CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

UNIDAD DE REDES 11.COMPUTER

Los sistemas informáticos
CFGS DAW

Alfredo Oltra / Sergio García
alfredo.oltra @ ceedcv.e s

2019/2020

Versión: 190927.1231

Licencia

nomenclatura

A lo largo de Este tema se utilizarán Distintos Símbolos para distinguir Elementos Importantes Dentro del contenido. Símbolos Estós hijo:

- Importante

- Atención

- interesante

ÍNDICE

UD11. RED DE COMPUTADORAS

1. INTRODUCCIÓN

Sin lugar a dudas, uno de los elementos que más ha contribuido en la evolución de la informática en los últimos años ha sido la capacidad de los equipos de conexión para el intercambio de información.

Toda la comunicación entre dos partes consiste en una serie de elementos:

- ***Mensaje:*** la información a transmitir.
- ***Enviador recibidor:*** el dispositivo que envía / recibe el mensaje. Por lo general se llaman anfitrión.
- ***Canal:*** es el medio que transmite el mensaje.
- ***transductor:*** el dispositivo que convierte el mensaje en una señal a ser transmitida. Por ejemplo, en un ser humano las cuerdas vocales o los oídos, o en un ordenador, la tarjeta de red.
- ***elementos accesorios:*** Los elementos que la comunicación ayuda a tomar mejores: un teléfono, una antena o, en redes de computadoras, un cubo, un router, un repetidor ...
- ***protocolos:*** los conjuntos de reglas que controlan el flujo de datos y definen parámetros físicos de los otros componentes en el sistema de comunicaciones. Por ejemplo: 1. que marcar un número,

    2. suena el teléfono,
    3. alguien lo recoge,
    4. dice "hola",
    5. la otra persona dice, “hola, soy yo”

2. TIPOS DE REDES

Hay muchas maneras de clasificar una red, aunque los más utilizados son:

2.1 Por área geográfica

- LAN (Local Area Network): La característica principal que la distancia entre las computadoras debe ser pequeña (de una habitación a unos pocos kilómetros). Son ampliamente utilizados para conectar los ordenadores personales y estaciones de trabajo en oficinas de la empresa y la fábrica con el fin de compartir recursos (impresoras, etc.) y el intercambio de información.

- WAN (Wide Area Network) es un tipo de red que cubre una distancia de entre 100 y 1.000 kilómetros, lo que le permite ofrecer conectividad a varias ciudades o incluso a todo un país. Por lo general, son ejecutadas por una empresa o una organización para uso privado, o incluso por un proveedor de servicios de Internet (ISP), para proporcionar conectividad a todos sus clientes.

> • Esta clasificación se puede ampliar con muchos otros tipos como MAN (Metropolitan Area Network) o CAN (Red de Área Campus) en función de la amplitud y la conectividad

2.2 Por los servicios

- Cliente-servidor: algunos equipos (clientes) la demanda de servicios y otros, los servidores, los ofrecen.

- Intercambio de archivos: todos los ordenadores pueden funcionar como clientes y servidores

2.3 Por tipo de comunicación

- Simplex: el canal sólo permite la comunicación en una dirección. Un ejemplo podría ser la emisión de radio.
- Half-duplex: el canal permite la comunicación en ambos sentidos, pero no simultáneamente. Un ejemplo podría ser el uso de “walkie talkie”.
- Dúplex: el canal permite la comunicación en ambas direcciones simultáneamente. Un ejemplo podría ser una llamada telefónica.

3. ARQUITECTURA

La arquitectura de red es un concepto que tiene como objetivo definir todos los aspectos formales de la implementación de una red. Su estudio abarca los protocolos de topología y de la comunicación.

3.1 Topología

La topología se refiere a la forma física en la que se conectan los hosts de red.

3.1.1 red por cable topologías (los medios de comunicación es un cable)

Autobús: todos los equipos están conectados a los mismos medios de comunicación. Para evitar ***ecos***
(Que el rebote de la señal y de retorno a los medios de comunicación), terminadores son necesarios. Los problemas son que si se rompe el cable falla toda la red y que tienen una baja velocidad ya que sólo un equipo puede utilizar los medios de comunicación al mismo tiempo.

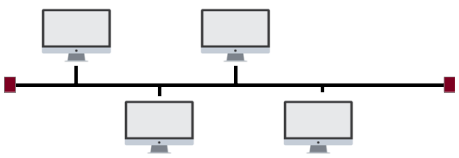


Figura 1. Bus

Estrella: cada host de red está conectado a un concentrador central con una conexión punto a punto. Todo el tráfico que atraviesa la red pasa a través del cubo central. La topología en estrella se considera la topología más fácil de diseñar y poner en práctica, ya que es muy fácil de añadir nodos adicionales. La principal desventaja de la topología en estrella es que si el hub falla falla toda la red.

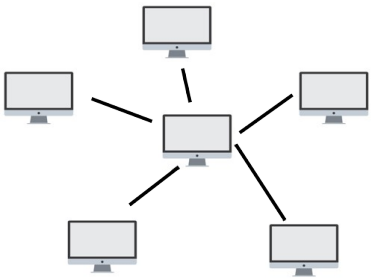


Figura 2. estrella

Anillo: similar a la tipología de bus, pero formando un bucle. Los datos se envían en una dirección y hasta que llega al host de destino.

Malla: cada equipo es punto a punto conectado con todos los demás equipos. La gran ventaja es que si un nodo cae, el resto de la red sigue funcionando.

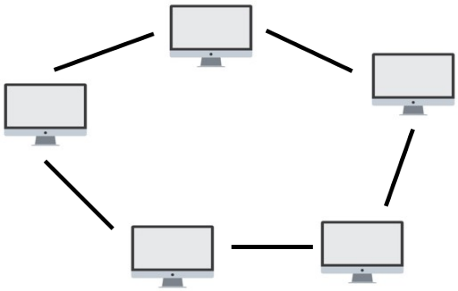


Figura 3. Anillo

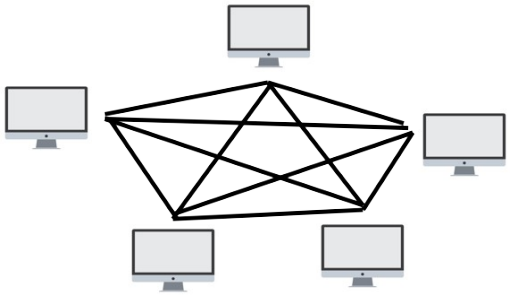


Figura 4. Malla

Árbol: eso es una mezcla entre la estrella la tecnología y la topología de bus: varias líneas de autobuses están conectados a otra línea de autobús. Esta conexión se realiza por medio de elementos auxiliares, tales como concentradores, encaminadores o conmutadores.

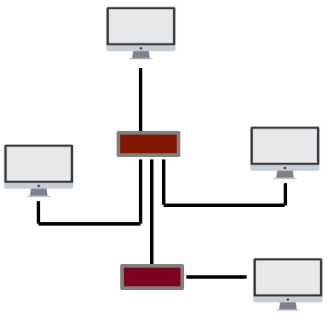


Figura 5. Árbol

3.1.2 topologías de red inalámbrica

Ad-hoc: redes ad-hoc no requieren un punto de acceso. En este modo de funcionamiento los dispositivos de interactuar con otros, lo que permite la comunicación directa entre los dispositivos. A veces se les llama ***de igual a igual*** redes inalámbricas.

Figura 6. ad-hoc

Infraestructura: esta topología se compone de un punto de acceso conectado a un segmento de cableado de red. Es la habitual que tenemos en las casas o en las organizaciones.

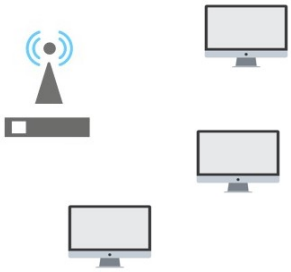


Figura 7. Infraestructura

3.2 Las capas y protocolos

En el comienzo de las redes, las diferentes soluciones que permitan la conexión entre las computadoras eran independientes, es decir, sólo era posible a los equipos de conexión que venían del mismo fabricante. Con el tiempo, y en busca de la interoperabilidad, se decidió que era necesario crear una norma que permitiría a todas las máquinas que interactúan entre sí, siempre que siguieron a ese estándar o modelo.

La idea general de la norma es el trabajo dividiendo el proceso de comunicación en pequeñas fases, fases que se ejecutan de manera secuencial permiten el envío y recepción de mensajes. En el remitente, la ejecución de estas fases con el fin termina con dejando el mensaje en los medios de comunicación. Una vez que esto se lee el receptor, ejecuta estas fases secuenciales pero de manera inversa. Cada una de estas fases se llama capas, y cada capa sólo se entiende la información proveniente de la misma capa de la computadora opuesto. Con el fin de comunicarse entre sí, cada una de estas capas utilizar uno o varios protocolos, es decir, varios procedimientos para recibir o enviar la información.

- El conjunto de todas las capas con sus respectivos protocolos se llama ***pila de protocolos.***

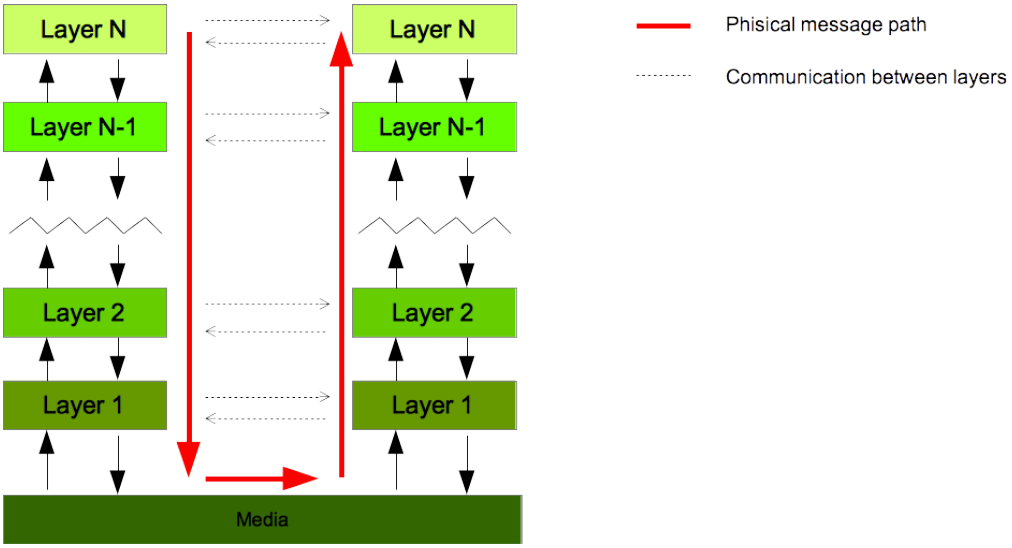


Figura 8. Envío de un mensaje entre ordenadores

Inicialmente el primer modelo adoptado fue el denominado modelo OSI, que diferenciaba siete capas. Aunque este modelo fue implementado inicialmente para lograr la estandarización, el tiempo más ha sido reemplazado por un modelo diferente utilizado en la actualidad por la gran mayoría de las computadoras. Este modelo es el llamado modelo TCP IP que los grupos de varias capas del modelo OSI, dejándolo solo en 4 capas

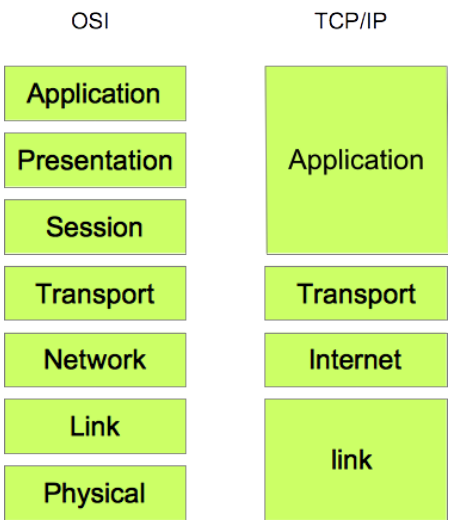


Figura 9. OSI vs TCP / IP

3.2.1 capa de enlace

Es el conjunto de protocolos que las tarjetas de interfaz de red utilizan para el intercambio de datos. Los protocolos de esta capa dependen de la tecnología de la
de la red y se almacenan normalmente en una memoria incorporada ROM de la tarjeta de red. Una de sus funciones es la de convertir los bits en impulsos eléctricos que deben ser transmitidas a través del medio, los protocolos más importantes son: Ethernet (utilizado en LAN), DOCSIS (para redes por cable de módem) y xDSL (como la ADSL).

3.2.2 capa de Internet:

Los protocolos de esta capa a encontrar caminos para que cualquier paquete llega a su nodo de destino. Una de sus funciones es definir cómo identificar los nodos de la red. Para hacerlo, utiliza protocolos como ***ipv4*** y ***IPv6.***

3.2.3 capa de transporte:

Se divide la información de que la capa superior (aplicación), que intenta enviar en pequeños bloques llamados paquetes y, además, se asegura de que los paquetes llegan al destino. Los protocolos más importantes de esta capa son los siguientes:

- TCP: Es un protocolo orientado a la conexión que proporciona una transmisión fiable de información a través de un canal no fiable.

  Las aplicaciones que envían y reciben los paquetes se identifican por sus números de puerto. Los servidores han fijado los números de puerto (el servidor web es el puerto 80), pero los programas cliente pueden tener un número de puerto aleatorio.

  Cada paquete tiene un número de secuencia diferente. Cuando un equipo envía un paquete TCP, el receptor envía un mensaje de confirmación con el mismo número de secuencia de vuelta al remitente.

  Si la confirmación no se recibe después de un intervalo de tiempo predefinido, el emisor asumirá que su paquete se pierde y lo enviará de nuevo. El receptor usará los números de secuencia para ordenar los paquetes y construir el mensaje original de nuevo

- UDP: Es un protocolo de conexión-menos útil para la transmisión. Este protocolo se identifican los equipos cliente y servidor utilizando números de puerto TCP como

  A diferencia de TCP del ordenador que envía los paquetes no espera ninguna confirmación desde el equipo que recibe el paquete. El receptor ignorará los paquetes con un número de secuencia erróneo

  - Este protocolo se utiliza cuando se reciben los datos en el tiempo es más importante que recibir todos los datos originales, por lo que se utiliza para difusión de audio y vídeo en Internet. A nadie le importará si una trama se pierde de vez en cuando mientras ve un vídeo. Sin embargo, si se está descargando un archivo y se pierde un paquete, el archivo se corrompe, por lo que este protocolo no se utiliza para la transmisión de datos.

capa 3.2.4 Aplicación

Se ocupa de la comunicación de las aplicaciones de usuario, como un servidor web y un navegador de Internet que se está ejecutando en diferentes máquinas. Los protocolos más conocidos son:

- HTTP: a las páginas web de solicitud.
- FTP: para cargar y descargar archivos.
- SMTP, POP3, IMAP: para enviar correos de servidor a servidor, descargar el correo electrónico a un cliente de correo electrónico y leer el correo electrónico directamente desde el servidor.
- DNS: para traducir la URL del (como google.com) en direcciones IP (por ejemplo, 45.24.28.55).

- DHCP: configurar automáticamente las direcciones IP de los ordenadores en una red dada.

Un ejemplo muy simplificado de la operación de una comunicación entre dos ordenadores (un cliente y un servidor) para hacer una petición de una página web sería:

1. A partir de la capa de aplicación del cliente del cliente, el protocolo y la URL de la página que se visualizará se indican.
2. Esta información se splited en pequeños paquetes del tamaño requerido por la norma.
3. En la capa de Internet, a cada uno de estos paquetes se añade información sobre la dirección IP del ordenador de destino.
4. Por último, en la capa de enlace, cada uno de esos paquetes se convierte en impulsos eléctricos que se envían a los medios de comunicación.
5. En el servidor de la capa de enlace recibe los impulsos y los convierte en paquetes.
6. En la capa de Internet del servidor, la dirección IP del paquete se comprueba a prueba si este paquete pertenecen a este equipo
7. Los paquetes con direcciones que coinciden con la dirección del servidor que se envían a la capa de transporte para unirse a formar el mensaje. (Capa de transporte)
8. Ese mensaje será procesada por el servidor de aplicaciones de servidor para obtener la página correcta. (Capa de aplicación)

4. Capa de Internet

A pesar de todas las capas tienen su importancia, en este curso nos centraremos sólo en la capa de Internet, donde se hace de direccionamiento y enrutamiento de paquetes (datagramas)

4.1 Dirección IP

Cada uno de los ordenadores de una red tiene una dirección IP única, o más bien, en la misma red no puede haber dos ordenadores con la misma dirección IP. De hecho, para hablar con propiedad, cada una de las interfaces de red (cada una de las tarjetas de red) debe tener una dirección IP única. Por ejemplo, un ordenador con una red Wi-Fi con cable y tendría dos interfaces y, por lo tanto, tendría dos direcciones IP asociadas con ella.

El formato de dirección IP 4.2

Una dirección IP es un número de 32 bits agrupados a partir de 8 a 8. Cada uno de los grupos separados por un punto. Por ejemplo:

10101010.10001101.11110000.00001111

o, en el modo decimal

170.141.240.15

El número de números que podemos representar con 8 bits es $2^8 = 256$ (de 0 a 255), por lo tanto, el rango de Las direcciones IP de 0.0.0.0 va a 255.255.255.255.

4.3 Clases de direcciones

Del mismo modo que una dirección postal consta de varios elementos (nombre de la calle, número, localidad, ...) una dirección IP también se compone de varias partes, en este caso, 2 partes:

- el ID de red, es decir, la parte que identifican a la red
- el ID de host, es decir, la parte que identifican el ordenador (la interfaz) La diferencia es que solo en la dirección postal de cada elemento se diferencia claramente, pero en una dirección de IP de las dos partes se mezclan y puede no ser obvio para localizarlos . De hecho, con el fin de localizar cada una de estas partes, tiene que utilizar otro número, con el mismo formato que la dirección IP, la llamada ***máscara de red.***

La máscara de red es un número que tiene 1 en la parte de la dirección IP que pertenece a la red y 0 en la parte que identifica la computadora. Por ejemplo:

11111111.11100000.00000000.00000000

Realizar una operación AND entre la dirección IP y la máscara de red, se puede localizar la parte del identificador de red:

10101010.10001101.11110000.00001111 -> IP (170.141.240.15)

Y 11111111.11100000.00000000.00000000 -> máscara de red (255.224.0.0)

10101010.10000000.00000000.00000000 = 170.128.0.0 -> ID de red

Como se puede ver, todas las máscaras de red constituyen una secuencia de unos seguidos de una secuencia de ceros. Por esta razón, es bastante común para definir la máscara sólo con un número que indica el número de unos. Esta notación se llama CIDR. Por ejemplo 170.141.240.15/11

Obviamente, haciendo una operación NOT de la máscara y la realización de un AND con la dirección IP se puede obtener la parte que identifica al host.

10101010.10001101.11110000.00001111 -> IP (170.141.240.15)

Y 00000000.00011111.11111111.11111111 -> NO máscara de red (0.31.255.255)

00000000.00001101.11110000.00001111 = 0.13.240.15 -> ID de host

4.4 clases de direcciones IP

Es posible clasificar las direcciones IP en 5 clases:

- Una clase: el primer bit de la dirección es 0 (es decir, el intervalo va desde 0.0.0.0 a 127.255.255.255) y su máscara de red es 255.0.0.0 o / 8. Por ejemplo: 25.124.200.200

- clase B: los dos primeros bits de la dirección son 10 (es decir, el rango de dirección va desde 128.0.0.0 a 191.255.255.255). La máscara de red es 255 255.0.0 o / 16. Por ejemplo: 165.124.200.200
- Clase C: los primeros tres bits de la dirección son 110 (es decir, el rango de dirección va desde 192.0.0.0 a 223.255.255.255). La máscara de red es 255 255.255.0 o / 24. Por ejemplo: 192.168.20.20
- Clase D: los primeros cuatro bits de la dirección son 1,110 (es decir, el rango de dirección va desde 224.0.0.0 a 239.255.255.255).
- Clase E: los cinco primeros bits de la dirección son 11.110 (es decir, el rango de direcciones va de 240.0.0.0 a 247.255.255.255).

> • clases D y E son muy especiales ya que se utilizan para la multidifusión y con fines de investigación.

Puede parecer sorprendente que en la sección anterior hemos puesto un ejemplo cuya máscara de red fue / 11, es decir, una máscara de red que no existe en ninguna de las clases de red anteriores. La explicación tiene dos razones:

- Esta clasificación es simplemente una clasificación formal, es decir, nadie me impide, por ejemplo, de una manera aislada que pueda utilizar una dirección que tiene el primer bit a 0 (clase A) con una máscara de red / 12. Pero si quiero conectar mi red a otras redes es muy probable que tenía problemas.

- Este tipo de redes no formales son creados internamente para dividir una red en otras redes y la eficiencia de ganancia y seguridad. Lo veremos en la sección subnettig.

4.5 Las direcciones públicas y privadas

Tal como se define una dirección IP, el número posible de dispositivos conectados a una red puede ser de hasta 256 * 256 * 256 * 256. Este número, aunque es muy alta, ya está claramente superado en redes como Internet. Por eso, una primera solución para poder optimizar el número de direcciones disponibles es separar las direcciones en direcciones públicas y las direcciones privadas.

- direcciones públicas son los que uno que es único y no se puede repetir
- Las direcciones privadas son aquellas que no se puede utilizar públicamente, pero internamente, por lo que la misma dirección privada puede ser utilizado por varios equipos de diferentes organizaciones. De esta manera, si estas direcciones pueden ser utilizadas por varios ordenadores, el número de posibles dispositivos conectados a la Internet aumenta.

El rango de direcciones privadas son:

- Una clase: de 10.0.0.0 a 10.255.255.255
- Clase B: a partir de 172.16.0.0 a 172.31.255.255
- clase C: desde 192.168.0.0 a 192.168.255.255

Es decir, si desea utilizar la dirección IP interna de su organización tiene que usar uno de ellos en función de la clase que está utilizando. De lo contrario su IP puede chocar con ninguna dirección pública

Pero la cuestión es: ¿cómo puede haber dos direcciones iguales en la misma red? La solución viene dada por el uso de técnicas tales como NAT, del que hablaremos más adelante.

4.6 direcciones especiales

Dentro de un segmento de red hay un conjunto de direcciones especiales, que tienen una función específica.

loopback: Dirección 127.0.0.1 se utiliza para realizar comprobaciones internas de la red propia interfaz.

- Esta dirección está asociada al nombre ***localhost***

- Se podría pensar que probar la dirección IP asignada a la NIC sería lo mismo que usar el bucle de retorno, pero esto es falso. Si el IP se utiliza las hojas de paquete y vuelve. En el caso del bucle de retorno de las pruebas internas.

Transmitir: Enviar un paquete a esta dirección recibirá el paquete llegue a todas las máquinas de la red. Se calcula estableciendo en 1 todos los bits del huésped.

por ejemplo la dirección de bradcast de una red 170.141.240.15/11 es (rojo red de color ID, color verde ID host):

170.141.240.15/11 → 10101010.100 **01101.11110000.00001111** → 10101010.100 **11111.11111111.11111111** → 170.159.255.255 (dirección de Difusión)

Puerta: No es una dirección específica igual que los anteriores, pero es muy importante. Indica la dirección del dispositivo que permitirá el envío de paquetes a la parte exterior del segmento de red local[1]. Por lo general, la segunda dirección de red se utiliza como puerta de enlace (la primera se utiliza generalmente como el nombre de red), por ejemplo 192.168.20.1

4.7 La división en subredes

Como se mencionó antes, el número de direcciones IP es finito y no muy grande, por lo que es necesario para ser eficiente en su asignación. Eso significa optimizar su uso y no perder las direcciones. Por esta una de las técnicas a utilizar es el ***subredes.***

La mejor manera de entender el proceso es con un ejemplo.

Supongamos que la nuestra de asignación de direcciones IP proporciona el ID de red 192.168.40.0/24 para nuestra organización. Esta red es una red privada de tipo C, por lo que su máscara de red es 255.255.255.0 y por lo tanto el número de posibles hosts es 256 (de 0 a 255).

La organización cuenta con cinco departamentos. En cada departamento hay 30 dispositivos que pueden requerir conexión a la red. Se podría utilizar toda la gama de direcciones (el 256) para distribuir entre todos los departamentos, pero una mejor idea sería la de la red asignado para crear cinco redes, una para el departamento. De esta manera haría un uso más óptimo de las direcciones y que también consigue cinco redes, lo que mejoraría el aislamiento, la seguridad y minimizar los posibles problemas de tráfico.

Para esto se utiliza la técnica de división en subredes. El proceso consiste en incluir en la dirección de red (además de la red ID y el ID de host) otro elemento, el ID de subred, que se obtiene por "robar" bits para el ID de host El proceso es:

1. Se calcula el número de bits necesarios para representar las 5 redes. En nuestro caso queremos 5 redes, a continuación, se necesitan 3 bits ($2^3 = 8$).
2. Comprobamos que tenemos suficientes bits para hacer frente a todos los hosts. En nuestro caso, la máscara de red es / 24, así que tenemos 8 bits para el anfitrión. De ellos nos vamos a dedicar a la subred 3, por lo que tenemos cinco bits libres para cada subred. El número de host será $2^5 = 32$, superior a los 30 que se necesita.
3. Calculamos las direcciones de las subredes (la primera dirección de cada subred). Por esta realizamos todas las combinaciones de 0 y 1 en los bits robados del huésped, dejando el resto a 0

1 En las siguientes secciones, se estudia lo que es un router NAT y

Neto (192.168.40)	subred	anfitrión	dirección de subred
11000000.10101000.001010 00.	000 00000		192.168.40.0
11000000.10101000.001010 00.	001 00000		192.168.40.32
11000000.10101000.001010 00.	010 00000		192.168.40.64
11000000.10101000.001010 00.	011 00000		192.168.40.96
11000000.10101000.001010 00.	100 00000		192.168.40.128
11000000.10101000.001010 00.	101 00000		192.168.40.160
11000000.10101000.001010 00.	110 00000		192.168.40.192
11000000.10101000.001010 00.	111 00000		192.168.40.224

- En nuestro caso sólo tenemos los primeros 5 redes

4. Calculamos la máscara de red de cada una de las subredes. Esta máscara será el mismo para todas las subredes. Para esto, se mezclan con la máscara inicial, el número de bits que han robado desde el host. En nuestro caso, será de 24 + 3.

Neto (192.168.40).	subred	anfitrión	dirección de subred
11000000.10101000.001010 00.	000 00000		192.168.40.0/27
11000000.10101000.001010 00.	001 00000		192.168.40.32/27
11000000.10101000.001010 00.	010 00000		192.168.40.64/27
11000000.10101000.001010 00.	011 00000		192.168.40.96/27
11000000.10101000.001010 00.	100 00000		192.168.40.128/27

5. Se calcula el rango de direcciones de cada red, lo que indica la dirección de difusión (el último) y la dirección de puerta de enlace (la segunda

uno). En nuestro caso tenemos 5 bits para definir los anfitriones, ($2^5 = 32$) de acogida por lo tanto, el rango de direcciones irá en bloques de 32.

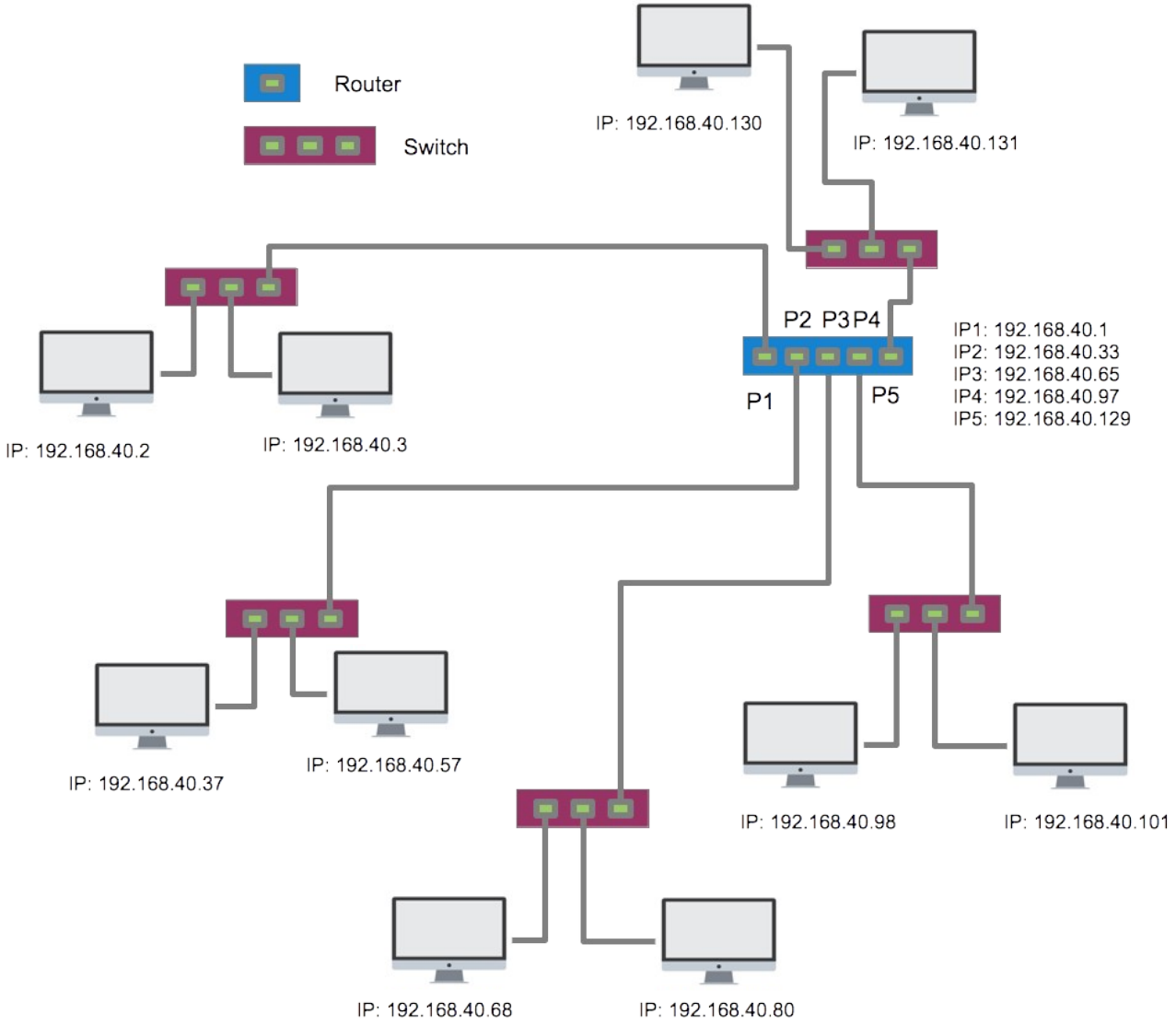
subred	rango	transmitir	puerta
192.168.40.0/27	192.168.40.0 - 192.168.40.31	192.168.40.31	192.168.40.1
192.168.40.32/2 7	192.168.40.32 - 192.168.40.63	192.168.40.63	192.168.40.33
192.168.40.64/2 7	192.168.40.64 - 192.168.40.95	192.168.40.95	192.168.40.65
192.168.40.96/2 7	192.168.40.96 - 192.168.40.127	192.168.40.12 7	192.168.40.97
192.168.40.128/ 27	192.168.40.128 - 192.168.40.159	192.168.40.15 9	192.168.40.129

En la figura 11 se puede observar el dibujo de la topología de las subredes resultantes. Para simplificar, sólo dos hosts por subred se han elaborado

4.8 enrutamiento

El enrutamiento es la técnica que le permite mover un paquete desde un ordenador a otro, incluso si pertenecen a redes diferentes. Este proceso se lleva a cabo por el router a través de las denominadas tablas de enrutamiento. De una manera muy simplificada, esta tabla se compone de 2 columnas

Objetivo	Interfaz



resultado Figura 11. Subnetting

La columna de destino se refiere a quién será el receptor del paquete. Puede ser un IP, una dirección de red o la ruta predeterminada (indicada con 0.0.0.0). La columna de interfaz se refiere a la interfaz del router[2] a través del cual el paquete tendrá que ser enviado a la dirección de destino. Por ejemplo, el enrutador de la figura anterior tiene la siguiente tabla de enrutamiento:

objetivo	Interfaz
192.168.40.0	P1
192.168.40.32	P2
192.168.40.64	P3
192.168.40.96	P4
192.168.40.128	P5

2 Un enrutador es un dispositivo que tiene como muchas interfaces como redes interconectadas.

4.9 NAT

Dada la escasez de direcciones IP, la técnica NAT permite que la información se transmite de una dirección IP pública a IPS privado y viceversa de forma transparente para el usuario.

Gracias a esta técnica, a partir de una dirección pública, el usuario puede configurar la red privada (con direcciones IP privadas y subredes) tan grandes como se desee. El router es responsable de añadir información sobre la dirección IP pública y un indicador de cuál de sus anfitriones locales se envía al paquete que va a la red externa. La respuesta a ese paquete llegará al router que será el encargado de dirigir al host local correspondiente.

4.10 IPv6

Incluso con técnicas tales como las subredes y NAT, el número de dispositivos continúa creciendo y las direcciones IP se están agotando. Para resolver este problema las organizaciones tienen crear varias soluciones al problema. Una de estas soluciones es IPv6. A diferencia de IPv4, que usa direcciones de 32 bits, IPv6 utiliza **direcciones de 128 bits, que ofrecen suficiente IP (2^{128}) direcciones.**

En este caso la notación se basa en números hexadecimales agrupados en bloques de 16 bits (de 0000 a ffff) separadas por :. Los ceros a la izquierda en cada grupo se pueden borrar y un conjunto de ceros pueden ser reemplazados por: :: sólo una vez por cada dirección. Por ejemplo, la dirección IPv6:

DE34: 0000: 0000: 0000: 045e: 0000: 0000: 0ffa

Para simplificar sería como:

DE34 :: 45e: 0: 0: FFA

Al igual que en el formato tradicional (IPv4), las tiendas de dirección del identificador de red, así como el ID de host. La única diferencia es que en la red IPv6 siempre es identificado por los primeros 64 bits, mientras que el anfitrión hace con el último 64.

ID de red: Identificación DE34 ::

Anfitrión: 45e: 0: 0: FFA

5. Hardware de red COMPONENTES

5.1 tarjeta de interfaz de red

La tarjeta de interfaz de red (NIC) es el componente de hardware que conecte el ordenador con los medios de comunicación. Todos los dispositivos conectados a una red deben tener por lo menos una [3]. Hay dos tipos, con y sin cables.

- Se trabaja en la capa de enlace

Se identifica físicamente por ID denomina dirección MAC (Media Access Control), un número único que se asigna por el fabricante y que es independiente de la pila de protocolos a utilizar. Un ejemplo podría ser 00: 35: AA: 28: 5F: 69

- Hoy en día la importancia de la conexión de red es tan grande que la mayoría de los dispositivos tienen una (ordenadores, móviles, impresoras, televisores ...)

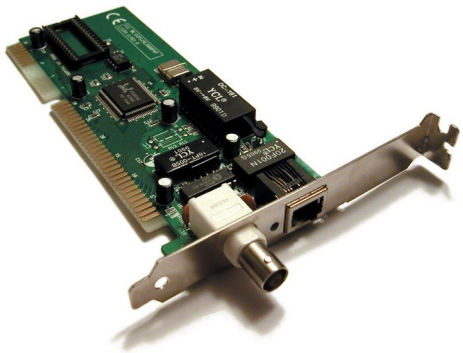


Figura 11. NIC

5.2 medios

- Ellos trabajan en la capa de enlace

5.2.1 medios guiadas

Son aquellos en los que guía el medio de la señal. Hay tres tipos: de par trenzado, coaxial y de fibra óptica.

Los pares trenzados

Están formados por dos cables de cobre. Ellos están trenzados a las interferencias evitar. Hay 3 tipos:

- ***UTP (par trenzado no apantallado).*** Ellos Don"t tienen ninguna protección adicional contra interferencias.

3 Cada uno de ellos conecta una red diferente

- ***FTP (Foiled par trenzado).*** Tiene una sola protección de malla que cubre todos los pares trenzados.

- ***STP (par trenzado apantallado).*** Cada par tiene una cubierta conductora independiente que está conectado a la conexión a tierra del equipo y mejora la protección contra interferencias.

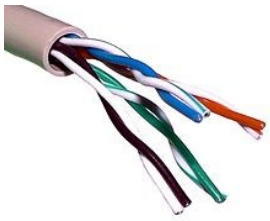


Figura 12. UTP

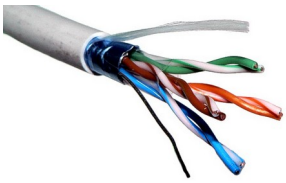


Figura 13. FTP

Figura 14. STP

- De hecho, es posible encontrar más tipos de cableado como S / UTP, S / FTP, S / STP o F / UTP. Estos nombre indica el tipo de escudo que cubre todos los cables, siendo F frustraron y S trenzadas [4].

Además, estos cables tipos también se clasifican por categorías, de 1 a 7 en función de la calidad de la misma: a más distancias de mayor calidad y mayor velocidad, pero, obviamente, más caro.

Hay dos tipos de conectores asociados con este tipo de medios, RJ-11 (usado en conexiones telefónicas y xDSL) y RJ-45 (utilizado en redes Ethernet)

Figura 15. RJ-11 y RJ-45

Coaxial

Ampliamente utilizado en redes MAN (aunque cada vez más está siendo sustituida por fibra óptica). Tiene un conductor central que transporta las señales eléctricas, un conductor externo que funciona como un escudo que protege el conductor interior contra interferencias y un dieléctrico aislar los dos cables.

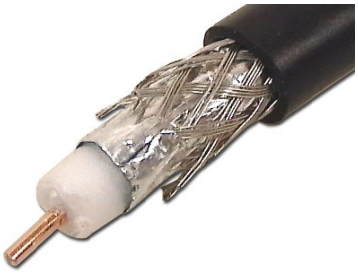


Figura 16. Coaxial

conector de la Figura 17. BNC

4 Las pantalla de hilos trenzados ofrecen mejor protección que los escudos de papel de aluminio.

El tipo de conector utilizado se llama BNC.

Fibra optica

La señal eléctrica se sustituye por señales luminosas emitidas por un láser, lo que los hace inmune a las interferencias electromagnéticas. Se componen de una chaqueta (una cubierta que aísla de la luz externa), elementos de refuerzo (añadido al cable de fibra óptica para evitar la rotura de la fibra de vidrio durante

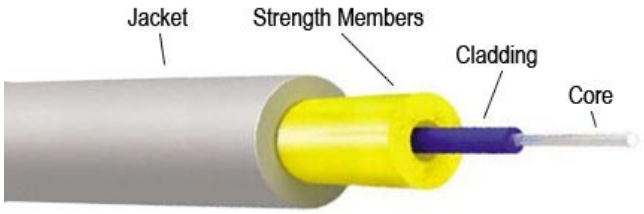


Figura 18. Coaxial

instalación), revestimiento y un núcleo.

Hay una gran cantidad de conectores: FDDI, LC, FC, SC ...

Figura 19. Conector FC

Figura 20. Conector FDDI

5.2.2 medios No guiadas

La información se envía por señales electromagnéticas que se propagan por el aire o en el espacio.

Su gran ventaja es la facilidad de instalación y su escalabilidad. Por otro lado su principal inconveniente es que están muy afectados por las condiciones atmosféricas y que su velocidad es mucho menor que en los medios guiadas.

microondas

Ejemplos típicos son Wi-Fi y Bluetooth, que funciona en las frecuencias en torno
2,4 GHz, las emisiones de TV funcionan en el rango de 50 MHz a 900 MHz o de trabajo Celulares en las frecuencias de 900 MHz, 1800 MHz and1900MHZ

Las señales infrarrojas

Están diseñados para la comunicación entre dispositivos muy cerca uno del otro y están muy afectados por externa ligero. Ejemplos típicos son remoto

controladores para la televisión.

5.3 módem

Módem es un acrónimo de modulador / demodulador. Cuando la señal se envía a través de un medio de viajar largas distancias que tiene que ser modulada [5]. Cuando esta señal llega al receptor, el proceso inverso debe ser realizado, es decir, que debe ser demodulada.

En general, es el dispositivo que permite la conexión de nuestra LAN con la red WAN o MAN que proporciona el servicio. De esta manera y en función del tipo de conexión, hay, por ejemplo, un módem por cable, módem ADSL, módem telefónico, ...

- Se trabaja en la capa de enlace

5.4 HUB

Un concentrador es un dispositivo con varios puertos de conexión y cuya tarea consiste en reenviar el paquete recibido por uno de los puertos para el resto, previamente amplificarla. A pesar de que ahora están siendo reemplazados por interruptores, se han utilizado ampliamente ya que su uso permite la creación de segmentos de red Ethernet [6].

- Si las obras en la capa de enlace

Su mayor problema es que, incluso si el remitente es solamente una computadora, la información se envía de nuevo a todos, por lo tanto, se incrementa el tráfico y la velocidad disminuye. Además de todas las tarjetas de la red en el segmento de tener que trabajar a la velocidad de la más lenta.

5.5 Interruptor

Un interruptor es un centro inteligente. El conmutador almacena una tabla con la dirección MAC del ordenador conectado a cada puerto. Cuando un paquete (mensaje) se envía desde un ordenador a otro, el interruptor retransmite el paquete sólo para el puerto de destino. Las ventajas de un interruptor en comparación con un concentrador son que evita la replicación de paquetes innecesarios y ayuda a reducir el tráfico de la red y aumenta la velocidad, y además cada dispositivo puede funcionar a una velocidad diferente. Externamente un concentrador y un conmutador son muy similares, de hecho, sólo pueden ser diferenciadas por la propia etiqueta.

Figura 21. HUB

Figura 22. Interruptor

5 https://en.wikipedia.org/wiki/Modulation

6 Dos o más ordenadores no pueden conectarse en un árbol si al menos no hay ningún elemento central, que era o bien una equipo con varias tarjetas de red o un concentrador, mucho más barato

- A pesar de que tiene algo de inteligencia, que funciona a nivel de capa de enlace, ya que no modifica ni redirigir el paquete, sólo se “abre o cierra la puerta” en función de su dirección.

5.6 Router

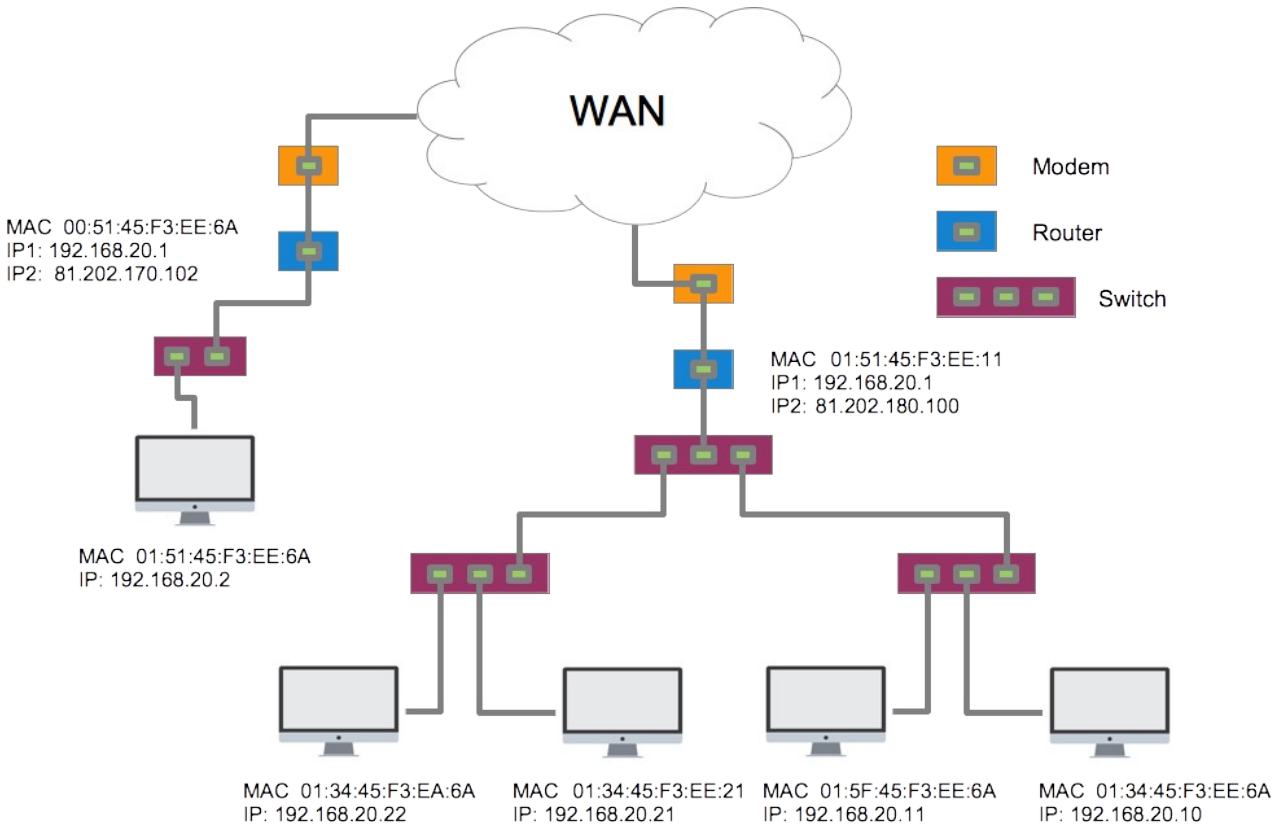
Figura 22. Router

Un router es un dispositivo mucho más inteligente que un interruptor. Funciona en la capa de Internet, por lo que entiende direcciones IP. Por lo tanto, se puede determinar el camino que un paquete debe seguir para llegar a un equipo que no está incluido en cualquier segmento de la red local. Es decir, el router es capaz de decidir si el paquete se dirige a un ordenador de la red local o en uno de la red externa y para enrutar correctamente (añadiendo la información necesaria para el paquete para que el destinatario sabe que para responder a las). Para hacerlo,

que tiene al menos dos NIC conectarse a diferentes redes (local y externa)

- Tenga en cuenta que la dirección MAC es un dato que viene de fábrica, mientras que la dirección IP es un conjunto de datos que se asignan a la tarjeta de red en función de la forma en que está conectado a la red. El MAC será siempre la misma, la dirección IP puede cambiar.

- Es muy común que en un entorno doméstico el módem y el router (e incluso el interruptor) están juntos en el mismo componente.



6. MATERIAL ADICIONAL

[1] Glosario. [2]

Ejercicios

7. BIBLIOGRAFÍA

[1] Informátcos Sistemas. Isabel Jiménez Ma Cumbreras. Garceta. 2012 [2] Las redes de ordenadores. S. Tanenbaum Andrew. Pearson. 2010 La licencia de componentes de hardware imágenes son:

- Licencia CC BY-SA 3.0. Autor: Wikipedia