1. **¿Cuál es la función de la capa de red en el modelo OSI? ¿Qué implementaciones conoce? ¿Qué es IPv6? ¿Por qué es necesaria su implementación?**

**Función de la capa de red en el modelo OSI**

La capa de red es la tercera capa del modelo OSI y se encarga de la gestión de la transmisión de datos entre diferentes redes, proporcionando direcciones lógicas y la capacidad de enrutar la información hacia su destino correcto. Sus principales funciones incluyen:

* Enrutamiento: Seleccionar la ruta más adecuada para que los datos lleguen a su destino.
* Direccionamiento lógico: Asignar direcciones lógicas (como las direcciones IP) a dispositivos en la red.
* Encapsulación y desencapsulación: Agregar información de encabezado a los datos que incluyen la dirección de origen y destino.
* Fragmentación: Dividir grandes paquetes en fragmentos más pequeños si la red subyacente no puede manejar paquetes de ese tamaño.
* Control de congestión: Evitar la congestión en la red, gestionando el tráfico de datos de manera eficiente.

**Implementaciones comunes**

Algunas implementaciones y protocolos que operan en la capa de red son:

IP (Protocolo de Internet):

* IPv4 (Internet Protocol version 4): Utiliza direcciones de 32 bits, lo que permite aproximadamente 4.3 mil millones de direcciones únicas. Es el protocolo más ampliamente implementado, aunque presenta limitaciones en la cantidad de direcciones disponibles.
* IPv6 (Internet Protocol version 6): Utiliza direcciones de 128 bits, lo que permite una cantidad de direcciones prácticamente ilimitada, siendo su adopción clave para el crecimiento de Internet.
* ICMP (Protocolo de Mensajes de Control de Internet): Utilizado para diagnosticar problemas en la red, como en herramientas de ping o traceroute.
* RIP (Routing Information Protocol), OSPF (Open Shortest Path First) y BGP (Border Gateway Protocol): Protocolos de enrutamiento que determinan las mejores rutas para el tráfico en la red.

**¿Qué es IPv6 y por qué es necesaria su implementación?**

IPv6 es la sexta versión del Protocolo de Internet (IP) y fue desarrollado para resolver los problemas de escasez de direcciones IP en IPv4. Algunas características clave de IPv6 incluyen:

* Direcciones más largas: Utiliza direcciones de 128 bits (en comparación con los 32 bits de IPv4), lo que permite un número de direcciones muchísimo mayor (2^128 direcciones).
* Autoconfiguración: IPv6 permite la autoconfiguración de las direcciones IP, lo que facilita la gestión de grandes redes.
* Seguridad integrada: IPv6 tiene soporte nativo para IPsec, un conjunto de protocolos para asegurar las comunicaciones.
* Eficiencia en el enrutamiento: El encabezado de IPv6 está optimizado para mejorar el enrutamiento y la entrega de paquetes.
* Movilidad mejorada: IPv6 ofrece mejor soporte para la movilidad de dispositivos, permitiendo que los dispositivos cambien de red sin perder su conectividad.

**¿Por qué es necesaria su implementación?**

La principal razón para implementar IPv6 es la escasez de direcciones IPv4. Con el crecimiento de Internet, dispositivos móviles, y tecnologías como el Internet de las Cosas (IoT), la demanda de direcciones IP ha superado la capacidad de IPv4. Además de resolver este problema, IPv6 también mejora aspectos de seguridad, eficiencia y escalabilidad, fundamentales para el futuro de la infraestructura de Internet.

En resumen, IPv6 es crucial para asegurar que Internet pueda seguir creciendo y soportar la creciente demanda de dispositivos conectados.

1. **Tomando un diagrama o una captura de un datagrama IPv4 e IPv6 indique la funcionalidad u objetivo de cada campo.**

Encabezado IPv4 (Formato básico)

Los campos y su funcionalidad en un datagrama IPv4 incluyen:

* Version: Indica la versión del protocolo (4 para IPv4).
* Header Length (IHL): Indica la longitud del encabezado en múltiplos de 4 bytes.
* Type of Service (ToS): Define la prioridad y calidad del servicio.
* Total Length: Longitud total del paquete IP (incluye datos).
* Identification: Identifica fragmentos de un datagrama dividido.
* Flags: Controla la fragmentación.
* Fragment Offset: Posición del fragmento dentro del datagrama.
* Time to Live (TTL): Limita el tiempo que un paquete puede permanecer en la red.
* Protocol: Indica el protocolo en la capa de transporte (TCP, UDP, etc.).
* Header Checksum: Verifica errores en el encabezado.
* Source IP Address: Dirección IP de origen.
* Destination IP Address: Dirección IP de destino.
* Options: Opciones adicionales que pueden ser usadas (ej. seguridad, enrutamiento).

Encabezado IPv6 (Formato básico)

* Version: Indica la versión del protocolo (6 para IPv6).
* Traffic Class: Define la prioridad y calidad del servicio.
* Flow Label: Identifica flujos de paquetes para el tratamiento especial.
* Payload Length: Longitud del campo de datos (equivalente al total length en IPv4).
* Next Header: Indica el protocolo de la capa superior (equivalente al campo "Protocol" de IPv4).
* Hop Limit: Similar a TTL en IPv4; limita la cantidad de saltos.
* Source Address: Dirección IP de origen.
* Destination Address: Dirección IP de destino.

**● Si un paquete llega a un router con un TTL = 1, ¿qué hace el router? ¿Cómo se llama el campo TTL en IPv6?**

En IPv4, si un paquete llega a un router con un TTL (Time to Live) de 1, el router descarta el paquete y envía un mensaje ICMP de "Time Exceeded" al origen del paquete. Esto ocurre porque el TTL llega a cero y su propósito es evitar que los paquetes se queden en la red de forma indefinida.

En IPv6, el campo equivalente es el Hop Limit. Funciona de manera similar al TTL: se decrementa en cada salto y, cuando llega a cero, el paquete es descartado.

**● ¿En qué se diferencia el checksum de IPv4 e IPv6? Y en cuanto a los campos checksum de TCP y UDP, ¿sufren alguna modificación? Si un paquete tiene un error de checksum cuando llega a un router ¿qué sucede en IPv4 y en IPv6?**

En IPv4, existe un campo Header Checksum que verifica errores solo en el encabezado del paquete.

En IPv6, no hay un campo de checksum en el encabezado, ya que la eliminación de este campo reduce la carga de procesamiento en los routers, mejorando el rendimiento. Además, se confía en los mecanismos de la capa de transporte (como TCP/UDP) y otras capas para la verificación de errores.

Checksum de TCP y UDP:

En IPv4, el checksum de TCP y UDP incluye las direcciones IP de origen y destino, el protocolo y los datos de la capa de transporte.

En IPv6, los checksums de TCP y UDP incluyen un pseudoencabezado que tiene las direcciones de origen y destino de IPv6, pero el cálculo sigue siendo esencialmente el mismo que en IPv4.

Si un paquete tiene un error de checksum:

En IPv4, el router descarta el paquete y, dependiendo del tipo de error, podría enviar un mensaje ICMP al origen.

En IPv6, no hay checksum a nivel de red, por lo que los errores se detectan y manejan en la capa de transporte o aplicación, y el router simplemente descarta los paquetes incorrectos.

● **¿Por qué no es necesario el campo Header Length en IPv6?**

El campo Header Length (IHL) no es necesario en IPv6 porque el tamaño del encabezado es fijo (40 bytes). En IPv4, el encabezado tiene una longitud variable debido a las posibles opciones adicionales, por lo que se requiere el campo IHL. En IPv6, cualquier funcionalidad extra se maneja a través de los headers extendidos, que se agregan fuera del encabezado básico.

**● Si quisiese que IPv4 soporte una nueva funcionalidad, ¿cómo lo haría? ¿y en IPv6?**

En IPv4, una nueva funcionalidad generalmente se añade utilizando el campo Options en el encabezado. Sin embargo, esto puede aumentar la longitud del encabezado y complicar el procesamiento en los routers, además de que las opciones no siempre son soportadas de manera eficiente por todos los dispositivos.

En IPv6, la arquitectura está diseñada para ser más flexible y escalable. Las nuevas funcionalidades se pueden implementar usando headers de extensión, que permiten agregar información adicional sin sobrecargar el encabezado básico. Esto facilita la introducción de nuevas características sin afectar la velocidad de procesamiento o compatibilidad con routers que no soporten la extensión.

1. **¿Qué es una red clase A? ¿Qué es una red clase B? ¿Qué es una red clase C? ¿Cuántas hay de cada una? ¿Cuántos hosts pueden haber en cada una? ¿Existen clases en IPv6? ¿Qué significa que el actual direccionamiento sea classless?**

El sistema de **clases de red en IPv4** fue una forma inicial de dividir el espacio de direcciones IP para asignar redes de diferentes tamaños. Existen tres clases principales, cada una con un rango específico de direcciones IP y una cantidad máxima de hosts que pueden tener.

**Red Clase A**

* **Rango de direcciones**: 0.0.0.0 - 127.255.255.255
* **Primer octeto**: El primer bit es siempre 0.
* **Máscara de red predeterminada**: 255.0.0.0 (/8).
* **Cantidad de redes**: Hay 128 redes de clase A posibles (2^7).
* **Hosts por red**: Cada red de clase A puede tener hasta **16,777,214 hosts** (2^24 - 2, porque se excluyen las direcciones de red y broadcast).
* **Uso típico**: Utilizadas para grandes organizaciones y grandes redes con un número significativo de dispositivos.

**Red Clase B**

* **Rango de direcciones**: 128.0.0.0 - 191.255.255.255
* **Primer octeto**: El primer bit es 1 y el segundo bit es 0.
* **Máscara de red predeterminada**: 255.255.0.0 (/16).
* **Cantidad de redes**: Hay 16,384 redes de clase B posibles (2^14).
* **Hosts por red**: Cada red de clase B puede tener hasta **65,534 hosts** (2^16 - 2).
* **Uso típico**: Asignadas a medianas y grandes organizaciones.

**Red Clase C**

* **Rango de direcciones**: 192.0.0.0 - 223.255.255.255
* **Primer octeto**: Los tres primeros bits son 110.
* **Máscara de red predeterminada**: 255.255.255.0 (/24).
* **Cantidad de redes**: Hay 2,097,152 redes de clase C posibles (2^21).
* **Hosts por red**: Cada red de clase C puede tener hasta **254 hosts** (2^8 - 2).
* **Uso típico**: Redes pequeñas, como redes de oficinas o redes domésticas.

**Redes de clase D y E**

* **Clase D**: Usada para multicast (rango 224.0.0.0 - 239.255.255.255).
* **Clase E**: Reservada para uso futuro o experimental (rango 240.0.0.0 - 255.255.255.255).

**¿Existen clases en IPv6?**

No, **IPv6 no utiliza clases** de red como IPv4. En lugar de clases, IPv6 adopta un esquema de direccionamiento **classless** que asigna prefijos de longitud variable para definir las redes, lo que otorga más flexibilidad en la asignación de direcciones.

**¿Qué significa que el actual direccionamiento sea "classless"?**

El **direccionamiento classless** o **CIDR (Classless Inter-Domain Routing)**, introducido en la década de 1990, elimina las restricciones rígidas de las clases de red. En lugar de asignar redes en bloques de tamaño fijo (clases A, B, C), **CIDR** permite definir el tamaño de una red mediante una **longitud de prefijo**, lo que permite un uso más eficiente del espacio de direcciones. Por ejemplo, una red puede tener una máscara de red /12, /22, o cualquier longitud entre 0 y 32, lo que permite adaptarse a las necesidades específicas de cada red.

1. **¿Cuál es la función de la máscara de red? ¿Qué otra notación alternativa se puede utilizar? ¿Cuál se utiliza en IPv6 y por qué?**

La **máscara de red** tiene como función **distinguir la parte de red y la parte de host** dentro de una dirección IP. Se usa para determinar a qué subred pertenece un dispositivo y ayuda a los routers a decidir cómo enrutar los paquetes.

* **Ejemplo**: En una red con la dirección IP 192.168.1.10 y una máscara 255.255.255.0, la máscara indica que los primeros 24 bits de la dirección pertenecen a la red (192.168.1), y los 8 bits restantes son para identificar los hosts (en este caso, el host es 10).

**Notación alternativa: CIDR**

La **notación CIDR** (Classless Inter-Domain Routing) es una forma más concisa de representar una red. En lugar de escribir la máscara de red completa (por ejemplo, 255.255.255.0), se indica la longitud del prefijo en bits. Ejemplo:

* **192.168.1.10/24**: Indica que los primeros 24 bits son la parte de red.

**¿Cuál se utiliza en IPv6 y por qué?**

En **IPv6**, la máscara de red se representa mediante una **longitud de prefijo** (similar al concepto de CIDR en IPv4), y la máscara más comúnmente utilizada es **/64**. Esto significa que los primeros 64 bits de la dirección IP se utilizan para identificar la **red**, mientras que los 64 bits restantes están destinados para identificar a los **hosts** dentro de esa red.

**¿Por qué /64 es el prefijo más común en IPv6?**

1. **Autoconfiguración de direcciones**: En IPv6, el prefijo **/64** es necesario para que los dispositivos puedan utilizar la **autoconfiguración sin estado** (SLAAC). Este mecanismo permite que los dispositivos generen automáticamente su dirección IPv6 sin la necesidad de un servidor DHCP.
2. **Balance entre red y hosts**: Con **/64**, se permiten **18.4 quintillones de hosts** por cada subred, lo que es una cantidad muy grande en comparación con las necesidades actuales. Aunque parece una sobreasignación de espacio, facilita la administración y simplifica la creación de subredes.

**Otras máscaras de red en IPv6**

* **/48**: Suele asignarse a empresas o grandes organizaciones que necesitan dividir su red en múltiples subredes **/64**.
* **/56**: A veces asignada a pequeñas organizaciones o para uso en redes de consumidores.
* **/128**: Se usa para identificar un único host (similar a una dirección IP individual en IPv4).

Aunque **/64** es el prefijo estándar y más utilizado para las subredes en IPv6, la flexibilidad de IPv6 permite asignar prefijos más cortos (como /48 o /56) según las necesidades de la red y la cantidad de subredes requeridas.

1. **Dada la red IP 65.0.0.0/8. Se necesitan definir 934 subredes. Indique qué máscara debería ser utilizada. Indique cuál sería la subred número 817 indicando el rango de direcciones asignables, dirección de red y broadcast.**

255.255.192.0

65.255.76.0/18

1. **Dada la red IP 195.200.45.0/24. Se necesitan definir 9 subredes. Indique la máscara utilizada y las nueve subredes. Luego tome una de ellas e indique el rango de direcciones asignables en esa subred, dirección de red y broadcast**

255.255.255.15

195.200.45.0/28 195.200.45.1/28 195.200.45.2/28

195.200.45.3/28 195.200.45.4/28 195.200.45.5/28

195.200.45.6/28 195.200.45.7/28 195.200.45.8/28

Red 195.200.45.0 : 195.200.45.1 – 195.200.45.14

1. **Indicar las clases de las siguientes direcciones, ¿Cuáles son direcciones privadas?**

● 172.16.7.12 ● 200.5.123.221 ● 224.0.0.9 ● 10.10.1.10 ● 172.15.7.98

● 192.168.10.5 ● 240.32.34.2 ● 1.1.1.1 ● 8.8.8.8 ● 239.12.34.3

 **172.16.7.12**

* **Clase**: B
* **Privada**: Sí, las direcciones en el rango 172.16.0.0 - 172.31.255.255 son privadas.

 **200.5.123.221**

* **Clase**: C
* **Privada**: No, es una dirección pública.

 **224.0.0.9**

* **Clase**: D (multicast)
* **Privada**: No, las direcciones de clase D son usadas para multicast.

 **10.10.1.10**

* **Clase**: A
* **Privada**: Sí, las direcciones en el rango 10.0.0.0 - 10.255.255.255 son privadas.

 **172.15.7.98**

* **Clase**: B
* **Privada**: No, está fuera del rango de direcciones privadas de clase B (172.16.0.0 - 172.31.255.255).

 **192.168.10.5**

* **Clase**: C
* **Privada**: Sí, las direcciones en el rango 192.168.0.0 - 192.168.255.255 son privadas.

 **240.32.34.2**

* **Clase**: E (reservada para uso experimental)
* **Privada**: No, las direcciones de clase E no se usan para la comunicación regular.

 **1.1.1.1**

* **Clase**: A
* **Privada**: No, es una dirección pública.

 **8.8.8.8**

* **Clase**: A
* **Privada**: No, es una dirección pública (utilizada por Google para DNS).

 **239.12.34.3**

* **Clase**: D (multicast)
* **Privada**: No, es una dirección de clase D para multicast.

**8. Para cada una de las siguientes direcciones obtener (si corresponde):**

**Dirección y Clase (A,B,C) de Red.**

**Pública/Privada/Reservada/Inválida.**

**Dirección de Subred y Dirección de Broadcast.**

**Cantidad posibles de redes si toda la red se hubiese “subneteado” con la misma máscara.**

**Cantidad de IP para hosts por subred utilizables.**

● 163.10.5.66/26 ● 127.0.0.1/8 ● 20.6.20.1/18 ● 200.5.10.3/30 ● 172.18.10.0/26

**1. 163.10.5.66/26**

* **Clase**: B
* **Pública/Privada**: Pública
* **Dirección de Red**: 163.10.5.64
* **Dirección de Subred**: 163.10.5.64 (subred obtenida del prefijo /26)
* **Dirección de Broadcast**: 163.10.5.127
* **Cantidad de posibles subredes**:
  + En una red Clase B (por defecto /16), al usar /26, se han tomado 10 bits adicionales para subnetting.
  + **Posibles subredes**: 210=10242^{10} = 1024210=1024 subredes.
* **Cantidad de IP para hosts utilizables por subred**:
  + Con un prefijo /26, hay 6 bits disponibles para hosts.
  + **IP de hosts utilizables**: 26−2=622^6 - 2 = 6226−2=62 hosts.

**2. 127.0.0.1/8**

* **Clase**: A
* **Pública/Privada**: Reservada (Loopback)
* **Dirección de Red**: No aplica (es la dirección de loopback, no se utiliza para redes reales)
* **Dirección de Subred**: No aplica
* **Dirección de Broadcast**: No aplica
* **Cantidad de posibles subredes**: No aplica
* **Cantidad de IP para hosts por subred utilizables**: No aplica

**3. 20.6.20.1/18**

* **Clase**: A
* **Pública/Privada**: Pública
* **Dirección de Red**: 20.6.0.0
* **Dirección de Subred**: 20.6.0.0 (subred obtenida del prefijo /18)
* **Dirección de Broadcast**: 20.6.63.255
* **Cantidad de posibles subredes**:
  + En una red Clase A (por defecto /8), al usar /18, se han tomado 10 bits adicionales para subnetting.
  + **Posibles subredes**: 210=10242^{10} = 1024210=1024 subredes.
* **Cantidad de IP para hosts utilizables por subred**:
  + Con un prefijo /18, hay 14 bits disponibles para hosts.
  + **IP de hosts utilizables**: 214−2=163822^{14} - 2 = 16382214−2=16382 hosts.

**4. 200.5.10.3/30**

* **Clase**: C
* **Pública/Privada**: Pública
* **Dirección de Red**: 200.5.10.0
* **Dirección de Subred**: 200.5.10.0 (subred obtenida del prefijo /30)
* **Dirección de Broadcast**: 200.5.10.3
* **Cantidad de posibles subredes**:
  + En una red Clase C (por defecto /24), al usar /30, se han tomado 6 bits adicionales para subnetting.
  + **Posibles subredes**: 26=642^6 = 6426=64 subredes.
* **Cantidad de IP para hosts utilizables por subred**:
  + Con un prefijo /30, hay 2 bits disponibles para hosts.
  + **IP de hosts utilizables**: 22−2=22^2 - 2 = 222−2=2 hosts (es comúnmente utilizada en enlaces punto a punto).

**5. 172.18.10.0/26**

* **Clase**: B
* **Pública/Privada**: Privada (rango privado 172.16.0.0 - 172.31.255.255)
* **Dirección de Red**: 172.18.10.0
* **Dirección de Subred**: 172.18.10.0 (subred obtenida del prefijo /26)
* **Dirección de Broadcast**: 172.18.10.63
* **Cantidad de posibles subredes**:
  + En una red Clase B (por defecto /16), al usar /26, se han tomado 10 bits adicionales para subnetting.
  + **Posibles subredes**: 210=10242^{10} = 1024210=1024 subredes.
* **Cantidad de IP para hosts utilizables por subred**:
  + Con un prefijo /26, hay 6 bits disponibles para hosts.
  + **IP de hosts utilizables**: 26−2=622^6 - 2 = 6226−2=62 hosts.

**9. ¿Cuáles de las siguientes no son direcciones IPv6 válidas, cuáles asignables a un host?**

● 2001:0:1019:afde::1 ● 2001::1871::4 ● 3ffg:8712:0:1:0000:aede:aaaa:1211 ● 3::1

● 3ffe:1080:1212:56ed:75da:43ff:fe90:affe ● :: ● 2001::

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

**1. 2001:0:1019:afde::1**

* **Válida**: Sí.
* **Asignable a un host**: Sí. Esta dirección es válida y está completa, por lo que puede asignarse a un host.

**2. 2001::1871::4**

* **Válida**: No.
  + Una dirección IPv6 no puede tener dos secuencias de doble dos puntos (::). Solo se puede usar una vez para indicar una secuencia de ceros.
* **Asignable a un host**: No, es una dirección malformada.

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

* **Válida**: No.
  + El carácter "g" no es válido en el sistema hexadecimal (solo se permiten dígitos del 0 al 9 y letras de la "a" a la "f").
* **Asignable a un host**: No, debido a caracteres no válidos.

**4. 3::1**

* **Válida**: Sí.
* **Asignable a un host**: Sí. Esta dirección es válida y puede ser asignada a un host.

**5. 3ffe:1080:1212:56ed:75da:43ff:fe90**

* **Válida**: Sí.
* **Asignable a un host**: Sí. Esta es una dirección completa de 128 bits y puede ser asignada a un host.

**6. ::**

* **Válida**: Sí.
  + Esta es una dirección especial que representa la dirección "no especificada" (equivalente a 0.0.0.0 en IPv4).
* **Asignable a un host**: No. No puede asignarse a un host ya que es usada para identificar la ausencia de una dirección.

**7. 2001::**

* **Válida**: Sí.
* **Asignable a un host**: No. Esta es la dirección de red, utilizada para identificar el bloque de direcciones. No puede ser asignada a un host.

**8. 3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001**

* **Válida**: No.
  + Esta dirección tiene más de 8 bloques (9 bloques), lo cual excede el límite de 128 bits para direcciones IPv6.
* **Asignable a un host**: No, es una dirección malformada.

**10. ¿Cómo se podrían sumarizar las siguientes direcciones aplicando CIDR? 200.10.0.0/24 200.10.1.0/24 200.10.2.0/24 200.10.3.0/24**

Para sumarizar las siguientes direcciones aplicando **CIDR (Classless Inter-Domain Routing)**, es necesario encontrar la cantidad mínima de bits comunes entre ellas y crear una única red que las englobe a todas.

Las direcciones proporcionadas son:

* 200.10.0.0/24
* 200.10.1.0/24
* 200.10.2.0/24
* 200.10.3.0/24

Primero, convertimos las direcciones en binario para observar los bits comunes:

* **200.10.0.0/24** → 11001000.00001010.00000000.00000000
* **200.10.1.0/24** → 11001000.00001010.00000001.00000000
* **200.10.2.0/24** → 11001000.00001010.00000010.00000000
* **200.10.3.0/24** → 11001000.00001010.00000011.00000000

Si comparamos los bits, observamos que los primeros **22 bits** son comunes en todas las direcciones. Por lo tanto, podemos sumarizarlas como una única red **/22**:

* **Dirección sumarizada**: 200.10.0.0/22

**Explicación:**

* La red **200.10.0.0/22** cubre el rango de direcciones desde **200.10.0.0** hasta **200.10.3.255**, lo que incluye todas las direcciones originales:
  + 200.10.0.0/24
  + 200.10.1.0/24
  + 200.10.2.0/24
  + 200.10.3.0/24

Esta es la red más eficiente que abarca todas las direcciones proporcionadas.

**11. ¿Cómo quedará la sumarización si necesita agrupar las 8 primeras redes (hasta las 200.10.7.0/24)**

200.10.0.0 🡪 200.10.00000000.00000000

200.10.7.0 🡪 200.10.00000111.00000000

Direccion sumarizada

200.10.0.0/21

**12. Y las siguientes: 195.80.0.0/24 195.80.1.0/24 195.80.2.0/24**

195.80.0.0/24 🡪 195.80.00000000.0

195.80.1.0/24 🡪 195.80.00000001.0

195.80.2.0/24 🡪 195.80.00000010.0

8 + 8 + 6 = 22bits

Direccion sumarizada: 195.80.0.0/22

**13. Dada la red IP 195.200.45.0/25. Se necesitan definir 6 subredes de 6 host c/u. Indique la máscara utilizada y la subred número 4.**

195.200.45.0/25

Mascara de red: 255.255.255.128 🡪 11111111.11111111.11111111.10000000

6 hosts necesitan 3bits (2^3 – 2(direcciones de broadcast y red) =6 hosts posibles)

Mascara de red: 255.255.255.128 🡪 11111111.11111111.11111111.11111000

195.200.45.0/29

Al usar la máscara **/29**, las subredes se incrementan de 8 en 8 (porque 232−29=82^{32-29} = 8232−29=8).

Las subredes serían:

1. **195.200.45.0/29** (rango de direcciones: 195.200.45.0 - 195.200.45.7)
2. **195.200.45.8/29** (rango de direcciones: 195.200.45.8 - 195.200.45.15)
3. **195.200.45.16/29** (rango de direcciones: 195.200.45.16 - 195.200.45.23)
4. **195.200.45.24/29** (rango de direcciones: 195.200.45.24 - 195.200.45.31)
5. **195.200.45.24/29** (rango de direcciones: 195.200.45.32 - 195.200.45.39)
6. **195.200.45.24/29** (rango de direcciones: 195.200.45.40 - 195.200.45.47)
7. **195.200.45.24/29** (rango de direcciones: 195.200.45.48 - 195.200.45.55)
8. **195.200.45.24/29** (rango de direcciones: 195.200.45.56 - 195.200.45.63)

**Subred número 4:**

* **Dirección de red**: 195.200.45.24/29
* **Rango de direcciones IP para hosts**: 195.200.45.25 - 195.200.45.30
* **Dirección de broadcast**: 195.200.45.31

Imagen que contiene Gráfico radial

Descripción generada automáticamente

Entre switch 1 y A

172.16.2.1/27

Clase B

Mascara subred: 255.255.255.224

Dirección de red: 172.16.2.0

Dirección de Broadcast: 172.16.2.31

Entre switch 1 y A

172.16.2.1/27

Clase B

Mascara subred: 255.255.255.224

Dirección de red: 172.16.2.0

Dirección de Broadcast: 172.16.2.31

**19. ¿Para qué sirve el protocolo ARP?**

El **Protocolo de Resolución de Direcciones (ARP)** se utiliza para mapear una dirección IP a una dirección MAC (dirección de enlace de capa 2) en redes locales. Cuando un dispositivo en una red conoce la dirección IP de destino pero no su dirección MAC, ARP se encarga de resolver esto para que la comunicación pueda ocurrir en la capa de enlace.

* **Función principal**: Traducir direcciones IP (Capa 3) a direcciones MAC (Capa 2) en una red local (LAN).

**¿En qué protocolos de enlace no sería necesario?**

ARP no es necesario en **protocolos de enlace que no usan direcciones MAC**. Algunos ejemplos:

* **Point-to-Point Protocol (PPP)**: Usado en conexiones punto a punto donde no hay necesidad de una dirección MAC.
* **Frame Relay o ATM**: Son tecnologías de capa de enlace que no usan direcciones MAC, por lo que ARP no es necesario.

**¿Es necesario en IPv6?**

No, **ARP no es necesario en IPv6**. En su lugar, **IPv6 utiliza Neighbor Discovery Protocol (NDP)** para la resolución de direcciones. NDP tiene una función similar a ARP pero con mejoras adicionales para el manejo de descubrimiento de routers, autoconfiguración de direcciones y detección de duplicados.

**20. ¿A qué dirección L2 se envían los mensajes ARP Request? ¿Y los ARP Reply?**

* **ARP Request**: Cuando un host envía una solicitud ARP (ARP Request), se dirige a la **dirección MAC de broadcast** en la red local, que es **FF:FF:FF:FF:FF**

. Esto asegura que todos los dispositivos en la red reciban la solicitud.

* **ARP Reply**: La respuesta ARP (ARP Reply), una vez que un dispositivo ha identificado que tiene la dirección IP solicitada, se envía directamente al solicitante, es decir, a la **dirección MAC del dispositivo que hizo la solicitud** (una dirección unicast).

**21. ¿Los mensajes ARP son re-enviados por los routers? Justifique**

No, **los mensajes ARP no son reenviados por los routers**.

**Justificación:**

ARP es un protocolo que opera exclusivamente en la **red local (LAN)** y solo entre dispositivos que están en la misma red. Los routers, por diseño, **segmentan las redes** y no propagan tráfico de capa de enlace entre redes diferentes. Si un dispositivo necesita comunicarse con otro que está en una red diferente, el router actúa como intermediario y la resolución de ARP se realiza dentro de cada red local, pero no se propagan las solicitudes o respuestas ARP entre redes.