

Práctica 7

Introducción

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 proporciona los servicios de enrutamiento y reenvío de paquetes (PDU) entre distintos hosts. El dispositivo principal de esta capa es el router.

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

Se lo considera un protocolo de mejor esfuerzo ya que se trata de un protocolo poco confiable, esto quiero decir que hace todo lo posible para entregar los datos, pero no garantiza que todos los paquetes llegaran al destino, ni de que lo haran en el orden correcto.

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

CLASE	REDES	HOSTS
A	128	16777214
B	16384	65534
C	2097152	254

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

Los prefijos de longitud fija por clase provocan un uso ineficiente en el espacio de direcciones y muchos equipos, produce escasez de direcciones.

Esto supone la aparición de las subredes, que básicamente permite que haya subgrupos en las redes, se utiliza para generar redes dentro de la red. Para ello toma una parte del hostid.

La división en subredes plantea que si una red de clase desperdicia muchas direcciones IP entonces la misma sea dividida en N subredes más pequeñas que aprovechen mejor el espacio de direccionamiento

Las máscaras se utilizan para saber en una dirección IP qué bits son de red y qué bits son de host.

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 indica el tipo de carga útil (payload) que sigue a la cabecera IP, es decir, especifica el protocolo de la capa superior al que se le entrega el paquete IP. Este campo es útil para que el dispositivo de destino sepa cómo interpretar y procesar los datos contenidos en el paquete. Es un campo de 8 bits

y puede contener valores numéricos que representan diferentes protocolos de capa de transporte.

Se asemeja la funcionalidad al campo que indica el puerto destino en las cabeceras de los protocolos de capa de transporte.

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)?

b. ¿Cuál es la dirección de subred?

172.16.58.223

10101100 10000000 00111010 11011111

11111111 11111111 11111111 11000000

163.10.5.49/27

10100011 00001010 00000101 00110001

11111111 11111111 11111111 11100000

128.10.1.0/23

10000000 00001010 00000001 00000000

11111111 11111111 11111110 00000000

10.1.0.0/24

00001010 00000001 00000000 00000000

11111111 11111111 11111111 00000000

8.40.11.179/12

00001000 00101000 00001011 10110011

11111111 11110000 00000000 00000000

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

d. ¿Cuál es la dirección de broadcast de esa subred?

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

	CLASE	SUBRED	CANT. MAX. HOSTS	DIR. BROADCAST	RANGO
172.16.58.223/26	B	172.16.58.192	62	172.16.58.255	172.16.58.193 - 172.16.58.254

163.10.5.49/27	B	163.10.5.32	30	163.10.5.63	163.10.5.33- 163.10.5.62
128.10.1.0/23	B	128.10.0.0	510	128.10.1.255	128.10.0.1 - 128.10.1.254
10.1.0.0/24	A	10.1.0.0	254	10.1.0.255	10.1.0.1 - 10.1.0.254
8.40.11.179/12	A	8.32.0.0	1048574	8.47.255.255	8.32.0.1 - 8.47.255.254

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

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

Es de host puesto que todos sus bits de hosts no están en 0.

Se trata de una dirección de clase B cuya mascara por defecto es 255.255.0.0.

128.50.10.0 en binario es 10000000 00110010 00001010 00000000
La máscara de red es 11111111 11111111 00000000 00000000

Podemos ver como los bits que corresponden a la parte de host no están en 0, por lo que se trata de una dirección de host.

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

Pertenece a la clase B y la máscara de la clase es 255.255.0.0

c. Cantidad de hosts posibles.

$2^{16} - 2$

65534

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

i. Máscara necesaria.

11111111 11111111 11111111 11000000

255.255.255.192

ii. Cantidad de redes asignables.

1024

iii. Cantidad de hosts por subred.

62

iv. Dirección de la subred 710.

La subred 710 en binario sería la 709 ya que se empieza a contar desde 0. 710 en binario es 10110001 01 (separó en octetos)

Por lo que la dirección para la subred sería:

10000000 00110010 10110001 01000000

128.50.177.64

v. Dirección de broadcast de la subred 710

10000000 00110010 10110001 01111111

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?

11111111 11111111 11111111 11110000

195.200.45.240

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

11111111 11111111 11111111 00000000 - 195.200.45.0

11111111 11111111 11111111 00010000 - 195.200.45.16

11111111 11111111 11111111 00100000 - 195.200.45.32

11111111 11111111 11111111 00110000 - 195.200.45.48

11111111 11111111 11111111 01000000 - 195.200.45.64

11111111 11111111 11111111 01010000 - 195.200.45.80

11111111 11111111 11111111 01100000 - 195.200.45.96

11111111 11111111 11111111 01110000 - 195.200.45.112

11111111 11111111 11111111 10000000 - 195.200.45.128

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

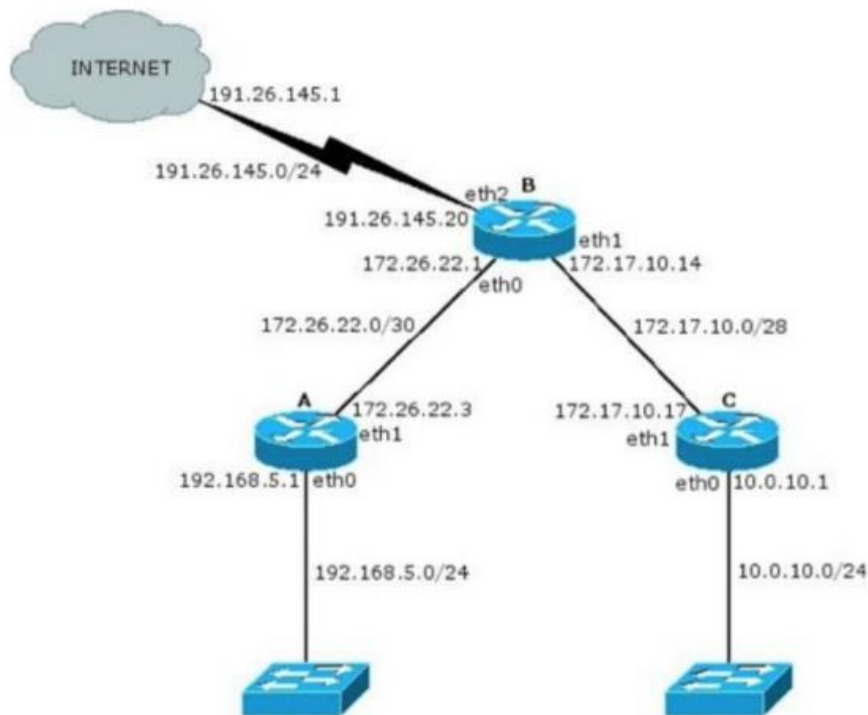
195.200.45.0

Broadcast: 11111111 11111111 11111111 00001111 – 195.200.45.15

Min: 11111111 11111111 11111111 00000001 – 195.200.45.1

Max: 11111111 11111111 11111111 00001110 – 195.200.45.14

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.

192.168.5.0 /24

11000000 10101000 00000101 00000000

11111111 11111111 11111111 00000000

192.168.5.1

11000000 10101000 00000101 00000001 Esta bien.

172.26.22.0 /30

10101100 00011010 00010110 00000000

11111111 11111111 11111111 11111100

172.26.22.3

10101100 00011010 00010110 00000011 Dirección de broadcast de la subred, está mal, esta debería ser 172.26.22.2.

172.26.22.1

10101100 00011010 00010110 00000011 Esta bien.

172.17.10.0 /28

10101100 00010001 00001010 00000000

11111111 11111111 11111111 11110000

172.17.10.14

10101100 00010001 00001010 00001110 Esta bien.

172.17.10.17

10101100 00010001 00001010 00010001 Esta mal, esta fuera del rango de los hosts de la red.

10.0.10.0 /24

00001010 00000000 00001010 00000000

11111111 11111111 11111111 00000000

10.0.10.1

00001010 00000000 00001010 00000001 Esta bien.

191.26.145.0 /25

10111111 11111010 10010001 00000000

11111111 11111111 11111111 10000000

191.26.145.1

10111111 11111010 10010001 00000001 Esta bien.

191.26.145.20

10111111 11111010 10010001 00010100 Esta bien.

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

Se tomaron 16, ya que se trata de una dirección de clase A cuya mascara default es 255.0.0.0 y acá se está usando 255.255.255.0 por lo que se tomaron 16 bits más.

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

(las que están mal no las pongo)

Privadas:

- 10.0.10.0
- 172.17.10.0
- 192.168.5.0
- 172.26.22.0

Publica:

- 191.26.145.0

CIDR

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

CIDR es una estrategia para frenar algunos problemas que se habían comenzado a manifestar con el crecimiento de Internet.

Los mismos son:

- Agotamiento del espacio de direcciones de clase B.
- Crecimiento de las tablas de enrutamiento más allá de la capacidad del software y hardware disponibles.
- Eventual agotamiento de las direcciones IP en general.

CIDR consiste básicamente en permitir máscaras de subred de longitud variable (VLSM) para optimizar la asignación de direcciones IP y utilizar resumen de rutas para disminuir el tamaño de las tablas de enrutamiento.

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

11111111 11111111 11111100 00000000

198.10.0.0/22

Esta red contiene todas las direcciones mencionadas.

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

- 200.56.168.0/21

Clase C. Mascara Default /24

11001000 00111000 10101000 00000000 Direccion
11111111 11111111 11111111 00000000 Mascara Default
11111111 11111111 11111000 00000000 CIDR

Las redes involucradas van desde:

11001000 00111000 10101000 00000000 – 200.56.168.0/24
11001000 00111000 10101111 00000000 – 200.56.175.0/24

- **195.24.0.0/13**

Clase C. Mascara Default /24

```
11000011 00011000 00000000 00000000
11111111 11111111 11111111 00000000 Mascara Default
11111111 11111000 00000000 00000000 CIDR
```

Las redes involucradas van desde:

```
11000011 00011000 00000000 00000000 – 195.24.0.0/24
11000011 00011111 11111111 00000000 – 195.31.255.0/24
```

- **195.24/13**

Clase C. Mascara Default /24

```
11000011 00011000 00000000 00000000
11111111 11111111 11111111 00000000 Mascara Default
11111111 11111000 00000000 00000000 CIDR
```

Las redes involucradas van desde:

```
11000011 00011000 00000000 00000000 – 195.24.0.0/24
11000011 00011111 11111111 00000000 – 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?

```
10000000 00000000 00000000 00000000
11111111 11111111 00000000 00000000 Mascara Default
11000000 00000000 00000000 00000000 CIDR
```

```
00000000 00000000 00000000 00000000
11111111 00000000 00000000 00000000 Mascara Default
10000000 00000000 00000000 00000000 CIDR
```

0.0.0.0/1

Si, equivale a listar todas las direcciones de clase B. El bloque CIDR que agrupa todas las redes de clase A es 0.0.0.0/1

VLSM

14. ¿Qué es y para qué se usa VLSM?

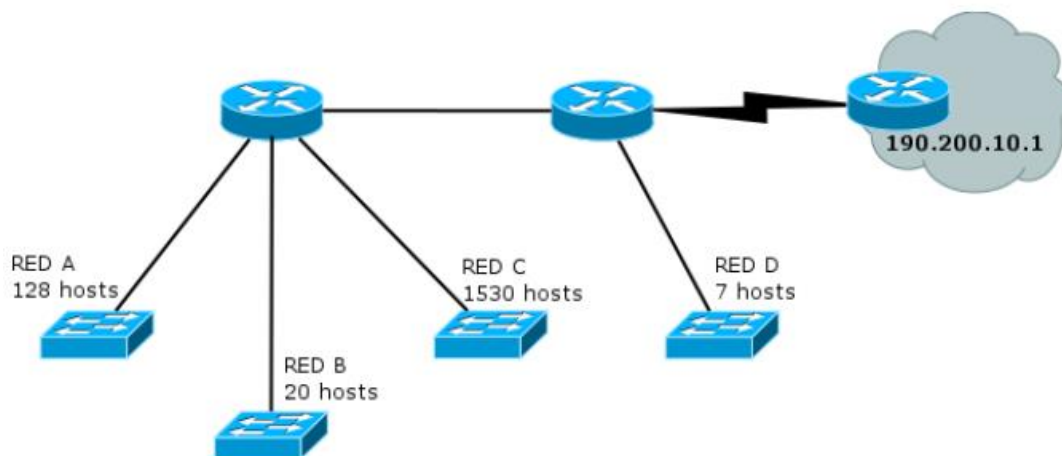
VLSM es realizar divisiones en subredes con máscaras de longitud variable. Sugiere hacer varios niveles de división en redes para lograr máscaras óptimas para las subredes. Se utiliza para evitar el agotamiento y desperdicio de direcciones IP.

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.

(el de con mis palabras te lo debo es un copie y pegue PERO QUE MAS PUEDO HACER)

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?

Necesito 6 subredes (una por cada red y otra por las que comunican a los routers, ahí necesito una punto a punto) por lo tanto necesito 3 bits

205.10.192.0/19

11001101 00001010 11000000 00000000

11111111 11111111 11100000 00000000 Mascara de red

11111111 11111111 11111100 00000000 Mascara de subred

Red C necesita 1530 hosts, necesita 11 bits que generarían un total de 2048 hosts. No se tienen los bits suficientes en la parte de host para asignarle a la red C los que necesita por lo que no se podrían usar.

b. Indique la cantidad de hosts que se desperdicia en cada subred. Asigne direcciones a todas las redes de la topología. Tome siempre en cada paso la primera dirección de red posible.

Red con mayor cantidad de hosts

Red C necesita 1532 hosts, necesita 11 bits que generarían un total de 2048 hosts (se desperdiciarían 516).

11001101 00001010 11000000 00000000

11111111 11111111 11100000 00000000 Mascara de red

11111111 11111111 11111000 00000000 Mascara de subred

Quedan 2 bits que se pueden utilizar para subredes

11001101 00001010 11000000 00000000 – 205.10.192.0/21 – Asignada a Red C

11001101 00001010 11001000 00000000 – 205.10.200.0/21 – Libre para seguir siendo dividida.

11001101 00001010 11010000 00000000 – 205.10.208.0/21

11001101 00001010 11011000 00000000 – 205.10.216.0/21

Red A necesita 130 hosts, necesita 8 bits que generarían un total de 256 hosts (se desperdiciarían 126)

11001101 00001010 11001000 00000000

11111111 11111111 11111000 00000000 Mascara de subred

11111111 11111111 11111111 00000000 Nueva mascara de subred

Quedan 3 bits que se pueden utilizar para subredes

11001101 00001010 11001000 00000000 – 205.10.200.0/24 – Asignada a Red A

11001101 00001010 11001001 00000000 – 205.10.201.0/24 – Libre para seguir siendo dividida.

11001101 00001010 11001010 00000000 – 205.10.202.0/24

11001101 00001010 11001011 00000000 – 205.10.203.0/24

11001101 00001010 11001100 00000000 – 205.10.204.0/24

11001101 00001010 11001101 00000000 – 205.10.205.0/24

11001101 00001010 11001110 00000000 – 205.10.206.0/24

11001101 00001010 11001111 00000000 – 205.10.207.0/24

Red B necesita 22 hosts, necesita 5 bits que generarían un total de 32 hosts (se desperdiciarían 10).

11001101 00001010 11001001 00000000

11111111 11111111 11111111 00000000 Mascara de subred

11111111 11111111 11111111 11100000 Nueva mascara de subred

Quedan 3 bits que se pueden utilizar para subredes

11001101 00001010 11001001 00000000 – 205.10.201.0/27 – Asignada a la Red B

11001101 00001010 11001010 00100000 – 205.10.201.32/27 – Libre para seguir siendo dividida.

11001101 00001010 11001010 01000000 – 205.10. 201.64 /27

11001101 00001010 11001010 01100000 – 205.10. 201.96/27

11001101 00001010 11001010 10000000 – 205.10. 201.128/27

11001101 00001010 11001010 10100000 – 205.10. 201.160/27

11001101 00001010 11001010 11000000 – 205.10. 201.192/27

11001101 00001010 11001010 11100000 – 205.10. 201.224/27

Red D necesita 9 hosts, necesita 4 bits que generarían un total de 32 hosts (se desperdiciarían 23)

11001101 00001010 11001010 00100000

11111111 11111111 11111111 11100000 Mascara de subred

11111111 11111111 11111111 11110000 Nueva mascara de subred

Queda 1 bit para ser usado para subredes

11001101 00001010 11001010 00100000 – 205.10.201.32/28 – Asignada a la Red D

11001101 00001010 11001010 00110000 – 205.10.201.48/28 – Libre para seguir siendo dividida.

Red E (punto a punto) necesita 4 hosts, necesita 2 bits que generarían un total de 4 hosts (se desperdician 0)

11001101 00001010 11001010 00110000

11111111 11111111 11111111 11110000 Mascara de subred

11111111 11111111 11111111 11111100 Nueva mascara de subred

Quedan 2 bits para ser usados para subredes

11001101 00001010 11001010 00110000 – 205.10.201.48/30 –
Asignada a la Red E

11001101 00001010 11001010 00110100 – 205.10.201.52/30 – Libre
para seguir siendo dividida.

11001101 00001010 11001010 00111000 – 205.10.201.56/30

11001101 00001010 11001010 00111100 – 205.10.201.60/30

- 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.**

Direcciones libres

11001101 00001010 11010000 00000000 – 205.10.208.0/21

11001101 00001010 11011000 00000000 – 205.10.216.0/21

CIDR → 11001101 00001010 11010000 00000000 – 205.10.208.0/20

11001101 00001010 11001010 00000000 – 205.10.202.0/24

11001101 00001010 11001011 00000000 – 205.10.203.0/24

CIDR → 11001101 00001010 11001010 00000000 – 205.10.202.0/23

11001101 00001010 11001100 00000000 – 205.10.204.0/24

11001101 00001010 11001101 00000000 – 205.10.205.0/24

11001101 00001010 11001110 00000000 – 205.10.206.0/24

11001101 00001010 11001111 00000000 – 205.10.207.0/24

CIDR → 11001101 00001010 11001100 00000000 – 205.10.204.0/22

11001101 00001010 11001010 01000000 – 205.10.201.64/27

11001101 00001010 11001010 01100000 – 205.10.201.96/27

CIDR → 11001101 00001010 11001010 01000000 – 205.10.201.64/26

11001101 00001010 11001010 10000000 – 205.10.201.128/27

11001101 00001010 11001010 10100000 – 205.10.201.160/27

11001101 00001010 11001010 11000000 – 205.10. 201.192/27

11001101 00001010 11001010 11100000 – 205.10. 201.224/27

CIDR → 11001101 00001010 11001010 10000000 – 205.10.201.128/25

11001101 00001010 11001010 00110100 – 205.10.201.52/30

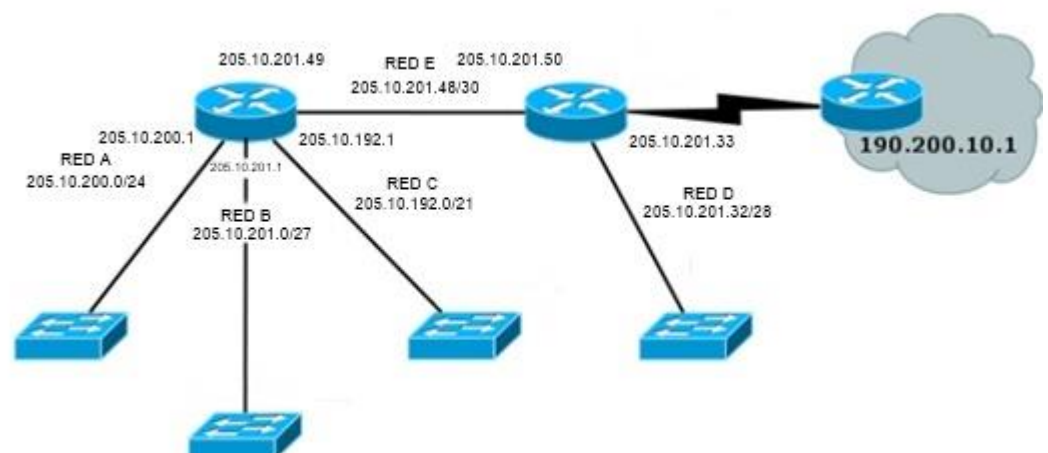
CIDR → 11001101 00001010 11001010 00110100 – 205.10.201.52/30

11001101 00001010 11001010 00111000 – 205.10.201.56/30

11001101 00001010 11001010 00111100 – 205.10.201.60/30

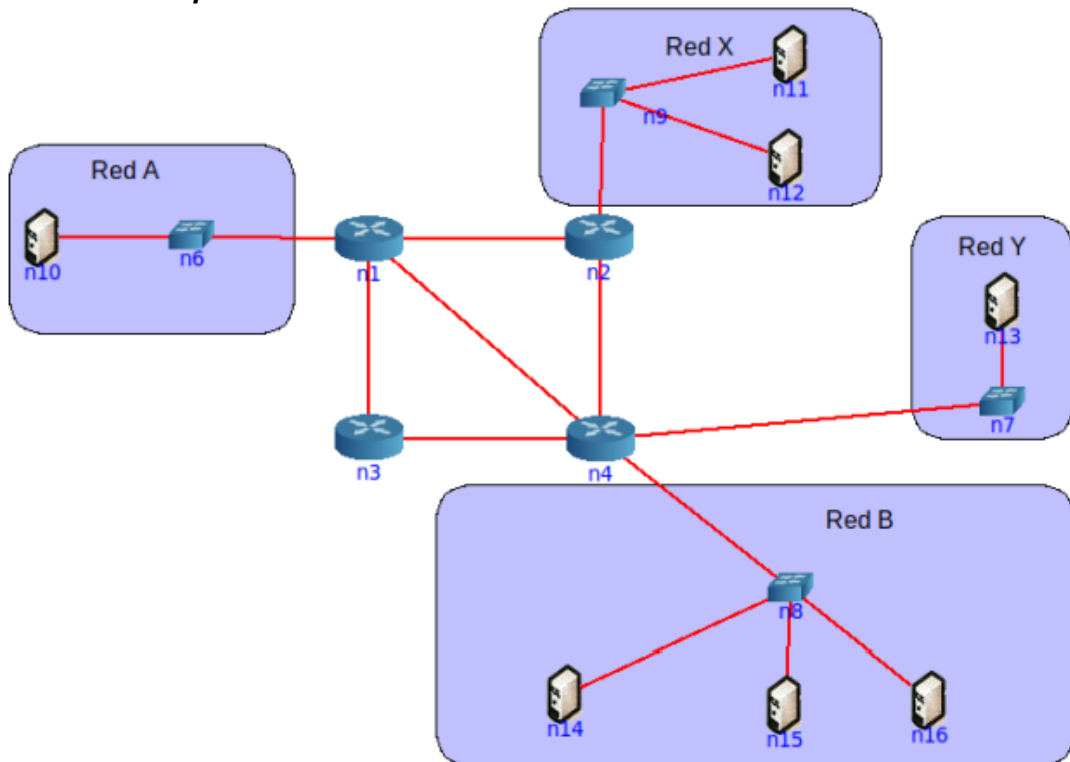
CIDR → 11001101 00001010 11001010 00111000 – 205.10.201.56/29

- 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:

Utilizar el bloque IPv4 200.100.8.0/22



- La red A tiene 125 hosts y se espera un crecimiento máximo de 20 hosts.
- La red X tiene 63 hosts.
- La red B cuenta con 60 hosts
- La red Y tiene 46 hosts y se espera un crecimiento máximo de 18 hosts.
- 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.

Red A necesita 147 hosts, necesita 8 bits que generarían 256 hosts

11001000 01100100 00001000 00000000

11111111 11111111 11111100 00000000 Mascara de red

11111111 11111111 11111111 00000000 Mascara de subred

Quedan 2 bits para ser usados para subredes

11001000 01100100 00001000 00000000 – 200.100.8.0/24 – Asignada a la Red A

11001000 01100100 00001001 00000000 – 200.100.9.0/24 – Libre para seguir siendo dividida.

11001000 01100100 00001010 00000000 – 200.100.10.0/24

11001000 01100100 00001011 00000000 – 200.100.11.0/24

Red Y y Red X necesitan 64 y 63 hosts respectivamente, necesitan 7 bits que generarían 128 hosts

11001000 01100100 00001001 00000000

11111111 11111111 11111111 00000000 Mascara de subred

11111111 11111111 11111111 10000000 Nueva mascara de subred

Queda 1 bits para ser usados para subredes

11001000 01100100 00001001 00000000 – 200.100.9.0/25 – Asignada a la Red Y

11001000 01100100 00001001 10000000 – 200.100.9.128/25 – Asignada a la Red X

Red B necesita 62 hosts, necesita 6 bits que generarían 64 hosts

11001000 01100100 00001010 00000000

11111111 11111111 11111111 00000000 Mascara de subred

11111111 11111111 11111111 11000000 Nueva mascara de subred

Quedan 2 bits para ser usados para subredes

11001000 01100100 00001010 00000000 – 200.100.10.0/26 – Asignada a la Red B

11001000 01100100 00001010 01000000 – 200.100.10.64/26 – Libre para seguir siendo dividida.

11001000 01100100 00001010 10000000 – 200.100.10.128/26

11001000 01100100 00001010 11000000 – 200.100.10.192/26

Redes N1-N2, N2-N4, N4-N3, N3-N1, N1-N4 necesitan 4 hosts, necesitan 2 bits que generarían 4 hosts

11001000 01100100 00001010 01000000

11111111 11111111 11111111 11000000 Mascara de subred

11111111 11111111 11111111 11111100 Nueva mascara de subred

Quedan 4 bits para ser usados para subredes

11001000 01100100 00001010 01000000 – 200.100.10.64/30 – Asignada a la Red N1-N2

11001000 01100100 00001010 01000100 – 200.100.10.68/30 – Asignada a la Red N2-N4

11001000 01100100 00001010 01001000 – 200.100.10.72/30 – Asignada a la Red N4-N3

11001000 01100100 00001010 01001100 – 200.100.10.76/30 – Asignada a la Red N3-N1

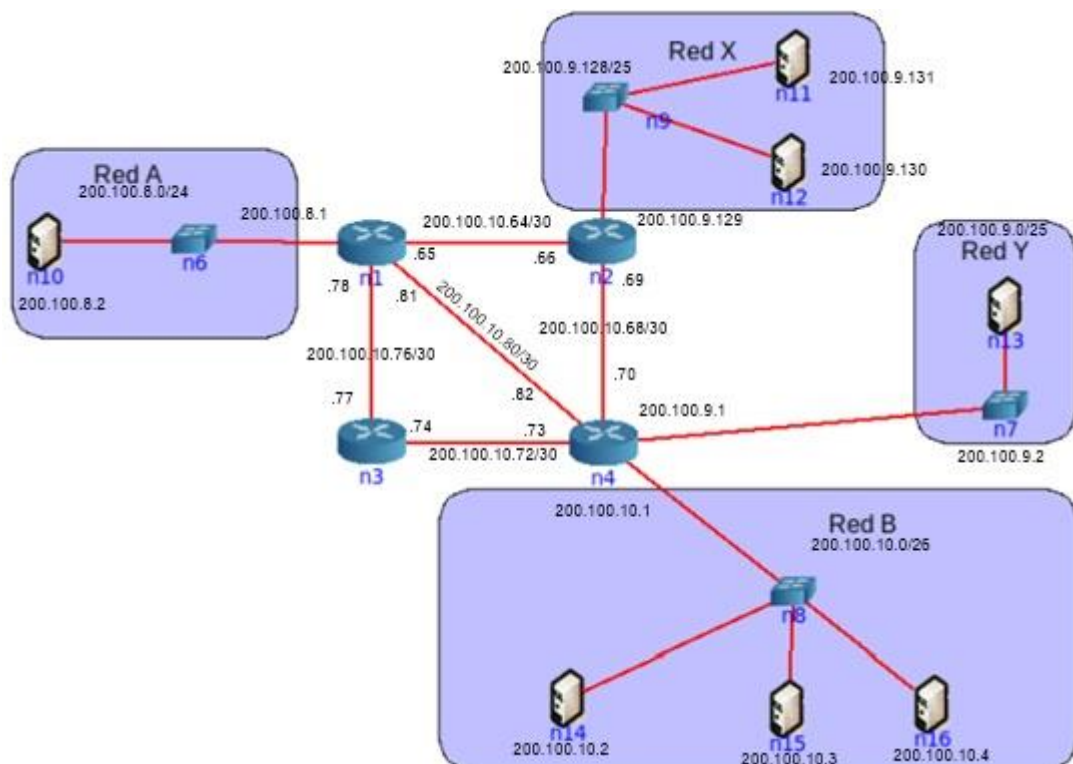
11001000 01100100 00001010 01010000 – 200.100.10.80/30 – Asignada a la Red N1-N4

11001000 01100100 00001010 01010100 – 200.100.10.84/30 – Libre para seguir siendo dividida.

11001000 01100100 00001010 01011000 – 200.100.10.88/30 – Libre para seguir siendo dividida.

11001000 01100100 00001010 01011100 – 200.100.10.92/30 – Libre para seguir siendo dividida.

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.

Internet Control Message Protocol es un protocolo "helper" de IP. Brinda un "feedback" para poder resolver problemas en la red. Este protocolo se encapsula en IP.

a. Analice cómo funciona el comando ping.

El comando "ping" se utiliza para probar la conectividad entre dos hosts en una red IP. Básicamente, envía un mensaje de solicitud (Echo Request) a un host y espera una respuesta (Echo Reply). Esto permite medir el tiempo que tarda en viajar la solicitud y regresar la respuesta. Esto se conoce como el RTT (Round-Trip Time), y el "ping" muestra estadísticas como el RTT mínimo, promedio, máximo y desviación estándar, junto con la pérdida de paquetes lo que puede ayudar a diagnosticar problemas de conectividad. Cuando un nodo recibe una solicitud "Echo Request", debe responder copiando el contenido del mensaje con un "Echo Reply" (pong).

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

Ping envía un paquete ICMP tipo 8 (Echo Request) con código 0. Este paquete contiene un mensaje de solicitud de eco. El código 0 especifica que es una solicitud estándar sin código específico.

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

Cuando el destino recibe una solicitud de eco (paquete ICMP tipo 8), responde con un paquete ICMP tipo 0 (Echo Reply) con código 0. El código 0 especifica que es una respuesta estándar sin código específico.

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

"traceroute" y "tracert" rastrean la ruta de un paquete IP ajustando el campo TTL del paquete. Comienzan con un TTL bajo y lo aumentan progresivamente. Cada salto de red reduce el TTL y envía una respuesta ICMP "Time Exceeded." El comando registra las direcciones IP de los saltos intermedios, lo que permite mostrar la ruta desde el origen hasta el destino.

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

```

agusr@DESKTOP-E5THSHN MINGW64 /a/Agus/Escritorio
$ tracert -d www.nasa.gov

Traza a la dirección nasa-gov.go-vip.net [192.0.66.108]
sobre un máximo de 30 saltos:

 1    3 ms    1 ms    1 ms    192.168.0.1
 2   31 ms   26 ms   22 ms   181.171.68.1
 3    *      *      *      Tiempo de espera agotado para esta solicitud.
 4    *      *      *      Tiempo de espera agotado para esta solicitud.
 5    *      *      *      Tiempo de espera agotado para esta solicitud.
 6   20 ms   15 ms   15 ms   181.96.113.234
 7    *      *      *      Tiempo de espera agotado para esta solicitud.
 8  179 ms   22 ms   14 ms   181.96.62.70
 9   17 ms   18 ms   15 ms   200.25.50.86
10    *      *      *      Tiempo de espera agotado para esta solicitud.
11   45 ms   55 ms   42 ms   200.25.51.246
12   45 ms   48 ms   46 ms   200.25.57.147
13   43 ms   45 ms   43 ms   192.0.66.108

Traza completa.

```

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

Para que no muestre el nombre del dominio asociado a la IP de cada salto, se puede usar la opción -d para evitar la resolución de nombres.

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

Cuando aparece un asterisco (*) en parte o en toda la respuesta de un salto, significa que ese enrutador o dispositivo de red no respondió a la solicitud de "traceroute" o "tracert". Puede ser una medida de seguridad, configuración o simplemente que el enrutador no responde a las solicitudes ICMP utilizadas por "traceroute" para rastrear la ruta.

- 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?**

```

agusr@DESKTOP-E5THSHN MINGW64 /a/Agus/Escritorio
$ tracert -d unlp.edu.ar

Traza a la dirección unlp.edu.ar [163.10.0.135]
sobre un máximo de 30 saltos:

 1    1 ms    1 ms    1 ms    192.168.0.1
 2   14 ms   14 ms   15 ms   181.171.68.1
 3    *      *      *      Tiempo de espera agotado para esta solicitud.
 4    *      *      *      Tiempo de espera agotado para esta solicitud.
 5    *      *      *      Tiempo de espera agotado para esta solicitud.
 6   19 ms   15 ms   15 ms   181.96.113.234
 7   18 ms   18 ms   11 ms   200.0.17.12
 8   17 ms   13 ms   13 ms   200.115.81.1
 9   14 ms   15 ms   15 ms   163.10.199.203
10    *      *      *      Tiempo de espera agotado para esta solicitud.
11    *      *      *      Tiempo de espera agotado para esta solicitud.
12    *      *      *      Tiempo de espera agotado para esta solicitud.
13    *      *      *      Tiempo de espera agotado para esta solicitud.
14    *      *      *      Tiempo de espera agotado para esta solicitud.
15    *      *      *      Tiempo de espera agotado para esta solicitud.
16    *      *      *      Tiempo de espera agotado para esta solicitud.
17    *      *      *      Tiempo de espera agotado para esta solicitud.
18    *      *      *      Tiempo de espera agotado para esta solicitud.
19    *      *      *      Tiempo de espera agotado para esta solicitud.
20    *      *      *      Tiempo de espera agotado para esta solicitud.
21    *      *      *      Tiempo de espera agotado para esta solicitud.
22    *      *      *      Tiempo de espera agotado para esta solicitud.
23    *      *      *      Tiempo de espera agotado para esta solicitud.
24    *      *      *      Tiempo de espera agotado para esta solicitud.
25    *      *      *      Tiempo de espera agotado para esta solicitud.
26    *      *      *      Tiempo de espera agotado para esta solicitud.
27    *      *      *      Tiempo de espera agotado para esta solicitud.
28    *      *      *      Tiempo de espera agotado para esta solicitud.
29    *      *      *      Tiempo de espera agotado para esta solicitud.
30    *      *      *      Tiempo de espera agotado para esta solicitud.

Traza completa.

```

No, no es posible determinar el camino que siguen los servidores de nombres del dominio unlp.edu.ar debido a que todas las respuestas muestran "Tiempo de espera agotado para esta solicitud.". Esto puede ser porque los servidores de nombres de dominio están configurados para no responder a traceroute o porque hay un problema en la red que impide que las respuestas lleguen de vuelta.

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

El bloque de direcciones IP 127.0.0.0/8 está reservado para el uso en la red de loopback. La dirección IP más comúnmente utilizada en este bloque es 127.0.0.1, que se conoce como "localhost". La dirección de loopback se utiliza para permitir que un dispositivo se comunique consigo mismo, lo que es útil en el diagnóstico y la prueba de aplicaciones y servicios de red sin la necesidad de acceder a una red real.

a. ping 127.0.0.1

El comando ping 127.0.0.1 recibirá una respuesta de la propia computadora.

b. ping 127.0.54.43

El comando ping 127.0.54.43 recibirá una respuesta de la propia computadora.

21. Investigue para qué sirven los comandos ifconfig y route. ¿Qué comandos podría utilizar en su reemplazo? 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.**
- ifconfig se utiliza para configurar y visualizar información de interfaces de red en sistemas Unix/Linux. Alternativamente, se recomienda utilizar ip para una funcionalidad más avanzada.
- route muestra y modifica la tabla de enrutamiento en sistemas Unix/Linux. En sistemas más recientes, se puede usar ip route o netstat -r para ver la tabla de enrutamiento, y ip route add y ip route del para agregar o eliminar rutas.

todo lo de este punto lo aplique en el 16 de la próxima practica así que no lo voy a completar.