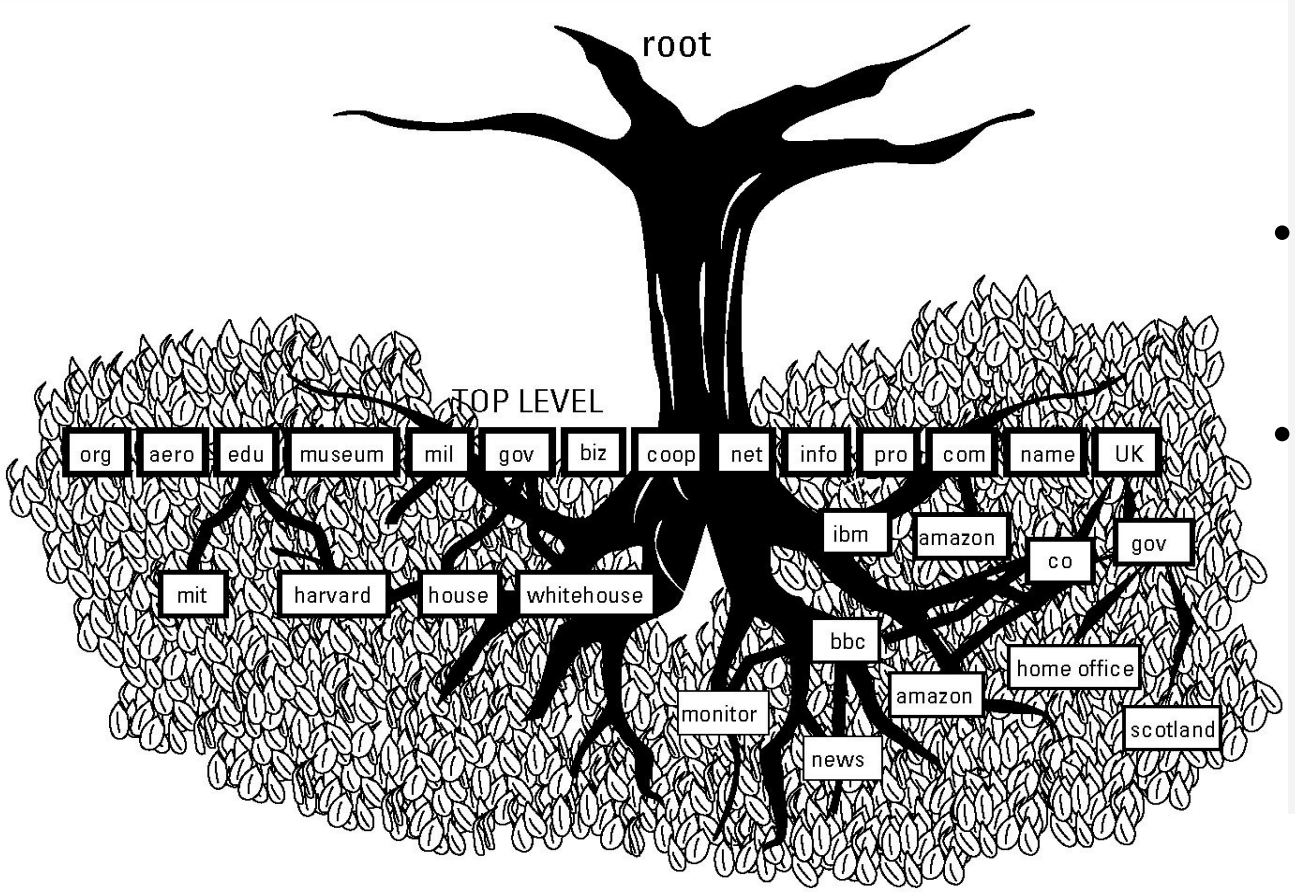
Servizi NIC e LIR
Tutorial sul DNS
(Prima Parte)

Vincenzo Puglia (Consortium GARR) | 01/10/2025

Argomenti trattati

- Servizi NIC e LIR (domini e indirizzi IP)
- Introduzione al DNS
- Processo di risoluzione dei nomi - diretta e inversa
- Files e Configurazioni su BIND
- I tools per il troubleshooting su DNS

Il servizio GARR-NIC Network Information Center



- Il GARR è il Registrar di tutti gli Enti facenti parte della comunità della ricerca e dell'istruzione Italiana.
- Ogni organizzazione autorizzata all'accesso al GARR può richiedere nomi a dominio al GARR NIC
- La registrazione di un dominio in modalità sincrona consente al GARR-NIC di portare a termine, in tempo reale, sia le procedure di aggiornamento dei domini già registrati che di registrazione di nuovi nomi a dominio, senza dover richiedere all'Ente registrante l'invio di alcuna documentazione cartacea al Registro.

Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

GARR-NIC: il registrar del GARR

- Registra nomi a dominio esclusivamente sotto i ccTLD
  - **.it**
  - **.eu**
  - Gli Enti collegati alla Rete della Ricerca che tramite GARR registrano nomi a dominio di secondo livello, non devono pagare la quota annuale. **I costi di registrazione** e mantenimento dei SLD **rientrano nella convenzione del servizio di accesso alla Rete GARR**
  - A partire dal 2018 accreditamento del GARR-NIC come Registrar per la registrazione di nomi a dominio sotto .**edu.it** per le scuole connesse alla Rete GARR

Registrazione di un nome a dominio con GARR-NIC

- Il GARR-NIC registra nuovi nomi a dominio solo per persone giuridiche, mai per persone fisiche

- Per registrare un nuovo nome a dominio ".it", ".eu" o "edu.it" occorre:

- Scaricare il modulo di registrazione per la Richiesta e Mantenimento di un dominio
  - ***https://www.servizi.garr.it/garr-nic/documenti-di-registrazione/domini-it***

- Inviare la richiesta di registrazione firmata dall'APA dell'Ente richiedente la registrazione

- Le richieste di registrazione per un nuovo nome a dominio ".it" o ".eu" vanno inviate via mail a nic@garr.it e in copia a segreteria@garr.it

Dati di registrazione

- Dati dell'Ente richiedente il dominio (**registrant**)
- Il riferimento amministrativo del dominio (**admin-c**)
- Il riferimento tecnico del dominio, ovvero l' APM o chi si occupa della gestione del DNS (**tech-c**)

- All'interno del modulo, è disponibile la sezione dedicata ai **nameserver autoritativi** della zona del nome a dominio che si intende registrare. Occorre indicare il nameserver primario e almeno un nameserver secondario. Se non si dispone di un nameserver secondario, si può richiedere a GARR di utilizzare il servizio di DNS secondario

- Il DNS deve essere configurato in modo conforme alle specifiche indicate nell'rfc1912

Operazioni sui domini

- Modificare il Registrar, il Registrant, o entrambi
  - **Trasferire** un nome a dominio *da un Registrar commerciale a GARR (o viceversa)*
  - **Cambiare** il **Registrant** Ente assegnatario del nome a dominio

- **Aggiornare** i dati di un dominio registrato

- **Cancellare** un nome a dominio

Procedura di cambio Registrar, Registrant

- Utilizzare lo stesso modulo valido per la richiesta di registrazione domini

- Per il **cambio Registrar o per il cambio Registrant + Registrar** è necessario indicare, nel modulo di richiesta, il codice **auth-info** (da richiedere al registrant da cui si intende trasferire il dominio). Inviare la richiesta a nic@garr.it e a segreteria@garr.it

- **Cambio Registrant tra Enti GARR**: compilare il modulo *selezionando l'operazione di "Cambio Registrant"*. Inviare la richiesta via email a nic@garr.it e a segreteria@garr.it, aggiungendo in copia APA e APM di entrambi gli Enti GARR coinvolti

- Per tutte le suddette procedure occorre configurare il DNS, eventualmente fare richiesta del servizio di nameserver secondario

Aggiornamento informazioni dei domini registrati

- Una volta registrato un dominio, i dati registrati **non vengono aggiornati automaticamente** dal GARR-NIC **ma solo su richiesta da parte dell'Ente registrante**

- Il riferimento amministrativo di un nome a dominio (admin) non sempre coincide con l'APA (Access Port Administrator)

- I dati dell'admin in molti casi non sono presenti nel sistema informativo GARR
  - Per questo, **l'aggiornamento dei riferimenti amministrativi e tecnici** dei domini già registrati deve essere esplicitamente richiesto **via email scrivendo a nic@garr.it**

Registro IT ed EURid

- I dati registrati presso il database del Registro*it* e di EUR*id* possono essere consultati via **whois**, che può essere utile anche per verificare se un determinato nome a dominio è libero e quindi registrabile

- Da linea di comando:

  whois -h whois.nic.it {*nome a dominio*}

  whois -h whois.eu {*nome a dominio*}

- Oppure via web alle seguenti URL:

  https://web-whois.nic.it/

  http://www.eurid.eu/en/whois-search

Il Cybersquatting

Supporto agli utenti per la **riassegnazione** di un nome a dominio, in seguito ad attività illecite come il Cybersquatting

Cosa è il Cybersquatting (1)

- **Attività illegale** di chi si appropria di nomi a dominio corrispondenti a marchi commerciali altrui o a nomi di personaggi famosi o di Enti Pubblici o Privati **al fine di realizzare un lucro sul trasferimento del dominio** a chi ne abbia interesse o un danno a chi non lo possa utilizzare.

- Pratica diffusissima negli Stati Uniti, ha avuto un notevole sviluppo anche in Italia, specialmente in seguito all'entrata in vigore nel 1999 della regola che consente ai titolari di partita IVA la registrazione di un numero illimitato di domini.

Cybersquatting: cosa fare? (2)

- Il problema si è concentrato sui domini .it. Gli Enti GARR sino ad ora più colpiti da Cybersquatting sono le Università Statali.

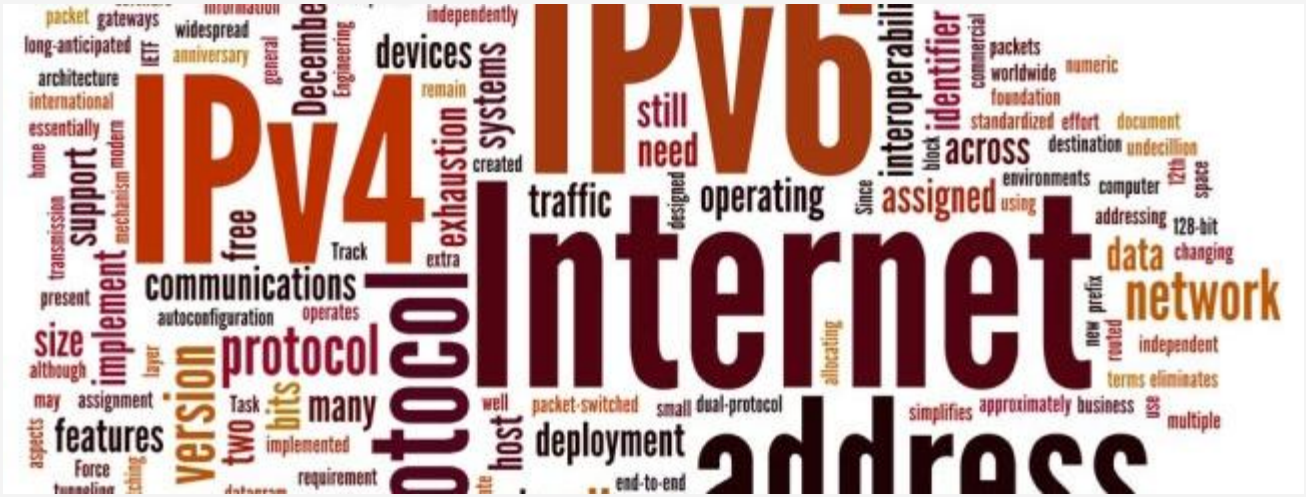
- Il Registro italiano del ccTLD .it mette a disposizione dei Registrant la **Procedura di Opposizione**. Essa "congela" l'assegnazione del dominio fino alla soluzione della controversia e consente a chi l'ha promossa di esercitare un diritto di prelazione sull'eventuale nuova assegnazione.

- Altra procedura che si può tentare è quella della **Verifica dei Requisiti Soggettivi**: si tratta di chiedere al potenziale *cybersquatter* di provare la veridicità dei suoi dati registrati nel database del Registro. Se questa verifica non viene portata a termine si revoca il nome a dominio che potrà essere riassegnato in favore dell'Ente vittima

Cybersquatting: cosa fare? (3)

- Nel caso dei domini .eu, EUR*id* non può intervenire in alcuna controversia
- Qualora i dati del registrante non fossero visibili su whois, fare una richiesta di **divulgazione dei dati personali**, compilando un apposito modulo fornito da EURid e inviandolo a **legal@eurid.eu**
- Se il registrante non intende liberare il nome a dominio oggetto di disputa può essere avviata una **procedura ADR (Risoluzione extragiudiziale delle controversie .eu)**.
- Le procedure ADR (Alternative Dispute Resolution) sono gestite dalla **Corte di Arbitrato Ceca (CAC) e dal Centro di Arbitrato e Mediazione (WIPO)** sono meccanismi alternativi alla giustizia ordinaria. Tutto avviene online tramite piattaforma dedicata (durata circa 4-6 mesi).
- Per informazioni più dettagliate sulle procedure ADR, consultare i siti web delle due Organizzazioni di riferimento:
  - http://eu.adr.eu/
  - http://www.wipo.int/amc/en/domains/

Il servizio di Local Internet Registry del GARR



Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Il progetto ARPA

- Il progetto ARPA (*Advanced Research Projects Agency)* venne avviato negli Stati Uniti nel 1959 in risposta al lancio della sonda sovietica Sputnik, avvenuto l'anno precedente.

- Obiettivo: mantenere le capacità tecnologiche statunitensi al passo, e possibilmente all'avanguardia

- Nel progetto di ricerca ad ampio raggio, che coinvolse vari ambiti di studio, vennero incluse anche le reti informatiche
  - ARPANET (Advanced Research Projects Agency Network)

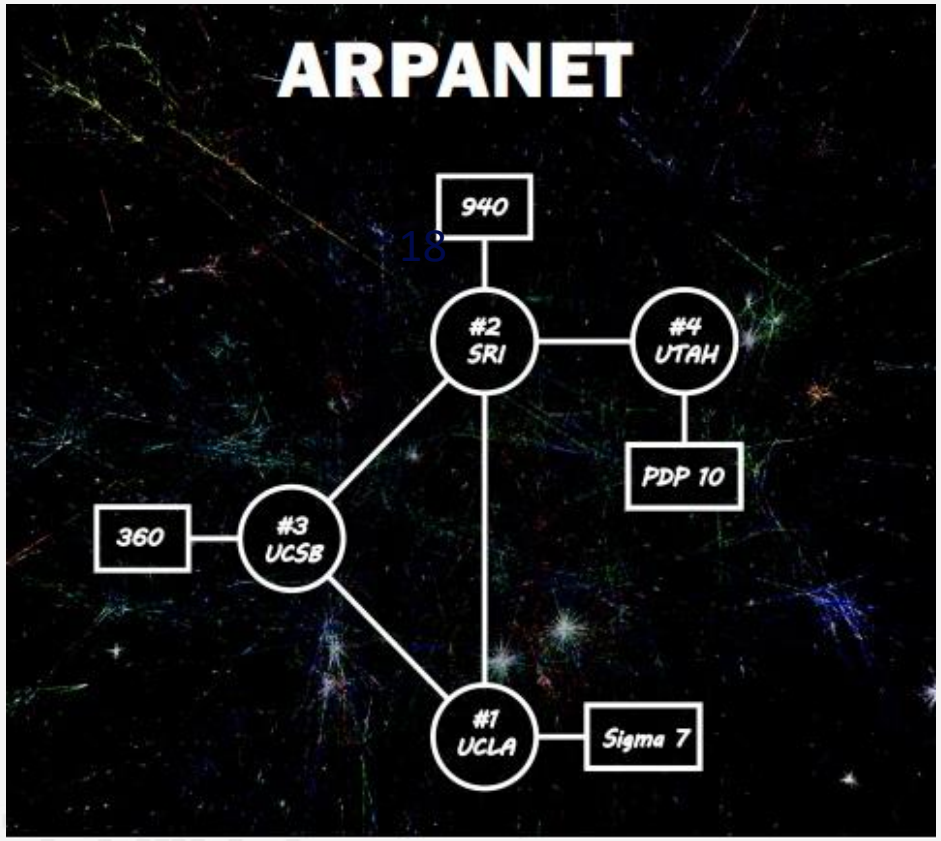
Il primo calcolatore collegato ad ARPANET

- L'SDS Sigma 7 a 32-bit realizzato dalla Scientific Data Systems nel 1966
- Il primo Sigma 7 venne installato presso la UCLA University, California, Los Angeles
- Si trattava di una macchina molto ingombrante, molto rumorosa, molto pesante ma soprattutto molto costosa
- Per questa ragione, uno dei primi aspetti da gestire e risolvere fu come condividere risorse tra le Università.

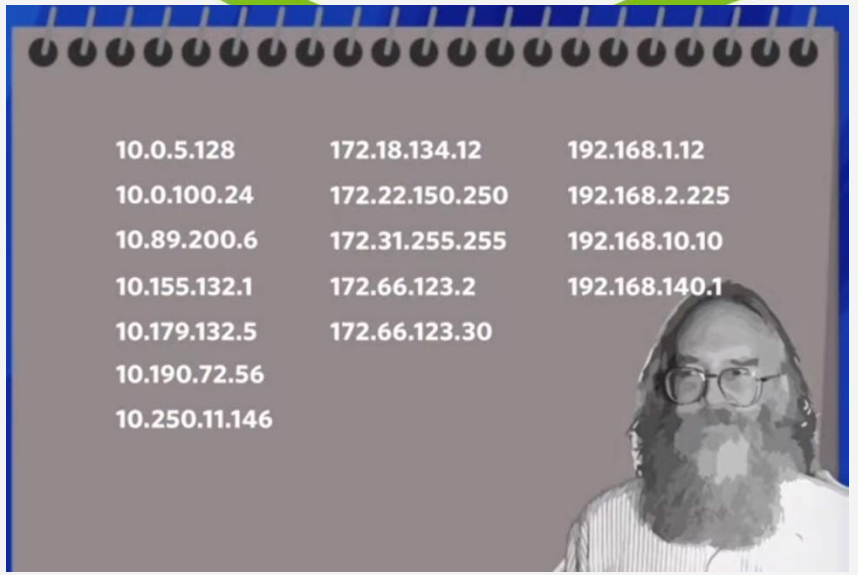
Il primo router: Interface Message Processor (IMP)

- Fu il primo router connesso ad ARPANET, prodotto dalla Bolt, Beranek and Newman

Vennero aggiunti 2 nodi: l'Università della California Santa Barbara (UCSB) e quella dello Utah



Jonathan Bruce Postel



- Prima della nascita ufficiale di **IANA (Internet Assigned Numbers Authority)**, **Jon Postel assegnava manualmente gli indirizzi IP e i numeri di protocollo**, spesso **annotandoli su un semplice quaderno o agenda cartacea**.

Negli anni '70, Internet (allora chiamata ARPANET) era ancora una rete sperimentale, usata da poche università e centri di ricerca.
Jon Postel era considerato la persona di riferimento per tutto ciò che riguardava la numerazione e l'organizzazione delle risorse di rete.
Quando qualcuno aveva bisogno di un **blocco di indirizzi IP** o di un **numero di porta o protocollo**, semplicemente gli scriveva o lo chiamava, e lui **registrava l'assegnazione nel suo taccuino personale**.
Questa storia è diventata quasi **leggendaria**, ma è ben documentata e confermata da molti colleghi dell'epoca.

IANA (Internet Assigned Numbers Authority)

- **Authority** fondata nel 1972, con mandato governativo degli Stati Uniti d'America.
- E' l'organizzazione che sovrintende all'**allocazione globale degli indirizzi IP**(solo IPv4) e di **Autonomous System Numbers** (AS)

I Regional Internet Registries

- Poiché tra la fine degli anni 80 e inizio 90 Internet cominciò a svilupparsi e ad espandersi velocemente in tutto il mondo, fu chiaro che IANA non potesse essere l'unica Authority a gestire lo spazio di indirizzamento pubblico per tutto il mondo
- Nel 1992 l'Internet Engineering Task Force (**IETF**) **decise che le risorse IPv4 dovessero essere amministrate, per aree geografiche**, da organizzazioni no profit: i **Regional Internet Registries**

Cosa è un Regional Internet Registry (RIR)

- E’ un'organizzazione che sovrintende all‘allocazione e alla registrazione delle risorse IP in una specifica area geografica. In particolare si occupa di gestire l’assegnazione di un determinato spazio di indirizzamento IPv4 ed Asn.

- IANA ha allocato spazio di indirizzamento pubblico ad ogni RIR sulla base delle necessità dell’area geografica che amministrano

L'Operatività dei RIR per aree geografiche

RIRs operate in large, geopolitical regions that are continental in scope. Currently, there are five RIRs:

AFRINIC	Serving Africa	Founded in 2005
APNIC	Serving the Asia Pacific region	Founded in 1993
ARIN	Serving North America	Founded in 1997
LACNIC	Serving South America and the Caribbean	Founded in 2001
RIPE NCC	Serving Europe, Central Asia and the Middle East	Founded in 1992

ICANN (Internet Corporation for Assigned Names and Numbers)

- Ente statunitense, con peso politico maggiore, istituito il 18 settembre 1998 con incarico di:
  - **assegnare gli indirizzi IP e AS**
  - **gestire il protocollo del sistema dei nomi a dominio di primo livello** (Top-Level Domain) generici (*g*TLD), dei country code (*cc*TLD) **e** dei **root servers**.
  - Per approfondimenti, al seguente link è disponibile lo statuto di ICANN (versione italiana): https:
  - //www.icann.org/resources/pages/bylaws-2012-02-25-it
- Da quel momento **IANA diventa un dipartimento di ICANN**
- ICANN trasferisce le responsabilità a livello operativo a IANA

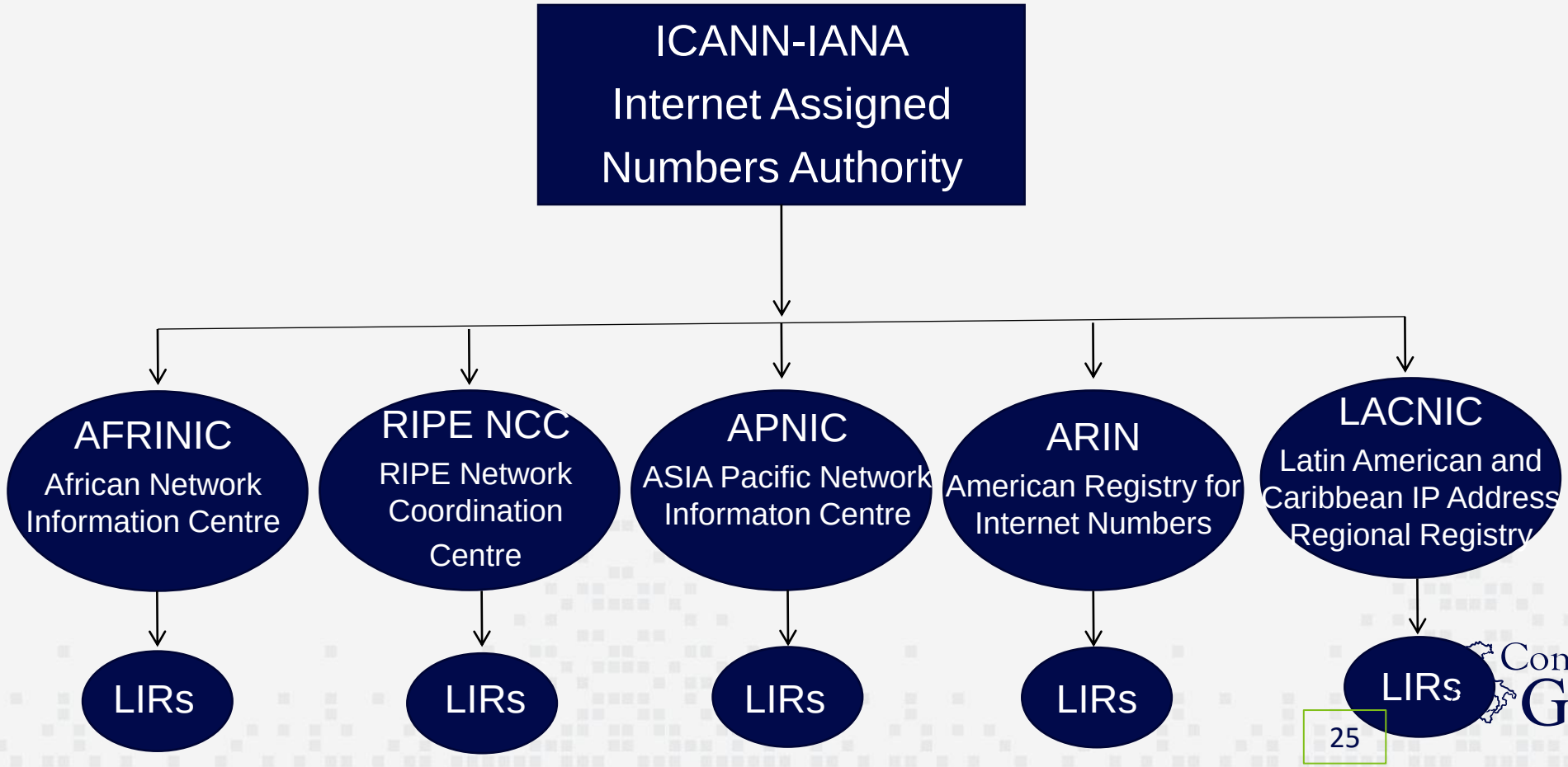
Cosa è un LIR

- Un **Local Internet Registry** (LIR) è un'organizzazione alla quale è stato assegnato un blocco di indirizzi IP e AS (Autonomous System) da un RIR che a sua volta ne controlla l'utilizzo.
- La maggior parte dei LIR sono fornitori di servizi Internet.
- Per essere LIR è richiesta l'appartenenza ad un RIR

- **Cosa fa un LIR:**
  - *Assegna le risorse IP* (allocate dal RIR) ai propri utenti;
  - *Gestisce il rapporto tra utenti finali e il RIR*;
  - *Mantiene i dati relativi alle risorse IP* assegnate alle proprie utenze all'interno del *database del RIR di appartenenza.*

La “Gerarchia” tra le Authorities

- I cinque RIR (RIPE NCC, APNIC, ARIN, LACNIC,AfriNIC) ricevono spazio di indirizzamento da IANA (Internet Assigned Numbers Authority) e a loro volta assegnano spazio IP ai LIR



GARR-LIR – IP address

Assegnazione di spazio IP dal GARR-LIR

GARR-LIR assegna nuovo spazio di indirizzamento:

- a tutte le Entità che rappresentano la Comunità Accademica e della Ricerca Scientifica italiana;
- alle Università e istituzioni culturali e/o scientifiche straniere con sede in Italia e per le quali esistono accordi con il Governo Italiano;
- alle scuole collegate alla Rete GARR

L'assegnazione viene fatta sulla base delle reali necessità di indirizzamento da parte degli utenti

L'Ente richiedente dovrà fornire informazioni riguardo alla struttura della propria rete locale.

- Utilizzo dello spazio IP attualmente assegnato
- Requisiti dello spazio IP richiesto
- Sviluppi futuri della rete

Classi IPv4 PI, PA e Legacy

- Le classi IPv4 registrate presso RIPE si differenziano, in base ai così detti status, in Provider Aggregàtable (PA), Legacy e Provider Indipendent (PI)

- Le **reti PA** vengono allocate dai RIR ai LIR. I LIR a loro volta assegnano *range* di spazio di indirizzamento di tipo PA all'utente finale

- Tutte le risorse IP (indirizzi IPv4 ed ASn) assegnate agli utenti finali prima o al di fuori dell'attuale sistema di registri Internet strutturato in RIR, sono risorse **Legacy**

- Le **reti PI** vengono invece assegnate dai RIR direttamente all'utente finale

Le classi IP GARR per indirizzamento utente

- Classi PA:
  - 90.147.0.0/16
  - 185.191.180.0/22 (backbone GARR-T)
  - 192.167.0.0/16
  - 193.204.0.0 - 193.206.255.255 (/15)
  - 212.189.128.0/17

- Classe Legacy per le scuole:
  - 138.41.0.0/16 (ex CRAI)

- Indirizzamento IPv6:
  - 2001:760::/32

Whois database

- Una volta **assegnato lo spazio di indirizzamento all'utente finale il GARR-LIR registra la risorsa IP** nel database del RIR (per IPv4 oggetto: **inetnum**)
- I dati registrati possono essere consultati mediante whois
- Per ricevere i dati dal whois di RIPE si interroga l'host whois.ripe.net

```
# whois –h whois.ripe.net {indirizzo IP}
```

- I dati possono essere controllati anche via web:

https://apps.db.ripe.net/db-web-ui/query

Oggetto Inetnum

193.204.0.0/24

inetnum: 193.204.0.0 - 193.204.0.255
netname: IEOMI02
descr: IRCCS IEO - Milano
country: IT
org: ORG-IEDO2-RIPE
admin-c: AF17462-RIPE
tech-c: GB18077-RIPE
status: ASSIGNED PA
remarks: This prefix is statically assigned
remarks: To notify abuse mailto: cert@garr.it
remarks: GARR - Italian academic and research network
mnt-by: GARR-LIR
mnt-irt: IRT-GARR-CERT
created: 2002-09-02T11:09:04Z
last-modified: 2023-07-19T14:56:45Z
source: RIPE

31

Perché si registrano le risorse IP nel RIPE DB?

- Una delle principali **attività del GARR-LIR è quella di mantenere aggiornate le informazioni** amministrative relative alle classi di indirizzamento pubblico IPv4/v6 registrate **presso RIPE NCC**

- **In caso di incidenti di sicurezza su IP GARR**, è indispensabile che le informazioni delle persone indicate sul database di RIPE come responsabili di tali IP siano aggiornate, al fine di **consentire al GARR-CERT**, il Computer Emergency Response Team della comunità dell'istruzione e della ricerca, **la gestione di incidenti di sicurezza** informatici in cui siano coinvolti IP assegnati ad Enti collegati alla Rete GARR

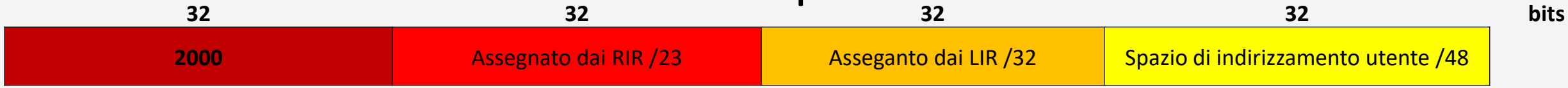
Allocazione spazio IPv6 da ICANN/IANA ai RIR

Prefix	Designation	Date	WHOIS	Status
2001:0200::/23	**APNIC**	**1999**-07-01	whois.apnic.net	ALLOCATED
2001:0400::/23	**ARIN**	1999-07-01	whois.arin.net	ALLOCATED
...				
2001:1200::/23	**LACNIC**	2002-11-01	whois.lacnic.net	ALLOCATED
...				
2001:4200::/23	**AFRINIC**	2004-06-01	whois.afrinic.net	ALLOCATED
...				
2002:0000::/16	6to4	2001-02-01		ALLOCATED
...				
2a00:0000::/12	**RIPE NCC**	2006-10-03	whois.ripe.net	ALLOCATED
2c00:0000::/12	AFRINIC	**2006**-10-03	whois.afrinic.net	ALLOCATED

Allocazione Spazio IPv6 ai LIR

- I RIR hanno adottato una politica comune per l'allocazione di spazio di indirizzamento IPv6 ai LIR
- I **RIR assegnano ai 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

Idealmente tutto lo spazio IPv6 **Global Unicast** può essere suddiviso in **quattro parti da 32 bit**. La prima parte costituisce l'intero spazio routabile (2000::/3 ovvero 2000 - 3FFF).

Nella seconda vengono definite le varie "sotto-classi" amministrate dai RIR **(/23), assegnato da IANA ai RIR** [RFC 1881].

- http://www.iana.org/assignments/ipv6-unicast-address-assignments/

La **terza** parte definisce la suddivisione dello spazio IPv6 **(/32) allocato dai RIR ai vari Local Internet Registries (LIR).**

Nella **quarta** stringa vengono definiti gli identificativi delle varie subnet **/48** (o aggregati più piccoli ricavabili dalle /48) **assegnate dai LIR agli utenti finali**.

Una **/48 corrisponde a 65.536** [(2^16) **/64**]. **Ogni /64 contiene 2^64** (18.446.744.073.709.551.616) **indirizzi IPv6** (18 trilioni)

A questo link è disponibile un tool per il calcolo del subnetting IPv6 :

http://www.gestioip.net/cgi-bin/subnet_calculator.cgi

Allocazione IPv6 al GARR-LIR

- La **/32 IPv6 assegnata al GARR-LIR** è una delle subnet estratte dalla 2001:600::/23 che costituisce una delle classi IPv6 amministrate da RIPE. Da cui GARR-LIR estrae le /48 per gli utenti.

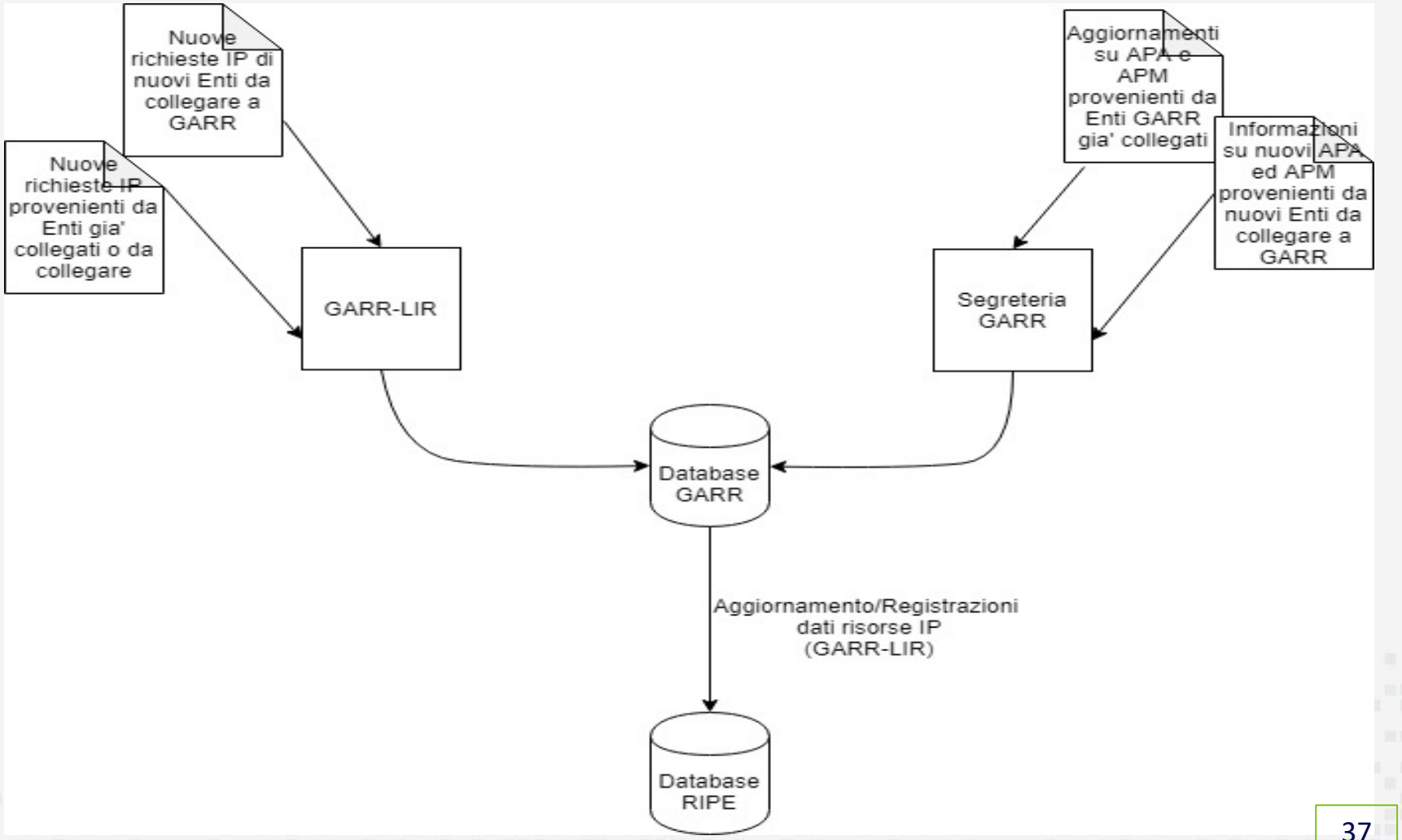
inet6num: 2001:760::/32
netname: IT-GARR-20011004
country: IT
org: ORG-GIRa1-RIPE
admin-c: GL965-RIPE
tech-c: GL965-RIPE
status: ALLOCATED-BY-RIR
mnt-by: RIPE-NCC-HM-MNT
mnt-by: GARR-LIR
mnt-routes: GARR-LIR
created: 2007-07-18T11:48:38Z
last-modified: 2017-02-21T13:08:32Z
source: RIPE

Registrazione dello spazio IPv6 nel DB RIPE (1)

- **Ogni /48 assegnata agli Enti** GARR dal GARR-LIR viene registrata sul database di RIPE esattamente come avviene per la /24 in IPv4 (inetnum) - **oggetto inet6num**

```
inet6num:       2001:760:422c::/48
netname:        INFN-RM1-TIER2-IPv6
descr:          INFN - Roma1
country:        IT
org:            ORG-INDF53-RIPE
admin-c:        ADS829-RIPE
tech-c:         CB12166-RIPE
status:         ASSIGNED
remarks:        This prefix is statically assigned
remarks:        To notify abuse mailto: cert@garr.it
remarks:        GARR - Italian academic and research network
mnt-by:         GARR-LIR
created:        2020-03-09T08:54:00Z
last-modified:  2023-09-13T07:02:14Z
source:         RIPE
```

Flusso dei dati per aggiornamento/registrazioni IP



1 - Domande

- Qual è la differenza tra LIR e RIR?
- Cosa posso fare se qualcuno registra un nome a dominio .it usando il nome istituzionale della mia organizzazione?
- Perché è importante registrare i dati nel DB di RIPE?

Assistenza su DNS per gli Enti GARR

I principali task svolti dal GARR-NIC/LIR su DNS

- Registrazione dei domini di secondo livello (.it , .eu e .edu.it)
  - Aggiorna le deleghe dei domini di secondo livello presso il Registro IT ed EUR*id* *(nameserver: Primario e Secondario/i)*

- Servizio di DNS secondario (su richiesta)
  - Non vi sono costi aggiuntivi per richiederne l'attivazione

- Fornisce supporto agli Enti GARR sul troubleshooting su DNS
  - Segnala agli APM eventuali anomalie rilevate sulla configurazione del DNS

- Nel caso di IPv4/IPv6 vengono aggiornate le zone di reverse lookup

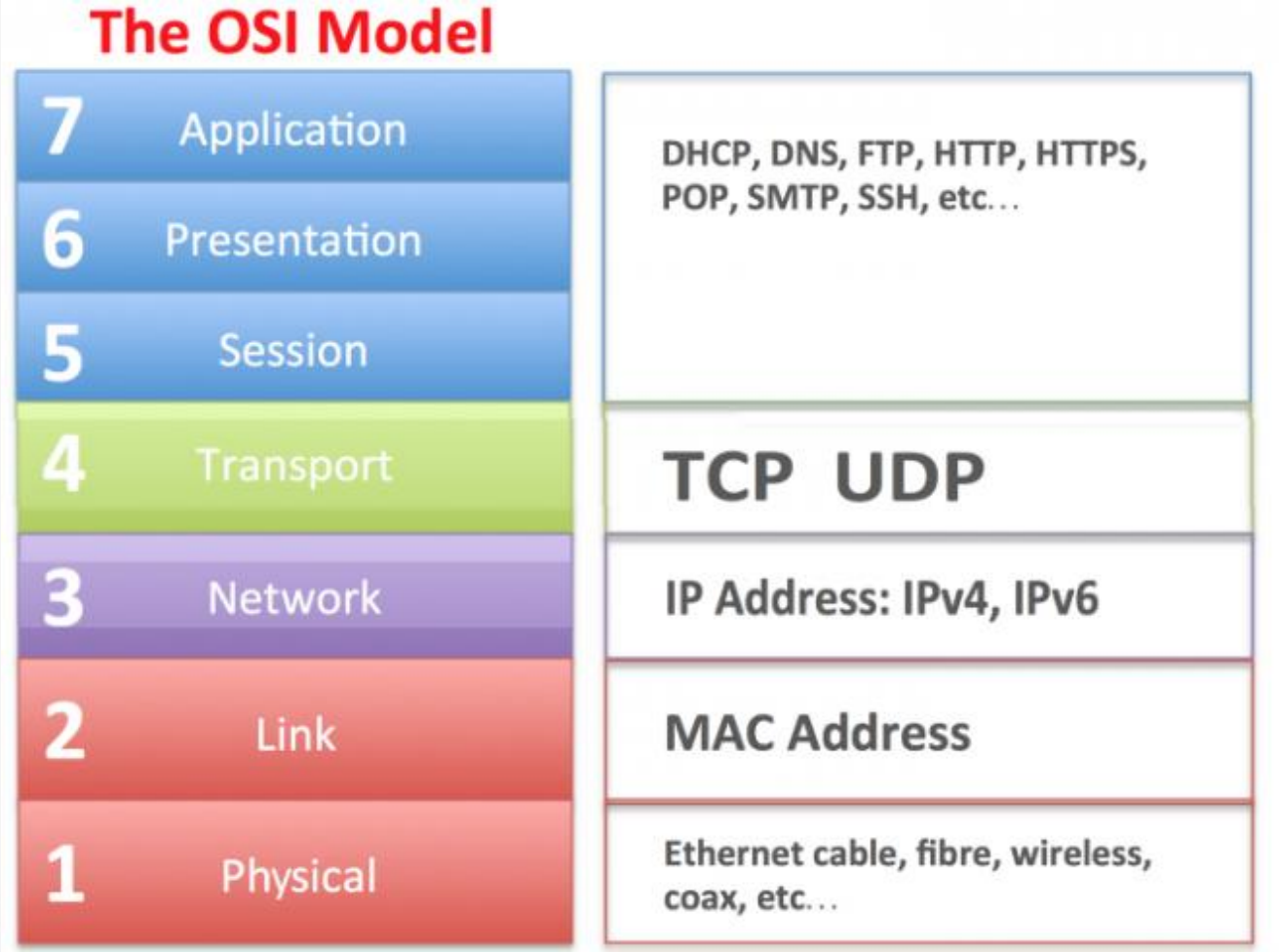
Introduzione al DNS

A cosa serve il DNS (1)

- Il DNS permette di associare un nome *Human-readable* ad un host (IP), più semplice da ricordare rispetto ad un indirizzo IP.
- L'univocità nella **determinazione dell'host** attraverso tale sistema è garantita mediante **l'adozione di una struttura gerarchica "a domini" per la quale ciascun host appartiene ad un dato dominio "registrato" ufficialmente in un database distribuito**.
- Es: www.garr.it individua una macchina il cui nome è www appartenente al dominio garr che è a sua volta parte del dominio (country code TLD) it .
- Il principio è simile a quello dell'elenco telefonico

Se avessimo un elenco di numeri di telefono senza nomi sarebbe molto complicato trovare quello giusto…

Il DNS nella Pila ISO/OSI



Le queries vengono trasportate in UDP su porta 53

Risposte :

- Dim. < 512 bytes : UDP porta 53
- Dim. > 512 bytes : TCP porta 53
  - Con EDNS il trasporto può avvenire su UDP anche per message > 512 bytes

Quando la dimensione della risposta supera la dimensione massima del pacchetto DNS, il server tronca la risposta e imposta il bit TC nell'header del pacchetto DNS.

Con il bit TC il server comunica al client di riprovare la query in TCP

Trasferimenti di zona :

- **TCP porta 53**

Il modello OSI è uno standard per la progettazione delle reti, rappresentato da una pila di protocolli suddivisa in 7 livelli, i quali insieme eseguono tutte le funzionalità della rete

Risoluzione diretta e inversa

Nel protocollo standard DNS vengono individuate e distinte 2 tipologie di risoluzioni:

- Risoluzione diretta:

Corrispondenza nome host – indirizzo IP

www.example.com IN A 192.168.0.1

- Risoluzione inversa:

Corrispondenza indirizzo IP – nome host

1.0.168.192.in-addr.arpa. IN PTR www.example.com.

DNS: caratteristiche principali

Il DNS consente ad ogni organizzazione che ha accesso ad Internet di:

- **amministrare la relazione tra nomi e indirizzi IP** del proprio dominio **in maniera autonoma**
- **risolvere i nomi** fuori del proprio dominio **accedendo alle informazioni gestite da altre organizzazioni**

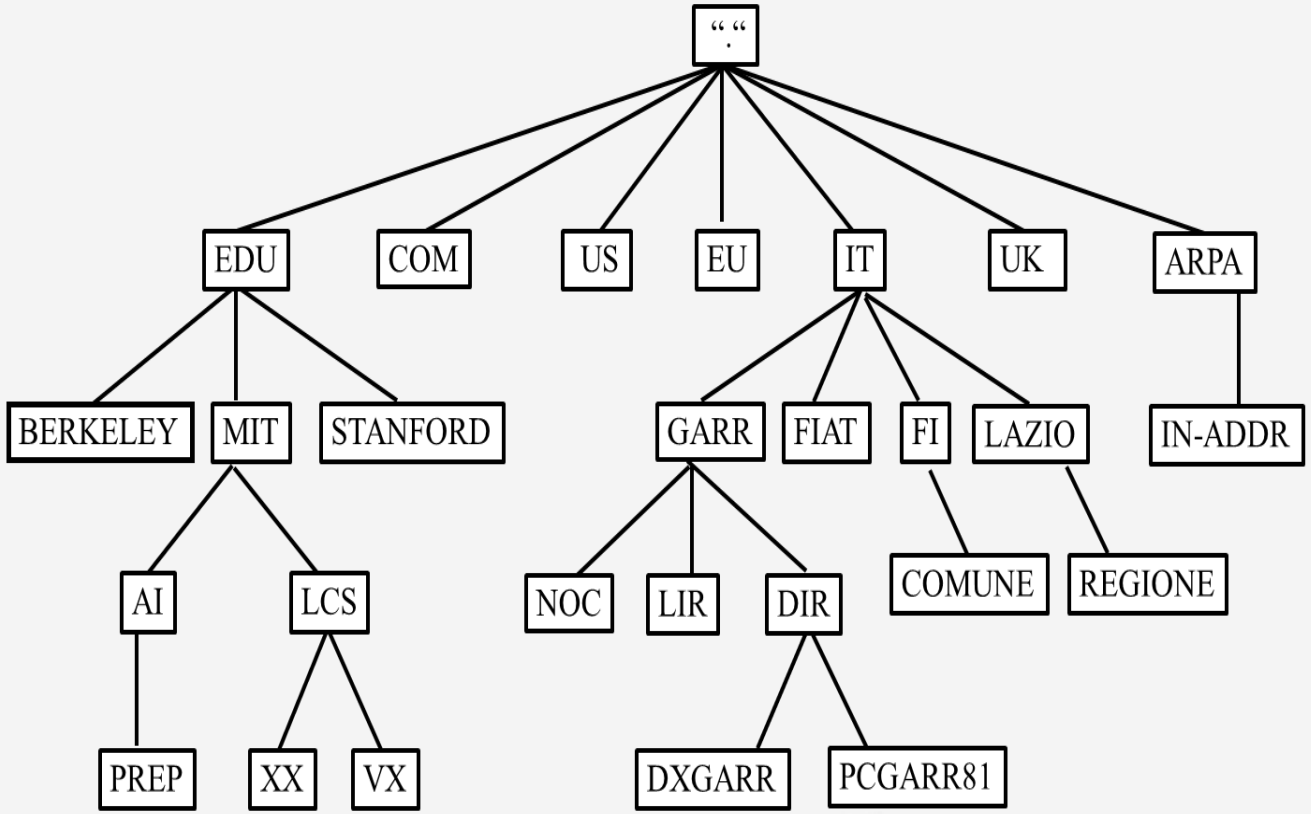
- Suddivisione gerarchica in domini
- Struttura ad albero rovesciato
- Dinamicamente consistente e coerente nei dati che amministra
- In grado di gestire vari tipi di records e dati
- Basato sul modello client/server

DNS: Struttura gerarchica

- Root (.)
- Top-Level Domains (**g**TLDs, **cc**TLD e **sponsored**TLC) come .com, .org, .net**;** .it, .uk, .de, .es**;** .gov, .edu, .museum **.**
- Nomi di dominio secondari (es. example.com, garr.it, infn.it).
- Sottodomini (es. blog.example.com, noc.garr.it). Fino ad arrivare agli fqdn (Fully Qualified Domain Name).
- Lista dei TLD:

  http://www.iana.org/domains/root/db

L’albero dei nomi



- Tutti i nomi a dominio esistenti su Internet in realtà terminano con un “.” (punto): lir.*garr.it.*
- Un nome a dominio viene analizzato **da destra verso sinistra** rispetto a come si scrive, ciascun nameserver fornisce informazioni soltanto sull'elemento che si trova a sinistra dell'ultimo punto.
- La stringa vuota che segue il punto finale è chiamata *dominio radice* (DNS root zone);

RIGHT-TO-LEFT

Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

Root nameserver (1)

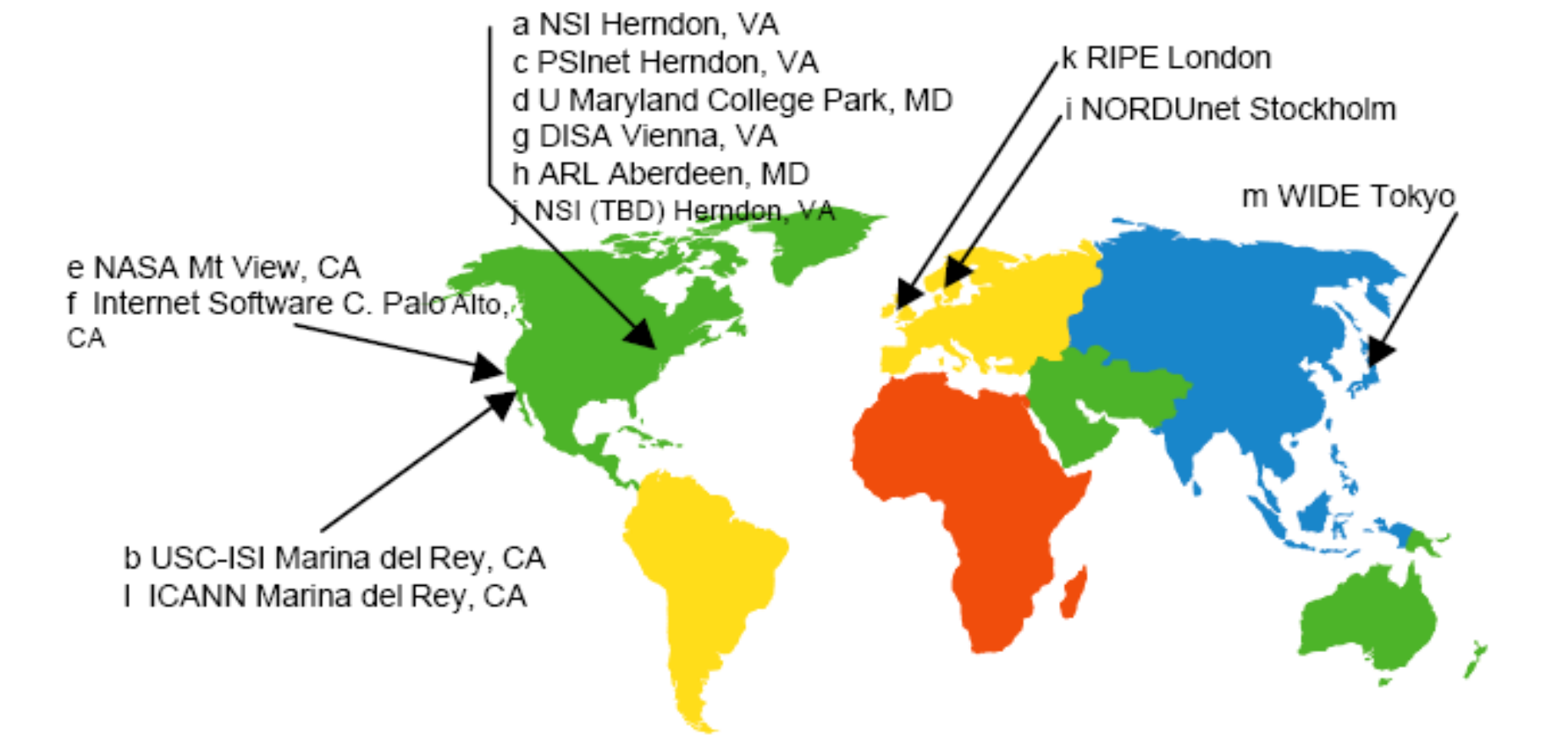
- I root nameserver sono i server responsabili (autoritativi) delle informazioni relative al dominio ".";
- Possiedono l'elenco dei server responsabili per ognuno dei domini di primo livello riconosciuti, e lo forniscono in risposta a ciascuna richiesta.
- Contengono anche le informazioni per la risoluzione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

Root nameserver (2)

Sono 13 nameservers controllati e gestiti da 12 differenti organizzazioni

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Root nameserver (3)



Root nameserver replicati (1)

- La ISC (Internet Systems 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. Ora ci sono oltre 1400 istanze dei 13 root nameserver in tutto il mondo

- Presupposti:
  - Configurare NS cloni da un master/primary server che contengano gli stessi dati (files);
  - Metodo Anycast (1 nome = 1 indirizzo IP = medesime informazioni) che consente di spostare l'univocità dal livello globale della Rete a solo parti di essa. **Raggiungibilità solo ad una porzione ristretta della Rete globale**.

Root nameserver replicati (2)

- **Le repliche** dei root nameserver **sono** state **installate in punti nevralgici** di Internet
  - Presso il NAMEX a Roma, la MIX a Milano ed altri Interner Exchange
    - **Presso MIX: repliche di I-root, K-root e J-root**
    - **Presso NAMEX: repliche di F.root, J.root**
- Vantaggi per gli ISP afferenti agli Internet Exchange: tempi di risposta più bassi per le richieste rivolte ai root NS.
- La raggiungibilità di queste repliche è possibile solo a questi Providers e non al di fuori delle loro reti.

Mappa dei root nameservers

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Processo di risoluzione dei nomi

Nameserver

Un **Name Server è un host** appartenente ad un dominio **che contiene tutti i record** (corrispondenze nomi-indirizzi e/o viceversa) **di tale dominio**

Ovvero il nameserver di un dato dominio **contiene il database locale** relativo a **quel dominio**, che è un **sottoinsieme del database globale**

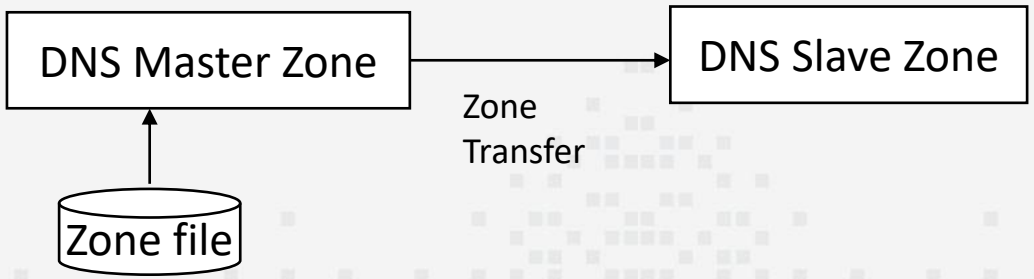
Un nameserver può essere configurato in vari modi:

- autoritative, root, master, slave, forwarders, ricorsivo, non ricorsivo…

Nameserver primari e secondari

- Per ogni dominio viene definito un Nameserver Primario e almeno un Secondario. Un nameserver si definisce **primario (master) quando possiede i file** delle informazioni ("file di zona") con tutti i records **della zona**. In ogni zona vi sarà un solo nameserver primario (accesso in lettura e scrittura alle info del database)
- Un nameserver si definisce **secondario (slave) quando acquisisce dal nameserver primario** (quindi ha una copia in sola lettura**) i dati relativi alla zona**, mediante una procedura automatica denominata "zone-transfer"
  - i parametri che regolano il funzionamento della procedura sono contenuti in uno specifico record del nameserver primario (record Start Of Authority - SOA)

- E' necessario valutare attentamente il numero e la dislocazione dei nameserver secondari in modo da ridurre il più possibile il rischio che problemi di connessione possano impedire la risoluzione dei nomi di un dominio (configurazione fault tolerant)



Query «non-recursive» o «recursive»

Se un name server riceve una query per un dominio che non gestisce **direttamente** sono possibili due opzioni:

1. Il name server può rispondere al client indicando un altro name server che sia in grado di rispondere in modo appropriato. *[Non riccorsivo]*

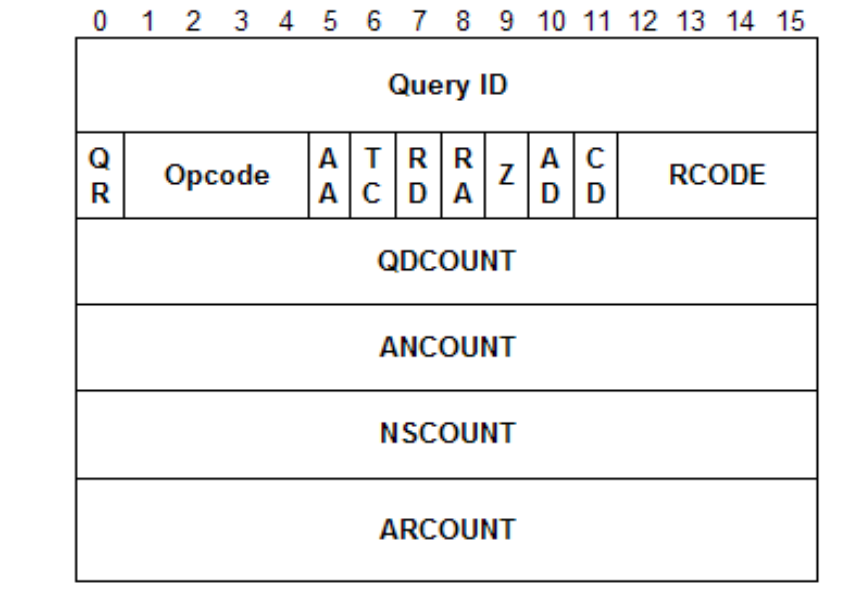
2. Il name server può cercare di risolvere in modo completo la richiesta attraverso una serie di richieste agli altri name servers, fino ad aver completato la risoluzione della richiesta. *[Ricorsivo]*

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” è **diviso in cinque sezioni**

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

Formato dell'Header (12 bytes)

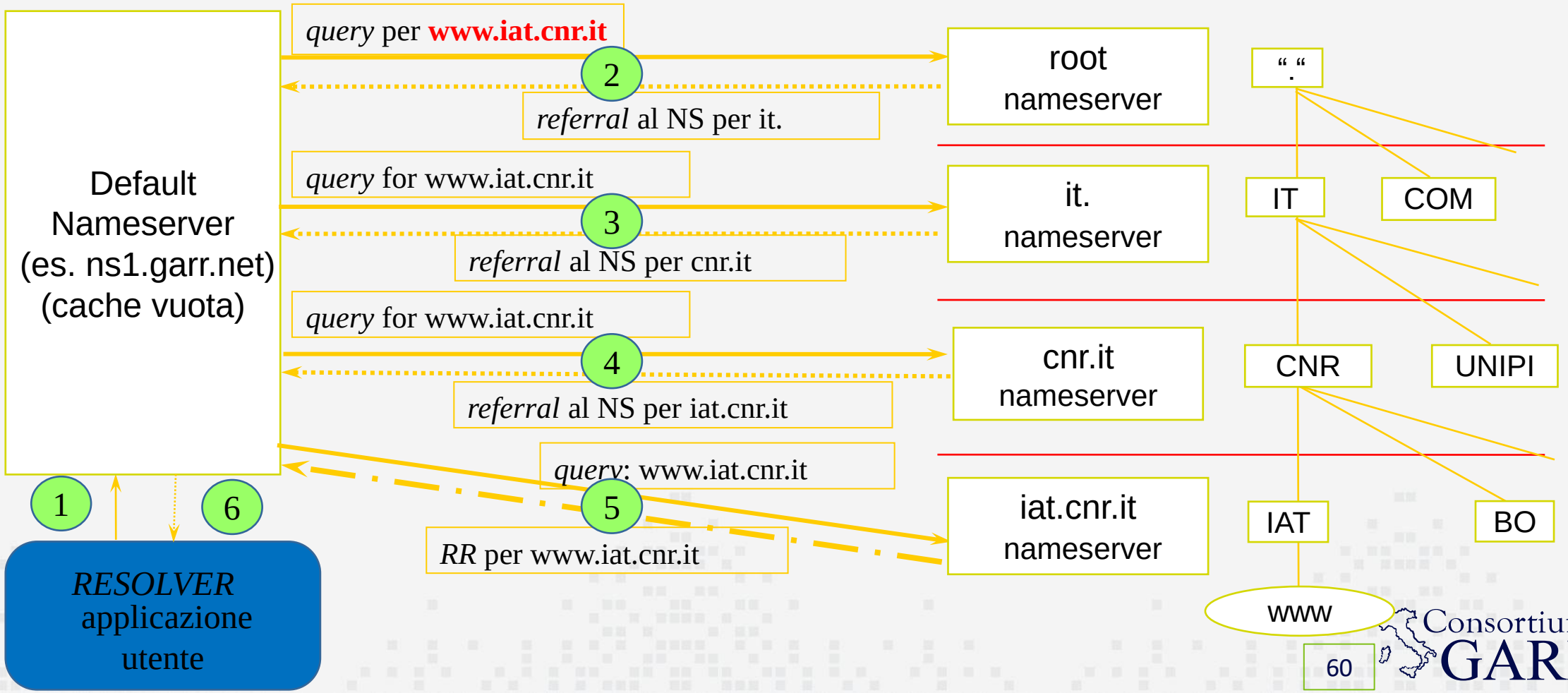


- Query ID: identificativo a 16 bits assegnato dal resolver che genera la query. Campo copiato; nella risposta corrispondente e serve al match tra domanda e risposta alla query fatta;
- QR: Campo a 1 bit che specifica se il messaggio è una domanda(0) o una risposta (1);
- OPcode: campo a 4 bits specifica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

- RD: Recursion Desired, predispone il nameserver a gestire la query in maniera ricorsiva, 1 bit;
- RA: Recursion Available, indica che la gestione ricorsiva della query è disponibile sul nameserver, 1 bit;
- Z: riservato ad usi futuri. Deve essere zero in tutte le domande e risposte, 1 bit;
- RCODE: definisce l'esito della risposta (no error, format error…), 4bits;
- QDCOUNT: indica il numero di entries nella sezione Question, 16bits;
- ANCOUNT: indica il numero di RR presenti nella sezione Answer 16bits;
- NSCOUNT: specifica il numero di NS indicati nella sezione Autority 16bits;
- ARCOUNT: indica il numero di RR nella sezione Additional 16bits;

Processo di risoluzione dei nomi

Quando un name server non è autoritativo di un nome a dominio per il quale viene interrogato e non dispone di quell'informazione nella propria cache deve necessariamente rivolgersi ai Root Name Servers per ottenerla

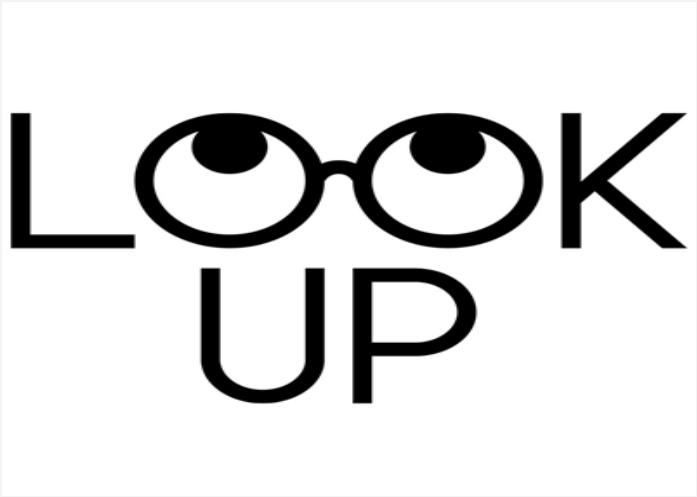


Il Reverse Lookup

- Corrispondenza tra indirizzi IP e nomi a dominio.
  - utilizzato da tools per troubleshooting sulla rete come traceroute o ping.

- Necessario per alcune applicazioni, ad esempio la posta elettronica.
  - Molti mail-server rifiutano posta la cui sorgente (mail-server da cui si riceve la mail) non ha un rDNS configurato.

- Responsabilità delle Local Internet Registry (LIR)
  - Le informazioni sul rDNS devono essere mantenute aggiornate nel DB di RIPE



L’albero per la risoluzione inversa (IPv4)

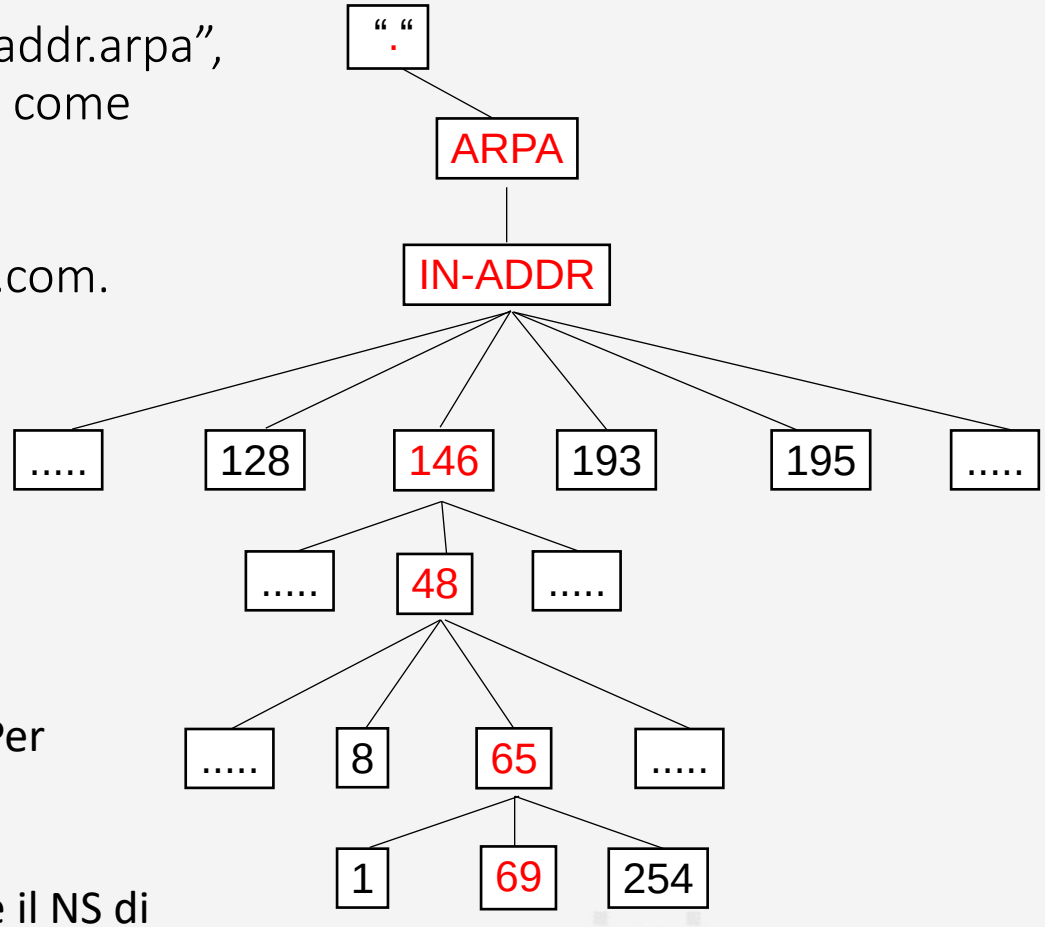
- Il reverse di un indirizzo IPv4 è espresso, nel dominio “in-addr.arpa”, da una sequenza di 4 bytes in ordine inverso, rappresentati come numeri decimali separati da un punto

- Es: 69.65.48.146.in-addr.arpa. IN **PTR** www.example.com.

48.146.in-addr.arpa

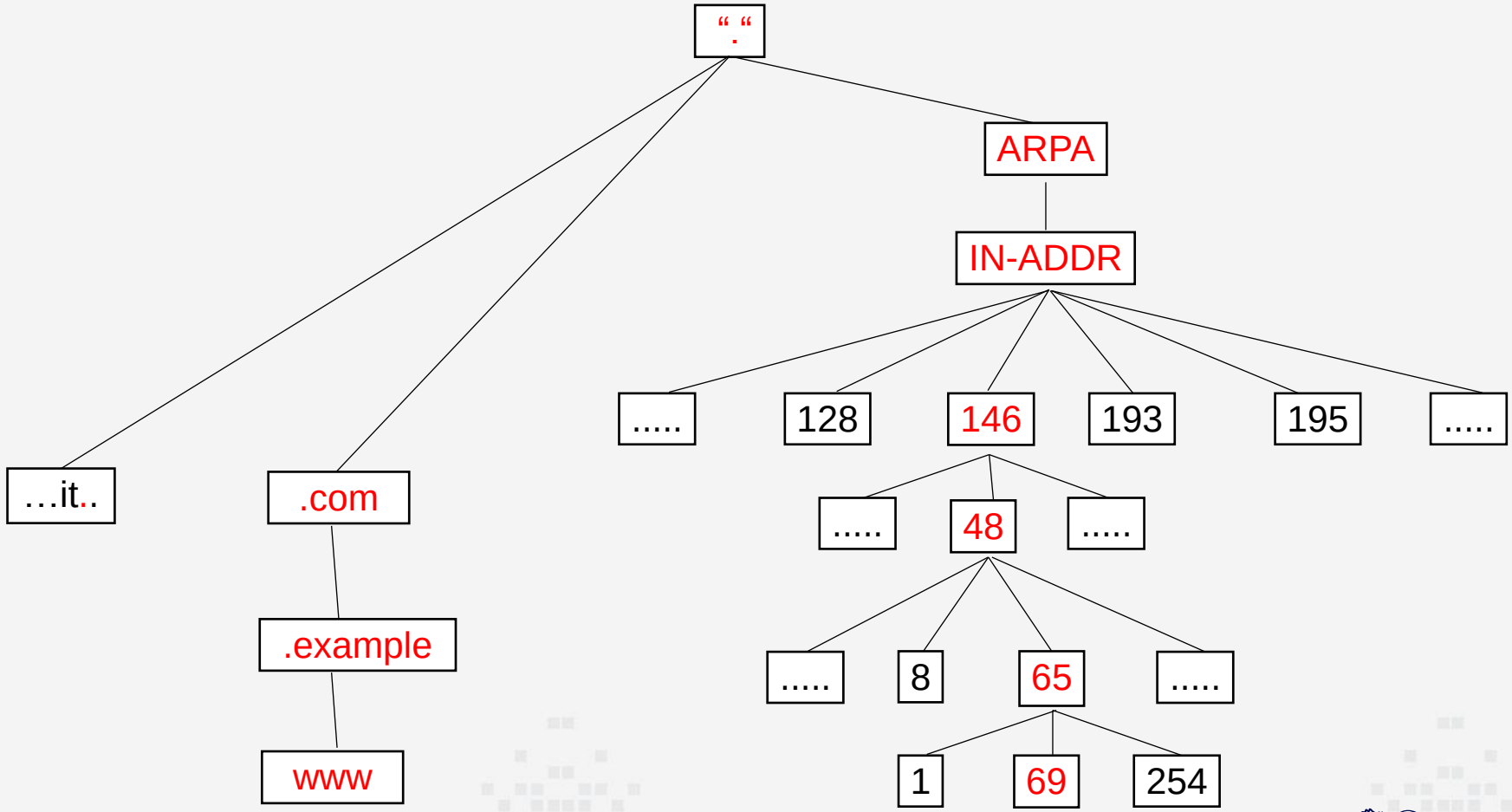
65.48.146.in-addr.arpa *dominio (/24)*

69.65.48.146.in-addr.arpa *macchina*



Es. NS1.GARR.NET riceve richiesta per il RR (il nome) di 146.48.65.69. Per raggiungere il ns autoritativo del RR, si rivolge al RootNS (.), .., che gli comunica il NS di riferimento della /16 (48.146.in-addr.arpa.)
Il NS della 48.146.in-addr.arpa, se non è autoritativo, comunica quale è il NS di riferimento della 65.48.146.in-addr.arpa (che è autoritativo per tutta la classe /24). Ha il file di zona con tuti i nomi inerenti a quella /24 compreso il nome della 146.48.65.69 (www.example.com.)

L’albero del DNS



Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Il Reverse Lookup – domain object

GARR-LIR, una volta ottenuta l'allocazione di spazio di indirizzamento e ogni volta che assegna spazio di indirizzamento ai propri utenti, registra nel database RIPE un **template per la delega della risoluzione inversa (domain object).** A sinistra l'oggetto domain della 192.167.0.0/16 (IPv4) e a destra dell'intera zona di reverse IPv6 2001:760::/32. Nel domain object vengono indicati i **nameserver autoritativi**.

domain: 167.192.in-addr.arpa
descr: GARR-Network
admin-c: GA1650-RIPE
tech-c: GL965-RIPE
zone-c: SM36651-RIPE
nserver: NS1.GARR.NET
nserver: NS2.GARR.NET
remarks:To notify abuse mailto: cert@garr.it
remarks:GARR - Italian academic and research network
mnt-by: GARR-LIR
created: 2006-10-09T12:58:28Z
last-modified: 2024-06-24T13:22:12Z
source: RIPE

domain: 0.6.7.0.1.0.0.2.ip6.arpa
descr: Reverse delegation for GARR
admin-c: EV182-RIPE
tech-c: GL965-RIPE
zone-c: GL965-RIPE
zone-c: GP4562-RIPE
nserver: ns1.garr.net
nserver: ns2.garr.net
mnt-by: GARR-LIR
source: RIPE

Files e Configurazioni su BIND

Hardware e Software del DNS

- **hardware**
  disponibile su quasi tutte le attuali piattaforme (PC, Macintosh, workstation, mainframe)

- **software**
  prodotti di pubblico dominio (**BIND** per Unix e Windows, MIND/NonSequitur per MacOS)
  prodotti commerciali (MacDNS, Windows server 2003)

  BIND v9 (Berkeley Internet Name Domain)
  è l'implementazione di nameserver più diffusa su Internet
  sviluppata per Unix BSD, ne esistono *porting* per molti altri ambienti
  spesso ne è inclusa una implementazione nel software di corredo di piattaforme come Unix

BIND e i suoi files

- il file named.conf
- il file localhost.rev
- il file named.root
- i files di **zona** per la risoluzione **diretta**
- i files di **zona** per la risoluzione **inversa**

Ogni file di zona contiene comandi (.soa) e Resource Record (A, PTR, NS, etc.)

Il file Named.conf

- il file *named.conf* è il file di configurazione principale per il funzionamento del processo nameserver dalla versione 9.x.y
  - **definisce le directory** in cui si trovano tutti i file necessari al funzionamento del nameserver *(directory)*
  - **definisce** la raccolta dei dati statistici relativi al processo nameserver ***(statistics-interval)***
  - **definisce i domini per i quali** il nameserver **è autoritativo** (**master e slave**)
  - **Definisce** (per i domini di cui siamo primari) **quali sono i** nameserver **secondari che possono prelevare le zone** per cui il nameserver è autoritativo ***(allow-transfer)***

Attenzione alla sintassi per i commenti (/ */, //, # invece di ;)*

Il file named.root

- **Contiene gli indirizzi IP dei server** DNS **di root** da cui attingere informazioni e deve essere posizionato nella directory: /var/named/etc/namedb
- E' possibile reperire la versione aggiornata del file da:

  ftp://ftp.rs.internic.net/domain/named.root.

Il file di zona e tipi di records

- Il file di zona contiene i riferimenti necessari **all'associazione tra i nomi delle macchine**, appartenenti ad una zona, **ed i loro indirizzi IP** (e viceversa).

- L'associazione è fatta mediante **specifici records** che descrivono le caratteristiche e le funzionalità del dominio e delle macchine che gli appartengono. I più importanti ed utilizzati sono:
  - SOA
  - NS
  - MX
  - A
  - CNAME
  - PTR

File di zona esempio (risoluzione diretta)

Formato di un file di zona diretta (risoluzione nome host – indirizzo):

```
$ORIGIN .
$TTL 86400      ; 1 day
example.garr.it     IN SOA  ns.example.garr.it. root.ns.example.garr.it. (
                            2025011601 ; serial
                            86400          ; refresh (1 day)
                            7200           ; retry (2 hours)
                            2592000        ; expire (4 weeks 2 days)
                            86400          ; ttl (1 day)
                            )
                    NS      ns1.garr.net.
                    NS      ns2.garr.net.
                    NS      ns.example.garr.it.
                    MX      0 ns.example.garr.it.
$ORIGIN example.garr.it.
srv01               A       192.168.0.1
pc01                A       192.168.0.2
lt01                A       192.168.0.3
```

Tipi di record – SOA

- **Serial**
  Corrisponde al numero di revisione del file della zona. Il numero viene incrementato (deve esserlo da ogni amministratore) ogni volta che si modifica un record di risorsa della zona.
- **Refresh**
  Corrisponde al tempo, in secondi, che intercorre prima che un server DNS secondario invii una richiesta di rinnovo della zona. Alla scadenza, il server DNS secondario, se i Serial risultano differenti, richiederà al server DNS primario di effettuare un trasferimento di zona.
  Retry
  Corrisponde al tempo, in secondi, che intercorre prima che un server secondario ripeta un tentativo di trasferimento di zona non riuscito.
- **Expire**
  Corrisponde al tempo, in secondi, che intercorre prima che un server secondario smetta di rispondere alle richieste, senza che la zona sia stata aggiornata. Alla scadenza i dati locali devono essere considerati inaffidabili dal secondario. Ad esempio: quando il primario non è più raggiungibile.
- **Minimum TTL**
  Valore predefinito TTL (Time-To-Live) della zona e intervallo massimo per la memorizzazione nella cache delle risposte alle query dei nomi. E' un valore a 32 bit tra 0 e 2147483647

Altri tipi di records

Codice	RFC di riferimento	Descrizione	Funzione
A	RFC 1035	**record di indirizzo**	restituisce un indirizzo IPv4 a 32 bit, normalmente utilizzato per collegare un nome host al suo indirizzo IP.
AAAA	RFC 3596	record di indirizzo IPv6	restituisce un indirizzo IPv6 a 128 bit, normalmente utilizzato per collegare un nome host al suo indirizzo IPv6.
CNAME	RFC 1035	**record di nome canonico**	Permette di collegare un nome DNS ad un altro. La risoluzione continuerà con il nuovo nome indicato dal record CNAME. Questa funzione è molto utile quando, ad esempio, sullo stesso server sono disponibili più servizi come FTP, HTTP, ecc. operanti su porte differenti. Ciascun servizio potrà avere il suo riferimento DNS (ad esempio `ftp.example.com.` e `www.example.com.`). È molto utile anche quando sullo stesso server ci sono più istanze web con differenti nomi ma utilizzando lo stesso indirizzo. Questa funzione richiede, però, il supporto da parte del server di identità multiple con riconoscimento dell'intestazione HTTP.
MX	RFC 1035	**Server di posta**	Collega un nome di dominio ad una lista di server di posta autorevoli per quel dominio. I record indicano anche la preferenza di un server rispetto ad un altro.
NS	RFC 1035	**Riferimento ai server DNS**	Delega una zona DNS ad essere gestita da un server DNS autorevole per quel nome di dominio.
PTR	RFC 1035	**Record puntatore**	Puntatore ad un nome canonico utilizzato per la risoluzione DNS inversa. Inserendo un record PTR per un nome canonico di dominio nella zona `in-addr.arpa.` (`ip6.arpa.` nel caso di IPv6) fa sì che si possa risalire al nome host dal suo indirizzo IP.
TXT	RFC 1035	**Record di testo**	Era stato pensato per aggiungere commenti leggibili ad un record DNS. Dall'inizio degli anni novanta, invece, è utilizzato per trasferire informazioni di sicurezza in accordo alla RFC 1464, opportunistic encryption, Sender Policy Framework e DomainKeys. Il sistema di DNS dinamico del server DHCP ISC utilizza campi di testo nelle zone dinamiche per identificare i record modificati dal server DHCP.

Tipi di record - A

- Il record A (Address) definisce la corrispondenza tra nome e IP, qual'è l'indirizzo IP (numerico) per la singola macchina.
- La sintassi con cui deve essere scritto è la seguente:

  <host> <ttl> <classe> A <indirizzo IP>

Esempio:

www.cnr.it. 86400 IN A 194.119.192.42

Tipi di record - PTR

- Il record PTR (PoinTeR) definisce la corrispondenza tra l'indirizzo IP della singola macchina ed il suo nome a dominio
- La sintassi con cui deve essere scritto è la seguente:

  <indirizzo IP> <ttl> <classe> PTR <host>

Esempio:

11.193.114.131.in-addr.arpa. 86400 IN PTR www.cnr.it.

Tipi di record - CNAME

- il record CNAME (Canonical NAME) definisce un **nome alternativo con cui può essere identificata la stessa macchina**

- La sintassi con cui deve essere scritto è la seguente (file zone example.com):
  <alias> <ttl> <classe> CNAME <host>

Esempio:

name	*ttl*	*class*	*RR*	*canonical name*
www.example.com	86400	IN	CNAME	joe.example.com.

File di zona per la risoluzione inversa

- Il file per la risoluzione inversa contiene i riferimenti necessari all'associazione tra gli indirizzi IP delle macchine ed il loro nome.
- l'associazione è fatta mediante **specifici record** che descrivono le caratteristiche e le funzionalità del dominio e delle macchine che gli appartengono.
- I più importanti ed utilizzati sono:
  SOA
  NS
  PTR

- Formato di un file di zona inversa (risoluzione indirizzo IP – nome host): della rete 192.167.5.0 (file: 5.167.192.soa)

```
5.167.192.in-addr.arpa IN SOA ns.example.garr.it. root.ns.example.garr.it.
(
                        2007121401 ; serial
                        86400      ; refresh (1 day)
                        3600       ; retry (1 hour)
                        604800     ; expire (1 week)
                        86400      ; minimum (1 day)
                        )
                NS      ns1.garr.net.
                NS      ns2.garr.net.

$ORIGIN 5.168.192.in-addr.arpa.
1       PTR     ns.example.garr.it.
…
…
10      PTR     srv01.example.garr.it.
```

(II) - Domande

- Che differenza c’è tra query ricorsiva e non ricorsiva?
- Quali protocolli vengono utilizzati per il trasporto di un pacchetto DNS ?
- A cosa serve il reverse DNS?

Troubleshooting the DNS

Tools disponibili online

- https://dns-check.nic.it/ Tool di verifica della configurazione del DNS del Registro. Funziona solo per i **domini .it**

- https://dnscheck.ripe.net/ Tool di verifica della configurazione del DNS di RIPE. Particolarmente utile per il check sulle **zone di reverse lookup**.

- https://dnsviz.net/ Tool per visualizzare lo stato di una zona DNS. È stato progettato per la comprensione e la risoluzione dei **problemi relativi a DNSSEC**. Fornisce un'analisi visiva della catena di autenticazione DNSSEC per un nome a dominio e il suo percorso di risoluzione nello spazio dei nomi DNS ed elenca gli errori di configurazione rilevati

- https://dnschecker.org/ Fornisce un servizio di **verifica del DNS a partire da un elenco selezionato di server DNS situati in più regioni del mondo**. Esegue una ricerca di propagazione DNS per qualsiasi nome a dominio e controlla i dati DNS raccolti dalla lista predefinita di server DNS **per controllare che i record siano completamente propagati**.

Comandi su nameserver BIND

- **named-checkzone**:
  - Verifica la sintassi di un file di zona
  - Esegue gli stessi controlli del named per il "*loading*" di una zona
  - Comando utile per una verifica della corretta sintassi di un file di zona prima di rendere operativa la configurazione

  - Esempio1: named-checkzone 247.189.212.in-addr.arpa 247.189.212.rev
- **named-checkconf**:
  - Verifica la sintassi di un file di configurazione named

  - Esempio2: named-checkconf /etc/bind/named.conf

Nslookup(1)

- E’ normalmente distribuito insieme al S.O. o alla distribuzione di BIND
- Si può utilizzare sia in modalità interattiva che tramite riga di comando
- Dispone di aiuto in linea

Nslookup (2)

- Come cercare i record A di un nome (associazione di un nome ad un IP):

```
#:~$ nslookup -type=A  garr.it
Server:         127.0.0.53
Address:        127.0.0.53#53
Non-authoritative answer:
Name:   garr.it
Address: 193.206.158.22
Name:   garr.it
Address: 2001:760:0:158::22
```

- Come cercare i record NS di un nome a dominio:

```
#:~$ nslookup -type=ns garr.it
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
garr.it nameserver = ns1.garr.net.
garr.it nameserver = ns2.garr.net.
```

Nslookup (3)

- Come eseguire una query per il record SOA (Start of Autority) di un nome a dominio

```
#:~$ nslookup -type=soa garr.it
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
garr.it
        origin = ns1.garr.net
        mail addr = postmaster.garr.it
        serial = 2021051401
        refresh = 86400
        retry = 1800
        expire = 2592000
        minimum = 86400
```

Nslookup (4)

- Come trovare i record MX responsabili dello scambio di email

```
nslookup -type=mx garr.it
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
garr.it mail exchanger = 15 mx2.dir.garr.it.
garr.it mail exchanger = 20 mx1.dir.garr.it.
```

Nslookup (5)

- Query con nslookup in modalità interattiva:

```
#:~$ nslookup
> server ns1.garr.net
Default server: ns1.garr.net
Address: 2001:760:ffff:ffff::aa#53
Default server: ns1.garr.net
Address: 193.206.141.38#53
> set query=any
> eduroam.it
Server:         ns1.garr.net
Address:        2001:760:ffff:ffff::aa#53
eduroam.it
        origin = ns1.garr.net
        mail addr = root.nic.garr.it
        serial = 2021030401
        refresh = 86400
        retry = 3600
        expire = 604800
        minimum = 86400
eduroam.it      nameserver = ns2.garr.net.
eduroam.it      nameserver = ns1.garr.net.
Name:   eduroam.it
Address: 193.206.158.6
```

Dig (1) Query ad un nameserver per il record SOA di un dominio

```
#:~$ dig @ns1.garr.net google.com soa

; <<>> DiG 9.10.3-P4-Debian <<>> @ns1.garr.net google.com SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38867
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      SOA

;; ANSWER SECTION:
google.com.             37      IN      SOA     ns1.google.com. dns-admin.google.com. 382987009 900 900 1800 60

;; Query time: 0 msec
;; SERVER: 193.206.141.38#53(193.206.141.38)
;; WHEN: Mon Jul 05 15:40:50 CEST 2021
;; MSG SIZE  rcvd: 89
```

Dig (2) Query ad un nameserver per i record NS (+TTL) di un dominio

```
dig -t ns google.com @ns1.google.com
; <<>> DiG 9.10.3-P4-Debian <<>> -t ns google.com @ns1.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47052
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      NS
;; ANSWER SECTION:
google.com.             345600  IN      NS      ns2.google.com.
google.com.             345600  IN      NS      ns3.google.com.
google.com.             345600  IN      NS      ns4.google.com.
google.com.             345600  IN      NS      ns1.google.com.
;; ADDITIONAL SECTION:
…..
…..
ns4.google.com.         345600  IN      A       216.239.38.10
ns4.google.com.         345600  IN      AAAA    2001:4860:4802:38::a
ns1.google.com.         345600  IN      A       216.239.32.10
ns1.google.com.         345600  IN      AAAA    2001:4860:4802:32::a
;; Query time: 54 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Tue Jun 29 10:37:50 CEST 2021
;; MSG SIZE  rcvd: 287
```

Dig (3) - bulk lookups

- Se occorre risolvere un numero elevato di host nella stessa ricerca, i nomi degli host possono essere inseriti in un file, un nome per riga

- Con l'opzione -f, la stessa query può essere eseguita per più hosts una dopo l'altra

  - # esegue un lookups per un determinato numero di hostnames
  - dig -f /path_to/hosts.txt

Host

- E’ incluso nella distribuzione di BIND ed è inoltre reperibile presso:
  - ftp://ftp.nikhef.nl/pub/network/host.tar.Z
- Non è interattivo: si utilizza da *linea di comando*
- permette di fare interrogazioni complesse a qualsiasi nameserver
- E’ dotato di aiuto in linea

```
host
host -av cnr.it nameserver.cnr.it
host -t soa cnr.it
```

Host (2)

Query per tutti i record del dominio cnr.it

```
> host -va cnr.it
Query about cnr.it for record types ANY
Trying cnr.it ...
Query done, 6 answers, status: no error
The following answer is not authoritative:
cnr.it                  542353  IN      NS      nameserver.cnr.it
cnr.it                  542353  IN      NS      dns2.nic.it
cnr.it                  542353  IN      NS      itgbox.iat.cnr.it
cnr.it                  542353  IN      NS      simon.cs.cornell.edu
cnr.it                  542353  IN      NS      ns1.surfnet.nl
cnr.it                  155353  IN      SOA     nameserver.cnr.it Daniele\.Vannozzi.iat.cnr.it (
                        2000111801  ;serial (version)
                        86400   ;refresh period (1 day)
                        1800    ;retry interval (30 minutes)
                        604800 ;expire time (1 week)
                        86400  ;default ttl (1 day)
                        )
```

.....

Host (3)

Query per il record SOA del dominio garr.it

```
 #:~$ host -t soa garr.it
    garr.it has SOA record ns1.garr.net.postmaster.garr.it.
2008012203
86400
1800
2592000
172800
```

Messaggi subliminali dal DNS

- **NXDOMAIN:** significa che il **dominio non esiste**, neppure alcun nodo definito al di sotto del dominio lungo l'albero DNS (vedi RFC 8020)

- **NODATA:** è un'abbreviazione per una risposta dns con RCODE == 0 (NOERROR), nessun dato disponibile nella ANSWER SECTION.
    - quando può accadere?
        - **Quando si fa una query per un record per il quale non ci sono dati associati**. **Ad esempio richiedo l'IPv6** associato al record AAAA **di un nome ma sono presenti solo dati IPv4** per il record A

- **SRVFAIL:** probabile errore di configurazione del nameserver sul record richiesto

- **REFUSED:** si verifica quando **un nameserver non è configurato come autoritativo per una certa zona** oppure quando un nameserver non accetta determinate query per motivi di policy. Ad esempio, un particolare dispositivo potrebbe essere bloccato se sta eseguendo ripetutamente query malevoli sul nameserver. Oppure, particolari operazioni, come un trasferimento di zona, potrebbero essere vietate

- **DNS request timed out:** il nameserver che interroghiamo ha **problemi di raggiungibilità**

Fine - Parte I