



## CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

[www.cef.es](http://www.cef.es)

[info@cef.es](mailto:info@cef.es)

## Índice Tema 4

---

1. El modelo OSI de ISO.
2. El modelo SNA.
3. Comparación con OSI.
4. SNA de segunda generación: APPN.
  - 4.1. LU 6.2.
  - 4.2. Nodos tipo 2.1.
  - 4.3. APPN (Advanced Peer-to-Peer Networking).
  - 4.4. Funcionamiento de APPN.
5. El modelo TCP/IP.
6. Protocolo IPv6.





## CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

### TEMA 4

**El modelo OSI de ISO. El modelo SNA. Comparación con OSI. SNA de segunda generación: APPN. El modelo TCP/IP. Protocolo IPv6.**

#### 1. EL MODELO OSI DE ISO.

El Open Systems Interconnection (OSI) fue originalmente definido por la Internacional Standards Organisation (ISO) como un modelo de referencia para la comunicación en Sistemas Abiertos. El modelo de referencia OSI consiste en una jerarquía de siete niveles de protocolos cada uno de los cuales utiliza los de nivel inferior para ofrecer un determinado servicio.

- CAPA 7. Nivel de APLICACIÓN.
- CAPA 6. Nivel de PRESENTACIÓN.
- CAPA 5. Nivel de SESIÓN.
- CAPA 4. Nivel de TRANSPORTE.
- CAPA 3. Nivel de RED.
- CAPA 2. Nivel de ENLACE.
- CAPA 1. Nivel FÍSICO.

Antes de entrar a analizar el modelo, consideremos las siguientes definiciones:

Protocolo: son las reglas que gobiernan la comunicación entre dos entidades similares, ambas situadas en el mismo nivel de comunicación (por ejemplo, ordenador a ordenador, télex a télex, persona a persona, proceso a proceso).

Interfaz: entre cada par de niveles adyacentes debe existir una interfaz, la cual facilita el entendimiento entre ambos niveles. Para cada interfaz, esta interacción puede ser de naturaleza física o lógica, o puede precisar formatos específicos para los mensajes, etc.

#### A) Nivel físico.

Este nivel se corresponde con la capa 1 del modelo de referencia OSI. Se ocupa de la transmisión en bruto de bits sobre un canal de comunicación. El único condicionante de diseño para esta capa a tener en cuenta es el de asegurarse que cuando se envía un bit a «1», se recibe un «1» y no un «0». En resumen, esta capa se ocupa de los condicionantes mecánicos, eléctricos y del medio físico de transmisión.

Las funciones de este nivel son:

- Establecimiento de caminos físicos en caso de no estar establecidos.
- Detección de errores de las señales eléctricas.
- Independizar a los niveles superiores del tipo de medio usado.
- Determinar los aspectos mecánicos y eléctricos de los conectores, cables o fibras utilizadas.

Las normas más usuales de este nivel son: EIA RS-232-C, EIA RS-449, CCITT X.21, CCITT X.21 bis, y RDSI.

#### B) Nivel de enlace.

Resuelve los problemas planteados por la falta de fiabilidad de los circuitos como consecuencia de los errores en los datos recibidos, inducidos por el ruido de transmisión u otras perturbaciones. La información se divide en tramas, que se envían secuencialmente a medida que el receptor manda hacia atrás validaciones de que han ido llegando correctamente. Una vez establecidos unos criterios mínimos de fiabilidad, ésta puede aumentar en la medida que lo hace el precio del servicio. También existe una relación entre la velocidad de transmisión y el coste del servicio. Todo ello influye en la calidad final que se pretenda ofrecer.

Las funciones de este nivel serían:

- Sincronización de tramas y transparencia.
- Coordinación de la comunicación.
- Control de errores de transmisión.
- Recuperación ante fallos.

- Control de flujo.
- Compartición del circuito físico.

Por último, señalar que el CCITT ha definido el protocolo de nivel de enlace dentro de la recomendación X.25.

#### C) Nivel de red.

Se encarga de la administración de la red, determinando cuántos y por dónde son enviados los paquetes desde la fuente al destino. El enrutamiento puede basarse en tablas de asignación estáticas, que proporcionan un enrutamiento fijado de antemano y que raramente cambia, o también pueden ser altamente dinámicas en las que cada paquete de información que llega recibe un enrutamiento distinto.

Las funciones de este nivel son:

- Responder a una gran variedad de configuraciones.
- Multiplexación de las conexiones.
- Encaminamiento.
- Mantener la secuencialidad de la información.
- Control de flujo.
- Funciones auxiliares, como negociación de facilidades.

El protocolo del nivel de red está definido por el CCITT dentro de su recomendación X.25.

#### D) Nivel de transporte.

La función básica de este nivel es aceptar datos desde el nivel de sesión, dividido en fragmentos más pequeños si es necesario, pasarlos al nivel de red, y asegurarse que todos los fragmentos llegan correctamente al otro extremo. Este nivel debe ser diseñado eficientemente, de forma que aísle al nivel de sesión de los inevitables cambios en la tecnología hardware.

Las funciones de este nivel son:

- Asegurar el trasvase de información extremo a extremo, con independencia del número de nodos intermedios y el tipo de red o redes.
- Se encarga de llevar el control de flujo de la comunicación.
- Permite la comunicación simultánea, utilizando una o varias direcciones de red, de una o varias sesiones de trabajo.

- Dispone de mecanismos para fragmentar y multiplexar la información.
- Este nivel puede utilizar uno o varios circuitos de nivel 3 para establecer comunicaciones simultáneas.

#### E) Nivel de sesión.

Este nivel permite que usuarios en diferentes máquinas establezcan sesiones entre ellos. Al igual que en la capa de transporte, una sesión permite el intercambio ordinario de datos. Entre los servicios más destacados que proporciona este nivel destacan:

- Permitir a un usuario entrar en un sistema remoto a tiempo compartido o transferir ficheros entre dos máquinas.
- En algunos protocolos es esencial que ambas partes no utilicen la misma operación al mismo tiempo.

Para controlar estas actividades esta capa proporciona testigos, cuya posesión permite realizar la operación y una vez finalizada el testigo es pasado.

- Otro servicio es la sincronización. En transmisiones con una duración superior a la tasa de fallo de la red, esta capa inserta puntos de chequeo que permiten reiniciar la transmisión a partir del punto más cercano al posible fallo y no desde el principio.

#### F) Nivel de presentación.

Hemos visto que mientras las capas inferiores se encargan del movimiento de bits y su fiabilidad, esta capa se encarga de la sintaxis y la semántica de la información transmitida.

Funciones de esta capa son:

- Traducciones de alfabetos. Por ejemplo, ASCII-EBCDIC.
- Compresión de mensajes.
- Cifrado de datos.
- Compatibilización de ficheros de distintos formatos.
- Manejo de distintos terminales.

#### G) Nivel de aplicación.

Es el nivel superior y último del modelo. Sus funciones están determinadas por los requerimientos del usuario. Es la capa que contiene un conjunto de protocolos que son comúnmente utilizados. Por ejemplo, consideremos un editor de pantalla que trabajase sobre una red de terminales con características distintas (monitores, teclados diferentes, etc.), en ellos el editor no trabajaría correctamente en todos (caracteres de escape y tamaño de monitores diferentes, etc.). La solución sería definir un terminal virtual abstracto, sobre el que diseñar editores. Todo el software de este terminal virtual descan-

saría sobre el nivel de aplicación. Otra función es la transferencia de ficheros entre sistemas diferentes que difieren en representar las líneas de texto, etc. Aplicaciones adicionales serían:

- Correo electrónico.
- Transferencia de documentos.
- Acceso a bases de datos.
- Etcétera.

#### H) Comunicaciones entre capas.

Para permitir el intercambio de información entre dos capas, debe existir un acuerdo sobre el conjunto de reglas en la interfaz. En una interfaz típica, la capa N+1 pasa una unidad de dato interfaz (IDU) a la capa N, a través del punto de acceso de servicio (SAP). El IDU está compuesto de una unidad de dato de servicio (SDU), e información de control de interfaz (ICI). La SDU es la información pasada a través de la red por las capas superiores a la N+1. El control de la información es necesario para ayudar a las capas inferiores en su trabajo (el número de bytes en la SDU), pero no es parte del dato en sí. Para permitir la siguiente transferencia de la SDU a las capas inferiores, la capa N puede tener que fragmentar esta información en N unidades de datos de protocolo (PDU). Estas cabeceras de PDU son usadas por las entidades pareadas para soportar sus propios protocolos.

En el modelo de referencia OSI, cualquier tipo de operación que se lleve a cabo entre capas puede clasificarse en cuatro grupos:

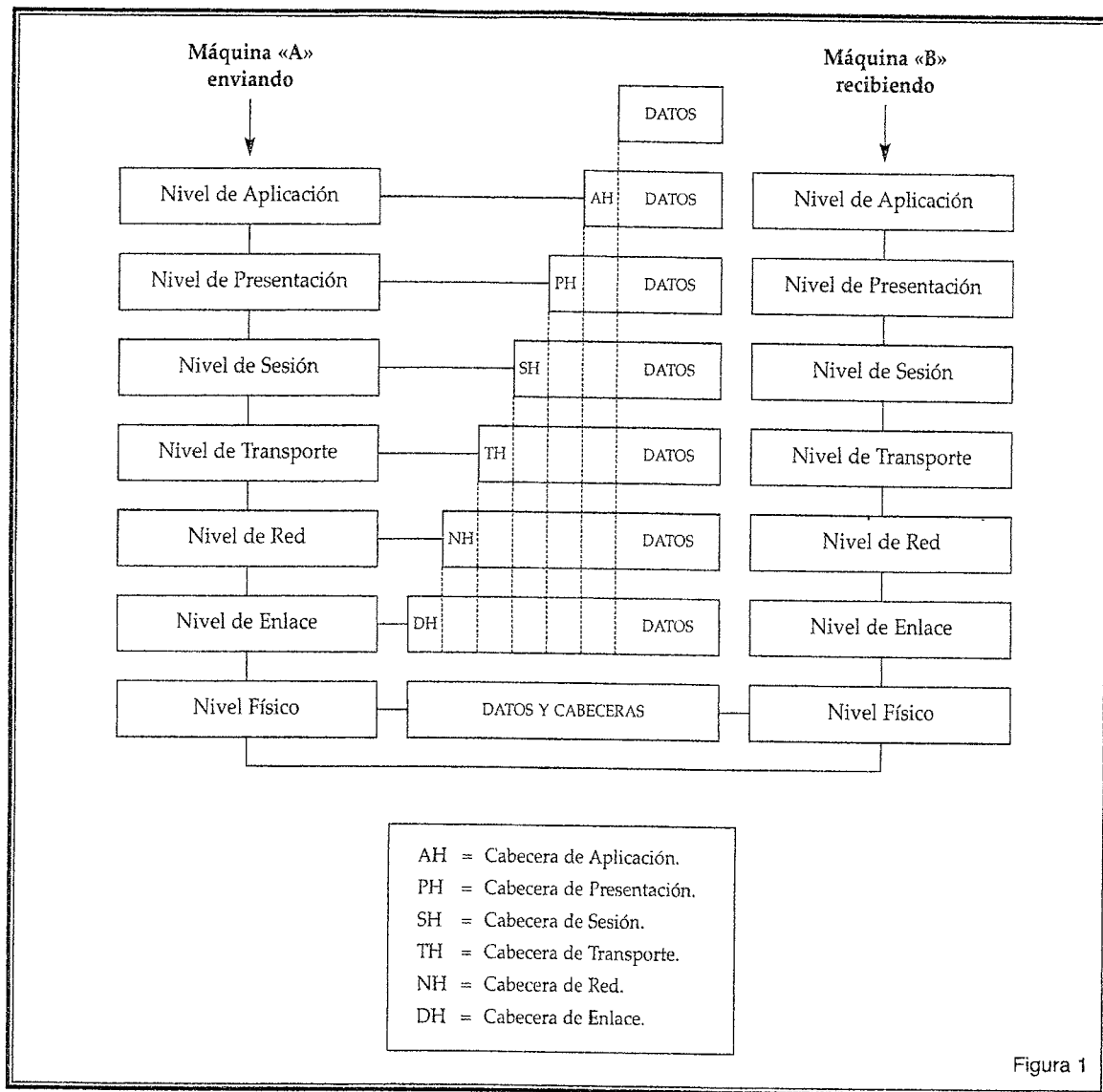
PETICIÓN:	una entidad solicita un servicio para realizar un trabajo.
INDICACIÓN:	una entidad es informada acerca de un suceso.
RESPUESTA:	una entidad responde a un suceso.
CONFIRMACIÓN:	una entidad es informada acerca de su petición.

Para comunicarse dos capas se necesitan tres sucesos:

- Conectarse: realizar la conexión.
- Dato: transmitir los datos deseados.
- Desconectarse: liberar la conexión.

También las comunicaciones entre dos capas se pueden clasificar de confirmadas o inconfirmadas. Una comunicación es confirmada si hay una petición, una indicación, una respuesta y una confirmación y es inconfirmada si sólo hay una petición y una indicación. Teniendo lo anterior en cuenta, el suceso de conectarse es una comunicación confirmada, el suceso de dato puede ser confirmada o inconfirmada dependiendo o no de la necesidad de un reconocimiento y el suceso de desconectarse es siempre inconfirmado.

En la figura siguiente se muestra una representación de los niveles OSI y la forma de establecer un diálogo entre diferentes dispositivos.



## MODELO OSI.

- Nivel físico.
- Nivel de enlace de datos.
  - Ethernet.
  - PPP.
- Nivel de red.
  - IP.
  - IPX.

- Nivel de transporte.
  - UDP.
  - IP.
- Nivel de sesión.
  - TCP.
  - NetBIOS.
  - UDP.
  - IPX.
  - Appletalk.
- Nivel de presentación.
- Nivel de aplicación.
  - SMTP.
  - FTP.
  - Telnet.
  - SSH.
  - IRC.
  - HTTP.
  - POP3.
- Ethernet Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico.
- PPP son las siglas para Protocolo Punto a Punto definido en el RFC 1661. Este protocolo se usa en redes que usen una interconexión Punto por Punto y se diseñó para sustituir a SLIP.
- IP. Internet Protocol. RFC 791. Es el protocolo más básico de Internet, y provee todos los servicios necesarios para el transporte de datos. Cualquier otro protocolo de Internet se basa en IP o le sirve de base.
- IPX. Siglas de Internet Packet Exchange (Intercambio de paquetes Internet). Protocolo de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

- UDP. Siglas de User Datagram Protocol. Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Se utiliza cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

- TCP.

El nombre TCP/IP proviene de dos protocolos importantes de la familia. El Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto. El TCP/IP es la base de Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos.

- NetBIOS. Protocolo de red originalmente creado para redes locales de computadoras IBM PC.

Appletalk. Protocolo propietario que se utiliza para conectar ordenadores Macintosh de Apple en redes locales. Admite las tecnologías Ethernet y Token Ring.

- SMTP.

Simple Mail Transfer Protocol, o protocolo simple de transferencia de correo electrónico. Protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras.

- FTP es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Archivos) y es el ideal para transferir datos por la red.
- Telnet es el nombre de un protocolo que permite acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajaban por la red sin cifrar (en «texto claro»).
- SSH es el nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas a través de una red, de forma similar a como se hacía con Telnet. La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos. Al igual que Telnet, sólo permite conexiones tipo terminal de texto, aunque puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.
- IRC son las siglas de Internet Relay Chat. Protocolo de comunicación en tiempo real permite debates en grupo y/o privado, el cual se desarrolla en canales de chat. Es el sistema de charlas más usado hasta el momento. El concepto del IRC se basa en una arquitectura cliente-servidor formándose redes entre los servidores para albergar a más usuarios.
- HTTP es el protocolo de la Web (www), usado en cada transacción. Sirve para mandar las consultas (o sea, peticiones de publicar un documento www), informaciones sobre dirigirse a un enlace o informaciones de un formulario. Es un protocolo de consulta/respuesta, por esto define la forma de ambas: consulta y respuesta.

El protocolo HTTP es un protocolo de tipo stateless, es decir, no guarda ninguna información sobre conexiones anteriores, al finalizar la transacción toda información se pierde. Por esto las cookies se hicieron tan populares. La versión actual es 1.1, y su especificación está en el RFC 2068. Dispone de una variante cifrada mediante SSL llamada HTTPS.

- POP (Post Office Protocol). Protocolo diseñado para la gestión, el acceso y la transferencia de mensajes de correo electrónico entre dos máquinas, habitualmente un servidor y una máquina de usuario.

## 2. EL MODELO SNA.

SNA (Systems Network Architecture) es la solución IBM en el ámbito de las arquitecturas, con la finalidad de proporcionar un sistema de comunicaciones global para cumplir con las demandas planteadas por los diseñadores, operadores y usuarios finales de las redes:

- Los diseñadores necesitan medios adecuados para instalar y mantener las aplicaciones.
- El personal de operación necesita acceso a la red y a las funciones de gestión.
- Los usuarios finales necesitan acceder a los datos/aplicaciones con mecanismos de transporte de datos transparentes a ellos.
- La organización en su conjunto requiere la mayor efectividad al menor coste posible.

La red SNA está caracterizada por:

- Está basada en una estructura de niveles funcionales, no en productos específicos de hardware o software.
- Los niveles funcionales residen en nodos SNA a través de los cuales circula la información. Para simplificar podemos considerar un nodo como una caja física que implementa varias funciones SNA.
- Los niveles SNA incluyen inteligencia para controlar el flujo de datos y permitir la gestión extremo a extremo de la información.
- Las funciones SNA nunca cambian los datos de usuario.

## 3. COMPARACIÓN SNA CON OSI.

SNA asigna funciones por niveles que presentan ciertas diferencias frente a OSI, pero que coincide en aspectos básicos:

- Los niveles actúan como interfase entre los caminos lógicos (entre los usuarios finales) y los caminos físicos de comunicaciones involucrados.
- Los niveles son independientes unos de otros, de forma que puede alterarse una función de un nivel (en ambos extremos del enlace) sin afectar a ninguna otra función de otro nivel.

- Los niveles están implantados en diversos nodos físicos, produciéndose una imagen especular entre los nodos origen y destino (cada uno de ellos tiene toda la «torre» completa e idéntica de niveles).
- Los niveles dan servicios al nivel superior y los piden del nivel inferior.
- Cuando un mensaje de usuario final viaja por la red a través de los diferentes niveles del nodo origen, cada nivel le añade información necesaria (en general cabeceras y/o colas) y el paquete resultante se envía al siguiente nivel. En el nodo destino se produce el proceso inverso, a medida que la información va subiendo por los niveles va perdiendo información de cabeceras y colas hasta quedarse en el nivel superior únicamente con el mensaje original transmitido.

Los niveles SNA y su correspondencia con los niveles OSI son los siguientes (entre paréntesis se incluye la abreviatura de los niveles SNA):

SNA	OSI
N7 Transaction Services (TS)	Nivel de Aplicación.
N6 Presentation Services (PS)	Nivel de Presentación.
N5 Data Flow Control (DFC)	Nivel de Sesión.
N4 Transmission Control (TC)	Nivel de Transporte.
N3 Path Control (PC)	Nivel de Red.
N2 Data Link Control (DLC)	Nivel de Enlace.
N1 Physical Control (PLC)	Nivel Físico.

Los tres niveles inferiores se encargan del encaminamiento de datos entre nodos de la red tratando con la Red Física, denominándose conjuntamente servicios de red y conformando la red de transporte.

Los tres siguientes niveles tratan la red lógica y se denominan servicios de sesión, encargándose de manejar las sesiones (conexiones de la Red Lógica) extremo a extremo.

Los niveles SNA contienen entre otras las funciones básicas (flujo de tráfico, control de congestión) para que el tráfico esté ordenado sobre las rutas físicas y lógicas definidas. Por último, se puede concluir que existen niveles en todos los nodos de la red, pero no todos los nodos contienen todos los niveles en una configuración típica, los nodos inicial y final incluyen los siete niveles, mientras que los nodos intermedios sólo contienen los tres niveles inferiores.

Se incluye una breve descripción de las funciones llevadas a cabo por cada uno de los niveles SNA.

#### A) N1 Physical Control.

Este nivel se encarga de los enlaces físicos gestionando la interface para el medio físico. Define las características eléctricas y de señalización que establecen, mantienen y terminan las conexiones físicas entre nodos adyacentes.

#### B) N2 Data Link Control.

El nivel 2 de la arquitectura SNA provee transmisión fiable extremo a extremo entre nodos contiguos. Por otro lado, se encarga de formatear los datos sobre la línea entre nodos adyacentes, detectando y recuperando errores. Para la transmisión, se usa un protocolo de control de línea.

- Para dispositivos locales: protocolo de canal 3270.
- Para líneas locales: protocolo SDLC (Synchronous Data Link Control) junto con los protocolos para Token-Ring y X.25.

#### C) N3 Path Control.

Al nivel 3 le corresponde la función de encaminar los datos por el enlace correcto de la red física, detectando rutas no operativas que se notificarán para gestión de la red. El manejo de datos sigue un algoritmo FIFO (First In First Out) entre los nodos.

Al nivel Path Control también le corresponde la tarea de prevenir la congestión de la red, para lo cual controla el flujo de datos (PACING) sobre una ruta: este nivel trabaja con un sistema de semáforos en cada ruta sobre el enlace. Entre las acciones que puede adoptar está el alterar el tamaño de los mensajes creando unidades más pequeñas o agrupando en unidades más grandes.

#### D) N4 Transmission Control.

Este nivel se encarga de asegurar que la sesión entre usuarios finales se desarrolle conforme a las reglas acordadas al comienzo de la misma. Otras de sus funciones consisten en:

- Prevenir una posible inundación por datos en el nodo destino adecuando el ritmo de intercambio de los datos con la capacidad de proceso.
- Encriptar la información que viaja si se requieren medidas de seguridad especiales.
- Ayudar en la recuperación de errores.

#### E) N5 Data Flow Control.

La función principal del nivel de Data Flow Control consiste en asegurarse que el orden del flujo de datos entre los usuarios finales se mantiene: para cumplir este cometido, este nivel asigna números de secuencia a los bloques de datos y verifica si un bloque necesita respuesta.

#### F) N6 Presentation Services.

El nivel 6 tiene la misión de controlar la comunicación entre programas de transacciones o usuarios finales, suya es la responsabilidad de preparar los datos que se transmiten. Este nivel decodifica y presenta los datos, invocando al programa correcto si es necesario formateando los datos tal como se requiera (ejemplo: para impresora o pantalla). La interfaz del nivel de presentación está disponible para permitir a los usuarios finales crear sus propias aplicaciones SNA, por ejemplo para gestión de red, distribución de documentos, etc.

## G) N7 Transaction Services.

En el nivel de Transaction Services se asegura que los servicios para el usuario final se establecen y mantienen adecuadamente: este nivel se comunica con los Programas de Servicios de Transacciones -por ejemplo, intercambio de documentos, acceso a bases de datos distribuidas, etc.- típicamente basados en la LU 6.2. Entre sus funciones está la de dar servicios que ayudan a la operación de la red, facilitando las tareas de configuración (asignando nuevas direcciones de red durante su reconfiguración dinámica), actuación de sesiones (traducción de nombres simbólicos a direcciones) y gestión de red (problemas, cambios, rendimiento...).

La red SNA hay que considerarla como dividida en dos partes (la red SNA física y la red SNA lógica) entre las cuales existe una correspondencia.

### 1.º NODOS DE LA RED FÍSICA SNA.

Los nodos SNA son máquinas físicas conectadas electrónicamente por enlaces. Los nodos más los enlaces forman la red física SNA. Los tipos de nodos físicos SNA organizados en una estructura jerárquica son los siguientes:

- Nodo host.
- Nodo controlador de comunicaciones.
- Nodo periférico.
- Nodo terminal.

Un nodo Host y un nodo Controlador de Comunicaciones con todos sus nodos periféricos constituyen una subárea, concepto importante en el direccionamiento de Red SNA, ya que cada subárea está identificada por un número único.

Seguidamente se enumeran las principales características de cada uno de ellos:

#### A) Nodo Host o CPU (Central Processing Unit).

- Es el nodo encargado de controlar la red SNA jerárquica.
- Contiene el Método de Acceso a las Telecomunicaciones (VTAM), un software que se encarga de realizar las funciones básicas de Gestión Lógica de la red.
- En el nodo host residen los Programas de Aplicación con los cuales se comunican los usuarios finales.
- Al hablar de CPUs, nos referimos a máquinas IBM de la serie 370, serie 390 y máquinas compatibles de otros fabricantes como Hitachi o Amdahl.

#### B) Nodo Controlador de Comunicaciones.

- Se trata de un front-end de comunicaciones.

- Es un dispositivo programable que ejecuta las funciones básicas inherentes a la Gestión Física de la red: controla los enlaces de comunicación y encamina los datos a lo largo de la red.
- En él reside el Network Control Program (NCP): este programa realiza funciones de activación de líneas, llamada y respuesta de estaciones conmutadas, recuperación y grabación de errores, etc.
- La identificación física del dispositivo es una 3270 ó 3745, según la terminología IBM.

#### C) Nodo Periférico.

Se trata de un dispositivo controlador inteligente que puede soportar una gran variedad de estaciones de trabajo. Son nodos SNA que contienen un servicio llamado Control Point que gestiona la red por debajo de estos nodos pero sin soportar servicios de red SNA completos, los cuales se delegan en el nodo host o nodo controlador de comunicaciones asociado al nodo periférico. Se distinguen dos categorías de nodos periféricos según el nivel de funciones que soporten:

##### a) Controladores de Terminales (Cluster Controllers).

- Son controladores de pantallas «tontas» encargados de gestionar las operaciones de E/S de dichos dispositivos.
- No contienen aplicaciones que se hablen con las que residen en el host: únicamente permiten a usuarios finales conectarse con dichas aplicaciones.
- Pueden conectarse a un Controlador de Comunicaciones o localmente a un nodo host a través de un canal de datos de CPU.
- Se identifican genéricamente como máquinas 3x74.

##### b) Procesador Distribuido.

- Son más «inteligentes» que los Controladores de Terminales pudiendo ser equipos AS400, PS/2, etc. En esencia, desde el punto de vista SNA, proporcionan funciones similares a las del host, excepto en lo referido a gestión de red.
- Cuando hay múltiples host en la red, alguno de ellos puede funcionar como procesador distribuido.
- Existen aplicaciones en los puestos que se hablan con aplicaciones en el host, habilitando un entorno cliente/servidor.

#### D) Nodo Terminal.

- Diseñado para soportar dispositivos de baja funcionalidad.

#### 2.º ENLACES DE LA RED FÍSICA SNA.

Los enlaces SNA conectan los nodos SNA. Pueden establecerse varias categorías para los enlaces SNA:

- Según la topología, enlaces punto a punto, multipunto o enlaces de acceso múltiple (satélite, redes LAN, redes de conmutación de paquetes).
- Según la distancia y el protocolo utilizado, enlaces locales (entre un host y un controlador de comunicaciones se emplea cableado estándar y el protocolo de canales de datos 370) y remotos (entre controladores de comunicaciones se usan cables telefónicos, fibras ópticas, microondas o enlaces por satélites, el protocolo es el descrito por SNA -por ejemplo SDLC, Synchronous Data Link Control- y la norma X.25 para enlaces de conmutación de paquetes).
- SNA no define los medios a usar o si los enlaces deben ser analógicos o digitales, si deben usarse en modo half-duplex o full-duplex. Sólo define cómo deben manejarse los datos y cómo se enrutarán.

La Red Lógica SNA está formada por NAU's (Network Addressable Units) y Sesiones basándose en los niveles funcionales implantados por la Red Física:

- Los nodos SNA contienen componentes lógicos SNA llamados NAU's, que actúan como origen o destino de la comunicación.
- Las conexiones lógicas temporales que se establecen entre ellos se llaman Sesiones, mediante las cuales los usuarios finales pueden establecer una comunicación.

### 3.º NODOS DE LA RED LÓGICA SNA.

Las NAU's son conjuntos de componentes HW y SW a través de los cuales los usuarios acceden a los servicios que proporciona la red SNA y los operadores controlan y gestionan el flujo de datos de la red. Cada NAU tiene una dirección de red única, identificando su localización en la red, la cual se usa para encaminar los mensajes. Se trata de direcciones internas a SNA que el usuario final no tiene por qué conocer, en su lugar, se refiere a ellas por el nombre simbólico que se le asignan al instalar la red. La dirección única para cada NAU se consigue en base a la subárea a la que pertenece la NAU y una dirección única de elemento de red dentro de la subárea. Existen tres tipos de NAU's:

- System Services Control Point (SSCP).
- Physical Unit (PU).
- Logical Unit (LU).

A continuación se resumen las principales características de cada uno de ellos:

#### A) System Services Control Point (SSCP).

Es el nodo que residiendo en una CPU del Host controla la red jerárquica conociendo todos sus recursos. Es el depositario de las aplicaciones con las cuales se comunican los usuarios finales. Contiene el VTAM (Método de Acceso a las Telecomunicaciones) que realiza funciones básicas de control de red. Proporciona servicio de establecimiento y gestión de conexiones entre las NAU's, una vez establecida la conexión o sesión, las NAUs pueden intercambiar información entre ellas por la red.

Realiza la traducción de nombre simbólico a la dirección única de red empleada por las funciones internas de SNA. Ayuda a la recuperación y mantenimiento de la red y se relaciona con el operador de red para gestionar los recursos.

Al conjunto de recursos controlados por un SSCP se le llama dominio. Cada host representa un dominio. Si existen varios hosts -varios SSCP's- interconectados tenemos una red Multidominio o Cross-Domain, por contra, si únicamente hay un host, tenemos una red Monodominio.

Dos o más SSCP's pueden actuar de backup para casos de fallo en otros dominios, por ejemplo, si uno de los hosts falla, el otro host puede tomar control de los recursos controlados por el SSCP que falló.

La posibilidad de establecer sesiones entre NAU's de distintos dominios sólo es posible si previamente los SSCP's respectivos han establecido una conexión entre ellos. Si tenemos varias redes SNA interconectadas tenemos una configuración SNI (SNA Interconnect) también llamada Multi-Network o Cross-Network.

#### B) Physical Unit (PU).

Una Physical Unit (PU) es una combinación de servicios SNA que monitoriza y controla los recursos de un nodo SNA a petición de un SSCP. Estos recursos pueden ser enlaces, terminales, etc. Cada nodo de una red SNA contiene un tipo específico de PU. De igual forma que un Host tiene un SSCP (System Services Control Point), una PU tiene su propio Control Point (CP), para manejar la PU y sus recursos dependientes.

Los tipos de PU's y su relación con elementos físicos de la red es la siguiente:

- PU tipo 1 – nodo Terminal.
- PU tipo 2 – nodo Periférico.
- PU tipo 4 – nodo Controlador de Comunicaciones.
- PU tipo 5 – nodo Host.

#### C) Logical Unit (LU).

Las LU's identifican el punto de terminación de la red SNA: el usuario final -estación de trabajo o programa de aplicación- al no ser parte directa de la red SNA necesita un mecanismo que le permita acceder a los servicios de la red. Esto se consigue mediante el tipo de NAU llamado Logical Unit (LU). La LU representa la puerta de acceso a la red SNA para el usuario final, a través de la cual puede comunicarse con otro usuario final o usar los servicios proporcionados por el SSCP. Las LU's hacen todas las funciones que son específicas de la comunicación entre usuarios finales, estando conectadas entre sí por caminos físicos de la red. Una LU puede soportar varios usuarios. Todos los nodos, salvo el nodo Controlador de Comunicaciones, soportan LU's. Los nodos periféricos y los nodos host pueden tener más de una LU. La clasificación de LU's indica cómo éstas presentan los datos, siendo las más frecuentes las siguientes:

- LU tipo 0: soporte no SNA.
- LU tipo 1: terminal o impresora SNA no 3270.

- LU tipo 2: dispositivos de pantalla 3270.
- LU tipo 3: dispositivos de impresora 3270.
- LU tipo 4: similar a LU1 pero con más funciones.
- LU tipo 6.1: aplicación a aplicación en host.
- LU tipo 6.2: aplicación a aplicación en host o en otros dispositivos.

LU 6.1 y 6.2 proporcionan funciones muy sofisticadas.

#### 4.º SESIONES.

Para que dos LU's -un programa de aplicación y un terminal de usuario- se puedan comunicar, previamente debe establecerse una conexión entre ellos. La conexión física debe existir, pero igualmente es necesaria una conexión lógica. A esta conexión lógica, full-duplex, se la denomina Sesión.

Además hay otro paso prerequisite: para que dos LU's de usuario final establezcan una sesión, el SSCP debe primero establecer sesiones con las PU's en cada lado y a continuación con las LU's.

Internamente el proceso de establecimiento de sesión se inicia con la creación por el SSCP de una asociación entre los bloques internos de control que representan las NAU's implicadas. A partir de ese momento, el SSCP puede seguir lo que sucede en la sesión, pedir detalles, detectar errores. Los tipos de sesiones y la finalidad de cada una de ellas son los siguientes:

- SSCP-PU: se usa para controlar un nodo y sus recursos.
- SSCP-LU: se emplea para mediar en la activación de sesiones LU-LU.
- LU-LU: se usa para permitir la comunicación entre usuarios finales.

Con los dos primeros se llevan datos de gestión SNA (comandos SNA, datos de control, recuperación de errores) mientras que la última (LU-LU) se utiliza para llevar datos de usuario final.

SNA define protocolos y formatos para construir redes pero la implantación puede ser muy distinta en máquinas o plataformas diferentes en función del SW y el HW utilizado para la instalación.

Se van a analizar los productos SW básicos y las Unidades de Control de Comunicaciones como elementos HW característicos de la arquitectura SNA donde reside el NCP (Network Control Program).

#### 5.º SOFTWARE BÁSICO SNA.

Los productos básicos de SNA jerárquico se refieren al modo en que se implantan las funciones SNA. Existen una serie de productos obligatorios para control de la red:

- La CPU del host requiere un Método de Acceso SNA (VTAM) para construir el SSCP que, además, ejecuta los comandos SNA.

- Las Unidades de Control de Comunicaciones contienen el NCP para trabajar con las operaciones de I/O de la red.
- Los nodos periféricos manejan aplicaciones y dispositivos para dar soporte a los usuarios finales.
- Por último, existen rutinas de generación/carga/volcado de NCP's llamadas System Support Programs (SSP's).

Para satisfacer las demandas de I/O, el trabajo se reparte de la siguiente forma:

- Los dispositivos remotos están controlados por un NCP, bajo la dirección del VTAM.
- Los dispositivos locales son directamente controlados por el propio VTAM.

Aparte de los anteriores, hay un conjunto cada vez más numeroso de productos (hardware y software) para optimizar y facilitar el uso y manejo de la red. Se trata de productos dirigidos a usuarios, operadores y diseñadores de redes.

#### 6.º HARDWARE: LAS UNIDADES DE CONTROL DE COMUNICACIONES (UCC's).

Los Controladores de Comunicaciones son CPU's especializadas cuya función básica es descargar al host de las tareas más sencillas de manejo de la red, tales como direccionamiento, sondeo, almacenamiento intermedio de datos, lectura de líneas y mantenimiento, disponiendo de soporte de terminal y discos para determinación de problemas y operación.

También están en comunicación con las herramientas de Gestión de Red (p. ej., Netview), suministrándoles información de estado y datos acerca de la red. Los elementos mínimos que contienen las UCC's son:

- Central Control Unit y memoria.
- Disco duro.
- Adaptadores de canal.
- Scanners de comunicaciones.
- Line Interface Units y Line Interface Couplers.
- Tarjetas de conexión Token-Ring.
- Pantalla de Subsistema de Mantenimiento y Operación (MOSS).

Estos elementos se agrupan de la siguiente forma:

- Subsistema de control: formado por Central Control Unit y la memoria.
- Subsistema de comunicaciones: formado por los adaptadores de canal, los scanners de comunicaciones, las Line Interface Couplers y las conexiones Token-Ring.
- Subsistema de mantenimiento y operación: formado por las facilidades del MOSS y el disco duro.

#### 4. SNA DE SEGUNDA GENERACIÓN: APPN.

SNA se desarrolló en un principio para proporcionar control y gestión centralizada de red desde uno o más procesadores de host. La red estaba organizada jerárquicamente y era la jerarquía quien determinaba cuánto control se ejercía. Sin embargo, las redes empezaron a crecer y tuvieron que adaptarse a cambios de tecnología y nuevos requisitos, de forma que en los sistemas SNA aparecieron aspectos «revolucionarios» por entonces. Surgió la necesidad de habilitar la comunicación entre aplicaciones (Aplicación-a-Aplicación) en varios hosts (p. ej., un CICS de una máquina hablándose con un CICS de otra máquina).

Los nodos periféricos (en un principio PU tipo 2) cada vez eran más sofisticados de forma que podían soportar aplicaciones y terminales. Un nodo periférico era capaz de contactar con otro nodo periférico sin necesidad de que un SSCP gestionara este tipo de conexión. A partir de este momento, al nodo periférico se le pasa a denominar PN (Peripheral Node) tipo 2.1.

##### 4.1. LU 6.2.

En un sistema distribuido tenemos una aplicación hablando con otra aplicación residiendo cada una de ellas en hosts diferentes. La LU2 tradicional no tiene las capacidades necesarias para trabajar en ese entorno (otras como LU0, LU 6.0 tienen algunas de esas funciones). Por tanto, fue necesario crear un nuevo tipo de LU para la comunicación programa a programa.

Con la LU 6.2 tenemos una forma estándar de comunicación entre programas usando protocolos SNA, independientemente del hardware en que se esté ejecutando cada programa. Abarca los cuatro niveles superiores del modelo SNA, incluyendo el nivel 7 de Transaction Services, a diferencia de la LU tradicional que no lo incluye.

Además, una LU 6.2 en un nodo tipo 2.1 puede establecer sesiones sin que intervenga un SSCP, denominándose LU's independientes, frente a las LU's tradicionales que requieren soporte de un SSCP, a las que llamamos LU's dependientes.

Las aplicaciones de las LU's 6.2 se denominan Transaction Programs (TP). Estos TP's se conectan por medio de conversaciones, de forma que una LU 6.2 puede representar a varios TP's (cada TP suele asociarse a un usuario final). La misión de la LU 6.2 es imponer al TP las reglas de la comunicación, por ejemplo, cómo se debe manejar el flujo de datos.

Cuando se comunican entre sí dos LUs 6.2 entran en sesión; esta sesión se utiliza para llevar la conversación entre dos TP's (cada sesión lleva una conversación). Después de acabar una conversación entre 2 TP's, la sesión entre las LUs 6.2 permanece y se puede volver a usar para establecer otra comunicación.

No obstante, puede existir más de una sesión entre 2 LU's 6.2, con lo cual es posible manejar más de una conversación, simultáneamente, entre un par de LU's. A estas sesiones se las llama paralelas.

##### 4.2. NODOS TIPO 2.1.

Con los Nodos tipo 2.1 se libera al SSCP de la tarea de gestionar y controlar todas las sesiones. Estos nodos pueden controlar sus propias sesiones sin necesidad de que haya un SSCP. Estos nodos

pueden soportar aplicaciones y la arquitectura LU 6.2, y pueden comunicarse directamente sin la necesidad de las subáreas tradicionales. Para todo esto, cuentan con funciones similares a las que tiene el SSCP, el nodo 2 se representa como un Control Point (CP) y las funciones se llaman Peripheral Node Control Point (PNCP) services.

#### 4.3. APPN (ADVANCED PEER-TO-PEER NETWORKING).

APPN representa una evolución del Nodo 2.1 cuando tenemos una estructura en malla de Nodos 2.1 de dos tipos:

- End Nodes (EN).
- Network Nodes (NN).

Un EN (End Node) APPN contiene un Control Point que sirve sólo a los recursos definidos en ese nodo. Los recursos se dice que están en el dominio de ese EN. Para acceder a los recursos situados en la red, un EN usa los servicios proporcionados por un NN (Network-Node) al que está conectado directamente. Un Network-Nodes (NN) APPN contiene un Control Point que da servicios a sus recursos propios y a los EN directamente conectados a él. Todos esos recursos están declarados como pertenecientes a su dominio.

Los Network Nodes proporcionan una serie de funciones dinámicas:

- Cálculo de rutas para el establecimiento de sesiones.
- Búsquedas de recursos en la red.
- Mantenimiento de directorio de red.

#### 4.4. FUNCIONAMIENTO DE APPN.

A diferencia de SNA jerárquico donde las rutas están preestablecidas (son estáticas), en APPN las rutas se calculan cuando es necesario, es decir, al establecerse la sesión las rutinas de Servicios de Directorio son las encargadas de buscar en cascada una petición para un recurso a través de los nodos de la red APPN hasta que el recurso es encontrado.

Otra novedad en APPN es que los recursos pueden definirse en cualquier momento, no sólo durante la definición del sistema. En el caso de APPN, la definición de la red se hace por medio de intercambio dinámico de topologías entre los nodos, registro de recursos por los nodos, y búsquedas no dirigidas son mecanismos que en modo alguno interrumpen el trabajo normal de la red.

Todos los nodos APPN tienen una Base de Datos de Directorio. Las LU's de cada nodo se definen en su directorio local por medio de las definiciones de sistema. La BD de un Network Node contiene la lista de sus recursos propios y los de los End Nodes conectados a él. Las LU's se registran cuando se conectan a la red. Si un End Node está conectado a más de un Network-Node, sus LU's se registran sólo en un Network Node servidor.

Los Network-Nodes APPN también pueden aprender nuevas LU's en su dominio durante la búsqueda de un recurso, para lo cual actualizan adecuadamente su BD de directorio. Se trata de una BD

de Directorio global distribuida entre los Network Nodes por toda la red, manteniendo cada uno una parte, de forma que un nodo encuentra la localización de un recurso buscando en el orden siguiente:

- En el nodo originario de la petición.
- Si éste es un EN, se busca en su NN servidor.
- Si un NN conoce la LU en una localización remota, reenvía la petición, si se recibe una confirmación, se calcula la ruta óptima.
- Si ningún nodo conocido controla el recurso, se envía una búsqueda no dirigida a todos los NN adyacentes. Éstos, a su vez, propagan la petición hasta que se haya interrogado a todos los NN, una respuesta positiva hace que se calcule la ruta, más una actualización de la BD topológico por el nodo emisor.

Una vez que se ha confirmado el nodo de la LU destino, el NN de la LU origen calcula dinámicamente la ruta preferente. Una vez calculada la ruta, el Control Point pasa esta información a la LU origen, que puede entonces enviar un BIND para activar la sesión. Es entonces cuando usando la sesión, los Transaction Programs (TP) pueden empezar una conversación.

## 5. EL MODELO TCP/IP.

La pila TCP/IP se llama así por dos de sus protocolos más importantes: TCP («Transmission Control Protocol») de IP («Internet Protocol»). Otro nombre es pila de protocolos de Internet, y es la frase oficial usada en documentos oficiales de estándares.

La primera meta de diseño de TCP/IP fue construir una interconexión de redes que proporcionase servicios de comunicación universales: una red, o Internet. Cada red física tiene su propia interfaz de comunicaciones, dependiente de la tecnología que la implementa, en la forma de una interfaz de programación que proporciona funciones básicas de comunicación (primitivas). Las comunicaciones entre servicios las proporciona el software que se ejecuta entre la red física y la aplicación de usuario, y da a estas aplicaciones una interfaz común, independiente de la estructura de la red física subyacente. La arquitectura de las redes físicas es transparente al usuario.

El segundo objetivo es interconectar distintas redes físicas para formar lo que al usuario le parece una única y gran red. Tal conjunto de redes interconectadas se denomina «internetwork» o Internet. Para poder interconectar dos redes, necesitamos un ordenador que esté conectado a ambas redes y que pueda retransmitir paquetes de una a la otra; tal máquina es un router. El término router IP también se usa porque la función de encaminamiento es parte de la capa IP de la pila TCP/IP. Las propiedades básicas de un router son:

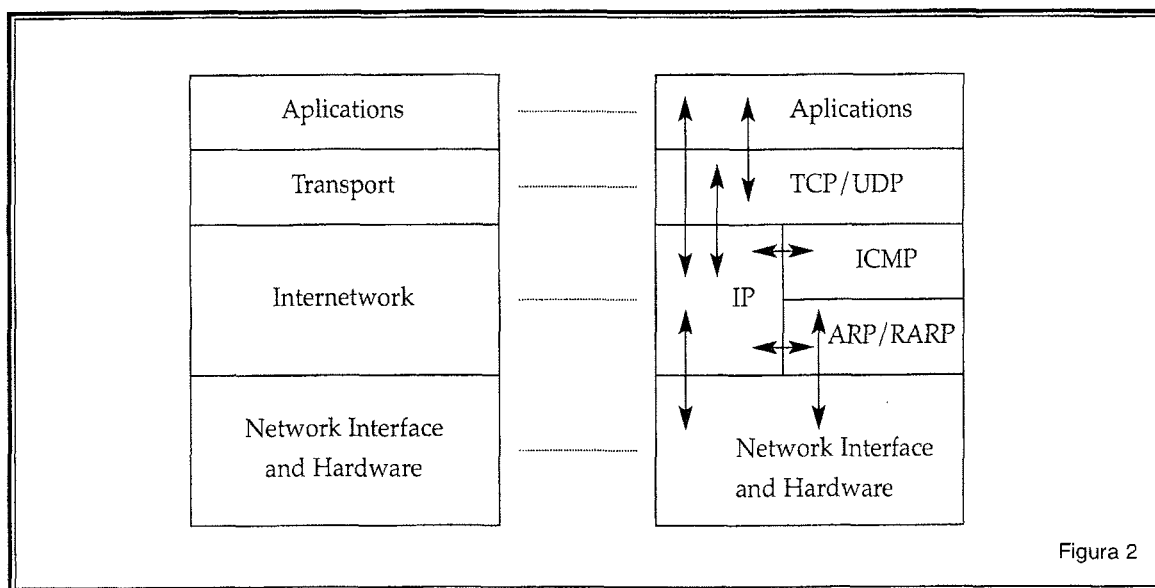
- Desde el punto de vista de la red, es un host normal.
- Desde el punto de vista del usuario, es invisible. El usuario sólo ve una gran red.

Para ser capaz de identificar un host en la red, a cada uno se le asigna una dirección, la dirección IP. Cuando un host tiene múltiples adaptadores de red, cada adaptador tiene una dirección IP separada. La dirección IP consta de dos partes:

dirección IP = <número de red><número de host>

El número de red lo asigna una autoridad central y es unívoco en Internet. La autoridad para asignar el número de host reside en la organización que controla la red identificada por el número de red.

TCP/IP, como la mayoría del software de red, está modelado en capas. Esta representación conduce al término pila de protocolos. Se puede usar para situar (pero no para comparar funcionalmente) TCP/IP con otras pilas, como SNA y OSI («Open System Interconnection»). Las comparaciones funcionales no se pueden extraer con facilidad de estas estructuras, ya que hay diferencias básicas en los modelos de capas de cada una. Los protocolos de Internet se modelan en cuatro capas:

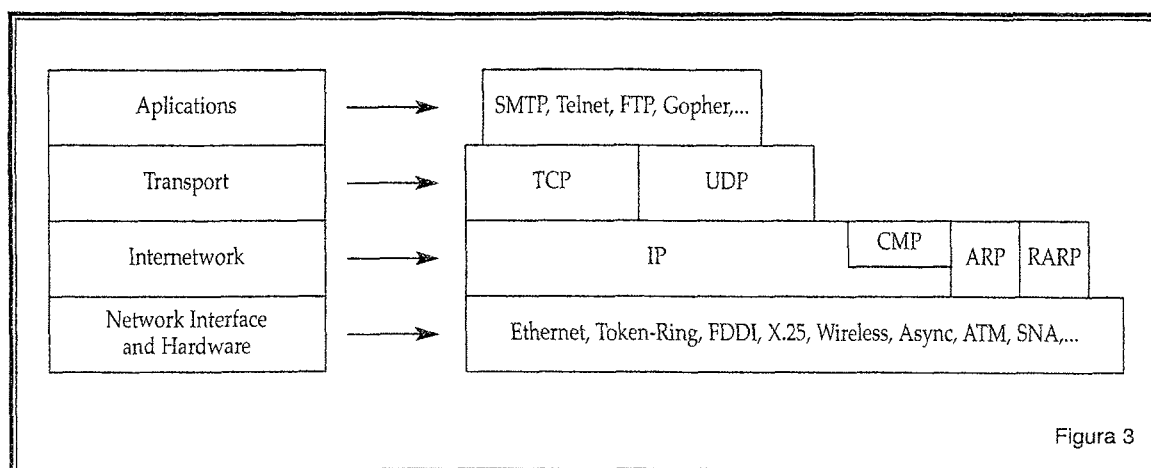


Aplicación es a un proceso de usuario que coopera con otro proceso en el mismo o en otro host. Ejemplos son TELNET (un protocolo para la conexión remota de terminales), FTP («File Transfer Protocol») y SMTP («Simple Mail Transfer Protocol»).

Transporte proporciona la transferencia de datos de entre los extremos. Ejemplos son TCP (orientado a conexión) y UDP (no orientado a conexión).

Internetwork, también llamada capa de red, proporciona la imagen de «red virtual» de Internet (es decir, oculta a los niveles superiores la arquitectura de la red). IP es el protocolo más importante de esta capa. Es un protocolo no orientado a conexión que no asume la fiabilidad de las capas inferiores. No suministra fiabilidad, control de flujo o recuperación de errores. Estas funciones deben proporcionarlas una capa de mayor nivel, bien de transporte con TCP, o de aplicación, si se utiliza UDP como transporte. Una unidad de un mensaje en una red IP se denomina datagrama IP. Es la unidad básica de información transmitida en redes TCP/IP Networks.

Network Interface o capa de enlace o capa de enlace de datos constituye la interfaz con el hardware de red. Esta interfaz puede proporcionar o no entrega fiable, y puede estar orientada a flujo o a paquetes. De hecho, TCP/IP no especifica ningún protocolo aquí, pero puede usar casi cualquier interfaz de red disponible, lo que ilustra la flexibilidad de la capa IP. Ejemplos son IEEE 802.2, X.25 (que es fiable por sí mismo), ATM, FDDI, PRN («Packet Radio Networks», como AlohaNet) incluso SNA.



La formación de una red conectando múltiples redes se consigue por medio de los routers. Es importante distinguir entre un router, un puente y una pasarela.

**Puente:** interconecta segmentos de LAN a nivel de interfaz de red y envía tramas entre ellos. Un puente realiza la función de retransmisión MAC, y es independiente de cualquier capa superior (incluyendo el enlace lógico). Proporciona, si se necesita, conversión de protocolo a nivel MAC. Un puente es transparente para IP. Es decir, cuando un host envía un datagrama a otro host en una red con el que se conecta a través de un puente, envía el datagrama al host y el datagrama cruza el puente sin que el emisor se dé cuenta.

**Router:** interconecta redes en el nivel de red y encamina paquetes entre ellas. Debe comprender la estructura de direccionamiento asociada con los protocolos que soporta y tomar la decisión de si se han de enviar, y cómo se ha de hacer, los paquetes. Los routers son capaces de elegir las mejores rutas de transmisión así como tamaños óptimos para los paquetes. La función básica de encaminamiento está implementada en la capa IP. Por lo tanto, cualquier estación de trabajo que ejecute TCP/IP se puede usar como router. Un router es visible para IP. Es decir, cuando un host envía un datagrama IP a otro host en una red conectada por un router, envía el datagrama al router y no directamente al host de destino.

**Pasarela:** interconecta redes a niveles superiores que los puentes y los routers. Una pasarela suele soportar el mapeado de direcciones de una red a otra, así como la transformación de datos entre distintos entornos para conseguir conectividad entre los extremos de la comunicación. Las pasarelas limitan típicamente la conectividad de dos redes a un subconjunto de los protocolos de aplicación soportados en cada una de ellas. Una pasarela es opaca para IP. Es decir, un host no puede enviar un datagrama IP a través de una pasarela: sólo puede enviarlo a la pasarela. La pasarela se ocupa de transmitirlo a la otra red con la información de los protocolos de alto nivel que vaya en él.

**Encaminamiento IP:** los datagramas entrantes se chequean para ver si el host local es el destinatario:

- Sí. El datagrama se pasa a los protocolos de nivel superior.
- No. El datagrama es para un host diferente.

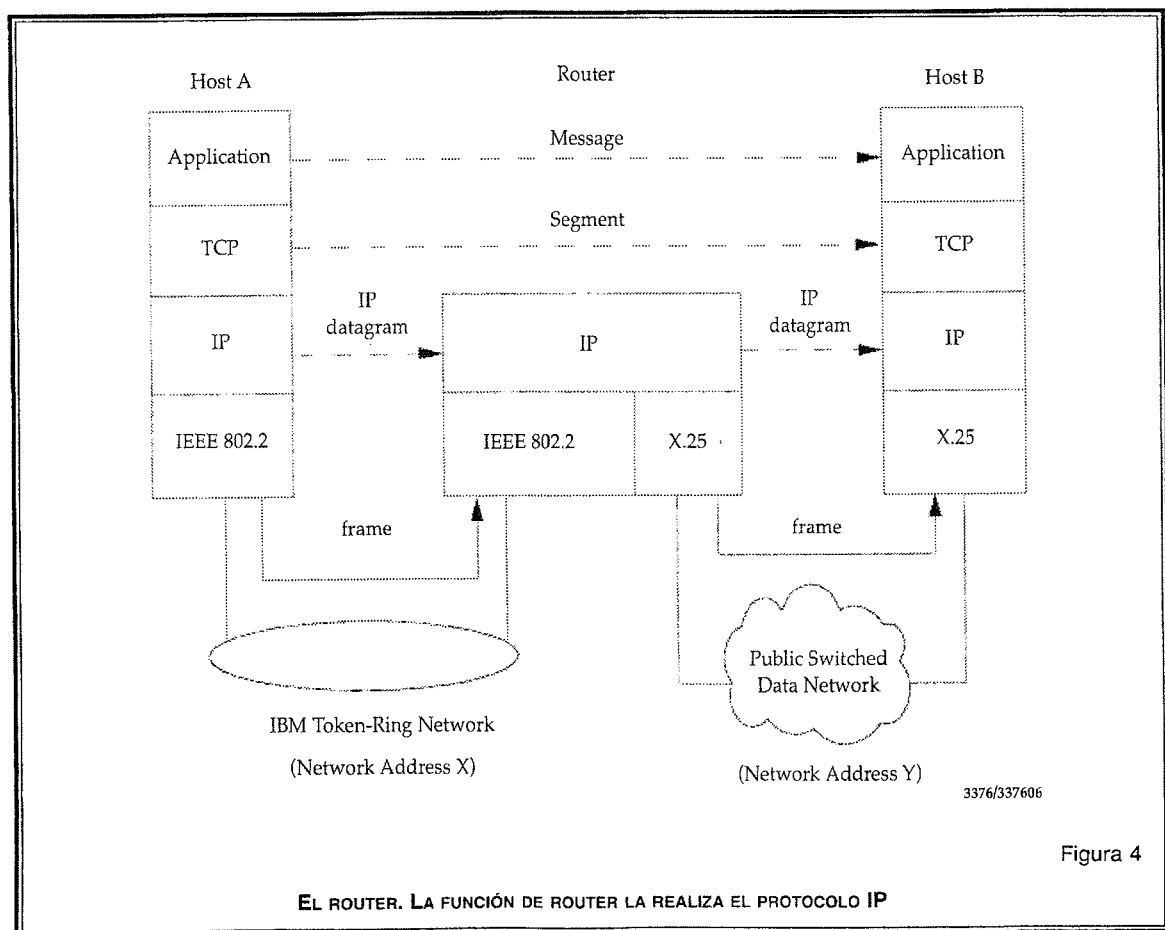
La acción depende del valor del flag «ipforwarding» (retransmisión IP).

- Verdadero. El datagrama se trata como si fuera un datagrama saliente y se encamina el siguiente salto según el algoritmo descrito abajo.
- Falso. El datagrama se desecha.

En el protocolo de red, los datagramas salientes se someten al algoritmo de encaminamiento IP que determina dónde enviar el datagrama de acuerdo con la dirección de destino.

- Si el host tiene una entrada en su tabla de encaminamiento IP que concuerde con la IP de destino, el datagrama se envía a la dirección correspondiente a esa entrada.
- Si el número de red de la dirección IP de destino es el mismo que el de uno de los adaptadores de red del host (están en la misma red) el datagrama se envía a la dirección física del host que tenga la dirección de destino.
- En otro caso, el datagrama se envía a un router por defecto.

Este algoritmo básico, necesario en toda implementación de IP, es suficiente para realizar las funciones de encaminamiento elementales. Como se señaló arriba, un host TCP/IP tiene una funcionalidad básica como router, incluida en IP. Un router de esta clase es adecuado para encaminamiento simple, pero no para redes complejas.



**La dirección IP:** los estándares para las direcciones IP se describen en RFC 1166 Números de Internet. Para ser capaz de identificar una máquina en Internet, a cada interfaz de red de la máquina o host se le asigna una dirección, la dirección IP, o dirección de Internet. Cuando la máquina está conectada a más de una red se le denomina «multi-homed» y tendrá una dirección IP por cada interfaz de red. La dirección IP consiste en un par de números:

IP dirección = <número de red><número de interfaz de red>

La parte de la dirección IP correspondiente al número de red está administrada centralmente por el InterNIC (Internet Network Information Center) y es única en toda la Internet.

Las direcciones IP son números de 32 bits representados habitualmente en formato decimal (la representación decimal de cuatro valores binarios de 8 bits concatenados por puntos). Por ejemplo 128.2.7.9 es una dirección IP, donde 128.2 es el número de red y 7.9 el de la interfaz de red. Las reglas usadas para dividir una dirección de IP en su parte de red y de interfaz de red se explican abajo.

El formato binario para la dirección IP 128.2.7.9 es:

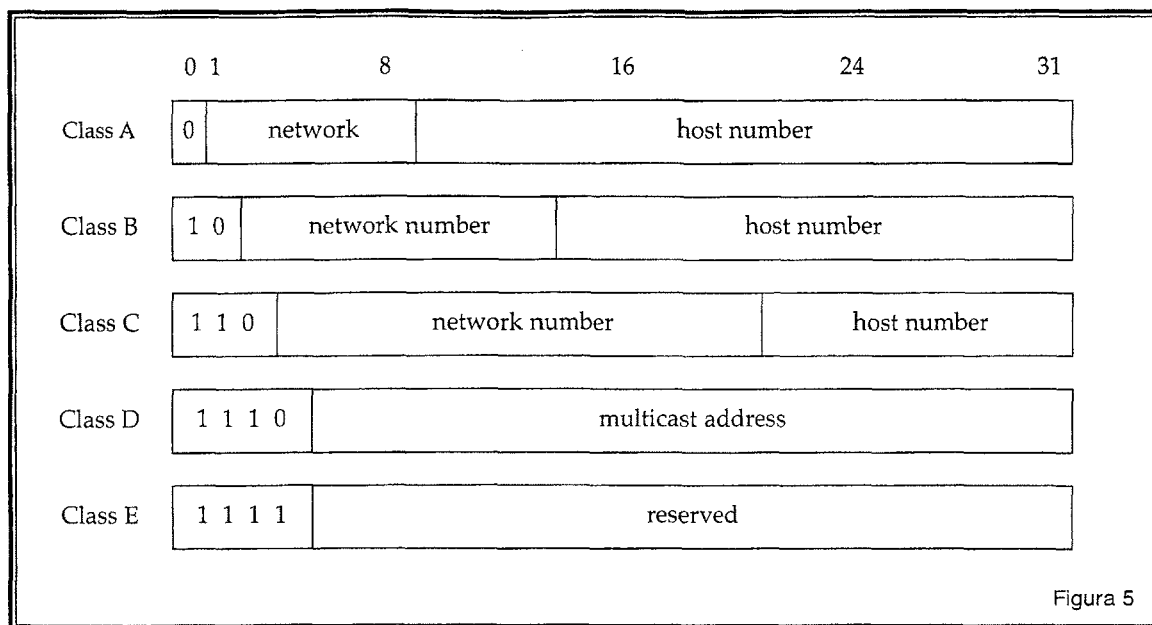
10000000 00000010 00000111 00001001

Las direcciones IP son usadas por el protocolo IP para definir únicamente un host en la red. Los datagramas IP (los paquetes de datos elementales intercambiados entre máquinas) se transmiten a través de alguna red física conectada a la interfaz de la máquina y cada uno de ellos contiene la dirección IP de origen y la dirección IP de destino. Para enviar un datagrama a una dirección IP de destino determinada, la dirección de destino debe ser traducida a una dirección física. Esto puede requerir transmisiones en la red para encontrar la dirección física de destino, por ejemplo, en LAN's el ARP («Address Resolution Protocol» se usa para traducir las direcciones IP a direcciones físicas MAC).

Los primeros bits de las direcciones IP especifican cómo el resto de las direcciones deberían separarse en sus partes de red y de interfaz.

Los términos dirección de red y netID se usan a veces en vez de número de red, pero el término formal, utilizado en RFC 1166, es número de red. Análogamente, los términos dirección de host y hostID se usan ocasionalmente en vez de número de host.

Hay cinco clases de direcciones IP.



Dos de los números de red de cada una de las clases A, B y C, y dos de los números de host de cada red están preasignados: los que tienen todos los bits a 0 y los que tienen todos los bits a 1. Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (veremos posteriormente que de cada par de direcciones de red y de host, dos tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red puede tener hasta 16,777,214 hosts.

- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16.382 redes de hasta 65.534 hosts cada una.
- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2.097,150 redes de hasta 254 hosts cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada.
- Las direcciones de clase E se reservan para usos en el futuro.

Es obvio que una dirección de clase A sólo se asignará a redes con un elevado número de hosts, y que las direcciones de clase C son adecuadas para redes con pocos hosts. Sin embargo, esto significa que las redes de tamaño medio (aquéllas con más de 254 hosts o en las que se espera que en el futuro haya más de 254 hosts) deben usar direcciones de clase IP. El número de redes de tamaño pequeño y medio ha ido creciendo muy rápidamente en los últimos años y se temía que, de haber permitido que se mantuviera este crecimiento, todas las direcciones de clase B se habrían usado para mediados de los 90. Esto es lo que se conoce como el problema del agotamiento de las direcciones IP.

Un hecho a señalar en la división de la dirección IP en dos partes es que esta división, a su vez, divide en dos partes la responsabilidad de elegir una dirección IP. El número de red es asignado por el InterNIC y el de host por la autoridad que controla la red. Como veremos en la siguiente sección, el número de host puede dividirse aún más: esta división también es controlada por la autoridad propietaria de la red, y no por el InterNIC.

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podrían ser necesarios cuando:

- Se instala una nueva red física.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.

Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de subred.

El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina subred. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como:

<número de red><número de subred><número de host>

La combinación del número de subred y del host suele denominarse «dirección local» o parte «local». La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de éstas, pero un host de una red distinta no lo es; sigue considerando la parte local de la dirección IP como un número de host.

La división de la parte local de la dirección IP en números de subred y de host queda a libre elección del administrador local; cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando una máscara de subred que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a 1 pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de «todos los bits a cero» y «todos los bits a uno» se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:

- El primer byte es el número de subred, el segundo el de host. Esto proporciona 254 (256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.
- Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4.094 posibles subredes (4.096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay muchas otras posibilidades.

Mientras el administrador es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un número de bits al número de subred y el resto a la dirección local. Por tanto, es corriente usar un bloque de bits contiguos al comienzo de la parte local para el número de subred, ya que así las direcciones son más legibles (esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

Hay otra dirección de especial importancia: el número de red de clase A con todos los bits a 1, 127, se reserva para la dirección de loopback. Todo lo que se envíe a una dirección con 127 como valor del byte de mayor orden, por ejemplo 127.0.0.1, no debe encaminarse a través de la red, sino directamente del controlador de salida al de entrada.

La mayoría de las direcciones IP se refieren a un sólo destinatario: se denominan direcciones de unicast. Sin embargo, como se ha señalado anteriormente, hay dos tipos especiales de direcciones IP que se utilizan para direccionar a múltiples destinatarios: las direcciones de broadcast y de multicast. Cualquier protocolo no orientado a conexión puede enviar mensajes de broadcast o de multicast, además de los unicast. Un protocolo orientado a conexión sólo puede usar direcciones de unicast porque la conexión existe entre un par específico de hosts.

DNS («DOMAIN NAME SYSTEM»).

El protocolo DNS es un protocolo estándar. Las configuraciones iniciales de Internet requerían que los usuarios emplearan sólo direcciones IP numéricas. Esto evolucionó hacia el uso de nombres de host simbólicos muy rápidamente. Por ejemplo, en vez de escribir TELNET 128.12.7.14, se podría escribir TELNET edum9, y edum9 se traduciría de alguna forma a la dirección IP 128.12.7.14. Esto introduce el problema de mantener la correspondencia entre direcciones IP y nombres de máquina de alto nivel de forma coordinada y centralizada.

Inicialmente, el NIC («Network Information Center») mantenía el mapeado de nombres a direcciones en un sólo fichero (HOSTS.TXT) que todos los hosts obtenían vía FTP. Se denominó espacio de nombres plano. Debido al crecimiento explosivo del número de hosts, este mecanismo se volvió demasiado tosco (considerar el trabajo necesario sólo para añadir un host a Internet) y fue sustituido por un nuevo concepto: DNS («Domain Name System»). Los hosts pueden seguir usando un espacio de nombres local plano (el fichero HOSTS.LOCAL) en vez o además del DNS, pero fuera de redes pequeñas, el DNS es prácticamente esencial. El DNS permite que un programa, ejecutándose en un host, le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de los nombres simbólicos y las direcciones IP.

EL ESPACIO DE NOMBRES JERÁRQUICO.

Consideremos la estructura interna de una gran organización. Como el jefe no lo puede hacer todo, la organización tendrá que partirse seguramente en divisiones, cada una de ellas autónoma dentro de ciertos límites. Específicamente, el ejecutivo a cargo de una división tiene autoridad para tomar decisiones sin requerir el permiso de su jefe.

Los nombres de dominio se forman de modo similar, y con frecuencia reflejarán la delegación jerárquica de autoridades usada para asignarlos. Por ejemplo, considerar el nombre:

lcs.mit.edu

Aquí, lcs.mit.edu es el nombre de dominio de nivel inferior, un subdominio de mit.edu, que a su vez es un subdominio de edu («education»), conocido como dominio raíz.

El dominio único que se halla sobre la cima no tiene nombre y se le conoce como dominio raíz. La estructura completa se explica en las siguientes secciones.

Cuando se usa el DNS, es común trabajar con sólo una parte de la jerarquía de dominios, por ejemplo el dominio `ral.ibm.com`. El DNS proporciona un método sencillo para minimizar la cantidad de caracteres a escribir en estos casos. Si el nombre de dominio termina en un punto (por ejemplo `wtscpok.itsc.pok.ibm.com.`) se asume que está completo. Es lo que se llama un FQDN («Fully Qualified Domain Name») o nombre absoluto de dominio. Si, sin embargo, no termina en punto, (por ejemplo `wtscpok.itsc`) estará incompleto y el procesador de nombres del DNS, como se verá más abajo, podrá completarlo, por ejemplo, añadiendo un sufijo como `.pok.ibm.com` al nombre de dominio. Las reglas para hacer esto dependen de la implementación y son configurables localmente.

#### DOMINIOS GENÉRICOS.

A los tres dominios de la cima se les llama dominios genéricos u organizacionales.

edu	Instituciones educativas
gov	Instituciones gubernamentales
com	Organizaciones comerciales
mil	Grupos militares
net	Redes
int	Organizaciones internacionales
org	Otras organizaciones

Puesto que Internet comenzó en los Estados Unidos, la estructura del espacio de nombres jerárquico tenía inicialmente sólo organizaciones estadounidenses en la cima de la jerarquía, y sigue siendo cierto que gran parte de las organizaciones de la cima de la jerarquía son estadounidenses. Sin embargo, sólo los dominios `.gov` y `.mil` están restringidos a los Estados Unidos.

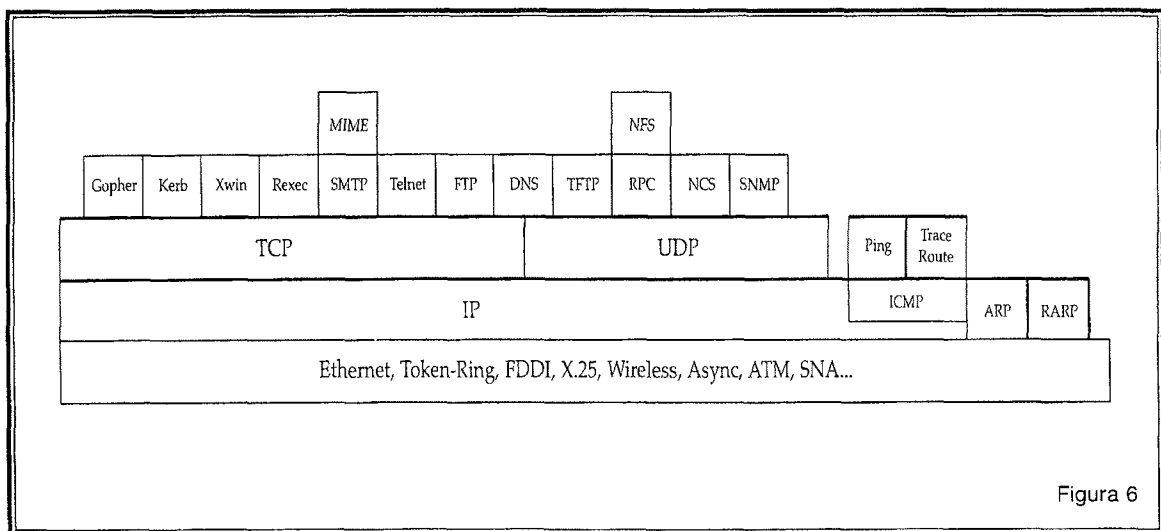
Además, hay dominios de nivel de cima para cada uno de los códigos internacionales de dos caracteres ISO 3166 para países (de `ae` para los Emiratos Árabes Unidos a `zw` para Zimbabwe). Se les conoce como dominios de países o dominios geográficos. Muchos países tienen sus propios dominios de segundo nivel por debajo, paralelamente a los dominios genéricos. Por ejemplo, en el Reino Unido, los dominios equivalentes a `.com` y `.edu` son `.co.uk` y `.ac.uk` («ac» es la abreviatura de «academic»). Está también el dominio `.us`, organizado geográficamente por estados (por ejemplo, `.ny.us` se refiere al estado de New York). El mapeado de nombres a direcciones, proceso denominado resolución de nombres de dominio, lo proporcionan sistemas independientes cooperativos, llamados servidores de nombres. Un servidor de nombres es un programa servidor que responde a peticiones de un cliente llamado procesador de nombres.

El DNS suministra el mapeado de nombres simbólicos a direcciones IP y viceversa. Mientras que en principio es algo sencillo buscar en la base de datos una dirección IP, dado su nombre simbólico, el proceso inverso no se puede hacer respetando la jerarquía. Por este motivo, existe otro espacio de nombres para el mapeado inverso. Se halla en el dominio `in-addr.arpa` («arpa» porque Internet era originalmente la red de ARPA). Como las direcciones IP suelen escribirse en formato decimal con pun-

tos, hay una capa de dominios para cada jerarquía. Sin embargo, debido a que los nombres de dominio tienen primero la parte menos significativa del nombre y el formato decimal con puntos los bytes más significativos primero, la dirección decimal se muestra en orden inverso. Por ejemplo, el dominio del DNS correspondiente a la dirección IP 129.34.139.30 es 30.139.34.129.in-addr.arpa. Dada una dirección IP, el DNS puede utilizarse para encontrar el nombre del host que sea su pareja. Una consulta de nombre de dominio para encontrar los nombres del host asociado a una dirección IP se llama «consulta con puntero».

EL DNS está designado para ser capaz de almacenar una gran cantidad de información. Una de las más importantes es la información del intercambio de correo, usada para el encaminamiento del correo electrónico. Esto aporta dos servicios: transparencia al reencaminar el correo a un host distinto del especificado y la implementación de pasarelas de correo, que pueden recibir correo electrónico y redirigirlo usando un protocolo diferente de aquel con el que lo reciben.

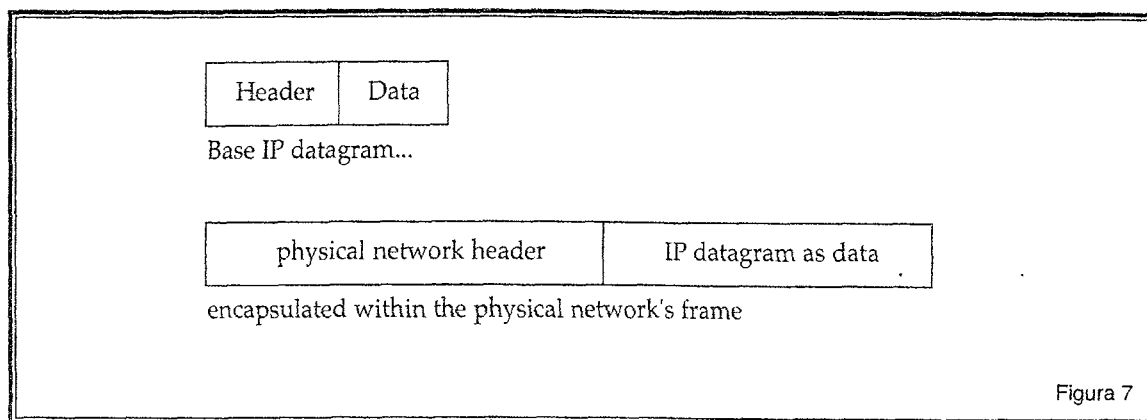
### IP («INTERNET PROTOCOL»).



IP es un protocolo estándar con STD 5 que además incluye ICMP e IGMP.

- Su especificación actual se puede encontrar en el RFC 1349.
- IP es el protocolo que oculta la red física subyacente creando una vista de red virtual. Es un protocolo de entrega de paquetes no fiable y no orientado a conexión, y se puede decir que aplica la ley del mínimo esfuerzo.
- No aporta fiabilidad, control de flujo o recuperación de errores a los prots de red inferiores. Los paquetes (datagramas) que envía IP se pueden perder, desordenar, o incluso duplicar, e IP no manejará estas situaciones. El proporcionar estos servicios depende de prots superiores.
- IP asume pocas cosas de las capas inferiores, sólo que los datagramas «probablemente» serán transportados al host de destino.

El datagrama IP es la unidad de transferencia en la pila IP. Tiene una cabecera con información para IP, y los datos relevantes para los protocolos superiores.



El datagrama IP está encapsulado en la trama de red subyacente, que suele tener una longitud máxima, dependiendo del hardware usado. Para Ethernet, será típicamente de 1.500 bytes. En vez de limitar el datagrama a un tamaño máximo, IP puede tratar la fragmentación y el reensamblado de sus datagramas. En particular, el IP no impone un tamaño máximo, pero establece que todas las redes deberían ser capaces de manejar al menos 576 bytes. Los fragmentos de datagramas tienen todos una cabecera, copiada básicamente del datagrama original, y de los datos que la siguen. Se tratan como datagramas normales mientras son transportados a su destino. Nótese, sin embargo, que si uno de los fragmentos se pierde, todo el datagrama se considerará perdido, y los restantes fragmentos se considerarán perdidos.

Cuando un datagrama IP viaja de un host a otro puede cruzar distintas redes físicas. Las redes físicas imponen un tamaño máximo de trama, llamado MTU («Maximum Transmission Unit»), que limita la longitud de un datagrama. Por ello, existe un mecanismo para fragmentar los datagramas IP grandes en otros más pequeños, y luego reensamblarlos en el host de destino. IP requiere que cada enlace tenga un MTU de al menos 68 bytes, de forma que si cualquier red proporciona un valor inferior, la fragmentación y el reensamblado tendrán que implementarse en la capa de la interfaz de red de forma transparente a IP. 68 es la suma de la mayor cabecera IP, de 60 bytes, y del tamaño mínimo posible de los datos en un fragmento, 8 bytes. Las implementaciones de IP no están obligadas a manejar datagrama sin fragmentar mayores de 576 bytes, pero la mayoría podrá manipular valores más grandes, típicamente ligeramente más de 8192 bytes, o incluso mayores, y raramente menos de 1.500.

Una función importante de la capa IP es el encaminamiento. Proporciona los mecanismos básicos para interconectar distintas redes físicas. Esto significa que un host puede actuar simultáneamente como host normal y como router. Un router básico de este tipo se conoce como router con información parcial de encaminamiento, ya que sólo contiene información acerca de cuatro tipos de destino:

- Los hosts conectados directamente a una de las redes físicas a las que está conectado el router.
- Los host o redes para las se le han dado al router definiciones específicas.
- Los hosts o redes para las que el host ha recibido un mensaje ICMP redirect.
- Un destino por defecto para todo lo demás.

Los dos últimos casos permiten a un router básico comenzar con una cantidad muy limitada de información para ir aumentando debido a que un router más avanzado lance un mensaje ICMP redirect cuando reciba un datagrama y conozca un router mejor en la misma red al que dirigir el datagrama. Este proceso se repite cada vez que un router básico se reinicia. Se necesitan protocolos adicionales para implementar un router completamente funcional que pueda intercambiar información con otros routers en redes remotas. Tales routers son esenciales, excepto en redes pequeñas.

#### DESTINOS DIRECTOS E INDIRECTOS.

Si el host de destino está conectado a una red a la que también está conectado el host fuente, un datagrama IP puede ser enviado directamente, simplemente encapsulando el datagrama IP en una trama. Es lo que se llama encaminamiento directo.

El encaminamiento indirecto ocurre cuando el host de destino no está en una red conectada directamente al host fuente. La única forma de alcanzar el destino es a través de uno o más routers. La dirección del primero de ellos (el primer salto) se llama ruta indirecta. La dirección del primer salto es la única información que necesita el host fuente: el router que reciba el datagrama se responsabiliza del segundo salto, y así sucesivamente.

Un host puede distinguir si una ruta es directa o indirecta examinando el número de red y de subred de la dirección IP.

1. Si coinciden con una de las direcciones IP del host fuente, la ruta es directa.

El host necesita ser capaz de direccionar correctamente el objetivo usando un protocolo inferior a IP. Esto se puede hacer automáticamente, usando un protocolo como ARP, que se usan en LAN's con broadcast, o estáticamente y configurando el host, por ejemplo, cuando un host MVS tiene una conexión TCP/IP sobre un enlace SNA.

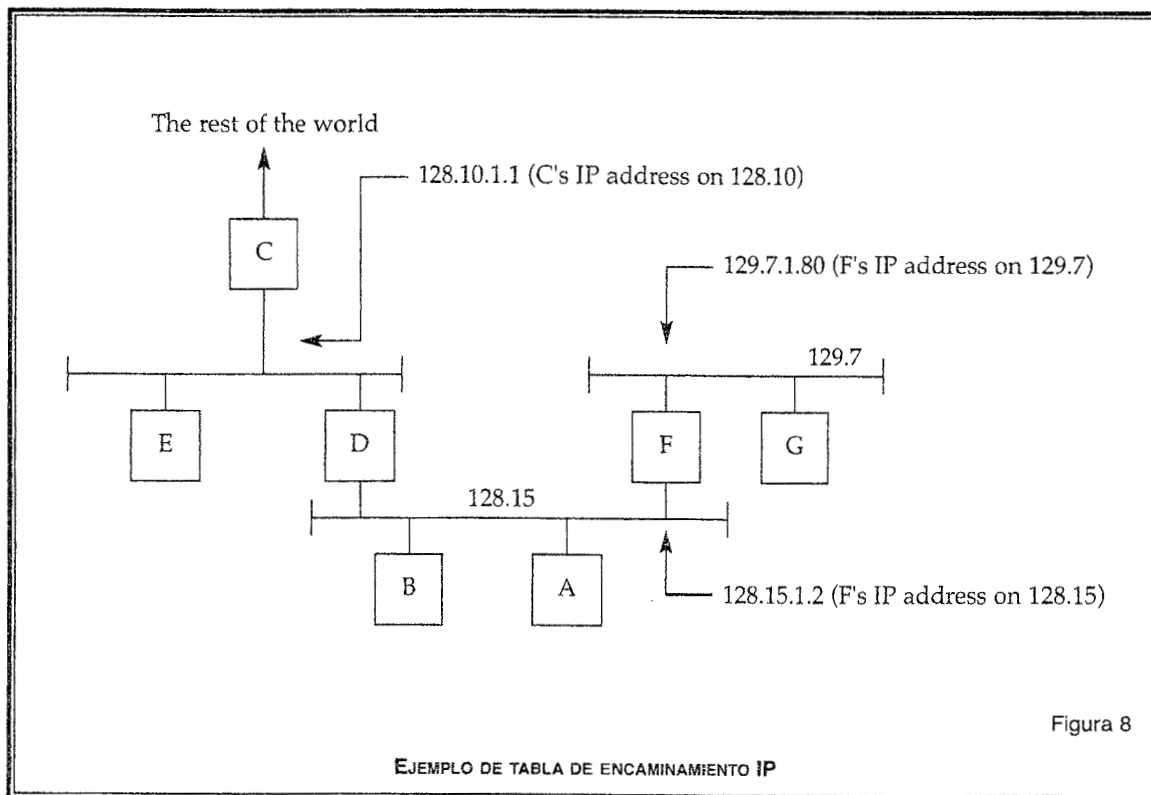
2. Para rutas indirectas, el único conocimiento requerido es la dirección IP de un router que conduzca a la red de destino.

Las implementaciones de IP pueden soportar también rutas explícitas, es decir, una ruta a una dirección IP concreta. En general, sin embargo, la información de encaminamiento se genera sólo mediante los números de red y de subred.

## TABLA DE ENCAMINAMIENTO IP.

Cada host guarda el conjunto de mapeados entre las direcciones IP de destino y las direcciones IP del siguiente salto para ese destino en una tabla llamada tabla de encaminamiento IP. En esta tabla se pueden encontrar tres tipos de mapeado:

1. Rutas directas, para redes conectadas localmente.
2. Rutas indirectas, para redes accesibles a través de uno o más routers.
3. Una ruta por defecto, que contiene la IP de un router que todas las direcciones IP no contempladas en las rutas directas e indirectas han de usar.



La tabla de encaminamiento contiene las siguientes entradas:

Destination

route via 128.10

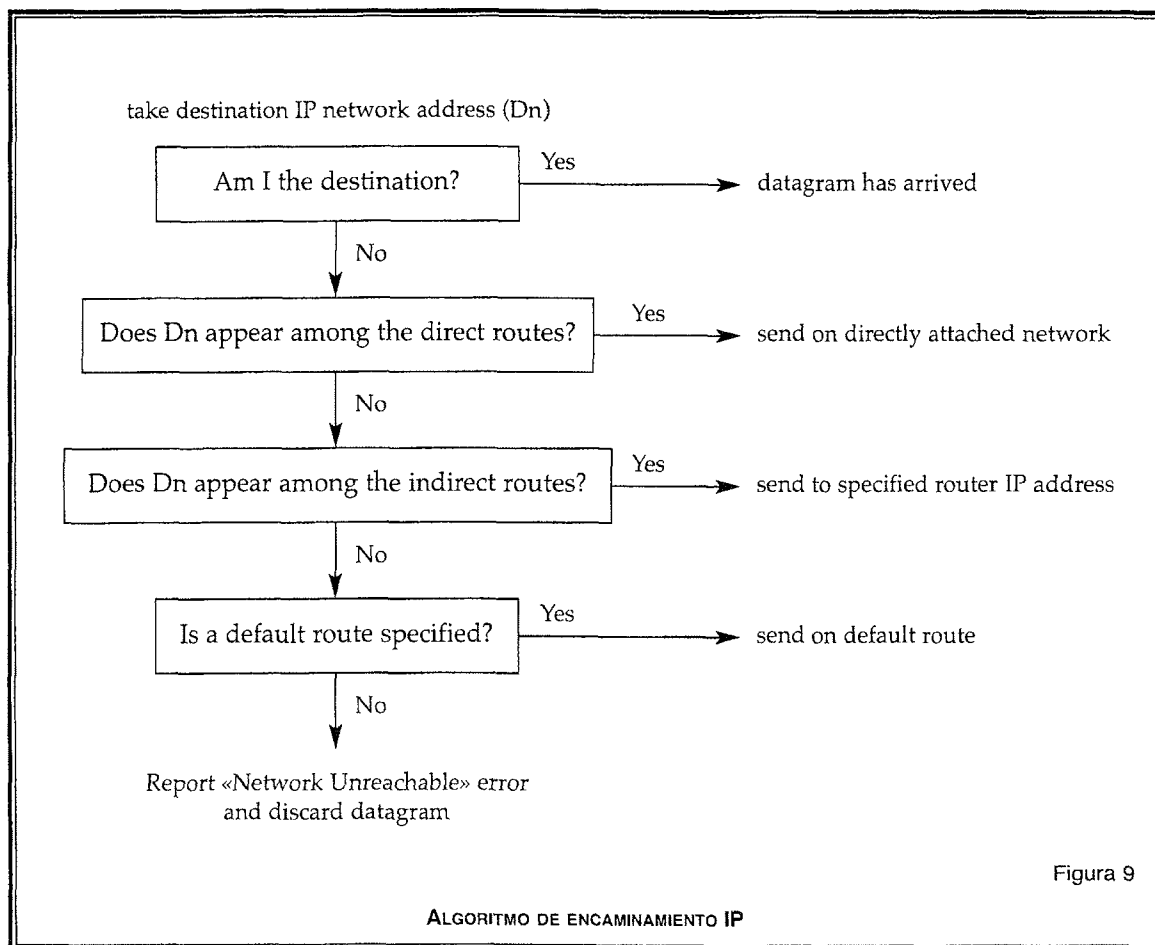
direct attachment 128.15

direct attachment 129.7 128.15.1.2

default 128.10.1.1

## ALGORITMO DE ENCAMINAMIENTO IP.

De los principios ya comentados de IP, es fácil deducir los pasos que IP debe tomar con el fin de determinar la ruta para un datagrama de salida. Es lo que se denomina algoritmo de encaminamiento IP.

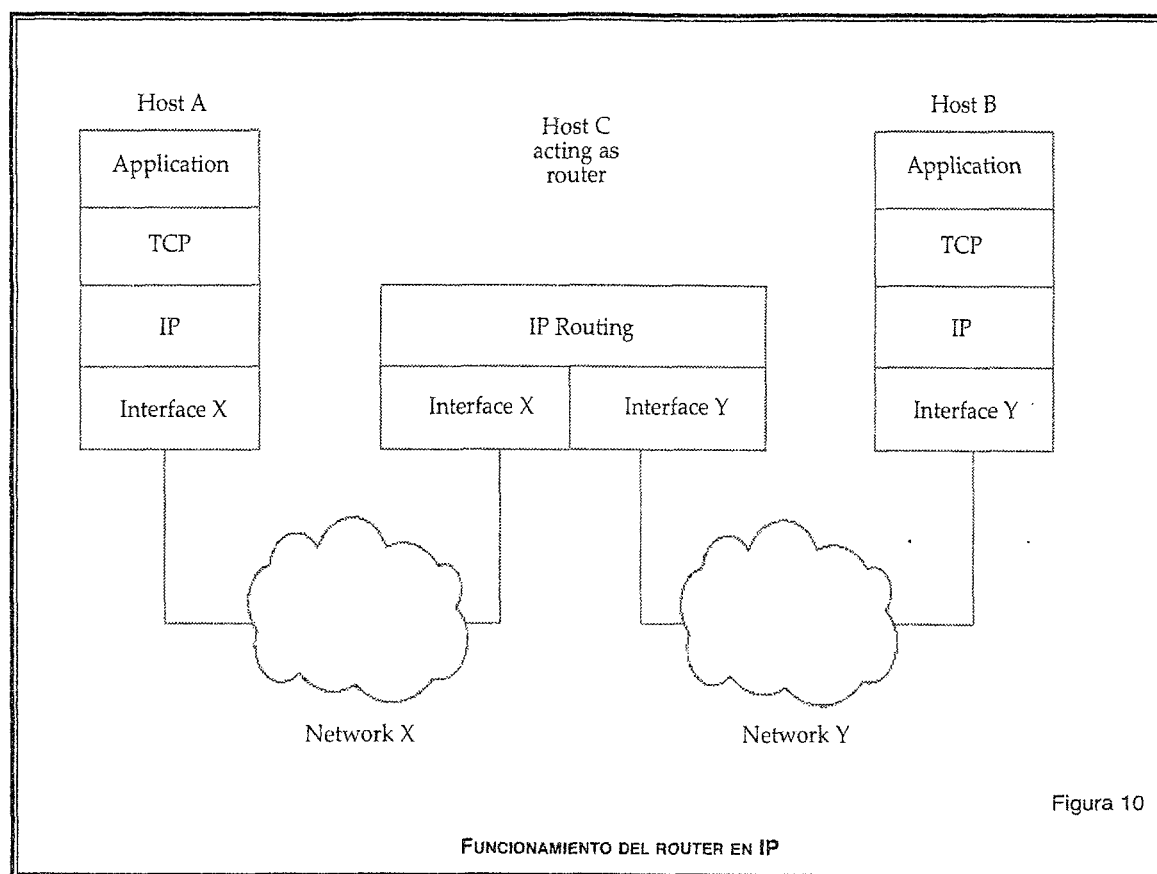


Nótese que se trata de un proceso iterativo. Se aplica a todo host que maneje un datagrama, exceptuando al host al que se entrega finalmente el datagrama.

La función fundamental de encaminamiento está presente en todas las implementaciones de IP:

- Un datagrama IP entrante que especifica una «IP de destino» distinta de la dirección local del host se trata como un datagrama IP saliente normal y corriente.

Este datagrama IP está sujeto al algoritmo de encaminamiento IP del host local, que selecciona el siguiente salto del datagrama (el siguiente host al que se enviará). Este nuevo destino puede estar en cualquiera de las redes físicas con las que el host está conectado. Si es una red física diferente de aquella en la que se recibió el datagrama, resulta que el host que hace de intermediario ha retransmitido el datagrama de una red física a otra.



La tabla de encaminamiento IP normal contiene información acerca de las redes conectadas localmente y de las direcciones IP de otros routers localizados en ellas, además de las redes con las que están conectados. Se puede extender con información de las redes IP que se hallan aún más lejos, y tener incluso una ruta por defecto, pero sigue representando una fracción de Internet. Por ello, se le llama router con información parcial de encaminamiento.

A estos routers se les aplican algunas consideraciones:

- No conocen todas las redes de Internet.
- Permiten la autonomía de sitios locales para establecer y modificar rutas.
- Una entrada de encaminamiento errónea en uno de los routers puede introducir inconsistencias, haciendo, por tanto, que parte de la red sea inalcanzable.

Deberían implementar algún mecanismo de informe de errores vía ICMP («Internet Control Message Protocol») descrito en ICMP («Internet Control Message Protocol»). Los siguientes errores deberían poderse enviar al host fuente:

- Destino IP desconocido con un mensaje ICMP Destination Unreachable.
- Redirección del tráfico a routers más adecuados enviando mensajes ICMP Redirect.

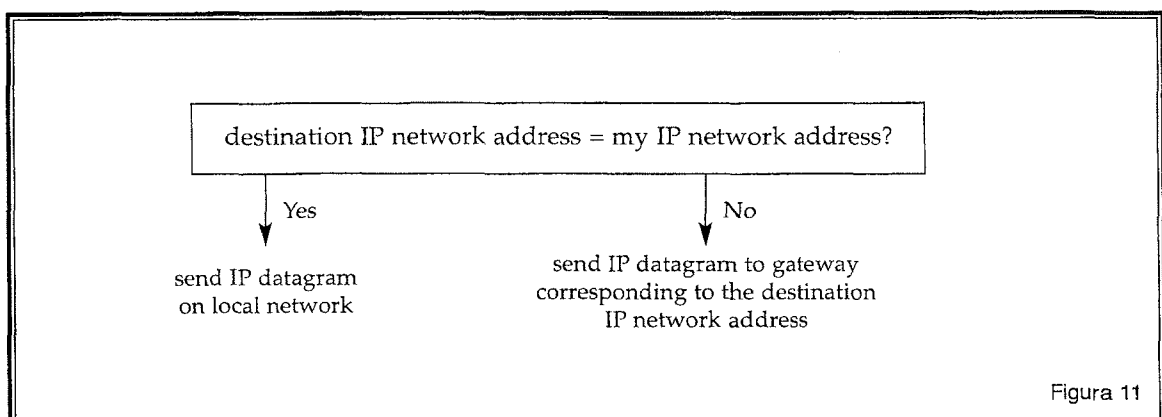
- Problemas de congestión (demasiados datagramas entrantes para el espacio disponible en el buffer) con el mensaje ICMP Source Quench.
- El campo TTL («Time-to-Live») de un datagrama IP ha llegado a cero. Se comunica con el mensaje ICMP Time Exceeded.
- Además, se deberían soportar las siguientes operaciones y mensajes ICMP básicos:
  - Problema de parámetros.
  - Máscara de dirección.
  - TS («Time stamp»).
  - Solicitud/respuesta de información.
  - Solicitud respuesta de eco.

Hace falta un router más inteligente si:

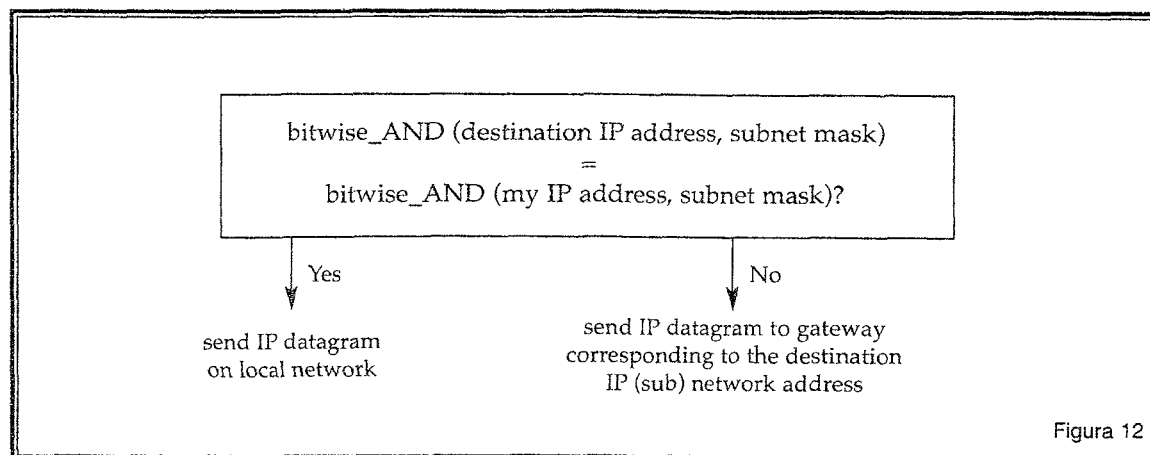
- Ha de conocer las rutas a todas las posibles redes IP, como era el caso de las pasarelas del núcleo de ARPANET.
- El router ha de tener tablas de encaminamiento dinámicas, que se actualizan con poca o ninguna intervención manual.
- El router ha de anunciar los cambios locales a los otros routers.

#### ENCAMINAMIENTO IP CON SUBREDES.

Para encaminar un datagrama IP en la red, el algoritmo general de encaminamiento IP tiene la forma siguiente:



Para ser capaz de distinguir entre subredes, el algoritmo de encaminamiento IP cambia y adopta la siguiente forma:



Algunas consecuencias de este algoritmo son:

- Es un cambio a algoritmo general. Por tanto, para poder operar de este modo, la correspondiente pasarela debe contener también el nuevo algoritmo. Algunas implementaciones pueden seguir usando el algoritmo general, y no funcionarán dentro de una red con subredes, aunque todavía podrán comunicarse con hosts en otras redes que no empleen «subnetting».
- Ya que el encaminamiento IP se usa en todos los hosts (aunque no en todos los routers), todos los hosts en la subred deben:
  1. Tener un algoritmo IP que soporte «subnetting».
  2. Tener la misma máscara de subred (a menos que existan subredes dentro de la subred).
- Si la implementación de algún host no soporta «subnetting», dicho host sólo podrá comunicarse con hosts de la propia subred, pero no con máquinas que se hallen en otra subred dentro de su misma red. Esto se debe a que el host sólo ve la red IP y su encaminamiento no puede distinguir entre un datagrama IP dirigido a un host de su subred y que se debería enviar a través de un router a una subred diferente.

RFC («REQUEST FOR COMMENTS»).

La pila de protocolos de Internet sigue evolucionando mediante el mecanismo conocido como RFC («Request For Comments»). Los investigadores están diseñando e implementando nuevos protocolos (en su mayoría del nivel de aplicación), que se ponen en conocimiento de la comunidad de Internet en la forma de un RFC. El RFC es descrito por el IAB («Internet Architecture Board»). La mayor fuente de RFC es el IETF («Internet Engineering Task Force») que es una organización subsidiaria del IAB. Sin embargo, cualquiera puede enviar un informe propuesto como RFC al editor de los RFC. Hay una serie de normas que los autores de RFC deben seguir para que su RFC sea aceptado. Estas reglas se describen en un RFC (RFC 1543) que además indica cómo enviar una propuesta de RFC.

Una vez que un RFC ha sido publicado, todas las revisiones y sustituciones se publican como nuevos RFC. Se dice que un nuevo RFC que revisa o sustituye a un RFC ya existente actualiza o desfasa a ese RFC. Asimismo, el RFC original es actualizado o desfasado por el nuevo. Por ejemplo, el RFC 1521 que describe el protocolo MIME es una segunda edición, siendo una revisión del RFC 1341, y el RFC 1590 es una enmienda del 1521. Por tanto, el RFC 1521 se etiqueta del modo siguiente: «Deja obsoleto al RFC 1341; Actualizado por el RFC 1590». En consecuencia, nunca hay confusión sobre si dos personas se refieren a dos versiones distintas de un RFC.

Algunos RFC se califican como documentos informativos mientras que otros describen protocolos de Internet. El IAB («Internet Architecture Board») mantiene una lista de todos los RFC que describen la pila de protocolos. A cada uno de ellos se le asigna un estado y un estatus.

## 6. PROTOCOLO IPv6.

El problema del agotamiento de las direcciones IP. El número de redes en Internet se ha ido doblando aproximadamente cada año durante varios años. Sin embargo, el uso de las redes de clase A, B y C difiere mucho: la mayoría de las redes asignadas a finales de 1980 eran de clase B, y en 1990 se hizo evidente que, de continuar así la tendencia, el último número de red de clase B sería asignado en 1994. Por otro lado, las redes de clase C apenas se usaban.

La razón de esta tendencia era que la mayoría de los usuarios potenciales hallaban a las redes de clase B lo bastante grandes para sus necesidades previstas, ya que acomoda hasta 65.534 hosts, mientras que una red de clase C, con un máximo de 254 hosts, restringe considerablemente el crecimiento potencial de hasta las redes pequeñas. Es más, la mayoría de las redes de clase B estaban asignadas a redes pequeñas. Hay un número relativamente pequeño de redes que necesiten 65.534 direcciones de hosts, pero muy pocas para que 254 sea un límite adecuado. En resumen, aunque las divisiones de clase A, B y C de las direcciones IP son lógicas y fáciles de usar (puesto que se producen a nivel de byte), en perspectiva no son las más prácticas, ya que las redes de clase C son demasiado pequeñas para la mayoría de las organizaciones mientras que son demasiado grandes para ser bien aprovechadas por nadie, excepto por las organizaciones más grandes.

Las nuevas direcciones son de 128 bits:  $3,4 \times 10$  elevado a 38 direcciones distintas ( $6,65 \times 10$  elevado a 23 ordenadores por cada metro cuadrado de la superficie terrestre). Las direcciones se escriben en 8 bloques de 16 bits, en hexadecimal, separados por el carácter ":" Pueden omitirse en cada bloque los ceros no significativos: 5A01:0:0:0:8:800:200C:417.<sup>a</sup>. Pueden sustituirse las secuencias de bloques consecutivos con los 16 bits a cero en la abreviatura "::". Esto sólo puede hacerse una vez por dirección: 5A01::8:800:200C:417. Con un octeto (ocho bits de la forma 00010111) se pueden representar los números de 0 a 255. Por tanto las direcciones IPv4 se componen de cuatro octetos, o 32 bits, lo cual genera los cuatro millones y pico de direcciones antes mencionadas.

En IPv6 las direcciones se componen de 16 octetos, es decir 128 bits. Esto daría lugar a 2.128 direcciones, más o menos 340 sextillones. No obstante, esta cifra no se alcanza, ya que parte de los dígitos identifican el tipo de dirección, con lo que se quedan en 3.800 millones. En cualquier caso, se garantiza que no se acabarán en un plazo razonable. Hay tres tipos de direcciones: unicast, anycast y multicast. Las direcciones unicast identifican un solo destino. Un paquete que se envía a una dirección unicast llega sólo al ordenador al que corresponda. En el caso de las direcciones anycast se trata de un conjunto de ordenadores o dispositivos, que pueden pertenecer a nodos diferentes. Si se envía un paquete a una de estas direcciones lo recibirá el ordenador más cercano de entre las rutas posibles. Las

direcciones multicast definen un conjunto de direcciones pertenecientes también a nodos diferentes, pero ahora los paquetes llegan a todas las máquinas identificadas por esa dirección. La arquitectura de direccionamiento de IPv6 se describe con detalle en la RFC 2373. Para representar las direcciones IPv6 como cadenas de texto (en lugar de ceros y unos) hay diferentes reglas.

- La primera se denomina preferred form y consiste en listar la dirección completa como 8 números hexadecimales de cuatro cifras (8 paquetes de 16 bits):

FEDC:2A5F:709C:216:AEBC:97:3154:3D12 1030:2A9C:0:0:0:500:200C:3A4

- La otra posibilidad es la forma comprimida o compressed form, en la que las cadenas que sean cero se sustituyen por un par de dos puntos "::" que indican que hay un grupo de ceros. Por ejemplo: FF08:0:0:0:0:209A:61 queda F08::209A:61 0:0:0:0:0:0:1 queda ::1
- Por último se pueden escribir en forma mixta, con las primeras cifras en hexadecimal y las últimas (las correspondientes a IPv4) en decimal: 0:0:0:0:0:0:193.136.239.163 ::193.136.239.163

Las seis secciones de 16 bits de mayor orden (las de la izquierda) se muestran en hexadecimal, pero el resto se muestra en la familiar notación decimal con puntos.

#### CARACTERÍSTICAS DE IPv6.

- La nueva versión debe ser capaz de coexistir e interoperar con las especificaciones actuales de IPv4.
- Admite un espacio de direccionamiento exponencialmente mayor que IPv4.
- Los paquetes de IPv6 son más ligeros para facilitar la transmisión por distintos medios.
- IPv6 retiene la mayoría de los conceptos básicos de IPv4.
- Al igual que IPv4, IPv6 es un servicio de entrega de datagramas no confiable y sin conexión.
- El formato de los datagramas en IPv6 es muy diferente al de IPv4.
- IPv6 provee nuevas funcionalidades como autenticación y seguridad.
- IPv6 organiza cada datagrama como una secuencia de encabezados seguida de datos.

Un datagrama siempre comienza con un encabezado base de 40 octetos, el cual contiene las direcciones fuente y destino y un identificador de flujo.

- El encabezado base puede estar seguido de 0 o más encabezados de extensión, seguido de datos.
- Los encabezados de extensión son opcionales; IPv6 los usa para codificar las mayoría de las opciones de IPv4.
- Las direcciones en IPv6 son de 128 bits.
- Las direcciones están divididas en tipos, de manera análoga a las clases en IPv4.

## DIFERENCIAS CON LA VERSIÓN 4.

- Capacidad de direccionamiento ampliada.

IPv6 incrementa el tamaño de la dirección desde los 32 bits a los 128 bits, para dar soporte a más niveles de jerarquías de direccionamiento, un mayor número de nodos direccionables, y a una autoconfiguración más sencilla de las direcciones. La escalabilidad del encaminamiento multicast se ve incrementada por la inclusión de un campo «scope» (finalidad) a las direcciones multicast addresses. Y se define un nuevo tipo de dirección denominada «anycast address», usada para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del formato de cabecera.

Algunos campos de la cabecera de IPv4 han sido eliminados o convertidos en opcionales para reducir el coste de proceso normal de los paquetes y limitar el coste en ancho de banda de la cabecera IPv6.

- Mayor soporte para extensiones y opciones.

Los cambios en la forma en que se codifican las opciones de la cabecera IP permiten una transmisión más eficiente, menos limitaciones para la longitud de las opciones y mayor flexibilidad para incluir nuevas opciones en un futuro.

- Capacidad de etiquetado de flujo.

Se ha añadido una nueva posibilidad para permitir el etiquetado de paquetes pertenecientes a un determinado «flujo» de tráfico para el que el emisor requiere de un manejo especial, como una calidad diferente de la de por defecto o servicio en tiempo real.

- Utilidades de autenticación y privacidad.

Extensiones para dar soporte de autenticación, integridad de los datos y opcionalmente confidencialidad de los datos.

## FORMATO DE CABECERA IPV6.

- Versión. Numero de versión de Internet Protocol (4 bits). Su valor es 6.
- Clase de tráfico. Campo de clase de trafico (8 bits).
- Etiqueta de flujo (20 bits).
- Longitud de carga útil. Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos (notar que cualesquiera de las cabeceras de extensión presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud).
- Cabecera siguiente. Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700].
- Límite de salto. Entero sin signo de 8 bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de saltos es decrementado hasta cero.

- Dirección de origen. Dirección de 128 bits del originador del paquete.
- Dirección destino. Dirección de 128 bits del recipiente pretendido del paquete (posiblemente no el último recipiente, si está presente una cabecera Enrutamiento).

Se han mejorado las cabeceras de los paquetes, eliminado algunos campos de la cabecera IPv4, haciendo que otros sean opcionales y utilizando cabeceras de extensión. Las cabeceras de extensión son cabeceras separadas que, con una excepción, no las examina ningún host en la ruta desde el origen al destino, mejorando la eficiencia del enrutamiento.

También permite una mayor flexibilidad en la codificación de opciones y capacidades de expansión para opciones futuras.

En IPv6 se introduce el etiquetado de flujos, lo que permite indicar que los paquetes pertenecen a determinado «flujo» de tráfico. De esta forma se permite manejar QoS y la administración de ancho de banda sin tener que analizar cabeceras de TCP ni de UDP.

También se han introducido extensiones que permiten autenticación, asegurar la integridad de los datos y cifrado de paquetes opcional.

En el IPv6, la información de capa Internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguiente distinto. Según esto un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión cada una identificada por el campo Cabecera Siguiente de la cabecera precedente.

