1. Introducción.

Una aplicación web necesita de servicios de red para poder funcionar de forma correcta y coherente. Estos son el servicio DHCP, DNS y el servicio de directorio LDAP.

2. Direccionamiento.

Es una función propia de los protocolos de la capa de red/internet que permite la identificación y transmisión de informacion entre nodos.

Existen los siguientes tipos de direccionamiento:

- ***Unicast:*** Identifica una interfaz de un único nodo.
- ***Multicast:*** Identifica un grupo de interfaces que pertenecen a distintos nodos. Cuando un paquete envía a una dirección multicast, va dirigido a todos los nodos que pertenecen a la misma. En IPv4, se encuentran en el rango de direcciones IP que comienzan con 224.0.0.0 y van hasta 239.255.255.255.
- ***Broadcast:*** Identifica al grupo formado por todas las interfaces de los nodos conectados a la red, permitiendo envíos de informacion a todos ellos con un único mensaje simultáneamente y sin necesidad de emitir el mismo mensaje nodo por nodo. Algunos ejemplos de su uso incluyen: ARP y DHCP.
- ***Anycast:*** Identifica un grupo de interfaces que pertenecen a diferentes nodos. Cuando un paquete se envía a una dirección anycast, va dirigido al nodo miembro del grupo anycast que este físicamente más cerca del remitente.

2.1. Protocolo IPv4.

Cuarta revisión del Protocolo de Internet (IP) que se usa para identificar dispositivos en una red a través de un sistema de direccionamiento. Es el más usado para conectar dispositivos.

2.1.1. Dirección IPv4.

Una dirección IPv4 es un conjunto de 4 octetos (32 bits) separados por puntos que ofrecen un espacio de direccionamiento de 2^{32} posibles valores. Cada octeto puede tomar valores comprendidos entre 0 y 255, también tienen su correspondiente representación en formato binario.

Estas se asignan a las interfaces de red de los diferentes nodos y se puede incluso asignar más de una dirección a la misma interfaz. Gracias a esta asignación, los nodos pueden identificarse y se permite la comunicación entre ellos. Cada dirección se utiliza en el nivel del modelo TCP IP y podrá ser fija o dinámica.

IPv4 puede emplear unicast, multicast o broadcast. Cada dirección puede clasificarse según su ámbito en:

- ***Privada:*** Tiene un nodo dentro de una red de área local y únicamente es visible desde esa misma red. Para acceder a un servicio ofrecido por un nodo desde otro nodo que resida en la misma red local, bastara con que este último conozca su dirección IP privada. Cualquier dispositivo que se conecta a una red doméstica o corporativa dispondrá de una dirección privada.
- ***Publica:*** Tiene conexión directa a internet y es la dirección que realmente es visible desde dicha red.

Para que un nodo que reside en una red local A pueda acceder a un servidor que está en otra red local B perteneciente a una organización diferente y para la que no hay forma de encaminar internamente los paquetes, será necesario conocer la dirección IP publica tras la que se encuentra dicho nodo. Generalmente, en esta comunicación se hace uso de NAT.

IMPORTANTE: La dirección IP publica de un dispositivo no puede conocerse desde la configuración del mismo equipo (no depende de ninguno de sus parámetros de conexión. Para conocer la IP publica, puedes hacer uso de páginas web.

2.1.2. Máscara de red.

Desde de cada dirección IPv4 hay una porción de los bits de orden superior que representa la dirección de la red en la que se encuentra.

Importante: Todos los nodos de la red tienen los mismos valores en esa porción de bits.

El número de bits que se toman para identificar la parte de red viene determinado por la máscara de red/subred (Conjunto de 4 octetos separados por puntos). Las máscaras no pueden tomar todo el rango de valores posible, y se permite únicamente un conjunto contiguo de bits a 1 que representa la porción de red y otro conjunto contiguo de bits a 0 que representa la porción de hosts. Las máscaras también pueden representarse en notación CIDR mediante /N (N es el número de bits activos [1] de la máscara).

Originalmente, las direcciones formaban parte de redes classfull en las que no se declaraban las máscaras de red de forma expresa. Eso era porque las direcciones IP estaban clasificadas en clases que tenían asociada una máscara de red implícita. Hoy en día las direcciones forman parte de redes classless y las direcciones IP deben definirse junto con su máscara de red/subred.

El proceso mediante el cual se incrementa el número de bits a 1 de la máscara por encima de los valores predeterminados se conoce como subnetting, permite dividir la red en redes más pequeñas que albergan un número menor de hosts. El proceso inverso que reduce el número de bits a 1 de la máscara por debajo de los valores predeterminados se conoce como supernetting, y permite unificar varias redes en otras que puedan albergar más hosts.

Gracias a VLSM (Variable Length Subnet Mask), es posible dividir una red en subredes aplicando una máscara y continuar dividiendo esas subredes de forma recursiva en redes más pequeñas aumentando de nuevo el número de bits de la porción de red.

2.2. Puerta de enlace.

Cuando un nodo quiere comunicarse con otro, comprueba si, tanto el como el nodo destino, están en la misma red. Esto lo hace obteniendo ambas redes mediante operaciones AND entre las IP y la máscara del nodo origen, y finalmente realizando la comparación bit a bit de ambas redes.

En caso de que ambas redes sean iguales, las comunicaciones se llevan a cabo sin problemas, si el recurso al que se quiere acceder no está en la misma red, se hace necesario usar algún elemento que, siendo accesible, reenvié los paquetes IP que no coinciden con ninguna ruta de la tabla de enrutamiento al destino. Ese elemento es un enlace para el equipo por ser una dirección alcanzable y que permite acceder a otras redes.

El término “puerta de enlace” aparece como “puerta de enlace predeterminada”, “puerta de acceso” o “Gateway”.

3. Servicios de red, protocolos y puertos.

Es un conjunto de recursos y procesos que buscan satisfacer las necesidades que los clientes demandan a través de la red.

La implantación de estos servicios reporta un elevado número de ventajas.

Los servicios de red se implantan en arquitecturas cliente-servidor, lo cual favorece su consumo por parte de los clientes. Los nodos que alojan y ofrecen estos servicios se denominan servidores. En algunos casos el servicio se encuentra distribuido entre varios nodos que cooperan entre sí

(arquitecturas P2P), descentralizándose de esta manera el papel del servidor, que pasa a residir en este caso en todos y cada uno de los pares.

Los servicios de red pueden residir en equipos con sistemas operativos diseñados especialmente para comportarse como servidores, aunque también pueden alojarse sobre equipos con sistemas operativos cliente.

Algunos de estos sistemas operativos ya tienen instalado por defecto el servicio, el cual puede estar deshabilitado, u ofrecen la posibilidad de instalarlo de forma fácil desde sus propias fuentes. En otros casos, es necesario instalar el software necesario desde fuentes externas al equipo que, ocasionalmente, es de terceros. Para que un equipo pueda actuar como servidor es necesario que disponga del software y el hardware necesario para prestar el servicio concreto, pues no todos los servicios precisan de los mismos requisitos.

En la siguiente tabla se muestra un listado de algunos de los servicios más comunes y los protocolos de la capa de aplicación del modelo TCP/IP asociados:

Servicio	Protocolo
Servicio de administración y configuración de sistemas	***DHCP (Dynamic Host Configuration Protocol):*** Protocolo de red que permite que los clientes de una red obtengan los parámetros de configuración IP automáticamente.
	DNS (Domain Name System): Protocolo empleado en la traducción de nombres de equipos y recursos a direcciones IP y viceversa.
Servicio de publicación de información en la web	***HTTP (Hypertext Transfer Protocol):*** Protocolo de comunicación empleado para la transmisión de documentos hipermedia como HTML.
Servicio de acceso remoto	***Telnet (Telecomunication Network):*** Protocolo empleado para hacer conexiones remotas no cifradas y cuyo programa cliente toma el mismo nombre.
	SSH (Secure Shell): Protocolo empleado para hacer conexiones remotas cifradas y cuyo programa cliente toma el mismo nombre.
Servicio de transferencia de ficheros	***FTP (File Transfer Protocol):*** Protocolo empleado para transferir ficheros a través de la red.
	TFTP (Trivial File Transfer Protocol): Protocolo empleado para transferir ficheros de pequeño tamaño a través de la red sin autenticar al usuario.
Servicios de impresión, compartición de archivos y sistemas de ficheros en red	***NFS (Network File System):*** Protocolo que permite que hosts remotos monten sistemas de ficheros sobre la red e interactúen con ellos como si estuvieran montados localmente. Incluido por delecto en la mayoría de los sistemas UNIX/LINUX
	SMB (Server Message Block): Se emplea para interconectar equipos Microsoft Windows y compartir archivos e impresoras entre ellos. SAMBA es la implementación de código abierto del protocolo SMB.

La capa de transporte del modelo TCP/IP, se ocupa de identificar el proceso o servicio del nodo destinatario que recibirá los datos lo cual permite que múltiples servicios estén ejecutándose de forma simultánea en el equipo servidor. Esto se consigue gracias al puerto (número que permite identificar el servicio destinatario del paquete recibido).

Aunque en cada protocolo se definen los puertos en los que por defecto el servicio debe escuchar peticiones, estos se pueden modificar. Se debe tomar precaucion de no elegir ningún puerto que este siendo utilizado por otro servicio, de lo contrario uno de los dos no se iniciara. Por ultimo, hay que asegurarse de que los clientes conocen el nuevo puerto de escucha, de lo contrario no podrán acceder al servicio.

A nivel de la capa de internet, algunos trabajan únicamente con IPv4, aunque la mayor parte de ellos son compatibles tanto con IPv4 como con IPv6.

4. Servicio DHCP.

4.1. Instalación de servidores de configuración de parámetros de red.

Actualizamos los repositorios:

sudo apt update

Actualizamos los paquetes:

sudo apt upgrade

Instalamos el paquete isc-dhcp-server:

sudo apt install isc-dhcp-server

4.2. Preparación del servicio para asignar configuraciones básicas de red.

- ***/etc/default/isc-dhcp-server:*** Guarda el valor de las interfaces físicas del servidor por donde se van a escuchar las peticiones de configuración de red de los clientes.
- ***/etc/dhcp/dhcpd.conf:*** Guarda los parámetros de configuración que se van a repartir a los clientes.
  Los mensajes que se mandan del cliente al servidor tendrán un puerto de destino 67 y los del servidor al cliente tendrán un puerto de destino 68. Ambos casos son tipos de paquete UDP.
  Este último archivo (dhcpd.conf) está compuesto por una serie de sentencias, que son los parámetros y las declaraciones. Las declaraciones a su vez pueden ser de varios tipos, aunque nos centraremos en las siguientes:
- **Subnet:** Indica la red bajo la cual van a recibir las configuraciones de red los clientes. Dentro de esta es obligatorio que este el parámetro ***range***:

  subnet nombre_red **netmask** máscara_de_subred **{**
  range ip_inicio ip_fin;
  [parámetros;]
  }
- **Host:** Sirve para realizar reservas estáticas para algunos equipos:

  host nombre_identificativo **{**
  [parámetros;]
  hardware Ethernet dirección_MAC;
  fixed-address dirección_IP;
  }

MUY IMPORTANTE: Para que las modificaciones realizadas en el fichero de configuración tengan efecto, se debe reiniciar el servicio con:

systemctl restart isc-dhcp-server Ó ***service isc-dhcp-server restart***

Si se quisiera configurar el servicio de una manera básica, los parámetros que se deberían configurar para que los clientes tengan conectividad a la red serían los siguientes:

- ***Range {ip_inicio} {ip_fin}:*** Indica el rango de direcciones que va a repartir.
- ***Option routers {Gateway}:*** Indica el valor de la puerta de enlace para comunicarse con otras redes.
- ***Option domain-name-servers {dns1, dns2, …, dnsN}:*** Se especificarán las direcciones IP de los servidores DNS que van a resolver los nombres a los clientes. Si se ponen varios, tomaría el primer valor como primario y los siguientes como secundarios.
- ***Default-lease-time {tiempo}:*** Indica el número por defecto que durara una concesión a un equipo si el cliente no solicita un tiempo de arrendamiento especifico.

- ***Max-lease-time {tiempo}:*** Señala la duración máxima en segundos que se asignara a una concesión. Este sería útil en el caso de que el cliente quisiera una asignación que durara un tiempo determinado, entonces no superaría este valor.
  NOTA: Al colocar los parámetros ***default-lease-time*** y ***max-lease-time*** fuera de la declaración subnet, se consigue que tengan validez para todas las declaraciones que se hicieran en el fichero. Si estuviesen dentro de la declaración subnet, solo afectarían a los parámetros de la red indicada en ese subnet.

4.3. Configuración de asignaciones estáticas.

La asignación estática se especificará en el fichero de configuración /etc/dhcp/dhcpd.conf. Para ello, se debe insertar una declaración que se incluiría al final del fichero con la sentencia host, donde se especificarían los siguientes valores:

- ***Hardware Ethernet {MAC}:*** donde {MAC} seria la dirección física del cliente que solicitara la configuración.
- ***Fixed-address {IP}:*** donde {IP} seria la dirección IP que se le asignaría a la dirección MAC especificada previamente.
  NOTA: También se pueden añadir otras directivas en el caso de que solo queramos que se apliquen a dicho host

5. Para saber más.

5.1. Dirección IP.

5.1.1. Que es y cómo funciona la dirección IP.

Una IP (Internet Protocol) es una dirección única que identifica a un dispositivo en una red. Esta se encuentra formada por cuatro números separados por un punto. Cada número está comprendido entre 0 y 255. Es importante tener en cuenta que pueden ser de varios tipos (pública, privada, fija y dinámica).

Un dispositivo envía un paquete de datos y el Router o los routers se encargan de hacerlo llegar hasta su destino, cumpliendo una serie de reglas conocidas como “protocolos de red”.

5.1.2. Para qué sirve la dirección IP.

Una de las utilidades principales de la dirección IP, es la de permitir la comunicación con otros dentro de una red. Esta red puede ser interna o externa, y en función de esto se utilizarán IP de tipo privada o pública.

Sirven de guía para que los paquetes enviados desde cualquier dispositivo sepan donde tienen que ir y regresar y no se encuentren perdidos sin dirección de origen y destino.

5.1.3. Tipos de direcciones IP.

Existen varios tipos de direcciones IP, dependiendo de su accesibilidad y de su perdurabilidad, como son:

- ***IP publica:*** Nos la proporciona el ISP para identificar de forma exclusiva nuestra conexión a internet. Se asigna únicamente a aquellos dispositivos que conecten de forma directa con internet. Estas siempre deben ser únicas y exclusivas (no se pueden repetir).
- ***IP privada:*** Identifica los dispositivos dentro de una red local (LAN). Pueden repetirse solamente cuando se encuentran en redes independientes y separadas entre sí. Como no llegan a conectarse a Internet, nunca conocerán la dirección IP de otros dispositivos de otra red privada, de lo contrario, crearían conflictos de IP e impedirían el correcto funcionamiento de las redes.

- ***IP dinámica:*** Dirección que va cambiando cada cierto tiempo. El uso de este tipo de IP impide el problema del agotamiento del rango de direcciones, evita algunos ataques, hace más difícil el rastreo ofreciendo una mayor privacidad y permite la optimización de recursos y tiempo por parte del administrador si se hace uso de un servidor DHCP. Suelen ser más adecuadas para la mayoría de los consumidores al tener un precio más bajo y un menor riesgo de seguridad.
- ***IP estática o fija:*** Aquella que se asigna de forma manual y permite que un dispositivo que se conecte a la red lo haga siempre haciendo uso de la misma IP. Con su utilización se lleva a cabo una comunicación en algunos casos mucho más rápida. Tienen un mayor coste y una menor privacidad al ser más fácil de hackear. Su configuración ya no es tan sencilla y automática como la de las IP dinámicas y suelen ser mas adecuadas para las empresas.

5.1.4. Clases de direcciones IP y sus rangos.

Se dividen en clases dependiendo del valor del primer octeto:

- ***Clase A (0.0.0.0 – 127.255.255.255):*** El primer octeto identifica la red y los tres restantes al dispositivo. Se usan para redes con un gran número de hosts.
- ***Clase B (128.0.0.0 – 191.255.255.255):*** Los primeros dos octetos identifican la red y los siguientes al dispositivo dentro de la red. Se suelen usar en medianas y grandes empresas.
- ***Clase C (192.0.0.0 – 223.255.255.255):*** Los primeros tres octetos identificaran a la red y el ultimo octeto al dispositivo dentro de la red. Se usan en redes que tienen una pequeña cantidad de dispositivos como son las pequeñas empresas.
- ***Clase D (224.0.0.0 – 239.255.255.255):*** Se usan para optimizar la velocidad y el ancho de banda de una red (multicast).
- ***Clase E (240.0.0.0 – 255.255.255.255):*** Son usadas para la investigación.

Dentro de la clasificación anterior existe un rango de direcciones que se encuentran reservadas para su uso en redes privadas:

- ***Clase A (10.0.0.0 – 10.255.255.255)***
- ***Clase B (172.16.0.0 – 172.31.255.255)***
- ***Clase C (192.168.0.0 – 192.168.255.255)***

5.2. NAT. Que es y para qué sirve.

NAT significa traducción de direcciones IP, coge una dirección IP privada y la traduce a una dirección IP publica o viceversa. Se usa cuando necesitamos que nuestros dispositivos en la red (con IP privadas) se comuniquen a través de Internet.

- Da solución provisional al problema de agotamiento de IPv4.
- Disminuye el costo elevado de obtención de IP públicas.
- Conecta miles de dispositivos a internet haciendo uso de una sola dirección IP pública.

Si queremos enviar un paquete desde nuestro PC a internet, se llevaría a cabo el siguiente proceso: Tenemos una IP local en nuestro dispositivo. El paquete será enviado a la NAT para que la traduzca a la IP pública y salga a internet. Internet lo que va a hacer es devolver el paquete a nuestra IP publica, la NAT va a traducir esa IP publica a la privada y la va a enviar al dispositivo que esperaba la respuesta.

La mayor parte de los routers de hogares y empresas en la actualidad están haciendo uso de NAT. Traducen la IP privada de cada dispositivo a la pública que le fue asignada por su ISP.