

Introducción a Redes

Módulo 5

Servicios de red

Identificación de hosts en la red:

Servicio WINS y NETBIOS

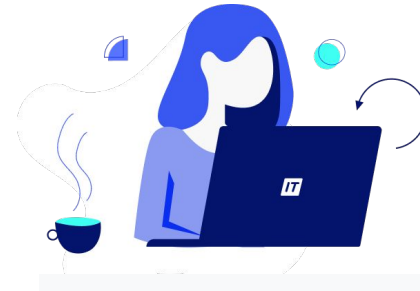
En el caso de las redes con hosts que ejecutan windows existen dos tipos de servicios que se encargan de anunciar al host e identificar un host en la red, veamos:



- **NetBIOS:** este servicio identifica un host bajo un nombre, es decir el **nombre de host**.
- **WINS: *Windows Internet Naming Service*** (WINS) es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red.

Los servicios de “anuncio de servicios” (carpetas e impresoras compartidas, etc.) y “nombres de hosts” informaran a todos los equipos de la red que sean compatibles el nombre propio y su dirección IP. El resto de los hosts mediante el servicio WINS tomarán nota del nombre de host y la dirección IP que le corresponde a cada equipo que se anuncie. Luego podemos referirnos a cualquier host por su IP o nombre de host.

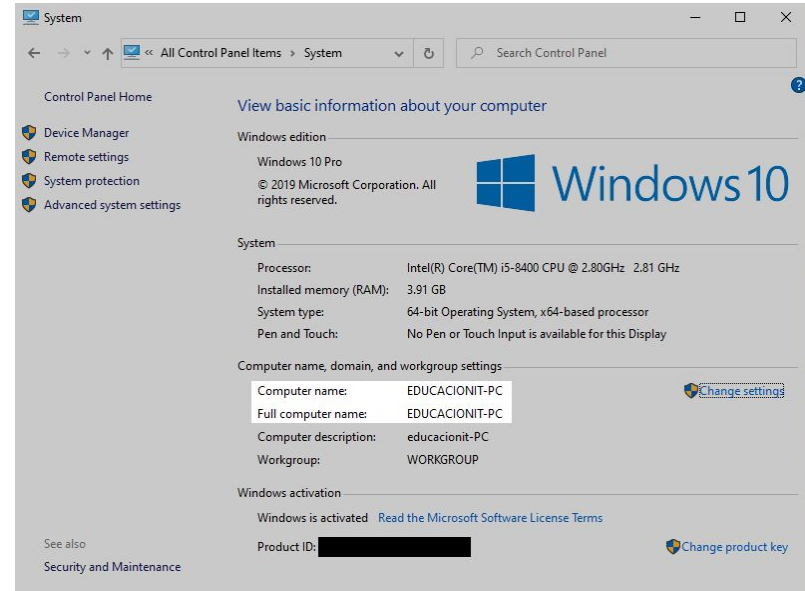
Muchas veces no existe compatibilidad entre sistemas operativos distintos, como el caso de linux y windows, pero en general dispositivos como impresoras de red trabajan con NetBIOS y WINS, es por eso que desde windows podemos visualizar una impresora por su nombre.



Nombre de host

En una red de computadoras no solo se identifican los dispositivos a partir de una dirección IP, además de la dirección los dispositivos se identifican bajo un nombre que debe ser único dentro de la red, entonces podemos “contactar” un host mediante su IP o su nombre.

El **nombre de host** se determina en el momento de instalación de un sistema operativo, en smartphones normalmente el nombre ya viene predefinido (marca y modelo), en el caso de las impresoras sucede lo mismo y en general es posible cambiar el nombre de host en cualquier momento.



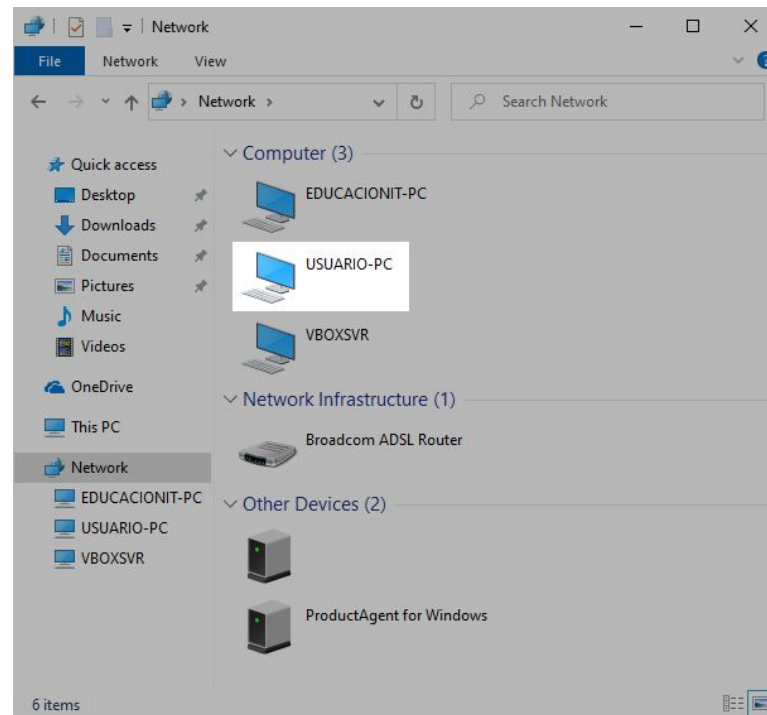
Nombre del host determinado en la etapa de instalación del SO.

Hosts y servicios descubiertos

Hosts en la red

En windows desde el navegador de archivos podemos ir a la sección red y ver los dispositivos anunciados a los que podemos acceder.

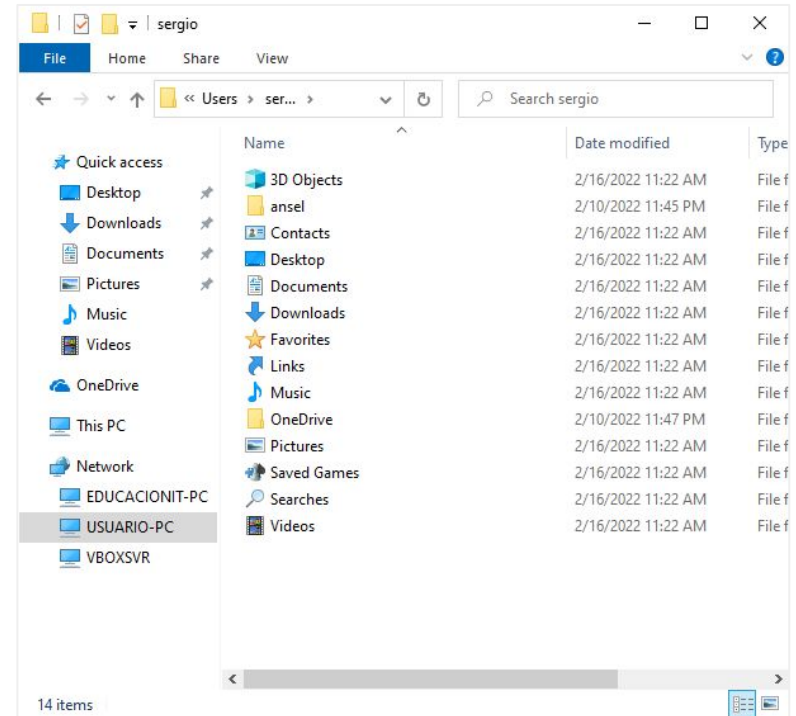
Host “USUARIO-PC” anunciado en la red.



Recursos compartidos

Ver los servicios de red que comparten los hosts descubiertos.

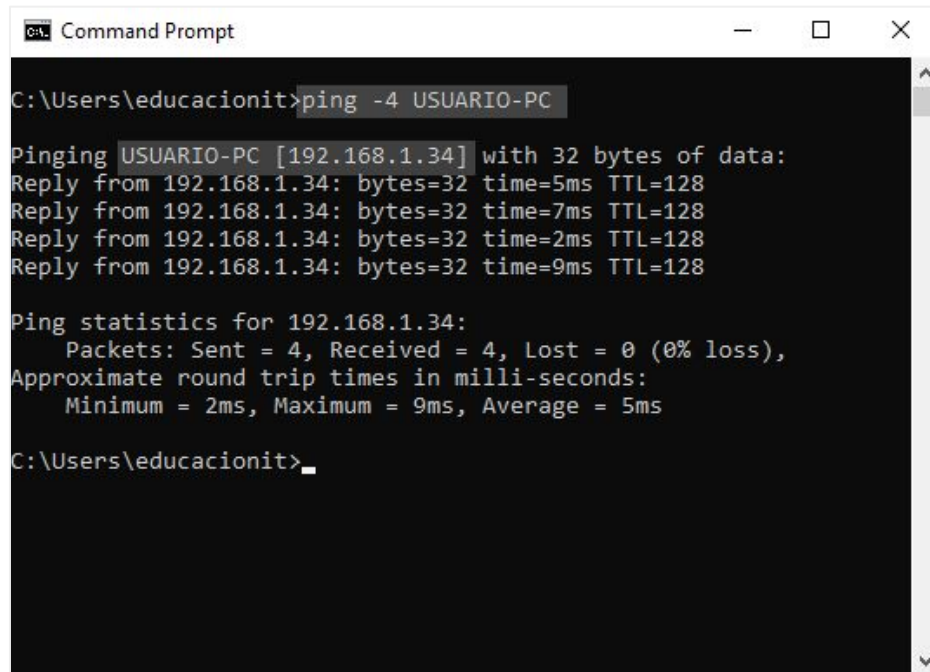
El host “USUARIO-PC” tiene compartido su directorio personal.



Herramienta PING

Utilizar la herramienta ping para probar la conexión usando el nombre de host.

Se indica el nombre del host como parámetro, el servicio WINS traduce el nombre en una IP.



```
cmd Command Prompt
C:\Users\educacionit>ping -4 USUARIO-PC

Pinging USUARIO-PC [192.168.1.34] with 32 bytes of data:
Reply from 192.168.1.34: bytes=32 time=5ms TTL=128
Reply from 192.168.1.34: bytes=32 time=7ms TTL=128
Reply from 192.168.1.34: bytes=32 time=2ms TTL=128
Reply from 192.168.1.34: bytes=32 time=9ms TTL=128

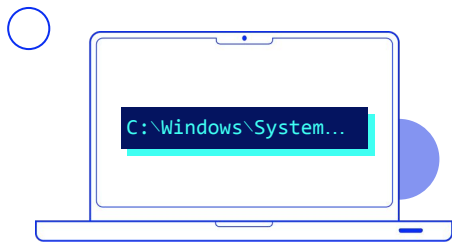
Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 5ms

C:\Users\educacionit>
```


Fichero 'hosts'

Se utiliza para **registrar los nombres de hosts** y las **direcciones IP** que les corresponden.

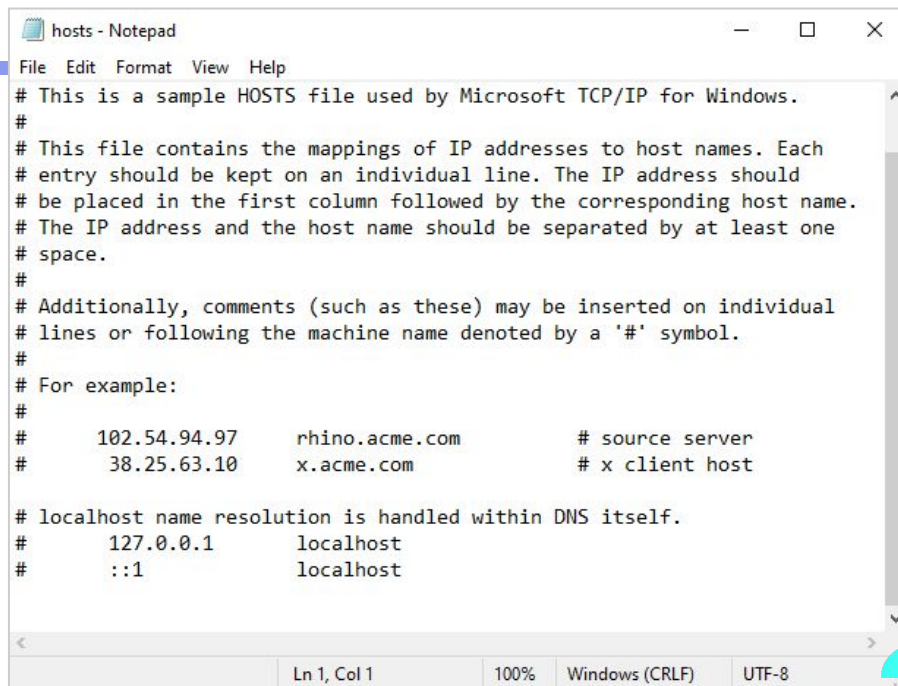
Normalmente no tenemos ninguna necesidad de modificar este archivo, los registros se actualizarán de forma dinámica a partir de los servicios NetBIOS y WINS.



Cabe mencionar que este fichero se utiliza en multitud de sistemas operativos y firmwares de dispositivos de red y tienen la misma estructura:

<dirección ip>	<nombre de host>
192.168.1.56	contabilidad
...	

En windows lo podemos encontrar en
“C:\Windows\System32\drivers\etc\hosts”.



```
hosts - Notepad
File Edit Format View Help
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

Contenido del fichero “hosts” de windows

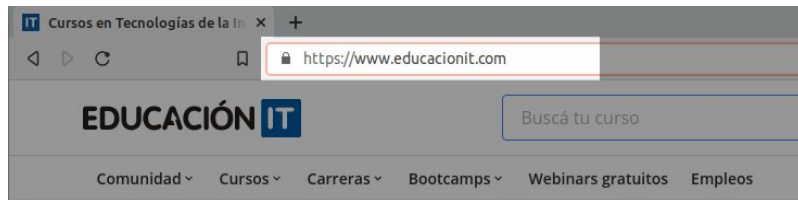
Servicio DNS

El **Sistema de Nombres de Dominio** o **DNS** se encarga de traducir nombres “amigables” para los usuarios en direcciones IP:

educacionit.com has address **54.207.106.237**

Cuando introducimos en el navegador una url esta se compone de varias partes:

- **Protocolo de aplicación:**
HTTP/HTTPS/FTP/FTPS
- **Dominio:** educacionit.com



Normalmente solo ponemos el nombre del sitio al que queremos acceder, la misma aplicación junto con el servidor determinarán el protocolo a utilizar.

Cuando introducimos una URL o el dominio en un navegador, en este caso “educacionit.com” estamos solicitando el contenido web a un servidor que aloja dicha web, veamos el proceso bajo el modelo de capas TCP/IP:

- **Capa de aplicación:** el usuario introduce el nombre del sitio “educacionit.com”, la aplicación genera un mensaje que es la solicitud de acceso a dicho sitio. El mensaje se estructura bajo el protocolo de aplicación que corresponda (HTTP o HTTPS).
- **Capa de transporte:** el mensaje se segmenta bajo el protocolo de transporte TCP, se establece la conexión de puerto a puerto (80 para http, 443 para https).
- **Capa de internetworking:** se generan los paquetes de datos y se agrega la dirección IP de destino “**54.207.106.237**”, el servidor donde se aloja el sitio.
- **Capa de acceso a la red:** se generan las tramas a partir de los paquetes de datos, estas tramas serán dirigidas al dispositivo de red que pueda llevar dicho paquete al destino, normalmente el *gateway*.

Analizando el proceso...

¿De dónde sale la dirección IP del servidor si solo indicamos el nombre del sitio “**educacionit.com**”?

En internet existe una red de miles de servidores DNS, estos servidores llevan registros de los nombres de dominios, subdominios, nombres de servidores de correo, etc. y las direcciones IP asociadas a estos tipos de registros. Cuando introducimos un dominio en un programa cliente este debe averiguar cuál es la dirección IP asociada a dicho dominio y lo hará consultando a un servidor DNS que pueda resolver la solicitud, una vez obtenida la IP se podrán enviar los mensajes al servidor correspondiente.

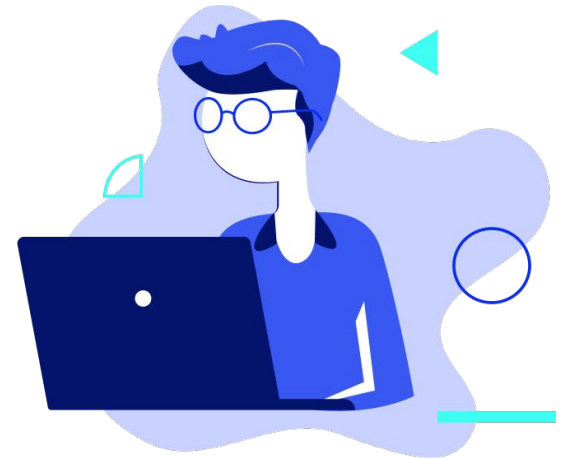
Es algo similar a lo que sucede con el nombre de host y el fichero “hosts”, pero a una escala mucho mayor, la red DNS es el sistema que nos permite conectar con cualquier host de internet a partir de un dominio registrado y propagado.



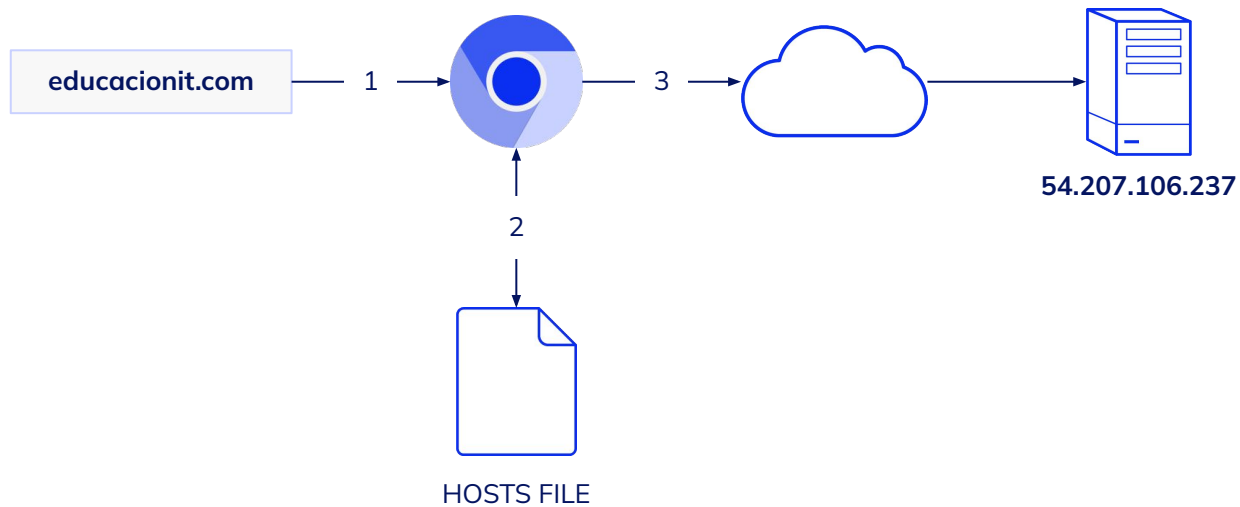
Funcionamiento

La resolución de un nombre de dominio es un proceso que puede ser complejo.

Es importante saber que las aplicaciones van a intentar obtener una dirección IP de dos maneras, por un lado buscará registros en el **fichero hosts** y, si no lo encuentra, recurrirá a un **servidor DNS**.



Fichero hosts



1. Se introduce el nombre de dominio en el navegador web.
2. Se busca un registro que relacione el nombre “educacionit.com” con una dirección IP.
3. Si este se encuentra en el fichero hosts se envía el paquete a la dirección IP asociada al registro.

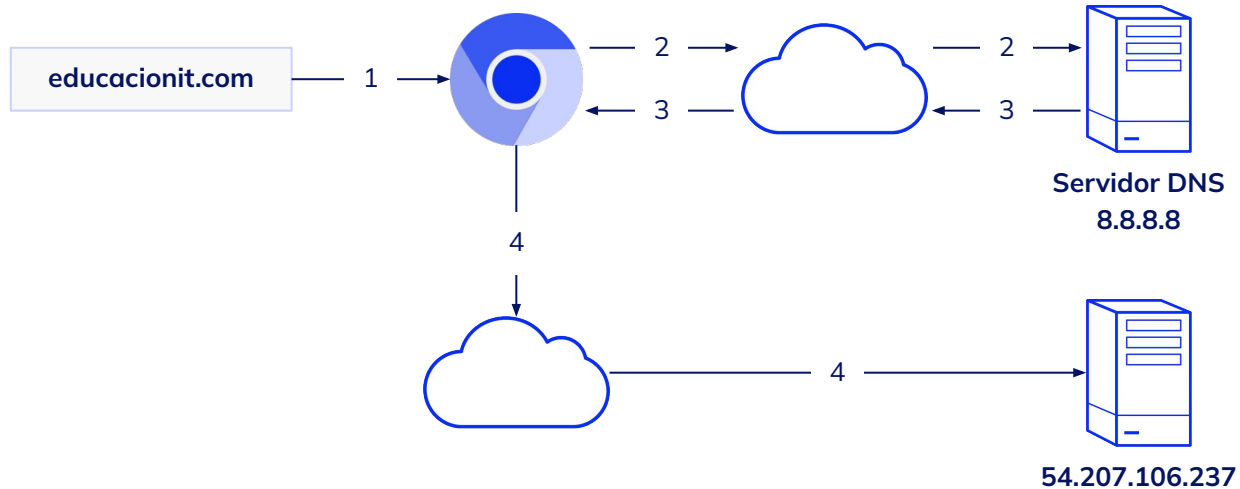
Es poco probable que en el fichero hosts exista un registro de dominios de internet.

Como vimos anteriormente en este fichero registramos direcciones de hosts dentro de la LAN en situaciones específicas, pero describiendo el proceso de resolución de nombre esto es lo que sucede primero.



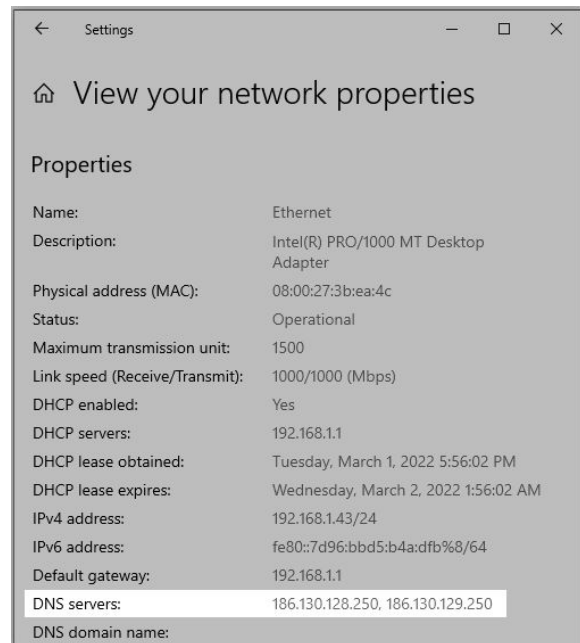
Consulta DNS

El fichero hosts, como era de esperar, no contiene ningún registro, entonces se intentará averiguar la dirección IP consultando a un servidor DNS.



1. Se introduce el nombre de dominio en el navegador web.
2. Se envía una petición de resolución de nombre de dominio a un servidor DNS de internet.
3. El servidor DNS responde con la dirección IP asociada al dominio que se intenta resolver.
4. Se envía la solicitud a la dirección IP devuelta por el servidor DNS.

Para que un host pueda resolver nombres de dominio necesita tener configurado un servidor DNS y tener acceso a él.

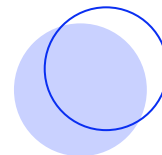


Servidores DNS configurados en el host
186.130.128.250 y 186.130.129.250.

Tipos de servidores DNS

La red de servidores DNS de internet es compleja, cada servidor tiene un rol en particular, dentro de una organización de escala global, pero estos servidores no solo existen en internet, sino también en redes LAN, WAN y MAN.

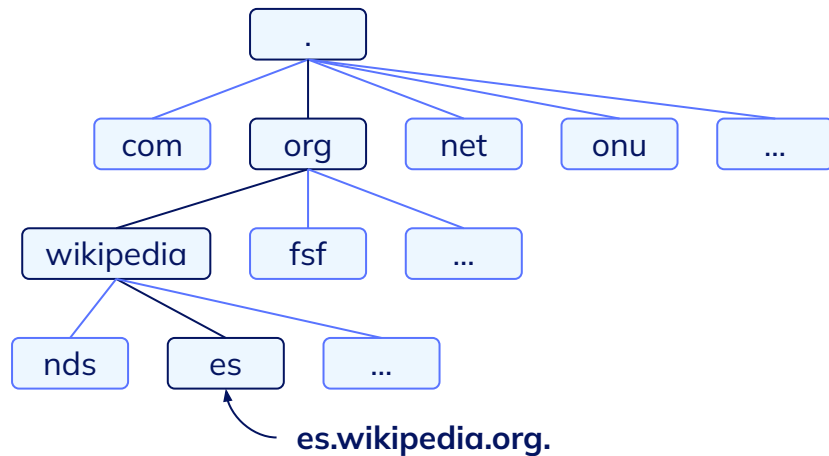
Vamos a explorar la funcionalidad de los servidores DNS según su rol.



Servidores de Nombres Dominio

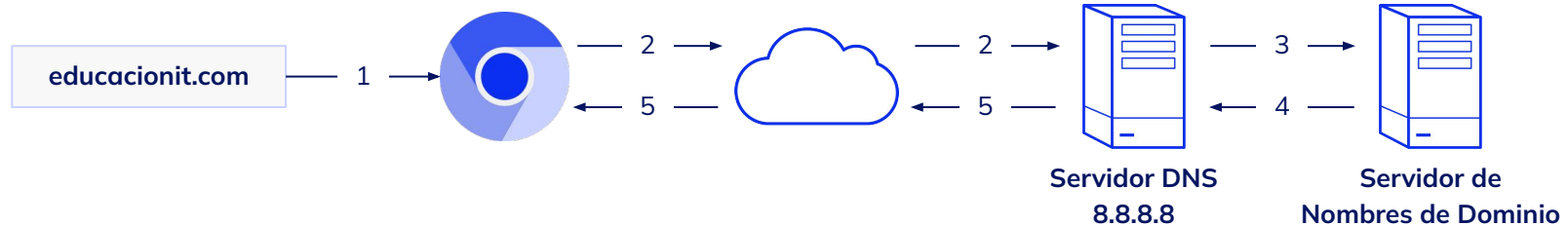
Estos servidores **guardan los registros de todos los nombres de dominios que existen en internet**, y tienen una **arquitectura jerárquica**, cada nivel sabe quien puede resolver un nombre completo.

Por ejemplo, cuando se pide “educacionit.com” los servidores que administran los “.com” indican quién puede saber el dominio completo “educacionit.com”.



Servidores de Resolución de nombres de dominio

Estos son los servidores que se encargan de resolver una petición, son los servidores que se configuran en el host.



1. Se introduce el nombre de dominio en el navegador web.
2. Se envía una petición de resolución de nombre de dominio a un servidor DNS de resolución de nombre de dominio de internet.
3. El servidor de resolución realiza la búsqueda en servidores de nombres de dominio.
4. El servidor de nombres de dominio devuelve al resolutor la información recabada.
5. El servidor de resolución de nombres entrega la dirección IP asociada al dominio que se intenta resolver.

Dentro de la infraestructura de red son los servidores de resolución los que nos van a permitir acceder al contenido web o cualquier otro servicio de red a partir de un nombre.

Dentro de una LAN se pueden colocar servidores DNS que pueden gestionar nombres de dominio que solo existen dentro de la LAN, por ejemplo “servidor-nas.intranet”.



DNS CACHE

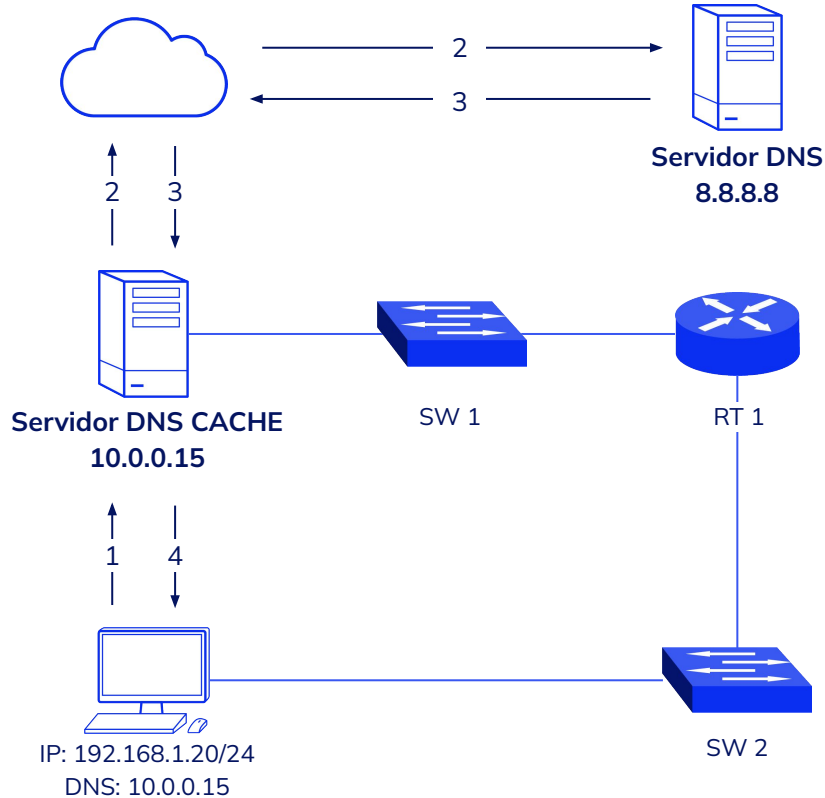
Los servidores pueden estar dentro de una LAN o ser accesibles desde internet, vamos a poner el foco a **servidores DNS dentro de una LAN**.

El propósito de tener un servidor DNS en una LAN es **evitar el uso de internet**. Imaginemos que cada host de la red haga las peticiones a un servidor de internet por cada sitio al que accede, estaríamos utilizando el ancho de banda de la conexión a internet, cuantos más hosts y más peticiones más ancho de banda es necesario y esto se suma a el resto del tráfico que pasa por dicha conexión.

En un red con salida a internet lo que se busca es minimizar el tráfico, todo aquello que se pueda

resolver de manera local evita el tráfico hacia la red pública y se economiza el ancho de banda, y por otra parte tenemos el beneficio de los tiempos de respuesta, es **más rápido realizar una consulta a un servidor local que a uno de internet**.

Bajo esta premisa entran en juego los **servidores DNS Caché, que actúan como servidores de resolución de nombres de dominio** y por cada consulta **guarda en una caché las respuestas**, en consultas posteriores para el mismo dominio no los buscara en internet, sino que responderá con lo que tenga registrado en la caché.



1. El host 192.168.1.20 envía un solicitud de resolución al servidor DNS Caché local.
 2. El servidor 10.0.0.15 realiza la resolución con un servidor de internet.
 3. El servidor de internet devuelve toda la información solicitada.
 4. El servidor DNS Caché local entrega al host la dirección IP del dominio a consultar.
- En el futuro cuando el host realice la misma consulta el servidor DNS Caché responderá con lo que tenga almacenado sin recurrir al servidor de internet. Esta información queda guardada un tiempo predefinido, luego se vuelve a repetir el proceso.

Servidores de resolución públicos y privados

Los servidores DNS de internet pueden ser públicos o privados, esto básicamente define quiénes pueden usar un servidor DNS.



Servidores públicos

Son los servidores de internet que **cualquiera puede usar** tanto en la propia computadora como para todos los hosts y servidores dentro de una red LAN, estos servidores forman parte del conglomerado DNS.

A la derecha vemos una lista de servidores DNS públicos.

- DNS de Google primaria: 8.8.8.8
- DNS de Google secundaria: 8.8.4.4
- DNS de OpenDNS primaria: 208.67.222.222
- DNS de OpenDNS secundaria: 208.67.220.220
- DNS de Cloudflare primaria: 1.1.1.1
- DNS de Cloudflare secundaria: 1.0.0.1
- DNS de Comodo Secure DNS primaria: 8.26.56.26
- DNS de Comodo Secure DNS secundaria: 8.20.247.20
- DNS de Quad9 primaria: 9.9.9.9
- DNS de Quad9 secundaria: 149.112.112.112
- DNS de DNS.Watch primaria: 84.200.69.80
- DNS de DNS.Watch secundaria: 84.200.70.40
- DNS de AdGuard DNS primaria: 176.103.130.130
- DNS de AdGuard DNS secundaria: 176.103.130.131
- DNS de Dyn primaria: 216.146.35.35
- DNS de Dyn secundaria: 216.146.36.36

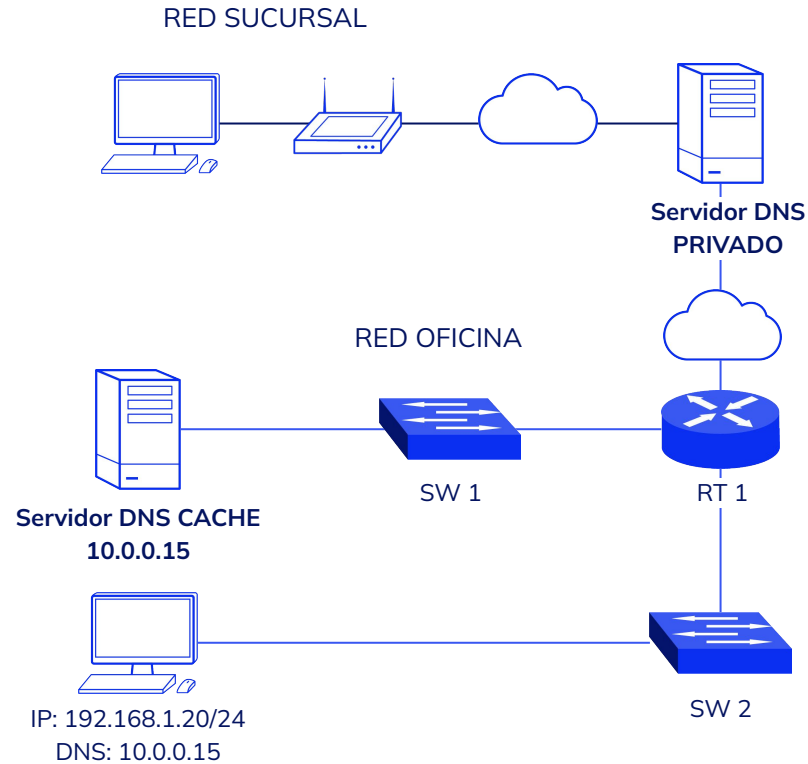
Servidores privados

Hay varios aspectos con respecto a estos servidores. Por un lado si disponemos de un servidor dentro de la LAN técnicamente estamos hablando de un servidor privado, que además puede gestionar dominios internos como “servidor-nas.intranet”. Pero en un sentido más concreto un **servidor DNS privado solo admite solicitudes de clientes predefinidos**.

Por ejemplo, normalmente en la red hogareña los servidores DNS son provistos por el ISP, pero esos servidores no pueden ser usados por cualquiera, solo los clientes del ISP. Del mismo modo hay servicios DNS de pago que ofrecen muchas características orientadas a la seguridad,

dominios privados, caché, velocidad, etc. En este tipo de servicios son admitidos los clientes que abonan una factura mensual, anual, etc. Los **servidores públicos también son servidores privados**, pero asociamos lo público a lo gratuito, los mismos servicios listados anteriormente tienen paquetes de servicios pagos.

Un último ejemplo de servidor privado es aquel que podemos instalar y configurar pero no dentro de la LAN, sino mediante la contratación de una VPS donde el administrador de sistemas instalará y configurará el servicio DNS para responder consultas a cualquier host admitido aun fuera de la red LAN.



Servicio DHCP

El **protocolo de configuración dinámica de host (DHCP)** es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Hasta el momento hemos visto como configurar distintos aspectos de red de un host:

- IP
- Máscara
- Gateway
- DNS

Siendo que la IP y la Máscara son los elementos fundamentales para que un host sea parte de una red, el resto son configuraciones importantes pero no estrictamente necesarias, si el host no precisa resolver nombres de internet, no lleva DNS; si no tiene comunicación con otras redes, no precisa de *Gateway*.

En una red puede resultar complejo y costoso tener que establecer de manera manual la configuración de red de cada host.

Para evitar esto el servicio **DHCP** es el que se encarga de **asignar un conjunto de parámetros a cada host en la red de manera automática**, siendo la IP y la Máscara las configuraciones esenciales, pero también puede asignar DNS y

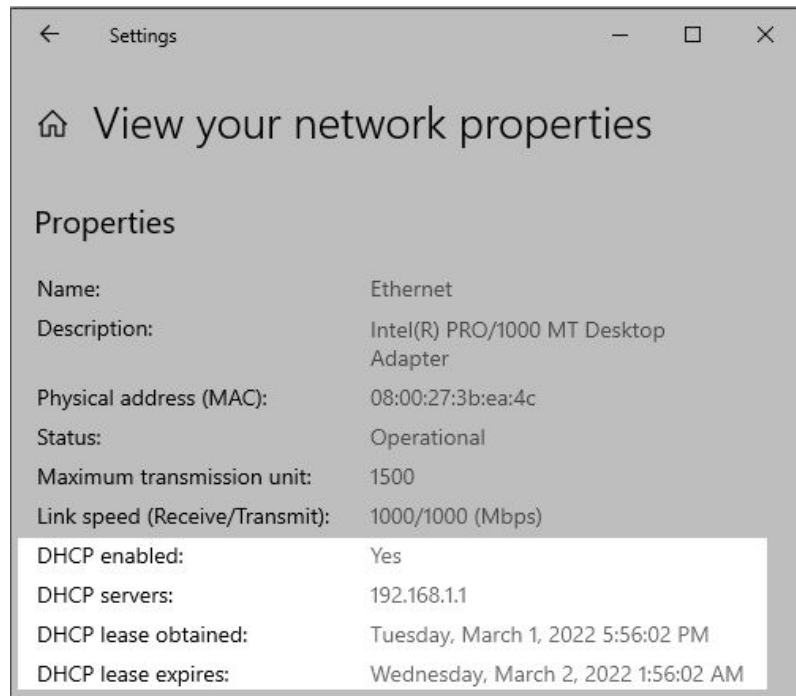
Gateway entre otros aspectos más avanzados. Los servidores DHCP son más comunes de lo que se piensa, de hecho **cada vez que conectamos un dispositivo móvil a una red wifi es el servidor DHCP de la red la que determinará la configuración de red del dispositivo**. Prácticamente todos los routers hogareños, modems provistos por el ISP, routers orientados a pequeñas empresas disponen de un servicio DHCP.



Funcionamiento

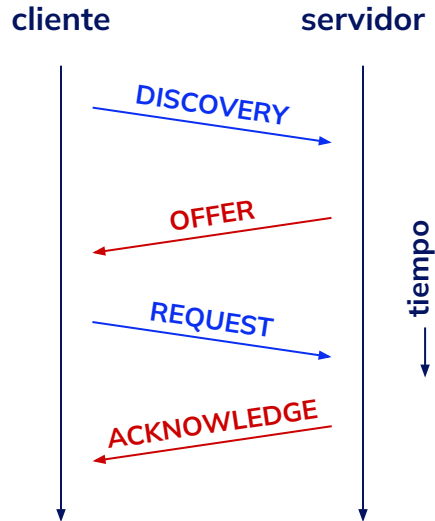
Cuando un host se enciende y se carga el sistema operativo, el cliente DHCP va a solicitar a un servidor DHCP la configuración de red, siempre y cuando el host este configurado de esa forma:

Según la imagen está activado el cliente DHCP por lo que la configuración de red es automática, el servidor DHCP es el 192.168.1.1 el “leasing” es la entrega de una dirección IP pero esta dirección no es siempre la misma para el mismo host, esta cambia cada ‘X’ cantidad de tiempo, es algo que está determinado en el servidor DHCP, pasado ese tiempo la dirección se renueva.



Obtención de IP

Cuando el host solicita una dirección se realizan una serie de pasos como se muestra aquí.



La comunicación entre cliente y servidor utiliza los puertos 67 para el servidor, 68 para el cliente y el protocolo de transporte es el UDP.

1. El cliente DHCP envía un paquete DHCPDISCOVER a la dirección 255.255.255.255 desde la dirección 0.0.0.0. Con esta denominada difusión amplia o broadcast, el cliente establece contacto con todos los integrantes de la red con el propósito de localizar servidores DHCP disponibles e informar sobre su petición. Si solo hay un servidor, entonces la configuración es extremadamente sencilla.
2. Todos los servidores DHCP que escuchan peticiones en el puerto 67 responden a la solicitud del cliente con un paquete DHCPOFFER, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.

3. El cliente DHCP escoge un paquete y contacta con el servidor correspondiente con DHCPREQUEST. El resto de servidores también reciben este mensaje de forma que quedan informados de la elección. Con esta notificación, el cliente también solicita al servidor una confirmación de los datos que le ha ofrecido. Esta respuesta también sirve para confirmar parámetros asignados previamente.
4. Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete DHCPACK (DHCP acknowledged o «reconocido»). Este paquete contiene otros datos (sobre servidores DNS, SMTP o POP3). El cliente DHCP guarda localmente los datos que ha recibido y se conecta con la red. Si el servidor no contara con ninguna dirección más que ofrecer o durante el proceso la IP fuera asignada a otro cliente, entonces respondería con DHCPNAK (DHCP not acknowledged o «no reconocido»).

Pool de direcciones

En una red todos los hosts van a compartir un conjunto de configuraciones:

- Máscara
- DNS
- Gateway

Pero cada host va a diferir en la ID de Host de su dirección IP, entendamos el concepto de DHCP como una plantilla, todos reciben la misma información pero una IP única para cada host.

En el servidor DHCP se especifica un rango de direcciones a repartir, una cantidad específica, este rango se denomina pool, cuando el pool se agota ya no puede seguir asignando direcciones.



DHCP Settings

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	<input type="text" value="192.168.1.100"/>
End IP Address:	<input type="text" value="192.168.1.199"/>
Address Lease Time:	<input type="text" value="120"/> minutes (1~2880 minutes, the default value is 120)
Default Gateway:	<input type="text" value="192.168.1.1"/> (optional)
Default Domain:	<input type="text"/> (optional)
Primary DNS:	<input type="text" value="0.0.0.0"/> (optional)
Secondary DNS:	<input type="text" value="0.0.0.0"/> (optional)

Configuración del servidor DNS router TP Link.

Como se mostró en la imagen anterior, el pool de direcciones establece que se pueden repartir IPs desde la 192.168.1.100 a la 192.168.1.199, en total 100 direcciones.

Además de las direcciones podemos configurar otros parámetros:

- Gateway
- Servidores DNS
- Lease Time
- Dominio por defecto (si hubiese un dominio de red)



Direcciones estáticas

No todos los hosts de una red obtienen direcciones dinámicas, algunos de ellos precisan tener **direcciones fijas** como es el caso de algunos hosts que ofrezcan servicios a la red externa, como por ejemplo el escritorio remoto de windows. En ese caso cuando se hace un mapeo de puertos se va a apuntar a una dirección IP que no debe cambiar nunca.

Un servidor DHCP permite la asignación de una dirección estática para un host en particular, esto se logra reservando una dirección asociándola a la MAC Address de la interfaz que va a recibir dicha dirección.

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	08-00-27-04-70-9B	192.168.1.145	Enabled	Modify Delete
2	08-00-27-04-70-9C	192.168.1.215	Enabled	Modify Delete
<div><button>Add New...</button><button>Enable All</button><button>Disable All</button><button>Delete All</button></div>				

Obviamente la forma de configurar el servidor va a depender del servidor en si mismo, por ejemplo la interfaz de usuario varía de dispositivo a dispositivo y en otros casos se realiza a través de la línea de comandos, pero en todos ellos los parámetros son los mismos.

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	08-00-27-04-70-9B	192.168.1.145	Enabled	Modify Delete
2	08-00-27-04-70-9C	192.168.1.215	Enabled	Modify Delete
<div><button>Add New...</button><button>Enable All</button><button>Disable All</button><button>Delete All</button></div>				

La forma de configurar el servidor va a depender del servidor en sí mismo, por ejemplo la interfaz de usuario varía de dispositivo a dispositivo y en otros casos se realiza a través de la línea de comandos, pero en todos ellos los parámetros son los mismos.

**¡Sigamos
trabajando!**

