DHCP (Dynamic Host Configuration Protocol)

El **DHCP** es un protocolo que permite a los dispositivos conectados a una red obtener automáticamente su configuración de red. Este proceso es esencial en redes medianas y grandes, ya que simplifica la asignación de direcciones IP y otros parámetros de red.

El funcionamiento de DHCP sigue un modelo cliente-servidor. El dispositivo que se conecta a la red actúa como cliente, mientras que un servidor DHCP, configurado para administrar un rango de direcciones IP, gestiona la asignación. El proceso se realiza en cuatro pasos principales:

1. **Descubrimiento (DHCP Discover)**: Cuando un dispositivo necesita conectarse a la red, envía un mensaje de broadcast para encontrar un servidor DHCP. Este mensaje llega a todos los dispositivos de la red, pero solo el servidor DHCP responde.

2. **Oferta (DHCP Offer)**: El servidor DHCP responde con una oferta que incluye:

    - Una dirección IP disponible dentro de su rango asignado.
    - La máscara de subred, que define qué parte de la IP identifica la red y qué parte identifica al dispositivo.
    - La puerta de enlace predeterminada (gateway), que permite al dispositivo comunicarse con redes externas.
    - Los servidores DNS, necesarios para traducir nombres de dominio a direcciones IP.
    - Un tiempo de concesión, que establece cuánto tiempo puede usar el cliente la dirección IP asignada.

3. **Solicitud (DHCP Request)**: El cliente elige una de las ofertas recibidas y envía un mensaje para solicitar esa configuración en particular.

4. **Confirmación (DHCP Acknowledgement o ACK)**: El servidor confirma la asignación, registrando la dirección IP en su base de datos para evitar que sea asignada a otro dispositivo.

Este mecanismo asegura que cada dispositivo conectado a la red tenga una configuración válida y única, evitando conflictos y mejorando la administración de la red.

SSH (Secure Shell)

SSH es un protocolo de red que permite a los usuarios conectarse de manera segura a otros dispositivos, generalmente servidores o equipos remotos. Su principal característica es la seguridad, ya que cifra toda la comunicación, evitando que terceros puedan interceptar o manipular los datos transmitidos.

SSH opera en un modelo cliente-servidor. El cliente inicia la conexión, proporcionando las credenciales necesarias (contraseña o clave SSH), y el servidor verifica la identidad del cliente antes de concederle acceso. El proceso de autenticación puede realizarse de dos formas principales:

1. **Por contraseña**: El cliente proporciona un nombre de usuario y una contraseña, que el servidor valida. Este método es sencillo pero menos seguro, ya que las contraseñas pueden ser vulnerables a ataques.

2. **Por clave SSH**: Este método utiliza un par de claves, una pública y una privada. La clave pública se almacena en el servidor, y la clave privada permanece en el cliente. Durante la conexión, el cliente

demuestra que posee la clave privada correspondiente sin enviarla directamente, lo que mejora significativamente la seguridad.

SSH no solo se utiliza para acceder a un servidor, sino también para transferir archivos de forma segura (mediante protocolos como **SCP** y **SFTP**) y para crear túneles cifrados que protejan otros tipos de tráfico.

NAT (Network Address Translation)

El **NAT** es una técnica que traduce las direcciones IP privadas de una red interna a una dirección IP pública, permitiendo que los dispositivos accedan a Internet. Esto es crucial porque las direcciones IP privadas no son enrutables fuera de la red local.

El funcionamiento de NAT se basa en un router o firewall que actúa como intermediario entre la red privada y la red externa. Cuando un dispositivo interno envía un paquete de datos hacia Internet:

1. El router reemplaza la dirección IP privada del dispositivo con su propia dirección IP pública.
2. El router guarda en una tabla de traducción el puerto y la dirección IP privada originales, para saber cómo enrutar la respuesta cuando regrese.

NAT puede operar de tres formas principales:

1. **NAT Estático**: Cada dirección IP privada se asigna a una dirección IP pública fija. Esto se utiliza para dispositivos que necesitan ser accesibles desde Internet, como servidores.
2. **NAT Dinámico**: Las direcciones IP privadas se asignan de manera dinámica a direcciones IP públicas disponibles en un grupo predefinido.
3. **PAT (Port Address Translation)**: Múltiples dispositivos comparten una única dirección IP pública, diferenciándose por el número de puerto. Es la forma más común en redes domésticas y pequeñas empresas.

Ventajas del NAT:

- Permite que muchos dispositivos accedan a Internet con una sola dirección IP pública.
- Oculta las direcciones internas, mejorando la seguridad.
- Ayuda a mitigar la escasez de direcciones IPv4.

VLAN (Virtual Local Area Network)

Una **VLAN** es una red lógica que segmenta una red física en varias subredes virtuales. Aunque todos los dispositivos estén conectados al mismo switch físico, cada VLAN actúa como una red independiente, aislando el tráfico entre ellas.

Las VLANs son útiles para:

- **Seguridad**: Separan el tráfico de diferentes departamentos o grupos, evitando que usuarios no autorizados accedan a recursos sensibles.
- **Rendimiento**: Reducen el tráfico de broadcast, mejorando la eficiencia de la red.
- **Flexibilidad**: Permiten reorganizar dispositivos sin necesidad de cambiar su conexión física.

El tráfico entre dispositivos de diferentes VLANs solo puede ocurrir mediante un dispositivo de capa 3, como un router o un switch con capacidades de ruteo. Esto asegura que las VLANs permanezcan aisladas a menos que se configure explícitamente la comunicación entre ellas.

Tipos de VLAN:

1. **VLAN por puerto**: Asigna un puerto del switch a una VLAN específica. Es la forma más sencilla de segmentar una red.
2. **VLAN por protocolo**: Segmenta el tráfico según el protocolo utilizado, como IPv4 o IPv6.
3. **VLAN por dirección MAC**: Asigna dispositivos a VLANs basándose en sus direcciones MAC, útil para redes dinámicas donde los dispositivos pueden moverse.

DNS (Domain Name System)

El **DNS** es el sistema encargado de traducir nombres de dominio legibles por humanos (como `www.google.com`) a direcciones IP comprensibles por las máquinas (como `172.217.16.195`). Sin DNS, los usuarios tendrían que recordar y escribir las direcciones IP para acceder a los recursos en Internet.

El funcionamiento de DNS implica varios pasos:

1. Cuando un usuario escribe un nombre de dominio en el navegador, el dispositivo realiza una consulta DNS.
2. Si la dirección no está en la caché local, la consulta se envía a un servidor DNS, que puede ser proporcionado por el proveedor de servicios de Internet o configurado manualmente.
3. Si el servidor DNS no tiene la dirección en su base de datos, consulta a otros servidores DNS jerárquicos hasta encontrar la dirección IP correspondiente.

DNS también permite características avanzadas, como:

- **Resolución inversa**: Convertir direcciones IP en nombres de dominio.
- **Balanceo de carga**: Asociar un nombre de dominio a múltiples direcciones IP, distribuyendo el tráfico entre servidores.

Importancia del DNS:

- Simplifica el acceso a los recursos en línea al usar nombres en lugar de direcciones IP.
- Optimiza la administración de redes grandes mediante la configuración de zonas DNS.