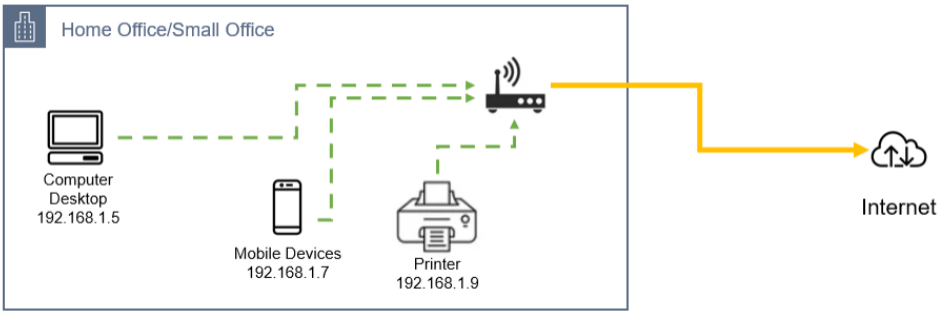
Redes para la nube

Las redes son un componente fundamental de cualquier infraestructura de IT, ya sea en las instalaciones o en la nube. Sin redes, no habría sido posible diseñar el complejo mundo de las comunicaciones en el que vivimos hoy. En ausencia de redes, no habría internet en el mundo moderno. Casi todas las empresas de hoy necesitan tener algún tipo de conectividad de red para colaborar con socios y clientes finales. En estas notas, analizamos algunos de los componentes básicos del diseño de una red.

Introducción a las redes locales

Casi todas las empresas tendrán algún tipo de red local. Incluso si trabajas por cuenta propia, es probable que tengas una oficina en casa que también cuenta con un entorno de red privada. Tu oficina en casa puede parecerse al siguiente diagrama:



En el diagrama anterior, los dispositivos de la red doméstica se comunican entre sí a través de la conexión Wi-Fi. Si envías una solicitud de impresión desde el escritorio de la computadora a la impresora, tu documento se imprimirá.
Esta comunicación es posible a través de la conectividad establecida a través de la red Wi-Fi. Para que los dispositivos se comuniquen entre sí, cada uno requiere una dirección IP única. Si el elemento de direccionamiento IP está correctamente definido, cada dispositivo en la red podrá ver al otro. El servicio Wi-Fi también conecta los dispositivos a Internet a través de un router/módem que establece una conexión con un proveedor de servicios de Internet. Esta conexión generalmente se realiza a través de algún tipo de cableado físico o conectividad de red celular a través de su proveedor de telecomunicaciones.

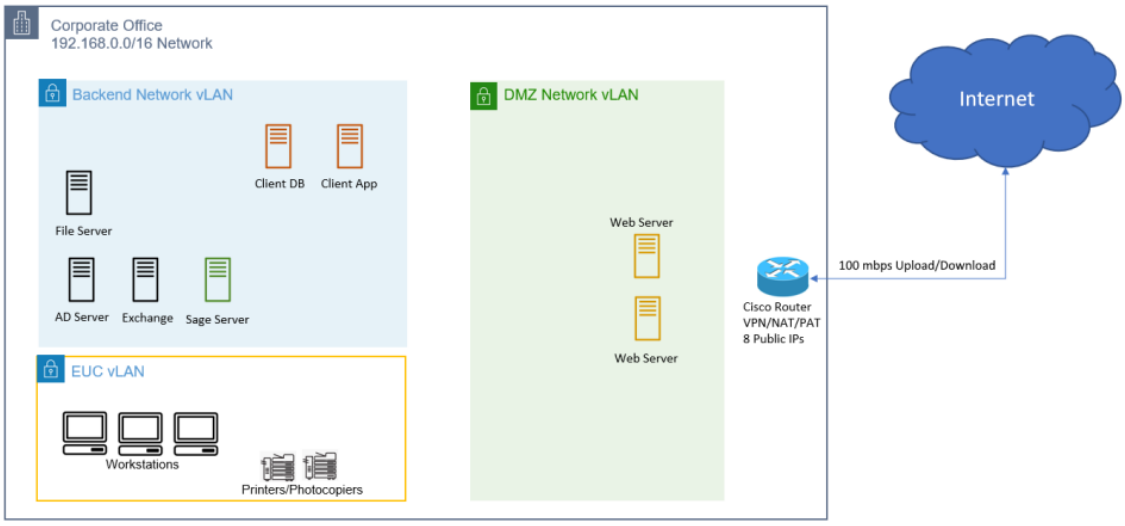
Redes corporativas básicas

Las redes corporativas requieren una planificación más cuidadosa ya que muchas de ellas también permitirán el acceso a aplicaciones desde fuera de la red. Por ejemplo, tu empresa puede publicar un sitio web desde la red corporativa para mostrar sus productos y servicios a clientes potenciales en Internet. El uso de routers de firewall que permiten que solo tipos específicos de tráfico ingresen a la red desde Internet y se dirijan al servidor apropiado es parte de la planificación segura para la conectividad con el mundo exterior.

Una red corporativa generalmente se dividiría en varias redes más pequeñas, cada una de las cuales se usaría para un propósito específico. En su nivel más básico, una red corporativa consistiría en dos subredes: una para propósitos internos de back-end y otra para ubicar servicios a los que se puede acceder desde Internet.

En el siguiente diagrama, una red corporativa se ha dividido en dos redes separadas: una denominada red interna y otra denominada zona desmilitarizada (DMZ). La DMZ es un área donde se

implementan servicios que pueden estar expuestos en Internet, por ejemplo, un servidor web. El tráfico a los servicios implementados en esta zona está restringido con estrictas reglas de entrada para garantizar altos niveles de seguridad.



Como se muestra en el diagrama anterior, la red corporativa se divide en tres subredes separadas. Esto asegura que podamos configurar reglas que definan el tipo de tráfico que puedes ingresar a cada subred y de qué fuente. Por ejemplo, podríamos configurar reglas de entrada desde Internet para otorgar acceso a nuestros servidores web a través del tráfico HTTP/HTTPS. Esto permitirá a los miembros del público acceder a nuestro sitio web corporativo y revisar nuestras ofertas de servicios.

Por otro lado, no esperaríamos permitir el tráfico entrante directo desde Internet al End User Computing (EUC) Virtual LAN (VLAN), ya que no existe ningún requisito para dicha conexión entrante y garantiza que nuestra red corporativa sea segura. Sin embargo, se permitiría el tráfico desde las estaciones de trabajo a Internet para permitir que los miembros del personal accedan a servicios y herramientas en línea. De manera similar, cuando creamos soluciones en AWS, necesitamos configurar redes virtuales en la nube que nos permitan alojar nuestras aplicaciones de una manera que ofrezca seguridad, aislamiento y acceso entrante solo donde sea necesario.

Fundamentos del direccionamiento IP y CIDR

Para que los dispositivos de su red se comuniquen entre sí, se requiere una dirección de Protocolo de Internet (dirección IP). Cada dispositivo de red, ya sea una computadora, computadora portátil, teléfono móvil, impresora o router de red, deberá tener asignada una dirección IP que sea enrutable en cada red. Además, la dirección IP de cada dispositivo debe ser única: no puedes tener más de un dispositivo con la misma dirección IP. Así es como funcionan los teléfonos. Cada teléfono tiene asignado un número único. Para llamar a alguien por teléfono, primero debes saber su número de teléfono y luego, marcar ese número, lo que da como resultado que su llamada se conecte. En la primera figura, habrás notado que cada uno de los dispositivos internos de la red doméstica tenía una dirección IP.

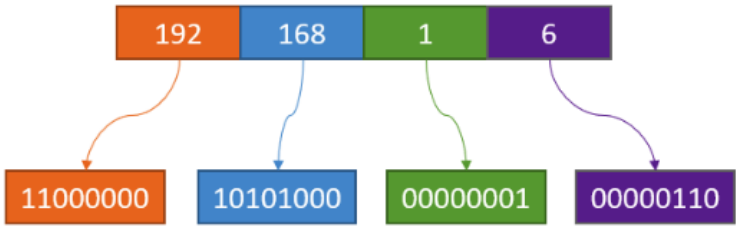
Hay dos tipos de dirección IP: IPv4 e IPv6.

Dirección IP versión 4 – IPv4

IPv4 fue la primera versión del sistema de direccionamiento IP que se implementó ampliamente y que finalmente formó la columna vertebral de Internet. El formato de dirección IPv4 estándar con el que está familiarizado y como se muestra en los diagramas anteriores sigue la estructura de cuatro números decimales separados por puntos. Un ejemplo de esto es 192.168.1.6. Cada notación decimal en una dirección IP se denomina **octeto** y puede ser cualquier número entre 0 y 255, base 10 (decimal). Como probablemente sepas, las computadoras usan números binarios en lugar de números decimales. Cada número decimal, cuando se convierte en binario, consta de 8 bits, unos y ceros. En ambos casos, ya sea decimal o binario, una dirección IPv4 tiene una longitud de 32 bits.

Tomemos un ejemplo de una dirección IP de 192.168.1.6. En binario, cada octeto estaría entre 8 ceros y 8 unos (00000000 a 11111111). Los números decimales individuales en la dirección IP se pueden convertir a su representación binaria equivalente, que comprendería una combinación de unos y ceros en cada octeto de 8 bits.

En el siguiente diagrama, la dirección IP 192.168.1.6 en decimal es la misma que 11000000.10101000.00000001.00000110 en binario:



La conversión de notación decimal a binaria requiere recordar el valor posicional de los bits individuales en cada octeto de 8 bits. También puedes calcular los valores posicionales si no quieres simplemente recordarlos de memoria.
Tomemos el ejemplo del último octeto en la dirección IP 192.168.1.6, que en este caso es el número decimal 6.

En binario, tienes 8 bits de ceros y unos para representar este número decimal. En la siguiente tabla, podemos ver cada uno de esos bits y sus valores posicionales:

X represents a '0' or '1' in binary

	x	x	x	x	x	x	x	x
Place value:	$X*2^7$ or X * 128	$X*2^6$ or X * 64	$X*2^5$ or X * 32	$X*2^4$ or X * 16	$X*2^3$ or X * 8	$X*2^2$ or X * 4	$X*2^1$ or X *2	$X*2^0$ or X * 1

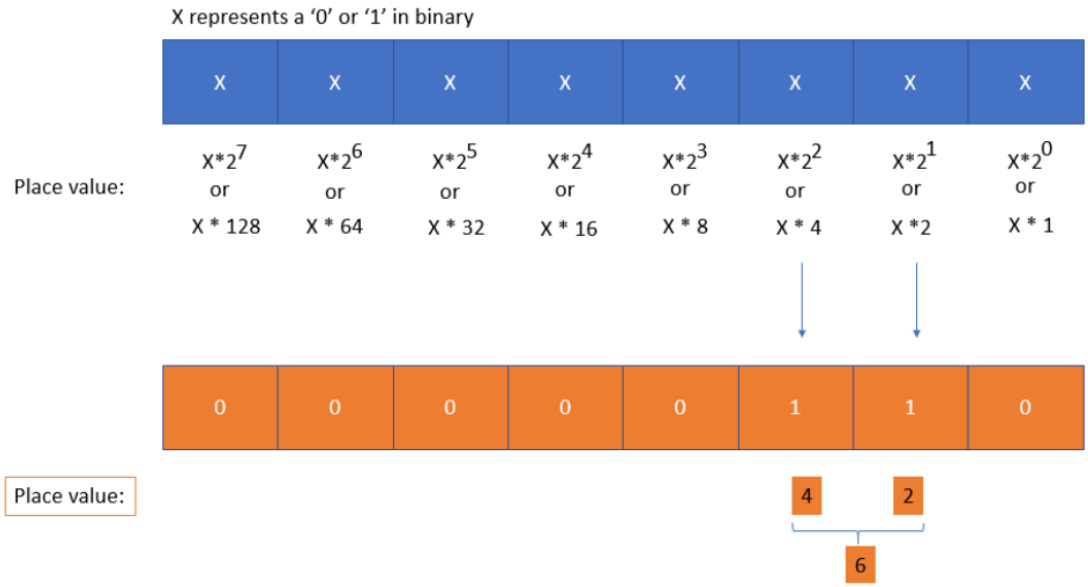
Para cada octeto, de derecha a izquierda, se aplica lo siguiente:

- El primer valor del primer bit siempre es igual a 1. Es 2 elevado a 0 (2^0), es decir, 1.
- El segundo bit es el doble del primero y es igual a 2 (2 elevado a 1, es decir, 2).
- El tercer bit es el doble del segundo bit y es igual a 4 (2 elevado a 2, es decir, 4).
- El cuarto bit es el doble del tercero y es igual a 8 (2 elevado a 3, es decir, 8) y así sucesivamente.

El cálculo del valor decimal de una representación binaria se realiza de la siguiente manera:

Decimales = (X*128) + (X*64) + (X*32) + (X*16) + (X*8) + (X*4) + (X*2) + (X*1)

A continuación, para convertir el número decimal 6 de la dirección IP 192.168.1.6 en binario, es necesario identificar cuáles de las "X" deben convertirse en ceros y cuáles en unos. Deseas convertir la cantidad mínima de bits a unos para obtener su representación decimal y, además, debes continuar convirtiendo solo esos bits a aquellos cuyo valor sea menor que su número decimal. Entonces, por ejemplo, como se muestra en la figura, tenemos lo siguiente:



- No convertirías el bit en el extremo izquierdo a 1 porque 128 es mayor que el último octeto, 6 en nuestra dirección IP. De manera similar, no convertiría el siguiente bit del extremo izquierdo a 1 en binario porque 64 también es mayor que el último octeto, y así sucesivamente.
- Convertirías el tercer bit desde el extremo derecho a 1 porque su valor de marcador de posición es igual a 4, que es menor que 6 en nuestra dirección IP.
- También convertirías el segundo bit desde el extremo derecho a 1 porque su valor de marcador de posición es igual a 2, que también es menor que 6 en nuestra dirección IP.
- Recuerda que desea convertir la menor cantidad de bits a unos para obtener su representación decimal. Entonces, en este caso, 4 más 2 es igual al último octeto, 6 en nuestra dirección IP. Como tal, no deberíamos convertir el último bit en 1, ya que el total sumaría 7, que es más de 6.

Por lo tanto, la representación binaria de 6 es 00000110. De manera similar, convertir la dirección IP 192.168.1.6 a binaria le daría 11000000.10101000.00000001.00000110.

Limitaciones de las direcciones IPv4

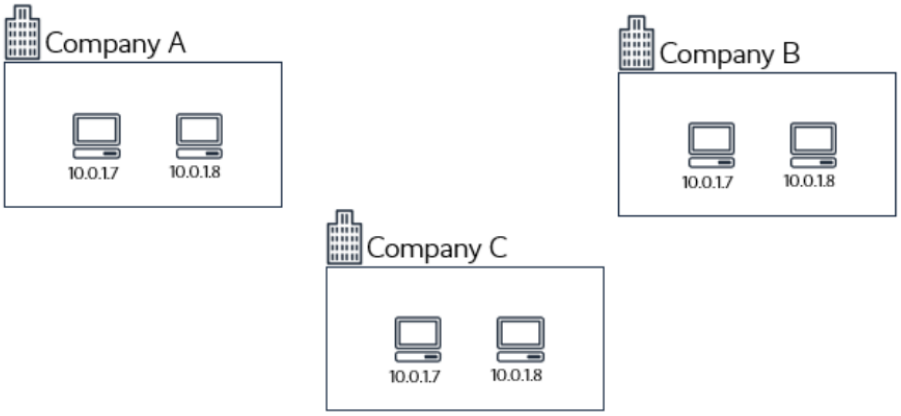
Una de las principales limitaciones de una dirección IPv4 es que solo tiene 32 bits de longitud. Esto significa que la cantidad máxima de direcciones que puede tener en un esquema de direccionamiento IPv4 es 2^32, que es 4,294,967,294 direcciones en total. Cuatro mil millones de direcciones pueden parecer una gran cantidad, pero el hecho es que hemos agotado este rango simplemente debido a la gran cantidad de dispositivos que ahora necesitan una dirección IP para participar en una red determinada.

Dado que los cuatro mil millones de direcciones no son suficientes para manejar los enormes volúmenes de dispositivos, la Autoridad de Números Asignados de Internet (IANA)[1] ideó un plan brillante para asignar un rango de direcciones IP solo para uso privado. Estos rangos de direcciones no son enrutables en Internet, lo que significa que las empresas (y los hogares) pueden configurar sus redes privadas internas utilizando estas direcciones sin posibilidad de que entren en conflicto con las redes de otras empresas, especialmente si esas empresas no planean conectar sus redes. juntos.

Los siguientes rangos de direcciones IP están diseñados para uso privado:

- 10.0.0.0/8 Direcciones IP: 10.0.0.0 – 10.255.255.255
- 172.16.0.0/12 Direcciones IP: 172.16.0.0 – 172.31.255.255
- 192.168.0.0/16 Direcciones IP: 192.168.0.0 – 192.168.255.255

Las direcciones restantes se consideran públicas y, por lo tanto, se pueden enrutar en Internet global. Para ilustrar cómo esto ayuda, veamos el siguiente diagrama:



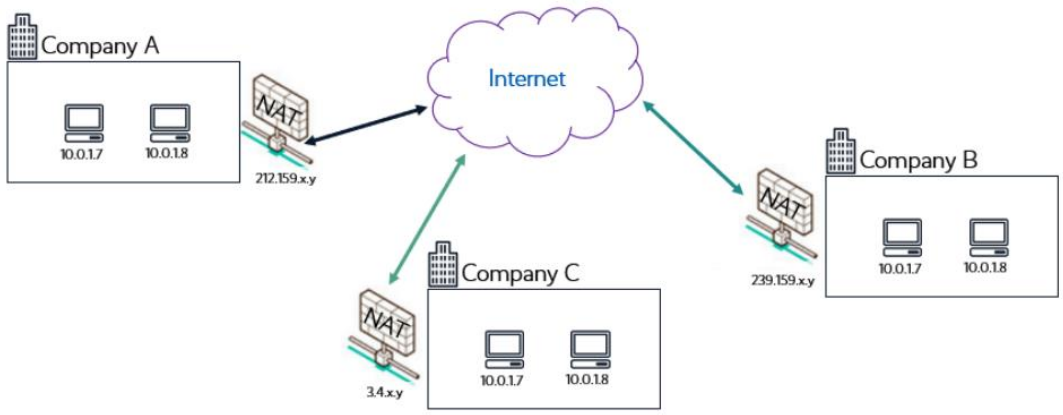
En el diagrama anterior las tres empresas pueden usar las mismas direcciones IP para sus dispositivos internos. Dado que estas empresas no están conectadas entre sí, no hay posibilidad de conflicto de direcciones IP. Las direcciones IP privadas, como las designadas por la IANA, han ayudado a las empresas a crear redes internas sin necesidad de adquirir ninguna de las direcciones públicas. El espacio de direcciones IP privadas también mejora la seguridad de la red interna porque estas direcciones no se pueden enrutar en Internet. También podemos permitir que más dispositivos se conecten en red, ya que los rangos de direcciones se pueden repetir entre empresas que no necesitan estar conectadas entre sí a través de la misma red.

Las empresas necesitan acceso a Internet

En la ilustración anterior, vemos que las empresas pueden definir rangos de direcciones IP de red interna que no se pueden enrutar a través de Internet. Estas empresas seguirán necesitando acceso a Internet, ya sea para enviar y recibir correos electrónicos de sus clientes o para alojar aplicaciones de comercio electrónico a las que sus clientes necesiten acceder desde Internet. Para facilitar la conectividad a Internet, se requieren direcciones IP públicas. Sin embargo, tener que asignar a cada dispositivo en Internet una dirección IP pública anularía el propósito de los rangos de IP privados y representaría un riesgo de seguridad. En cambio, la red interna se puede configurar para acceder a Internet a través de un servicio llamado Traducción de direcciones de red (NAT).

[1] Internet Assigned Numbers Authority

En el siguiente diagrama, podemos ver que las empresas ahora pueden acceder a Internet a través de un servicio NAT configurado en su router externo.



El servicio NAT requiere como mínimo una sola dirección IP pública y transmite las solicitudes de los dispositivos internos a Internet, actuando como un proxy en el medio. El servicio NAT también gestiona las respuestas a esas solicitudes, lo que garantiza que se redirigen correctamente al dispositivo interno que realizó la solicitud original. Dada la limitación de IPv4, IPv6 fue desarrollado por el Grupo de trabajo de ingeniería de Internet (IETF) [2]en la década de 1990. A continuación, echamos un vistazo a IPv6 y analizamos cómo supera la limitación de direcciones de 32 bits de IPv4.

¿Qué pasa con IPv6?

Para abordar las limitaciones de IPv4, el IETF desarrolló IPv6. IPv6 usa una dirección de 128 bits, lo que nos daría 2^128 direcciones. IPv6 también se indica en formato hexadecimal en lugar del formato decimal estándar. Con IPv6, técnicamente, cada dispositivo podría tener su propia dirección IP pública.
De hecho, Amazon Web Services (AWS) ofrece IPv6 como una opción para configurar redes en la nube. Incluso si necesitas proteger los dispositivos de la Internet pública, aún puedes usar una dirección IPv6 para un servidor virtual en la nube y permitir que envíe tráfico a través de Internet mediante una puerta de enlace de Internet de solo salida.

Sin embargo, muchas empresas continúan usando IPv4, en parte debido a las capacidades de los servicios NAT y en parte para garantizar la interoperabilidad con dispositivos heredados que pueden no ser compatibles con IPv6.

Clases y tamaños de red

Originalmente, el IETF diseñó diferentes clases de direcciones IPv4 para ayudar a definir diferentes tamaños de red y casos de uso. Las clases A a C representan direcciones IP unicast genéricas (con algunas excepciones) que los miembros del público pueden usar para construir redes de diferentes tamaños. La clase D comprende direcciones de multicast y la clase E se ha reservado para uso experimental.

La forma en que estas clases ayudan a definir los tamaños de red es dividiendo la dirección IP en una parte de red y una parte de host. Veamos esto individualmente por clase:

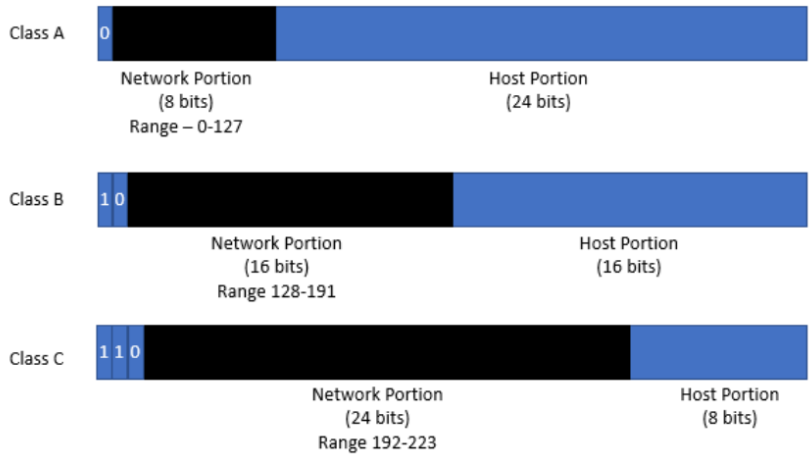
- Clase A: los primeros 8 bits de una dirección de clase A definen la parte de la red y los 24 bits restantes se utilizan para indicar la parte del host. Los bits de red se indican con 1 (un

[2] Internet Engineering Task Force (IETF)

uno en binario) y los bits de host se indican con 0 (ceros). Además, el bit más a la izquierda de una dirección de clase A se establece en 0.

- Clase B: los primeros 16 bits de una dirección de clase B definen la parte de la red y los 16 bits restantes se utilizan para indicar la parte del host. En una red de clase B, los dos bits del extremo izquierdo se establecen en 10.
- Clase C: los primeros 24 bits de una dirección de clase C definen la parte de la red y los 8 bits restantes se utilizan para indicar la parte del host. Además, en una red de clase C, los dos bits del extremo izquierdo se establecen en 11.

Para ilustrar mejor cómo se ven realmente estas tres clases de redes, veamos el siguiente diagrama:



En el diagrama anterior, puedes identificar a qué clase pertenece una dirección IP en particular e identificar instantáneamente la cantidad potencial de direcciones IP de host que tendría ese bloque de IP. Entonces, por ejemplo si tomamos la dirección IP 192.168.1.6, podemos confirmar que es una dirección de clase C.

Lo que esto significa es que la parte de red de la dirección IP es 192.168.1.x. En este ejemplo, x puede ser cualquier número entre 1 y 254. Eso te da un total de 254 direcciones IP en la parte de host del bloque de IP. Aunque el número total de direcciones IP que puede tener en cualquier octeto es 256 (2^8, lo que equivale a 256), es importante recordar que la primera y la última dirección IP no se pueden utilizar. La primera dirección IP siempre se conoce como ID de red, que en este caso es 192.168.1.0. Aquí, el último octeto estaría representado solo por ceros (o, en binario, 00000000). La última dirección IP es 192.168.1.255, que se conoce como la dirección broadcast.

Aquí, el último octeto estaría representado por todos unos (o, en binario, 11111111). Una fórmula simple para calcular la cantidad de direcciones IP utilizables en un bloque de IP es la siguiente:

Número de direcciones IP utilizables = 2^Número de bits de host - 2

En el ejemplo anterior, tenemos una dirección IP de 192.168.1.6, que pertenece a un bloque de IP que solo puede contener 254 direcciones IP utilizables.

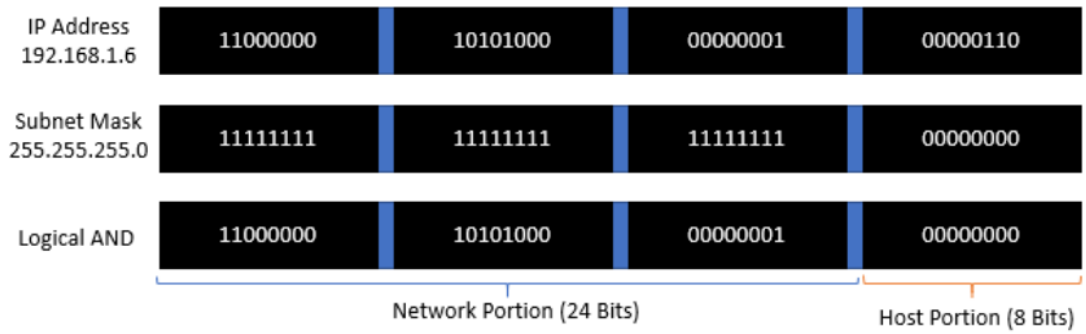
¿Qué son las máscaras de subred?

Las máscaras de subred te permiten dividir un bloque de direcciones IP en una parte de red y una parte de host. Los dispositivos anfitriones (host) en la misma parte de la red pueden comunicarse fácilmente entre sí y necesitarán algún tipo de enrutamiento para comunicarse con los anfitriones en otras redes. En la red de clase C anterior, los primeros tres octetos pertenecen a la parte de la red y solo el último octeto (los últimos 8 bits) pertenece a la parte del host.

Una subred es un número de 32 bits que se crea configurando los bits del host en todos ceros y configurando los bits de red en todos los unos. Luego se realiza una operación AND lógica con un bloque de dirección IP correspondiente para definir la cantidad de direcciones IP de host que pueden estar disponibles en cada bloque.

Entonces, por ejemplo, podemos verificar que la dirección IP 192.168.1.6 pertenece a una dirección de clase C porque una clase C enmascara los primeros tres octetos (primeros 24 bits en binario) como la parte de red y deja el último octeto (últimos 8 bits) para los bits de host.

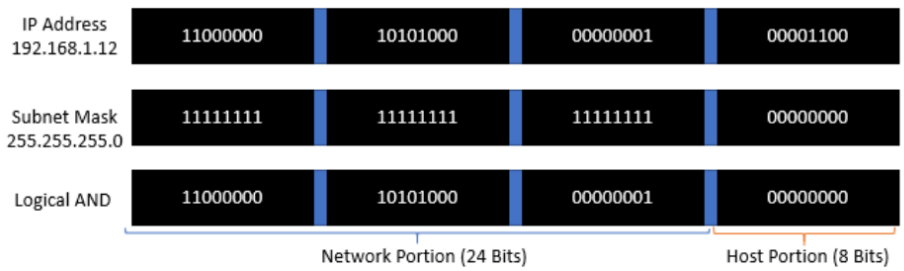
En binario, la dirección IP 192.168.1.6 y su máscara de subred asociada se representan de la siguiente manera:



Según el resultado de la operación lógica AND anterior, notarás que si alguno de los primeros tres octetos de la dirección IP cambiara, por ejemplo, si en lugar de 192 usáramos 193, eso produciría un resultado diferente para el correspondiente bloque de operación lógico AND. Dado que los primeros tres octetos representan la parte de red de una dirección IP, el cambio resultante denotaría efectivamente una red diferente.

Además, debido a que la parte del host en la máscara de subred está configurada en ceros y solo está representada por el último octeto (últimos 8 bits), cualquier variación en este octeto mantendrá la dirección IP dentro de la misma red.

Por ejemplo, veamos la dirección IP 192.168.1.12. Representar esto en el siguiente diagrama mientras se realiza una operación AND con la máscara de subred produciría lo siguiente:



Lo que notarás de los dos diagramas anteriores es que la operación lógica AND produce el mismo patrón de números binarios, lo que indica lo siguiente:

- Ambas direcciones IP pertenecen a la misma red.
- La parte de red en ambos casos es la misma, derivada de la máscara de subred de 255.255.255.0 (o 11111111 11111111 11111111 00000000).

Ahora que sabemos cómo se utilizan las máscaras de subred para enmascarar partes de una dirección IP como parte de la red y parte del host, examinemos el concepto de división en subredes[3].

¿Qué es la división en subredes?

En la discusión anterior sobre las máscaras de subred, definimos tres clases de redes. Las redes se derivan mediante el uso de máscaras de subred con longitudes fijas para crear estas clases. Entonces, por ejemplo, en una red de clase A, el primer octeto de un bloque de IP representa la parte de la red y los tres octetos restantes la parte del host.

Esto es posible gracias al uso de lo que llamamos máscaras de subred. Específicamente, usamos una máscara de subred de 255.0.0.0 para separar el primer octeto de la parte de la red. Cualquier cambio en el primer octeto de una dirección IP con una máscara de subred de 255.0.0.0 generaría una red diferente. Por ejemplo, 10.0.0.0 está en una red diferente a 31.0.0.0.

La división en subredes es el proceso mediante el cual se puede crear subredes dentro de una red más grande. En cada red, es posible crear partes más pequeñas y aisladas de la red, como una parte para hospedar todos los servidores backend y otra para hospedar servidores web frontend. La división en subredes nos permite dividir una red grande en estas subredes más pequeñas. El proceso de creación de subredes implica tomar prestados bits adicionales de la parte del host de un rango de direcciones IP. Estos bits prestados se utilizan para crear subredes más pequeñas dentro de una red principal más grande.

Por ejemplo, si tenemos un requisito comercial para ocho subredes, cada una con capacidad para albergar 30 direcciones IP para 30 dispositivos, entonces, al usar una dirección estándar de clase C, podríamos usar los siguientes bloques de IP:

- Red 1: 192.168.1.0 (máscara de subred: 255.255.255.0)
- Red 2: 192.168.2.0 (máscara de subred: 255.255.255.0)
- Red 3: 192.168.3.0 (máscara de subred: 255.255.255.0)
- Red 4: 192.168.4.0 (máscara de subred: 255.255.255.0)
- Red 5: 192.168.5.0 (máscara de subred: 255.255.255.0)
- Red 6: 192.168.6.0 (máscara de subred: 255.255.255.0)
- Red 7: 192.168.7.0 (máscara de subred: 255.255.255.0)
- Red 8: 192.168.8.0 (máscara de subred: 255.255.255.0)

Si bien este diseño de red funciona perfectamente, tenemos mucho desperdicio en términos de la cantidad de direcciones IP disponibles en comparación con la cantidad de direcciones IP requeridas. Cada una de estas ocho redes contiene 254 direcciones IP utilizables, pero solo necesitamos 30 direcciones por red según el requisito.

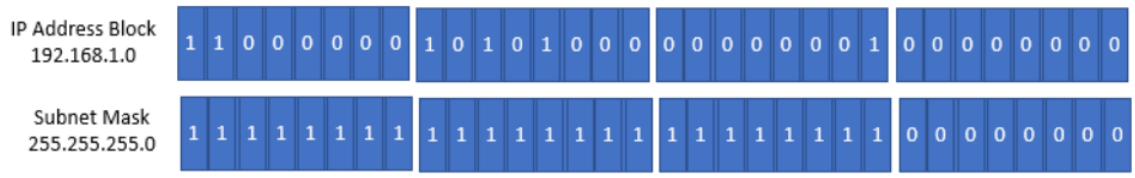
Cuando se usan rangos de direcciones IP privadas, esto puede no importar tanto, pero cuando consideramos aplicar el mismo enfoque al rango limitado de direcciones IP públicas, se vuelve imposible de lograr. Además, ten en cuenta que, por lo general, debes pagar por las direcciones IP públicas.

En lugar de este enfoque, podemos usar el subnetting y máscaras de subred para dividir una sola red en redes más pequeñas, conservando y utilizando de manera eficiente el espacio de direcciones IP disponible dentro de una red determinada. Entonces, por ejemplo, podemos tomar la red de clase C de 192.168.1.0 con una máscara de subred de 255.255.255.0 y dividirla en subredes más

[3] subnetting

pequeñas. Para hacer esto, tomamos prestados bits adicionales de la parte del host del bloque de direcciones IP para representar nuestras subredes en la red.

Echemos un vistazo al siguiente diagrama para ilustrar este concepto:



En una red de clase C estándar, el bloque de direcciones IP anterior de 192.168.1.0 con una máscara de subred de 255.255.255.0 produciría una sola red con 254 direcciones IP. Esto se debe a que hemos usado los primeros tres octetos (24 bits) para representar la parte de la red y el último octeto (8 bits) para representar la parte del host. Debido a que tenemos 8 bits para representar bits de host, podemos usar la fórmula 2^8, que es igual a 256. Sin embargo, recuerda que la primera y la última dirección IP no se pueden utilizar, por lo que es 256-2, lo que nos da 254 direcciones IP utilizables.

Ahora, si tomamos prestados los primeros 3 bits de la parte del host del bloque de direcciones IP para construir subredes, tendremos la siguiente representación:

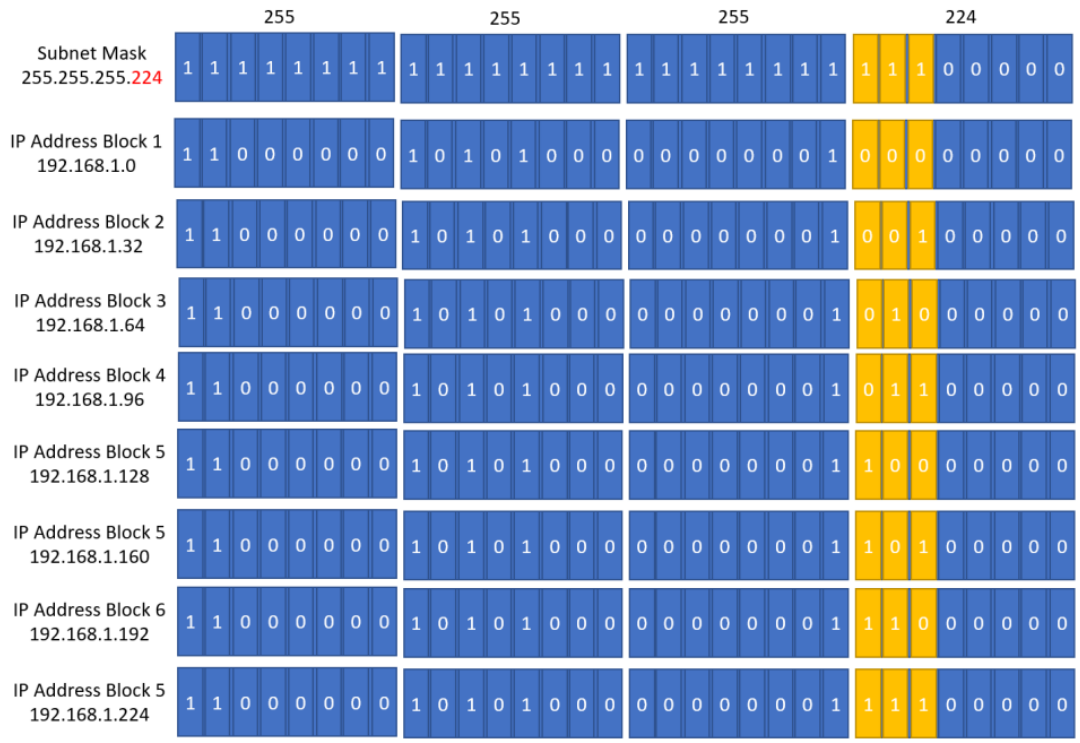
Tomando prestados 3 bits del extremo izquierdo del cuarto octeto (la parte del host), podemos crear efectivamente ocho redes de subred. Esto se obtiene mediante la siguiente fórmula:

Número de subredes = 2^número de bits de host prestados

En este caso, 2^3 = 8 y así, esto nos da 8 subredes. Además, debido a que ahora solo nos quedan 5 bits para representar la parte del host, podemos calcular la cantidad de direcciones IP que tenemos por subred. La fórmula es: Número de hosts = 2^Número de bits de host restantes. En este caso, son 2^5 (porque quedan 5 bits de host) = 32 direcciones IP. Además, como se mencionó anteriormente, la primera y la última dirección IP no se pueden usar y, como resultado, restamos 2 de la cantidad de direcciones IP (32-2), lo que nos da nuestras 30 direcciones IP.

Si observamos la representación de la máscara de subred de los 3 bits prestados, tendremos una nueva máscara de subred de la siguiente manera:

Usando una máscara de subred de 255.255.255.224, podemos ver que tenemos ocho subredes individuales que se pueden crear.

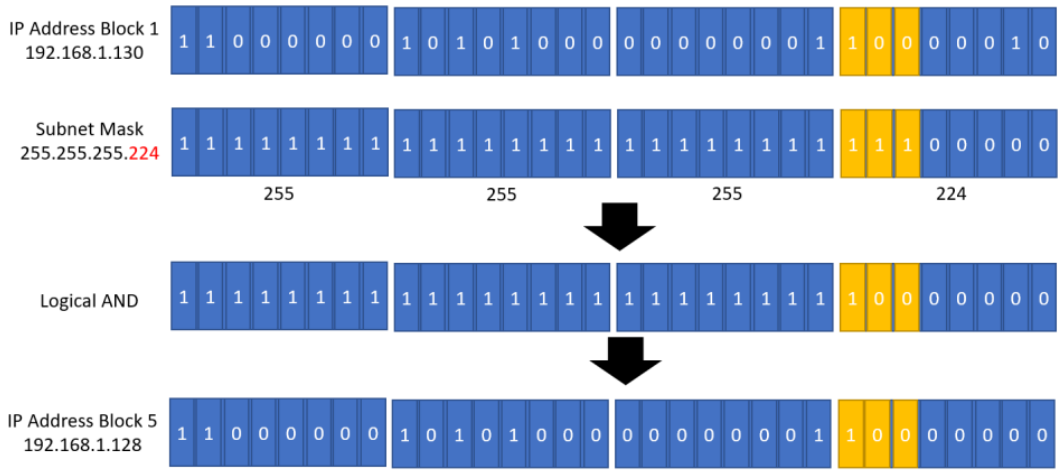


Notaremos la diferencia de patrón en los bloques de IP que se muestran en binario. Específicamente, la diferente combinación de unos y ceros en los bits prestados define las ocho redes diferentes. Los siguientes bloques de direcciones IP son las ocho subredes que se pueden crear tomando prestados 3 bits de la parte del host del bloque de direcciones IP 192.168.1.0. Cada subred tiene 30 direcciones IP utilizables. Las ocho redes son las siguientes:

- 192.168.1.0 (192.168.1.0 a 192.168.1.31)
- 192.168.1.32 (192.168.1.32 a 192.168.1.63)
- 192.168.1.64 (192.168.1.64 a 192.168.1.95)
- 192.168.1.96 (192.168.1.96 a 192.168.1.127)
- 192.168.1.128 (192.168.1.128 a 192.168.1.159)
- 192.168.1.160 (192.168.1.160 a 192.168.1.191)
- 192.168.1.192 (192.168.1.192 a 192.168.1.223)
- 192.168.1.224 (192.168.1.224 a 192.168.1.255)

Usando el enmascaramiento de subred, puedes identificar a qué red pertenece un bloque de direcciones IP en particular. Entonces, por ejemplo, la dirección IP 192.168.1.130 pertenecería al bloque de IP 192.168.1.128 con una máscara de subred de 255.255.255.224. Esto queda más claro cuando miramos la representación binaria y realizamos la operación lógica AND, como se muestra en el siguiente diagrama.

Puedes ver que los resultados de la operación AND lógica coinciden con el bloque de dirección IP 5:



Esta representación binaria y la operación AND lógica muestran cómo el bloque de direcciones IP 5 cae en la misma red que el bloque de direcciones IP 1, como se muestra en las celdas amarillas.

Enrutamiento entre dominios sin clases (CIDR) [4]

En lugar de usar máscaras de subred y la complejidad discutida anteriormente, podemos usar CIDR. Con CIDR, puedes crear redes de diferentes tamaños, como la forma en que usas la máscaras de subred. CIDR es esencialmente otra forma de representar máscaras de subred, pero ofrece más flexibilidad. El tamaño de tu red determinará cuántas direcciones IP puedes tener en esa red. También puedes dividir tu red en varias redes más pequeñas (subredes) configurando subconjuntos específicos del bloque de IP mediante bloques CIDR.

Al definir una red, los bloques CIDR se muestran como parte del bloque de direcciones IP con una barra inclinada (/) seguida de un número decimal entre /8 y /32. Por ejemplo, la dirección IP 192.168.1.6 podría pertenecer a una red 192.168.1.0/24. Veamos cómo funciona esto.

En una red con un bloque CIDR de /24, podemos calcular la cantidad de direcciones IP que la red puede alojar y, por lo tanto, la cantidad de dispositivos que se pueden colocar en la red. Dado que la cantidad total de bits en un rango de IPv4 es 32, entonces para un CIDR /24, simplemente restamos 24 de 32, lo que nos da 8 bits. Estos 8 bits representan el número total de direcciones IP que podemos tener en esa red. Específicamente, 2^8 es igual a 256. Entonces, el número total de direcciones IP en la red 192.168.1.0/24 es 256 direcciones IP. Recuerda que en cualquier red dada, la primera y la última dirección IP no se pueden utilizar. Entonces, el número total de direcciones IP utilizables es 256 - 2, lo que equivale a 254.

Un punto importante a tener en cuenta aquí es que la red IP con un bloque CIDR de 192.168.1.0/24 es una sola red y dentro de esta red, puedes alojar hasta 254 dispositivos, cada uno de los cuales necesitaría una dirección IP. El rango de direcciones IP sería de 192.168.1.1 a 192.168.1.254 (recuerda que la primera IP 192.168.1.0 y la última IP 192.168.1.255 no son utilizables).

Veamos otro ejemplo.

Usaremos el rango de IP de 10.0.0.0 a 10.0.255.255, que es un rango privado para la red interna. Supongamos que eliges una IP de red con un bloque CIDR de 10.0.0.0/16. En esta red, tu bloque CIDR es un /16. En esta red puedes tener un total de 65.536 direcciones IP. Recuerda que para calcular la cantidad de direcciones IP, debes restar el valor de 32 de la notación de bloque CIDR, en

[4] Classless Interdomain Routing

este caso, 16. Esto le da 16 bits que pueden usar los dispositivos en su red. Dos elevado a 16 (2^16) es igual a 65.536 direcciones IP. Recuerde restar otros 2 del número total de direcciones IP, lo que le da un número total de 65 534 direcciones IP utilizables. Esta es una red muy grande y es posible que desees dividir esta red más grande en subredes más pequeñas (subredes) para el aislamiento y la separación de recursos. Con el mismo bloque de IP de red, puedes crear subredes aumentando el valor del bloque CIDR. Por ejemplo, en la red principal de 10.0.0.0/16, puedes crear varias subredes utilizando el bloque CIDR de /20. Esto significa que te quedan 12 bits para la parte de hosts de tu bloque de dirección IP (32 bits – 20 bits para la red).

Entonces, dentro de la red 10.0.0.0/16, puedes tener subredes con el bloque de IP de 10.0.0.0/20. Cada subred tendría un total de 4096 direcciones IP (quedan 2^12 bits de host) o 4094 direcciones IP utilizables (restando las 2 IP que no se pueden usar).