

RFC: 791

INTERNET PROTOCOL
(Protocolo Internet)

DARPA INTERNET PROGRAM

ESPECIFICACION del PROTOCOLO

Septiembre 1981
(Traducción al castellano: Mayo 1999)
(Por: Pedro J. Ponce de León <pjleon@arrakis.es>)

preparado para

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

por

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

INDICE

PREFACIO	iii
1. INTRODUCCION	1
1.1 Motivación	1
1.2 Ámbito	1
1.3 Interfaces	1
1.4 Operación	2
2. PANORAMA GENERAL	5
2.1 Relación con Otros Protocolos	9
2.2 Modelo de Operación	5
2.3 Descripción de Funciones	7
2.4 Pasarelas ("Gateways")	9
3. ESPECIFICACION	11
3.1 Formato de Cabecera Internet	11
3.2 Discusión	23
3.3 Interfaces	31
APENDICE A: Ejemplos y Escenarios	34
APENDICE B: Orden de Transmisión de Datos	39
GLOSARIO	41
REFERENCIAS	45

PREFACIO

Este documento especifica el Protocolo Internet Estándar del DoD (N.T.: Department of Defense, USA). Este documento está basado en seis ediciones anteriores de la Especificación del Protocolo Internet de ARPA, y el presente texto se basa en gran medida en ellas. Han habido muchos colaboradores en este trabajo en términos de conceptos y texto. Esta edición revisa aspectos de direccionamiento, tratamiento de errores, códigos de opción, y de las características de seguridad, prioridad, compartimientos y manejo de restricciones del protocolo Internet.

Jon Postel

Editor

RFC: 791
Sustituye a: RFC 760
IENs 128, 123, 111,
80, 54, 44, 41, 28, 26

PROTOCOLO INTERNET

DARPA INTERNET PROGRAM ESPECIFICACION DE PROTOCOLO

1. INTRODUCCION

1.1. Motivación

El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes. A un sistema de este tipo se le conoce como "catenet" [1]. El protocolo internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet también se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

1.2. Ambito

El Protocolo Internet está específicamente limitado a proporcionar las funciones necesarias para enviar un paquete de bits (un datagrama internet) desde un origen a un destino a través de un sistema de redes interconectadas. No existen mecanismos para aumentar la fiabilidad de datos entre los extremos, control de flujo, secuenciamiento u otros servicios que se encuentran normalmente en otros protocolos host-a-host. El protocolo internet puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio.

1.3. Interfaces

Este protocolo es utilizado por protocolos host-a-host en un entorno internet. Este protocolo utiliza a su vez protocolos de red locales para llevar el datagrama internet a la próxima pasarela ("gateway") o host de destino.

Por ejemplo, un módulo TCP llamaría al módulo internet para tomar un segmento TCP (incluyendo la cabecera TCP y los datos de usuario) como

la parte de datos de un datagrama internet. El módulo TCP suministraría las direcciones y otros parámetros de la cabecera internet al módulo internet como argumentos de la llamada. El módulo internet crearía entonces un datagrama internet y utilizaría la interfaz de la red local para transmitir el datagrama internet.

En el caso de ARPANET, por ejemplo, el módulo internet llamaría a un módulo de red local el cual añadiría el encabezado 1822 [2] al datagrama internet creando así un mensaje ARPANET a transmitir al IMP. La dirección ARPANET sería deducida de la dirección internet por la interfaz de la red local y sería la dirección de algún host en ARPANET, el cual podría ser una pasarela a otras redes.

1.4. Operación

El protocolo internet implementa dos funciones básicas: direccionamiento y fragmentación.

Los módulos internet usan las direcciones que se encuentran en la cabecera internet para transmitir los datagramas internet hacia sus destinos. La selección de un camino para la transmisión se llama encaminamiento.

Los módulos internet usan campos en la cabecera internet para fragmentar y reensamblar los datagramas internet cuando sea necesario para su transmisión a través de redes de "trama pequeña".

El modelo de operación es que un módulo internet reside en cada host involucrado en la comunicación internet y en cada pasarela que interconecta redes. Estos módulos comparten reglas comunes para interpretar los campos de dirección y para fragmentar y ensamblar datagramas internet. Además, estos módulos (especialmente en las pasarelas) tienen procedimientos para tomar decisiones de encaminamiento y otras funciones.

El protocolo internet trata cada datagrama internet como una entidad independiente no relacionada con ningún otro datagrama internet. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo).

El protocolo internet utiliza cuatro mecanismos clave para prestar su servicio: Tipo de Servicio, Tiempo de Vida, Opciones, y Suma de Control de Cabecera.

El Tipo de Servicio se utiliza para indicar la calidad del servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet. Esta indicación de tipo de servicio

será usada por las pasarelas para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o la siguiente pasarela al encaminar un datagrama internet.

El Tiempo de Vida es una indicación de un límite superior en el periodo de vida de un datagrama internet. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado. Si el tiempo de vida se reduce a cero antes de que el datagrama llegue a su destino, el datagrama internet es destruido. Puede pensarse en el tiempo de vida como en un plazo de autodestrucción.

Las Opciones proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y encaminamiento especial.

La Suma de Control de Cabecera proporciona una verificación de que la información utilizada al procesar el datagrama internet ha sido transmitida correctamente. Los datos pueden contener errores. Si la suma de control de cabecera falla, el datagrama internet es descartado inmediatamente por la entidad que detecta el error.

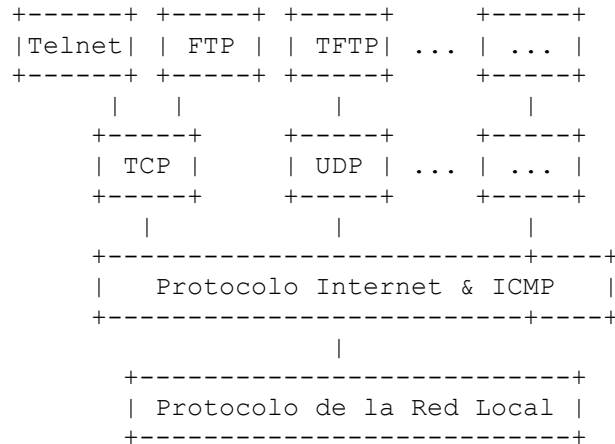
El protocolo internet no proporciona ningún mecanismo de comunicación fiable. No existen acuses de recibo ni entre extremos ni entre saltos. No hay control de errores para los datos, sólo una suma de control de cabecera. No hay retransmisiones. No existe control de flujo.

Los errores detectados pueden ser notificados por medio del Internet Control Message Protocol (ICMP) (Protocolo de Mensajes de Control de Internet) [3] el cual está implementado en el módulo del protocolo internet.

2. PANORAMA GENERAL

2.1. Relación con Otros Protocolos

El siguiente diagrama ilustra el lugar del protocolo internet en la jerarquía de protocolos:



Relación entre Protocolos

Figura 1.

El protocolo Internet interactúa por un lado con los protocolos host-a-host de alto nivel y por otro con el protocolo de la red local. En este contexto una "red local" puede ser una pequeña red en un edificio o una gran red como ARPANET.

2.2. Modelo de Operación

El modelo de operación para transmitir un datagrama de una aplicación a otra se ilustra en el siguiente escenario:

Suponemos que esta transmisión involucra a una pasarela intermedia.

La aplicación remitente prepara sus datos y llama a su módulo internet local para enviar esos datos como un datagrama y pasa la dirección de destino y otros parámetros como argumentos de la llamada.

El módulo internet prepara una cabecera de datagrama y adjunta los datos a él. El módulo internet determina una dirección de la red de área local para esta dirección internet, que en este caso es la dirección de una pasarela.

Envía este datagrama y la dirección de red local a la interfaz de red local.

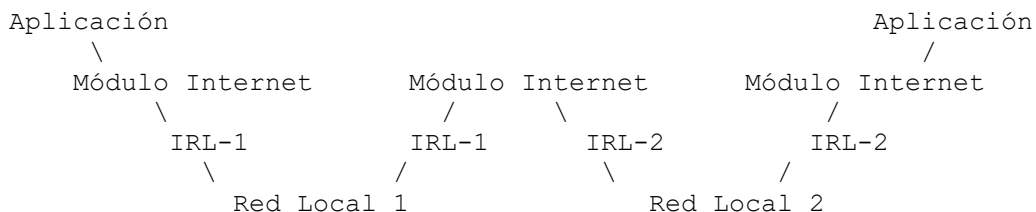
La interfaz de red local crea una cabecera de red local, le adjunta el datagrama y entonces envía el resultado a través de la red local.

El datagrama llega a un host pasarela encapsulado en la cabecera de red local, la interfaz de red local desprende esta cabecera y dirige el datagrama hacia el módulo internet. El módulo internet determina a partir de la dirección internet que el datagrama debe ser reenviado a otro host en una segunda red. El módulo internet determina una dirección de red local para el host de destino. Llama a la interfaz de red local de esa red para enviar el datagrama.

Esta interfaz de red local crea una cabecera de red local y le adjunta el datagrama enviando el resultado al host de destino.

En este host de destino la interfaz de red local le quita al datagrama la cabecera de red local y se lo pasa al módulo internet.

El módulo internet determina que el datagrama va dirigido a una aplicación en este host. Pasa los datos a la aplicación en respuesta a una llamada al sistema, pasando la dirección de origen y otros parámetros como resultado de la llamada.



Trayectoria de la transmisión

Figura 2

2.3. Descripción de Funciones

La función o propósito del Protocolo Internet es mover datagramas a través de un conjunto de redes interconectadas. Esto se consigue pasando los datagramas desde un módulo internet a otro hasta que se alcanza el destino. Los módulos internet residen en hosts y pasarelas en el sistema internet. Los datagramas son encaminados desde un módulo internet a otro a través de redes individuales basándose en la

interpretación de una dirección internet. Por eso, un importante

mecanismo del protocolo internet es la dirección internet.

En el enrutamiento de mensajes desde un módulo internet a otro, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad se proporciona un mecanismo de fragmentación en el protocolo internet.

Direccionamiento

Se establece una distinción entre nombres, direcciones y rutas [4]. Un nombre indica qué buscamos. Una dirección indica dónde está. Una ruta indica cómo llegar allí. El protocolo internet maneja principalmente direcciones. Es tarea de los protocolos de mayor nivel (es decir, protocolos host-a-host o entre aplicaciones) hacer corresponder nombres con direcciones. El módulo internet hace corresponder direcciones de internet con direcciones de red local. Es tarea de los procedimientos de menor nivel (es decir, redes locales o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

Las direcciones son de una longitud fija de 4 octetos (32 bits). Una dirección comienza por un número de red, seguido de la dirección local (llamada el campo "resto"). Hay 3 formatos o clases de direcciones internet: En la Clase A, el bit más significativo es 0, los 7 bits siguientes son la red, y los 24 bits restantes son la dirección local; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección local; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección local.

Se debe tener cuidado al relacionar direcciones internet con direcciones de red local; un host individual físicamente hablando debe ser capaz de actuar como si fuera varios hosts distintos, hasta el punto de usar varias direcciones internet distintas. Algunos hosts tendrán también varios interfaces físicos (multi-homing).

Esto quiere decir que se debe establecer algún mecanismo que permita a un host tener varios interfaces físicos de red, cada uno de ellos con varias direcciones lógicas internet.

Se pueden encontrar ejemplos de correspondencias de direcciones en "Correspondencias de Direcciones" [5].

Fragmentación

La fragmentación de un datagrama internet es necesaria cuando éste se origina en una red local que permite un tamaño de paquete grande

y debe atravesar una red local que limita los paquetes a un tamaño inferior para llegar a su destino.

Un datagrama internet puede ser marcado como "no fragmentar". Todo datagrama internet así marcado no será fragmentado entre distintas redes bajo ninguna circunstancia. Si un datagrama internet marcado como "no fragmentar" no puede ser entregado en su destino sin fragmentarlo, entonces debe ser descartado.

La fragmentación, transmisión y reensamblaje a través de una red local invisible para el módulo del protocolo internet se llama fragmentación intranet y puede ser utilizada [6].

El procedimiento de fragmentación y reensamblaje en internet tiene que ser capaz de dividir un datagrama en un número casi arbitrario de piezas que puedan ser luego reensambladas. El receptor de los fragmentos utiliza el campo de identificación para asegurarse de que no se mezclan fragmentos de distintos datagramas. El campo posición ("offset") le indica al receptor la posición de un fragmento en el datagrama original. La posición y longitud del fragmento determinan la porción de datagrama original comprendida en este fragmento. El indicador "más-fragmentos" indica (puesto a cero) el último fragmento. Estos campos proporcionan información suficiente para reensamblar datagramas.

El campo identificador se usa para distinguir los fragmentos de un datagrama de los de otro. El módulo de protocolo de origen de un datagrama internet establece el campo identificador a un valor que debe ser único para ese protocolo y par origen-destino durante el tiempo que el datagrama estará activo en el sistema internet. El módulo de protocolo de origen de un datagrama completo pone el indicador "más-fragmentos" a cero y la posición del fragmento a cero.

Para fragmentar un datagrama internet grande, un módulo de protocolo internet (p. ej., en una pasarela) crea dos nuevos datagramas internet y copia el contenido de los campos de cabecera internet del datagrama grande en las dos cabeceras nuevas. Los datos del datagrama grande son divididos en dos trozos tomando una resolución mínima de 8 octetos (64 bits) (el segundo trozo puede no ser un múltiplo entero de 8 octetos, pero el primero sí debe serlo). Llamemos al número de bloques de 8 octetos en el primer trozo NFB (Number of Fragment Blocks: Número de Bloques del Fragmento). El primer trozo de datos es colocado en el primer nuevo datagrama internet y el campo longitud total se establece a la longitud del primer datagrama. El indicador "más fragmentos" es puesto a uno. El

segundo trozo de datos es colocado en el segundo nuevo datagrama internet y el campo longitud total se establece a la longitud del segundo datagrama. El indicador "más fragmentos" lleva el mismo

valor que en el datagrama grande. El campo posición del segundo nuevo datagrama se establece al valor de ese campo en el datagrama grande más NFB.

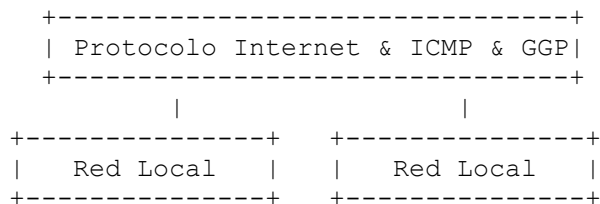
Este procedimiento puede generalizarse para una n-partición, mejor que para la división en dos partes descrita.

Para ensamblar los fragmentos de un datagrama internet, un módulo de protocolo internet (por ejemplo en un host de destino) combina todos los datagramas internet que tengan el mismo valor en los cuatro campos: identificación, origen, destino y protocolo. La combinación se realiza colocando el trozo de datos de cada fragmento en su posición relativa indicada por la posición del fragmento en la cabecera internet de ese fragmento. El primer fragmento tendrá posición cero, y el último fragmento tendrá el indicador "más fragmentos" puesto a cero.

2.4. Pasarelas

Las pasarelas implementan el protocolo internet para reexpedir datagramas entre redes. Las pasarelas también implementan el Protocolo Pasarela a Pasarela (Gateway to Gateway Protocol, GGP) [7] para coordinar el encaminamiento y otra información de control internet.

En una pasarela los protocolos de nivel superior no necesitan ser implementados y las funciones GGP son añadidas al módulo IP.



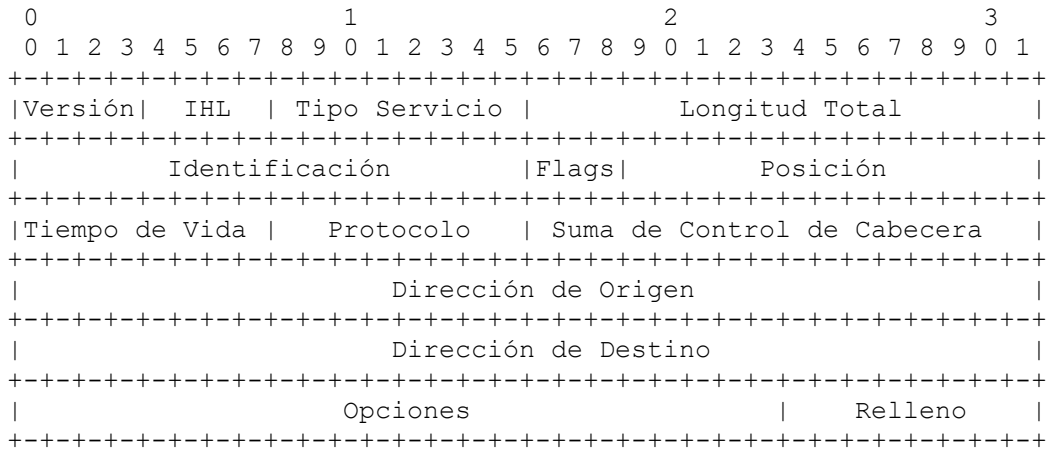
Protocolos de Pasarela

Figura 3.

3. ESPECIFICACION

3.1. Formato de la Cabecera Internet

A continuación vemos un resumen del contenido de la cabecera internet.



Ejemplo de Cabecera de un Datagrama Internet

Figura 4.

Nótese que cada marca (-) corresponde a una posición de un bit.

Versión: 4 bits

El campo Versión describe el formato de la cabecera internet. Este documento describe la versión 4.

IHL: 4 bits

Longitud de la Cabecera Internet (Internet Header Length), es la longitud de la cabecera en palabras de 32 bits, y por tanto apunta al comienzo de los datos. Nótese que el valor mínimo para una cabecera correcta es 5.

Tipo de Servicio: 8 bits

El Tipo de Servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada. Estos parámetros se usarán para guiar la selección de los parámetros de servicio reales al transmitir un datagrama a través de una red en particular. Algunas redes ofrecen prioridad de servicio, la cual trata de algún modo el tráfico de alta prioridad como más importante que el resto

del tráfico (generalmente aceptando sólo tráfico por encima de cierta prioridad en momentos de sobrecarga). La elección más común es un compromiso a tres niveles entre baja demora, alta fiabilidad, y alto rendimiento.

Bits 0-2: Prioridad.
 Bit 3: 0 = Demora Normal, 1 = Baja Demora.
 Bit 4: 0 = Rendimiento Normal, 1 = Alto rendimiento.
 Bit 5: 0 = Fiabilidad Normal, 1 = Alta fiabilidad.]
 Bits 6-7: Reservado para uso futuro.

0	1	2	3	4	5	6	7
+	+	+	+	+	+	+	+
	PRECEDENCIA		D		T		R
							0
							0
+	+	+	+	+	+	+	+

Precedencia

- 111 - Control de Red
- 110 - Control Entre Redes
- 101 - CRITICO/ECP
- 100 - Muy urgente (Flash Override)
- 011 - Urgente (Flash)
- 010 - Inmediato
- 001 - Prioridad
- 000 - Rutina

El uso de las indicaciones de Retraso, Rendimiento y fiabilidad puede incrementar el coste (en cierto sentido) del servicio. En muchas redes un mejor rendimiento para uno de estos parámetros conlleva un peor rendimiento en algún otro. Excepto para casos excepcionales no se deben establecer más de dos de estos tres indicadores.

El tipo de servicio se usa para especificar el tratamiento del datagrama durante su transmisión a través del sistema internet. Se dan ejemplos de relación entre el tipo de servicio internet y el servicio real proporcionado por redes como AUTODIN II, ARPANET, SATNET y PRNET en "Correspondencias de Servicios" [8]

La denominación de precedencia 'Control de Red' está pensada para ser usada dentro de una sola red. El uso y control efectivos de este modo es responsabilidad de cada red. El modo 'Control Entre Redes' está pensado para su uso exclusivo por parte de generadores de control de pasarela. Si el uso efectivo de estos modos de precedencia concierne a una red en particular, es responsabilidad de

esa red controlar el acceso a, y el uso de, esos modos de precedencia.

Longitud Total: 16 bits

La Longitud Total es la longitud del datagrama, medida en octetos,

incluyendo la cabecera y los datos. Este campo permite que la longitud máxima de un datagrama sea de 65,535 octetos. Los datagramas de tal longitud no son prácticos para la mayoría de hosts y redes. Todos los hosts deben estar preparados para aceptar datagramas de hasta 576 octetos (tanto si llegan completos como en fragmentos). Se recomienda que los hosts envíen datagramas mayores de 576 octetos sólo si tienen la seguridad de que el destinatario está preparado para aceptarlos.

El número 576 se ha seleccionado para permitir que un bloque de datos de tamaño razonable sea transmitido junto a la información de cabecera necesaria. Por ejemplo, este tamaño permite que un bloque de datos de 512 octetos más 64 octetos de cabecera quepa en un datagrama. La cabecera internet de tamaño máximo son 60 octetos, y una cabecera internet típica son 20 octetos, admitiendo así un margen para cabeceras de protocolos de nivel superior.

Identificación: 16 bits

Es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un datagrama.

Flags (indicadores): 3 bits

Son diversos indicadores de control.

Bit 0: reservado, debe ser cero.

Bit 1: (DF) No Fragmentar (Don't Fragment) 0 = puede fragmentarse, 1 = No Fragmentar.

Bit 2: (MF) Más Fragmentos (More Fragments) 0 = Último Fragmento, 1 = Más Fragmentos.

0	1	2
+---+---+---+		
	D M	
0 F F		
+---+---+---+		

Posición del Fragmento: 13 bits

Este campo indica a que parte del datagrama pertenece este fragmento.

La posición del fragmento se mide en unidades de 8 octetos (64 bits). El primer fragmento tiene posición 0.

Tiempo de Vida: 8 bits

Este campo indica el tiempo máximo que el datagrama tiene permitido permanecer en el sistema internet. Si este campo contiene el valor

cero, entonces el datagrama debe ser destruido. Este campo es modificado durante el procesamiento de la cabecera internet. El tiempo es medido en segundos, pero como todo módulo que procese un datagrama debe decrementar el TTL (Time To Live: Tiempo de Vida) al menos en uno, incluso si procesa el datagrama en menos de un segundo, se debe pensar en el TTL sólo como un límite superior del tiempo durante el cual un datagrama puede existir. La intención es hacer que los datagramas imposibles de entregar sean descartados, y limitar el máximo periodo de vida de un datagrama.

Protocolo: 8 bits

Este campo indica el protocolo del siguiente nivel usado en la parte de datos del datagrama internet. Los valores de varios protocolos son especificados en "Números Asignados" [9].

Suma de Control de Cabecera: 16 bits

Suma de Control de la cabecera solamente. Dado que algunos campos de la cabecera cambian (p. ej. el tiempo de vida), esta suma es recalculada y verificada en cada punto donde la cabecera internet es procesada.

El algoritmo de la suma de control es:

El campo suma de control es el complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera. A la hora de calcular la suma de control, el valor inicial de este campo es cero.

Esta es una suma de control fácil de calcular y la evidencia experimental indica que es adecuada, pero es provisional y puede ser reemplazada por un procedimiento CRC, dependiendo de la experiencia ulterior.

Dirección de Origen: 32 bits

La dirección de origen. Ver sección 3.2.

Dirección de Destino: 32 bits

J. Postel

[Pág. 15]

RFC 791

Protocolo Internet

Septiembre 1981

La dirección de destino. Ver sección 3.2.

Opciones: variable

Las opciones pueden o no aparecer en los datagramas. Deben ser implementadas por todos los módulos IP (host y pasarelas). Lo que es opcional es su transmisión en cualquier datagrama en particular, no su implementación.

En algunos entornos la opción de seguridad puede ser requerida en todos los datagramas.

El campo opción es de longitud variable. Pueden existir cero o más opciones. Existen dos casos para el formato de una opción:

Caso 1: Un sólo octeto de tipo-opción.

Caso 2: Un octeto tipo-opción, un octeto longitud-opción y los octetos correspondientes a los datos de opción.

El octeto longitud-opción es la cuenta del octeto tipo-opción y el octeto longitud-opción así como los octetos de datos de opción.

El octeto tipo-opción tiene 3 campos

1 bit indicador de copiado,
2 bits clase de opción,
5 bits número de opción.

El indicador de copiado indica si esta opción es copiada en todos los fragmentos al fragmentar.

0 = no copiada
1 = copiada

Las clases de opción son:

0 = control
1 = reservado para uso futuro
2 = depuración y medida
3 = reservado para uso futuro

Se definen las siguientes opciones de internet:

CLASE	NUMERO	LONGITUD	DESCRIPCION
----	-----	-----	-----
0	0	-	Fin de la lista de opciones. Esta opción ocupa un sólo octeto. No tiene octeto de

			longitud.
0	1	-	Sin Operación. Esta opción ocupa un sólo octeto. No tiene octeto de longitud.
0	2	11	Seguridad. Usado para Seguridad, Compartimentación, Grupo de Usuario (TCC), y Códigos de Manejo de Restricciones compatibles con los requerimientos del Departamento de Defensa.
0	3	var.	Encaminamiento de Origen No Estricto

			(Loose Source Routing). Usado para encaminar el datagrama internet en base a la información suministrada por el origen.
0	9	var.	Encaminamiento de Origen Fijo (Strict Source Routing). Usado para encaminar el datagrama internet en base a la información suministrada por el origen.
0	7	var.	Registrar Ruta (Record Route). Usado para rastrear la ruta que sigue un datagrama internet.
0	8	4	Identificador de Flujo (Stream ID). Usado para transportar el identificador de flujo.
2	4	var.	Marca de Tiempo Internet (Internet Timestamp)

Definiciones de Opciones Específicas

Fin De La Lista de Opciones

```
+-----+
|00000000|
+-----+
Tipo=0
```

Esta opción indica el final de la lista de opciones. Esta puede no coincidir con el final de la cabecera internet según expresa la longitud de cabecera internet. Se usa al final de todas las opciones, no al final de cada opción, y sólo es necesario usarla si, caso de no hacerlo, el final de las opciones no coincidiera con el final de la cabecera internet.

Puede ser copiado, introducido o borrado en la fragmentación, o por cualquier otra razón.

Sin Operación

```
+-----+
|00000001|
+-----+
Tipo=1
```

Esta opción puede usarse entre opciones para, por ejemplo, ajustar el comienzo de una opción siguiente a una posición múltiplo de 32 bits.

Puede ser copiado, introducido o borrado en la fragmentación, o por cualquier otra razón.

Seguridad

Esta opción proporciona a los hosts una forma de enviar parámetros de seguridad, compartimentación, manejo de restricciones y TCC (grupo de usuarios cerrado). El formato de esta opción es el siguiente:

```
+-----+-----+---//---+---//---+---//---+---//---+
|10000010|00001011|SSS SSS|CCC CCC|HHH HHH| TCC |
+-----+-----+---//---+---//---+---//---+---+
Tipo=130 Longitud=11
```

Seguridad (campo S): 16 bits

Especifica uno de entre 16 niveles de seguridad (ocho de los cuales están reservados para uso futuro)

00000000	00000000	- No Clasificado
11110001	00110101	- Confidencial
01111000	10011010	- EFTO
10111100	01001101	- MMMM
01011110	00100110	- PROG
10101111	00010011	- Restrtingido
11010111	10001000	- Secreto
01101011	11000101	- Alto Secreto
00110101	11100010	- (Reservado para uso futuro)
10011010	11110001	- (Reservado para uso futuro)
01001101	01111000	- (Reservado para uso futuro)
00100100	10111101	- (Reservado para uso futuro)
00010011	01011110	- (Reservado para uso futuro)
10001001	10101111	- (Reservado para uso futuro)
11000100	11010110	- (Reservado para uso futuro)
11100010	01101011	- (Reservado para uso futuro)

Compartimentos (Campo C): 16 bits

Cuando la información no está compartimentada se usa un valor de todo ceros. Otros valores para el campo Compartimentos pueden obtenerse de la Agencia de Inteligencia de Defensa.

Manejo de Restricciones (campo H): 16 bits

Los valores para los marcadores de control y liberación son digrafos alfanuméricos y están definidos en el Manual DIAM 65-19 "Marcadores de Seguridad Estándar", de la Agencia de

Inteligencia de Defensa.

Código de Control de Transmisión (Campo TCC): 24 bits

Proporciona un mecanismo para segregar el tráfico y definir comunidades de interés controladas entre diversos suscriptores. Los valores TCC son trigrafos, se pueden encontrar en "HQ DCA Code 530".

Debe copiarse al fragmentar. Esta opción aparece como máximo una vez en un datagrama.

Ruta de Origen No Estricta y Registrar Ruta

```
+-----+-----+-----+-----//-----+
|10000011| long.  | puntero|  datos de ruta  |
+-----+-----+-----+-----//-----+
Tipo=131
```

La opción de Encaminamiento de Origen No Estricto y Registrar Ruta ("loose source and record route (LSRR)") proporciona un mecanismo mediante el cual el origen de un datagrama internet puede suministrar información de encaminamiento que será usada por las pasarelas para transmitir el datagrama a su destino, y para almacenar la información de la ruta.

La opción comienza con el código de tipo de opción. El segundo octeto es la longitud de la opción que incluye al código de tipo de opción, al propio octeto de longitud, al octeto con el puntero y a los (long. - 3) octetos de datos de la ruta. El tercer octeto es el puntero a los datos de ruta que indica el octeto en el cual comienza la siguiente dirección de origen a procesar. El puntero es relativo a esta opción, y el valor legal más pequeño para el puntero es 4.

Los datos de ruta se componen de una serie de direcciones internet. Cada dirección internet son 32 bits o 4 octetos. Si el

puntero es mayor que la longitud, la ruta de origen está vacía (y la ruta registrada llena) y el encaminamiento debe basarse en el campo de la dirección de destino.

Si se ha alcanzado la dirección indicada en el campo dirección de destino y el puntero no es mayor que la longitud, la siguiente dirección en la ruta de origen sustituye a la dirección del campo de dirección de destino, y la dirección de ruta registrada sustituye a la dirección de origen recién usada, y se suma cuatro al puntero.

La dirección de ruta registrada es la propia dirección internet

que tiene el módulo internet en el entorno en el cual el datagrama está siendo reenviado.

Este procedimiento de sustituir la ruta de origen con la ruta registrada (si bien está en orden inverso del necesario para ser usada como ruta de origen) significa que la opción (y la cabecera IP en su totalidad) sigue teniendo una longitud constante a medida que el datagrama progresa a través de internet.

Esta opción es una ruta de origen no estricta porque la pasarela o IP del host puede utilizar cualquier ruta con cualquier número de pasarelas intermedias para alcanzar la siguiente dirección en la ruta.

Debe copiarse al fragmentar. Aparece como máximo una vez en un datagrama.

Ruta de Origen Estricta y Registrar Ruta

```
+-----+-----+-----+-----//-----+
|10001001| long.  | puntero|  datos de ruta  |
+-----+-----+-----+-----//-----+
Tipo=137
```

La opción de Ruta de Origen Estricta y Registrar Ruta (strict source and record route (SSRR)) proporciona al origen de un datagrama internet un medio de suministrar información de encaminamiento a ser usada por las pasarelas al reenviar el datagrama al destino y para registrar la información de la ruta.

La opción comienza con el código de tipo de opción. El segundo octeto es la longitud de la opción que incluye al código de tipo de opción, al propio octeto de longitud, al octeto con el puntero y a los (long. - 3) octetos de datos de la ruta. El tercer octeto es el puntero a los datos de ruta que indica el

octeto en el cual comienza la siguiente dirección de origen a procesar. El puntero es relativo a esta opción, y su menor valor legal es 4.

Los datos de ruta se componen de una serie de direcciones internet. Cada dirección internet son 32 bits o 4 octetos. Si el puntero es mayor que la longitud, la ruta de origen está vacía (y la ruta registrada llena) y el encaminamiento debe basarse en el campo de la dirección de destino.

Si se ha alcanzado la dirección indicada en el campo de dirección de destino y el puntero no es mayor que la longitud, la siguiente dirección en la ruta de origen sustituye a la

dirección del campo de dirección de destino, y la dirección de ruta registrada sustituye a la dirección de origen recién usada, y se suma cuatro al puntero.

La dirección de ruta registrada es la propia dirección internet del módulo internet tal y como es en el entorno en el cual el datagrama está siendo reexpedido.

Este procedimiento de sustituir la ruta de origen con la ruta registrada (si bien está en orden inverso del necesario para ser usada como ruta de origen) significa que la opción (y la cabecera IP en su totalidad) sigue teniendo una longitud constante a medida que el datagrama progresa a través de internet.

Esta opción es una ruta de origen estricta porque la pasarela o el IP del host deben enviar el datagrama directamente a la siguiente dirección en la ruta de origen sólo a través de la red conectada directamente indicada en la siguiente dirección, para alcanzar la siguiente pasarela o host especificado en la ruta.

Debe copiarse al fragmentar. Aparece como máximo una vez en un datagrama.

Registrar Ruta

```
+-----+-----+-----+-----//-----+
|00000111| long. | puntero|   datos de ruta  |
+-----+-----+-----+-----//-----+
Tipo=7
```

La opción de Registrar Ruta proporciona un mecanismo para registrar la ruta de un datagrama internet.

La opción comienza con el código de tipo de opción. El segundo octeto es la longitud de la opción que incluye al código de tipo de opción, al propio octeto de longitud, al octeto con el puntero y a los (long. - 3) octetos de datos de la ruta. El tercer octeto es el puntero a los datos de ruta que indica el octeto en el cual comienza la siguiente área para almacenar una dirección de ruta. El puntero es relativo a esta opción, y su menor valor legal es 4.

Una ruta registrada se compone de una serie de direcciones internet. Cada dirección internet son 32 bits o 4 octetos. Si el puntero es mayor que la longitud, el área de datos de la ruta registrada está llena. El host de origen debe construir esta opción con una área de datos de ruta con suficiente espacio para

contener todas las direcciones esperadas. El tamaño de la opción no cambia al agregar direcciones. El contenido inicial del área de datos de ruta debe ser cero.

Cuando un módulo internet encamina un datagrama, comprueba si la opción Registrar ruta está presente. Si lo está, inserta su propia dirección internet, tal y como se la conoce en el entorno en el cual el datagrama está siendo transmitido, en la ruta registrada, comenzando en el octeto indicado por el puntero, e incrementa el puntero en cuatro.

Si el área de datos de ruta ya está llena (el puntero sobrepasa a longitud) el datagrama es transmitido sin insertar la dirección en la ruta registrada. Si hay algo de espacio pero no el suficiente para insertar una dirección completa, el datagrama original es considerado erróneo y descartado. En ambos casos se puede enviar un mensaje de problema de parámetros ICMP al host de origen [3].

No se copia al fragmentar, va sólo en el primer fragmento. Aparece como máximo una vez en un datagrama.

Identificador de Flujo

```
+-----+-----+-----+-----+
|10001000|00000010|   ID de Flujo   |
+-----+-----+-----+-----+
Tipo=136 Longitud=4
```

Esta opción proporciona una forma de transportar el identificador de flujo SATNET de 16 bits a través de redes que no soportan el concepto de flujo.

Debe copiarse al fragmentar. Aparece como máximo una vez en un

datagrama.

Marca de tiempo Internet

```
+-----+-----+-----+-----+
|01000100| long.  | puntero|oflw|flg|
+-----+-----+-----+-----+
|           dirección internet           |
+-----+-----+-----+-----+
|           Marca de tiempo              |
+-----+-----+-----+-----+
|           .                             |
|           .                             |
|           .                             |
```

Tipo = 68

La Longitud de opción es el número de octetos en la opción contando los octetos de tipo, longitud, puntero y desbordamiento/indicadores (oflw/flg, overflow/flags) (máxima longitud: 40)

El puntero es el número de octetos desde el principio de esta opción hasta el final de las marcas de tiempo mas uno (es decir, apunta al octeto de comienzo del espacio para la siguiente marca de tiempo). El valor legal mínimo es 5. El área de marca de tiempo está llena cuando el puntero es mayor que la longitud.

El Desbordamiento (oflw) (4 bits) es el número de módulos IP que no han podido registrar marcas de tiempo debido a falta de espacio.

Los valores de los Indicadores (4 bits) son

- 0 -- Sólo marcas de tiempo, almacenadas en palabras de 32 bits consecutivas,
- 1 -- cada marca de tiempo es precedida con la dirección internet de la entidad registradora,
- 3 -- Los campos de dirección internet están preespecificados. Un módulo IP registra su marca de tiempo sólo si su dirección concuerda con la siguiente dirección internet especificada.

La Marca de Tiempo es una marca temporal de 32 bits, justificada a la derecha, en milisegundos desde la medianoche UT. Si el tiempo no está disponible en milisegundos o no puede darse con respecto a la medianoche UT, entonces se puede insertar

cualquier tiempo como marca de tiempo, siempre que el bit de mayor orden sea puesto a uno para indicar el uso de un valor no estándar.

El host de origen debe construir esta opción con un área de datos para la marca de tiempo lo suficientemente grande para que quepa toda la información de marcas temporales esperada. El tamaño de la opción no cambia al añadir marcas de tiempo. El contenido inicial del área de datos de marcas de tiempo debe ser cero o pares dirección internet/cero.

Si el área de datos de marca de tiempo ya está llena (el puntero sobrepasa a la longitud) el datagrama es transmitido sin insertar marca de tiempo, pero el contador de desbordamiento es incrementado en uno.

Si hay algo de espacio pero no el suficiente para insertar una marca de tiempo completa, o el contador de desbordamiento el mismo se desborda, el datagrama original es considerado erróneo y descartado. En ambos casos se puede enviar un mensaje de problema de parámetros ICMP al host de origen [3].

La opción de marca de tiempo no se copia al fragmentar. Es transportada sólo en el primer fragmento. Aparece como máximo una vez en un datagrama.

Valor de Relleno: variable

El Valor de Relleno se usa para asegurar que la cabecera internet ocupa un multiplo de 32 bits. El valor de relleno es cero.

3.2. Discusión

La implementación de un protocolo debe ser robusta. Cada implementación debe estar preparada para interoperar con otras creadas por diferentes individuos. Aunque el objeto de esta especificación es ser explícita acerca del protocolo, existe la posibilidad de que se produzcan interpretaciones discrepantes. En general, una implementación debe ser conservadora en su comportamiento al enviar, y tolerante al recibir. Es decir, debe tener cuidado de enviar datagramas bien formados, pero debe aceptar cualquier datagrama que pueda interpretar (p. ej. no poner pegasa errores técnicos cuando a pesar de ello el significado sea claro).

El servicio básico internet está orientado a datagramas y posibilita la fragmentación de datagramas en las pasarelas, teniendo lugar el reensamblaje en el módulo internet de destino en el host de destino. Naturalmente, la fragmentación y el reensamblaje de datagramas en una

J. Postel

[Pág. 24]

RFC 791

Protocolo Internet

Septiembre 1981

red o mediante acuerdo privado entre las pasarelas de una red está permitido también, dado que esto es transparente a los protocolos internet y a protocolos de nivel superior. Este tipo de fragmentación y reensamblaje transparente se denomina fragmentación "dependiente de la red" (o intranet) y no se tratará más sobre ello aquí.

En las direcciones internet se distingue entre orígenes (fuentes) y destinos a nivel de host y se proporciona también un campo en el protocolo para ellas. Se ha asumido que cada protocolo proporcionará los medios para cualquier multiplexado que sea necesario en un host.

Direccionamiento

Para proporcionar flexibilidad en la asignación de direcciones a redes y tener en cuenta un gran número de redes de pequeño a medio tamaño, la interpretación del campo dirección está codificada para especificar un pequeño número de redes con un gran número de hosts,

un número moderado de redes con un número moderado de hosts, y un gran número de redes con un pequeño número de hosts. Además existe un código de escape para un modo de direccionamiento extendido.

Formatos de dirección:

Bits de mayor orden	Formato	Class
-----	-----	-----
0	7 bits de red, 24 bits de host	a
10	14 bits de red, 16 bits de host	b
110	21 bits de red, 8 bits de host	c
111	cód. escape para modo extendido	

Un valor cero en el campo de red indica la red actual. Sólo se usa en ciertos mensajes ICMP. El modo de direccionamiento extendido no está definido. Ambas características están reservadas para uso futuro.

Los valores efectivos asignados para direcciones de red se dan en "Números asignados" [9].

La dirección local, asignada por la red local, debe tener en cuenta que un sólo host puede actuar como varios hosts internet distintos. Es decir, debe existir una correspondencia, entre direcciones de host internet e interfaces de red/host que permitan que a un interface le correspondan varias direcciones internet. Se debe tener en cuenta que un host puede tener varios interfaces físicos y deba tratar los datagramas de varios de ellos como si fueran destinados al mismo host.

La correspondencia entre direcciones internet y direcciones para

J. Postel

[Pág. 25]

RFC 791

Protocolo Internet

Septiembre 1981

ARPANET, SATNET, PRNET y otras redes se describen en "Correspondencias entre direcciones" [5].

Fragmentación y Reensamblaje.

El campo de identificación internet (ID) se usa junto con las direcciones de origen y destino, y los campos de protocolo, para identificar fragmentos de datagrama para su reensamblaje.

El bit indicador Más Fragmentos ("More Fragments") (MF) está a uno si el datagrama no es el último fragmento. El campo Posición de Fragmento ("Fragment Offset") identifica la posición del fragmento, relativa al comienzo del datagrama original no fragmentado. Los fragmentos se miden en unidades de 8 octetos. La estrategia de fragmentación está diseñada de forma que un datagrama no fragmentado tiene toda su información de fragmentación a cero (MF = 0, posición de fragmento = 0). Si un datagrama internet es fragmentado, su parte de datos debe ser dividida en múltiplos de 8 octetos.

Este formato permite $2^{13} = 8192$ fragmentos de 8 octetos cada uno, para un total de 65,536 octetos. Nótese que esto es consistente con el campo de longitud total del datagrama (por supuesto, la cabecera se cuenta en la longitud total y no en los fragmentos).

Cuando tiene lugar la fragmentación, algunas opciones se copian, pero otras permanecen sólo en el primer fragmento.

Cada módulo internet debe ser capaz de transmitir un datagrama de 68 octetos sin necesidad de más fragmentación. Esto es porque una cabecera internet puede ser de hasta 60 octetos, y el fragmento mínimo son 8 octetos.

Todo destino internet debe ser capaz de recibir un datagrama de 576 octetos en una sola pieza o en fragmentos a reensamblar.

Los campos que pueden verse afectados por la fragmentación incluye a:

- (1) el campo opciones
- (2) el indicador Más Fragmentos
- (3) la posición del fragmento
- (4) el campo longitud de la cabecera internet
- (5) el campo longitud total
- (6) la suma de control de la cabecera

Si el indicador "Don't Fragment" (No Fragmentar) (DF) está a uno, entonces NO está permitida la fragmentación de este datagrama, si bien puede ser descartado. Esto puede utilizarse para prohibir la

J. Postel

[Pág. 26]

RFC 791

Protocolo Internet

Septiembre 1981

fragmentación en casos donde el host receptor no dispone de suficientes recursos para reensamblar los fragmentos internet.

Un ejemplo del uso de la característica "Don't Fragment" es aliviar la carga de un pequeño host. Un pequeño host podría tener un programa de arranque que acepte un datagrama, lo almacene en memoria y lo ejecute.

Los procedimientos de fragmentación y reensamblaje se describen de forma mucho más sencilla mediante ejemplos. Los siguientes procedimientos son o implementaciones de ejemplo.

Notación general en los pseudo-programas siguientes: " \leq " significa "menor o igual que", " \neq " significa "no igual", " $=$ " significa "igual", " \leftarrow " significa "se le asigna". Además, "x to y" incluye 'x' y excluye 'y'; por ejemplo, "4 to 7" incluiría 4, 5 y 6 (pero no 7).

Un Ejemplo de Procedimiento de Fragmentación

Al datagrama de tamaño máximo que se puede transmitir a través de la siguiente red se le llama la unidad de transmisión máxima (maximum transmission unit (MTU)).

Si la longitud total es menor o igual la unidad de transmisión máxima entonces pasar este datagrama al siguiente paso en el procesamiento de datagrama; sino partir el datagrama en dos fragmentos, siendo el primero de tamaño máximo, y el segundo el resto del datagrama. El primer fragmento es pasado al siguiente paso en el procesamiento de datagramas, mientras que el segundo fragmento se pasa otra vez a este procedimiento en caso de ser todavía demasiado grande.

Notación:

FO	-	Posición de Fragmento ("Fragment Offset")
IHL	-	Long. de la cabecera internet (Internet Header Length)
DF	-	Indicador No Fragmentar ("Don't Fragment")
MF	-	indicador Más Fragmentos ("More Fragment")
TL	-	Longitud total (Total Length)
OFO	-	FO Previo ("Old Fragment Offset")
OIHL	-	IHL Previo
OMF	-	indicador MF Previo (Old More Fragments)
OTL	-	Longitud total previa (Old Total Length)
NFB	-	Núm. de bloques de fragmento (Number of Fragment Blocks)
MTU	-	Unidad de transmisión máxima (Maximum Transmission Unit)

J. Postel

[Pág. 27]

RFC 791

Protocolo Internet

Septiembre 1981

Procedimiento:

```
SI TL <= MTU ENTONCES
    Pasar este datagrama al siguiente paso en el procesamiento
    de datagramas.
SINO SI DF = 1 ENTONCES
    descartar el datagrama
SINO
    Para producir el primer fragmento:
    (1) Copiar la cabecera internet original;
    (2) OIHL <- IHL; OTL <- TL; OFO <- FO; OMF <- MF;
    (3) NFB <- (MTU-IHL*4)/8;
    (4) Adjuntar los primeros NFB*8 octetos de datos;
    (5) Corregir la cabecera:
        MF <- 1; TL <- (IHL*4)+(NFB*8);
        Recalcular la Suma de Control;
    (6) Pasar este datagrama al siguiente paso en el procesamiento
        de datagramas;
```

Para producir el segundo fragmento:

- (7) Copiar de forma selectiva la cabecera internet (algunas opciones no se copian, ver definiciones de opción);
- (8) Añadir los datos restantes;
- (9) Corregir la cabecera:

$$IHL \leftarrow (((OIHL * 4) - (\text{long. de opciones no copiadas})) + 3) / 4;$$

$$TL \leftarrow OTL - NFB * 8 - (OIHL - IHL) * 4;$$

$$FO \leftarrow OFO + NFB; \quad MF \leftarrow OMF; \quad \text{Recalcular Suma de Control};$$
- (10) Pasar este fragmento al test de fragmentación; FIN.

En el procedimiento anterior cada fragmento (excepto el último) fue construido con el tamaño máximo permitido. Otra alternativa podría producir datagramas menores que el tamaño máximo. Por ejemplo, uno podría implementar un procedimiento de fragmentación que dividiera repetidamente los datagramas grandes en dos hasta que los fragmentos resultantes fueran de menor tamaño que el tamaño de la unidad de transmisión máxima.

Un ejemplo de Procedimiento de Reensamblaje

Para cada datagrama el identificador de buffer se calcula como la concatenación de los campos de origen, destino, protocolo e identificación. Si se trata de un datagrama completo (es decir, los campos Posición de Fragmento y Más Fragmentos son cero), entonces todos los recursos de reensamblaje asociados con este identificador de buffer son liberados y el datagrama se pasa al siguiente paso en el procesamiento de datagramas.

Si no hay a mano otros fragmentos con este identificador de buffer

entonces se asignan recursos de reensamblaje. Los recursos de reensamblaje consisten en un buffer de datos, un buffer de cabecera, una tabla de bits de bloque de fragmento, un campo de longitud total de datos, y un temporizador. Los datos contenidos en el fragmento se guardan en el buffer de datos de acuerdo con su posición de fragmento y longitud y se modifican bits en la tabla de bits de bloques de fragmento correspondientes a los bloques de fragmento recibidos.

Si este es el primer fragmento (es decir, la posición del fragmento es cero) esta cabecera se guarda en el buffer de cabecera. Si este es el último fragmento (es decir, su campo Más Fragmentos es cero) se calcula la longitud total de los datos. Si este fragmento completa el datagrama (lo cual se comprueba mirando los bits puestos a uno en la tabla de bloques de fragmento), entonces el datagrama es enviado al siguiente paso en el procesamiento de datagramas; sino se le asigna al temporizador el máximo de su valor actual y el valor del campo Tiempo de Vida de este fragmento; y por último la rutina de reensamblaje devuelve el control.

Si el temporizador se agota, se liberan todos los recursos de reensamblaje para este identificador de buffer. El valor inicial del temporizador es un límite inferior del tiempo de espera de reensamblaje. Esto es así porque el tiempo de espera será incrementado si el Tiempo de Vida del fragmento recién llegado es mayor que el valor actual del temporizador, pero no será decrementado si es menor. El valor máximo que este temporizador puede alcanzar es el tiempo de vida máximo (aproximadamente 4.25 minutos). La recomendación actual para el valor inicial del temporizador es 15 segundos. Este puede variar conforme la experiencia con este protocolo se acumule. Nótese que la elección del valor de este parámetro está relacionada con la capacidad de buffer disponible y la velocidad de datos del medio de transmisión; es decir, la velocidad de datos por el valor del temporizador es igual al tamaño del buffer (p. ej., 10Kb/s X 15s = 150 Kb).

Notación:

FO	-	Posición del Fragmento ("Fragment Offset")
IHL	-	Long. de la cabecera internet (Internet Header Length)
MF	-	indicador Más Fragmentos ("More Fragments")
TTL	-	Tiempo de Vida
NFB	-	Núm. de bloques de fragmento (Number of Fragment Blocks)
TL	-	Longitud total (Total Length)
TDL	-	Longitud total de Datos (Total Data Length)

J. Postel

[Pág. 29]

RFC 791

Protocolo Internet

Septiembre 1981

BUFID	-	Identificador de buffer (Buffer Identifier)
RCVBT	-	Tabla de Bits de Fragmentos Recibidos (Fragment Received Bit Table)
TLB	-	Límite Inferior del Temporizador (Timer Lower Bound)

Procedimiento:

```

(1)  BUFID <- origen|destino|protocolo|identificación;
(2)  SI FO = 0 Y MF = 0
(3)      ENTONCES SI está reservado el buffer con BUFID
(4)      ENTONCES liberar todo el reensamblaje para este BUFID;
(5)      Pasar el datagrama al siguiente paso; FIN.
(6)  SINO SI no está reservado el buffer con BUFID
(7)      ENTONCES Asignar recursos de reensamblaje con
          BUFID;
          TEMPORIZADOR <- TLB; TDL <- 0;
(8)      guardar los datos del fragmento en el buffer de
          datos con BUFID desde el octeto FO*8 al octeto
          (TL-(IHL*4))+FO*8;
(9)      poner a uno los bits RCVBT desde FO
          a FO+((TL-(IHL*4)+7)/8);
(10)  SI MF = 0 ENTONCES TDL <- TL-(IHL*4)+(FO*8)

```

```

(11)      SI FO = 0 ENTONCES
           guardar cabecera en buffer de cabecera
(12)      SI TDL # 0
(13)      Y todos los bits RCVBT desde 0 a (TDL+7)/8 son uno
(14)      ENTONCES TL <- TDL+(IHL*4)
(15)      Pasar el datagrama al siguiente paso;
(16)      liberar todos los recursos de reensamblaje
           para este BUFID; FIN.
(17)      TEMPORIZADOR <- MAX(TEMPORIZADOR,TTL);
(18)      ceder control hasta siguiente fragmento o hasta que
           el temporizador se agote;
(19) El temporizador se ha agotado: vaciar todo el reensamblaje
           con este BUFID; FIN.

```

En el caso en que dos o más fragmentos contengan los mismos datos tanto idénticamente como por solapamiento parcial, este procedimiento usará la copia llegada más recientemente en el buffer de datos y en el datagrama entregado.

Identificación

La elección del Indentificador de un datagrama está basada en la necesidad de proporcionar una forma de identificar de forma única un datagrama en particular. El módulo del protocolo que reensambla fragmentos los evalúa como pertenecientes al mismo datagrama si tienen el mismo origen, destino, protocolo e Identificador. De este

J. Postel

[Pág. 30]

RFC 791

Protocolo Internet

Septiembre 1981

modo el remitente debe elegir un Identificador que sea único para ese par origen-destino y ese protocolo, y durante el tiempo que el datagrama (o cualquier fragmento suyo) pueda perdurar en internet.

Parece entonces que un módulo de protocolo que actúe de remitente necesite mantener una tabla de Identificadores, con una entrada por cada destino con el que haya comunicado en el último periodo de máxima duración de un paquete en internet.

Sin embargo, dado que el campo Identificador permite 65,536 valores diferentes, algún host puede ser capaz de usar simplemente identificadores únicos independientemente del destino.

Para algunos protocolos de nivel superior resulta adecuado elegir el identificador. Por ejemplo, los módulos de protocolo TCP pueden retransmitir un segmento TCP idéntico, y la probabilidad de una recepción correcta se vería ampliada si la retransmisión lleva el mismo identificador que la transmisión original, ya que se podrían usar fragmentos de cualquiera de los dos datagramas para construir un segmento TCP correcto.

Tipo de Servicio

El Tipo de servicio (Type Of Service (TOS)) se utiliza para la selección de la calidad del servicio internet. El tipo de servicio se especifica a través de los parámetros abstractos de precedencia, demora, rendimiento, y fiabilidad. Estos parámetros abstractos se hacen corresponder con parámetros de servicio efectivos de las redes particulares que el datagrama atraviesa.

Precedencia. Medida independiente de la importancia de este datagrama.

Demora. La entrega inmediata es importante para datagramas con esta indicación.

Rendimiento. Una alta velocidad de datos es importante para datagramas con esta indicación.

Fiabilidad. Para datagramas con esta indicación es importante un mayor nivel de esfuerzo para asegurar la entrega.

Por ejemplo, La ARPANET tiene un bit de prioridad, y la posibilidad de elegir entre mensajes "estándar" (tipo 0) y "no controlados" (tipo 3) (La elección entre mensajes de paquete único o multipaquete puede considerarse también un parámetro de servicio). Los mensajes no controlados tienden a ser entregados con menos fiabilidad y a sufrir menos demora. Supóngase que un datagrama internet se va a

J. Postel

[Pág. 31]

RFC 791

Protocolo Internet

Septiembre 1981

enviar a través de ARPANET. Sea el tipo de servicio internet dado como:

```
Precendencia: 5
Demora:      0
Rendimiento: 1
Fiabilidad:  1
```

En este ejemplo, la correspondencia de estos parámetros con aquellos disponibles para ARPANET sería poner a uno el bit de prioridad de ARPANET, ya que la precedencia Internet se sitúa en la mitad superior de su escala, seleccionar mensajes estándar ya que se han indicado los requerimientos de rendimiento y fiabilidad y no de demora. Se dan más detalles sobre correspondencias de servicio en "Correspondencias de Servicio ("Service Mappings") [8].

Tiempo de Vida

El tiempo de vida es establecido por el remitente al tiempo máximo que un datagrama puede estar en el sistema internet. Si el datagrama permanece en el sistema internet durante más tiempo que su tiempo de vida, entonces el datagrama debe ser destruido.

Este campo debe ser decrementado en cada punto donde se procese para

reflejar el tiempo invertido en procesar el datagrama. Incluso si no existe información local acerca del tiempo realmente empleado, el campo debe decrementarse en 1. El tiempo es medido en unidades de segundo (es decir, el valor 1 significa un segundo). Por tanto, el tiempo de vida máximo son 255 segundos o 4.25 minutos. Como todo módulo que procese un datagrama debe decrementar el TTL por lo menos en uno incluso si lo procesa en menos de un segundo, debe pensarse en el TTL sólo como un límite superior del tiempo que un datagrama puede existir. La intención es hacer que los datagramas que no se pueden entregar sean descartados, y limitar el máximo periodo de vida del datagrama.

Algunos protocolos de conexión fiables de alto nivel se basan en la presunción de que los datagramas duplicados más viejos no llegarán después de pasar un cierto tiempo. El TTL es para tales protocolos un medio de tener la seguridad de que su suposición se cumple.

Opciones

Las opciones son opcionales en cada datagrama, pero obligatorias en las implementaciones. Es decir, la presencia o ausencia de una opción es elección del remitente, pero cada módulo internet debe ser capaz de analizar cualquier opción. Puede haber varias opciones presentes en el campo opción.

J. Postel

[Pág. 32]

RFC 791

Protocolo Internet

Septiembre 1981

Las opciones pueden no ocupar exactamente un espacio múltiplo de 32 bits. La cabecera debe ser completada con octetos de ceros. El primero de estos será interpretado como la opción fin-de-opciones, y el resto como el relleno de la cabecera internet.

Todo módulo internet debe ser capaz de actuar en cada opción. La Opción de Seguridad es obligatoria si se debe atravesar un tráfico clasificado, restringido o compartimentado.

Suma de Control

La suma de control de la cabecera internet es recalculada si la cabecera es modificada. Por ejemplo, una reducción del tiempo de vida, las adiciones o cambios en las opciones internet, o debido a la fragmentación. Esta suma de control a nivel internet está pensada para proteger de errores de transmisión los campos de la cabecera internet.

Existen algunas aplicaciones donde son aceptables unos pocos errores en los bits de datos, mientras que los retrasos por retransmisión no lo son. Si el protocolo internet impusiera la exactitud de datos tales aplicaciones no podrían ser soportadas.

Errores

Los errores en el protocolo internet pueden indicarse mediante los mensajes ICMP [3].

3.3. Interfaces

La descripción funcional de interfaces de usuario para IP es, en el mejor de los casos, ficticia, ya que cada sistema operativo dispondrá de distintos recursos. En consecuencia, debemos advertir a los lectores que diferentes implementaciones IP pueden tener diferentes interfaces de usuario. Sin embargo, todas deben proporcionar un cierto conjunto mínimo de servicios para garantizar que todas las implementaciones IP pueden soportar la misma jerarquía de protocolos. Esta sección especifica las interfaces funcionales obligatorias para todas las implementaciones IP.

El protocolo internet interactúa con la red local por un lado y con un protocolo de nivel superior o una aplicación por el otro. En lo que sigue, el protocolo de nivel superior o aplicación (o incluso un programa pasarela) será llamado el "usuario", dado que es lo que usa el módulo internet. Como el protocolo internet es un protocolo de datagramas, se mantiene un mínimo de memoria o estado entre transmisiones de datagramas, y cada llamada del usuario al módulo del protocolo internet proporciona toda la información necesaria para que

J. Postel

[Pág. 33]

RFC 791

Protocolo Internet

Septiembre 1981

el IP ejecute el servicio pedido.

Interface Ejemplo de nivel superior

Las siguientes dos llamadas de ejemplo satisfacen los requisitos de la comunicación entre el usuario y el módulo del protocolo internet ("=>" significa 'devuelve'):

```
SEND (src, dst, prot, TOS, TTL, BufPTR, len, Id, DF, opt => result)
```

donde:

```
src = dirección de origen
dst = dirección de destino
prot = protocolo
TOS = tipo de servicio
TTL = tiempo de vida
BufPTR = puntero a buffer
len = longitud del buffer
Id = Identificador
DF = No Fragmentar
opt = datos de opción
result = respuesta
    OK = datagrama enviado correctamente
    Error = error en los argumentos o error en la red local
```

Nótese que la precedencia se incluye en el TOS y la seguridad/compartimiento se pasa como opción.

RECV (BufPTR, prot, => result, src, dst, TOS, len, opt)

donde:

BufPTR = puntero a buffer
prot = protocolo
result = respuesta
 OK = datagrama recibido correctamente
 Error = error en los argumentos
len = longitud del buffer
src = dirección de origen
dst = dirección de destino
TOS = tipo de servicio
opt = datos de opción

Cuando el usuario envía un datagrama, ejecuta la llamada SEND suministrando todos los argumentos. El módulo del protocolo internet, al recibir esta llamada, comprueba los argumentos y prepara y envía el

J. Postel

[Pág. 34]

RFC 791

Protocolo Internet

Septiembre 1981

mensaje. Si los argumentos son válidos y el datagrama es aceptado por la red local, la llamada retorna con éxito. Si los argumentos no son correctos, o bien el datagrama no es aceptado por la red local, la llamada retorna sin éxito. En retornos de llamada sin éxito, se debe construir un informe razonable sobre la causa del problema, pero los detalles de tales informes corresponden a las distintas implementaciones.

Cuando un datagrama llega al módulo del protocolo internet desde la red local, o hay una llamada RECV pendiente del usuario al que va dirigido o no la hay. En el primer caso, la llamada pendiente es satisfecha pasando la información desde el datagrama al usuario. En el segundo caso, se notifica al usuario de destino que tiene un datagrama pendiente. Si el usuario de destino no existe, se devuelve un mensaje de error ICMP al remitente, y los datos son desechados.

La notificación de un usuario puede ser a través de una pseudo interrupción o un mecanismo similar, correspondiente al entorno particular del sistema operativo de la implementación.

Una llamada RECV de usuario puede ser inmediatamente satisfecha por un datagrama pendiente, o bien quedar pendiente hasta que llegue un datagrama.

La dirección de origen se incluye en la llamada SEND en el caso de que el host remitente tenga varias direcciones (múltiples conexiones físicas o direcciones lógicas). El módulo internet debe comprobar que

Este es un datagrama internet en la versión 4 del protocolo internet; la cabecera internet consta de 5 palabras de 32 bits, y la longitud total del datagrama es de 21 octetos. Este datagrama es un datagrama completo (no un fragmento).

J. Postel

[Pág. 36]

RFC 791

Protocolo Internet

Septiembre 1981

Ejemplo 2:

En este ejemplo, se muestra primero un datagrama internet de tamaño medio (452 octetos de datos), y después dos fragmentos internet que podrían ser resultado de la fragmentación de este datagrama si la transmisión de máximo tamaño permitida fuese de 280 octetos.

```

      0              1              2              3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|Ver= 4 |IHL= 5 | Tipo de Serv. |           Long. Total = 472           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Identificación = 111           |Flg=0| Pos. de Fragmento = 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|   TTL  = 123 | Protocolo = 6 |           suma de control           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     dirección de origen                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     dirección de destino                                    |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     datos                                                  |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     datos                                                  |
\                                     \
\                                     \
|                                     datos                                                  |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     datos                                                  |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Ejemplo de Datagrama Internet

Figura 6.

J. Postel

[Pág. 37]

RFC 791

Protocolo Internet

Septiembre 1981

Ahora el primer fragmento resultado de dividir el datagrama a los 256 octetos.

```

      0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Ver= 4 |IHL= 5 | Tipo de Serv. |           Long. Total = 276       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Identificación = 111       |Flg=1| Pos. de Fragmento = 0 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   TTL  = 119 | Protocolo = 6 |           suma de control         |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               dirección de origen                  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               dirección de destino                  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               datos                                 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               datos                                 |
\                               \                                    \
\                               \                                    \
|                               datos                                 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               datos                                 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Ejemplo de Fragmento Internet

Figura 7.

Y el segundo fragmento.

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Ver= 4 |IHL= 5 | Tipo de Serv. |           Long. Total = 216       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Identificación = 111       |Flg=0|  Pos. de Fragmento = 32 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   TTL  = 119 | Protocolo = 6 |           suma de control         |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     dirección de origen           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     dirección de destino           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     datos                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     datos                           |
\                                     \                               \
\                                     \                               \
|                                     datos                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     datos                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Ejemplo de Fragmento Internet

Figura 8.

Example 3:

Aqui se muestra un ejemplo de un datagrama que contiene opciones:

```

      0              1              2              3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Ver= 4 |IHL= 8 | Tipo de Serv. |           Long. Total = 576       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Identificación = 111       |Flg=0| Pos. de Fragmento = 0 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   TTL  = 123 | Protocolo = 6 |           suma de control         |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                           dirección de origen                                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                           dirección de destino                                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Cód. Opc. = x | Long. Opc.= 3 | valor opción | Cód. Opc. = x |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Long. Opc.= 4 |           valor de opción           | Cód. Opc. = 1 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Cód. Opc. = y | Long. Opc.= 3 | valor opción | Cód. Opc. = 0 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                           datos                                           |
\                                           \
\                                           \
|                                           datos                                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                           datos                                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Ejemplo de Datagrama Internet

Significado de Bits

Figura 11.

De forma similar, cuando un campo multiocteto representa una cantidad numérica el bit más a la izquierda de todo el campo es el bit más significativo. Cuando una cantidad multi-octeto es transmitida se transmite primero el octeto más significativo.

J. Postel

[Pág. 41]

RFC 791

Protocolo Internet

Septiembre 1981

GLOSARIO

1822

BBN Report 1822, "Especificación de la Interconexión de un Host y un IMP". La especificación de la interfaz entre un host y ARPANET.

ARPANET leader

La información de control en un mensaje ARPANET en la interfaz host-IMP.

mensaje ARPANET

La unidad de transmisión entre un host y un IMP en ARPANET. El tamaño máximo es aproximadamente 1012 octetos (8096 bits).

paquete ARPANET

Una unidad de transmisión usada internamente entre IMPs en ARPANET. El tamaño máximo es aprox. 126 octetos (1008 bits).

Destino

La dirección de destino, un campo de la cabecera internet.

DF

El bit 'Don't Fragment' (No Fragmentar) del campo de indicadores.

Indicadores (Flags)

Un campo de la cabecera internet con varios indicadores de control.

Posición del Fragmento

Posición del fragmento. Este campo de la cabecera internet

indica a que lugar del datagrama internet pertenece un fragmento.

GGP

Gateway to Gateway Protocol (Protocolo Pasarela a Pasarela), el protocolo usado principalmente entre pasarelas para controlar el encaminamiento y otras funciones de pasarela.

cabecera

Información de control al principio de un mensaje, segmento, datagrama, paquete o bloque de datos.

ICMP

Internet Control Message Protocol (Protocolo de Mensajes de

J. Postel

[Pág. 42]

RFC 791

Protocolo Internet

Septiembre 1981

Control de Internet), implementado en el módulo internet, el ICMP es usado de pasarelas a hosts y entre hosts para informar de errores y hacer sugerencias de encaminamiento.

Identificación

Un campo de la cabecera internet que almacena el valor identificador asignado por el remitente como ayuda para ensamblar los fragmentos de un datagrama.

IHL

El campo de la cabecera internet 'Internet Header Length' (Longitud de la cabecera internet) es la longitud de la cabecera internet medida en palabras de 32 bits.

IMP

Interface Message Processor (Procesador de Mensajes de Interfaz), el intercambiador de paquetes de ARPANET.

Dirección Internet

Una dirección de origen o destino de 4 octetos (32 bits) formada por un campo de Red y un campo de Dirección Local.

Datagrama internet

La unidad de datos intercambiada entre un par de módulos internet (incluye la cabecera internet).

Fragmento internet

Una parte de los datos de un datagrama internet con una cabecera internet.

Dirección Local

La dirección de un host en una red. La relación real entre una dirección local internet con las direcciones de un host en una red es muy general, permitiéndose relaciones de muchos a uno.

MF

El indicador 'More-Fragments' (Más Fragmentos) presente en el campo indicadores de la cabecera internet.

módulo

Una implementación, normalmente en software, de un protocolo u otro procedimiento.

indicador 'more-fragments'

Un indicador que dice si este datagrama internet contiene el final de un datagrama internet, presente en el campo Indicadores de la cabecera internet.

J. Postel

[Pág. 43]

RFC 791

Protocolo Internet

Septiembre 1981

NFB

Number of Fragment Blocks (Número de Bloques de Fragmento) en la parte de datos de un fragmento internet. Es decir, la longitud de una parte de datos medida en unidades de 8 octetos.

octeto

Un byte de 8 bits.

Opciones

El campo Opciones de la cabecera internet puede contener varias opciones, y cada una de ellas puede ser de varios octetos de longitud.

Valor de Relleno (Padding)

El campo Valor de Relleno de la cabecera internet se utiliza para asegurar que el campo de datos comienza en una dirección múltiplo de 32 bits. El relleno es cero.

Protocolo

En este documento, un campo de la cabecera internet, el identificador del protocolo del siguiente nivel superior.

Resto

La parte de dirección local de una dirección internet.

Origen

La dirección de origen, un campo de la cabecera internet.

TCP

Transmission Control Protocol (Protocolo de Control de Transmisión): Un protocolo host-a-host para comunicación fiable en entornos internet.

Segmento TCP

La unidad de datos intercambiada entre dos módulos TCP

(incluyendo la cabecera TCP).

TFTP

Trivial File Transfer Protocol (Protocolo de Transferencia de Archivos Trivial): Un sencillo protocolo de transferencia de archivos construido sobre UDP).

Tiempo de Vida

Un campo de la cabecera internet que indica el límite superior de cuánto tiempo puede existir el datagrama.

TOS

J. Postel

[Pág. 44]

RFC 791

Protocolo Internet

Septiembre 1981

Type of Service (Tipo de Servicio)

Longitud Total

El campo de la cabecera Internet 'Longitud Total' es la longitud del datagrama en octetos, incluyendo cabecera y datos.

TTL

Time to Live (Tiempo de Vida)

Tipo de Servicio

Un campo de la cabecera internet que indica el tipo (o calidad) de servicio para este datagrama.

UDP

User Datagram Protocol (Protocolo de Datagrama de Usuario): Un protocolo a nivel de usuario para aplicaciones orientadas a transacciones.

Usuario

El usuario del protocolo internet. Este puede ser un módulo de protocolo de nivel superior, una aplicación, o un programa pasarela.

Versión

El campo Versión indica el formato de una cabecera internet.

REFERENCIAS

- [1] Cerf, V., "The Catenet Model for Internetworking", Information Processing Techniques Office, Defense Advanced Research Projects Agency, IEN 48, Julio 1978.
- [2] Bolt Beranek and Newman, "Specification for the Interconnection of a Host and an IMP", BBN Technical Report 1822, Revisado Mayo 1978.
- [3] Postel, J., "Internet Control Message Protocol - DARPA Internet Program Protocol Specification", RFC 792, USC/Information Sciences Institute, Septiembre 1981.
- [4] Shoch, J., "Inter-Network Naming, Addressing, and Routing", COMPCON, IEEE Computer Society, Otoño 1978.
- [5] Postel, J., "Address Mappings", RFC 796, USC/Information Sciences Institute, Septiembre 1981.
- [6] Shoch, J., "Packet Fragmentation in Inter-Network Protocols," Computer Networks, v. 3, n. 1, Febrero 1979.
- [7] Strazisar, V., "How to Build a Gateway", IEN 109, Bolt Beranek and Newman, Agosto 1979.
- [8] Postel, J., "Service Mappings," RFC 795, USC/Information Sciences Institute, Septiembre 1981.
- [9] Postel, J., "Assigned Numbers," RFC 790, USC/Information Sciences Institute, Septiembre 1981.

