# Protocolo DNS

Redes y Comunicaciones

2025

# Historia

- Internet: necesidad de utilizar nombres en lugar de direcciones IP.
- Mecanismos para mapear nombre de internet (nombre de dominio) a dir. IP.
- 1973, archivo global, `HOSTS.TXT`, mantenido por el SRI (Stanford Research Institute, hoy SRI International).
- Sistema Centralizado: Solicitudes de cambio por E-MAIL. Bajado por FTP.
- 1980 el servicio era muy difícil de mantener y no escalaba.
- 1983 Paul Mockapetris, de USC, desarrolla DNS (Domain Name System): [RFC-882], [RFC-883].
- 1984 Primeras implementaciones Unix BSD.
- El servicio a ido teniendo modificaciones: [RFC-1034], [RFC-1035], etc.
- Servicio NO utilizado directamente por los usuarios.

# Aspectos de DNS

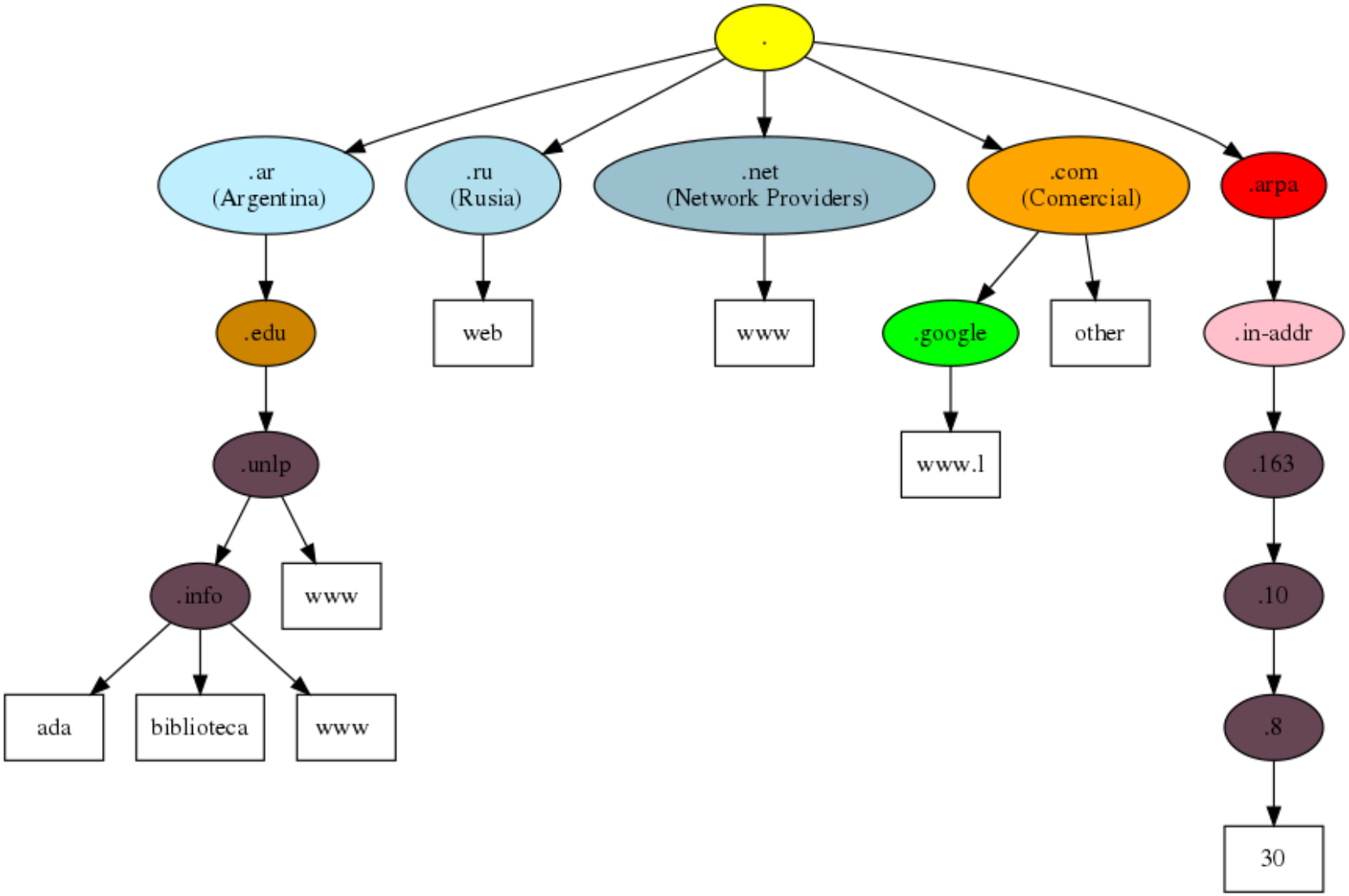
- DNS cubre los siguientes aspectos:
  - Especifica la sintaxis de los nombres y las reglas para delegar autoridad sobre los nombres.
  - Especifica sistema distribuido para "mapear" nombres con direcciones y otras operaciones.
  - Define la implementación de un protocolo para comunicación de las componentes del sistema.
- Descentralizar el mecanismo de asignación de nombres, aunque sigue sistema jerárquico.
- Delegar autoridad y responsabilidad de la asignación y mapeo en organismos intermedios.
- Podemos verlo como una base de datos (DB) distribuída.

# Elementos de DNS

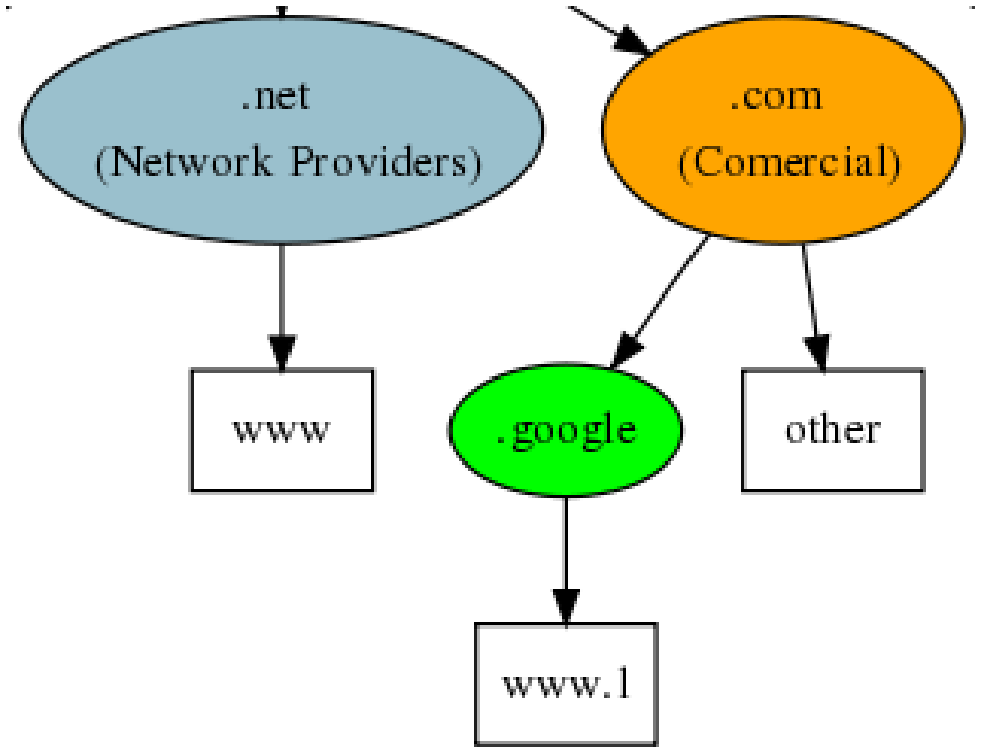
- Nombre de dominio FQDN: lista de etiquetas (labels) separadas por puntos.
- Se leen desde el nodo/etiqueta de la izquierda hasta la raíz del árbol (el punto), estructura jerárquica con sub-nombres (niveles).
- La sintaxis jerárquica refleja la delegación de autoridad.
- No son case-sensitive, cada etiqueta Máximo 63 chars.
- Máximo etiquetas 127, nombre no más de 255 chars, acepta valores internacionales, UTF-8, Unicode.

```
paraguil (No FQDN)
paraguil.cities.org. (FQDN)
paraguil.cities.org (Considerado FQDN)
```

# Esquema de Nombres de DNS



# Esquema de Nombres de DNS (Cont'd)



# TLDs (Top Level Domains)

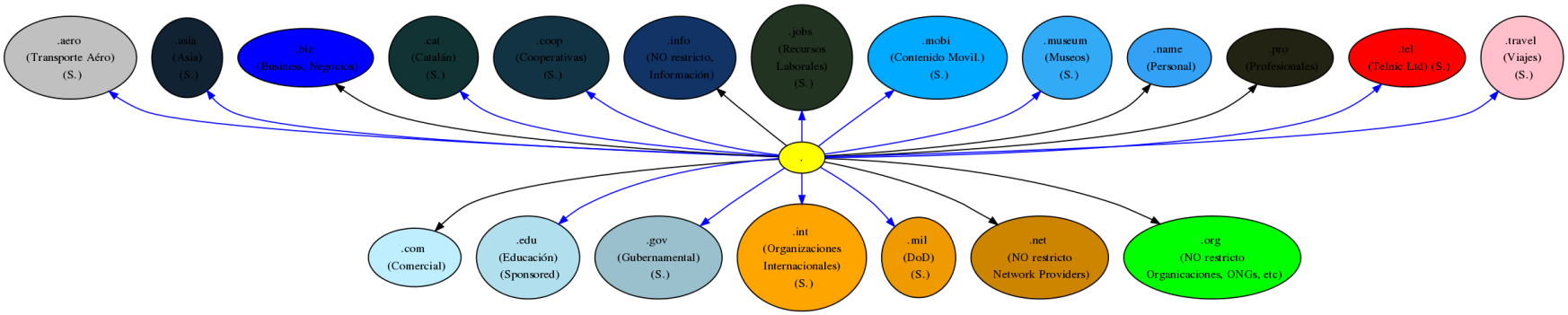
- Los TLDs se podrían clasificar en 3 grupos:

  gTLDs, Generic TLDs: contienen dominios con propósitos particulares, de acuerdo a diferentes actividades. políticas definidas por el ICANN:**Unsponsored TLD** o definidas por otra organización: **Sponsored TLD**.

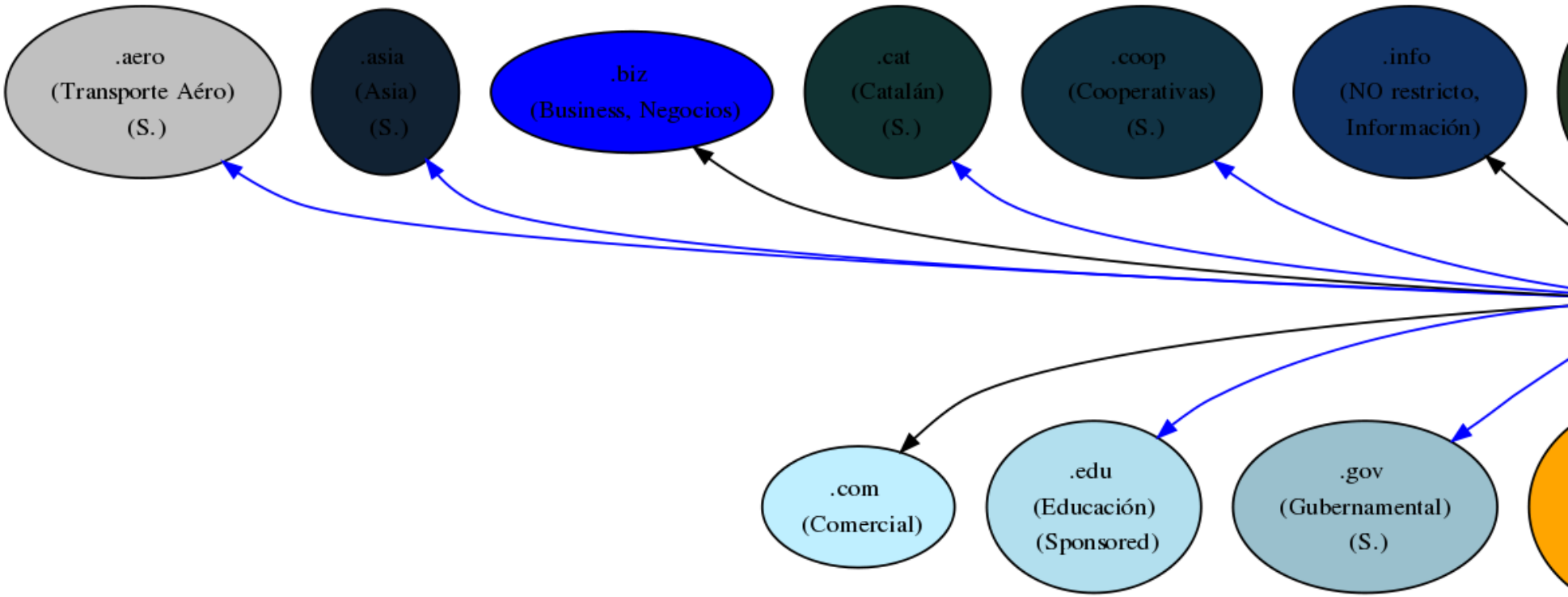
  ccTLD Country-Code TLDs: contienen dominios delegados a los diferentes países del mundo. ISO 3166-1 alfa-2.

  .ARPA TLD: es un dominio especial, usado internamente para resolución de reversos.

# Generic TLDs antes de new gTLDs



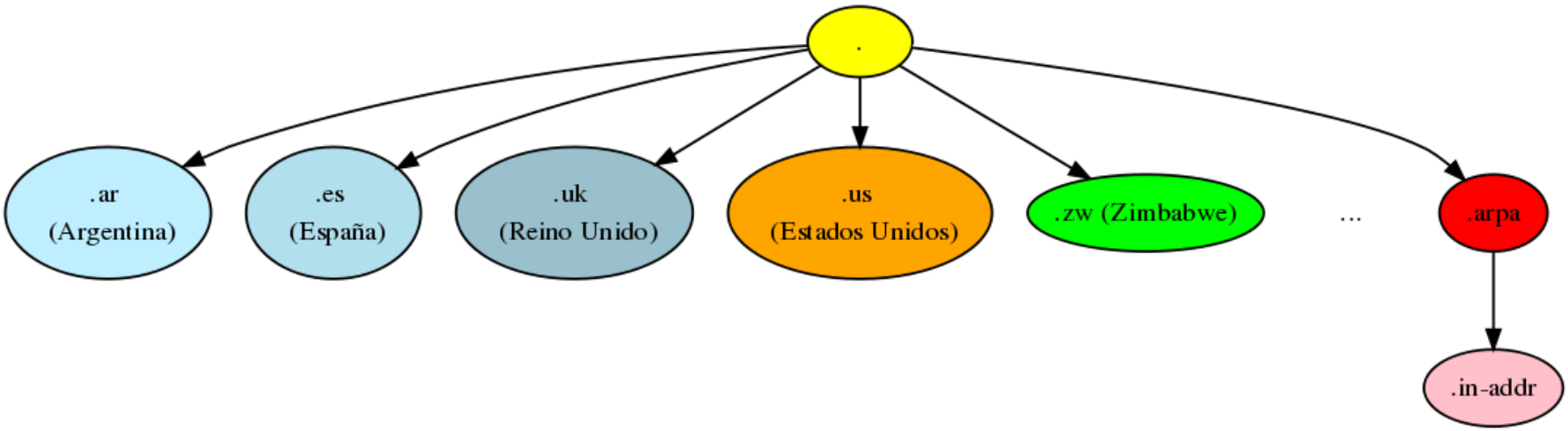
# Generic TLDs antes de new gTLDs (Cont'd)



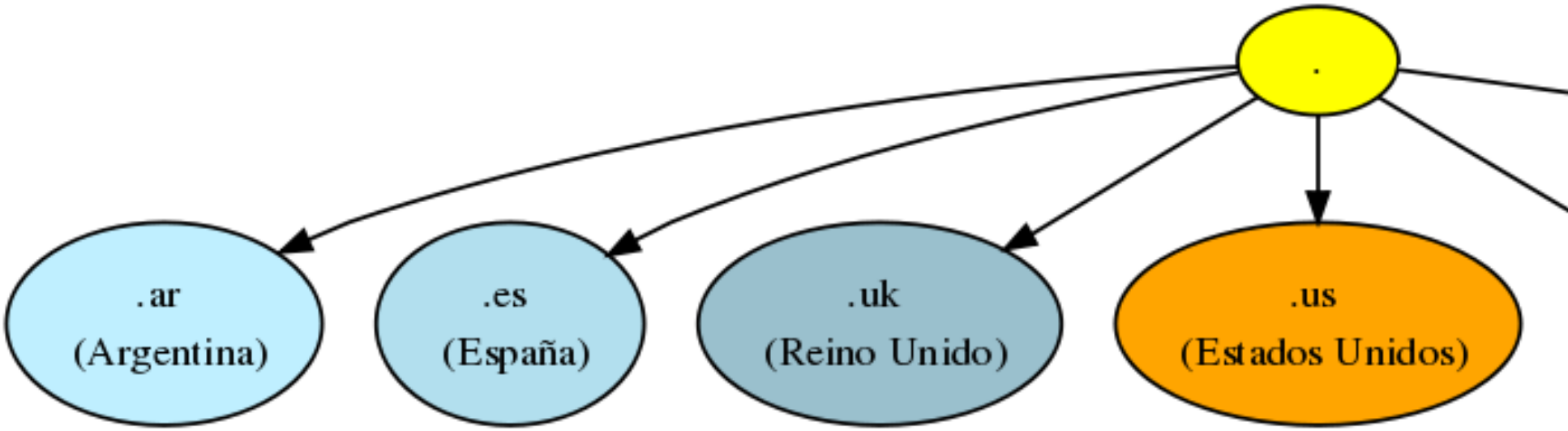
# Generic TLDs actualmente

- A partir de 2012 se comenzó a aceptar nuevas aplicaciones para new gTLDs.
- Proceso de licitación, donde hay en juego grandes sumas de dinero.
- Nuevos dominios registrados (500+):
  - .academy, .casa, ...
  - .beer, .bike, .futbol, ...
  - .pizza, .paris
  - .wiki, .viajes, ...
  - ...

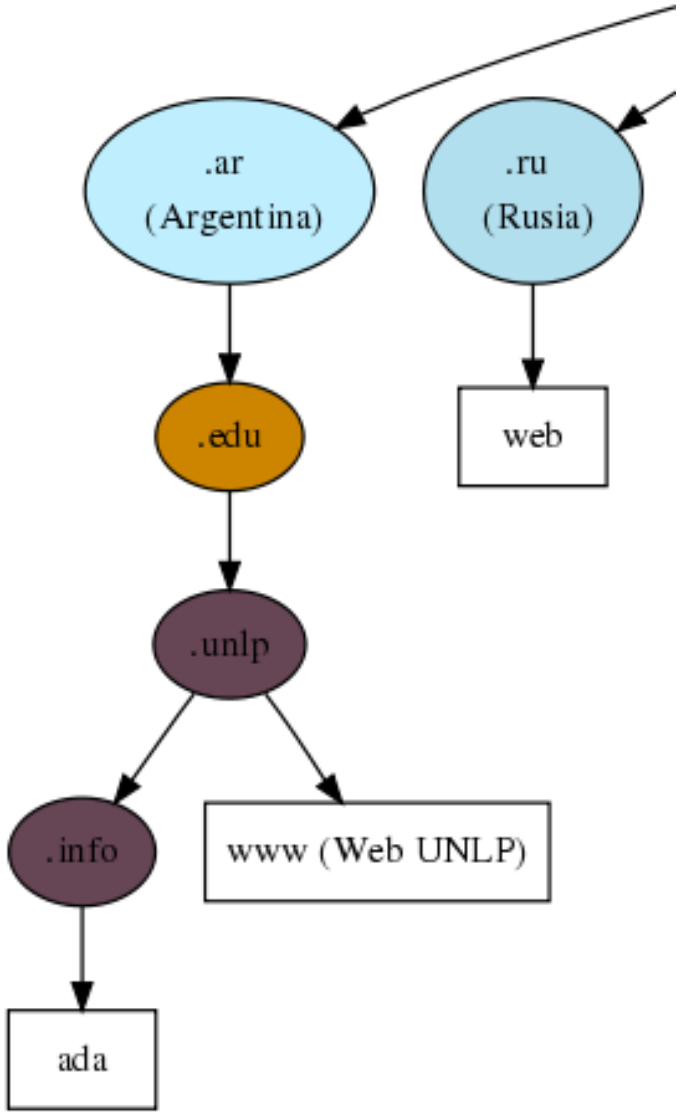
# Country Code y ARPA TLD



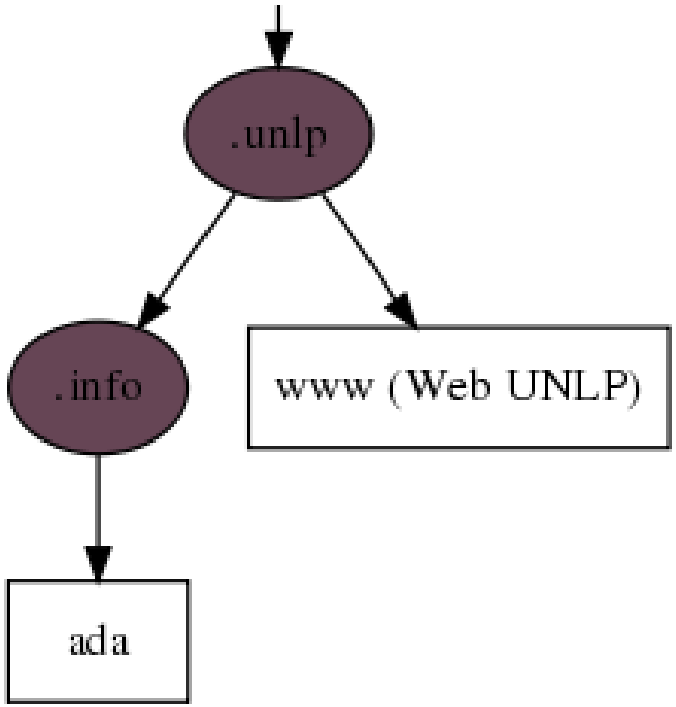
# Country Code TLD



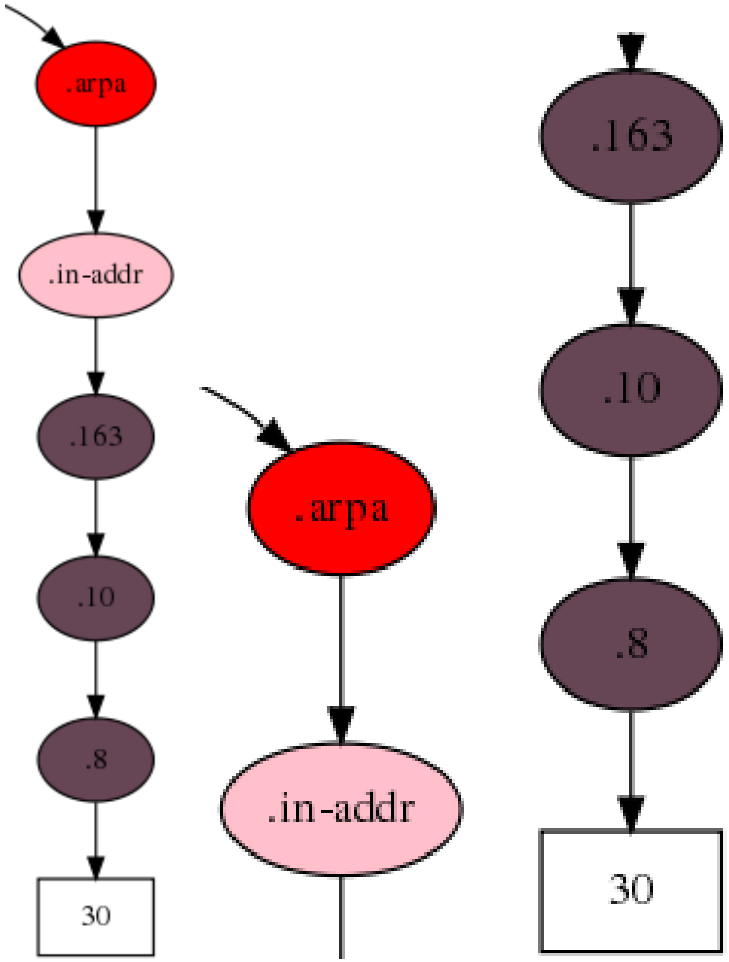
# Esquema de Nombres de DNS (CC)



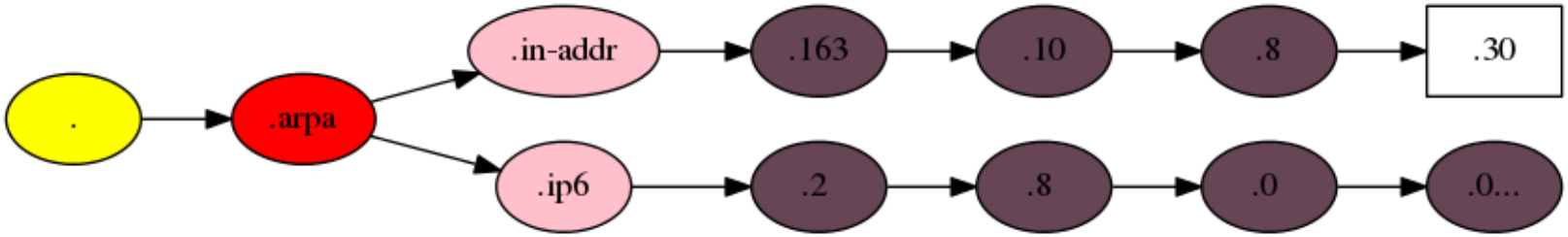
# Esquema de Nombres de DNS (CC Cont'd)



# Esquema de Nombres de DNS (ARPA Cont'd)



# Esquema de Nombres de DNS (ARPA Cont'd)

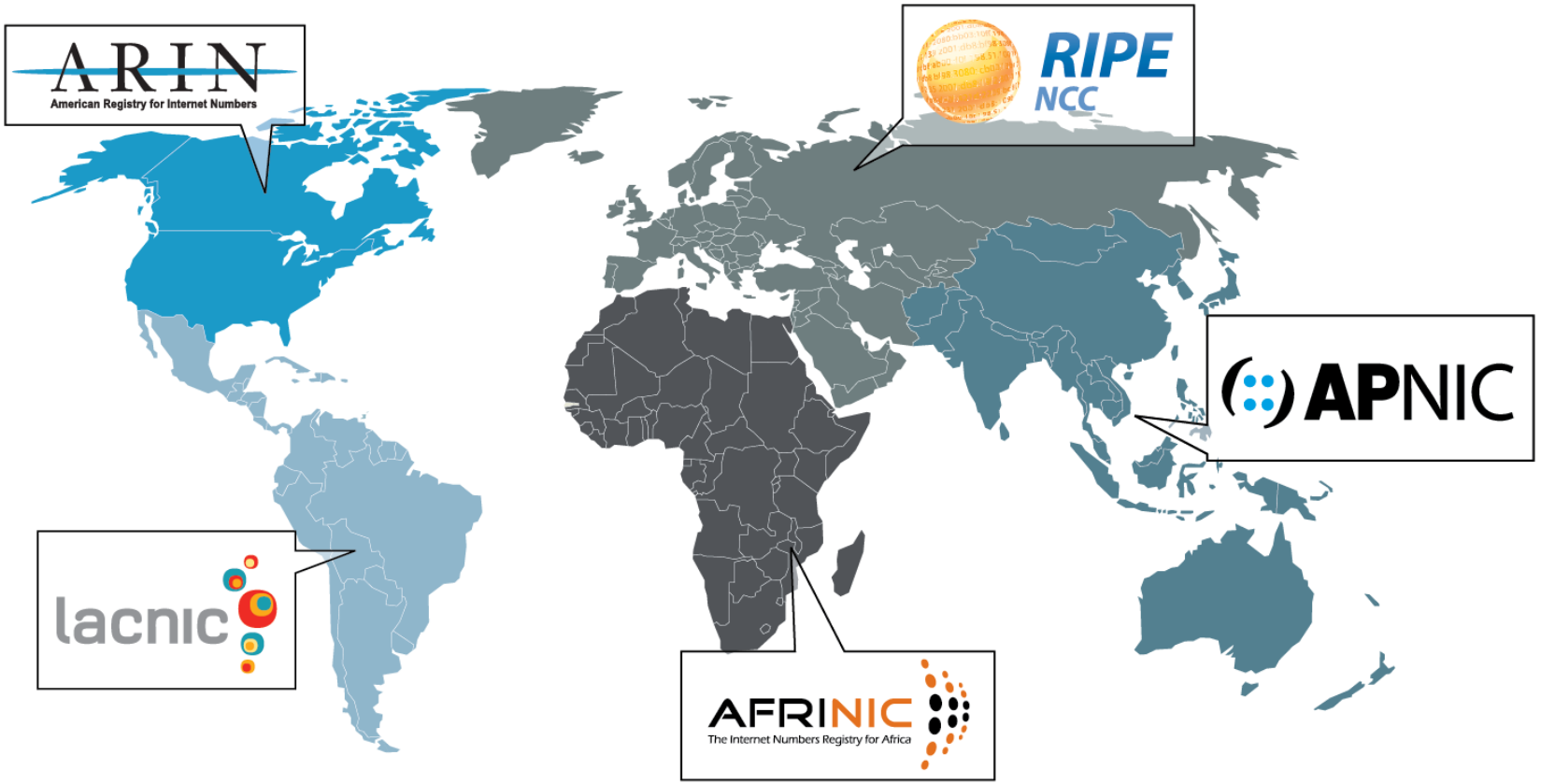



$ host 163.10.8.30 30.8.10.163.in-addr.arpa domain name pointer host163-10-8-30.presi.unlp.edu.ar.
$ host 2800:340:0:64::145 5.4.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.6.0.0.0.0.0.0.0.4.3.0.0.0.8.2.ip6.arpa domain name pointer www.unlp.edu.ar.

# Organización del DNS

- Sistema distribuido y jerárquico.
- Organización mediante dominios, sub-dominios y host o servicios.
- IANA a través del ICANN (Internet Corporation for Assigned Names and Numbers) controla el funcionamiento.
- Existen organizaciones paralelas: Open Root Server Network (ORSN), OpenNIC.
- Delegación mediante RIRs (Regional Internet Registers):
  - American Registry for Internet Numbers (ARIN).
  - RIPE NCC -Europa y parte de Asia- (RIPE).
  - Asia-Pacific Network Information Centre (APNIC).
  - Latin American and Caribbean NIC (LACNIC).
  - African Network Information Centre (AfriNIC).
- Nombres se delegan a países, direcciones IP no.

# Organización del DNS (Cont'd)



# Ejemplo: Delegación de autoridad

- **ada.info.unlp.edu.ar**
- "Ada" fue registrada por la administración de la red de la Facultad de Informática.
- El administrador de la Facultad obtuvo previamente la autoridad sobre el dominio "info.unlp.edu.ar". a partir de la administración de la universidad UNLP.
- La Universidad obtuvo autoridad sobre el dominio "unlp.edu.ar" a partir de la administración de "edu.ar", RIU (Red Inter-universitaria).

# Ejemplo: Delegación de autoridad (Cont'd)

- La RIU obtuvo autoridad sobre "edu.ar" a partir de la delegación de la Cancillería o el ente a cargo de ".AR" (Argentina).
- La administración de nombres en la Argentina, sea la Secretaría Legal y Técnica u otro ente obtuvo la autoridad delegada a partir del IANA o ICANN.

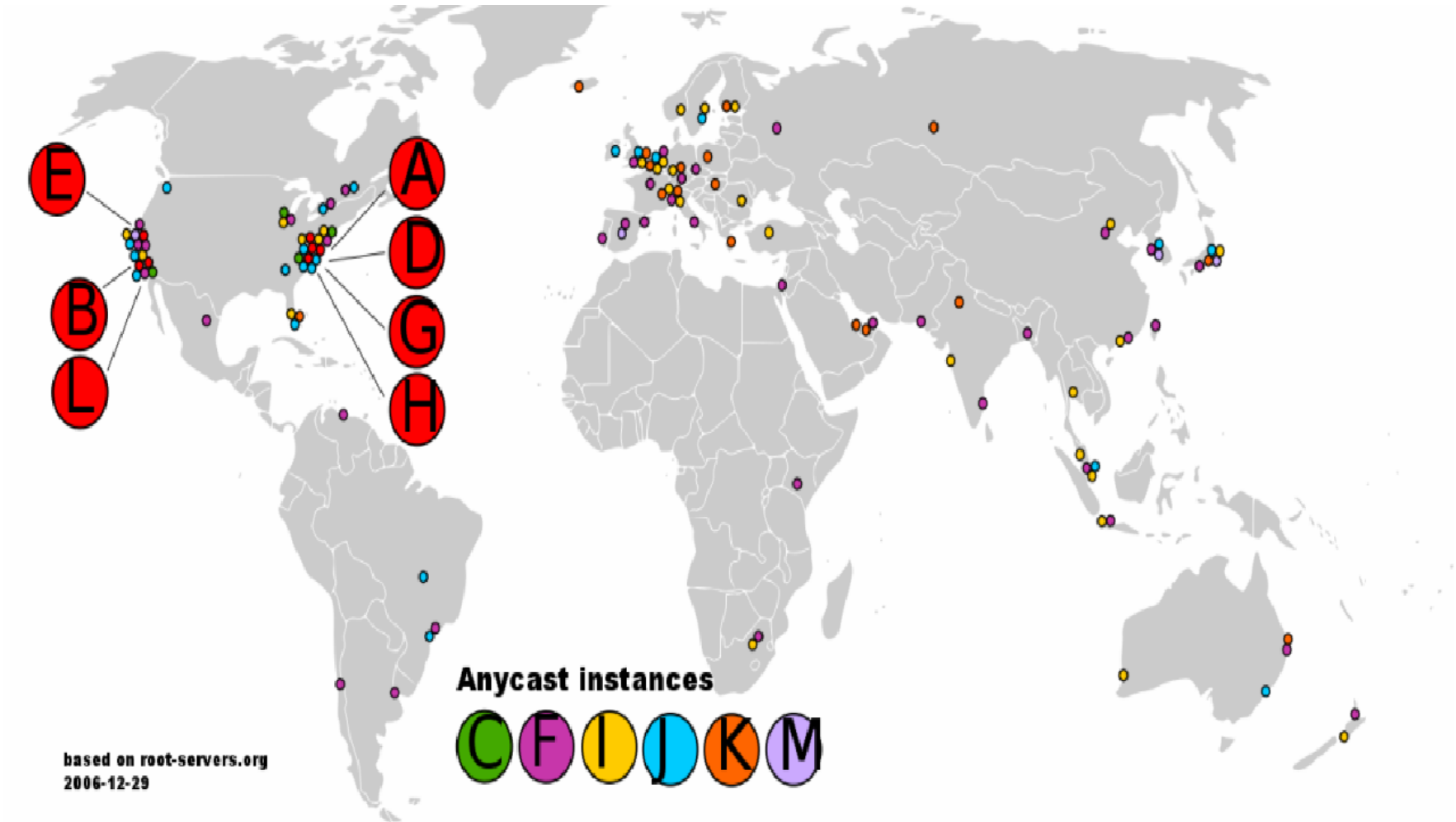
# Delegación de Dominios

- Actualidad: 13 **ROOT Servers** distribuidos en todo el mundo.
- Los cuales trabajan con redundancia y las réplicas están distribuidos geográficamente.
- Redundancia, combinada con **Ruteo Anycast**.

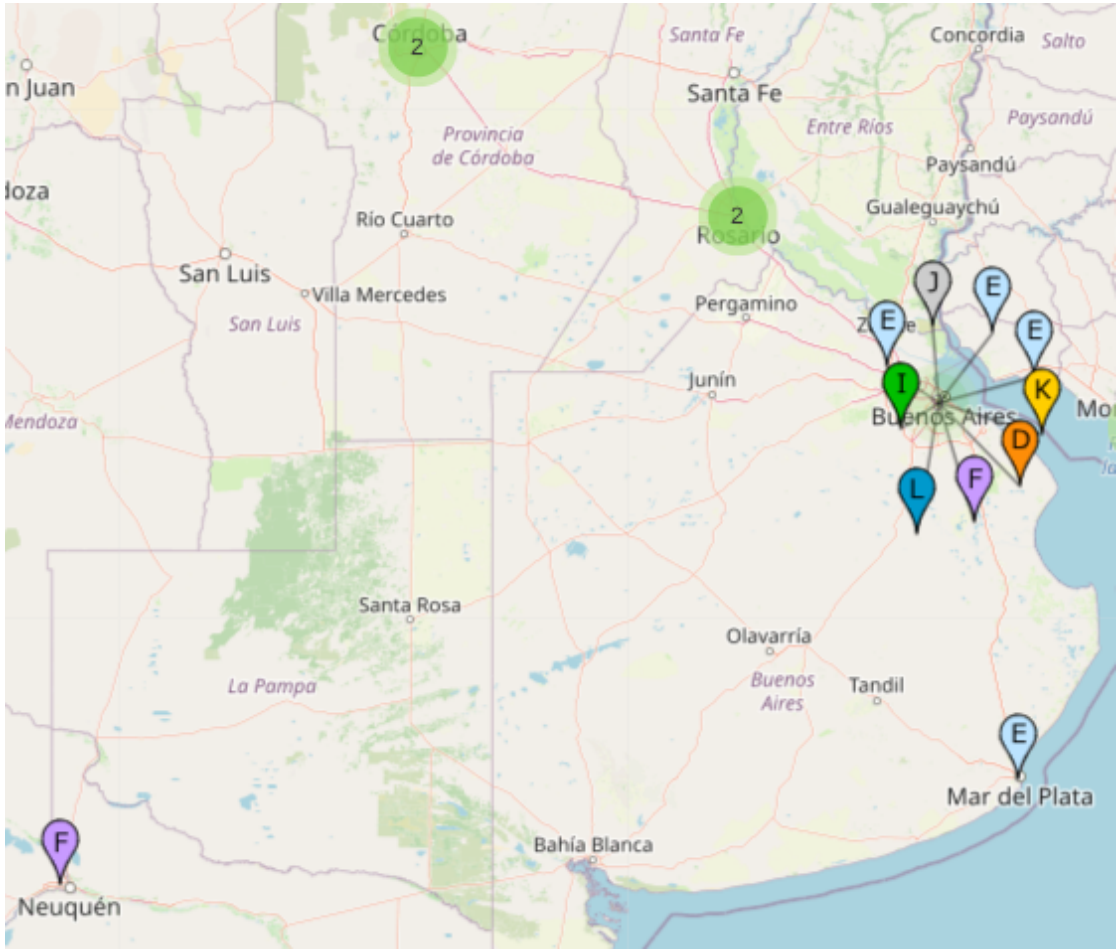
```
.   518400   IN      NS      A.ROOT-SERVERS.NET. # Versign-grs.com
.   518400   IN      NS      B.ROOT-SERVERS.NET. # ISI.edu
.   518400   IN      NS      C.ROOT-SERVERS.NET. # Cogent.com (ANYCAST)
.   518400   IN      NS      D.ROOT-SERVERS.NET. # UMD.edu (Univ. Maryland)
.   518400   IN      NS      E.ROOT-SERVERS.NET. # NASA.gov
.   518400   IN      NS      F.ROOT-SERVERS.NET. # ISC.org (ANYCAST)
.   518400   IN      NS      G.ROOT-SERVERS.NET. # NIC.mil
.   518400   IN      NS      H.ROOT-SERVERS.NET. # ARMY.mil
.   518400   IN      NS      I.ROOT-SERVERS.NET. # NIC.ddn.mil (ANYCAST)
.   518400   IN      NS      J.ROOT-SERVERS.NET. # Versign-grs.com (ANYCAST)
.   518400   IN      NS      K.ROOT-SERVERS.NET. # RIPE.net (ANYCAST)
.   518400   IN      NS      L.ROOT-SERVERS.NET. # ICANN.org (ANYCAST)
.   518400   IN      NS      M.ROOT-SERVERS.NET. # WIDE.ad.jp (ANYCAST)
```

# Distribución de ROOT Servers - 2008

# Distribución de ROOT Servers (Cont'd)

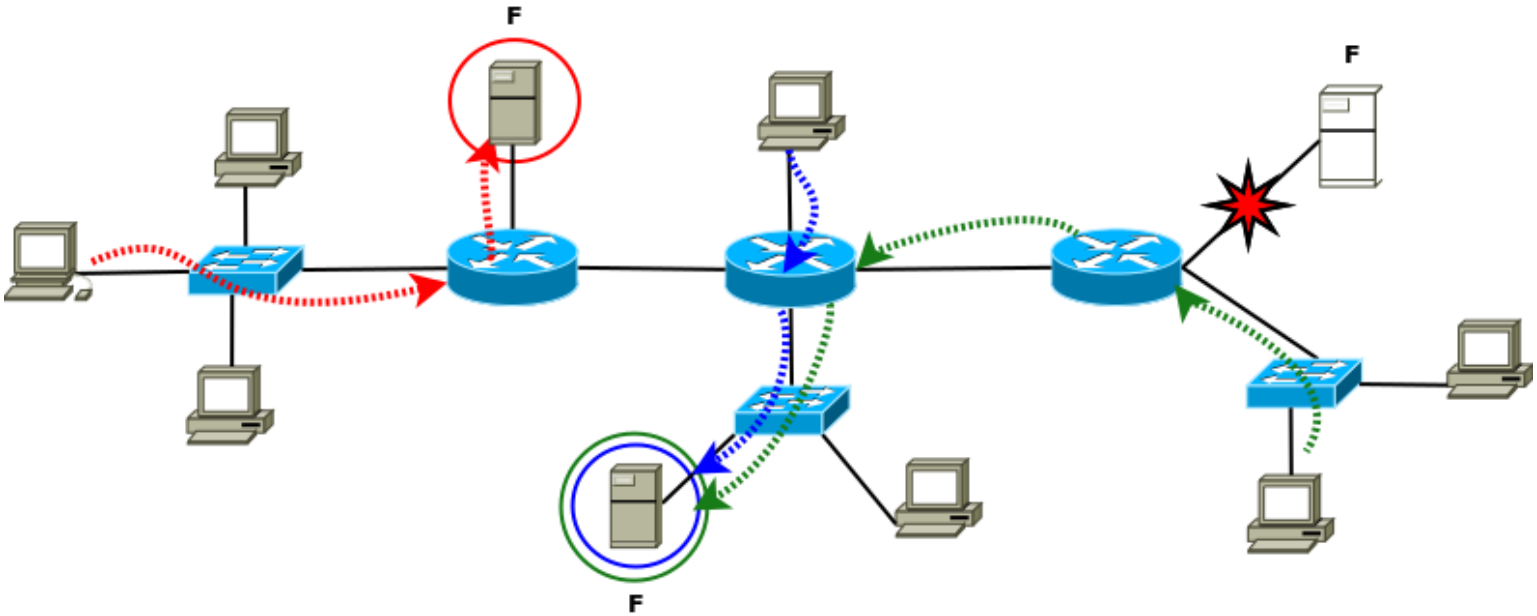


# Distribución de ROOT Servers parte Arg. 2025




fuente:root-servers.org

# Distribución de ROOT Servers, Anycast



# Tipos de Servidores

Servidor Raíz: servidor que delega a todos TLD (Top Level Domains). No debería permitir recursivas.

Servidor Autoritativo: servidor con una zona o sub-dominio de nombres a cargo. podría sub-delegar.

Servidor Local/Resolver Recursivo: es un servidor que es consultado dentro de una red. mantiene cache. Puede ser **Servidor Autoritativo**. Permite recursivas "internas". También llamado **Caching Name Server**.

Open Name Servers: servidores de DNS que funcionan como locales para cualquier cliente. Por ejemplo 8.8.8.8, 8.8.4.4, 4.2.2.2, 4.2.2.3.

# Tipos de Servidores (Cont'd)

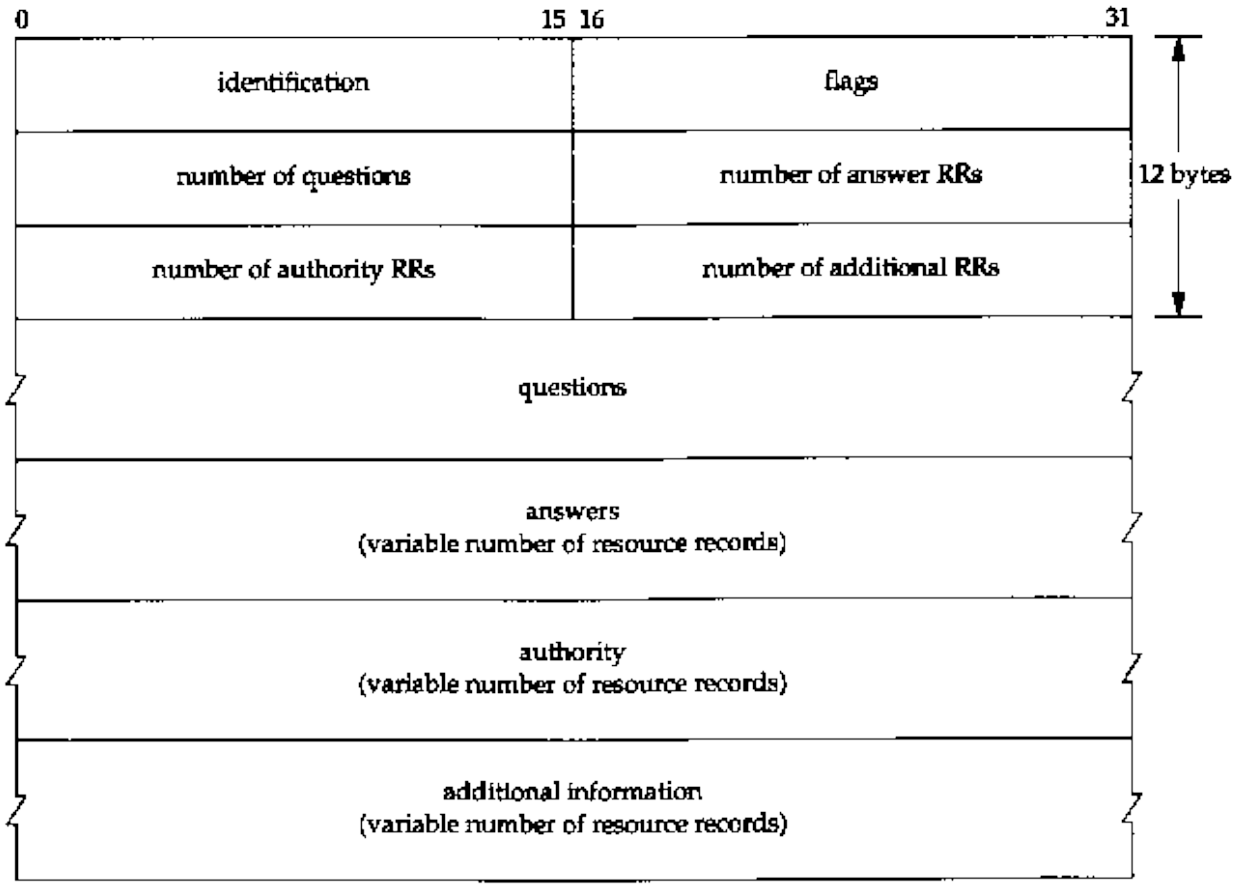
Forwarder Name Server: interactúan directamente con el sistema de DNS exterior. Son DNS proxies de otros DNS internos.

Servidor Primario y Secundario: solo una cuestión de implementación. donde se modifican los datos realmente.

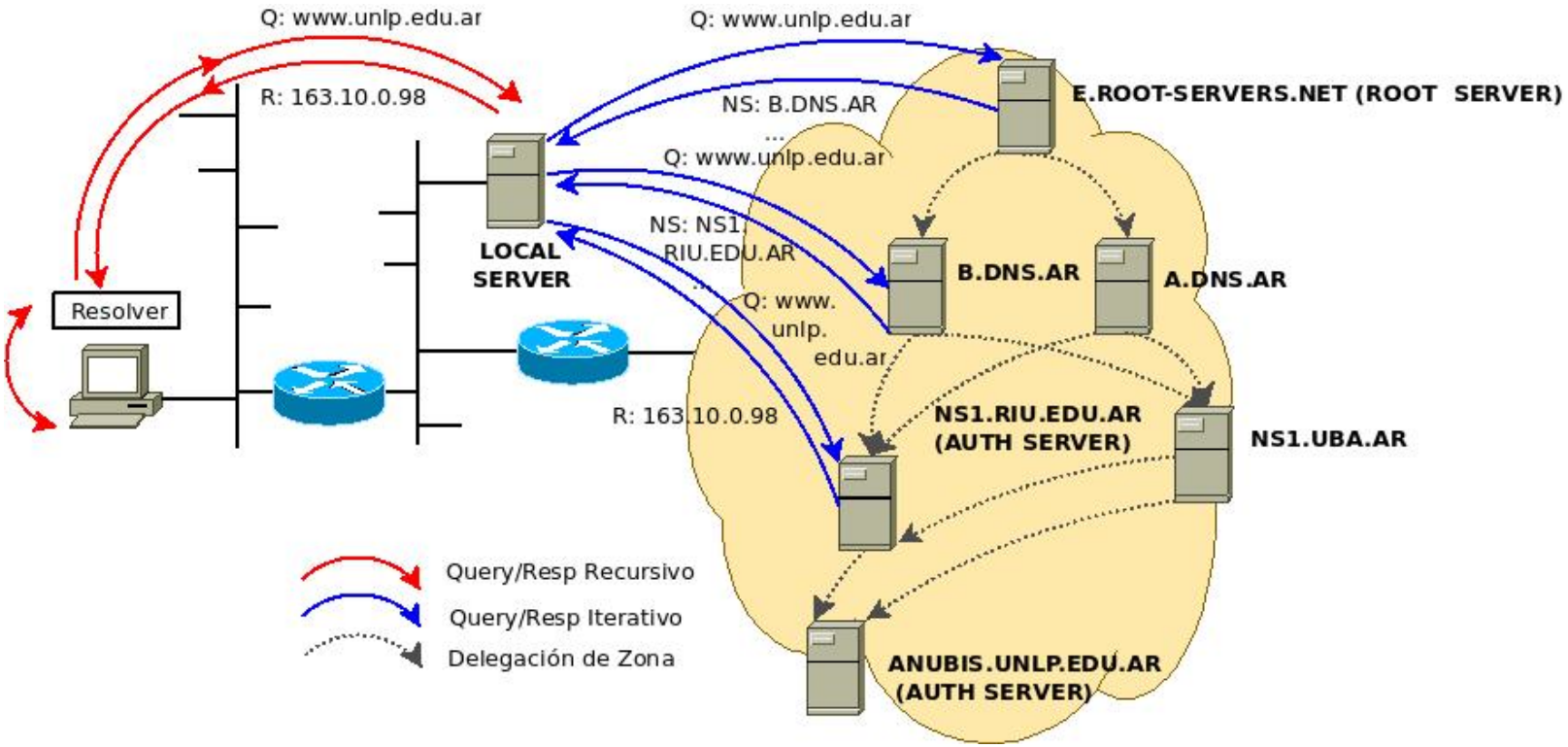
# Funcionamiento de DNS

- Modelo cliente/servidor, Request/Response.
- También hay diálogo entre los servidores.
- Protocolo corre sobre **UDP** y **TCP**, puerto **53**.
- El cliente escoge cualquier puerto no privilegiado.
- No Trabaja sobre texto ASCII.
- Si el mensaje supera los 512 bytes se utiliza TCP, e.g. zone transfer.
- Clientes: resolver + cualquier aplicación que requiera la resolución de nombres.
  - Unix el resolver conjunto de funciones **C library (libc)**.
  - Otras implementaciones **Smart Resolver** servidor Local en cada equipo, caching.
- Servidores: BIND (Berkeley Internet Name Domain/Daemon) de ISC; UNBOUND.

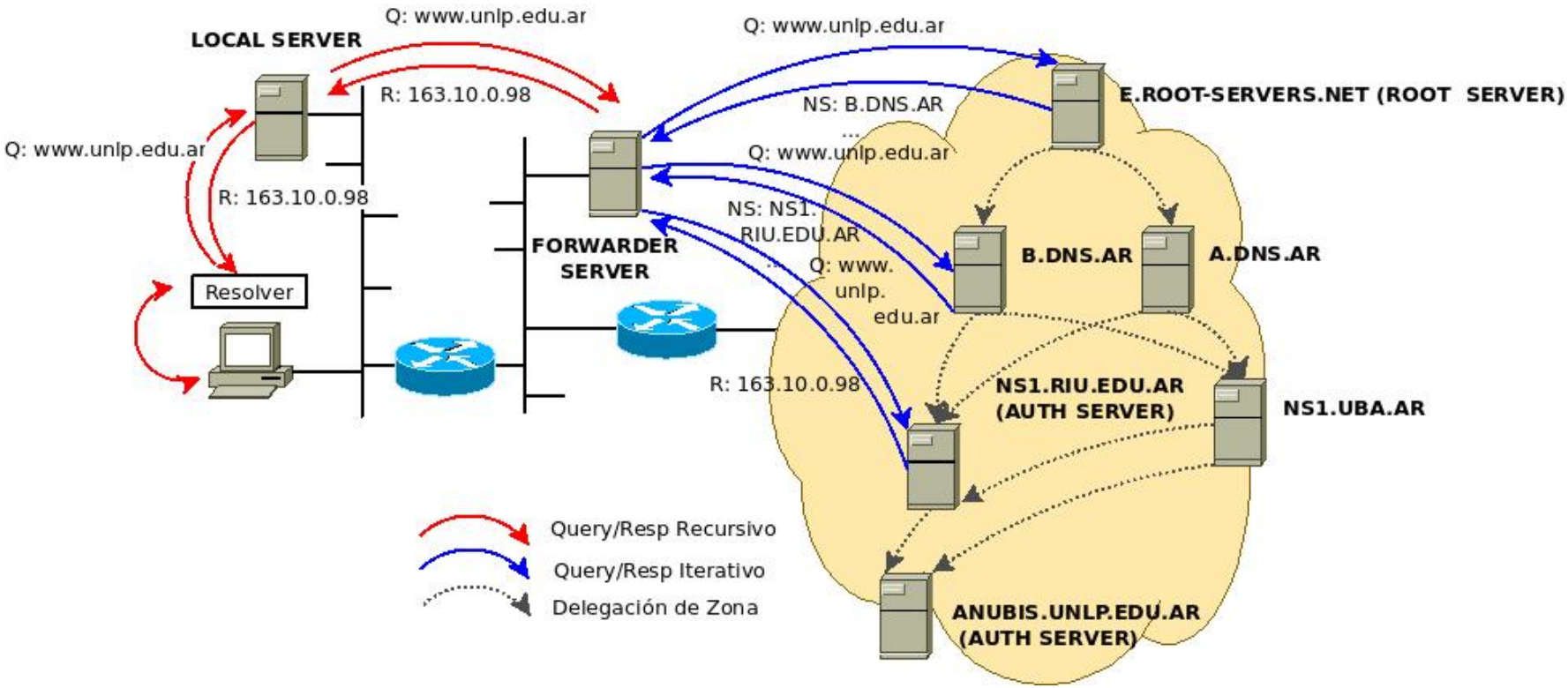
# Estructura de mensaje de DNS



# Resolución de Nombres, Iterativo vs. Recursivo



# Resolución de Nombres, Iterativo vs. Recursivo



# Servicios y Registros de DNS

- Servidor de DNS almacena la información formando base de datos (DB) de RR (Resource Records).
- No necesariamente es DB relacional.
- Cada registro diferente tipo de información (Algunos Registros):

  Registros A, AAAA (Address): nombre → IP, IPv6.
  Registros PTR (Pointer): IP → nombre.
  Registros CNAME (Canonical Name): nombre → nombre.
  Registros HINFO (Hardware Info): nombre → info.
  Registros TXT (Textual): nombre → info.
  Registros MX (Mail Exchanger): nombre-dom → mail exchanger(s).
  Registros NS (Name Server): nombre-dom → dns server(s).
  Registros SOA (Start Of Authority): params. de dominio.

# Registros A (Address)

```
# less /etc/bind/db.cities.org
...
berlin.cities.org.          IN          A     172.20.1.100
brasilia.cities.org.        IN          A     172.20.1.5
paraguil-br0.cities.org.    IN          A     172.20.1.1
...
```

# Registros AAAA (IPv6 Address)

```
# less /etc/bind/db.cities.org
...
berlin.cities.org.    IN AAAA 2001:db8:1234:4567::100
brasilia.cities.org.  IN AAAA 2001:db8:1234:4567::5
...
```

# Registros PTR (Pointer)

```
# less /etc/bind/db.172
...
1.1.20    IN      PTR     paraguil-br0.cities.org.
5.1.20    IN      PTR     brasilias.cities.org.
100.1.20  IN      PTR     berlin.cities.org.
...
5.1.19    IN      PTR     sucre.lat.org.
1.1.19    IN      PTR     paraguil-tap2.lat.org.
...
```

# Registros CNAME (Canonical Name)

```
# less /etc/bind/db.cities.org
...
ftp.cities.org.   IN    CNAME    berlin.cities.org.
www.cities.org.   IN    CNAME    berlin.cities.org.
...
```

# Registros MX (Mail Exchanger)

```
# less /etc/bind/db.cities.org
...
cities.org.     IN        MX 1   brasilia.cities.org.
cities.org.     IN        MX 10  berlin.cities.org.
...

# dig -t mx gmail.com
...
gmail.com   IN    MX     5 gmail-smtp-in.l.google.com.
gmail.com   IN    MX    10 alt1.gmail-smtp-in.l.google.com.
gmail.com   IN    MX    10 alt2.gmail-smtp-in.l.google.com.
gmail.com   IN    MX    50 gsmtp147.google.com.
gmail.com   IN    MX    50 gsmtp183.google.com.
...
```

# Registros NS (Name Server)

```
# less /etc/bind/db.cities.org
...
; ## ZONA RAIZ
cities.org.              IN  NS berlin.cities.org.
cities.org.              IN  NS brasilia.cities.org.
; ## ZONA delegada
trees.cities.org.        IN  NS brasilia.cities.org.
trees.cities.org.        IN  NS berlin.cities.org.
trees.cities.org.        IN  NS oak.trees.cities.org.
; ## GLUE RECORD ##
oak.trees.cities.org.    IN  A 192.168.40.1
...
```

# Registros SOA (Start Of Authority)

```
$TTL    604800 ; ### TTL global para todos
cities.org. IN      SOA     berlin.cities.org.
                            root.berlin.cities.org. (
                         2008092901   ; ## Serial
                            604800    ; ## Refresh
                             86400    ; ## Retry
                           2419200    ; ## Expiry
                            604800 )  ; ## Neg Cache TTL
...
```

# Ejemplos con DNS

- Consultas a los DNS.

```
? host -t a berlin.cities.org 127.0.0.1

? dig +nocomments -t a brasilia.cities.org @127.0.0.1
? dig +recurse +short www.unlp.edu.ar @192.112.36.4
? dig +recurse +short www.unlp.edu.ar @127.0.0.1
? dig +short -t ptr 100.1.20.172.in-addr.arpa  @127.0.0.1

? host -t mx cities.org 127.0.0.1
? host -t ns cities.org 127.0.0.1
```

# TTL y Registros TXT

```
? dig www.unlp.edu.ar | grep -A1 "ANSWER SECTION"
;; ANSWER SECTION:
www.unlp.edu.ar. 155 IN A 163.10.0.145

? dig -t mx gmail.com | grep -A1 "ANSWER SECTION"
;; ANSWER SECTION:
gmail.com. 3599 IN MX 20 alt2.gmail-smtp-in.l.google.com.
```

# TTL y Registros TXT

```
? dig -t txt gmail.com | grep -A1 "ANSWER SECTION"
;; ANSWER SECTION:
gmail.com. 299 IN TXT "v=spf1 redirect=_spf.google.com"

? dig -t txt _spf.google.com | grep -A1 "ANSWER SECTION"
;; ANSWER SECTION:
_spf.google.com. 299 IN TXT
            "v=spf1 include:_netblocks.google.com
             include:_netblocks2.google.com
             include:_netblocks3.google.com ~all"
```

# Otras Características del DNS

- Transferencia de Zona: AXFR.
  - Entre servidores de DNS primario y secundario.
  - Se realiza sobre TCP de forma periódica.
- Dynamic DNS: DDNS.
  - Actualización dinámica de registros, usada con IP dinámicas.
- Split DNS.
  - Responder de acuerdo de donde proviene la consulta.

# Cuestiones de Seguridad

- DNS no viaja cifrado ni autenticado.
- Para chequear integridad: DNSSEC (Desde auth $\Rightarrow$ resolver).
- DNS over HTTPS (DoH) - Cambia como se usa la infra-estructura de servidores.
- DNS over TLS (DoT) - Cambia como se usa la infra-estructura de servidores.
- DNS RPZ.

[StevI] TCP/IP Illustrated, Volume 1: The Protocols, Addison-Wesley, 1994. W. Richard Stevens.

[KR] Kurose/Ross: Computer Networking (3rd Edition).

[LX] The Linux Home Page: http://www.linux.org/.

[Siever] Linux in a Nutshell, Fourth Edition June, 2003. O'Reilly. Ellen Siever, Stephen Figgins, Aaron Weber.

[BIND] DNS and BIND, Fourth Edition By Paul Albitz, Cricket Liu. O'Reilly. La Third Edtion de 1998 esta disponible online: http://www.unix.com.ua/orelly/networking/dnsbind/index.htm.

[LNAG] Linux Network Administrators Guide. Olaf Kirch & Terry Dawson. 2nd Edition June 2000. http://oreilly.com/catalog/linag2/book/index.html.

[RFC-768] http://www.rfc-editor.org/rfc/rfc768.txt. User Datagram Protocol (Jon Postel 1980 USC-ISI IANA).

[RFC-793] http://www.rfc-editor.org/rfc/rfc793.txt. TCP Transmission Control Protocol (Jon Postel 1981 USC-ISI IANA).

[RFC-882] http://www.rfc-editor.org/rfc/rfc882.txt. DOMAIN NAMES - CONCEPTS and FACILITIES (P. Mockapetris 1983 ISI).

[RFC-883] http://www.rfc-editor.org/rfc/rfc883.txt DOMAIN NAMES - IMPLEMENTATION and SPECIFICATION (P. Mockapetris 1983 ISI).

[RFC-1034] http://www.rfc-editor.org/rfc/rfc1034.txt. DOMAIN NAMES - CONCEPTS AND FACILITIES (P. Mockapetris 1987 ISI).

[RFC-1035] http://www.rfc-editor.org/rfc/rfc1035.txt. DOMAIN NAMES - IMPLEMENTATION and SPECIFICATION (P. Mockapetris 1987 ISI).

[COM05] Ethereal, Wireshark. Autor original Gerald Combs, 2005. http://www.ethereal.com/. http://www.wireshark.org/.