Practica 7 redes y comunicaciones

Introduccion

1. ¿Qué servicios presta la capa de red? ¿Cuál es la PDU en esta capa? ¿Qué dispositivo es considerado sólo de la capa de red?

- La capa de red de Internet proporciona enrutamiento y reenvío de paquetes solo con **mejor esfuerzo**. Esto significa que no hay garantías con respecto al tiempo, el orden o la entrega de los paquetes.
- La PDU (Unidad de Datos de Protocolo) en la capa de red se llama **datagrama**.
- El dispositivo considerado sólo de la capa de red es el **router**.

2. ¿Por qué se lo considera un protocolo de mejor esfuerzo?

Esto significa que no hay garantías con respecto al tiempo, el orden o la entrega de los paquetes pero hace todo lo posible para lograrlo.

3. ¿Cuántas redes clase A, B y C hay? ¿Cuántos hosts como máximo pueden tener cada una?

Clase de Red	Cantidad Máxima de Redes	Cantidad Máxima de Hosts
A	128	16,777,214
B	16,384	65,534
C	2,097,152	254

Explicación:

- **Clase A:** Utiliza 8 bits para la dirección de red y 24 bits para la dirección de host.
- **Clase B:** Utiliza 16 bits para la dirección de red y 16 bits para la dirección de host.
- **Clase C:** Utiliza 24 bits para la dirección de red y 8 bits para la dirección de host.

4. ¿Qué son las subredes? ¿Por qué es importante siempre especificar la máscara de subred asociada?

- Una **subred** es una subdivisión lógica de una red IP. Se utiliza para dividir una red grande en redes más pequeñas y manejables. Todos los dispositivos dentro de una subred comparten la misma dirección de subred. Para determinar las subredes, se desconecta cada interfaz de su host o router, creando islas de redes aisladas. Cada una de estas islas se considera una subred.

- La **máscara de subred** es un valor que se usa para determinar qué parte de una dirección IP identifica la red y qué parte identifica el host. Es esencial especificar la máscara de subred asociada porque:

    - Permite a los dispositivos de la red determinar si un destino está dentro de la misma subred o en una subred diferente.
    - Define el tamaño de la subred, es decir, la cantidad de hosts que puede contener.
    - Facilita el enrutamiento, ya que los routers pueden usar la máscara de subred para determinar la mejor ruta para un paquete.
- **Ejemplo:**

    - Una dirección IP: 192.168.1.100
    - Una máscara de subred: 255.255.255.0
- En este caso, los primeros 24 bits de la máscara de subred (que corresponden a los tres octetos 255) indican la parte de red de la dirección IP, mientras que los últimos 8 bits (correspondientes al octeto 0) indican la parte de host. Por lo tanto, la dirección de subred sería 192.168.1.0 y la dirección de host sería 100.

5. ¿Cuál es la finalidad del campo Protocol en la cabecera IP? ¿A qué campos de la capa de transporte se asemeja en su funcionalidad?

El campo "Protocol" en la cabecera de un datagrama IP se utiliza para indicar el **protocolo específico de la capa de transporte** al que se deben entregar los datos contenidos en ese datagrama. Este campo solo se utiliza cuando el datagrama llega a su destino final.

Existe una lista completa de valores y sus correspondientes protocolos en el documento "IANA Protocol Numbers".

Similitud con la capa de transporte

El campo "Protocol" en la cabecera IP es **análogo al campo que almacena el número de puerto** en un segmento de la capa de transporte. Ambos campos sirven para **enlazar dos capas adyacentes en el modelo de red**.

División en subredes

6. Para cada una de las siguientes direcciones IP (172.16.58.223/26, 163.10.5.49/27, 128.10.1.0/23, 10.1.0.0/24, 8.40.11.179/12) determine:

a. ¿De qué clase de red es la dirección dada (Clase A, B o C)?

Para determinar la clase de red a la que pertenece una dirección IP, es necesario observar el valor del primer octeto (los primeros 8 bits) de la dirección.

Tabla de Clases de Red

Clase	Primer octeto (decimal)	Bits para red	Bits para host
A	1-126	8	24
B	128-191	16	16
C	192-223	24	8

- **172.16.58.223/26**: **Clase B**. El primer octeto es 172, lo que cae dentro del rango de las direcciones de clase B.
- **163.10.5.49/27**: **Clase B**. Similar al caso anterior, el primer octeto (163) indica que pertenece a la clase B.
- **128.10.1.0/23**: **Clase B**. El primer octeto es 128, que corresponde al inicio del rango de direcciones de clase B.
- **10.1.0.0/24**: **Clase A**. El primer octeto es 10, lo que la ubica dentro del rango de direcciones de clase A.
- **8.40.11.179/12**: **Clase A**. El primer octeto es 8, por lo que se clasifica como clase A.

b. ¿Cuál es la dirección de subred?

Para determinar la dirección de subred de una dirección IP con su máscara de subred, se realiza una operación AND bit a bit entre la dirección IP y la máscara.

Ejemplo:

Para la dirección IP 192.168.1.100 con máscara de subred 255.255.255.0:

- Convertimos las direcciones a binario:
    - 192.168.1.100 = 11000000.10101000.00000001.01100100
    - 255.255.255.0 = 11111111.11111111.11111111.00000000
- Realizamos la operación AND bit a bit:

11000000.10101000.00000001.01100100 (Dirección IP)
11111111.11111111.11111111.00000000 (Máscara de subred)

11000000.10101000.00000001.00000000 (Dirección de subred)

- Convertimos el resultado a decimal: 192.168.1.0

Aplicando este proceso a las direcciones IP proporcionadas:

Primero, es necesario convertir la notación CIDR (/26, /27, etc.) a su representación en máscara de subred:

- 172.16.58.223/26: Máscara de subred 255.255.255.192
- 163.10.5.49/27: Máscara de subred 255.255.255.224
- 128.10.1.0/23: Máscara de subred 255.255.254.0
- 10.1.0.0/24: Máscara de subred 255.255.255.0
- 8.40.11.179/12: Máscara de subred 255.240.0.0

Ahora, realizamos la operación AND bit a bit para cada dirección IP y su máscara de subred para obtener las direcciones de subred:

- **172.16.58.223/26**: **172.16.58.192**
- **163.10.5.49/27**: **163.10.5.32**
- **128.10.1.0/23**: **128.10.0.0**
- **10.1.0.0/24**: **10.1.0.0**
- **8.40.11.179/12**: **8.32.0.0**

c. ¿Cuál es la cantidad máxima de hosts que pueden estar en esa subred?

Fórmula general:

Cantidad máxima de hosts = 2^(número de bits de host) - 2

Se restan 2 direcciones porque:

- La dirección con todos los bits de host en 0 se utiliza para identificar la propia subred.
- La dirección con todos los bits de host en 1 se utiliza como dirección de broadcast para la subred.

Aplicando la fórmula a las direcciones IP proporcionadas:

Primero, identificamos el número de bits de host a partir de la notación CIDR (/26, /27, etc.):

- 172.16.58.223/26: 32 - 26 = 6 bits para host
- 163.10.5.49/27: 32 - 27 = 5 bits para host
- 128.10.1.0/23: 32 - 23 = 9 bits para host
- 10.1.0.0/24: 32 - 24 = 8 bits para host
- 8.40.11.179/12: 32 - 12 = 20 bits para host

Ahora, calculamos la cantidad máxima de hosts para cada subred:

- **172.16.58.223/26**: 2^6 - 2 = **62 hosts**
- **163.10.5.49/27**: 2^5 - 2 = **30 hosts**
- **128.10.1.0/23**: 2^9 - 2 = **510 hosts**
- **10.1.0.0/24**: 2^8 - 2 = **254 hosts**
- **8.40.11.179/12**: 2^20 - 2 = **1,048,574 hosts**

d. ¿Cuál es la dirección de broadcast de esa subred? La dirección de broadcast se obtiene estableciendo todos los bits de la porción de host de la dirección de subred en 1.

- **Ejemplo:**

Para la subred 192.168.1.0 con máscara de subred 255.255.255.0:

- La dirección de subred en binario es: 11000000.10101000.00000001.00000000
- Establecemos los bits de host en 1: 11000000.10101000.00000001.11111111
- La dirección de broadcast en decimal es: 192.168.1.255

Aplicando este proceso a las direcciones IP proporcionadas:

- **172.16.58.223/26:** Dirección de broadcast: **172.16.58.255**
- **163.10.5.49/27:** Dirección de broadcast: **163.10.5.63**
- **128.10.1.0/23:** Dirección de broadcast: **128.10.1.255**
- **10.1.0.0/24:** Dirección de broadcast: **10.1.0.255**

- **8.40.11.179/12:** Dirección de broadcast: **8.47.255.255**

e. ¿Cuál es el rango de direcciones IP válidas dentro de la subred?

El rango de direcciones IP válidas dentro de una subred excluye la dirección de subred y la dirección de broadcast. Se define como todas las direcciones entre la dirección de subred + 1 y la dirección de broadcast - 1.

Ejemplo:

Para la subred 192.168.1.0 con máscara de subred 255.255.255.0:

- Rango válido: **192.168.1.1** a **192.168.1.254**

Aplicando este proceso a las direcciones IP proporcionadas:

- **172.16.58.223/26:** Rango válido: **172.16.58.193** a **172.16.58.254**
- **163.10.5.49/27:** Rango válido: **163.10.5.33** a **163.10.5.62**
- **128.10.1.0/23:** Rango válido: **128.10.0.1** a **128.10.1.254**
- **10.1.0.0/24:** Rango válido: **10.1.0.1** a **10.1.0.254**
- **8.40.11.179/12:** Rango válido: **8.32.0.1** a **8.47.255.254**

7. Su organización cuenta con la dirección 128.50.10.0. Indique:

a. ¿Es una dirección de red o de host?

Al ser una dirección B con máscara por defecto (11111111 11111111 00000000 00000000) algunos números de host no están en 0 entonces es de host.

b. Clase a la que pertenece y máscara de clase.

B y clase 255.255.0.0

c. Cantidad de hosts posibles.

2^16-2

d. Se necesitan crear, al menos, 513 subredes. Indique:

i. Máscara necesaria.

513 subredes requieren al menos log2(513)≈ 9 bits para identificarlas.

Una dirección IPv4 tiene 32 bits. Si usamos 9 bits para subredes, nos quedan 32−9=23 bits.
Esto corresponde a una máscara 255.255.255.192 o notación CIDR `/26`.

ii. Cantidad de redes asignables.

1024

iii. Cantidad de hosts por subred.

Con una máscara `/26`:

- Los bits restantes para los hosts son 32−26=632 - 26 = 632−26=6.
- Cada subred puede tener 26=642^6 = 6426=64 direcciones en total, pero se restan 2 (una para la dirección de red y otra para el broadcast).
- Por lo tanto, cada subred tiene 64−2=6264 - 2 = 6264−2=62 hosts utilizables.

Por lo tanto, la cantidad de hosts por subred es **62**.

iv. Dirección de la subred 710.

La subred 710 se encuentra al calcular sus límites.

1. **Incremento de cada subred**:
    - El incremento depende de la máscara. Con `/26`, el tamaño de cada subred es de 64 direcciones.
    - Las direcciones comienzan desde el primer bloque (128.50.0.0, en este caso).
2. **Fórmula para encontrar la subred específica**:
    - Dirección inicial + 64×subred
    - 128.50.0.0+(64×710)

    Para 710:

- Calculamos: 64×710=45440
- Convertimos 45440 a la dirección IP, lo que da como resultado **128.50.177.64**.

Por lo tanto, la dirección de la subred 710 es **128.50.177.64**.

v. Dirección de broadcast de la subred 710.

La dirección de broadcast de una subred es la última dirección válida dentro de esa subred:

- Para la subred que comienza en 128.50.177.64, el siguiente bloque comenzará en 128.50.177.128.
- La dirección de broadcast es una menos que el inicio del siguiente bloque: 128.50.177.128−1 = 128.50.177.127.

Por lo tanto, la dirección de broadcast es **128.50.177.127**.

8. Si usted estuviese a cargo de la administración del bloque IP 195.200.45.0/24

a. ¿Qué máscara utilizaría si necesita definir al menos 9 subredes?

255.255.255.240 -> La cantidad de bits para definir al menos 9 redes dan un máximo de 16, por eso sacamos eso a número final de la máscara, en este caso 2^4. /28

b. Indique la dirección de subred de las primeras 9 subredes.

Son múltiplos de 16 porque tenemos máximo de 16 redes:

195.200.45.0
195.20.45.16
195.20.45.32
195.20.45.48
195.20.45.64
195.20.45.80
195.20.45.96
195.20.45.112
195.20.45.128

c. Seleccione una e indique dirección de broadcast y rango de direcciones asignables en esa subred.

Si elegimos 195.20.45.48, para sacar broadcast podemos calcularlo así:

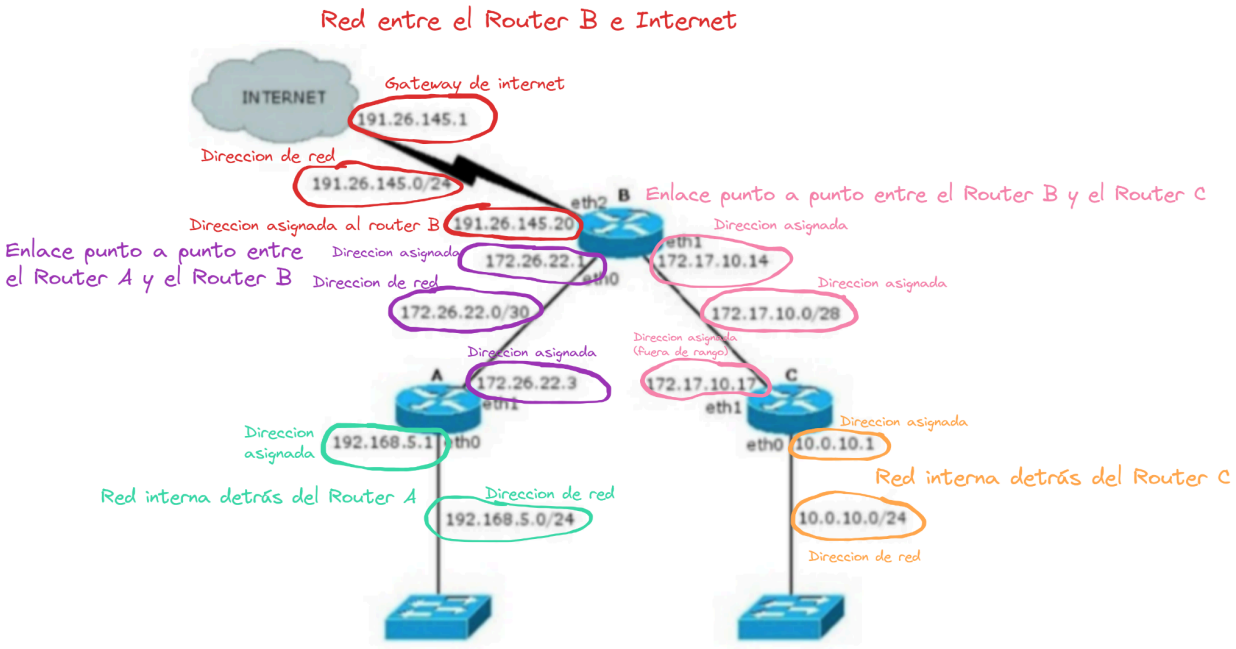
La dirección de broadcast es la última dirección del rango de la subred. Para calcularla, sumamos 16−1= 15 al valor de la dirección de red:

195.200.45.48+15=195.200.45.63

Dirección de broadcast: 195.200.45.63.

El rango sería entonces de 195.200.45.49 a 195.200.45.62.

9. Dado el siguiente gráfico:



a. Verifique si es correcta la asignación de direcciones IP y, en caso de no serlo, modifique la misma para que lo sea.

191.26.145.0/24 ->
Mascara: 1111 1111 1111 1111 1111 1111 0000 0000
Rango de direcciones asignables: **191.26.145.1 - 191.26.145.254**
Por tanto **191.26.145.1** es correcto

191.168.5.0/24 ->
Máscara: 1111 1111 1111 1111 1111 1111 0000 0000
Rango de direcciones asignables: **191.168.5.1 - 191.168.5.254**
Por tanto **191.168.5.1** es correcto

172.26.22.0/30 ->
Mascara: 1111 1111 1111 1111 1111 1111 1111 1100
Rango de direcciones asignables: **172.26.22.1 - 172.26.22.2**
Por tanto **172.26.22.3** esta mal ya que esl dirección broadcast, **172.17.22.1** si es correcta

172.17.10.0/28 ->
Mascara: 1111 1111 1111 1111 1111 1111 1111 0000
Rango de direcciones asignables: **172.17.10.1 - 172.17.10.14**
Por tanto **172.17.10.17** no es correcta, está fuera del rango, **172.17.10.14** si es correcta.

10.0.10.0/25 ->
Mascara: 1111 1111 1111 1111 1111 1111 0000 0000
Rango de direccion asignables: **10.0.10.1 - 10.0.10.254**
Por tanto **10.0.10.1** es correcta

b. ¿Cuántos bits se tomaron para hacer subredes en la red 10.0.10.0/24? ¿Cuántas subredes se podrían generar?

Al ser una dirección del rango 0.0.0.0 a 127.255.255.255, es de clase A por tanto la máscara tiene 16 bits extra (la máscara por defecto es 255.0.0.0) en este caso se pueden generar 2^16 subredes.

c. Para cada una de las redes utilizadas indique si son públicas o privadas.

Rango de Direcciones Privadas:

1. **Clase A:** 10.0.0.0 - 10.255.255.255
2. **Clase B:** 172.16.0.0 - 172.31.255.255
3. **Clase C:** 192.168.0.0 - 192.168.255.255

Análisis de las direcciones en tus ejemplos:

1. **191.26.145.0/24**
    - **Dirección IP:** 191.26.145.0
    - Este rango no está dentro de los rangos de direcciones privadas, por lo tanto, **es una dirección pública**.
2. **191.168.5.0/24**
    - **Dirección IP:** 191.168.5.0
    - Aunque comienza con 191, este rango no pertenece a direcciones privadas, ya que está fuera de los rangos privados definidos. Entonces, **es una dirección pública**.
3. **172.26.22.0/30**
    - **Dirección IP:** 172.26.22.0

    - El rango **172.16.0.0 - 172.31.255.255** pertenece a direcciones privadas, y 172.26.22.0 está dentro de este rango. Por lo tanto, **es una dirección privada**.
4. **172.17.10.0/28**
    - **Dirección IP:** 172.17.10.0
    - Como mencioné antes, el rango **172.16.0.0 - 172.31.255.255** es privado, y 172.17.10.0 está dentro de ese rango. Por lo tanto, **es una dirección privada**.
5. **10.0.10.0/25**
    - **Dirección IP:** 10.0.10.0
    - El rango **10.0.0.0 - 10.255.255.255** es privado, por lo que esta dirección **es privada**.

Resumen:

- **Públicas:**
    - 191.26.145.0/24
    - 191.168.5.0/24
- **Privadas:**
    - 172.26.22.0/30
    - 172.17.10.0/28
    - 10.0.10.0/25

CIDR

10. ¿Qué es CIDR (Class Interdomain routing)? ¿Por qué resulta útil?

CIDR (Classless Interdomain Routing), o Enrutamiento entre dominios sin clase, es la estrategia actual de asignación de direcciones en Internet. Generaliza la noción de direccionamiento de subred, dividiendo la dirección IP de 32 bits en dos partes: una parte de red y una parte de host. La notación utilizada es a.b.c.d/x, donde "x" indica la cantidad de bits de la primera parte, que corresponde a la red.

Beneficios de CIDR

CIDR resulta **útil por varias razones:**

- **Uso eficiente del espacio de direcciones:** Antes de CIDR, se utilizaba un sistema de direccionamiento con clases (clase A, B y C), que asignaba bloques de direcciones con tamaños fijos. Esto llevaba a una mala utilización del espacio de direcciones, ya que muchas organizaciones recibían bloques de direcciones

demasiado grandes para sus necesidades.

- **Agregación de rutas:** Los routers externos a una organización solo necesitan considerar la parte de red de la dirección (los "x" bits del prefijo) para enrutar paquetes hacia ella. Esto permite **agregar múltiples rutas en una sola entrada en las tablas de enrutamiento**, lo que reduce significativamente el tamaño de las tablas y la complejidad del proceso de enrutamiento.

- **Flexibilidad:** CIDR ofrece mayor flexibilidad al permitir a las organizaciones subdividir sus bloques de direcciones en subredes internas según sus necesidades, adaptando la estructura de la red a su topología y requerimientos específicos.

11. ¿Cómo publicaría un router las siguientes redes si se aplica CIDR?

a. 198.10.1.0/24

b. 198.10.0.0/24

c. 198.10.3.0/24

d. 198.10.2.0/24

Es todo lo mismo:
198.10.0.0/22: Esta única entrada en la tabla de enrutamiento del router representaría las cuatro subredes proporcionadas (a, b, c y d).
CIDR permite agregar múltiples rutas en una sola entrada en la tabla de enrutamiento utilizando un prefijo común. En este caso, las cuatro subredes comparten el prefijo 198.10. Al tomar 22 bits para la parte de red, se crea un bloque de direcciones que abarca las cuatro subredes:

- 198.10.0.0/24
- 198.10.1.0/24
- 198.10.2.0/24
- 198.10.3.0/24

12. Listar las redes involucradas en los siguientes bloques CIDR:

- 200.56.168.0/21

  No contabilizando las subredes, sino solo las redes, va desde:
  200.56.168.0/24 - 200.56.175.0/24, debido a la máscara de red /21.

- 195.24.0.0/13

  195.24.0.0/24 - 195.31.255.0/24

- 195.24/13

  195.24.0.0/24 – 195.31.255.0/24

13. El bloque CIDR 128.0.0.0/2 o 128/2, ¿Equivale a listar todas las direcciones de red de clase B? ¿Cuál sería el bloque CIDR que agrupa todas las redes de clase A?

Si, equivale, el rango de direcciones del bloque es:
Dirección de red: 128.0.0.0 (10000000 00000000 00000000 00000000)
Primera dirección utilizable: 128.0.0.1
Última dirección utilizable: 191.255.255.254 (10111111 11111111 11111111 11111110)
Broadcast: 191.255.255.255 (10111111 11111111 11111111 11111111)

Y por tanto el rango de direcciones una clase B es:
128.0.0.0 - 191.255.255.255 que es exactamente lo nuestro.

VLSM

14. ¿Qué es y para qué se usa VLSM?

VLSM es una técnica que permite utilizar diferentes máscaras de subred dentro de la misma red. Esto contrasta con el enfoque tradicional donde se usa una sola máscara de subred para toda la red.

Beneficios y uso de VLSM

- **Uso eficiente del espacio de direcciones:** VLSM optimiza la asignación de direcciones IP al dividir una red en subredes de distintos tamaños. Esto evita el desperdicio de direcciones que ocurre cuando se utiliza una sola máscara de subred.
- **Flexibilidad:** VLSM se adapta a las necesidades específicas de cada segmento de la red, permitiendo crear subredes con el número exacto de hosts necesarios.
- **Enrutamiento más preciso:** Facilita la creación de rutas de enrutamiento más específicas y eficientes.

Ejemplo de VLSM

Una empresa con una red /24 (256 direcciones) puede utilizar VLSM para crear diferentes subredes:

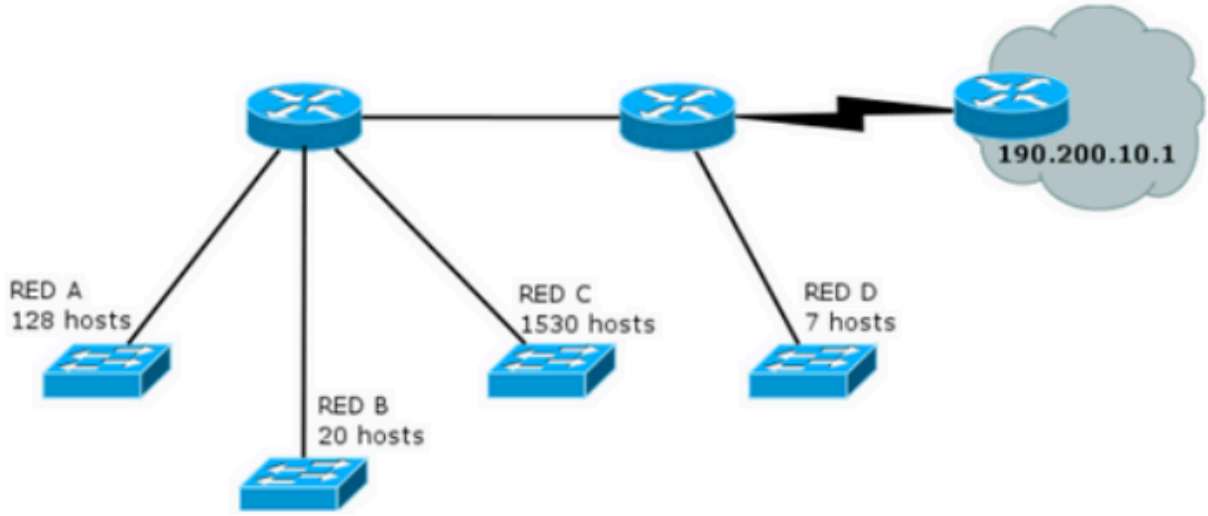
- Subred A: /26 (64 direcciones) para un departamento con muchos hosts.
- Subred B: /28 (16 direcciones) para un departamento pequeño.
- Subred C: /29 (8 direcciones) para conectar dos routers.

VLSM permite asignar sólo las direcciones necesarias a cada subred, evitando el desperdicio de direcciones IP.

15. Describa, con sus palabras, el mecanismo para dividir subredes utilizando VLSM.

1) Subnetear para la red con mayor cantidad de hosts.
2) De las subredes obtenidas, asignar todas las que se puedan con el menor desperdicio posible.
3) Si quedan segmentos de red sin una subred asignada volver al paso 1.

16. Suponga que trabaja en una organización que tiene la red que se ve en el gráfico y debe armar el direccionamiento para la misma, minimizando el desperdicio de direcciones IP. Dicha organización posee la red 205.10.192.0/19, que es la que usted deberá utilizar.



a. ¿Es posible asignar las subredes correspondientes a la topología utilizando subnetting sin VLSM? Indique la cantidad de hosts que se desperdicia en cada subred.

Como tal no es posible, necesitamos 6 subredes y 3 bits para ello.

- La red 205.10.192.0/19 (11001101 00001010 11000000 00000000), con máscara de red 1111 1111 1111 1111 11100000 00000000.
- La máscara de subred tendría 3 bits más: 1111 1111 1111 1111 11111100 00000000.
- La subred más grande necesita 11 bits de dirección para sus 1530 hosts, y ya **no alcanza con los bits restantes** (nos quedaban 10 teniendo en cuenta máscara de subred).

b. Asigne direcciones a todas las redes de la topología. Tome siempre en cada paso la primera dirección de red posible.

Probablemente algún número está mal, ignorar los libres de este, aparecen más abajo correctamente.

Red C requiere 1532 direcciones

Por tanto requiere 11 bits para direccionar todo eso (máscara de /21):

DIR original 11001101 00001010 11000000 00000000 205.10.192.0

MASCARA/19 11111111 11111111 11100000 00000000

bits libres (13 o 8096 direcciones)

Mascara para red C -> /21 11111111 11111111 11111000 00000000

Dir de red de la red C 11001101 00001010 11000000 00000000

Siguiente dir a dividir 11001101 00001010 11001000 00000000

Queda libre si viniera una red mas grande

11001101 00001010 11010000 00000000

11001101 00001010 11011000 00000000

En resumen la estrategia es que, nosotros asignamos la dirección inicial a la red más grande, hacemos que la direcciones de la siguiente red sea la anterior, pero con el bit en 1 donde termina la máscara de la red anterior, y en el medio quedan todas esas direcciones libres.

Mascara para red A -> /24 11111111 11111111 11111111 00000000

Dir de red de la red A 11001101 00001010 11001000 00000000

Siguiente dir a dividir 11001101 00001010 11001001 00000000

Libres: 11001101 00001010 11001010 00000000

011

100

101

110

111

Mascara para red B -> /27	11111111 11111111 11111111 11100000
Dir de la red B	11001101 00001010 11001001 00000000
Siguiente dir a dividir	11001101 00001010 11001001 00100000
Libres	11001101 00001010 11001001 010 00000
	011
	100
	101
	110
	111

Mascara para red D -> /28

Dir de la red D	11001101 00001010 11001001 00100000
Siguiente dir a dividir	11001101 00001010 11001001 00110000

Mascara para red E -> /30	11111111 11111111 11111111 11111100
Dir de la red E	11001101 00001010 11001001 00110000
Siguiente dir a dividir	11001101 00001010 11001001 00110100

11001101 00001010 11001001 00111000/29
11001101 00001010 11001001 00110100/30

c. Para mantener el orden y el inventario de direcciones disponibles, haga un listado de todas las direcciones libres que le quedaron, agrupándolas utilizando CIDR.

Libres del C:
11001101 00001010 11010000 00000000
11001101 00001010 11011000 00000000
CIDR: 11001101 00001010 11010000 00000000/20

Libres del A:

```
11001101 00001010 11001010 00000000
                          011
                          100
                          101
                          110
                          111
```

CIDR:

11001101 00001010 11001100 0000 0000/22
11001101 00001010 11001010 0000 0000/23

Libres del B:

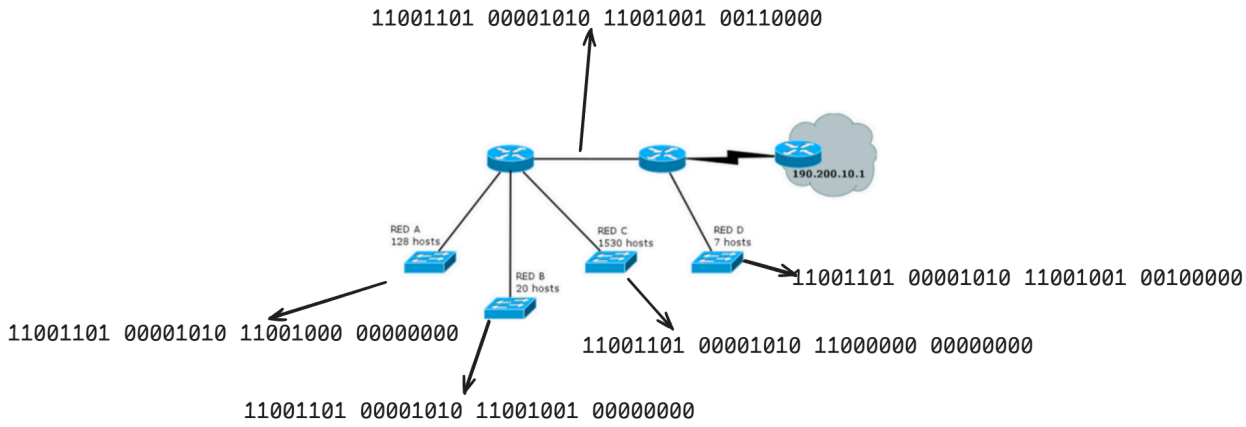
```
11001101 00001010 11001001 01000000
                           011
                           100
                           101
                           110
                           111
```

CIDR:

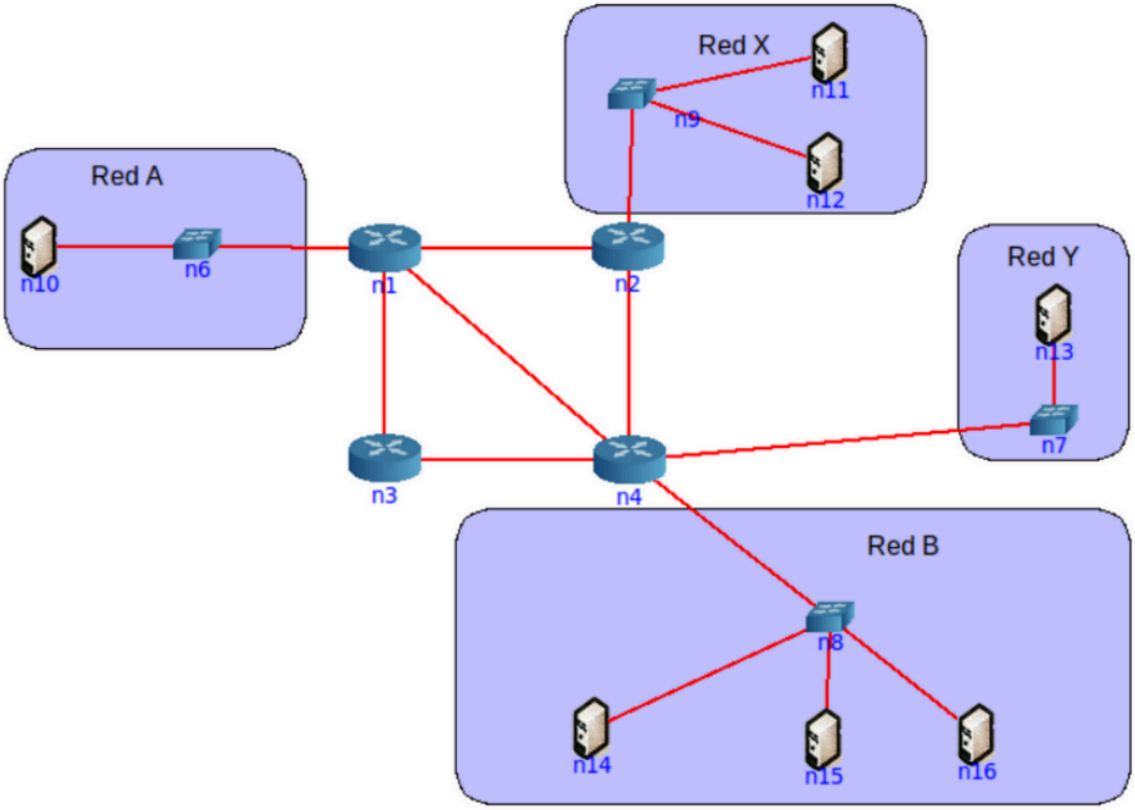
11001101 00001010 11001001 10000000/25
11001101 00001010 11001001 01000000/26

Libres del E: 11001101 00001010 11001001 00111000
11001101 00001010 11001001 00110100
11001101 00001010 11001001 00110100/30
11001101 00001010 11001001 00111000/29

d. Asigne direcciones IP a todas las interfaces de la topología que sea posible.



17. Utilizando la siguiente topología y el bloque asignado, arme el plan de direccionamiento IPv4 teniendo en cuenta las siguientes restricciones:



a. Utilizar el bloque IPv4 200.100.8.0/22.

b. La red A tiene 125 hosts y se espera un crecimiento máximo de 20 hosts.

c. La red X tiene 63 hosts.

d. La red B cuenta con 60 hosts

e. La red Y tiene 46 hosts y se espera un crecimiento máximo de 18 hosts.

f. En cada red, se debe desperdiciar la menor cantidad de direcciones IP posibles. En este sentido, las redes utilizadas para conectar los routers deberán utilizar segmentos de red /30 de modo de desperdiciar la menor cantidad posible de direcciones IP.

Utilizar el bloque IPv4 200.100.8.0/22

a. La red A tiene 125 hosts y se espera un crecimiento máximo de 20 hosts.
b. La red X tiene 63 hosts.
c. La red B cuenta con 60 hosts
d. La red Y tiene 46 hosts y se espera un crecimiento máximo de 18 hosts.
e. En cada red, se debe desperciciar la menor cantidad de direcciones IP posibles. En este sentido, las redes utilizadas para conectar los routers deberán utilizar segmentos de red /30 de modo de desperdiciar la menor cantidad posible de direcciones IP.

BASE: 200.100.8.0/22

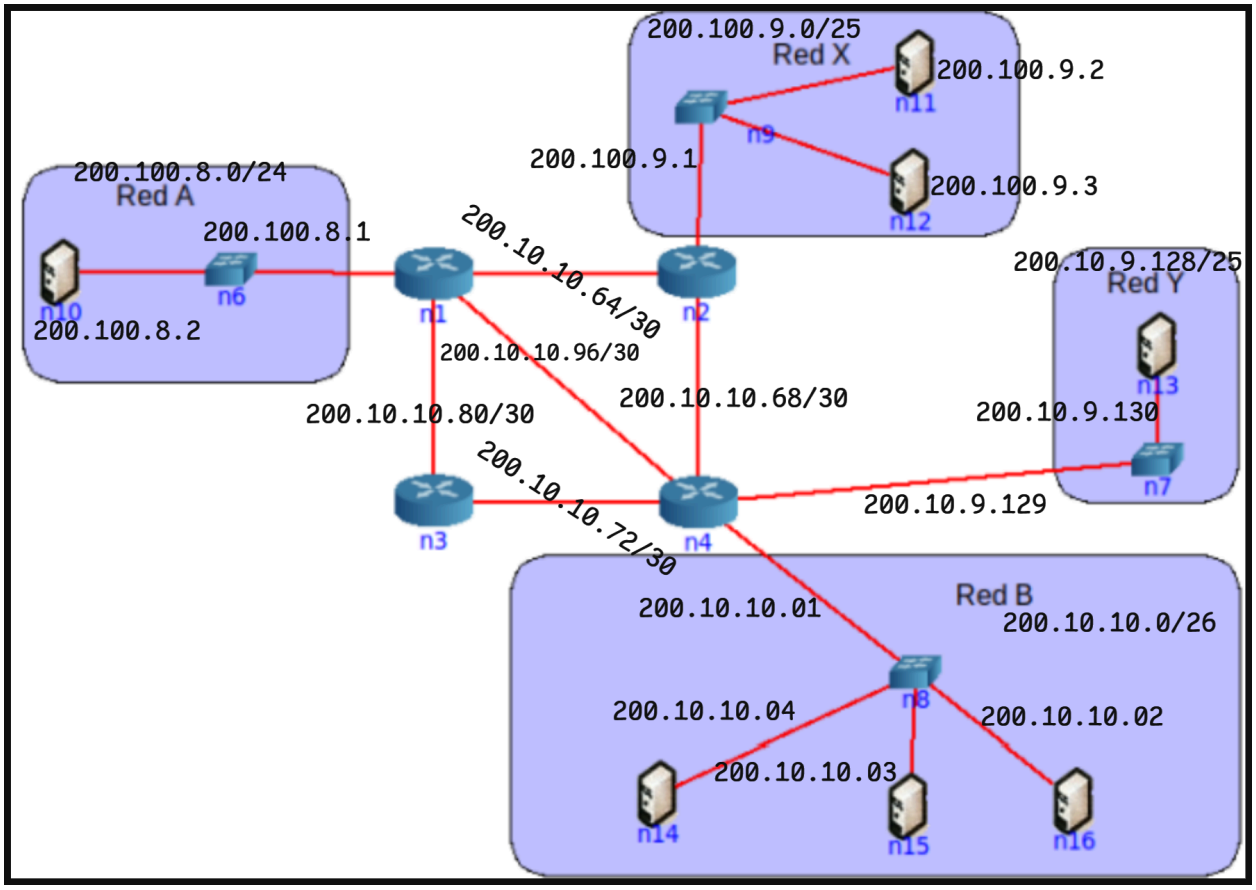
Dirección red A: 200.100.8.0	11001000.01100100.00001000.00000000
Mascara: /24	11111111.11111111.11111111.00000000
Siguiente:	11001000.01100100.00001001.00000000
Libres:	11001000.01100100.00001010.00000000
	11001000.01100100.00001011.00000000

Dirección red X:	11001000.01100100.00001001.00000000
Dirección red Y:	11001000.01100100.00001001.10000000
Mascara:/25	11111111.11111111.11111111.10000000
Siguiente: (uno de las libres de A)	11001000.01100100.00001010.00000000

Dirección red B:	11001000.01100100.00001010.00000000
Mascara:/26	11111111.11111111.11111111.11000000
Siguiente:	11001000.01100100.00001010.01000000
Libres:	11001000.01100100.00001010.10000000
	11001000.01100100.00001010.11000000

Dirección red n1-n2:	11001000.01100100.00001010.01000000
Dirección red n2-n4:	11001000.01100100.00001010.01000100
Dirección red n4-n3:	11001000.01100100.00001010.01001000
Dirección red n3-n1:	11001000.01100100.00001010.01010000
Dirección red n1-n4:	11001000.01100100.00001010.01100000
Mascara:/30	11111111.11111111.11111111.11111100

18. Asigne direcciones IP en los equipos de la topología según el plan anterior.



ICMP y Configuraciones IP

19. Describa qué es y para qué sirve el protocolo ICMP.

El **Protocolo de Mensajes de Control de Internet (ICMP)** es utilizado por los hosts y routers para intercambiar información sobre la capa de red. Aunque a menudo se considera parte de IP, el ICMP se encuentra **arquitectónicamente por encima de IP**, ya que sus mensajes se transportan dentro de los datagramas IP como carga útil.

Función principal: Informes de Error

La función más común de ICMP es la **generación de informes de error**. Por ejemplo, cuando un router no encuentra una ruta hacia un host, genera un mensaje ICMP para informar del error "Red de destino inalcanzable".

Estructura de los mensajes ICMP

Los mensajes ICMP tienen:

- Campos de tipo y código que especifican la naturaleza del mensaje.
- La cabecera y los primeros 8 bytes del datagrama IP que originó el mensaje, lo que permite al emisor identificar la causa del error.

Tipos de Mensajes ICMP

ICMP no solo se utiliza para informar errores, sino también para otras funciones. Algunos tipos de mensajes ICMP son:

- **Solicitud de eco (tipo 8, código 0)** y **respuesta de eco (tipo 0, código 0)**, utilizados por el programa **ping** para comprobar la conectividad y medir la latencia.
- **Regulación del origen (tipo 4, código 0)**, utilizado en el pasado para el control de congestión, aunque hoy en día se usa con poca frecuencia.
- **TTL caducado (tipo 11, código 0)** y **puerto inalcanzable (tipo 3, código 3)**, utilizados por el programa **Traceroute** para rastrear la ruta de un datagrama.

ICMP en IPv6

En IPv6, se utiliza una nueva versión de ICMP (ICMPv6) que, además de reorganizar los tipos y códigos existentes, incluye:

- Nuevos tipos y códigos para la funcionalidad específica de IPv6.
- La funcionalidad del Protocolo de gestión de grupos de Internet (IGMP).

Importancia de ICMP

ICMP es una parte integral de la capa de red de Internet, ya que proporciona mecanismos esenciales para la **detección y notificación de errores**, así como para el **diagnóstico y la resolución de problemas de red**.

a. Analice cómo funciona el comando ping.

El comando ping es una herramienta de diagnóstico de red que se utiliza para comprobar la conectividad entre un host de origen y un host de destino. Su funcionamiento se basa en el Protocolo de Mensajes de Control de Internet (ICMP).

El comando ping funciona de la siguiente manera:

- El host de origen envía un mensaje ICMP de **tipo 8, código 0**, conocido como **solicitud de eco**, al host de destino.
- El host de destino, al recibir la solicitud de eco, genera un mensaje ICMP de **tipo 0, código 0**, conocido como **respuesta de eco**, y lo envía de vuelta al host de origen.
- El host de origen, al recibir la respuesta de eco, calcula el **tiempo de ida y vuelta (RTT)**, que es el tiempo transcurrido entre el envío de la solicitud de eco y la recepción de la respuesta de eco.

La información obtenida a través del comando ping permite:

- **Verificar si el host de destino está activo y alcanzable**. Si el host de origen recibe una respuesta de eco, significa que el host de destino está activo y que la ruta entre ambos hosts está funcionando correctamente.
- **Medir la latencia de la conexión**. El RTT indica el tiempo que tarda un paquete en viajar desde el host de origen al host de destino y viceversa. Un RTT alto puede indicar problemas de congestión o de rendimiento en la red.
- **Detectar la pérdida de paquetes**. Si el host de origen no recibe una respuesta de eco para algunas de las solicitudes de eco enviadas, significa que algunos paquetes se han perdido en la red.

I. Indique el tipo y código ICMP que usa el ping.

Solicitud de eco (tipo 8, código 0): Este mensaje se utiliza para solicitar una respuesta de eco al host de destino.

ii. Indique el tipo y código ICMP que usa la respuesta de un ping.

Respuesta de eco (tipo 0, código 0): Este mensaje se utiliza para responder a una solicitud de eco.

b. Analice cómo funcionan comandos como traceroute/tracert de Linux/Windows y cómo manipulan el campo TTL de los paquetes IP.

Los comandos traceroute (en Linux) y tracert (en Windows) son herramientas de diagnóstico de red que permiten determinar la ruta que siguen los paquetes IP desde un host de origen hasta un host de destino. Su funcionamiento se basa en la manipulación del campo Tiempo de Vida (TTL) de los paquetes IP y en el uso del Protocolo de Mensajes de Control de Internet (ICMP).

Funcionamiento de traceroute/tracert:

1. **Envío de paquetes UDP con TTL incremental:** El comando traceroute/tracert envía una serie de datagramas IP al host de destino, cada uno con un segmento

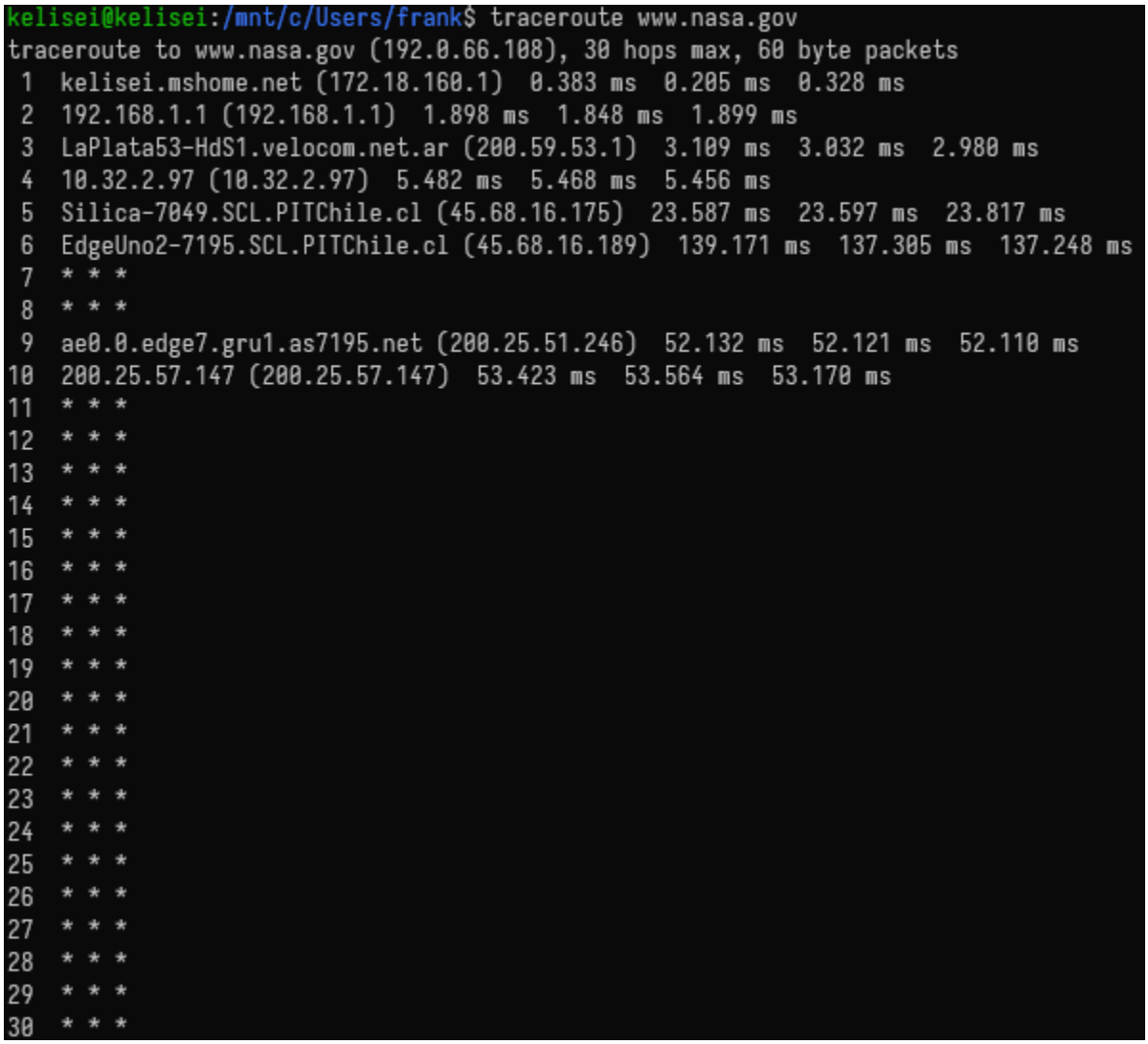
UDP que contiene un número de puerto UDP improbable. La característica clave es que cada datagrama se envía con un valor de TTL incremental, comenzando con TTL=1 para el primer datagrama, TTL=2 para el segundo, y así sucesivamente.

2. **Caducidad del TTL y generación de mensajes ICMP:** Cuando un datagrama IP llega a un router en la ruta, el router decrementa el valor del campo TTL en una unidad. Si el TTL llega a 0, el router descarta el datagrama y envía un mensaje ICMP de tipo 11, código 0 ("TTL caducado") al host de origen. Este mensaje ICMP incluye el nombre y la dirección IP del router que lo generó.
3. **Recepción de mensajes ICMP y reconstrucción de la ruta:** El host de origen recibe los mensajes ICMP "TTL caducado" y registra el tiempo de ida y vuelta (RTT) para cada router, junto con su nombre y dirección IP. De esta forma, puede reconstruir la ruta completa que siguen los paquetes desde el host de origen hasta el host de destino.
4. **Finalización del rastreo:** El proceso continúa hasta que un datagrama IP llega al host de destino con un TTL mayor que 0. En este caso, el host de destino, al recibir un segmento UDP con un puerto improbable, genera un mensaje ICMP de tipo 3, código 3 ("Puerto inalcanzable") y lo envía al host de origen. Al recibir este mensaje, traceroute/tracert finaliza el proceso de rastreo, ya que ha encontrado la ruta completa hasta el host de destino.

Manipulación del campo TTL:

El campo TTL es fundamental para el funcionamiento de traceroute/tracert. Al enviar paquetes con un TTL incremental, se fuerza la caducidad del TTL en cada router de la ruta, lo que permite obtener información sobre cada router a través de los mensajes ICMP generados.

c. Indique la cantidad de saltos realizados desde su computadora hasta el sitio www.nasa.gov. Analice:



i. Cómo hacer para que no muestre el nombre del dominio asociado a la IP de cada salto.

Traceroute, por defecto, intenta resolver las direcciones IP a nombres de dominio. Para evitar que muestre el nombre de dominio, se puede utilizar la opción -n en Linux o la opción -d en Windows. Esto le indicará a traceroute que solo muestre las direcciones IP numéricas.

ii. La razón de la aparición de * en parte o toda la respuesta de un salto.

La aparición de asteriscos (*) en la salida de traceroute indica que el router correspondiente no respondió a la solicitud de eco ICMP dentro de un tiempo determinado.

- Pérdida de paquetes: Esto puede deberse a la pérdida de paquetes en la red, lo que significa que los paquetes ICMP enviados por traceroute no llegaron al router o las respuestas del router no llegaron al host de origen.
- Filtrado de tráfico: Algunos routers pueden estar configurados para no responder a solicitudes ICMP, especialmente aquellas con valores TTL bajos utilizados por traceroute. Esto se hace por razones de seguridad, para evitar ataques de reconocimiento de red.
- Sobrecarga del router: Si un router está muy sobrecargado, puede que no tenga tiempo para procesar y responder a las solicitudes ICMP de traceroute.

d. Verifique el recorrido hacia los servidores de nombre del dominio unlp.edu.ar. En base al recorrido realizado, ¿podría confirmar cuál de ellos toma un camino distinto?

```
kelisei@kelisei:/mnt/c/Users/frank$ traceroute unlp.edu.ar
traceroute to unlp.edu.ar (163.10.0.135), 30 hops max, 60 byte packets
 1  kelisei.mshome.net (172.18.160.1)  0.225 ms  0.192 ms  0.156 ms
 2  192.168.1.1 (192.168.1.1)  0.830 ms  0.944 ms  1.086 ms
 3  LaPlata53-HdS1.velocom.net.ar (200.59.53.1)  3.659 ms  3.591 ms  3.509 ms
 4  * 10.32.2.97 (10.32.2.97)  4.808 ms *
 5  * * *
 6  200.0.17.12 (200.0.17.12)  6.134 ms  3.773 ms  3.703 ms
 7  200.115.81.1 (200.115.81.1)  3.993 ms  3.914 ms  6.309 ms
 8  163.10.199.203 (163.10.199.203)  6.204 ms  6.189 ms  6.177 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Explicación de la salida:

- **Línea 1:** Muestra la dirección IP (163.10.0.135) del servidor de unlp.edu.ar. También indica que se permite un máximo de 30 saltos (routers intermedios) y que se utilizarán paquetes de 60 bytes.
- **Línea 2 a 31:** Cada línea representa un salto o router en la ruta hacia unlp.edu.ar.
    - El primer número (1, 2, 3, etc.) es el número de salto.
    - El nombre de dominio y la dirección IP entre paréntesis corresponden al router en ese salto.
    - Los tres valores en milisegundos (ms) son los tiempos de ida y vuelta (RTT) de tres paquetes enviados a ese router.

Análisis de los resultados:

- **Saltos 1 a 3:** `kelisei.mshome.net (172.18.160.1)`, `192.168.1.1 (192.168.1.1)` y `LaPlata53-HdS1.velocom.net.ar (200.59.53.1)` corresponden a tu red local y al proveedor de internet.
- **Salto 4:** El asterisco (*) en el salto 4, junto con la dirección IP `10.32.2.97`, indica que ese router no respondió a las solicitudes ICMP de `traceroute`.
- **Salto 5:** Los tres asteriscos (*) indican que no se recibió respuesta de ningún router en este salto.
- **Saltos 6 a 8:** `200.0.17.12 (200.0.17.12)`, `200.115.81.1 (200.115.81.1)` y `163.10.199.203 (163.10.199.203)` son routers dentro de la red de la Universidad Nacional de La Plata (UNLP).
- **Saltos 9 a 30:** Todos los saltos restantes muestran asteriscos, lo que significa que `traceroute` no pudo obtener información sobre la ruta completa hasta el servidor final de unlp.edu.ar.

Conclusión:

En base al recorrido realizado, **no se puede confirmar** si algún servidor de nombre del dominio unlp.edu.ar toma un camino distinto. La salida de `traceroute` solo llega hasta el router `163.10.199.203` dentro de la red de la UNLP, y a partir de ahí no se obtiene más información.

Es posible que los servidores de nombre se encuentren detrás de este router y que `traceroute` no pueda acceder a ellos. La falta de respuesta de los routers en los saltos posteriores podría deberse a configuraciones de seguridad que bloquean las solicitudes ICMP.

20. ¿Para que se usa el bloque 127.0.0.0/8? ¿Qué PC responde a los siguientes comandos?

El bloque de direcciones 127.0.0.0/8 se utiliza para la comunicación de loopback, también conocida como localhost. Esta es una dirección especial que permite a una computadora enviarse paquetes a sí misma. Se utiliza principalmente para pruebas y depuración de aplicaciones y servicios de red.

a. ping 127.0.0.1

Este comando siempre será respondido por la misma PC donde se ejecuta. La dirección 127.0.0.1 es la dirección de loopback estándar y está reservada para este propósito.

b. ping 127.0.54.43

Al igual que con el comando anterior, este comando también será respondido por la misma PC donde se ejecuta. Todas las direcciones dentro del rango 127.0.0.0/8 se consideran direcciones de loopback y apuntan a la propia máquina.
En resumen, cualquier dirección IP dentro del bloque 127.0.0.0/8 se referirá a la propia computadora, permitiendo la comunicación interna sin necesidad de acceder a una red externa.

21. Investigue para qué sirven los comandos ifconfig y route. ¿Qué comandos podría utilizar en su reemplazo?

Comando `ifconfig`

El comando **`ifconfig`** se usa para **configurar los parámetros de una interfaz de red**. Si bien las fuentes proporcionadas no mencionan específicamente este comando, se puede inferir su utilidad a partir de la descripción de la **configuración de direcciones IP** y la **administración de red**. Algunas de sus funciones incluyen:

- **Mostrar la configuración actual de las interfaces de red:** Esto incluye la dirección IP, la máscara de subred, la dirección MAC, el estado de la interfaz (activa o inactiva) y estadísticas de la interfaz.
- **Configurar una dirección IP en una interfaz:** Permite asignar una dirección IP estática a una interfaz de red.
- **Quitar una dirección IP de una interfaz:** Permite eliminar la dirección IP asignada a una interfaz de red.
- **Activar o desactivar una interfaz de red:** Permite cambiar el estado de una interfaz de red a activa o inactiva.

Alternativas a `ifconfig`

En sistemas operativos modernos, el comando **`ip`** está reemplazando a `ifconfig`. El comando `ip` es más versátil y potente, y ofrece una sintaxis más consistente. Algunas de las funciones de `ifconfig` pueden replicarse con los siguientes comandos `ip`:

- **`ip addr show`**: Muestra la configuración de las interfaces de red.
- **`ip addr add <dirección_IP>/<máscara_de_subred> dev <interfaz>`**: Configura una dirección IP en una interfaz.
- **`ip addr del <dirección_IP>/<máscara_de_subred> dev <interfaz>`**: Quita una dirección IP de una interfaz.
- **`ip link set <interfaz> up`**: Activa una interfaz de red.
- **`ip link set <interfaz> down`**: Desactiva una interfaz de red.

Comando `route`

El comando **`route`** se utiliza para **manipular la tabla de enrutamiento** de un sistema. Las fuentes mencionan el **enrutamiento** como una función esencial de la **capa de red**. La tabla de enrutamiento se utiliza para determinar la mejor ruta para enviar paquetes de red a un destino determinado.

Algunas de las funciones del comando `route` son:

- **Mostrar la tabla de enrutamiento actual:** Esto incluye las redes de destino, la puerta de enlace utilizada para llegar a cada red y la interfaz de red utilizada para enviar paquetes.
- **Agregar una ruta estática:** Permite agregar una ruta manual a la tabla de enrutamiento.
- **Eliminar una ruta estática:** Permite eliminar una ruta manual de la tabla de enrutamiento.

Alternativas a `route`

Al igual que con `ifconfig`, el comando **`ip`** también puede utilizarse para manipular la tabla de enrutamiento. Algunas de las funciones del comando `route` pueden replicarse con los siguientes comandos `ip`:

- **`ip route show`**: Muestra la tabla de enrutamiento actual.
- **`ip route add <red_de_destino> via <puerta_de_enlace>`**: Agrega una ruta estática.
- **`ip route del <red_de_destino>`**: Elimina una ruta estática.

Práctica en CORE

Para practicar el uso de estos comandos en CORE, se puede seguir el siguiente procedimiento general:

1. **Iniciar una topología en CORE:** Crea una nueva topología o utiliza una existente.
2. **Crear una máquina:** Agrega una máquina virtual a la topología.
3. **Acceder a la máquina:** Inicia sesión en la máquina virtual.
4. **Usar los comandos:** Ejecuta los comandos `ifconfig`, `route`, `ip addr` e `ip route` para configurar y ver la información de red de la máquina.

Ejemplos de uso:

Configurar una dirección IP en una interfaz:

- **`ifconfig eth0 192.168.1.100 netmask 255.255.255.0`**
- **`ip addr add 192.168.1.100/24 dev eth0`**

Quitar una dirección IP de una interfaz:

- **`ifconfig eth0 0.0.0.0`**
- **`ip addr del 192.168.1.100/24 dev eth0`**

Ver la tabla de ruteo:

- **`route -n`**
- **`ip route show`**

Inicie una topología con CORE, cree una máquina y utilice en ella los comandos anteriores para practicar sus diferentes opciones, mínimamente:

● Configurar y quitar una dirección IP en una interfaz.

● Ver la tabla de ruteo de la máquina.

No lo voy a hacer.