

Deber 2

1.

a) Probabilidad de que A gane la segunda carrera de retroceso después de la primera colisión

Para calcular la probabilidad de que A gane la segunda carrera de retroceso inmediatamente después de la primera colisión, necesitamos considerar las opciones de tiempo de retroceso para A y B. A puede retroceder 0 x T o 1 x T, mientras que B puede retroceder 0 x T, 1 x T, 2 x T o 3 x T.

A ganará si elige un tiempo de retroceso menor que B. Tenemos las siguientes posibles combinaciones de tiempos de retroceso para A y B:

- A: 0 x T, B: 1 x T, 2 x T, 3 x T
- A: 1 x T, B: 2 x T, 3 x T

Hay 5 combinaciones en total en las que A gana. Como hay 8 combinaciones posibles de tiempos de retroceso para A y B (2 opciones para A y 4 para B), la probabilidad de que A gane la segunda carrera de retroceso es:

$$P(A \text{ gana}) = 5/8 = 0.625$$

b) Probabilidad de que A gane la tercera carrera de retroceso después de la primera colisión si A gana la segunda carrera

Si A gana la segunda carrera de retroceso, A intentará transmitir A3 y luego A4, mientras que B intentará transmitir B1 nuevamente. Ahora, A puede retroceder 0 x T, 1 x T, 2 x T o 3 x T, mientras que B puede retroceder 0 x T, 1 x T, 2 x T, 3 x T, 4 x T, 5 x T, 6 x T o 7 x T.

Existen 20 combinaciones en las que A gana (A elige un tiempo de retroceso menor que B). Hay 32 combinaciones posibles en total (4 opciones para A y 8 para B), por lo que la probabilidad de que A gane la tercera carrera de retroceso es:

$$P(A \text{ gana}) = 20/32 = 0.625$$

c) Límite inferior razonable para la probabilidad de que A gane todas las carreras de retroceso restantes

Como A siempre tendrá menos opciones de tiempo de retroceso que B, la probabilidad de que A gane una carrera de retroceso nunca será menor que en el caso anterior (tercera carrera de retroceso). Por lo tanto, un límite inferior razonable para la probabilidad de que A gane todas las carreras de retroceso restantes es:

$$P(A \text{ gana}) \geq 0.625$$

d) ¿Qué sucede con el fotograma B1?

Si A continúa ganando todas las carreras de retroceso, el fotograma B1 nunca se transmitirá con éxito. Este efecto, en el cual un dispositivo (en este caso, A) domina la transmisión y evita que otro dispositivo (en este caso, B) transmita con éxito sus datos, se conoce como el efecto de captura en Ethernet.

2.

a) Probabilidad de que en una red de 1024 hosts, dos direcciones sean iguales

Para calcular la probabilidad de que en una red de 1024 hosts, dos direcciones sean iguales, debemos usar el principio del complemento y el problema del cumpleaños.

La probabilidad de que dos direcciones **no** sean iguales es:

$$1 - (\text{número de direcciones ya usadas}) / (\text{número total de direcciones})$$

Donde el número total de direcciones es 2^{48} (ya que las direcciones Ethernet tienen 48 bits).

Entonces, para 1024 hosts, la probabilidad de que **no** haya direcciones duplicadas es el producto de todas las probabilidades individuales:

$$P(\text{no duplicados}) = (1 - 0/2^{48}) * (1 - 1/2^{48}) * \dots * (1 - 1023/2^{48})$$

Ahora, usando el principio del complemento, la probabilidad de que haya al menos una dirección duplicada es:

$$P(\text{duplicados}) = 1 - P(\text{no duplicados})$$

b) Probabilidad de que el evento ocurra en una o más de 2^{20} redes

Para calcular la probabilidad de que el evento ocurra en una o más de 2^{20} redes, podemos usar nuevamente el principio del complemento y calcular la probabilidad de que **no** ocurra en ninguna de las redes:

$$P(\text{no ocurre en ninguna red}) = (P(\text{no duplicados}))^{2^{20}}$$

Y la probabilidad de que ocurra en al menos una red es:

$$P(\text{ocurre en al menos una red}) = 1 - P(\text{no ocurre en ninguna red})$$

c) Probabilidad de que, de los 2^{30} hosts en todas las redes de (b), algún par tenga la misma dirección

Para calcular esta probabilidad, podemos tratar todos los 2^{30} hosts como si fueran parte de una única red grande. Entonces, aplicamos el mismo enfoque que en la parte (a):

$$P(\text{no duplicados}) = (1 - 0/2^{48}) * (1 - 1/2^{48}) * \dots * (1 - (2^{30} - 1)/2^{48})$$

Y la probabilidad de que haya al menos una dirección duplicada es:

$$P(\text{duplicados}) = 1 - P(\text{no duplicados})$$

3.

- **Resistencia a fallos:** La topología de malla es más resistente a fallos, ya que cada nodo está conectado a múltiples otros nodos. Si un nodo falla, la información puede ser reenviada a través de otros nodos. En una estación base, si la estación central falla, toda la red se ve afectada.
- **Redundancia:** En una topología de malla, hay múltiples rutas para que los datos viajen entre nodos. Esto proporciona redundancia y permite que la red siga funcionando aunque algunas conexiones se vean afectadas por el desastre.
- **Escalabilidad:** Las redes de malla pueden crecer fácilmente sin necesidad de aumentar la capacidad de la estación base. Se pueden agregar nuevos nodos a la red simplemente conectándolos a otros nodos cercanos.

4.

a) Suponiendo que todos los fragmentos recibidos deben haber sido parte de la misma transmisión:

Probabilidad de pérdida de un fragmento: 1% (0.01)

Probabilidad de éxito de un fragmento: 99% (0.99)

Probabilidad de éxito de todos los fragmentos en una transmisión: $(0.99)^{10} \approx 0.9044$

Probabilidad de pérdida de al menos un fragmento en una transmisión: $1 - 0.9044 \approx 0.0956$

Probabilidad de pérdida de al menos un fragmento en ambas transmisiones: $(0.0956)^2 \approx 0.0091$

Probabilidad de pérdida neta del paquete completo si se transmite dos veces: 0.91%

b) Suponiendo que cualquier fragmento dado puede haber sido parte de cualquiera de las transmisiones:

Probabilidad de perder un fragmento en ambas transmisiones: $(0.01)^2 = 0.0001$

Probabilidad de éxito de un fragmento en al menos una transmisión: $1 - 0.0001 = 0.9999$

Probabilidad de éxito de todos los fragmentos en al menos una transmisión: $(0.9999)^{10} \approx 0.9990$

Probabilidad de pérdida neta del paquete completo si se transmite dos veces: $1 - 0.9990 \approx 0.10\%$

c) Explicación del uso del campo "ident" en este contexto:

El campo "ident" (identificación) en un paquete IP se utiliza para identificar los fragmentos que pertenecen al mismo paquete original. Cuando un paquete se fragmenta, todos los fragmentos reciben el mismo valor de identificación. En este caso, el campo "ident" podría

ser útil para rastrear y agrupar correctamente los fragmentos de las dos transmisiones diferentes. Al comparar los valores de "ident" de los fragmentos recibidos, el receptor podría determinar si los fragmentos provienen de la misma transmisión o de transmisiones diferentes y, por lo tanto, asegurarse de que se ensamblen correctamente los paquetes.

5.

A continuación, se muestran las tablas de reenvío de datagramas para cada nodo en la red dada. Los enlaces se etiquetan con costos relativos y las tablas deben reenviar cada paquete a través de la ruta de menor costo hacia su destino.

Nodo A:

Destino	Siguiente Salto	Peso
A	-	0
B	C	5
C	C	3
D	C	4
E	C	4
F	C	9

Nodo B:

Destino	Siguiente Salto	Peso
A	E	5
B	-	0
C	E	3
D	E	4
E	E	2
F	E	8

Nodo C:

Destino	Siguiente Salto	Peso
A	A	3
B	E	2
C	-	0
D	E	1
E	E	1

F	F	6
---	---	---

Nodo D:

Destino	Siguiente Salto	Peso
A	C	4
B	E	2
C	C	1
D	-	0
E	E	2
F	C	7

Nodo E:

Destino	Siguiente Salto	Peso
A	C	3
B	B	2
C	C	1
D	C	1
E	-	0
F	C	6

Nodo F:

Destino	Siguiente Salto	Peso
A	C	9
B	C	8
C	C	6
D	C	7
E	C	7
F	-	0

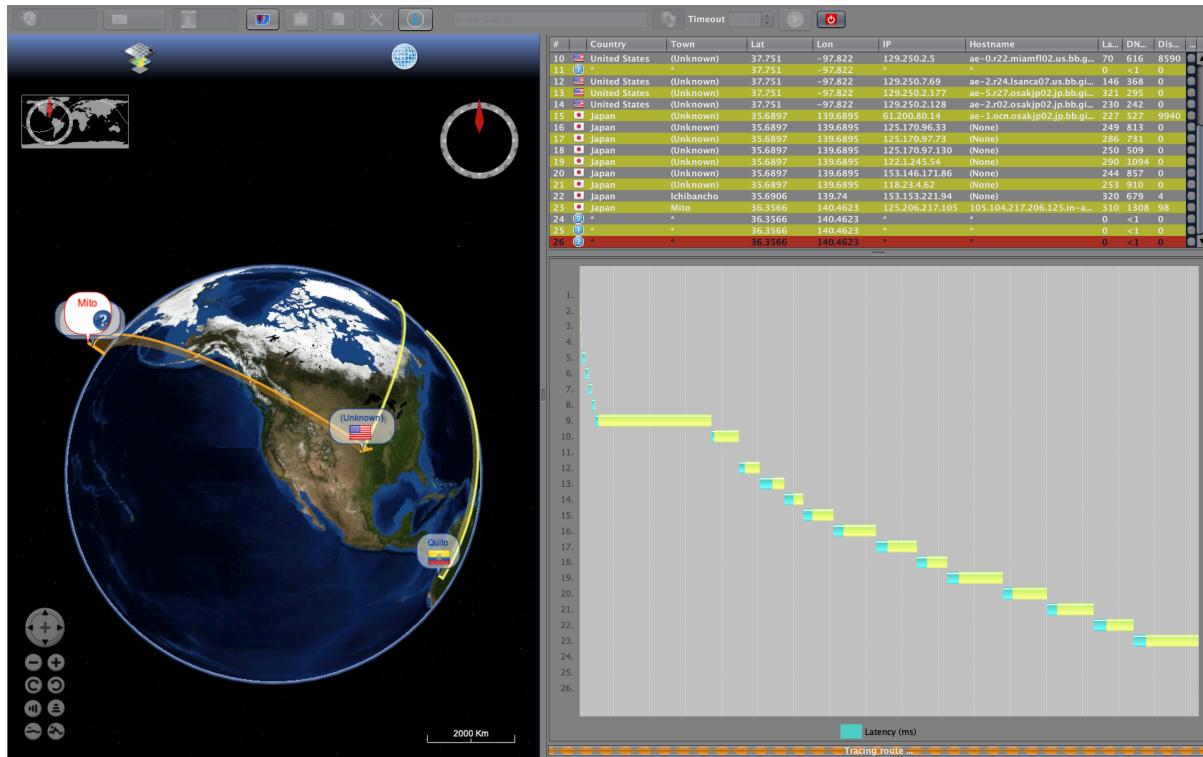
6.

El STA no considera todos los ports que sea bloqueados o que no esten asignados. Por lo tanto las conexion que salen desde B3 y que causan un loop no seran consideradas en el final spanning tree.

7.

Podemos tambien usar le programa Open Visual Traceroute:

IBU university, Japan - Budo-u.ac.jp



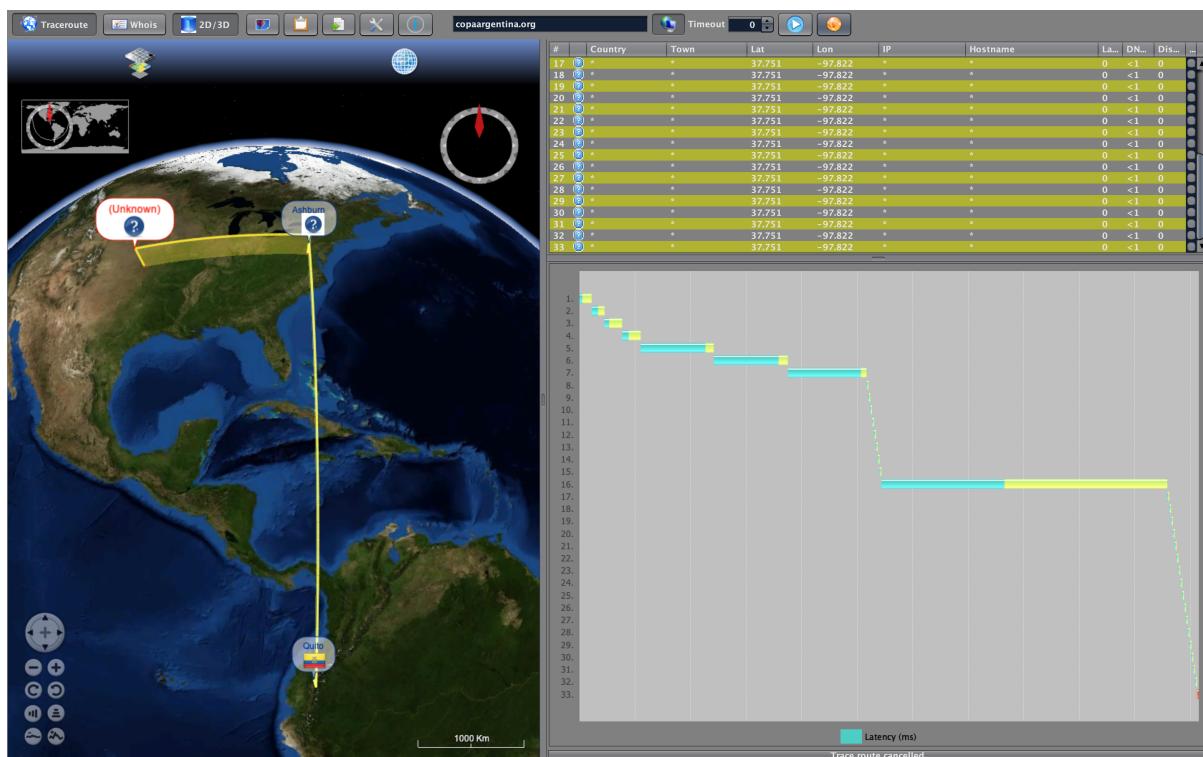
```
User ~ % traceroute budo-u.ac.jp
traceroute to budo-u.ac.jp (125.206.217.106), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  6.851 ms  3.281 ms  2.069 ms
 2  10.59.0.1 (10.59.0.1)  5.296 ms  13.260 ms  22.173 ms
 3  186.252.152.190.static.anycast.cnt-grms.ec (190.152.252.186)  18.696 ms  4.735 ms  4.827 ms
 4  185.252.152.190.static.anycast.cnt-grms.ec (190.152.252.185)  13.701 ms  29.423 ms  11.006 ms
 5  10.9.1.37 (10.9.1.37)  73.489 ms  112.229 ms  71.216 ms
 6  10.9.1.37 (10.9.1.37)  68.887 ms  79.634 ms  81.586 ms
 7  ae29.miami15.mia.seabone.net (89.221.41.44)  98.607 ms  86.740 ms  101.504 ms
 8  ae1.miami16.mia.seabone.net (195.22.199.82)  91.138 ms  84.024 ms  114.584 ms
 9  ntt-verio.miami16.mia.seabone.net (195.22.199.33)  111.054 ms  120.986 ms  84.115 ms
10  ae-0.r22.miamfl02.us.bb.gin.ntt.net (129.250.2.5)  93.418 ms  128.364 ms  150.708 ms
11  * * *
12  * * *
13  ae-5.r27.osakjp02.jp.bb.gin.ntt.net (129.250.2.177)  240.007 ms  279.227 ms  257.072 ms
14  ae-2.r03.osakjp02.jp.bb.gin.ntt.net (129.250.7.33)  254.042 ms  253.130 ms
   ae-2.r02.osakjp02.jp.bb.gin.ntt.net (129.250.2.128)  244.266 ms
15  ae-1.ocn.osakjp02.jp.bb.gin.ntt.net (61.200.80.14)  248.511 ms  289.576 ms
   ae-2.ocn.osakjp02.jp.bb.gin.ntt.net (61.200.80.74)  226.485 ms
16  153.149.219.145 (153.149.219.145)  341.934 ms
   125.170.96.33 (125.170.96.33)  248.989 ms
   153.149.219.145 (153.149.219.145)  292.838 ms
17  125.170.97.73 (125.170.97.73)  248.752 ms
   122.1.245.189 (122.1.245.189)  241.830 ms  287.213 ms
18  122.1.245.206 (122.1.245.206)  233.164 ms
   125.170.97.130 (125.170.97.130)  277.854 ms
   122.1.245.206 (122.1.245.206)  238.637 ms
19  122.1.245.50 (122.1.245.50)  251.829 ms
```

```

122.1.245.54 (122.1.245.54) 238.828 ms
60.37.54.70 (60.37.54.70) 236.801 ms
20 153.146.171.90 (153.146.171.90) 242.681 ms
153.146.171.94 (153.146.171.94) 248.065 ms
153.146.171.90 (153.146.171.90) 259.458 ms
21 118.23.4.66 (118.23.4.66) 328.367 ms 254.864 ms 231.665 ms
22 153.153.221.94 (153.153.221.94) 228.526 ms 238.202 ms 232.181 ms
23 rt1.budo-u.ac.jp (125.206.217.105) 255.343 ms 246.831 ms 250.288 ms

```

Copa Argentina - copaargentina.org



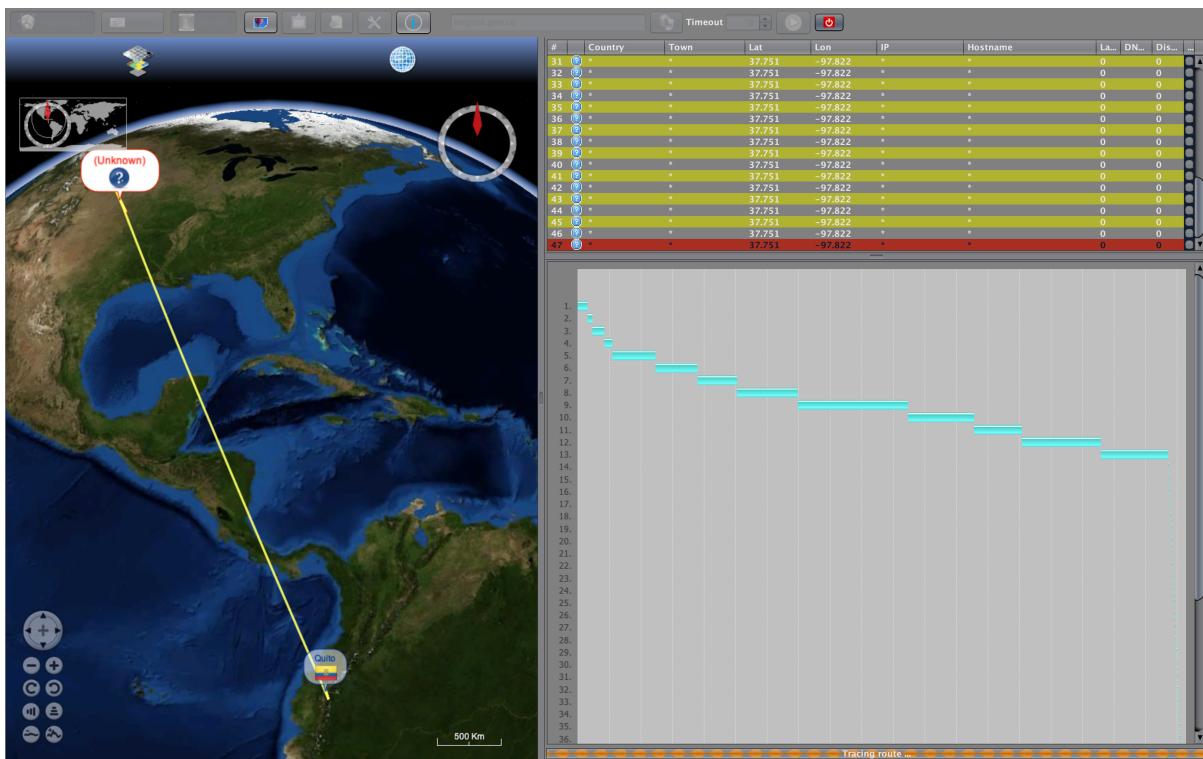
```

User ~ % traceroute copaargentina.org
traceroute to copaargentina.org (54.84.153.100), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  2.579 ms  1.677 ms  1.631 ms
 2  10.59.0.1 (10.59.0.1)  5.164 ms  5.287 ms  17.738 ms
 3  186.252.152.190.static.anycast.cnt-grms.ec (190.152.252.186)  8.740 ms  8.557 ms  5.329 ms
 4  185.252.152.190.static.anycast.cnt-grms.ec (190.152.252.185)  4.390 ms  3.913 ms  7.084 ms
 5  10.9.2.29 (10.9.2.29)  70.353 ms  71.922 ms  79.970 ms
 6  10.9.2.29 (10.9.2.29)  69.400 ms  81.770 ms  69.268 ms
 7  99.83.69.238 (99.83.69.238)  79.618 ms  79.248 ms  70.409 ms

```

despues de esto dio timeout

Ministerio de Bogota - bogota.gov.co



```
User ~ % traceroute bogota.gov.co
traceroute to bogota.gov.co (20.85.28.209), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  2.216 ms  1.869 ms  1.974 ms
 2  10.59.0.1 (10.59.0.1)  16.416 ms  4.731 ms  8.239 ms
 3  186.252.152.190.static.anycast.cnt-grms.ec (190.152.252.186)  4.590 ms  4.323 ms  4.519 ms
 4  185.252.152.190.static.anycast.cnt-grms.ec (190.152.252.185)  6.762 ms  4.292 ms  6.360 ms
 5  10.9.1.37 (10.9.1.37)  84.530 ms  80.192 ms  83.936 ms
 6  10.9.1.37 (10.9.1.37)  79.895 ms  85.724 ms  69.762 ms
 7  ae76-0.mia-96cbe-1a.ntwk.msn.net (104.44.36.83)  59.807 ms  81.451 ms  93.099 ms
 8  ae23-0.ear04.mia.ntwk.msn.net (104.44.230.205)  93.654 ms  128.674 ms  77.849 ms
 9  be-24-0.ibr01.mia.ntwk.msn.net (104.44.33.169)  100.411 ms
    be-24-0.ibr02.mia.ntwk.msn.net (104.44.33.167)  98.773 ms  93.063 ms
10  be-6-0.ibr01.fll30.ntwk.msn.net (104.44.19.15)  102.939 ms  102.466 ms  100.449 ms
11  * * *
12  be-8-0.ibr04.bn6.ntwk.msn.net (104.44.29.38)  103.140 ms *
    be-6-0.ibr03.bn6.ntwk.msn.net (104.44.29.8)  98.918 ms
13  ae162-0.icr04.bn6.ntwk.msn.net (104.44.20.138)  111.509 ms
    ae152-0.icr07.bn6.ntwk.msn.net (104.44.32.143)  90.920 ms  91.545 ms
14  * * *
15  * * *
16  * * be-4-0.ibr03.bn6.ntwk.msn.net (104.44.7.182)  104.272 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *

y despues solo timeout
```

La herramienta Unix 'traceroute' permite rastrear la ruta que siguen los paquetes de datos desde un origen hasta un destino en la red, proporcionando información detallada sobre cada salto intermedio. Según la documentación, esta herramienta funciona mediante el envío de paquetes de protocolo de Internet (IP) con valores de tiempo de vida (TTL) incrementales. Al alcanzar el TTL, los dispositivos intermedios devuelven un mensaje de error, permitiendo a 'traceroute' identificar los nodos en la ruta. La implementación se realiza de manera iterativa, incrementando el TTL en cada paso y capturando la información relevante de los dispositivos intermedios, hasta que el paquete llega a su destino. Esto ayuda a identificar problemas de enrutamiento o latencia en la red, y a obtener una visión más clara del camino que toman los datos.

8.

a) Rango de direcciones requerido

Para soportar los planes de crecimiento de la empresa durante al menos 7 años, necesitamos calcular cuántas direcciones IP se necesitarán en cada división al final de este período.

- **Ingeniería:** 5 máquinas iniciales + 1 máquina por semana * 52 semanas por año * 7 años = $5 + 364 = 369$ máquinas.
- **Marketing:** 16 máquinas (nunca necesitará más).
- **Ventas:** Necesitamos determinar cuántos clientes tendrán en promedio al final de los 7 años. Supongamos que tienen 6 clientes al inicio del año 2. La probabilidad de aumentar un cliente es 60%, disminuir un cliente es 20% y mantener el mismo número es 20%. En promedio, cada semana tendrán un crecimiento neto de 0.4 clientes (0.6 - 0.2). Entonces, en 6 años (312 semanas) tendrán aproximadamente $6 + (0.4 * 312) = 130.8$ clientes. Necesitan una máquina por cada dos clientes, por lo que requieren 66 máquinas.

En total, la empresa necesitaría espacio para 369 (Ingeniería) + 16 (Marketing) + 66 (Ventas) = 451 direcciones IP.

El rango de direcciones requerido para soportar estos planes de crecimiento sería un bloque CIDR con una máscara de red /23, que permite hasta 510 direcciones IP utilizables ($2^{(32-23)} - 2$).

b) Duración y asignación de direcciones

La asignación de direcciones 23 duraría al menos 7 años, ya que hemos calculado las necesidades de IP en función de los planes de crecimiento de la empresa durante ese período.

Al final de los 7 años, las direcciones se asignarían aproximadamente de la siguiente manera:

- **Ingeniería:** 369 direcciones IP.
- **Marketing:** 16 direcciones IP.
- **Ventas:** 66 direcciones IP.

c) Opciones sin CIDR

Si el direccionamiento CIDR no estuviera disponible, la empresa tendría algunas opciones para obtener espacio de direcciones:

1. **Solicitar más direcciones IP** a su ISP, aunque esto podría resultar en un uso ineficiente del espacio de direcciones y mayores costos.
2. **Utilizar NAT (Network Address Translation)** para compartir una cantidad limitada de direcciones IP públicas entre las máquinas internas de la red corporativa. Esto permite a la empresa utilizar direcciones IP privadas para sus dispositivos y ahorrar en el uso de direcciones IP públicas.
3. **Implementar IPv6**, que tiene un espacio de direcciones mucho más grande que IPv4 y permite asignar una gran cantidad de direcciones IP sin preocuparse por la escasez.