



Universidad Simón Bolívar
Laboratorio F
Laboratorio Docente de Computación

Protocolos de Internet

(ARP,RARP,TCP/IP)

Daniela A. Torres Faría
daniela@ldc.usb.ve

Valle de Sartenejas, 11 de Junio de 2009

Índice

1. Introducción	4
2. Historia	4
3. Mapeo de Direcciones de Internet a Direcciones Físicas (ARP)	5
3.1. Comportamiento	5
3.2. Formato de ARP	6
4. Determinación de una Dirección Física (RARP)	7
5. Protocolo de Internet (IP)	7
5.1. Direcciones IP	8
5.2. Datagramas	8
6. Protocolo de Envío controlado de Mensajes (ICMP)	9
6.1. Formato y Encapsulamiento	10
7. Protocolo de Control de Transmision (TCP)	10
7.1. Principales Características	10
7.2. Funciones Principales	11
7.3. Confiabilidad de las transferencias	13
7.4. Cómo establecer una conexión	13
7.5. Como terminar una conexion.	14
8. Protocolos por Capas: Modelo de Referencia OSI	14
8.1. Niveles del Modelo OSI	15
9. Modelo TCP/IP por capas	17
9.1. Capa de acceso a la red	18
9.2. Capa de Internet	18
9.3. Capa de transporte	18
9.4. Capa de aplicación	19
10.Subredes (Subnetting)	19
10.1. Funcionamiento	19
11.Máscaras de Subred	20
11.1. Funcionamiento	20
12.Enrutamiento (Directo e Indirecto)	20
12.1. Tablas de Enrutamiento	21

1. Introducción

Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras, para que esta comunicación se pueda dar de manera correcta es necesario que las computadoras dominen el mismo protocolo entre ellas, de esta idea nacen los llamados protocolos de internet, los cuales son un conjunto de protocolos de red en los que esta basado internet y permiten la transmisión de datos entre computadoras.

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI (Open System Interconnection), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), el cual se utiliza para acceder a las páginas web, ARP (Address Resolution Protocol) cuya función es la resolución de direcciones,FTP (File Transfer Protocol) para transferencia de archivos,SMTTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para la transmisión de correo electrónico.

TCP/IP es el principal protocolo utilizado para la comunicación mediante internet, su nombre se debe a que esta compuesto por dos importantes protocolos: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), los cuales fueron los primeros en definirse, además de ser los más utilizados de la familia.Podemos agregar que TCP/IP es un conjunto de aplicaciones utilizadas para la comunicaciones, transmisión de datos, manejo de redes de área local e intranets orientado a sistemas UNIX.TCP/IP es el responsable de la fundación y establecimiento de la Internet.

2. Historia

La Familia de Protocolos de Internet fueron el resultado del trabajo llevado a cabo por la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA por sus siglas en inglés) a principios de los 70. Después de la construcción de la pionera ARPANET en 1969 DARPA comenzó a trabajar en un gran número de tecnologías de transmisión de datos.

Para el verano de 1973, Robert E. Kahn quien trabajo en la comunicación de paquetes por satélite y por ondas de radio para DARPA y Vint Cerf desarrollador del protocolo de ARPANET, Network Control Program(NPC),quienes se unieron para crear una arquitectura abierta de interconexión y diseñar así la nueva generación de protocolos de ARPANET, habían conseguido una remodelación fundamental, donde las diferencias entre los protocolos de red se ocultaban usando un Protocolo de comunicaciones y además, la red dejaba de ser responsable de la fiabilidad de la comunicación, como pasaba en ARPANET , era el host el responsable. Cerf reconoció el mérito de Hubert Zimmerman y Louis Pouzin, creadores de la red CYCLADES, ya que su trabajo estuvo muy influenciado por el diseño de esta red.

Con el papel que realizaban las redes en el proceso de comunicación reducido al mínimo, se convirtió en una posibilidad real comunicar redes diferentes, sin importar las características que estas tuvieran esto se lograba mediante un ordenador denominado router (un nombre que fue después cambiado a gateway, puerta de enlace, para evitar confusiones con otros tipos de Puerta de enlace) esta dotado con una interfaz para cada red, y envía Datagrama de ida y vuelta entre ellos.

Esta idea fue llevada a la práctica de una forma mas detallada por el grupo de investigación que Cerf tenía en Stanford durante el periodo de 1973 a 1974, dando como resultado la primera especi-

cación TCP. Entonces DARPA fue contratada por BBN Technologies, la Universidad de Stanford, y la University College de Londres para desarrollar versiones operacionales del protocolo en diferentes plataformas de hardware. Se desarrollaron cuatro versiones diferentes: TCP v1, TCP v2, una tercera dividida en dos TCP v3 y IP v3 en la primavera de 1978, y después se estabilizó la versión TCP/IP v4 — el protocolo estándar que todavía se emplea en Internet actualmente.

En 1975, se realizó la primera prueba de comunicación entre dos redes con protocolos TCP/IP entre la Universidad de Stanford y la University College de Londres(UCL). En 1977, se realizó otra prueba de comunicación con un protocolo TCP/IP entre tres redes distintas con ubicaciones en Estados Unidos, Reino Unido y Noruega. Varios prototipos diferentes de protocolos TCP/IP se desarrollaron en múltiples centros de investigación entre los años 1978 y 1983. La migración completa de la red ARPANET al protocolo TCP/IP concluyó oficialmente el día 1 de enero de 1983 cuando los protocolos fueron activados permanentemente.[5]

En marzo de 1982, el Departamento de Defensa de los Estados Unidos declaró al protocolo TCP/IP el estándar para las comunicaciones entre redes militares

3. Mapeo de Direcciones de Internet a Direcciones Físicas (ARP)

El protocolo ARP (address resolution protocol) es el encargado de “traducir” las direcciones IP de 32 bits a las correspondientes direcciones de hardware, las cuales suelen tener 48 bits. En una sola red, los hosts individuales se conocen a través de su dirección física, los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (en este caso la dirección IP), cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, el manejador de dispositivo no la entiende, en consecuencia, se suministra un módulo (ARP) que traducirá la dirección IP a las dirección física del host de destino; esta utiliza una tabla (llamada a veces caché ARP) para realizar la traducción. Cuando la dirección no se encuentra en la caché ARP, se envía un broadcast en la red, con un formato especial llamado petición ARP, si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una respuesta ARP al host que la solicitó, la cual contendrá la dirección física del hardware así como información de direccionamiento (si el paquete ha atravesado puentes durante su trayecto). Tanto esta dirección como la ruta se almacenan en la caché del host solicitante y todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el manejador de dispositivo para mandar el datagrama a la red.

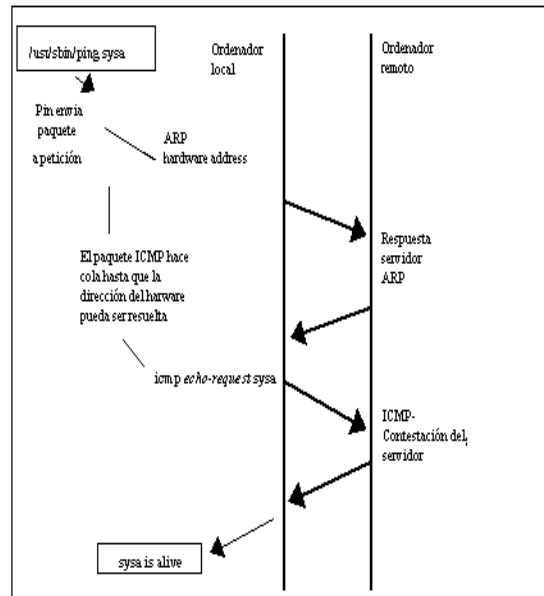
ARP se utiliza en cuatro casos referentes a la comunicación entre dos hosts:

1. Dos hosts están en la misma red y uno quiere enviar un paquete a otro.
2. Dos host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
3. Un router necesita enviar un paquete a un host a través de otro router.
4. Un router necesita enviar un paquete a un host de la misma red.

3.1. Comportamiento

El protocolo ARP se puede comportar de dos maneras distintas dependiendo de si el los host se encuentran o no dentro de la misma red. Si los host se encuentran en la misma red el que desea enviar el paquete mirará su tabla ARP para poner en la trama la dirección destino física correspondiente a la IP del receptor. De esta forma, cuando llegue a todos los host no habrá que deshacer la trama para comprobar si el mensaje es para los demas.

Si los host están en redes diferentes el mensaje deberá salir de la red. Así, el host emisor envía la trama a la dirección física de salida del router, esta dirección física la obtendrá a partir de la IP del router, utilizando la tabla ARP, si la entrada no está en la tabla, mandará un mensaje ARP a esa IP (llegará a todos los host), para que le conteste indicándole su dirección física. Una vez en el router, éste consultará su tabla de direccionamiento, obteniendo el próximo nodo para llegar al destino, y saca el mensaje por el interfaz correspondiente. El proceso se repite por todos los nodos, hasta llegar al último router, que es el que comparte el medio con el host destino. Luego el proceso cambia, la interfaz del router tendrá que encontrar la dirección física de la IP destino que se le ha solicitado, mediante la tabla ARP, y en caso de no existir la entrada correspondiente a la IP, la obtiene realizando una multidifusión.



3.2. Formato de ARP

Cuando una solicitud ARP viaja de una máquina a otra deben ser enviados en marcos o tramas físicas. Para identificar el marco como una solicitud ARP o una respuesta ARP el emisor asigna un valor especial al campo "tipo" en el header del marco y coloca el cuerpo del mensaje en el campo "data" del marco. Cuando un marco llega a un host, el sistema examina el tipo del marco para determinar que contiene.

A diferencia de la mayoría de los protocolos, los datos en los paquetes ARP no tienen un formato establecido definido. En vez, el mensaje está diseñado para ser útil en una variedad de tecnologías de red.

0	8	16	24	31
TIPO DE HARDWARE		TIPO DE PROTOCOLO		
HLEN	PLEN	OPERACION		
SENDER HA (octeto 0 - 3)				
SENDER HA (OCTETO 4 - 5)		SENDER IP (OCTETO 0 - 1)		
SENDER IP (OCTETO 2 - 3)		TARGET HA (OCTETO 0 - 1)		
TARGET HA (octeto 2 - 5)				
TARGET IP (octeto 0 - 3)				

4. Determinación de una Dirección Física (RARP)

El protocolo RARP es utilizado para resolver la dirección IP de una dirección hardware dada, realiza la traducción inversa ARP de allí proviene su nombre (Reverse Address Resolution Protocol) La resolución de direcciones inversa se lleva a cabo de la misma manera que la resolución de direcciones de ARP. El mismo formato de paquete que usa ARP. Una excepción es el campo de "tipo" que ahora toma el valor correspondiente a la operación inversa.

Características Principales

- ARP asume únicamente que cada host sabe la correspondencia existente entre su propia dirección hardware y la dirección de protocolo. RARP requiere uno o más hosts de servidores de la red para mantener una base de datos de correspondencias entre direcciones hardware y direcciones de protocolo así que serán capaces de responder a peticiones de hosts de clientes.
- Debido al tamaño que esta base de datos puede tomar, parte de la función del servidor se implementa con frecuencia fuera del microcódigo del adaptador, con una caché pequeña opcional en el microcódigo. La parte de microcódigo es responsable únicamente de la recepción y transmisión de las tramas RARP, la propia correspondencia RARP está a cargo del software del servidor que se ejecute como un proceso normal en la máquina.
- La naturaleza de esta base de datos también requiere algún software para crear y actualizar manualmente la base de datos.
- En caso de haya múltiples servidores RARP en la red, el solicitante RARP sólo usará la primera respuesta RARP recibida en su respuesta RARP broadcast, y descartarán las otras.

5. Protocolo de Internet (IP)

Protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de como estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes (switches) y los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

5.1. Direcciones IP

Se refiere a un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo dentro de una red que utilice el protocolo de Internet (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Un usuario que se conecta a Internet utiliza una dirección IP, esta dirección puede cambiar al reconectar, y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica.

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija, es decir, no cambia con el tiempo. Los servidores de correo, dns, ftp públicos, servidores web, necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se facilita su ubicación. Las máquinas tienen una gran facilidad para manipular y jerarquizar la información numérica, y son altamente eficientes para hacerlo y ubicar direcciones IP. Sin embargo, los seres humanos debemos utilizar otra notación más fácil de recordar y utilizar; tal es el caso URLs y resolución de nombres de dominio DNS.

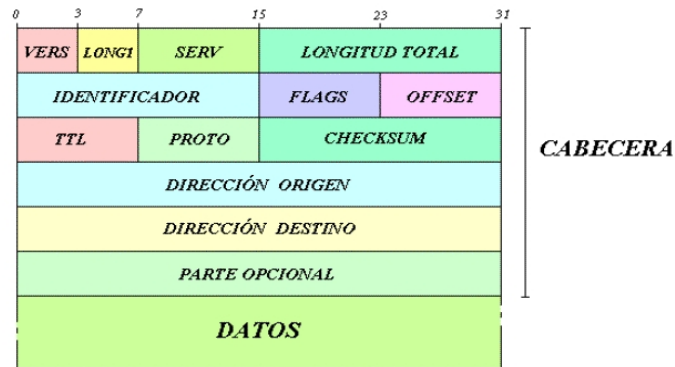
5.2. Datagramas

Fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes.

Los datagramas IP son las unidades principales de información de Internet. Los términos trama, mensaje, paquete y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Un datagrama tiene una cabecera de IP que contiene información de direcciones. Los encaminadores examinan la dirección de destino de la cabecera de IP, para dirigir los datagramas al destino.

Formato de un Datagrama



6. Protocolo de Envío controlado de Mensajes (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. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:

Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Tipos de mensaje ICMP

Tipo	Tipo de Mensaje
0	Respuesta de Eco
3	Destino Inalcanzable
4	Origen saturado
5	Redireccion (cambiar ruta)
8	Solicitud de eco
11	Tiempo excedido para un datagrama
13	Problema de parametros en un datagrama
13	Solicitud de fecha y hora
14	Respuesta de fecha y hora
17	Solicitud de mascara de direccion
18	Respuesta de mascara de direccion

6.1. Formato y Encapsulamiento

La encapsulación del mensaje del ICMP es dos - doble el proceso. Los mensajes se encapsulan en los datagramas del IP, que se encapsulan en marcos, pues viajan a través del Internet. Básicamente, el ICMP utiliza los mismos medios de comunicaciones no fiables que un datagrama. Esto significa que los mensajes de error del ICMP pueden ser perdidos o ser duplicados.

El formato del ICMP incluye un tipo de mensaje campo, indicando el tipo de mensaje; un campo del código que incluye la información detallada sobre el tipo; y un campo de la suma de comprobación, que proporciona la misma funcionalidad que la suma de comprobación del IP. Cuando un mensaje del ICMP divulga un error, incluye el jefe y los datos del datagrama que causó el problema especificado. Esto ayuda a la estación de recepción a entender qué uso y protocolo envió el datagrama. (la sección siguiente tiene más información sobre tipos de mensaje del ICMP.)

ICMP no incluye control de flujo o la recuperación de error, y así que puede ser duplicado fácilmente.

7. Protocolo de Control de Transmision (TCP)

Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

7.1. Principales Características

- Protocolo orientado a conexión. Es decir, las aplicaciones solicitan la conexión al destino y luego usan esa conexión para entregar los datos, garantizando que estos serán entregados sin problemas.
- Una conexión TCP tiene dos extremos, emisor y receptor. Confiabilidad. TCP garantiza que los datos transferidos serán entregados sin ninguna pérdida, duplicación o errores de transmisión.
- Los extremos que participan en una conexión TCP pueden intercambiar datos en ambas direcciones simultáneamente.
- Conexión de inicio confiable. Garantiza una conexión de inicio confiable y sincronizada entre los dos extremos de la conexión.
- Conexión de finalización aceptable. TCP garantiza la entrega de todos los datos antes de la finalización de la conexión.

7.2. Funciones Principales

- Asociar puertos con conexiones.
- Realizar un arranque lento para evitar sobrecargas.
- Dividir los datos en segmentos para su transmisión.
- Numerar los datos.
- Manejar los segmentos entrantes duplicados.
- Calcular las sumas de control.
- Regular el flujo de datos usando las ventanas de envío y recepción.
- Terminar las conexiones de manera ordenada.
- Abortar conexiones.
- Marcar datos urgentes.
- Confirmación positiva de retransmisión.
- Calculo de los plazos de retransmisión.
- Reducir el trafico cuando la red se congestiona
- Indicar los segmentos que llegan en desorden.
- Comprobar si las ventanas de recepción están cerradas.

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores. Esto significa que los routers (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Por eso es que decimos que estamos en un entorno Cliente-Servidor. Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Otra función del TCP es la capacidad de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman segmentos.

Funcion Multiplexión

TCP posibilita la realización de una tarea importante: multiplexar/demultiplexar; es decir transmitir datos desde diversas aplicaciones en la misma línea o, en otras palabras, ordenar la información que llega en paralelo. Estas operaciones se realizan empleando el concepto de puertos (o conexiones), es decir, un número vinculado a un tipo de aplicación que, cuando se combina con una dirección de IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.

Formato de los datos

Un segmento TCP está formado de la siguiente manera:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Puerto de origen																Puerto de destino															
Número de secuencia																															
Número de acuse de recibo																															
Margen de datos				Reservado						URG	ACK	PSH	RST	SYN	FIN	Ventana															
Suma de control																Puntero urgente															
Opciones																						Relleno									
Datos																															

Significado de los campos

- Puerto de origen (16 bits): Puerto relacionado con la aplicación en curso en la máquina origen
- Puerto de destino (16 bits): Puerto relacionado con la aplicación en curso en la máquina destino
- Número de secuencia (32 bits): Cuando el indicador SYN está fijado en 0, el número de secuencia es el de la primera palabra del segmento actual.
- Cuando SYN está fijado en 1, el número de secuencia es igual al número de secuencia inicial utilizado para sincronizar los números de secuencia (ISN).
- Número de acuse de recibo (32 bits): El número de acuse de recibo, también llamado número de descarga se relaciona con el número (secuencia) del último segmento esperado y no el número del último segmento recibido.
- Margen de datos (4 bits): Esto permite ubicar el inicio de los datos en el paquete. Aquí, el margen es fundamental porque el campo opción es de tamaño variable.
- Reservado (6 bits): Un campo que actualmente no está en uso pero se proporciona para el uso futuro.
- Indicadores (6x1 bit): Los indicadores representan información adicional:
 - URG: Si este indicador está fijado en 1, el paquete se debe procesar en forma urgente.
 - ACK: Si este indicador está fijado en 1, el paquete es un acuse de recibo.
 - PSH (PUSH): Si este indicador está fijado en 1, el paquete opera de acuerdo con el método PUSH.
 - RST: Si este indicador está fijado en 1, se restablece la conexión.
 - SYN: El indicador SYN de TCP indica un pedido para establecer una conexión.
 - FIN: Si este indicador está fijado en 1, se interrumpe la conexión.
- Ventana (16 bits): Campo que permite saber la cantidad de bytes que el receptor desea recibir sin acuse de recibo.
- Suma de control (CRC): La suma de control se realiza tomando la suma del campo de datos del encabezado para poder verificar la integridad del encabezado.

- Puntero urgente (16 bits): Indica el número de secuencia después del cual la información se torna urgente.
- Opciones (tamaño variable): Diversas opciones
- Relleno: Espacio restante después de que las opciones se rellenan con ceros para tener una longitud que sea múltiplo de 32 bits.

7.3. Confiabilidad de las transferencias

El protocolo TCP permite garantizar la transferencia de datos confiable, a pesar de que usa el protocolo IP, que no incluye ningún monitoreo de la entrega de datagramas.

De hecho, el protocolo TCP tiene un sistema de acuse de recibo que permite al cliente y al servidor garantizar la recepción mutua de datos. Cuando se emite un segmento, se lo vincula a un número de secuencia. Con la recepción de un segmento de datos, la máquina receptora devolverá un segmento de datos donde el indicador ACK esté fijado en 1 (para poder indicar que es un acuse de recibo) acompañado por un número de acuse de recibo que equivale al número de secuencia anterior.

Además, usando un temporizador que comienza con la recepción del segmento en el nivel de la máquina originadora, el segmento se reenvía cuando ha transcurrido el tiempo permitido, ya que en este caso la máquina originadora considera que el segmento está perdido.

Sin embargo, si el segmento no está perdido y llega a destino, la máquina receptora lo sabrá, gracias al número de secuencia, que es un duplicado, y sólo retendrá el último segmento que llegó a destino.

7.4. Cómo establecer una conexión

Considerando que este proceso de comunicación, que se produce con la transmisión y el acuse de recibo de datos, se basa en un número de secuencia, las máquinas originadora y receptora (cliente y servidor) deben conocer el número de secuencia inicial de la otra máquina.

La conexión establecida entre las dos aplicaciones a menudo se realiza siguiendo el siguiente esquema:

- Los puertos TCP deben estar abiertos.
- La aplicación en el servidor es pasiva, es decir, que la aplicación escucha y espera una conexión.
- La aplicación del cliente realiza un pedido de conexión al servidor en el lugar donde la aplicación es abierta pasiva. La aplicación del cliente se considera "abierta activa".

Las dos máquinas deben sincronizar sus secuencias usando un mecanismo comúnmente llamado negociación en tres pasos que también se encuentra durante el cierre de la sesión.

Este diálogo posibilita el inicio de la comunicación porque se realiza en tres etapas, como su nombre lo indica:

En la primera etapa, la máquina originadora (el cliente) transmite un segmento donde el indicador SYN está fijado en 1 (para indicar que es un segmento de sincronización), con número de secuencia N llamado número de secuencia inicial del cliente.

En la segunda etapa, la máquina receptora (el servidor) recibe el segmento inicial que viene del cliente y luego le envía un acuse de recibo, que es un segmento en el que el indicador ACK está fijado en 1 y el indicador SYN está fijado en 1 (porque es nuevamente una sincronización). Este segmento incluye el número de secuencia de esta máquina (el servidor), que es el número de secuencia inicial

para el cliente. El campo más importante en este segmento es el de acuse de recibo que contiene el número de secuencia inicial del cliente incrementado en 1.

Por último, el cliente transmite un acuse de recibo, que es un segmento en el que el indicador ACK está fijado en 1 y el indicador SYN está fijado en 0 (ya no es un segmento de sincronización). Su número de secuencia está incrementado y el acuse de recibo representa el número de secuencia inicial del servidor incrementado en 1.

Después de esta secuencia con tres intercambios, las dos máquinas están sincronizadas y la comunicación puede comenzar.

Existe una técnica de piratería llamada falsificación de IP, que permite corromper este enlace de aprobación con fines maliciosos.

7.5. Como terminar una conexión.

El cliente puede pedir que se termine una conexión del mismo modo que el servidor. Para terminar una conexión se procede de la siguiente manera:

- Una de las máquinas envía un segmento con el indicador FIN fijado en 1, y la aplicación se autocoloca en estado de espera, es decir que deja de recibir el segmento actual e ignora los siguientes.
- Después de recibir este segmento, la otra máquina envía un acuse de recibo con el indicador FIN fijado en 1 y sigue enviando los segmentos en curso. Después de esto, la máquina informa a la aplicación que se ha recibido un segmento FIN y luego envía un segmento FIN a la otra máquina, que cierra la conexión.

8. Protocolos por Capas: Modelo de Referencia OSI

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con estos lineamientos, OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

Estructura multinivel: Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas.

El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

Puntos de acceso: Entre los diferentes niveles existen interfaces llamadas "puntos de acceso." a los servicios.

Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.

Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje esta constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

Unidades de información: En cada nivel, la unidad de información tiene diferente nombre y estructura.

8.1. Niveles del Modelo OSI

1. Aplicación:

- Proporciona servicios al usuario del Modelo OSI.
- Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
- Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), etc.

2. Presentación:

- Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.
- Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
- Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
- Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Opera la visualización.

3. Sesión:

- Provee los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.
- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.
- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

4. Transporte: Actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a el procesamiento. Además:

- Garantiza una entrega confiable de la información.
- Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).

- Define como direccionar la localidad física de los dispositivos de la red.
- Asigna una dirección única de transporte a cada usuario.
- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío del mensaje.
- Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

5. **Red:**

- Define el enrutamiento y el envío de paquetes entre redes.
- Tiene la responsabilidad establecer, mantener y terminar las conexiones.
- Proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
- Conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
- Define el estado de los mensajes que se envían a nodos de la red.

6. **Enlace de datos:** Proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red, es decir, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información, esto tiene los siguientes objetivos:

- Detectar errores en el nivel físicos
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes además de realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.

En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

7. **Físico.** Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

- Definir conexiones físicas entre computadoras.
- Describir el aspecto mecánico de la interface física.
- Describir el aspecto eléctrico de la interface física.
- Describir el aspecto funcional de la interface física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.
- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

9. Modelo TCP/IP por capas

El objetivo de un sistema en capas es dividir el problema en diferentes partes (las capas), de acuerdo con su nivel de abstracción.

Cada capa del modelo se comunica con un nivel adyacente (superior o inferior). Por lo tanto, cada capa utiliza los servicios de las capas inferiores y se los proporciona a la capa superior.

El modelo TCP/IP, influenciado por el modelo OSI, también utiliza el enfoque modular (utiliza módulos o capas), pero sólo contiene cuatro:

1. Capa de acceso a la red
2. Capa de internet
3. Capa de transporte
4. Capa de aplicación

Como puede apreciarse, las capas del modelo TCP/IP tienen tareas mucho más diversas que las del modelo OSI, considerando que ciertas capas del modelo TCP/IP se corresponden con varios niveles del modelo OSI.

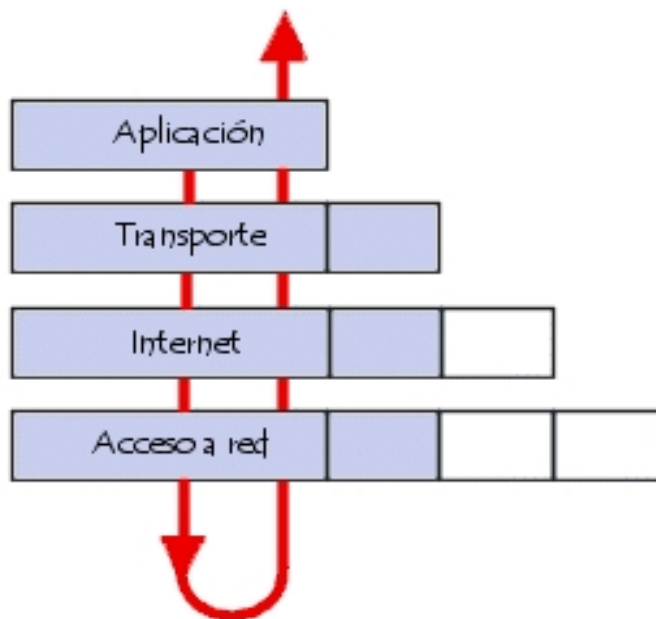
Las funciones de las diferentes capas son las siguientes:

1. Capa de acceso a la red: especifica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado;
2. Capa de Internet: es responsable de proporcionar el paquete de datos (datagrama);
3. Capa de transporte: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión;
4. Capa de aplicación: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

Durante una transmisión, los datos cruzan cada una de las capas en el nivel del equipo remitente. En cada capa, se le agrega información al paquete de datos. Esto se llama encabezado, es decir, una recopilación de información que garantiza la transmisión. En el nivel del equipo receptor, cuando se atraviesa cada capa, el encabezado se lee y después se elimina. Entonces, cuando se recibe, el mensaje se encuentra en su estado original.

En cada nivel, el paquete de datos cambia su aspecto porque se le agrega un encabezado. Por lo tanto, las designaciones cambian según las capas:

- El paquete de datos se denomina mensaje en el nivel de la capa de aplicación;
- El mensaje después se encapsula en forma de segmento en la capa de transporte;
- Una vez que se encapsula el segmento en la capa de Internet, toma el nombre de datagrama;
- Finalmente, se habla de trama en el nivel de capa de acceso a la red.



9.1. Capa de acceso a la red

La capa de acceso a la red es la primera capa de la pila TCP/IP. Ofrece la capacidad de acceder a cualquier red física, es decir, brinda los recursos que se deben implementar para transmitir datos a través de la red. Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una red de área local (Red en anillo, Ethernet, FDDI), conectada mediante línea telefónica u otro tipo de conexión a una red.

9.2. Capa de Internet

La capa de Internet es la capa "más importante", ya que es la que define los datagramas y administra las nociones de direcciones IP. Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben.

9.3. Capa de transporte

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones. De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, etc. Además, el nombre de la aplicación puede variar de sistema en sistema. Es por ello que se ha implementado un sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se denominan puertos.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores).

9.4. Capa de aplicación

Se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo.

10. Subredes (Subnetting)

Para conseguir mayor funcionalidad podemos dividir nuestra red en subredes dividiendo en dos partes el número de host, una para identificar la subred, y la otra parte para identificar la máquina (subnetting). Esto lo decidirá el responsable de la red sin que intervenga el NIC. La idea es tomar una parte de red de una dirección de IP y asignar las direcciones IP de esa parte de red a varias redes físicas, que serán ahora referidas como subredes.

El mecanismo con el cual se puede lograr compartir un número de red (parte de red) entre distintas redes involucra la configuración de todos los nodos en cada subred con una máscara de red, la misma para todos los nodos dentro de una subred. Con las máscaras de redes se logra jerarquizar aún más la estructura jerárquica de un IP, que como se dijo antes está constituida por (parte de red) + (parte de host), incluyendo un nuevo nivel de jerarquía que llamaremos (número de subred). Como ya se sabe, todos los hosts en una misma red tienen la misma (parte de red), pero ahora todos los hosts en la misma red física tendrán el mismo (número de subred), lo que hace que los hosts en la misma red, pero en distintas redes físicas compartan la (parte de red) pero no el (número de subred), y esto como se puede notar ayuda notablemente en la transmisión de información, pues se complementa las tablas de direccionamiento con otro campo que ayudará a mejorar la eficiencia de envío de paquetes.

Supongamos que se quiere dividir una red Clase B en varias redes. Podríamos utilizar una máscara de red de la forma 255.255.255.0 (lo que pasado a binario son 1s en los primeros 24 bits y 0s en los últimos 8). Por lo tanto podríamos pensar que ahora los primeros 24 bits de una dirección IP representan la (parte de red) y los últimos 8 la (parte de host). Como los primeros 16 bits identifican una red Clase B, podemos pensar que la dirección no tiene dos sino tres partes: la (parte de red) + (parte de subred) + (parte de host).

10.1. Funcionamiento

Lo que subnetting significa para un host es que ahora está configurado con una dirección IP y una máscara de red para la subred a la cual se encuentra conectado. Cuando un host quiere enviar un paquete a una cierta dirección IP, lo primero que hace es realizar una operación de Y (AND) de bits entre su propia máscara de red y la dirección de destino. Si el resultado es igual al número de subred del host que envía el paquete, entonces sabe que el host de destino está en la misma subred y el paquete de entregado directamente a través de la subred. Si el resultado no es igual, el paquete necesita ser enviado a un router para ser enviado desde este a otra subred. Así como el trabajo de envío de un host cambia en una subred, también el trabajo de un router se ve afectado cuando se introduce la implementación de subnetting. Normalmente para satisfacer la estructura jerárquica de (parte de red) + (parte del host) el router tiene una tabla de direccionamiento la cual está formada por campos de la forma (número de red, próximo salto). Para soportar subnetting la tabla deberá estar conformada por entradas de la forma (número de subred, máscara de subred, próximo salto). Para encontrar el lugar correcto en la tabla el router aplica una operación AND entre la dirección de destino del paquete y la correspondiente máscara de subred para cada una de las entradas y cada vez revisa si el resultado al

número de subred de la entrada en turno. Si esto sucede entonces esa es la entrada correcta a utilizar y el router envía el paquete al router o host especificado en el campo proximo salto.

11. Máscaras de Subred

Es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

11.1. Funcionamiento

Básicamente, mediante la máscara de red una computadora (principalmente la puerta de enlace, router...) podrá saber si debe enviar los datos dentro o fuera de la red. Por ejemplo, si el router tiene la ip 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras ips, para fuera (internet, otra red local mayor...).

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. También se puede escribir como 10.0.0.0/8

Como la máscara consiste en una seguidilla de unos consecutivos, y luego ceros (si los hay), los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254, y 255.

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados por las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.00000000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

Una máscara de red representada en binario son 4 octetos de bits.

12. Enrutamiento (Directo e Indirecto)

Los routers son dispositivos que permiten "elegir" la ruta que tomarán los datagramas para llegar a destino. Son equipos con diversas tarjetas de interfaz de red, cada una conectada a una red distinta. Entonces, en la configuración más simple, el router sólo tiene que "mirar" qué red se encuentra un equipo para enviarle datagramas desde el remitente.

Sin embargo, en Internet el esquema es mucho más complicado dado que un router generalmente está conectado a una gran cantidad de redes y dichas redes pueden conectarse a otras redes, que el router no puede ver directamente.

Por lo tanto, los routers funcionan con tablas y protocolos, según el siguiente modelo:

1. El router recibe una trama de un equipo conectado a una de las redes a las que está conectado;
2. Los datagramas se envían en la capa IP;
3. El router se fija en el encabezado del datagrama;
4. Si la dirección IP de destino pertenece a una de las redes a las que una de las interfaces del router está conectada, la información debe enviarse en la capa 4, después de que el encabezado IP haya sido desencapsulado (eliminado).

5. Si la dirección IP de destino es parte de una red distinta, el router consulta su tabla de enrutamiento, la cual establece la ruta a tomar para una determinada dirección;
6. El router envía el datagrama, utilizando la tarjeta de interfaz de red conectada a la red por la que el router decide enviar el paquete.

Entonces, tenemos dos situaciones. Si el remitente y el destinatario pertenecen a la misma red, hablamos de entrega directa. Pero, si hay al menos un router entre el remitente y el destinatario, hablamos de entrega indirecta.

En el caso de una entrega indirecta, la función del router y, en particular, la de la tabla de enrutamiento es muy importante. Por lo tanto, el funcionamiento de un router está determinado por el modo en el que se crea esta tabla de enrutamiento.

- Si el administrador introduce manualmente la tabla de enrutamiento, es un enrutamiento estático (adecuado para redes pequeñas).
- Si el router construye sus propias tablas de enrutamiento, utilizando la información que recibe a través de los protocolos de enrutamiento, es un enrutamiento dinámico.

12.1. Tablas de Enrutamiento

La tabla de enrutamiento es una tabla de conexiones entre la dirección del equipo de destino y el nodo a través del cual el router debe enviar el mensaje. En realidad es suficiente que el mensaje se envíe a la red en la que se encuentra el equipo. Por lo tanto, no es necesario almacenar la dirección IP completa del equipo: sólo necesita almacenarse el identificador de red de la dirección IP (es decir, la identificación de la red).

Con esta tabla, y si el router conoce la dirección del destinatario encapsulada en el mensaje, podremos descubrir a través de qué interfaz enviar el mensaje (se debe conocer qué tarjeta de interfaz de red usar) y a qué router, directamente accesible en la red a la que la tarjeta está conectada, enviar el datagrama. Este mecanismo que sólo consiste en conocer la dirección de la próxima conexión hacia el destino se denomina próximo salto.

Sin embargo, puede suceder que el destinatario pertenezca a una red a la que no se hace referencia en la tabla de enrutamiento. En este caso, el router utiliza un router predeterminado (también denominado pasarela predeterminada).

Por lo tanto, el mensaje se envía de router a router a través de sucesivos saltos, hasta que el destinatario pertenezca a una red directamente conectada a un router. Éste, entonces, envía el mensaje directamente al equipo de destino.

En el caso de enrutamiento estático, es el administrador quien actualiza la tabla de enrutamiento. En el caso de enrutamiento dinámico, existe un protocolo denominado protocolo de enrutamiento que permite la actualización automática de la tabla para que contenga la ruta óptima en cualquier momento.

13. Glosario

- Protocolo: Conjunto de normas y procedimientos útiles para la transmisión de datos, conocido por el emisor y el receptor.
- Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican mediante una dirección de broadcast.
- Gateway : 1. Puerta de enlace, acceso, pasarela. Nodo en una red informática que sirve de punto de acceso a otra red. 2. Dispositivo dedicado a intercomunicar sistemas con protocolos incompatibles. Se trata de un intermediario entre ambos para poder comunicarlos.
- Router: Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Referencias

- [1] http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet
- [2] <http://e-articles.info/t/i/1954/1/es/>
- [3] <http://es.kioskea.net/contents/internet/icmp.php3>
- [4] <http://www.profesores.frc.utn.edu.ar/sistemas/ingsanchez/Redes/Archivos/datagramaIP.asp>
- [5] <http://www.monografias.com/trabajos7/protoip/protoip.shtml>
- [6] <http://es.kioskea.net/contents/internet/tcpip.php3>
- [7] <http://es.kioskea.net/contents/internet/routage.php3>
- [8] <http://es.kioskea.net/contents/internet/tcp.php3>
- [9] <http://es.kioskea.net/contents/internet/ip.php3>
- [10] <http://medusa.unimet.edu.ve/electrica/fpie43/introsub.html>
- [11] <http://www.gestiopolis.com/recursos6/Docs/Ger/sistemas-de-informacion-tcp.htm>
- [12] http://es.wikipedia.org/wiki/Modelo_OSI
- [13] http://www.webopedia.com/quick_ref/OSI_Layers.asp