

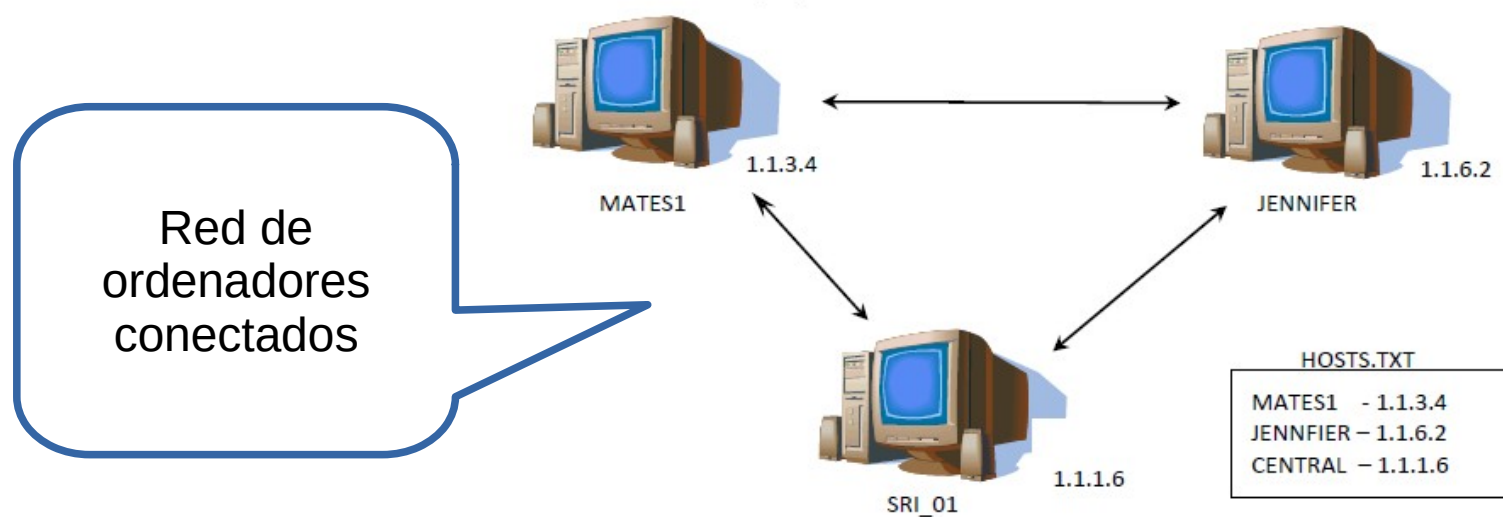
Módulo: Servicios en Red
Curso: 2º SMR



Servicio DNS

Profesor: José A. Jiménez (jose.jimenezcastillo@educa.madrid.org)
IES Clara del Rey – Madrid

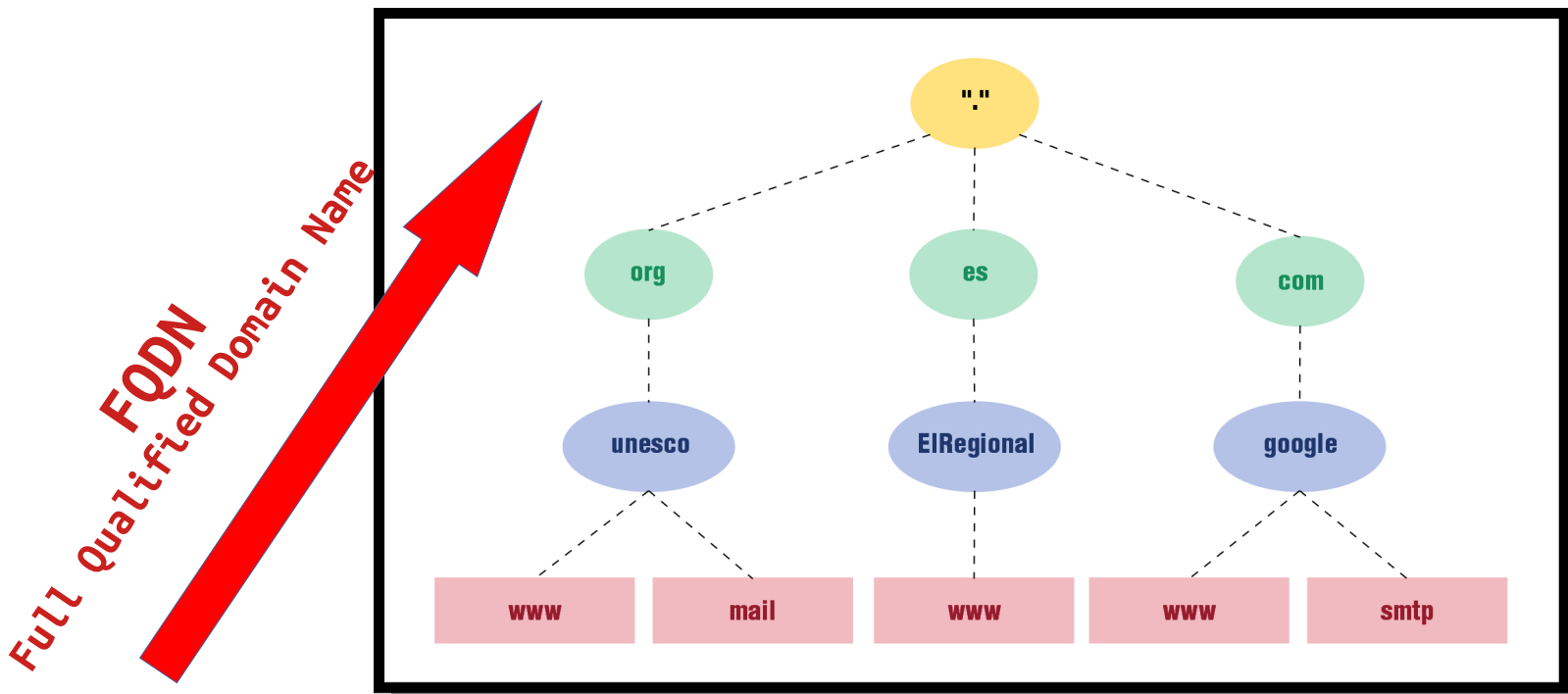
Orígenes del DNS



- Las direcciones IP son difíciles de recordar.
- Las tablas “hosts.txt” no son escalables.
- DNS = Domain Name Service, base de datos distribuida
- Nombres de dominio asignados por el ICANN (a nivel español, www.red.es – www.dominios.es)

Espacio de nombres de dominio

- Servicio de resolución de nombres: conversión nombre-IP, con tres componentes:
 - **Ciente DNS:** programa en ejecución en el ordenador. Realiza peticiones.
 - **Servidor DNS:** contesta a las peticiones de clientes.
 - **Zonas de autoridad.**



Dominios y niveles

- Dominios genéricos: gTLD
.com, .org, .info, .pro
- Dominios geográficos: ccTLD
.es, .uk, .us, .fr
- Dominio .arpa: usado para resolución inversa
Conocer el FQDN de una dirección IP
- Nombres reservados (no asignables)
.test, .example, .invalid, .localhost
- Delegación de dominio / Delegación de zona
Se transfiere la gestión de un dominio y descendientes

Whois: Base de datos distribuida que guarda los datos de dominios registrados

<http://www.iana.org/whois>

Funcionamiento de DNS

- Resolución directa

Dirección IP destino almacenada en caché

- Operación de solicitud DNS

Petición al servidor DNS - puerto 53

- Si el servidor no conoce la solución, remitirá la petición a un servidor de nivel superior:
 - **Recursiva:** proporciona respuesta completa
 - **Iterativa:** proporciona la mejor respuesta aproximada (la de un servidor intermedio).

- Resolución inversa

Preguntar el FQDN de una dirección IP

- Servidores públicos DNS de Google:

- **Primario:** 8.8.8.8 / **Secundario:** 8.8.4.4

Cientes DNS

- Comandos clientes
`nslookup`
- Fichero configuración

`/etc/resolv.conf`

- Resolver: componente del sistema en ejecución

Encargado de enviar solicitudes al servidor DNS

- Caché del resolver

Mantiene la información durante TTL (Time to Live)

En Windows: `IPCONFIG /DISPLAYDNS`

- Caché negativa (falta de resolución)

Evita repetir solicitudes de recursos inexistentes

Vaciar caché en Windows: `IPCONFIG /FLUSHDNS`

```
jose@Audax:~/Desktop$ nslookup www.google.es
Server:         127.0.0.53
Address:        127.0.0.53#53
```

```
Non-authoritative answer:
Name: www.google.es
Address: 216.58.214.163
Name: www.google.es
Address: 2a00:1450:4003:80a::2003
```

Base de datos del servicio (1/3)

- Registro de recursos

[Propietario] [TTL] [clase] [Tipo de Registro] [RDATA - Valor del dato]

- Tipos de registros

Registro	Función
SOA	Inicio de autoridad. Fija los parámetros de la zona.
NS	Servidor de Nombre. Nombre de un servidor autorizado para el dominio.
A	Dirección de anfitrión. Asigna a un nombre una dirección.
CNAME	Nombre canónico. Establece un alias para un nombre verdadero.
MX	Intercambio de correo. Especifica qué máquinas intercambian correo.
TXT	Texto arbitrario. Forma de añadir comentarios.
PTR	Puntero. Permite la conversión de una dirección a nombre.

Base de datos del servicio (2/3)

- Registro SOA – Zona de autoridad

```
ejemplo.es. IN SOA servidor.ejemplo.es. root.servidor.ejemplo.es. (
1998072701 ; Serial Number
86400      ; Refresh 24 hours - tiempo de transferencia a secundario
3600      ; Retry 1 hour - tiempo espera reintento del secundario
3600000; Expire 1000 hours - Caducidad
86400 ) ; Minimun 24 hours - validez de respuestas negativas
```

- Registros NS – Servidores de nombres autorizados

```
miempresa.es.      IN      NS      dns1.miempresa.es.
miempresa.es.      IN      NS      dns2. miempresa.es.
```

- Registros MX – Servidores de correo electrónico

```
miempresa.es. IN MX 10 correo.miempresa.es.
miempresa.es. IN MX 20 correo2.miempresa.es.
```

Prioridad (mayor cuanto más bajo sea el número.)

Base de datos del servicio (3/3)

- Registro A – Direcciones IP

```
ldap.miempresa.es.    IN      A      130.206.8.10
```

- Registros CNAME – alias apuntando a un mismo equipo

```
pop3      IN      CNAME  ldap
imap      IN      CNAME  ldap
smtp      IN      CNAME  ldap
```

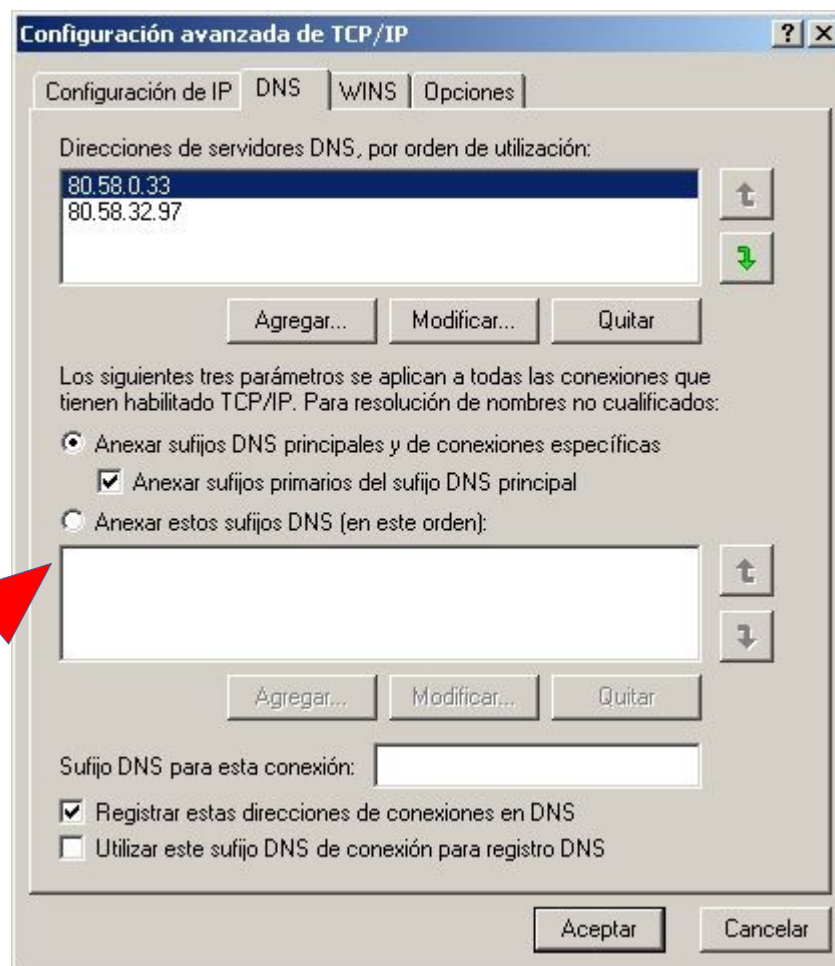
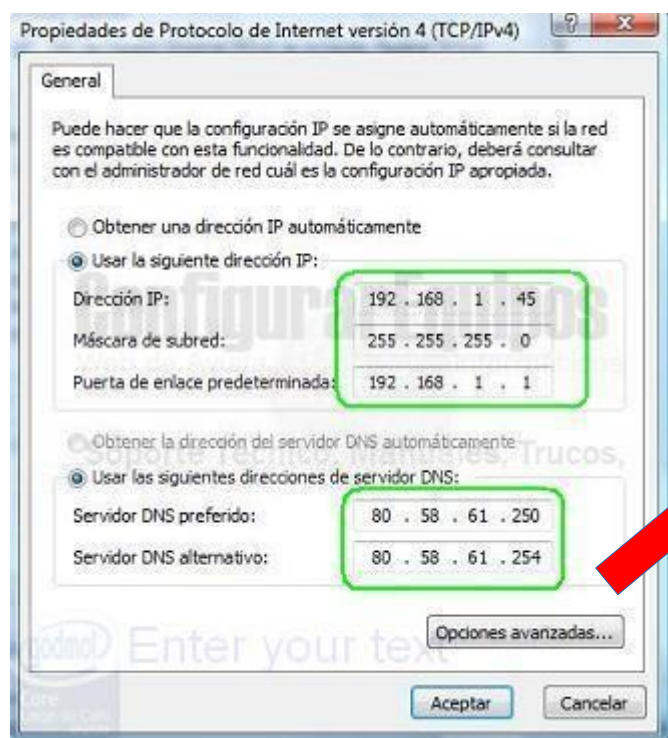
- Registros PTR – Resolución inversa

```
10.8.206.130.in-addr.arpa.  IN      PTR    ldap.miempresa.es.
```



`/etc/named.conf.local`

Ciente DNS en Windows



Cliente DNS en Linux

```
$ cat /etc/nsswitch.conf
passwd:          compat systemd
group:           compat systemd
shadow:         compat
gshadow:        files
hosts:           files mdns4_minimal [NOTFOUND=return] dns
networks:       files
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
netgroup:       nis
```

“files” indica que se usará `/etc/hosts`

“dns” indica que se usará `/etc/resolv.conf`

```
$ cat /etc/resolv.conf
nameserver 127.0.0.53
```

IP del servidor DNS del dominio

Servidor DNS en Linux

Paquete "Bind" – Ficheros de configuración

```
servidordns:/etc/bind$ ls -al
(..)
-rw-r--r--  1 root bind   463 mar 23  2018 named.conf
-rw-r--r--  1 root bind   490 mar 23  2018 named.conf.default-zones
-rw-r--r--  1 root bind   165 mar 23  2018 named.conf.local
-rw-r--r--  1 root bind   890 mar 23  2018 named.conf.options
(...)
```

Ejemplo para "miclase.local":

```
servidordns:/etc/bind$ cat named.conf.local
```

```
//Zona de búsqueda directa
zone "miclase.local"{
    type master;
    file "/etc/bind/db.miclase.local";
};
```

Servidor DNS en Linux

```
servidordns:/etc/bind$ cat db.miclase.local
```

```
; Fichero db.miclase.local
```

```
$TTL 1D
```

```
@          IN          SOA      miclase.local.   administrador.miclase.local. (
                                1           ; Serial
                                604800        ; Refresh
                                86400         ; Retry
                                2419200       ; Expire
                                10800 )      ; Negative Cache TTL (3 horas)
```

```
; Servidores DNS del dominio
```

```
          IN          NS      servidordns.miclase.local.
```

```
; Hosts
```

```
clientedns      IN          A      192.168.100.1
```

```
servidordns     IN          A      192.168.100.254
```

```
; Alias
```

```
ns1             IN          CNAME   servidordns
```

```
www             IN          CNAME   servidordns
```

```
ftp            IN          CNAME   servidordns
```

```
mail           IN          CNAME   clientedns
```

```
; Servidores de correo (MTA)
```

```
@             IN          MX      10      clientedns
```

Servidor DNS en Linux

Comprobar que la configuración es correcta:

```
servidordns:/etc/bind$ sudo named-checkconf /etc/bind/named.conf
servidordns:/etc/bind$ sudo named-checkzone miclase.local
/etc/bind/db.miclase.local
zone miclase.local/IN: loaded serial 1
OK
```

Chequear si funciona:
servidordns:/etc\$ nslookup mail.miclase.local
Non-authoritative answer:
mail.miclase.local (...)
Address: 192.168.100.1

Arrancar el servicio DNS:

```
servidordns:/etc/bind$ sudo systemctl restart bind9
```

```
jose@servidordns:/etc/bind$ sudo systemctl status bind9
```

```
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: en
   Active: active (running) since Sat 2018-10-20 01:29:03 CEST; 4s ago
     Docs: man:named(8)
   Process: 2662 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
```

Resolución inversa

```
servidordns:/etc/bind$ cat named.conf.local
```

```
(...)  
//Zona de búsqueda inversa  
zone "0.100.168.192.in-addr.arpa"{  
    type master;  
    file "/etc/bind/db.100.168.192";  
};
```

```
servidordns:/etc/bind$ cat db.100.168.192
```

```
;  
; BIND reverse data file for 192.168.100  
;  
$TTL      1D  
$ORIGIN 100.168.192.in-addr.arpa.  
@      IN      SOA     servidordns.miclase.local. root.miclase.local. (  
                                1242760444  
                                14400  
                                3600  
                                60480  
                                604800  
)  
      IN      NS      servidordns.miclase.local.  
254.100.168.192.in-addr.arpa.  IN  PTR servidordns.miclase.local.  
1.100.168.192.in-addr.arpa.  IN  PTR clientedns.miclase.local.
```

Comprobar:

```
servidordns$ host 192.168.100.254  
254.100.168.192.(...) pointer servidordns.
```

Fin



Dudas y preguntas: en el Aula Virtual.

Profesor: José A. Jiménez (jose.jimenezcastillo@educa.madrid.org)
IES Clara del Rey – Madrid

Realizado bajo licencia [Creative Commons Reconocimiento-NoComercial CC-BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/)

