

Practica 7 DIRECCIONAMIENTO

Dudas

12 - ~~Revisar IP 124.24/13~~ → Es lo mismo que escribir con los 0

13 - ~~Revisar segunda pregunta~~ → Esta bien hay que justificar mejor

16 - ~~Revisar proceso y resultado~~

~~Yo en el ejercicio al hacer la primera division, es decir, asignar la primera red (la C) tome 2 bits de los host, lo hice pq asi lo vimos en la explicacion practica, pero estoy desperdiciando 2 redes, porque no puedo simplemente tomar un bit y listo?~~

→ Podes

~~¿Cuál es la notacion para cuando tenemos subredes de subredes? → No te compliques~~

~~¿Es correcta la asignacion de ip (carpeta)?~~

→ Si

19 - ~~Revisar Salida del inciso D~~ → Ejercicio caducado

Ejercicio 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 brinda los siguientes servicios:

- Enrutamiento: Para determinar la mejor ruta para enviar paquetes desde el origen hasta el destino.
- Control de congestionamiento: Este servicio ayuda a gestionar la cantidad de trafico que se envía a través de la red.
- Fragmentación y re-ensamblaje: Los paquetes de datos pueden ser demasiado grandes para la transmisión en algunas redes. La capa de red se encarga de fragmentar estos paquetes en partes mas pequeñas que puedan ser transmitidas.
- Direccion logica: La capa de red asigna direcciones logicas a los dispositivos en la red. Estas direcciones son únicas dentro de su red y permiten la identificación y localización de dispositivos.

La PDU de la capa de red es el **PAQUETE (packet)**

El dispositivo que es cosiderado exclusivamente de la capa de red es el **ROUTER** (enrutador)

Ejercicio 2

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

IP es un protocolo de mejor esfuerzo porque no asegura una entrega fiable de los paquetes, es decir, IP no garantiza los datos ni el orden, solo se ocupa de transportar paquetes desde el origen a un destino sin hacer garantías de calidad de servicio (Esto es controlado por la capa superior, como TCP).

Ejercicio 3

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

Clase A:

- Rango: 10.0.0 a 126.255.255.255
- Cantidad de redes: **128 redes ($2^7 - 2$ reservadas para loopback y multicast)**
- Cantidad de hosts por red: **16,777,214 hosts ($2^{24} - 2$ reservados para red y broadcast)**

Clase B:

- Rango: 128.0.0.0 a 191.255.255.255
- Cantidad de redes: **16,384 redes (2^{14})**
- Cantidad de hosts por red: **65,534 hosts ($2^{16} - 2$)**

Clase C:

- Rango: 192.0.0.0 a 223.255.255.255
- Cantidad de redes: **2,097,152 redes (2^{21})**
- Cantidad de hosts por red: **254 hosts ($2^8 - 2$)**

Ejercicio 4

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

Las **subredes (subnets)** son divisiones lógicas de una red IP más grande en segmentos más pequeños y manejables. Esto permite organizar y optimizar el flujo de datos en una red y **mejorar la eficiencia en el uso de direcciones IP**.

En lugar de tener una sola red grande, se crean múltiples subredes, cada una con su propio rango de direcciones IP.

Por ejemplo, una red clase B (172.16.0.0/16) puede subdividirse en subredes más pequeñas como 172.16.0.0/24, 172.16.1.0/24, etc.

¿Por qué es importante especificar siempre la máscara de subred?

La **máscara de subred (subnet mask)** es fundamental porque define:

1. Identificación de Red vs. Host:

- La máscara permite diferenciar la parte de la dirección IP que representa la red y la parte que representa el host.
- Por ejemplo:
 - IP: 192.168.1.10
 - Máscara: 255.255.255.0
 - La red es 192.168.1.0 y el host es 10.

2. Determinación del Rango de IPs:

- La máscara establece los límites del rango de IPs que pertenecen a una subred.
- Sin la máscara, no se puede saber si 192.168.1.10 y 192.168.2.10 están en la misma subred o en subredes distintas.

3. Enrutamiento Correcto:

- Los **routers usan la máscara de subred para tomar decisiones de enrutamiento**. Si no se especifica la máscara, no pueden determinar correctamente la red de destino.

4. Seguridad y Segmentación:

- Dividir una red en subredes permite aplicar políticas de seguridad más precisas y reducir el tráfico de broadcast.

Ejercicio 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?

La cabecera Protocol identifica el protocolo de la capa superior (TCP, UDP, etc).

Se asemeja a los campos DestinationPort y SourcePort de la capa de transporte, estos campos indican a que aplicación o servicio deben dirigirse los datos recibidos

Ejercicio 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:

- ¿De qué clase de red es la dirección dada (Clase A, B o C)?
- ¿Cuál es la dirección de subred?
- ¿Cuál es la cantidad máxima de hosts que pueden estar en esa subred?
- ¿Cuál es la dirección de broadcast de esa subred?
- ¿Cuál es el rango de direcciones IP válidas dentro de la subred?

IP	Clase	Dirección Subred	Host Máximos	Dirección Broadcast	Rango de IP válidas dentro de la subred
172.16.58.223/26	B	172.16.58.192	62	172.16.58.255	172.16.58.193 a 172.16.58.254
163.10.5.49/27	B	163.10.5.32	30	163.10.5.63	163.10.5.33 a 163.10.5.62
128.10.1.0/23	B	128.10.0.0	510	128.10.1.255	128.10.0.1 a 128.10.1.254
10.1.0.0/24	A	10.1.0.0	254	10.1.0.255	10.1.0.1 a 10.1.0.254
8.40.11.179/12	A	8.32.0.0	1048574	8.47.255.255	8.32.0.1 a 8.47.255.255

Ejercicio 7

Su organización cuenta con la dirección 128.50.10.0. Indique:

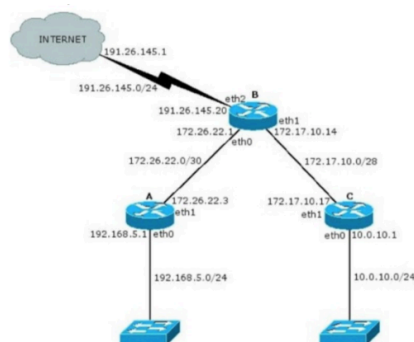
- ¿Es una dirección de red o de host?
- Clase a la que pertenece y máscara de clase.
- Cantidad de hosts posibles.
- Se necesitan crear, al menos, 513 subredes. Indique:
 - Máscara necesaria.
 - Cantidad de redes asignables.
 - Cantidad de hosts por subred.
 - Dirección de la subred 710.
 - Dirección de broadcast de la subred 710.

Ejercicio 8

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

- ¿Qué máscara utilizaría si necesita definir al menos 9 subredes?
- Indique la dirección de subred de las primeras 9 subredes.
- Seleccione una e indique dirección de broadcast y rango de direcciones asignables en esa subred.

Ejercicio 9 En función de las máscaras verificar si están dentro del rango



- Verifique si es correcta la asignación de direcciones IP y, en caso de no serlo, modifique la misma para que lo sea.
- ¿Cuántos bits se tomaron para hacer subredes en la red 10.0.10.0/24? ¿Cuántas subredes se podrían generar?
- Para cada una de las redes utilizadas indique si son públicas o privadas.

Ejercicio 10

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

El **CIDR** permite agrupar direcciones IP de manera más flexible, sin depender de clases fijas (A, B, C).

- Reduce el crecimiento de las tablas de ruteo, ya que permite agrupar redes contiguas en una sola entrada.
- Se usa una notación de longitud de prefijo, como **/22**, que indica cuántos bits representan la red.

Ejercicio 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

Ejercicio 12

Listar las redes involucradas en los siguientes bloques CIDR:

- 200.56.168.0/21
- 195.24.0.0/13
- 195.24/13

Ejercicio 13 Revisar Carpeta

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?

Ejercicio 14

¿Qué es y para qué se usa VLSM?

El **VLSM** permite usar diferentes longitudes de máscara de subred en una misma red, lo cual es útil cuando tienes subredes con diferentes necesidades de hosts.

Este tipo de direccionamiento permite optimizar el uso de direcciones al asignar la cantidad de direcciones justas según los requerimientos de cada red.

Ejercicio 15

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

1. Partimos de una red base
Por ejemplo 192.168.1.0/24 (256 direcciones)
2. Listamos las subredes que necesito ordenadas de mayor a menor
Tenemos que saber cuantas subredes necesitamos y cuantos host necesita cada una
Ejemplo:
Subred A → 60 hosts
Subred B → 30 hosts
Subred C → 10 hosts
Subred D → 2 hosts
3. Asignamos direcciones segunda la cantidad de hosts

2^¿cuantos bits necesitamos para representar la cantidad de host?

En un principio teníamos la red 192.168.1.0/24 que expresada en bits es la siguiente:

1100000 10101000 00000001 00000000

11111111 11111111 11111111 00000000 → Mascara /24

De esta mascara necesitamos ahora representar los siguientes hosts por lo tanto primero tomamos 1 bit de la parte de los host

A → 2^6 → $64 - 2 = 62$ hosts

$32 - 6 = /26$

11111111 11111111 11111111 11000000 → /26

B → 2^5 → $32 - 2 = 30$ hosts

$32 - 5 = /27$

11111111 11111111 11111111 11100000 → /27

C → 2^4 → $16 - 2 = 14$ hosts

$32 - 4 = /28$

11111111 11111111 11111111 11110000 → /28

D → $2^2 \rightarrow 4 - 2 = 2$ hosts

$32 - 2 = /30$

11111111 11111111 11111111 11111100 → /30 (nivel maximo de subdivision)

4. Rango de direcciones IP de las subredes

00 → Red 1 /26

01 → Red 2 /26

10 → Red 3 /26

11 → Red 4 /26

SUBRED 1 → Corresponde a la red A → Ya que puede contener hasta 62 host

Comienzo 192.168.1.00 000000 → 192.168.1.0 (Subred)

Fin 192.168.

00111111 → 192.168.1.63 (Broadcast)

SUBRED 2 → No corresponde a la red B → Ya que necesita 30 host, esta red puede contener 62

Comienzo 192.168.1.01000000 → 192.168.1.64 (Subred)

Fin 192.168.1.

01111111 → 192.168.1.127 (Broadcast)

SUBRED 3 → No corresponde a la red C → Ya que necesita 10 host, esta red puede contener 62

Comienzo 192.168.1.10000000 → 192.168.1.128 (Subred)

Fin 192.168.1.

10111111 → 192.168.1.191 (Broadcast)

SUBRED 4 → No corresponde a la red C → Ya que necesita 2 host, esta red puede contener 62

Comienzo 192.168.1.11000000 → 192.168.1.192 (Subred)

Fin 192.168.1.

11111111 → 192.168.1.255 (Broadcast)

El siguiente paso es seguir subdividiendo la red 2

192.168.1.64 /26 = 62 hosts

11111111 11111111 11111111 01000000 → Tomo un bit mas

32 - 27 = 4 = 2^4 = 30 host

010 → Red 2.1 = 192.168.1.64 /27 = 30 hosts

011 → Red 2.2 = 192.168.1.96 /27 = 30 hosts

SUBRED 2.1 → Corresponde a la red B → Ya que puede contener hasta 30 host

Comienzo 192.168.1.

01000000 → 192.168.1.64 (Subred)

Fin 192.168.1.01011111 → 192.168.1.95 (Broadcast)

SUBRED 2.2 → No corresponde a la red C → Ya que necesita 10 host y esta red puede contener 30

Comienzo 192.168.1.01100000 → 192.168.1.96 (Subred)

Fin 192.168.1.01111111 → 192.168.1.127 (Broadcast)

El siguiente paso es seguir subdividiendo la red 2.2

192.168.1.96 /27 = 30 hosts

11111111 11111111 11111111 01100000 → Tomo un bit mas

32 - 28 = 4 = 2^4 = 14 hosts

0110 → Red 2.2.1 = 192.168.1.96 /28 = 14 hosts

0111 → Red 2.2.2 = 192.168.1.112 /28 = 14 hosts

SUBRED 2.2.1 → Corresponde a la red C → Ya que puede contener hasta 14 host

Comienzo 192.168.1.01100000 → 192.168.1.96 (Subred)

Fin 192.168.1.01101111 → 192.168.1.111 (Broadcast)

SUBRED 2.2.2 → No corresponde a la red D → Ya que puede contener hasta 14 host y necesita solo 2 **✗**
 Comienzo 192.168.1.01110000 → 192.168.1.112 (Subred)
 Fin 192.168.1.01111111 → 192.168.1.127 (Broadcast)

El siguiente paso es seguir subdividiendo la red 2.2.2

192.168.1.112 /28 = 14 hosts

11111111 11111111 11111111 01110000 → Tomo un bit mas

32 - 29 = 3 = 2^3 = 6 hosts → NOSOTROS NECESITAMOS SOLAMENTE 2 → Tomamos 1 bit mas

11111111 11111111 11111111

01110000

32 - 30 = 2 = 2^2 = 2 hosts

011100 → Red 2.2.2.1 = 192.168.1.112 /30 = 2 hosts

011101 → Red 2.2.2.2 = 192.168.1.116 /30 = 2 hosts

011110 → Red 2.2.2.3 = 192.168.1.120 /30 = 2 hosts

011111 → Red 2.2.2.4 = 192.168.1.124 /30 = 2 hosts

SUBRED 2.2.2.1 → Corresponde a la red D → Ya que puede contener hasta 2 hosts **✓**

Comienzo 192.168.1.01110000 → 192.168.1.112 (Subred)

Fin 192.168.1.01110011 → 192.168.1.115 (Broadcast)

SUBRED 2.2.2.2

Comienzo 192.168.1.01110100 → 192.168.1.116 (Subred)

Fin 192.168.1.01110111 → 192.168.1.119 (Broadcast)

SUBRED 2.2.2.3

Comienzo 192.168.1.01111000 → 192.168.1.120 (Subred)

Fin 192.168.1.01111011 → 192.168.1.123 (Broadcast)

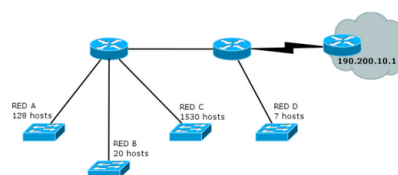
SUBRED 2.2.2.4

Comienzo 192.168.1.01111100 → 192.168.1.124 (Subred)

Fin 192.168.1.01111111 → 192.168.1.127 (Broadcast)

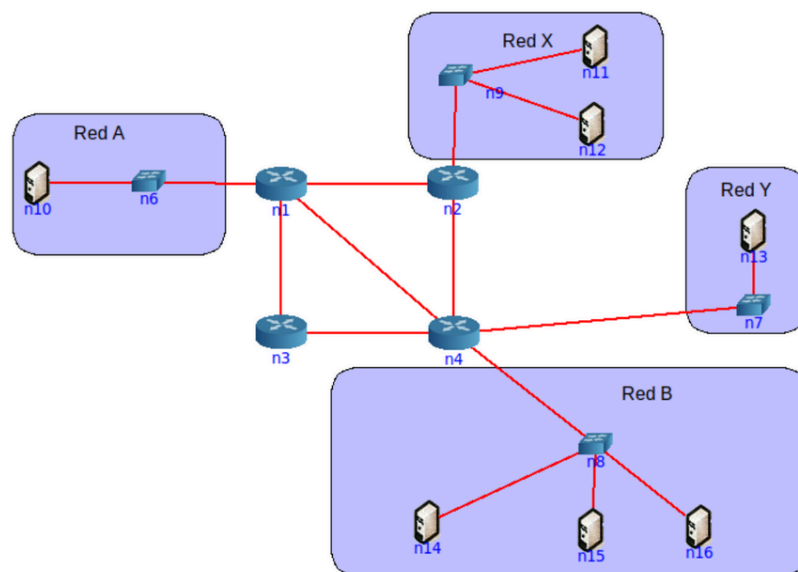
Ejercicio 16 Rehacer

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.



- ¿Es posible asignar las subredes correspondientes a la topología utilizando subnetting sin VLSM? 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.
- Para mantener el orden y el inventario de direcciones disponibles, haga un listado de todas las direcciones libres que le quedaron, agrupándolas utilizando CIDR.
- Asigne direcciones IP a todas las interfaces de la topología que sea posible.

Ejercicio 17



- 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.

Ejercicio 18

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

Ejercicio 19

Describa qué es y para qué sirve el protocolo ICMP.

- Analice cómo funciona el comando ping.
 - Indique el tipo y código ICMP que usa el ping.
 - Indique el tipo y código ICMP que usa la respuesta de un ping.
- Analice cómo funcionan comandos como traceroute/tracert de Linux/Windows y cómo manipulan el campo TTL de los paquetes IP.

c. Indique la cantidad de saltos realizados desde su computadora hasta el sitio

www.nasa.gov. Analice:

- Cómo hacer para que no muestre el nombre del dominio asociado a la IP de cada salto.
- La razón de la aparición de * en parte o toda la respuesta de un salto.

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?

ICMP (Internet Control Message Protocol) es un protocolo auxiliar de la suite TCP/IP. Su función principal es **enviar mensajes de control y error** para diagnosticar problemas en la red. Por ejemplo: si haces un **ping**, estás usando ICMP.

ICMP no transporta datos de aplicaciones como TCP o UDP; su función principal es notificar eventos de red (por ejemplo, "host inalcanzable", "TTL expirado", etc.).

- a. El comando ping permite probar la conectividad a nivel de IP con otro equipo TCP/IP mediante el envío de mensajes de solicitud de eco del protocolo de mensajes de control de internet (ICMP). Este último muestra la recepción de los mensajes de respuesta de eco correspondientes, junto a los tiempos de ida y de vuelta. Desde la computadora A se genera un mensaje llamado ICMP Echo Request, este mensaje se envía a la dirección IP del destino que quieres verificar, el otro extremo responde con un ICMP Echo Reply, se mide el RTT de ida y de vuelta. Este proceso se repite varias veces

¿Cómo funciona el comando

ping ?

ping utiliza ICMP para comprobar si un host está accesible y medir el tiempo de ida y vuelta (RTT: Round Trip Time).

Proceso:

1. Tu máquina envía un mensaje **ICMP Echo Request** al destino.
 2. Si el destino está disponible, responde con un **ICMP Echo Reply**.
 3. ping mide el tiempo entre el envío y la recepción, mostrando:
 - Tiempo de ida y vuelta (RTT)
 - Número de paquetes enviados/recibidos
 - Porcentaje de pérdida de paquetes
 - i. Un paquete ICMP utiliza los campos entre otros campos
 - Campo Type que define el tipo de mensaje ICMP que se está enviando (Echo Request es el 8)
 - Campo Code es una subcategoría que brinda más información sobre el tipo específico del mensaje (el código para un Echo Request es el 0)
 - ii. El tipo y código de respuesta de un ping es el tipo 0 y el código es el 0
- b. Traceroute y Tracert ambos comandos descubren la ruta (hops) que siguen los paquetes para llegar a un destino. Lo hacen manipulando el campo TTL en los encabezados IP

Proceso común:

1. Envían un paquete con TTL = 1.
 - El primer router descarta el paquete y responde con ICMP "TTL exceeded".
2. Luego envían otro paquete con TTL = 2.
 - El segundo router hace lo mismo.
3. Se repite aumentando el TTL hasta llegar al destino.
 - El destino responde con un **Echo Reply** (tracert) o **Port Unreachable** (traceroute con UDP).

Esto permite descubrir **la ruta** (los routers intermedios) y medir el **retardo por salto**.





TTL de 64, 128, 255 además de permitir navegar por más routers, es decir llegar más lejos en la red son implementados según el SO para medir el tiempo en el que va a existir el paquete

TTL de 1 se utiliza en los comandos como traceroute y tracert para descubrir la ruta por la cual pasa el paquete

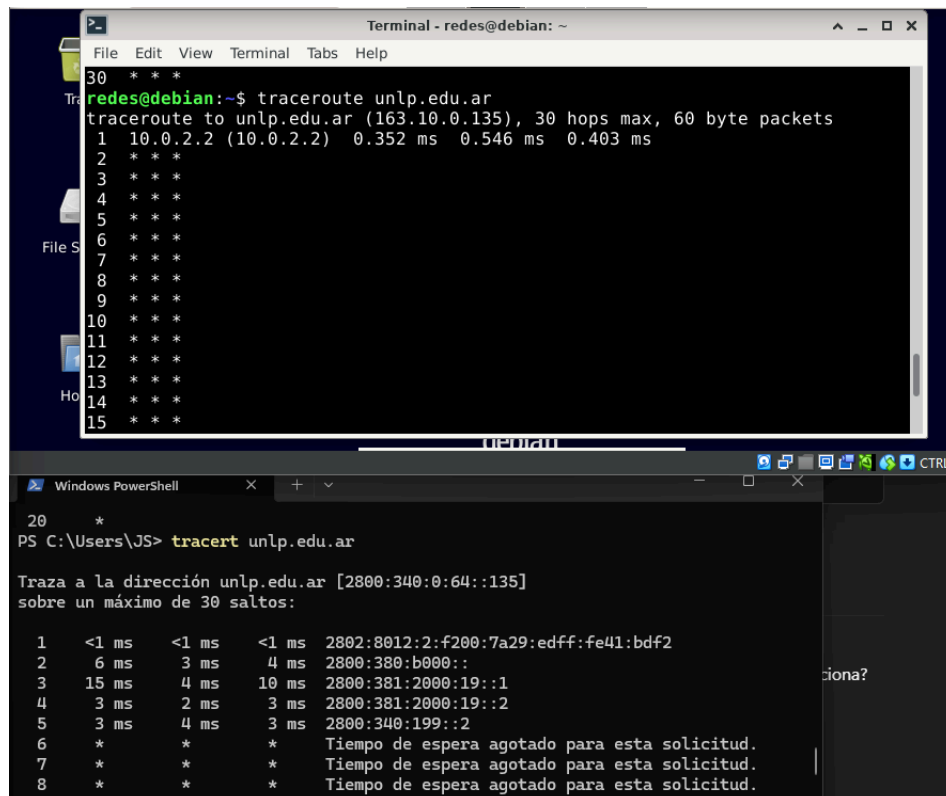
- c. 8 Saltos
- i. traceroute -n www.nasa.gov
tracert -d www.nasa.gov
 - ii.

Los asteriscos * indican que **no se recibió una respuesta ICMP "Time Exceeded" (TTL excedido)** desde ese salto **dentro del tiempo de espera**.

Esto puede deberse a:

Causa	Explicación
 Router/firewall bloquea ICMP	Algunos dispositivos intermedios están configurados para no enviar respuestas ICMP (por seguridad o configuración del administrador).
 Tiempo de espera agotado	El salto intermedio es lento o la red está congestionada.
 El router está sobrecargado	Algunos routers de backbone no responden a paquetes TTL vencido para evitar carga innecesaria.
 Políticas anti-trace	Algunos proveedores de servicios bloquean traceroute intencionalmente para ocultar su topología.

d.



```

Terminal - redes@debian: ~
30 * * *
redes@debian:~$ traceroute unlp.edu.ar
traceroute to unlp.edu.ar (163.10.0.135), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.352 ms  0.546 ms  0.403 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *

Windows PowerShell
20 *
PS C:\Users\JS> tracert unlp.edu.ar

Trazo a la dirección unlp.edu.ar [2800:340:0:64::135]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms    2802:8012:2:f200:7a29:edff:fe41:bdf2
 2  6 ms     3 ms     4 ms     2800:380:b000::
 3  15 ms    4 ms     10 ms    2800:381:2000:19::1
 4  3 ms     2 ms     3 ms     2800:381:2000:19::2
 5  3 ms     4 ms     3 ms     2800:340:199::2
 6  *        *        *        Tiempo de espera agotado para esta solicitud.
 7  *        *        *        Tiempo de espera agotado para esta solicitud.
 8  *        *        *        Tiempo de espera agotado para esta solicitud.

```

Ejercicio 20

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

- ping 127.0.0.1
- ping 127.0.54.43

El bloque corresponde al loopback también conocida como localhost usada para pruebas en el dispositivo local.

- Mi propia PC
- Mi propia PC

Ejercicio 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 – Interface Configuration

¿Para qué sirve?

Muestra y permite configurar las interfaces de red del sistema.

Usos comunes:

Comando	Función
<code>ifconfig</code>	Muestra todas las interfaces de red activas y su configuración actual.
<code>ifconfig eth0</code>	Muestra la configuración de la interfaz <code>eth0</code> .
<code>ifconfig eth0 down</code>	Desactiva la interfaz <code>eth0</code> .
<code>ifconfig eth0 up</code>	Activa la interfaz <code>eth0</code> .
<code>ifconfig eth0 192.168.1.10</code>	Asigna la IP 192.168.1.10 a <code>eth0</code> .

 Nota: En distribuciones modernas, `ifconfig` ha sido reemplazado por `ip addr` o `ip link`.


`route` – Tabla de enrutamiento

¿Para qué sirve?

Muestra o modifica la **tabla de rutas** del sistema, que indica cómo se deben enviar los paquetes según su destino.

Usos comunes:

Comando	Función
<code>route</code> o <code>route -n</code>	Muestra la tabla de enrutamiento del sistema (<code>-n</code> evita resolución de nombres).
<code>route add default gw 192.168.1.1</code>	Agrega una ruta por defecto a través del gateway <code>192.168.1.1</code> .
<code>route del default</code>	Elimina la ruta por defecto.

 La ruta por defecto (default gateway) es a donde van los paquetes cuando el destino no coincide con ninguna otra ruta.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.1.1	0.0.0.0	UG	100	0	0	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

Explicación de cada columna:

Columna	Significado
Destination	Red de destino o IP a la que se dirige el paquete.
Gateway	IP del router o puerta de enlace (gateway) por donde debe salir el paquete. Si es <code>0.0.0.0</code> , significa que no necesita pasar por un gateway (es una red local).
Genmask	Máscara de red que define el tamaño de la red de destino.
Flags	Indicadores importantes: <code>U</code> = ruta activa, <code>G</code> = usa gateway, <code>H</code> = host (no red).
Metric	Costo de la ruta. Cuanto más bajo, más preferida.
Ref	Obsoleto en la mayoría de los sistemas.
Use	Cuántos paquetes usaron esta ruta (estadística).
Iface	Interfaz de red usada (ej: <code>eth0</code> , <code>wlan0</code>).

Equivalentes modernos:

En sistemas modernos (basados en `iproute2`), los comandos más actualizados son:

Acción	Comando nuevo
Ver interfaces	<code>ip addr</code> o <code>ip a</code>
Activar/desactivar íface	<code>ip link set dev eth0 up/down</code>
Ver tabla de rutas	<code>ip route</code>
Agregar ruta	<code>ip route add default via 192.168.1.1</code>