Práctica 9 - Redes y Comunicaciones

1. **¿Qué es IPv6? ¿Por qué es necesaria su implementación?**

- **IPv6 (Protocolo de Internet versión 6)** es un protocolo de red diseñado para reemplazar a **IPv4 (Protocolo de Internet versión 4)**, fue creado debido a la creciente preocupación de que el espacio de direcciones de 32 bits de IPv4 se estaba agotando rápidamente. **IPv6 utiliza direcciones de 128 bits**, lo que proporciona un número exponencialmente mayor de direcciones IP únicas, asegurando que el mundo no se quede sin direcciones. **La implementación de IPv6 es necesaria por varias razones:**
    - **Agotamiento de direcciones IPv4:** El rápido crecimiento de Internet, con la incorporación de nuevos dispositivos como teléfonos inteligentes, tabletas y dispositivos del Internet de las cosas, ha acelerado el agotamiento del espacio de direcciones IPv4.
    - **Seguridad mejorada:** IPv6 integra características de seguridad como IPsec, que ofrece autenticación y cifrado para proteger el tráfico de red.
    - **Calidad de servicio (QoS):** IPv6 incluye mecanismos de QoS que permiten priorizar el tráfico sensible al tiempo, como las videollamadas y los juegos en línea.
    - **Simplificación de la configuración:** IPv6 admite la autoconfiguración de direcciones, lo que facilita la conexión de dispositivos a la red.

2. **¿Por qué no es necesario el campo “Header Length” en IPv6?**

- El campo "Header Length" (Longitud de la cabecera) no es necesario en IPv6 porque **la cabecera de IPv6 tiene una longitud fija de 40 bytes.** Esto contrasta con IPv4, donde el campo "Header Length" era necesario debido a la presencia de un campo de opciones de longitud variable que hacía que **la cabecera de IPv4 tuviera una longitud variable.**

3. **¿En qué se diferencia el checksum de IPv4 e IPv6? Y en cuánto a los campos checksum de TCP y UDP, ¿sufren alguna modificación en cuanto a su obligatoriedad de cálculo?**

- La principal diferencia en el checksum entre IPv4 e IPv6 reside en su presencia en la cabecera: **IPv4 lo incluye, mientras que IPv6 no**.
    - **IPv4: La "Suma de comprobación de cabecera"** en IPv4 permite a los routers detectar errores de bit en los datagramas. Se calcula sumando todos los pares de bytes de la cabecera con aritmética de complemento a 1. El resultado, conocido como "suma de comprobación de Internet", se almacena en el campo checksum. Los routers deben recalcular esta suma para cada datagrama, ya que el campo TTL, entre otros, puede cambiar en el trayecto. Si la suma calculada no coincide con la del datagrama, este se descarta.

- **IPv6:** Se **eliminó el campo de checksum de cabecera para simplificarla y así agilizar el procesamiento en los routers.** Se confía en los checksums de las capas superiores, como **TCP y UDP** en la capa de transporte y **Ethernet** en la capa de enlace, para la detección de errores.

4. **¿Qué sucede con el campo “Opciones” en IPv6? ¿Existe, en IPv6, alguna forma de enviar información opcional?**

- En **IPv6**, el campo **"Opciones"** ya **no forma parte de la cabecera estándar** del datagrama. Sin embargo, **no ha desaparecido por completo.**
  En lugar de estar incluido en la cabecera principal, el campo "Opciones" se implementa como una de las posibles **"siguientes cabeceras"** a las que se apunta desde la cabecera de IPv6. Esto significa que, al igual que las cabeceras de los protocolos TCP o UDP pueden ser la siguiente cabecera dentro de un paquete IP, también puede serlo un campo "Opciones".

5. **Si quisiese que IPv6 soporte una nueva funcionalidad, ¿cómo lo haría?**

- Se debería de implementar como una extensión de encabezado.

6. **¿Es necesario el protocolo ICMP en IPv6? ¿Cumple las mismas funciones que en IPv4?**

- **Sí, el protocolo ICMP es necesario en IPv6.** Aunque IPv6 simplifica algunos aspectos de la cabecera en comparación con IPv4, ICMP sigue siendo esencial para el control y la comunicación de información importante en la capa de red.
  En **IPv6**, se utiliza una nueva versión de ICMP, llamada **ICMPv6**, especificada en el RFC 4443. ICMPv6 no solo conserva las funciones principales de ICMP en IPv4, sino que también agrega nuevas funcionalidades para soportar las características específicas de IPv6.
    - **ICMP en IPv4 e IPv6 cumple funciones similares, incluyendo:**
        - **Informes de errores:** ICMP se utiliza para notificar a los hosts sobre problemas en la entrega de datagramas. Por ejemplo, si un router no puede encontrar una ruta al destino, envía un mensaje ICMP de "Destino inalcanzable" al host de origen.
        - **Mensajes de control:** ICMP se utiliza para enviar mensajes de control, como "solicitud de eco" y "respuesta de eco" utilizados en la herramienta ping. Ping se utiliza para verificar la conectividad y medir el tiempo de ida y vuelta a un host remoto.
    - **Diferencias y Nuevas Funcionalidades en ICMPv6:**
        - **Reorganización de tipos y códigos:** ICMPv6 reorganiza y redefine algunos de los tipos y códigos de mensajes ICMP existentes en IPv4.
        - **Nuevos tipos y códigos:** ICMPv6 introduce nuevos tipos y códigos para soportar las nuevas funcionalidades de IPv6. Algunos ejemplos son el mensaje "Paquete demasiado grande", utilizado cuando un

datagrama IPv6 es demasiado grande para ser reenviado por un enlace, y el código de error "Opciones IPv6 no reconocidas".

- **Integración de IGMP:** ICMPv6 integra la funcionalidad del Protocolo de Gestión de Grupos de Internet (IGMP, Internet Group Management Protocol), que se utilizaba en IPv4 para la gestión de multidifusión.

7. **¿Qué funciones cumple el protocolo Neighbour Discovery? ¿Puede funcionar IPv6 sin él? ¿Y sin una dirección de tipo link-local?**

- El protocolo Neighbour Discovery (ND) en IPv6 cumple varias funciones importantes:
  - **Descubrimiento de Routers:** Los nodos IPv6 usan ND para descubrir los routers en su enlace. Esto es crucial para que los hosts puedan enviar tráfico fuera de su propia subred.
  - **Descubrimiento de Vecinos:** Permite que los nodos en un enlace determinen las direcciones MAC de otros nodos en el mismo enlace. Esta información es necesaria para que los nodos puedan comunicarse directamente entre sí a nivel de enlace.
  - **Resolución de Direcciones:** ND reemplaza al protocolo ARP de IPv4, proporcionando un mecanismo para traducir direcciones IPv6 a direcciones MAC.
  - **Detección de Duplicados de Direcciones:** Antes de usar una dirección IPv6, un nodo la anuncia a sus vecinos para asegurarse de que ningún otro nodo ya la esté usando. Esto ayuda a prevenir conflictos de direcciones.
  - **Detección de Vecinos Inalcanzables:** ND permite que los nodos monitoreen la accesibilidad de sus vecinos. Si un vecino no responde a las solicitudes ND, se considera inalcanzable.
  - **Mantenimiento de Información de Enrutamiento:** Los routers usan ND para anunciar sus prefijos a los hosts en el enlace, proporcionando información de enrutamiento local.
  - **Redirección:** Los routers pueden usar ND para redirigir el tráfico a un router más cercano al destino.

  Ipv6 depende esencialmente de Neighbor Discovery. Sin ND, muchas de las funciones básicas de IPv6, como la autoconfiguración de direcciones, la detección de duplicados y la resolución de direcciones, no serían posibles. Esto afectaría gravemente la operación normal de una red IPv6, especialmente en redes locales (LAN).

  IPv6 no puede funcionar sin una dirección link-local, estas son necesarias porque:
  - **Comunicación local:** Todas las interfaces IPv6 deben tener al menos una dirección link-local para comunicarse con otros dispositivos en la misma red local (enlace).
  - **Neighbor Discovery y Router Discovery:** ND y otras funciones críticas, como la detección de routers y la resolución de direcciones, dependen de las direcciones link-local.
  - **Sin link-local, no hay ND:** Las operaciones de Neighbor Discovery utilizan direcciones link-local para enviar y recibir mensajes.

8. **¿Cuál de las siguientes direcciones IPv6 no son válidas?**

- **Cosas a tener en cuenta:**
    - Las direcciones IPv6 usan dígitos **hexadecimales (0-9, a-f)** en grupos de **16 bits**, separadas por **":".**
    - Ceros contiguos se pueden eliminar usando **"::",** esto **solo se pueda usar una vez.**
    - Los **ceros** al inicio de cada grupo se pueden obviar.

a. 2001:0:1019:afde::1

- Es una dirección IPv6 válida.

b. 2001::1871::4

- No es una dirección IPv6 válida, está usando más de una vez el conjunto **"::"** para representar la compresión de ceros. **2001::1871::4**

c. 3ffg:8712:0:1:0000:aede:aaaa:1211

- No es una dirección IPv6 válida, los dígitos hexadecimales van desde el 0 hasta la F, la **"g"** no está comprendida como un dígito hexadecimal. **3ffg:8712:0:1:0000:aede:aaaa:1211.**

d. 3::1

- Es una dirección IPv6 válida.

e. ::

- Es una dirección IPv6 válida, esta dirección se conoce como **dirección nula o dirección no especificada**. Representa una dirección en la que todos los bits son cero.

f. 2001::

- Es una dirección IPv6 válida.

g. 3ffe:1080:1212:56ed:75da:43ff:fe90:affe

- Es una dirección IPv6 válida.

h. 3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001

- No es una dirección IPv6 válida, al ser direcciones de 128 bits con grupos de 16 bits separados por ":" eso significa que solo podríamos tener 8 grupos de

16 bits separados por ":", en este caso hay 9 grupos.
3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001

9. **¿Cuál sería una abreviatura correcta de 3f80:0000:0000:0a00:0000:0000:0000:0845?**

    a. **3f80::a00::845**
    b. **3f80::a:845**
    c. **3f80::a00:0:0:0:845:4567**
    d. **3f80:0:0:a00::845** → Esta es la abreviatura válida.
    e. **3f8:0:0:a00::845**

10. **Indique si las siguientes direcciones son de link-local, global-address, multicast, etc.**

    a. **fe80::1/64**

    - Es una dirección **link-local.**

    b. **3ffe:4543:2:100:4398::1/64**

    - Esta es la dirección especial **6Bone que es Global Unicast**.

    c. **::**

    - Es la dirección especial **any.**

    d. **::1**

    - Es una dirección especial **Loopback/Localhost.**

    e. **ff02::2**

    - Es una dirección **Multicast.**

    f. **2818:edbc:43e1::8721:122**

    - Esta es una dirección **Global Unicast.**

    g. **ff02::9**

    - Es una dirección **Multicast.**

11. **Al autogenerarse una dirección IPv6 sus últimos 64 bits en muchas ocasiones no se deducen de la dirección MAC, se generan de forma random, ¿por qué sucede esto? ¿Qué es lo que se intenta evitar? (Ver direcciones temporarias, RFC 8981)**

- En IPv6, cuando un dispositivo autogenera una dirección, los últimos 64 bits (la **identificación de interfaz** o **IID**) pueden derivarse de diferentes maneras. Tradicionalmente, se utilizaba la **dirección MAC** del dispositivo para generar estos bits mediante el formato **EUI-64**. Sin embargo, en muchas implementaciones modernas, se generan de forma **aleatoria** o **pseudoaleatoria**. Esto se debe a preocupaciones relacionadas con la **privacidad** y la **seguridad**.
    - **Privacidad y rastreo de dispositivos:** Las direcciones MAC son únicas y estáticas. Si se utilizan para generar la IID, la dirección IPv6 también será única y constante para un dispositivo específico. Esto permite que los dispositivos sean rastreados fácilmente en diferentes redes, lo cual representa una vulnerabilidad para la **privacidad** del usuario.
    - **Identificación persistente:** Cuando un dispositivo se conecta a diferentes redes, podría ser identificado fácilmente si mantiene siempre la misma IID basada en la dirección MAC. Esto facilita que terceros (como anunciantes o atacantes) creen un perfil del dispositivo o del usuario.
    - **Seguridad:** Las direcciones basadas en MAC pueden revelar información sobre el hardware del dispositivo. Esto podría ser explotado por atacantes para identificar vulnerabilidades específicas de ciertos fabricantes o modelos.

  Solución: Direcciones aleatorias (RFC 8981)
    - El **RFC 8981** introduce la idea de usar **identificadores de interfaz aleatorios** para las direcciones IPv6. Esto se conoce como **direcciones temporales** o **Privacy Extensions**. Estas direcciones se generan de forma pseudoaleatoria y cambian periódicamente.

      Ventajas:
        - **Mejora la privacidad:** Al cambiar regularmente la dirección, se dificulta el rastreo del dispositivo.
        - **Evita la correlación entre redes:** La misma dirección no se reutiliza en diferentes redes, lo que hace más difícil identificar un dispositivo en distintas ubicaciones.

  Direcciones IPv6 temporales:
    - Además de la dirección principal (basada en el prefijo de red y la IID), un dispositivo puede generar **direcciones temporales** que utiliza para conexiones salientes. Estas direcciones temporales tienen una duración limitada y son reemplazadas periódicamente.

      Funcionamiento:
        - Se genera una IID aleatoria.
        - Se vincula con el prefijo de red local.
        - Después de un período de tiempo, se genera una nueva IID aleatoria, y la antigua se descarta.