UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS

Escuela Profesional de Ciencia de la Computacion
Cod. CC312 Administracion de Redes

DNS

Prof. Jose Lozano

2021

Domain Name System (DNS)

Provee un nombre simbólico a los host, es usado indirectamente por la mayoría de los servicios de aplicación debido a que los usuarios normalmente se refieren al host con su nombre de DNS.

Proposito de DNS

- DNS es usado para resolver el problema de no comprension de direcciones IP a nombres entendibles por los usuarios por ejemplo truerestoration.org
- Las PCs usan direcciones IP y no nombres
- Nombres son mas facil de usar y recordar que las direcciones IP, por ejempo cual seria la direccion IP de truerestoration.org
- Cuando se escribe truerestoration.org en el navegador, tu maquina va a preguntar al servidor DNS por la direccion IP de truerestoration.org

DNS

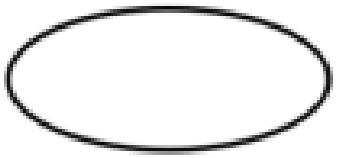
- Propuesto por Paul Mokapetris 1983
- Resolucion, resolucion inversa
- Encontrar la informacion a partir de un nombre de dominio
- Mantiene una base de datos distribuida y jerárquica de asociaciones de direcciones IP - nombre (llamados Resource Record, RR)
- Cada nombre en DNS consiste en un
  - Nombre del nodo (node name o hostname)
  - Nombre del dominio (domain name)
- ICANN
  - Internet Corporation for Assigned Names and Numbers
  - Es el organismo que gestiona DNS

Organizacion general

Organizacion jerarquica, delegacion

- algunos servidores raiz conocen los servidores de alto dominio (.pe, org, com, net, etc)
- el servidor .pe conoce el servidor para https://www.uni.edu.pe/
- para cada dominio, hay un servidor primario o maestro y un muchos servidores secundarios o esclavos
- las informaciones pueden ser conservadas por otros servidores intermediarios (caches)

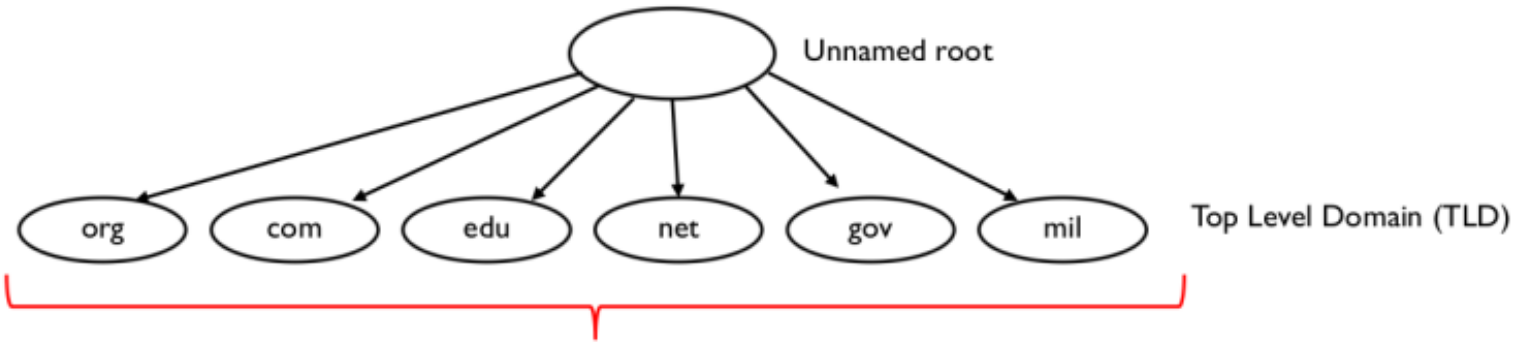
Jerarquia de dominios



Unnamed root

La base de datos distribuida y jerárquica del DNS tiene estructura a árbol donde la raíz es el único punto que no tiene nombre

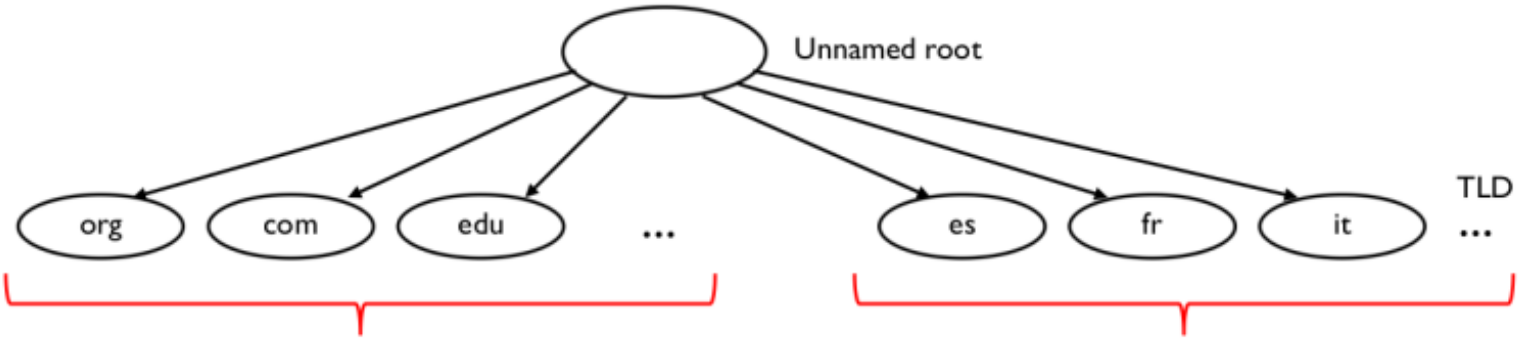
Jerarquia de dominios



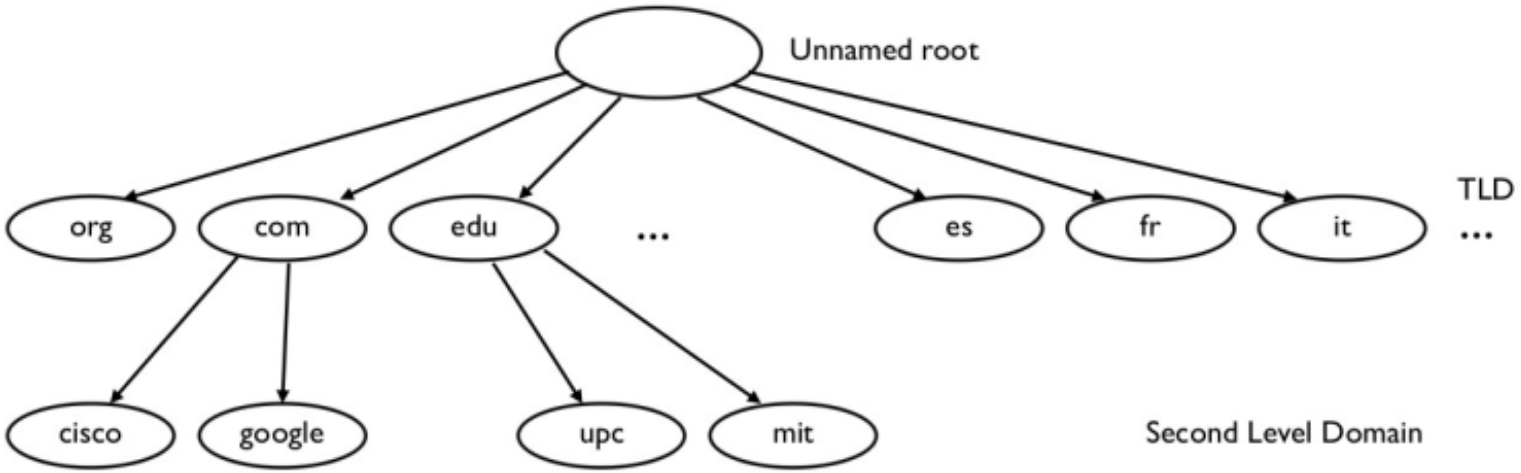
Dominios genéricos

Al principio se definieron 6 de estos dominios. A finales de los '90 empezaron luego a crearse algunos más como arts, info, store, and web, otros a principio del 2000 como aero, coop, museum, etc. Hoy en día hay miles.

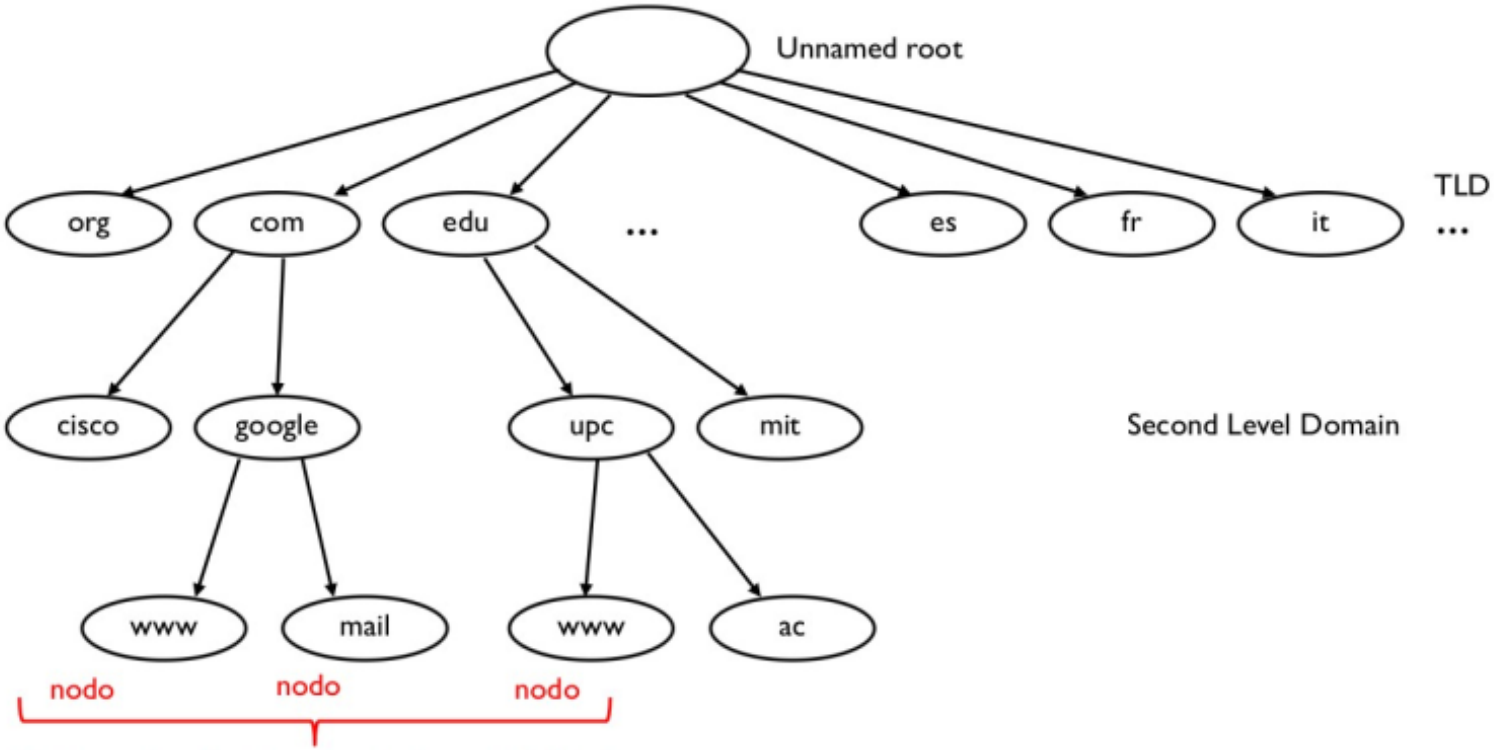
Jerarquia de dominios



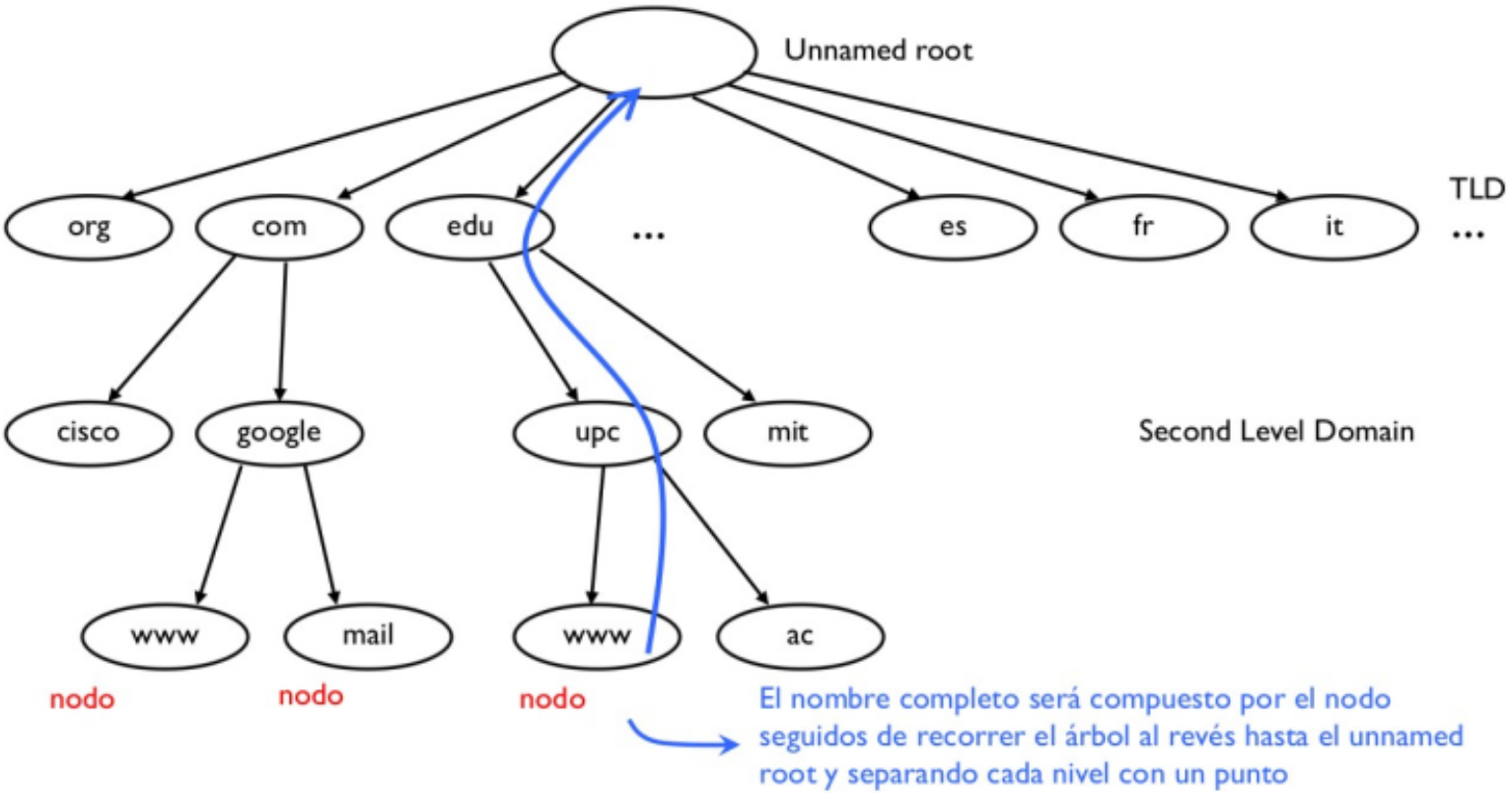
Jerarquia de dominios



Jerarquia de dominios



Jerarquia de dominios

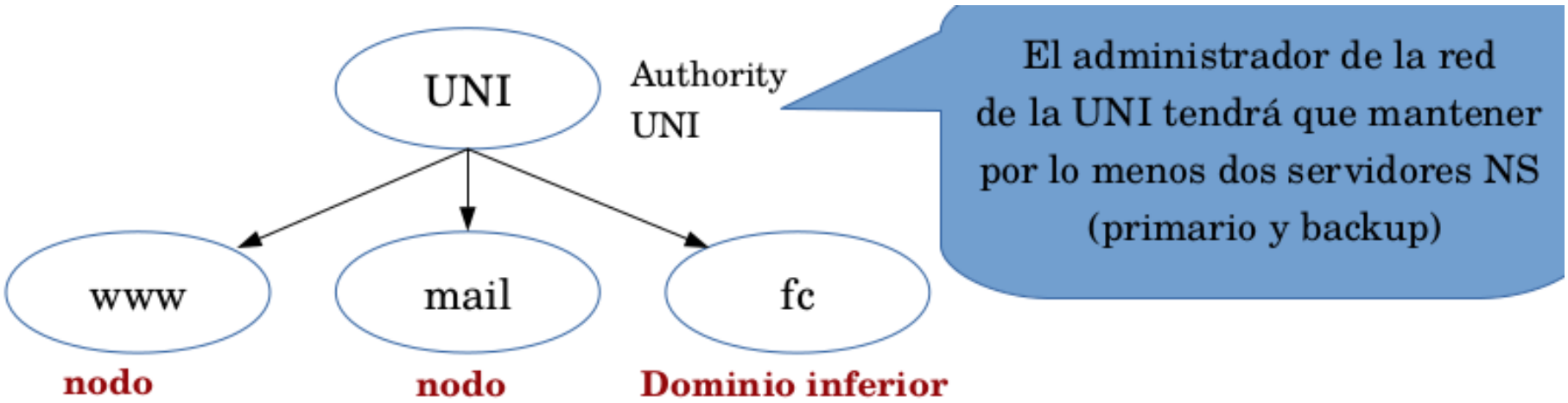


Servidores de Nombre

- Los Name Servers (NS) son los servidores que se ocupan de cada dominio (o zona). Son las authorities del dominio
- En cada dominio hay dos servidores NS
  - Servidor NS primario
  - Servidor NS de backup (se hace una copia del primario generalmente cada 3 h)
- Estos servidores NS mantienen una parte de la base de datos, en concreto
  - Nombres y direcciones IP de los nodos del dominio
  - Nombres y direcciones IP de las authorities (los NS) del nivel inferior
  - Cada entrada de esta base de datos se llama Resource Record (RR)
    - Hay RR permanentes (se configuran manualmente)
    - Hay cached RR (se eliminan pasado un tiempo)

Ejemplo

- Los NS del dominio UNI tendrán que mantener los RR del propio dominio
- Por un lado las asociaciones nombre de los nodos - direcciones IP
  - El nodo www (servidor de paginas web de la UNI) y su IP 190.119.192.130
  - El nodo mail y su IP 190.119.192.131
- Por el otro los nombres y direcciones IP de las authorities del nivel inferior. El NS del subdominio fc y su direccion IP 190.119.192.132



Ejemplo

- www.fc.uni.edu.pe , ¿cuál es el dominio? : fc.uni.edu.pe
- ¿cuál es el nombre del nodo de este dominio? www
- ¿Quién es el authority de este dominio? el servidor de nombres (NS) de la FC

Ejemplo

- Los NS del dominio FC tendrán que mantener los RR del propio dominio
- Por un lado las asociaciones nombre de los nodos - direcciones IP
- El nodo www (servidor de paginas web de la UNI) y su direccion IP 190.119.192.133
    - El nodo IUT-SCi (laboratorio de la FC) y su direccion IP 190.119.192.134
- Por el otro los nombres y la direccion IP de las authorities del nivel inferior
    - El NS del subdominio CIFC y su direccion IP 190.119.192.135

Servidores Raiz

- Los Name Servers (NS) de la authority de root se llaman Root Servers
- Hay 13 Root Servers (RS) primarios en el mundo. Se llaman A, B, C, D, . . . , M
- Hay varios backups. Tienes las direcciones IP y los nombres de los NS del nivel TLD en: http://www.root-servers.org

Componentes

- Sistema de nombres de dominio: base de datos distribuida y jerárquica de servidores DNS.
- Espacio de nombres de dominio: estructura lógica en forma de árbol generada por los nombres en la base de datos DNS.
- Dominio y subdominio: nodos en el espacio de nombres.
- Zona: agrupación de dominios que permite la administración distribuida.
- DNS es BBDD que mapea nombres a direcciones

Componentes

- Resolver: Cliente DNS entre una aplicación y un servidor de nombres. Hay que especificar la IP de quién tiene el servicio DNS. En el fichero: /etc/resolv.conf
- Servidor de Nombres: sistema que recibe peticiones de un cliente y devuelve la respuesta (IP o nombre).
- Espacio de nombres de dominios: Agrupación jerárquica de nombres en forma de camino invertido. En la cima el dominio root y después los dominios de primer nivel de los que cuelgan los demás

Normas del nombrado

- Estándar de facto nombrar a los hosts por servicio prestado: www.uni.edu, ftp.uni.edu, ...
- Limitar el número de niveles del dominio.
- Nombres de host: tres o cuatro niveles de profundidad.
- Más niveles aumenta las tareas administrativas.
- Usar nombres únicos.
- Cada subdomnio usa un nombre único dentro del dominio padre.
- Usar nombres simples.
- Evitar nombres de dominio largos.
- Utilizar caracteres estándares de DNS y Unicode
- Caracteres A-Z, a-Z, 0-9 y el guión (-).

Funcionamiento

- Un cliente interroga un servidor que el conoce
- Dos tipos de servidores
  - recursivo: se ocupa de encontrar una respuesta y transmitirla al cliente
  - iterativo: reenvia el cliente sobre un otro servidor

Ejemplo de resolucion

Un puesto del departamento de Teologia, quiere conocer la direccion de truerestoration.org

- El puesto interroga un DNS local
- Este DNS local interroga un servidor raiz que le da la direccion de un servidor por org
- El solicita a este servidor la direccion DNS para truerestoration
- El demanda al DNS de truerestoration la direccion de www.truerestoration.org
- El da la respuesta a cliente

Consideraciones

- En realidad, ciertas etapas pueden ser evitadas
- El servidor DNS local se comporta como mandatorio (proxy) por el cliente
- Aca, el servidor DNS en modo recursivo: el se encarga de la resolucion del cliente

La resolucion inversa

A partir del numero IP, encontrar los nombres de dominio

- Mismo principio pero al inverso
- el nombre mas general es la derecha
- la parte general de un numero IP es a la izquierda

Consideraciones

- Permitir tratar de manera homogenea la resolucion directa y la resolucion inversa
- se basa en la división de direcciones IP según los límites de bytes (clases A, B y C)

Protocolos

Intercambiar por

- UDP cuando sea posible por razones de eficiencia
- por TCP caso contrario (transferencia de zonas)
- Puerto Servidor =53, puerto cliente mayor a 1023

Utilizacion de cache

- Problema de eficiencia: reutilizamos las informaciones conocidas
- Almacenamiento en estas caches
- Pero las informaciones pueden cambiar. Para esto estan las tecnicas
  - duracion de vida declarada
  - numero de version

Redundancia

- disponibilidad muchos servidores para un mismo dominio
- servidor maestro, servidores esclavos
- el servidor maestro notifica a los servidores esclavos
- los esclavos interrogan al maestro
- Implantacion de servidores esclavos en redes remotas
- regla de duracion de vida y retraso de interrogacion

En linux

La direccion DNS puede ser proveida por DHCP Sino se inserta en el archivo /etc/resolv.conf

DNS y correos

- El DNS es indispensable al sistema de transmision de correos
- El envio del mail fides@spes.pe: el correo es transmitido al servidor del correo de spes.pe

Subdominios

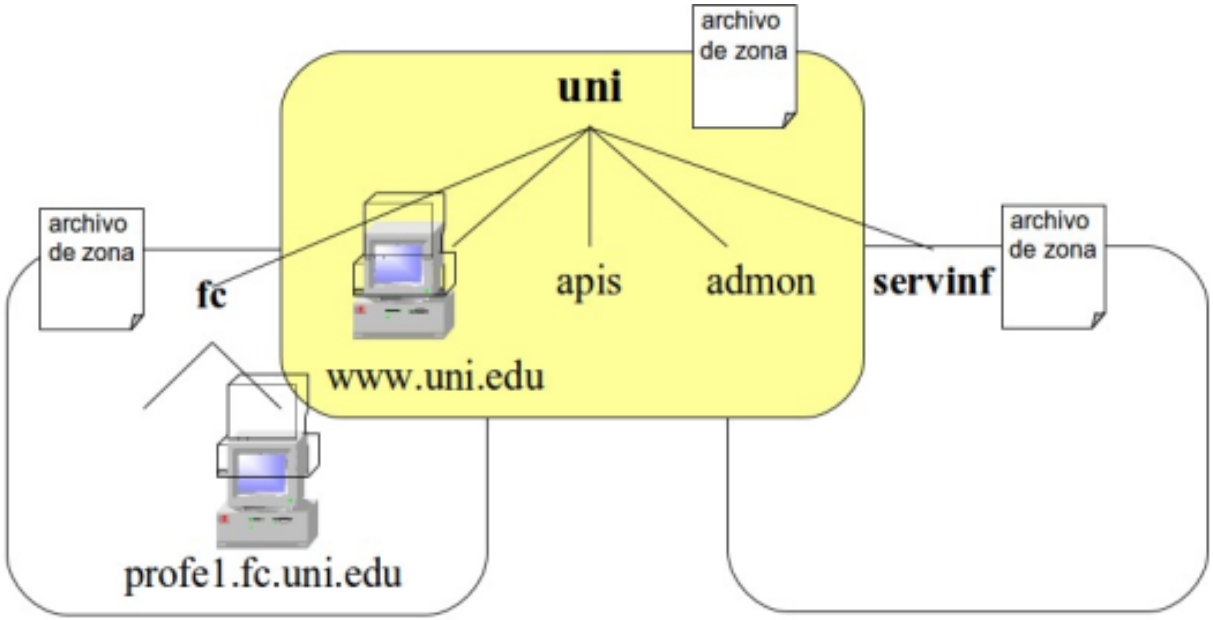
Un subdominio puede ser administrado por el mismo servidor o por otro, u otros muchos.
La declaracion de subdominio se hace con al directiva NS

Dominios y zonas de autoridad

- Dominio:
  - Cada nodo en el árbol de la BD DNS, y sus nodos hijo.
  - Pueden contener computadoras y otros dominios: subdominios.
  - Ej: dominio uni.edu, con host www.uni.edu y subdominios: fiis.uni.edu e fc.uni.edu.
- Zona de autoridad:
  - Porción del Domain Name Space de la que es responsable un determinado servidor de nombres.
  - El servidor almacena todas sus direcciones IP para la zona.
  - Un archivo físico por zona para almacenarlas: archivo de zona.
  - Cada zona abarca al menos un dominio: dom. raíz/principal de zona.
  - La zona de autoridad también puede incluir subdominios.
  - Un único servidor DNS puede manejar una o múltiples zonas.

Dominios y zonas de autoridad

Distribuir el dominio entre varios archivos de zona:

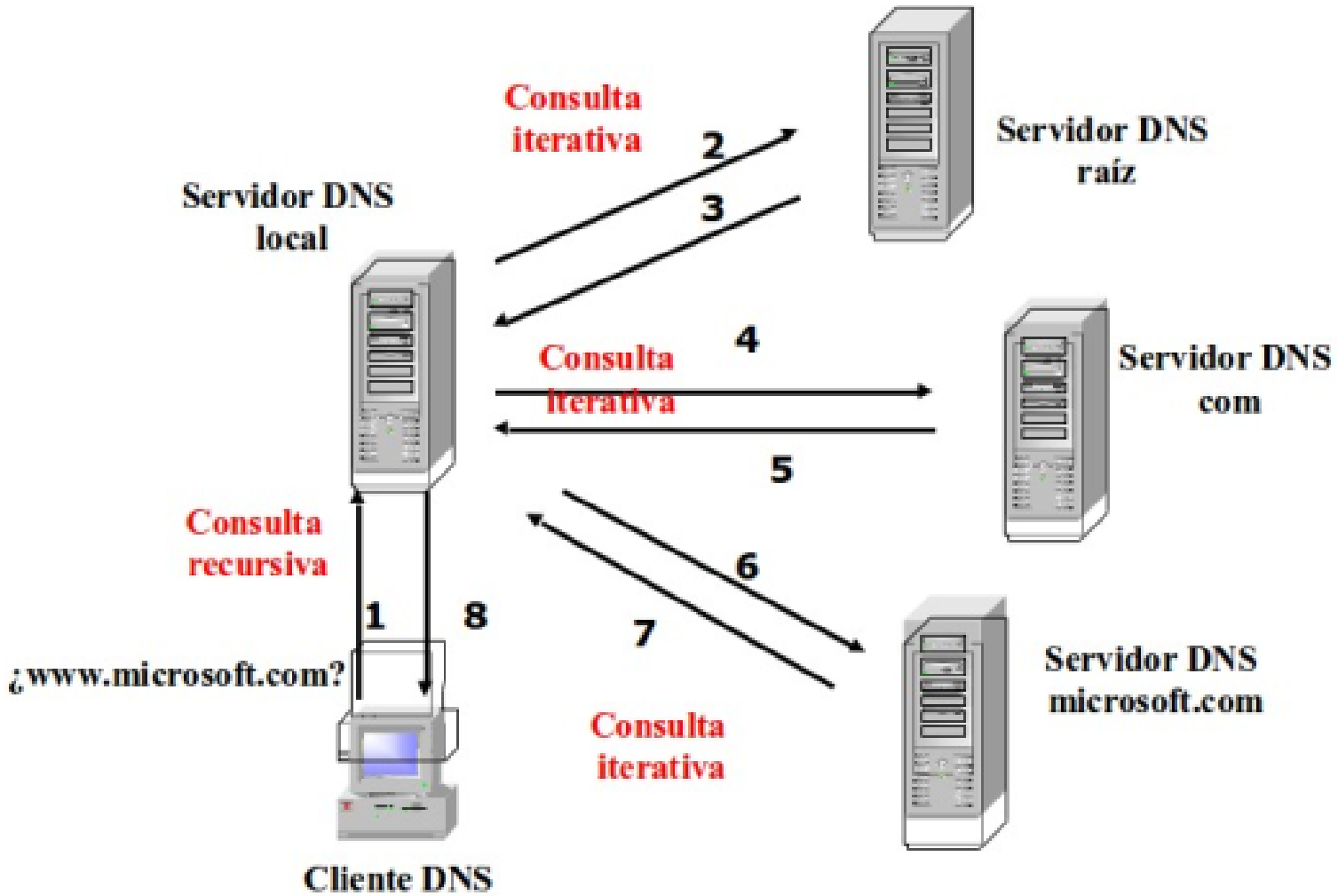


- Distribuir la administración del dominio a diferentes grupos.
- Eficiencia en la replicación de datos.

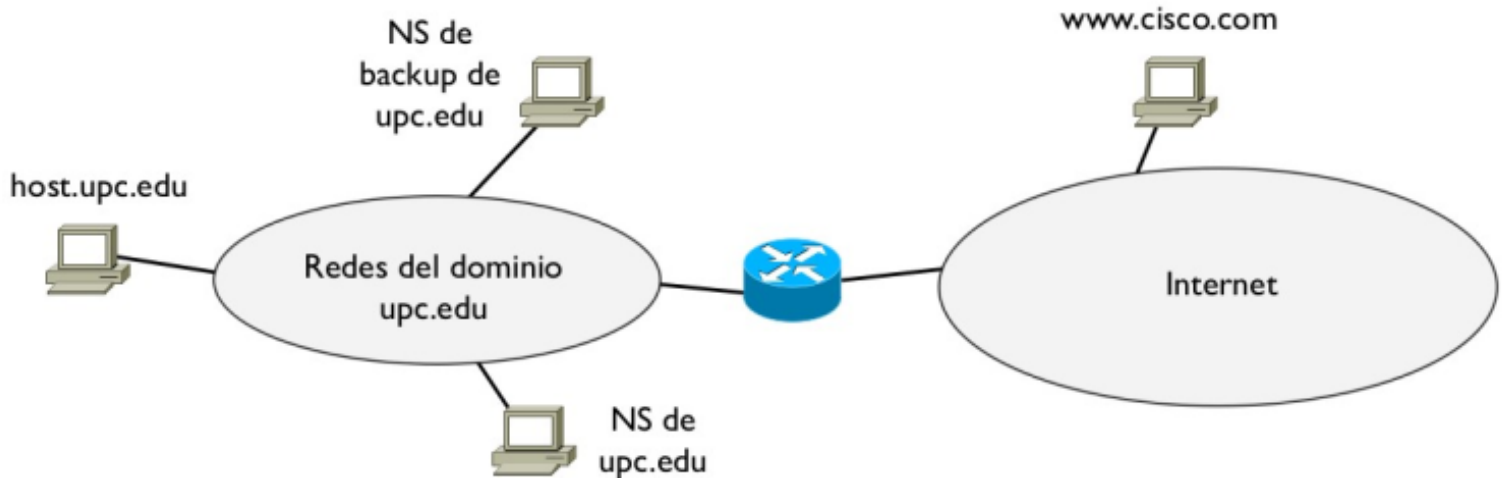
Consultas DNS

- Recursiva:
  - Típica entre cliente y servidor, (y entre esclavo y forwarder).
  - El NS devuelve el dato solicitado o un error.
  - El NS no puede transferir la consulta a otro, pero sí consultar a otros NS.
- Iterativa:
  - El NS puede devolver la respuesta o la IP de otro NS mejor.
  - Típica entre dos servidores DNS, tratando de resolver una recursiva.
- Inversa:
  - El resolver conoce una IP y trata de obtener el nombre del nodo.
  - Como las IPs no tienen una estructura jerárquica como los nombres, se debería hacer una búsqueda en todos los dominios.
  - Se crea un dominio especial: in-addr.arpa
  - Ej. para la red 155.54.12.0 se crea el dominio 12.54.155.in-addr.arpa

Consultas recursivas e iterativas



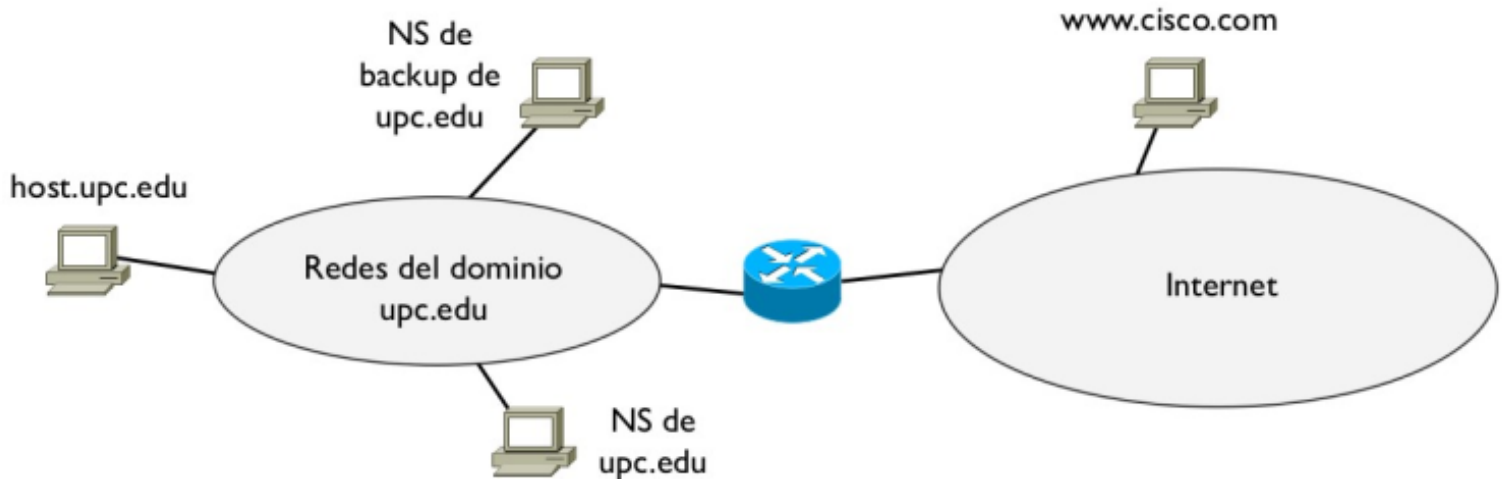
Simulacion



El host host.upc.edu quiere ver la página web de www.cisco.com

- www.cisco.com es un nombre mientras que las redes funcionan con IP
- El host tiene que encontrar la IP de www.cisco.com
- Se dice que se tiene que hacer una resolución de un nombre

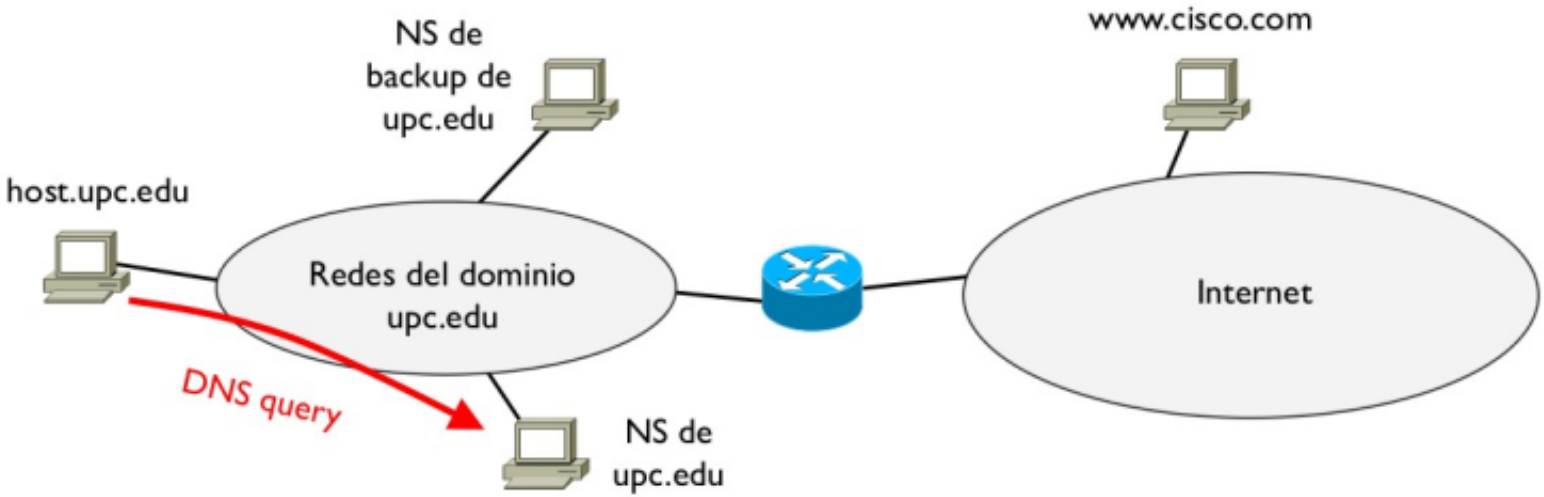
Simulacion



El host comprueba si tiene una resolución ya disponible en su memoria cache del DNS

- En efecto, cada vez que se hace una resolución DNS, los hosts mantienen esta resolución durante un cierto tiempo en una memoria llamada cache
- Este tiempo es programable

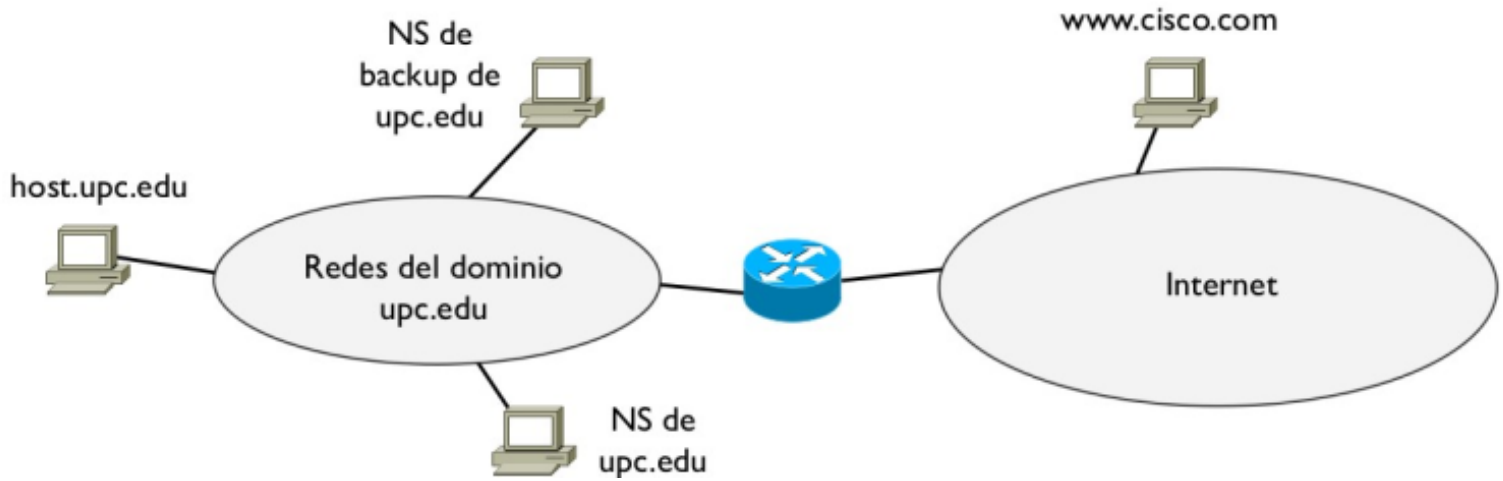
Simulacion



Si no tiene esta resolución, contacta el authority (el NS primario) de su dominio

- Envía al NS una petición de resolución (DNS query) con el nombre a resolver, es decir www.cisco.com
- Se usa el protocolo UDP con puerto destino 53
- El puerto origen es un número efimero

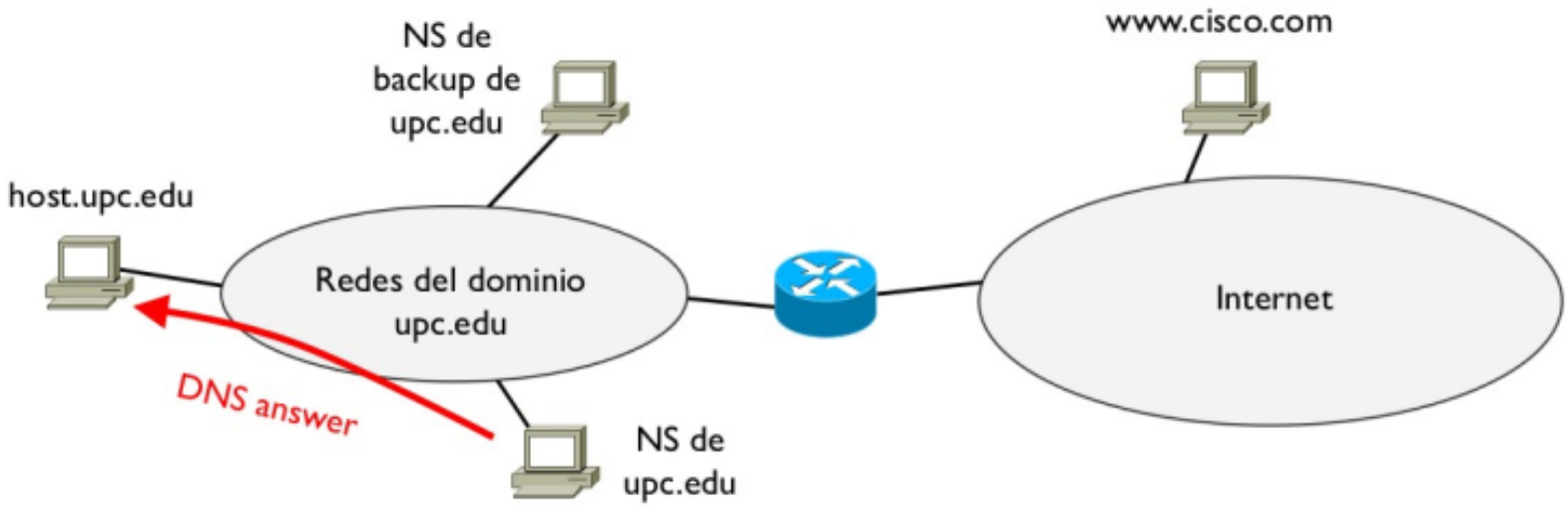
Simulacion



El NS comprueba si ya tiene resuelto el nombre www.cisco.com

- El NS tiene una base de datos con algunas resoluciones ya configuradas (estáticas, es decir están configuradas manualmente y no se borran con el tiempo)
- A parte, el NS se guarda todas las resoluciones hechas de forma dinámica durante generalmente 2 días (en una memoria llamada cached RR)
- Es decir podría ser que otro host del dominio upc.edu haya pedido una misma resolución en el pasado y por lo tanto el NS podría tenerla

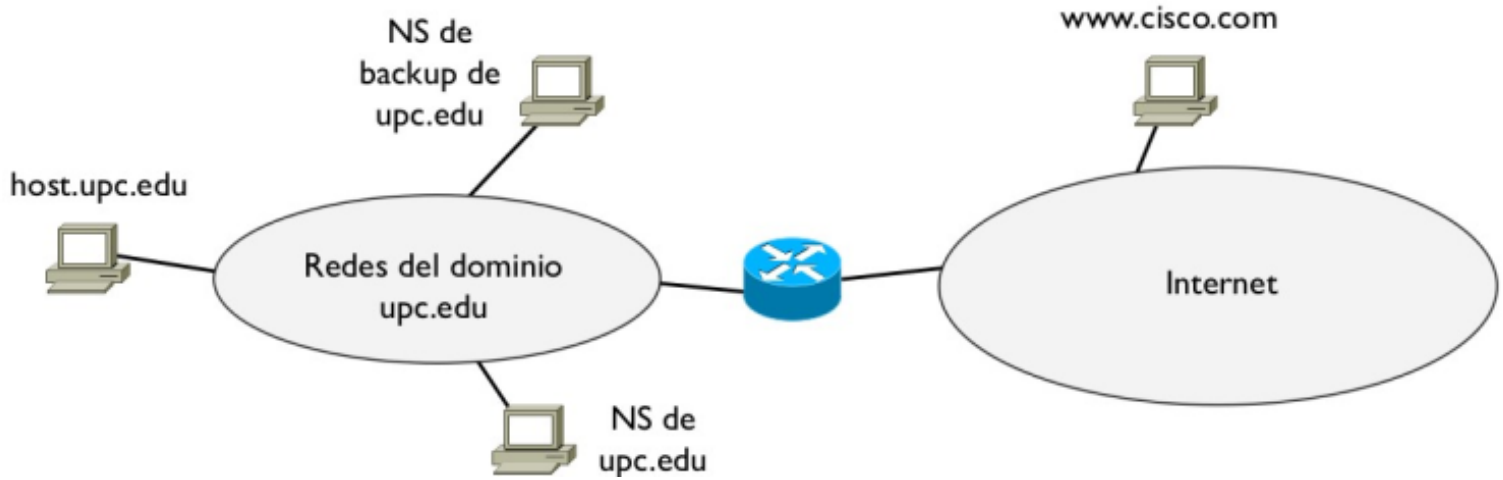
Simulacion



Si ya tiene esta resolución, el NS contesta con un DNS answer al host

- En la respuesta se indica la IP de www.cisco.com y también el nombre y la direccion IP del authority que ha proporcionado esta resolución

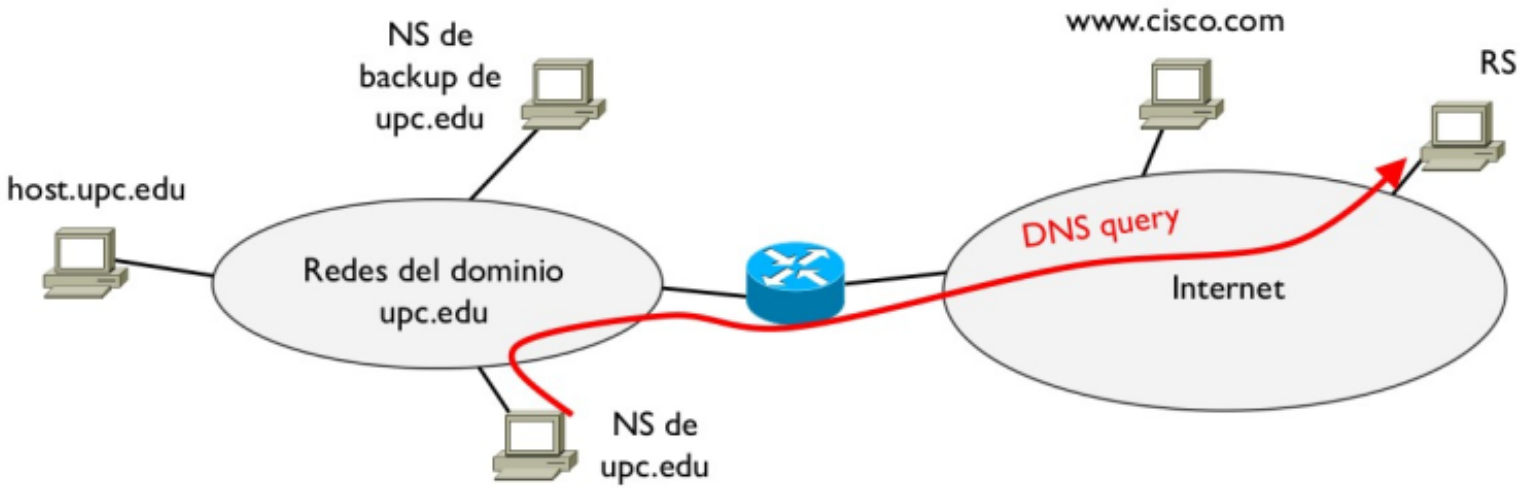
Simulacion



Si no la tiene, el NS debe buscar la resolución en Internet

- Suponiendo que el NS no sabe nada del nombre www.cisco.com, el NS debe empezar la resolución a partir de un RS
- Un NS debe por lo tanto tener configurado en su base de datos el nombre y direccion IP de por lo menos un RS

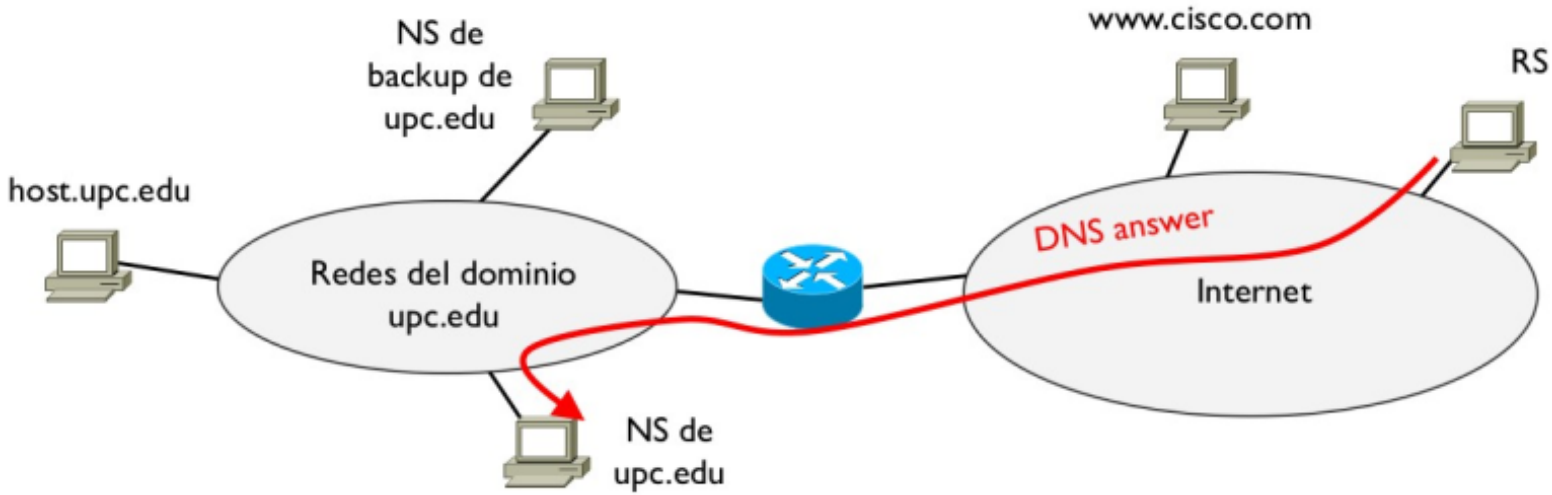
Simulacion



El NS de upc.edu pide a un RS la direccion IP de un NS del dominio.com

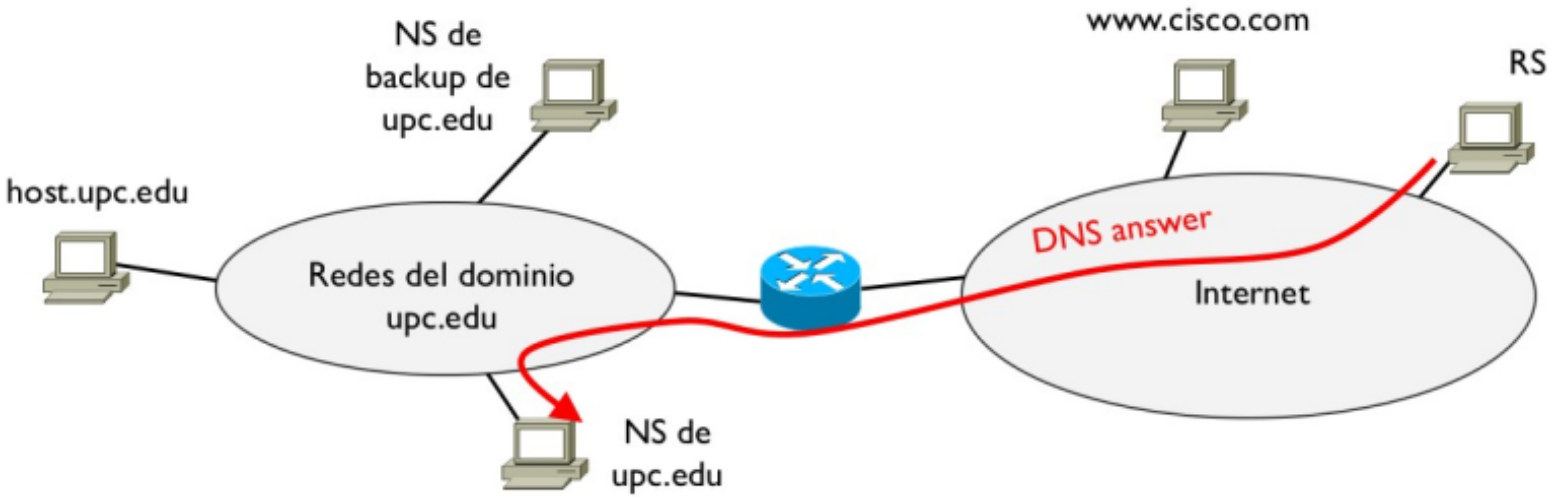
- Es decir la resolución siempre es a partir de la raíz y se recorre el árbol hasta la hoja

Simulacion



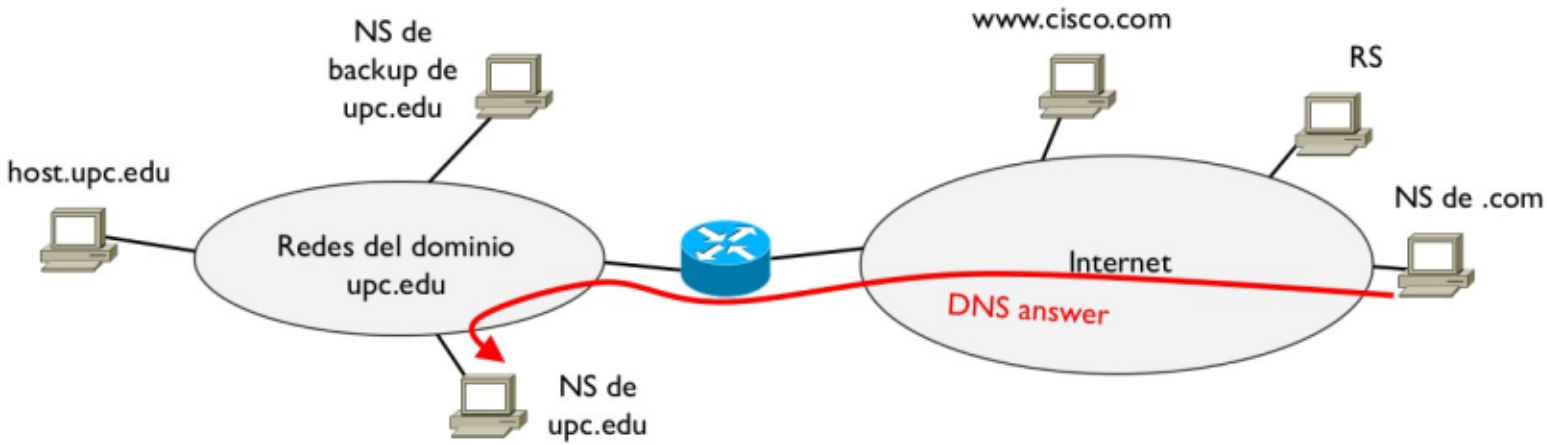
El RS contesta con la IP de un NS del dominio.com

Simulacion



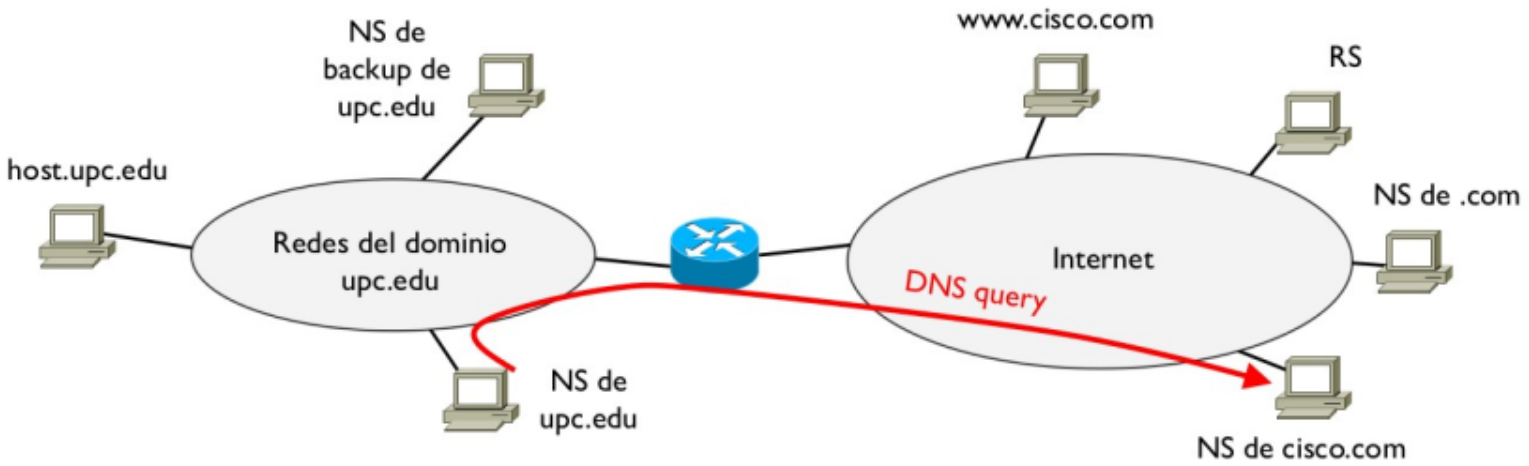
Con esta información, el NS de upc.edu ahora puede pedir al NS del dominio.com la direccion IP de un NS del dominio inferior cisco.com. Es decir se ha bajado de la authority unnamed root a una authority del nivel TLD

Simulacion



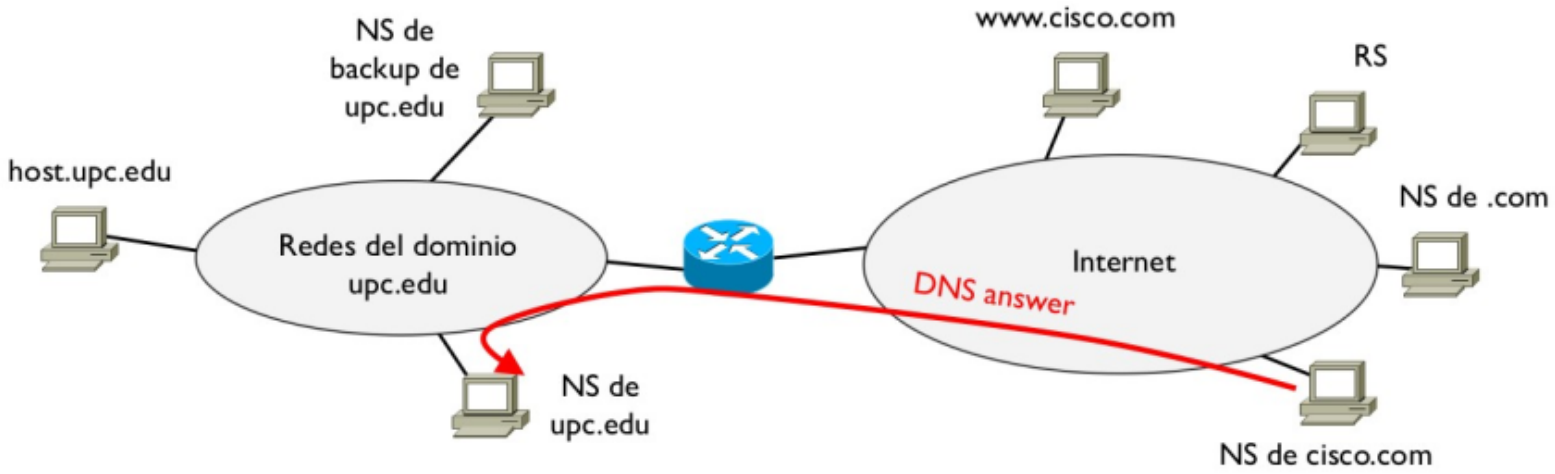
El NS del dominio.com contesta con la IP del NS del subdominio cisco.com

Simulacion



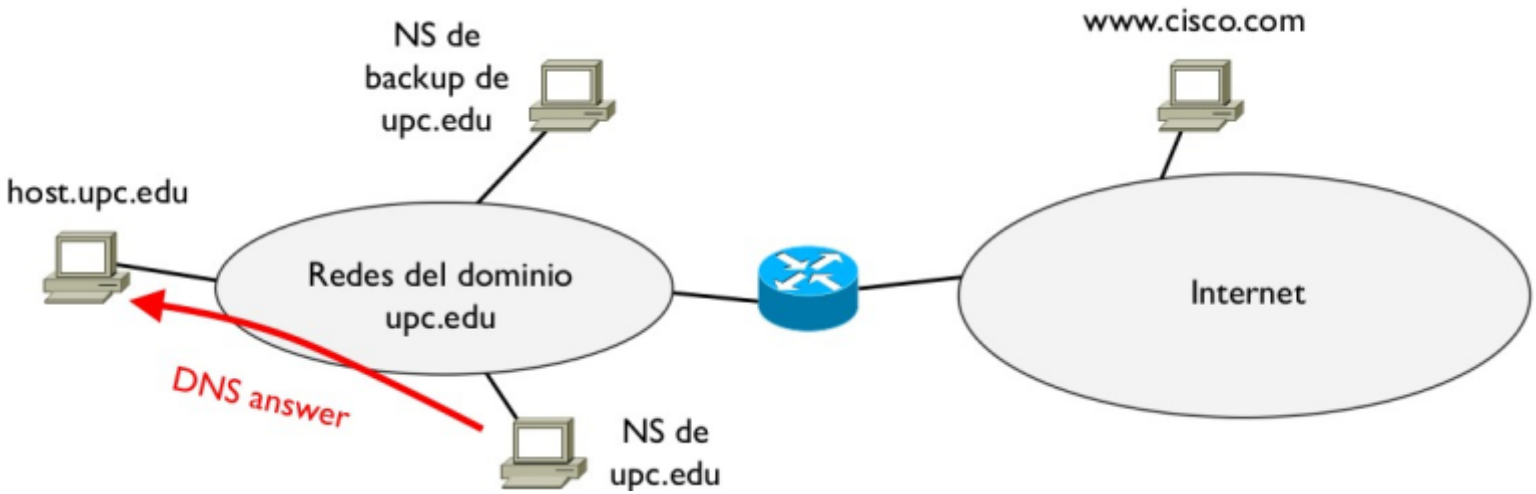
Con esta información, el NS de upc.edu ahora puede pedir al NS del dominio cisco.com la IP de uno de sus nodos, en concreto el www (servidor de paginas web). Es decir ya se ha llegado a la authority que conoce lo que se estaba buscando

Simulacion



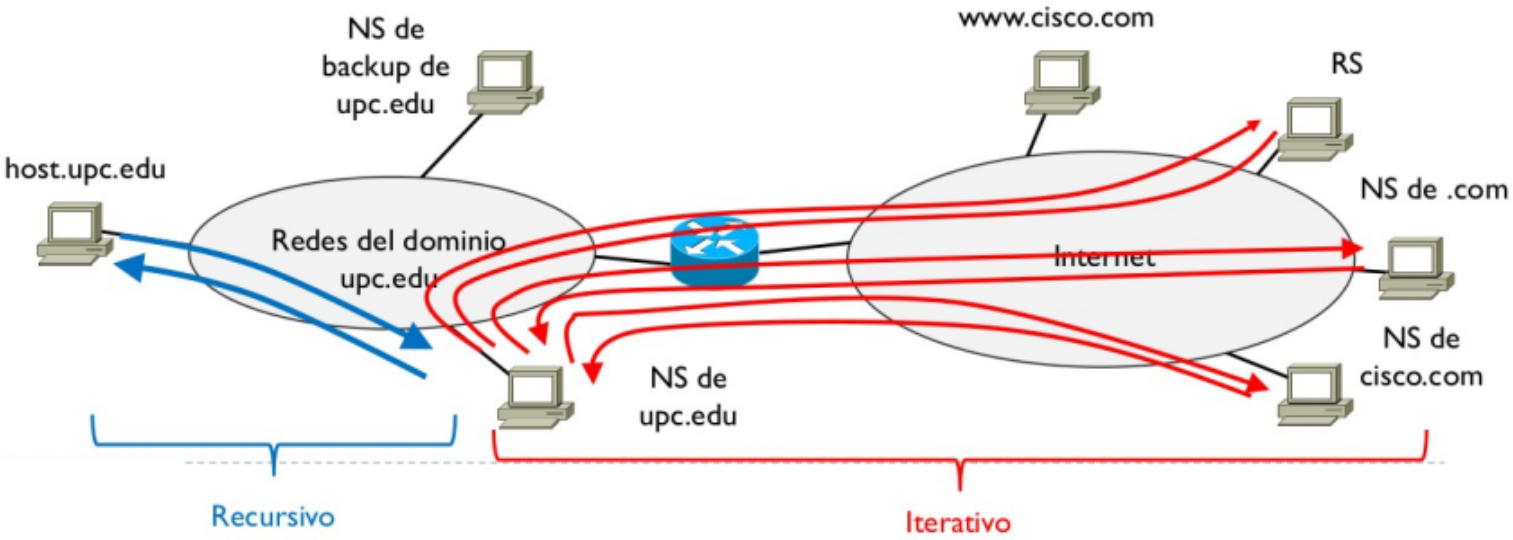
El NS de cisco.com proporciona la IP del servidor de paginas web de su dominio, es decir la IP de www.cisco.com

Simulacion



Ahora el NS de upc.edu tiene lo que le había pedido el host y finalmente le puede contestar

Simulacion Detalles



Simulacion Detalles

Un mismo nombre puede estar asociado a diferentes IP (es decir diferentes nodos)

- Por ejemplo no existe un único servidor www.google.com
- En estos casos, los NS generalmente proporcionan la IP del nodo más próximo al que ha pedido la resolución)

Un mismo host puede tener diferentes nombres

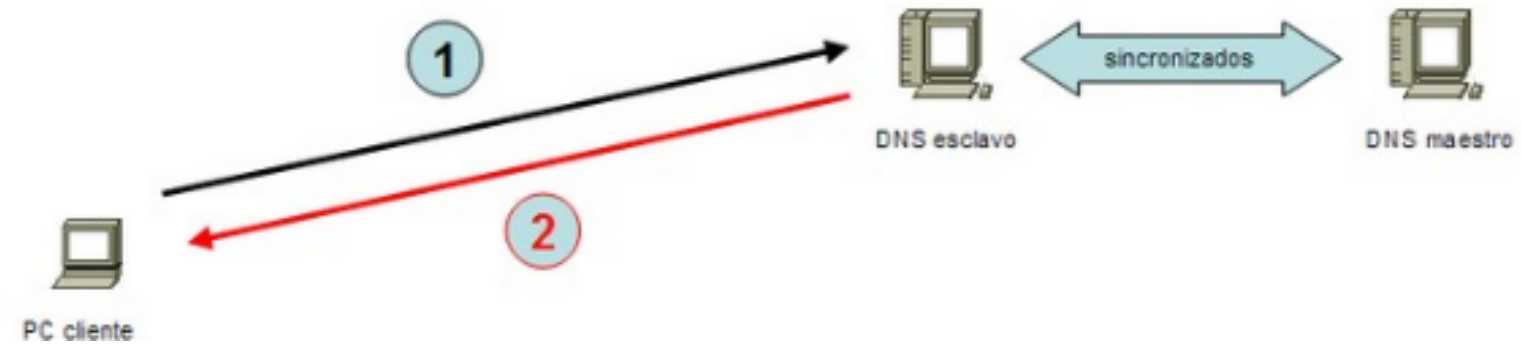
- Se llaman alias
- Se puede pedir que un NS proporcione todos los alias de un nombre
- Es una resolución que se dice de tipo CNAME

También existe la resolución inversa

- Conocida la IP, se pide por el nombre
- Es una resolución que se dice de tipo PTR

Servidores DNS

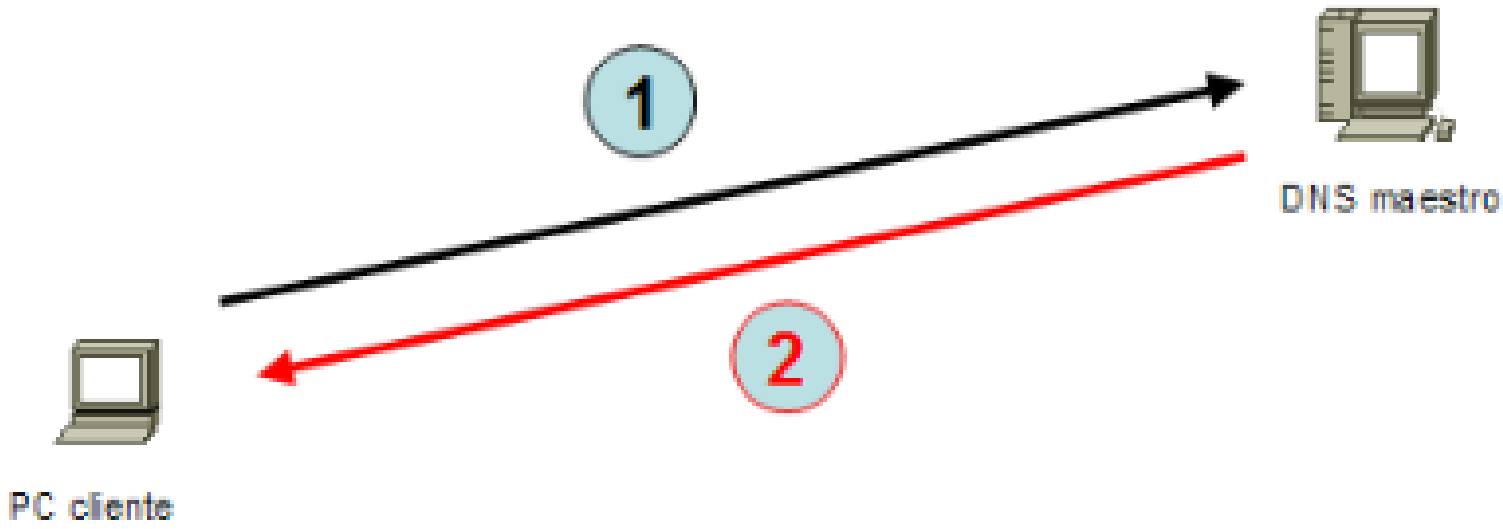
Toda zona debe tener al menos un servidor de nombres.
Una zona puede tener varios servidores que la gestionen, pero sólo uno será el servidor principal, y los otros serán secundarios.
Un servidor puede ser principal para una o varias zonas y al mismo tiempo ser servidor secundario de una o varias zonas.



Servidores DNS Primario

Gestiona una zona de autoridad.

- Realiza los cambios en la zona (añadir dominios o hosts)
- Obtiene los datos de la zona de sus ficheros locales
- Toda zona debe tener un servidor primario o principal



1 – Consulta DNS: ¿Cuál es la IP de aula5pc7.ieslapaloma.com?

2 – Respuesta DNS: La IP de aula5pc7.ieslapaloma.com es 192.168.0.107

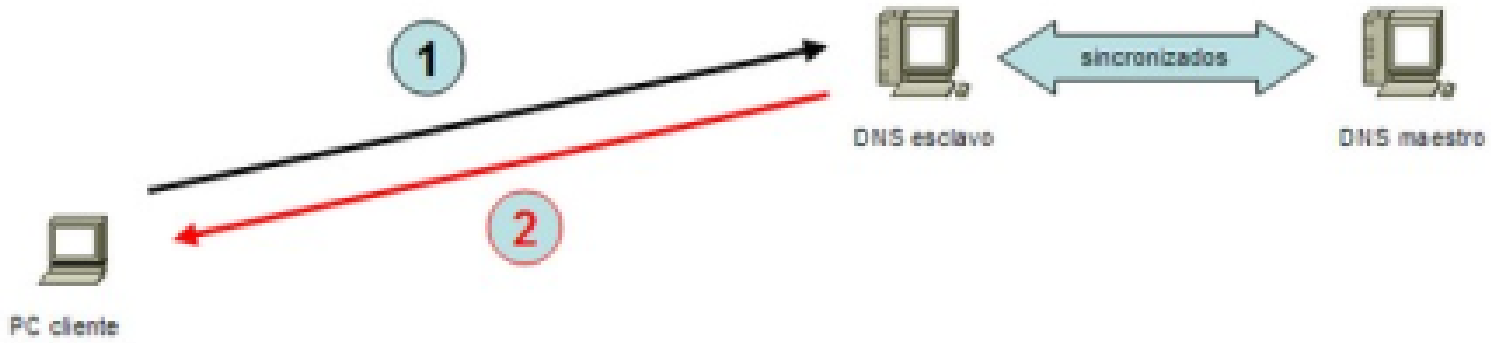
Servidores DNS secundario

Obtiene datos para sus zonas desde otro servidor. Proceso de transferencia de zona (zone transfer).
Razones para tener servidor DNS secundario:

- Redundancia:
  - Al menos un servidor primario y uno secundario para cada zona.
  - El servidor primario sólo resuelve nombres si cae el secundario o no tiene la IP/nombre.
- Acceso más rápido para delegaciones remotas. Teniendo servidor secundario cada delegación posibilita el acceso rápido de esos clientes para la resolución de nombres.
- Reducción de carga del servidor primario.

Todo servidor secundario necesita un servidor maestro del cual obtener los datos por transferencia de zona. Cuando el servidor secundario arranca, contacta con el servidor maestro e inicia una trasferencia de zona con este servidor.

DNS secundario



Cache y TTL

- Todo NS almacena temporalmente consultas resueltas.
- TTL: Las repuestas contienen un tiempo de validez.
- Es establecido por el administrador de DNS.
- Si la respuesta está en la caché y no ha caducado, se devuelve su valor.
- Los resolvers también tienen una caché.
- Valores altos TTL: menos carga en servidores y menos consistencia de datos

Servidor DNS solo cache

- Su único trabajo es ejecutar consultas, almacenar las respuestas, y devolver resultados.
- No tienen autoridad sobre ningún dominio.
- Al iniciarse no tiene información y la irá adquiriendo.
- Para redes muy lentas, se genera menos tráfico que en una transferencia de zona.
- No hace transferencia de zona.
- No puede ser servidor maestro de ningún otro

Roles de Servidores DNS