Capa Aplicación: DNS

ELO322: Redes de Computadores

Agustín J. González

Este material está basado en:

- Material de apoyo al texto *Computer Networking: A Top Down Approach Featuring the Internet.* Jim Kurose, Keith Ross.

Capítulo 2: Capa Aplicación

- 2.1 Principios de la aplicaciones de red
- 2.2 Web y HTTP
- 2.3 Correo Electrónico
  - SMTP, POP3, IMAP
- 2.4 DNS
- 2.5 Aplicaciones P2P
- 2.6 Video streaming y redes de distribución de contenidos
- 2.7 Programación de sockets con UDP y TCP

DNS: Domain Name System (Sistema de nombres de dominio)

Personas: muchos identificadores:

- ROL, RUT, name, # pasaporte

Host y router en Internet:

- Dirección IP (32 bit) – usada para direccionar datagramas (ideal para router por ser máquina)
- "nombre", e.g., www.google.com – son usados por humanos

Q: ¿Quién mapea entre nombres y direcciones IP?

Domain Name System:

- *Base de datos distribuida* implementada en una jerarquía de muchos *servidores de nombres*
- *Protocolo de capa aplicación* permite a host, routers, y servidores de nombre comunicarse para *resolver* nombres (traducción nombre ↔ dirección)
- Gracias al DNS nosotros usamos nombres mientras que la red utiliza números.
  - DNS es función central de la Internet implementada como protocolo de capa aplicación
  - La idea de diseño de Internet es dejar la complejidad en la "periferia" de la red.

DNS: Servicios y estructura

Servicios DNS

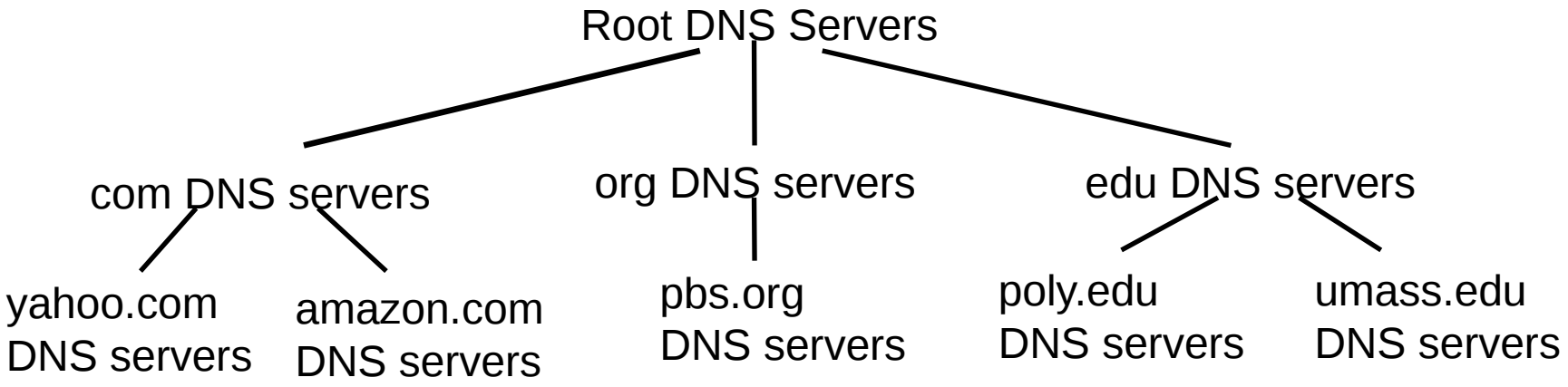
- Traducción de nombre de host a dirección IP
- Alias para host
  - Nombre canónico y alias
  - Usamos alias para servidor de correo entre otros
- Distribución de carga
  - Servidores Web replicados: conjunto de direcciones IP para un nombre canónico
  - Servidor DNS rota entre direcciones IP, o asigna del de menor carga, etc.

¿Por qué no centralizar DNS?

- Sería punto único de falla.
- Volumen de tráfico, muchos necesitan el DNS
- Sería una base de datos centralizada distante con grandes retardos de acceso.
- Mantención, es mejor que cada dominio gestione sus nombres

Respuesta: No escala*!*

DNS: Base de datos jerárquica y distribuida

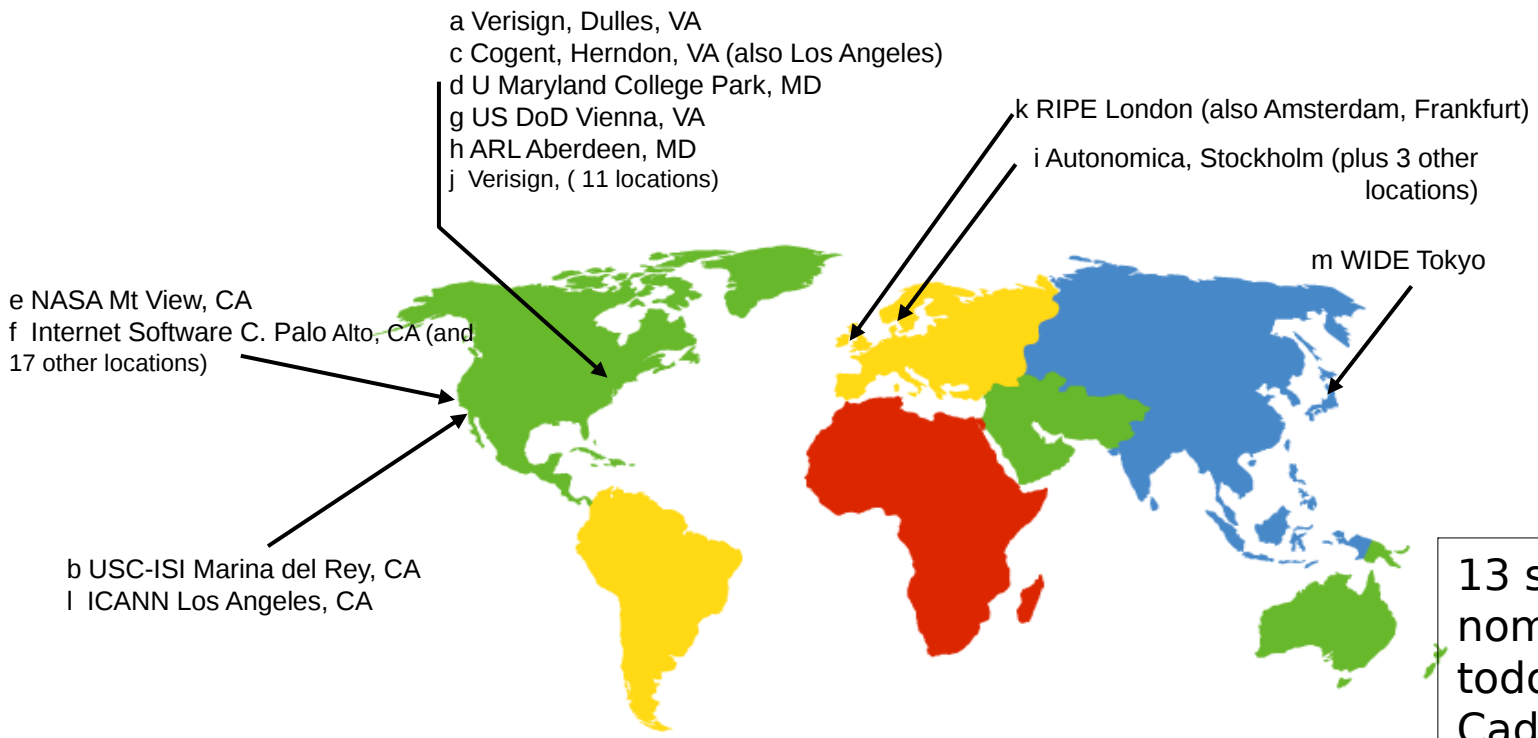


Cliente desea IP de www.amazon.com; 1ra aprox. :

- Cliente consulta al servidor raíz para encontrar servidor DNS de com
- Cliente consulta servidor DNS de .com para obtener servidor DNS de amazon.com
- Cliente consulta servidor DNS amazon.com para obtener dirección IP de www.amazon.com

DNS: servidores de nombre en raíz

- Son contactados por servidores de nombre locales que no pueden resolver un nombre
- Sus direcciones IPs están contenidas en el software DNS.
- Su ubicación se puede ver en: http://www.root-servers.org/



13 servidores de nombre raíz en todo el mundo. Cada uno replicado varias veces.

TLD y Servidores Autoritarios

- Top-level domain (TLD) servers: responsable por com, org, net, edu, etc., y todos los dominios superiores de cada país: uk, fr, ca, jp, cl, etc..
  - Network solutions mantiene servidores para el TLD de com
  - Educause para el TLD de edu
  - Nic (network information center) para el TLD de cl (www.nic.cl)
- Servidores DNS autoritarios: son servidores DNS de las organizaciones y proveen mapeos autoritarios entre hostname e IP (ej., Web y mail).
  - Éstos pueden ser mantenidos por la organización o el proveedor de servicio

Servidor de nombre local (DNS local)

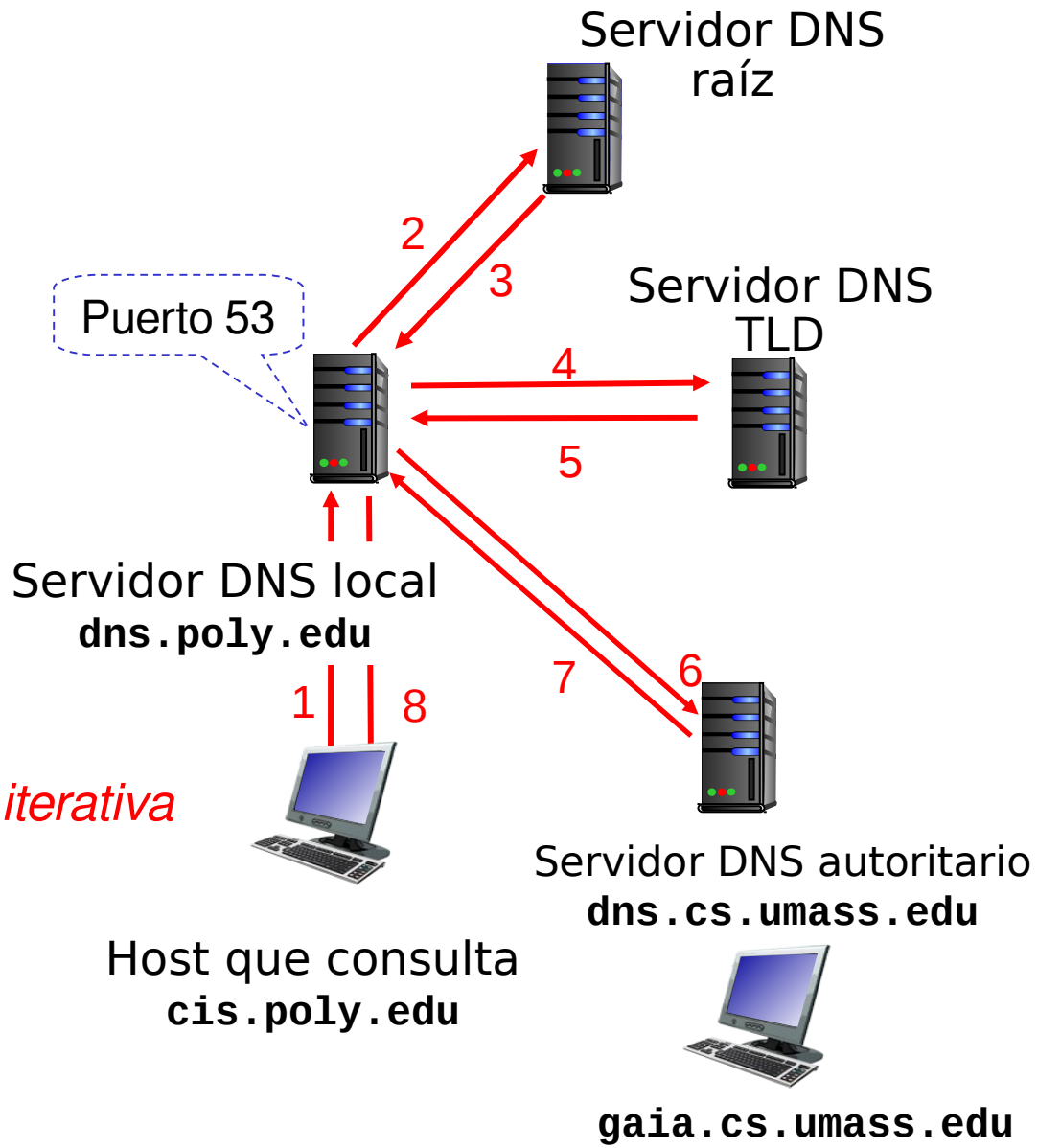
- No pertenece estrictamente a la jerarquía
- Cada ISP (ISP residencial, compañía, universidad) tiene uno.
  - También son llamados “servidor de nombre por omisión” (default name server)
- Cuando un host hace una consulta DNS, ésta es enviada a su servidor DNS local
  - Actúa como **proxy**, re-envía consulta dentro de la jerarquía.
  - Maneja un cache local de mapeos recientes (puede estar obsoleto -mapeo incorrecto-)

Ejemplo 1

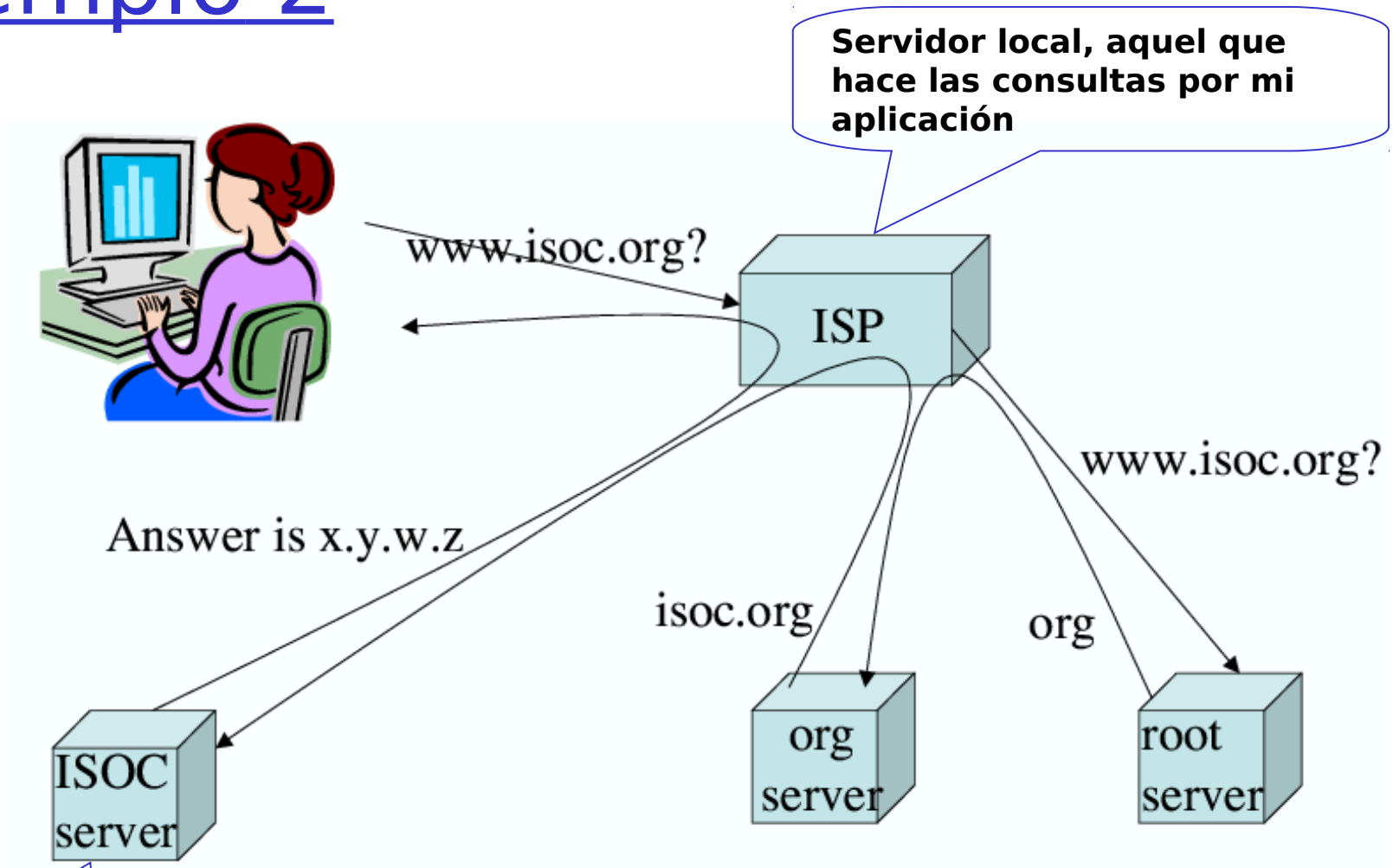
- Host en cis.poly.edu quiere la dirección IP de gaia.cs.umass.edu

Consulta iterativa:

- Servidor contactado responde con el nombre del servidor a contactar
- "Yo no conozco este nombre, pero pregunta a este servidor"



Ejemplo 2

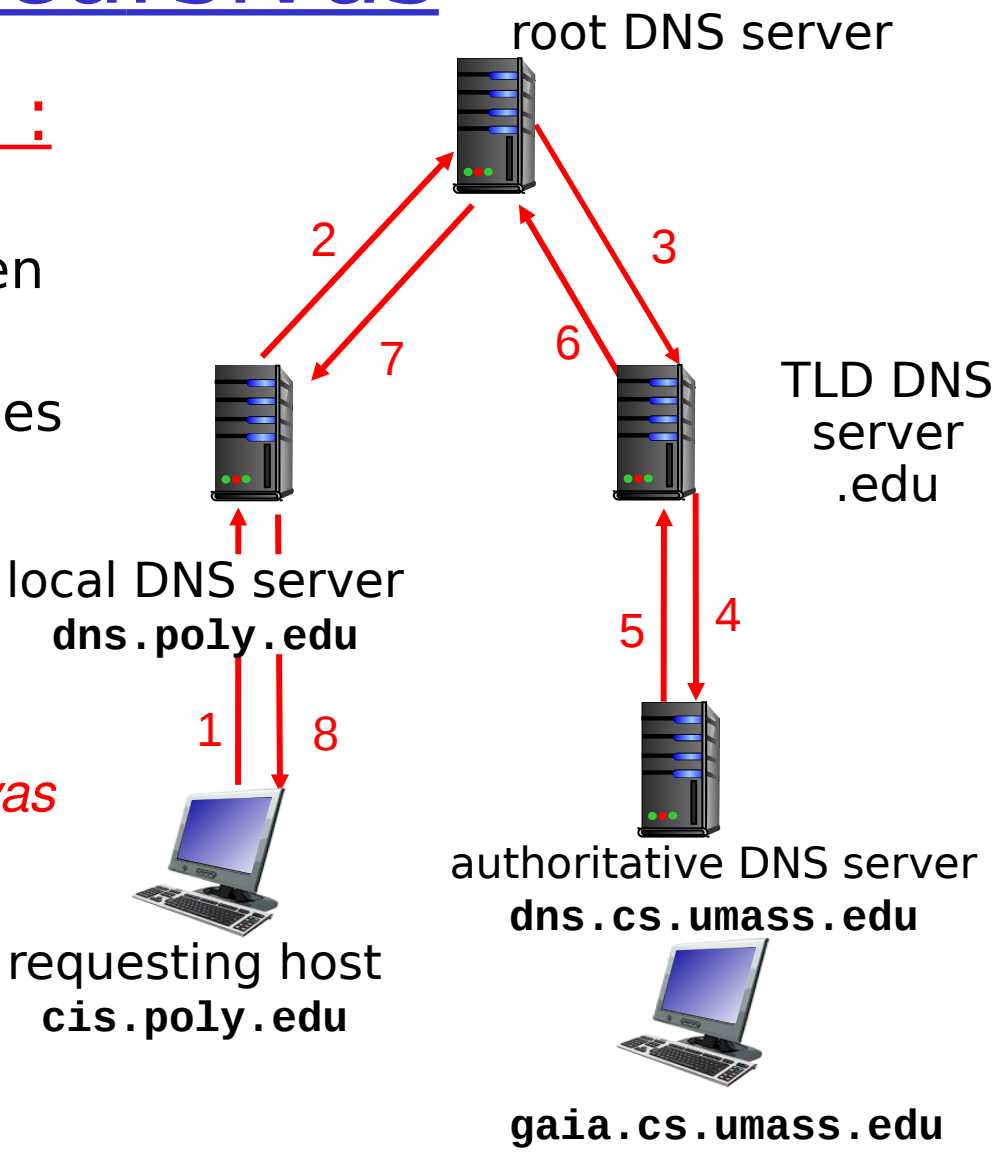

Servidor local, aquel que hace las consultas por mi aplicación
www.isoc.org?
ISP
www.isoc.org?
Answer is x.y.w.z
isoc.org
org
ISOC server
org server
root server
Consulta iterativa
Servidor autoritario, aquel que define el mapeo nombre <-> IP

Consultas Recursivas

Consulta recursiva :

- Pone la carga de la resolución de nombre en servidor contactado.
- ¿Qué pasa en situaciones de alta carga?

Consultas Recursivas



Ejemplo

- Hacer algo del tipo:
  $ nslookup www.elo.utfsm.cl
- Luego:
  $ nslookup 200.1.17.5
- Finalmente:
  $nslookup www.google.com
- Y
  $ nslookup 64.233.161.99
- Estando en aragorn hacer:
  $ nslookup 200.1.17.195

Es común que las máquinas tengan asignados alias; por ejemplo profesores.elo.utfsm.cl es un alias para deneb.elo.utfsm.cl. ¿Expliqué por qué no conviene usar profesores.elo.utfsm.cl como nombre canónico de la máquina?

- Usando profesores.elo.utfsm.cl como alias es posible configurar otra máquina para reemplazar el servidor WEB y una vez que esté lista, sólo hacemos el cambios del alias en el DNS para que los accesos futuros se dirijan al nuevo servidor. Esta operación resulta transparente para los usuarios. Si fuera nombre canónico, mientras configuramos el nuevo servidor WEB, requeriríamos tener dos máquinas con igual nombre. Esto no funciona, al igual que las IPs los nombres canónicos deben ser únicos en la red.

DNS: Cache y actualización de registros

- Una vez que un servidor de nombre conoce un mapeo, éste *guarda* (caches) el mapeo
  - Las entradas del cache expiran (desaparecen) después de algún tiempo (TTL, time to leave)
  - Servidores TLD típicamente están en cache de los servidores de nombre locales
    - Así los servidores de nombre raíz no son visitados con frecuencia
- Valores almacenados pueden estar obsoletos
  - Si la IP de un nombre de máquina cambia, puede demorar hasta TTL en ser conocido en todo Internet.
  - El mecanismo para cambiar nombres está estandarizado (RFC 2136).

Registros DNS

DNS: es una base de datos distribuida que almacena registros de recursos (resource records, RR)

Formato RR: **(name, value, type, ttl)**

Type=A

- **name** es un hostname (nombre real o canónico)
- **value** es una dirección IP

Type=NS

- **name** es un dominio (e.g. foo.com)
- **value** es la dirección IP (nombre) del servidor autoritario que sabe cómo obtener las direcciones IP de este dominio.

Type=CNAME

- **name** es un alias para algún nombre real (indicado en type A)
- www.ibm.com es realmente servereast.backup2.ibm.com
- **value** es el nombre real (canónico)

Type=MX

- **value** es el nombre del servidor de correo asociado con **name**

Inserción de registros en DNS

- Ejemplo: Recién se crea una empresa “Network Utopia”
- Debemos registrar el nombre networkuptopia.com en un administrador de dominio (e.g., Network Solutions)
  - Necesitamos proveer el nombre y la dirección IP de nuestro servidor de nombre autoritario (primario y secundario)
  - Administrador del dominio inserta dos RRs en el servidor TLD .com:

```
(networkutopia.com, dns1.networkutopia.com, NS)
(dns1.networkutopia.com, 212.212.212.1, A)
```

- Incorporar en el servidor autoritario un registro Tipo A para www.networkuptopia.com y un registro Tipo NS para networkutopia.com
- En Chile debemos acceder a NIC Chile para arrendar un nombre de dominio.

Pregunta tipo certamen

Explique por qué los resultados de varios PING a www.youtube.com muestran direcciones IPs distintas:
agustin@agustin-laptop:~$ ping www.youtube.com
PING youtube-ui.l.google.com (74.125.224.76) 56(84) bytes of data.
64 bytes from 74.125.224.76: icmp_seq=1 ttl=52 time=162 ms
.... Luego:
agustin@agustin-laptop:~$ ping www.youtube.com
PING youtube-ui.l.google.com (74.125.224.42) 56(84) bytes of data.
64 bytes from 74.125.224.42: icmp_seq=1 ttl=52 time=160 ms
.... Luego:
agustin@agustin-laptop:~$ ping www.youtube.com
PING youtube-ui.l.google.com (74.125.224.79) 56(84) bytes of data.
64 bytes from 74.125.224.79: icmp_seq=1 ttl=52 time=175 ms
...
Explique cómo esto es posible.

?

- El ping a un mismo nombre lógico condujo a tres máquinas distintas por ello tres IPs distintas. Esto se explica porque el servicio de youtube es atendido por un conjunto de máquinas para poner servir a más usuarios a la vez.
- Esto es posible gracias al servidor DNS. Cuando el ping consulta por la IP de www.youtube.com, el servidor que maneja este nombre identifica la máquina adecuada de entre el conjunto para atender la petición y retorna esa dirección IP.

Ataques DNS

Ataque DDoS (distributed denial-of-service)

- Bombardear servidor raíz con tráfico
  - No son exitosos hoy.
  - La red filtra el tráfico
  - Servidor DNS local guarda IPs de servidores TLD
- Bombardear servidores TLD
  - Potencialmente más peligroso

Ataques de redirección

- man-in-middle
  - Intercepta y responde consulta
- Envenenamiento DNS
  - Envía respuestas falsas al servidor DNS, quien las caches

aprovechar DNS para DDoS

- Enviar consultas con dirección origen falsa (es la IP atacada)
- requiere amplificación (muchas máquinas haciendo lo mismo)

Capítulo 2: Capa Aplicación

- 2.1 Principios de la aplicaciones de red
- 2.2 Web y HTTP
- 2.3 Correo Electrónico
  - SMTP, POP3, IMAP
- 2.4 DNS
- 2.5 Aplicaciones P2P
- 2.6 Video streaming y redes de distribución de contenidos
- 2.7 Programación de sockets con UDP y TCP