Curso “Redes telemáticas I”

192.168.10.5/27

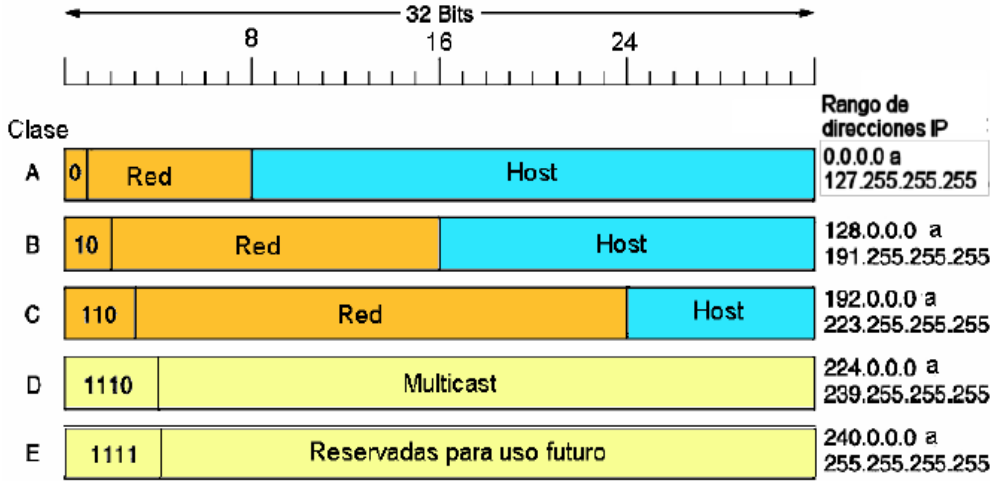
PLANIFICACIÓN DEL DIRECCIONAMIENTO IP

0.1 LAS DIRECCIONES IP. REDES CON CLASE

Una dirección IP es una secuencia de 32 bits unos y ceros separados en grupos de 8 bits. Para facilitar el manejo cada grupo de 8 bits se traduce a decimal y se conoce como formato **decimal punteado.** La dirección IP 192.168.1.2 en notación binaria sería 11000000.10101000.00000001.000000010.

Las direcciones IP forman un direccionamiento jerárquico porque contiene diferentes niveles o partes.

- Red
- Subred
- Host



Clase	Bits netid	Bits hostid	Nº redes	Nº hosts
A	8	24	$2^{(8-1)} = 128$	$2^{24} = 16.777.216$
B	16	16	$2^{(16-2)} = 16384$	$2^{16} = 65.536$
C	24	8	$2^{(24-3)} = 2.097.152$	$2^{8} = 256$

Tradicionalmente se han dividido las direcciones IP en clases:

CLASE A: comienzan por un 0 binario, y hasta completar el primer octeto representa la identificación de la red, pudiendo tener un máximo de 128 redes. Los 24 bits restantes permiten direccionar hasta 16.777.214 host.

CLASE B: tiene 16 bits para identificar la red, de los cuales los dos primeros son siempre "10", por lo que permite llegar a las 16.384 redes, eso si con un número máximo de host de 65.534. Con este tipo de direcciones el rango va desde la red 128.0.0.0 a la red 191.255.0.0.

CLASE C: reservan sólo 8 bits para numerar los host, con un máximo de 254 por red. El rango de este tipo de direcciones va desde la red 192.0.0.0 a la 223.255.255.0.

CLASE D: comienzan por la secuencia de bits 1110. El rango de este tipo de direcciones va desde la red 224.0.0.0 a la 239.255.255.255. Son direcciones de multicast, es decir una dirección de clase D que identifica a un grupo de dispositivos que ejecuta un determinado protocolo o aplicación.

CLASE E: comienzan por la secuencia de bits 1111. El rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, de 240 a 255

La Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet.

Direcciones públicas y privadas

Las direcciones IP privadas son otra solución al problema del agotamiento de las direcciones IP públicas.

La RFC 1918 aparta los tres siguientes bloques de direcciones IP privadas:

- Una red Clase A 10.0.0.0
- Diecisiete direcciones Clase B de 172.16.0.0 a 172.31.0.0 y además la 169.254.0.0
- 256 direcciones Clase C de 192.168.0.0 a 192.168.255.0

Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los Routers de Internet descartan inmediatamente estas direcciones privadas.

Para conectar una red que utiliza direcciones privadas a internet, se requiere que las direcciones privadas sean convertidas en direcciones públicas. Este proceso de conversión se conoce como Traducción de direcciones de red (NAT). En general, un Router es el dispositivo que realiza la NAT.

Por otra lado la red 127.0.0.0 se reserva para bucles de prueba en equipos, para comprobar si funciona bien la tarjeta de red y están cargados la pila de protocolos TCP/IP.

Direcciones reservadas

Dirección de red

Cuando en una dirección IP de cualquier clase el campo del host termine en ceros nos estamos refiriendo a la dirección de esa red. Estas direcciones no se pueden utilizar para identificar equipos.

La dirección 117.0.0.0 se refiere a la red de clase A 117 no a un host de esa red.

La dirección 197.41.32.0 se refiere a la red de clase C 197.41.32 no a un host de esa red.

Dirección de broadcast

Hay otras direcciones que se utilizan para difusión, broadcast, es decir para mandar información a todos los equipos de una red.

La dirección de boadcast en la red de clase A 117.0.0.0 es 117.255.255.255

La dirección de broadcast en una red de clase C como la 197.41.32.0 es 197.41.32.255

En general **en cualquier red de internet la primera dirección y la última están reservadas**. **La primera por ser la dirección genérica de la red y la más alta por ser la de broadcast.**

La dirección 255.255.255.255 se utiliza en conexiones punto a punto o cuando un equipo no tiene una dirección IP de ninguna clase, y la utiliza para decir que está en la red o quiere entrar a una red, (vocea que está ahí y si es posible que le asignen una dirección IP).

Direcciones multicast

Otro tipo de direcciones son las direcciones de multicast, que son de clase D y que hacen referencia a un grupo de dispositivos que ejecutan un protocolo o aplicación determinada. Por ejemplo un mensaje enviado a la dirección 224.0.0.5 significa que ese mensaje deben leerlo todos los routers que ejecuten el OSPF.

Resumiendo:

- **Unicast:** Hace referencia a un solo equipo de la red.
- **Multicast**: Hace referencia a un grupo de equipos de la red o sistema autónomo.
- **Broadcast**: Hace referencia a todos los equipos de la red.

0.2 SUBREDES

Hay veces que se necesita dividir las redes en redes más pequeñas, denominadas subredes, para brindar mayor flexibilidad y poder administrar mejor la red, sobre todo en redes de gran tamaño.

El campo de subred y el campo de host se crean a partir de la porción de host original. **La forma dividir la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad para el direccionamiento al administrador de red.**

Una red de clase A tiene mas de 16 millones de direcciones de host, si no se dividiera en subredes sería imposible de manejar.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred.

Dentro de cada subred el funcionamiento es el mismo que en el caso de las redes, no se puede utilizar la primera dirección, porque es la de subred y tampoco se puede utilizar la última porque es la de broadcast.

Por esta razón cuando se hacen subredes hay que dejar como mínimo 2 bits para el campo de host, pues si se deja un solo bit, entonces sólo tendría un número de red (el 0 de red) y el número de broadcast (el 1 de broadcast).

Las razones principales para usar una subred son:

- **Reducir el tráfico de broadcast**: Si en una red de clase A todos los host estuviesen conectados directamente con el tráfico de broadcast generado al arrancar cada equipo bastaría para que la red no pudiera funcionar, pues no dejaría ancho de banda.

- **Facilitar el enrutamiento**: en una red de clase A y clase B una vez dividida en subredes se facilita el paso de la información de los equipos de una subred a otra, mediante el uso de rotures.
- **Por seguridad**: se puede controlar el tráfico de unas subredes a otras, mediante el uso de Listas de Control de Acceso.

Por otro lado, cuando un administrador de una red (sea A, B, C) hace subredes (y por supuesto usa routers en ellas) las otras redes de internet las ven como a una sola. Desde internet **no se ven**, ni se saben las subredes, sólo la red.

Tiene el inconveniente de que cuando el administrador haga subredes van a perderse algunas direcciones, que no se pueden aprovechar, por eso no se debe hacer subredes sin una buena planificación.

El funcionamiento de las subredes es el mismo que el de las redes. Si una red está dividida en subredes, la única manera en que pueden intercambiar información los equipos es a través de **un router**.

Máscara de subred

La máscara de subred, le indica a los dispositivos de red cuál es la parte de una dirección que corresponde al campo de red (incluyendo los bits de subred) y cuál es la parte que corresponde al campo de host. Su misión es **facilitar el enrutamiento**. Una máscara de subred tiene una longitud de 32 bits y tiene 4 octetos, al igual que la dirección IP.

La máscara de subred para una dirección IP de subred particular, se crea expresando el campo de red y subred en forma de unos y el campo de host en forma de ceros (todos ellos binarios) y luego pasándola de nuevo a decimal punteado.

Por defecto, si no se pide ningún bit prestado, la máscara de subred para una red de Clase B sería 255.255.0.0.

La máscara de subred predeterminada indica exclusivamente la parte de red (no subred).

Ejemplo 1:

La máscara de subred predeterminada para las siguientes IP es:

119.234.133.7	→	255.0.0.0	(Clase A)
178.249.69.54	→	255.255.0.0	(Clase B)
199.97.39.73	→	255.255.255.0	(Clase C)

En el momento que en una red se hagan subredes la máscara de subred ya no es la predeterminada y siempre hay que decir la máscara de subred, pues esta depende del diseño de red y los routers no la conocen de antemano.

Si queremos hacer subredes en una red de clase B y se pidieran prestados 8 bits para el campo de subred, la máscara de subred incluiría 8 bits a "1" adicionales y se transformaría en 255.255.255.0.

Si en vez de coger 8 bits hubiésemos tomado 4 la máscara de subred sería 255.255.240.0.

La máscara de subred usa una porción del campo de host para hacer subredes, es decir **incluye la parte de red y la parte de subred**. Por ejemplo:

119.234.133.7/14 → 255.252.0.0

178.249.69.54/20 → 255.255.240.0

199.97.39.73/27 → 255.255.255.224

Ejemplo 2:

La red de Clase C, 197.150.220.0, se divide en subredes con una máscara de subred 255.255.255.224. También se puede poner como 197.150.220.0/27.

Con un valor de 224 en el ultimo octeto (11100000 en números binarios), la porción de red de Clase C de 24 bits se ha ampliado en 3 bits, para obtener un total de 27 bits.

Los routers de Internet (que no conocen la máscara de subred) solo se ocuparán del enrutamiento hacia la red de Clase C 197.15.220.0, mientras que los routers que están ubicados dentro de esa red, que conocen la máscara de subred, tomarán en cuenta los 27 bits para tomar una decisión de enrutamiento

En el caso anterior:

- ¿cuantas subredes tenemos?
- ¿Cuántos host en cada subred?
- ¿A qué subred pertenece la dirección 197.150.220.131?

Ejemplo 3:

Partiendo de la red de clase C: 192.168.1.0 se han realizado 4 subredes (2 bits para el campo de subred):

- ¿cuantas subredes tenemos?
- ¿Cuántos host en cada subred?
- ¿A qué subred pertenece la dirección 192.168.1.120?
- ¿Cuál es la dirección de broadcast que usará un PC configurado con la IP 192.168.1.70/26?

0.3 REDES CON NAT Y PAT

Según hemos visto RFC 1918 aparta los siguientes bloques de direcciones IP privadas:

- Una red Clase A 10.0.0.0
- Diecisiete direcciones Clase B de 172.16.0.0 a 172.31.0.0 más la 169.254.0.0
- 256 direcciones Clase C de 192.168.0.0 a 192.168.255.0

Estas direcciones son sólo para el uso particular de la red interna. Estas direcciones no se usan en internet ni los equipos pueden salir con ellas a internet, sino que deben ser cambiadas o traducidas.

NAT y PAT son mecanismos que se utilizan en la frontera de las redes stub, en conexiones a través de proveedores ISP, como las ADSL, o cable MODEM, donde se hacen redes internas con IP privadas.

Una de las razones principales por las que **NAT** fue desarrollada es para **ahorrar direcciones IP registradas**. NAT también puede brindar seguridad a las PC, los servidores y los dispositivos de red al evitar que sus direcciones host de IP actuales tengan acceso directo a Internet.

NAT significa **Traducción de Direcciones de Red**.

Al configurar NAT en un router, hay algunos términos que ayudan a clarificar la forma en que el router realiza la NAT:

Red local interna: hace referencia a cualquier red conectada a una interfaz de router que forma parte de la LAN privada. Los hosts en las redes internas tienen sus propias direcciones IP que serán traducidas antes de ser transmitidas a los destinos externos.

Red global externa: toda red que se conecta al router y que es externa a la LAN y que no reconoce las direcciones privadas que se asignan a los host en la LAN.

Las traducciones NAT clásicas pasan las direcciones privadas a públicas, una a una, y hay dos formas:

- En una NAT estática tenemos que decir la IP pública que se dará a cada IP privada.
- En una NAT dinámica mapea un conjunto de IP privadas sobre un conjunto de IP públicas.

La ventaja que tiene la NAT estática es que puede permitir que equipos de la red pública puedan acceder a determinados equipos de la red privada.

PAT

Cuando una organización tiene un pequeño grupo de direcciones IP registrado, o una sola dirección IP, puede hacer que varios usuarios accedan simultáneamente a la red pública con un mecanismo denominado **sobrecarga de NAT**, **o traducción de la dirección de puerto (PAT).**

Por medio de NAT, el router integrado puede traducir muchas **direcciones IP internas** a **una dirección pública (PAT)**. En la tabla NAT anota las direcciones locales con la dirección global pública asociada.

Por tanto para salir a internet los equipos de la red interna que tienen direcciones IP privadas deben compartir una IP pública entre todos. Para diferenciarles el router asigna a cada IP privada un **número de puerto diferente de la IP pública.**

- PAT traduce varias direcciones privadas sobre una (o varias) IP pública. De ahí la sobrecarga.
- En los números de puerto conocidos 0-512 intenta mantener el número de puerto original (Correo, ftp, dns,...) pero normalmente a los equipos les asigna números de puerto del **1024 en adelante**.
- Teóricamente son posibles 56536 conexiones, pero en realidad sólo se asignan hasta 4000 puertos.

La traducción se mantiene sólo durante cada conexión, de forma que la combinación de dirección IP global y número de puerto se eliminan una vez finaliza la conversación.

Sólo es necesario traducir los paquetes destinados a otras redes. Estos paquetes deben pasar por la puerta de enlace (gateway por defecto), donde el router integrado reemplaza la dirección IP privada del host de origen con su propia dirección IP pública y un número de puerto que no esté en uso.

Ventajas de las NAT y de las PAT

- No hay que cambiar la configuración de la red al cambiar de proveedor.
- Requiere pocas direcciones externas para traducir muchos hosts.
- Protege la seguridad de la red pues no publica la red privada ni la topología.

Desventajas de las NAT y de las PAT.

- Algunas aplicaciones aumentan la carga de trabajo del router ya que incorporan una dirección IP como parte de los datos encapsulados. El router debe reemplazar las combinaciones de direcciones IP de origen y puertos incluidas dentro de los datos y las direcciones de origen en el encabezado IP.
- La división en subredes, el direccionamiento IP privado y el uso de NAT fueron desarrollados para brindar una solución temporal al problema del agotamiento de las direcciones IP. Estos métodos, a pesar de ser útiles, no crean más direcciones IP.

0.4 LAS DIRECCIONES IPV6

En el protocolo IP versión 6 se utilizan **128 bits** en vez de 32 con lo cual teóricamente es posible $3{,}4x10^{38}$ máquinas. Esta versión de IP debe proporcionar suficientes direcciones para las necesidades de comunicación futuras.

Se piensa que es la solución definitiva al problema de la escasez de direcciones IP. Se estima que si se repartiesen en toda la superficie de la tierra habría $6{,}67x10^{23}$ IPs por m2., o que si el tamaño de las IPv4 es de una canica el de las IPv6 es el del planeta Saturno.

La notación utilizada no es decimal punteada, sino que se utiliza el binario, o mejor dicho su equivalente hexadecimal. Se hacen grupos de 16 bits separados por dos puntos. Así, por ejemplo:

Ejemplo IPv6:	0780 : FE00 : 83AC : 0000 : 0000 : 0000 : 01D4 : 005C

Las direcciones IPv6 también están jerarquizadas en tres partes:

- El **prefijo global** está compuesto por los primeros tres bloques de la dirección y se lo asigna a una organización mediante un **registro de nombres** de Internet (viene a ser la dirección de red).
- Campo de **subred**
- Campo de ID de interfaz (**host**) controlado por el administrador de red.

Prefijo global	Subred	Identificador de interfaz
0870 : FE00 : 83AC :	0000 :	0000 : 0000 : 01D4 : 005C

0.5 BIBLIOGRAFÍA

Bibliografía utilizada y material para ampliar conocimientos:

- Currículo de la certificación de redes Cisco CCNA Discovery.
- Redes de computadoras. Andrew S. Tanenbaum. Ed. Pearson.
- Existe además en Internet abundante información y cursos relacionados.

Curso “Redes telemáticas I”

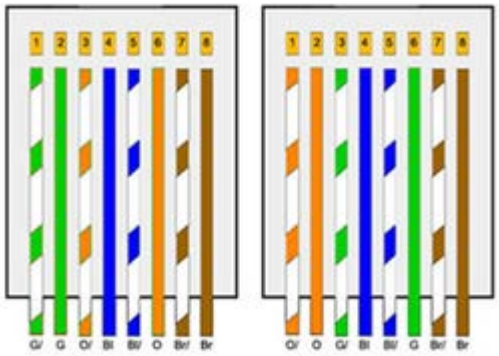
Tarea práctica

192.168.10.5/27

PLANIFICACIÓN DEL DIRECCIONAMIENTO IP

LATIGUILLOS CABLE UTP

Se deberá de conectorizar cables utp según la norma EIA/TIA-**568-B**, estándar para montaje de conectores **ethernet** RJ-45, para ello se realizará según la siguiente relación de pares identificados por sus códigos de colores.



Materiales necesarios:

- ✓ Cable utp de la longitud requerida (según distancia entre los dispositivos).
- ✓ Conectores macho RJ-45.
- ✓ Herramienta para el crimpado de los conectores
- ✓ Tijera
- ✓ Comprobador de cableado utp

Cable utp directo:

Se usa para cables de conexión entre equipos de diferentes características:

- ✓ PC a Switch
- ✓ Router a Switch

Ambos extremos con conectores según el código de colores 568B.

Se deberá de comprobar mediante el comprobador de cableado que el conector ha quedado bien crimpado y que el mapa de pares es correcto.

Cable utp cruzado:

Se usa para cables de conexión entre equipos de similares características:

- ✓ PC a PC
- ✓ Router a Router
- ✓ Switch a Switch
- ✓ PC a Router

Un extremo con conector según el código de colores 568B, y en el otro extremo según el código de colores 568A.Se deberá de comprobar mediante el comprobador de cableado que el conector ha quedado bien crimpado y que el mapa de pares es correcto.