

UD5

Direccionamiento de la red: IPv4

0. Introducción

El direccionamiento es una función clave de los protocolos de capa de red que permite la comunicación de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente.

Este capítulo examina detalladamente la estructura de las direcciones IPv4 y su aplicación en la construcción y prueba de redes y subredes IP.

1. Estructura de una dirección IPv4

Cada dispositivo de una red debe definirse en forma exclusiva. En la capa de red, es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Ejemplo de estructura IPv4 ([Plataforma cisco 6.1.1](#))

192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

La computadora que utiliza esta dirección IP se encuentra en la red 192.168.10.0.

2. Tipos de direcciones en una red IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

Dirección de red: la dirección en la que se hace referencia a la red.

Dirección de broadcast: una dirección especial que se utiliza para enviar datos a todos los hosts de la red.

Direcciones host: las direcciones asignadas a los dispositivos finales de la red.

Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la red de la figura como "red 10.0.0.0". Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red". Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red.

Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

Dirección de broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se la conoce como broadcast dirigido.

Direcciones host

Como se describe anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.

Tipos de direcciones			
Red			Host
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

Prefijos de red

Una pregunta importante es: ¿Cómo es posible saber cuántos bits representan la porción de red y cuántos bits representan la porción de host? Al expresar una dirección de red IPv4, se agrega una longitud de prefijo a la dirección de red. La longitud de prefijo es la cantidad de bits en la dirección que conforma la porción de red. Por ejemplo: en 172.16.4.0 /24, /24 es la longitud de prefijo e

indica que los primeros 24 bits son la dirección de red. Esto deja a los 8 bits restantes, el último octeto, como la porción de host.

No siempre se asigna un prefijo /24 a las redes. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes para las diferentes duraciones de prefijos. En esta figura puede ver también que la cantidad de host que puede ser direccionada a la red también cambia.

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red	Rango de host	Dirección de broadcast
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED
PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE
BROADCAST PARA CADA
PREFIJO

2.2. Calculo de direcciones host, red y broadcast

Hasta ahora, el usuario podría preguntarse: ¿Cómo se calculan estas direcciones? Este proceso de cálculo requiere que el usuario considere estas direcciones como binarias.

Para comenzar a comprender este proceso de determinar asignaciones de dirección, se desglosarán algunos ejemplos en datos binarios.

Observe la figura para obtener un ejemplo de la asignación de dirección para la red 172.16.20.0 /25.

En el primer cuadro, se encuentra la representación de la dirección de red. Con un prefijo de 25 bits, los últimos 7 bits son bits de host. Para representar la

dirección de red, todos estos bits de host son "0". Esto hace que el último octeto de la dirección sea 0. De esta forma, la dirección de red es 172.16.20.0/25.

En el segundo cuadro, se observa el cálculo de la dirección host más baja. Ésta es siempre un número mayor que la dirección de red. En este caso, el último de los siete bits de host se convierte en "1". Con el bit más bajo en la dirección host establecido en 1, la dirección host más baja es 172.16.20.1.

El tercer cuadro muestra el cálculo de la dirección de broadcast de la red. Por lo tanto, los siete bits de host utilizados en esta red son todos "1". A partir del cálculo, se obtiene 127 en el último octeto. Esto produce una dirección de broadcast de 172.16.20.127.

El cuarto cuadro representa el cálculo de la dirección host más alta. La dirección host más alta de una red es siempre un número menor que la dirección de broadcast. Esto significa que el bit más bajo del host es un '0' y todos los otros bits '1'. Como se observa, esto hace que la dirección host más alta de la red sea 172.16.20.126.

A pesar de que para este ejemplo se ampliaron todos los octetos, sólo es necesario examinar el contenido del octeto dividido.

Dirección de red	Primera dirección host
172 . 16. 20. 0/25 10101100.00010000.00010100.00000000 -----Red ----- host - 0+0+0+0+0+0+0+0=0 Dirección de red = 172.16.20.0	172 . 16. 20. 1 10101100.00010000.00010100.00000001 -----Red ----- host - 0+0+0+0+0+0+0+1=1 Dirección host más baja = 172.16.20.1
Paso 1	
Paso 2	

Dirección de broadcast	Última dirección host
172 . 16. 20. 127 10101100.00010000.00010100.01111111 -----Red ----- host - 0+64+32+16+8+4+2+1=127 Dirección de broadcast = 172.16.20.127	172 . 16. 20. 126 10101100.00010000.00010100.01111110 -----Red ----- host - 0+64+32+16+8+4+2+0=126 Dirección host más alta = 172.16.20.126
Paso 3	
Paso 4	

Actividad 1

2.3. Tipos de comunicación: Unicast, Broadcast y Multicast

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

Unicast: el proceso por el cual se envía un paquete de un host a un host individual.

Broadcast: Enviar los datos a todos los destinos posibles (un "broadcast a todos los hosts") permite al emisor enviar los datos una única vez a todos los receptores. En el [protocolo IP](#), la dirección **255.255.255.255** representa un broadcast limitado localmente. También se puede hacer un broadcast directo (y limitado) combinando el prefijo de red con el sufijo de hosts compuesto únicamente de 1 binarios. Por ejemplo para una red con el prefijo 192.0.2 la dirección IP a usar será la 192.0.2.255 (asumiendo que la máscara de red es la 255.255.255.0).

Multicast: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts. Una dirección multicast está asociada con un grupo de receptores interesados. Las direcciones desde la **224.0.0.0 a la 239.255.255.255** están destinadas para ser direcciones de multicast. Este rango se llama formalmente "Clase D".

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

Tráfico unicast

La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast **usan direcciones especiales como la dirección de destino**. Al utilizar estas direcciones especiales, **los broadcasts**

están generalmente restringidos a la red local. El ámbito del tráfico multicast también puede estar limitado a la red local o enrutado a través de una internet.



Ejemplo de transmisión unicast (**Plataforma CISCO. 6.2.3**)

Transmisión de broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast.

La transmisión de broadcast se usa para ubicar servicios o dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe proporcionar información a todos los hosts de la red.

Algunos ejemplos para utilizar una transmisión de broadcast son:

-  Solicitar una dirección
-  Intercambiar información de enrutamiento por medio de protocolos de enrutamiento

Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta. Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast.





De forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente se restringen a la red local. Esta restricción depende de la configuración del router que bordea la red y del tipo de broadcast. Existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado.

Transmisión de multicast

La transmisión de multicast está diseñada para conservar el ancho de banda de la red IPv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino.

Algunos ejemplos de transmisión de multicast son:

-  Distribución de audio y video
-  Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
-  Distribución de software
-  Suministro de noticias

2.4. Rangos de direcciones IPv4 reservadas

Expresado en formato de decimal , el rango de direcciones IPv4 es de 0.0.0.0 a 255.255.255.255. No todas estas direcciones pueden usarse como direcciones host para la comunicación unicast.

Direcciones experimentales

Un importante bloque de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 experimentales de 240.0.0.0 a 255.255.255.254. Actualmente, estas direcciones se mencionan como reservadas para uso futuro . Esto sugiere que podrían convertirse en direcciones utilizables. En la actualidad, no es posible utilizarlas en redes IPv4. Sin embargo, estas direcciones podrían utilizarse con fines de investigación o experimentación.

Direcciones multicast

Como se mostró antes, otro bloque importante de direcciones reservado con objetivos específicos es el **rango de direcciones multicast IPv4 de 224.0.0.0 a 239.255.255.255**.

Las direcciones IPv4 multicast de 224.0.0.0 a 239.255.255.255 son direcciones de enlace local reservadas. Estas direcciones se utilizarán con grupos multicast en una red local. Los paquetes enviados a estos destinos siempre se transmiten con un valor de período de vida (TTL) de 1. Por lo tanto, un router conectado a la red local nunca debería enviarlos.

Las direcciones agrupadas globalmente son de 240.0.0.0 a 255.255.255.255. Se les puede usar para transmitir datos en Internet mediante multicast. Por ejemplo, 224.0.0.1 ha sido reservada para el Protocolo de hora de red (NTP) para sincronizar los relojes con la hora del día de los dispositivos de la red.

Direcciones host

Después de explicar los rangos reservados para las direcciones experimentales y las direcciones multicast, queda el rango de direcciones de 0.0.0.0 a 223.255.255.255 que podría usarse con hosts IPv4. Sin embargo, dentro de este rango existen muchas direcciones que ya están reservadas con objetivos específicos.

2.5. Direcciones públicas y privadas

Aunque la mayoría de las direcciones host IPv4 son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. Estas direcciones se denominan direcciones privadas.

Direcciones privadas

Los bloques de direcciones privadas son:

🚦 de 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)

✚ de 172.16.0.0 a 172.31.255.255 (172.16.0.0 /16)

✚ de 192.168.0.0 a 192.168.255.255 (192.168.0.0 /24)

Los bloques de direcciones del espacio privado, como se muestra en la figura, se reservan para uso en redes privadas.

Muchos hosts en distintas redes pueden utilizar las mismas direcciones de espacio privado.

Traducción de direcciones de red (NAT)

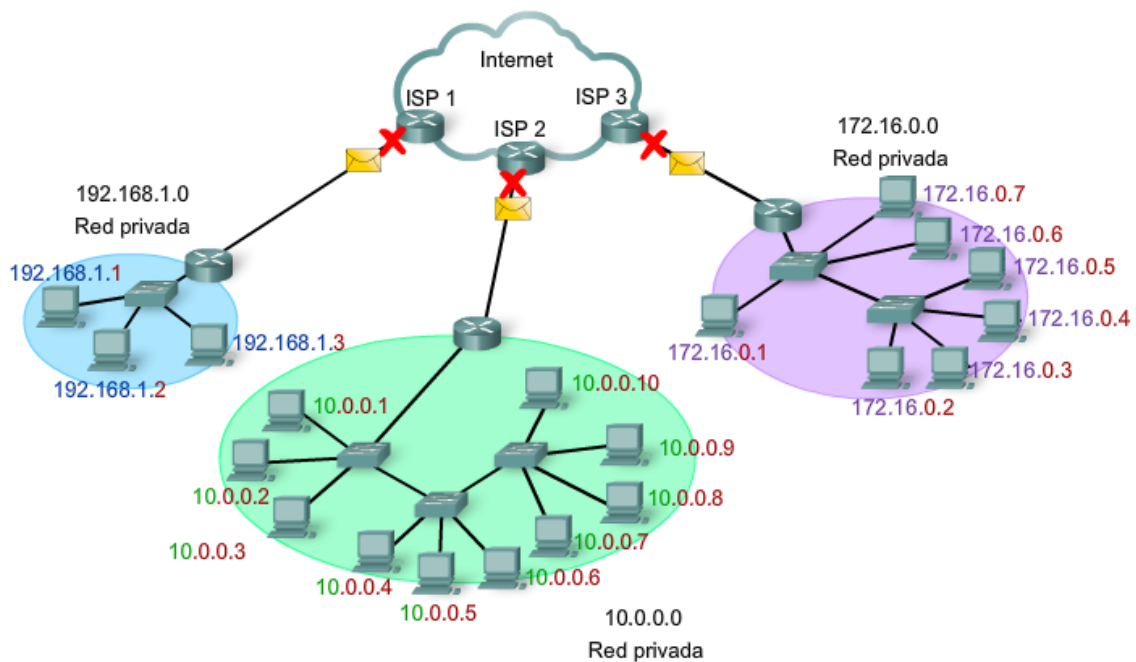
Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada.

La NAT permite a los hosts de la red "pedir prestada" una dirección pública para comunicarse con redes externas.

Direcciones públicas

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aún dentro de estos bloques de direcciones, existen muchas direcciones designadas para otros fines específicos.

Direcciones privadas utilizadas en redes sin NAT



2.6. Direcciones IPv4 especiales

Hay determinadas direcciones que no pueden asignarse a los hosts por varios motivos. También hay direcciones especiales que pueden asignarse a los hosts pero con restricciones en la interacción de dichos hosts dentro de la red.

Direcciones de red y de broadcast

Como se explicó anteriormente, no es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son, respectivamente, la dirección de red y la dirección de broadcast.

Ruta predeterminada

Como se mostró anteriormente, la ruta predeterminada IPv4 se representa como 0.0.0.0. La ruta predeterminada se usa como ruta "comodín" cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

Loopback

Una de estas direcciones reservadas es la dirección de loopback IPv4 127.0.0.1. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loop back dentro del host local. Las direcciones dentro de este bloque no deben figurar en ninguna red.

2.7. Clases de IPv4

Bloques de clase A

Se diseñó un bloque de direcciones de clase A para admitir redes extremadamente grandes con más de 16 millones de direcciones host. Las direcciones IPv4 de clase A usaban un prefijo /8 fijo, donde el primer octeto indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host.

Para reservar espacio de direcciones para las clases de direcciones restantes, todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que sólo había 128 redes de clase A posibles, de 0.0.0.0 /8 a 127.0.0.0 /8, antes de excluir los bloques de direcciones reservadas.

Bloques de clase B

El espacio de direcciones de clase B fue diseñado para satisfacer las necesidades de las redes de tamaño moderado a grande con más de 65.000

hosts. Una dirección IP de clase B usaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las direcciones host. Al igual que con la clase A, debía reservarse espacio de direcciones para las clases de direcciones restantes.

Con las direcciones de clase B, los dos bits más significativos del octeto de orden superior eran 10. De esta forma, se restringía el bloque de direcciones para la clase B a 128.0.0.0 /16 hasta 191.255.0.0 /16. La clase B tenía una asignación de direcciones un tanto más eficiente que la clase A debido a que dividía equitativamente el 25% del total del espacio total de direcciones IPv4 entre aproximadamente 16.000 redes.

Bloques de clase C

El espacio de direcciones de clase C era la clase de direcciones antiguas más comúnmente disponible. Este espacio de direcciones tenía el propósito de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts.

Los bloques de direcciones de clase C utilizaban el prefijo /24. Esto significaba que una red de clase C usaba sólo el último octeto como direcciones host, con los tres octetos de orden superior para indicar la dirección de red.

Los bloques de direcciones de clase C reservaban espacio de direcciones para la clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringió el bloque de direcciones para la clase C de 192.0.0.0 /24 a 223.255.255.0 /24. A pesar de que ocupaba sólo el 12.5% del total del espacio de direcciones IPv4, podía suministrar direcciones a 2 millones de redes.




Actividad-3

3. Asignación de direcciones

3.1 Planificación del direccionamiento de la red

Es necesario que la asignación del espacio de direcciones de la capa de red dentro de la **red corporativa esté bien diseñada**. Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. Tampoco la asignación de direcciones dentro de la red debe ser aleatoria.

La asignación de estas direcciones dentro de las redes debería ser planificada y documentada a fin de:

-  Evitar duplicación de direcciones
-  Proporcionar y controlar el acceso
-  Controlar seguridad y rendimiento

Evitar duplicación de direcciones

Como se sabe, **cada host en una red local debe tener una dirección única**. Sin la **planificación y documentación** adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

Proporcionar y controlar el acceso

Algunos hosts proporcionan recursos tanto para la red interna como para la red externa. Un ejemplo de estos dispositivos son los servidores. El acceso a estos recursos puede ser controlado por la dirección de la Capa 3. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Por ejemplo, **si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a su dirección y es posible que los clientes no puedan ubicar este recurso**.

Controlar seguridad y rendimiento

De igual manera, es necesario controlar la seguridad y el rendimiento de los hosts de la red y de la red en general. Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red que tiene una dirección problemática.

3.2 Direccionamiento estático o dinámico para dispositivos de usuario final

Asignación dinámica de direcciones

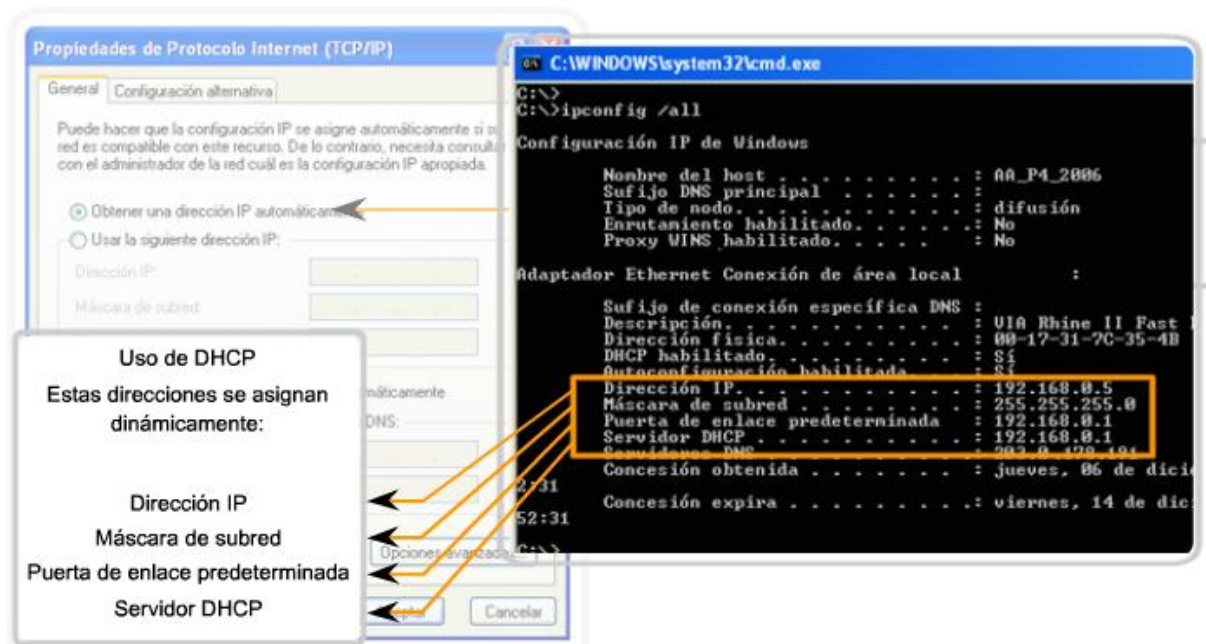
Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones que se asignan en forma dinámica utilizando el protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.

El DHCP permite la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración. La configuración del servidor DHCP requiere definir un bloque de direcciones, para asignarlo a los clientes DHCP en una red.

Generalmente, el DHCP es el método que se prefiere para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para el personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección vuelve a estar disponible para volver a utilizarse.

Asignación de direcciones dinámicas



3.3. Asignación de direcciones a otros dispositivos

Direcciones para servidores y periféricos

Cualquier recurso de red como un servidor o una impresora debe tener una **dirección IPv4 estática**, como se muestra en la figura. Los hosts clientes acceden a estos recursos utilizando las direcciones IPv4 de estos dispositivos. Por lo tanto, son necesarias direcciones predecibles para cada uno de estos servidores y periféricos.

Direcciones para hosts accesibles desde Internet

Al igual que todos los dispositivos en una red que proporciona recursos de red, **las direcciones IPv4 para estos dispositivos deben ser estáticas**.

Las variaciones en la dirección de uno de estos dispositivos hará que no se pueda acceder a éste desde Internet. En muchos casos, estos dispositivos se encuentran en una red numerada mediante direcciones privadas. Esto significa que el router o el firewall del perímetro de la red debe estar configurado para traducir la dirección interna del servidor en una dirección pública.

Direcciones para dispositivos intermediarios

Los dispositivos intermediarios también son un punto de concentración para el tráfico de la red. Casi todo el tráfico dentro redes o entre ellas pasa por alguna forma de dispositivo intermediario. Por lo tanto, estos dispositivos de red ofrecen una ubicación oportuna para la administración, el monitoreo y la seguridad de red.

A la mayoría de los dispositivos intermediarios se le asigna direcciones de **Capa 3**. Ya sea para la administración del dispositivo o para su operación. Los dispositivos como hubs, switches y puntos de acceso inalámbricos no requieren direcciones IPv4 para funcionar como dispositivos intermediarios. Sin embargo, si es necesario acceder a estos dispositivos como hosts para configurar, monitorear o resolver problemas de funcionamiento de la red, éstos deben tener direcciones asignadas.

Debido a que es necesario saber cómo comunicarse con dispositivos intermediarios, éstos **deben tener direcciones predecibles**. Por lo tanto, **típicamente, las direcciones se asignan manualmente**. Además, las direcciones de estos dispositivos deben estar en un rango diferente dentro del bloque de red que las direcciones de dispositivos de usuario.

Routers

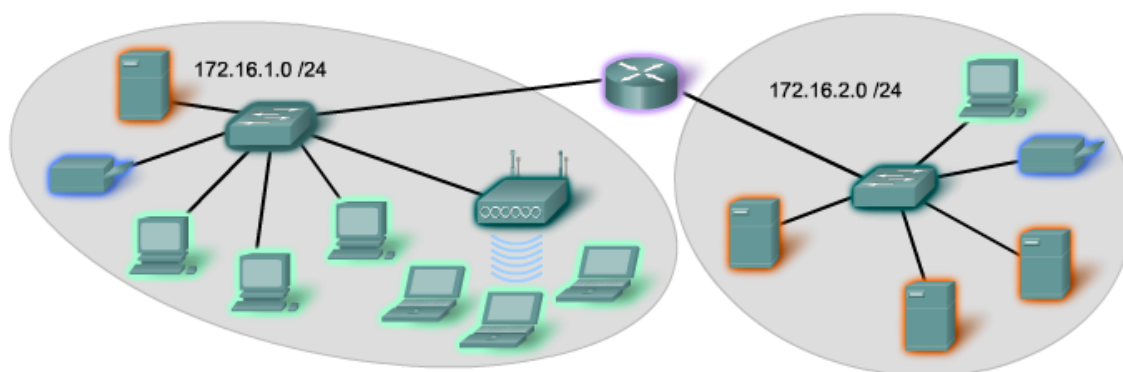
A diferencia de otros dispositivos intermediarios mencionados, se asigna a los dispositivos de router y firewall una dirección IPv4 para cada interfaz. Cada interfaz se encuentra en una red diferente y funciona como gateway para los hosts de esa red. **Normalmente, la interfaz del router utiliza la dirección más baja o más alta de la red**.

Las interfaces de router son el punto de concentración del tráfico que entra y sale de la red. Debido a que los hosts de cada red usan una interfaz de dispositivo router como gateway para salir de la red, existe un flujo abundante de paquetes en estas interfaces. Por lo tanto, estos dispositivos pueden cumplir una función importante en la seguridad de red al filtrar los paquetes según las direcciones IPv4 de origen y destino. Agrupar los diferentes tipos de

dispositivos en grupos de direccionamiento lógico hace que la asignación y el funcionamiento del filtrado de paquetes sea más eficiente.

Rangos de direcciones IP de los dispositivos

Uso	Primera dirección	Última dirección	Dirección de resumen
Dirección de red	172.16.x.0	172.16.x.0 /25
Hosts de usuarios (pool de DHCP)	172.16.x.1	172.16.x.127	
Servidores	172.16.x.128	172.16.x.191	172.16.x.128 /26
Periféricos	172.16.x.192	172.16.x.223	172.16.x.128 /26
Dispositivos de networking	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	
Broadcast	172.16.x.255	



4. Mascara de subred

Como se enseñó anteriormente, una dirección IPv4 tiene una porción de red y una porción de host. Se hizo referencia a la duración del prefijo como la cantidad de bits en la dirección que conforma la porción de red.

Para definir las porciones de red y de host de una dirección, los dispositivos usan un patrón separado de 32 bits llamado máscara de subred, como se muestra en la figura. La máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host.

Como se muestra en la figura, un prefijo /24 se expresa como una máscara de subred como 255.255.255.0 (11111111.11111111.11111111.00000000). Los bits restantes (orden inferior) de la máscara de subred son ceros, que indican la dirección host dentro de la red.

La máscara de subred se configura en un host junto con la dirección IPv4 para definir la porción de red de esa dirección.

Por ejemplo, veamos el host 172.16.20.35/27:

dirección

172.16.20.35

10101100.00010000.00010100.00100011

máscara de subred

255.255.255.224

11111111.11111111.11111111.11100000

dirección de red

172.16.20.32

10101100.00010000.00010100.00100000

4.1 Lógica AND

Dentro de los dispositivos de redes de datos, se aplica la lógica digital para interpretar las direcciones. Cuando se crea o envía un paquete IPv4, la dirección de red de destino debe obtenerse de la dirección de destino. Esto se hace por medio de una lógica llamada AND.

Se aplica la lógica AND a la dirección host IPv4 y a su máscara de subred para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND a la dirección y a la máscara de subred, el resultado que se produce es la dirección de red.

La operación AND

La lógica AND es la comparación de dos bits que produce los siguientes resultados:

$$\text{1 AND 1} = 1$$

$$\text{1 AND 0} = 0$$

$$\text{0 AND 1} = 0$$

$$\text{0 AND 0} = 0$$

Se aplica la lógica AND a cada bit de la dirección con el bit de máscara de subred correspondiente.

Motivos para utilizar AND

La aplicación de AND a la dirección host y a la máscara de subred se realiza mediante dispositivos en una red de datos por diversos motivos.

Los routers usan AND para determinar una ruta aceptable para un paquete entrante. El router verifica la dirección de destino e intenta asociarla con un salto siguiente. Cuando llega un paquete a un router, éste realiza el procedimiento de aplicación de AND en la dirección IP de destino en el paquete entrante y con la máscara de subred de las rutas posibles. De esta forma, se obtiene una dirección de red que se compara con la ruta de la tabla de enrutamiento de la cual se usó la máscara de subred.

Un host de origen debe determinar si un paquete debe ser directamente enviado a un host en la red local o si debe ser dirigido al gateway. Para tomar esta determinación, un host primero debe conocer su propia dirección de red.

Aplicación de la máscara de subred							
Un dispositivo con la dirección 192.0.0.1 pertenece a la red 192.0.0.0							
Bits de orden superior				Bits de orden inferior			
Prefijo /16							
192 . 0 . 0 . 1							
Dirección de host	11000000		00000000		00000000		00000001
Máscara de subred	255		255		0		0
	11111111		11111111		00000000		00000000
Dirección de red	11000000		00000000		00000000		00000000
Red	192 . 0 . 0 . 0						

5. Subredes

5.1 Principios de división en subredes

La división en subredes permite crear múltiples redes lógicas de un único bloque de direcciones. Como usamos un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuanto más bits de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin

embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

El RouterA en la figura posee dos interfaces para interconectar dos redes. Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es "0" y para la otra subred, este bit es "1".

Fórmula para calcular subredes

Use esta fórmula para calcular la cantidad de subredes:

2^n donde n corresponde a la cantidad de bits que se tomaron prestados.

En este ejemplo, el cálculo es así:

$$2^1 = 2 \text{ subredes}$$

Cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula $2^n - 2$ donde n corresponde a la cantidad de bits para hosts.

La aplicación de esta fórmula, ($2^7 - 2 = 126$) muestra que cada una de estas subredes puede tener 126 hosts.

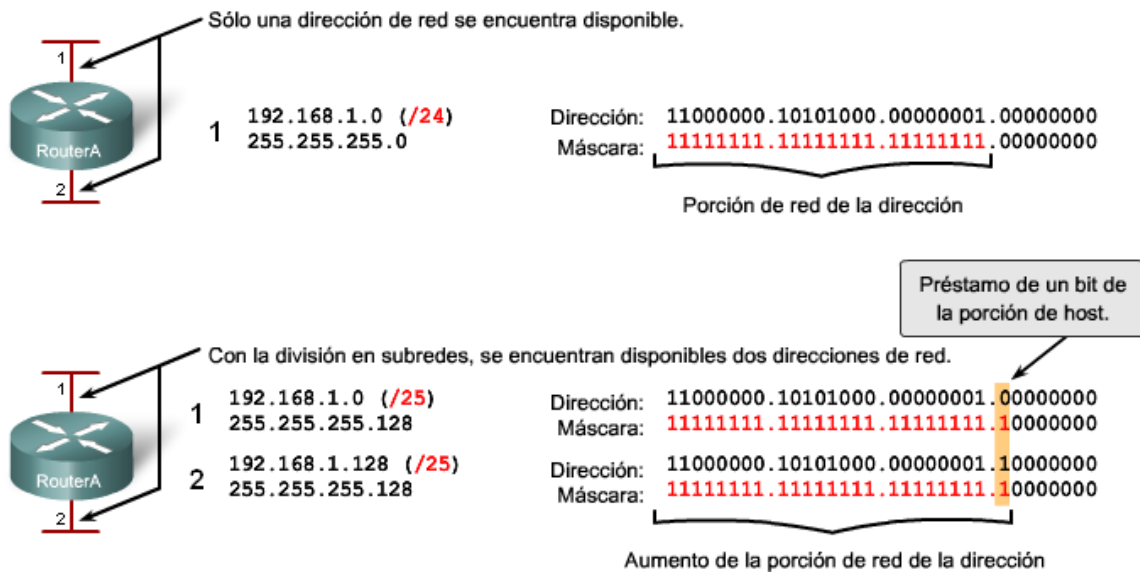
En cada subred, examine el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: 00000000 = 0

Subred 2: 10000000 = 128

Observe la figura del esquema de direccionamiento para estas redes.

Préstamo de bits para las subredes



Esquema de direccionamiento: Ejemplo de 2 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255