

Unidad 2 - DHCP y DNS

DHCP (Dynamic Host Configuration Protocol)

Este protocolo sirve para proporcionar un servicio de red que permita a equipos de una red TCP/IP **obtener automáticamente los parámetros de configuración de red**.

¿Por qué usar DHCP?

Todos los **dispositivos** de una red **basada** en **TCP/IP** deben tener una **dirección IP** de unidifusión única para acceder a la red y sus recursos.

- Con DHCP el **servidor DHCP** mantiene un grupo de **direcciones IP** y concede una **dirección** a **cualquier cliente habilitado** para DHCP cuando se inicia en la red.
- Si no, las **IP** serían **estáticas**, y las deberíamos de **configurar manualmente** en cada equipo.
- Los servidores DHCP que mantienen la información de configuración de TCP/IP y proporcionan la configuración de direcciones a los clientes habilitados para DHCP en forma de una oferta de concesión.
- DHCP se basa en la utilización del primitivo protocolo BOOTP (Bootstrap Protocol)
- Este protocolo permite a los equipos sin disco obtener una dirección IP antes de cargar un sistema operativo.

Ventajas de DHCP

- Configuración de dirección IP confiable. DHCP minimiza los errores de configuración como errores tipográficos, asignación de una dirección IP a más de un equipo al mismo tiempo.
- Administración de red reducida. reduce la administración de red:
 - Configuración de TCP/IP centralizada y automatizada.
 - La capacidad de asignar un intervalo completo de valores de configuración adicionales de TCP/IP mediante opciones DHCP
 - Los equipos pueden cambiar de ubicación (subred) sin tener que reconfigurar la dirección IP manualmente
 - El reenvío de mensajes DHCP iniciales mediante un agente de retransmisión DHCP, lo que elimina la necesidad de un servidor DHCP en cada subred.
 - Configuración segura y libre de errores. Se evitan errores manuales al introducir las configuraciones de red.

Inconvenientes

- Dependencia del servidor DHCP, si el servidor falla puede interrumpir la conectividad de todos los dispositivos.
- Mucho tráfico de difusión (broadcast)
- DHCP por sí solo no tiene mecanismos de seguridad nativos para verificar la autenticidad de las solicitudes de DHCP (Spoofing o starvation)

- Gestionar el "pool" de direcciones IP disponibles y asegurarse de que no se agoten.
- Conflictos de IP: IP estática entra en conflicto con asignación DHCP o varios servidores DHCP están mal configurados.

Tipos de asignaciones

Sin DHCP, cada dirección IP debe configurarse manualmente en cada dispositivo y, si el dispositivo se mueve a otra subred, se debe configurar otra dirección IP diferente.

El DHCP le permite al **administrador supervisar y distribuir** de forma **centralizada** las **direcciones IP** necesarias y, automáticamente, asignar y enviar una nueva IP si fuera el caso de un dispositivo que es conectado en un lugar diferente de la red.

Asignación manual o estática

La asignación manual implica que un administrador de red configura manualmente una dirección IP fija a un dispositivo específico (como un servidor o una impresora) en la red.

Características:

- La dirección IP no cambia a menos que sea modificada por el administrador.
- Usualmente se usa para dispositivos que necesitan estar siempre disponibles en la misma dirección IP, como servidores o dispositivos críticos.

Ventaja: Proporciona control completo al administrador

Desventaja: Es laboriosa en redes grandes y propensa a errores si no se gestiona correctamente.

Asignación automática (DHCP auto)

El servidor **DHCP (Dynamic Host Configuration Protocol)** asigna automáticamente direcciones IP a los dispositivos de una red a partir de un rango predefinido (conocido como "pool" de direcciones IP). La asignación puede ser temporal.

Características:

- El dispositivo solicita una IP cuando se conecta a la red, y el servidor DHCP le asigna una dirección IP automáticamente.
- El dispositivo recibirá siempre la misma IP cada vez que se conecte a la red, incluso después de desconectarse por períodos largos (asociada a MAC).

Ventaja: IP constante, facilita la gestión en redes grandes, ya que no requiere intervención manual para cada dispositivo.

Desventaja: podría agotarse el "pool" de direcciones IP, especialmente en redes grandes con frecuentes conexiones y desconexiones.

Asignación dinámica

Similar a la asignación automática, también se gestiona a través de DHCP, pero en este caso, la IP asignada al dispositivo tiene un tiempo de arrendamiento limitado. Una vez que expire este tiempo, la IP puede reasignarse a otro dispositivo.

Características:

- Las direcciones IP se otorgan por un tiempo limitado

- El dispositivo puede recibir una dirección IP diferente cada vez que se conecte

Ventaja: Optimiza el uso de direcciones IP en redes donde hay más dispositivos que direcciones disponibles

Desventaja: No es adecuada para dispositivos que requieren una IP fija

Asignación estática con reserva (DHCP reserva)

Se trata de una asignación dinámica controlada, donde el servidor DHCP asigna siempre la misma dirección IP a un dispositivo específico basado en su dirección MAC. Es una especie de mezcla entre asignación manual y automática.

Características:

- El administrador reserva una dirección IP específica para un dispositivo, que el servidor DHCP otorga cada vez que el dispositivo se conecta.
- Se utiliza generalmente para dispositivos que necesitan tener siempre la misma IP, pero gestionados automáticamente por el servidor DHCP.

Ventaja: El dispositivo recibe una dirección IP constante sin necesidad de configuración manual en el dispositivo

Desventaja: Requiere configurar la reserva en el servidor DHCP, lo que puede implicar cierta complejidad administrativa.

Parámetros DHCP

Un cliente habilitado para DHCP, al aceptar una oferta de concesión, recibe los siguientes parámetros:

Parámetros por defecto:

- Dirección IP del cliente
- Máscara de subred

Parámetros opcionales:

- Puerta de enlace
- Direcciones de los servidores DNS
- Nombre o sufijo del dominio DNS

Necesidades del cliente

- **Dirección IP** que actúe como identificador y le permita ser reconocido unívocamente en Internet o en una intranet.
- **Máscara de subred**, para conocer la parte de la dirección IP que describe la red o subred donde se halla el equipo y la otra parte que sirve para identificarlo.
- **Dirección IP de la puerta de enlace**, usada por defecto, que se corresponde con un router que permitirá enrutar el tráfico a Internet o a otras partes de la red.
- **Direcciones IP de los servidores DNS**, encargados de "resolver" o traducir los nombres de dominio usados en Internet en su correspondiente dirección IP. Así se evita que el usuario deba conocer las direcciones IP de los equipos a los que desea acceder.

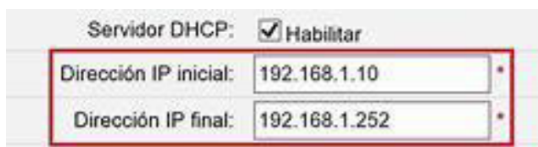
Información que almacena el servidor DHCP en una base de datos

- Parámetros de configuración TCP/IP
- Direcciones IP válidas, direcciones excluidas
- IP reservada direcciones asociadas a clientes DHCP concretos
- La duración de la concesión de la dirección IP

Rango de direcciones

Es un conjunto ordenado de direcciones IP consecutivas.

- Definido por la primera y la última del rango y que incluye ambas.
- Especifica el número máximo de clientes a los que puede dar servicio
- Ej: Un rango de 51 equipos sería desde 10.0.0.150 hasta 10.0.0.200.



A screenshot of a DHCP server configuration window. The 'Servidor DHCP' section has a checked 'Habilitar' checkbox. Below it, two text boxes are highlighted with a red rectangle: 'Dirección IP inicial' with the value '192.168.1.10' and 'Dirección IP final' with the value '192.168.1.252'.

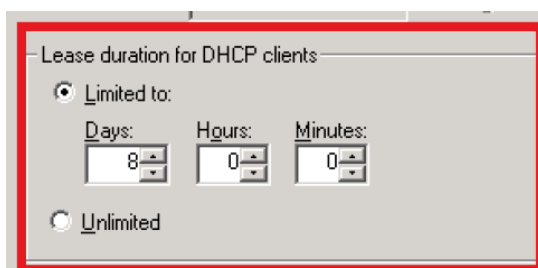
Reserva

Una reserva permite **asignar** direcciones **IP** de forma **fija a través** de la dirección **MAC** o dirección física de la tarjeta de red.

Lease o concesión

La concesión o **lease** se define como el **período de tiempo** durante el cual un servidor DHCP asigna una **dirección IP** a un cliente.

El período de concesión configurado para un servidor DHCP se aplica a todas las direcciones IP que un servidor DHCP asigna dinámicamente a sus clientes.

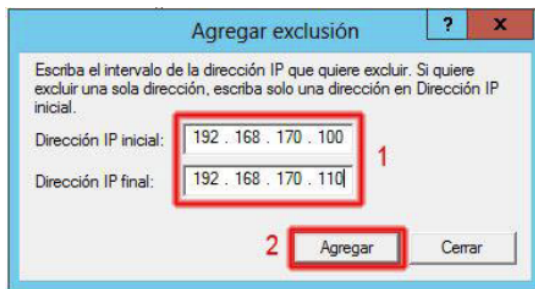


A screenshot of the 'Lease duration for DHCP clients' configuration window. The 'Limited to' radio button is selected. Below it, three spin boxes are shown: 'Days' with the value '8', 'Hours' with the value '0', and 'Minutes' with the value '0'. The 'Unlimited' radio button is also visible but not selected. The entire configuration area is highlighted with a red rectangle.

Exclusión

Es la dirección o **rango IP** que **no puede conceder** un servidor DHCP.

- Ej: si se excluye el rango 10.0.0.8-10.0.0.10, la única forma de que un equipo pueda obtener una de esas tres direcciones es a través de su configuración manual o estática.

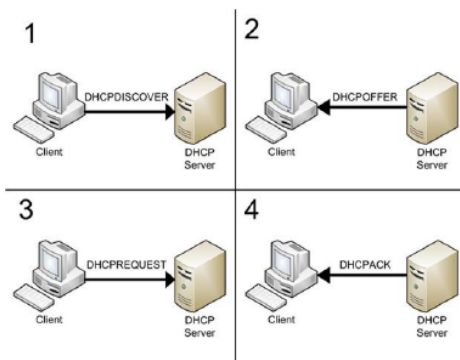


Funcionamiento del protocolo DHCP

- Un cliente obtiene los parámetros de red válidos para que se pueda conectar a la red.
- Usa la capa de transporte con el protocolo **UDP** (evita usar TCP que es más lento por el establecimiento de conexión) usando el **puerto 68** para **enviar** datos y el **67** para **recibir**.
- De este modo el cliente enviará por difusión una petición de dirección IP a los posibles servidores que se encuentren a la escucha en la red. A su vez, estos remitirán su respuesta utilizando como medio un paquete que contenga una IP válida.

Funcionamiento DHCP (Solicitud de IP)

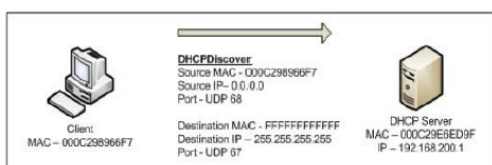
Para que el servicio de DHCP funcione, tanto en servidor como en cliente, deben enviarse varios mensajes el uno al otro para la correcta comunicación y asignación de las direcciones.



Estructura del protocolo

El modo de funcionamiento más sencillo para un cliente que no dispone de dirección IP se denomina ciclo básico DHCP y consta de cuatro mensajes que se detallan a continuación:

1. El cliente emite un mensaje **DHCP DISCOVER** por **difusión** para poder descubrir si existe algún servidor DHCP a la escucha en la subred. En él podría incluir su dirección MAC y el tiempo de concesión requerido.
 - El cliente hace un broadcast de un mensaje DHCP DISCOVER en su subred física que llega al servidor DHCP



2. Los servidores DHCP activos envían un mensaje **DHCP OFFER**, donde **ofrecen una configuración IP** al cliente, es decir, una dirección libre.
 - Cada servidor puede responder con un mensaje **DHCP OFFER** que incluye una dirección de red disponible y otras opciones de configuración.
 - El cliente recibe uno o más mensajes **DHCP OFFER** de uno o más servidores y elige uno basándose en los parámetros de configuración. Hace un **broadcast** de un mensaje **DHCP REQUEST** que incluye la opción identificadora del servidor para indicar qué **mensaje ha seleccionado**.
3. El cliente manda por **difusión (broadcast)** la primera **oferta aceptada** a todos los **servidores DHCP**. Esto lo hace a través de un mensaje por difusión **DHCP REQUEST** que debe incluir el identificador del servidor elegido y la dirección IP ofrecida. Así, se declinan las demás ofertas.
 - Los servidores reciben el broadcast de DHCP REQUEST del cliente. Los servidores no seleccionados utilizan el mensaje como notificación que el cliente ha obtenido dirección de otro servidor. El servidor seleccionado, vincula al cliente al almacenamiento y responde con un mensaje DHCP ACK.
4. El servidor seleccionado indica que se **acepta la petición solicitada** enviando un mensaje **DHCP ACKNOWLEDGE**
 - El **servidor** seleccionado **vincula la IP al cliente** y **responde** con un mensaje **DHCP ACK** que contiene los parámetros de configuración para el cliente.
 - El campo "your IP address" en los mensaje **DHCP ACK** se rellena con la dirección de red seleccionada
 - El **cliente recibe** el mensaje **DHCP ACK** con **parámetros de configuración**. Realiza un chequeo final de estos parámetros y registra la duración del arrendamiento y la cookie de identificación de éste especificado en el mensaje **DHCP ACK**. En este punto, el cliente está configurado.
 - Si el cliente recibe un mensaje DHCPNAK, el cliente reinicia el proceso de configuración.
5. DHCP DECLINE (opcional)
 - Si el cliente detectase un problema con los parámetros en el mensaje DHCP ACK, enviaría un mensaje DHCP DECLINE al servidor y reinicia el proceso de configuración. El cliente espera al menos diez segundos antes de reiniciar este proceso para evitar un exceso de tráfico en la red en caso de que se produzca algún bucle.

Renovación de la concesión

Cuando se acepta el DHCP ACK proveniente del servidor DHCP, se colocan tres valores de temporización y el cliente DHCP se mueve al estado BOUND (asociado).

- T1 → temporizador de renovación de alquiler
- T2 → temporizador de reenganche
- T3 → duración del alquiler

El DHCP ACK siempre trae consigo el valor de T3. Los valores de T1 y T2 se configuran en el servidor DHCP; de no ser así, se usan los valores por defecto siguientes:

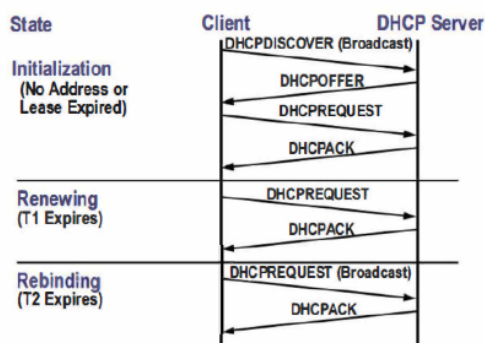
- $T1 = 0,5 * T3$

- $T2 = 0,875 * T3$

El tiempo actual en que los temporizadores expiran se calcula añadiendo el valor del temporizador al tiempo en que se envió el mensaje DHCP REQUEST, el cual generó la respuesta DHCP ACK.

- La RFC 2131 recomienda añadir un factor a T1 y T2 para evitar que varios clientes DHCP expiren sus temporizadores al mismo tiempo.

Mensajes DHCP



Todos los mensajes DHCP

Los mensajes en verde son ordenes enviadas por el cliente y en azul son enviadas por el servidor.

Mensaje	Descripción
DHCP DISCOVER	Mensaje que envía el cliente en una trama de difusión para detectar los servidores DHCP activos en la red
DHCP OFFER	Mensaje de respuesta del servidor hacia el cliente como respuesta a un DHCP DISCOVER que incluye una oferta de configuración (parámetros).
DHCP REQUEST	Mensaje para aceptar la configuración propuesta (acepta la oferta de un servidor determinado y rechaza el resto de ofertas recibidas).
DHCP ACK	Mensaje para confirmar la configuración asignada
DHCP RENEW	Mensaje utilizado para solicitar una renovación del tiempo de concesión de la IP
DHCP RELEASE	Mensaje para indicar que la IP queda libre
DHCP NACK	Indica al cliente que su dirección IP ya no es valida, por que ha finalizado el tiempo de concesión.
DHCP DECLINE	Mensaje del cliente que indica al servidor que la IP asignada ya esta en uso
DHCP INFORM	Mensaje del cliente al servidor DHCP para consultar los parámetros de configuración local. Cuando se envía, el cliente ya esta configurado.

Servidor autorizado DHCP

Un servidor DHCP no autorizado o mal configurado puede causar problemas.

- Ej: un servidor DHCP no autorizado, podría empezar a conceder direcciones IP incorrectas a los clientes o a confirmar de forma negativa los clientes DHCP que intenten renovar las concesiones actuales de direcciones IP.

Los servidores DHCP pertenecientes a una red de dominio comprueban en el **controlador de dominio si están autorizados**. Si lo están, inician el servicio y si no lo están no inician el servicio.

Por tanto, en un entorno de red de dominio, para que se pueda **iniciar un servidor DHCP** hay que:

- Instalar y configurar el servidor.
- Autorizar al servidor en el controlador de dominio
- Cuando hay dos o más servidores, se encarga de ofrecer las direcciones IP y, en caso de que algún cliente tenga una IP no válida en la subred, procederá a enviarle un mensaje DHCP NACKNOWLEDGE para que deje de utilizarla.

Configuración dinámica sin servidor DHCP

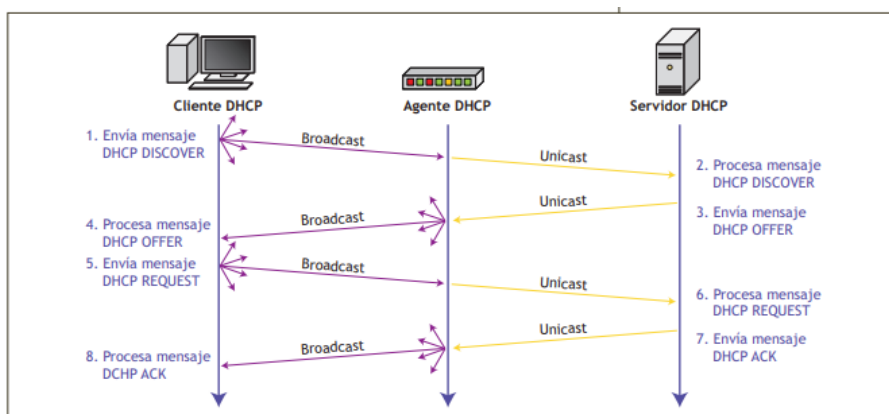
En ocasiones, un fallo inesperado en un switch puede impedir el acceso al servidor DHCP.

- En este caso, el sistema operativo asignará automáticamente una dirección IP en el rango 169.254.0.1-169.254.255.254 con una máscara de subred de clase B: 255.255.0.0. Este tipo de asignación se conoce como **APIPA** (Automatic Private IP Addressing).
- APIPA es un método de autoconfiguración creado por el IETF para redes sin servidor DHCP, permitiendo la asignación dinámica de direcciones IP.
- El paquete avahi-autoipd es el encargado de gestionar esa situación en GNU/Linux, mientras que Microsoft tiene previsto ese escenario en su implementación interna del protocolo TCP/IP

Servicio DHCP a varias redes: Agente Relay DHCP

El **Agente Relay DHCP** es un equipo o router configurado para escuchar broadcast DHCP/BOOTP de clientes DHCP y reenviar esos mensajes a los DHCP Servers en diferentes subredes.

- Los clientes **DHCP utilizan broadcasts** para obtener el lease del DHCP Server, pero los Routers normalmente **no dejan pasar** tráfico con direcciones **IP de broadcast** excepto que estén configurados específicamente para **dejarlos pasar**.
- Por lo tanto, sin configuración adicional, los **DHCP Servers** solo proveen direcciones **IP a clientes en su subred local**.
- Para que se puedan asignar direcciones a clientes en otros segmentos, se debe configurar la red para que los DHCP broadcasts puedan llegar desde el cliente al DHCP Server.
- Esto se puede hacer de dos maneras: configurando los routers que conectan las subredes para dejar pasar DHCP broadcasts, o configurando Agente Relay DHCP.



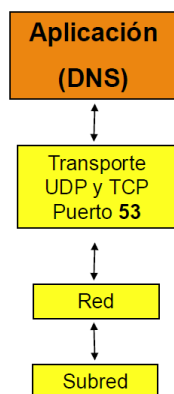
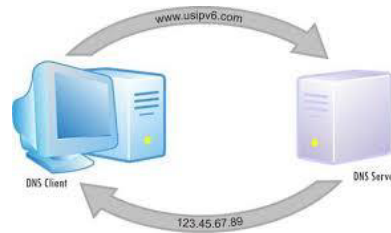
Cómo funciona el agente relay DHCP

Si el cliente realiza una petición de IP, el Agente Relay DHCP cogerá la petición y se la enviará mediante un mensaje unicast al servidor DHCP, el cual se encuentra en otra red, que le devolverá la dirección MAC y la IP asociada, que el Relay DHCP enviará por broadcast a toda su red.

¿En qué consiste el servicio DNS?

El Sistema de Nombres de Dominio (DNS) facilita la identificación de recursos en redes TCP/IP al asociar direcciones IP complejas (IPv4 o IPv6) con nombres de dominio simples. Así, en lugar de recordar direcciones numéricas, los usuarios emplean nombres fáciles de reconocer (por ejemplo, el IP 192.168.33.93 se puede identificar como `1600.jcolonia.local`). El protocolo DNS opera en la capa de aplicación y utiliza el puerto 53.

Un servidor de nombres de dominio NS (Name Server) es un host que dispone de software capaz de responder a las peticiones que le formule un cliente DNS. El cliente DNS le proporciona un nombre articulado (nombre DNS) y espera como respuesta la IP de ese nombre.



Componentes del servicio DNS

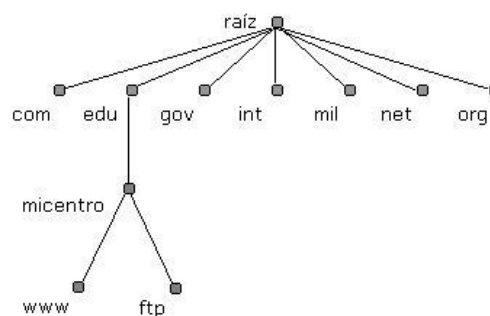
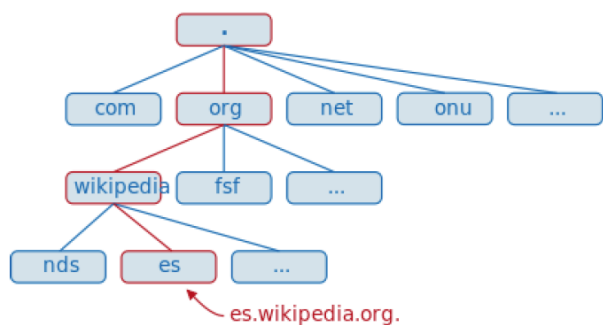
Espacio de nombres de dominio

Organiza jerárquicamente los nombres de dominio (nodos en redes TCP/IP) de manera jerárquica, formando una estructura de árbol invertido.

Este sistema permite gestionar nombres agrupados por criterios específicos, como en un sistema de archivos o una lista telefónica.

La jerarquía inicia en un nodo raíz (nivel cero), y generalmente se usan hasta cinco niveles en total; por ejemplo, en "www.juandecolonia.es" se emplean tres niveles.

- El nombre completo de un dominio se denomina FQDN (Fully Qualified Domain Name).
- Toda la estructura de nombres bajo DNS se llama "espacio de nombres de dominio".



- Ejemplo nombres de dominio
 - Pc1.ElRegional.es = . → es → ElRegional → Pc1
 - Cpd.unesco.org = . → org → unesco → Cpd
 - daw2.localhost = . → localhost → daw2
- Ejemplo de nombres de servicios
 - www.google.com = . → com → google → www
 - ftp.elregional.es = . → elregional → ftp

El nivel superior de dominios (TLD) se organiza en tres categorías:

- **Genéricos (gTLD)** incluyen:
 - .com para organizaciones comerciales
 - .edu para entidades educativas universitarias
 - .net para empresas de Internet y telecomunicaciones
 - .org para organizaciones no comerciales
 - .gov para agencias gubernamentales de EE.UU.
- **De país (ccTLD)** utilizan dos letras para representar países, como .es para España.
- **De propósito específico** incluye dominios como .arpa (infraestructura) y otros reservados como .localhost y .test.

Clasificación	TLD	Porcentaje de sitios web que usan TLD
1	.com	52.8%
2	.org	4.4%
3	.ru	4.2%
4	.net	3.1%
5	.uk	1.8%
6	.au	1.8%
7	.in	1.7%
8	.de	1.6%
9	.ir	1.5%
10	.ca	1.1%

Dominios de nivel superior (TLD) más populares

El ICANN es el organismo responsable de gestionar los dominios raíz y de nivel superior (TLDs), y desde 2004 permite registrar dominios con caracteres internacionales (IDN).

A nivel de país, el NIC (Network Information Center) es la autoridad que gestiona los dominios, y en España esta función la realiza **Red.es**, una entidad pública vinculada al Ministerio de Economía y Empresa. Para registrar un dominio .es, se debe hacer a través de **Red.es** o de empresas registradoras autorizadas.

Base de datos distribuida

La base de datos DNS consiste en archivos de zona distribuidos entre varios servidores de nombres, lo que la hace redundante y distribuida. Estos archivos de zona pueden ser archivos de texto plano o bases de datos estructuradas (como en tablas relacionales), según el tipo y configuración del servidor. Los archivos de zona almacenan su información en registros de recursos (RR), y cada zona corresponde a un dominio o subdominio.

Tipos de zonas:

Directas

Inversas

```
GNU nano 2.2.6 Archivo: /etc/bind/db.online.edu
;
; BIND data file for local loopback interface
$TTL 604800
@ IN SOA online.edu. root.online.edu. (
    3
    604800
    86400
    2419200
    604800 )
;
@ IN NS dns.online.edu.
@ IN MX 10 mail.online.edu.
;HOSTS
dns IN A 192.168.201.65
mail IN A 192.168.201.65
w7 IN A 192.168.201.66
```

```
;
; BIND reverse data file for local loopback interface
$TTL 604800
@ IN SOA webebre.net. root.webebre.net. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS webebre.net.
1 IN PTR webebre.net.
1 IN PTR dns.webebre.net.
10 IN PTR dns2.webebre.net.
2 IN PTR pc1.webebre.net.
3 IN PTR pc2.webebre.net.
```

Servidores de nombres

Los servidores DNS (Name Servers) almacenan información de dominio y responden a consultas de clientes DNS (resolvers).

Protocolo DNS

Define cómo los clientes y servidores DNS interactúan para resolver nombres de dominio en direcciones IP.

Estructura de un registro de recurso (RR)

Un **registro de recurso (RR)** en DNS es una entrada que contiene información sobre un dominio y se compone de varios campos:

- **Nombre de dominio:** dominio asociado al RR.
- **TTL:** tiempo de vida en caché del registro (opcional).
- **Clase:** identifica el protocolo, generalmente IN para TCP/IP.
- **Tipo:** tipo de recurso, que puede ser A, PTR, CNAME, SOA, NS, SRV, MX, entre otros.
- **Datos:** información relevante al dominio, que varía según el tipo de registro.

Tipos de registros de recursos (RR)

- **SOA (Start Of Authority):** Este es el registro principal de una zona y designa el servidor NS con autoridad sobre la misma, siendo la fuente más confiable de información para todos los registros en esa zona.
- **NS (Name Server):** Define los servidores de nombres autorizados para una zona. Se recomienda tener al menos dos: un servidor primario y uno secundario, para asegurar redundancia y disponibilidad.
- **A (Address) o registro de host:** Vincula un nombre de dominio totalmente cualificado (FQDN) con una dirección IP específica, lo que permite la resolución directa de nombres a IPs. Para IPv6, se usa el registro **AAAA**.
- **CNAME (Canonical Name):** Crea un alias para un dominio, lo cual permite utilizar múltiples nombres diferentes para un mismo servidor al vincularlos a un registro de tipo A o AAAA.
- **MX (Mail Exchange):** Determina el servidor de correo de un dominio, permitiendo la entrega de emails a través de servidores específicos.
- **PTR (Pointer Record):** Asocia una dirección IP con un nombre de dominio FQDN y se utiliza para la resolución inversa, transformando direcciones IP en nombres de dominio.
- **SRV (Service Record):** Identifica servidores que proporcionan servicios específicos dentro de la red, como el de mensajería instantánea o voz sobre IP (VoIP).

Nota: Para configurar un servidor de nombres (NS) en una zona, es necesario incluir tanto un registro NS como un registro A en esa zona directa.

Añadir registro

La configuración de DNS de IONOS está inactiva cuando se está usando un servidor de nombres propio. Cuando usa el DNS secundario, la configuración DNS de IONOS está inactiva.

<input type="checkbox"/>	TIPO	NOMBRE DE HOST	VALOR	SERVICIO ▲	ACCIONES
<input type="checkbox"/>	CNAME	_domainconnect	_domainconnect.1and1.com	Domain Connect	 
<input type="checkbox"/>	MX	@	mx00.ionos.es	Mail	 
<input type="checkbox"/>	MX	@	mx01.ionos.es	Mail	 
<input type="checkbox"/>	CNAME	autodiscover	adsredir.ionos.info	Mail	  
<input type="checkbox"/>	A	@	212.227.247.208	Webhosting	 
<input type="checkbox"/>	AAAA	@	2001:8d8:1000:801e:43dd:bc0d:4755:480f	Webhosting	  
<input type="checkbox"/>	A	www	212.227.247.208	Webhosting	  
<input type="checkbox"/>	AAAA	www	2001:8d8:1000:801e:43dd:bc0d:4755:480f	Webhosting	  

 > Dominios & SSL > yises.com

Añadir registro DNS

A	Asigne una dirección IPv4 a su dominio o subdominio.	>
AAAA	Asigne una dirección IPv6 a su dominio o subdominio.	>
CAA	Defina un proveedor SSL para su dominio para proteger su sitio web contra el uso indebido de certificados.	>
CNAME	Cree un alias para otro dominio o sitio web. Solo para subdominios. Para el dominio principal, use la función > Redireccionamiento	>
MX	Asigne un servidor de correo a su dominio o subdominio.	>
NS	Asigne un servidor DNS alternativo a un subdominio. Solo para subdominios. Para el dominio principal, use los > Servidor DNS	>
SRV	Defina una herramienta de conexión de servicio para su dominio, como Jabber o Lync.	>
IONOS SPF (TXT)	Identifique a la red de IONOS como remitente legítimo de sus correos electrónicos. Aumente la confianza del destinatario.	>
SPF (TXT)	Defina libremente qué servidores pueden enviar sus correos electrónicos.	>
TXT	Añada información textual a su dominio o subdominio, como DMARC o DKIM.	>

Servidores DNS

Servidores autorizados: almacenan la información completa de una zona.

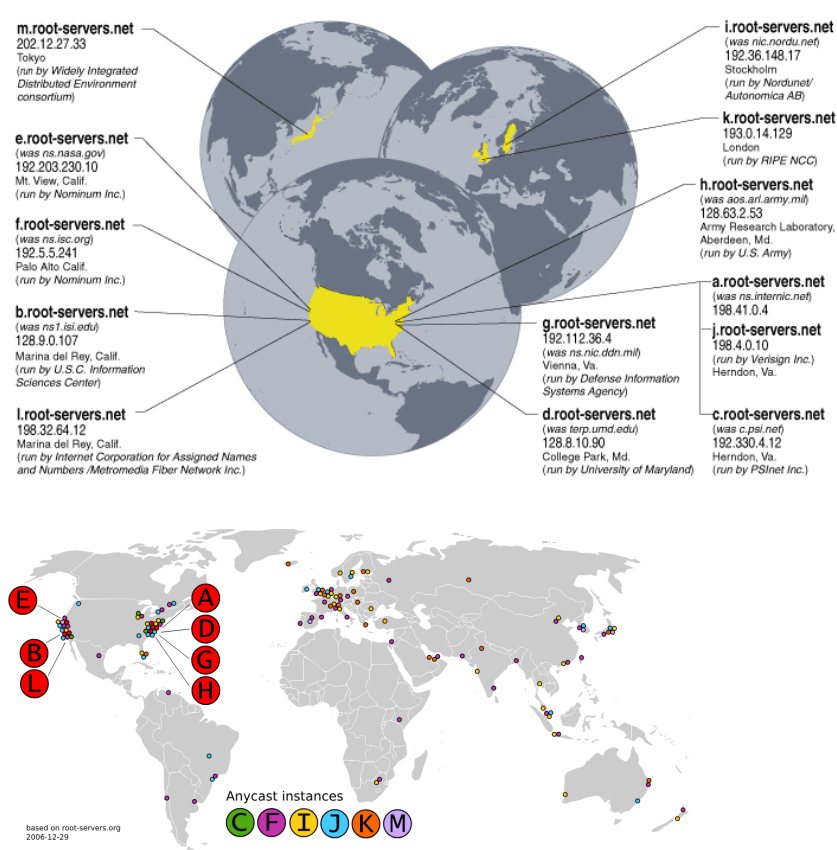
- **Servidores raíz:** gestionan el dominio raíz "." y contienen la información de los servidores DNS para cada dominio TLD.
- **Servidor primario o maestro:** permite la edición de archivos de zona por el administrador, quien puede agregar, modificar o eliminar registros de recursos (RR).
- **Servidor secundario o esclavo:** recibe copias de los archivos de zona desde el servidor primario, pero sólo los lee (transferencia de zona).

Servidores no autorizados no almacenan zonas para resolver consultas.

- **Reenviadores:** redirigen las consultas que no pueden resolver a otros servidores y generalmente son servidores de caché, que construyen una base de datos a partir de consultas previas.

Ubicación servidores raíz (root)

La **sugerencia de raíz** es un registro de recurso (RR) que ayuda a localizar la IP de los servidores DNS raíz. En Windows, se guarda en `c:\windows\system32\dns\cache.dns` y puede actualizarse mediante el archivo `named.root` disponible en [ftp.internic.net](ftp://ftp.internic.net).



Servidor primario y servidor secundario

1. El servidor DNS preferido es aquél con el que el cliente prueba en primer lugar


2. Si el servidor preferido falla, el cliente prueba con el servidor DNS alternativo

3. Opcionalmente, puede especificar una lista completa de servidores DNS alternativos

4. Los servidores DNS preferidos y alternativos especificados en la página de Propiedades aparecen automáticamente en la parte superior de esta lista, y los servidores preferidos y alternativos se consultan en el orden en el que aparecen en la lista

Transferencia de zona

La **transferencia de zona** es el proceso de copiar los datos de una zona desde un servidor DNS primario a uno secundario, permitiendo que el secundario aloje una copia.



Este diagrama ilustra la replicación de datos entre dos servidores. A la izquierda se encuentra el 'Servidor secundario' y a la derecha el 'Servidor primario'. Ambos están representados como unidades de almacenamiento en un círculo amarillo. Entre ellos hay dos flechas rojas horizontales: la superior apunta de izquierda a derecha, indicando la replicación de datos desde el secundario al primario, y la inferior apunta de derecha a izquierda, indicando la replicación de datos desde el primario al secundario.

La **delegación de zona** permite distribuir la gestión de un dominio extenso con muchos subdominios, asignando algunos subdominios a otros servidores DNS primarios.

Un dominio puede subdividirse sin ceder la autoridad sobre los subdominios, pero también puede optar por delegarla para algunos de ellos si así se decide.

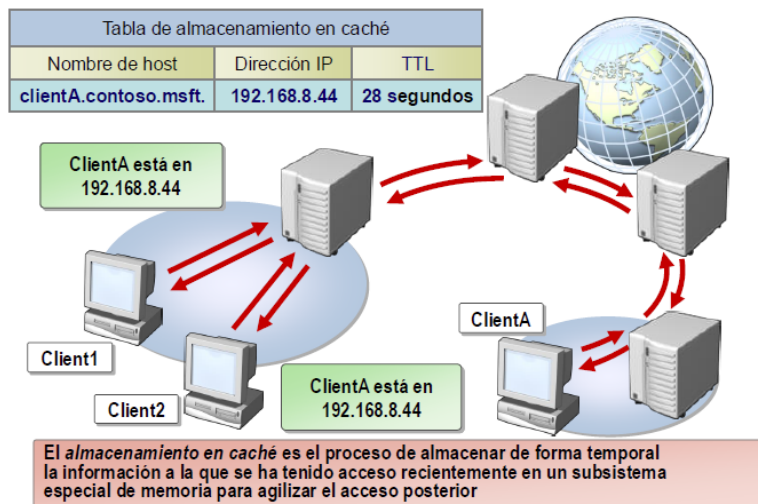


The diagram illustrates the recursive DNS resolution process for the domain `juandecolonia.edu`. It shows the following components and interactions:

- Computer1:** The local client initiating the request.
- Servidor DNS local:** The local DNS server that receives the recursive query from Computer1.
- Root Hint (.):** The root of the DNS hierarchy.
- .edu:** The authoritative server for the `.edu` top-level domain.
- Juandecolonia.edu:** The authoritative server for the `juandecolonia.edu` domain.

The resolution process follows these steps:

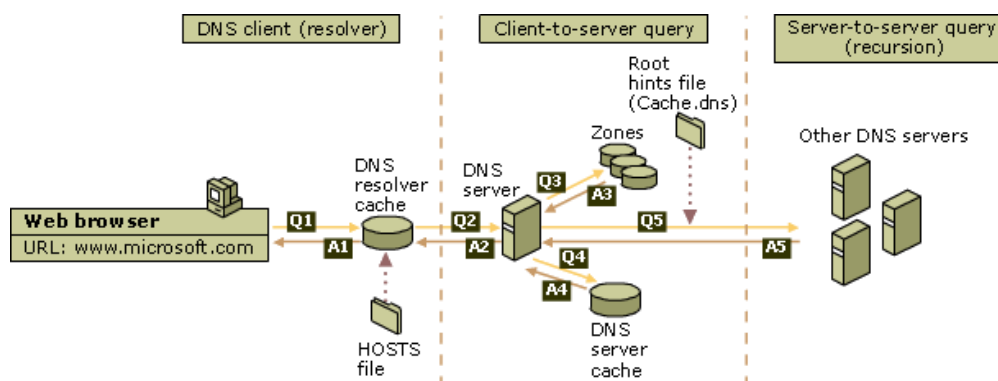
- Computer1 sends a **Consulta recursiva para `www.juandecolonia.edu`** to the Servidor DNS local.
- The Servidor DNS local sends an **Consulta iterativa** to the Root Hint (.), asking to **Preguntar `.edu`**.
- The Root Hint (.) responds with an **Consulta iterativa** to the `.edu` server, asking to **Preguntar `juandecolonia.edu`**.
- The `.edu` server responds with an **Consulta iterativa** to the `Juandecolonia.edu` server, asking to **Preguntar `juandecolonia.edu`**.
- The `Juandecolonia.edu` server returns a **Respuesta autorizada** (authoritative answer) containing the IP address `172.16.64.11`.
- The Servidor DNS local receives the IP address and returns the **Consulta recursiva** to Computer1, providing the IP address `172.16.64.11`.



Proceso de resolución de nombres

- Verificación local:** Primero, el cliente busca la IP en su caché DNS (accesible mediante `ipconfig /displaydns`) o en el archivo hosts (`c:\windows\system32\drivers\etc\hosts`), que se carga al iniciar el cliente DNS.
- Consulta al servidor DNS:** Si no encuentra la IP localmente, envía un mensaje UDP al servidor DNS configurado (primario o secundario). Este servidor realiza varias acciones:
 - Consulta sus propios registros de recursos (RR).
 - Verifica su caché local.
 - Si no encuentra la información, puede reenviar la consulta a otros servidores DNS. Esto puede ser de forma recursiva, si consulta a servidores raíz, o iterativa, si utiliza servidores reenviadores.

Proceso de consultas DNS completo



- (Q1)** El cliente intenta resolver la consulta localmente verificando su caché.
- (Q2)** Si no tiene la información, consulta al servidor DNS preferido.
- (Q3)** El servidor DNS verifica si tiene autoridad sobre la zona del dominio solicitado.
- (Q4)** Si no tiene autoridad, busca la información en su propia caché.
- (Q5)** Si no encuentra la respuesta, consulta a otros servidores, ya sea a los servidores raíz (para los que tiene sugerencias en su archivo `cache.dns`) o a servidores reenviadores.

Búsqueda directa e inversa

- **Búsqueda directa:** Consulta que permite localizar la IP asociada a un nombre de dominio.
- **Búsqueda inversa:** Consulta que permite encontrar el nombre de dominio correspondiente a una dirección IP.

