Tema 4_1

DIRECCIONAMIENTO IP Y CONFIGURACIÓN DE ROUTERS

SI | 23-24

Indices

Sistemas en red II

1. Direccionamiento IP

Sin duda alguna Internet se ha convertido en la red más grande y con mayor crecimiento de la historia. Cada vez se ofrecen más servicios a través de Internet como comercio electrónico, banca electrónica, formación,… Por lo que se hace necesario que cualquier empresa disponga de una red y que pueda conectarse a Internet.

Los pasos que hay que realizar para la puesta en marcha de una red son:

- **Creación de la red a nivel físico**. Se crea la infraestructura necesaria para poner la red en funcionamiento. Para ello se instala el cableado de la red y luego se ponen en marcha los dispositivos de interconexión (hub, switch, routers…).
- **Creación de la red a nivel lógico**. Se crean las diferentes redes lógicas y se asignan las direcciones IP a los diferentes equipos de la red.
- **Configuración de los routers.** Se configuran los routers para permitir aceptar o denegar la comunicación que se realizan a través de él.

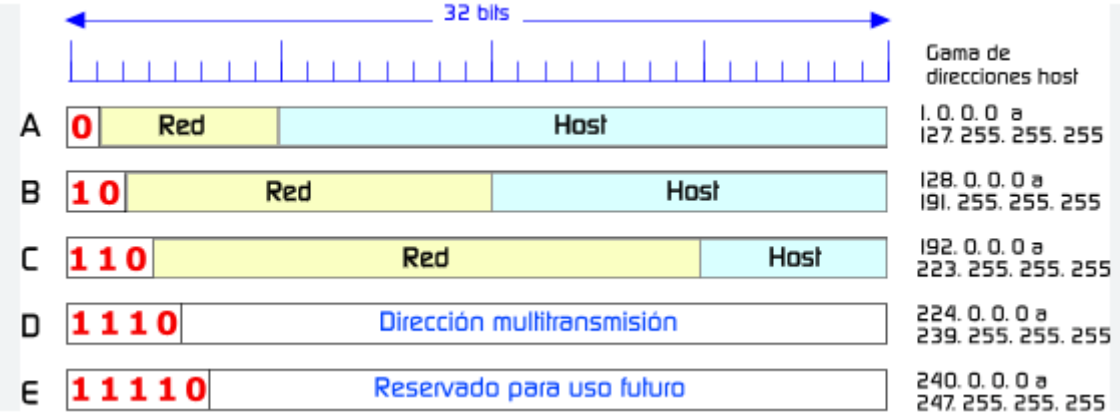
Además, veremos los conceptos más importantes sobre los servicios más utilizados en las redes de ordenadores e Internet.

Para poder trabajar en red, cada interfaz de red de un equipo (host o router) necesita una dirección IP, esta dirección identifica al equipo mediante una dirección única de 32 bits. Las direcciones IP se suelen representar por cuatro números decimales separados por puntos, que equivalen al valor de cada uno de los cuatro bytes que componen la dirección. Por ejemplo, una dirección IP válida sería 147.156.23.208.

El direccionamiento IP es la parte encargada de asignar de forma correcta a cada equipo una dirección IP, de forma que los equipos puedan comunicarse correctamente entre sí.

1.1. CLASES DE DIRECCIONES (IPV4)

Las direcciones IP tienen una estructura jerárquica. Una parte de la dirección corresponde a la red (netid), y la otra al host dentro de la red (hostid). Cuando un router recibe un datagrama (mensaje) por una de sus interfaces compara la parte de red de la dirección con las entradas contenidas en sus tablas (que normalmente sólo contienen direcciones de red, no de host) y envía el datagrama por la interfaz correspondiente.



Dependiendo del número de bits que se utiliza para indicar la red (netid) o el equipo (hostid) se definen varios tipos de direcciones de red. Los diferentes tipos de direcciones IP dan una mayor flexibilidad y permiten definir direcciones IP para grandes, medianas y pequeñas redes, conocidas como redes de clase A, B y C, respectivamente:

- **Una red de clase A** (que corresponde a las redes originalmente diseñadas) se caracteriza por tener a 0 el primer bit de dirección; el campo red ocupa los 7 bits siguientes y el campo host los últimos 24 bits. Puede haber hasta 126 redes de clase A con 16 millones de hosts cada una.
- **Una red de clase B** tiene el primer bit a 1 y el segundo a 0; el campo red ocupa los 14 bits siguientes, y el campo host los 16 últimos bits. Puede haber 16382 redes clase B con 65534 hosts cada una.
- **Una red clase C** tiene los primeros tres bits a 110; el campo red ocupa los siguientes 21 bits, y el campo host los 8 últimos. Puede haber hasta dos millones de redes de clase C con 254 hosts cada una.

Para indicar qué parte de la dirección corresponde a la red y qué parte al host, se suele utilizar una notación denominada "**máscara de red"**, consistente en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden a la parte host. Así, por ejemplo, diremos que una red clase A tiene una máscara 255.0.0.0, lo cual equivale a decir que los ocho primeros bits especifican la red y los 24 restantes el host. Análogamente decimos que una red clase B tiene una máscara 255.255.0.0 y una clase C una máscara 255.255.255.0. Otra notación utilizada en muchos sistemas es expresar de forma conjunta con la dirección IP el número de bits de la máscara de red. Así por ejemplo, para expresar una dirección de clase A sería 12.15.19.1/8, de clase B 172.16.0.1/16 y de clase C 192.168.1.1/24. Esta notación se llama "notación CIDR" y la estudiaremos en el siguiente apartado.

Además, existen direcciones de **clase D** (no redes) cuyos primeros cuatro bits valen 1110, que se utilizan para definir grupos multicast (el grupo viene definido por los 28 bits siguientes). Por lo tanto, no se debe utilizar para identificar a ningún host o estación de una red.

Por último, la clase E, que corresponde al valor 11110 en los primeros cinco bits, está reservada para usos futuros por falta de IP's, no obstante, el siguiente paso es la versión 6 del direccionamiento IP, llamado IPv6.

A partir de los valores de los primeros bits de cada una de las clases mencionadas anteriormente, se puede deducir el rango de direcciones que corresponde a cada una de ellas. Así pues, en la práctica es inmediato saber a qué clase pertenece una dirección determinada sin más que leer el primer byte de su dirección. La siguiente tabla resume toda la información esencial sobre los tipos de direcciones de Internet.

A modo de resumen, a continuación, puedes ver un esquema de las diferentes clases de direcciones y en la tabla puedes ver las características principales de las clases de direcciones.

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

1.2. CIDR

Originalmente, las direcciones de Internet IPv4 se asignaban según redes que seguían el esquema expuesto anteriormente, según redes de clase A, B o C. A este se le llama "classful networking" o "redes por clases". Este método era altamente ineficiente, ya que en muchas ocasiones las asignaciones de redes de clase A o B resultaban en que muchas de las direcciones pertenecientes a esas redes quedaban sin ser utilizadas. Por ejemplo, si al asignar una red de tipo B (65.534 hosts posibles) a un proveedor de Internet solamente se utilizaban 10.000 direcciones, esto suponía que se estaban desperdiciando 65.534 - 10.000 = 55.534 direcciones IP. El gran crecimiento de Internet llevó al rápido agotamiento de las direcciones IP, unido al problema del gran crecimiento de las tablas de enrutamiento globales.

Con el objetivo de reducir estos problemas se introdujo en 1993 el método de asignación de direcciones **CIDR, que significa "enrutamiento entre dominios sin clases".** Según este método las direcciones IP se agrupan en "prefijos de red" o "bloques CIDR" de tamaño libre. A las direcciones se les añade un número precedido por una barra '/', lo cual indica el número de bits utilizados para la parte de red de la dirección. Mientras que anteriormente todas las redes tenían un tamaño que era /8 (255.0.0.0) para redes de clase A, /16 (255.255.0.0) para redes de clase B y /24

(255.255.255.0) para redes de clase C, ahora las asignaciones de direcciones se pueden realizar según agrupamientos de otros tamaños.

Por ejemplo:

El prefijo 90.74.84.0**/22** (máscara equivalente 255.255.252.0) puede ser publicado como tal en las tablas de enrutamiento de Internet, y contiene desde la dirección 90.74.84.0 hasta la 90.74.87.255, lo cual sería equivalente a cuatro redes de tamaño /24 contiguas entre sí.

Según el esquema por clases, esta asignación sería solamente una parte de la red 90.0.0.0/8 de clase A.

Como se puede comprobar, el sistema CIDR permite que la forma de asignar direcciones IP sea mucho más granular.

Decimos que una dirección IP está incluida en un bloque CIDR, y que "*encaja"* con el prefijo CIDR, si los N bits iniciales de la dirección y el prefijo son iguales. Por tanto, para entender CIDR es necesario visualizar la dirección IP en binario. Dado que la longitud de una dirección IPv4 es fija, de 32 bits, un prefijo CIDR de N-bits deja 32-N bits sin encajar, y hay 2^(32-N) combinaciones posibles con los bits restantes. Esto quiere decir que 2^(32-N) direcciones IPv4 encajan en un prefijo CIDR de N-bits.

Ejemplo el bloque: 208.130.28.0/22, es capaz de admitir 1024 direcciones IP (32-22= 10; 2^10 = 1024).

1.3. DIRECCIONES DE USO ESPECIAL (IPV4)

Existen unas reglas y convenios en cuanto a determinadas direcciones IP que es importante conocer:

- La dirección **broadcast** 255.255.255.255 se utiliza para enviar un mensaje a la propia red, cualquiera que sea (y sea del tipo que sea).
- La dirección **0.0.0.0** identifica al host actual. Sólo se puede usar como dirección de origen, no de destino.
- La dirección con el **campo host todo a ceros** se utiliza para indicar la **red misma**, y por tanto no se utiliza para ningún host. Por ejemplo, la dirección 193.147.7.0 identifica una red de clase C.
- La dirección con el **campo host todo a unos** se utiliza como la dirección **broadcast** de la red indicada, y por tanto no se utiliza para ningún host. Por ejemplo, para enviar un mensaje broadcast en la red anterior, utilizaríamos la dirección 193.147.7.255.
- La dirección 127.0.0.1 se utiliza para pruebas **loopback;** todas las implementaciones de IP **devuelven a la dirección de origen** los datagramas enviados a esta dirección sin intentar enviarlos a ninguna parte.

Como consecuencia de las reglas 3 y 4 siempre hay **dos direcciones no asignables** a hosts en una red. Por ejemplo, si tenemos la red 200.200.200.0 (clase C) tendremos que reservar la dirección 200.200.200.0 para denotar la red misma, y la dirección 200.200.200.255 para envíos broadcast a toda la red; dispondremos pues de 254 direcciones para hosts, no de 256.

A modo de resumen, en la tabla puedes ver un ejemplo de las diferentes direcciones específicas.

Dirección especial	Netid	Hostid	Ejemplo (193.147.7.32/24)
Dirección de red	Específica	Todo a 0	193.147.7.0
Dirección directa de broadcast	Específica	Todo a 1	193.147.7.255
Dirección broadcast limitada	Todo a 1	Todo a 1	255.255.255.255
Host específico en esta red	Todo a 0	Específica	0.0.0.32
Dirección loopback	127	Cualquiera	127.0.0.1

1.4. DIRECCIONES PRIVADAS (IPV4)

El RFC 1918 (En Internet, una red privada es una red de computadoras que usa el espacio de direcciones IP especificadas en el documento **RFC 1918.** A los equipos o terminales puede asignárseles direcciones de este espacio cuando deban comunicarse con otros terminales dentro de la red interna/privada (una que no sea parte de Internet/red pública) pero no con Internet directamente) establece que los bloques de direcciones **10/8, 172.16/12 y 192.168/16 están reservados para redes privadas (intranets)**. Estos números no se asignan a ninguna dirección válida en Internet y por tanto pueden utilizarse para construir redes privadas. Por ejemplo, detrás de un firewall o cortafuegos, sin riesgo de entrar en conflicto de acceso a redes válidas de Internet, que usan direcciones públicas.

Clase	Nombre	Rango	Prefijo	Direcciones disponibles	Número de redes (en notación pre-CIDR)
A	Bloque de 24 bits	10.0.0.0 - 10.255.255.255	10.0.0.0/8	16.777.216	1 red clase A
B	Bloque de 20 bits	172.16.0.0 - 172.31.255.255	172.16.0.0/12	1.048.576	16 redes clase B
C	Bloque de 16 bits	192.168.0.0 - 192.168.255.255	192.168.0.0/16	65.536	256 redes clase C

Nótese que, a pesar de que la notación por clases **pre-CIDR** está obsoleta, sigue siendo común llamar a estos bloques como "direcciones privadas de clase A" (10/8), "de clase B" (172.16/12) y "de clase C" (192.168/16).

Por contraposición, todas las demás direcciones que pueden ser usadas en Internet y que no estén dentro de los rangos privados ni ningún otro rango de direcciones de uso especial se consideran direcciones públicas. Por ejemplo: Las direcciones 216.58.211.227 y 8.8.4.4 son direcciones públicas de Internet, la dirección 127.0.0.1 es una dirección reservada para pruebas de loopback, y la dirección 172.20.12.48 es una dirección privada perteneciente al bloque 172.16/12.

1.5. DIRECCIONES IPV6

Internet Protocol version 6 (IPv6) es la última revisión del Internet Protocol (IP) y la primera versión del protocolo que se difundan ampliamente. IPv6 fue desarrollado por el Internet Engineering Task Force (IETF) para hacer frente a la tan esperada problema de agotamiento de las direcciones ipv4.

A diferencia de IPv4, que utiliza una dirección IP de 32 bits, las direcciones IPv6 tienen un tamaño de 128 bits. Por lo tanto, IPv6 tiene un espacio de direcciones mucho más amplio que IPv4.

Las direcciones IPv6 se clasifican según las políticas de direccionamiento y encaminamiento más comunes en redes: direcciones unicast, anycast y multicast.

- Una dirección **unicast** identifica una única interfaz de red. El protocolo de Internet entrega los paquetes enviados a una dirección unicast a la interfaz específica.
- Una dirección **anycast** es asignada a un grupo de interfaces, normalmente de nodos diferentes. Un paquete enviado a una dirección anycast se entrega únicamente a uno de los miembros, típicamente el host con menos coste, según la definición de métrica del protocolo de encaminamiento. Las direcciones anycast no se identifican fácilmente pues tienen el mismo formato que las unicast, diferenciándose únicamente por estar presente en varios puntos de la red. Casi cualquier dirección unicast puede utilizarse como dirección anycast.
- Una dirección **multicast** también es usada por múltiples interfaces, que consiguen la dirección multicast participando en el protocolo de multidifusión (multicast) entre los routers de red. Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se hayan unido al grupo multicast correspondiente.

IPv6 no implementa direcciones **broadcast.** El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all-nodes). Sin embargo, no se recomienda el uso del grupo all-nodes, y la mayoría de protocolos IPv6 usa un grupo multicast de enlace-local exclusivo en lugar de molestar a todos los interfaces de la red.

Partes de una dirección IPv6

Una dirección IPv6 tiene un tamaño de **128 bits** y se compone de **ocho campos de 16 bits,** cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la figura siguiente, las equis representan números hexadecimales.

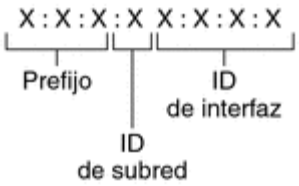
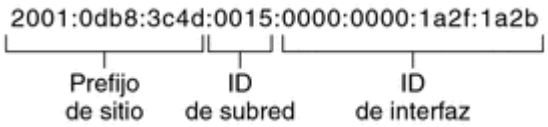


Ilustración 1: Formato básico de las direcciones IPv6

Ejemplo*:*



La figura muestra las tres partes de que consta una dirección IPv6, que se describen en el texto siguiente.

Los tres campos que están más a la izquierda (48 bits) contienen el **prefijo de sitio.** El prefijo describe la topología pública que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el **ID de subred** de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la **topología privada**, denominada también topología del sitio, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el **ID de interfaz**, también denominado token. El ID de interfaz se puede configura automáticamente desde la dirección MAC de interfaz o manualmente en formato **EUI-64** ((Identificador Único de Entidad de 64 bits) es un formato de identificación único utilizado en redes de área local (LAN) y en el protocolo de Internet (IP))

Ejemplo:

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

En este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, 2001:0db8:3c4d, contienen el prefijo de sitio y representan la topología

pública. Los siguientes 16 bits, 0015, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, 0000:0000:1a2f:1a2b, contienen el ID de interfaz.

Abreviación de direcciones IPv6

La mayoría de las direcciones IPv6 no llegan a alcanzar su tamaño máximo de 128 bits. Eso comporta la aparición de campos rellenados con ceros o que sólo contienen ceros.

La arquitectura de direcciones IPv6 permite utilizar la notación de dos puntos consecutivos (: :) para representar campos contiguos de 16 bits de ceros. Por ejemplo, la dirección IPv6 del ejemplo (**2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b**) se puede abreviar reemplazando los dos campos contiguos de ceros del ID de interfaz por dos puntos, solo se puede hacer una vez. La dirección resultante es **2001:0db8:3c4d:0015::1a2f:1a2b**. Otros campos de ceros pueden representarse como un único 0. Asimismo, puede omitir los ceros que aparezcan al inicio de un campo, como por ejemplo cambiar 0db8 por db8.

Así pues, la dirección **2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b** se puede abreviar en **2001:db8:3c4d:15::1a2f:1a2b**.

La notación de los dos puntos consecutivos se puede emplear para reemplazar cualquier campo contiguo de ceros de la dirección IPv6. Por ejemplo, la dirección IPv6 2001:0db8:3c4d:0015:0000:d234::3eee:0000 se puede contraer en 2001:db8:3c4d:15:0:d234:3eee::.

En la abreviación de direcciones Ipv6, si se tiene un «hexteto» con 4 ceros, se pueden eliminar y dejar un solo cero. El dispositivo IPv6 agregará los 3 ceros restantes.

- Abreviado: 2042:0000:220F::AA5B:2345
- Más abreviado: 2042:0:220F::AA5B:2345

En la abreviación de direcciones Ipv6, los ceros iniciales también se pueden eliminar. Al eliminar estos ceros obtenemos una buena dirección IPv6 corta

- Original: 2001:0002:0003:0003:0006:0005:0006:0007
- Abreviado: 2001:2:3:3:6:5:6:7

Prefijos de IPv6

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes de IPv6. Los prefijos de IPv6 tienen el formato siguiente:

prefijo/tamaño en bits

El tamaño del prefijo se expresa en notación **CIDR** (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo en bits.

El prefijo de sitio de una dirección IPv6 ocupa como máximo los **48** bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48 se ubica en los 48 bits que hay más a la izquierda, 2001:db8:3c4d.

Usando la representación con ceros comprimidos, este prefijo:

2001:db8:3c4d::/48

También se puede especificar un prefijo de subred, que define la topología interna de la red respecto a un enrutador. La dirección IPv6 de ejemplo tiene el siguiente prefijo de subred:

2001:db8:3c4d:15::/64

El prefijo de subred siempre contiene 64 bits. Estos bits incluyen 48 del prefijo de sitio, además de 16 bits para el ID de subred.

EUI-64 y EUI-64 Modificado

El EUI-64 (identificador único extendido) es un formato de identificación única que se utiliza comúnmente en redes, especialmente en el contexto de IPv6. Este formato se deriva de una dirección MAC de 48 bits y se utiliza para crear direcciones de interfaz únicas de 64 bits.Una dirección MAC 00:1D:BA:06:37:64 se convierte en una dirección EUI-64 de 64 bits insertando FF:FE en el medio: 00:1D:BA:FF:FE:06:37:64. Pero modificamos este EUI-64 cuando lo usamos para formar una dirección IPv6: invertimos el bit Universal/Local (el séptimo bit más significativo del EUI-64), de manera que un 0 en dicho bit del EUI-64 resultará un 1 en el EUI-64 Modificado. Para identificar la interfaz anterior en la red IPv6 2001:db8:1:2::/64 usaríamos la dirección 2001:db8:1:2:021d:baff:fe06:3764 (con el bit subrayado U/L invertido de 0 a 1).

Para obtener el EUI-64 a partir de una dirección MAC de 48 bits, se siguen estos pasos:

1. **Dirección MAC original:**
    - Ejemplo: 00:11:22:33:44:55
2. **Inserción de FF:FE:**
    - Se inserta FF:FE en el medio de la dirección MAC.
    - EUI-64: 02:11:22:FF:FE:33:44:55

EUI-64 Modificado:

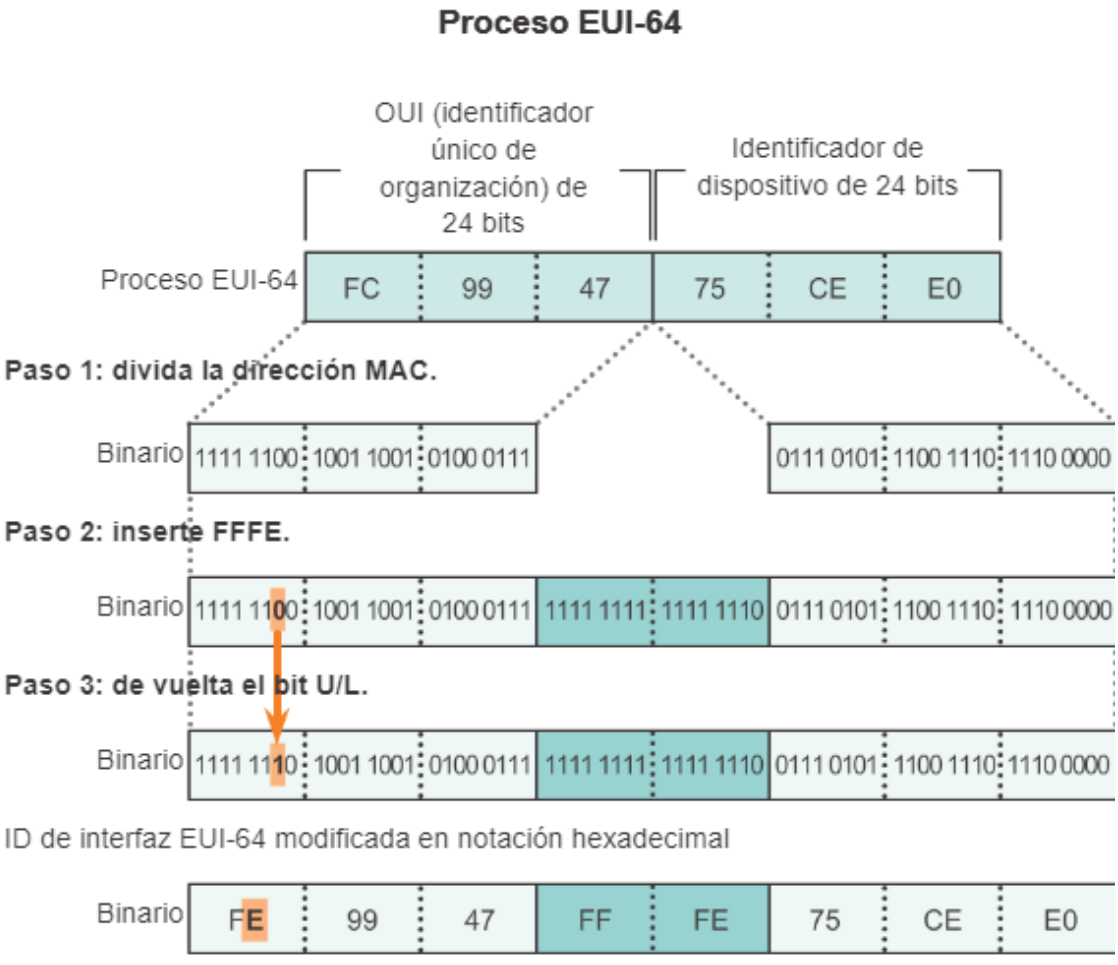
Además del EUI-64, a veces se realiza una modificación adicional para indicar que la dirección es global en lugar de local. Esta modificación implica cambiar el séptimo bit

(contando desde la izquierda) de la dirección EUI-64. Si es 0, se cambia a 1, y si es 1, se cambia a 0.

Para obtener el EUI-64 modificado a partir del EUI-64:

1. **Cambio del séptimo bit:**
    - Cambiamos el séptimo bit (contando desde la izquierda) de 0 a 1 o de 1 a 0.
    - EUI-64 Modificado: 02:11:22:33:FF:FE:44:55

Modificamos EUI-64 para reducir las probabilidades de duplicidad entre direcciones manuales y automáticas.



Ejercicios IPv6

1.6. SUBREDES

La subdivisión de redes, comúnmente conocida como **"subnetting,"** es una técnica utilizada en redes informáticas para dividir una red IP en subredes más pequeñas. Esto se hace para **varios propósitos**, como:

- mejorar la administración de direcciones IP,
- aumentar la seguridad de la red y
- optimizar el rendimiento.

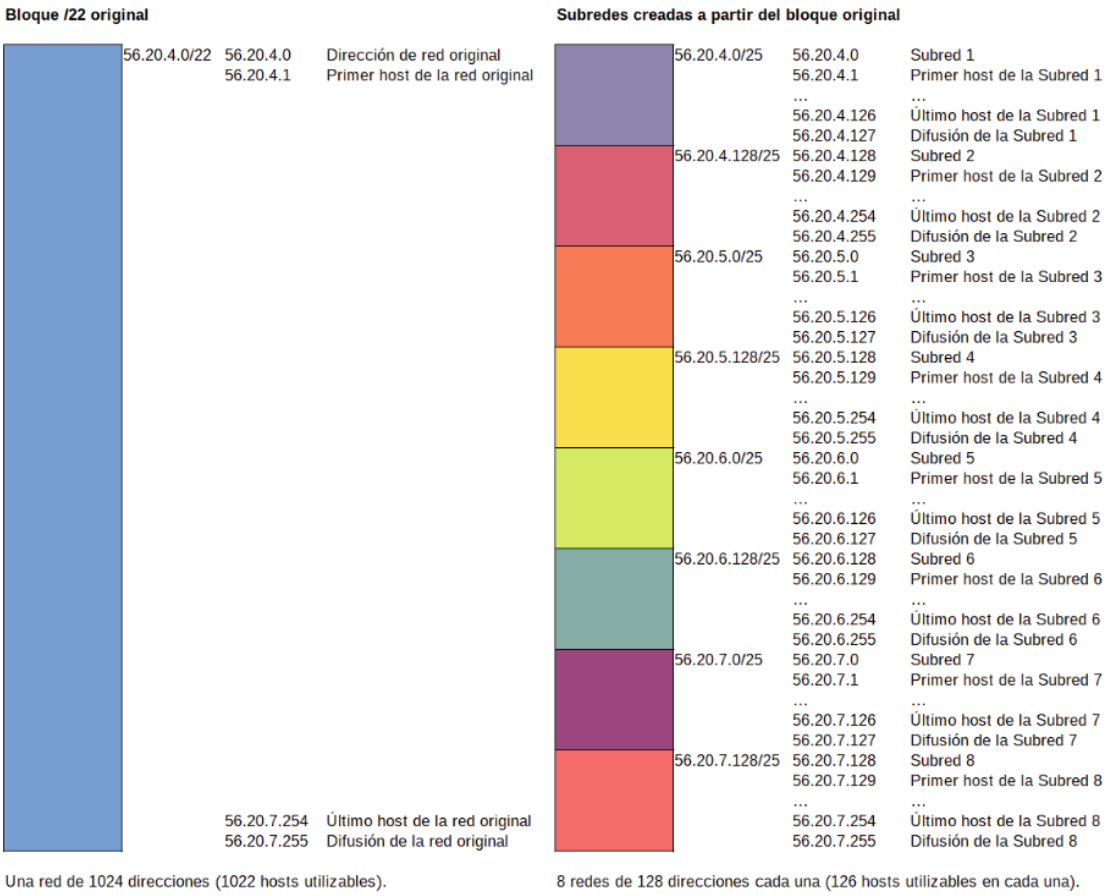
Subnetting es una parte fundamental de la gestión de redes y es esencial para comprender cómo funcionan las direcciones IP y cómo se comunican los dispositivos en una red.

Cuando se realiza el subnetting, **se divide una red en subredes más pequeñas** asignando una máscara de subred adecuada. Esto permite crear segmentos de red independientes dentro de la red original. Cada subred tiene su propia gama de direcciones IP y su propia máscara de subred.

Por ejemplo, si tienes una red con la dirección IP "192.168.1.0" y deseas crear **cuatro** subredes (2 bits), puedes usar una máscara de subred **"/26"** (que permite 64 direcciones IP por subred) para dividir la red en cuatro segmentos, como:

- Subred 1: 192.168.1.0/26
- Subred 2: 192.168.1.64/26
- Subred 3: 192.168.1.128/26
- Subred 4: 192.168.1.192/26

Cuando se usa el método CIDR los administradores de las redes pueden gestionar el direccionamiento de estas, lo cual incluye el poder subdividir las redes en subredes independientes de tamaños inferiores. Por ejemplo, el bloque de direcciones 56.20.4.0/22 puede ser originalmente asignado a un proveedor de Internet. Este bloque comprende las direcciones de la 56.20.4.0 a 56.20.7.255, con un total de 1.024 direcciones IP distintas. El proveedor de Internet puede decidir subdividir este bloque en redes independientes más pequeñas. En la siguiente imagen se puede observar cómo el administrador de la red original la ha subdividido en 8 subredes de 128 direcciones cada una.



Se puede observar que dentro de todas las redes **hay dos direcciones IP que no se pueden asignar a hosts**. Estas direcciones son la primera y la última de cada red o subred. La primera dirección, que corresponde a aquella en la que la parte del host o "HostID" tiene todos sus bits a 0, es la dirección de red de la red o subred, y se usa para identificar a la red. La última dirección, que corresponde a aquella en la que la parte del host tiene todos sus bits a 1, es la dirección de multidifusión (o difusión, broadcast en inglés) de la red o subred, y se usa para enviar paquetes a todos los hosts que pertenecen a dicha red o subred. Este es el motivo de que en todas las redes el número de hosts disponibles sea igual al número total de direcciones IP de la red menos 2.

En el pasado se recomendaba no utilizar tampoco la primera y última subred creadas al subdividir una red en otras más pequeñas, dado que el uso de estas redes podía crear confusiones y situaciones no deseadas, especialmente en el caso del uso de mensajes de multidifusión en la última subred. En el ejemplo que acabamos de poner esto se traduciría en no utilizar las subredes 1 y 8 con el fin de evitar estas hipotéticas situaciones conflictivas. Esta técnica desperdicia muchas direcciones IP que quedarían sin ser usadas. Aunque en la actualidad es común encontrar bibliografía que hace referencia a esta práctica, está ya está obsoleta y no es necesario aplicarlo. Tanto el hardware como el software de red actuales son capaces de utilizar sin problemas estas dos subredes. Solamente es necesario eliminar dichas redes cuando se trabaja con equipamiento de red muy antiguo.

Ejemplo Subredes.

1.6.1. VLSM

En el ejemplo anterior se ha mostrado un caso simple de subdivisión de un bloque de direcciones en varias subredes del mismo tamaño. El método **CIDR permite** el uso de **VLSM, o "máscaras de subred de tamaño variable".** Con **VLSM** se pueden crear subredes de **distinto tamaño** a partir de un bloque de direcciones, lo cual permite adaptar el tamaño de las distintas subredes creadas a las necesidades específicas de cada caso.

Supongamos que tienes una red principal con la dirección IP "192.168.1.0/24" y deseas subdividirla en subredes más pequeñas para varios departamentos de una empresa, como ventas, marketing, y recursos humanos. Además, se necesita un número diferente de direcciones IP para cada departamento:

- Ventas: 50 direcciones IP
- Marketing: 30 direcciones IP
- Recursos Humanos: 10 direcciones IP

Paso 1: Asignación de subredes

Primero, debes determinar la cantidad de direcciones IP necesarias para cada departamento y luego asignar máscaras de subred adecuadas para satisfacer esas necesidades. En este caso, necesitas tres subredes con diferentes tamaños.

- Ventas: Necesita al menos **50 direcciones IP (6 bits)**. La máscara de subred más pequeña que puede acomodar al menos 50 direcciones IP es "/26," lo que proporciona 64 direcciones IP por subred.
- Marketing: Necesita al menos **30 direcciones IP (5 bits).** De nuevo, puedes usar una máscara de subred "/26" para proporcionar 64 direcciones IP por subred, aunque algunas direcciones se quedarán sin usar.
- Recursos Humanos: Necesita al menos 10 direcciones IP. Para esto, puedes usar una máscara de subred "/28," que proporciona 16 direcciones IP por subred.

Paso 2: Asignación de direcciones IP

Ahora, asigna las direcciones IP a cada subred con sus máscaras de subred correspondientes:

- Subred de Ventas: 192.168.1.0/26
  - Rango de direcciones: 192.168.1.0 - 192.168.1.63
- Subred de Marketing: 192.168.1.64/26
  - Rango de direcciones: 192.168.1.64 - 192.168.1.127

- Subred de Recursos Humanos: 192.168.1.128/28
  - Rango de direcciones: 192.168.1.128 - 192.168.1.143

Con VLSM, estás utilizando máscaras de subred de diferentes tamaños según las necesidades de cada departamento. Esto te permite utilizar eficientemente las direcciones IP y garantizar que cada departamento tenga suficientes direcciones disponibles para sus dispositivos sin desperdiciar direcciones en subredes más grandes.

Ejemplo VLSM.

¿Cómo determinar si dos equipos pertenecen a la misma red?

Para que dos equipos puedan comunicarse entre ellos de manera directa deben pertenecer a la misma red o subred. Esta comunicación tiene lugar a nivel 2 (nivel de enlace de datos) del modelo OSI. Dos equipos que pertenezcan a redes o subredes distintas pueden comunicarse entre sí si existe un mecanismo de enrutamiento que permita el tráfico entre dichas redes. Esta comunicación tiene lugar a nivel 3 (nivel de red) del modelo OSI.

Para saber si dos equipos pertenecen a la misma red o subred se utilizan sus direcciones IP y sus máscaras de red. Se aplica la operación "Y lógica" entre las direcciones IP y las máscaras, y esto determina las redes a las que pertenecen las direcciones. Veamos un ejemplo:

- Host A
  - IP: 198.10.62.7
  - Máscara: 255.255.248.0 (equivalente a /21)
- Host B
  - IP: 198.10.58.39
  - Máscara: 255.255.248.0 (equivalente a /21)

Para obtener la dirección de red del Host A:

- 198.10.62.7 → 11000110.00001010.00111110.00000111
- 255.255.248.0 → 11111111.11111111.11111000.00000000
- Y lógico

11000110.00001010.00111000.00000000 → 198.10.56.0

198.10.56.0 es la dirección de la red a la que pertenece el Host A.

Para obtener la dirección de red del Host B:

- 198.10.58.39 → 11000110.00001010.00111010.00100111
- 255.255.248.0 → 11111111.11111111.11111000.00000000
- Y lógico

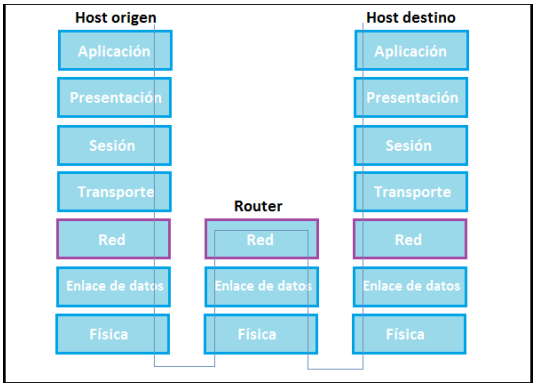
11000110.00001010.00111000.00000000 → 198.10.56.0

198.10.56.0 es la dirección de la red a la que pertenece el Host B.

En este ejemplo ambos hosts, A y B, pertenecen a la misma red y por tanto se podrían comunicar entre ellos de manera directa sin necesidad de enrutamiento entre redes.

2. Configuración de routers

Como hemos visto anteriormente, un router es un dispositivo de interconexión que permite regular el tráfico que pasa entre varias redes. Un router es muy útil a la hora de defendernos de posibles intrusiones o ataques externos. Pero como desventaja es que un router no se configura por sí sólo. Mientras que un router bien configurado puede ser muy útil, un router mal configurado no nos proporciona ningún tipo de protección o, simplemente, no llega a comunicar dos redes.



2.1. TABLAS DE ENRUTADO

Para configurar un router debemos crear lo que se denomina “tabla de enrutado” o “directivas de firewall”. En ella se guardan las acciones que hay que realizar sobre los mensajes que recibe el router para redirigirlos a su destino. Existen dos tipos de encaminamiento: encaminamiento clásico y encaminamiento regulado.

Elementos clave de la tabla de enrutamiento clásico:

- **Red de Destino (Destination Network):** Es la dirección de la red de destino a la que se intenta llegar. Puede expresarse en términos de una dirección IP y una máscara de red.
- **Máscara de Red (Subnet Mask):** Indica qué parte de la dirección IP representa la red y qué parte representa los hosts. Ayuda a determinar si una dirección IP de destino está en la misma red local o si se debe enrutar hacia otra red.
- **Gateway Predeterminado (Default Gateway):** Es la dirección IP del router o dispositivo que se utiliza como el próximo salto predeterminado cuando la dirección de destino no está presente en la tabla de enrutamiento.
- **Interfaz de Salida (Outgoing Interface**): Indica a través de qué interfaz de red (puerto) debe enviarse el paquete para llegar a la red de destino.
- **Métrica (Metric):** Es un valor numérico utilizado para determinar la preferencia de una ruta en comparación con otras rutas posibles. Cuanto menor sea el valor métrico, más preferida será la ruta.
- **Tipo de Ruta (Route Type):** Puede indicar si la ruta es estática (configurada manualmente) o dinámica (aprendida automáticamente a través de un protocolo de enrutamiento como RIP, OSPF o BGP).
- **Estado de la Ruta (Route State):** Indica si la ruta está activa o inactiva. Las rutas activas están disponibles para el enrutamiento, mientras que las inactivas no se utilizan actualmente.
- **Próximo Salto (Next Hop):** Indica la dirección IP del siguiente dispositivo al que se debe enviar el paquete para llegar a la red de destino. Puede ser una dirección IP específica o el término "directamente conectado" si la red de destino está en la misma red local.

Con el encaminamiento clásico, las reglas utilizadas para encaminar los paquetes se basan, exclusivamente, en la dirección destino que aparece en la cabecera del paquete. Así se distinguen las siguientes reglas:

- Permitir un equipo de nuestra red.
- Permitir cualquier equipo de nuestra red.
- Permitir un equipo de otra red.
- Permitir cualquier equipo de otra red.

La última regla (por defecto) se aplica en el caso de que no se cumpla ninguna de las anteriores y se suele utilizar para poder enviar los mensajes a la puerta de enlace de la red.

Sin embargo, en la actualidad, con la explosión del uso de Internet y la llegada del concepto de calidad de servicio (QoS) y la seguridad, los routers utilizan el llamado encaminamiento regulado, con el que, a la hora de escribir la tabla de enrutado, se pueden utilizar los siguientes elementos:

- **Interfaz:** interfaz de red por donde se recibe la información.
- **Origen / Destino**: origen y destino del mensaje. Normalmente el origen y el destino de un mensaje es una dirección IP, pero algunos routers permiten utilizar como dirección origen y destino usuarios o grupos de usuarios.
- **Protocolo:** permitir o denegar el acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto para que un cliente (que inicia la conexión) pueda conectarse. Por ejemplo un servidor web trabaja en el puerto 80, un servidor de FTP en el puerto 21, etcétera.
- **Seguimiento:** indica si el router debe de realizar un seguimiento de los lugares por los que pasa un mensaje.
- **Tiempo:** espacio temporal en el que es válida la regla.
- **Autentificación de usuarios:** indica si el usuario debe de estar autentificado para utilizar la regla.
- **Acción:** especifica la acción que debe realizar el router. Un router puede realizar las siguientes acciones:
- **Aceptar:** dejar pasar la información.
- **Denegar:** no deja pasar la información.
- **Reenviar:** envía el paquete a una determinada dirección IP.

```
C:\Documents and Settings\Alumno>route print
===========================================================================
ILista de interfaces
0x1 ........................... MS TCP Loopback interface
0x2 ...00 14 85 ec 5a 9c ...... Broadcom NetLink (TM) Gigabit Ethernet - Minipue
rto del administrador de paquetes
===========================================================================
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de acceso   Interfaz  Métrica
          0.0.0.0          0.0.0.0      172.16.0.1     172.16.0.86       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
       172.16.0.0      255.255.0.0      172.16.0.86     172.16.0.86       20
     172.16.0.86  255.255.255.255        127.0.0.1       127.0.0.1       20
  172.16.255.255  255.255.255.255      172.16.0.86     172.16.0.86       20
        224.0.0.0        240.0.0.0      172.16.0.86     172.16.0.86       20
  255.255.255.255  255.255.255.255      172.16.0.86     172.16.0.86       1
Puerta de enlace predeterminada:        172.16.0.1
===========================================================================
Rutas persistentes:
  ninguno

C:\Documents and Settings\Alumno>
```

Ejemplo Enrutamiento de 2 y 3 Routers

2.2. ELEMENTOS DE CONFIGURACIÓN DE UN ROUTER

Existen diferentes tipos de routers por lo que en un principio podemos caer en la tentación de pensar que el proceso de configuración para cada router es totalmente diferente a los demás. Pero entre los routers más utilizados, ya sean hardware o software, tenemos:

- FireWall 1 de CheckPoint.
- Private Internet Exchange (PIX) de Cisco System.
- IOS Firewall Feature Set de Cisco System.
- Firewall del núcleo de Linux, Iptables.
- Enterprise Firewall de Symantec.
- Internet Security and Acelerador (ISA Server) de Microsoft.

Si se comparan los elementos que utilizan los diferentes routers (ver tabla) puede ver cómo los más utilizados a la hora de realizar una tabla de enrutado son la interfaz, la dirección origen y destino, el puerto y la acción que debe realizar el router.

Comparativa sobre los elementos de las tablas de enrutado.

Modelo	Interfaz	Origen/destino	Protocolo	Seguimiento	Tiempo	Autentificación de usuarios	Acción
FireWall 1	√	√**	√	√	√		√
PIX	√	√	√*				√
IOS Firewall	√	√	√				√
Firewall Linux	√	√	√				√
Enterprise Firewall	√	√**	√		√	√	√
ISA Server	√	√**	√*		√	√	√

*Distingue entre puerto de origen y destino.

**Permiten especificar como origen o destino direcciones IPs o usuarios.

A la hora de indicar la dirección de origen o la dirección de destino es importante utilizar la máscara de red para indicar un mayor o menor número de ordenadores. Así por ejemplo, si en la dirección destino utiliza la dirección de clase B 142.165.2.0/16 se hace referencia a todas las direcciones IP del tipo 142.165.x.x. Si utiliza la dirección de clase C 192.165.2.0/24, hace referencia a las direcciones del tipo 192.165.2.x. Por lo tanto, si aumentamos la máscara de red, estamos disminuyendo el número de direcciones IP a las que se hace referencia y si disminuimos la máscara de red, entonces se hace referencia a un mayor número de direcciones IP. En la tabla siguiente, puedes ver algunas de las posibilidades más habituales.

Ejemplos de utilización de la máscara de red en la configuración de routers

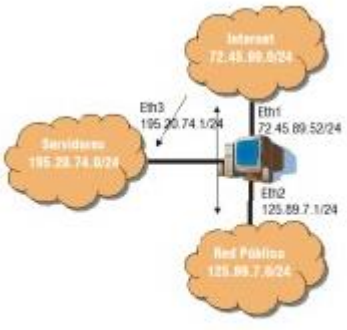
Ejemplo	Comentario
192.165.2.23/32	Representa a un único ordenador (por ejemplo, un servidor web)
192.165.2.0./24	Representa a todas las direcciones IP del tipo 192.165.2.X
192.165.0.0/16	Representa a todas las direcciones IP del tipo 192.165.X.X
192.0.0.0/8	Representa a todas las direcciones IP del tipo 192.X.X.X
0.0.0.0/0	Representa a todas las direcciones IP del tipo X.X.X.X

Durante el filtrado de paquetes se aplica la regla de “coincidencia total”. Todos los criterios de la regla tienen que coincidir con el paquete entrante; en caso contrario, no se aplica la regla. Esto no significa que se rechace el paquete o que se elimine, sino que la regla no entra en vigor. Normalmente, las reglas se aplican en orden secuencial, de arriba hacia abajo. Aunque hay varias estrategias para implementar filtros de paquetes, las dos que se describen a continuación son las más utilizadas por los especialistas de seguridad:

Construir reglas desde la más específica a la más general. Esto se hace así para que una regla general no "omita" a otra más específica, pero conflictiva, que entra dentro del ámbito de la regla general.

Las reglas deberían ordenarse de tal forma que las que más se utilizan estén en la parte superior de la lista. Esto se hace por cuestiones de rendimiento. Normalmente un router detiene el procesamiento de una lista cuando encuentra una coincidencia total.

2.3.EJEMPLO DE CREACIÓN DE UNA TABLA DE ENRUTADO



Ejemplo de red

La figura muestra un router conectado a tres redes diferentes. Debemos crear el conjunto de reglas para permitir que: la red pública se conecte a Internet y que los

servidores sean accesibles desde Internet; el servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.

La tabla de enrutado representa el conjunto de reglas que actúan como medida de seguridad para determinar si se permite que un paquete pase o no.

El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes. Las notas acerca de la implementación se incluyen siguiendo la descripción de cada línea del conjunto de reglas.

Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.

Tabla de enrutamiento

Reglas	Interfaz	Origen	Destino	Puerto	Acción
1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.7/32	25, 110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

- **Regla 1.** Esta regla permite el acceso entrante en el puerto 80, que normalmente se utiliza para el tráfico http. El host que está en 195.20.74.5 es el servidor web. La organización no puede predecir quién va a tener acceso a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.
- **Regla 2**. Esta regla permite el acceso entrante a los puertos 25 y 110, que normalmente se utiliza para correo electrónico (el puerto 25 es el servidor smtpo correo saliente y el puerto 110 es el servidor pop3 o correo entrante). El servidor de correo está en la dirección 195.20.74.7. Al igual que en la regla anterior, como no se puede predecir quién va a tener acceso al servidor de correo no se restringen las direcciones IP de origen.
- **Regla 3**. Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como las reglas 1 y 2 se ejecutan antes, sí se permite el tráfico que va dirigido a los servidores web y correo electrónico. Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a ningún servidor.

- **Reglas 4 y 5**. La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y la quinta regla deja pasar el tráfico que va desde la red pública a la red de Internet.
- **Regla 6.** Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría de los casos, permite registrar los paquetes que coinciden con ella. Esto es útil por motivos jurídicos y administrativos.