Subnetting Exercise

Transcribed on July 27, 2025 at 9:39 AM by Minutes AI

Speaker 1 (00:02)

Bienvenidos a esta nueva sesión, en esta sesión vamos a resolver el ejercicio relacionado con la segmentación de red o subnetting que hemos propuesto.

Para resolver el ejercicio voy a abrir una máquina virtual que podéis ver en pantalla, la cual la he dividido en la parte de la terminal y abajo un documento de texto en el que os voy a explicar cómo he ido siguiendo todo el proceso para resolver el ejercicio.

Bien pues utilizaremos una herramienta llamada IPCalc para verificar los cálculos que haremos ahora, para ello la vamos a instalar, ya la tenemos, pero lo que vamos a hacer es resolverlo primero nosotros de forma matemática y después comprobarlo con ipcal para para ver que realmente los hemos hecho bien todos los cálculos, de esta forma también aprendemos mejor cómo se hace todo lo que es el proceso de subnetting para este tipo de ejercicios.

Lo primero sería determinar la máscara de subred para al menos 30 host, pues bien para eso tenemos que saber cuántos bits se requieren para soportar al menos ese número de host que son 30, para eso utilizamos la siguiente fórmula.

Bien pues entonces tenemos que determinar la máscara de subred para al menos 30 host, para eso tenemos que saber cuántos bits se requieren para soportar al menos 30 host, y para eso usamos la fórmula genérica que es la siguiente 2 elevado a n-2 y esto debe ser mayor o igual a 30.

Esto sería un poco la primera fórmula que tenemos que aplicar, la cosa es identificar ese valor n, n es el número de bits del host, entonces haciendo un pequeño cálculo sabemos que 2 elevado a 5 menos 2 nos da igual a 30.

Entonces está claro que nos hacen falta 5 bits para los host, y dado que un byte tiene 8 bits, si le quitamos los 5 bits que nos hacen falta para los host nos quedan 3 bits para las subredes en el último octeto recordemos que la dirección que tenemos es esta, la que aparece en el enunciado con la máscara 24, la máscara 24 en binario sería algo así, tendría 8 bits 1, 2, 3, 4, 1, 2, 3, 4 otros 8 bits en el segundo bloque, en el tercero otros 8 bits y después ya tendríamos pues 8 ceros 1, 2, 3, 4.1, 2, 3, 4 lo pongo así para que veáis muy bien en detalle cómo se realiza todo este cálculo.

Entonces si ahora agregamos 3 bits para las subredes, la máscara pasa a ser 27, que sería algo así Igual que antes.

Igual que antes.

Igual que antes, pero ahora añadimos los 3 bits y ya sería el resto así.

Esto si lo pasamos a decimal tendríamos 255.255.255 2 2 4 bien, vamos ahora a calcular el número de subredes posibles.

Entonces con la máscara hemos tomado tres bits del espacio de host para usarlo en las subredes.

Esto nos daría un 2 elevado a 3, lo que es igual a 8 subredes posibles.

Ahora vamos a ver cómo se puede verificar esto en ipcalc.

Bien, pues ya que tenemos esto podemos empezar a resolver el ejercicio y lo que nos pide es obtener el rango de direcciones IP para la primera subred.

La primera subred con la máscara 27 se calcularía de la siguiente man Esto ahora lo vamos a verificar con ipcalc, pero directamente lo que tendríamos sería Veríamos que la dirección de red sería 192.168.10 esta sería la primera IP de la subred y se utilizará para identificarla.

Después tenemos la primera dirección asignable que sería 192.168 en este caso sería la primera IP que podemos utilizar para uno de los host.

La última dirección que podemos asignar sería la 192.168.1.30 esta sería la última IP que se puede utilizar en un host justo antes del broadcast que veremos ahora, que es la siguiente.

Entonces la siguiente sería ya la 192.

168.1.31 que sería la última IP de la subred y esta sí que es el broadcast.

Bien, pues todo esto que hemos hecho en un ratillo con algunos cálculos, vamos a ver que IP calc no lo va a resolver en cuestión de segundos.

Vamos a verlo.

Me iría al terminal y ejecutaría el comando ipcalc pondría la dirección que tenemos en el enunciado.

168 die s Bien, pues 192.168.10 es la dirección de red original, 24 es la máscara de subred actual y el guión s le está diciendo a IPCalc que queremos subredes que puedan soportar al menos 30 host.

Lo ejecutamos y vemos la salida.

Bien, pues vamos a analizar en detalle la salida que nos ha ofrecido ipcal.

Para ello voy a ampliar un poco la pantalla para que nos ocupe todo.

Aquí lo vemos, vemos los tres bloques que nos ha dado.

Bien, podemos ver perfectamente que hay tres bloques diferenciados.

El primer bloque que podéis ver aquí, lo que está indicando es la información inicial de la red, después vemos la solicitud de sus redes para albergar los 30 host y finalmente nos da una información adicional.

En el bloque principal, que es la información de la red original, podemos ver que la red proporcionada es la 192.

168.

10.

4, la que teníamos en el enunciado, con una máscara de subred de 255.000 255.000 255.0 y esto permite hasta 254 hostias.

Esta configuración es la típica de una subred de clase C, donde el último octeto, o sea los últimos 8 bits se usa para las direcciones del host.

Pues bien, la dirección mínima del host donde pone hostmin es 192.

168.1 y la máxima que es host match es 192.168.1.254 con 192.168 1.255 siendo la dirección de broadcast.

Pues estos detalles son clave para entender la capacidad y la estructura de la red antes de hacer la subdivisión.

El siguiente bloque, el que pone sus redes requeridas para 30 host, este de aquí, vamos a analizar ese bloque ahora.

Lo que estamos viendo aquí es que IPK lo que hace que calcula para justo eso, para al menos 30 host en cada subred y para eso necesita una máscara de 27, que fue justamente lo que hemos calculado nosotros, que es 255.

255.

255.

224.

Esto lo que hace es que divide la red original en 8 subredes posibles, que es 2 a la 3, que también lo ha visto antes.

La primera subred tiene las direcciones asignables que van desde la 192.

168.1 a la 192.

168.1.

1.30.

Esto lo he explicado antes cuando os decía por ejemplo que 30 son para los host y 2 que había una para la dirección de red y uno para el broadcast.

El siguiente bloque son las direcciones de subredes no utilizadas que es esta parte de la salida.

Entonces aquí lo que nos está diciendo es que nos está informando sobre las subredes que no se han utilizado en el proceso de la subdivisión, que son las 192.

168.1.32 con la subred 27 con la máscara.

Perdón.

192.

168.1.64 con máscara 26 y 192.

168 128 con barra 25.

Cuando ponemos la notación 27.26.25 lo que estamos haciendo es reflejando la cantidad de direcciones disponibles en cada una, indicando una mayor cantidad de direcciones para subred con una máscara de subred que sea numéricamente menor.

Como podéis ver, la segmentación de las redes es una práctica crítica en la gestión y seguridad de redes, y herramientas como esta como epcalc son esenciales para realizar de manera efectiva esta operación.

Al dividir una red grande en su redes más pequeñas, los administradores de red pueden mejorar muchísimo la seguridad y el rendimiento.

Cada subred actúa como una zona aislada, lo que limita la propagación de tráfico malicioso y reduce el dominio de broadcast, minimizando así el riesgo de ataque de red y la congestión.

Además, la segmentación facilita la implementación de políticas de seguridad diferenciadas, permitiendo un control más granular del acceso y los recursos de la Cuando usamos IPCAL para estos ejercicios, un administrador de red puede calcular con precisión los parámetros de la subred, evitando errores manuales que pueden ser muy frecuentes por los sencillos cálculos, pero al final siempre tendemos a cometer fallos, y asegurando que cada subred esté optimizada para la cantidad exacta de hosts requeridos, lo que refuerza la eficiencia operativa y mantiene una postura de seguridad robusta.

Este ejercicio de subnetting proporciona una herramienta crucial para mejorar la seguridad de las redes a reducir los dominios de difusión y limitar el impacto de posibles ataques.

Al implementar el subnetting en entornos reales se facilita la gestión de recursos y se permite la segmentación de red, y esto contribuye a crear un entorno de red más seguro y manejable.

Esta práctica es fundamental para proteger la integridad y la confidencialidad de los datos de redes empresariales y proporciona una sólida defensa contra intrusiones y amenazas.

En resumen, el subnetting es una estrategia esencial para securizar redes de datos y garantizar su eficiencia y confiabilidad en el mundo real.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.