



# **Domain Name System**

**Ing. Norberto Gaspar Cena**  
Redes de Información

4to Año Ingeniería en Sistemas de Información

# Introducción

Las comunicaciones son a través de direcciones de IP

Cuántas direcciones de IP pueden memorizar?

Los nombres son mucho más fáciles de recordar

Cada nombre corresponde a una dirección IP

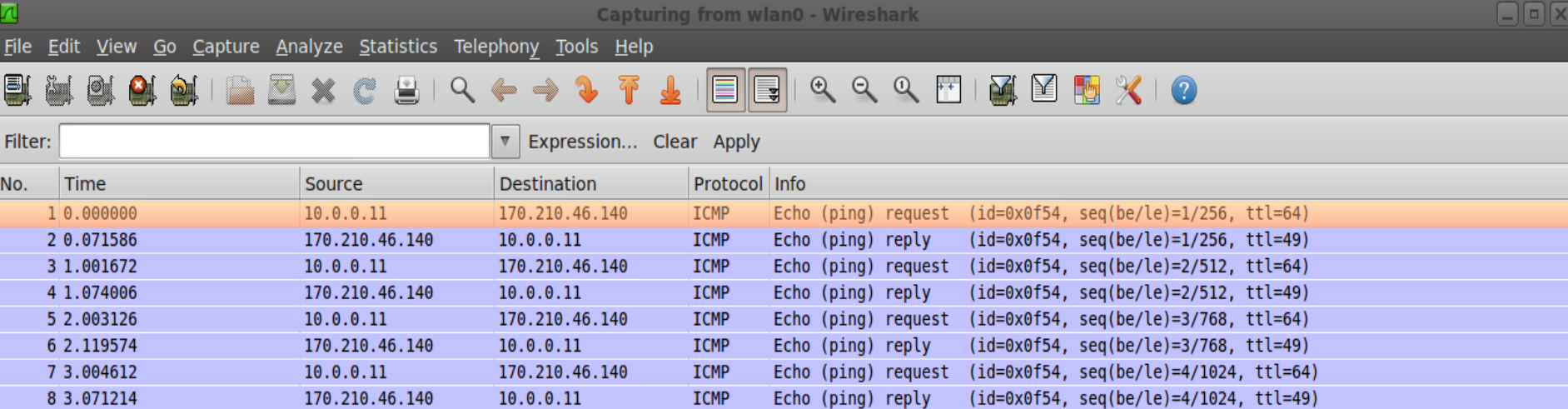
- `www.frvn.utn.edu.ar` corresponde a `190.114.198.110`

Una opción es tener un archivo de hosts con entrada para todas las estaciones

- En windows `.../system32/drivers/etc/hosts`
- En linux `/etc/hosts`

Una solución más lógica es utilizar el sistema de nombres de dominio

# DNS – Ej. Captura ping ip



Capturing from wlan0 - Wireshark

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.11	170.210.46.140	ICMP	Echo (ping) request (id=0x0f54, seq(be/le)=1/256, ttl=64)
2	0.071586	170.210.46.140	10.0.0.11	ICMP	Echo (ping) reply (id=0x0f54, seq(be/le)=1/256, ttl=49)
3	1.001672	10.0.0.11	170.210.46.140	ICMP	Echo (ping) request (id=0x0f54, seq(be/le)=2/512, ttl=64)
4	1.074006	170.210.46.140	10.0.0.11	ICMP	Echo (ping) reply (id=0x0f54, seq(be/le)=2/512, ttl=49)
5	2.003126	10.0.0.11	170.210.46.140	ICMP	Echo (ping) request (id=0x0f54, seq(be/le)=3/768, ttl=64)
6	2.119574	170.210.46.140	10.0.0.11	ICMP	Echo (ping) reply (id=0x0f54, seq(be/le)=3/768, ttl=49)
7	3.004612	10.0.0.11	170.210.46.140	ICMP	Echo (ping) request (id=0x0f54, seq(be/le)=4/1024, ttl=64)
8	3.071214	170.210.46.140	10.0.0.11	ICMP	Echo (ping) reply (id=0x0f54, seq(be/le)=4/1024, ttl=49)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on wlan0, interface 0, 0 packets captured, 0 packets filtered

Ethernet II, Src: HonHaiPr\_d4:32:27 (4c:00:02:d4:32:27), Dst: 02:00:00:00:00:00

Internet Protocol, Src: 10.0.0.11 (10.0.0.11), Dst: 170.210.46.140

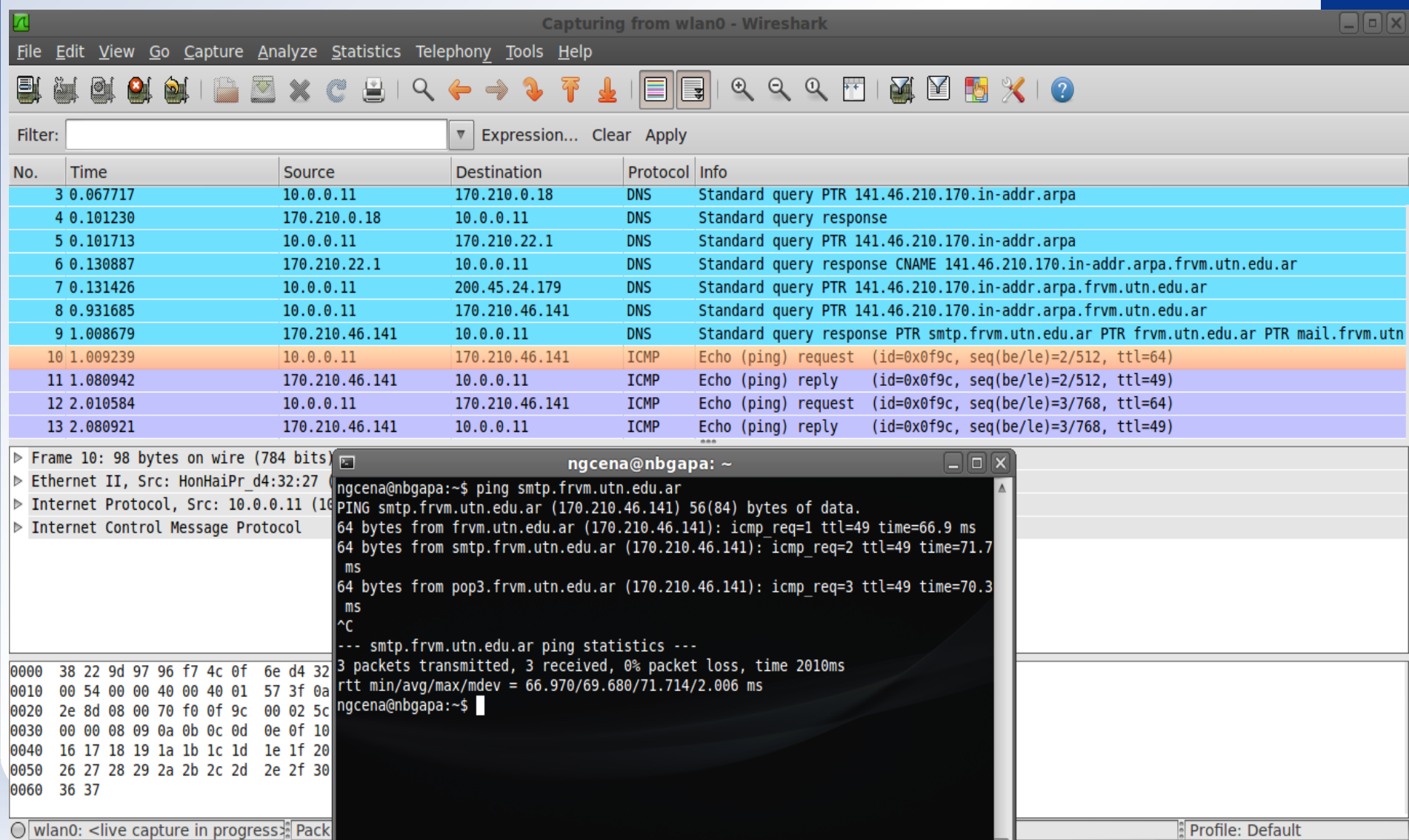
Internet Control Message Protocol

```
ngcena@nbgapa: ~  
ngcena@nbgapa:~$ ping 170.210.46.140  
PING 170.210.46.140 (170.210.46.140) 56(84) bytes of data.  
64 bytes from 170.210.46.140: icmp_req=1 ttl=49 time=71.6 ms  
64 bytes from 170.210.46.140: icmp_req=2 ttl=49 time=72.3 ms  
64 bytes from 170.210.46.140: icmp_req=3 ttl=49 time=116 ms  
64 bytes from 170.210.46.140: icmp_req=4 ttl=49 time=66.6 ms  
^C  
--- 170.210.46.140 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 66.626/81.769/116.473/20.157 ms  
ngcena@nbgapa:~$
```

wlan0: <live capture in progress> Packets: 0

Profile: Default

# DNS – Ej. Captura ping nombre



The image displays a Wireshark packet capture window titled "Capturing from wlan0 - Wireshark". The main packet list shows 13 packets. Packets 3 through 13 are highlighted in blue, indicating they are selected. The details pane on the left shows the selected packet (No. 10) as an ICMP Echo (ping) request. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Info
3	0.067717	10.0.0.11	170.210.0.18	DNS	Standard query PTR 141.46.210.170.in-addr.arpa
4	0.101230	170.210.0.18	10.0.0.11	DNS	Standard query response
5	0.101713	10.0.0.11	170.210.22.1	DNS	Standard query PTR 141.46.210.170.in-addr.arpa
6	0.130887	170.210.22.1	10.0.0.11	DNS	Standard query response CNAME 141.46.210.170.in-addr.arpa.frv.m.utn.edu.ar
7	0.131426	10.0.0.11	200.45.24.179	DNS	Standard query PTR 141.46.210.170.in-addr.arpa.frv.m.utn.edu.ar
8	0.931685	10.0.0.11	170.210.46.141	DNS	Standard query PTR 141.46.210.170.in-addr.arpa.frv.m.utn.edu.ar
9	1.008679	170.210.46.141	10.0.0.11	DNS	Standard query response PTR smtp.frv.m.utn.edu.ar PTR frv.m.utn.edu.ar PTR mail.frv.m.utn.edu.ar
10	1.009239	10.0.0.11	170.210.46.141	ICMP	Echo (ping) request (id=0x0f9c, seq(be/le)=2/512, ttl=64)
11	1.080942	170.210.46.141	10.0.0.11	ICMP	Echo (ping) reply (id=0x0f9c, seq(be/le)=2/512, ttl=49)
12	2.010584	10.0.0.11	170.210.46.141	ICMP	Echo (ping) request (id=0x0f9c, seq(be/le)=3/768, ttl=64)
13	2.080921	170.210.46.141	10.0.0.11	ICMP	Echo (ping) reply (id=0x0f9c, seq(be/le)=3/768, ttl=49)

Frame 10: 98 bytes on wire (784 bits)  
Ethernet II, Src: HonHaiPr\_d4:32:27  
Internet Protocol, Src: 10.0.0.11 (10.0.0.11)  
Internet Control Message Protocol

```
ngcena@nbgapa: ~  
ngcena@nbgapa:~$ ping smtp.frv.m.utn.edu.ar  
PING smtp.frv.m.utn.edu.ar (170.210.46.141) 56(84) bytes of data.  
64 bytes from frv.m.utn.edu.ar (170.210.46.141): icmp_req=1 ttl=49 time=66.9 ms  
64 bytes from smtp.frv.m.utn.edu.ar (170.210.46.141): icmp_req=2 ttl=49 time=71.7 ms  
64 bytes from pop3.frv.m.utn.edu.ar (170.210.46.141): icmp_req=3 ttl=49 time=70.3 ms  
^C  
--- smtp.frv.m.utn.edu.ar ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2010ms  
rtt min/avg/max/mdev = 66.970/69.680/71.714/2.006 ms  
ngcena@nbgapa:~$
```

wlan0: <live capture in progress> Pack

Profile: Default

# DNS – Estructura

## Centralizado vs Distribuido

- Único punto de fallo
- Volumen de tráfico
- Mantenimiento

## Sistema jerárquico distribuido

- El **sistema de nombres de dominio** se basa en un esquema jerárquico que permite asignar nombres.
- Las **consultas al DNS** son realizadas por los clientes a través de las rutinas de resolución (“*resolver*” o *resolvedor* o *resolutor*)



# DNS – Estructura

## Servidores DNS Raíz

- 13 en todo al mundo (a-m)
- Replicados

## Servidores de dominio de nivel superior (TLD)

- com, edu, ar, net, gov, etc.

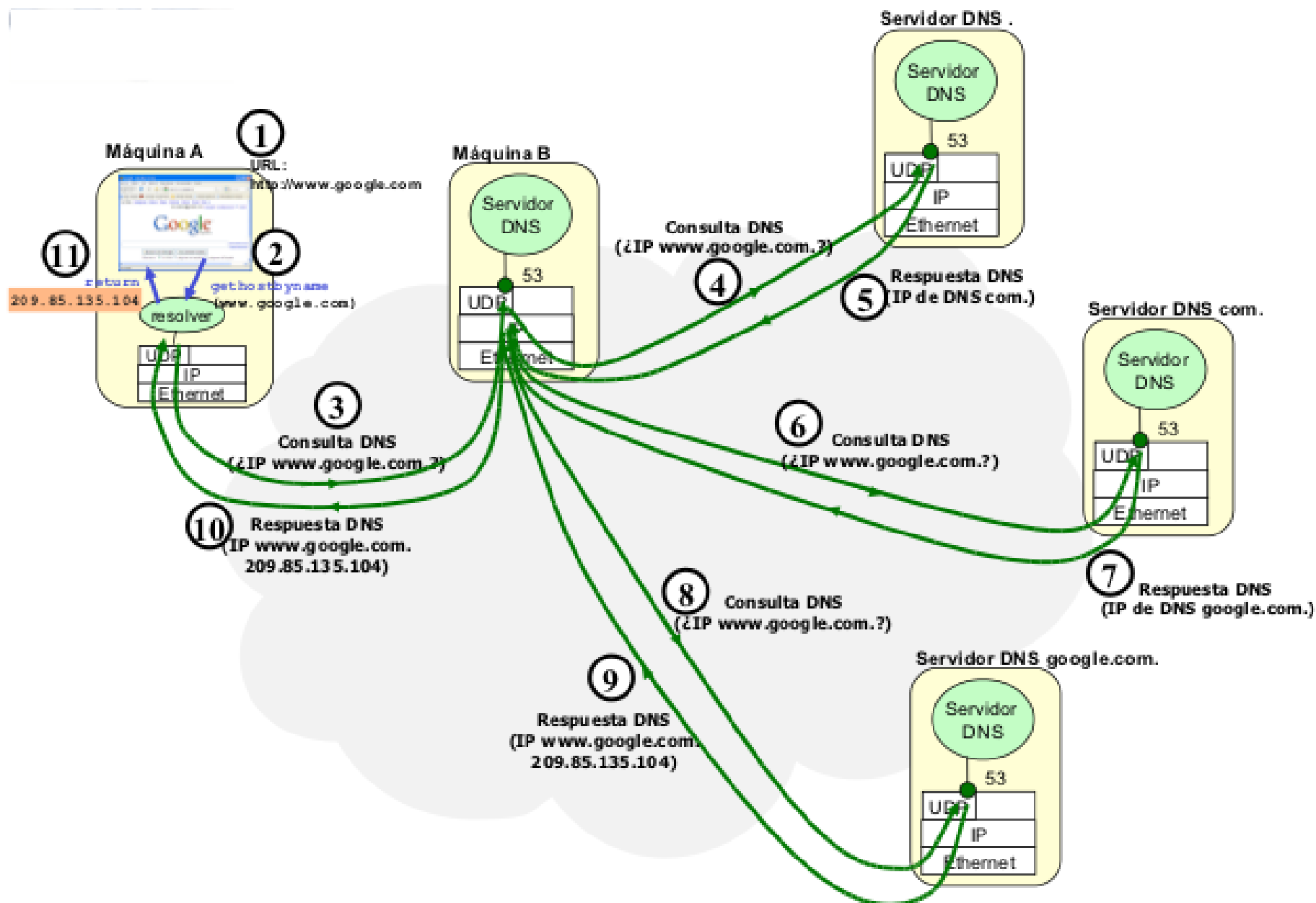
## Servidores DNS autoritativos

- DNS de nivel inferior
- DNS de las organizaciones
  - Principales y secundarios
  - Terciarizados o propios

# DNS – Estructura

<http://www.root-servers.org>







# DNS – Caché

Cuando un servidor hace una búsqueda, aprende un dato que no sabía, lo guarda en su caché

La configuración especifica el tiempo que puede estar ese dato en una caché

Algunos sistemas operativos pueden almacenar una cache a través de sus resolver

Algunas aplicaciones mantienen una caché (navegadores)

# DNS – Sintaxis de los nombres

El **Nombre de dominio** es una cadena de hasta 255 caracteres

Esta formada por etiquetas separadas por puntos de forma jerárquica

No se distinguen mayúsculas de minúsculas

**Ejemplo:** frvm.utn.edu.ar tiene 4 etiquetas

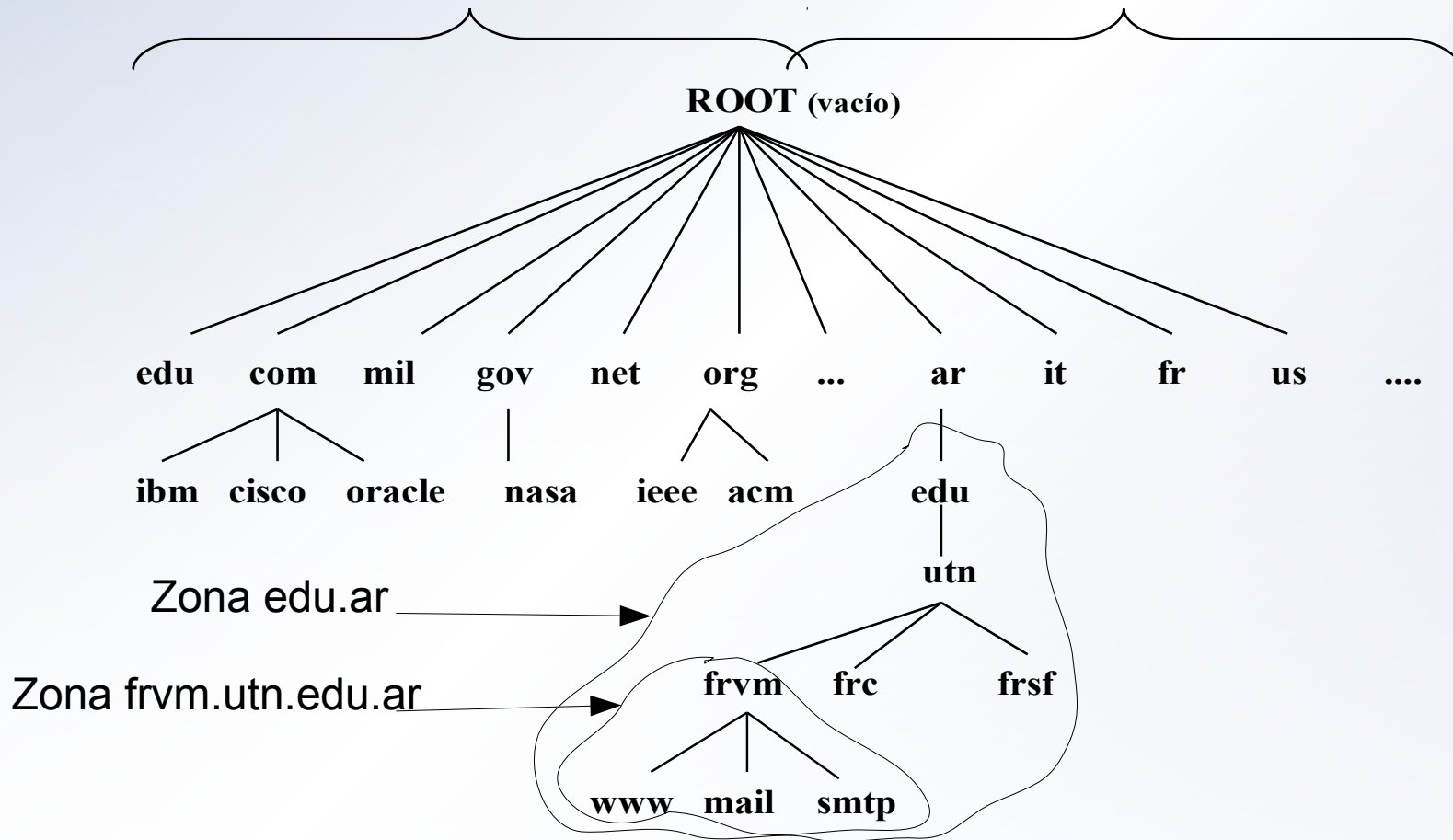
**Dominio de nivel superior “ar.”**

**Dominio de 2º nivel “edu.ar.”**

**Dominio de 3º nivel “utn.edu.ar.”**

**Dominio de nivel inferior “frvm.utn.edu.ar.”**

# DNS – Árbol de clasificación



Puede haber nombres duplicados en dominios diferentes

# DNS – Árbol de clasificación

Nombre de Dominio	Significado
COM	Organizaciones comerciales, Microsoft.com, ibm.com
EDU	Universidades, Instituciones academicas,...
GOV	Instituciones Gubernamentales
MIL	Organizaciones militares
ORG	Organizaciones no comerciales
NET	Grupos relacionados con la Red
INT	Organizaciones Internacionales

TLD = Top Level Domain

# DNS – Delegación de Autoridad

La organización que posee un nombre de dominio, es responsable del funcionamiento y mantenimiento de los servidores de nombres.

- Esta área de influencia se llama zona de autoridad

La solicitud de registro se realiza a una autoridad competente.

Es necesario identificar al menos 2 DNS

Cada país a su vez también dispone de autoridades de registro

La autoridad del dominio TLD “ar.” que registra los dominios de 2º nivel: [www.nic.ar](http://www.nic.ar) ([mrecic.gov.ar](http://mrecic.gov.ar))

En una zona existe un administrador local *que a su vez puede delegar* en otros administradores.

- ej. “[utn.edu.ar](http://utn.edu.ar).” delega para cada facultad regional (“[frvm.utn.edu.ar](http://frvm.utn.edu.ar).”) para gestionar este dominio inferior



# DNS – Registro de Recursos

<b>Tipo de Registro</b>	<b>Descripción</b>
SOA <i>Start Of Authority</i>	Inicio de autoridad, identificando el dominio o la zona. Fija una serie de parámetros para esta zona.
NS <i>Name Server</i>	El nombre de dominio se hace corresponder con el nombre de una computadora de confianza para el dominio o servidor de nombres.
A <i>Address</i>	Dirección IP de un host en 32 bits. Si este tiene varias direcciones IP, multihomed, habrá un registro diferente por cada una de ellas.
CNAME	Es un alias que se corresponde con el nombre canónico verdadero.
MX	Se trata de un intercambiador de correo (Mail eXchanger), es decir, un dominio dispuesto a aceptar solo correo electrónico.
TXT	Texto, es una forma de añadir comentarios a la Base de Datos. Por Ej., para dar la dirección postal del dominio.
PTR	Apuntador, hace corresponder una dirección IP con el nombre de un sistema. Usado en archivos direcciónnombre, la inversa del tipo A.

# DNS - Ejemplo de mapa

\$ORIGIN villamaria.gob.ar.

```
@           IN      SOA    villamaria.gob.ar. hostmaster.villamaria.gob.ar. (
                                20082710      ; Serial
                                10800         ;Refresh
                                7200          ;Retry
                                604800        ;Expire
                                86400 )       ;Min ttl
                                IN      NS     host4.villamaria.gob.ar.
                                IN      NS     host5.villamaria.gob.ar.
                                IN      MX     5 mail
                                IN      MX     10 correo
                                IN      A      200.43.77.4
www          IN      A      200.43.77.4
smtp         IN      A      200.43.77.4
pop3         IN      A      200.43.77.4
correo       IN      A      200.43.77.4
mail         IN      A      200.43.77.4
webmail      IN      A      200.43.77.4
villamaria.gob.ar. IN  TXT  "v=spf1 mx ptr ~all"
```

# DNS – Dinámico y vistas

Utilizado principalmente en redes de área local mediante una “vista interna”

Facilita la administración de las redes

Cuando una pc solicita número de IP se actualiza el servidor DNS

Ej.: En el dominio “frvm.edu”

- pc1 solicita dirección de IP
- DHCP entrega IP número 192.168.100.20
- DHCP le indica al DNS el nuevo registro de “frvm.edu”
- El DNS lo agrega a su configuración
  - pc1 IN A 192.168.100.20
- La pc1 puede ser accedida ahora a través de pc1.frvm.edu

# DNS – Herramientas

## nlookup

- nslookup www.google.com.ar
- nslookup www.google.com.ar servidor

## host

- host -a google.com.ar

## dig

- dig google.com.ar
- dig @servidor google.com.ar A
- dig @servidor google.com.ar any
- dig @servidor google.com.ar mx
- dig @servidor google.com.ar txt

# DNS

## Consultar inversas

- in-addr.arpa
- Cada vez más servicios controlan esta funcionalidad

## Seguridad en DNS

- DDoS a través de ICMP (10/2002)
- Ataques por intermediación (MIM)
- Es importante firmar las zonas (DNSSEC)



# Palabras Claves

DNS

SOA

DNS cache

Árbol de clasificación

Delegación de autoridad

DNS dinámico y vistas

Herramientas (dig/nslookup/host)

RFC's principales (RFC 920: Domain Requirements, RFC 1101: DNS Encoding of Network Names and Other Types, RFC 1033 : Domain Administrators Operations Guide, RFC 1034: Domain Names – Concepts and Facilities, RFC 1035: Domain Names – Implementation and Specification, RFC 1591: Domain Name System Structure and Delegation, RFC 1183: New RR Types)