Práctica 9 RyC

1. ¿Qué es IPv6? ¿Por qué es necesaria su implementación? 2
2. ¿Por qué no es necesario el campo "Header Length" en IPv6? 2
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? 3
4. ¿Qué sucede con el campo "Opciones" en IPv6? ¿Existe, en IPv6, alguna forma de enviar información opcional? 3
5. Si quisiese que IPv6 soporte una nueva funcionalidad, ¿cómo lo haría? 4
6. ¿Es necesario el protocolo ICMP en IPv6? ¿Cumple las mismas funciones que en IPv4? 4
7. ¿Qué funciones cumple el protocolo Neighbour Discovery? ¿Puede funcionar IPv6 sin él? 5
Funcionamiento de IPv6 sin Neighbour Discovery 5
Funcionamiento de IPv6 sin Direcciones Link-Local 6
8. ¿Cuál de las siguientes direcciones IPv6 no son válidas? 6
- 2001:0:1019:afde::1 6
- 2001::1871::4 6
- 3ffg:8712:0:1:0000:aede:aaaa:1211 6
- 3::1 6
- :: 6
- 2001:: 6
- 3ffe:1080:1212:56ed:75da:43ff:fe90:affe 6
- 3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001 6

9. ¿Cuál sería una abreviatura correcta de 3f80:0000:0000:0a00:0000:0000:0000:0845? 7
- 3f80::a00::845 7
- 3f80::a:845 7
- 3f80::a00:0:0:0:845:4567 7
- 3f80:0:0:a00::845 7
- 3f8:0:0:a00::845 7

10. Indique si las siguientes direcciones son de link-local, global-address, multicast, etc 7
- fe80::1/64 7
- 3ffe:4543:2:100:4398::1/64 7
- :: 7
- ::1 8
- ff02::2 8
- 2818:edbc:43e1::8721:122 8
- ff02::9 8

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).....8

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.

La transición de IPv4 a IPv6 ha sido gradual, ya que la infraestructura de Internet existente está basada en IPv4. Se están utilizando varios métodos para facilitar esta transición, como la tunelización, que permite encapsular el tráfico IPv6 dentro de paquetes IPv4 para atravesar redes IPv4.

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 inferiores, como TCP y UDP en la capa de transporte y Ethernet en la capa de enlace, para la detección de errores.

En cuanto a **TCP y UDP**, **ambos protocolos siguen utilizando el checksum de manera obligatoria** para asegurar la integridad de los datos. Este checksum, llamado "suma de comprobación de Internet", se calcula sobre todos los campos del segmento, incluyendo tanto la cabecera como los datos. El receptor verifica la suma de comprobación recibida y descarta el segmento si no coincide con la que calcula.

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".

Esta decisión de diseño se tomó para lograr una **cabecera de IPv6 de longitud fija (40 bytes)**, lo que **simplifica y agiliza el procesamiento del datagrama** por parte de los routers. En IPv4, la presencia del campo "Opciones" con una longitud variable complicaba el análisis de la cabecera, ya que no se podía determinar a priori dónde comenzaban los datos.

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

Extendiendo el 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?

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.

Funcionamiento de IPv6 sin Neighbour Discovery

No, IPv6 no puede funcionar sin el protocolo Neighbour Discovery. ND es esencial para el funcionamiento básico de IPv6, ya que proporciona las funciones de descubrimiento de vecinos, resolución de direcciones y enrutamiento local. Sin ND, los nodos no podrían comunicarse entre sí a nivel de enlace ni enviar tráfico fuera de su propia subred.

Funcionamiento de IPv6 sin Direcciones Link-Local

No, IPv6 no puede funcionar sin direcciones link-local. Las direcciones link-local son direcciones IPv6 que se asignan automáticamente a una interfaz y se utilizan para la comunicación dentro del mismo enlace. Son esenciales para el funcionamiento del protocolo Neighbour Discovery, ya que se utilizan en los mensajes de descubrimiento de vecinos, resolución de direcciones y detección de duplicados de direcciones.

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

■ 2001:0:1019:afde::1

■ 2001::1871::4

■ 3ffg:8712:0:1:0000:aede:aaaa:1211

■ 3::1

■ ::

■ 2001::

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

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

Las siguientes direcciones IPv6 **no son válidas**:

- **3ffg:8712:0:1:0000:aede:aaaa:1211:** Las direcciones IPv6 usan dígitos hexadecimales (0-9 y a-f). La "g" en esta dirección no es un dígito hexadecimal válido.
- **2001::1871::4:** Una dirección IPv6 solo puede tener un único conjunto de dos puntos consecutivos (::) para representar la compresión de ceros. Esta dirección tiene dos conjuntos, lo cual no es permitido.
- **3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001:** Una dirección IPv6 tiene 128 bits, lo cual se traduce en 8 grupos de 16 bits. Esta dirección tiene 9 grupos, excediendo el límite.

Las demás direcciones son válidas:

- **2001:0:1019:afde::1:** Esta es una dirección IPv6 válida, con un único conjunto de dos puntos (::) representando la compresión de ceros al final.

- **3::1:** Esta es una dirección IPv6 válida, con un único conjunto de dos puntos (::) representando la compresión de ceros al principio.
- **:::** Esta es la dirección IPv6 no especificada, una dirección especial que no se puede asignar a una interfaz.
- **2001:::** Esta es una dirección IPv6 válida, con un único conjunto de dos puntos (::) representando la compresión de ceros al final.
- **3ffe:1080:1212:56ed:75da:43ff:fe90:affe:** Esta es una dirección IPv6 válida, con 8 grupos de 16 bits.

Formato de: RFC 2460 y RFC 4291.

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

■ 3f80::a00::845

■ 3f80::a:845

■ 3f80::a00:0:0:0:845:4567

■ 3f80:0:0:a00::845

■ 3f8:0:0:a00::845

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

■ fe80::1/64

Las direcciones link-local comienzan con el prefijo `fe80::/10`. Son direcciones que se asignan automáticamente a una interfaz.

■ 3ffe:4543:2:100:4398::1/64

Global unicast. Estas direcciones se usan para la comunicación global en Internet.

■ ::

Cualquiera.

■ ::1

Loopback. Similar a 127.0.0.1 en IPv4, se usa para que un nodo se envíe tráfico a sí mismo.

■ ff02::2

Multicast. Las direcciones multicast se usan para enviar un único paquete a un grupo de nodos. El prefijo `ff02::/16` se usa para multicast a nivel de enlace local.

■ 2818:edbc:43e1::8721:122

Global unicast.

■ ff02::9

Multicast. El prefijo `ff02::/16` se usa para multicast a nivel de enlace local.

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)

La autogeneración de direcciones IPv6, donde los últimos 64 bits son generados de forma aleatoria en lugar de deducirse de la dirección MAC, se realiza principalmente para **mejorar la privacidad del usuario**. Esta técnica se describe en el RFC 8981, que introduce el concepto de **direcciones IPv6 temporales**.

¿Qué se intenta evitar con la generación aleatoria?

Al generar aleatoriamente los últimos 64 bits de una dirección IPv6, se busca evitar la **correlación entre la dirección IP y la dirección MAC del dispositivo**. Si los últimos 64 bits se dedujeran directamente de la dirección MAC, sería posible rastrear la actividad de un dispositivo a través de diferentes redes y a lo largo del tiempo. Esto podría utilizarse para:

- **Crear perfiles de usuario:** Las empresas y anunciantes podrían recopilar información sobre los hábitos de navegación, las aplicaciones utilizadas y los sitios web visitados por un usuario, incluso si cambia de red.

- **Rastrear la ubicación física:** La dirección MAC, al ser un identificador único del dispositivo, podría utilizarse para rastrear la ubicación física de un usuario a medida que se mueve entre diferentes redes.
- **Ataques de seguridad:** Los atacantes podrían utilizar la correlación entre la dirección IP y la MAC para realizar ataques de denegación de servicio o para interceptar el tráfico de un usuario.

Direcciones IPv6 temporales

El uso de direcciones IPv6 temporales, con los últimos 64 bits generados aleatoriamente, ayuda a mitigar estos riesgos de privacidad. Las direcciones temporales cambian periódicamente, lo que dificulta el rastreo de un dispositivo. El RFC 8981 recomienda que los sistemas operativos generen y utilicen direcciones temporales de forma predeterminada para la comunicación con otros nodos.