DNS

Una aplicación web necesita de varios servicios de red para funcionar correctamente. Estos son DNS y LDAP (Protocolo Ligero de Acceso al Directorio).

DNS, **Domain Name System** o **Sistema de Nombres de Dominio**, es un servicio de resolución de nombres. Este servicio es imprescindible para conectar el equipo con la red exterior de la organización.

Un DNS es una base de datos jerárquica y distribuida que contiene las relaciones entre nombres de equipos, host, o sitios y su dirección ip. Un DNS hace una resolución de nombres, es decir, traduce un nombre alfanumérico como A24-PR o www.iessantiagohernandez.com en una ip numérica del tipo 216.160.0.230. Para ello está dividido en zonas, directa e inversa, que tienen registros que permiten resolver las direcciones que buscan los usuarios.

La resolución de nombre es importante porque los equipos necesitan una ip para comunicarse entre ellos y las personas recuerdan más fácilmente un nombre que un conjunto de números como una ip.

Las ventajas más importantes de usar un servidor DNS son:

- No hay duplicidad de nombres.
- Se elimina la carga excesiva en la red y en los host puesto que la información está distribuida por toda la red.
- Coherencia de la información debido a que la información se actualiza automáticamente sin necesidad de la intervención de nadie.

Las desventajas más importantes de usar un servidor DNS son:

- Es relativamente fácil hackear el servicio dns.
- Aunque es fácil de configurar, un error de configuración puede ser costoso de encontrar y solucionar.

Nombre de dominio

Un **nombre de dominio** es la dirección de una empresa, organización, grupo o una persona en Internet. Hay varios niveles de dominios en Internet:

1. Primer nivel. Son los que terminan en .com, .gob, .org, .es, .fr y algunos similares. No hay comprobaciones previas y se otorga al primer solicitante que lo pide. Son asignados por el ICANN, Internet Corporation for Assigned Names and Numbers o Corporación de Internet para la Asignación de Nombres y Números.
2. Segundo nivel. Son los más habituales ya que hacen referencia a la organización, marca o persona que está detrás del sitio web. Están relacionados con el país en el que se dan de alta. En España es Red.es quien asigna el dominio al primero que lo solicita. Normalmente se suelen pedir a través de las páginas de hosting.
3. Tercer nivel. Son los correspondientes al tipo .com.us, .org.ve, .edu.es o

similares. Mezcla un dominio genérico con un dominio específico de país. Se sigue un criterio de prioridad temporal en la solicitud. Además deben cumplir con las leyes vigentes y las reglas de sintaxis.

4. Subdominios. Es un anexo a un dominio de segundo nivel.

Una dirección normal de internet como http://www.iessantiagohernandez.com/ está formada por:

- http://. Protocolo de hipertexto que permite visualizar una página web en un navegador.
- www. Subdominio que identifica el servidor que aloja la página web.
- iessantiagohernandez. Subdominio que identifica la empresa u organización que ha comprado el dominio.
- com. Dominio de primer nivel que identifica la página web pertenece a una empresa u organización.

Un **nombre de host** es el nombre DNS de un dispositivo en una red. Los nombres de host se usan para encontrar equipos en la red, son alias para identificar un host tcp/ip.

Un nombre de host es una parte del nombre del dominio completo. Es más fácil recordar el nombre de host que la ip, aunque puede ser cualquier cadena de 255 caracteres. Se puede usar el nombre de host para hacer un ping u otras herramientas tcp/ip.

Un **nombre de dominio completo o fully qualified domain name,** FQDN, que determina de manera unívoca la ubicación del dispositivo en el árbol de espacios del dominio. Los caracteres válidos para nombre de dominio son letras, mayúsculas y minúsculas, números y guiones. Los guiones bajos están reservados para fine especiales. Si se usa un carácter no válido, se sustituye por un guion.

Por ejemplo, iesapp.iessantiagohernandez.com, iesapp es el nombre host y el resto es el sufijo dns y todo junto forma el FQDN.

Zonas de búsqueda, tipos de DNS y registros

Los servidores DNS tienen zonas que son las encargadas de contener los distintos tipos de registros. Las zonas pueden ser:

- **Zona de búsqueda directa**. Traduce un nombre de dominio en una dirección IP.
- **Zona de búsqueda inversa**. Obtiene el nombre del dominio a partir de una dirección IP.

Las zonas de búsqueda pueden ser de tres tipos:

- **Master** o **Maestro**. Crea sus propios registros en modo lectura y escritura, no los obtiene de otro servidor DNS. Los registros se añaden en una zona que se guarda como un archivo que es fácil de recuperar en caso de fallo. Se recomienda que haya redundancia de servidores DNS por si se produce un fallo en uno de ellos.

- **Slave** o **Esclavo**. Contiene la misma información que otros DNS. Sus funciones son liberar carga a los DNS principales y proporcionar un respaldo en caso de fallo.
- **Caché**. Contiene copias de las resoluciones DNS que han realizado los dns maestros y esclavos. Evita tener archivos de zona.

De manera similar a a las zonas, los servidores DNS pueden ser:

- **Primarios** o **maestros**. Guardan información de las zonas de las que son autorizados. Sus archivos son de lectura y escritura. Todos los cambios deben ser notificados a estos servidores para que mantengan la información actualizada.
- **Secundarios** o **esclavos**. Contienen la misma información que los maestros, aunque no pueden crear ni modificar registros. Sirven de respaldo por si se produce un fallo en los principales o para quitarles carga de trabajo.
- **Locales** o **caché**. Realiza peticiones a otros servidores dns para tener preparadas las respuestas de futuras solicitudes, aunque no tienen autoridad en ninguna zona. Se usan para liberar carga a otros servidores, reducir tráfico de red y reducir los tiempos de respuesta.

Un **registro** es un archivo de mapeo que indica al servidor dns cuál es la dirección ip a la que está asociado un nombre concreto. Hay muchos tipos de registros dns. Los más habituales son:

- **A** (**address**). Traduce nombres de dominios en direcciones ip.
  - Sintaxis: **`new.com A xxxx.xxxx.xxxx.xxxx.`**
- **PTR** (**Pointer**). Traduce direcciones ip en nombres de dominio.
  - Sintaxis: **`3-0-0-20.in-addr.arpa PTR host.new.com.`**
- **MX** (**Mail Exchanger**). Asocia un nombre de dominio a un servidor de correo. El número indica preferencia, a menor número, mayor preferencia.
  - Sintaxis: **`new.com 10 correo.new.com.`**
- **CNAME**. Es un alias que se le asigna a un host que tiene una dirección ip.
  - Sintaxis: **`alias.new.com CNAME nombre.new.com.`**
- **NS**. Define los servidores principales de un dominio. Debe haber, al menos, uno en el dominio.
  - Sintaxis: **`new.com IN NS servidor.new.com.`**
- **SOA**. Es el primer registro de la zona; solo puede haber uno configurado. Especifica el servidor dns primario del dominio. Pieza clave del archivo de zona.
- **TXT**. Ofrece información adicional a un dominio. También se usa como almacenamiento en claves de cifrado.
  - Sintaxis: **`new.com TXT información adicional.`**
- **SPR**. Es un registro de tipo texto que se crea en la zona directa del DNS. Se usa principalmente para evitar la suplantación de identidad.
  - Sintaxis: **`new.com IN SPR “v=spf1 a:exchange.new.com -all”.`**

Resolución de nombres de host

La resolución de nombres de host es el proceso mediante el cual un nombre de equipo o dominio se resuelve en una dirección ip. El proceso de resolución de nombres de host es el siguiente:

1. El proceso comienza cuando una aplicación o servicio pasa el nombre de host al servicio cliente DNS.
2. El servicio cliente DNS busca en la caché de resolución del cliente una asignación entre nombre de host y dirección ip.
   - Si el servicio cliente DNS no encuentra ninguna asignación en la caché de resolución del cliente, reenvía la consulta a un servidor DNS. Cuando responde el servidor DNS, se le pasa la ip devuelta a la aplicación que que inició la petición.

La **caché de resolución del cliente** es una ubicación de la memoria donde se almacenan los nombres de host que se han resuelto recientemente en direcciones ip. Si tenemos una dirección ip porque hemos ido hace poco a un sitio y se guarda en la caché durante un cierto tiempo la dirección ya que se supone que podemos querer regresar al mismo sitio web.
El tiempo predeterminado durante el que se guarda la dirección ip es de 5 minutos. Podemos utilizar la consola para visualizar los datos almacenados:

- Si queremos ver la caché dns debemos escribir **ipconfig /displaydns**.
- Si queremos eliminar dicha cahé, **ipconfig /flushdns**.

La caché de resolución del cliente también se carga con los datos que contenga el archivo host. Éste es un archivo estático que se mantiene en el equipo local y se usa para cargar alguna direcciones fijas que sepamos que vamos a utilizar ya que se reduce el uso de la red. Se encuentra en la ruta **%Systemroot%\System32\drivers\etc\host**. Sus entradas son del estilo ip y nombre de equipo o de dominio. Es un archivo importante y, según lo que se haga, puede hacer inviable utilizar la red.

Consulta al DNS

Una **consulta** es una solicitud de resolución de nombres que se envía a un servidor DNS. Hay dos tipos de consultas, recursivas e iterativas.
Una **consulta recursiva** es una consulta en la el cliente DNS solicita una respuesta completa a la consulta. No se puede redirigir la pregunta a otro servidor. El servicio DNS no tiene la obligación de soportar este tipo de consultas, es el dispositivo el que las negocia.
Las únicas respuestas aceptables son:

- La respuesta completa con la dirección de un registro de tipo A, acompañada del registro CNAME, si es que existe.
- Un error NXDOMAIN, que significa que el dominio o equipo no existe.
- Un error temporal que no permite acceder al servidor DNS por problemas de conectividad.

Una **consulta iterativa** es una consulta es una consulta en la el cliente DNS solicita la mejor respuesta a la consulta. El resultado puede ser una respuesta similar a la recursiva o una referencia a otro servidor DNS para que haga una nueva solicitud a ese servidor. Si el cliente obtiene una referencia, hace solicitudes hasta que le dan la respuesta o que no es correcta la consulta.
Una **consulta inversa** es una petición que se realiza cuando un dispositivo quiere saber el nombre del dominio al que pertenece un registro en particular. No se suelen usar ya que se han convertido en obsoletas.

Los pasos de una consulta son:

1. El usuario inicia una aplicación que requiere de un servidor externo como teclear una dirección en el navegador.
2. La aplicación consulta al dispositivo cuál es la ip de destino.
3. El dispositivo, si no conoce la respuesta, pregunta al servidor DNS configurado por defecto.
4. El servicio DNS mira si la respuesta se encuentra en su caché o archivo host.
   - Si la encuentra termina el proceso devolviendo el resultado.
   - Si no la encuentra depende del tipo de consulta:
     - Si es recursiva devuelve que no existe el sitio buscado.
     - Si es iterativa devuelve la lista de los servidores raíz.
5. El servicio DNS elige un servidor raíz y le envía la consulta.
6. El servidor raíz responde la consulta o le envía la dirección del servidor autoritario del dominio de primer nivel.
7. El servicio DNS le envía la consulta al servidor y este responde con el resultado o con la dirección de otro servidor DNS de un nivel inferior que acote la consulta.
8. Se repite el paso anterior hasta que el cliente recibe, finalmente, una respuesta como en una consulta recursiva.

Una **sugerencia de raíz** es un registro de recursos DNS almacenados en un servidor DNS que indica la dirección ip de los servidores raíz DNS. En una consulta iterativa, si falla el DNS falla con la zona de búsqueda directa y la caché, consulta a un servidor DNS que esté en el archivo de sugerencias de raíz y resuelve la respuesta.
Las sugerencias de raíz se guardan en el archivo cache.dns dentro de la carpeta **%Systemroot%\System32\dns**.

Un **reenviador** es un dns que se usa para resolver consultas ajenas al dominio o la organización. El proceso de los reenviadores es el siguiente:

1. El servidor DNS recibe una consulta recursiva de un cliente DNS.
2. El servidor DNS local reenvía la consulta al reenviador.
3. El reenviador envía la consulta a al servidor raíz para obtener un servidor

autorizado.

4. El servidor raíz responde con una referencia a un servidor DNS cercano al nombre de dominio enviado.
5. El reenviador realiza una consulta iterativa al servidor DNS que está más cerca del nombre enviado.
6. El proceso continua hasta que el reenviador recibe una respuesta autorizada.
7. El reenviador envía la respuesta al servidor DNS local , que envía la respuesta al cliente DNS.

Se puede hablar de muchas otras cosas como relación del dns con el dominio, dns primario y secundario, autorización del los dns, añadir equipos al dns, actualización del dns, transferencias de zonas, delegar zonas,…

Servicio de transferencia de ficheros

FTP, **File Transfer Protocol**, es un protocolo que permite la transferencia de archivos entre equipos de redes TCP/IP. FTP permite, entre otras cosas:

- Acceder a sistemas remotos y listar sus directorios y archivos.
- Transferir archivos desde (download o descargar) o hacia (upload o subir) el servidor FTP.
- Realizar acciones del sistema como modificar permisos o crear carpetas, renombrarlas, moverlas o borrarlas.

El servicio de ftp se basa en el modelo cliente servidor, necesitando:

1. **Cliente FTP**. Equipo con un programa que permite acceder a un servidor FTP para subir o descargar un archivo. Un cliente FTP como puede ser de los siguientes tipos:
   - Cliente por línea de comandos. La mayoría de los sistemas operativos incorpora un comando **ftp** que permite iniciar una conexión con el servidor del estilo **ftp servidor**. Tras establecer la conexión, se pueden usar una lista de comandos para encontrar el archivo que se quiera y gestionar su subida, descarga, permisos,...
   - Cliente gráfico. Usan interfaz gráfica para facilitar la conexión al servidor y suelen ofrecer otras funcionalidades adicionales.
   - Navegadores. Los navegadores actuales sirven como cliente FTP. En la ruta debe indicarse el protocolo FTP, sería algo del estilo **ftp://[usuario][:contraseña]@servidor**. Si se quiere entrar como usuario anónimo no hay que poner ni usuario ni contraseña.
2. **Servidor FTP**. Un servidor FTP es un equipo con un programa que procesa las conexiones de los clientes y otras configuraciones como los privilegios de los usuarios, limitaciones de subida y descarga, tiempos de conexión y espera,… Los archivos no tienen por qué estar el el propio servidor FTP.
3. **Protocolo FTP**. Conjunto de reglas que sirven para que se entiendan el servidor y el cliente. Es un subprotocolo de TCP.

Los servidores FTP permiten dos tipos de acceso al cliente:

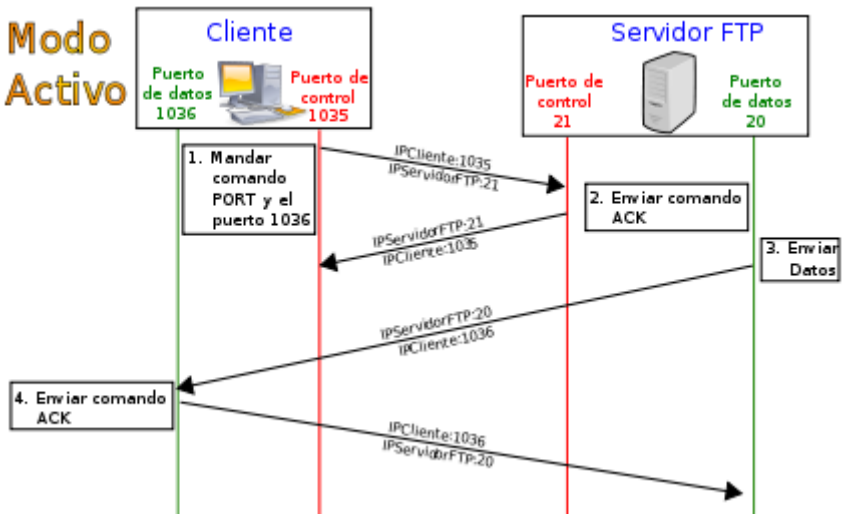
- **Acceso anónimo**. El cliente se conecta como un usuario especial anónimo. Se suele llamar anonymous o ftp. Tiene muy restringidos permisos y normalmente solo puede descargar archivos de alguna carpeta concreta muy controlada.
- **Acceso autorizado**. El cliente se conecta al servidor como un usuario registrado ya sea en el equipo en el que está instalado el servidor. un usuario creado para acceder al servidor FTP o un usuario de un dominio. Cada usuario tiene unos privilegios establecidos por el administrador del servidor FTP que le permiten moverse por el sistema de archivos del servidor y gestionar archivos.

El protocolo FTP utiliza varas conexiones y puertos independientes para el control y la transferencia de datos:

- **Conexión de control**. Es la conexión inicial que utiliza el cliente para dialogar con el servidor. Por defecto, se utiliza el puerto TCP 21. Sirve para que el cliente le diga lo que quiere hacer, subir o descargar archivos, al servidor. Dura hasta que el cliente la cierre la sesión o la cierre el servidor por no "hablar" durante un cierto tiempo. Un servidor puede administrar múltiples conexiones de control al mismo tiempo.
- **Conexión de datos**. Es por donde se mandan los archivos entre el servidor y el cliente. Por defecto, se utiliza el puerto TCP 20, aunque no es raro que algunos programas usen otros puertos. Puede haber varias conexiones de datos asociadas a una de control para subir o descargar varios archivos a la vez. Esto se determina en la configuración del servidor.

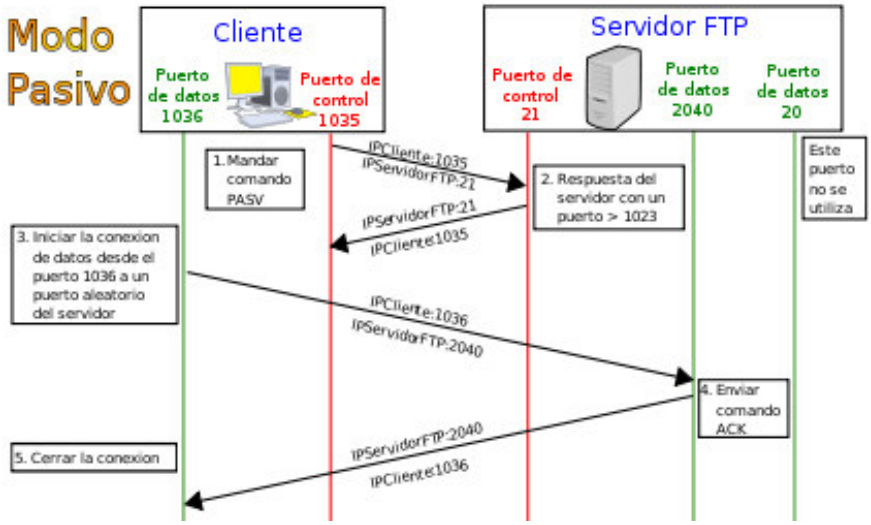
El cliente FTP puede conectarse de dos formas distintas:

- **Modo activo**. Es el modo por defecto al usar ftp. El principal problema es que el puerto de datos del cliente es aleatorio con lo que, si tenemos un cortafuegos activo, la conexión de datos puede ser rechazada. Un ejemplo de conexión sería:



1. El puerto de control del cliente, mayor de 1024, se conecta al puerto de control del servidor, 21, y envía el puerto de datos del cliente, mayor de 1024.
2. El servidor responde con un ACK, acknowledgment o acuse de recibo al puerto de control del cliente.
3. El servidor inicia una conexión entre su puerto de datos, 20, y el puerto de datos del cliente.
4. El cliente responde con un ACK al servidor.

- **Modo pasivo**. Es el cliente el que empieza la conexión, con lo que un posible cortafuegos no interrumpirá la conexión. Un ejemplo de conexión sería:



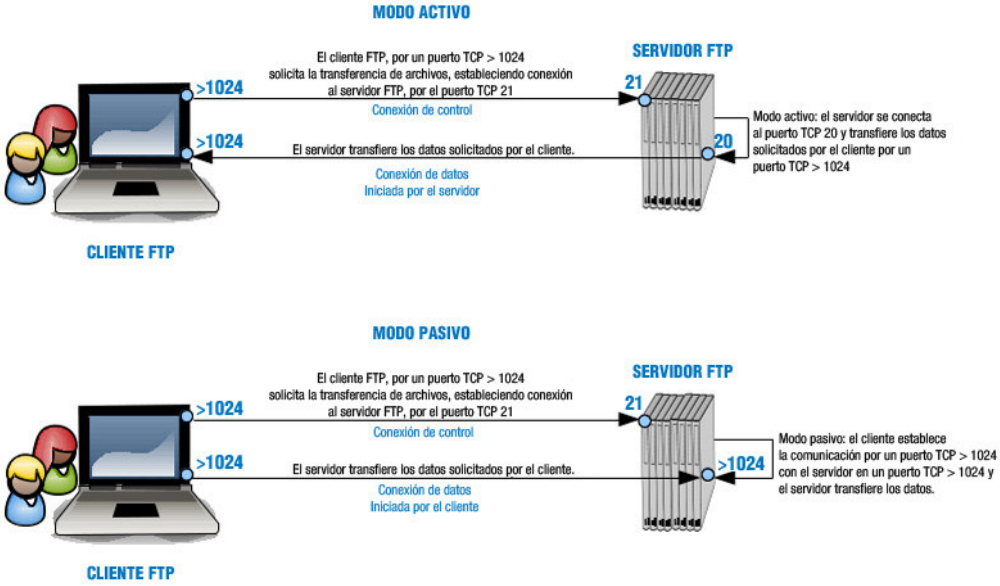
  1. El puerto de control del cliente, mayor de 1024, se conecta al puerto de control del servidor, 21, indicando que se quiere usar el modo pasivo, por consola se usaría el comando **pasv**.
  2. El servidor responde al cliente ofreciéndole un puerto aleatorio de datos abierto a efectos de conexiones de datos.
  3. El cliente inicia una conexión entre su puerto de datos, mayor de 1024, y el puerto de datos del servidor.
  4. El servidor envía un ACK al puerto de datos del cliente.

En FTP hay dos formas de transferencia de archivo, aunque los clientes detectan el tipo de archivo y usan el que es más apropiado:

- **Formato ASCII**. Se transmite byte a byte. Se usa con archivos de texto como txt, html, xml, java,…
- **Formato binario**. Se transmite bit a bit. Se usa para archivos que no son de texto como vídeos, imágenes, ejecutables, otros formatos,...

FTP no es un protocolo seguro ya que cuando se diseñó se pensó más en que fuese rápido. Los principales problemas de seguridad del servicio FTP son:

- No se garantiza que los equipos involucrados en la transferencia de archivos sean quienes dicen ser, por lo que FTP es vulnerable a ataques de suplantación de identidad o spoofing.
- Todo el intercambio de información, incluyendo la autenticación, se hace sin ningún tipo de cifrado. Se es vulnerable a ataques de análisis de tráfico de red o sniffing.


MODO ACTIVO
SERVIDOR FTP
El cliente FTP, por un puerto TCP > 1024
solicita la transferencia de archivos, estableciendo conexión
al servidor FTP, por el puerto TCP 21
Conexión de control
>1024
21
>1024
El servidor transfiere los datos solicitados por el cliente.
Conexión de datos
Iniciada por el servidor
20
Modo activo: el servidor se conecta
al puerto TCP 20 y transfiere los datos
solicitados por el cliente por un
puerto TCP > 1024
CLIENTE FTP
MODO PASIVO
SERVIDOR FTP
El cliente FTP, por un puerto TCP > 1024
solicita la transferencia de archivos, estableciendo conexión
al servidor FTP, por el puerto TCP 21
Conexión de control
>1024
21
>1024
El servidor transfiere los datos solicitados por el cliente.
Conexión de datos
Iniciada por el cliente
>1024
Modo pasivo: el cliente establece
la comunicación por un puerto TCP > 1024
con el servidor en un puerto TCP > 1024 y
el servidor transfiere los datos.
CLIENTE FTP