Resolución de Nombres

Objetivos

- Nombres de "Hosts"
- Resolución de Nombres
- Archivo Hosts
- DNS: Dominios y Subdominios
- Tipos de Servidores DNS
- Archivos de DNS
- Registros de Recursos
- Formato de mensajes DNS
- Planificación de DNS

Esquemas de Nombres TCP/IP

- Ambientes Microsoft
  - Direcciones IP
  - Nombres NetBIOS
    - Ejemplo: net use x: \\servidor_db
    - servidor_db es un nombre NetBIOS
    - Este nombre es asociado a una dirección IP
- Ambientes UNIX
  - Direcciones IP
  - Nombres de Hosts ("Host names")
    - Esquema Plano ("flat")
    - Ejemplo: proxy_2
  - Nombres de Dominio
    - Esquema jerárquico
    - Ejemplo: proxy_2.herrera.unt.edu.ar
- En la actualidad se está unificando el esquema al nombramiento con nombres de dominio

Host Name

- Es un Alias Utilizado para Referenciar a un Equipo TCP/IP.
  - Se podría asignar múltiples nombres de hosts a un host TCP/IP
- Provee una Forma Simplificada de Acceder a un Host TCP/IP.
- Utilizado por Utilitarios TCP/IP (PING, Telnet, etc.)
  - Si el esquema de resolución de nombres funciona correctamente, es similar referirse a un host por su dirección IP que por su nombre
- Las Entradas son Almacenadas en el Archivo HOSTS o en DNS.
  - Archivos hosts – Esquema Estático.
  - Archivos DNS – Bases de Datos Distribuidas. Esquema Dinámico.

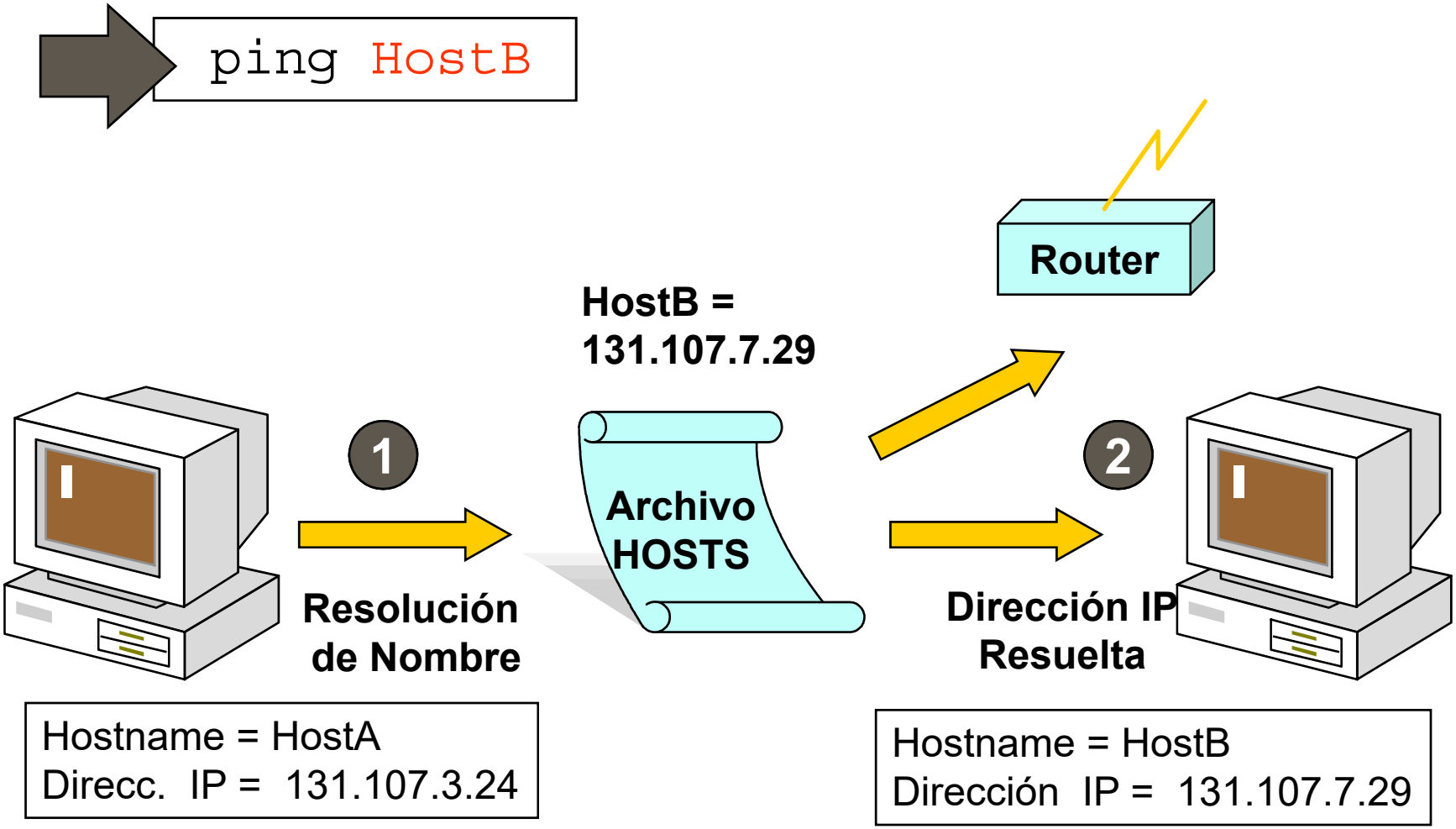
Nombres plano vs. jerárquico

- Nombres Planos ("flat")
  - Nombre consistentes de un secuencia de caracteres sin estructura
  - Ventajas:
    - Nombre cortos
  - Desventajas:
    - El nombre no ofrece ningún indicativo del hosts
    - No puede ser generalizado a un gran número de máquinas
    - No se puede **distribuir** su administración y control.
- Nombres Jerárquicos
  - Se particiona el nombre en distintas porciones
  - La principal ventaja de este esquema, es la posibilidad de delegación de la tarea administrativa en el manejo de nombres

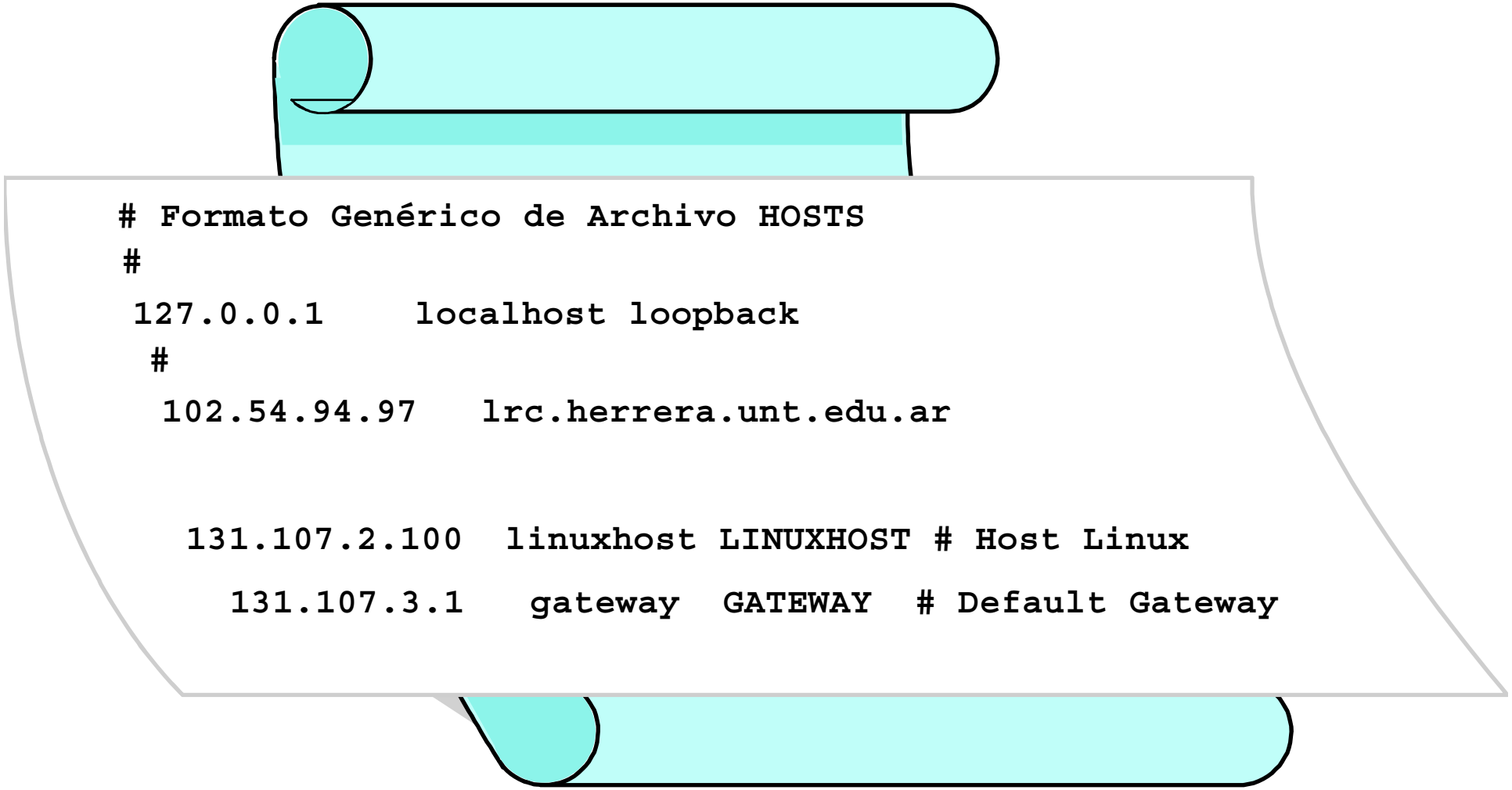
Resolución de Nombres

- Es el Proceso de Mapeo de nombres de Hosts a una Dirección IP
- Los Métodos de Resolución de nombre de hosts son:
  - Archivo HOSTS
    - Archivo de texto **local** en cada host que contiene el mapeo de nombres a direcciones IP
  - DNS ("Domain Name System")
    - Servidores que mantienen base de datos **distribuidas**.
    - Estas bases de datos contienen el mapeo de nombres a direcciones IP

Resolución de Nombres con Archivo HOSTS

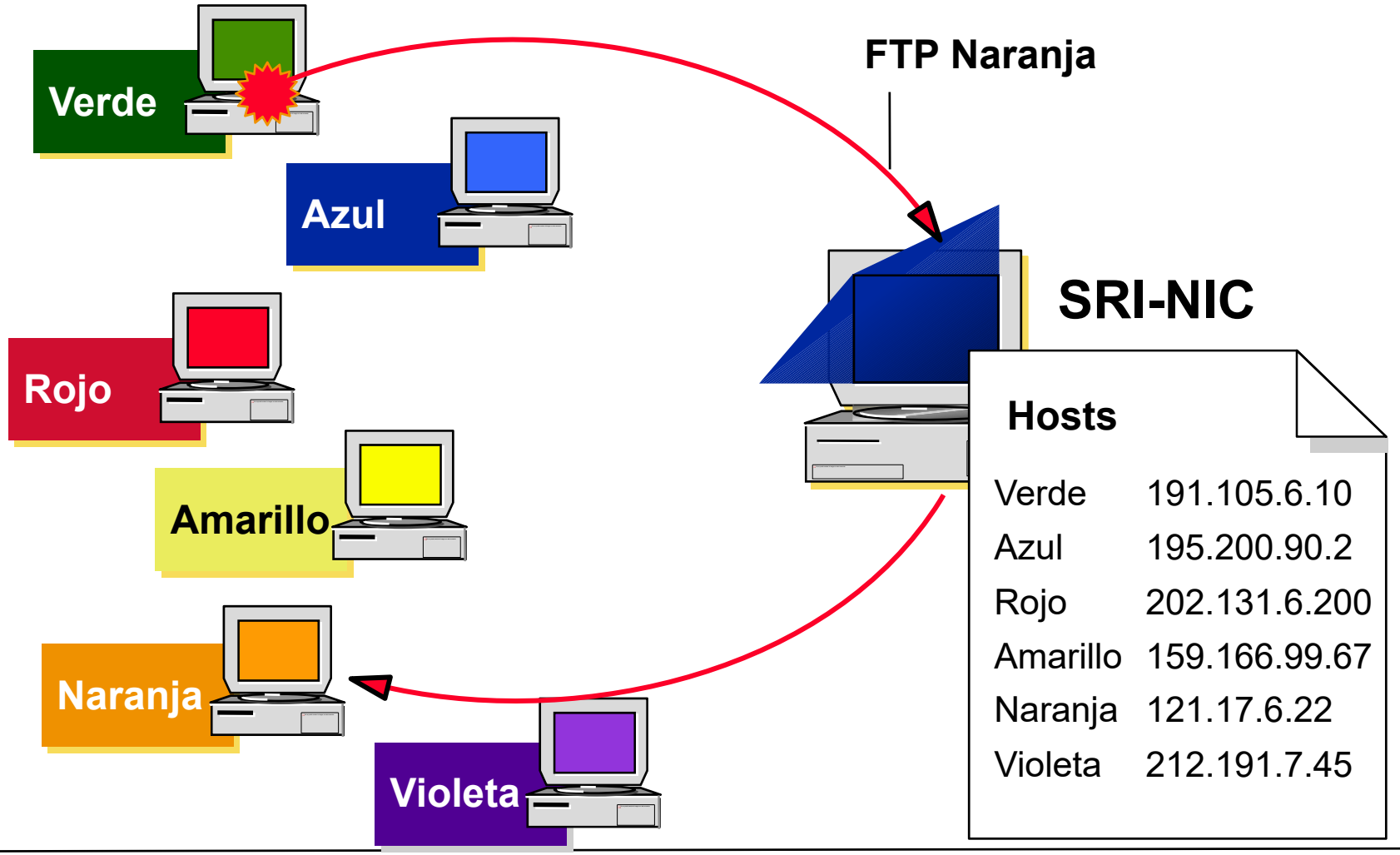


El Archivo Hosts



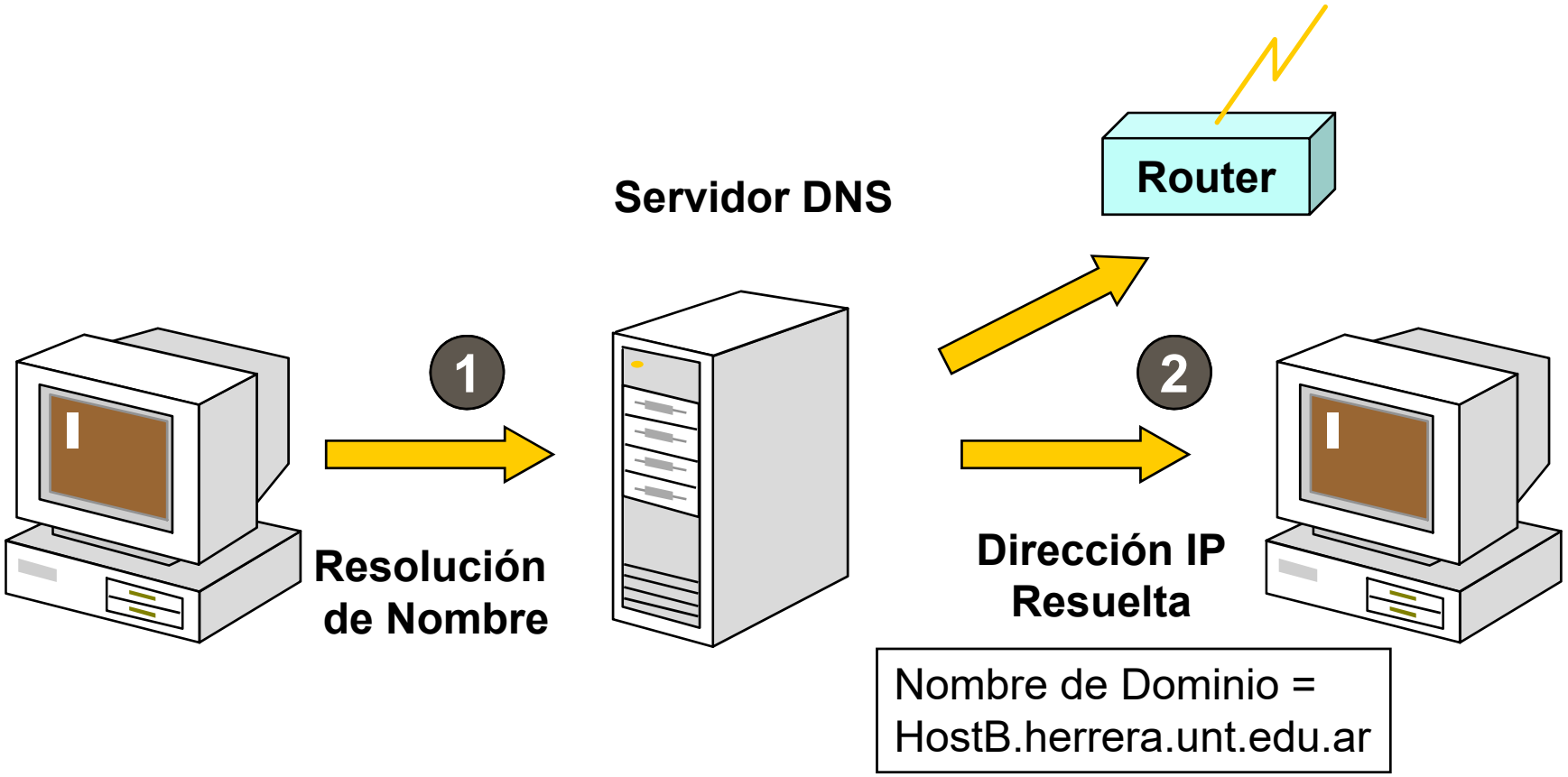
```
# Formato Genérico de Archivo HOSTS
#
 127.0.0.1     localhost loopback
  #
   102.54.94.97    lrc.herrera.unt.edu.ar


    131.107.2.100   linuxhost LINUXHOST # Host Linux
      131.107.3.1    gateway   GATEWAY   # Default Gateway
```

DNS ("Domain Name System"): Historia



Resolución de Nombres con DNS

```
ping HostB.herrera.unt.edu.ar
```

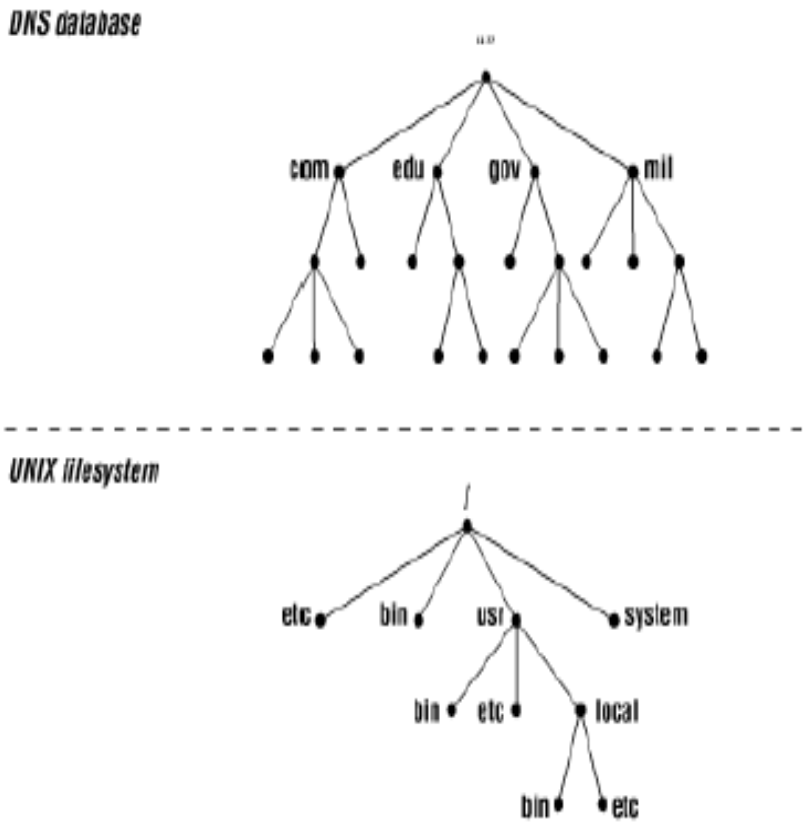


DNS (RFC 1032 al 1035 - '87): Características Principales

- DNS es un sistema de Base de Datos distribuidas del tipo Cliente/Servidor
- DNS es un esquema de resolución de nombres:
  - Eficiente
    - Mayoría de los nombres resueltos localmente
  - Confiable
    - La caída de un servidor, no hace que el sistema no funcione
  - Propósitos Generales
    - No solo restringido a nombres de hosts
  - Distribuido
    - Conjunto de servidores (en múltiples sitios) resuelven nombres en forma cooperativa.
  - Escalable
    - Permite la resolución de nombres a un gran número de hosts.

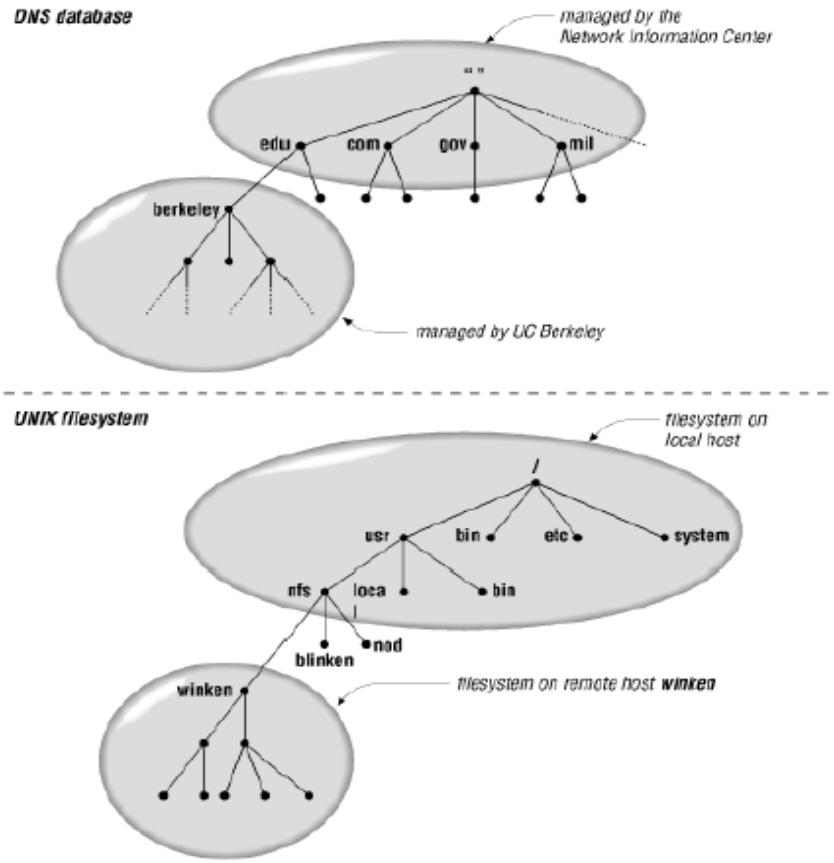
DNS vs Filesystem Unix

- Estructura de DNS es similar a la de un FS de UNIX.
  - Arbol invertido
  - Cada nodo está asociado con un nombre
    - Dominio/Directorio
  - El nodo raíz simbolizado por "." o "/" respectivamente
  - Cada nodo puede ser subdividido en otros nodos
    - Subdominios/Subdirectorios
  - Esquema de nombres de dominio y nombres de directorios
    - **DNS (desde abajo hacia arriba)**
    - FS (desde arriba hacia abajo)

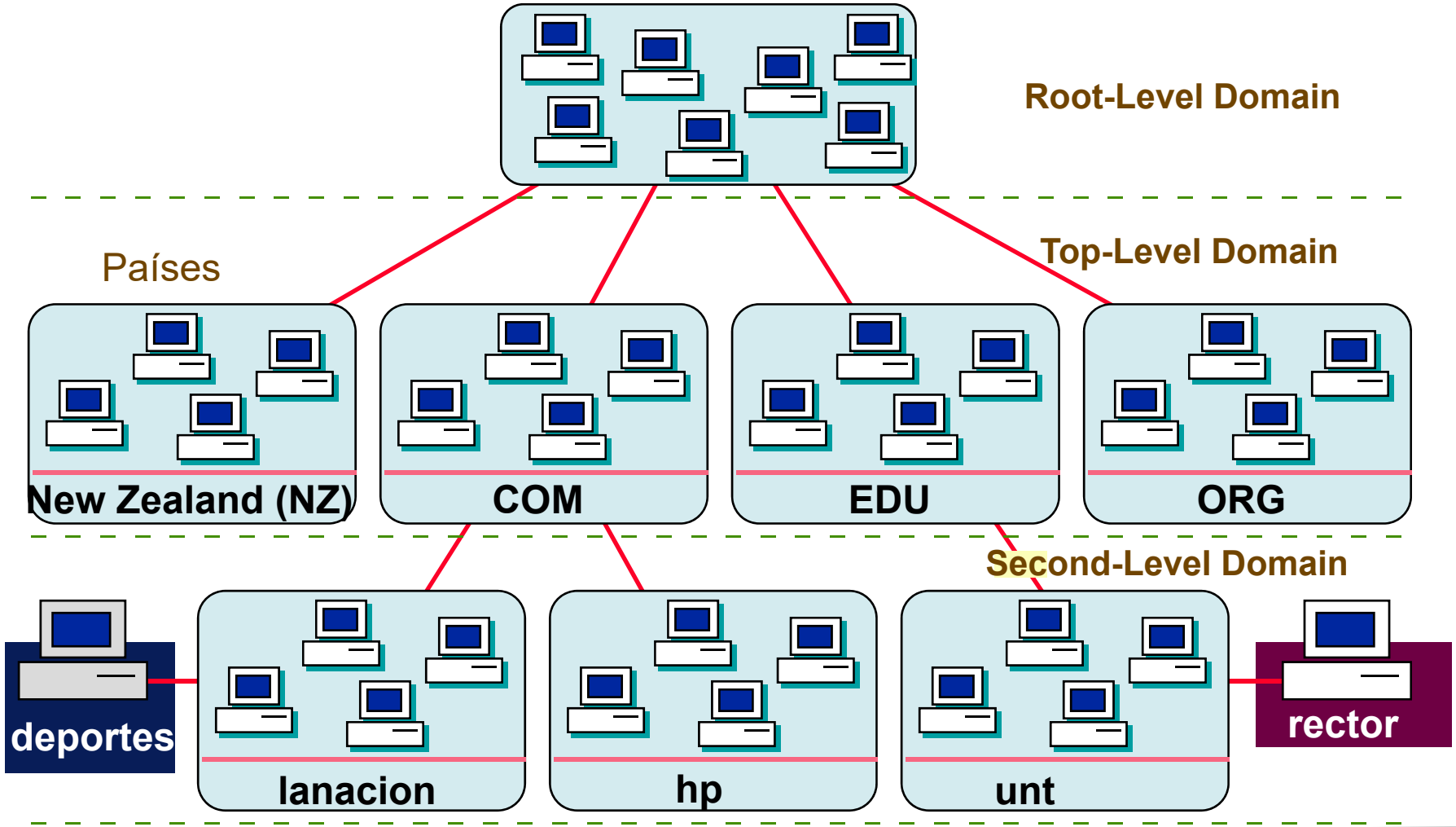


DNS vs Filesystem Unix

- En DNS cada dominio puede ser administrado por una organización diferente.
- Similar a UNIX respecto a NFS, en donde cada filesystem es administrado en forma autónoma
- También los links de archivos tienen su equivalencia en DNS donde se habla de "alias" (a nombres canónicos).



Nombramiento Jerárquico: Espacio de Nombre de Dominio



Dominios: Delegación de Autoridad

- Ejemplo:
  - Modelo de Jerarquía de Personal en una empresa
  - "Root level domain" – Presidente de Empresa
    - Tiene autoridad para crear/eliminar nuevas gerencias
    - Delegan autoridad a cada gerencia
  - "Top Level Domain" – Gerentes de Empresa
    - Tienen autoridad para crear/eliminar nuevas jefaturas dentro de sus gerencias
    - Pueden delegar autoridad a cada jefe en su gerencia
  - "Second Level Domain" – Jefes de Empresa
    - Tienen autoridad para crear/eliminar empleados que dependen de su jefatura.
    - También tienen autoridad para crear "subjefaturas"
    - Puede delegar autoridad a los "subjefes"

Observaciones

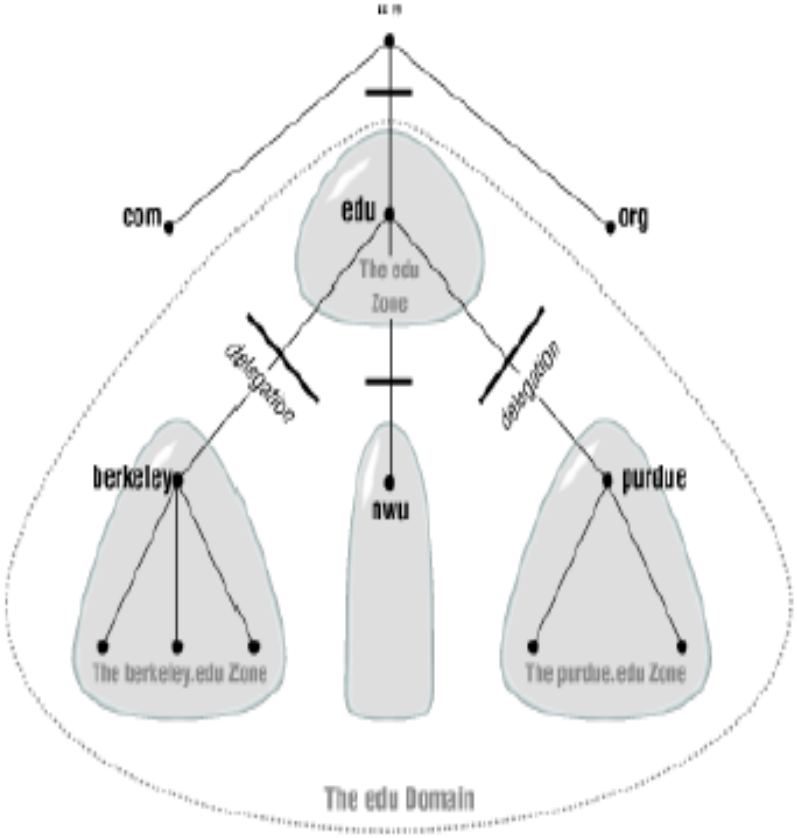
- El FQDN está formado por el nombre completo del host
  - Ejemplo: **deportes.lanacion.com**
- La partición de nombres en jerarquía permite distribuir la **administración** de nombre
- Cada dominio tiene autoridad sobre él y puede (debe) administrar los nombres del mismo
- Un dominio puede crear subdominios
- La partición de nombres en jerarquías no implica necesariamente una división por ubicación **física**
  - Los nombres de máquinas son asignados de acuerdo a la estructura de la organización no de acuerdo a la estructura física de la misma

Top Level Domains

- Constituyen los nombres de dominios oficiales de Internet.
- Son creados y mantenidos por autoridades de Internet
- Originalmente eran 7 entre los cuales están
  - .com, : Empresas comerciales
  - .edu: Instituciones Educativas
  - .gov: Instituciones gubernamentales
  - .mil: grupos militares
  - .net: Soporte de red
- Actualmente son más (.areo, .coop, .museum,...)
- También se crearon los ccTLD (country Code TLD) para representar países. Ejemplo:
  - .ar: argentina
  - .es: españa
- Muchos países crearon estructuras de árbol similares a la del árbol DNS por debajo de sus ccTLD

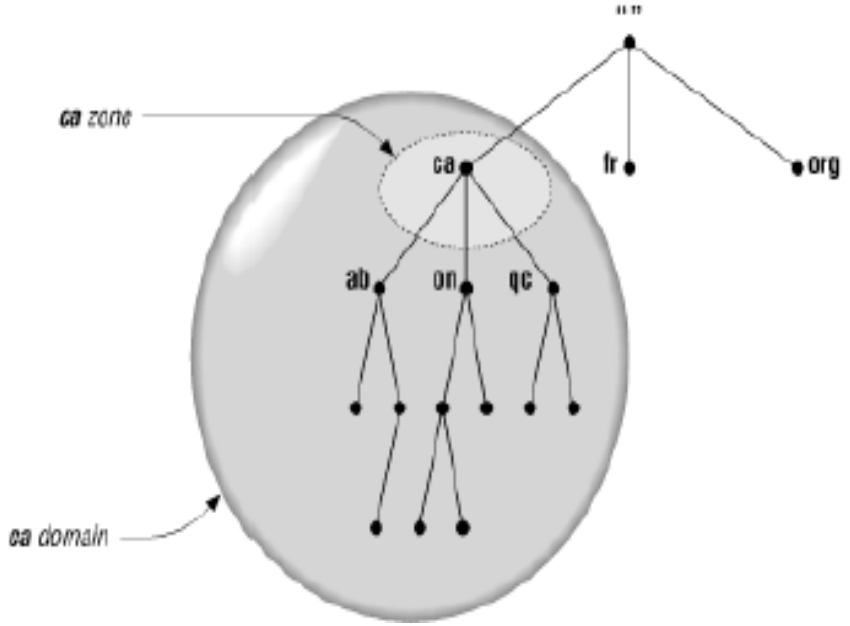
Dominio vs. Zona

- Los dominios son divididos en unidades mas simples de administrar.
- De esta forma se delega autoridad.
- Estas unidades "autoritativas" se denominan zonas.
- Ejemplo:
  - Dominio edu se divide en varias zonas (berkeley, nwu, purdue,...)
  - Al dividir en zonas, realizo una delegación de autoridad
  - Todas las zonas conforman el dominio **edu**.
  - A su vez cada subdominio puede ser dividido en zonas.



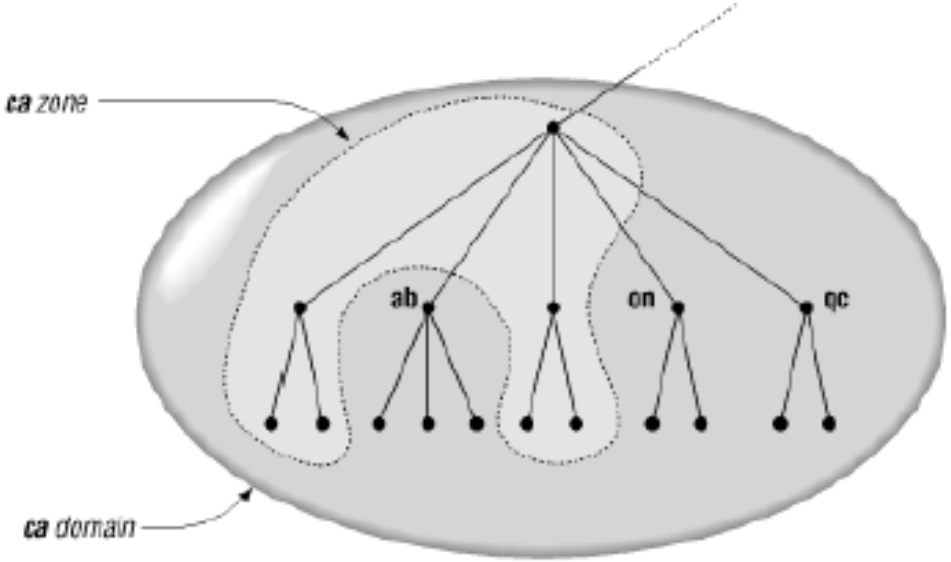
Dominios vs. Zona

- El dominio es un concepto lógico de ordenamiento de nombres, mientras que la zona es un concepto real o de implementación de la delegación de autoridad.
- Los servidores de nombre contienen datos de **zonas** y no de **dominios**.
- Un dominio contiene todos los datos del dominio como de los subdominios.
- Una zona solamente contiene datos de la zona.
- Ejemplo
  - La zona *ca* solo contiene datos de *ca* (principalmente punteros a las zonas delegadas)
  - El dominio *ca* contiene datos de ca y de ab.ca, on.ca y qc.ca

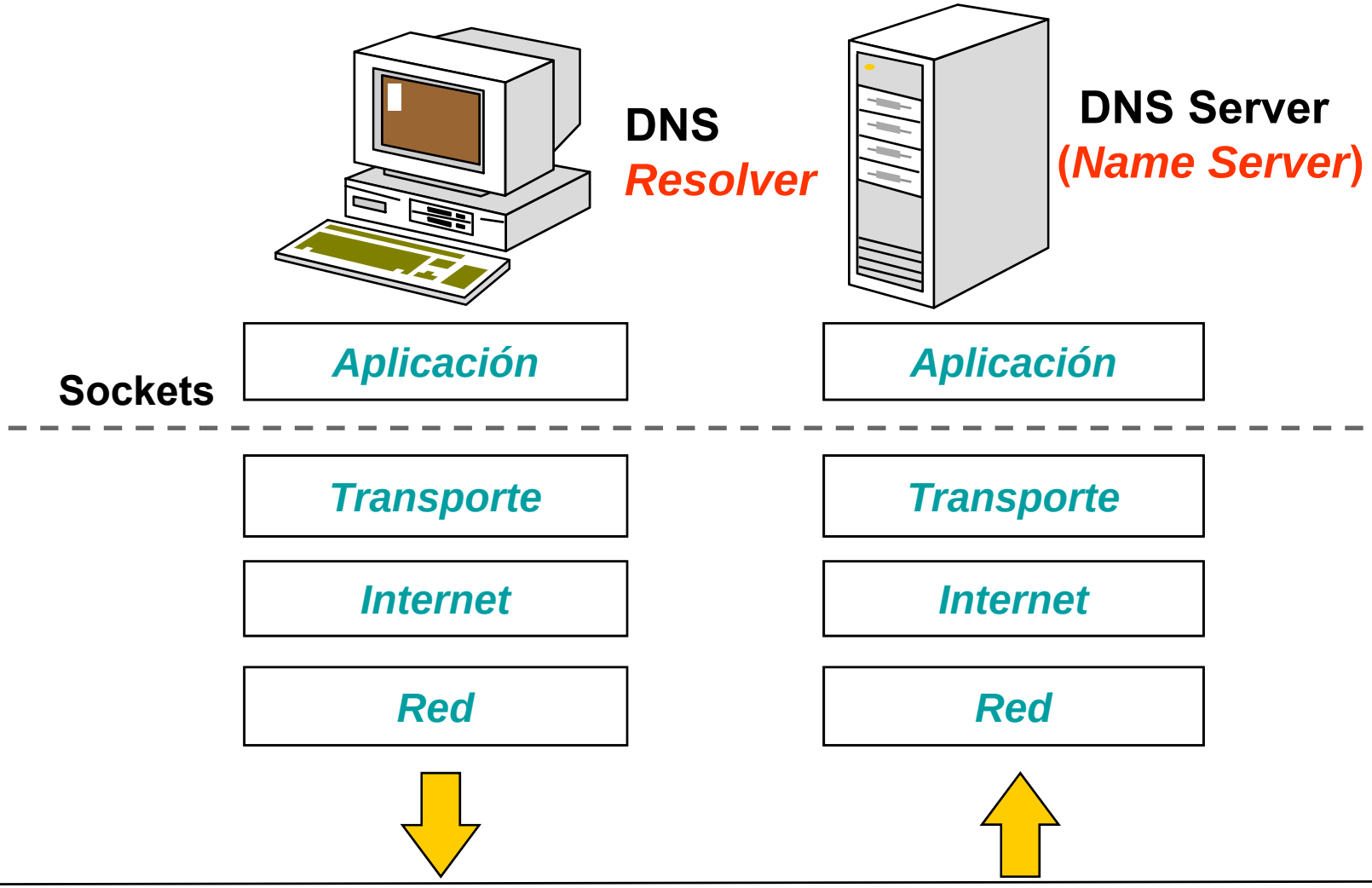


Dominios vs. Zona

- Es posible que un subdominio de un dominio no sea delegado
- En este caso, la zona contiene datos del dominio y del subdominio.
- Ejemplo:
  - La zona ***ca*** debe contener los datos de los **sub-dominios** no delegados de ***ca***.
  - Por esta razón es que los name servers utilizan archivos de **zonas** y no dominios.
  - Un dominio puede contener más datos que el servidor de nombre puede necesitar.



DNS: Funcionamiento



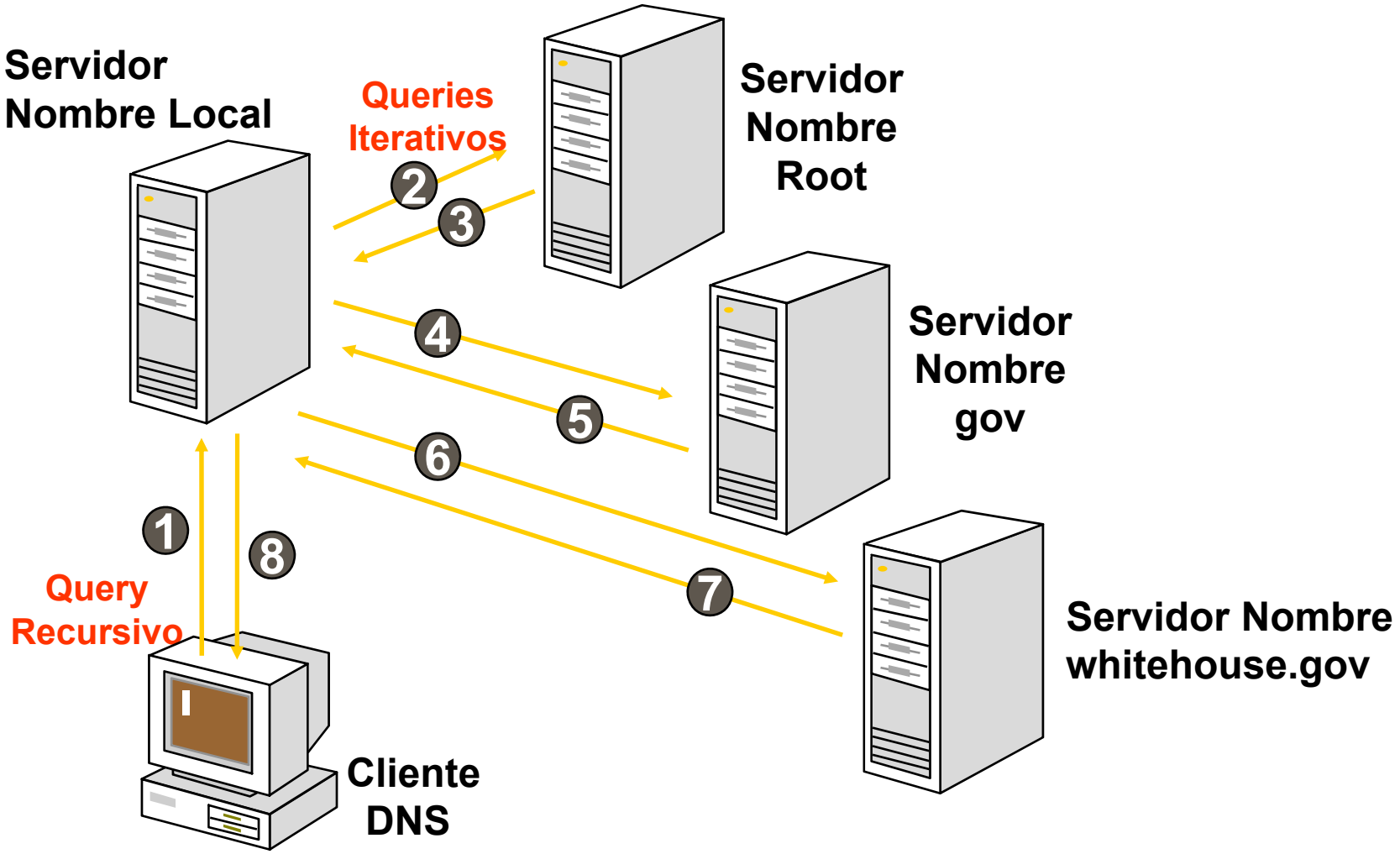
DNS: Funcionamiento

- DNS es una aplicación TCP/IP
- Utiliza UDP como protocolo de transporte (principalmente) (puerto "well known" 53)
- En DNS los clientes se denominan "Resolvers" y los servidores "Name Servers" o servidores de nombre
- La función de los "resolvers" es enviar "request" de nombres entre las aplicaciones y los servidores de nombre.
- Los "name servers" toman los "requests" de los resolvers y traducen el nombre de host a una dirección IP.
- Si un "name server" no puede resolver el request, puede reenviar el "request" a otro servidor de nombre para su resolución

Tipos de Queries

- Existen dos tipos de queries a un servidor DNS:
  - Query recursivo ("complete translation")
    - Se solicita que el servidor responda con el resultado de la traducción (o con error sino existe el dato)
    - Si un servidor recibe este tipo de query, normalmente no trasladan este tipo de consulta a otro servidor de nombres
    - Son comunes en clientes DNS ("resolvers")
  - Query iterativo (no-recursivo)
    - En este caso, el servidor entrega la dirección IP que el servidor de nombre debería contactar a continuación para resolver el nombre
    - Estos queries se generan entre servidores DNS, intentando resolver un query recursivo de un cliente

Resolución de Nombres



Resolución de Nombres

- ¿Cómo encuentra un "resolver" un servidor de nombre para empezar la búsqueda?
  - En el resolver se configura la dirección IP de por lo menos un servidor DNS
- ¿Cómo encuentra un servidor a otro servidor de nombres para continuar el procesos de resolución de nombre?
  - Cada servidor de nombre debe conocer la dirección de por lo menos un root server
  - Los root servers son varios (13), por performance y confiabilidad.
  - Sus nombres, direcciones y ubicación se lo puede encontrar en: http://www.root-servers.org/
- Las implementaciones actuales de DNS, permiten que cuando un servidor de nombre reciba un "query" recursivo, intente buscar la resolución de nombre en servidores lo más cercano posible al nombre buscado (es decir se dirija al root como último recurso).
  - De esta manera la resolución se hace más rápida.
  - Esto lo realiza gracias al mecanismo de caching que utiliza DNS

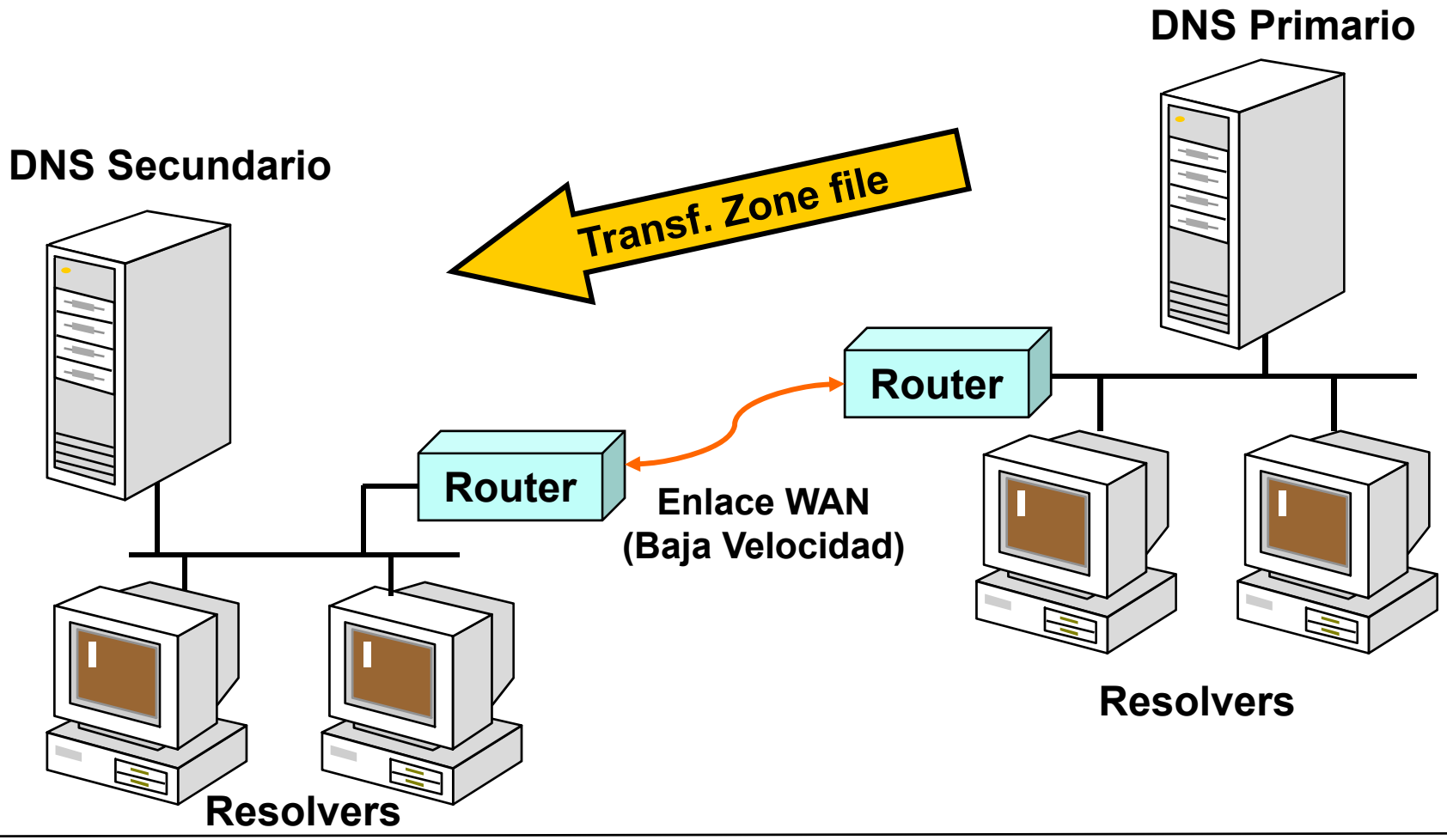
Tipos de Servidores de Nombres

- Servidor Primario
  - Obtiene la información del dominio directamente de un archivo de disco ("**zone file**").
    - El archivo de zona constituye la base de datos del dominio
    - Esta base de datos contiene el mapeo de nombres a direcciones IP.
  - Son Autoritativos
    - Tienen información completa y certera de su zona
  - Normalmente existe **un** servidor primario por Dominio (o zona).
    - Aunque es posible crear más de un Primario, la sincronización de archivos de zona debe realizarse manualmente, lo que torna compleja la administración.

Tipos de Servidores de Nombres

- Servidor Secundario (o servidor **esclavo**)
  - Información del dominio es obtenida de otro servidor de nombre ("**zone file transfer**").
    - Se transfiere la base de datos de un servidor primario o de otro **secundario**.
    - También puede leer el archivo de zona de un respaldo propio.
      - Esto se usa en caso de una caída del secundario (luego de levantar el archivo de zona, verifica si su contenido es auténtico).
  - Son también **autoritativos**.
  - Pueden existir más de un servidor secundario por Dominio.
  - Varias razones para tener servidores secundarios:
    - Redundancia
    - Velocidad de acceso en sitios remotos
    - Reducción de carga en el servidor primario

Ejemplo de Uso de Servidores DNS – Enlaces WAN



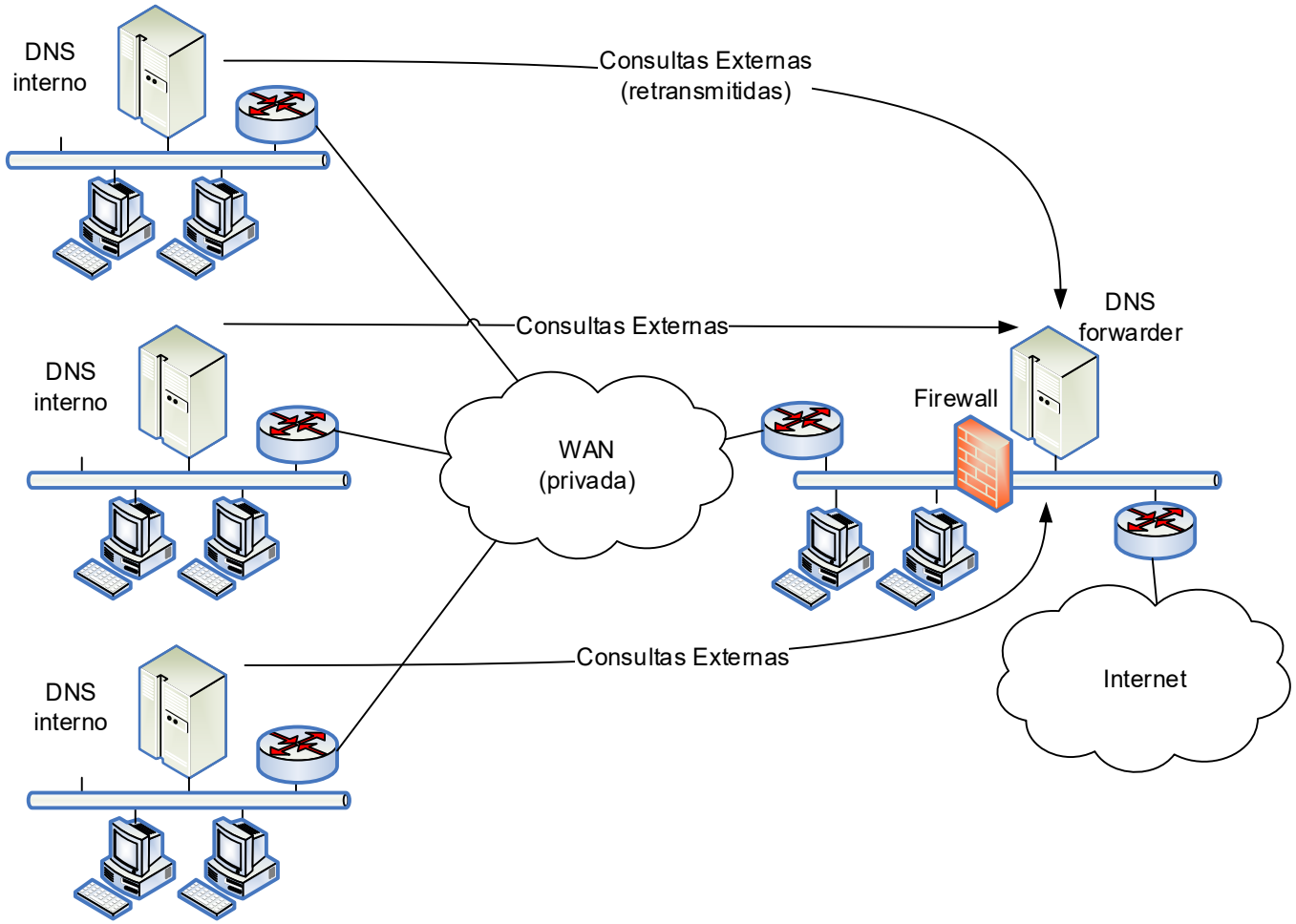
Tipos de Servidores de Nombres

- Maestro o "Master"
  - Solamente una denominación (no un tipo de servidor en si)
  - Fuente de información para un servidor secundario.
  - Puede ser un servidor primario o secundario.
- Solo de Cacheo ("caching-only servers")
  - Todos los servidores DNS almacenan en un cache los nombres resueltos
  - Los Servidores Cache-onliy solo almacenan los resultado de la resolución, pero **no** mantienen un archivo de zona.
  - El tiempo de vida de un mapeo lo define el servidor autoritativo de la zona
  - Los servidores Caching-Only son **no** autoritativos.
  - Van construyendo su cache en forma gradual.

Tipos de Servidores de Nombres

- "Forwarders"
  - Se utilizan cuando los servidores DNS reenvían o retrasmiten los queries a otros servidores (forwarders) que son los que realizan los queries propiamente dicho.
  - Se utilizan en instalaciones donde el ancho de banda de salida es limitado y no se desea que los servidores DNS locales resuelvan los queries (ya que derivan en un alto intercambio de queries-response – "queries iterativos").
    - Los servidores autoritativos resuelven solo los queries locales. Los demás son resueltos por los forwarders.
    - La idea es que los forwarders contengan un cache con gran cantidad de direcciones.
  - Los servidores DNS que utilizan un "forwarder" deben poseer la dirección IP de los servidores que actuarán como "forwarders".
    - Los servidores DNS autoritativos de una zona deben ser configurados de manera especial en la presencia de "forwarders", ya que las consultas no resueltas por su cache o zona, son dirigidas a los forwarders en forma de "query" recursivo, para que este ultimo encuentre la traducción.
  - También se utilizan forwarders como una mejora a la seguridad de DNS.
    - Normalmente son instalados antes del Firrewall (de cara a Internet)

Forwarders: Ejemplo



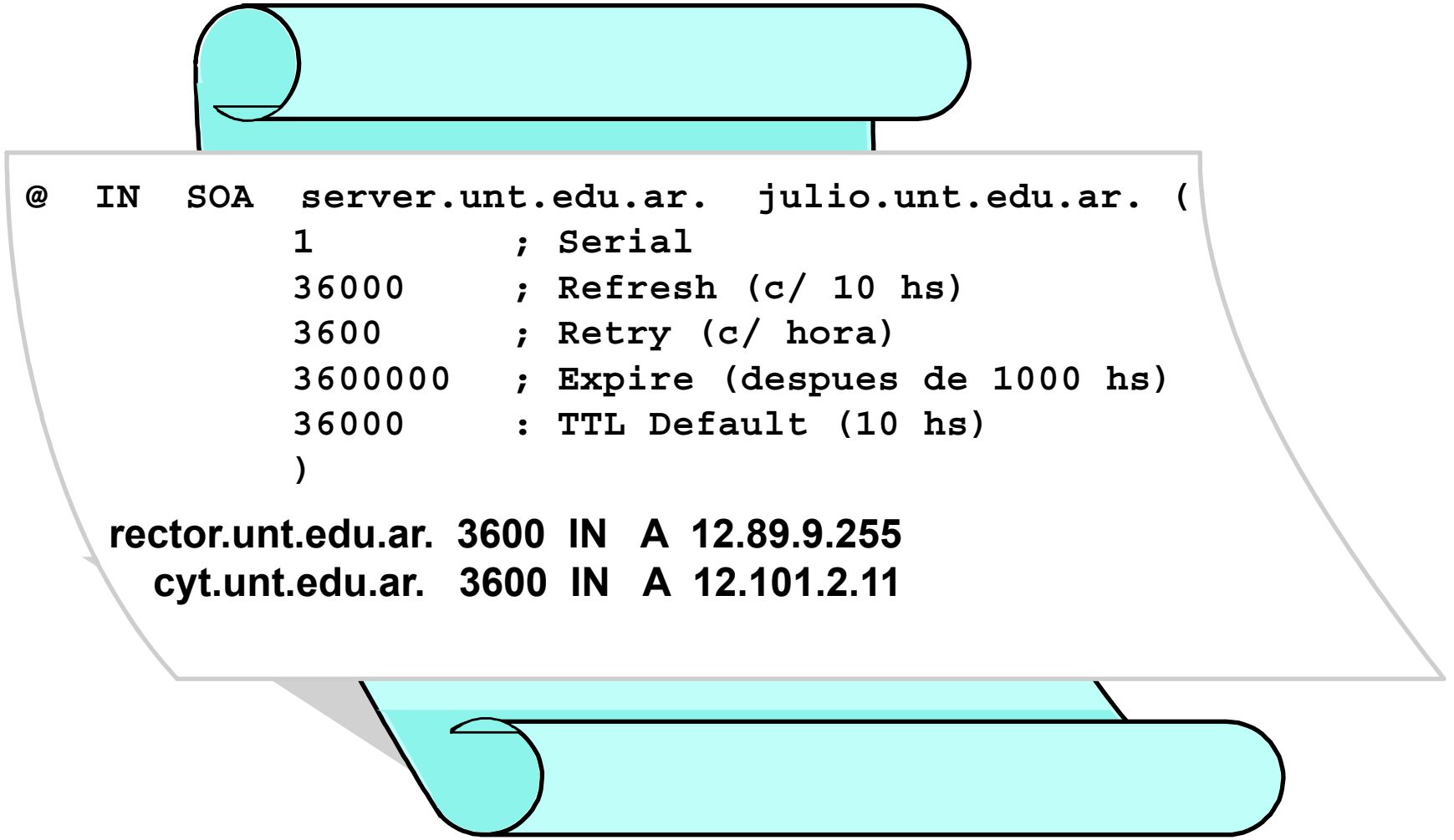
Caching y TTL

- Los Servidores DNS "cachean" los Queries Iterativos
  - Al almacenar los queries iteractivos, está almacenando no solo los servidores que proveen la traducción, sino todos los servidores que utilizó para tal traducción.
  - De esta manera, se acorta la búsqueda en queries posteriores.
- A cada Entrada "Cacheada" se le da un "Time to Live (TTL)"
- El TTL es parte de la configuración del servidor autoritativo para la zona (primario/secundario)
- Cuando el TTL expira, la entrada es borrada del Cache
- Dependiendo de la implementación, el Resolver también puede cachear el mapeo hasta que expira el TTL (normalmente lo hace).
- Observar que una traducción a través del cache puede **no** ser correcta (cambio antes de expirar el TTL).
  - El mecanismo de Caching funciona correctamente, porque los nombres no cambian con mucha frecuencia en Internet.
- Los resolver y servidores de nombre, también pueden cachear respuesta negativas ("negative caching") (opcional y TTL de 10 minutos)

Archivos de DNS

- Un servidor DNS, posee varios archivos de configuración. Estos archivos configuran el comportamiento del servidor y además constituyen la base de datos para definir el mapeo de nombres a direcciones.
- Son los siguientes:
  - Archivo de Base de Datos
    - Contiene **registro de recursos** para la zona
    - Típicamente mapea nombres de hosts a direcciones IP.
  - Archivo de "Reverse Lookup" File
    - Mapea direcciones IP a nombres de hosts.
  - Archivo Cache
    - Nombres y direcciones de los servidores del "root domain".
  - Archivo Boot
    - Utilizado para la configuración de arranque del DNS

Archivo de Zona



Tipos de Registros de Recursos

Registro	Tipo	Función
Start of Authority	SOA	Comienzo de datos de zona. Define parámetros para toda la zona
Name Server	NS	Identifica un servidor de nombre a través de su Nombre.
Address	A	Convierte un nombre a una dirección
Pointer	PTR	Convierte una dirección a un nombre
Mail Exchange	MX	Identifica a donde entregar correos para un dado dominio. Interacción con SMTP.
Canonical Name	CNAME	Define un alias para un nombre de host
Host Info	HINFO	Describe Hardware y OS de un host

Registro de Recurso (RR)

- El formato general de un registro de recurso es:

  [*name*] [*ttl*] [class] *type data*

  - Donde:
    - **Name**: Nombre del objeto del dominio al cual hace referencia el registro de recurso.
      - Puede ser un host o un dominio
      - El *name* es relativo al dominio actual, a menos que termine con un "**.**"
    - **Ttl**: define el tiempo (en seg) que la información en este recurso debería ser mantenido en el cache.
    - **Class**: Identifica el registro como un registro de recurso de Internet DNS.
    - **Type**: Identifica el tipo de Registro de Recurso.
    - **Data**: Información específica de acuerdo al tipo de recurso.
  - Observar que siguiendo la notación de UNIX, los parámetros entre corchetes son opcionales.

Registro SOA

- Formato standard:

[*zone*] [*ttl*] IN SOA *Origin* *Contact* (
serial
refresh
retry
expiry
ttl
)

- Ejemplo:

```
@  IN  SOA  server.unt.edu.ar.  jcalvo.unt.edu.ar. (
                1          ; Serial
                36000      ; Refresh (c/ 10 hs)
                3600       ; Retry (c/ hora)
                3600000    ; Expiry (despues de 1000 hs)
                36000      : TTL Default (10 hs)
                )
```

Registro SOA

- zone
  - Nombre de la zona
  - Generalmente contiene el carácter **@**, referenciando al nombre de dominio definido en el archivo **boot** .
- ttl
  - Normalmente queda en blanco en este registro
- IN
  - Clase de dirección
  - Siempre IN para Registro de Recursos
- SOA
  - Registro de recurso tipo SOA
- Origen
  - Nombre de host del "Primary name server" para este dominio
  - Debe ser un **FQDN**
  - Observar que termina con "**.**"

Registro SOA

- Contact
  - Dirección de email de la persona responsable del dominio
  - Se reemplaza el @ por un primer punto
  - No es usado por DNS sino como información de contacto
- Serial
  - Número de versión de la zona
  - Máximo 8 dígitos
  - El formato depende del administrador
    - Ejemplo: 20050806 (YYYYMMDD)
  - Cada vez que cambia el archivo de zona, el serial debe incrementarse
  - Se utiliza por los servidores secundarios para saber si la zona ha sido modificada
  - En caso que exista un cambio en el serial, se solicita una transferencia de zona completa.

Registro SOA

- Refresh
  - Tiempo (en seg) que transcurre entre el chequeo del servidor secundario al primario por un cambio de zona.
  - Valor típico: 86400/43200 (una o dos veces por día)
- Retry
  - Tiempo (en seg) que reintenta el servidor secundario en contactar nuevamente al primario en caso que no responda
  - Valor típico: 3600/1800 (una o media hora)
- Expire
  - Tiempo (en seg) en que se considera válida la información del servidor secundario sin que reciba un refresco de zona
  - Valor típico: 3.600.000 (42 días)

Registro SOA

- Minimum
  - Valor del **ttl** (en seg) por **default** utilizado para todos los registros a los que no se le definió explícitamente este valor
  - Este valor define el intervalo de tiempo que el registro dura en el cache del host remoto.
  - Valor típico: 604.800 (una semana)
  - En las versiones modernas de BIND este parámetro establece el tiempo de caching de una respuesta **negativa**.
    - En ese caso, el valor por defecto del TTL se establece como una variable **$ TTL** al comienzo del archivo de zona.
  - También se pueden expresar tiempos con prefijos de letras: s (segundos), m (minutos), h (horas), d (días) y w (semanas).
    - Ejemplo, el campo refresh de una hora y media podría ser expresado como 1h30m o el campo "expiry" de 3 semanas y 2 días como 3w2d.

Registro A ("Address Record")

- La mayoria de los registros en un archivo de zona son los registros tipo **A**, ya que son los que convierten nombres de hosts en direcciones IP
- El formato es:

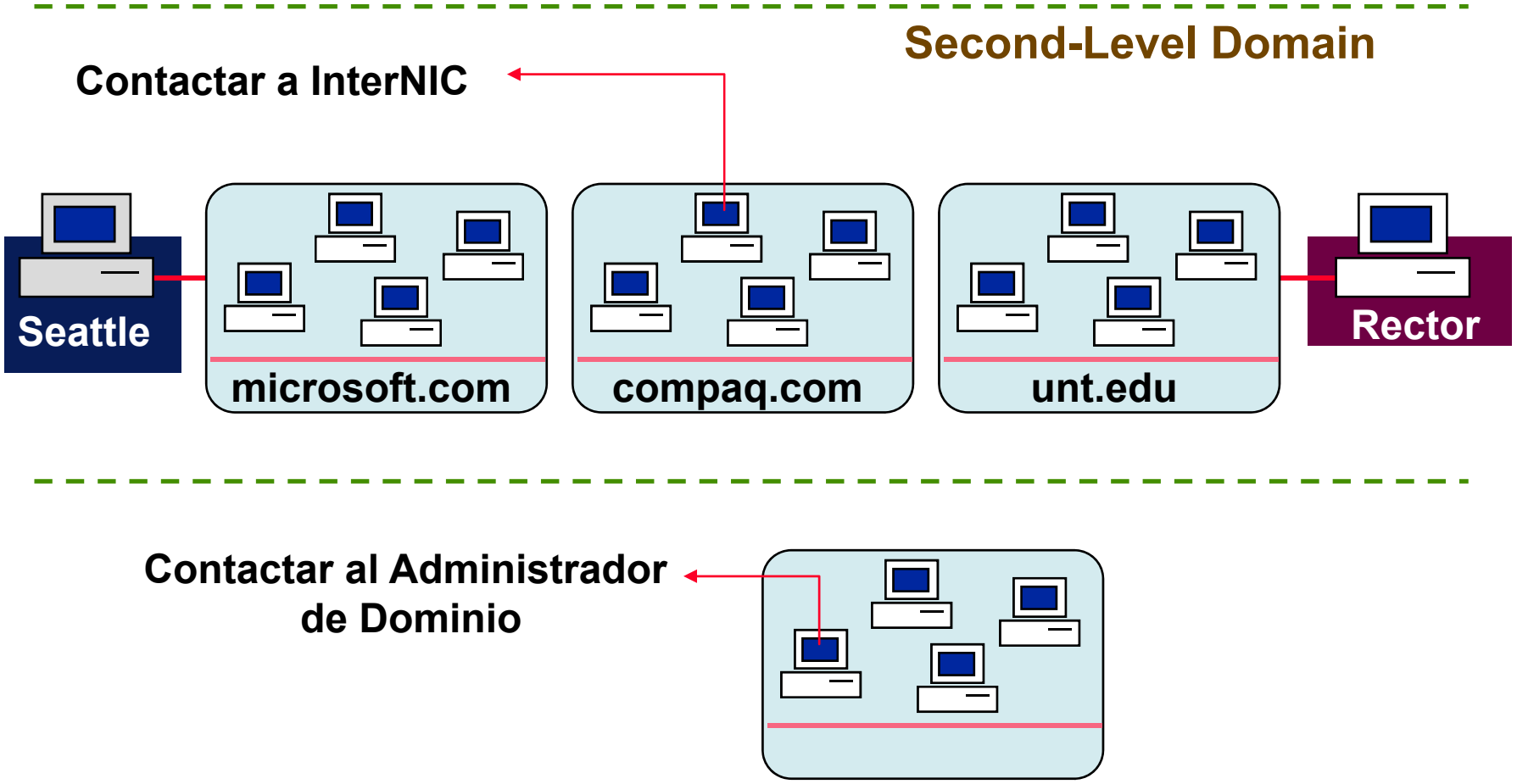
  Host [*ttl*] [*IN*] **A** *address*

  - Donde:
    - Host: Nombre del host cuya dirección es provisto en el campo *address*
    - Ttl: Si está vacío, utiliza el definido en el SOA
    - IN: Clase de direccion IN
    - A: Tipo de Registro
    - Address: Dirección IP del host
- Ejemplo:
  - **hp1 A 134.10.9.0**
  - Define el mapeo de hp1 a la dirección 134.10.9.0 para la zona definida
  - Observar que hp1, no termina con un "." por lo que se incluirá al nombre de este host, el nombre del dominio completo.

Registro NS ("Name Server")

- Identifica los servidores autoritativos para una zona
- Estos registros cumplen dos propósitos:
  1. Son los que especifican los nombres de los servidores de nombre para cada zona.
     - Toda zona debe tener por lo menos un registro NS que indica el nombre del servidor Primario de la zona.
     - Obviamente puede tener varios de estos registros (servidores esclavos).
  2. Son los punteros que unen la jerarquía de dominio, con su correspondiente delegación de autoridad.
     - Los registros NS en el dominio "top-level" apuntan a servidores en el dominio de segundo nivel.
     - Los dominios de segundo nivel, mantienen registros NS que apuntan a subdominios y asi sucesivamente.

Registración con el Dominio Padre (Registro tipo NS)



Registro NS

- El formato del registro NS es:

  [***domain***] [*ttl*] **IN NS** *server*

  - Donde:
    - Domain: Nombre del dominio donde el servidor *server* es autoritativo (puede contener el carácter @).
    - Ttl: Generalmente en blanco
    - IN: Clase de dirección
    - NS: Tipo de registro
    - Server: Nombre de host del computador autoritativo para este dominio.
- Ejemplos:
  - En servidor de nombre del dominio unt.edu.ar, si name_server1 es el primario y name_server2 es el secundario:
    - unt.edu.ar. NS name_server1
    - unt.edu.ar . NS name_server2
  - O:
    - @ NS name_server1
    - @ NS name_:server2
  - O:
    - NS name_server1 ; si el RR sigue al SOA (Blank equivale al ultimo parámetro, es decir @)

Registro NS: Delegación y Glue Records

- Se tiene el dominio unt.edu.ar y se crea un nuevo dominio con su zona: herrera.unt.edu.ar
- Los servidores de nombre (Pri y Sec) para herrera son dns1 y dns2 respectivamente.
- Se crean los registros NS en el archivo de zona del servidor **dns1** (obviamente que existen los NS para la zona unt.edu.ar no mostrados):
  - @ IN NS dns1.herrera.unt.edu.ar.
  - @ IN NS dns2.herrera.unt.edu.ar.
- Estos registros declaran para la zona herrera, quienes son los servidores de nombre de la misma.
- Para poder delegar autoridad de unt.edu.ar a estos servidores de nombre, debemos crear en archivo de zona de dns primario de **unt.edu.ar** los siguientes registros:
  - herrera IN NS dns1.herrera.unt.edu.ar.
  - herrera IN NS dns2.herrera.unt.edu.ar.
  - dns1.herrera.unt.edu.ar. IN A 10.10.10.1; glue record 1
  - dns2.herrera.unt.edu.ar. IN A 10.10.10.2; glue record 2

Registro NS: Observaciones

- Debe quedar en claro que el registro NS declara cuales son los servidores de nombre para una zona, pero no declara si estos servidores son **primarios** o **secundarios**.
- Esta declaración se realiza en la configuración propiamente dicha del servidor (archivo de inicialización).
- No necesariamente todos los servidores (primario y secundarios) deben estar asociados con registros NS, sino solo los que se quieren acceder por otros servidores de nombres en la jerarquía.
  - Se pueden tener otros servidores de nombres utilizados internamente por hosts del dominio ("resolvers"), que no esten asociados a registros NS.

Otros Registros

- MX: Mail Exchanger Record
  - Redirige correos electrónicos a un servidor de mail (SMTP)
  - Ver mas adelante.
- CNAME: Canonical Name Record
  - Define un alias para un nombre oficial (canónico) de un host
  - Formato: alias IN CNAME nombre_canonico.
  - Ejemplo: lrc.herrera.unt.edu.ar. IN CNAME labredcomp.herrera.unt.edu.ar.
    - lrc.herrera.unt.edu.ar es un alias para el nombre canónico labredcomp.herrera.unt.edu.ar.
- PTR: Domain Name Pointer Record
  - Utilizado para convertir direcciones de IP numéricas a nombres de hosts
  - Utilizados para construir el archivo de reverse lookup (en el dominio in-addr.arpa)
  - Formato: z.y.x.w.in-addr.arpa IN PTR nombre_host

Otros registros

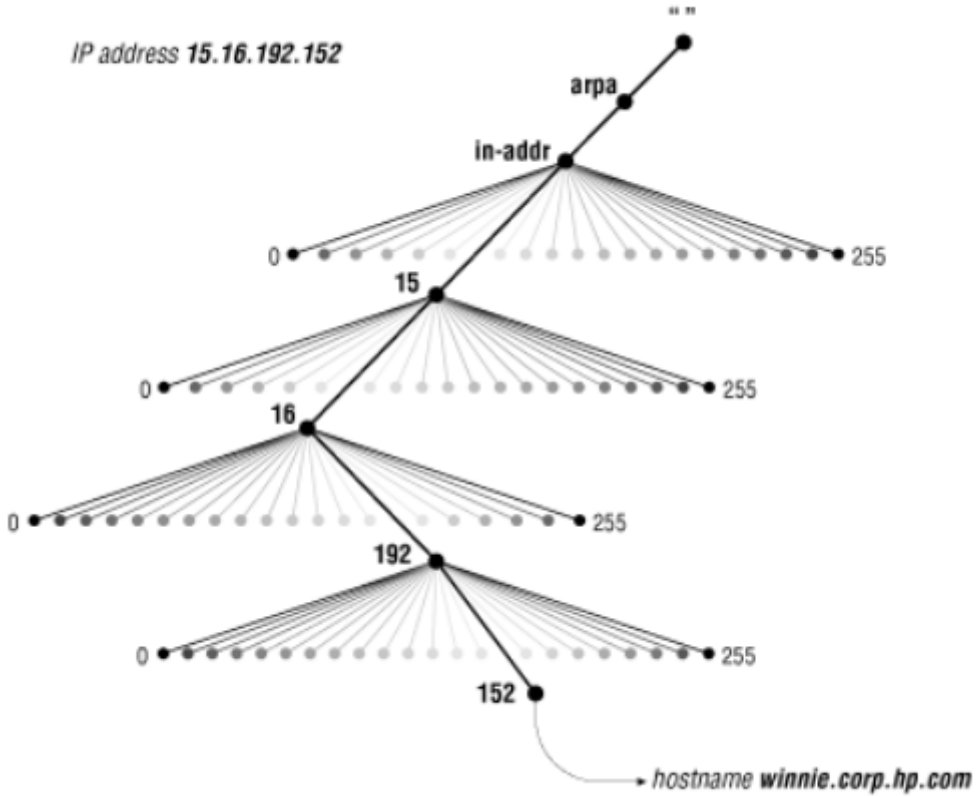
- SRV: Services Record
  - Nombre de servicios de red provisto por un host en particular
  - _servicio._protocolo.nombre SRV prioridad peso puerto nombre_servidor
  - Ejemplo:

```
_ftp._tcp.herrera.unt.edu.ar.   SRV  1  0  21  ftp1.herrera.unt.edu.ar.
                                SRV  2  0  21  ftp2.herrera.unt.edu.ar
```

- AAAA: Address Record IPv6
  - Similar sintaxis al RR A pero explicitando una dirección IPv6 del host

Dominio in-addr.arpa

- Utilizado para traducción inversa (IP->Nombre de Dominio).
- Observar que la dirección se busca en orden invertido, es decir se comienza por el MSB (octeto izquierdo) … hasta el LSB.
- En el ejemplo, el host winnie.corp.hp.com tiene direccion 15.16.192.152 (lo que crearía un registro PTR: 152.192.16.15 en el archivo in-addr.arpa)



Transferencia de Archivos de Zona ("Zone File Transfer")

- "Full Zone File Transfer"
  - El Master Name Server trasmite el archivo de zona al servidor secundario.
  - Puede consumir gran ancho de banda
- Proceso para transferencia de zona:
  - Servidor secundario espera el **Refresh Time** del SOA y solicita registro SOA del servidor Master
  - El master envía el registro SOA al secundario
  - El servidor secundario compara los Números de serie de los SOA. Si el SN del SOA del Master es mayor que SN de su SOA, solicita un Full Zone Transfer (AXFR Request: Campo Query Type dentro de la sección de consulta. Ver mas adelante)
  - Master envía el archivo de Zona al slave.
- Si el Master no contesta al Secundario, el secundario reintenta (Retry del RR SOA), o descarta la Zona luego de vencido el campo Expire del RR SOA.

Notificación de Cambios de Zona (DNS Notify)

- Revisión del estándar (RFC 1996 – ano 1996) que permite que un Master Server notifique a ciertos servidores secundarios cuando existe un cambio en el archivo de zona.
- Se mejora la consistencia de datos entre servidores Master y Secundarios.
- Puede existir una lista de notificación ("Notify List") que contenga la lista de servidores a notificar (opcional).
- La notificación se realiza mediante el envío de un mensaje DNS modificado. El servidor esclavo, actúa como si su timer de refresco de zona hubiese expirado.

Transferencia de Archivo de Zona Incremental

- RFC 1995 permite enviar solo los registros modificados del archivo de zona desde la última modificación (el master va registrando los cambios desde el último "zone file transfer").
- Funciona en forma similar al "full zone transfer" excepto que ahora el servidor secundario (o esclavo) envía un "request" IXFR en lugar de AXFR (al expirar el timer de refresco de zona)
- El servidor Master envía solo los registros modificados desde el último "file zone transfer"
- Cuando un servidor secundario recibe una transferencia de zona incremental, crea una nueva versión del archivo de zona, comenzado a reemplazar o copiar RR.
- Luego elimina el archivo de zona viejo.
- No todos los servidores soportan transferencia incremental.
- **IMPORTANTE**: Transferencia incremental funciona en conjunción con "dynamic update" (ver prox. Ppt).

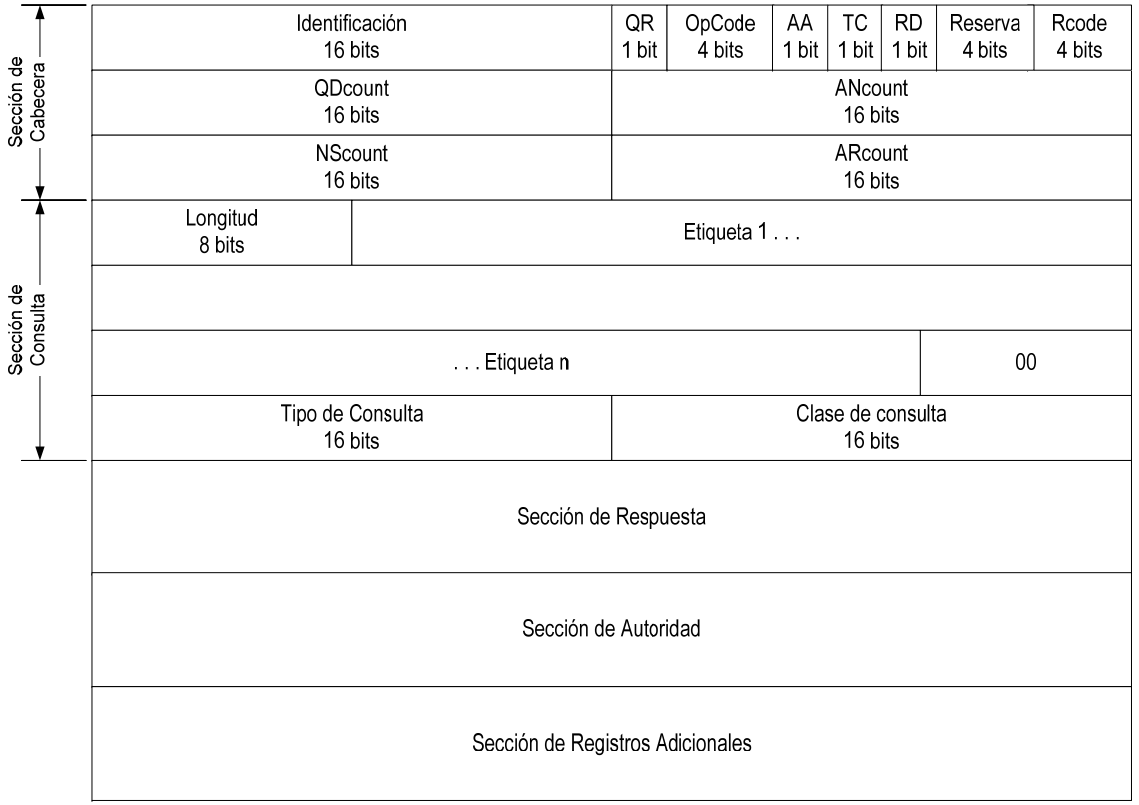
DNS Dinámico (Dynamic DNS Update)

- Problema:
  - DNS soporta consultas a una base de datos de nombres /direcciones estática o con cambios pocos frecuentes.
- Con DNS Dinámico introducido por el RFC 2136 (Año 1997), el servidor primario puede modificar su archivo de zona por orden de otro host que soporta actualizaciones dinámicas.
  - Por ejemplo, puede recibir actualizaciones de un servidor DHCP.
- Las actualizaciones son enviadas a través de un mensaje de UPDATE, y puede incluir la adición o borrado de uno o varios RR.
- Como parte del UPDATE se incremente el SN de la Zona.
- El estándar especifica procedimientos seguros para que estos updates puedan ser llevados a cabo.
- "Active Directory" de Microsoft utiliza este mecanismo para asociar nombres y direcciones IP.
- También es utilizado en la Internet para el caso en que los ISP's entreguen direcciones IP a clientes en forma dinámica y se desee mantener un único nombre.

Formato de Mensajes DNS

- Los Mensajes DNS van encapsulados en datagramas UDP (y en ciertas ocasiones TCP)
- El puerto bien conocido que se utiliza es el 53 (UDP/TCP)
- Los datagramas UDP en DNS tienen un tamaño máximo de 512 Bytes. Si los mensajes DNS no pueden ser encapsulados en esos 512B, se configura un bit de truncado (TC) en el Header del Mensaje DNS y se puede solicitar retrasmisión a través de TCP.
- Observar que al ser UDP no confiable, DNS debe detectar y retrasmitir los mensajes DNS perdidos.
- El formato de mensaje DNS es único, independientemente de si es un "query" o un "response".
- Consta de cinco posibles secciones:
  - Encabezamiento
  - Consulta
  - Respuesta
  - Autoridad
  - Registros Adicionales

Formato del Mensaje DNS



Referencias:

QR: Query/Response bit
AA: Respuesta Autoritativa
TC: Bit de Truncado
RD: Recursión Deseada
RA: Recursión Disponible

Rcode: Código de Respuesta
QDcount: Número de entradas en sección consulta
ANcount: Número de RR en sección de respuesta
NScount: Número de RR de Servidor de Nombre en sección de Autoridad
ARcount: Número de RR en

Sección de Encabezamiento

- Sección obligatoria del mensaje y la única de tamaño **fijo** (12 Bytes)
- Contiene entre otros campos a:
  - Identificador del mensaje (usado por el resolver y el server)
  - QR: Indica si es un "query" o un "response"
  - Op Code: Indica si es un "query" estándar, inverso (obsoleto), una solicitud de estado del servidor, DNS Notify (notificación de cambio de zona) o DNS UPDATE (Dynamic DNS)
  - TC ("Truncation Flag"): Truncado del mensaje DNS
  - QDCount: Número de Entradas en Sección "Question"
  - ANCount: Número de RR en sección "Answer"
  - NSCount: Número de RR en sección "Authority"
  - ARCount: Número de RR en sección de registros adicionales

Sección de Consulta ("question")

- Opcional (por ejemplo si es una respuesta)
- Contiene la consulta para el servidor de nombre (cuando el mensaje DNS es un query)
- Contiene:
  - Nombre de dominio
  - Tipo de Consulta (tipo de RR: A, NS, PTR, MX, etc.)
    - Aquí puede aparecer una consulta tipo AXFR o IXFR para Zone Transfer (full o incremental).
  - Clase de Consulta (Internet: IN)

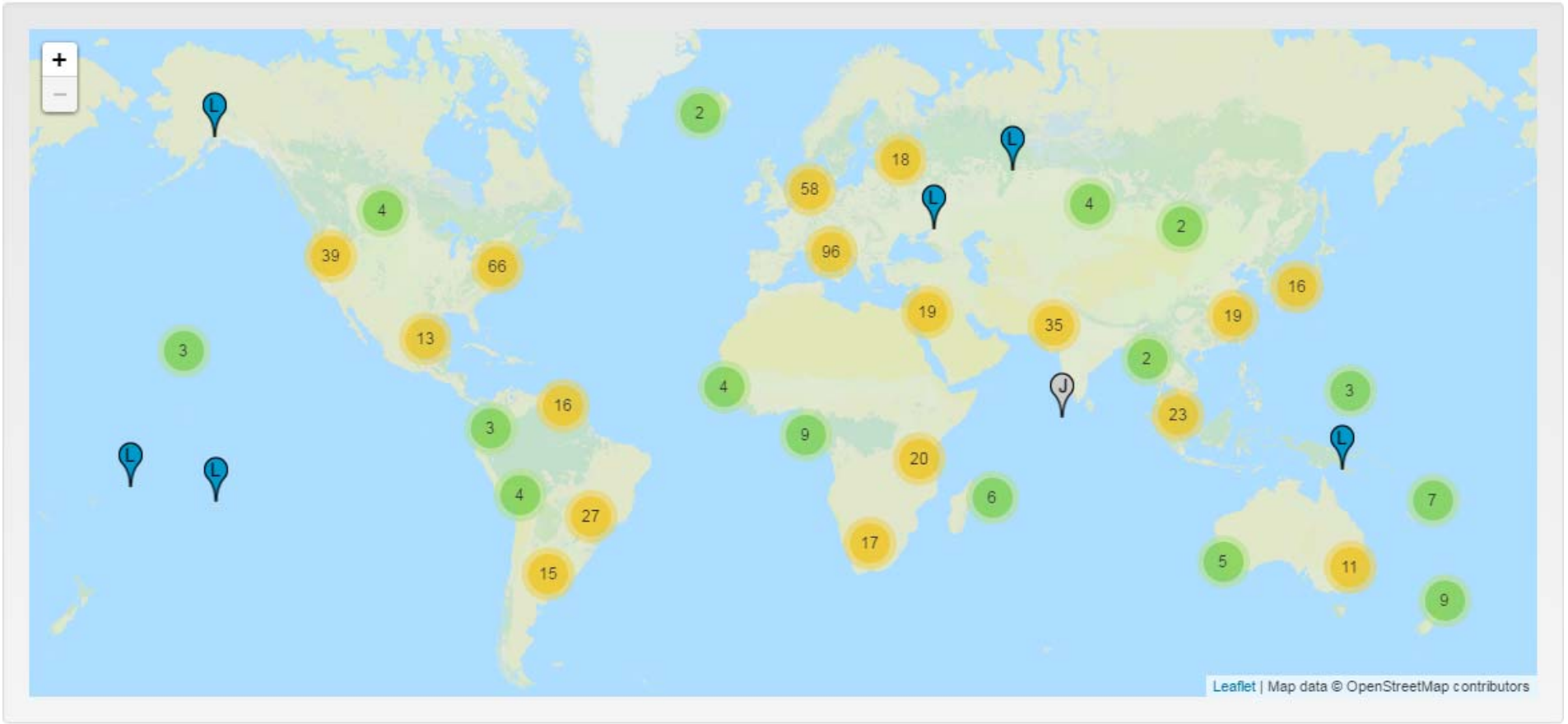
Otras Secciones

- Sección de Respuesta
  - Contiene RR que contestan la consulta
  - Una respuesta puede devolver múltiples RR
- Sección de Autoridad
  - Contiene RR que apuntan a un Servidor(es) de Nombre(s) Autoritativo(s) que permiten seguir con el proceso de resolución ("queries" iteractivos).
- Sección de Registros Adicionales
  - Contiene RR relacionados con la consulta; pero que no son estrictamente necesarios (dentro de la sección de respuesta).
  - Por ejemplo en algunos casos el servidor puede responder un query y suponer que se va a solicitar información extra que el puede responder. En dicho caso pone dicha información extra en esta sección.
  - Ejemplo: Un server provee el nombre de otro Name Server en la sección de Autoridad. Puede suponer que va a solicitar la IP de dicho name server, por lo que provee dicha dirección como un registro adicional. (También se verá un ejemplo mas adelante cuando se estudie el Registro MX)

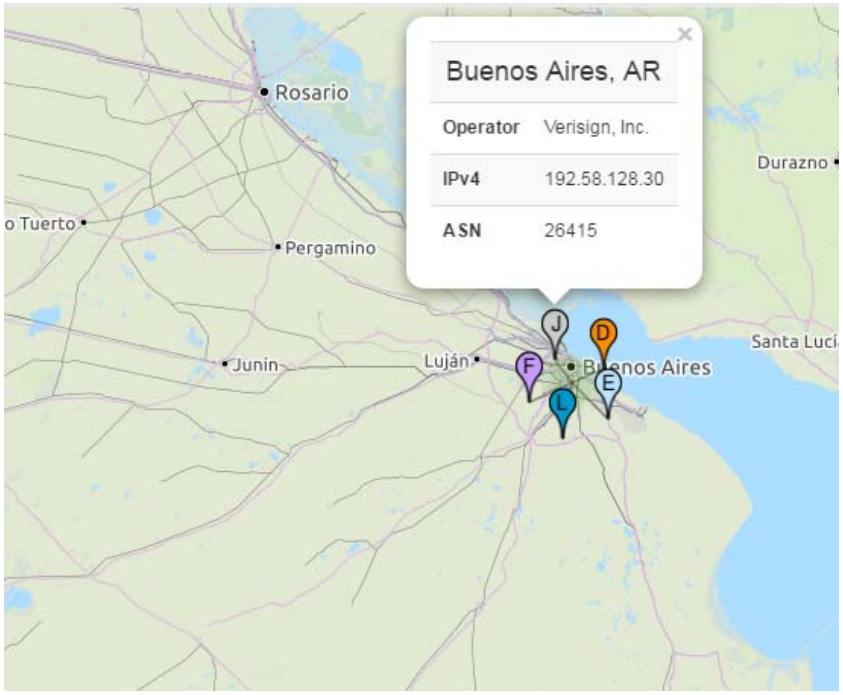
Planeamiento Instalación de DNS

- Pequeñas Empresas
  - Utilizar Servidores DNS de ISP para "queries" y almacenamiento de nombres de la Empresa
- Empresas medianas y grandes
  - Utilizar servidores DNS propios
- ISP's
  - Utilización de servidores DNS propios "obligatorio"
- Se recomienda el uso de por lo menos 2 servidores DNS
  - Un Servidor Primario
  - Un Servidor Secundario

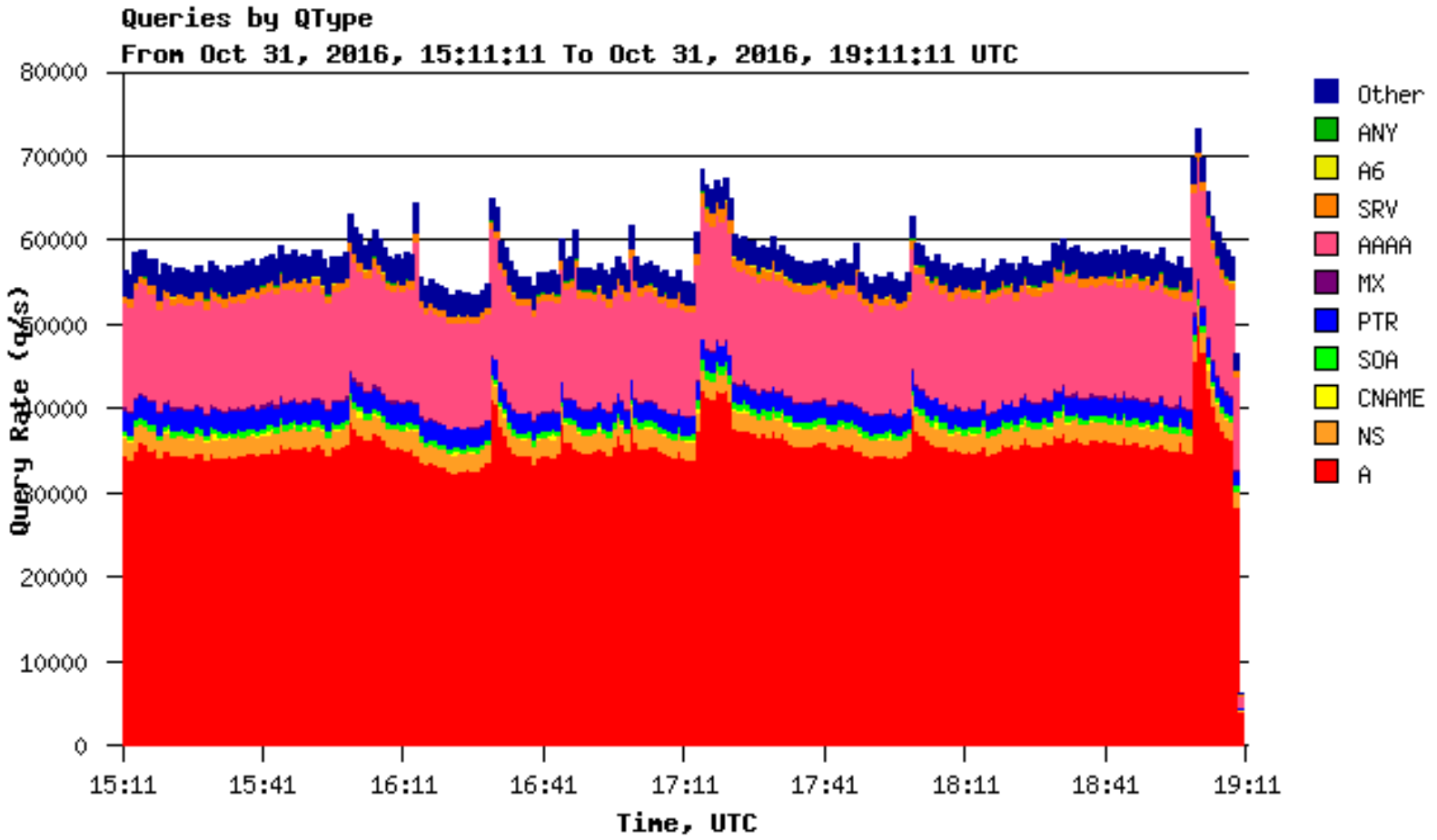
www.root-servers.org



Roots servers en Argentina



Queries Root C (1 día)



IPv4 vs IPv6 Address Record Queries (1 dia)