DNS

(Domain Name System /Sistema de Nombres de Dominio)

Es un conjunto de protocolos y servicios **que** permite a los usuarios utilizar nombres en vez de tener **que** recordar direcciones IP numéricas. Además de ser más fácil de recordar, el nombre es más fiable.

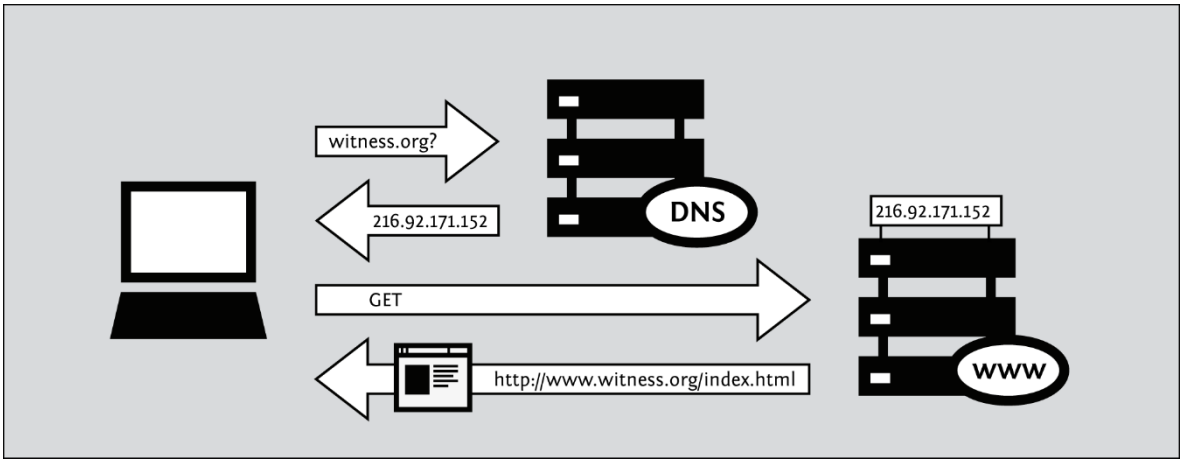
Puerto que utiliza: 53 TCP/UDP.

Ejemplos:

www.cisco.com	23.203.213.62
www.google.com.ar	142.251.45.67
www.unlam.edu.ar	170.210.32.98
www.greenpeace.org	104.20.54.128

**Estos registros de IPs pueden variar dependiendo de la necesidad de la empresa/organización o del IPS*

En Internet, esos nombres de dominio, como www.cisco.com, son mucho más sencillos de recordar que 198.133.219.25, que es la dirección numérica real para este servidor. Además, si Cisco decide cambiar la dirección numérica, para el usuario es transparente ya que el nombre de dominio seguirá siendo www.cisco.com. La nueva dirección simplemente estará enlazada con el nombre de dominio existente y la conectividad se mantendrá.



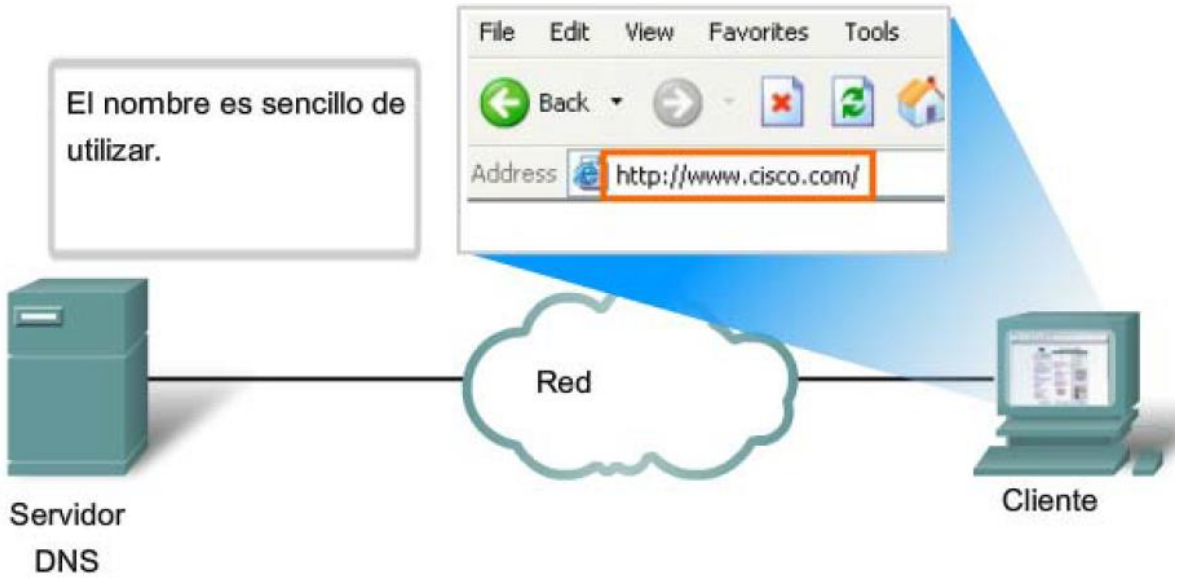
Protocolo DNS

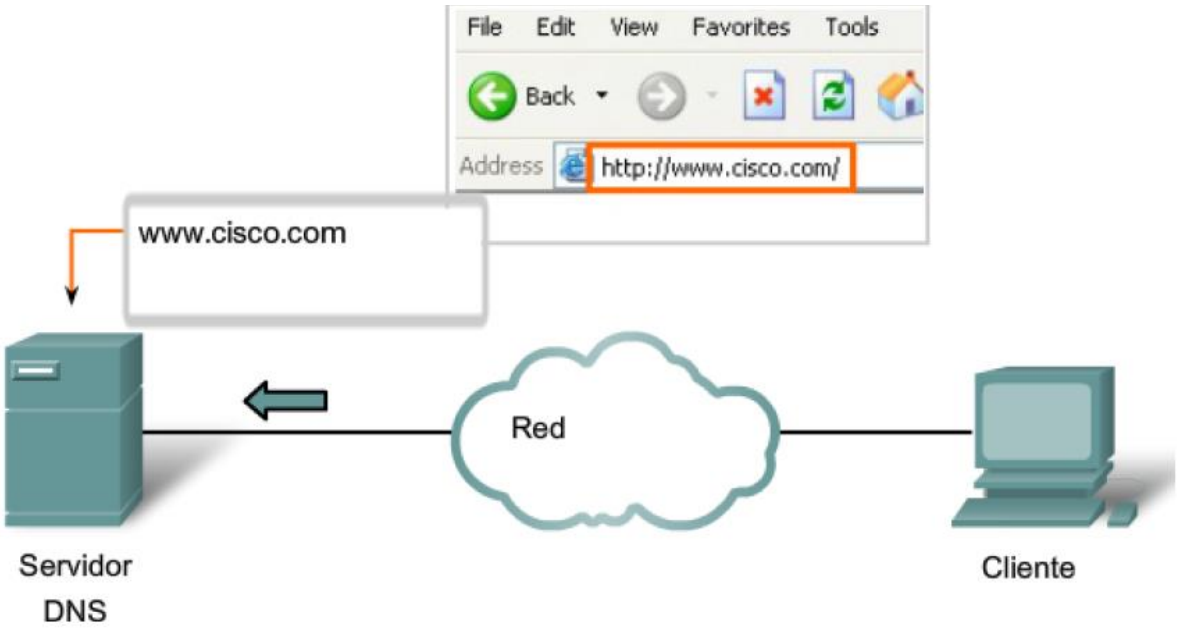
Utiliza un formato simple llamado “mensaje”

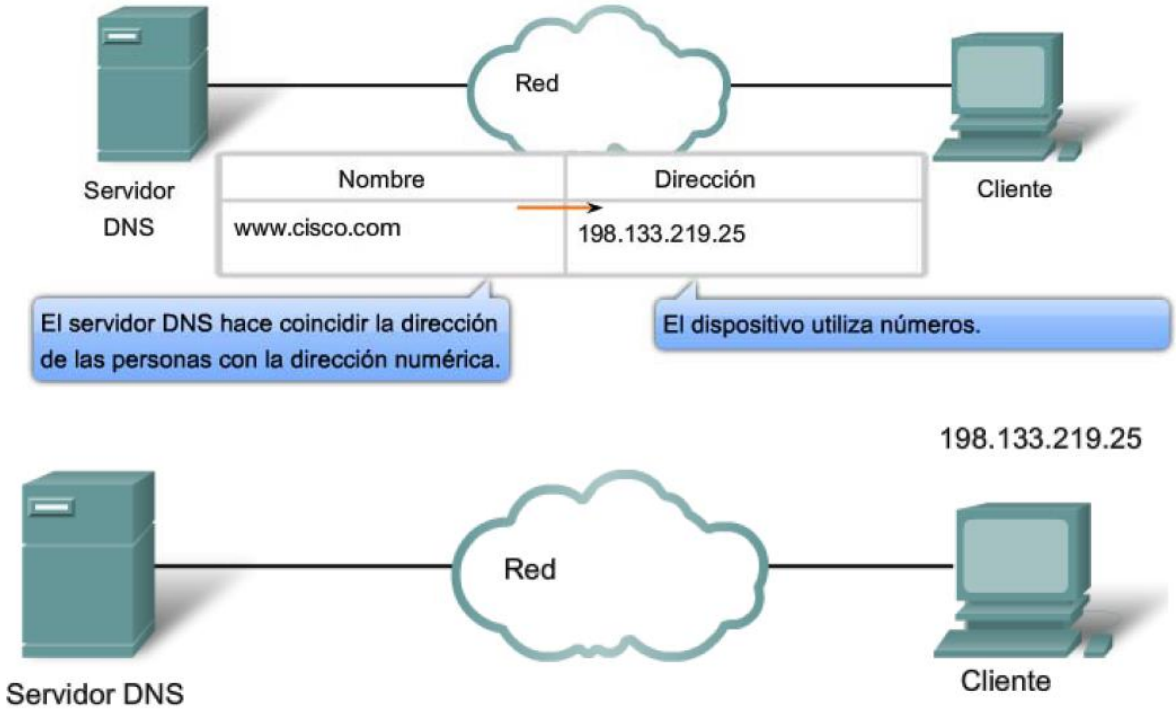
Este mensaje se utiliza para todos los tipos de solicitudes de:

- Clientes y respuesta del servidor

- Mensajes de error
- Transferencia de información de registros de recursos entre servidores





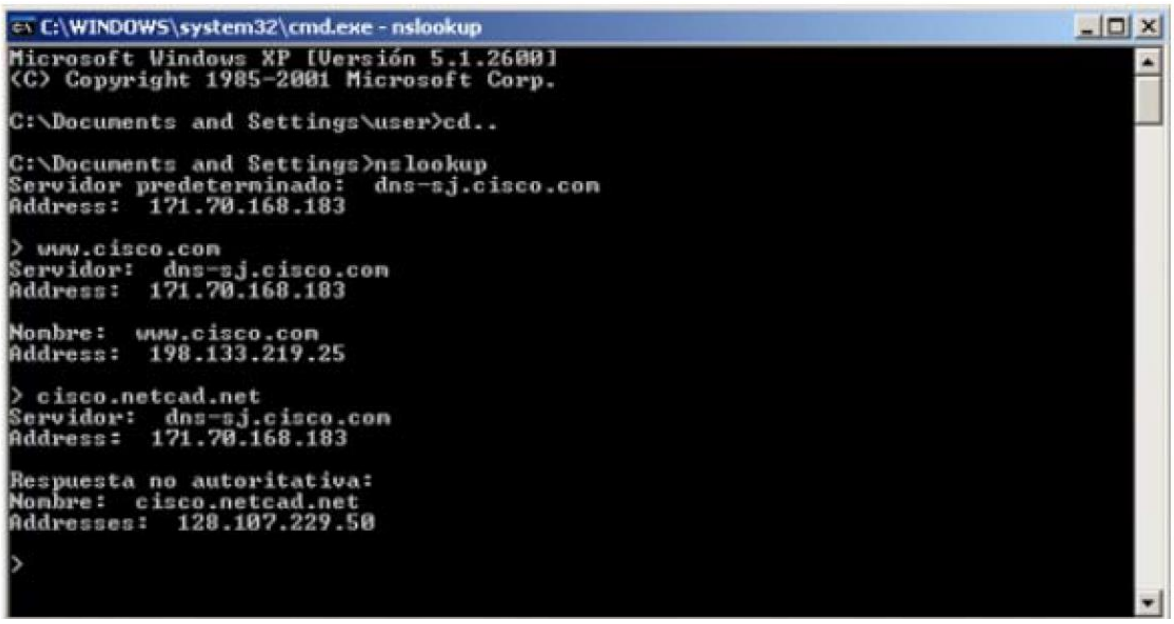


Al configurar un dispositivo de red, generalmente proporcionamos una o más direcciones del servidor DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet provee las direcciones para utilizar con los servidores DNS.

Los sistemas operativos informáticos también tienen una utilidad denominada nslookup que permite al usuario consultar manualmente los servidores de nombre para resolver un determinado nombre de host. Esta utilidad también puede utilizarse para resolver los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

En la figura, cuando se ejecuta nslookup, se muestra el servidor DNS por defecto configurado para su host. En este ejemplo, el servidor DNS es dns-sj.cisco.com que tiene una dirección de 171.68.226.120.

Luego podemos escribir el nombre de un host o dominio para el cual deseamos obtener la dirección. En la primera consulta de la figura, se hace una consulta para www.cisco.com. El servidor de nombre que responde proporciona la dirección 198.133.219.25.



REGISTROS DNS

- **A**: Es una dirección de un Host Final

- **NS**: Este hace referencia a que servidor de nombres es el autorizado para el dominio.

- **CNAME**: Cuando vemos el registro “CNAME”, este hace referencia a un alias de otro dominio. Es decir, su función es hacer que un dominio sea un alias de otro dominio. Normalmente este tipo de registros se utilizan para asociar nuevos subdominios con dominios ya existentes del registro A.

- **MX**: Cuando vemos el registro “MX”, este hace referencia a una lista de servidor de intercambio de correo que se debe utilizar para el dominio.

- **TXT**: Un registro TXT es un registro DNS que proporciona información de texto a fuentes externas a tu dominio y que se puede utilizar con distintos fines. El valor de los registros TXT puede ser texto legible por máquinas o por personas. Con los servicios de Google Cloud, los registros TXT se utilizan para verificar la propiedad del dominio y para implementar medidas de seguridad del correo, tales como SPF, DKIM y DMARC.

Nombre	Tipo	Contenido	Ttl	Prio	Serial	Activo
ejemplo.com	SOA	ns1.cuentadns.com dns-admin@ns1.cuentadns.com 2013091007	3600		1373532128	✓
ejemplo.com	NS	ns1.cuentadns.com	3600	0	1373532128	✓
ejemplo.com	NS	ns2.cuentadns.com	3600	0	1373532128	✓
ejemplo.com	NS	ns3.cuentadns.com	3600	0	1373532128	✓
ejemplo.com	A	89.140.237.75	3600	0	1378819625	✓
www	A	89.140.237.75	3600	0	1378819634	✓
ftp	A	89.140.237.75	3600	0	1378819641	✓
ejemplo.com	MX	mx1.aspl.es	3600	10	1378819679	✓
ejemplo.com	MX	mx2.aspl.es	3600	20	1378819706	✓
mail	CNAME	mailbox01.aspl.es	3600	0	1378819725	✓
smtp	CNAME	smtp-01.aspl.es	3600	0	1378819740	✓
pop3	CNAME	pop-01.aspl.es	3600	0	1378819759	✓

Filter: All A AAAA CAA CNAME MX SRV TXT

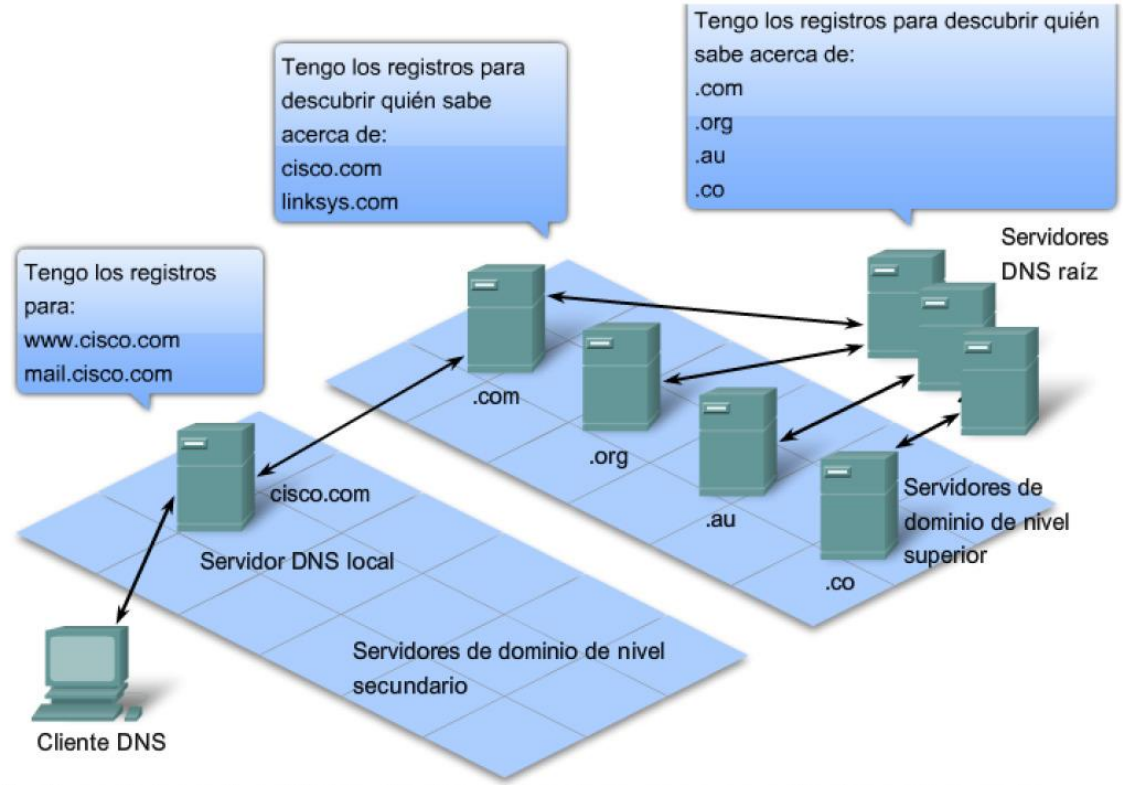
Name	TTL	Class	Type	Record
default._domainkey.[redacted]	14400	IN	TXT	v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvi0legM87KrTtjm3hD1cfi5DbDOByXWa637WyXssemq1d+BXfFr+Ztdx5Ry/+dZ984zv/y4v8hnFerGEWsusc4dixZ4Jy+wqSJKhS2nHPVKQgC7WAM7v0sX6LoMTXtSH0pClBUx0qsTjL5TD2eVw5/rQJ97C9PkQHIbK87FXkWb0vn9RgkFaOjv96n0qhUvXANuRNXZGIuZqIsfw3WCNfjipjbLPzb0iBKR7VyB0vdmsBNCumk6C9FP8yvl+JLxjxb3JPYkjkUyy9CyDswWusLdOL3ughezvTPpq0cOcowwcGwwEiA+pWvX46LDOgKeKZX0MumJqWLyc[redacted];
[redacted]	14400	IN	TXT	google-site-verification=yxyw4wD5THUak[redacted]1yPgtUwkm80Z5vsyb704
[redacted]	14400	IN	TXT	v=spf1 +mx +a +ip4:194.150.248.139 include:relay.mailchannels.net ~all
_dmarc.[redacted]	14400	IN	TXT	v=DMARC1;p=none;sp=none;pct=100;adkim=r;aspf=r;rua=mailto:dmarc@[redacted];ruf=mailto:dmarc@[redacted];rf=afrf;ri=86400;fo=0:1:d:s

SISTEMA JERARQUICO

El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres. La jerarquía es similar a un árbol invertido con la raíz en la parte superior y las ramas por debajo (consulte la ilustración). DNS utiliza nombres de domino para formar la jerarquía.

La estructura de denominación se divide en zonas pequeñas y manejables. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS. Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción.

Nota: DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.



Una jerarquía de servidores DNS contiene los registros de recursos que coordinan los nombres con las direcciones.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Entre los ejemplos de dominios del nivel superior se encuentran:

- .au: Australia
- .co: Colombia
- .com: una empresa o industria
- .jp: Japón
- .org: una organización sin fines de lucro

Después de los dominios del nivel superior, se encuentran los nombres de los dominios de segundo nivel y debajo de estos hay otros dominios de nivel inferior. Cada nombre de dominio es una ruta hacia este árbol invertido que comienza de la raíz. Por ejemplo, como se muestra en la ilustración, es posible que el servidor DNS raíz no sepa exactamente dónde se encuentra el registro del servidor de correo electrónico, mail.cisco.com, pero conserva un registro del dominio .com dentro del dominio de nivel superior. Asimismo, es posible que los servidores dentro del dominio .com no tengan un registro de mail.cisco.com, pero sí tienen un registro del dominio. Los servidores dentro del dominio cisco.com tienen un registro (un registro MX para ser precisos) para mail.cisco.com.

El DNS depende de esta jerarquía de servidores descentralizados para almacenar y mantener estos registros de recursos. Los registros de recursos enumeran nombres de dominios que el servidor puede resolver y servidores alternativos que también pueden procesar solicitudes. Si un servidor dado tiene registros de recursos que corresponden a su nivel en la jerarquía de dominios, se dice que es autoritativo para dichos registros. Por ejemplo, un servidor de nombre en el dominio cisco.netacad.net no sería autoritativo para el registro de mail.cisco.com, porque dicho registro se mantiene en un servidor de nivel de dominio superior, específicamente el servidor de nombre en el dominio cisco.com.

FTP (FILE TRANSFER PROTOCOL)

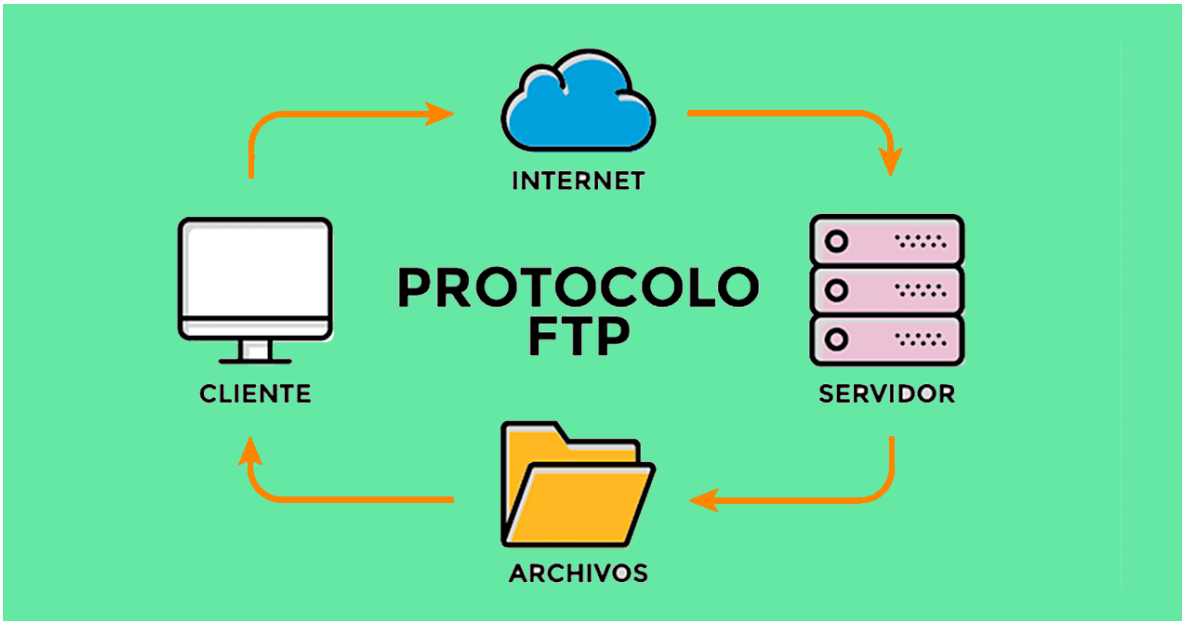
Es un protocolo que se utiliza en la capa de aplicación.

Se desarrollo para la transferencia de archivos entre cliente <–> servidor.

Un cliente FTP es una aplicación que se puede ejecutar en una PC y se utiliza para cargar y descargar archivos desde un servidor que ejecuta el Daemon FTPD

El FTP requiere de 2 conexiones entre cliente-servidor:

1. Una para comandos y respuestas (puerto 21)
2. Para transferencia de archivos reales (puerto 20)



SFTP (SSH “File Transfer Protocol” o Protocolo de Transferencia de Archivos SSH)

SFTP es un protocolo de transferencia de archivos construido sobre la capa de transporte SSH (Secure Shell), que se utiliza para mover de forma segura grandes cantidades de información a través de una conexión a Internet. SFTP toma de forma predeterminada el puerto **22**, que es el puerto SSH predeterminado.

A continuación se encuentran **algunos de los comandos de FTP más comunes** que podemos utilizar:

- help o ? – Enumerar todos **los comandos de FTP disponibles**.
- cd – Cambia el directorio en la máquina remota.
- lcd – Cambiar el directorio en la máquina local.
- ls – Ver los nombres de los archivos y directorios en el directorio remoto actual.
- mkdir – Crea un nuevo directorio dentro del directorio remoto.
- pwd – Imprime el directorio de trabajo actual en la máquina remota.
- delete – Elimina un archivo en el directorio remoto actual.
- rmdir- Elimina un directorio en el directorio remoto actual.
- get – Copia un archivo del servidor remoto a la máquina local.
- mget – Permite copiar múltiples archivos del servidor remoto a la máquina local.
- put – Copia un archivo de la máquina local a la máquina remota.
- mput – Copia un archivo de la máquina local a la máquina remota.

SSH

SSH normalmente admite los siguientes métodos para la autenticación de usuarios:

- Autenticación basada en contraseña: se suministra un nombre de usuario y una contraseña.
- Autenticación basada en claves: se suministra un nombre de usuario y una clave SSH. La autenticación basada en claves tiene la ventaja de poder utilizar la misma clave para distintos servidores y elimina la administración de contraseñas.
- Autenticación de doble factor: se suministra un nombre de usuario, una contraseña, y una clave SSH. La autenticación de doble factor ofrece el nivel de Seguridad más alto.

Aunque SSH no requiere una autenticación de doble factor, tiene la opción de requerir claves SSH además de un ID de usuario y una contraseña para que la conexión sea más segura. El uso de claves SSH ayuda a evitar que posibles impostores se conecten al servidor.

Antes de usar las claves SSH para la autenticación, primero debe generar una clave SSH privada y una clave SSH pública. La clave SSH pública se envía a su socio de Negocio, quien debe cargarla en su servidor SSH o SFTP y asociarla a su cuenta. Cuando usted se conecte al servidor SSH o SFTP de su socio, el servidor verificará la clave y, si todo coincide, la autenticación se realizará correctamente.