**Calcula  subnetting**

IP de red y máscara de subred con IPv4

Una dirección IP es un número de identificación lógico de un equipo en la red, o de una red o subred. Las direcciones IPv4 tienen 32 bits en formato decimal separado por puntos, no se debe confundir con la dirección MAC que se representa con notación hexadecimal separado por dos puntos o guiones. Las direcciones IP pueden cambiar dinámicamente, tanto a nivel de direccionamiento IP público como privado, aunque también se podría dar el caso de que sea fija. El subnetting es la técnica de dividir una red grande en redes más pequeñas (subredes), para calcular qué máscara de subred necesitaremos utilizar en la nueva red, deberemos calcular diferentes parámetros. Hoy en RedesZone os vamos a enseñar cómo podemos realizar subnetting de una forma fácil y rápida, tanto de forma «manual» como también usando calculadoras IP que nos facilitarán la vida.

Disponer de redes en donde el funcionamiento es el adecuado y óptimo, es algo muy importante hoy en día. Esto es algo que no se consigue tan solo adquiriendo materiales de calidad o que permitan altas velocidades, sino que tener un buen diseño de la red es un factor determinante. Aquí es donde entra el subnetting y todas sus características y posibilidades.

**Qué es el subnetting, tipos y clases de direcciones**

El subnetting consiste en dividir una red grande en varias subredes más pequeñas, esto se debe realizar con mucho cuidado y planificación para no desaprovechar direcciones IPv4. Generalmente el subnetting se realiza a nivel local, utilizando el rango de direccionamiento IP privado que tenemos disponible para nuestro uso sin limitaciones, sin embargo, también se puede hacer subnetting de cara al direccionamiento IP público, siempre que trabajes o tengas tu propio operador y tu propio rango de direcciones IP públicas para utilizar. En este tutorial vamos a trabajar específicamente con direccionamiento IP privado en todos los ejemplos.

Existen muchos motivos para querer dividir una red grande en varias redes más pequeñas, como, por ejemplo:

* **Ampliar o reducir el rango de direcciones IP de la red local**. Si tenemos una red muy grande, es posible que queramos reducir el número de direcciones IP disponibles, con el objetivo de administrarlas de forma más sencilla. Vamos a lograr algo más manejable.
* **Optimización de la red**: una red muy grande podría tener muchísimo tráfico de broadcast, esto hace que la red sea mucho más lenta. Si quieres optimizar los recursos y lograr que funcione lo mejor posible, es una buena opción.
* **Mejorar la organización de toda la red**: podremos dividir una red muy grande en subredes más pequeñas, para usar cada subred para un determinado público. Por ejemplo, podríamos crear una subred de gestión, de administración, de equipos de ventas, una subred para invitados etc. Muy útil de cara a una empresa que quiera dividirlas.
* **Mayor seguridad y control del tráfico**: al dividir en subredes pequeñas, podremos segmentar adecuadamente nuestra red en VLANs (nivel 2) y usar diferente direccionamiento IP (nivel 3) para permitir o denegar el tráfico entre los diferentes equipos. Gracias al subneteo o subnetting, los administradores de redes pueden gestionar de manera más sencilla todo el tráfico entrante y saliente.

Una vez que hemos visto qué es el subnetting y todas sus ventajas, vamos a hablar de los diferentes tipos de direcciones IPv4 que existen.

**Tipos de direcciones IPv4**

En redes IPv4 existen un total de tres tipos de direcciones IP, cada tipo de dirección IP está orientado a una determinada tarea, estas direcciones IP son:

* **Dirección de red**: es la dirección IP a la que hace referencia la red o subred. Para calcular la dirección de red es necesario realizar la operación AND entre una dirección IP orientada a los hosts (ordenadores, servidores) y la máscara de subred configurada. La dirección de red es la que incluyen sus routers en sus tablas de enrutamiento, para saber llegar a un determinado destino, y para saber cuál es el origen de un determinado paquete.
* **Dirección de host**: son las direcciones IP asignadas a los equipos finales de la red. Un ordenador, una impresora o un smartphone tendrá una dirección IP de host. Básicamente, cualquier dispositivo que se conecte al router va a tener una distinta y va a ser imprescindible para poder establecer la comunicación.
* **Dirección de broadcast**: es una dirección especial, se utiliza para enviar datos a todos los hosts dentro de una red. La dirección de broadcast dentro de una subred siempre es la última dirección IP. También existe una dirección especial de broadcast cuando no hemos obtenido aún direccionamiento IP por parte del servidor DHCP, o por parte del administrador de red de forma manual, esta dirección especial es la 255.255.255.255.

La mayoría de nosotros en nuestros hogares tenemos un router que tiene la dirección IP 192.168.1.1, y los equipos que se conectan a la red tienen direccionamiento 192.168.1.2 hasta el 192.168.1.254 habitualmente. Por eso tu ordenador, móvil, televisión o cualquier aparato que conectes al router y tenga acceso a Internet, va a tener una dirección IP asignada del tipo 192.168.1.x. En todos estos hosts se está utilizando una máscara de subred 255.255.255.0. Todas estas direcciones IP son direcciones de host, la dirección de red la podemos calcular haciendo la operación (192.168.1.1 AND 255.255.255.0), que tiene como resultado 192.168.1.0, por tanto, la dirección de red es la 192.168.1.0. En cuanto a la dirección de broadcast, es la última dirección de la red, por tanto, en este caso la dirección de broadcast es la 192.168.1.255.

Si tu router no tuviera la dirección IP 192.168.1.1, puedes averiguar fácilmente cuál es. Para ello, en Windows, tienes que ir a Inicio, entras en la Terminal y ejecutas el comando ipconfig. Verás información de tu red y uno de los datos es la puerta de enlace predeterminada. Aunque esa que hemos indicado es la más habitual, es posible que la hayas cambiado o que el modelo de router que utilizas tenga otra distinta configurada. Algunos modelos traen otra de forma predeterminada, aunque igualmente siempre la vas a poder cambiar si prefieres otra. Una muy común también en muchos routers es la puerta de enlace predeterminada 192.168.0.1.

La máscara de subred juega un papel fundamental a la hora de hacer subnetting, porque nos va a indicar qué bits pertenecen a la parte de red y cuál pertenece a la parte de hosts. La máscara de subred determina la dirección IP de red, el rango de direcciones IP para los hosts, y también la dirección IP de broadcast. La máscara de subred se puede expresar en binario, en decimal separado por puntos como una dirección IP, y también en notación CIDR. La notación CIDR es básicamente el número de 1 que tenemos de izquierda a derecha en la máscara de subred en notación binaria. En la siguiente tabla podéis todas las máscaras de subred en binario, decimal y notación CIDR, además, también podéis ver el número de host máximo dependiendo de la máscara de subred.

| **Binario** | **Decimal** | **Notación CIDR** | **Máximo número de host** |  |
| --- | --- | --- | --- | --- |
| 11111111.11111111.11111111.11111111 | 255.255.255.255 | /32 |  |  |
| 11111111.11111111.11111111.11111110 | 255.255.255.254 | /31 |  |  |
| 11111111.11111111.11111111.11111100 | 255.255.255.252 | /30 | 2 |  |
| 11111111.11111111.11111111.11111000 | 255.255.255.248 | /29 | 6 |  |
| 11111111.11111111.11111111.11110000 | 255.255.255.240 | /28 | 14 |  |
| 11111111.11111111.11111111.11100000 | 255.255.255.224 | /27 | 30 |  |
| 11111111.11111111.11111111.11000000 | 255.255.255.192 | /26 | 62 |  |
| 11111111.11111111.11111111.10000000 | 255255255128 | /25 | 126 |  |
| 11111111.11111111.11111111.00000000 | 255.255.255.0 | /24 | 254 |  |
| 11111111.11111111.11111110.00000000 | 255.255.254.0 | /23 | 510 |  |
| 11111111.11111111.11111100.00000000 | 255.255.252.0 | /22 | 1022 |  |
| 11111111.11111111.11111000.00000000 | 255.255.248.0 | /21 | 2046 |  |
| 11111111.11111111.11110000.00000000 | 255.255.240.0 | /20 | 4094 |  |
| 11111111.11111111.11100000.00000000 | 255.255.224.0 | /19 | 8190 |  |
| 11111111.11111111.11000000.00000000 | 255.255.192.0 | /18 | 16382 |  |
| 11111111.11111111.10000000.00000000 | 255.255.128.0 | /17 | 32766 |  |
| 11111111.11111111.00000000.00000000 | 255.255.0.0 | /16 | 65534 |  |
| 11111111.11111110.00000000.00000000 | 255.254.0.0 | /15 | 131070 |  |
| 11111111.11111100.00000000.00000000 | 255.252.0.0 | /14 | 262142 |  |
| 11111111.11111000.00000000.00000000 | 255.248.0.0 | /13 | 524286 |  |
| 11111111.11110000.00000000.00000000 | 255.240.0.0 | /12 | 1048574 |  |
| 11111111.11100000.00000000.00000000 | 255.224.0.0 | /11 | 2097150 |  |
| 11111111.11000000.00000000.00000000 | 255.192.0.0 | /10 | 4194302 |  |
| 11111111.10000000.00000000.00000000 | 255.128.0.0 | /9 | 8388606 |  |
| 11111111.00000000.00000000.00000000 | 255.0.0.0 | /8 | 16777214 |  |
| 11111110.00000000.00000000.00000000 | 254.0.0.0 | /7 | 33554430 |  |
| 11111100.00000000.00000000.00000000 | 252.0.0.0 | /6 | 67108862 |  |
| 11111000.00000000.00000000.00000000 | 248.0.0.0 | /5 | 134217726 |  |
| 11110000.00000000.00000000.00000000 | 240.0.0.0 | /4 | 268435454 |  |
| 11100000.00000000.00000000.00000000 | 224.0.0.0 | /3 | 536870910 |  |
| 11000000.00000000.00000000.00000000 | 192.0.0.0 | /2 | 1073741822 |  |
| 10000000.00000000.00000000.00000000 | 128.0.0.0 | /1 | 2147483646 |  |
| 00000000.00000000.00000000.00000000 | 0. | /0 | 4294967294 |  |

Hay determinadas direcciones IPv4 que no pueden asignarse a los hosts, como la dirección IP de red o la dirección IP de broadcast, el sistema operativo directamente nos daría error. También encontramos IPv4 que pueden asignarse a los hosts pero con restricciones en la interacción de dichos hosts dentro de la red.

**Clases de direcciones IPv4**

En el direccionamiento con IPv4 existen diferentes tipos de redes, cada una con una función distinta. Estas fueron creadas con el objetivo de crear redes de tamaño grande, mediano y pequeño. Actualmente todos los routers de Internet hacen uso de protocolos de enrutamiento dinámico de pasarela interior (IGP) y también protocolos EGP que son classless, por tanto, estaremos haciendo uso de VLSM (Máscaras de subred de tamaño variable) con el objetivo de ahorrar muchas direcciones IP y no malgastarlas.

Existen direcciones de clase A, B, C que son las más utilizadas, también tenemos las clases D que son las direcciones de Multicast, y las de clase E que son para uso experimental o de pruebas. En la siguiente tabla se puede ver un resumen de las diferentes clases que tenemos:

| **Clase** | **A** | **B** | **C** | **D** | **E** |
| --- | --- | --- | --- | --- | --- |
| Rango de direcciones IP | 0.0.0.0 a 127.255.255.255 | 128.0.0.0 a 191.255.255.255 | 192.0.0.0 a 223.255.255.255 | 224.0.0.0 a 239.255.255.255 | 240.0.0.0 a 254.255.255.255 |
| Máscara de subred | 255.0.0.0 | 255.255.0.0 | 255.255.255.0 | Sin definir | Sin definir |
| Máscara de subred CIDR | 8 | 16 | 24 | Sin definir | Sin definir |
| Direccionamiento privado | 10.0.0.0 a 10.255.255.255 | 172.16.0.0 a 172.31.255.255 | 192.168.0.0 a 192.168.255.255 |  |  |

Tal y como podéis ver, tanto en las direcciones de clase A, B y C tenemos un rango de direccionamiento IP privado que podemos utilizar en nuestro hogar o empresa sin problemas, pero siempre de manera local. Este direccionamiento IP privado no es enrutable a través de Internet. También existen otras direcciones IP reservadas, como la 0.0.0.0 para indicar que es una ruta predeterminada, las direcciones IP de loopback que son las 127.0.0.0/8 o las direcciones IP de APIPA que son del rango 169.254.0.0/16.

El rango válido del primer octeto en el caso de la clase A es de 1 a 126; el de la clase B es de 128 a 191 y el de clase C de 192 a 223.

A la hora de calcular subredes, debemos tener en cuenta qué es lo que queremos calcular: ¿cuántas subredes caben dentro de una red más grande? ¿calcular la subred en función del número máximo de host a introducir dentro de una red? Toda esta información es necesario tenerla en cuenta.

**Clases de redes**

Cuando hablamos de subnetting, debemos saber que este es diferente para los diferentes tipos de redes que nos podemos encontrar. Puesto que el proceso no es el mismo. Estas son las siguientes:

* Redes de clase A: Se trata de redes muy grandes, como pueden ser las de una compañía a nivel internacional. Esta clase la formaría un primer octeto de 1 a 126, ya que los demás octetos se usarían para identificar a cada anfitrión. Lo que quiere decir, que hay 126 redes de clase A, las cuales pueden contener un gran número de posibles anfitriones. Las redes de clase A, totalizan la mitad de las direcciones que hay disponibles actualmente. En estas el valor del bit del primer octeto es siempre 0.
* Redes de clase B: Se utilizan para redes de tamaño mediano, como por ejemplo un campus de una universidad. En este caso están formadas por un primer octeto de 128 a 192. Los demás octetos se utilizan para los anfitriones correspondientes. Estas redes de clase B, totalizan un cuarto de todas las direcciones IP disponibles, con un valor del primer bit de 1, y un segundo bit de 0 en el primer octeto.
* Redes de clase C: En este caso ya estamos ante redes para pequeños o medianos negocios. Tienen un primer octeto que va desde 192 hasta 223 e incluyen segundos y terceros octetos como una parte del identificador neto. Estas cubren un octavo de las direcciones IP totales. El valor de si primer bit es de 1, igual que el segundo, y un tercer bit con valor de 0, de nuevo en el primer octeto.
* Redes de clase D: Están dedicadas a los multicast, y es levemente diferente a las tres primeras. El valor de los tres primeros bits es de 1 respectivamente, y un cuarto que tiene un valor de 0. Los otros 28 bits se utilizan para identificar a los dispositivos que pertenecen a la red.
* Redes de clase E. Es el tipo de red que está destinada a realizar experimentos. Al igual que las de clase D, esta se diferencia de las demás con el valor de sus bits, con valores de 1 para los cuatro.

Cuando hablamos de redes multicast, nos referimos a las entregas de datos de forma simultánea a un determinado grupo de nodos receptores, los cuales son el destino. En cambio las unicast, solamente un emisor se comunica con un único receptor de destino

**Subnetting masivo**

Uno de los ejemplos más claros del subnetting masivo, se encuentra en los proveedores de servicios (ISP). Estos adquieren grandes bloques de direcciones IP de los Registros de Internet Regionales (RIR), y proceden a dividirlos en subredes más pequeñas para poder distribuir a sus clientes posteriormente. Cada uno de los clientes recibe una subred con un rango de direcciones IP suficiente para cubrir sus necesidades. Esto da la oportunidad al ISP de poder maximizar el uso de las direcciones IP que han adquirido, y evitar así la escasez de las mismas.

Los centros de datos y grandes corporaciones, también hacen uso del subnetting a nivel masivo, ya que necesitan gestionar redes muy grandes. Cada uno de los departamentos o unidad de empresa, puede llegar a tener su propia subred. Facilitando así la asignación de direcciones IP. Esto también ayuda a mejorar la seguridad, y a reducir la cantidad de tráfico de red que no es deseado. En los centros de datos, cada uno de los racks de servidores puede disponer de su propia subred. De forma que simplifican la gestión de la misma, y probablemente mejorando el rendimiento de forma significativa.

Sin lugar a dudas, el subnetting a nivel masivo ayuda a mejorar la escalabilidad de las redes. Cuando es necesario añadir un nuevo departamento en una empresa, por ejemplo, se puede realizar la asignación de una dirección IP a una nueva subred. Y todo ello sin la necesidad de cambiar la configuración de la red. Por lo cual se facilita mucho el proceso de expansión y crecimiento del sistema. Por otro lado, es capaz de proporcionarnos nuevas capas de seguridad. Si una de las subredes se llega a ver comprometida, el daño puede aislarse a esa subred en específico. Lo cual ayuda a proteger la red principal de un problema mucho más importante. En todo caso, esto es especialmente útil en el sector empresarial, donde la seguridad es un factor crítico.

**Calcular máximo número de subredes dentro de una red más grande**

En este ejemplo vamos a calcular cuántas subredes caben dentro de una red más grande. Imaginemos que queremos **meter un total de 40 redes en la red 192.168.1.0/24**, ¿qué máscara de subred deben utilizar los diferentes hosts? ¿qué rango de IP tenemos disponible de cara a los hosts? ¿cuál sería la dirección IP de red y la dirección IP de broadcast? Lo primero que debemos saber es que, para poder hacer este ejercicio, es totalmente necesario reservar un total de 2 bits de cara a los hosts, por tanto, en una red de clase A con máscara /8 tendremos disponibles un total de 22 bits, en una red de clase B con máscara /16 tendremos disponibles un total de 14 bits, y en una red de clase C con máscara /24 tendremos disponibles un total de 6 bits.

Los pasos para realizar el cálculo es el siguiente:

1. Pasar a binario las 40 redes: Lo primero que tenemos que hacer es pasar el 40 a binario, que es 101000, esto significa que tenemos un total de 6 bits para posteriormente calcular la máscara de subred final.
2. La máscara de subred predeterminada es /24 o 255.255.255.0, si esta máscara la pasamos a binario tenemos: 11111111.11111111.11111111.00000000.
3. Reservamos los 6 bits calculados (40 redes) de izquierda a derecha, empezando por el primer 0 que aparezca, por tanto, estaremos trabajando en el cuarto octeto.
4. La máscara de subred nueva quedaría de la siguiente forma: 11111111.11111111.11111111.11111100; por tanto, estamos ante una máscara de subred /30 o 255.255.255.252. Si la última parte de la máscara (11111100) la pasamos a decimal nos da el número de 252.

Con esta información, para calcular las diferentes subredes que podemos crear dentro de la red 192.168.1.0/24, tenemos que hacer 2 elevado al número de ceros de la máscara de subred que hemos calculado, si nos fijamos, tenemos que la parte final de la máscara es «11111100», tenemos dos ceros, por tanto, 2^2 que es igual a 4. Este 4 es el incremento que debemos usar para calcular las diferentes direcciones de red de las diferentes subredes.

El rango de direccionamiento IP de las subredes calculadas serían las siguientes, lógicamente en todas ellas se usará la máscara de subred /30 o 255.255.255.252 que hemos calculado.

* 192.168.1.0 – 192.168.1.3; la primera dirección IP es la dirección de red, y la última es la dirección de broadcast. Las direcciones 192.168.1.1 y 192.168.1.2 que están «en el medio» son de cara a los hosts.
* 192.168.1.4 – 192.168.1.7
* 192.168.1.8 – 192.168.1.11
* 192.168.1.12 – 192.168.1.15
* ….
* 192.168.1.**252** – 192.168.1.255

La última dirección de red, en su último octeto, siempre se corresponde con la máscara de subred calculada en este ejemplo (255.255.255.**252**)

**Calcular subredes en función del máximo número de hosts por subred**

En este ejemplo vamos a calcular cuántos hosts caben dentro de una subred que está dentro de una red más grande. En una red 192.168.1.0/24 caben un total de 254 hosts como hemos visto antes, aunque hay 256 direcciones, la primera dirección es la de red y la última la de broadcast, por tanto, no se pueden usar de cara a los hosts.

Imaginemos que queremos **meter un total de 40 hosts en una subred, tomando como base la red superior 192.168.1.0/24**, ¿qué máscara de subred deben utilizar los diferentes hosts? ¿qué rango de IP tenemos disponible de cara a los hosts? ¿cuál sería la dirección IP de red y la dirección IP de broadcast? Lo primero que debemos saber es que, para poder hacer este ejercicio, siempre van a «sobrar» direcciones IP de los hosts, en este caso, no solamente van a caber 40 hosts en cada subred, sino un total de (2^8)-2.

Los pasos para realizar el cálculo son muy similar al anterior, pero con un **cambio muy importante en el paso número tres**.

1. Pasar a binario los 40 hosts: Lo primero que tenemos que hacer es pasar el 40 a binario, que es 101000, esto significa que tenemos un total de 6 bits para posteriormente calcular la máscara de subred final.
2. La máscara de subred predeterminada es /24 o 255.255.255.0, si esta máscara la pasamos a binario tenemos: 11111111.11111111.11111111.00000000.
3. Reservamos los 6 bits calculados (40 hosts) de derecha a izquierda poniendo ceros, y lo completaremos con 1 hasta la izquierda del todo.
4. La máscara de subred nueva quedaría de la siguiente forma: 11111111.11111111.11111111.**11000000**; por tanto, estamos ante una máscara de subred /26 (tenemos un total de 26 unos) o 255.255.255.192. Si la última parte de la máscara (11000000) la pasamos a decimal nos da el número de 192.

Con esta información, para calcular las diferentes subredes que podemos crear dentro de la red 192.168.1.0/24, tenemos que hacer 2 elevado al número de ceros de la máscara de subred que hemos calculado, si nos fijamos, tenemos que la parte final de la máscara es «11000000», tenemos seis ceros, por tanto, 2^6 que es igual a 64. Este 64 es el incremento que debemos usar para calcular las diferentes direcciones de red de las diferentes subredes.

El rango de direccionamiento IP de las subredes calculadas serían las siguientes, lógicamente en todas ellas se usará la máscara de subred /26 o 255.255.255.192 que hemos calculado.

* 192.168.1.0 – 192.168.1.63; la primera dirección IP es la dirección de red, y la última es la dirección de broadcast. Las direcciones IP que están «en el medio» son de cara a los hosts.
* 192.168.1.64 – 192.168.1.127
* 192.168.1.128 – 192.168.1.191
* 192.168.1.192 – 192.168.1.255

Si queremos meter 40 hosts por red, tan solo podremos crear un total de cuatro subredes dentro de la red 192.168.1.0/24 tal y como hemos visto.

**Beneficios que podemos encontrar**

El subnetting nos puede ayudar a dividir series de redes, que pueden facilitar mucho el trabajo al administrador de las mismas. Si se usa de una forma eficiente, puede tener beneficios en la propia red, como por ejemplo hacer que el envío y recepción de datos, se realice de forma más rápida. Esto ocurre porque el subnetting permite ampliar o reducir el rango de direcciones IP, lo que en sí, es una depuración de la red para que sean más claras. También trae beneficios a nivel de congestión, pues permite contener el tráfico de broadcast lo que favorece la velocidad y optimización.

Esto, lo podemos ejemplificar fácilmente, si un paquete para enviar información, es difundido a todos los dispositivos que están conectados a esa red, solo existirá un punto de entrada para dicho paquete y además si dicho paquete, por ejemplo, contiene spam, es más que probable que todos los dispositivos de dicha red reciban ese spam y puede provocar un colapso agotando la capacidad de la red.

Sin embargo, al realizar la división de esa red, en distintas subredes, nos permite asegurarnos de que la información que es enviada, se divida a su vez entre las distintas subredes. Esto lo que nos garantiza es que, las otras subredes maximicen su velocidad y eficacia y al mismo tiempo nos garantiza el control del flujo del tráfico que pasa por ellas.

Otra función que resulta interesante, es que al dividir las redes, estas se pueden destinar a otros fines específicos, permitiendo que el redireccionamiento sea más controlable, a la vez que ordena la red de una forma eficiente. Esto también aumentará los niveles de seguridad, al poder contener las difusiones innecesarias. Estas pueden ralentizar el funcionamiento de la red. Siempre que hagamos una división en subredes, es muy recomendable hacer uso de VLANs a nivel L2 o capa de enlace, de esta manera, vamos a poder crear diferentes VLANs en los switches gestionables de toda la red, para separar las subredes de forma correcta y proporcionar la mejor seguridad posible. El router también debe ser capaz de «entender» el protocolo 802.1Q, de lo contrario, las VLANs no podrán comunicarse unas con otras, algo que es totalmente necesario en ciertos escenarios, por lo que debes tenerlo muy en cuenta.

Siguiendo con el apartado de la seguridad, otro punto a tener en cuenta es que dividir la red en distintas subredes aumenta precisamente en gran medida la seguridad de la misma, de distintas formas, empezando por que puede controlarse el flujo utilizando por ejemplo QoS o mapas de enrutamiento que nos permiten al mismo tiempo identificar las diferentes amenazas y cerrarle los puntos de entrada.

También podemos realizar uso de distintos routers para dividir nuestra red y realizar configuración de ACL entre dichos routers y los switches y como resultado de esto, todos los dispositivos que pertenezcan a esa subred, no serán capaces de acceder a la totalidad de dicha red y esto minimiza el riesgo de que se propaguen amenazas si algún dispositivo se ve comprometido.

Las subredes también nos dan versatilidad al momento de controlar el crecimiento de nuestra red, ya que al momento de planificar y diseñar su tamaño es algo que siempre debe tenerse en cuenta y las subredes son ideales para ello y es por eso que cada vez son más implementadas en más sitios.

**Cómo influye en el rendimiento de la red**

Como puedes ver, el subnetting es una técnica utilizada para poder dividir las redes en apartados más pequeños. Esto es algo que tiene una gran influencia en el rendimiento de la misma, ya que principalmente ayuda a reducir de forma considerable la cantidad de tráfico, mejorando así la eficiencia de la comunicación de todos los dispositivos que componen la red. Una de sus principales ventajas, es precisamente este, la reducción del tamaño de las redes. Cuando una red es demasiado grande, el tráfico broadcast aumenta y afecta al rendimiento de la misma. Una vez la dividimos, se reduce ese tráfico de broadcast, ayudando al rendimiento.

Por otro lado, a la hora de administrar la red, también nos veremos muy influenciados. Con estas divisiones, se pueden asignar las direcciones IP de una forma mucho más eficiente. Y tendremos la posibilidad de tener todos los equipos bajo control, reduciendo así el tiempo que es necesario para solucionar algunos problemas que se pueden dar. Por lo cual, de nuevo estamos ante un factor que no solo influye en el rendimiento, sino en la operatividad de la propia red.

Pero lo cierto es que el rendimiento, también es algo que va ligado con la seguridad de las comunicaciones. Establecer algunos límites mediante reglas de firewall, o de acceso entre las diferentes subredes, ayuda a optimizar la red mucho más. Sin olvidarnos de que tendremos más capas de seguridad contra posibles ataques. En todo caso, todo debe ser realizado de la forma correcta, ya que, de lo contrario, se pueden originar más problemas que soluciones.

Por lo cual, esta técnica tiene una gran influencia en el rendimiento de la red. Lo cual es algo que a muchas empresas les interesa, de forma que pueden obtener beneficios en otros sectores como el rendimiento del trabajo, la eficacia, o el sector económico. Formando así on conjunto en el que se debe prestar atención en el momento que empezamos a instalar redes, y equipos.

**Calculadoras de subnetting**

Si realizar todo este proceso te resulta un poco engorroso, siempre puedes optar por utilizar una calculadora de subnetting. Estas se pueden encontrar en internet de forma gratuita, dejando las opciones de pago para versiones de las mismas orientadas más al sector profesional.

* **Advanced Subnet Calculator:** Está desarrollada por SolarWinds, la cual es una de las mejores empresas dedicadas a la administración de redes. En este caso, su aplicación para cálculos de subnetting también es de las más avanzadas. Se ejecuta en Windows y nos permite ahorrar mucho tiempo cuando tratamos de buscar direcciones disponibles. Cuenta con calculadora IP, creador de subred y una calculadora CIDR. Entre otras opciones, nos permite hacer listados de direcciones y resoluciones de DNS.
* **Tech-FAQ:** De nuevo nos encontramos ante una aplicación gratuita, la cual se divide en tres pestañas. Una en la que tendremos la calculadora de red en formato clásico. una dedicada al direccionamiento y la división de subredes. Y la última, donde tendremos una calculadora de máscara de wildcard. Juntas hacen de estas herramienta una de las que más opciones facilitan al usuario.
* **Subnet Ninja:** Se trata de una herramienta muy sencilla, la cual al contrario de las anteriores, no requiere instalación, ya que está basada en web. Esto hace que se pueda usar en cualquier dispositivo, desde ordenadores a teléfonos móviles. Es muy intuitiva y sencilla de utilizar.
* **Spiceworks:** Otra aplicación basada en web. De nuevo estamos ante un servicio sencillo, con pocas opciones, pero eso es lo que hace que sea tan accesible. Su especialidad está en la división de subredes.
* **SubnetCalc:** Esta se ejecuta en Mac OS, y nos permite realizar todos los cálculos de subred que se puedan necesitar, lo cual hace de ella una de las más completas junto con las primeras de la lista. Como con todo lo que podemos instalar en los sistemas operativos de Apple, cuenta con una interfaz muy agradable.

**Subnetting variable**

Las máscaras de subred variables (VLSM), son otra estrategia a la hora de diseñar y planificar una red. Se trata de una zona segmentada que forma parte de una gran red, en donde las máscaras de subred pueden tener tamaños diferentes. A esto se le llama división de subredes en subredes. Lo cual permite utilizar máscaras para diferentes subredes, de una sola red que puede ser de clase A, B o C. Con esto el espacio asignado a las direcciones IP se puede dividir en una jerarquía, la cual bien definida puede tener diferentes tamaños. A su vez, esto nos ayuda a mejorar la usabilidad de las diferentes subredes, las cuales pueden incluir tamaños variables.

**Fundamentos de VLSM**

* **Máscara de subred:** Se encarga de dividir las direcciones IP en direcciones de host y de red. Lo cual ayuda a la definición sobre la zona de la IP de donde partimos, y la que pertenece a los dispositivos.
* **División de subredes:** Es la razón por la cual una gran red, puede abordar la congestión de la red. Lo cual nos ayuda a gestionar el impacto negativo que siempre tiene esta en la congestión de la red, ayudando a tener una mayor velocidad y mejor productividad. También se mejora la eficiencia, debido a la forma en la que se utiliza el espacio de direcciones en redes pequeñas. Pero no son los únicos beneficios, si no que con esto es posible realizar una mejor gestión en el control de acceso. Mejorando la seguridad de la red.
* **Supernetting:** Se trata de la creación de superredes. Lo cual, en sí, son varias redes contiguas que se combinan en una sola red más grande. Este es muy útil en la agregación de rutas, de forma que se puede reducir el tamaño de las tablas de enrutamiento. Y también permite que se reduzca el tamaño de las actualizaciones necesarias en el enrutamiento.

**Aprender subnetting**

El subnetting en redes, es un apartado que puede ser bastante complejo en algunos casos. Pero también es cierto que una vez implementado con la configuración y administración adecuadas, es una herramienta muy valiosa para todos los que trabajan en el campo de las tecnologías. En todo caso, hay algunos consejos que podemos seguir para aprender a hacerlo. Estos son:

* **Entender conceptos de dirección IP:** Antes de comenzar a adentrarnos en el mundo del subnetting, es muy importante estar familiarizado con las direcciones IP. Disponer de una **comprensión básica de lo que ofrecen, y cómo funcionan.**
* **Familiarizarse con el formato:** No todas las direcciones IP son iguales. Estas se componen de cuatro números separados por puntos, y cada uno de ellos tiene una razón de ser. Se comprenden entre el 0 y el 255, por lo cual las direcciones posibles son muchas.
* **Comprender las diferentes IPs:** En el mundo de la tecnología, nos podemos encontrar con varios tipos de dirección IP. Se dividen por clases como son A, B y C, y cuentan con rangos de direcciones disponibles diferentes, así como una diferencia en el número de bots que se utilizan para las direcciones que componen la red.
* **Conocer las máscaras:** Las máscaras de subred se utilizan para establecer una definición de la cantidad de bits, los cuales se van a utilizar para las direcciones de red. También se componen de 4 números, al igual que las direcciones IP.
* **Cálculo broadcast:** Una vez disponemos de los conocimientos básicos de las direcciones IP, las clases y sus máscaras, podremos empezar a calcular direcciones de red y broadcast. Los cuales se utilizarían para redes determinadas.
* **Practicar ejercicios:** No hay mejor manera de aprender sobre estos temas que practicar. En Internet nos podemos encontrar con muchos sitios web diferentes, y con muchas herramientas disponibles. Los cuales nos van a ayudar a generar todo tipo de ejercicios con sus respectivos problemas, para ponernos en todas las situaciones que sean posibles durante la formación.
* **Implementación:** Pasar la idea del papel al mundo real, es otra de las mejores prácticas que podemos llevar a cabo. Esto nos permitirá ver que todo funciona de la forma adecuada, pero en todo caso, lo mejor siempre será tratar de hacerlo en entornos controlados para no causar algún tipo de problema.

**Salidas profesionales**

Si bien el subnetting no es una habilidad que de por sí tenga salidas profesionales, es un gran complemento si nos queremos dedicar al mundo de las redes. Muchos puestos relacionados con estas instalaciones, pueden ser mucho más accesibles si no controlamos el subnetting a la perfección. Siendo una actividad que puede ser compleja, no puede traer grandes beneficios a nivel profesional. Podremos aplicar nuestros conocimientos de diferentes formas y en diferentes puestos.

Como administradores de redes, el subnetting juega un papel fundamental. Esto nos permitirá crear diseños de las redes, y ver si van a ser eficientes. Esto nos da algunas ventajas a la hora de realizar las instalaciones y a la vez mantener la infraestructura totalmente escalable y optimizada. Lo cual es importante para asegurar la distribución de una forma adecuada de todas las direcciones IP, para que el tráfico no tenga problemas.

En las ingenierías también puede jugar un papel fundamental. Muchas empresas contratan profesionales de alto nivel para encargarse de la implementación y el mantenimiento de sus redes. Con habilidades en subnetting, podemos diseñar toda la infraestructura de la red, a un alto nivel de complejidad. Lo cual nos puede asegurar que la segmentación sea la más adecuada, sobre todo cuando es posible que incluso sea necesaria una red de gran tamaño.

En las consultorías también pueden hacer falta profesionales con habilidades en subnetting. Muchas empresas suelen acudir a estos servicios de consultoría para asesorarse en la planificación, implementación y optimización de las redes que disponen. Esto implica todos los aspectos, desde los lógicos a los recursos de hardware. Por lo cual disponer de esos conocimientos nos va a ayudar sin ninguna duda.

Esperamos que este tutorial os haya servido para calcular vuestras subredes en función del número de redes y del número de hosts que queramos meter dentro de una subred. Has podido ver los pasos necesarios para llevar a cabo, así como los diferentes tipos de direcciones IPv4 y sus clases. Como hemos explicado, es una opción útil para poder manejar mejor una gran red, mejorar la organización y también lograr que funcione de forma más óptima. Por ejemplo, en una empresa que quiera crear una subred de gestión, administración, ventas, etc. Es una posibilidad a tener en cuenta.