Martín Gómez Caicedo
Martín Gómez

# Nivel de Aplicación en el Modelo OSI

## DHCP (Dynamic Host Configuration Protocol)

protocolo de red que se utiliza para asignar direcciones IP y configuración de red automáticamente a los dispositivos que se conectan a una red. En lugar de tener que configurar manualmente cada dispositivo con una dirección IP, DHCP simplifica el proceso al asignar direcciones de manera dinámica

consta de 4 pasos

1. **DHCP Discover** (Descubrimiento DHCP): Cuando un dispositivo se conecta a una red, envía un mensaje DHCP Discover (Descubrimiento DHCP) a través de la red local. Este mensaje es una solicitud de configuración de red que busca servidores DHCP disponibles en la red.
2. **DHCP Offer** (Oferta DHCP): Los servidores DHCP que reciben el mensaje DHCP Discover pueden responder con un mensaje DHCP Offer (Oferta DHCP). En este mensaje, el servidor DHCP ofrece al cliente una dirección IP disponible junto con otros parámetros de configuración de red, como la máscara de subred y la puerta de enlace predeterminada.
3. **DHCP Request** (Solicitud DHCP): Después de recibir una o más ofertas de servidores DHCP, el cliente DHCP elige una y envía un mensaje DHCP Request (Solicitud DHCP) al servidor DHCP seleccionado. En este mensaje, el cliente confirma la aceptación de la oferta y solicita oficialmente la asignación de la dirección IP y otros parámetros de configuración.
4. **DHCP Acknowledgement** (Reconocimiento DHCP): El servidor confirma oficialmente la asignación de la dirección IP al cliente. Además de la dirección IP, el mensaje DHCP Acknowledgement también puede incluir información adicional de configuración de red, como la duración del tiempo de arrendamiento de la dirección IP y la dirección IP del servidor DNS.

## Servidores DNS (Domain Name System)

### Función Principal

La función principal de un servidor DNS es actuar como un directorio de nombres de dominio y direcciones IP en Internet. Cuando un usuario introduce un nombre de dominio en su navegador web o en otra aplicación, el servidor DNS se encarga de buscar y devolver la dirección IP asociada con ese nombre de dominio.

### Resolución de Nombres de Dominio

Los servidores DNS realizan el proceso de resolución de nombres de dominio, que implica traducir un nombre de dominio legible por humanos en la correspondiente dirección IP numérica. Este proceso se realiza en múltiples pasos, involucrando consultas a través de diferentes servidores DNS hasta que se encuentra la dirección IP deseada.

### Jerarquía de Servidores DNS

- Servidores raíz: servidores DNS de nivel superior en la jerarquía y almacenan información sobre la ubicación de los servidores de dominio de nivel superior (TLD).
- Servidores TLD: responsables de los dominios de nivel superior específicos, como .com, .org, .net, etc.
- Servidores autorizados: continence información específica sobre los dominios y pueden proporcionar respuestas directas a consultas DNS.
- Servidores de caché: almacenan temporalmente información de consultas DNS previas para mejorar la eficiencia y reducir la carga en la red.

### Funcionamiento de las Consultas DNS

El funcionamiento de las consultas DNS implica que un cliente envía una consulta al Servidor DNS solicitando la traducción del nombre de dominio a una dirección IP.

El Servidor DNS buscará la información en su base local o realizará consultas a otros servidores para obtener la respuesta adecuada.

Una vez encontrada, el servidor responderá con la dirección IP asociada al nombre de dominio solicitado, permitiendo así establecer la conexión requerida por el cliente.

### Seguridad y Redundancia

Los servidores DNS implementan medidas de seguridad, como el DNSSEC (Domain Name System Security Extensions), para proteger las consultas DNS de manipulaciones maliciosas.

- Para garantizar la disponibilidad y la redundancia, los nombres de dominio suelen tener múltiples servidores DNS autorizados que pueden responder a las consultas de los clientes.

## Capa SSL (Secure Sockets Layer)

SSL es un protocolo de seguridad que proporciona comunicaciones seguras a través de una red

Pasos

1. **Solicitud de SSL:** El proceso comienza cuando un cliente intenta establecer una conexión segura con un servidor, solicitando una conexión SSL.
2. **SSL Handshake** (Negociación de SSL): El cliente y el servidor realizan un intercambio de mensajes para negociar los parámetros de seguridad de la conexión SSL
   - **Client Hello** (Saludo del Cliente): El cliente envía un mensaje "Client Hello" al servidor, indicando sus capacidades SSL, incluidos los algoritmos de cifrado y versiones SSL compatibles.
   - **Server Hello** (Saludo del Servidor): El servidor responde con un mensaje "Server Hello" al cliente, seleccionando una versión de SSL y un conjunto de parámetros de seguridad para la conexión.
   - **Aprobación del Cliente:** El cliente puede verificar el certificado SSL del servidor para confirmar su autenticidad y decidir si confía en él.
   - **Verificación:** El servidor puede solicitar al cliente que se autentique mediante un certificado SSL. Esta autenticación puede ser opcional o requerida, según la configuración del servidor.
3. **Intercambio de Datos Seguro**: Una vez que se ha completado el handshake SSL y se han establecido las claves de sesión compartidas, los datos intercambiados entre el cliente y el servidor se cifran utilizando estas claves. Esto garantiza la confidencialidad e integridad de los datos durante la transmisión.
4. **Terminación de una Sesión SSL**: Una vez que la comunicación entre el cliente y el servidor ha concluido, la sesión SSL se puede cerrar de manera ordenada. Las claves de sesión se eliminan y la conexión segura se finaliza.

## Aplicaciones SSH (Secure Shell) y SCP (Secure Copy Protocol)

- SSH: protocolo de red que permite a los usuarios acceder de forma segura y controlar de manera remota otros dispositivos a través de una conexión encriptada. Se utiliza comúnmente para administrar servidores y dispositivos de red de forma remota.
- SCP: protocolo que se basa en SSH y se utiliza para transferir archivos de forma segura entre un cliente y un servidor. SCP utiliza la misma autenticación y encriptación que SSH, lo que garantiza la seguridad de la transferencia de archivos.