

---

**SMIX M07**

**UF1: DNS**

**EDUARD LARA**

# INDICE

---

1. Servicio DNS
2. DNS en Windows y Linux
3. Jerarquía de dominios en DNS
4. Dominio y Zona DNS
5. Servidores DNS
6. Consulta recursiva
7. Consulta iterativa

# 1. SERVICIO DNS

---

- ❖ El **Domain Name System (DNS)** es una base de datos distribuida y jerárquica que gestiona y mantiene información asociada a nombres de dominio en redes como Internet.
- ❖ Su uso más común es la asignación de nombres de dominio a direcciones IP de los nodos de Internet y la localización de los servidores de correo electrónico de cada dominio.
- ❖ DNS permite traducir los nombres de dominio (campus.stucom.com) a sus respectivas direcciones IP (82.223.162.102)

# 1. SERVICIO DNS

---

- ❖ Cuando queramos acceder a una máquina (Web, Ftp, Telnet, ...) en vez de recordar su @ IP, basta recordar el nombre del servidor:

`ftp ftp.smbserver.com → ftp 178.98.56.23`

`http://www.elmundo.es → http://132.56.23.22`

- ❖ DNS permite recordar fácilmente los nombres de todos los servidores conectados a Internet.
- ❖ El nombre es más fiable. La dirección numérica podría cambiar por muchas razones, pero no el nombre que identifica el servidor.

# 1. HISTORIA DNS

---

- ❖ En un inicio, SRI (ahora SRI International) alojaba un archivo llamado *HOSTS* que contenía todos los nombres de dominio conocidos (la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts).
- ❖ El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo *HOSTS* no resultara práctico.
- ❖ En 1983 apareció el primer sistema DNS, el cual ha ido evolucionado hasta el DNS moderno.

# 1. CARACTERÍSTICAS BÁSICAS DNS

---

- ❖ Es una base de datos jerárquica que contiene asociaciones de nombres de dominios a @ IP.
- ❖ Está formada por un conjunto de servidores distribuidos por todo Internet, en lugar de mantenerla centralizada en un único servidor.
- ❖ Sigue el paradigma cliente/servidor con nivel de transporte TCP/UDP y puerto 53.
- ❖ Usa un resolvedor ("resolver") que permite realizar las consultas a la bbdd.
- ❖ Utiliza un protocolo para intercambiar información de nombres.

## 2. DNS EN WINDOWS

---

### C:\windows\system32\drivers\etc\hosts

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Éste es un ejemplo de archivo HOSTS usado por Microsoft TCP/IP para Windows.
#
# Este archivo contiene las asignaciones de las direcciones IP a los nombres de
# host. Cada entrada debe permanecer en una línea individual. La dirección IP
# debe ponerse en la primera columna, seguida del nombre de host correspondiente.
# La dirección IP y el nombre de host deben separarse con al menos un espacio.
#
# También pueden insertarse comentarios (como éste) en líneas individuales
# o a continuación del nombre de equipo indicándolos con el símbolo "#"
#
# Por ejemplo:
#
# 102.54.94.97    rhino.acme.com    # servidor origen
# 38.25.63.10    x.acme.com        # host cliente x
#
127.0.0.1       localhost
```

---

## 2. DNS EN LINUX

---

```
exemple# cat /etc/hosts
127.0.0.1    localhost
201.24.31.87  pc1.uu.vi.com pc1
201.24.31.105 pc2.uu.vi.com pc2
201.24.31.106 pc3.uu.vi.com pc3
```

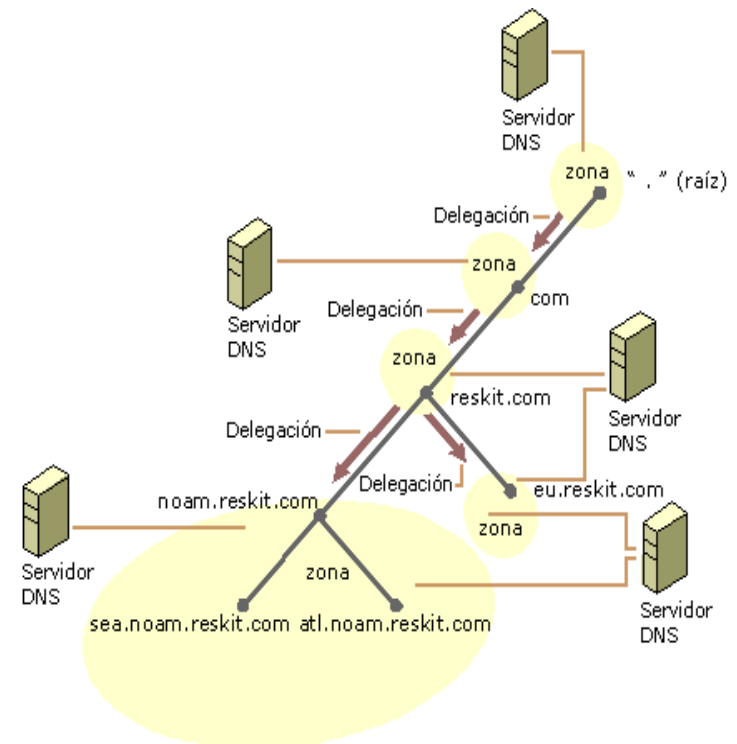
```
exemple# cat /etc/resolv.conf
domain uu.vi.com
nameserver 201.24.31.3
nameserver 201.24.31.4
```

- ❖ Las aplicaciones que acceden al sistema DNS consultan inicialmente el fichero `/etc/host` donde está la correspondencia nombre-@IP.
- ❖ Si no puede resolver el nombre, entonces intenta contactar con un servidor DNS.
- ❖ En el fichero `/etc/resolv.conf` se guarda la @ IP de los servidores DNS primario y secundario y el dominio local



### 3. JERARQUIA DE DOMINIOS DNS

- ❖ La jerarquía de DNS esta organizada en dominios o zonas.
- ❖ Un dominio es un mecanismo de identificación utilizado en Internet.
- ❖ Es una rama en un árbol invertido llamado **espacio de nombres de dominio**



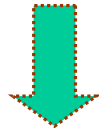
### 3. JERARQUIA DE DOMINIOS DNS

---

❖ Un nombre de dominio consiste en dos o más etiquetas, separadas por puntos (formato texto)

→ host....Subdominio1.Dominio.TLD

→ rogent.ac.upc.edu



#### Fully Qualified Domain Name:

Cuando el nombre incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo



#### Dominio de nivel superior

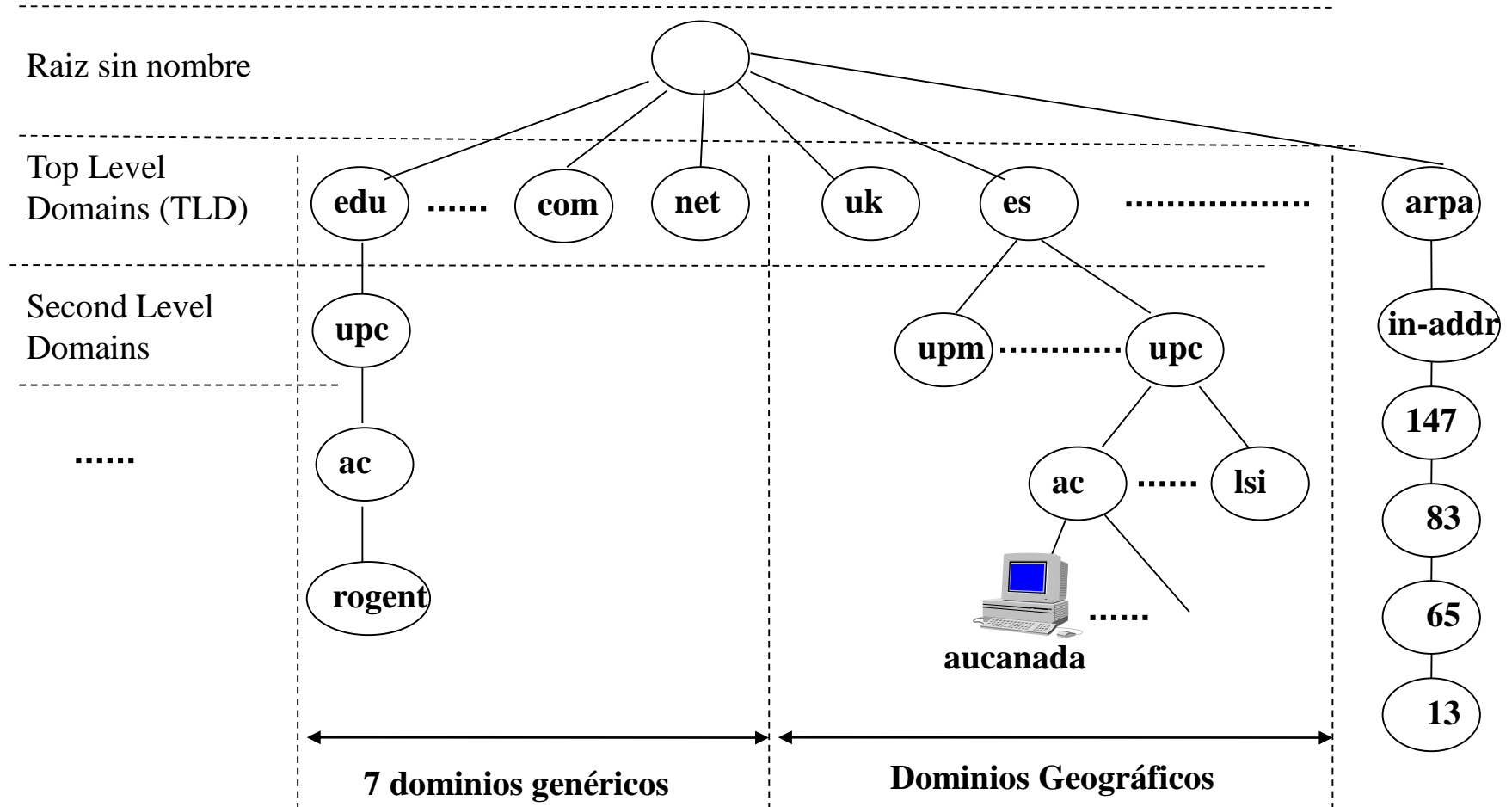
(*Top Level Domain*)  
Parte final de un dominio de Internet

### 3. JERARQUIA DE DOMINIOS DNS

---

- ❖ Cada etiqueta a la izquierda especifica una subdivisión o **subdominio**.
- ❖ El dominio y subdominio indican un conjunto de nombres que identifican a la organización:
  - "ac.upc" designa el departamento de Arquitectura de Computadores de la UPC.
- ❖ La parte más a la izquierda del dominio suele expresar el nombre de la máquina
- ❖ Las empresas deben **registrar** su nombre para que pase a ser su marca en Internet (problemas con marcas ya registradas)

# 3. JERARQUÍA DE DOMINIOS DNS



### 3. JERARQUÍA DE DOMINIOS DNS

---

#### Dominio raíz sin nombre

Los servidores raíz se encuentran al inicio de la jerarquía. Son los que responden cuando se busca resolver un dominio de 1º y 2º nivel.


Actualmente está formado por 13 servidores root-servers que tienen las direcciones de los TLD (top level domains):

a.root-server.net

b.root-server.net

...

m.root-server.net



Están distribuidos  
por todo el mundo.

# 3. JERARQUÍA DE DOMINIOS DNS

---

## Top Level Domain (TLD)

La IANA clasifica los TLDs en 3 clases dominios:

1) 7 dominios genéricos:

.com → comercial	.int → org. Internacional
.mil → militar	.org → org. no gubernamental
.edu → educación	.gov → institución gubernamental
.net → centros soporte de red	

Propuesta (de CORE) para ampliar el número de dominios genéricos: .firm, .shop, .info, .web, .nom, .arts, .rec

---

# 3. JERARQUÍA DE DOMINIOS DNS

---

## Top Level Domain (TLD)

2) Dominios geográficos por países: .  
es, .fr, .uk, .it, ...

3) 1 dominio de infraestructura: .arpa. Permite la resolución inversa de direcciones. Cada servidor gestiona una rama que comienza con la etiqueta "in-addr" de la que cuelgan las direcciones en sentido numérico inverso: @IP 147.83.65.13 estaría como 13.65.83.147.in-addr.arpa.

# 3. JERARQUÍA DE DOMINIOS DNS

---

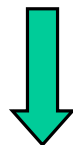
## Second Level Domain (SLD)

Cada uno de los TLD tiene un administrador (*registrar* en el argot DNS) que delega parte de su dominio en subdominios secundarios.

❖ Ejemplo: campus.stucom.com



Nombre de la máquina dentro del dominio de stucom



De com cuelga el dominio de nivel secundario stucom, cuya administración está delegada al centro stucom



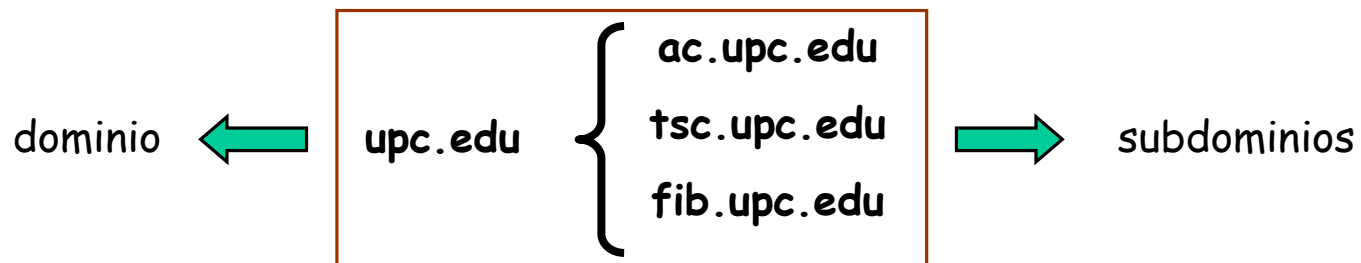
com es el TLD de comercial



## 4. DOMINIO Y ZONA DNS

---

- ❖ El **dominio** es un subárbol del espacio de nombres de dominio, es decir, un nodo con todos los nodos por debajo de él. El dominio contiene máquinas y otros dominios llamados subdominios.
- ❖ La **zona** es un archivo que contiene ciertos registros de la BBDD del espacio de nombres de dominio, que pueden identificar a un dominio o más y permiten atender las peticiones de los clientes.



## 4. ZONAS DE AUTORIDAD DNS

---

- ❖ Un servidor DNS almacena información acerca algunas partes del espacio de nombres del dominio
- ❖ Cada una de esas partes se llama **zona**. Se dice el servidor DNS tiene **autoridad sobre la zona**.
- ❖ Cada dominio o subdominio tiene una o más **zonas de autoridad** que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido.
- ❖ Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos no han sido delegados a otras zonas de autoridad.

## 4. DELEGACIÓN DE AUTORIDAD

---

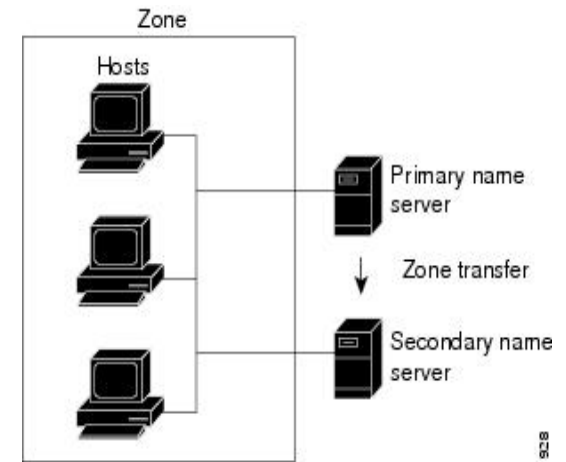
- ❖ La división de un dominio en subdominios no implica siempre la cesión de la autoridad sobre ellos.
- ❖ En principio un dominio puede mantener la autoridad sobre ellos. Pero también puede, si así lo decide delegar la autoridad de alguno/s de sus subdominios.
- ❖ Se define un **servidor de nombres de dominio DNS autoritario** para una zona como aquel que contiene los registros para dicha zona.
- ❖ Para ello se utilizan los registros de recursos SOA y NS.

# 5. SERVIDORES DNS

---

Los servidores de nombres se pueden clasificar en:

- Servidor primario (Primary name)
- Servidor secundario (Secondary name)
- Servidor caché (solamente)



**Transferencia de la zona:**

Es un proceso mediante el cual se obtiene información actualizada de la zona por medio de la red.

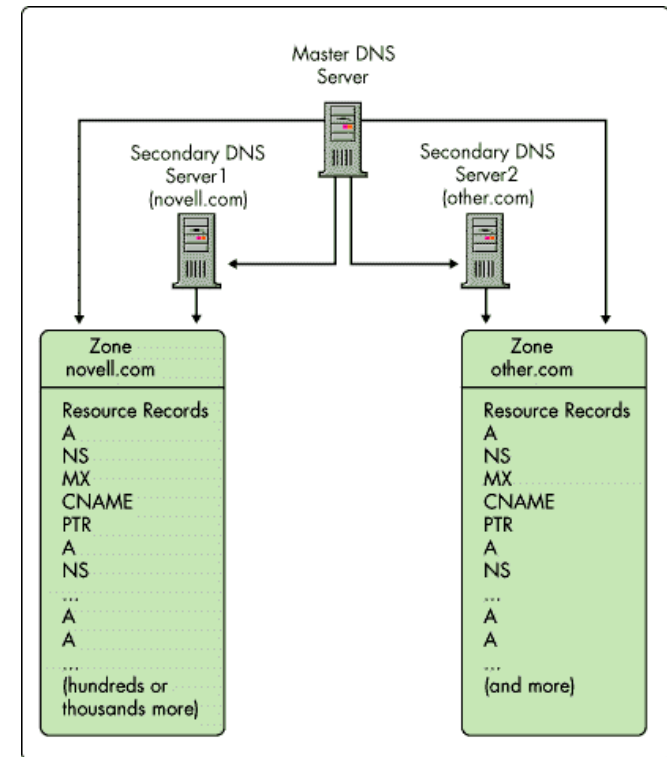
# 5. SERVIDORES DNS

❖ Cada administrador de sistemas de una zona (dominio o subdominio) es responsable de:

❖ Mantener un servidor primario (disk file), que tiene la información de una zona y la autoridad sobre ella.

❖ Mantener uno o varios servidores de DNS secundarios (backups) independientes del primario pero que obtienen la información a partir de él.

❖ Son servidores conocidos como "authority" del dominio.



## 5. SERVIDORES DNS

---

- ❖ La información nueva {@IP, nombre} se añade al primario. Los secundarios la obtendrán ya que hacen "querys" del primario cada 2/3 horas.
- ❖ En estos servidores han de estar los nombres de los hosts que cuelgan de su dominio y el nombre y dirección de los servidores primarios y secundarios de las autoridades de los subdominios que haya delegado.
- ❖ Si la información no está en el DNS de la zona, los servidores DNS deben conocer la @IP de los root-servers para acceder y obtenerla.

# 5. SERVIDORES DNS

---

Domain Name: ISMAILAX.COM

Registrar: GO DADDY SOFTWARE, INC.

Whois Server: whois.godaddy.com

Referral URL: <http://registrar.godaddy.com>

Name Server: NS45.DOMAINCONTROL.COM

Name Server: NS46.DOMAINCONTROL.COM

Status: clientDeleteProhibited

Status: clientRenewProhibited

Status: clientTransferProhibited

Status: clientUpdateProhibited

Updated Date: 17-apr-2007

Creation Date: 17-apr-2007

Expiration Date: 17-apr-2008

## 5. SERVIDORES DNS

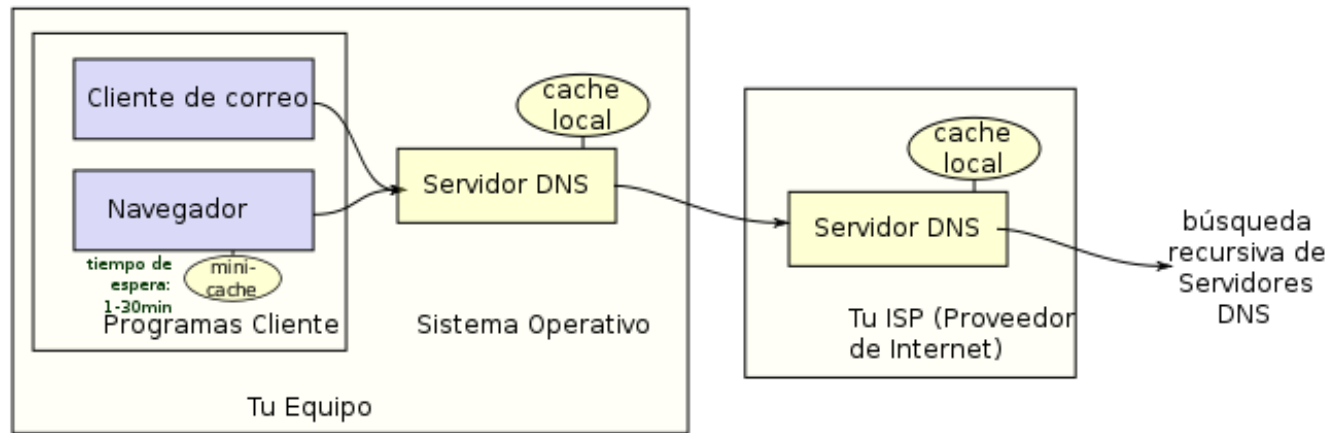
---

- ❖ Los servidores DNS (no los resolver de la aplicación) disponen de *caches* para resolver nombres que han mapeado recientemente
- ❖ Caching: Los servidores DNS guardan en su cache las direcciones IP solicitadas un cierto tiempo indicado por TTL (TTL típico 2 días). De esta manera, si el mismo host u otro vuelve a solicitar la resolución del mismo nombre, devolverá la dirección inmediatamente sin tener que hacer de nuevo la resolución.



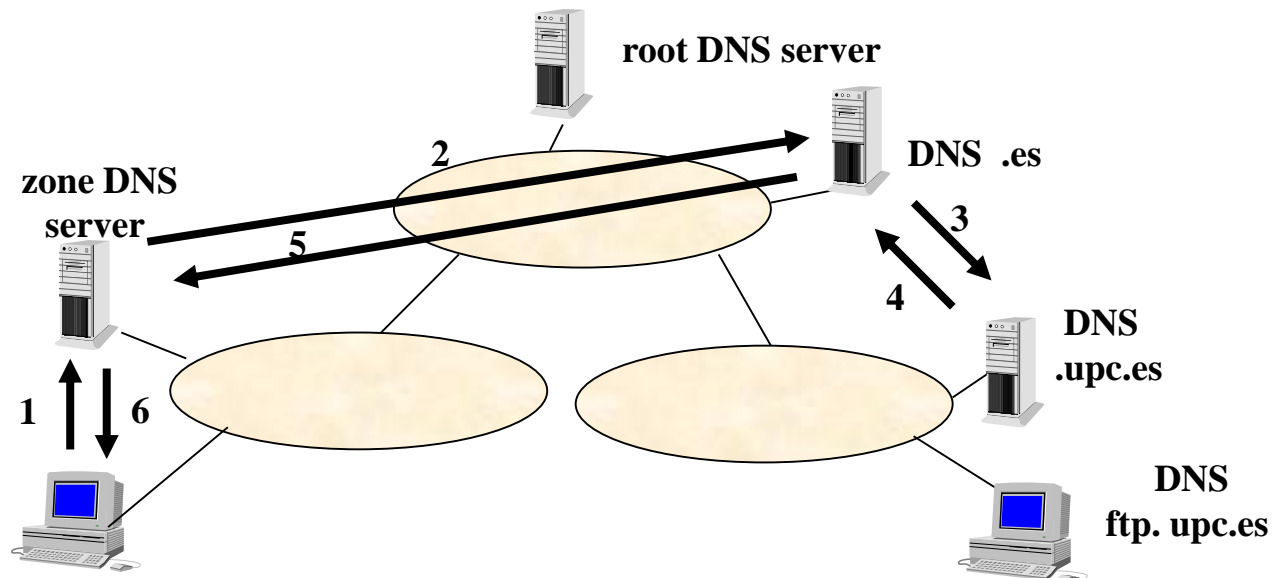
## 6. CONSULTA RECURSIVA

Se realiza una petición de resolución de nombres al servidor DNS local. Si el servidor no dispone de dicha información reenvía la petición al servidor de nombres con autoridad que la contiene. De forma recursiva se buscará la información y será devuelta al cliente.



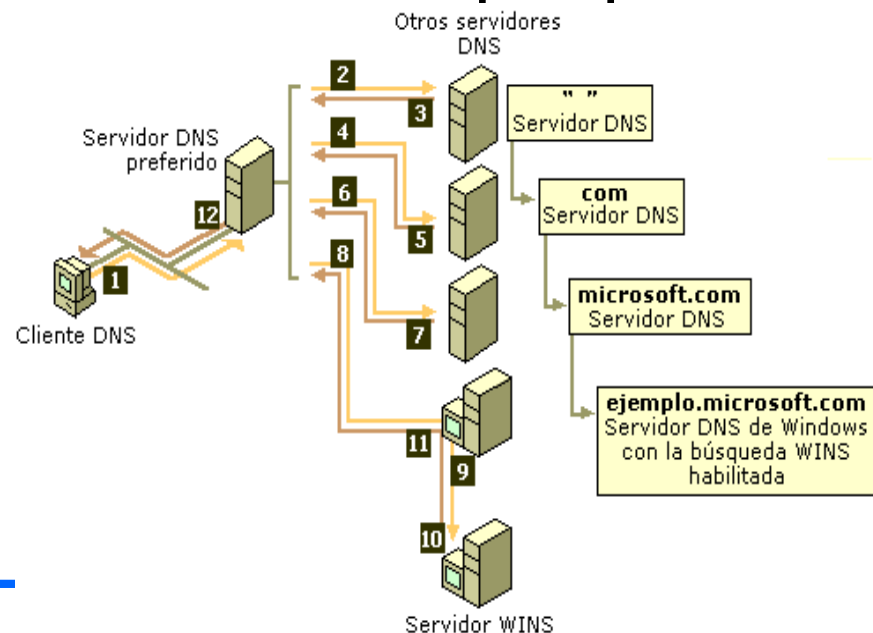
## 6. CONSULTA RECURSIVA

- (1) - Host pregunta por ftp.upc.es al servidor DNS de su zona (dominio)
- (2) - El servidor DNS de la zona pregunta al DNS server con dominio .es
- (3) - El servidor DNS .es pregunta al servidor DNS con dominio .upc.es
- (4) - El servidor DNS .upc.es le devuelve la @IP del servidor ftp.upc.es al dominio .es
- (5) (6) - Se devuelve la @IP del servidor ftp.upc.es al cliente.



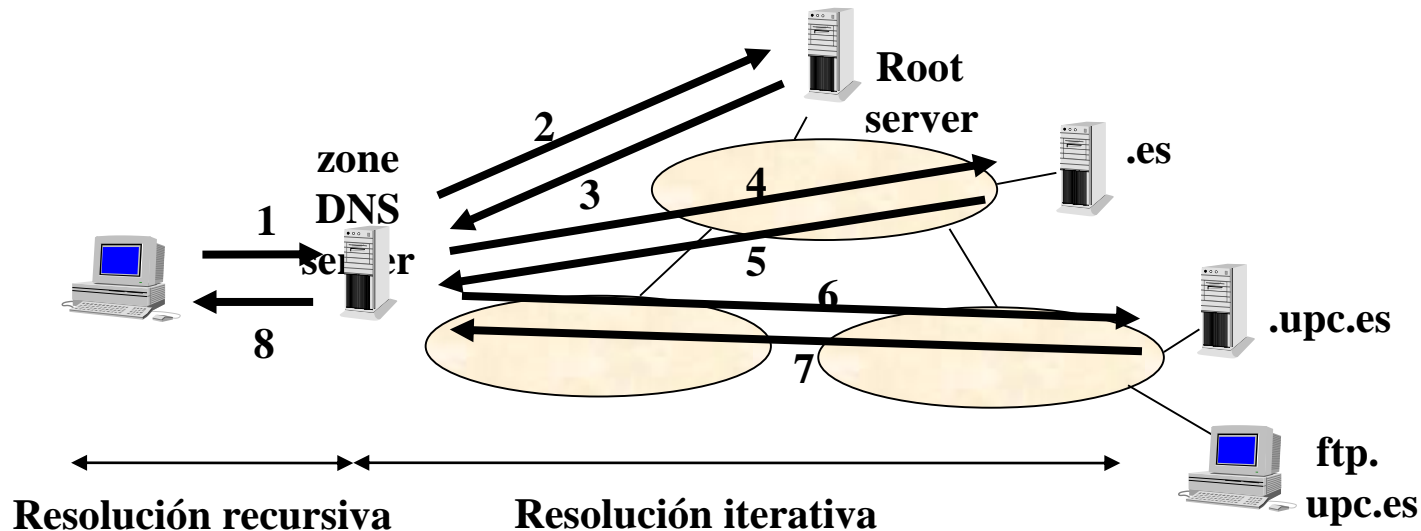
## 7. CONSULTA ITERATIVA (AKAMAI)

El servidor DNS local responde al cliente en función del contenido de su caché. Si no dispone de la información solicitada, entonces realiza una resolución iterativa: consulta iterativamente los servidores de los dominios hasta resolver la dirección buscada, comenzando siempre por un servidor raíz.

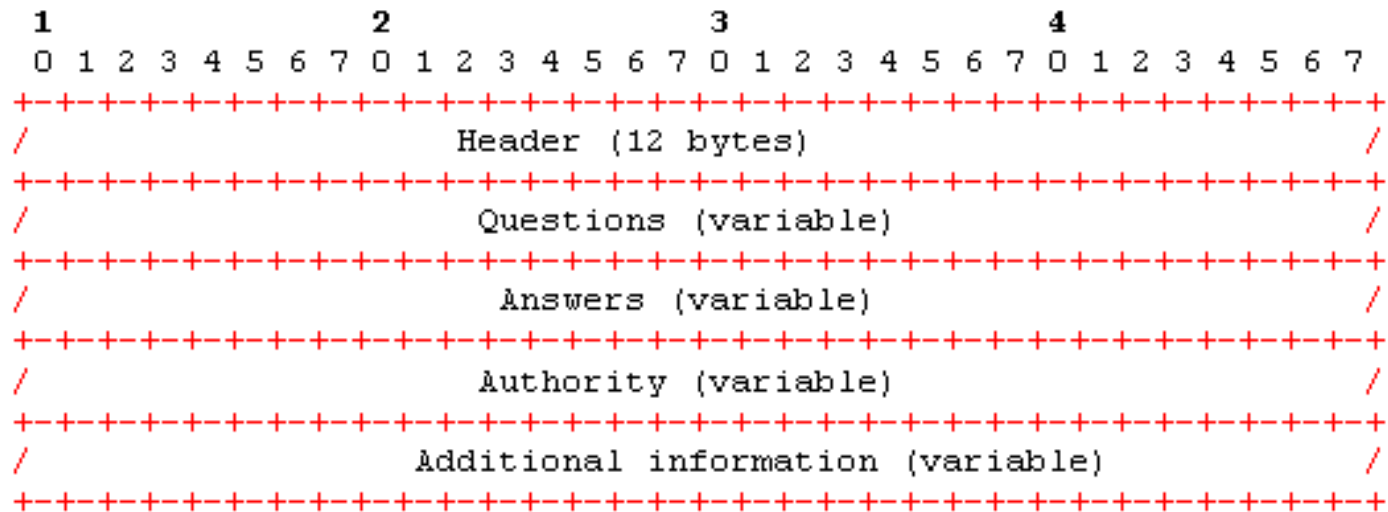


# 7. CONSULTA ITERATIVA (AKAMAI)

- (1) - Host pregunta por ftp.upc.es a su servidor DNS
- (2) - El server Zone DNS pregunta a su root server DNS
- (3) - El root server DNS le devuelve la @IP del servidor DNS con dominio .es
- (4) - Zone DNS pregunta al DNS .es.
- (5) - DNS .es devuelve la @IP de DNS .upc.es.
- (6) - Zone DNS pregunta a DNS .upc.es.
- (7) - DNS .upc.es devuelve @IP de server ftp.upc.es.
- (8) - Zone DNS devuelve la @IP del server al host.

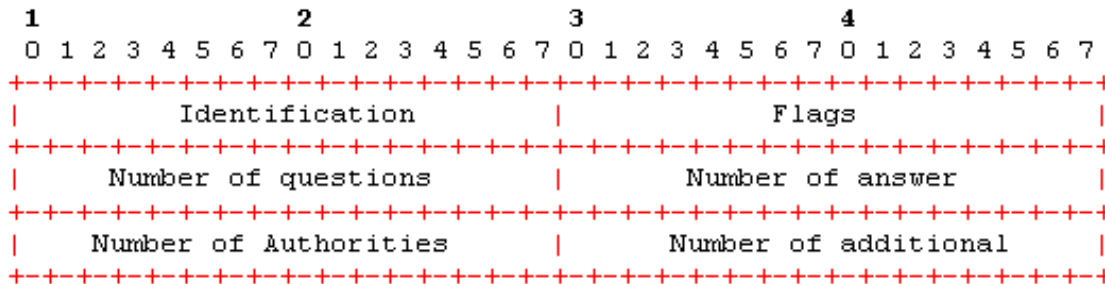


# FORMATO MENSAJE DNS



- ❖ Los campos Question, Answer, Authority y Additional son opcionales.
- ❖ Header: Especifica el tipo de mensaje.
- ❖ Question: Especifica lo que se quiere resolver.
- ❖ Answer: Especifica la respuesta.
- ❖ Authority: Especifica el nombre de la autoridad del dominio.
- ❖ Additional: Información adicional (típicamente, las @ IP de las autoridades del dominio).

# FORMATO CAMPO HEADER



- ❖ Identification: permite relacionar los mensajes de query (pregunta) y reply (respuesta). Es activado por el cliente y retornado por el servidor.
- ❖ 16-bit flags: Estan divididos en múltiples campos. Los flags más importantes son:
  - Flag QR (Query-Response): Si QR=0 mensaje de query (pregunta). Si QR=1 mensaje de reply (respuesta).
  - Flag AA (Authoritative Answer): Si AA=1 indica que ha respondido la autoridad del dominio. Si AA=0 indica que la respuesta estaba en la cache del servidor donde se ha hecho la pregunta. La respuesta no autoritativa si el DNS tiene que consultar otro DNS para obtener la respuesta. La respuesta puede ser autoritativa si el DNS tiene autoridad sobre el dominio consultado.
  - Flag RD (Recursion-Desired): Si la resolución será recursiva o iterativa.
- ❖ Number of questions: N° de entradas en la sección "Questions".
- ❖ Number of answer RRs: N° de entradas de la sección "Answers".
- ❖ Number of Authority RRs: N° de entradas de la sección "Authority".
- ❖ Number of additional RRs: N° de entradas de la sección "Additional".

# FORMATO CAMPO QUESTION

Contiene las consultas al servidor de nombres. Normalmente tiene una sola cuestión.

1								2								3								4							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
	6	r	o	g	e	n	t		2	a	c	3	u	p	c		3	e	d	u	0										
								Query name																							
Query type																Query class															

- ❖ Query name: Especifica el nombre que se quiere resolver (e.g. rogent.ac.upc.edu). Es un campo que contiene un contador + string: (e.g 8 rogent 2 ac ...)
- ❖ Query type: Especifica el tipo de pregunta. Hay hasta 20 valores diferentes.
  - Query type = 1 → Tipo A (Address) o resolución de @IP a partir del nombre.
  - Query type = 2 → Tipo NS (Name Server) o resolución de un name server
  - Query type = 12 → Tipo PTR (Pointer Record) o resolución inversa (conozco la @IP y quiero el nombre). Se da un nombre del tipo 7.40.45.180.in-addr.arpa
  - Query type = 13 → Tipo MX (Mail Exchange) para encaminar correo electrónico.
- ❖ Query class: Especifica el tipo de dirección que se quiere resolver. En el caso de referirse a una dirección de Internet vale 1.

# TIPOS REGISTROS DNS

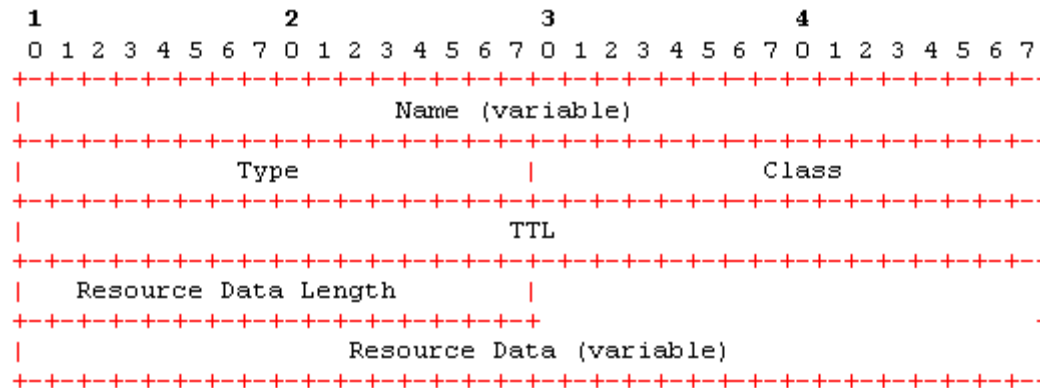
Nombre del recurso	Tipo de registro	Función
Inicio de autoridad	<b>SOA</b>	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	<b>NS</b>	Identifica servidores de nombres autorizados para una zona.
Dirección	<b>A</b>	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	<b>PTR</b>	Asocia una dirección IP a un nombre de dominio FQDN. Para las búsquedas inversas.
Registro de correo	<b>MX</b>	Indica máquinas encargadas de la entrega de correo en el dominio.
Nombre canónico	<b>CNAME</b>	Permite asignar uno o más nombres a una máquina. Alias.
Text	<b>TXT</b>	Almacena cualquier información.
Servicio	<b>SRV</b>	Ubicación de los servidores para un servicio.



# FORMATO CAMPOS ANSWER, AUTHORITY

---

Los campos *Answer*, *Authority* y *Additional* estan formados por secuencias de uno o más *Resource Records*. La siguiente figura muestra el formato de un RR.



- ❖ Los tres primeros campos (*Name*, *Type* y *Class*) tienen el mismo significado que en el campo *Question*.
- ❖ TTL (Time-to-live): Es el número de segundos que un RR puede permanecer en la cache del cliente (normalmente 2 días)
- ❖ Resource data length: la cantidad de bytes del "Resource Data"
- ❖ Resource data: Depende del campo "type". Si Type = 1 (Tipo A) es una @IP y por tanto tiene 4 bytes. Si Type = 2 (Tipo NS) es el nombre de la autoridad (resolución de un name server)

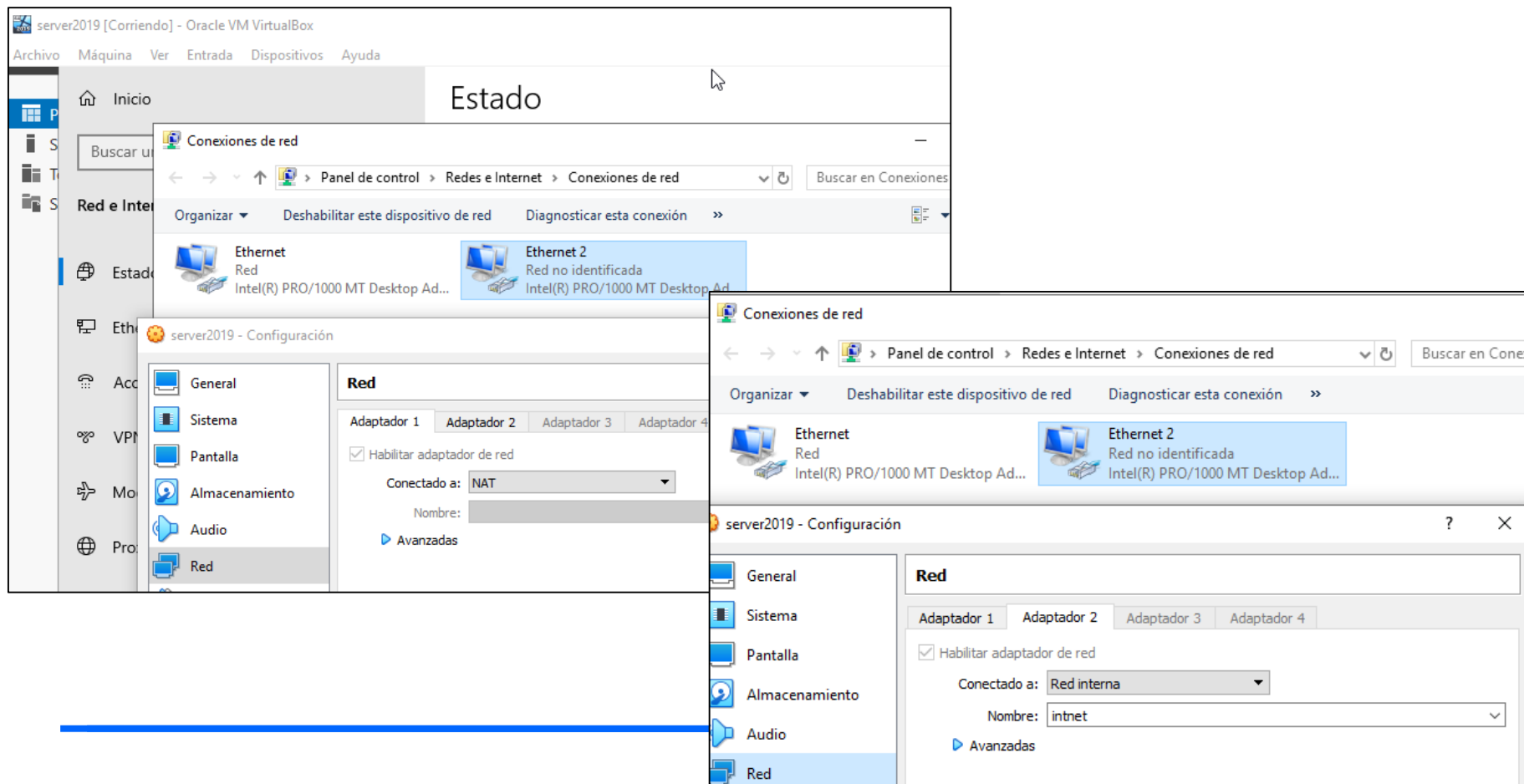
# GESTIÓN ASIGNACIÓN DOMINIOS

---

- ❖ La asignación de dominios es gestionada por la ICANN, entidad privada sin ánimo de lucro, que se encarga de dar tanto dominios genéricos como @IP.
  - ❖ Los dominios genéricos son registrados por compañías a las que ICANN da el derecho a que actúen como tales bajo ciertas restricciones (Accredited Registrars)
  - ❖ En España, el Ministerio de Fomento (servicio es-nic, <http://www.nic.es> ) gestionado por INECO (empresa pública), se encarga del registro y asignación del dominio .es
  - ❖ En España, se puede pedir dominios a Nominalia (<http://www.nominalia.com>) o <http://www.interdomain.es>
  - ❖ La información de los administradores de los TLD se pueden encontrar en <http://www.internic.net>. Internic tiene un listado de empresas que efectúan esta asignación. Internic es la autoridad que añade la información al DNS.
-

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 0.** Arranca una maquina virtual con Windows Server 2019 en VirtualBox y/o VMware. Debe tener dos interfaces: una NAT con conexión a Internet y la otra Red Interna, por donde actuara el servidor DNS.



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

**Paso 1.** Configura la interfaz de red 'Red Interna' del Server 2019 con la IP 192.168.1.1/24, puerta de enlace 192.168.1.1 y direccion DNS primario 127.0.0.1:

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 1 . 1

Máscara de subred: 255 . 255 . 255 . 0

Puerta de enlace predeterminada: . . . .

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 127 . 0 . 0 . 1

Servidor DNS alternativo: . . . .

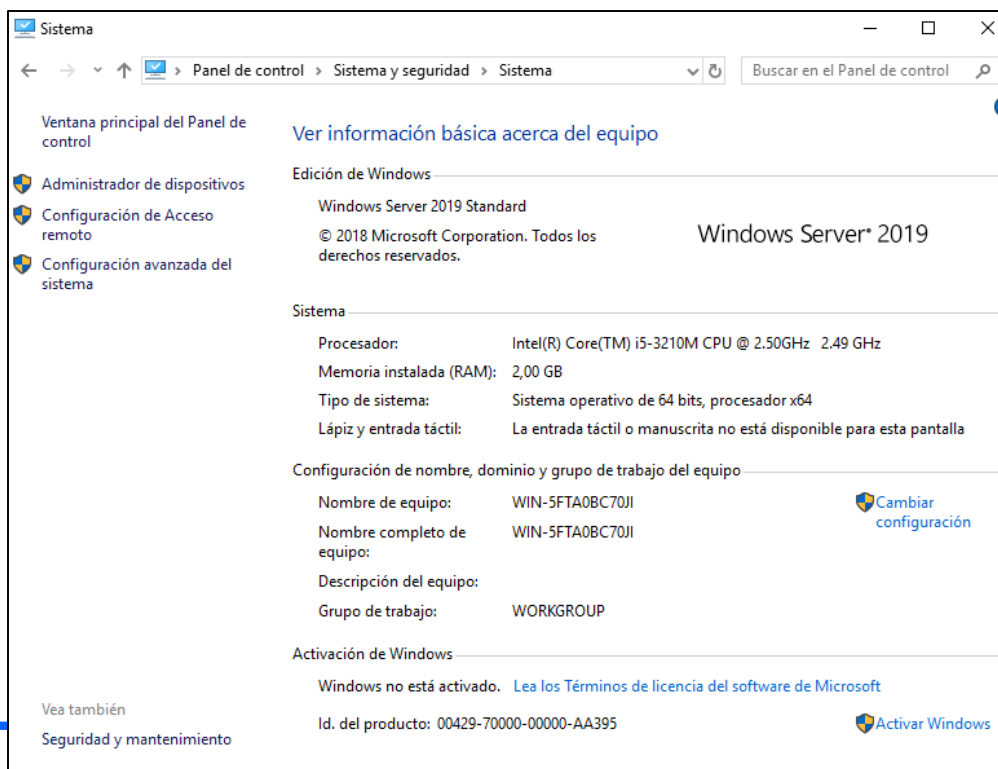
☐ Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

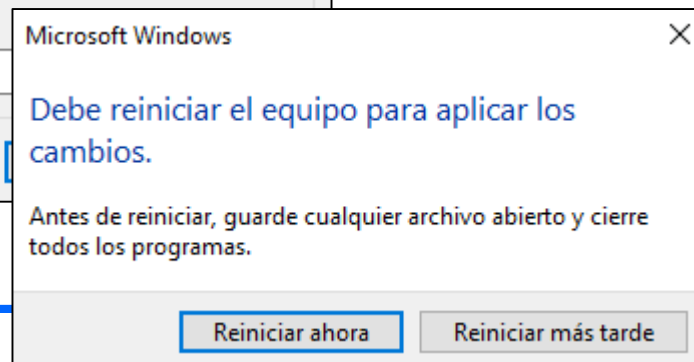
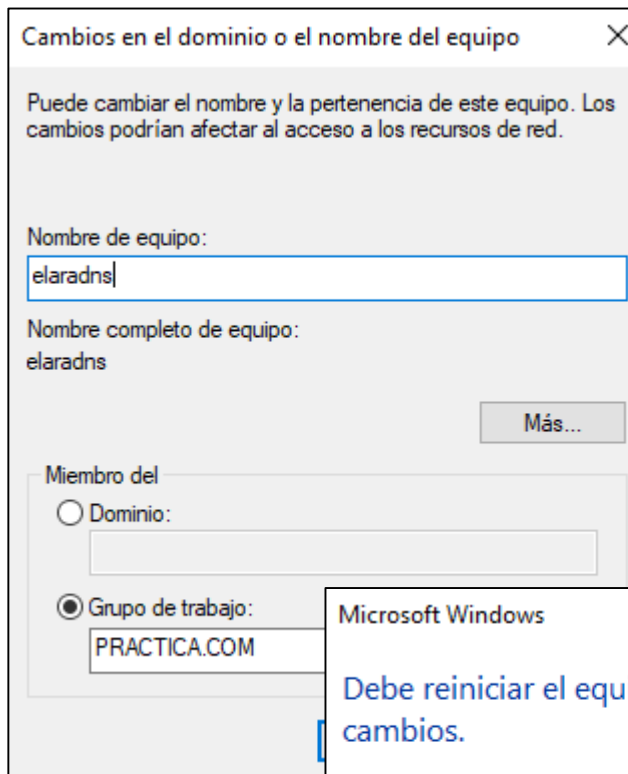
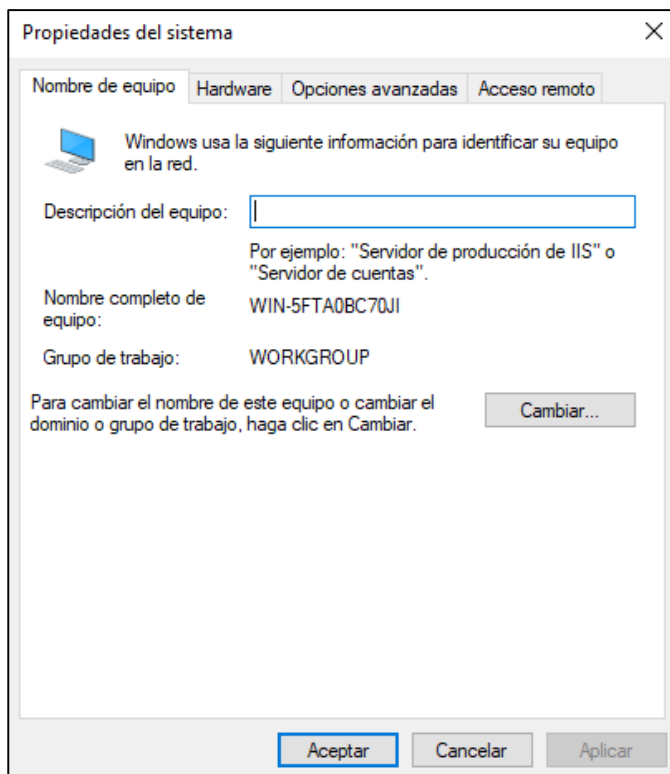
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 2.** Como no tenemos dominio todavía, ya que no está instalado el Active Directory, sumaremos el equipo Windows Server 2019 al grupo de trabajo a "practica.com" y también cambiaremos el nombre al equipo a **nombrealumnoDNS**. Ir a Panel de control/Sistema y seguridad/Sistema. Hacemos click en Cambiar configuración.



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 3.** En propiedades del Sistema hacemos click en el botón Cambiar y cambiamos el nombre del equipo y el grupo de trabajo:



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 4.** Reiniciamos el equipo y vemos que los cambios han tomado efecto:

Ver información básica acerca del equipo

---

Edición de Windows

Windows Server 2019 Standard

© 2018 Microsoft Corporation. Todos los derechos reservados.

Windows Server\* 2019

---

Sistema

Procesador: Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz 2.49 GHz

Memoria instalada (RAM): 2,00 GB

Tipo de sistema: Sistema operativo de 64 bits, procesador x64

Lápiz y entrada táctil: La entrada táctil o manuscrita no está disponible para esta pantalla

---


Configuración de nombre, dominio y grupo de trabajo del equipo

Nombre de equipo: elaradns

Nombre completo de equipo: elaradns

Descripción del equipo:

Grupo de trabajo: PRACTICA.COM


 Cambiar configuración

---

Activación de Windows

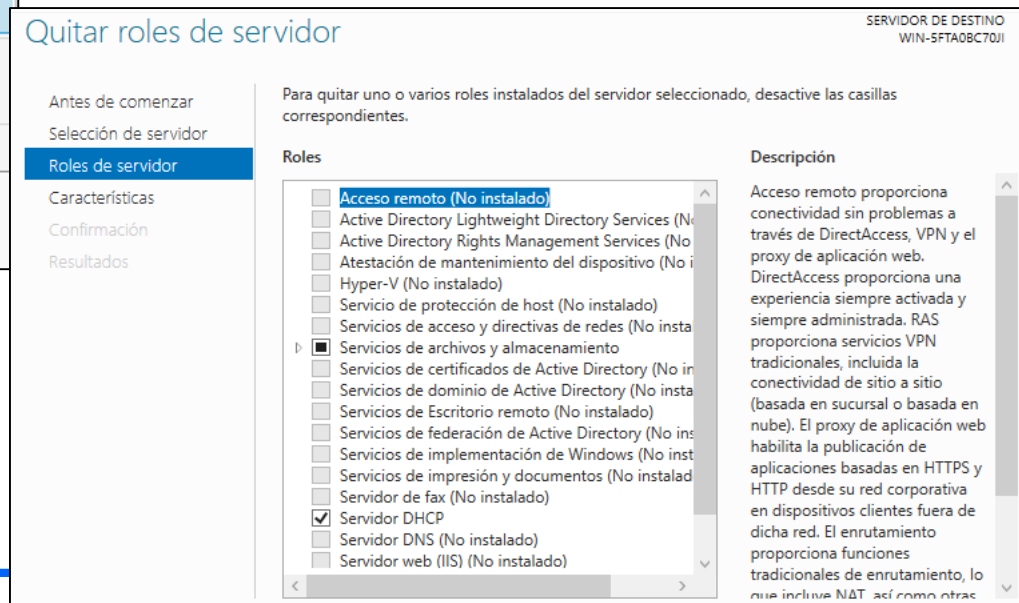
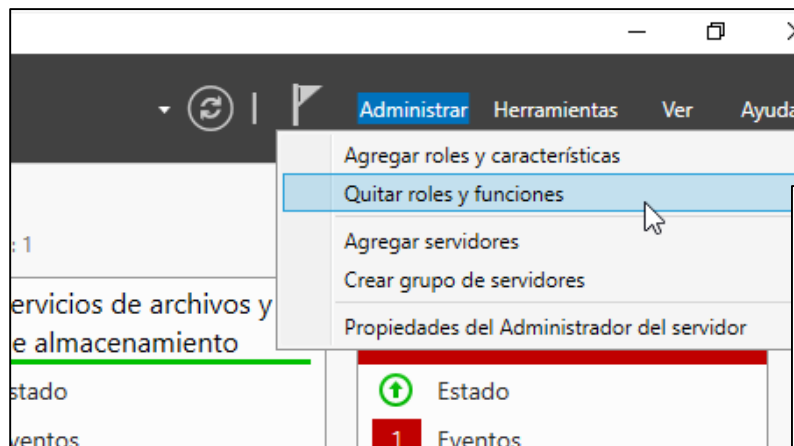
Windows no está activado. [Lea los Términos de licencia del software de Microsoft](#)

Id. del producto: 00429-70000-00000-AA395

 Activar Windows

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

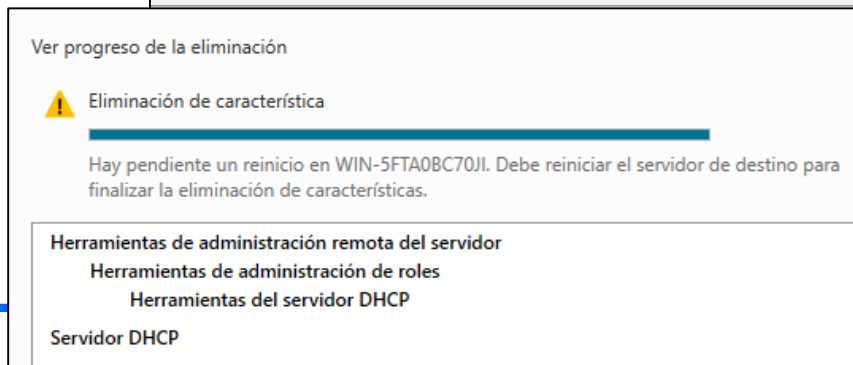
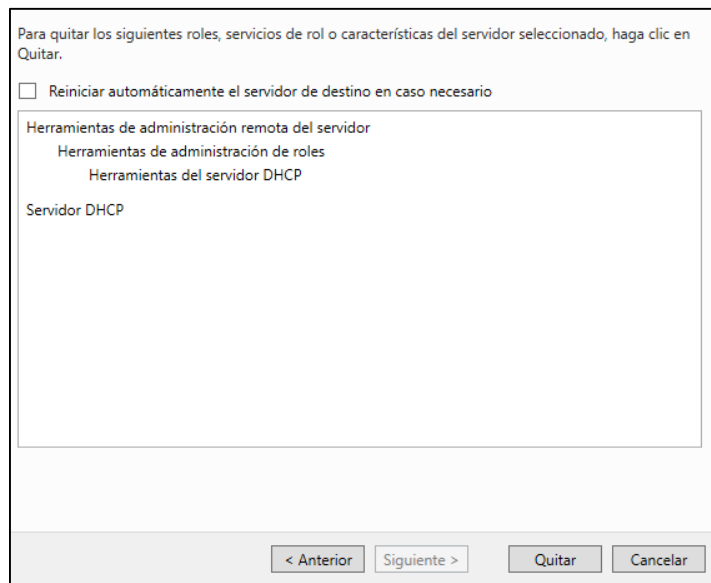
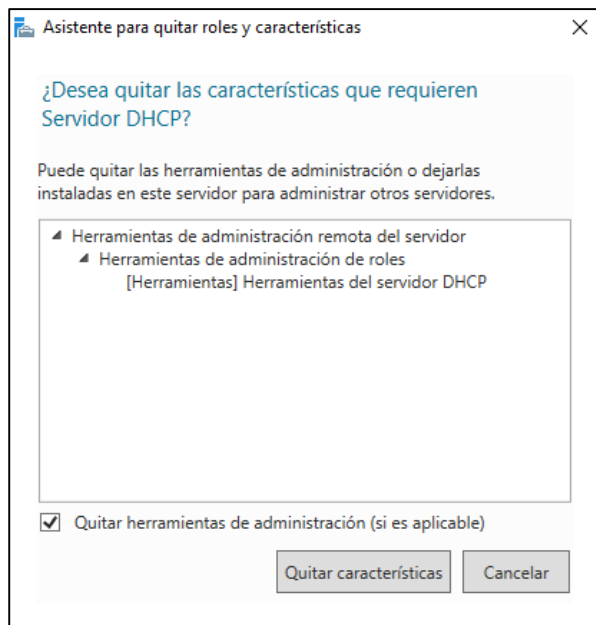
**Paso 5.** Abre la herramienta Administrador del servidor. Si hubiera algun otro servicio activado (por ejemplo DHCP), elimínalo del servidor. Desde el Administrador del servidor haz clic en Administrar y después en Quitar roles y funciones. Selecciona el servidor local y en la página Quitar roles de servidor, desmarque la casilla de Servidor DHCP.





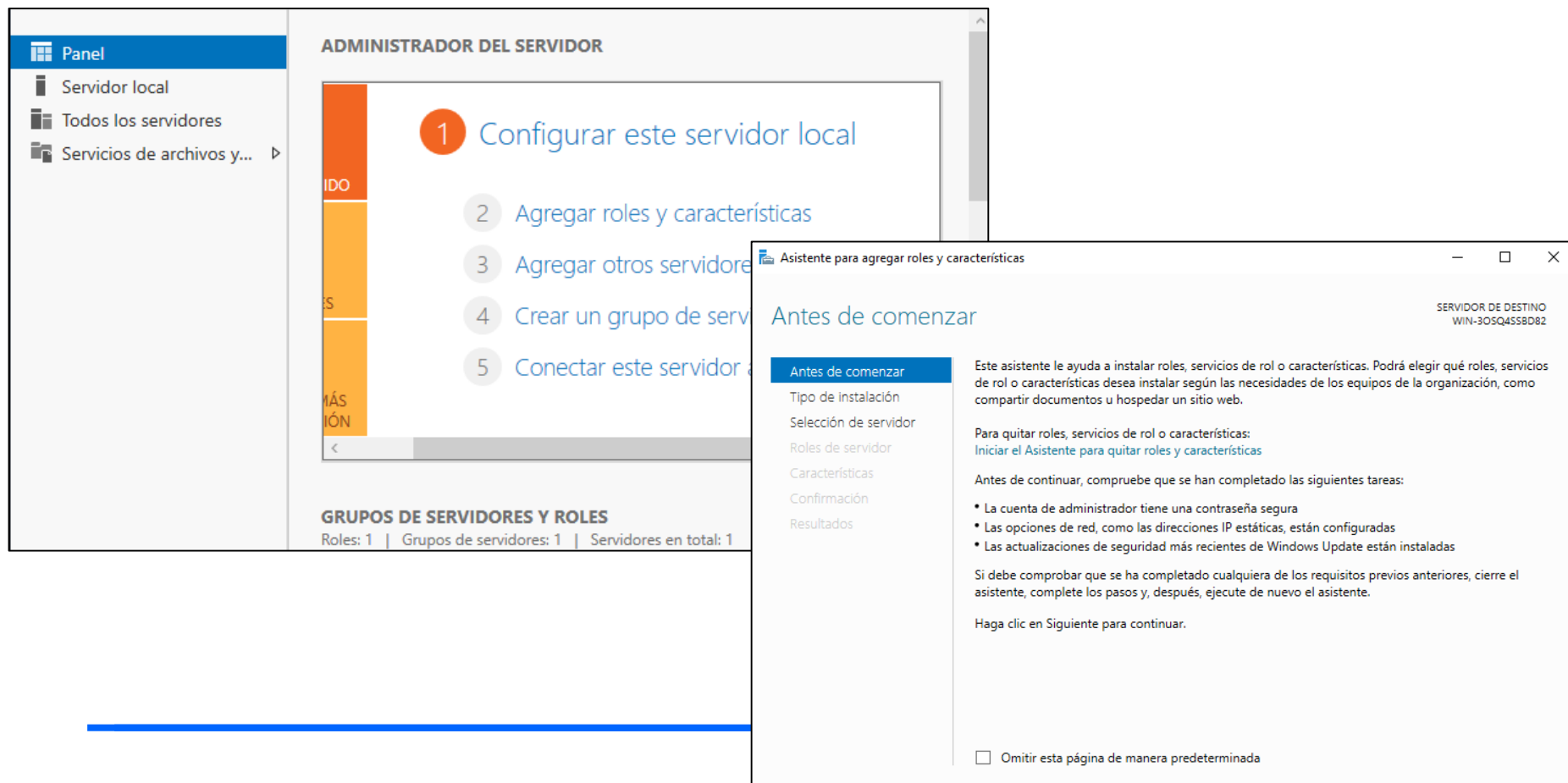
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 6.** A continuación haz click en el botón Quitar características y finalmente click en el botón Quitar. Se iniciará la eliminación del servicio DHCP. Finalmente pedirá reiniciar el servidor



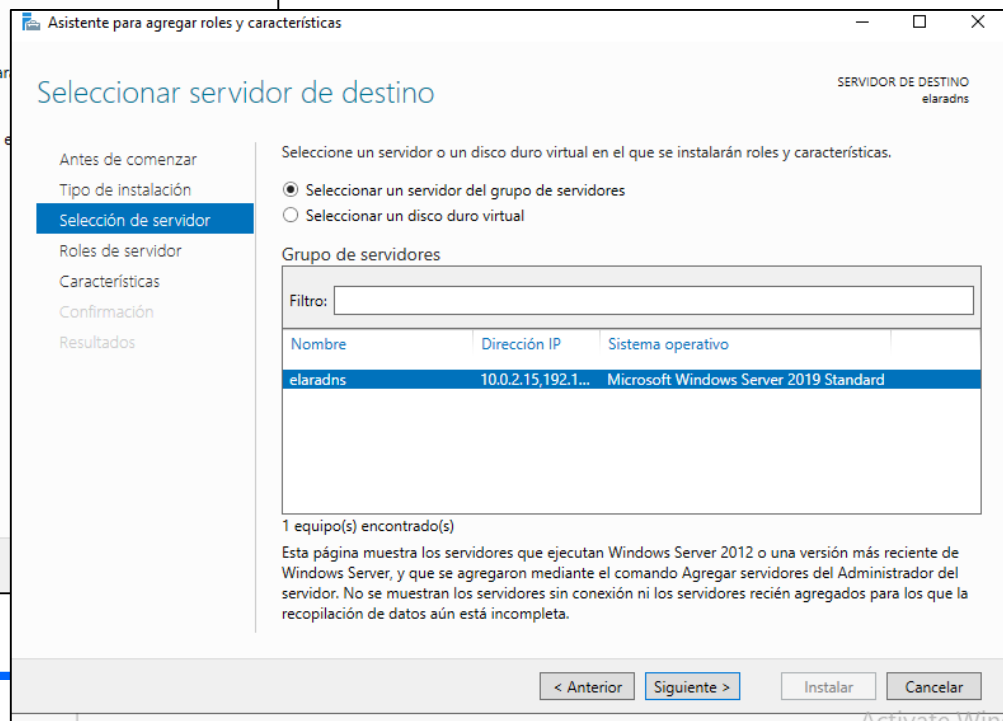
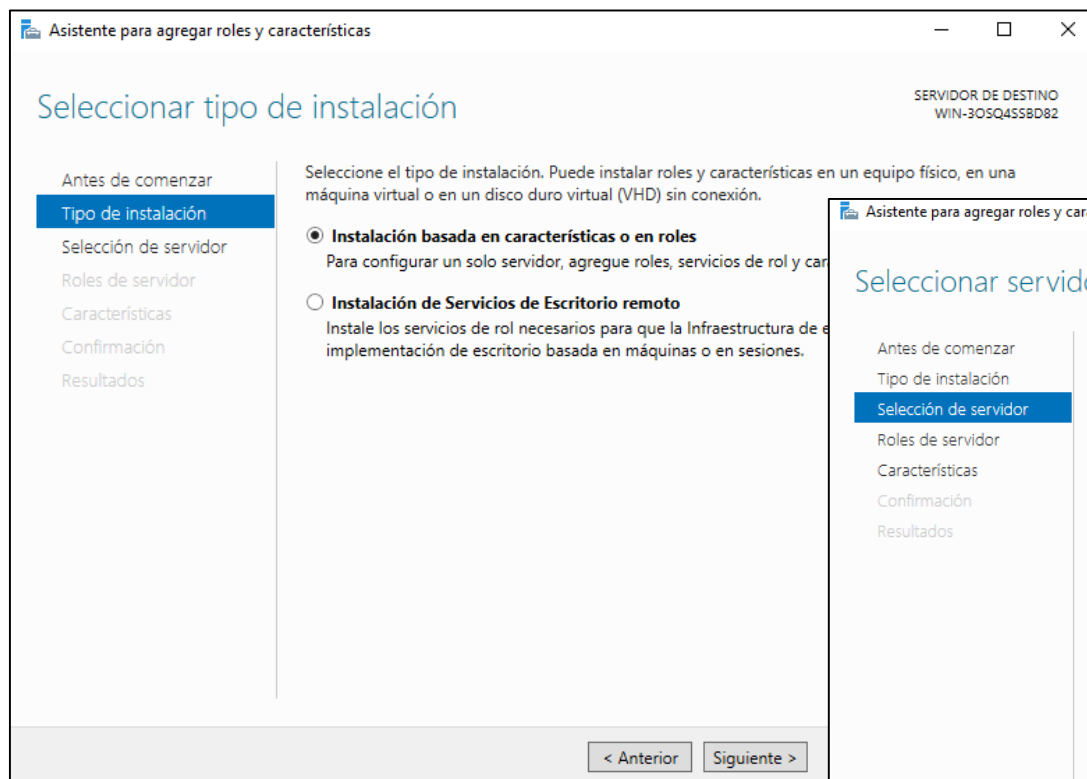
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 7.** La instalación del servidor DNS en windows Server 2019 se realiza con la herramienta Administrador del servidor. Seleccionamos la opción "Agregar roles y características". Nos aparece el asistente:



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 8.** Seleccionamos la opción "Instalación basada en características o en roles". A continuación indicamos el servidor donde vamos a realizar la instalación, es decir, nuestro mismo servidor:



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 9.** Nos aparece la lista de roles que podemos instalar en el servidor. Seleccionamos "Servidor DNS" y agregamos características requeridas:

Asistente para agregar roles y características

Selección de roles de servidor

Antes de comenzar  
Tipo de instalación  
Selección de servidor  
**Roles de servidor**  
Características  
Confirmación  
Resultados

Seleccione uno o varios roles para instalarlos en el servidor seleccionado.

SERVIDOR DE DESTINO  
elaradns

Roles	Descripción
<input type="checkbox"/> Acceso remoto	El servidor del Sistema de archivos de dominio (DNS) proporciona resolución de nombres por redes TCP/IP. El servidor es fácil de administrar cuando está instalado en el mismo servidor que los Servicios de dominio de Active Directory. Si selecciona el rol de Servicios de dominio de Active Directory, puede instalar los Servicios de dominio de Active Directory para que trabajen en conjunto.
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Atestación de mantenimiento del dispositivo	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Servicio de protección de host	
<input type="checkbox"/> Servicios de acceso y directivas de redes	
<input checked="" type="checkbox"/> Servicios de archivos y almacenamiento (1 de 12 roles)	
<input type="checkbox"/> Servicios de certificados de Active Directory	
<input type="checkbox"/> Servicios de dominio de Active Directory	
<input type="checkbox"/> Servicios de Escritorio remoto	
<input type="checkbox"/> Servicios de federación de Active Directory	
<input type="checkbox"/> Servicios de implementación de Windows	
<input type="checkbox"/> Servicios de impresión y documentos	
<input type="checkbox"/> Servidor de fax	
<input type="checkbox"/> Servidor DHCP	
<input checked="" type="checkbox"/> <b>Servidor DNS</b>	
<input type="checkbox"/> Servidor web (IIS)	
<input type="checkbox"/> Volume Activation Services	

¿Desea agregar las características requeridas para Servidor DNS?

Las siguientes herramientas son necesarias para administrar esta característica, pero no tienen que instalarse en el mismo servidor.

- ▲ Herramientas de administración remota del servidor
  - ▲ Herramientas de administración de roles [Herramientas] Herramientas del servidor DNS

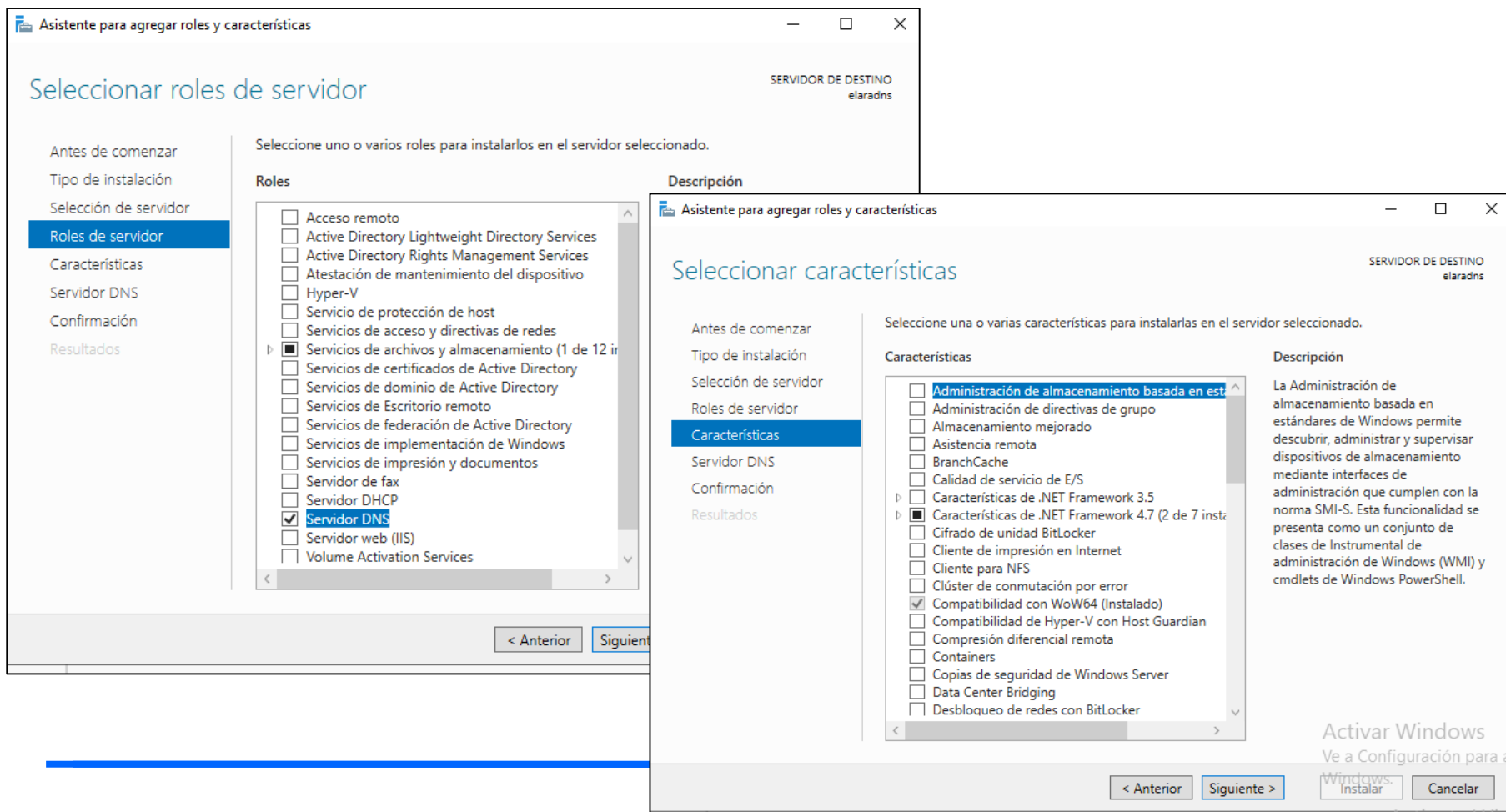
☒ Incluir herramientas de administración (si es aplicable)

Agregar características Cancelar

< Anterior Siguiete > Instalar

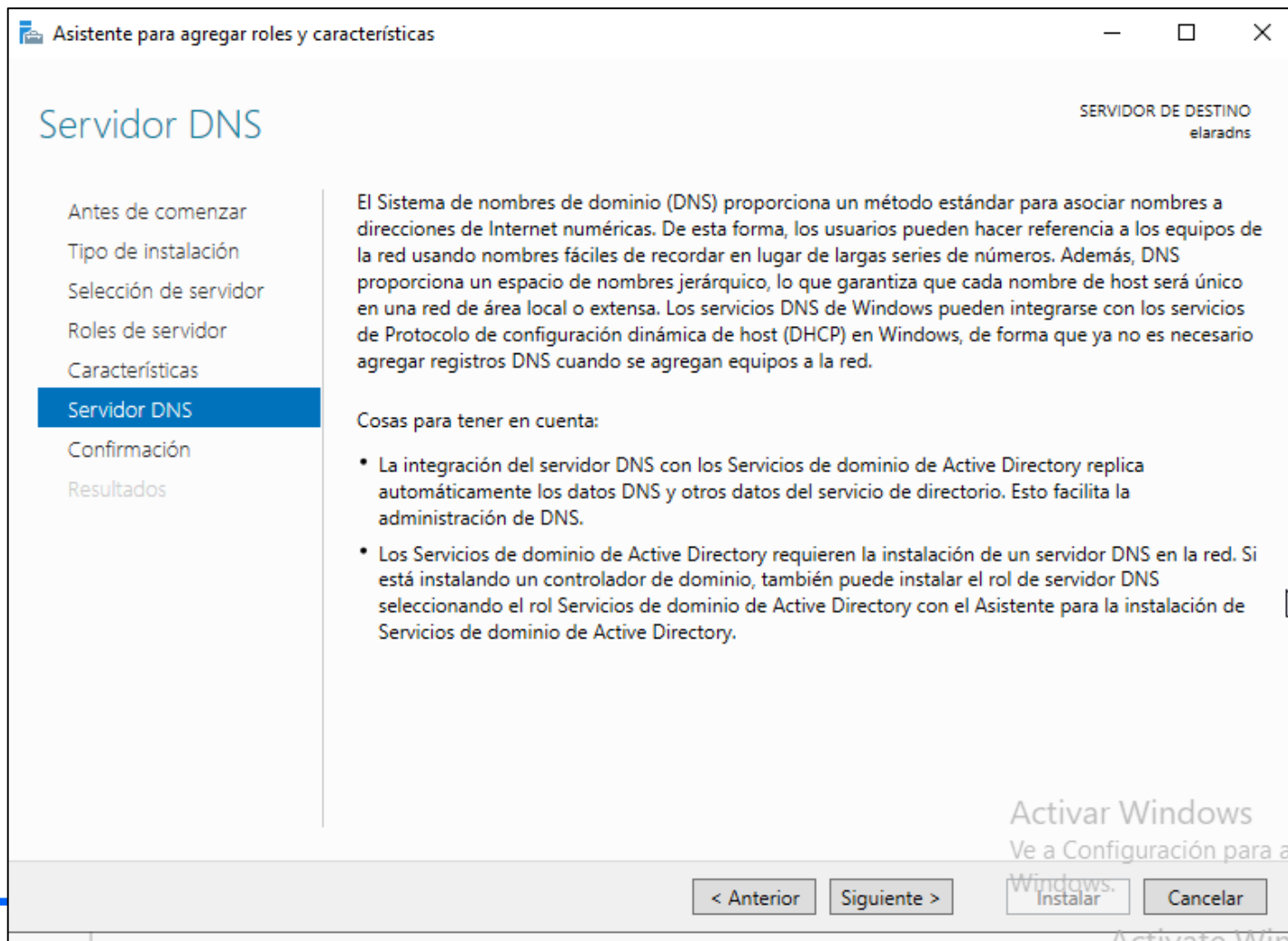
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 10.** Aparecen las distintas opciones de características que podemos agregar al servidor DNS. En principio no marcamos nada nuevo:



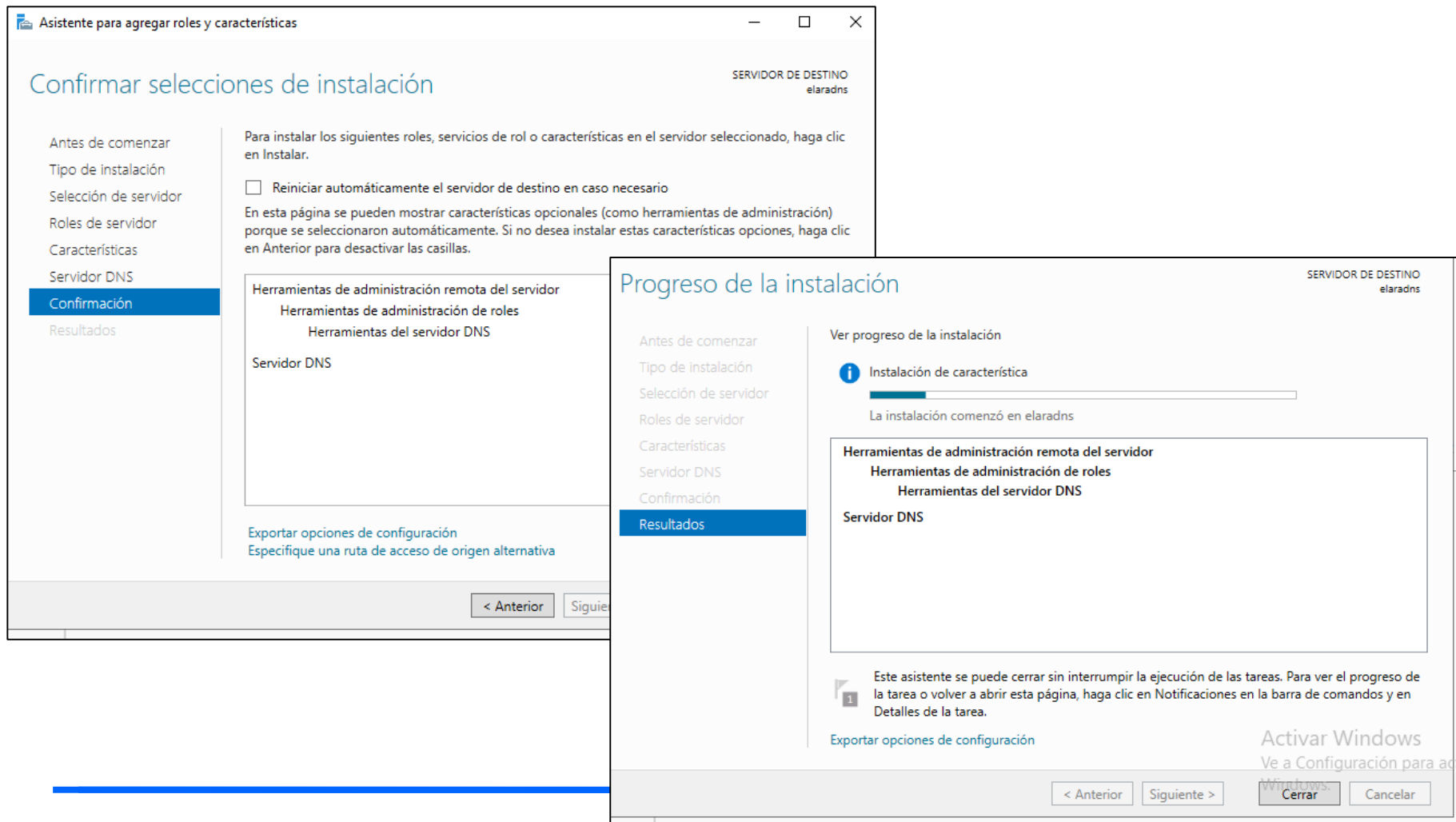
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 11.** En la siguiente pantalla nos explican que es un servidor DNS



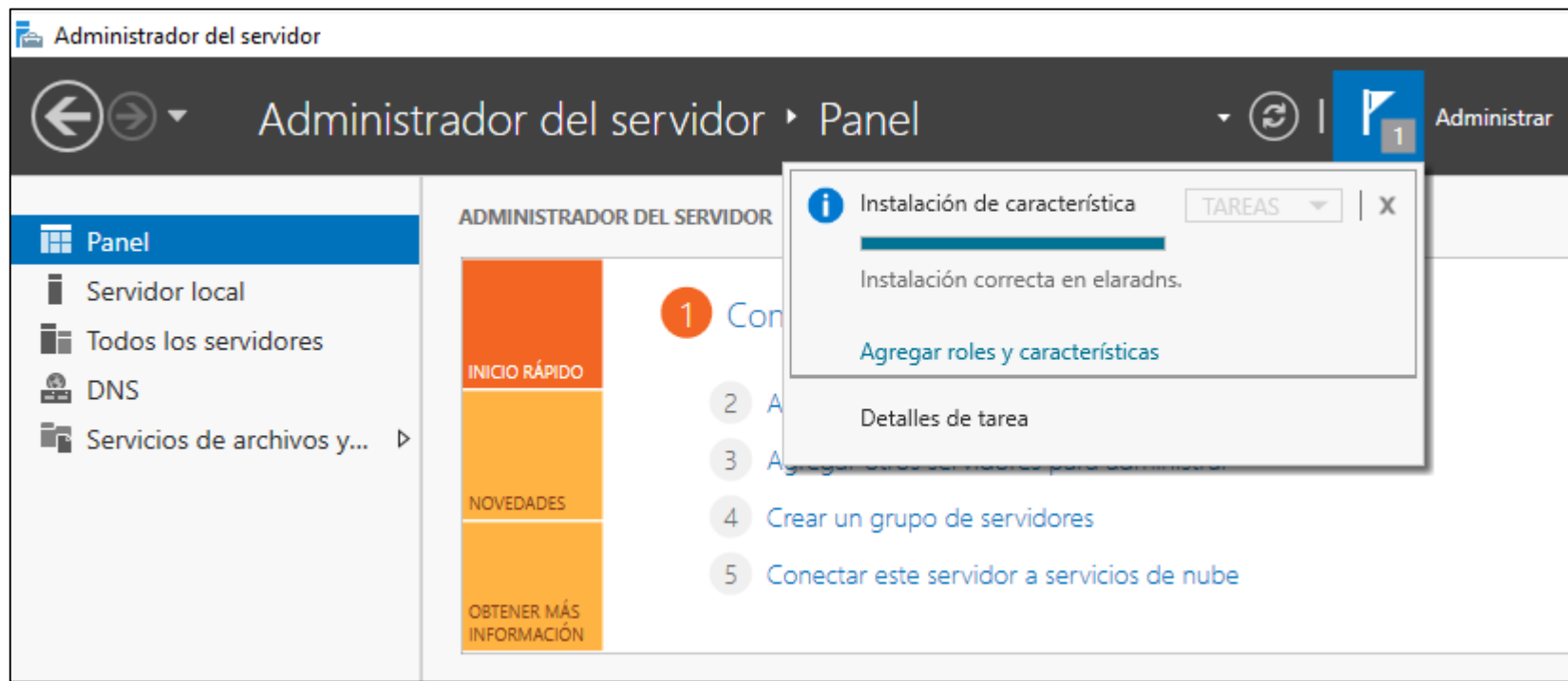
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

**Paso 12.** Confirmamos la instalacion y hacemos click en el boton Instalar.



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

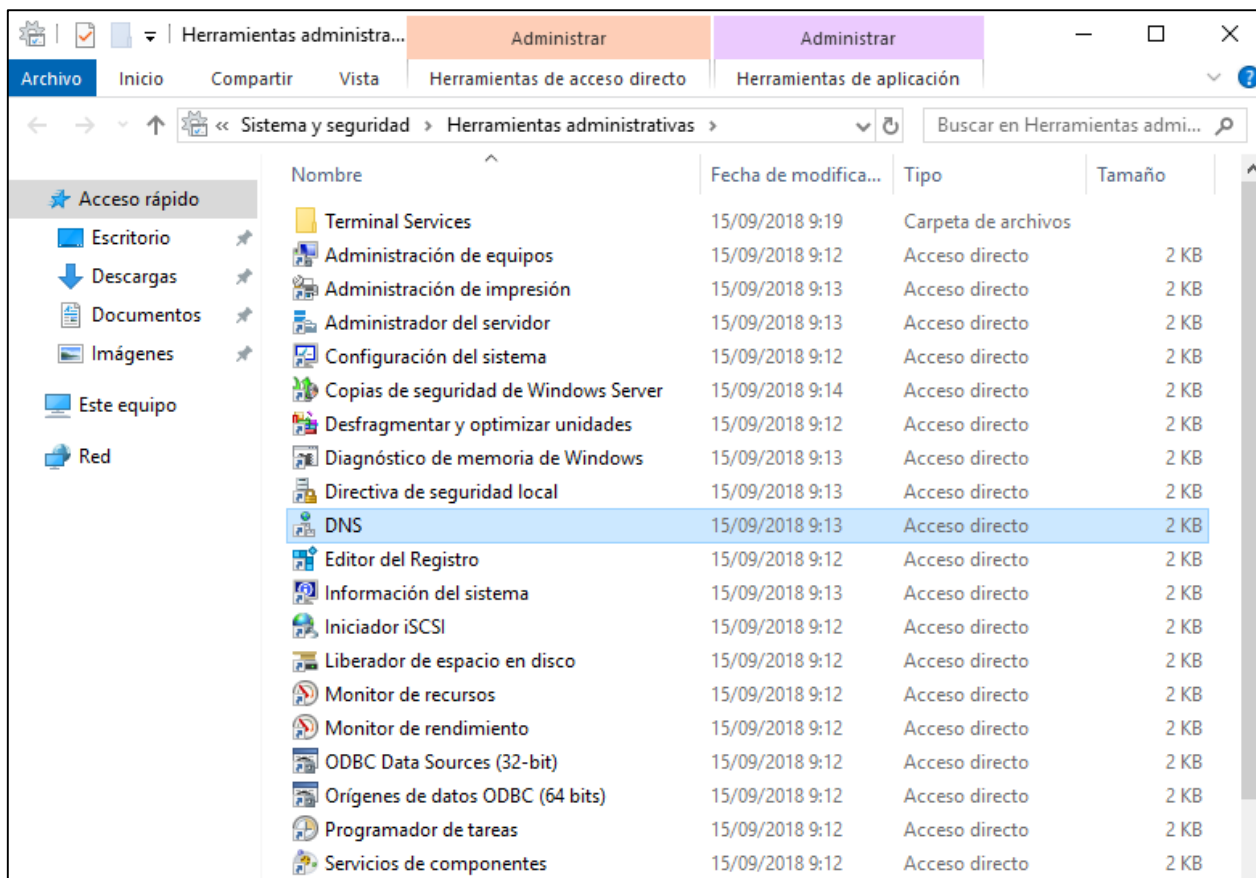
**Paso 13.** Una vez instalado el servidor DNS, en la barra de Administrador del servidor aparece una notificación que nos indica que la instalación se ha realizado de forma satisfactoria.





# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

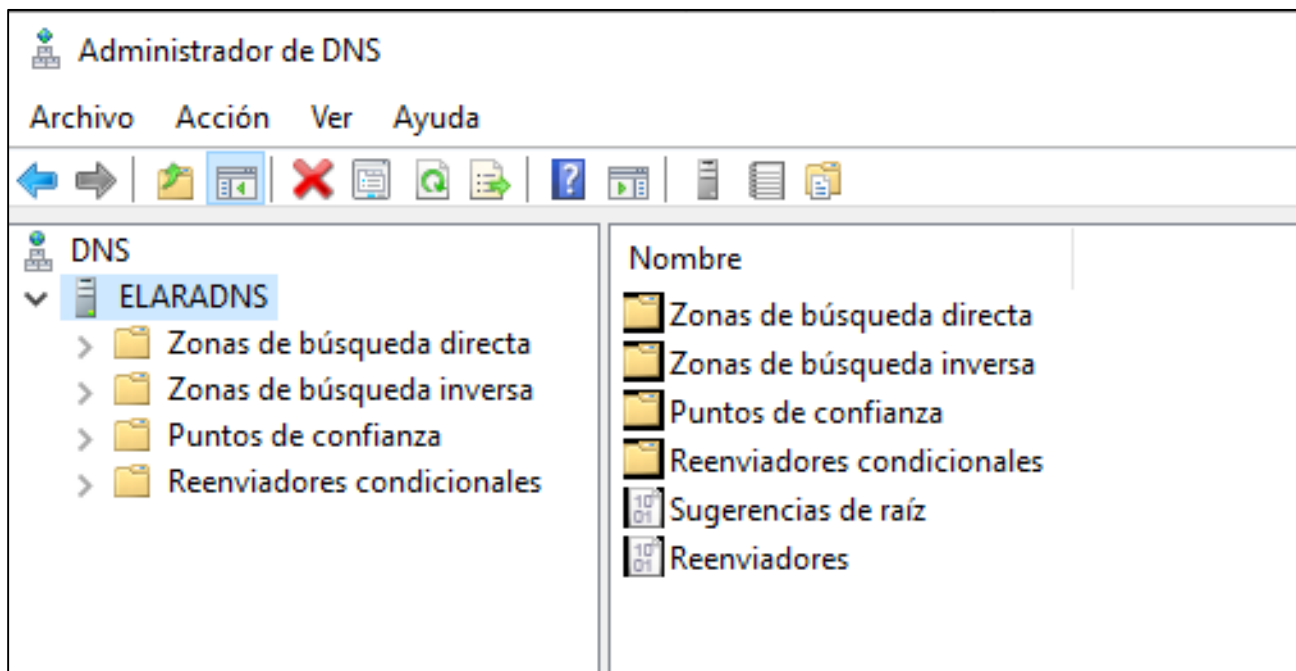
**Paso 14.** Una vez hemos instalado nuestro rol DNS el siguiente paso será configurarlo. Vamos a Inicio/Herramientas administrativas/DNS.



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

**Paso 15.** La primera pantalla que nos aparecerá mostrará las principales tareas que podemos realizar con las DNS: como son creación de zonas, reenviadores y puntos de confianza.

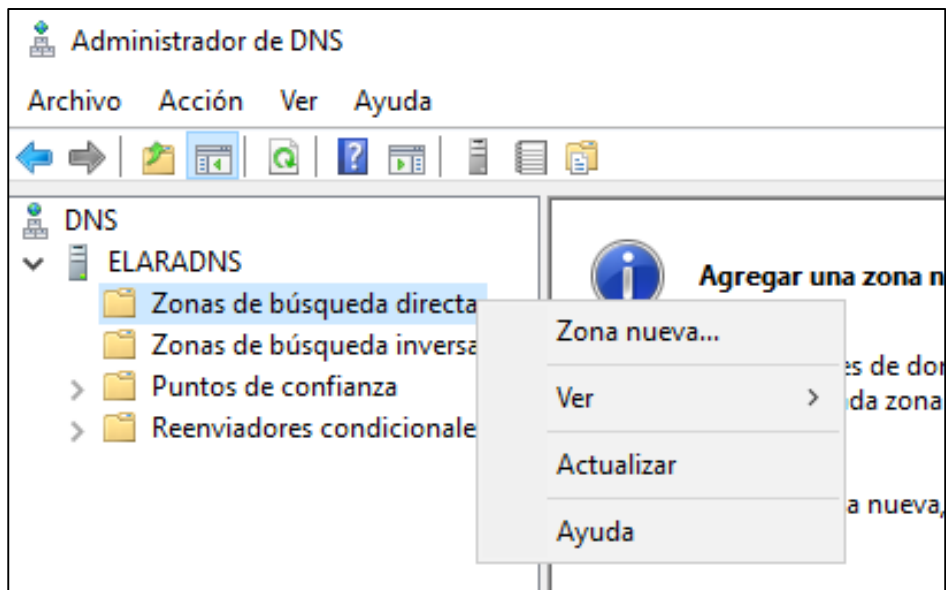


# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación de una nueva zona directa

**Paso 16.** Las zonas directas son las encargadas de realizar las traducciones de una cadena de nombre de host a la dirección IP. Pulsaremos sobre la zona de búsqueda directa haciendo click botón derecho y seleccionaremos Zona nueva.



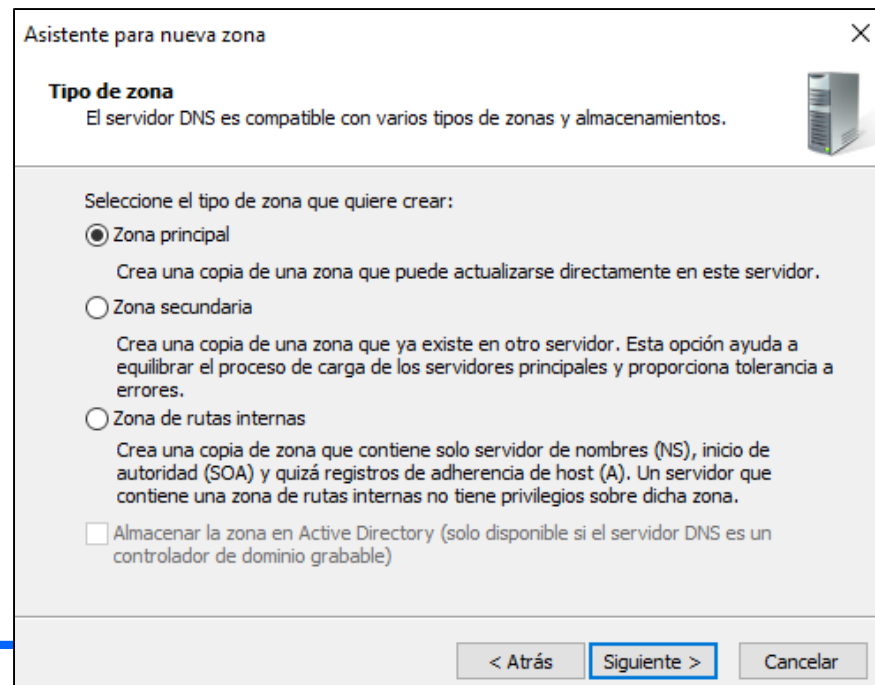
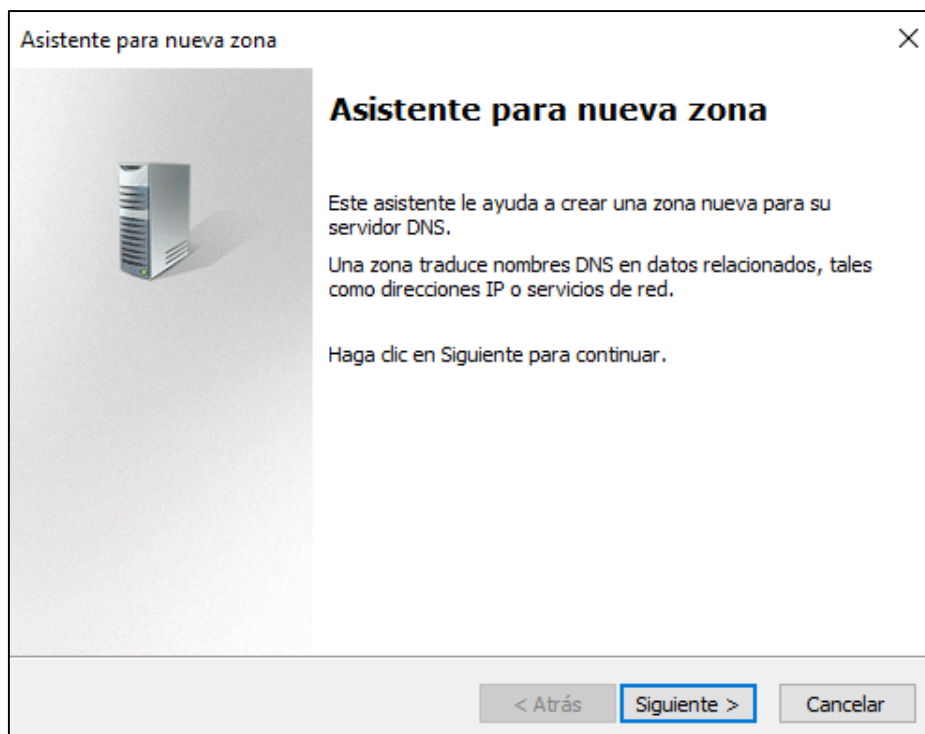
DNS permite a un espacio de nombres DNS ser dividido en zonas. Cada zona almacena información acerca de uno o mas dominios DNS contiguos

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación de una nueva zona directa

**Paso 17.** Nos aparece un asistente. Seleccionamos el tipo de zona principal:



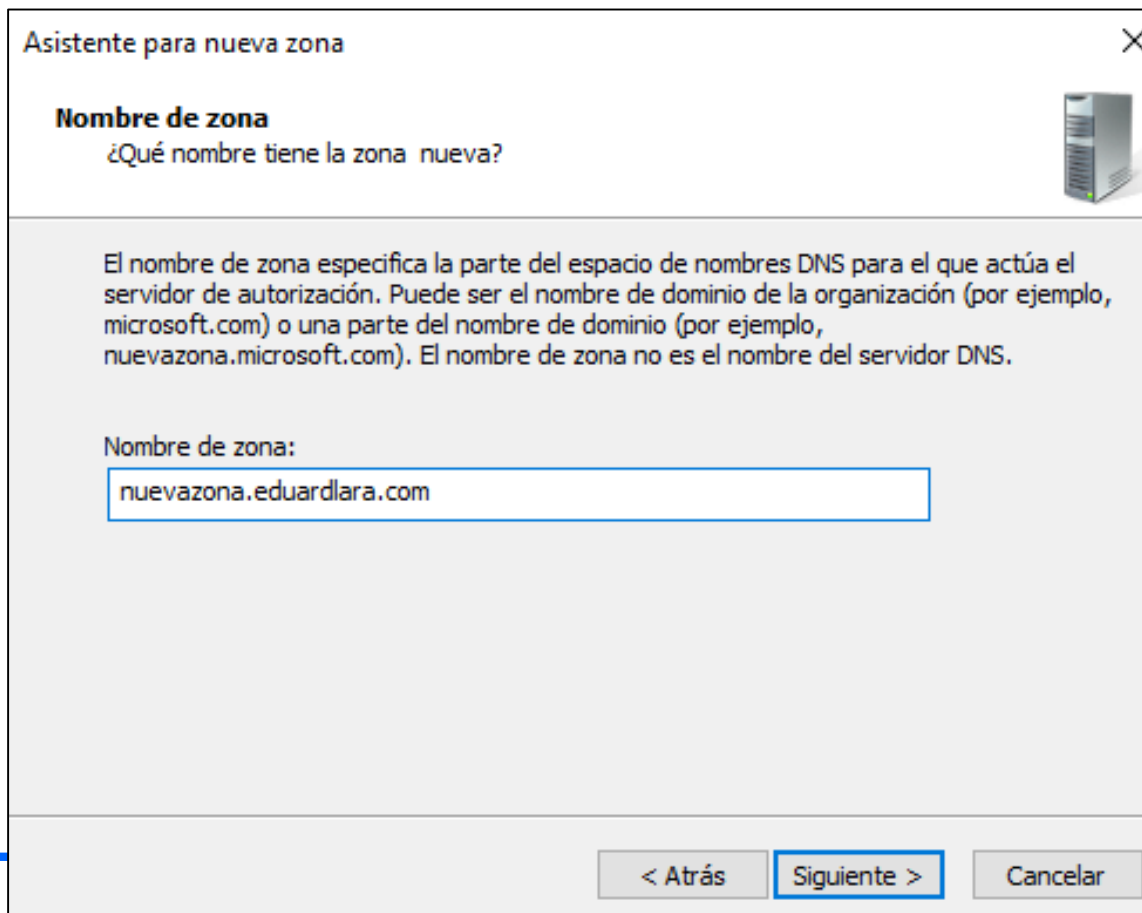
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación de una nueva zona directa

Paso 18. A continuation definimos el nombre de la zona:

nuevazona.nombrealumno.com



Asistente para nueva zona

**Nombre de zona**  
¿Qué nombre tiene la zona nueva?

El nombre de zona especifica la parte del espacio de nombres DNS para el que actúa el servidor de autorización. Puede ser el nombre de dominio de la organización (por ejemplo, microsoft.com) o una parte del nombre de dominio (por ejemplo, nuevazona.microsoft.com). El nombre de zona no es el nombre del servidor DNS.

Nombre de zona:

nuevazona.eduardlara.com

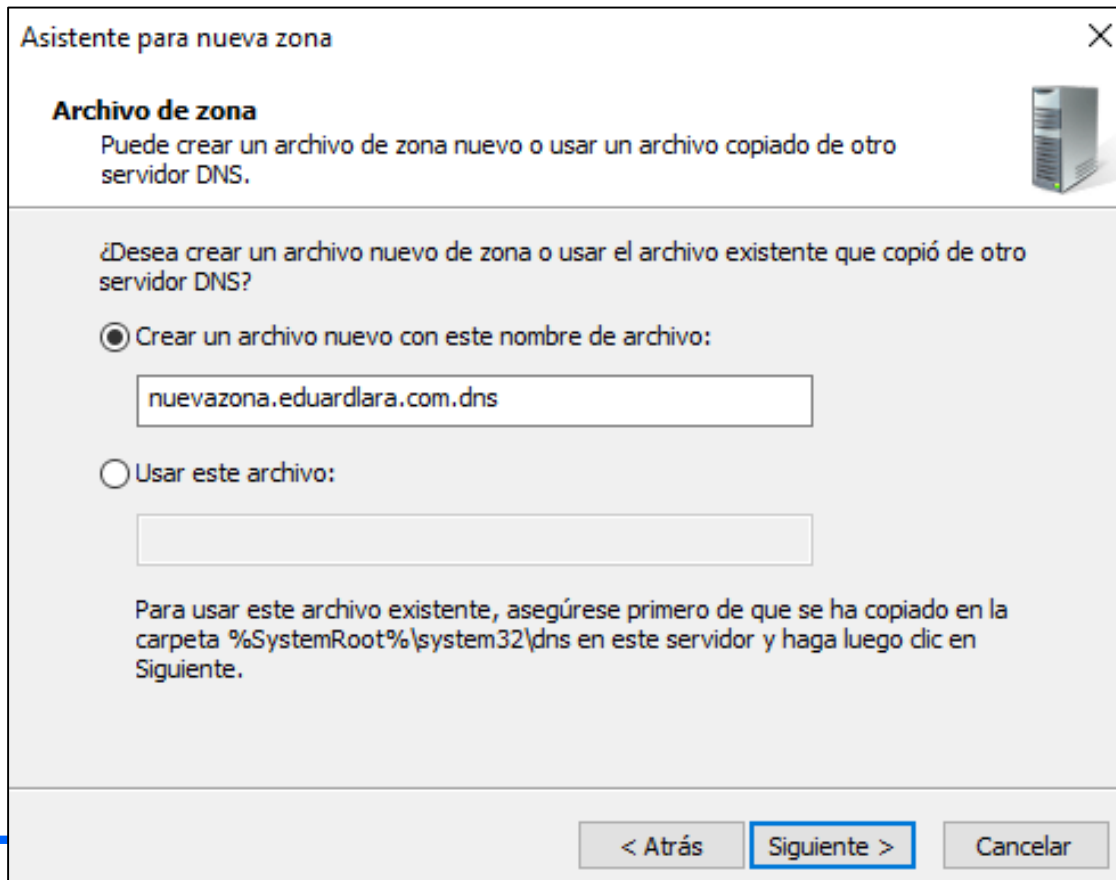
< Atrás    Siguiete >    Cancelar

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación de una nueva zona directa

Paso 19. Definimos el nombre del archivo de la zona que estamos creando: **nuevazona.nombrealumno.com.dns**



Asistente para nueva zona

**Archivo de zona**

Puede crear un archivo de zona nuevo o usar un archivo copiado de otro servidor DNS.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro servidor DNS?

☒ Crear un archivo nuevo con este nombre de archivo:

nuevazona.eduardlara.com.dns

☐ Usar este archivo:

Para usar este archivo existente, asegúrese primero de que se ha copiado en la carpeta %SystemRoot%\system32\dns en este servidor y haga luego clic en Siguiente.

< Atrás Siguiente > Cancelar

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación de una nueva zona directa

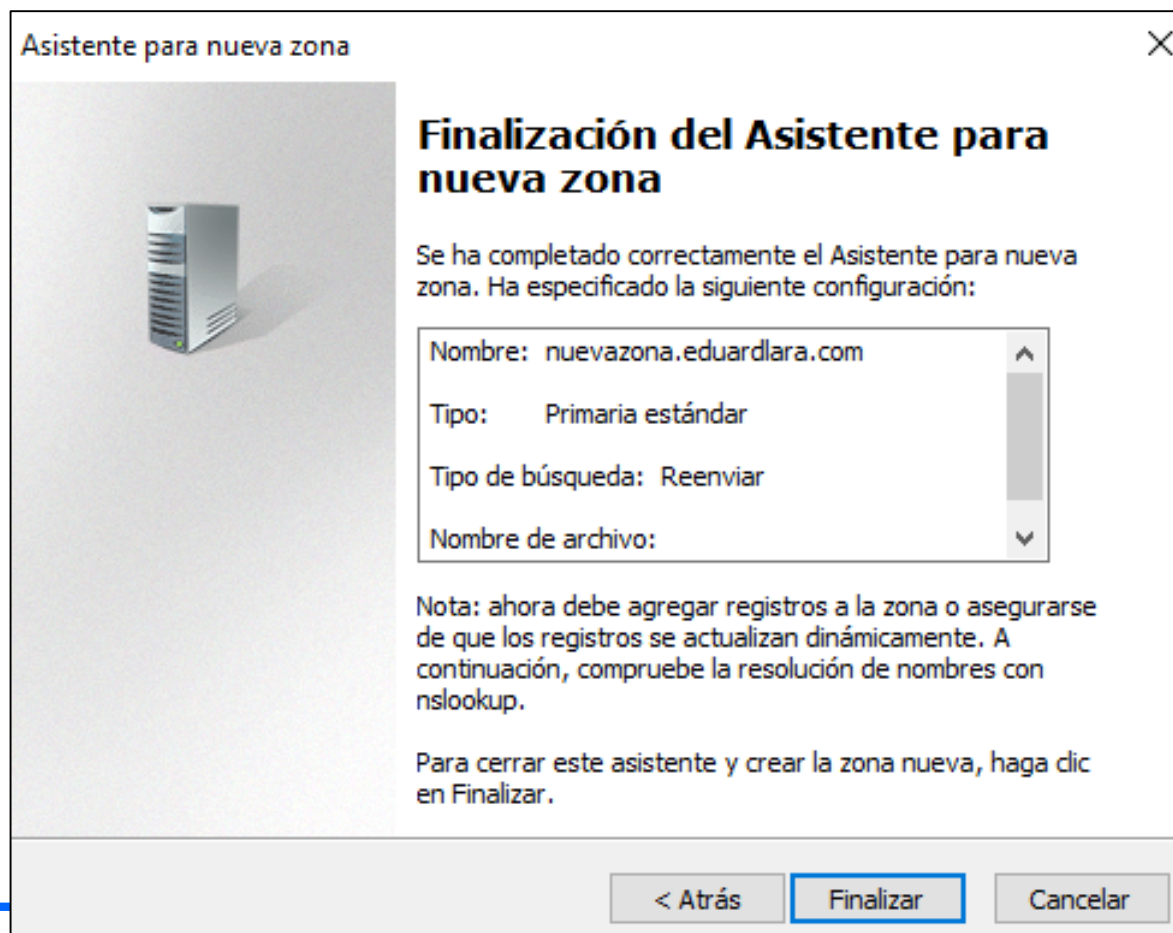
Paso 20. Establecemos la forma en la que se obtendrán las actualizaciones. Indicar **No admitir actualizaciones dinámicas**

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación de una nueva zona directa

Paso 21. Pulsamos en Finalizar para crear nuestra primera zona.

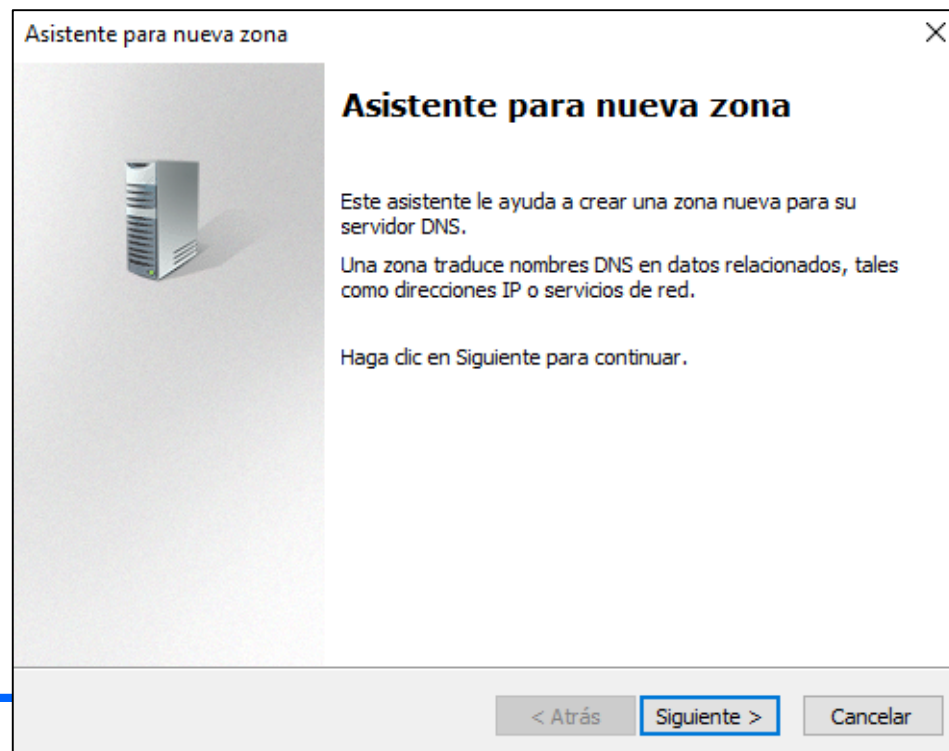
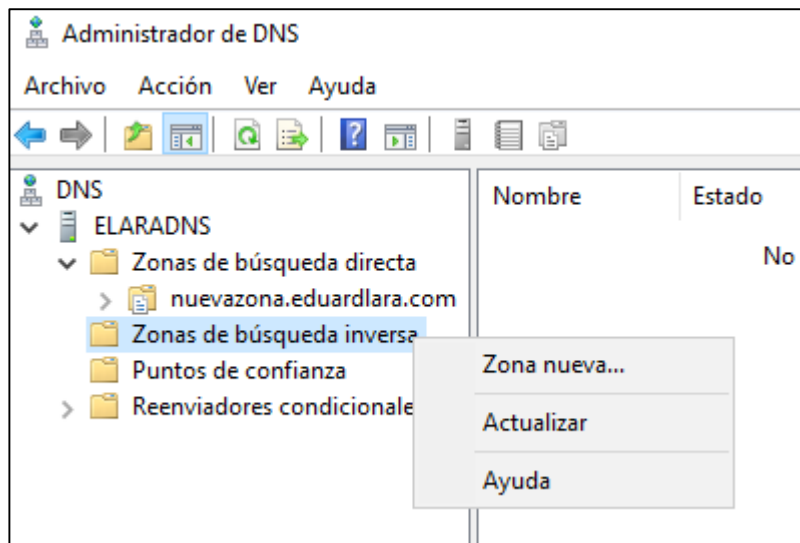




# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

## Creación una nueva zona inversa

**Paso 22.** Las zonas inversas hace lo contrario a las zonas directas, es decir, se encargan de realizar las traducciones de una dirección IP al nombre de host. Para crear una nueva zona indirecta, pulsaremos sobre la carpeta Zonas de búsqueda inversa, haciendo click botón derecho y seleccionaremos Zona nueva.



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Creación una nueva zona inversa

**Paso 24.** Elegir el tipo de zona Zona Principal y Zona de búsqueda inversa para IPv4:

Asistente para nueva zona

**Tipo de zona**  
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.

Seleccione el tipo de zona que quiere crear:

☒ Zona principal  
Crea una copia de una zona que puede actualizarse directamente en este servidor.

☐ Zona secundaria  
Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar el proceso de carga de los servidores principales y proporciona tolerancia a errores.

☐ Zona de rutas internas  
Crea una copia de zona que contiene solo servidor de nombres (NS), inicio de autoridad (SOA) y quizá registros de adherencia de host (A). Un servidor que contiene una zona de rutas internas no tiene privilegios sobre dicha zona.

☐ Almacenar la zona en Active Directory (solo disponible si el servidor DNS es un controlador de dominio grabable)

< Atrás   **Siguiente >**   Cancelar

Asistente para nueva zona

**Nombre de la zona de búsqueda inversa**  
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.

☒ Zona de búsqueda inversa para IPv4

☐ Zona de búsqueda inversa para IPv6

< Atrás   **Siguiente >**   Cancelar

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

## Creación una nueva zona inversa

**Paso 25.** El Nombre de la zona de búsqueda inversa: **1.168.192.in-addr.arpa**  
El archivo de zona: **1.168.192.in-addr.arpa.dns**

Asistente para nueva zona

**Nombre de la zona de búsqueda inversa**  
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

☐ Id. de red:

El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).

Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.

☒ Nombre de la zona de búsqueda inversa:

< Atrás    **Siguiente >**    Cancelar

Asistente para nueva zona

**Archivo de zona**  
Puede crear un archivo de zona nuevo o usar un archivo copiado de otro servidor DNS.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro servidor DNS?

☒ Crear un archivo nuevo con este nombre de archivo:

☐ Usar este archivo:

Para usar este archivo existente, asegúrese primero de que se ha copiado en la carpeta %SystemRoot%\system32\dns en este servidor y haga luego clic en Siguiente.

< Atrás    **Siguiente >**    Cancelar

# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

## Creación una nueva zona inversa

**Paso 26.** No admitir actualizaciones dinámicas y por ultimo finalizar el asistente de nueva zona

**Asistente para nueva zona**

**Actualización dinámica**  
Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

- ☐ Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory)  
Esta opción solo está disponible para las zonas que están integradas en Active Directory.
- ☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)  
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.  
 Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.
- ☒ No admitir actualizaciones dinámicas  
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

< Atrás **Siguiente >** Cancelar

**Asistente para nueva zona**

**Finalización del Asistente para nueva zona**

Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:

Nombre: 1.168.192.in-addr.arpa  
Tipo: Primaria estándar  
Tipo de búsqueda: Invertir  
Nombre de archivo: 1.168.192.in-addr.arpa.dns

Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.

Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.

< Atrás **Finalizar** Cancelar

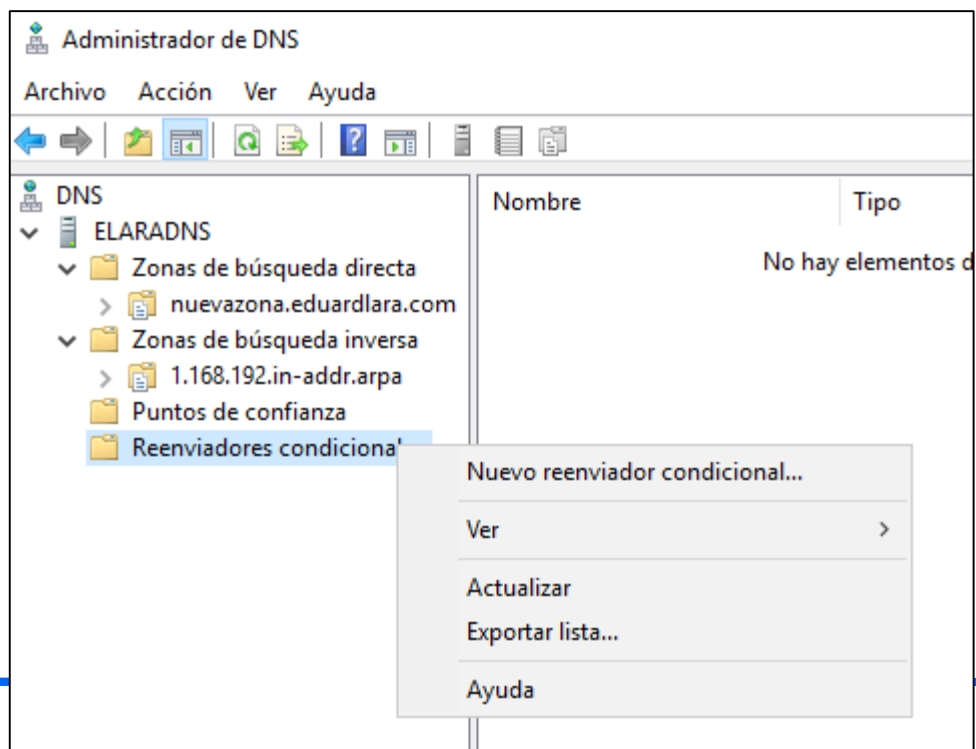
# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

## Establecer un reenviador DNS

**Paso 27.** Es conveniente crear un reenviador condicional para permitir a nuestro servidor DNS consultar a otros servidores DNS externos aquellos registros que él no sea capaz de resolver por si mismo.

Para crear un nuevo reenviador pulsamos con el **botón derecho sobre Reenviadores condicionales** y seleccionaremos **Nuevo reenviador condicional**.



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

## Establecer un reenviador DNS

**Paso 28.** En primer lugar especificamos el nombre del dominio, para nuestro ejemplo Google, y en la lista de direcciones iremos agregando las direcciones IP del servidor DNS externo seleccionado. Una vez rellena la información pulsamos en Aceptar para crear nuestro reenviador condicional el cual usará nuestro servidor DNS local cuando éste no sea capaz de resolver un registro DNS

Nuevo reenviador condicional

Dominio DNS:  
Google

Direcciones IP de los servidores maestros:

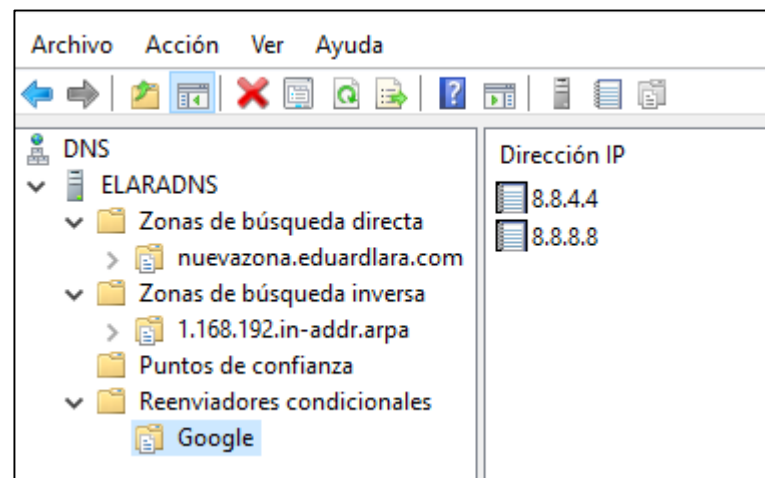
Dirección IP	FQDN de servidor	Validado
<Haga clic aquí para ...>		
8.8.4.4	dns.google	Aceptar
8.8.8.8	dns.google	Aceptar

☐ Almacenar este reenviador condicional en Active Directory y replicarlo como sigue:  
Todos los servidores DNS en este bosque

Segundos transcurridos hasta agotarse el tiempo de espera de reenvío de consultas: 5

El FQDN del servidor no estará disponible si no están configuradas las entradas y zonas de búsqueda inversa apropiadas.

Aceptar Cancelar



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

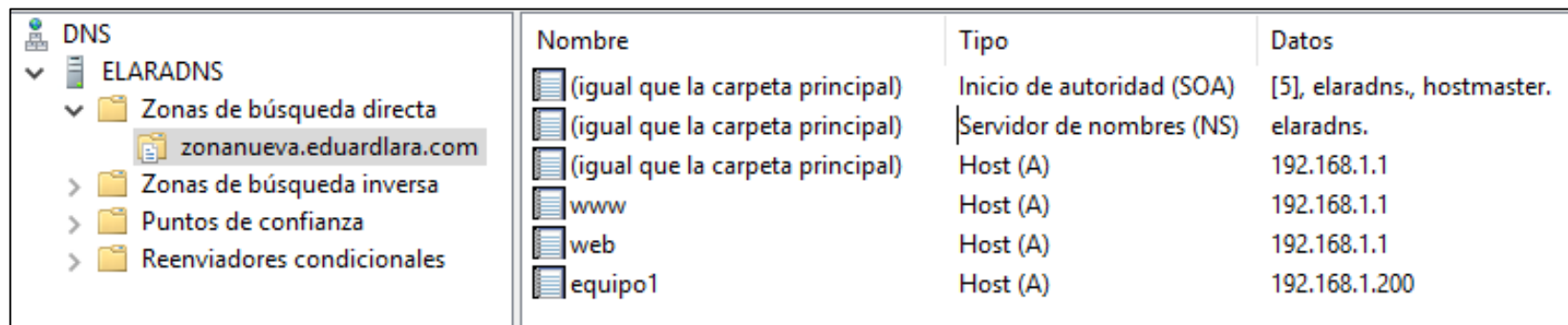
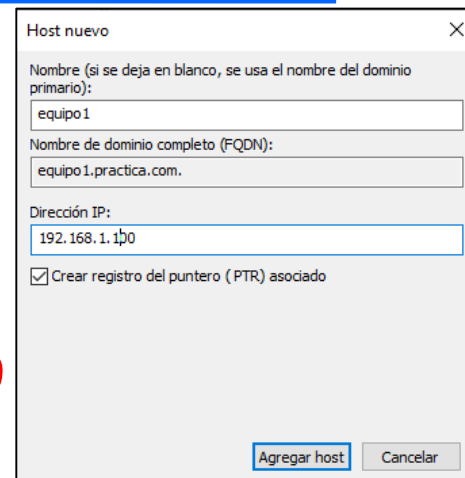
Paso 29. Crea 3 registros de tipo A → Nuevo Host

nuevazona.alumno.com ↔ 192.168.1.1

www.nuevazona.alumno.com ↔ 192.168.1.1

web.nuevazona.alumno.com ↔ 192.168.1.1

equipo1.nuevazona.alumno.com ↔ 192.168.1.200



Nombre	Tipo	Datos
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[5], elaradns., hostmaster.
(igual que la carpeta principal)	Servidor de nombres (NS)	elaradns.
(igual que la carpeta principal)	Host (A)	192.168.1.1
www	Host (A)	192.168.1.1
web	Host (A)	192.168.1.1
equipo1	Host (A)	192.168.1.200

Selecciona los registros PTR. Son lo opuesto a los registros A: no asignan un nombre de dominio a una dirección IP, sino viceversa. Por eso, se dice que los registros PTR hacen posible la **búsqueda inversa**



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

Paso 30. Abre un cliente windows 10. En la red interna compartida indica la dirección IP a 192.168.1.200 y servidor dns 192.168.1.1

Paso 31. Desde el Server ejecuta: **nslookup 192.168.1.200**,  
**nslookup 192.168.1.1**, **nslookup equipo1.zonanueva.alumno.com**

Paso 32. Desde el Server ejecuta: **ping 192.168.1.200**,  
**ping equipo1.zonanueva.alumno.com** ¿funciona?

The screenshot shows the DNS console with the following configuration:

Nombre	Tipo
(igual que la carpeta princip...	Inicio de autoridad (SOA)
(igual que la carpeta princip...	Servidor de nombres (NS)
(igual que la carpeta princip...	Host (A)
www	Host (A)
web	Host (A)
equipo1	Host (A)

The command prompt shows the following output:

```
C:\Users\Administrador>ping 192.168.1.200

Haciendo ping a 192.168.1.200 con 32 bytes de datos:
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

The screenshot shows the DNS console with the following configuration:

Nombre	Tipo	Datos
(igual que la carpeta princip...	Inicio de autoridad (SOA)	[5], elaradns., hostm...
(igual que la carpeta princip...	Servidor de nombres (NS)	elaradns.
(igual que la carpeta princip...	Host (A)	192.168.1.1
www	Host (A)	192.168.1.1
web	Host (A)	192.168.1.1
equipo1	Host (A)	192.168.1.200

The command prompt shows the following output:

```
C:\Users\Administrador>ping equipo1.zonanueva.eduarlara.com

Haciendo ping a equipo1.zonanueva.eduarlara.com [192.168.1.200] con 32 bytes de datos:
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```



# PRACTICA 4. SERVIDOR DNS EN WINDOWS SERVER 2019

---

Paso 33. Desde el equipo windows10, ejecuta:

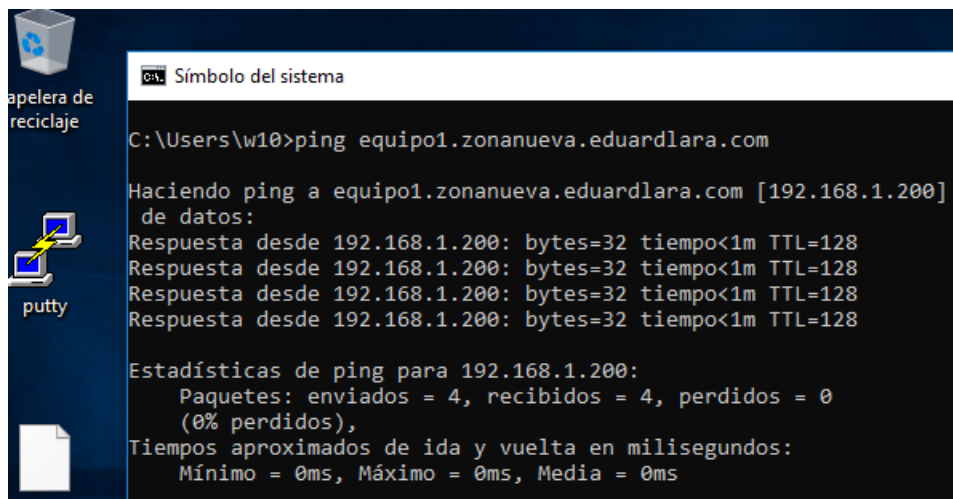
**nslookup 192.168.1.1, nslookup equipo1.zonanueva.alumno.com**

Paso 33. Desde el equipo windows10, prueba ahora:

**ping 192.168.1.1**

**ping equipo1.zonanueva.alumno.com**

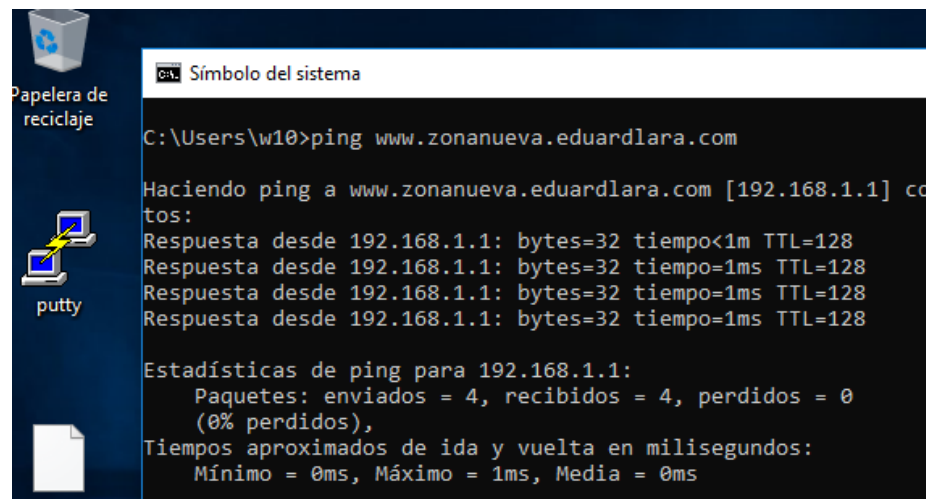
**ping www.zonanueva.alumno.com**



```
C:\Users\w10>ping equipo1.zonanueva.eduardlara.com

Haciendo ping a equipo1.zonanueva.eduardlara.com [192.168.1.200] de datos:
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```



```
C:\Users\w10>ping www.zonanueva.eduardlara.com

Haciendo ping a www.zonanueva.eduardlara.com [192.168.1.1] de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```