Unidad didáctica 09:
Sistemas Informáticos:
Redes (II)

Sumario

1. Introducción

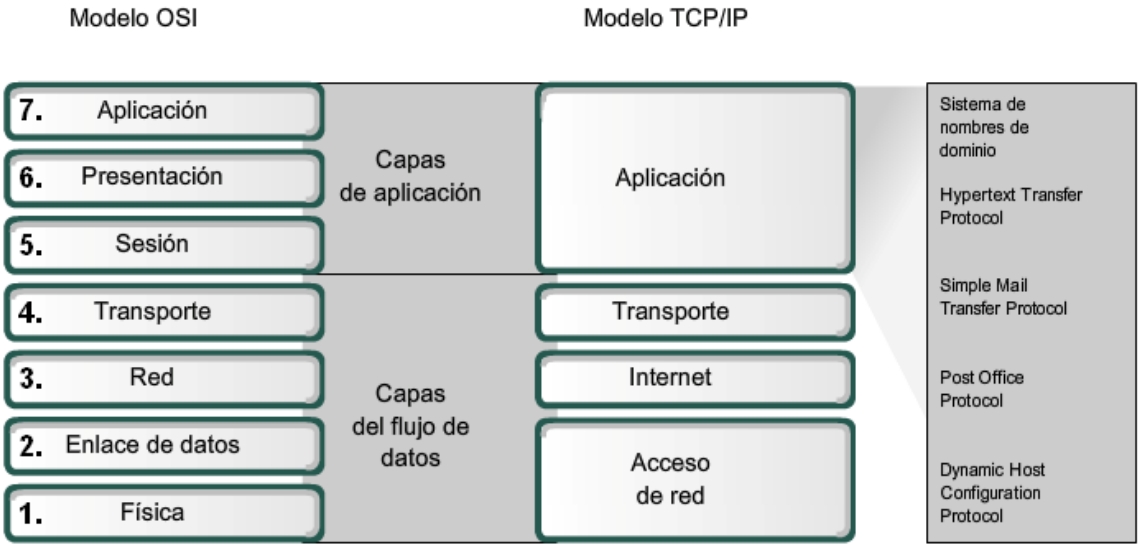
En este tema vamos a estudiar los protocolos que rigen las comunicaciones de las redes locales a distintos niveles: nivel de red, nivel de transporte y nivel de aplicación.

1.1. ¿Qué es un protocolo?

Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

1.2. La familia de protocolos TCP/IP

Cabe decir, que TCP/IP no sigue la arquitectura de OSI. La familia de protocolos TCP está formada por un conjunto de protocolos de los que cabe destacar los protocolos IP y TCP. El protocolo IP estaría englobado en el nivel de red, y el protocolo TCP en la capa de transporte.



Estudiaremos los siguientes protocolos:

Capa de Acceso al medio: Ethernet
Capa Internet (Red): IP, ARP, RARP, e ICMP.
Capa de transporte: Protocolos TCP y UDP.
Capa de aplicación: Protocolos DNS, WINS, SMTP, POP3/IMAP, FTP, DHCP, SMB, TELNET, y SSH.

2. EL protocolo IPv4

IP (Internet Protocol), protocolo entre redes. Es un protocolo no orientado a conexión, cuya versión actual es la cuatro (IPv4). La unidad de datos del protocolo se llama **datagrama** o **paquete IP**.

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.

Las tres direcciones siguientes representan a la misma máquina (podemos utilizar cualquier calculadora binaria online para realizar las conversiones).

(decimal) 128.10.2.30 = (binario) 10000000.00001010.00000010.00011110

2.1. Direcciones IP.

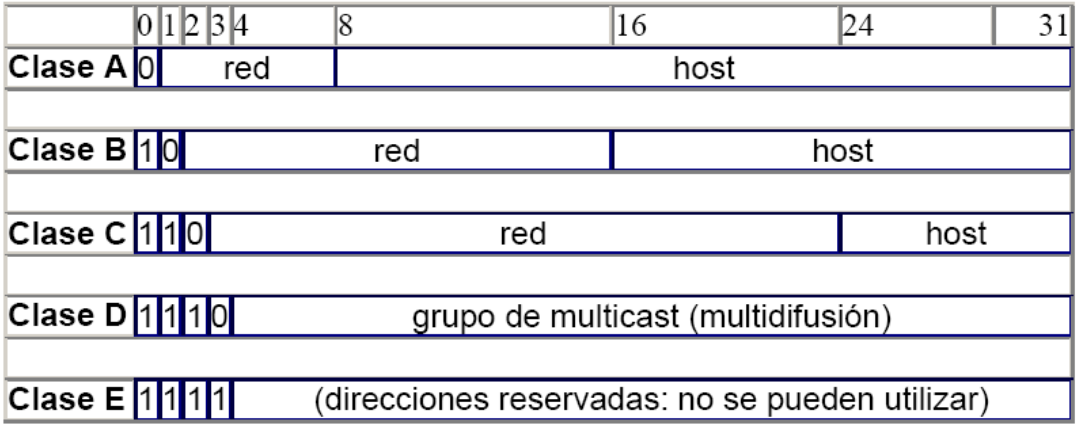
La dirección IP es el identificador de cada host en Internet. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Conversión Binaria a Decimal
Suma las posiciones si tienen un 1. Valores: 128 64 32 16 8 4 2 1
Ejemplo: 1 0 0 0 0 1 1 0 = 128+4+2=134
Conversión Decimal a Binario
Ir restando las potencias de 2 (128, 64, 32, 16, 8, 4, 2, 1).Si lo puedes restar 1 sino 0
Ejemplo 132: 132-128=4, 4-4=0 1 0 0 0 0 1 0 0
O divisiones sucesivas entre 2 y coger el ultimo cociente y todos los restos.

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el identificador de red y el identificador de host.

1.1. Clases

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las **clases primarias A, B y C**. La **clase D** está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de **clase E** no se pueden utilizar (están reservadas).



Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	Máscara de subred
A	r.h.h.h	128	16.777.214	0.0.0.0-127.0.0.0	255.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0-191.255.0.0	255.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0-223.255.255.0	255.255.255.0
D	Multi difusión	-	-	224.0.0.0-239.255.255.255	-
E	No validas	-	-	240.0.0.0-255.255.255.255	-

Nota: Las direcciones usadas en Internet están definidas en la RFC 1166 (en inglés).

Difusión (broadcast) se refiere a todos los hosts de una red.

Multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión para referirse a un único host.

1.2. Direcciones IP especiales y reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Dirección por defecto	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
red	todos 0	Nombre de la Red	192.168.1.0
red	todos 1	Difusión en mi red	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1
todos 1		Difusión	255.255.255.255

Difusión o *broadcasting* es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de *loopback* (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (*intranets*). Una dirección IP que pertenezca a una de estas redes se dice que es una *dirección IP privada*.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Las direcciones IP se clasifican en:

- **Direcciones IP públicas**. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas** (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- **Direcciones IP estáticas** (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- **Direcciones IP dinámicas**. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

1.3. Máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Ejemplo: Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

IP: 148.120.33.110 = 10010100.01111000.00100001.01101110
<------RED------> <------HOST----->
Mascara 255.255.0.0 = 11111111.11111111.00000000.00000000

Nombre de Red: copia la parte de red y el resto de bits a 0.

148.120.0.0 10010100.01111000.00000000.00000000
<------RED------> <------HOST----->

Dirección Broadcast o Difusión: copia la parte de red y el resto de bits a 1.

148.120.255.255 10010100.01111000.11111111.11111111
<------RED------> <------HOST----->

Ejemplo: Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

IP: 148.120.33. 89 = 10010100.01111000.00100001.01011001
<------RED------> <------HOST----->
Mascara 255.255.0.0 = 11111111.11111111.00000000.00000000

Dirección de su subred 148.120.0.0 10010100.01111000.00000000.00000000

En cambio, si tomamos la 148.115.89.3, observamos que **no** pertenece a la misma subred que las anteriores.

IP: 148.115.89.3 = 10010100.01110011.01011001.00000011
<------RED------> <------HOST----->
Mascara 255.255.0.0 = 11111111.11111111.00000000.00000000

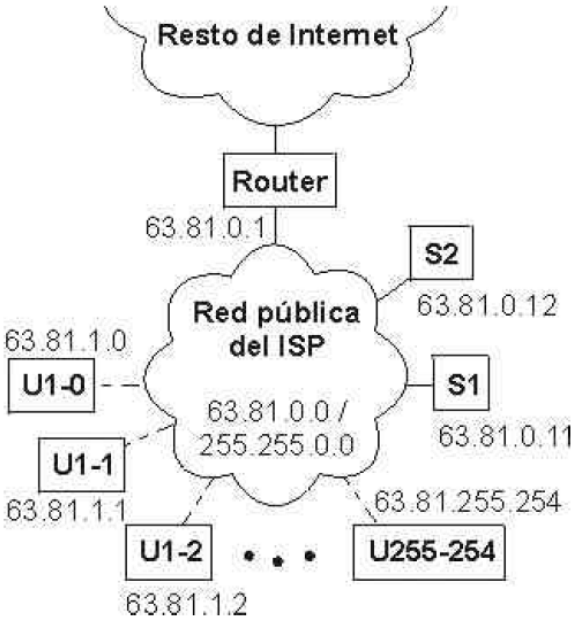
Dirección de su subred 148.115.0.0 10010100.01110011.00000000.00000000

En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un ordenador sabe si otro ordenador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

EJEMPLO.- Los proveedores de Internet habitualmente disponen de una o más redes públicas para dar acceso a los usuarios que se conectan por módem. El proveedor va cediendo estas direcciones públicas a sus clientes a medida que se conectan y liberándolas según se van desconectando (direcciones dinámicas). Supongamos que cierto ISP (proveedor de servicios de Internet) dispone de la red 63.81.0.0 con máscara

255.255.0.0. Para uso interno utiliza las direcciones que comienzan por 63.81.0 y para ofrecer acceso a Internet a sus usuarios, las direcciones comprendidas entre la 63.81.1.0 hasta la 63.81.1.254 (las direcciones 63.81.0.0 y 63.81.255.255 están reservadas).

Si un usuario conectado a la red de este ISP tiene la dirección 63.81.1.1 y quiere transferir un archivo al usuario con IP 63.81.1.2, el primero advertirá que el destinatario se encuentra en su misma subred y el mensaje no saldrá de la red del proveedor (no atravesará el router).



Subredes

Debido a la poca flexibilidad del sistema de clases desde comienzos de los años 90 se ha venido utilizando el esquema CIDR (encaminamiento Inter.-Dominios sin Clases) para el direccionamiento en Internet. CIDR se basa en el concepto de subred y mascaras de subred.

Una subred es una parte de una red que se identifica por si sola.

Por ejemplo en una oficina en una red corporativa de un banco. A nivel de direccionamiento las subredes son paritciones jerárquicas del espacio de direcciones, que incorporan el término dirección de subred y un número de estaciones.

Las subredes se suelen especificar mediante la denominada mascara de subred que indica el número de bits empleado para la dirección de red y subred. Veamos un ejemplo:

Dirección IP: 193.16.11.230/27 (macara de subred)

Identificación de red: 24 bits (193.16.11)

Identificación de subred: 3 bits (8 subredes)

Identificación de estación: 5 bits (32 estaciones en cada subred)

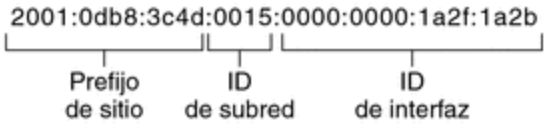
Decimal:	193.	16.	11.	230
Binario:	11000001	00010000	00001011	11100110

La utilización de subredes tiene la ventaja de hacer las redes más manejables y utilizar protocolos de encaminamiento sin clases. De esta forma el esquema CIDR utiliza mascaras de subred de tamaño variable (VLSM) para la asignación de direcciones. CIDR permite la agregación de subredes en redes mayores, proceso conocido como supernetting (proceso inverso al subnetting).

1.4. El protocolo IPv6

IPv6 es el protocolo introducido para solucionar el problema de agotamiento de direcciones IP que se prevé en un futuro cercano. Una dirección IPv6 consta de 128 bits y la ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Representado con números hexadecimales, agrupados de 4 en 4, separados por comas, por ejemplo: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b.



Como hoy en día tenemos tantos dispositivos que se conectan a Internet, nos estamos quedando sin IPv4 para asignar. Por eso, las direcciones IPv6 tienen 128 bits, agrupados en números hexadecimales (0,1,2,3,4,5,6,7,8,9, A,B,C,D,E,F)

Ejemplo: 2001:0000:00AB:CF00:1234:0000:1234:0023

Las IPv6 como son tan largas se suelen omitir los ceros

- Se quitan los 0 por la izquierda en cada :
- Se agrupa SOLO UNA VEZ todos los 0 y se pone ::

Ejemplo: 2001:0000:0000:0000:0000:0000:1234:0023

2001:0 :0 :0 :0 :0 :1234:23

2001 : : 1234:23

Ejemplo: 2001:0000:0001:0000:0000:0000:1234:0023

2001:0 :1 : : 1234:23

Cambios de hexadecimal a binario y viceversa.

Hexadecimal a binario

Recuerda que para pasar de hexadecimal a coges cada cifra y la sustituyes por su valor en binario.

Ejemplo: $2222_{16} = 10\ 0010\ 0010\ 0010_2$

Binario a hexadecimal

Agrupa desde la derecha de 4 en 4. Sustituye dependiendo de la posición por 8421 cuando tengas un 1 y sumas.

Ejemplo: $1001\ 0101\ 1010\ 0001_2 = ¿?_{16}$

8+1 4+1 8+2 1 $9\ 5\ A\ 1_{16}$

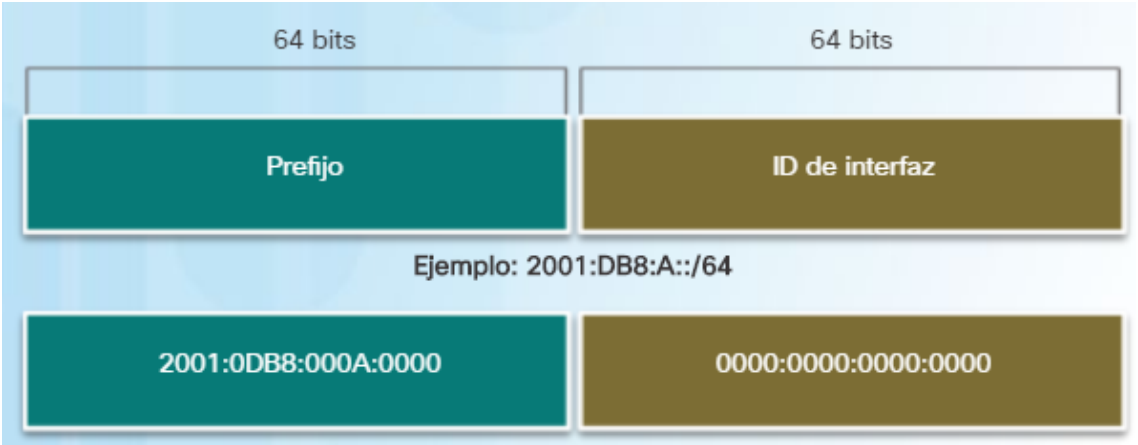
Ejercicios

a) $56B6_{16} = 0101\ 0110\ 1011\ 0110_2$
b) $89F5_{16} = 1000\ 1001\ 1111\ 0101_2$
c) $1010\ 0111\ 1011\ 0011_2 = A\ 7\ B\ 3_{16}$
d) $0110\ 1100\ 0101\ 1000_2 = 6C58_{16}$

Máscaras de IPv6

NO se escriben como en IPv4 255.255.255.0

Sino que se indica /64 (64 unos que indican la parte de red)



En IPv4 existe:

- Unicast: 1 destinatario
- Multicast: varios destinatarios
- Broadcast o difusión: todos los de la RED

Tipos de direcciones IPv6

- Unidifusión
  - **Unidifusión global** como las IP públicas de IPv4
  - **Link-local** como las IP privada de IPv4, solo en mi red.

El siguiente cuadro, resultará útil para identificar los diferentes tipos de direcciones IPv6 según los números en el primer hexteto.

Primer hexteto (extremo izquierdo)	Tipo de dirección IPv6
De 0000 a 00FF	Dirección de bucle invertido, cualquier dirección, dirección no especificada o compatible con IPv4
De 2000 a 3FFF	Dirección de unidifusión global (una dirección enrutable en un intervalo de direcciones que actualmente se encuentra bajo la responsabilidad de la Internet Assigned Numbers Authority [IANA])
De FE80 a FEBF	Link-local (una dirección de unidifusión que identifica el equipo host en la red local)
De FC00 a FCFF	Local única (una dirección de unidifusión que puede asignarse a un host para identificarlo como parte de una subred específica en la red local)
De FF00 a FFFF	Dirección de multidifusión

Coexistencia IPv4 e IPv6

- Dual-stack: el sistema soporta IPv4 e IPv6
- Tunelización: utiliza túneles en las redes IPv4
- Traducción: traduce con NAT 64 de IPv4 a IPv6 y viceversa

1.5. ICMP

Sirve para hacer **ping,** con la información de respuesta podemos detectar errores.

- **Confirmación de host**: está conectado y funciona
- **Destino o servicio inaccesible:** o no esta enchufado o no está configurado bien.

Información que muestra:

TTL: Time To Live, por cuantos routers va a pasar un paquete hasta que se elimine.

Para **comprobar** si he conectado bien una **tarjeta de red** y tiene los drivers:

Hacer un ping a mi mismo: **ping 127.0.0.1** (127.0.0.1-127.255.255.254) IPv4

ping ::1 IPv6

Cuando **configuramos** un **equipo** debemos indicar:

- La **IP** que lo identifica
- La **máscara** de esa red
- La puerta de enlace o **Gateway** que va a ser la dirección del router que tiene conectado.

2. Protocolo ICMP

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje.

Nota: *El protocolo ICMP está definido en la RFC 792*

El protocolo se compone de un conjunto de mensajes de contar a los que responden los enrutadores. La utilidad **ping** se utiliza para determinar la conectividad IP entre dispositivos.

Sintaxis: ping 192.168.1.1 [- nº de paquetes]

- **Respuesta**. El cableado entre A y B, las tarjetas de red de A y B, y la configuración IP de A y B están correctos.
- **Tiempo de espera agotado**. Comprobar el host B y el cableado entre A y B.
- **Host de destino inaccesible**. Comprobar las direcciones IP y máscaras de subred de A y B porque no pertenecen a la misma red.
- **Error**. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar A>ping 127.0.0.1 para asegurarse.

3. ARP (Address Resolution Protocol)

El protocolo ARP para redes IPv4 es uno de los protocolos fundamentales de Internet y de las redes locales. Este protocolo también trabaja junto con el protocolo IP para **mapear direcciones IP en relación a las direcciones de hardware** utilizados por un protocolo de enlace datos. A estas direcciones de hardware se las denominan **direcciones MAC**. Estas direcciones sirven de código de identificación para cada una de las interfaces de red de los dispositivos. ARP opera en el medio de la capa de red y la capa de acceso al medio (si consideramos al modelo TCP/IP). Este protocolo se aplica cuando se utiliza el protocolo IP sobre Ethernet.

4. Protocolos de la capa de transporte

4.1. Transmission Control Protocol (TCP)

TCP es el aliado de IP para garantizar que los datos se transmiten de manera adecuada a través de Internet. Su función principal es a**segurar que el tráfico llegue a destino de una manera confiable.** Esta característica de confiabilidad no es posible lograrla únicamente mediante IP. Otras funciones de TCP son:

- Que no se pierdan los paquetes de datos.

- Control del orden de los paquetes de datos.
- Control de una posible saturación que se llegue a experimentar.
- Prevención de duplicado de paquetes.

4.1.1. El uso de puertos

Diversos programas TCP/IP pueden ejecutarse simultáneamente en Internet (por ejemplo, se puede navegar por páginas HTML mientras se hace una videoconferencia). Cada uno de estos programas funciona con un protocolo. A veces el equipo debe poder distinguir las diferentes fuentes de datos.

Por lo tanto, para facilitar este proceso, a cada una de estas aplicaciones puede serle asignada una dirección única en equipo, codificada en 16 bits: **un puerto** (por consiguiente, la combinación de dirección IP + puerto es una dirección única en el mundo denominada socket).

De esta manera, la dirección IP sirve para identificar de manera única un equipo en la red mientras que el **número de puerto especifica la aplicación a la que se dirigen los datos**. Así, cuando el equipo recibe información que va dirigida a un puerto, los datos se envían a la aplicación relacionada. Si se trata de una solicitud enviada a la aplicación, la aplicación se denomina aplicación servidor. Si se trata de una respuesta, entonces hablamos de una aplicación cliente.

Existen miles de puertos (codificados en 16 bits, es decir que se cuenta con 65.536 posibilidades). Es por ello que la IANA (Internet Assigned Numbers Authority [Agencia de Asignación de Números de Internet]) desarrolló una aplicación estándar para ayudar con las configuraciones de red.

Los puertos del 0 al 1.023 on los puertos conocidos o reservados. En términos generales, están reservados para procesos del sistema (daemons) o programas ejecutados por usuarios privilegiados. Sin embargo, un administrador de red puede conectar servicios con puertos de su elección. Los puertos del 1.024 al 49.151 son los puertos registrados. Los puertos del 49.152 al 65.535 son los puertos dinámicos y/o privados.

A continuación se indican algunos de los puertos conocidos más utilizados:

Puerto	Servicio o aplicación
21	FTP
23	Telnet
25	SMTP
53	Sistema de nombre de dominio. DNS.
63	Whois
79	Finger
80	HTTP
110	POP3

Por lo tanto, un servidor (un equipo conectado que ofrece servicios como FTP, Telnet, etc.) cuenta con números de puerto fijos a los cuales el administrador de red conecta los servicios. Entonces, los puertos del servidor generalmente se encuentran entre 0 y 1.023 (rango de valores relacionado con servicios conocidos).

Del lado del cliente, el sistema operativo elige el puerto entre aquellos que están disponibles de forma aleatoria. Por lo tanto, los puertos del cliente nunca incluirán los puertos que se encuentran entre 0 y 1.023, ya que este rango de valores representa a los puertos conocidos.

4.2. User Datagram Protocol (UDP)

A diferencia del protocolo TCP, UDP no es tan confiable. Este no cuenta con posibilidad de realizar revisiones en búsqueda de errores o correcciones de transmisiones de datos. Sin embargo, hay ciertas aplicaciones en donde UDP es más factible de utilizar en vez de TCP. Un ejemplo de esto es una sesión de juegos en línea, en donde UDP permite que los paquetes de datos se descarten sin posibilidad de reintentos.

Lo malo es que este protocolo no es recomendado para realizar transferencia de datos. Ya que si algunos paquetes se pierden durante el proceso de transferencia, el resultado final es que el archivo se corrompe, y las capas superiores (capa de aplicación) es quien debe realizar la solicitud para que se vuelva a enviar el datagrama de nuevo. Un archivo corrupto no puede ser utilizado para el fin por el cual fue enviado. Igualmente, para este escenario de juegos en línea o sesiones de streaming de vídeos, UDP es el protocolo recomendado.

5. Protocolos de la capa de aplicación

5.1. Hypertext Transfer Protocol (HTTP)

Es el protocolo que permite que los **navegadores y servidores web se comuniquen adecuadamente**. Este es utilizado por navegadores web para solicitar archivos HTML de parte de los servidores remotos. Así, los usuarios podrán interactuar con dichos archivos mediante la visualización de las páginas web que cuentan con imágenes, música, vídeos, texto, etc.

El protocolo HTTP tiene como base a TCP, el cual implementa un modelo de comunicación cliente-servidor. Existen varios tipos de mensajes que HTTP utiliza, siendo dos los más usados:

- HTTP GET: Se envía un mensaje al servidor que contiene una URL con o sin parámetros. El servidor responde retornando una página web al navegador, el cual es visible por el usuario solicitante.

- HTTP POST: Se envía un mensaje al servidor que contiene datos en la sección «body» de la solicitud. Esto se hace para evitar el envío de datos a través de la propia URL, algo sí como sucede con HTTP GET.

No debemos olvidar el protocolo HTTPS, el cual nos proporciona seguridad punto a punto (entre el cliente y el servidor web). El protocolo HTTPS utiliza el protocolo TLS (Transport Layer Security) que también utiliza TCP por encima.

5.2. Domain Name System (DNS)

Es el servicio encargado de **traducir/interpretar nombres de dominio a direcciones IP**. Recordemos que los nombres de dominio se constituyen en base a caracteres alfabéticos (letras),

los cuales son más fáciles de recordar. Para el usuario, es más fácil recordar un nombre que una serie numérica de cierta longitud. Sin embargo, Internet en general funciona en gran parte mediante las direcciones de IP. Siempre y cuando introduzcas un nombre de dominio en tu navegador, un servicio DNS recibe esa información para interpretarla y permitir la visualización de la página web deseada.

Tengamos presente que cuando contratamos un servicio de Internet, este nos provee la conectividad mediante sus propios servidores DNS. Sin embargo, es posible optar por DNS alternativos tanto para conectarnos desde el ordenador como nuestro móvil.

5.3. File Transfer Protocol (FTP)

El protocolo FTP es utilizado para compartir archivos entre dos ordenadores. Así como el protocolo HTTP, FTP implementa el modelo cliente-servidor. Para que se pueda ejecutar FTP, se debe lanzar el cliente FTP y conectar a un servidor remoto que cuente con un software del mismo protocolo. Una vez que la conexión se ha establecido, se deben descargar los archivos elegidos de parte del servidor FTP.

Por otro lado, el protocolo TFTP fue diseñado para dispositivos con menor capacidad. Sus siglas corresponden a Trivial File Transfer Protocol. Este provee un uso básico que contiene solamente las operaciones elementales de FTP. Este protocolo se suele utilizar para cargar los firmwares en routers y switches gestionables, ya que es un protocolo muy simple de comunicación.

6. Protocolos de la capa de aplicación orientados al correo electrónico

Los protocolos que citaremos a continuación, también interactúan con IP y con TCP. Una de las razones de ser del mundo corporativo es el correo electrónico. Día tras día, nos llegan mensajes, los respondemos y ese ciclo se repite un gran número de veces. Sin embargo, ¿tenemos idea de cómo se llevan a cabo las conexiones? ¿Cómo es posible visualizar los correos y a su vez, mantener una copia de los mismos en nuestro ordenador?

6.1. Post-Office Protocol Version 3 (POP3)

Es un protocolo estándar de Internet es utilizado por los distintos clientes de correo electrónico. se utiliza para poder recibir correos de parte de un servidor remoto a través de una conexión TCP/IP. Haciendo un poco de historia, POP3 fue concebido por primera vez en el año 1984 y se ha vuelto uno de los más populares. Es utilizado por prácticamente el total de los clientes de correo electrónico conocidos, es simple de configurar, operar y mantener.

En la mayoría de los casos, los servidores de correo electrónico son ofrecidos y alojados por parte de los ISP. En este caso, dicho proveedor debe facilitarte los datos para poder configurar correctamente tu cliente de correo electrónico. A parte de visualizar los mensajes, es posible descargar una copia de los mismos y mantenerlos en nuestro ordenador. **Una vez que se descargan los mensajes, estos ya desaparecen de parte del servidor remoto.** Sin embargo, existen casos en los que los usuarios configuran que los correos se mantengan en el servidor por un período determinado de tiempo.

El número de puerto TCP utilizado normalmente por parte de POP3 es el **110**. Si es que la comunicación cifrada está disponible, los usuarios pueden escoger conectarse mediante el comando STLS (TLS seguro) o bien, utilizando POP3S (POP3 seguro). Este último puede valerse de TLS o SSL en el puerto TCP 995 para conectarse al servidor de correo.

6.2. Internet Message Access Protocol (IMAP)

Es un estándar para el acceso a correos electrónicos alojados en un servidor web, mediante un cliente de correo electrónico local. Para establecer las conexiones de comunicación, utiliza el protocolo de la capa de transporte TCP. Lo cual permite el uso de un servidor remoto de correo electrónico. Ahora bien, el puerto utilizado para IMAP es el **143**. Tiene utilidades y características similares a POP3.

Una consideración importante es que IMAP es protocolo para servidores remotos de archivos, a diferencia de aquellos que se valen del protocolo POP3, el cual permite el almacenamiento de dichos mensajes. En otras palabras, **gracias a IMAP los mensajes de correo electrónico se mantienen en el servidor hasta que el usuario decide borrarlos.** Por otro lado, este protocolo permite la administración de una sola cuenta de correo electrónico de parte de más de un cliente.

Cuando un usuario solicita el acceso a un mensaje de correo electrónico, dicha solicitud se encamina a través de un servidor central. Algunos de los beneficios del protocolo IMAP consisten en la posibilidad de borrar los mensajes del servidor y la búsqueda mediante palabras clave entre los mensajes que se encuentran en nuestro buzón. Por tanto, se puede crear y administrar múltiples buzones y/o carpetas, y la visualización de vistas previas de los mensajes.

6.3. Simple Mail Transfer Protocol (SMTP)

Este protocolo, así como los que hemos citado anteriormente, es considerado como uno de los servicios más valiosos de Internet. La mayoría de los sistemas que funcionan a través de Internet se valen de SMTP como un método para **enviar/transferir correos electrónicos.**

El cliente que quiere enviar un correo electrónico, establece una conexión TCP al servidor SMTP. Después, envía el mensaje a través de dicha conexión. El servidor siempre está en modo listening. Tan pronto se hace eco de una conexión TCP, el proceso SMTP inicia una conexión mediante su puerto asignado que es el número **25**. Una vez que se haya establecido exitosamente una conexión TCP, el cliente procede al envío automático del correo electrónico.