenenti alla /64 indicata nell'acl internal intercettano la view internal

Configurazione delle zone

- **Tre azioni:**
 - Rendere i propri nameserver autoritativi per la risoluzione diretta e inversa su IPv6.
 - Aggiungere i Resource Records nei file di zona (sia AAAA che PTR)
 - Aggiornare le deleghe

Azione 1: configurazione di una zona master e una slave

- Nel named.conf del master:

```
zone "prova.it" {  
    type master;  
    file "master/dom/prova-it.soa";  
    allow-query { any; };  
    allow-transfer { 90.148.80.2;  
                    2001:760:1010::8; };  
};
```

- Nel named.conf dello slave:

```
zone "prova.it " {  
    type slave;  
    file "slave/dom/prova-it.for";  
    masters {  
        90.148.80.1;  
        2001:760:1010::7;  
    };  
    allow-query { any; };  
    allow-transfer { none; };  
};
```

Azione 1: configurazione di una zona di reverse IPv6 master e di una slave

- Configurazione per la 2001:760:1010::/48
- Nel named.conf del master:

```
zone "0.1.0.1.0.6.7.0.1.0.0.2.ip6.arpa" {  
    type master;  
    allow-query { any; };  
    file "master/ipv6/2001.760.1010.soa";  
    allow-transfer {  
        90.148.80.2;  
        2001:760:1010::8;  
    };  
};
```

- Nel named.conf dello slave:

```
zone "0.1.0.1.0.6.7.0.1.0.0.2.ip6.arpa" {  
    type slave;  
    file "slave/ipv6/2001.760.1010.soa";  
    masters {  
        90.148.80.1;  
        2001:760:1010::7;  
    };  
    allow-query { any; };  
};
```

Azione2: aggiungere i records nei file di zona per risoluzione diretta e inversa

- Aggiungere i records NS e qualunque altro record necessario nel file di zona di "prova.it"
- Verificare la versione del Serial nel record SOA ed aggiornarlo
- Eseguire un rndc reload "prova.it"
- Fare una verifica dei log sia sul nameserver master che sullo slave

Il Record AAAA (quad A)

- Record Address IPv6 [RFC 3596]
- Gestisce la risoluzione diretta dei nomi associati ad un indirizzo IPv6

\$ORIGIN prova.it

www IN AAAA 2001:760:1010::3

- Equivalente al record **A** utilizzato in IPv4

AAAA e A6: la guerra dei records

- Lungo dibattito in IETF sulla scelta tra il record AAAA e A6.
 - Entrambi gli approcci sono validi
 - AAAA e' semplice concettualmente
 - A6 piu' flessibile ma assai complicato [RFC 2874] .
- La decisione venne presa in favore dell'ottimizzazione del criterio di risoluzione di nomi e indirizzi
 - Vennero scelti AAAA e PTR
 - A6 ancora attivo e supportato da BIND ma solo SPERIMENTALE

Configurazione del file di zona per prova.it

```
$ORIGIN .
prova.it      IN SOA ns1.prova.it. staff-dns.prova.it. (
              2008011101 ; serial
              86400      ; refresh (1 day)
              7200       ; retry (2 hours)
              2592000    ; expire (4 weeks 2 days)
              345600     ; minimum (4 days)
              )
$TTL 86400
              NS       ns1.prova.it.
              NS       ns2.prova.it.
```

```
$ORIGIN prova.it.
srv1          IN      A          10.0.0.1
              IN      AAAA       2001:760:1010::1
srv2          IN      A          10.0.0.2
              IN      AAAA       2001:760:1010::2
www           IN      A          10.0.0.3
              IN      AAAA       2001:760:1010::3
ns1           IN      A          10.0.0.4
              IN      AAAA       2001:760:1010::7
ns2           IN      A          10.0.0.5
              IN      AAAA       2001:760:1010::8
.....
```

II Record PTR

- Record Pointer IPv6 [RFC 1035]
- Gestisce la risoluzione inversa di un indirizzo IPv6 associando un indirizzo ad un nome

```
$ORIGIN 1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa  
d.1.c.f.7.1.e.f.f.f.7.2.0.9.2.0 IN PTR www.6net.garr.it
```

- Lo stesso tipo di record utilizzato per IPv4
 - Un nuovo modello di *top level* usato per IPv6:
 - da ip6.int (deprecato dall'IETF I Giugno 2006)
 - a ip6.arpa

Azione3: aggiornamento delle deleghe

- Nel caso di prova.it: aggiornare le deleghe presso il Registro nella zona del ".it"
 - E' compito del GARR-NIC fornire al Registro i dati sui nameserver autoritativi verso cui configurare le deleghe.
- Nel caso della zona di reverse della /48 (0.1.0.1.0.6.7.0.1.0.0.2.ip6.arpa), aggiornare il file di zona di reverse della /32
 - E' compito del GARR-LIR provvedere all'aggiornamento del file di zona di reverse della 2001:760::/32 aggiungendo i records NS relativi ai nameserver autoritativi della zona di reverse della /48

Esempi di delega IPv6: 2001.760.soa

```
$TTL 86400      ; 1 day
@               IN SOA ns1.garr.net. staff-dns.garr.it. (
                2009052401 ; serial
                21600      ; refresh (6 hours)
                3600       ; retry (1 hour)
                1814400    ; expire (3 weeks)
                10800      ; minimum (4 days)
                )
NS              ns1.garr.net.
NS              ns2.garr.net.
NS              ns.ripe.net.
;
;
; Reverse CNR Torino
;
0.0.6.2        NS      server8.to.cnr.it.
                NS      server9.to.cnr.it.
                NS      ns1.garr.net.
;
; Reverse CNR Pisa
;
0.0.0.4        NS      dns.iit.cnr.it.
                NS      nameserver.cnr.it.
                NS      dns.pi.cnr.it.
;
; Reverse INFN Roma3
;
2.0.0.4        NS      gw6.roma3.infn.it.
                NS      ns1.garr.net.
```

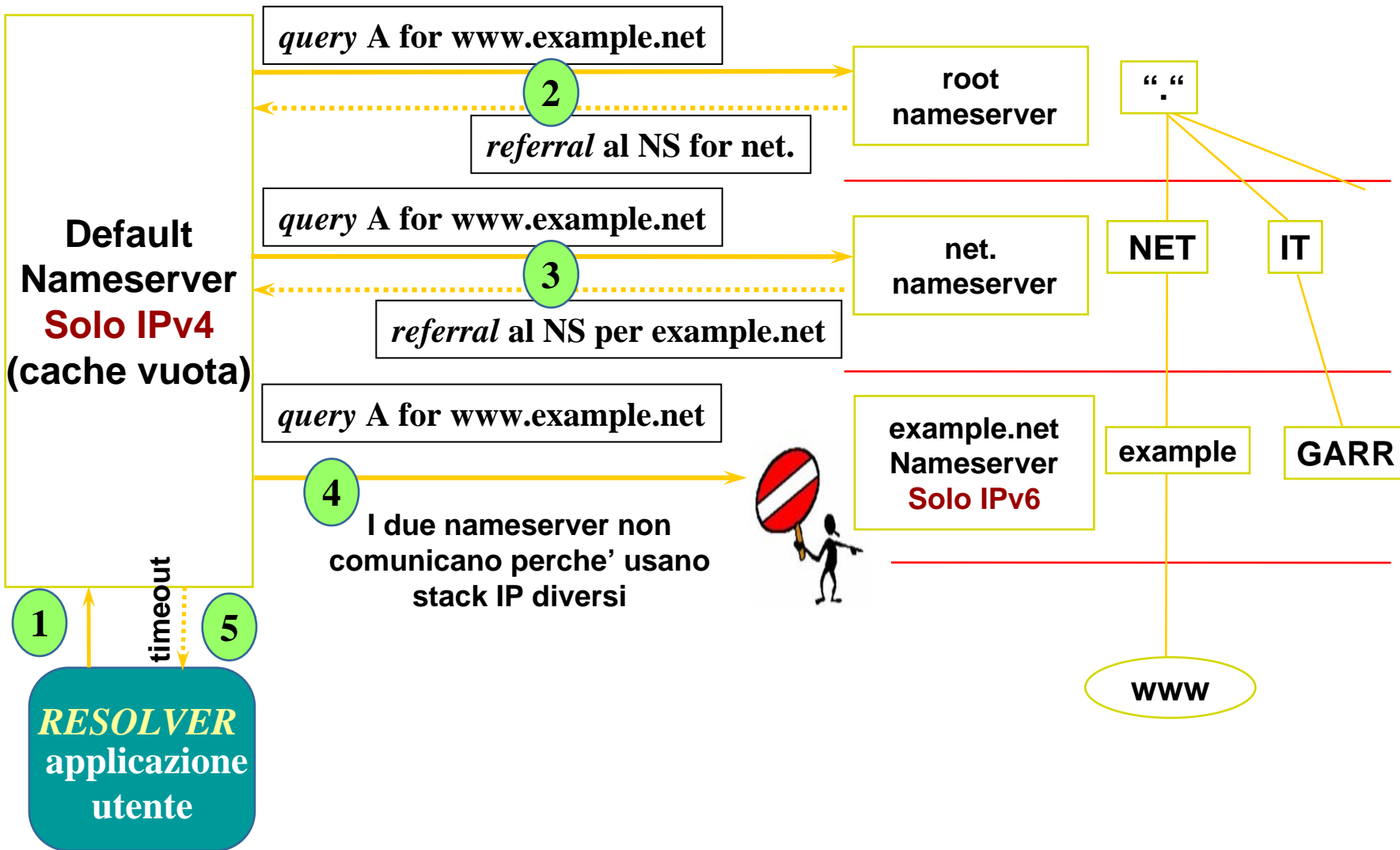
Requisiti operativi del DNS su IPv6 e raccomandazioni (1)

- L'obiettivo (allo stato attuale) **NON** e' quello di una netta transizione da un sistema basato solo su IPv4 ad un sistema poggiato esclusivamente su IPv6
- Per arrivare a questo risultato occorre:
 - Cominciare testando il DNS su IPv6 su una piccola rete
 - Il server (gli hosts) deve supportare IPv6 (in dual stack)
 - Il software DNS che si utilizza deve supportare IPv6
 - **NON** DISTRUGGERE quello che certamente funziona bene: il DNS su IPv4 in produzione!

Requisiti operativi del DNS su IPv6 e raccomandazioni (2)

- Evitare la **frammentazione** dello spazio dei nomi [RFC 3901]
 - Configurare nameserver in grado di trasportare i dati del DNS solo su IPv6 **NON** e' una buona politica perche' frammenta lo spazio dei nomi che ha da sempre funzionato solo su IPv4.
- Le linee guida del trasporto del DNS su IPv6 raccomandano di:
 - configurare i nameserver che si amministrano sempre in **dual-stack** o al piu' solo in IPv4. E' buona regola **evitare** di configurare nameserver **solo** su trasporto **IPv6**.
 - Rendere **autoritativo** di ogni zona che si amministra **almeno un nameserver raggiungibile solo su IPv4** in modo che quelle zone siano visibili su tutto lo spazio dei nomi

Esempio di frammentazione



Tools per il troubleshooting

dig ed nslookup per IPv6

- Sia con dig che con nslookup e' possibile fare query al DNS su records IPv6.
 - dig non è interattivo; si utilizza da *linea di comando*; restituisce risposte ricche di informazioni alle query fatte ai nameserver ma e' possibile ottenere anche output piu' brevi
 - nslookup lo si può utilizzare sia in modalità interattiva che tramite riga di comando

Esempio di query su IPv6 con dig

```
dig @2001:760:ffff:ffff::aa -x 2001:760:ffff:b0::34
```

```
; <<>> DiG 9.4.2-P2 <<>> @2001:760:ffff:ffff::aa -x 2001:760:ffff:b0::34
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55808
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
;4.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.0.f.f.f.f.0.6.7.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
4.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.0.f.f.f.f.0.6.7.0.1.0.0.2.ip6.arpa. 259200 IN PTR mirror1.mirror.garr.it.

;; AUTHORITY SECTION:
0.0.f.f.f.f.0.6.7.0.1.0.0.2.ip6.arpa. 259200 IN NS ns2.garr.net.
0.0.f.f.f.f.0.6.7.0.1.0.0.2.ip6.arpa. 259200 IN NS ns1.garr.net.
0.0.f.f.f.f.0.6.7.0.1.0.0.2.ip6.arpa. 259200 IN NS nlsrv.garr.net.

;; ADDITIONAL SECTION:
ns1.garr.net.      86400 IN      A       193.206.141.38
ns1.garr.net.      86400 IN      AAAA    2001:760:ffff:ffff::aa
ns2.garr.net.      86400 IN      A       193.206.141.42
ns2.garr.net.      86400 IN      AAAA    2001:760:ffff:ffff::ba

;; Query time: 1 msec
;; SERVER: 2001:760:ffff:ffff::aa#53(2001:760:ffff:ffff::aa)
;; WHEN: Sun May 24 11:11:20 2009
;; MSG SIZE rcvd: 278
```

Esempio di query su IPv6 con dig (2)

- E' possibile eseguire query per ottenere output piu' semplici:

```
dig mirror1.mirror.garr.it CNAME +short  
bo.mirror.garr.it.
```

```
dig mirror1.mirror.garr.it AAAA +short  
bo.mirror.garr.it.  
2001:760:ffff:b0::34
```

Esempio di query su IPv6 con nslookup (1)

```
#nslookup
> set query=any
> 0.6.7.0.1.0.0.2.ip6.arpa
Server:      193.206.141.38
Address:     193.206.141.38#53

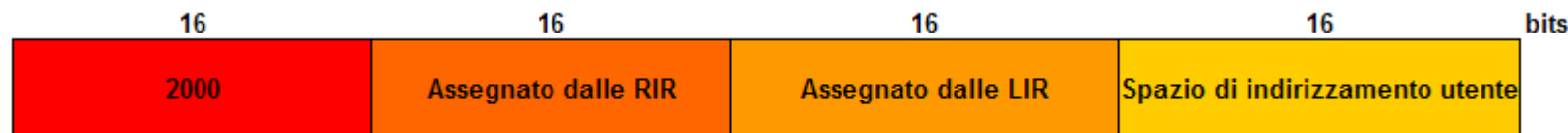
0.6.7.0.1.0.0.2.ip6.arpa
  origin = ns1.garr.net
  mail addr = staff-dns.garr.it
  serial = 2008051501
  refresh = 21600
  retry = 3600
  expire = 1814400
  minimum = 10800
0.6.7.0.1.0.0.2.ip6.arpa      nameserver = ns2.garr.net.
0.6.7.0.1.0.0.2.ip6.arpa      nameserver = ns.ripe.net.
0.6.7.0.1.0.0.2.ip6.arpa      nameserver = ns1.garr.net.
```


L'indirizzamento IPv6 per gli Enti GARR

Allocazione Spazio IPv6

- Le Regional Internet Registries (RIR) hanno adottato una politica comune per l'allocazione di spazio di indirizzamento IPv6 alle Local Internet Registries (LIR)
- Le RIR assegnano alle LIR una /32 da cui poi vengono estratti i prefissi da assegnare agli utenti finali.

Suddivisione dello spazio IPv6 routabile



Struttura dello spazio di indirizzamento IPv6 Global Unicast

- La prima stringa esadecimale (2000) rappresenta l'intero spazio routabile (2000::/3 ovvero 2000 - 3FFF). Viene assegnato da IANA alle RIR [RFC 1881].
- Nella seconda vengono definite le varie "sotto-classi" amministrare dalle RIR
 - <http://www.iana.org/assignments/ipv6-unicast-address-assignments/>
- La terza stringa definisce la suddivisione dello spazio IPv6 (/32) allocato dalle RIR alle varie Local Internet Registries (LIR) che a loro volta andranno ad assegnare agli utenti finali con prefissi di grandezza /48.
- Nella quarta stringa vengono definiti gli identificativi delle varie subnet ricavabili dalle /48 assegnate agli utenti finali dalle LIR.

Allocazione IPv6 al GARR-LIR

- La /32 assegnata al GARR-LIR e' una delle 512 subnet estratte dalla 2001:600::/23 che costituisce una delle classi IPv6 amministrata da RIPE

```
inet6num: 2001:760::/32
netname: IT-GARR-20011004
descr: GARR Italian Academic and Research Network
country: IT
org: ORG-GIRa1-RIPE
admin-c: EV182-RIPE
tech-c: GL965-RIPE
status: ALLOCATED-BY-RIR
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: GARR-LIR
mnt-routes: GARR-LIR
source: RIPE
```

- Dalla 2001:760::/32 GARR-LIR estrae le varie sotto-classi /48 da assegnare agli Enti facenti parte della comunita' GARR.

Registrazione sul DB RIPE

- Ogni /48 assegnata agli Enti GARR dal GARR-LIR viene registrata sul database di RIPE esattamente come avviene per IPv4

```
inet6num:    2001:760:4000::/48
netname:     CNR-PI-IPv6-NET
descr:       CNR Pisa
country:     IT
admin-c:     EV182-RIPE
tech-c:      GL965-RIPE
tech-c:      MS12905-RIPE
status:      ASSIGNED
mnt-by:      GARR-LIR
changed:     bataloni@garr.it 20080325
source:      RIPE
```

Delega sotto l'ip6.arpa

- GARR-LIR, una volta ottenuta l'allocazione di spazio di indirizzamento IPv6, ha registrato del database RIPE un template per la delega dell'intera zona della /32 allocata in cui vengono indicati i nameserver autoritativi.

```
domain:      0.6.7.0.1.0.0.2.ip6.arpa
descr:       Reverse delegation for GARR sub-tla
admin-c:     EV182-RIPE
tech-c:      GL965-RIPE
zone-c:      GL965-RIPE
zone-c:      GP4562-RIPE
nserver:     ns1.garr.net
nserver:     ns2.garr.net
nserver:     ns.ripe.net
mnt-by:      GARR-LIR
changed:     paolini@garr.it 20030228
changed:     paolini@garr.it 20060728
source:      RIPE
```

Aggiornamento dati reverse-lookup

- Per le /48 assegnate agli utenti non e' necessario registrare domain object nel database RIPE.
- Le deleghe verso i nameserver autoritativi delle utenze vengono definite nel file di zona dell'intera /32 gestita da GARR-LIR

Aggiornamento deleghe per il reverse-lookup

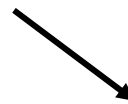
- Le richieste di aggiornamento delle deleghe per il reverse devono essere inviate via email al GARR-LIR (staff-dns@garr.it).
- Il GARR-LIR controlla la corretta configurazione del DNS.
- IL GARR-LIR provvede a configurare la delega sul nameserver GARR autoritativo della 32 allocata da RIPE a GARR verso i nameserver autoritativi della /48.

Piano di Indirizzamento IPv6 Enti GARR

- L'intera /32 allocata da RIPE al GARR-LIR e' stata suddivisa in 16 /36
- Ogni /36 e' stata a sua volta suddivisa in 16 /40.
- Dalle 256 /40 cosi' ottenute, ne sono state scelte alcune ed assegnate una per regione.
- Ad ogni Ente GARR afferente ai PoP facenti parte della stessa regione viene assegnata una /48.

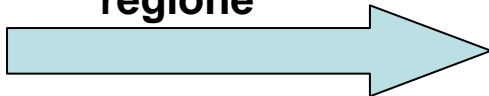
Piano di Indirizzamento IPv6 Enti GARR

Intero spazio di indirizzamento IPv6 GARR



2001:760::/32				
2001:0760::/36	2001:0760:1000::/36	...	2001:0760:e000::/36	2001:0760:f000::/36
2001:0760::/40	2001:0760:1000::/40	...	2001:0760:e000::/40	2001:0760:f000::/40
2001:0760:0100::/40	2001:0760:1100::/40	...	2001:0760:e100::/40	2001:0760:f100::/40
2001:0760:0200::/40	2001:0760:1200::/40	...	2001:0760:e200::/40	2001:0760:f200::/40
2001:0760:0300::/40	2001:0760:1300::/40	...	2001:0760:e300::/40	2001:0760:f300::/40
2001:0760:0400::/40	2001:0760:1400::/40	...	2001:0760:e400::/40	2001:0760:f400::/40
2001:0760:0500::/40	2001:0760:1500::/40	...	2001:0760:e500::/40	2001:0760:f500::/40
2001:0760:0600::/40	2001:0760:1600::/40	...	2001:0760:e600::/40	2001:0760:f600::/40
2001:0760:0700::/40	2001:0760:1700::/40	...	2001:0760:e700::/40	2001:0760:f700::/40
2001:0760:0800::/40	2001:0760:1800::/40	...	2001:0760:e800::/40	2001:0760:f800::/40
2001:0760:0900::/40	2001:0760:1900::/40	...	2001:0760:e900::/40	2001:0760:f900::/40
2001:0760:0a00::/40	2001:0760:1a00::/40	...	2001:0760:ea00::/40	2001:0760:fa00::/40
2001:0760:0b00::/40	2001:0760:1b00::/40	...	2001:0760:eb00::/40	2001:0760:fb00::/40
2001:0760:0c00::/40	2001:0760:1c00::/40	...	2001:0760:ec00::/40	2001:0760:fc00::/40
2001:0760:0d00::/40	2001:0760:1d00::/40	...	2001:0760:ed00::/40	2001:0760:fd00::/40
2001:0760:0e00::/40	2001:0760:1e00::/40	...	2001:0760:ee00::/40	2001:0760:fe00::/40
2001:0760:0f00::/40	2001:0760:1f00::/40	...	2001:0760:ef00::/40	2001:0760:ff00::/40

/40 assegnate per regione



Tools online (e non) per il subnetting IPv6

- <http://www.liquidalchemy.com/liquidalchemy/>
- <http://www.ipv6calculator.net/>
- ipcalc e sipcalc: tools per il subnetting IPv4 e IPv6.
 - Si usano da linea di comando
 - Forniscono output sia classfull che CIDR
 - Generazione di reverse (utile per IPv6)
- Per l'installazione su Linux:
 - `$ sudo apt-get install sipcalc ipcalc`

Esempi di output con sipcalc

```
$ sipcalc 2001:760::/64  
-[ipv6 : 2001:760::/64] - 0
```

[IPV6 INFO]

```
Expanded Address      - 2001:0760:0000:0000:0000:0000:0000:0000  
Compressed address   - 2001:760::  
Subnet prefix (masked) - 2001:760:0:0:0:0:0:0/64  
Address ID (masked)  - 0:0:0:0:0:0:0:0/64  
Prefix address       - ffff:ffff:ffff:ffff:0:0:0:0  
Prefix length        - 64  
Address type         - Aggregatable Global Unicast Addresses  
Network range        - 2001:0760:0000:0000:0000:0000:0000:0000 -  
                      2001:0760:0000:0000:ffff:ffff:ffff:ffff
```

Esempi di output con sipcalc

```
$ sipcalc 2001:760:4000::/48 --v6split=64 | grep Network | awk ' {print $3}' | more
```

```
2001:0760:4000:0000:0000:0000:0000:0000  
2001:0760:4000:0001:0000:0000:0000:0000  
2001:0760:4000:0002:0000:0000:0000:0000  
2001:0760:4000:0003:0000:0000:0000:0000  
2001:0760:4000:0004:0000:0000:0000:0000  
2001:0760:4000:0005:0000:0000:0000:0000  
2001:0760:4000:0006:0000:0000:0000:0000  
2001:0760:4000:0007:0000:0000:0000:0000  
2001:0760:4000:0008:0000:0000:0000:0000  
2001:0760:4000:0009:0000:0000:0000:0000  
2001:0760:4000:000a:0000:0000:0000:0000  
2001:0760:4000:000b:0000:0000:0000:0000  
2001:0760:4000:000c:0000:0000:0000:0000  
2001:0760:4000:000d:0000:0000:0000:0000  
2001:0760:4000:000e:0000:0000:0000:0000  
2001:0760:4000:000f:0000:0000:0000:0000  
2001:0760:4000:0010:0000:0000:0000:0000
```

.....

Contatti

E-mail del GARR-LIR: lir@garr.it

Staff DNS: staff-dns@garr.it

Tel.: +39-06.4962.2550

Fax: +39-06.4962.2044

Buon Lavoro...

- <http://www.isc.org>: Bind
- <http://www.ietf.org/rfc.html>
- <http://www.iana.org>: IANA
- <http://www.icann.org>: ICANN
- <http://www.nic.it>: Registro
- <http://www.eurid.eu>: EUR*id*
- <http://www.dns.net/dnsrd/>: DNS Resources Directory
- <http://www.bind9.net/>
- <http://www.icann.org/en/committees/security/sac018.pdf>
- <http://www.6diss.org/tutorials/dns.pdf>

