Introducción a DNS

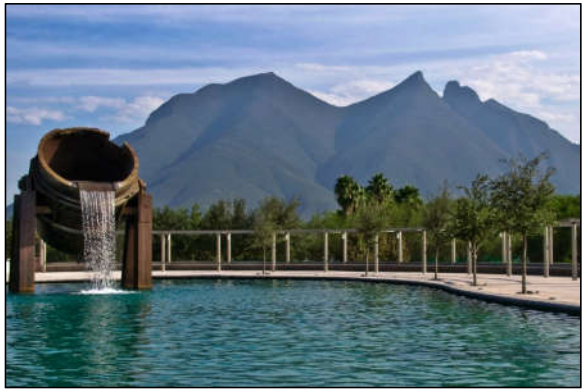
Marzo 2020

Mérida, Yucatán

Pacto entre damas y caballeros

Todos estamos aquí para aprender

Todos participamos en la plática



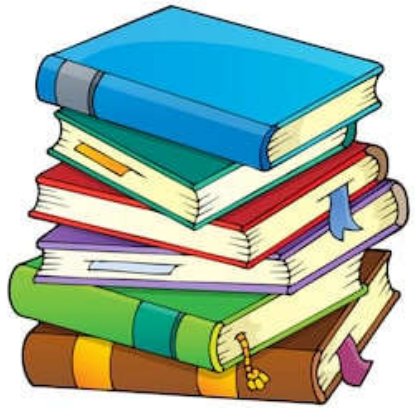
Perdonamos y aceptamos el acento norteño del instructor

Sistema de Nombres de Dominio (DNS)

- Definido originalmente en 1983:
  - [RFC 882] Domain Names – Concepts and Facilities.
  - [RFC 883] Domain Names – Implementation and Specification.
- Re-Definido en 1987:
  - [RFC 1034] Domain Names – Concepts and Facilities.
  - [RFC 1035] Domain Names – Implementation and Specification.

Sistema de Nombres de Dominio (DNS)

Existen 297 RFC relacionados con DNS



De los cuales:

- 48 son obsoletos.
- 4 son históricos.
- 4 sin clasificación.

Nos quedan 238 documentos por leer, y que equivalen a 4,001 páginas.

Para referencia, los 7 libros de Harry Potter suman 4,100 páginas.


History

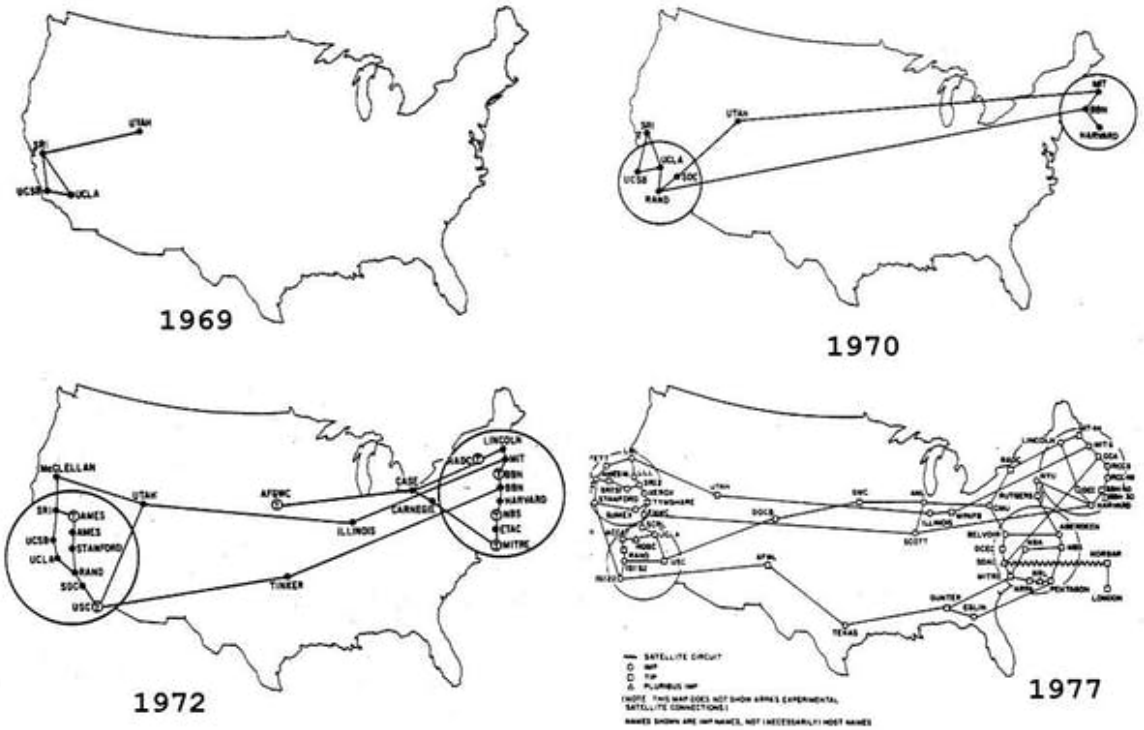
Historia: La Guerra Fría

Historia: Crisis de Misiles

Historia: ARPANET

Primeros 4 nodos:

- UCLA
- Stanford
- UCSB
- UTAH



Historia: ARPANET

Nombre	Dirección
athenas	21
zeus	23
platon	40
usc	43
california	59

*IP existió hasta 1981

Hosts file

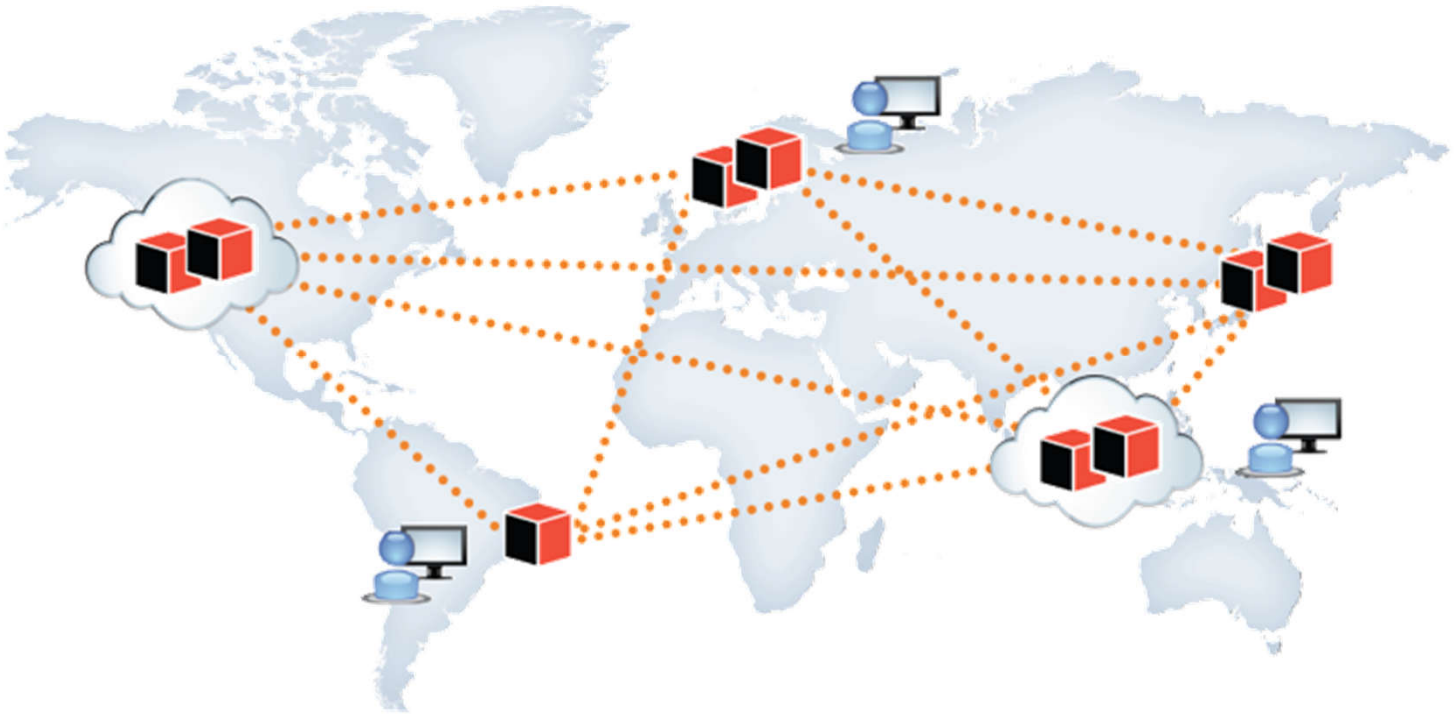
Nombres de Dominio

```
# Hosts file.
127.0.0.1          localhost
172.271.15.14      google.com
200.34.200.231     itesm.mx
200.94.180.59      nic.mx
54.173.169.115     netflix.com
17.178.96.59       apple.com
140.82.114.4       github.com
104.244.42.193     twitter.com
…
```

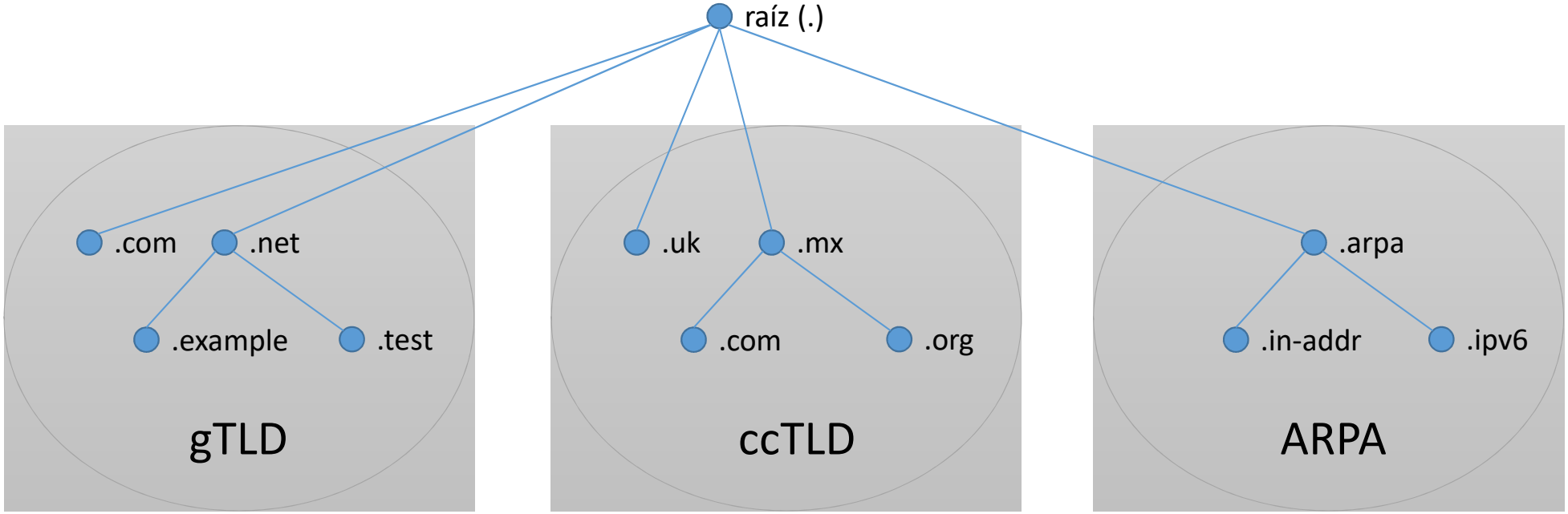
Sistema Operativo	Locación
UNIX	/etc/hosts
Windows 7, 8, 10	\System32\drivers\etc\hosts
Apple OS X	/etc/hosts
Android	/etc/hosts
Apple iOS	/etc/hosts

Nombres de Dominio	350 millones
Espacio por cada Dominio	100 bytes
Tamaño del archivo	32.60 GB

Base de datos distribuida



Delegación de nombres de dominio



Country Codes of the World

Ejemplos de gTLD

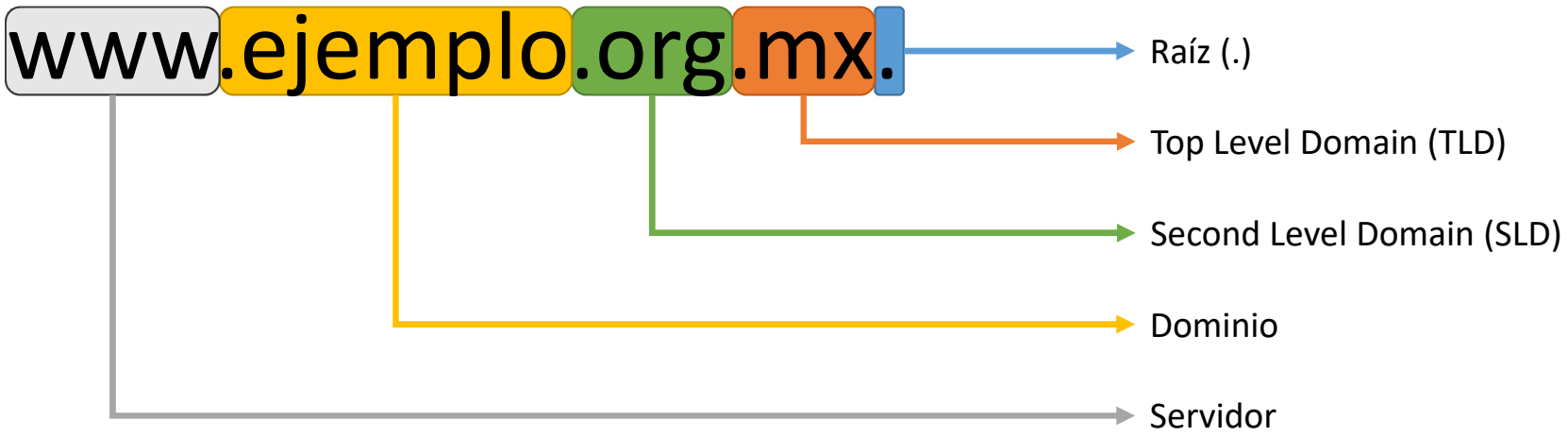
Originales	Empresas	Localidades	Comunidades
• com	• amazon	• asia	• football
• net	• apple	• boston	• futbol
• org	• google	• tokyo	• games
• edu	• ibm	• nyc	• gay
• info	• lego	• vegas	• lat
• gov	• mitsubishi	• paris	• pizza

Nombre de dominios

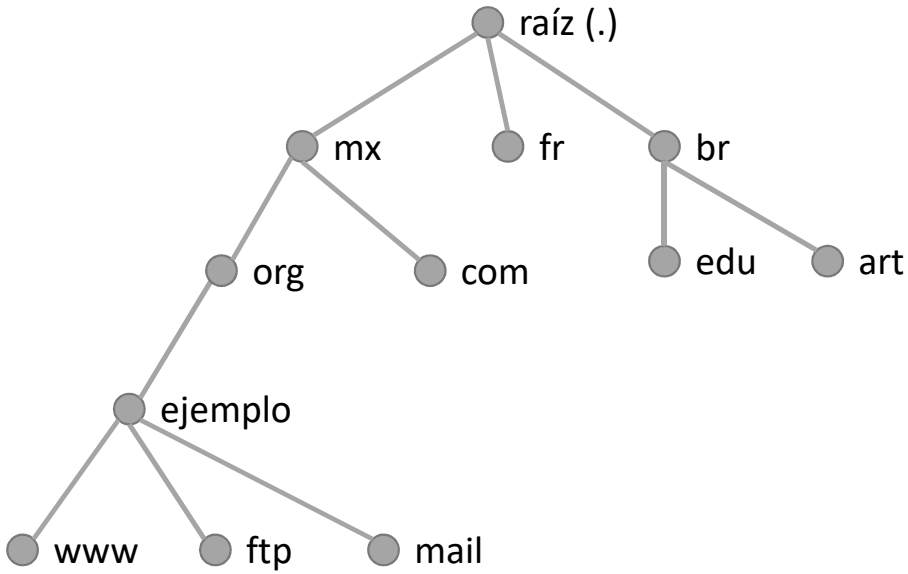
Reglas de las Etiquetas

- Insensible a mayúsculas y minúsculas.
- Letras, números y guiones.
- Tamaño máximo de 63 caracteres.
- No puede empezar o finalizar con guion o tener dos guiones seguidos.

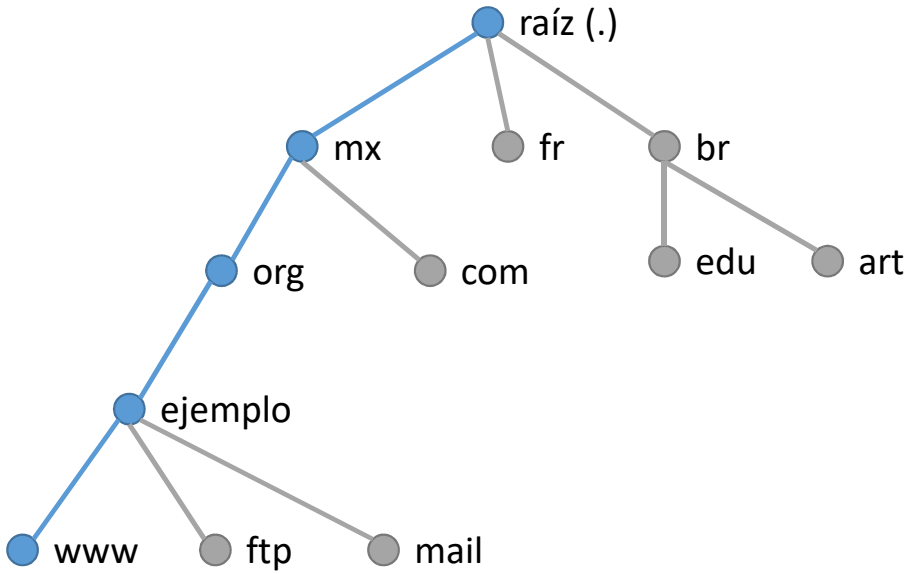
Nombre de dominios



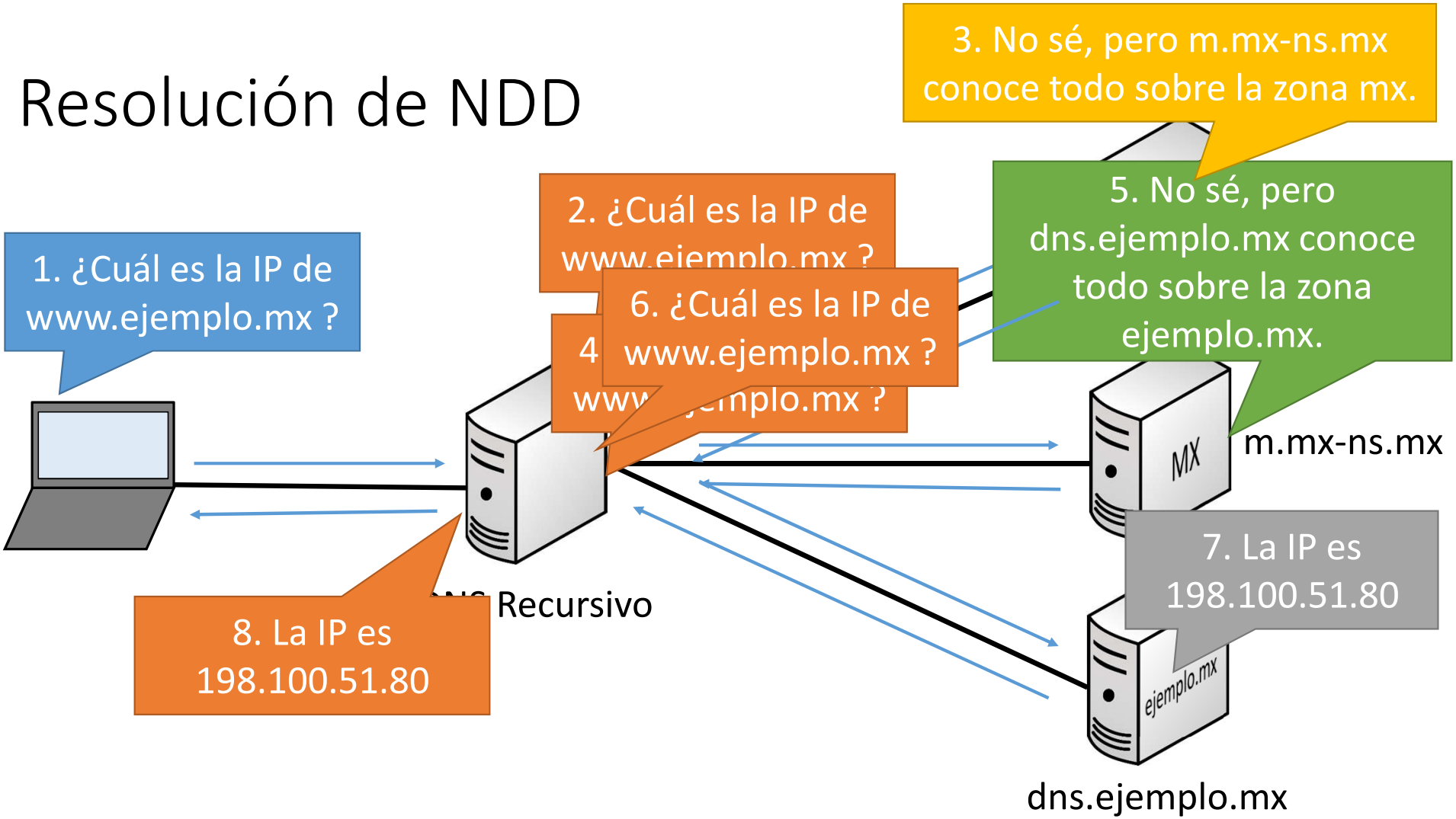
Árbol Invertido



Árbol Invertido



Resolución de NDD



Ejemplo de Consulta Recursiva

```
$:\> dig www.nic.mx. A

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.3 <<>>
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40983
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.nic.mx.            IN A

;; ANSWER SECTION:
www.nic.mx.            299 IN A 200.94.180.59
www.nic.mx.            299 IN A 200.94.180.58
www.nic.mx.            299 IN A 200.94.180.61
www.nic.mx.            299 IN A 200.94.180.60

;; Query time: 105 msec
;; MSG SIZE  rcvd: 103
```

Zonas de DNS

Las zonas de DNS están formadas por registros RR (Resource Records)

Cada registro tiene el siguiente formato:

Owner	TTL	Class	Type	RData
www.example.mx.	300	IN	A	198.51.100.24
www.example.mx.	300	IN	A	192.0.2.80
www.example.mx.	300	IN	AAAA	2001:db8:cafe::20
ftp.example.mx.	600	IN	A	192.0.2.200

Ejemplos de Tipos de RR

- A
- NS
- CNAME
- SOA
- PTR
- HINFO
- MINFO
- MX
- TXT
- KEY
- AAAA
- SRV
- OPT
- DNAME
- TLSA
- DS
- NSEC
- NSEC3
- NSEC3PARAM
- RRSIG
- DNSKEY
- ZONEMD
- GPOS
- SMIMEA

Ejemplos de Tipos de RR

- A
- NS
- CNAME
- SOA
- PTR
- HINFO
- MINFO
- MX
- TXT
- KEY
- AAAA
- SRV
- OPT
- DNAME
- TLSA
- DS
- NSEC
- NSEC3
- NSEC3PARAM
- RRSIG
- DNSKEY
- ZONEMD
- GPOS
- SMIMEA

Ejemplos de Tipos de RR

- A
- NS
- CNAME
- SOA
- PTR
- HINFO
- MINFO
- MX
- TXT
- KEY
- AAAA
- SRV
- OPT
- DNAME
- TLSA
- DS
- NSEC
- NSEC3
- NSEC3PARAM
- RRSIG
- DNSKEY
- ZONEMD
- GPOS
- SMIMEA

Ejemplo de Zona de DNS

```
# Owner             TTL     Class   Type    RData
example.mx.         86400   IN      SOA     dns.example.mx. root.example.mx. (
                                            80          ; serial
                                            28800       ; refresh (8h)
                                            7200        ; retry (2h)
                                            2419200     ; expire (4w)
                                            86400)      ; minimum (1d)

example.mx.         3600    IN      NS      dns.example.mx.
dns.example.mx.     3600    IN      A       192.0.2.1
```

Ejemplo de Zona de DNS

# Owner	TTL	Class	Type	RData
example.mx.	3600	IN	MX	10 mail.example.mx.
example.mx.	3600	IN	MX	20 mail.example.com.
mail.example.mx.	3600	IN	A	192.0.2.35
mail.example.com.	3600	IN	A	198.51.100.102
www.example.mx.	3600	IN	A	192.0.2.80
ftp.example.mx.	3600	IN	CNAME	www.example.mx.
mty.example.mx.	3600	IN	NS	dns.mty.example.mx.
mid.example.mx.	3600	IN	NS	dns.mid.example.mx.

Ejemplo de Zona de DNS

# Owner	TTL	Class	Type	RData
example.mx.	3600	IN	MX	10 mail.example.mx.
example.mx.	3600	IN	MX	20 mail.example.com.
mail.example.mx.	3600	IN	A	192.0.2.35
mail.example.com.	3600	IN	A	198.51.100.102
www.example.mx.	3600	IN	A	192.0.2.80
ftp.example.mx.	3600	IN	CNAME	www.example.mx.
mty.example.mx.	3600	IN	NS	dns.mty.example.mx.
mid.example.mx.	3600	IN	NS	dns.mid.example.mx.
dns.mty.example.mx.	3600	IN	A	128.66.10.1
dns.mid.example.mx.	3600	IN	A	128.66.20.1

Lame delegation

Glue records

Ejemplo de Zona de DNS

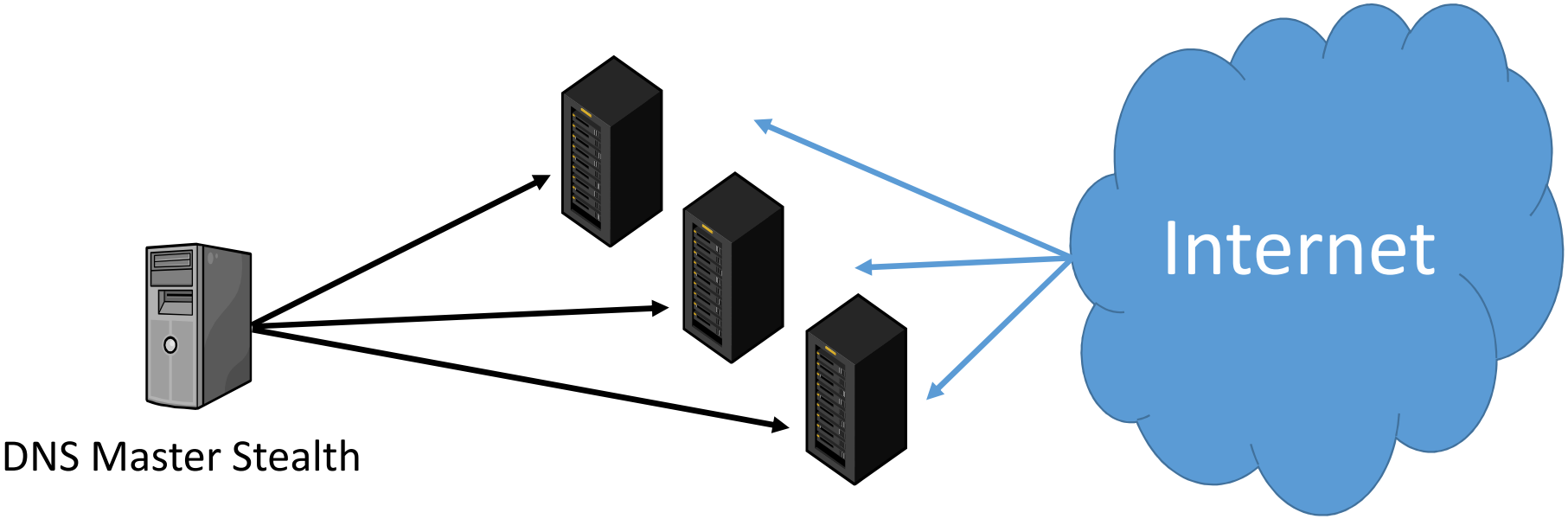
```
$ORIGIN example.mx.
$TTL  3600
@           IN    SOA   dns.example.mx. root.example.mx. (80 8h 2h 4w 1d)
            IN    NS    dns.example.mx.
            IN    MX    10 mail.example.mx.
            IN    MX    20 mail.example.com.

dns         IN    A     192.0.2.1
mail        IN    A     192.0.2.35
www         IN    A     192.0.2.80
ftp         IN    CNAME www.example.mx.
```

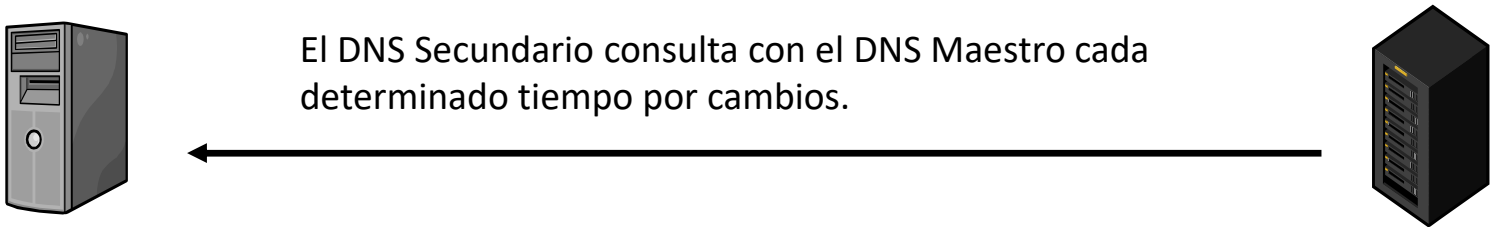
Ejemplo de Zona de DNS

```
mty          IN    NS    dns.mty.example.mx.
mid          IN    NS    dns.mid.example.mx.
dns.mty      IN    A     128.66.10.1
dns.mid      IN    A     128.66.20.1
```

Servidores DNS Autoritativos en Producción



Sincronización de Zonas



Campo	Ejem	Descripción
Serial	80	Identificador de la versión de la zona.
Refresh	8h	Indica cada cuando el DNS Secundario busca actualizaciones en el DNS Master Stealth
Retry	2h	Indica el tiempo que debe esperar el DNS Secundario en caso de error de comunicación con DNS Master Stealth
Expire	4w	Si el DNS Secundario no logra conectarse con DNS Master Stealth en este tiempo, el secundario “olvidará la zona”
Minimum	1h	TTL para guardar las respuestas negativas.

Sincronización de Zonas “Nueva Forma”

Cuando el DNS Master Stealth tiene cambios manda un mensaje llamado Notify a los esclavos.

DNS Master Stealth

DNS Secundario

Transferencias de Zonas de DNS

- AXFR.
  - El servidor esclavo solicita la zona completa al servidor maestro.
  - El servidor maestro manda la zona completa al servidor esclavo.

- IXFR.
  - El servidor secundario le indica al maestro el serial que tiene de la zona.
  - El servidor maestro manda solo los cambios entre la versión que tiene el servidor esclavo y la actual.

Servidores Autoritativos de la Zona MX

- México
  - Monterrey
  - Ciudad de México
- Estados Unidos
  - San José, CA
  - Dallas, TX
  - New York, NY
- Chile
  - Santiago

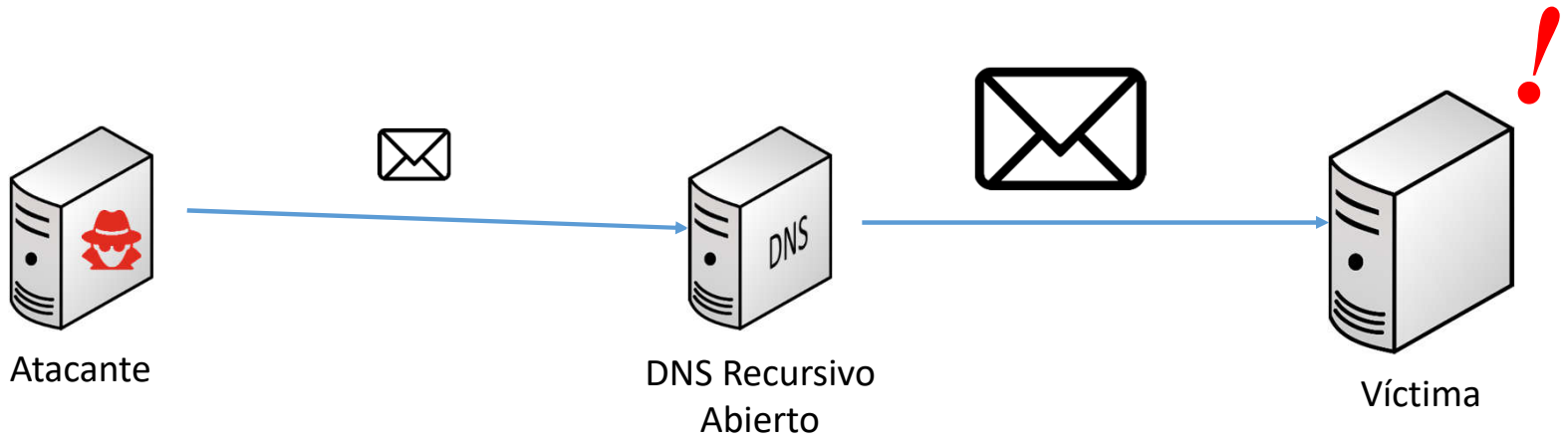
NIC MÉXICO

Servidores Autoritativos de la Zona MX

Tips de Seguridad para Servidores DNS

1. Audita tus zonas de DNS.
2. Mantén actualizado el software del servidor de DNS.
3. Ocultar versión del software del servidor de DNS.
4. En caso de servidores autoritativos:
   a. Restringir las transferencias de zonas.
   b. Deshabilitar las consultas recursivas.
5. En caso de servidores recursivos:
   a. restringir el servicio a solo mis usuarios.

Ataque de DoS – Amplificación



Servidores DNS Recursivos Públicos

Proveedor	IPv4	IPv6
Cloudflare	1.1.1.1 1.0.0.1	2606:4700:4700::1111 2606:4700:4700::1001
Google	8.8.8.8 8.8.4.4	2001:4860:4860::8888 2001:4860:4860::8844
Quad9	9.9.9.9 149.112.112.112	2620:fe::fe 2620:fe::9

“When something online is free, you’re not the customer, you’re the product.”

Servidores DNS de Código Abierto

IDN

- [1987] El RFC 1034 define los nombres de dominio como letras, números y guiones.
  - Las letras aceptadas solo son las del ASCII-7.
  - Es decir, letras usadas en idioma inglés.

- [2003] El RFC 3490 define: “Internationalizing Domain Names in Applications (IDNA)”.

- [2010] Los RFC 5890 y 5891 redefinen los IDN.

IDN

En IDN, nombres de dominios con letras fuera del alfabeto inglés son posibles:

- ✓ www.mérida.mx.
- ✓ tienda.piñatas.mx.
- ✓ 日本語ドメイン.jp.
- ✓ example.中国.

IDN

Un temor que se tenía al momento de definir IDN, es que los servidores no soportarán letras fuera del ASCII-7.

IDN	**Punycode**
• www.mérida.mx.	www.xn--mrida-bsa.mx.
• tienda.piñatas.mx.	tienda.xn--piatas-xwa.mx.
• 日本語ドメイン.jp.	xn--eckwd4c7c5976acvb2w6i.jp.
• example.中国.	example.xn--fiqs8s.

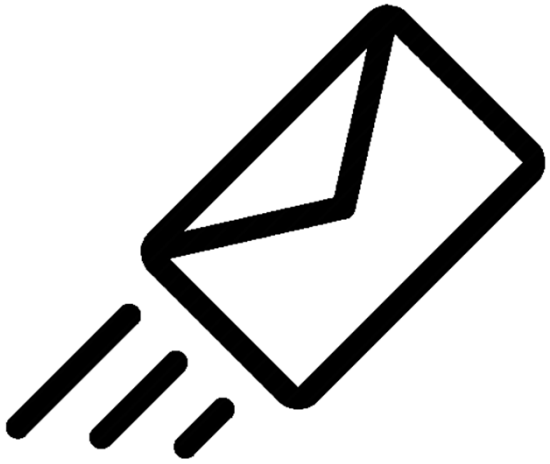
IDN

Un temor que se tenía al momento de definir IDN, es que los servidores no soportarán letras fuera del ASCII-7.

IDN	**Punycode**
• www.mérida.mx.	www.xn--mrida-bsa.mx.
• tienda.piñatas.mx.	tienda.xn--piatas-xwa.mx.
• 日本語ドメイン.jp.	xn--eckwd4c7c5976acvb2w6i.jp.
• example.中国.	example.xn--fiqs8s.

Transportes usados por DNS

- TCP
- UDP
- HTTPS (DnsOverHTTPS o DoH)
- TLS (DnsOverTLS o DoT)



¿Preguntas?