CAPITULO I

CONCEPTOS INICIALES

1.1 Descripción de IPv4

1.2 Breve Historia de TCP/IP e Internet

1.3 Organización de Internet

1.4 Modelo de Referencia OSI frente a TCP/IP

1.5 Problemas con IPv4

1.6 IPv4 versus IPv6. ¿Porque cambiar a IPv6?

1.7 Historia del IPv6

1.1 Descripción de IPv4

La base de ***Internet*** ha sido el ***protocolo*** **IP**, es este protocolo el que le ha permitido crecer tanto en tamaño como en aplicaciones manejadas, fue creado como un estándar de facto por gente que usa Internet, pero se adapta al modelo OSI. Permite comunicar cualquier sistema con otro con gran facilidad, en esto ha residido su enorme éxito. *[WWW021]*

Su espacio de direcciones resulto insuficiente, debido al crecimiento de Internet y al número cada vez mayor de elementos activos con ***dirección IP*** conectados a la red.

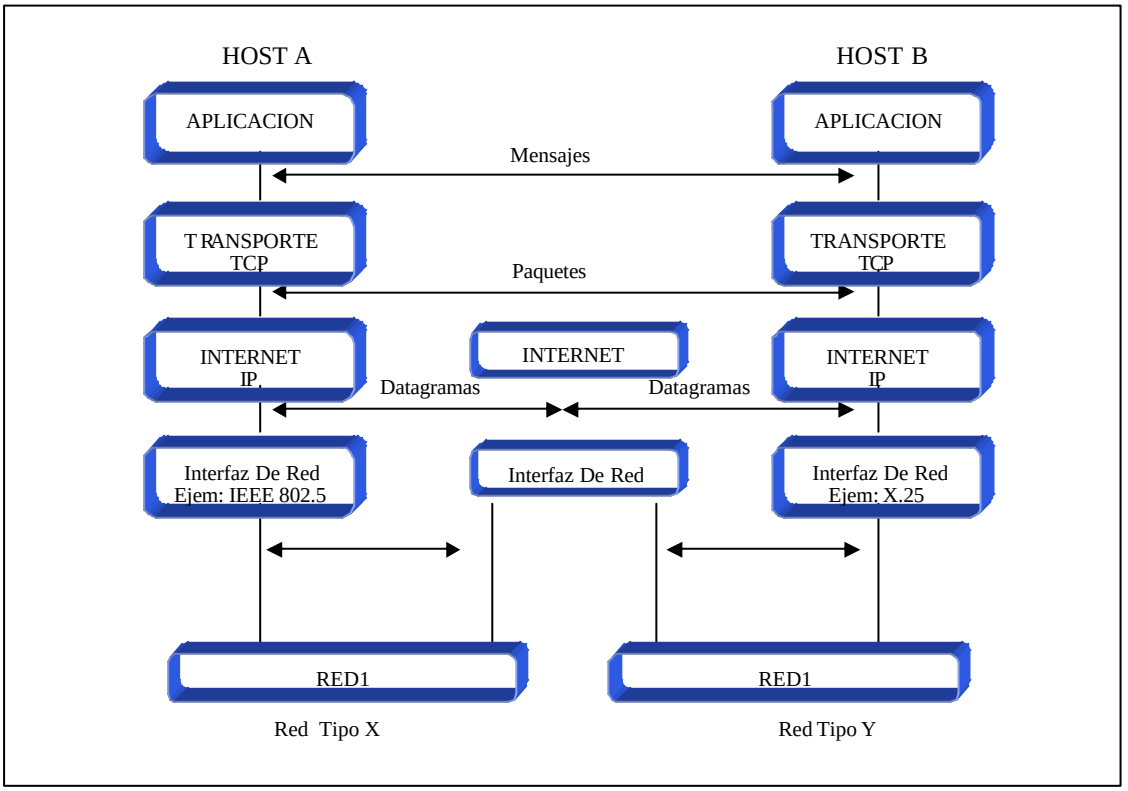


Fig 1.1 Comunicación de diferentes sistemas en Internet

1.2 Breve Historia de TCP/IP e Internet

EEUU estaba buscando una forma de mantener las comunicaciones vitales del país en el posible caso de una Guerra Nuclear. Este hecho marcó profundamente su evolución, ya que aún ahora los rasgos fundamentales del proyecto se hallan presentes en lo que hoy conocemos como Internet. *[WWW018]*

No debía haber una autoridad central, y debía operar en situaciones difíciles. Cada máquina conectada debería tener el mismo status y la misma capacidad para mandar y recibir información.

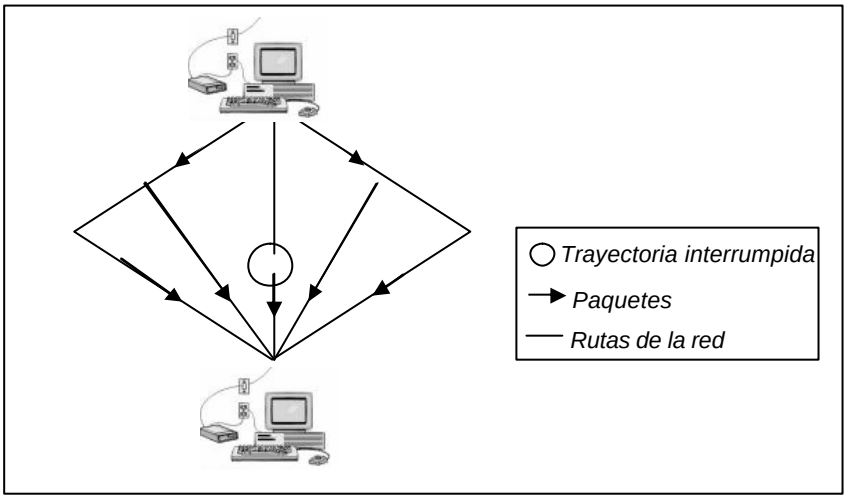


Fig 1. 2 Rutas alternativas en Internet

El envío de los datos debería descansar en un mecanismo que pudiera manejar la destrucción parcial de la Red. Se decidió entonces que los mensajes deberían de dividirse en pequeñas porciones de información o paquetes, los cuales contendrían la dirección de destino pero sin especificar una ruta específica para su arribo; por el contrario, cada paquete buscaría la manera de llegar al destinatario por las rutas disponibles y el destinatario reensamblaría los paquetes individuales para reconstruir el mensaje original. La ruta que siguieran los paquetes no era importante; lo importante era que llegaran a su destino.

Se buscaba:

Protocolos comunes. Que puedan especificarse cualquier red para simplificar los procesos

Interoperabilidad. Que equipos de diversos fabricantes puedan funcionar juntos

Comunicaciones sólidas. Una norma fiable y de alto rendimiento

Facilidad de reconfiguración. Facilidad de reconfigurar, y añadir o eliminar computadoras sin interrumpir las comunicaciones.

TCP/IP no pertenece a nadie porque se desarrollo en público, adquirió gran popularidad cuando se incorporó a la versión 4.2 del UNIX de BSD (Berkley Standard Distribution).

La descentralización de ARPANET y la disponibilidad sin costo de programas basados en TCP/IP permitió que ya en 1977, otro tipo de redes no necesariamente vinculadas al proyecto original, empezaran a conectarse.

En 1983, el segmento militar de ARPANET se separa y forma su propia red que se conoció como MILNET. ARPANET, y sus "redes asociadas" empezaron a ser conocidas como Internet. *[LIB001]*

En 1984, la Fundación Nacional para la Ciencia (National Science Foundation) inicia una nueva "red de redes" vinculando en una primera etapa a los centros de supercómputo en los E.U. (6 grandes centros de procesamiento de datos distribuidos en el territorio de los E.U.) a través de nuevas y más rápidas conexiones. Esta red se le conoció como NSFNET y adoptó también como protocolo de comunicación a TCP/IP.

Eventualmente, empezaron a conectarse no solamente centros de supercómputo, sino también instituciones educativas con redes más pequeñas. El crecimiento exponencial que experimentó NSFNET así como el incremento continuo de su capacidad de transmisión de datos, determinó que la mayoría de los miembros de ARPANET terminaran conectándose a esta nueva red y en 1989, ARPANET se declara disuelta. Actualmente NSFNET es la espina dorsal de Internet gestionada por el ANS (Advanced Network Services).

1.3 Organización de Internet

Internet comenzó, y con un objetivo claro de descentralización total, por razones de seguridad, tampoco debía existir una forma de controlar su operación, por esto no existía un "Centro de Administración de Internet", sin embargo, para mantener su coherencia y velar

por su desarrollo, se anunció en Junio de 1991 en Copenhague la creación dela **Internet Society** la cual entró a operar a partir de Enero de 1992 como una entidad sin ánimo de lucro y como una organización internacional no gubernamental orientada a la cooperación global y coordinación de la Internet y de sus tecnologías y aplicaciones de redes. *[WWW020]*

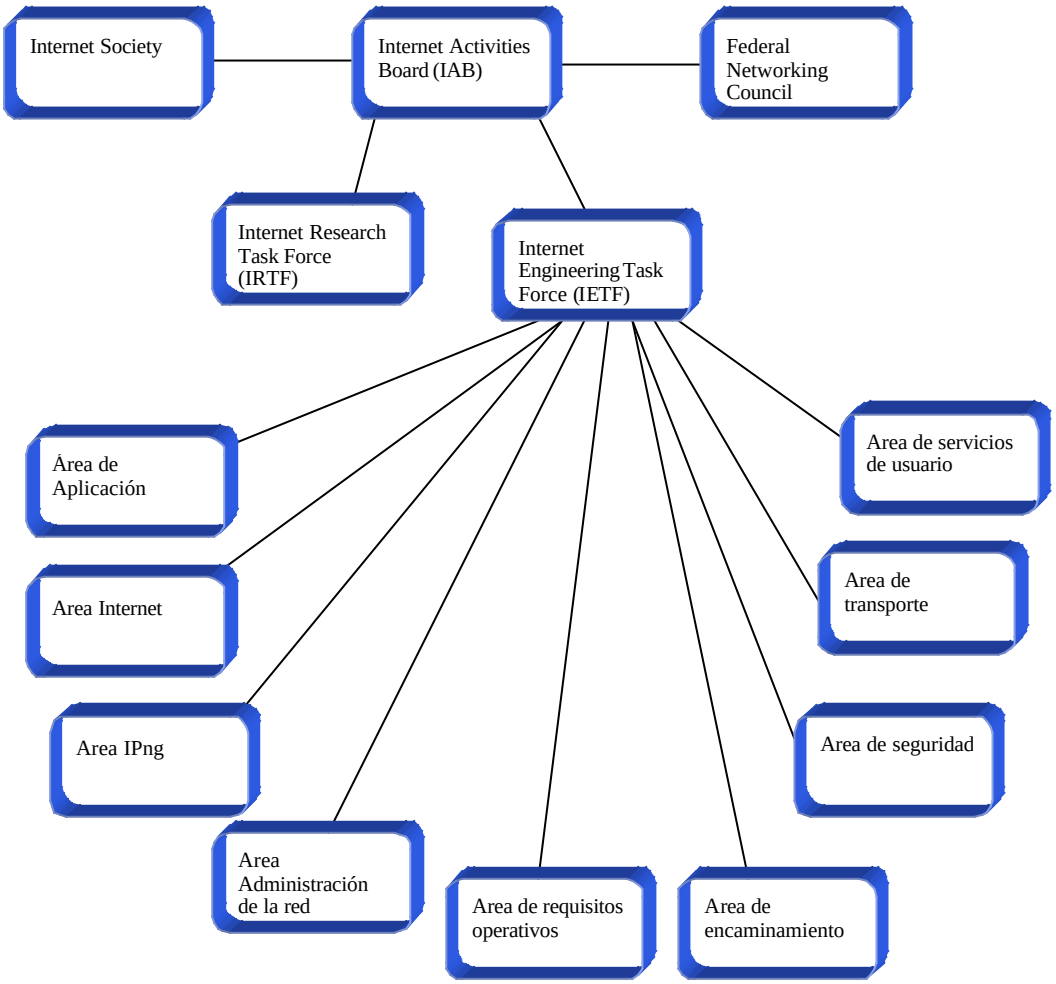


Figura 1.3 Organización del IAB

1.4 Modelo de Referencia OSI frente a TCP / IP

A continuación se detalla la relación de TCP / IP con respecto al modelo de referencia OSI (Open Systems Interconnection) de la ISO. Sesion

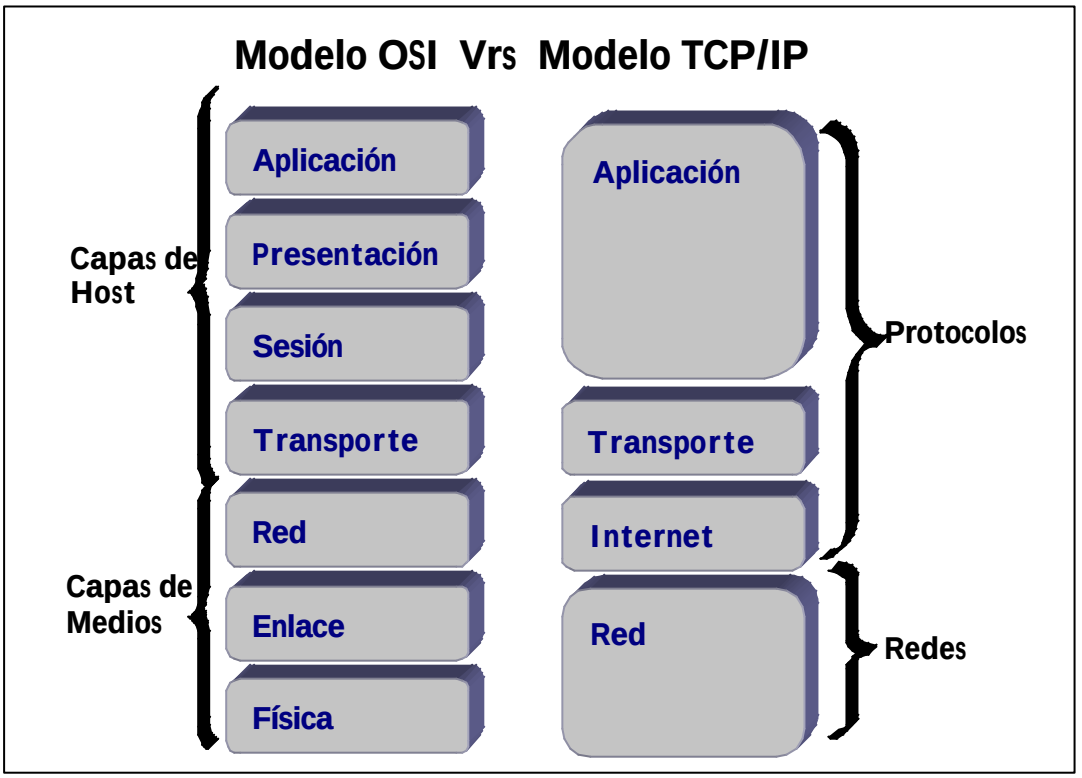


Fig 1.4 OSI vs. TCP/IP

El modelo de referencia OSI fue desarrollado en capas con el propósito de que la una fuese independiente de la otra. *[LIB002]*

Estas capas son:

Física. Comunica directamente con el medio de comunicación, tiene dos responsabilidades enviar y recibir bits.

Enlace de Datos **(trama de datos).** Proporciona comunicación ***nodo*** a nodo en una misma LAN, sus funciones son: proporcionar un mecanismo de direcciones que permita entregar los mensajes en los nodos correctos y debe traducir los mensajes de las capas superiores en bits que puedan ser transmitidos por la capa física.

***Red* (paquete de datos).** Dirige los mensajes de una red a otra. Añade al mensaje una cabecera con la dirección de red de origen y de destino (encamina)

***Transporte* (datagramas).** Divide en fragmentos que coinciden con el límite del tamaño de la red, al otro lado los reensambla. Asigna puertos al mensaje según su proceso para que se comunique con el correspondiente proceso. Y su entrega puede ser fiable: detecta errores y no fiable: no detecta errores.

Sesión. Controla los diálogos entre distintos nodos, establece conexión, transfiere y libera la conexión

Presentación. Traduce de un formato de datos a otro, también encripta y desencripta.

Aplicación. Proporciona los servicios usados por las aplicaciones para que lo usuarios se comuniquen a través de la red

Así como el modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por 4 niveles :

El nivel de acceso a la red [enlace y físico]. Se encarga del intercambio de datos entre un ***host*** y la red y entre dispositivos de la misma red

***El nivel de interred* [Red, IP].** Se encarga de encaminar los mensajes a través de las interredes. El protocolo TCP/IP de esta capa es IP que implementa un sistema de direcciones lógicas de host denominadas *"direcciones IP"*. Estas son usadas por la capa de interred y las superiores para identificar los dispositivos y realizar el encaminamiento entre las redes.

La capa host a host.(transporte). Protocolo proveedor de servicio [Transporte, TCP o UDP] se encarga de la integridad de los datos de punto a punto.

Nivel de aplicación. Abarca las funciones de las capas de sesión presentación y aplicación de OSI.

OSI distingue de forma clara los servicios (lo que una capa hace), las interfaces (cómo se pueden acceder a los servicios) y los protocolos (implementación de los servicios). TCP/IP no lo hace así, no dejando de forma clara esta separación. OSI fue definido antes de

implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente. TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación. TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola capa. TCP/IP parece ser más simple porque tiene menos capas.
Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, no se crean redes a partir de protocolos específicos relacionados con OSI, aunque todo el mundo utiliza el modelo OSI como guía. *[WWW021]*

1.4.1 El Protocolo Internet (Internet Protocol - IP)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP. Las características de este protocolo son:

- No orientado a conexión
- Transmisión en unidades denominadas datagramas.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

La forma general de un datagrama es la siguiente:

ENCABEZADO DEL DATAGRAMA	ÁREA DE DATOS DEL DATAGRAMA

Un datagrama se divide en áreas de encabezado y datos. El encabezado del datagrama contiene la dirección de la fuente y del destino, contiene también un campo de tipo que identifica el contenido del datagrama. El IP no especifica el formato del área de datos; el datagrama se puede utilizar para transportar datos arbitrarios.

Un arreglo de campos en un datagrama es el siguiente:

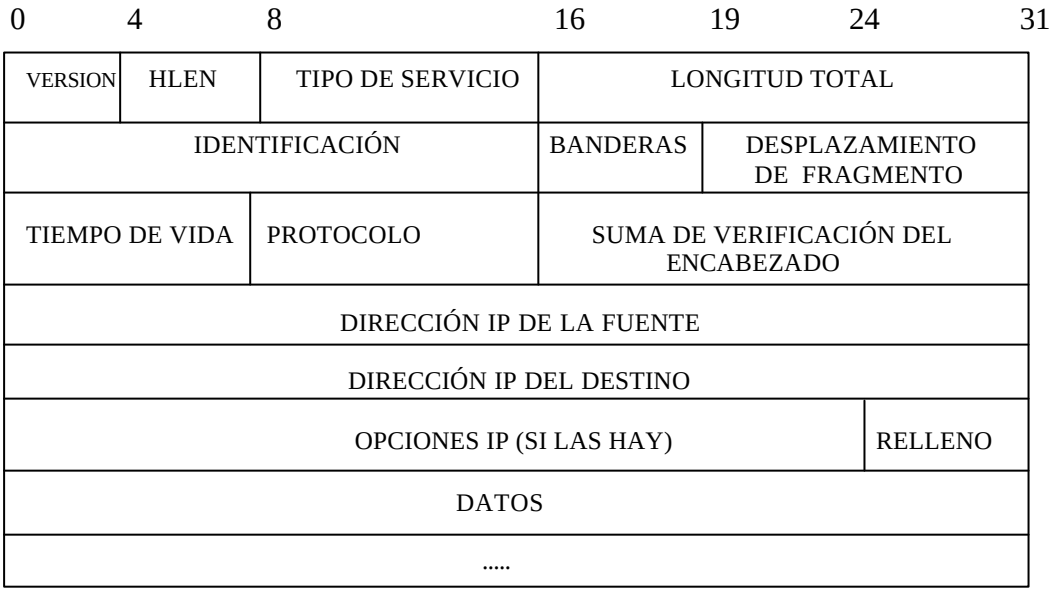


Figura 1.5 Datagrama IP

Explicación del Datagrama IP

Version	contiene la versión del protocolo IP
Hlen	Tamaño de la cabecera en palabras.
TOS	Tipo de servicio. Se especifica prioridad y tipo de transporte
Longitud Total	Mide en bytes la longitud de todo el Datagrama. Permite calcular el tamaño del campo de datos: Datos = Longitud Total – 4 * Hlen.
Identificación	Numero de 16 bits que identifica al Datagrama, que permite implementar números de secuencias y que permite reconocer los diferentes fragmentos de un mismo Datagrama, pues todos ellos comparten este numero.
Banderas	Un campo de tres bits donde el primero está reservado. El segundo, llamado bit de No - Fragmentación significa: 0 = Puede fragmentarse el Datagrama o 1 = No puede fragmentarse el Datagrama. El tercer bit es llamado Más – Fragmentos y significa: 0 = Unico fragmento o Ultimo fragmento, 1 = aun hay más fragmentos. Cuando hay un 0 en más – fragmentos, debe evaluarse el campo desp. De Fragmento: si este es cero, el Datagrama no esta fragmentado, si es diferente de cero, el Datagrama es un último fragmento.
Desp. de Fragmento	A un trozo de datos se le llama Bloque de Fragmento. Este campo indica el tamaño del desplazamiento en bloques de fragmento con respecto al Datagrama original, empezando por el cero

TTL	Tiempo de Vida del Datagrama, especifica el numero de segundos que se permite al Datagrama circularpor la red antes de ser descartado
Protocolo	Especifica que protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos de Datagrama IP. Algunos valores posibles son: 1 = ICMP, 6 = TCP, 17 = UDP, 88 = IGRP (Protocolo de Enrutamiento de Pasarela Interior de CISCO).
Suma de verificación	Es un campo de 16 bits que se calcula haciendo el complemento a uno de cada palabra de 16 bits del encabezado, sumándolas y haciendo su complemento a uno. Esta suma hay que recalcularla en cada nodo intermedio debido a cambios en el TTL o por fragmentación
Dirección IP de la Fuente	Dirección IP de la Fuente
Dirección IP del Destino	Dirección IP del Destino
Opciones IP	Existen hasta 40 bytes extra en la cabecera del Datagrama IP que pueden llevar una o más opciones. Su uso es bastante raro
Datos	Datos del datagrama

Tabla 1.1 Explicacion del Datagrama IP

El tamaño máximo posible de un datagrama IP es 2^{16} o 65.535 octetos.La entrega del datagrama en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje. Por otra parte, el IP no contiene suma de verificación para el contenido de datos del datagrama, solamente para la información del encabezado. *[LIB004]*

1.4.2 Direccionamiento IP

El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Unicamente el NIC (Centro de Información de Red) asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro).

CLASE	Dirección más baja	Dirección más alta
CLASE A	0.1.0.0	126.0.0.0
CLASE B	128.0.0.0	191.255.0.0
CLASE C	192.0.1.0	223.255.255.0
CLASE D	224.0.0.0	239.255.255.255
CLASE E	240.0.0.0	247.255.255.255

Tabla 1.2 Clases de direcciones IP

Clase A

Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir. Local (hostid) en donde se identifica la red y el host dentro de la red.

La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits (de orden más alto).

Las direcciones de Clase A corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

Clase B

Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 host en cada una.

Clase C

Las direcciones de Clase C tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Por último, las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Clase E

Cabe decir que, las direcciones de clase E (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits. Por comodidad estos bits se representan como si estuviesen separados por un punto.

A partir de una dirección IP, una red puede determinar si los datos se enviarán a través de una compuerta (Gateway, Router). Obviamente, si la dirección de la red es la misma que la dirección actual (enrutamiento a un dispositivo de red local, llamado host directo), se evitará la compuerta; pero todas las demás direcciones de red se enrutarán a una compuerta para que salgan de la red local.

La compuerta que reciba los datos que se transmitirán a otra red, tendrá entonces que determinar el enrutamiento con base en la dirección IP de los datos y una tabla interna que contiene la información de enrutamiento.

Otra de las ventajas que ofrece el direccionamiento IP es el uso de direcciones de difusión (broadcast addresses), que hacen referencia a todos los host de la misma red. Según el estándar, cualquier dirección local (hostid) compuesta toda por 1s está reservada para difusión (broadcast). Por ejemplo, una dirección que contenga 32 1s se considera un mensaje difundido a todas las redes y a todos los dispositivos. Es posible difundir en todas las máquinas de una red alterando a 1s toda la dirección local o de anfitrión (hostid), de manera que la dirección 147.10.255.255 para una red de Clase B se recibiría en todos los dispositivos de dicha red; pero los datos no saldrían de dicha red.

Consideremos la siguiente dirección IP en binario:

11001100.00001000.00000000.10101010 (204.8.0.170)

La dirección de la máscara (MASK) es en binario:

11111111.11111111.11100000.00000000 (255.255.224.0)

Según lo visto anteriormente, para hallar la dirección se SubRED (SubNet) tomamos la IP y considerando que todo lo que tenga 1s en la máscara se queda como esta en la IP, y todo lo que tenga 0s en la mascara se pone a 0 en la IP. Entonces, la dirección de SubRed es:

11001100.00001000.00000000.00000000 (204.8.0.0)

1.4.3 Direcciones de red y de difusión

La mayor ventaja de la codificación de información de red en las direcciones de red en IP tiene una ventaja importante: hacer posible que exista un ruteo eficiente. Las direcciones IP

se pueden utilizar para referirse a redes así como a anfitriones individuales. Por regla, una dirección que tiene todos los bits del campo hostID a 0, se reserva para referirse a la red en sí misma.

Otra ventaja significativa del esquema de direccionamiento IP es que éste incluye una dirección de difusión (BROADCAST) que se refiere a todos los anfitriones de la red. De acuerdo con el estándar, cualquier campo hostID consistente solamente en 1s, esta reservado para la difusión (BROADCAST). Esto permite que un sistema remoto envíe un sólo paquete que será publidifundido en la red especificada.

1.4.4 Resumen de reglas especiales de direccionamiento:

En la práctica, el IP utiliza solo unas cuantas combinaciones de ceros (“esta”) o unos (“toda”). En la siguiente figura se listan las posibilidades.

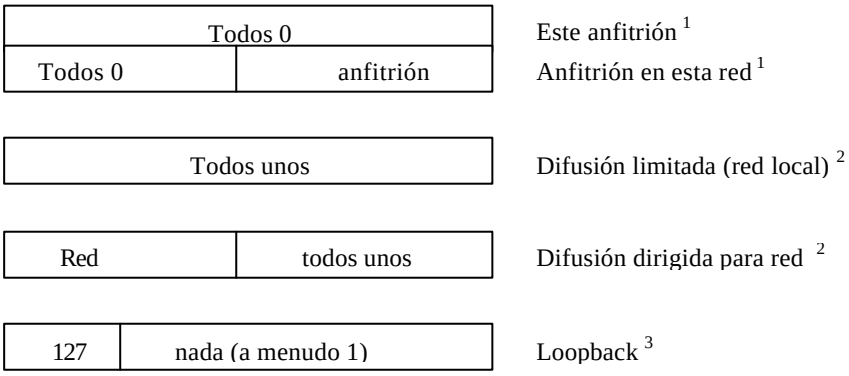


Figura 1.6 Resumen de reglas especiales de direccionamiento

Notas:

1 es permitido solamente en el arranque del sistema pero nunca es una dirección valida de destino.

2 nunca es una dirección válida de origen.

3 Nunca debe aparecer en una red.

1.4.5 Protocolos de resolución de direcciones

Permiten a los programas de un nivel más alto trabajar sólo con direcciones IP en lugar de direcciones físicas (MAC).

ARP	**Protocolo de Asociación de Direcciones.**
RARP	**Protocolo de Asociación de Direcciones por replica.**

Protocolo de Asociación de Direcciones (ARP):

El ARP permite que un anfitrión encuentre la dirección física de otro anfitrión dentro de la misma red física con sólo proporcionar la dirección IP de su objetivo. La información se guarda luego en una tabla ARP de orígenes y destinos.

La idea detrás de la asociación dinámica con ARP es muy sencilla: cuando un host A quiere definir la dirección IP, transmite por difusión (broadcast) un paquete especial que pide al anfitrión (host) que posee la dirección IP, que responda con su dirección física. Todos los anfitriones reciben la solicitud, incluyendo a B, pero sólo B reconoce su propia dirección IP y envía una respuesta que contiene su dirección física. Cuando A recibe la respuesta, utiliza la dirección física para enviar el paquete IP directamente a B. *[WWW021]*

Los datos en los paquetes ARP no tienen un encabezado con formato fijo. Para hacer que ARP sea útil para varias tecnologías de red, la longitud de los campos que contienen direcciones depende del tipo de red.

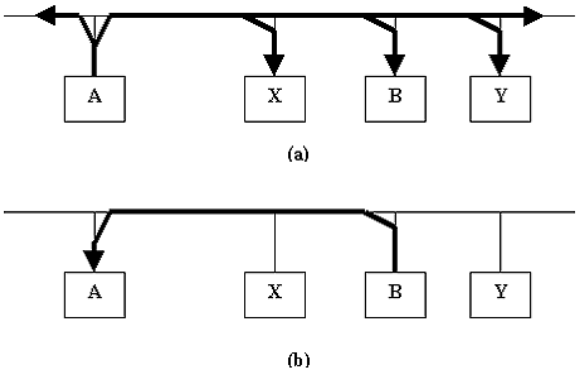


Figura 1.7 Esquema de funcionamiento ARP

Para determinar la dirección física de B, desde su dirección IP, el anfitrión A transmite por difusión una solicitud ARP que contiene a todas las máquinas en la subred, y el anfitrión B envía una respuesta ARP que contiene la dirección física.*[WWW001]*

Protocolo de Asociación de Direcciones por Réplica (RARP):

Una máquina sin disco utiliza RARP (Protocolo Inverso de Asociación de Direcciones), a fin de obtener su dirección IP desde un servidor.

En el arranque del sistema, utiliza la dirección de red para obtener la dirección IP de la máquina, transmite por difusión la solicitud RARP. Los servidores en la red reciben el mensaje, buscan la transformación en una tabla y responden al transmisor. Una vez que la máquina obtiene su dirección IP, la guarda en memoria y no vuelve a utilizar RARP hasta que se inicia de nuevo.

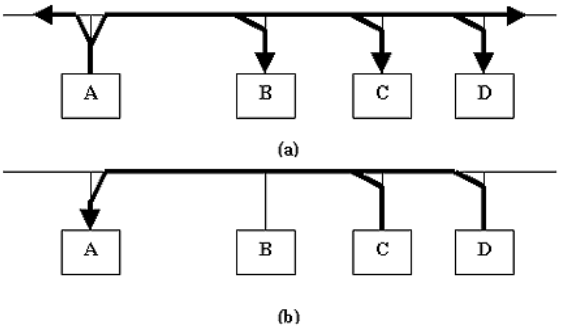


Figura 1.8 Esquema de funcionamiento RARP

Ejemplo de un intercambio en el que se utiliza el protocolo RARP. la máquina A transmite por difusión una solicitud RARP especificándose como destino y las máquinas autorizadas para proporcionar el servicio RARP (C y D) responden directamente a *A. [WWW001]*

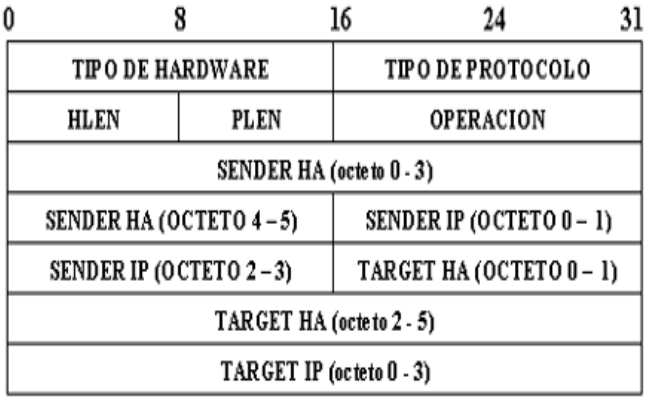


Figura 1.9 Formato de mensaje ARP/RARP

Tipo de Hardware	Especifica un tipo de interfaz de hardware para el que el transmisor busca una respuesta; contiene el valor 1 para Ehternet De forma similar
Tipo de Protocolo	Especifica el tipo de dirección de protocolo de alto nivel que proporcionó el transmisor. contiene 0800_{16} para la dirección IP
Operación	Especifica una solicitud ARP (1), una respuesta ARP (2), una solicitud RARP (3) o una respuesta RARP (4)

HLEN	Longitud de la dirección de hardware
PLEN	Longitud de la dirección del protocolo de alto nivel
SENDER HA	Dirección de hardware del transmisor.
SENDER IP	Dirección IP del transmisor.
TARGET HA	Dirección de hardware del objetivo (RARP), proporcionada por el transmisor
TARGET IP	Dirección IP del objetivo (ARP), proporcionada por el transmisor

1.4.6 Mensajes de error y control en IP (ICMP)

El ***ICMP*** permite que los routers envíen mensajes de error o de control hacia otros routers o anfitriones

Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

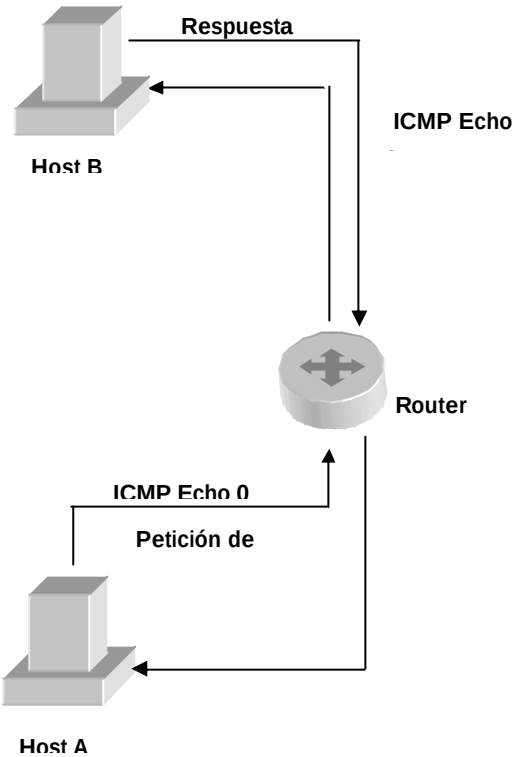
Formato de los mensajes ICMP

Cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo TYPE (TIPO) de mensaje, de 8 bits y números enteros, que identifica el mensaje; un campo CODE (CODIGO), de 8 bits, que proporciona más información sobre el tipo de mensaje, y una campo CHECKSUM (SUMA DE VERIFICACIÓN), de 16 bits. Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema. El campo TYPE de ICMP define el significado del mensaje así como su formato.

TIPO (8 o 0)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Datos Opcionales		

Tabla 1.3 **Formato de los mensajes ICMP**

Esquema ICMP



El Host A usa Echo para detectar si el Host B esta activo en la red. Envía el "echo 8" ICMP al Host B, el Host B cambia el tipo del mensaje a "echo reply 0" y devuelve el datagrama al Host A.

Una de las herramientas de depuración más utilizadas incluye los mensajes ICMP de echo request (8) y echo reply (0). En la mayoría de los sistemas, el comando que llama el usuario para enviar solicitudes de eco ICMP se conoce como ping.

Los mensajes de ICMP requieren doble encapsulacion: Los mensajes ICMP viajan empaquetados en Datagramas IP. Aun así, no se considera a ICMP un protocolo de nivel superior a IP. *[WWW002]*

1.4.7 Sistema de Nombre de Dominio (DNS)

Los host en Internet se identifican entre sí mediante una **dirección IP** (216.32.74.52) pero es mas facil de recordar nombres como www.yahoo.com, y esto ofrece la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él. Para realizar esta conversión entre nombres y direcciones IP se utilizan los servidores ***DNS***. *[WWW023]*

La estructura

Un sistema de nombres de dominio (DNS) consta de una base de datos de nombres distribuida. Los nombres de la base de datos DNS establecen una estructura lógica de árbol, conocida como *espacio de nombres del dominio*. Cada nodo o dominio del espacio de nombres del dominio tiene un nombre y puede contener subdominios. Los dominios y subdominios se agrupan en zonas para permitir la administración distribuida del espacio de nombres.

El nombre del ***dominio*** identifica la posición del mismo en la jerarquía lógica del DNS respecto de su dominio principal, al separar cada rama del árbol con un punto. En la siguiente figura se muestran varios dominios superiores, entre los que se encuentra **Midominio**, y un host llamado **host**, dentro del dominio **midominio.com**. Si alguien quisiera contactar con ese host, usarían el nombre completo host.midominio.com.

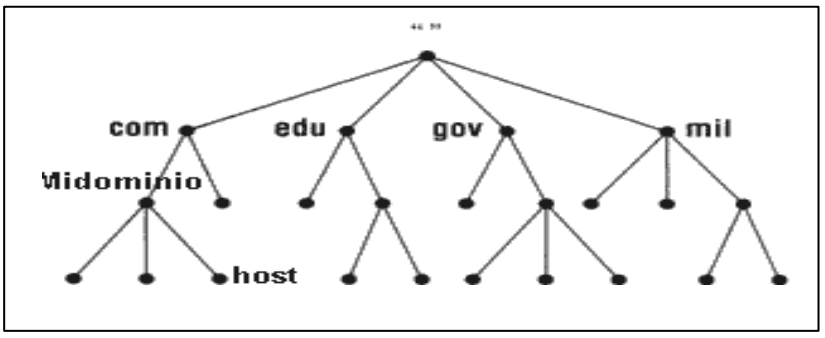


Figura 1.10 Estructura de Dominios DNS

1.5 Problemas con IPv4

La necesidad de un espacio de direcciones extenso está forzando un cambio inmediato en el IP, otros factores que también contribuyen. Son soporte de nuevas aplicaciones. Por ejemplo, debido a que el audio y el video en tiempo real necesitan determinadas garantías en los retardos, una nueva versión del IP debe proporcionar un mecanismo que haga posible asociar un datagrama con una reservación de fuente preasignada. Además, como varias de las nuevas aplicaciones de Internet necesitan comunicaciones seguras, una nueva versión del IP deberá incluir capacidades que hagan posible autenticar al emisor y que brinden seguridad a nivel de red. *[LIB006]*

La escasez de direcciones hace que haya menos direcciones disponibles para ser asignadas, limita el crecimiento de Internet, obstaculiza el uso de Internet a nuevos usuarios, el ruteo es ineficiente, provoca que los usuarios usen NAT
Podemos resumir los problemas de IPv4 en la siguiente tabla:

Independencia de medio y/o protocolo (*IP over everything*)	• IP incluye un sistema de direccionamiento independiente del medio/protocolo subyacente, incluyendo gestión del encaminamiento. • El sistema de direccionamiento no asegura que las direcciones de emisor y receptor sean auténticas: • IPv4 incluye un mecanismo de fragmentación y reensamblado. IPv6 prohíbe la fragmentación en nodos intermedios.
Transporte de datos sin estado (orientado a datagramas)	• Cada paquete recibe tratamiento independiente • No hay reserva de recursos • Protocolos y aplicaciones por encima de IP a veces necesitan este estado, y eso tiene implicaciones para IPsec

Servicio no fiable	• IP ofrece un servicio no fiable en dos sentidos: o no se garantiza la entrega de un datagrama o no se comprueba la integridad de los datos del datagrama (sí, en parte, de la cabecera) • TCP (sobre todo) se encarga de asegurar la entrega, mediante asentimientos y retransmisiones, pero lo hace extremo a extremo. • Consecuencia: Ni IP ni TCP tienen un control exacto del tráfico, lo que permite eliminar, redirigir o inyectar datagramas «al vuelo».
Problemas más acuciantes: • Escasez de direcciones • Explosión del tamaño de tablas de encaminamiento	
Sistema de asignación basado en clases muy ineficiente: falta de flexibilidad en la asignación de rangos de direcciones. Consecuencias: • Agotamiento de direcciones clase B (corto plazo) • Agotamiento del espacio total de direcciones IP (medio plazo)	

Tabla 1.4 Problemas de IPv4

Soluciones

Expansión de las capacidades de direccionamiento. IPv6 incrementa el tamaño de las direcciones de 32 bits (IPv4) a 128 bits, para soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de autoconfiguración de direcciones. Se añade un nuevo tipo de dirección, la llamada "anycast", de forma que es posible enviar un paquete a cualquier nodo entre un grupo de ellos.
Simplificación de la cabecera. Algunos campos de la cabecera del IPv4 son eliminados o pasan a ser opcionales, tanto para reducir el coste de procesamiento como el tamaño de la cabecera.

Mayor flexibilidad para extensiones y nuevas opciones. *En IPv6 no existe un campo "opciones", como tal. La gestión de opciones se realiza por un campo "siguiente cabecera". Eliminando así las limitaciones de tamaño en la cabecera, e introduciendo una gran flexibilidad en el desarrollo de nuevas opciones.*
Capacidades de control de flujo. Se añaden capacidades que permiten marcar los paquetes que pertenezcan a un determinado tipo de tráfico, para el cual el remitente demanda una calidad mayor a la especificada por defecto o servicios en tiempo real.
Capacidades de autenticación y privacidad de datos. *IPv6 provee extensiones para soportar autenticación, e integridad y confidencialidad de datos.*

Tabla 1.5 Soluciones que brinda IPv6

1.6 IPv4 versus IPv6. ¿Porque cambiar a IPv6?

La versión 4 del protocolo de Internet IP proporciona los mecanismos de comunicación básicos del conjunto TCP/IP y la red global Internet; ha probado ser un diseño flexible y poderoso se ha mantenido casi sin cambio desde su inserción a fines de los años setenta. Desde el momento en que se diseñó el IPv4, el desempeño de los procesadores se ha incrementado exponencialmente, el tamaño de las memorias se ha incrementado, al igual que el ancho de banda de la columna vertebral de la red Internet se ha incrementado, las tecnologías LAN han emergido y el número de anfitriones en Internet ha crecido hasta llegar por mas de 4 millones. Además, los cambios no ocurren de manera simultánea, el IP se ha adaptado a los cambios de una tecnología antes de adaptarse a los cambios de otras.

A pesar de su diseño, el IPv4 también debe ser reemplazado. El inminente agotamiento del espacio de direcciones. Cuando el IP se diseñó, un espacio de 32 bits era más que suficiente. Sólo un puñado de organizaciones utilizaba las LAN; pocas tenían una WAN corporativa. Ahora, sin embargo, muchas corporaciones de tamaño mediano tienen varias LAN y varias de las grandes corporaciones cuentan con una WAN corporativa. En

consecuencia, el espacio de direcciones IP de 32 bits que se usa actualmente no puede adaptarse al crecimiento proyectado de la red global de Internet. *[WWW022]*

La tecnología básica TCP/IP ha funcionado bien por mucho tiempo. ¿Por qué debería cambiarse? En términos generales, los procesos que estimulan la evolución del TCP/IP y de la arquitectura de Internet son los siguientes:

- **Nuevas tecnologías de comunicación y computación**
- **Nuevas aplicaciones**
- **Incrementos en el tamaño y en la carga**
- **Multiprotocolo**
- **Seguridad**
- **Tiempo Real**
- **Tarificación**
- **Comunicaciones Móviles**
- **Facilidad de Gestión**
- **Política de enrutado**

- **Nuevas tecnologías de comunicación y computación:**

Los investigadores e ingenieros que trabajan en los protocolos TCP/IP mantienen un agudo interés por las nuevas tecnologías. Tan pronto como una nueva computadora de alta velocidad está disponible, la utilizan en anfitriones y ruteadores. En cuanto una nueva tecnología de red emerge, la utilizan para transportar datagramas IP, creando nuevas necesidades de funcionalidades en los protocolos actuales.

- **Nuevas aplicaciones:**

Las nuevas aplicaciones constituyen una de las fronteras de investigación y desarrollo de Internet más interesantes y por lo general crean una demanda de infraestructura o servicios que los protocolos actuales no pueden proporcionar. Por ejemplo, el interés creciente en multimedios ha creado una demanda de protocolos que puedan transferir imágenes y sonido eficientemente. De la misma forma, el interés en la comunicación en tiempo real de audio y video ha creado una demanda de protocolos que puedan garantizar la entrega de la información con retardos fijos, así como protocolos que puedan sincronizar audio y video con flujos de datos.

- **Incrementos en el tamaño y en la carga:**

La red global de Internet ha tenido varios años de crecimiento exponencial.
Sorpresivamente, la carga de tráfico en Internet ha crecido más rápido que el número de redes. El incremento en el tráfico puede atribuirse a varias causas. En primer lugar, la población de Internet cambió, deja de estar formada por académicos e investigadores, la gente ahora utiliza Internet luego de sus horas de trabajo para actividades comerciales y de entretenimiento. En segundo lugar, las nuevas aplicaciones que transfieren imágenes y video en tiempo real generan más tráfico que las aplicaciones que transfieren texto. En tercer lugar, las herramientas de búsqueda automatizada generan una cantidad sustancial de tráfico y lo hacen más lento al sondear en las localidades de Internet para encontrar datos.

- **Multiprotocolo:**

Cada vez resulta más necesaria la convivencia de diversas familias de protocolos: IP, OSI, IPX... Se necesitan mecanismos que permitan abstraer al usuario de la tecnología subyacente para permitir que concentre su atención en los aspectos realmente importantes de su trabajo. Se tiende, pues, hacia una red orientada a aplicaciones, que es con lo que el usuario interacciona, más que a una red orientada a protocolos (como hasta el momento).

- **Seguridad:**

El mundo IPv4 es el mundo académico, científico, técnico y de investigación. Un ambiente, en general, que podría calificarse como "amigable", desde el punto de vista de la gestión y la seguridad en la red. Con la aparición de servicios comerciales y la conexión de numerosísimas empresas, el enorme incremento en el número de usuarios y su distribución por todo el planeta, y la cantidad, cada vez mayor, de sistemas que necesitan de Internet para su correcto funcionamiento, etc., es urgente definir unos mecanismos de seguridad a nivel de red. Son necesarios esquemas de autentificación y privacidad, tanto para proteger a los usuarios en sí como la misma integridad de la red ante ataques malintencionados o errores.

- **Tiempo Real:**

IPv4 define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. A pesar de que en la cabecera IP hay un campo destinado a fijar, entre otras cosas, la prioridad del datagrama, en la práctica ello no supone ninguna garantía. Se necesita una extensión que posibilite el envío de tráfico de tiempo real, y así poder hacer frente a las nuevas demandas en este campo.

- **Tarificación:**

Con una red cada día más orientada hacia el mundo comercial hace falta dotar al sistema de mecanismos que posibiliten el análisis detallado del tráfico, tanto por motivos de facturación como para poder dimensionar los recursos de forma apropiada.

- **Comunicaciones Móviles:**

El campo de las comunicaciones móviles está en auge, y aún lo estará más en un futuro inmediato. Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios. La seguridad de las comunicaciones, en este tipo de sistemas, se ve, además, especialmente comprometida.

- **Facilidad de Gestión:**

Con el volumen actual de usuarios y su crecimiento estimado, resulta más que obvio que la gestión de la red va a ser una tarea ardua. Es preciso que la nueva arquitectura facilite al máximo esta tarea. Un ejemplo de ello sería la autoconfiguración de los equipos al conectarlos a la red.

- **Política de enrutado:**

Tradicionalmente los datagramas se han encaminado atendiendo a criterios técnicos tales como el minimizar el número de saltos a efectuar, el tiempo de permanencia en la red, etc. Cuando la red pertenece a una única organización eso es lo ideal, pero en el nuevo entorno económico en el que diferentes proveedores compiten por el mercado. Es imprescindible que la fuente pueda definir por qué redes desea que pasen sus datagramas, atendiendo a criterios de fiabilidad, coste, retardo, privacidad, etc. Internet se expande hacia nuevas industrias y nuevos países, cambiando de forma fundamentalmente adquiere nuevas autoridades y políticas administrativas. Muchos de los esfuerzos de investigadores e ingenieros alrededor del TCP/IP continúan enfocados a encontrar formas de adaptarse a nuevos grupos administrativos.

1.7 Historia del IPv6

En Internet hubo una crisis en 1990. El espacio para direcciones de bits definido por lPv4 se estaba agotando. Más agobiante era el crecimiento masivo en el tamaño de las tablas de encaminamiento de los encaminadores de Internet. Si estas tablas seguían creciendo, no parecía posible seguir fabricando encaminadores lo suficientemente potentes como para afrontar reto. El desarrollo de la versión 6 de IP comenzó en 1992 como respuesta a esta crisis. *[LIB008]*

La versión 6 del Protocolo de Internet fue desarrollada para afrontar estos problemas. IPv6 utiliza direcciones de 128 bits, lo cual crea un nuevo espacio para direcciones muy vasto. Además, IPv6 aborda la complejidad de la configuración de los hosts, lo que estaba obstaculizando la velocidad de despliegue de IP. Los diseñadores de lPv6 no mejoraron las

partes del protocolo que ya funcionaban bien. Evitaron añadir complejidad a los protocolos. El resultado es que se ha simplificado la estructura del paquete IPv6, y es razonable esperar que una pila de protocolo IPv6 se comporte igual o mejor que una implementación IPv4 en el mismo host.

Mientras IPv6 todavía estaba en desarrollo, se ideó una solución que plantaba cara al crecimiento explosivo de las tablas de encaminamiento de IPv4 Se desarrolló el Encaminamiento Inter Dominio Sin Clase (CIDR), y se desplegó a través el protocolo BGP Esto redujo en gran medida el número de rutas mantenidas en los encaminadores de Internet.

Además, la adopción de redes privadas ha reducido algo la presión sobre el espacio para direcciones. Esto es un alivio aunque retrasa lo inevitable: la actualización de redes más grande y compleja del mundo.

Dado el estado de las cosas la versión 6 de IP está esperando ahora a iniciar la transición En esta vía hay mucha investigación y pruebas, una red IPv6 que se esta construyendo sobre la versión IPv4 existente.

1.7.1 Desarrollo de una nueva versión del IP

Nº de versión IP	Denominación
0-3	No asignado
4	Internet Protocol (actual)
5	ST (Stream Protocol)
6	SIP-SIPP-IP v6
7	IP v7- TC/IX-CAT NIP

8	Pip
9	TUBA
10-15	No asignado

Tabla 1.6 Versiones del protocolo IP

Los grupos en el ***IETF*** han estado trabajando para formular una nueva versión del IP por varios años, han invitado a toda la comunidad a participar en el proceso de estandarización, investigadores, fabricantes de computadoras, vendedores de hardware y software de red, programadores, administradores, usuarios, compañías telefónicas y televisoras por cable han especificado sus requerimientos para la próxima versión IP y han comentado todos sus propuestas específicas.

Se han propuesto muchos diseños para servir a un propósito en particular o a una comunidad en especial. Uno de los diseños propuestos haría al IP más sofisticado y el costo por el incremento en la complejidad de procesamiento se elevaría. Otro diseño propone utilizar una modificación protocolo CLNS de OSI. Un tercer diseño mayor propone conservar la mayor parte de las ideas del IP, y hacer extensiones para adaptarlo a direcciones extensas. El diseño conocido como SIP (Simple IP) ha sido la base para una propuesta extendida que incluye ideas de otras propuestas la versión extendida del SIP ha sido llamada Simple IP Plus (SIPP) y finalmente emerge como el diseño elegido como base para el próximo IP.

La selección de la nueva versión del IP no ha sido fácil por la pugna entre muchos grupos por favorecerse. Además, se han involucrado algunas personalidades algunas opiniones técnicas individuales se mantienen fuertemente. En consecuencia, las discusiones han generado argumentaciones acaloradas.

1.7.2 Nombre del próximo IP

IAB publicó una declaración política que se refería a la próxima versión como IP versión 7, este error ocurrió porque el protocolo ST estaba asignado como la versión número 5 y uno de los documentos disponibles por el IAB reportaba erróneamente a la versión actual como la versión 6.

Para evitar la confusión, el IETF cambió el nombre, eligió "IP - la próxima generación" y el esfuerzo comenzó a conocerse como ***IPng***.

Formalmente, se ha decidido que a la próxima versión del IP se le asigne el número de versión 6. En el pasado, el término IPng ha sido utilizado en un contexto amplio para referirse a todas las discusiones y propuestas para una próxima versión del IP, mientras que el término IPv6 se ha utilizado para referirse a una propuesta específica que proviene del IETF. IPng se refiere a todos los esfuerzos relacionados con el desarrollo de una nueva generación del IP. *[WWW022]*