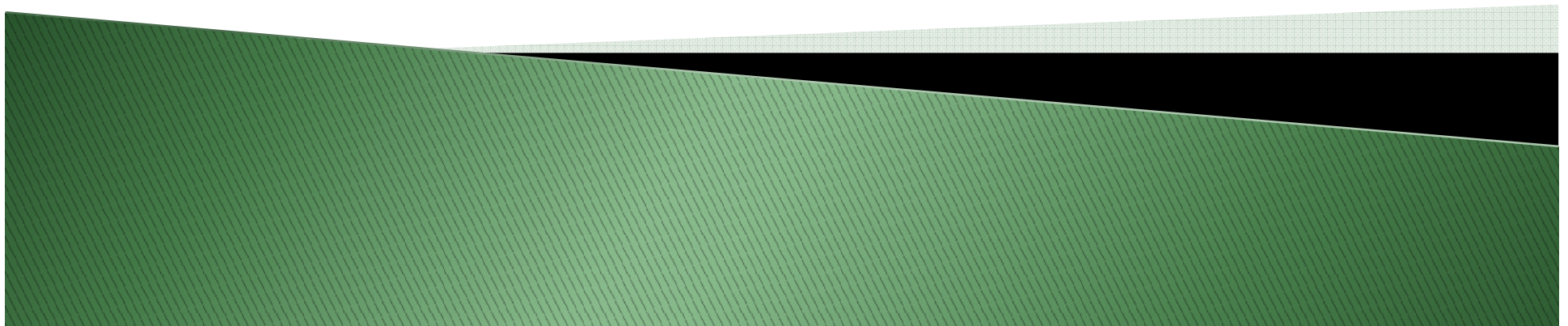


Unidad 3

Servicio de nombres de dominio

Despliegue de aplicaciones web



Índice

- ▶ Introducción.
- ▶ Características.
- ▶ Componentes y funcionamiento.
- ▶ Espacio de nombres de dominio.
- ▶ Servidores
 - Introducción.
 - Zonas.
 - Tipos.
 - Ejemplos de servidores DNS.

Índice

- ▶ Clientes DNS (*Resolvers*).
- ▶ Proceso de resolución.
- ▶ Registros de recursos.
- ▶ Resolución inversa.
- ▶ Otros.

Introducción

▶ Red TCP/IP

- Los protocolos utilizan direcciones numéricas (direcciones IP).

- Números de 32 bits (Ej.: 216.239.59.104).
- Sencillas de manejar para las máquinas.
- Complicado para los humanos.

- ## ▶ Para la personas es mucho mas sencillo utilizar y recordar nombres (Ej.: www.google.es).

Introducción



Introducción

- ▶ **Servicios de resolución de nombres**
 - Asociar nombres sencillos con direcciones numéricas.
 - “Resolver” nombres.
- ▶ **DNS (*Domain Name System* o Sistema de Nombres de Dominio)**
 - El principal servicio de resolución de nombres usado en redes TCP/IP, y por lo tanto en Internet.
 - Modelo cliente/servidor.

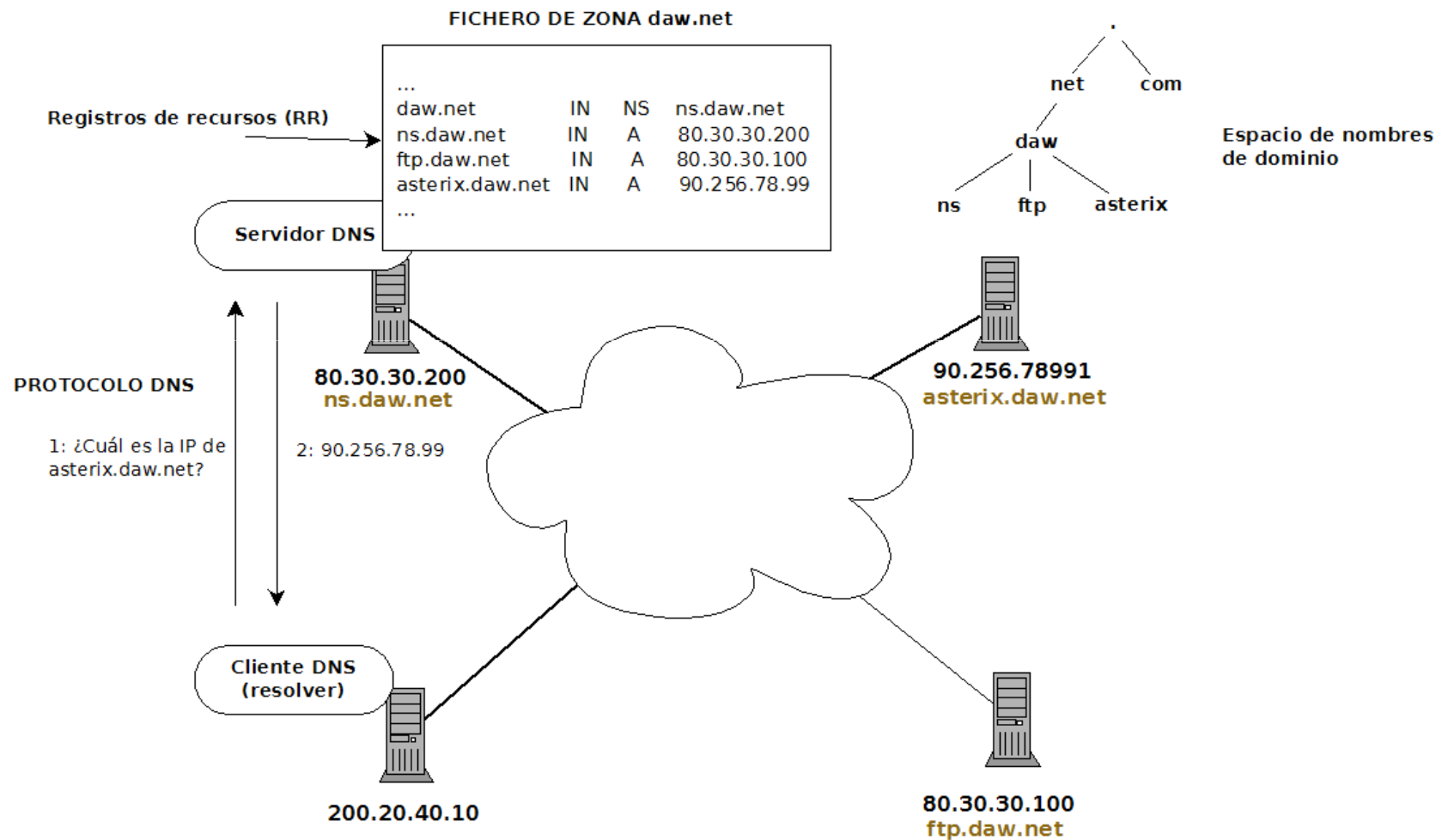
Características

- ▶ Servicio de almacenamiento y consulta de información.
- ▶ Utilidad
 - Resolución directa
 - ¿Cuál es la IP de www.daw.net?
 - Resolución inversa
 - ¿Cuál es el nombre asociado a la IP 100.200.30.45?
 - Resolución de servidores de correo.
 - Otros propósitos: balanceo de carga, claves públicas, ...

Componentes y funcionamiento

- ▶ El servicio DNS define los siguientes componentes
 - **Espacio de nombres de dominio** (*domain name space*).
 - **Base de datos distribuida** que almacenan los **servidores de nombres** (base de datos DNS) -> almacena **registros de recursos (RR)** organizados en **zonas**.
 - **Servidores de nombres** (*name servers*).
 - **Cientes DNS** (*resolvers*).
 - **Protocolo DNS**.

Componentes y funcionamiento



Componentes y funcionamiento

- ▶ Los clientes DNS (resolver) preguntan a los servidores de nombres.
- ▶ Los servidores de nombres se comunican entre sí:
 - Pueden realizar preguntas a otros servidores de nombres cuando no tienen la información por la que les han preguntado.
 - Pueden intercambiar información sobre sus zonas (transferencias de zona).
- ▶ Vídeo
 - ▶ <http://www.youtube.com/embed/dIGxJCqLJIY>

Práctica

► Práctica 3.1

- Funcionamiento del servicio DNS.
- Herramientas de consulta a servidores DNS
 - nslookup
 - dig

```
C:\Users\alumno>nslookup www.google.es
Servidor:  google-public-dns-a.google.com
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:   www-cctld.l.google.com
Addresses: 173.194.34.247
           173.194.34.248
Aliases:  www.google.es
```

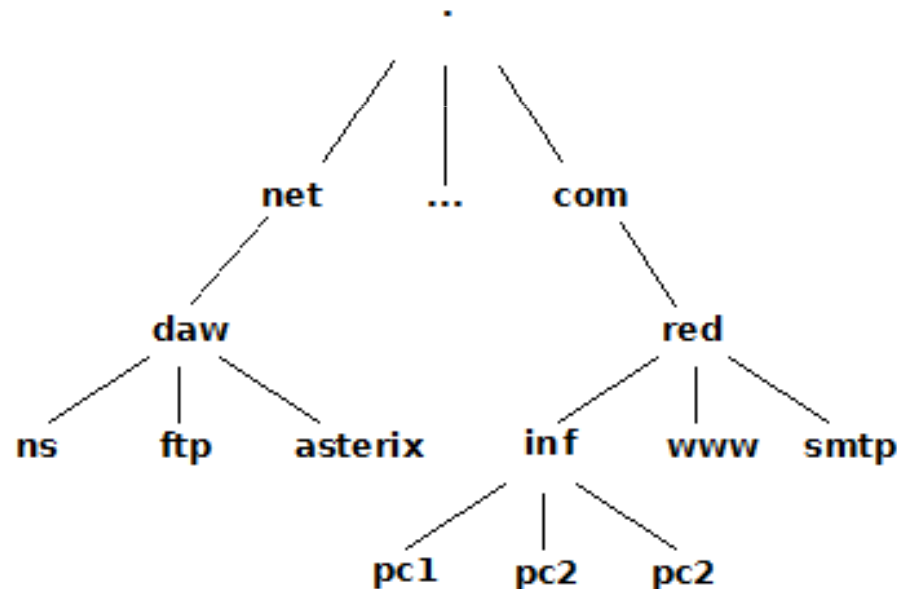
Espacio de nombres de dominio

► Nombre de dominio

- Una o varias cadenas de caracteres separadas por puntos.
- Ejemplos:
 - pc.daw.net.
 - com.
 - google.com.
 - ...

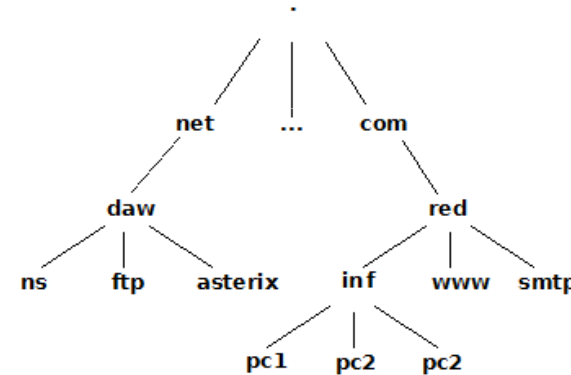
Espacio de nombres de dominio

- ▶ Conjunto de nombres → Espacio de nombres de dominio.
 - Representación jerárquica en forma de árbol.



Espacio de nombres de dominio

- ▶ Dominio raíz -> “.”
- ▶ Dominios y subdominios.
- ▶ Nombres absolutos vs. Nombre relativos
 - Nombres relativos
 - www, ftp.daw, ...
 - Nombres absolutos
 - ftp.daw.net., asterix.daw.net, daw.net., ...
 - Nombres completos (FQDN, *Fully Qualified Domain Names*).



Espacio de nombres de dominio

► Importante

- Dominio raíz y la ICANN.
- Dominios TLD y los operadores de registro.
- Delegación.
- Registro de dominios. Agentes registradores.
- Registrar un nombre de dominio en Internet.

Servidores

Introducción

- ▶ **Servidor de nombre = Servidor DNS**
 - Almacenan información sobre nombres de dominio (una parte de la base de datos DNS) –> **Zonas**.
 - Responden a las preguntas de:
 - Clientes DNS (*resolvers*)
 - Otros servidores DNS.
- ▶ **Puertos**
 - 53/TCP .
 - 53/UDP.

Servidores

Zonas

- ▶ Parte contigua del espacio de nombres de dominio.
 - Ejemplo: Fichero de zona del dominio daw.org almacenado en un servidor DNS (192.168.1.100)

```
...
daw.org      IN      NS      ns.daw.org
ns.daw.org   IN      A       192.168.1.100
www.daw.org  IN      A       192.168.1.200
smtp.daw.org IN      A       192.168.1.220
ftp.daw.org  IN      CNAME   www.daw.org
zipi.daw.org IN      CNAME   smtp.daw.org
...
```

Servidores

Zonas

► Ficheros de zona

- Contienen registros de recursos (RR, *Resource Records*).

- `smtp.daw.org IN A 192.168.1.220`
- `ftp.daw.org IN IN CNAME www.daw.org`

- Almacenados en ficheros de texto, tablas de una BBDD, servicios de directorio, ...

► Cuando un servidor de nombres contiene una zona se dice que es autorizado (*authoritative*) para esa zona.

Servidores

Zonas

► Problemas

- ¿Qué ocurre si un servidor autorizado para la zona “daw.org”, tiene un problema y deja de estar activo?
- ¿Qué pasará cuando los clientes DNS le preguntasen?

Servidores

Zonas

- ▶ Para ofrecer balanceo de carga, rapidez y una mayor tolerancia a fallos.
- ▶ Es posible almacenar una misma zona en varios servidores DNS.
 - Zonas maestras o primarias.
 - Zonas esclavas o secundarias.
 - Transferencias de zona.

Servidores

Tipos

- ▶ Según la función que realizan
 - Servidor maestro o primario.
 - Servidor esclavo o secundario
 - Transferencias de zona
 - Servidor *cache*.
 - Cache y TTL (*Time To Live*).
 - Servidor reenviador (*forwarding*).
 - Servidor solo autorizado (*authoritative*).

- ▶ **IMPORTANTE: Un mismo servidor DNS puede combinar varias de estas funciones simultáneamente.**

Servidores

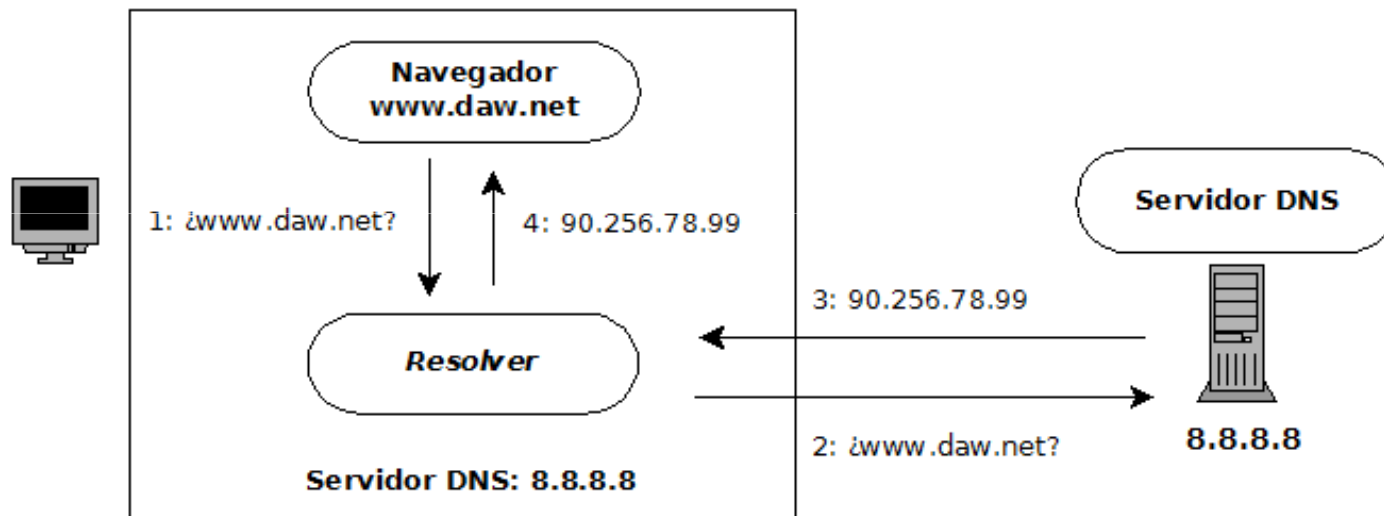
Ejemplos de servidores de nombres

- ▶ *BIND*
- ▶ *Servidor DNS de Microsoft*
- ▶ *PowerDNS*
- ▶ *NSD*
- ▶ *Simple DNS*
- ▶ *Cisco Network Registrar*
- ▶ *Dnsmasq*
- ▶ *...*

Clientes DNS (*Resolvers*)

- ▶ Preguntan a los servidores de nombres.
- ▶ Integrados en los sistemas operativos.
- ▶ Invocados por las aplicaciones (navegadores, clientes FTP, ...)
- ▶ Pueden utilizar una *cache* de respuestas.

Clientes DNS (*Resolvers*)



Proceso de resolución

► Funcionamiento básico

- El cliente DNS (*resolver*) consulta al servidor DNS.
- El servidor DNS
 - Si es autorizado (almacena la zona que contienen el nombre de dominio preguntado), responde.
 - Si no es autorizado (no contiene la información) pregunta a otros servidores DNS.

Proceso de resolución

- ▶ **Importante**
 - Consultas
 - Recursivas
 - Iterativas.
 - *Cache* y TTL.

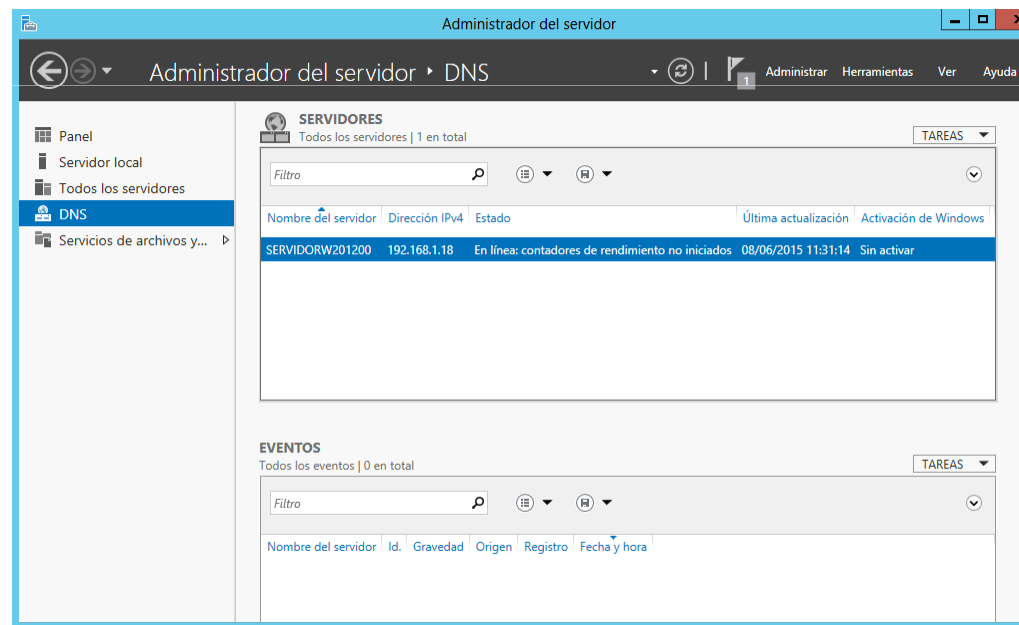
Registros de recursos

- ▶ Tipos que utilizamos en el curso:
 - SOA
 - NS
 - A
 - CNAME
 - MX
 - PTR
 - ...
- ▶ **Importante**
 - Delegación y registros pegamento (*glue records*).

Práctica

► Práctica 3.2 o Práctica 3.5

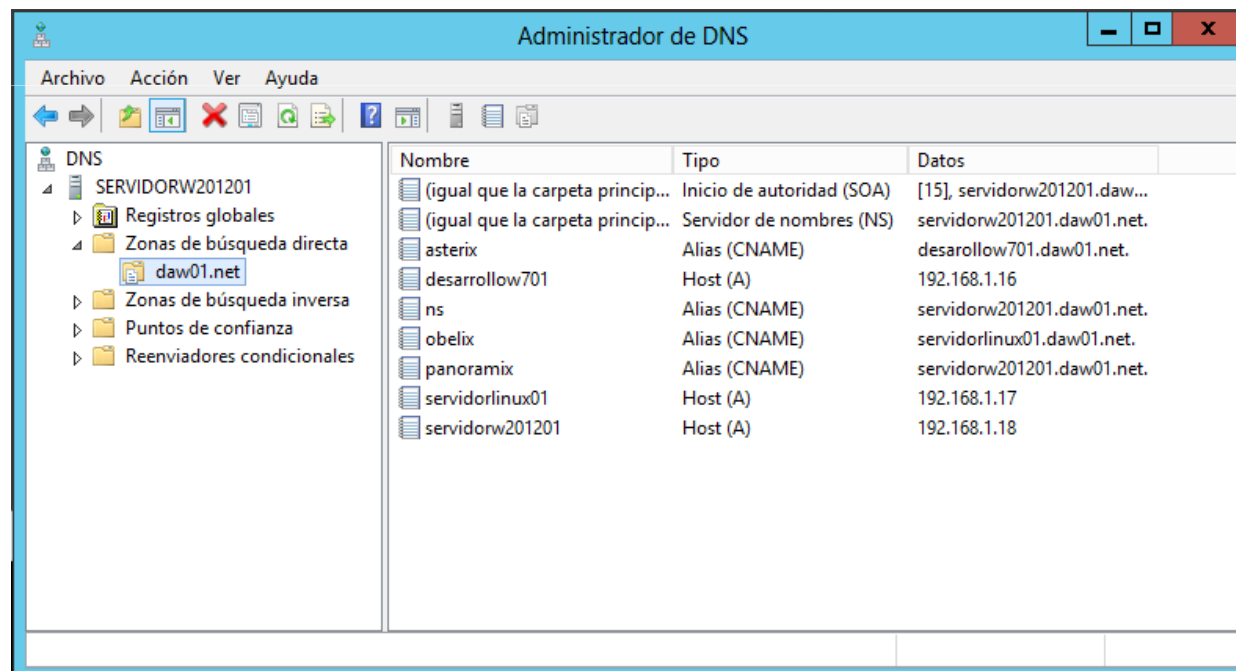
- Servidor DNS en *Microsoft Windows 2008/2012 Server*. Instalación y configuración del servidor DNS como solo *cache*.



Práctica

► Práctica 3.3 o Práctica 3.6

- Servidor DNS en *Microsoft Windows 2008/2012 Server*. Configuración como primario (maestro) para una zona de resolución directa.

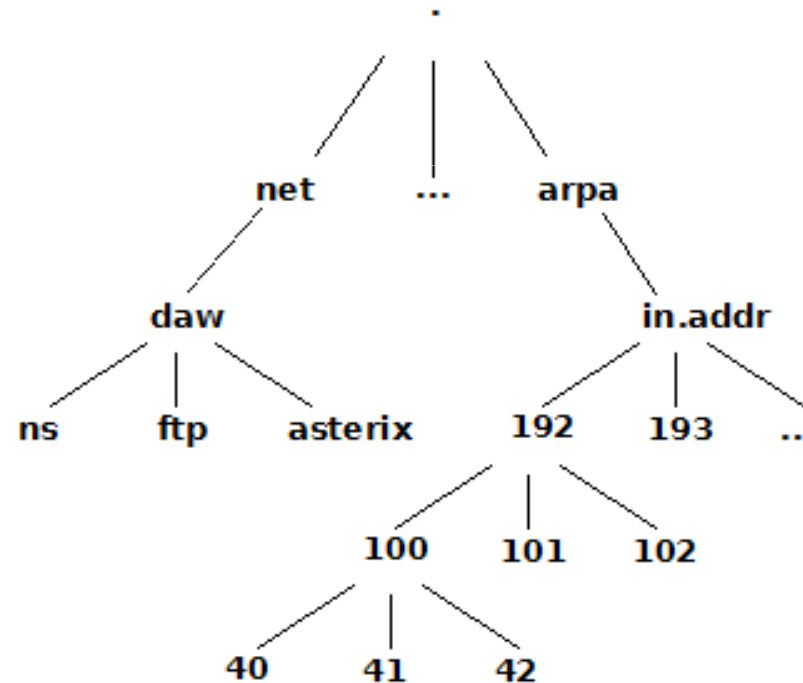


Resolución inversa

- ▶ ¿Cual es o cuales son los nombres de dominio asociados a la dirección IP 200.100.89.10?
- ▶ Motivos para preguntar por los nombres de dominio asociados a una IP
 - Resolver problemas de red.
 - Detectar spam en los servidores de correo
 - Seguir la traza de un ataque
 - ...

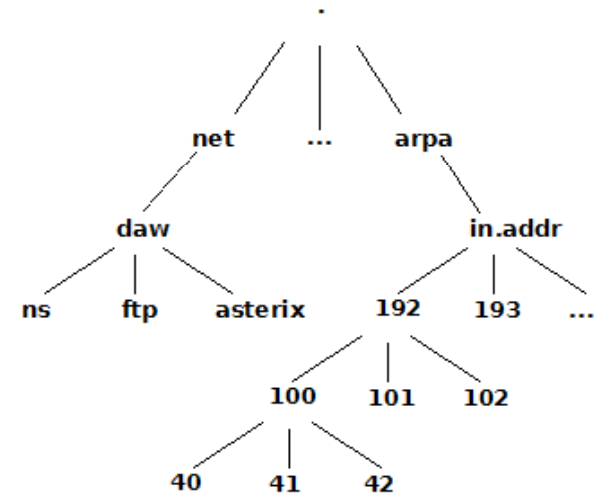
Resolución inversa

- ▶ Otro espacio de nombres de dominio para resoluciones DNS inversas.



Resolución inversa

- ▶ Las direcciones IP se tratan como nombres donde cada byte es un dominio que cuelga de los dominios
 - “in-addr.arpa”
 - Para direcciones IPv4
 - “ip6.arpa”
 - Para las direcciones IPv6.



Resolución inversa

► Zonas de resolución inversa

- Ejemplo: Fichero de zona de resolución inversa del dominio `1.100.192.in.addr.arpa.` que permite resolver consultas inversas sobre direcciones IP de la red `192.168.1.0/24`.

```
...
100.1.168.in.addr.arpa IN PTR ns.daw.org.
200.1.168.in.addr.arpa IN PTR www.daw.org.
200.1.168.in.addr.arpa IN PTR ftp.daw.org.
220.1.168.in.addr.arpa IN PTR smtp.daw.org.
220.1.168.in.addr.arpa IN PTR zipi.daw.org.
...
```

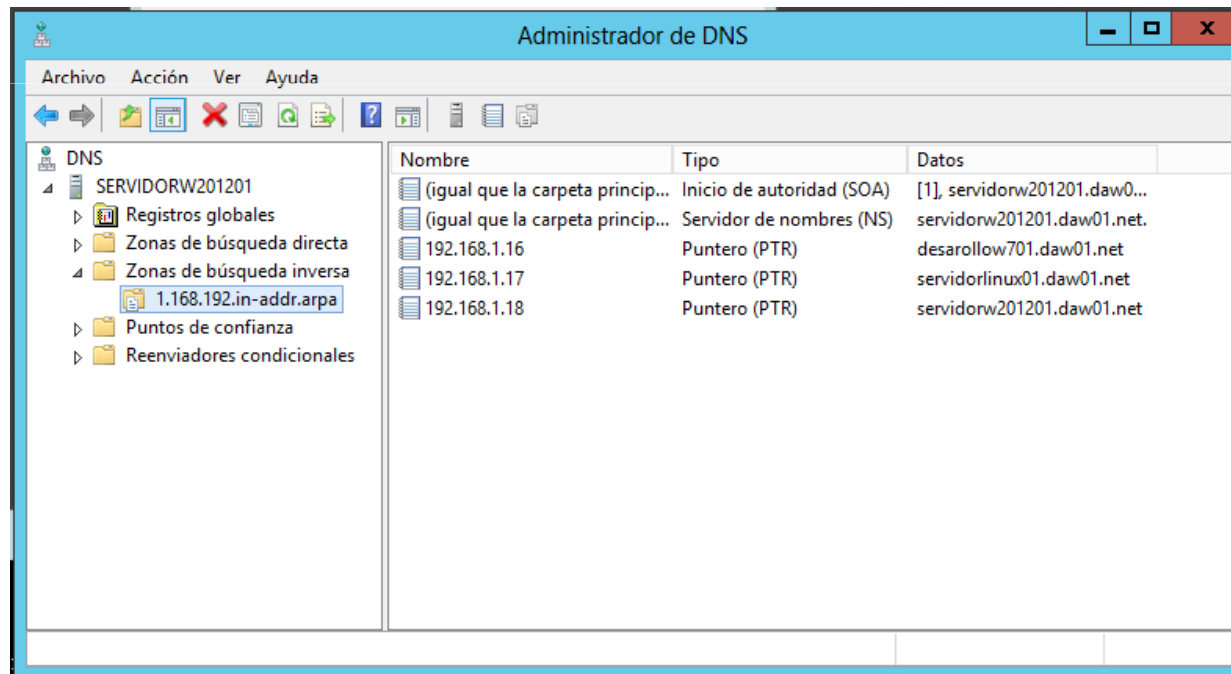
Resolución inversa

- ▶ Las zonas directas e inversas son independientes.
- ▶ Responsabilidad de los administradores que contengan información coherente y que no existan discrepancias.
- ▶ El proceso de resolución inversa es similar al de resolución directa.

Práctica

► Práctica 3.4 o Práctica 3.7

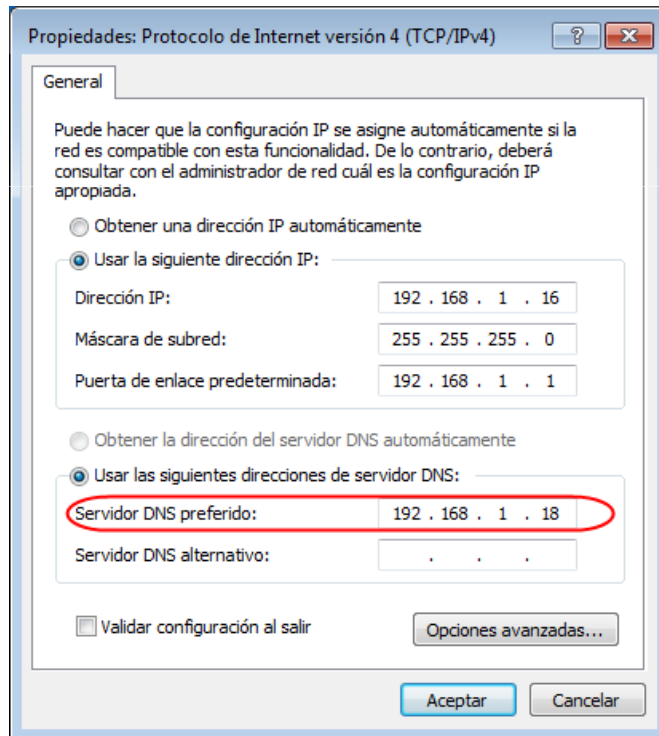
- Servidor DNS en *Microsoft Windows 2008/2012 Server*. Configuración como primario (maestro) para una zona de resolución inversa.



Práctica

► Práctica 3.8

- Clientes DNS en las otras máquinas.



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.17
    netmask 255.255.255.0
    gateway 192.168.1.1
    dns-nameservers 192.168.1.18
    dns-search daw01.net
```

Otros

► Importante

- Transferencias de zona.
 - Completas.
 - Incrementales.
- DNS Dinámico (*Dynamic* DNS)
 - Actualizaciones manuales.
 - Actualizaciones DNS Dinámicas.
 - DNS Dinámico en Internet.
- Protocolo DNS.
- *Whois*.

Bibliografía

- ▶ Servicios de Red e Internet. Álvaro García Sánchez, Luis Enamorado Sarmiento, Javier Sanz Rodríguez. Editorial Garceta.
- ▶ <http://www.wikipedia.org>