INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

Curso *online*: **Seguridad en Redes WAN e Internet**

Módulo 3 ARQUITECTURA DE TCP/IP

Autores: Daniel Díaz y Andrés Marín

Índice de contenidos

Capítulo 1 Sistemas abiertos 2

1.1. ARQUITECTURA TCP/IP 3
1.2. NIVEL DE ACCESO A LA RED 5

Capítulo 2 NIVEL DE INTERNET 6

2.1. PROTOCOLO INTERNET (IP) 6
2.1.1. EL DATAGRAMA 6
2.1.2. ENRUTAMIENTO Y FRAGMENTACIÓN DE DATAGRAMAS 8
2.2. PROTOCOLO INTERNET DE MENSAJES DE CONTROL (ICMP) 10

Capítulo 3 DIRECCIONAMIENTO *IP* 11

3.1. AGOTAMIENTO DE DIRECCIONES 13
3.2. DIRECCIONES *IP* PRIVADAS 13
3.3. SUBREDES 14
3.4. IPv6 15
3.4.1. Direccionamiento en IPv6 18
3.4.2. DIRECCIONES *IP* PRIVADAS EN LA ADMINISTRACIÓN PÚBLICA ESPAÑOLA 19
3.5. NOMBRES SIMBÓLICOS 20
3.6. ARQUITECTURA DE ENRUTAMIENTO DE INTERNET 22
3.7. LA TABLA DE ENRUTAMIENTO 23

Capítulo 4 NIVEL DE TRANSPORTE 25

4.1. PROTOCOLO DE DATAGRAMA DE USUARIO (UDP) 25
4.2. PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP) 26

Capítulo 5 NIVEL DE APLICACIÓN 31

Capítulo 6 PROTOCOLOS, PUERTOS Y SOCKETS 32

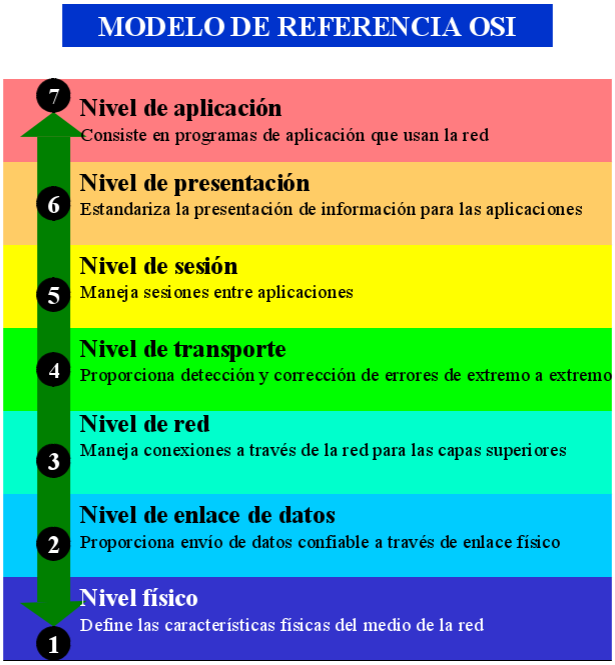
6.1. NÚMEROS DE PROTOCOLO 32
6.2. NÚMEROS DE PUERTO 33
6.3. SOCKETS 35

CAPÍTULO 1 SISTEMAS ABIERTOS

Se define como Sistema Abierto aquél que es capaz de interconectarse con otros de acuerdo con unas normas establecidas por una institución independiente de normalización. Consiguientemente, la interconexión de sistemas abiertos se ocupará del intercambio de información entre estos sistemas y tratará de que puedan trabajar cooperativamente.

En 1978, el JTC1 de ISO/IEC propuso el modelo de referencia para la interconexión de sistemas abiertos, OSI-RM (*Open Systems Interconection*, *Reference Model*), que sigue la técnica de estructuración de separación de capas. De este modo, las funcionalidades de comunicación quedan separadas en un conjunto jerárquico de capas. En concreto el modelo OSI-RM especifica siete capas funcionales para un sistema de interconexión.

El Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI, *Open Systems Interconnections*) desarrollado por la Organización Internacional de Normas (ISO, *International Standars Organization*), proporciona una referencia común para describir la estructura y funciones de los protocolos de comunicación de datos. El modelo establece siete niveles, en la Figura se puede observar que estos niveles se estructuran como una pila de bloques de construcción colocados uno encima del otro.



Los protocolos establecen una descripción formal de los formatos que deberán presentar los mensajes para poder ser intercambiados entre ordenadores y definen las reglas que deben seguir para lograrlo.

En cada nivel se define una función de comunicación de datos que puede ser realizada por uno o varios protocolos, cada uno de los cuales proporciona un servicio apropiado para la función de ese nivel. Por ejemplo, un protocolo de transferencia de archivos y otro de correo electrónico proporcionan servicios de usuario y ambos son parte del nivel de aplicación. Cada protocolo se comunica con su compañero o mejor dicho con su par. Un par es una implementación del mismo protocolo en el nivel equivalente de un sistema remoto *"peer to peer"*.

También debe haber concordancia en como fluye la información entre los niveles dentro de un ordenador, los niveles superiores se basan en los inferiores para transferir la información a través de la red. La información desciende por la pila de un nivel al siguiente, hasta que se transmite a través de la red por los protocolos de nivel físico. En el extremo remoto, la información asciende por la pila a la aplicación receptora. Los niveles individuales no necesitan saber cómo funcionan los niveles que se ubican por arriba o por debajo de ellos; sólo deben saber cómo pasarles la información. Aislar las funciones de comunicación en diferentes niveles minimiza el impacto del cambio tecnológico en todo el grupo de protocolos. Pueden agregarse nuevas aplicaciones sin cambiar la red física, y puede instalarse nuevo hardware de red sin tener que cambiar el software de aplicación.

1.1. ARQUITECTURA TCP/IP

En 1973, la agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA), de los Estados Unidos, inició un programa para la investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El proyecto tenía por objeto la interconexión de redes, por lo que se le denominó "*Internetting*", y a la familia de redes de ordenadores que surgió de esta investigación se le denominó "Internet". Al Conjunto de Protocolos desarrollados se les denominó TCP/IP, por dos de los protocolos más importantes que pertenecen a él y que ya estaban previamente desarrollados: El Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP).

Las principales características de TCP/IP son:

- Estándares de protocolos abiertos, ampliamente disponibles y desarrollados independientemente del hardware y de sistemas operativos específicos.
- Independencia del hardware específico de la red. TCP/IP puede utilizarse sobre *Ethernet*, *Token Ring*, línea telefónica básica, red X.25.
- Esquema común de direccionamiento que permite que cualquier dispositivo TCP/IP se identifique de modo único en toda la red.
- Protocolos estándares de alto nivel para servicios de usuario consistentes y ampliamente disponibles

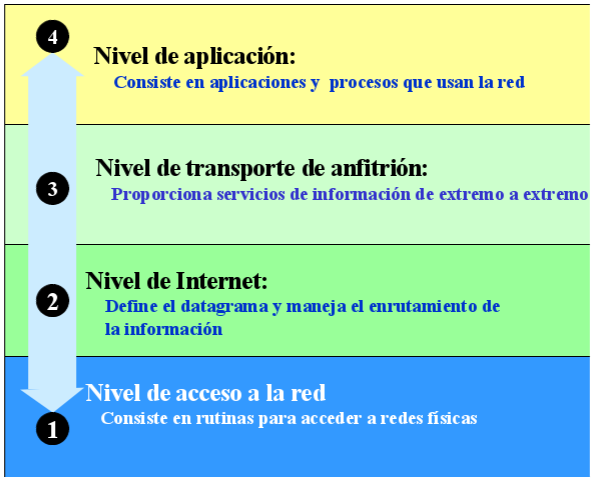
TCP/IP requiere que los documentos sobre estándares estén disponibles públicamente. El conjunto de protocolos que conforman el TCP/IP se definen en una de las tres publicaciones siguientes:

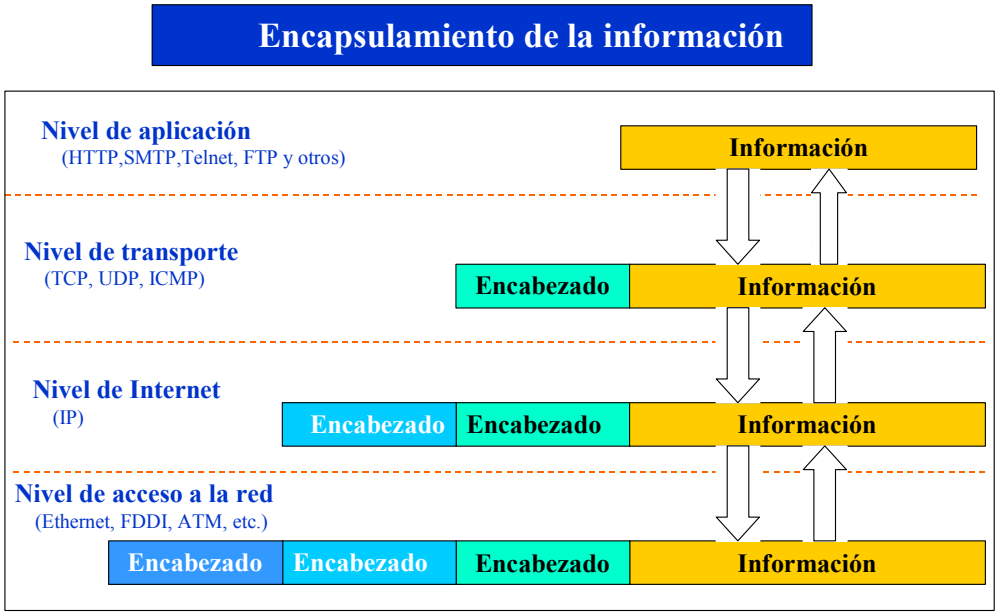
- Estándares Militares (*MIL STD*).
- Notas de Ingeniería de Internet (IEN), que ya fue abandonada.
- Solicitud de Comentarios (RFC, *Requests for Comments*) que es como se publica la mayor parte de la información sobre los protocolos TCP/IP. Las RFC contienen las versiones más recientes de las especificaciones de todos los protocolos TCP/IP.

El Internet *Activity Board* (IAB) mantiene una lista completa de RFC's y define cuales de ellos son estándares asignándoles en estado y un estatus. El estado tiene que ver con las diferentes fases a seguir en su definición: protocolo estándar, borrador estándar, propuesta estándar, experimental, informativo y protocolo histórico. El estatus tiene que ver con el nivel de integración dentro de la serie de protocolos TCP/IP: protocolo requerido, recomendado, opcional, de uso limitado y protocolo no recomendado.

La terminología del modelo de referencia OSI ayuda a describir TCP/IP, pero para comprenderlo mejor es recomendable usar un modelo que refleje directamente la estructura de TCP/IP, normalmente se propone el modelo indicado en la siguiente figura, en donde los niveles OSI de Sesión y Presentación son responsabilidad del nivel de Aplicación y los de Enlace de Datos y Físico son vistos como el nivel de Red. Por ello, el modelo TCP/IP sólo utiliza cuatro capas o niveles funcionales: Aplicación, Transporte, Internet y Acceso a Red

NIVELES EN LA ARQUITECTURA DEL TCP/IP





La figura de arriba ilustra como, en la estructura de cuatro niveles de TCP/IP, la información que se maneja desciende por la pila de protocolos del nivel de aplicación a la red física. Los niveles no son obligatorios y más bien representan empaquetamientos funcionales, es posible mantener conexiones directas entre diferentes niveles. Para asegurar el envío adecuado, cada nivel añade información de control llamada *encabezado* por colocarse delante de la información a transmitir. Cada nivel trata toda la información que recibe del nivel superior como datos y le coloca delante su propio encabezado. La adición de información de envío en cada nivel se conoce como encapsulamiento.
Cuando se recibe la información, sucede lo opuesto, cada nivel quita su encabezado antes de pasar la información al nivel superior. Conforme fluye la información de regreso hacia arriba, los datos recibidos desde un nivel inferior se interpretan como encabezado más información.

1.2. NIVEL DE ACCESO A LA RED

Es el nivel más bajo (inferior) de la jerarquía de TCP/IP. Emite al medio físico los flujos de bits y recibe los que de él provienen. Define cómo usar la red para transmitir un datagrama IP. Los protocolos del nivel de acceso a la red deben conocer los detalles básicos de la red (su estructura de paquetería, forma de envío, etc.) a fin de formatear correctamente los datos que están siendo transmitidos para cumplir con las necesidades de la red; como consecuencia hay muchos protocolos de acceso, uno para cada estándar de red física.

Las funciones que se efectúan en este nivel incluyen el encapsulamiento de los datagramas IP, unidades básicas de transmisión en Internet, dentro de las tramas transmitidas por la red, así como la traducción de direcciones IP a las direcciones físicas usadas por la red.

CAPÍTULO 2 NIVEL DE INTERNET

Es el que está por encima del de acceso a la red. El protocolo más importante de este nivel es el Protocolo Internet (IP), RFC 791, que da el servicio básico de envío de paquetes sobre el que se construyen las redes TCP/IP. Todos los protocolos, del nivel por encima de Internet (TCP, UPD) y los de por debajo (*Ethernet*, FDDI, ATM y otros), lo usan para enviar la información. Toda la información TCP/IP fluye a través de IP.

2.1. PROTOCOLO INTERNET (IP)

El protocolo IP realiza las siguientes funciones:

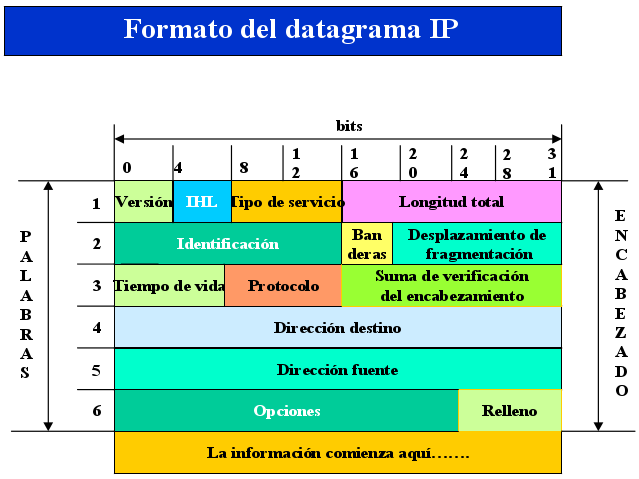
- Definir el datagrama.
- Definir el esquema de direccionamiento de Internet.
- Mover la información entre el nivel de acceso a la red y el nivel de transporte de anfitrión a anfitrión.
- Enrutar datagramas hacia anfitriones remotos.
- Realizar la fragmentación y ensamblaje de los datagramas.

IP es un *protocolo no orientado a conexión*, no intercambia información de control al establecer una conexión extremo a extremo antes de transmitir los datos. Si se necesita un servicio orientado a conexión, IP confía en protocolos de otros niveles para establecer la conexión.

2.1.1. EL DATAGRAMA

Los protocolos TCP/IP se construyeron para transmitir datos sobre ARPANET, que era una red de conmutación de paquetes. Un *paquete* es un bloque de información que lleva consigo la información necesaria para ser enviado, de modo similar a una carta postal, la cual tiene una dirección escrita en su sobre. Una red de conmutación de paquetes usa la información de direccionamiento de los paquetes para conmutar los paquetes de una red física a otra, moviéndolos hacia su destino final. Cada paquete viaja por la red de modo independiente de cualquier otro paquete

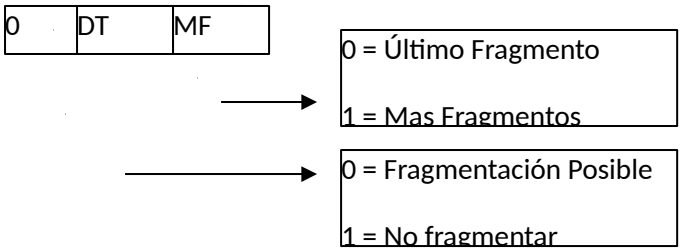
> El datagrama es el formato de paquete definido por IP, la figura representa un datagrama IP. Las primeras cinco o seis palabras de 32 bits del datagrama son información de control, llamada encabezado. De modo predeterminado, el encabezado tiene cinco palabras; la sexta palabra es opcional. Como el tamaño del encabezado es variable, incluye un campo llamado Longitud del Encabezado de Internet (IHL), que indica el tamaño del encabezado en palabras.



Formato del datagrama IP

El encabezado contiene toda la información necesaria para enviar el paquete, donde cada campo tiene el siguiente significado:

Versión: versión del Protocolo IP. La actual es la 4
IHL: longitud de la cabecera medida en unidades de 32 bits
Tipo de servicio: tipo de servicio solicitado (No se suele utilizar)
Longitud total: del datagrama completo en octetos
Identificación: Valor asignado en origen al datagrama para ayudar al reensamblado de fragmentos
Banderas:



Desplazamiento de fragmentación: posición del fragmento dentro del datagrama (en unidades de 8 octetos)
Tiempo de vida: tiempo máximo que un datagrama puede permanecer en la red (en número de saltos)
Protocolo: protocolo de IP (P.e. TCP, UDP)
Suma de verificación del encabezado: código de protección contra errores
Dirección destino y Dirección fuente: direcciones IP de destino y de origen
Opciones: opcional, facilidades para pruebas y depuración (P.e. registro de ruta, encaminamiento fijado en origen, marca de tiempo,….)

IP envía el datagrama consultando la Dirección destino, que es una dirección IP estándar de 32 bits que identifica la red destino y un anfitrión específico de esa red. Si la Dirección destino es

la dirección de un anfitrión que se encuentra en la red conectada directamente, el paquete se envía directamente al destino. Si la Dirección destino no está en la red local, el paquete pasa por una compuerta para su envío. Las compuertas son mecanismos que conmutan los paquetes entre las distintas redes físicas. Decidir que compuerta de acceso usar se conoce como enrutamiento. IP efectúa enrutamiento para cada paquete individual.

2.1.2. ENRUTAMIENTO Y FRAGMENTACIÓN DE DATAGRAMAS

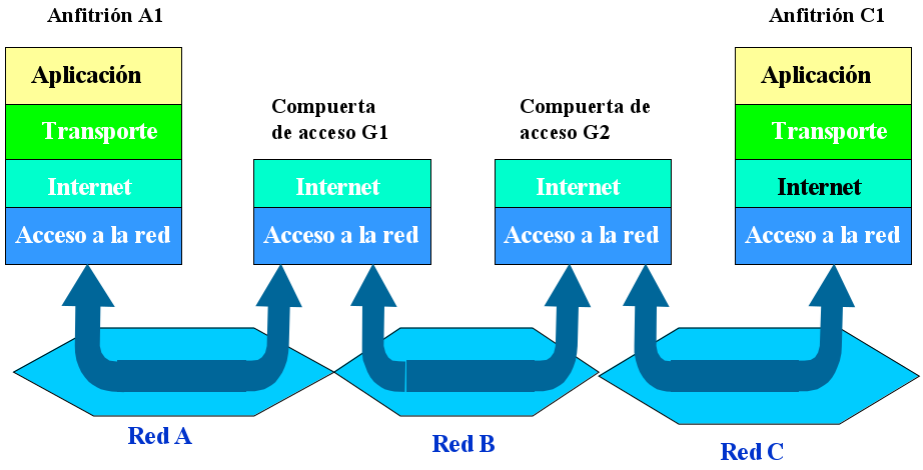
El objetivo del enrutamiento es la búsqueda de rutas en una red desde un punto origen a un destino que satisfagan una serie de condiciones (ej: rutas de mínimo costo, mínimo retardo, máxima cadencia eficaz o algún criterio administrativo). El algoritmo de encaminamiento es la parte del software del nivel de red responsable de decidir el camino a seguir por un paquete. Si la transmisión es no orientada a conexión la decisión debe tomarse para cada datagrama, si es orientada a conexión, únicamente durante el establecimiento del camino virtual.

Para comunicar redes los protocolos TCP/IP proponen una arquitectura que ve como iguales a todas las redes a conectar. En el modelo tradicional de TCP/IP, sólo hay dos tipos de dispositivos de red: las compuertas de acceso y los anfitriones. Las compuertas de acceso, también llamadas enrutadores IP, enrutan los paquetes entre las redes. Los anfitriones normalmente no enrutan paquetes, sin embargo, si un anfitrión está conectado a más de una red (anfitrión multiacceso), puede actuar como una compuerta de acceso y enviar paquetes entre redes. Actualmente se distingue entre compuertas de acceso y enrutadores: una compuerta de acceso mueve los datos entre los distintos protocolos, y un enrutador mueve los datos entre las diferentes redes

Los anfitriones (o sistemas finales) procesan los paquetes a través de los cuatro niveles del protocolo, mientras las compuertas de acceso (o sistemas intermedios) procesan los paquetes sólo hasta el nivel de Internet, donde se toman las decisiones de enrutamiento. Los anfitriones sólo pueden enviar paquetes a mecanismos conectados a la misma red física.

La figura a continuación muestra como se envían los paquetes, los paquetes de A1, destinados al anfitrión C1, son enviados a través de las compuertas de acceso G1 y G2. El anfitrión A1 envía el paquete a la compuerta G1, con la que comparte la red A. La compuerta G1 envía el paquete a G2, a través de la red B. Entonces la compuerta G2 envía el paquete directamente al anfitrión C1, pues ambos están conectados a la red C. El anfitrión A1 no tiene conocimiento de ninguna compuerta de acceso más allá de G1.

Enrutamiento a través de puertas de acceso



Enrutamiento a través de compuertas de acceso

Al enrutar un datagrama a través de diversas redes, puede ser necesario que una compuerta de acceso lo divida en fragmentos más pequeños. Un datagrama recibido desde una red puede ser demasiado grande para ser transmitido en un solo paquete por otra red de características físicas diferentes.

Cada tipo de red tiene una Unidad Máxima de Transferencia *(MTU, Maximum Transmission Unit)*, que indica la longitud máxima que puede tener un paquete a transferir por esa red. Si el datagrama recibido desde otra red es mayor que la MTU de la red por la que se va enviar, es necesario dividirlo en fragmentos menores para transmitirlo. Este proceso se llama fragmentación. Por ejemplo, IP debe dividir un paquete de *Ethernet* relativamente largo en paquetes más pequeños antes de que pueda transmitirlos sobre una red X.25.

El formato de cada fragmento es el mismo que el de cualquier datagrama normal. La palabra 2 del encabezado contiene el campo Identificación, que identifica al datagrama al que pertenece el fragmento, el campo Desplazamiento de fragmentación, que indica la parte del datagrama inicial al que corresponde este fragmento, y en el campo Banderas el bit Más Fragmentos le dice a IP si se han vuelto a unir todos los fragmentos del datagrama.

Cuando IP recibe un datagrama dirigido al anfitrión local, debe pasar la parte de información del datagrama al protocolo del nivel de transporte correcto. Esto se hace usando el Número de protocolo de la palabra 3 del encabezado del datagrama. Cada protocolo del nivel de transporte tiene un número de protocolo único que lo identifica.

2.2. PROTOCOLO INTERNET DE MENSAJES DE CONTROL (ICMP)

Una parte integral del nivel de Internet, es el protocolo ICMP, definido en la RFC 792, este protocolo usa la facilidad de envío de datagramas IP para enviar mensajes de error o de control a otras pasarelas o sistemas finales (anfitriones). Los paquetes ICPM se envían en el cuerpo de los paquetes IP, igual que los paquetes TCP y UDP. A diferencia de TCP o UDP, ICMP no tiene puertos fuente o destino, ni ningún otro protocolo sobre él. En vez de eso, un código dicta la interpretación del resto del paquete ICMP, los diferentes mensajes que se generan a través de ICMP sirven para:

Control de flujo

Cuando los datagramas llegan demasiado rápido para ser procesados, el anfitrión destino de una compuerta de acceso intermedia devuelve un mensaje ICMP de "Apaciguamiento de fuente" (*Source Quench*) al emisor, que le dice que cese temporalmente el envío de datagramas.

Detección de destinos inalcanzables

Cuándo un destino es inalcanzable, el sistema que detecta el problema envía un mensaje ICMP "Destino inalcanzable" al emisor del datagrama original. Si el destino inalcanzable es una red o un anfitrión, el mensaje se envía por una compuerta de acceso intermedia. Pero si el destino es un puerto inalcanzable, es el anfitrión destino el que envía el mensaje.

Redirección de rutas

Una compuerta de acceso envía el mensaje ICMP "Redirigir" para decir a un anfitrión que use otra compuerta de acceso, supuestamente porque es una opción mejor. Este mensaje sólo puede usarse cuando el anfitrión fuente está en la misma red que las dos compuertas de acceso.

Verificación de anfitriones remotos

Un anfitrión puede enviar el mensaje ICMP de solicitud de eco, para ver si el protocolo IP de un sistema remoto está activado y en operación. Cuando un sistema recibe un mensaje de eco, devuelve el mismo paquete al anfitrión fuente, respuesta de eco. El comando ping de UNIX usa este mensaje.

Tiempo excedido

Lo que devuelve un enrutador cuando determina que un paquete parece estar ciclado; un nombre más intuitivo podría ser número máximo de saltos excedido

Un ejemplo práctico del uso de este tipo de mensaje ICMP es el comando *Traceroute*, que permite conocer la ruta por la que pasa un datagrama. Se basa en enviar ecos ICMP con tiempos de vida bajos para provocar que las pasarelas atravesadas generen mensajes de error (Tiempo de vida excedido) y así conocer el camino seguido.

Los errores producidos en la transmisión de datagramas con mensajes ICMP no generan nuevos mensajes ICMP.

Capítulo 3 DIRECCIONAMIENTO *IP*

Para que en una red dos ordenadores puedan comunicarse entre sí deben estar identificados con precisión. Las direcciones IP identifican de modo único a cada anfitrión

Cada datagrama se envía a la dirección contenida en la Dirección destino, de su propio encabezado. La Dirección destino es una dirección IP estándar de 32 bits que contiene suficiente información para identificar de modo único una red y un anfitrión específico de esa red.

Una dirección IP contiene una parte de red y una parte de anfitrión, IP usa la parte de red para enrutar el datagrama entre las redes, y la parte de anfitrión se usa para hacer la entrega final cuando el datagrama llega a la red destino.

En una dirección IP, el número de bits utilizados para identificar la dirección de la red y la del anfitrión, varían de acuerdo con la *clase* de la dirección. Hay tres clases principales de direcciones: clase A, clase B y clase C.
IP examina los bits iniciales de una dirección para determinar la clase de dirección y, por lo tanto, su estructura:

- Si el primer bit de una dirección IP es 0, es una dirección de una red clase A. Los siete bits siguientes identifican la red; los últimos 24 bits identifican al anfitrión.
- Si los dos primeros bits de la dirección son 1 0, es una dirección de red clase B. Los siguientes catorce bits del primer byte identifican la red; los últimos dieciséis identifican al anfitrión.
- Si los tres primeros bits de la dirección son 1 1 0, es una dirección de red clase C. En una dirección clase C, los primeros tres bits identifican la clase; los siguientes 21 bits de los tres primeros bytes son dirección de red; los últimos ocho identifican al anfitrión.
- Si los tres primeros bits de la dirección son 1 1 1, es una dirección especial reservada. A veces, estas direcciones se llaman direcciones clase D, pero en realidad no se refieren a redes específicas. La direcciones *Multicast* se usan para direccionar grupos de varios ordenadores a la vez. Asimismo, identifican un grupo de ordenadores que comparten una red común.

Generalmente las direcciones IP se escriben como cuatro números decimales separados por puntos. Cada uno de los cuatro números se encuentra en el rango 0-255 (los valores decimales posibles para un byte). Como los bits que identifican la clase son contiguos a los bits de la red de la dirección, podemos juntarlos y ver la dirección como si estuviera compuesta de bytes completos de dirección de red y bytes completos de dirección de anfitrión. Así, un valor del primer byte:

- Menor que 128 indica una dirección clase A; el primer byte es el número de red y los tres siguientes son la dirección de anfitrión.
- Del 128 al 191 es una dirección clase B; los dos primeros bytes identifican la red y los dos últimos al anfitrión.
- Del 192 al 223 es una dirección clase C; los primeros tres bytes son la dirección de red y el último es el número de anfitrión.

- Mayor que 223, indica que la dirección está reservada. Podemos ignorar las direcciones reservadas.

Clase	**Bits en el primer byte**	**Rango de direcciones de red**	**Parte de red**	**Parte de anfitrión**
A B C D y E	0xxxxxxx 10xxxxxx 110xxxxx 111xxxxx	1.1.1.0. – 127.0.0.0 128.0.0.0 – 191.255.0.0 192.0.0.0 – 223.255.255.0 224.0.0.0 – 255.255.255.0	1 byte 2 byte 3 bytes Especial/ reservada Multicast	3 bytes 2 bytes 1 byte ___

El número de redes por clase es: (no es relevante para las redes Clase D y E):

- Clase A: 128
- Clase B: 64 * 256 = 16 128
- Clase C: 32 * 256^2 = 2 097 152

El número de anfitriones por red es: (no es relevante para las redes Clase D y E):

- Clase A: 256^3 = 16 777 216
- Clase B: 256^2 = 65 536
- Clase C: 256

No todas las direcciones de red o anfitrión están disponibles para usarlas. Ya hemos dicho que las direcciones cuyo primer byte sea mayor que 223 están reservadas. También hay dos direcciones clase A, la 0 y la 127, reservadas para usos especiales. La red 0 designa la ruta predeterminada y la red 127 es la *dirección de loopback*. La ruta predeterminada se usa para simplificar la información de enrutamiento que debe manejar IP. La dirección de loopback simplifica las aplicaciones de la red al permitir que el anfitrión local sea direccionado del mismo modo que el anfitrión remoto, direcciones de loopback.- son la 127.0.0.0 y 127.0.0.1. que se utilizan por las aplicaciones y procesos de los nodos para pruebas, diagnósticos de la tarjeta, para configurar un anfitrión etc.

También hay direcciones de anfitrión reservadas para usos especiales. En todas las clases de red, los números de anfitrión 0 y 255 están reservados. Una dirección IP con todos los bits de anfitrión a cero identifica la propia red, estas direcciones se usan en las tablas de enrutamiento para referirse a redes completas. Por ejemplo, 26.0.0.0 se refiere a la red 26, y 128.66.0.0 se refiere a la red 128.66. Una dirección IP con todos los bits de anfitrión a uno es una dirección de *broadcast*. Una dirección de *broadcast* se usa para direccionar simultáneamente todos los anfitriones de una red. La dirección *broadcast* de la red 128.66 es 128.66.255.255. Un datagrama enviado a esta dirección se entrega a cada anfitrión de la red 128.66.

Con frecuencia las direcciones IP se conocen como direcciones de anfitrión, pero esto es un poco confuso. Una compuerta de acceso tiene una dirección diferente para cada red a la que está conectada. La compuerta de acceso es conocida por los otros dispositivos por medio de la dirección asociada con la red que comparte con esos dispositivos.

3.1. AGOTAMIENTO DE DIRECCIONES

La dirección de IP, que proporciona direccionamiento universal a través de todas las redes Internet, es una de las mayores ventajas del conjunto de protocolos TCP/IP. Sin embargo, los diseñadores de TCP/IP no previeron el enorme tamaño de las redes actuales. Cuando TCP/IP se estaba diseñando, las redes se limitaban a grandes organizaciones, entonces una dirección de 32 bits parecía tan larga que se dividía en clases para reducir la carga de procesamiento en los enrutadores, aunque dividir la dirección en clases reducía bastante el número de direcciones de anfitrión verdaderamente disponibles. Por ejemplo, asignar a una red grande una sola dirección clase B, en lugar de seis direcciones clase C, reduce la carga en el enrutamiento porque el enrutador sólo necesita mantener una ruta para toda esa organización. Sin embargo, la organización a la que se le dio la clase B tal vez no tenga 64000 ordenadores, por lo que la mayoría de las direcciones de anfitrión disponibles a esa organización nunca serán asignadas.

El diseño de direccionamiento actual, que favorece el crecimiento de los enrutadores, está en crisis a causa del rápido crecimiento de Internet. Este factor propicia el paso de la actual versión 4 de IP a la versión 6 (IPv6).

3.2. DIRECCIONES *IP* PRIVADAS

En general, cada instalación debe obtener y utilizar las direcciones IP que específicamente le hayan asignado, ya sea el proveedor del servicio o el Centro de Información de Red (NIC o *Network Información Center)* de su país. Esta asignación coordinada de direcciones evita las direcciones IP duplicadas y facilita el direccionamiento.

El acceso a Internet por parte de cualquier organización plantea dos problemas fundamentales:

- Escasez de direcciones: Se ha establecido una férrea disciplina por parte de los Centros de Información de Red que limitan el número y clase de direcciones que se asignan a las organizaciones que desean conectarse

- Problemas de seguridad: Toda máquina conectada directamente a Internet pasa a estar en un dominio público y a expensas de posibles accesos no controlados. Un simple fallo en un nodo conectado a la red puede poner en serio peligro la seguridad de toda la organización.

Sin embargo, hay organizaciones que por los motivos que sean utilizan direcciones IP inventadas por ellos. El problema surge cuando estas organizaciones quieren comunicarse con quien oficialmente tiene esas direcciones, por medio de una conexión directa o a través de Internet, no podrán hacerlo debido a sus direcciones duplicadas.

La RFC 1597, elaborada en marzo de 1994, reconoce esta práctica, que se lleva a cabo desde hace mucho tiempo, y para ello la Autoridad de Asignación de Números (IANA) reservó tres bloques de direcciones IP para uso privado de cualquier organización (en la clase A una red, la 10; en la clase B 16 redes, las comprendidas entre 172.16 y la 172.31; y en la clase C 255 redes, las comprendidas entre 192.168.0 y 192.168.255). Estas direcciones nunca serán oficialmente asignadas a nadie y nunca deben utilizarse fuera de la propia red de una organización. Este esquema de direccionamiento sólo es válido a nivel interno, pero garantiza la conectividad

entre todos los ordenadores de ambos grupos entre sí mediante el empleo de las pasarelas adecuadas.

Como se indica en la RFC 1627 (que es una actualización de la RFC 1597), si un sitio que utiliza direcciones privadas quiere enlazar a través de Internet con otro sitio que también utiliza direcciones privadas, todas sus conexiones tendrán que realizarse vía un *proxy*, pues las direcciones privadas nunca deben pasar a Internet.

3.3. SUBREDES

Con el esquema de direcciones estándar, un único administrador se debe encargar de manejar las direcciones de anfitrión para toda la red, la **creación de subredes** permite el manejo no centralizado de las direcciones de anfitrión, el administrador puede delegar la asignación de direcciones a organizaciones más pequeñas dentro de su organización. Si no se quiere tratar con un departamento determinado, se les puede asignar su propia subred y dejar que ellos mismos la manejen.

Para superar **problemas de topología o de organización**, la estructura estándar de una dirección IP se puede modificar localmente usando bits de dirección de anfitrión como bits adicionales de dirección de red. Las subredes son redes físicas independientes que comparten la misma dirección IP, la que identifica a la red principal.

Una subred se define aplicando una **máscara de bits**, la máscara de subred, a la dirección IP. Si un bit está encendido en la máscara, el bit equivalente en la dirección se interpreta como un bit de red. Si un bit de la red está desactivado, pertenece a la parte de la dirección de anfitrión. La subred sólo se conoce localmente, para el resto de Internet, la dirección se sigue interpretando como una dirección IP estándar.

Por **ejemplo**, la máscara de subred que estaría asociada con las direcciones clase B es 255.255.0.0. La máscara de subred más usada extiende la porción de red de una dirección clase B en un byte adicional, esta máscara de subred es 255.255.255.0; donde están activados todos los bits de los tres primeros bytes, y desactivados todos los bits del último byte. Los primeros dos bytes definen la red clase B; el tercer byte define la dirección de subred; el cuarto byte define el anfitrión en esa subred.

Muchos administradores de redes prefieren usar **máscaras orientadas a bytes** porque son fáciles de leer y entender. Sin embargo, no es imprescindible definir las máscaras ajustadas a bytes. La máscara de subred está orientada a bits y puede aplicarse a cualquier clase de dirección.

Para escribir las máscaras, en lugar de indicarlas como cuatro octetos, se está empezando a utilizar, cada vez mas, la forma "**/bits**". Por ejemplo, "/24" especifica una máscara de red de 24 bits, los primeros 24 bits a unos, equivalente a 255.255.255.0 pero mucho más rápida de escribir. La nueva nomenclatura presupone que las máscaras de red se conforman con bits continuos (por ejemplo, se presupone que nunca se usará el siguiente tipo de máscara 255.0.255.0).

A veces y en particular con los **enrutadores Cisco** y **en especificaciones de filtrado de paquetes**, también se usa el término de **máscaras comodines**. Las máscaras comodines son,

esencialmente, lo opuesto a las máscaras subred; mientras las máscaras de subred usan un bit para especificar los bits significativos (los bits que hay que observar), las máscaras comodines especifican los bits no significativos (los bits que hay que ignorar). Por lo tanto la máscara de subred 255.255.0.0 es equivalente a una máscara comodín de 0.0.255.255, y una máscara de subred 255.255.240.0 es equivalente a una máscara comodín de 0.0.15.25

3.4. IPv6

La nueva versión del Protocolo IP (IPv6) surge principalmente por la necesidad de aumentar el número de direcciones disponibles, aunque se añaden otras características más adaptadas al escenario actual en Internet, como por ejemplo catalogación de tráfico, tráfico en tiempo real o mecanismos de seguridad.

En lo respecto al direccionamiento, permite la asignación de cuatro millones de direcciones IP por cada persona del Planeta, frente a IPv4 que en total permite 4.000 millones de direcciones (ni siquiera una por persona) y repartida desigualmente ya que el 74% de las direcciones IP han sido asignadas a organizaciones de origen norteamericano. Además de una mayor capacidad, IPv6 permite una red más estable, eficiente, segura, potente y privada, y el despliegue de una amplia variedad de tecnologías y servicios, especialmente entre las comunicaciones móviles. Como curiosidad, IPv6 ese número de versión (6) y no 5 porque esta versión ya fue asignada por la IANA (Internet Assigned Numbers Authority) para un protocolo experimental que integraba voz, video y audio llamado ST-II (Stream Protocolo version 2).

Este aumento en el número de direcciones en IPv6 con respecto a v4 se debe a que el tamaño reservado para definir direcciones pasa de 32bits a 128bits. Además se añaden direcciones especiales como la "anycast address" usado para enviar un paquete cualquiera a un grupo de nodos. Este aumento en el tamaño de direcciones permite tener 2^{128} direcciones (340sextillones de direcciones), lo que nos permitiría conseguir que cada dispositivo tuviera una única dirección, mejorando y haciendo más sencillos aspectos como la autoconfiguración o la escalabilidad del enrutamiento a múltiples direcciones.

Además, se simplifica enormemente la cabecera con respecto a la definida para IPv4. Muchos campos que aparecían obligatorios directamente se han eliminado o se han hecho opcionales, reduciendo el coste de procesamiento de los paquetes en los nodos y optimizando el uso de ancho de banda. No obstante también se mejora la flexibilidad a la hora de permitir añadir nuevas opciones en el futuro. Además, de forma nativa se definen mecanismos de calidad de servicio y etiquetado de tráfico, permitiendo añadir información a los paquetes para que sean tratados de distinta forma (por ejemplo, tráfico en tiempo real prioritario con respecto a otro tipo de tráfico no crítico).

La seguridad y la privacidad también se ha tenido en cuenta al diseñar IPv6, añadiendo extensiones para autenticación, comprobación de integridad de datos o confidencialidad.

La cabecera en IPv6 queda estructurada de la siguiente manera:

- La cabecera **versión** se mantiene pero actualizada con el nuevo valor: 6
- **Clase de tráfico** de 8bits, permite dar priodidad a ciertos paquetes a lo largo de una ruta.
- La **cabecera etiqueta de flujo**, (de 20bits) puede ser usada por el origen para etiquetar secuencias de paquetes para los que se solicita un manejo especial por parte de los nodos intermedios (calidad de servicio o tiempo real).
- La **longitud de carga útil** es un entero sin signo, de 16bits, que indica el número de octetos que tiene el paquete a partir de la cabecera. Las cabeceras de extensión se consideran parte de esta carga útil, y por tanto está incluida en el conteo de esta longitud.
- **Cabecera siguiente**, de 8bits, indentifica el tipo de cabecera que sigue inmediatamente después a la cabecera IPv6. Se usan los mismos valores que los que se especifican en IPv4 (definidos estos en el RFC-1700)
- **Límite de saltos** (TTL en IPv4), entero sin signo de 8bits que se decrementa en 1 por cada nodo que reenvía el paquete. Si este valor llega a cero se descarta el paquete.
- **Dirección origen**, de 128bits, con el formato que se explica más abajo en esta sección.
- **Dirección destino**, de 128bits que indica el destino del paquete. Este destino no tiene porqué ser el destinatario final de la comunicación. Si se ha añadido la cabecera enrutamiento, este destino puede ser un nodo intermedio.

A partir de la dirección destino se pueden añadir extensiones a la cabecera. El colocar aquí las cabeceras de extensión permite que si un nodo intermedio no tiene que procesarlas, pueda optimizar el rendimiento, ignorándolas directamente y procesando sólo las cabeceras obligatorias de IPv6.

Cada una de estas cabeceras de extensión tiene además un identificador que permite conocer cuál es la siguiente cabecera. En caso de ser la última cabecera, este identificador apuntaría ya a la cabecera de TCP.

Cabecera IPv6 (Cabecera Siguiente: TCP)	Cabecera TCP	Datos

Cabecera IPv6 (Cabecera Siguiente: enrutamiento)	Cabecera Enrutamiento (Cabecera Siguiente: TCP)	Cabecera TCP	Datos

Cabecera IPv6 (Cabecera Siguiente: enrutamiento)	Cabecera Enrutamiento (Cabecera Siguiente: Fragmento)	Cabecera Fragmento (Cabecera Siguiente: TCP)	Cabecera TCP	Datos

Actualmente están definidas las siguientes cabeceras de extensión:

- **Opciones de salto a salto**: contiene información que debe ser examinada por todos los nodos a lo largo de la ruta.
- **Opciones de destino**: contiene información que debe ser examinada únicamente bien por el destino final de la comunicación o bien por el nodo que aparece en el campo Dirección Destino de la cabecera obligatoria.
- **Enrutamiento**. Permite indicar una ruta por la que el paquete debe pasar obligatoriamente. Contiene una lista de direcciones de los nodos de la ruta que se van extrayendo sucesivamente a medida que se va pasando por cada nodo de la ruta, modificándose el campo Dirección Destino con la dirección que se va extrayendo de esta cabecera.
- **Fragmento**: Esta cabecera se usa cuando es necesario fragmentar la información a enviar porque no caben en el tamaño máximo de paquete definido en origen. En IPv6 se requiere que cada enlace tenga una MTU de 1280 octetos o más. Si en algún enlace no se puede llevar un paquete de 1280 octetos de una pieza tiene que fragmentarse y el nodo origen tendrá que añadir esta cabecera, que contiene información para poder reconstruir el paquete en el destino. Se recomienda además que todos los nodos implementen el mecanismo de descubrimiento de la MTU de la ruta, definido en la RFC-1981, para poder elegir aquellas que cumplen con una MTU de 1280 y no tener así que fragmentar el paquete.
- **Autenticación**. Definida en detalle en la RFC-2402 y basado en IPSEC, permite añadir información de quién envió la información, permitiendo conocer quién envió el paquete. Estos datos del origen pueden ocupar hasta 32bits y va cifrado con una clave de al menos 128bits. Puede también proporcionar no repudio, dependiendo del algoritmo criptográfico y el mecanismo de gestión de claves. La cabecera de autenticación incluye una sección para indicar la asociación de seguridad que está utilizando en una comunicación, es decir, el conjunto de algoritmos y parámetros que se está usando para cifrar y autenticar un flujo particular en una dirección. También se incluyen los datos de autenticación que incluye la información de autenticación cifrada. La longitud de este campo es variable y depende del tipo de algoritmo usado para cifrar, que al menos de forma obligatoria debería ser MD5 o SHA-1.
- **Seguridad del encapsulado de la carta útil** (definido en la RFC-2406). Permite indicar que los datos no se lean por intermediarios a lo largo del transporte de origen a destino, es decir, se consigue confidencialidad, tanto de contenido como limitada del flujo de tráfico. Este mecanismo puede usarse para cifrar datos de un protocolo de nivel superior (TCP, UDP o ICMP) o incluso un paquete IP completo. Puede funcionar en dos modos:

- **Modo túnel**, en el que se puede encapsular un paquete IP completo dentro de la cabecera. Este cifrado se extiende a parte de la cabecera, de modo que se imposibilita en análisis de tráfico. Este paquete se encapsula en una nueva cabecera IP con información de encaminamiento y poder llegar al destino, pero no se podrá analizar el contenido porque este va cifrado.
- **Modo transporte**, en el que se encapsulan cifradas las unidades de datos de un protocolo superior como TCP o UDP dentro de la cabecera y luego se añade una nueva cabecera IP en claro. El origen cifrará parte de la cabecera de encapsulado, dejando en claro el campo de parámetros de seguridad. También se cifra el elemento de la capa de transporte del mensaje. En el destino se examina la cabecera IP, se detecta que hay cabecera de encapsulado de seguridad, se extraen los parámetros de seguridad (que iban en claro) y se utilizan para descifrar el resto del paquete.

Se recomienda además que las cabeceras aparezcan en ese orden. Todas pueden aparecer sólo una vez, excepto la cabecera de destino, que puede aparecer como mucho dos veces. Una antes de la cabecera de enrutamiento para el caso de tener que ser procesada por el nodo que aparece en el campo Dirección Destino, y otra antes de la capa superior en el caso de tener que procesarse por el destinatario final de la comunicación.

3.4.1. Direccionamiento en IPv6

Las direcciones en IPv6 son de 128bits y por tanto el número de direcciones posibles se ha elevado enormemente con respecto a las que había disponible en IPv4. Al tener un número tan elevado de direcciones y un aumento tan significativo en el número de bits disponibles para construirlas, fue necesario también rediseñar por completo en formato de las direcciones.

En IPv6 se utiliza notación hexadecimal, agrupando dígitos de cuatro en cuatro y separándolo por dos puntos. Por ejemplo:

2001:0db8:85a3:0003:1319:8a2e:0370:7334

Estas direcciones se pueden abreviar. Por ejemplo, se pueden omitir los ceros al comienzo de un grupo:

2001:db8:85a3:3:1319:8a2e:370:7334

También los grupos de ceros consecutivos se pueden sustituir por ::

2001:0db8:85a3:0000:1319:0000:0370:7334 pasa a a ser 2001:0db8:85a3::1319::0370:7334

Al igual que en IPv4, cuando se quiera identificar un rango de direcciones diferenciable por medio de los primeros bits, se añade este número de bits tras el carácter /.

Hay tres tipos de direcciones IPv6:

- **Unicast**: Representan a un solo nodo. Se pueden agrupar acompañando un prefijo que especifica una cantidad determinada de bits significativo. Hay tres tipos de direcciones unicast:
  - **Direcciones globales**. Tienen una estructura de tres niveles:

- Un prefijo de enrutamiento global (red) de 48bits
- Un identificador de enrutamiento local (subted) de 16bits
- Un identificador de interfaz de 64bits de longitud.

Actualmente la IANA está asignando direcciones de este grupo en el rango 2000::/3.

- **Direcciones unique local**: Son direcciones que tienen el alcance de un sitio específico sin garantía de que sean únicas. Constan de un prefijo FC00::/7 de 8bits, un identificador global de 40bits que no tiene porqué ser único, un identificador de subred de 16bits y un identificador de interfaz de 64bits. Estas direcciones no pueden reenviarse a internet porque puede que no sean únicas.
- **Direcciones Link local:** Son direcciones de ámbito local y no son reenviadas. Son generadas automáticamente con el prefijo FE80::/10 con un identificador para cada interfaz de 64bits. Son en cierto modo, equivalente al rango de direcciones 192.168.1.0 que se suelen utilizar en IPv4 para redes olcales.
- **Anycast**: Define un grupo de nodos. Un paquete enviado a una dirección de este tipo debe entregarse exactamente a un nodo (el más cercano o más fácilmente accesible del grupo). Las direcciones anycast se toman del rango de direcciones de unicast y requieren que la interfaz esté configurada de tal forma que se pueda identificar a esa dirección como dirección anycast.
- **Multicast**: Representa un grupo. Un paquete multicast se debe entrar a todos los miembros del grupo. Son direcciones definidas por el prefijo FF00::/8, donde el segundo octeto define el alcance de esta dirección. El identificador del grupo de multicast está definido por los restantes 112 bits. El rango FF00:: a FF0F:: está reservado y asisnado a través de la RFC-2375

Además hay direcciones que están reservadas:

- **Dirección no especificada**: Es la dirección con todo ceros ("::"). Es equivalente al 0.0.0.0 de IPv4.
- **Dirección de loopback**: Es la dirección "::1". Es equivalente al 127.0.0.1.

3.4.2. DIRECCIONES *IP* PRIVADAS EN LA ADMINISTRACIÓN PÚBLICA ESPAÑOLA

El Grupo de Usuarios de Telecomunicaciones en la Administración, propuso un plan de direccionamiento de red para protocolos TCP/IP que definiera un espacio de direccionamiento privado común para todos los Centros de la Administración.

La propuesta de direccionamiento se basa en el establecimiento de un directorio de direcciones de red IP, a partir del cual cada entidad u organismo pueda establecer de manera independiente sus planes de numeración IP, en función de su infraestructura de red, o distribución orgánica o departamental, pero manteniendo una coordinación que evite el uso de direcciones duplicadas dentro de la Administración. Las consideraciones básicas que se han tomado como punto de partida son:

1. El plan de direccionamiento diseñado debía tener en cuenta la previsión de que a medio-largo plazo todas las dependencias de la Administración pudieran contar con redes locales. Cada red local de un centro funcionará como una subred dentro de la red global de la Administración.

2. Fijar un sistema de direccionamiento según Clase A, adoptando el rango de direcciones 10.0.0.0 - 10.255.255.255 para uso privado de la Administración tal como se recomienda en el documento RFC 1597.

3. Con objeto de simplificar la configuración de las redes y los procedimientos de encaminamiento se puede optar por utilizar máscaras de red de 24 bits, con lo cual es posible definir hasta 64516 subredes independientes con capacidad equivalente a redes tipo C que pueden conectar hasta 254 nodos por segmento. Con este criterio la máscara de red que emplee cualquier equipo sería 255.255.255.0 independientemente de su ubicación física.

4. La distribución inicial del espacio de direccionamiento se hace de forma centralizada por la Secretaría del GTA en función de las necesidades de cada Centro Directivo teniendo en cuenta criterios de organización, flexibilidad y racionalización. Una vez asignado un rango de direcciones será responsabilidad del Centro determinar como hacer uso de ellas y establecer un plan de direccionamiento propio que tenga en cuenta las características de su infraestructura informática y de comunicaciones.

5. El último grupo de bits destinados a la identificación del *Host* (típicamente 8 en clase C) se utilizarán de forma ascendente para permitir posibles "*subnetings*" futuros en zonas no asignadas todavía.

   Para facilitar la gestión de los equipos se recomienda reservar unos valores de direcciones bajos para los servidores y los equipos de comunicaciones.

   La numeración de los equipos de usuarios, típicamente ordenadores personales o estaciones de trabajo, comenzará por encima de dicho valor.

   Este mecanismo permite ocupar en la asignación las primeras direcciones dentro del rango y dejar libres los últimos grupos de direcciones para su posible segmentación y uso en otras redes que lo precisen.

3.5. NOMBRES SIMBÓLICOS

Para facilitar el manejo humano de las direcciones IP, a cada dirección se le puede asociar un nombre. Los dispositivos conectados a una red pueden ser identificados tanto por su dirección como por un nombre simbólico asociado a dicha dirección de red.

Este mecanismo se basa en la existencia de unas tablas de equivalencia que pueden ser mantenidas a nivel local de cada equipo (fichero *hosts*) o a nivel de red mediante servidores de nombres que de forma distribuida cooperan configurando un sistema de nombres de dominio, conocido por sus siglas DNS.

Un DNS puede ser privado, si gestiona un espacio de nombres y direcciones en el ámbito interno de una organización o público, como el sistema de nombres que existe en Internet, que gestiona el espacio de nombres y direcciones oficiales de todos los nodos integrados en la red. Al ser un sistema distribuido, cada organización conectada a Internet cuenta con su propio

servidor de nombres y se responsabiliza de administrar la porción del espacio de nombres que tenga asignada, no existiendo un órgano de supervisión central.

Las principales características del sistema DNS son:

- Es un sistema jerárquico por el que se delega la autoridad sobre cada porción del espacio de nombres. DNS define un espacio de nombres estructurado en forma de árbol con un único nodo raíz. Cada nodo de primer nivel corresponde a una Autoridad, quien se encarga de crear y gestionar los nodos de segundo nivel, con la restricción de que cada nombre de nodo sea único en su nivel. Así, por ejemplo, hay establecidas autoridades a nivel de cada país y deben establecerse a nivel interno de cada organización.

  La autoridad delegada para el primer nivel del árbol puede a su vez delegar en diversas autoridades para la gestión de los dominios de niveles inferiores, denominados subdominios. Así, un dominio está constituido por un nodo y todos sus nodos descendientes. Un nombre de dominio define de forma unívoca a un nodo dentro de un dominio.

  El sistema establece la posibilidad de delegación jerárquica en los sucesivos nodos descendientes, aunque se recomienda no extender el número de niveles más de lo estrictamente necesario, para no crear nombres de nodo excesivamente complejos.

  El nombre completo del nodo se forma con los nombres de los nodos de los que aquel depende, separándolos mediante puntos. Así, ulises.map.es corresponde al nodo "ulises", dentro del dominio "map", del Ministerio de Administraciones Públicas, a su vez perteneciente al dominio de primer nivel "es" (España).

- Permite una Distribución dinámica de las búsquedas nombre-dirección IP, de modo que no es preciso mantener manualmente copias de las relaciones de dichas equivalencias.

- Los algoritmos de búsqueda de nombres y/o direcciones permiten una Redundancia, de modo que un nombre puede localizarse en más de un servidor DNS. Con ello se consigue repartir la carga de este trabajo entre varios nodos. Al mismo tiempo se logra cierta tolerancia a fallos al no depender exclusivamente de un único servidor.

- El sistema garantiza la capacidad de crecimiento, ya que DNS permite definir otros recursos, además de la traslación entre nombres y direcciones IP.

3.5.1.1 *CONVERSIÓN DE DIRECCIONES IP A DIRECCIONES FÍSICAS*

Los protocolos TCP/IP están enfocados a la transmisión de paquetes de información, buscando la independencia de la arquitectura de la red. Arquitecturas como la de *Ethernet* logran la comunicación sólo mediante el conocimiento de la dirección física de los equipos. Así en cada ordenador que opere con el protocolo IP debe contar con algún procedimiento para la translación de la dirección IP a la dirección física del ordenador con el que establezca comunicación.

Existen tres métodos básicos para convertir las direcciones IP a direcciones físicas:

- Estática por tablas. Alto costo en mantenimiento

- Por aplicación de algoritmos. Dificultad de elegir el algoritmo más eficiente, puede no lograrse una distribución homogénea de direcciones y existe la posibilidad remota de duplicación de direcciones.

- Dinámica. Se consulta, mediante un solo mensaje, que se emite a todos los equipos de la red, por el poseedor de cierta dirección IP.

La conversión dinámica es la más adecuada, debido a que se obtiene la dirección física por respuesta directa del nodo que posee la dirección IP destino. Una vez obtenida la dirección física se guarda en una tabla temporal para subsecuentes transmisiones, de no ser así podría haber una sobrecarga de tráfico en la red debido a la conversión de direcciones cada vez que se transmitiera un paquete.

El Protocolo de Resolución de Direcciones ARP (*Address Resolution Protocol*) permite a un equipo obtener la dirección física de un equipo destino, ubicado en la misma red física, proporcionando solamente la dirección IP destino.

ARP es un protocolo de bajo nivel que permite asignar direcciones IP a los equipos en una red física. Se utiliza en redes con mecanismo de difusión (*broadcast*), por ejemplo *Ethernet*, cuando la interface de red recibe un datagrama IP para enviarlo a un equipo destino, coteja la tabla temporal de conversión:

- Si existe la referencia adecuada ésta se incorpora al paquete y se envía.

- Si no existe la referencia, se genera y envía un paquete ARP, de emisión general, con la dirección IP destino. Todos los equipos en la red física reciben el mensaje general y comparan la dirección IP que contiene con la suya propia, enviando un paquete de respuesta que contiene su dirección IP. El ordenador origen actualiza su tabla temporal y envía el paquete IP original, y los subsecuentes, directamente al ordenador destino.

Las ventajas de ARP son que:

- No requiere tablas estáticas
- Permite añadir sistemas sin modificar nada
- Independiza las direcciones IP de las direcciones físicas

3.6. ARQUITECTURA DE ENRUTAMIENTO DE INTERNET

Como ya se ha dicho, la estructura inicial de Internet se construyó a partir de ARPANET, en esta red había una jerarquía de compuertas de acceso que constituían un medio de envío centralizado para tráfico de larga distancia. Este sistema central se llamaba núcleo, y las compuertas manejadas de manera centralizada que lo interconectaban se llamaban compuertas de acceso del núcleo.

Cuando se usa una estructura jerárquica, la información de enrutamiento sobre todas las redes de Internet se pasa por las compuertas del núcleo, las cuales procesan esta información y luego

la intercambian entre sí usando el Protocolo de Compuerta a Compuerta (GGP, *Gateway to Gateway Protocol)*. La información de enrutamiento procesada pasa luego de regreso a las compuertas externas.

Fuera del núcleo de Internet hay grupos de redes independientes llamadas Sistemas Autónomos *(AS)*. Un sistema autónomo no es realmente una red independiente, es un conjunto de redes y compuertas de acceso con su propio mecanismo interno para recolectar información de enrutamiento y pasarla a otros sistemas de red independientes. La información de enrutamiento pasada a los otros sistemas de red se llama información de alcance, esta información indica a que redes se puede tener acceso a través de ese sistema autónomo. El protocolo más usado para intercambiar información de enrutamiento entre sistemas autónomos, era el Protocolo de Compuerta de Acceso Exterior (EGP, *Exterior Gateway Protocol*).

La parte Internet conocida como *Defense Data Network* (DDN) sigue usando el modelo del núcleo para distribuir la información de enrutamiento. Pero su modelo jerárquico obliga al núcleo a procesar cada una de las rutas, lo que genera una gran carga de proceso para el núcleo y, conforme Internet crece, la carga aumenta. En el lenguaje de red, se dice que este modelo de enrutamiento no se escala bien y por esta razón ha surgido un nuevo modelo.

Actualmente el estándar para el intercambio de información entre sistemas autónomos en Internet es el BGP 4, que permite definir políticas de encaminamiento entre sistemas autónomos y soporta CIDR (*Classless InterDomain Routing*), es decir, encaminamiento basado únicamente en prefijos de *routing* (dirección de red+mascara indicativa de hasta donde llega la parte de red de la dirección), sin tener en cuenta la tradicional distinción en clases A, B y C ya superada.

El uso de CIDR y BGP4 es lo que ha permitido a Internet seguir funcionando, a pesar de su espectacular crecimiento, al ser posible agregar los bloques de redes contiguas asignados a cada proveedor de acceso, resumiendo esta información en la frontera de cada sistema autónomo de cara al exterior. Con lo cuál las tablas de encaminamiento en Internet se reducen considerablemente.

El nuevo modelo de enrutamiento se basa en conjuntos similares de sistemas autónomos, llamados dominios de enrutamiento. Estos dominios intercambian información de enrutamiento con otros dominios usando el Protocolo de Compuerta de Frontera (BGP). Cada dominio procesa la información que recibe de otros dominios. A diferencia del modelo jerárquico, este modelo no depende de un solo sistema de núcleo para elegir las “mejores” rutas. Cada dominio de enrutamiento hace su procesamiento por sí mismo; por lo tanto, este modelo es más escalable. Los dominios comparten información, pero no dependen de ningún sistema para proporcionar la información de enrutamiento.

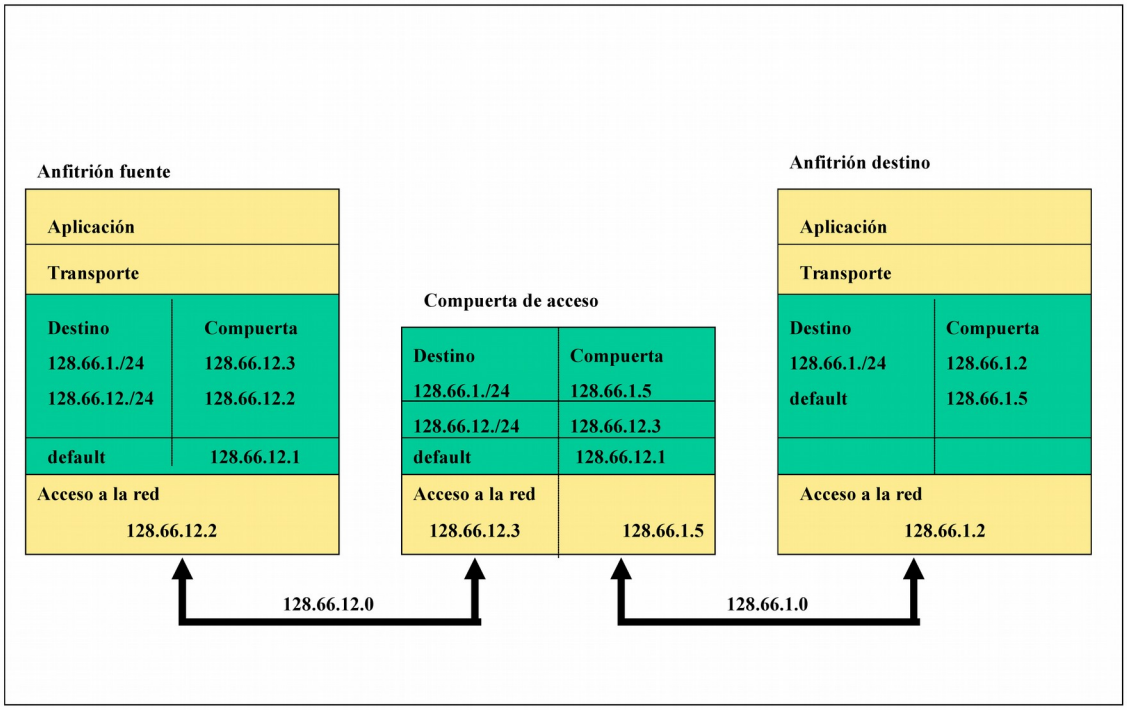
Independientemente de cómo se derive, al final la información de enrutamiento termina en su compuerta de acceso local, donde IP la usa para tomar las decisiones de enrutamiento.

3.7. LA TABLA DE ENRUTAMIENTO

Aunque específicamente, las compuertas de acceso son las que enrutan la información entre redes, también los anfitriones como compuertas de acceso, deben tomar decisiones de enrutamiento simples, tales como:

- Si el anfitrión destino está en la red local, la información se envía al anfitrión destino
- Si el anfitrión destino está en una red remota, la información se envía a la compuerta de acceso local

Como el enrutamiento está orientado a redes, IP toma las decisiones de enrutamiento basándose en la parte de dirección de red, para ello previamente determina la clase de dirección de que se trata, analizando los bits de mayor orden de la dirección IP de destino. La clase de dirección determina que parte de la dirección usa IP para identificar la red.



Después de determinar la red destino, el módulo IP enruta los paquetes hacia su destino de acuerdo con lo que le indica la tabla de enrutamiento local. Si la red destino es la red local, la máscara de subred local se aplica a la dirección destino.

La figura anterior muestra cómo funciona el enrutamiento en una red imaginaria. El nivel IP de cada anfitrión y compuerta se reemplaza por una parte de una tabla de enrutamiento, que muestra las redes destino y las compuertas de acceso usadas el anfitrión fuente (128.66.12.2) envía información al anfitrión destino (128.66.1.2), primero se determina que 128.66.1.2 es una dirección clase B de la red local y aplica la máscara de subred (se crean subredes de la red 128.66.0.0 usando la máscara 255.255.255.0). Después de aplicar la máscara de subred, IP sabe

que la dirección de red destino es 128.66.1.0. La tabla de enrutamiento muestra que la información dirigida a 128.66.1.0 debe enviarse a la compuerta de acceso128.66.12.3. Esta compuerta hace entrega directa a través de su interface 128.66.1.5.. Se puede observar que 128.66.12.1 es la compuerta de acceso tanto para 128.66.12.2 como para 128.66.12.3. Pero como 128.66.1.2 no puede llegar directamente a la red 128.66.12.0, tiene una ruta predeterminada diferente.

Una tabla de enrutamiento no contiene rutas extremo a extremo. Una ruta solo apunta a la siguiente compuerta de acceso, llamada *el siguiente salto*, a lo largo de la trayectoria hacia la red destino. El anfitrión depende de la compuerta local para enviar la información y la compuerta depende de otras compuertas. Un datagrama pasa de una compuerta a otra, hasta llegar a una que esté conectada directamente a su red destino. Es esta última compuerta la que envía finalmente los datos al anfitrión destino.

CAPÍTULO 4 NIVEL DE TRANSPORTE

Encima del nivel de Internet está el nivel de transporte de anfitrión a anfitrión, que abreviado se le denomina nivel de transporte.

Este nivel provee comunicación extremo a extremo desde un programa de aplicación a otro, de tal manera que los datos que envíe una aplicación sean recibidos por la aplicación remota, regula el flujo de información y puede proveer un transporte confiable asegurándose que los datos lleguen sin errores y en la secuencia correcta.

Los dos protocolos más importantes del nivel de transporte son:

- El Protocolo de Control de Transmisión (TCP), que proporciona un servicio de envío de datos confiable con detección y corrección de errores de extremo a extremo.

- El Protocolo de Datagrama de Usuario (UDP), que proporciona un servicio de envío de datagramas con menos información de control, sin conexión.

4.1. PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)

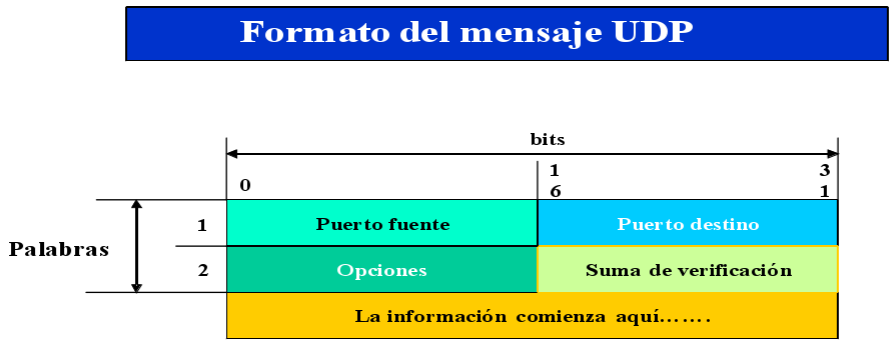
UDP da a los programas de aplicación acceso directo a un servicio de entrega de datagramas, como el que proporciona IP. Esto permite que las aplicaciones intercambien mensajes a través de la red con un mínimo de información de control.

UDP es un protocolo orientado a no conexión, no verifica que la información llegó correctamente al otro extremo de la red. Cada paquete (datagrama) UDP es independiente. Enviar paquetes UDP es como dejar tarjetas postales en el correo: si se envían cien postales aunque todas tengan la misma dirección, no se puede tener la certeza de que todas llegarán a

su destino, y las que lleguen quizá no llegarán en el mismo orden en que fueron enviadas. La figura a continuación muestra el formato de UDP

A diferencia de las tarjetas postales, los paquetes UDP se pueden hacer llegar más de una vez, son posibles múltiples copias porque el paquete puede ser duplicado por los niveles inferiores de red. Por ejemplo, en una *Ethernet*, el paquete se duplicaría si un enrutador pensara que se produjo una colisión. Si el enrutador está equivocado y el paquete original no sufrió una colisión, tanto el original como el duplicado llegarán finalmente a su destino.

Utilizar UDP como servicio de transporte de datos, es recomendable cuando la cantidad de información que se transmite es pequeña (por ejemplo un servicio de hora), o bien las aplicaciones multimedia que no se pueden permitir una desviación del retardo excesiva, como la que causa el tener un envío asegurado, que requiere de posibles retransmisiones. Que no haya paradas provocadas por la espera de una retransmisión es mejor que perder algunos paquetes. Las aplicaciones multimedia, se encargan de llevar su propio mecanismo de control de buffer para garantizar la calidad de la reproducción.



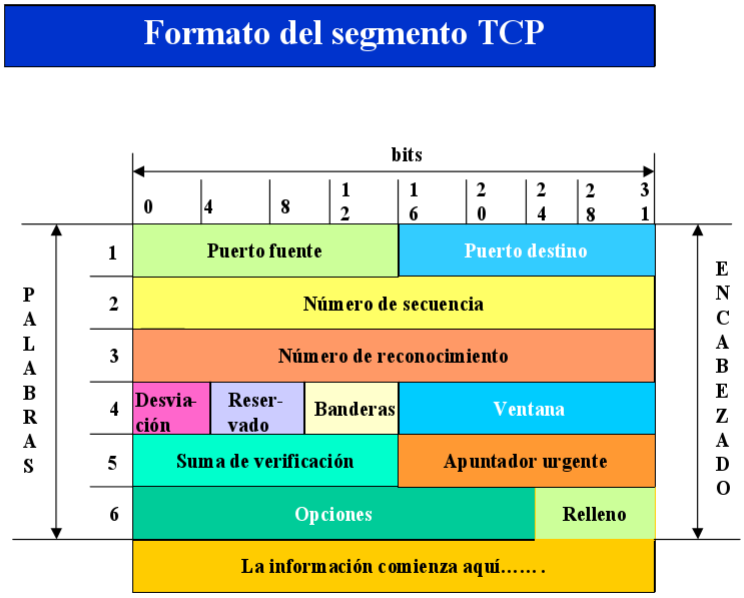
4.2. PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

Las aplicaciones que requieren que el protocolo de transporte proporcione un envío confiable de datos usan TCP porque verifica que los datos son enviados a través de la red y recibidos en destino en la secuencia adecuada. TCP es un protocolo confiable orientado a conexión.

TCP proporciona una conexión bidireccional confiable entre dos extremos. Abrir una conexión TCP es como hacer una llamada telefónica: marcado el número y tras un

breve periodo de espera, se establece una conexión lo suficientemente confiable con quien se quiere hablar.

TCP es confiable porque garantiza a la aplicación destino que recibe toda la información, en el orden en que fue enviada y que no recibe información duplicada. TCP corta una conexión antes de violar una de estas garantías. Por ejemplo, si la mitad de los paquetes TCP de una sesión se pierden en su tránsito al destino, TCP hace que se retransmitan antes de pasar la información al nivel de aplicación. Si alguna información no puede recobrarse, a pesar de intentos repetidos, el nivel TCP corta la conexión y lo reporta al nivel de aplicación, en lugar de pasarle la información incompleta.



La unidad de información intercambiada entre los módulos TCP cooperativos se llama segmento, cada segmento contiene una suma de verificación que usa el receptor para verificar que la información no sufrió daños. (ver la figura anterior).

El campo Banderas, consta de 6 bits: URG (urgente), ACK (reconocimiento), PSH ("*push*"), RST (restaurar), SYN (sincronismo), FIN (fin)

Las características básicas de TCP son:

- Confiabilidad, TCP da confiabilidad a través de un mecanismo llamado Reconocimiento Positivo con Retransmisión *(PAR, Positive Acknowledgement with Retransmition)*. Un sistema que use PAR reenvía la información a menos que el sistema remoto confirme que llegó bien. Si el segmento de información se recibe sin

daños, el receptor envía un reconocimiento positivo al emisor, si el segmento está dañado, el receptor lo descarta y no envía el conforme, después de un lapso apropiado de suspensión, el módulo emisor retransmite cualquier segmento del que no haya recibido reconocimiento positivo.

- Orientado a conexión, TCP establece una conexión lógica extremo a extremo entre los dos anfitriones que se comunican. Antes de que se transmitan los datos, TCP establece un diálogo, negociación *(hand-shake)*, en el que se intercambia información de control entre los dos extremos.

- Orientado a cadenas de bytes, TCP controla la secuencia de los segmentos estableciendo el bit apropiado en el campo *Banderas* de la palabra 4 del encabezado del segmento. La entidad emisora TCP permite al proceso de aplicación (emisor) transmitir un flujo continuo de octetos que la entidad TCP emisora va recogiendo, numerando y agrupando en segmentos (las unidades de datos de TCP), de tal manera que la unidad TCP receptora pase al proceso de aplicación (receptor) exactamente la misma secuencia de octetos y en el mismo orden.

El tipo de negociación usada por TCP se llama negociación en tres sentidos *(three way hand-shake)* porque se intercambian tres segmentos. La forma más sencilla de negociación en tres sentidos es la siguiente:

- El anfitrión A inicia la conexión enviando un segmento al anfitrión B con el bit "Sincronizar números de secuencia" (SYN) encendido. El segmento dice al anfitrión B qué número de secuencia usará como número inicial de sus segmentos (los números de secuencia se usan para mantener la información en el orden apropiado).

- El anfitrión B responde al A con un segmento que tiene encendidos los bits "Reconocimiento" ACK (*Acknowledgment Segment)* y SYN. El segmento de B reconoce la recepción del segmento de A, e informa a A con que número de secuencia comenzará el anfitrión B.

- Por último, el anfitrión A envía un segmento que reconoce la recepción del segmento B, y transfiere la primera información real.

El primer segmento en cada dirección tiene encendido el bit SYN, y todos los paquetes subsecuentes tienen encendido el bit ACK.

Después de este intercambio, el TCP del anfitrión A tiene una evidencia positiva de que el TCP remoto está "vivo" y listo para recibir datos. Cuando los módulos cooperativos han concluido las transferencias de información, intercambian una negociación en tres sentidos con segmentos que contienen el bit "No mas información del emisor" (bit FIN) para cerrar la conexión que debe ser confirmado por el corresponsal con FIN y ACK.

TCP visualiza la información que envía como una cadena (un flujo) de bytes continua, no como paquetes independientes. Por lo tanto TCP se ocupa de mantener la secuencia en que los bytes son enviados y recibidos. Los campos "Número de secuencia" y "Número de reconocimiento" del encabezado del segmento TCP llevan la cuenta de los bytes.

El estándar de TCP no requiere que cada sistema comience a numerar los bytes con un número específico; cada sistema elige el número que usará como punto de inicio. Para llevar correctamente la cuenta de la cadena de datos, cada extremo de la conexión debe conocer el número inicial del otro extremo. Los dos extremos de la conexión sincronizan los sistemas de numeración de bytes intercambiando segmentos SYN durante la negociación. El campo "Número de secuencia" del segmento SYN contiene el número inicial de secuencia (ISN, *Initial Sequence Number)*, que es el punto de inicio del sistema de numeración de bytes. El ISN se elige al azar.

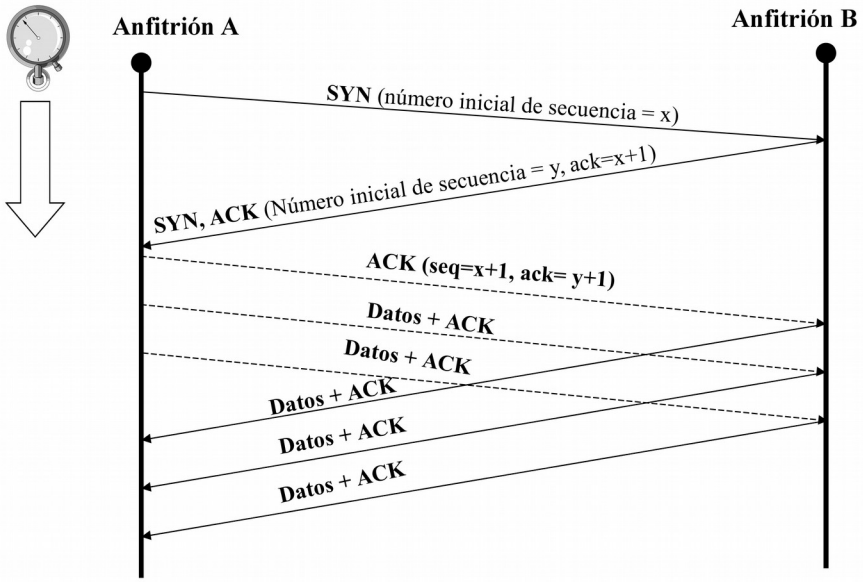
Cada byte de información se numera secuencialmente a partir del ISN, de modo que el primer byte real de información enviado tiene el número de secuencia ISN+1. El número de secuencia en el encabezado de un segmento de información identifica la posición secuencial en la cadena de datos del primer byte de información del segmento. Por ejemplo, si el primer byte de la cadena de datos fue el número de secuencia 1 (ISN=0) y ya se han transferido 4000 bytes de información, entonces el primer byte de información en el segmento actual es el byte 4001, y el número de secuencia seria el 4001.

El segmento de reconocimiento ACK, cumple dos funciones: reconocimiento positivo y control de flujo: El reconocimiento dice al emisor cuanta información fue recibida y cuanta más puede aceptar el receptor. El número de reconocimiento es el número de secuencia del último byte recibido en el extremo remoto. El estándar no requiere un reconocimiento individual para cada paquete. El número de reconocimiento es un reconocimiento positivo de todos los bytes hasta ese número. Por ejemplo, si el primer byte se numeró con el número 1 y se han recibido con éxito 2000 bytes, el número de reconocimiento sería 2000.

El campo ventana contiene el número de bytes que puede aceptar el extremo remoto. Si el receptor es capaz de aceptar 6000 bytes más, la ventana sería de 6000. La ventana indica al emisor que puede seguir enviando segmentos mientras que el número total de bytes que envíe sea menor que la ventana de bytes que puede aceptar el receptor. El receptor controla el flujo de bytes del emisor cambiando la medida de la ventana. Una ventana en cero dice al emisor que deje de transmitir hasta que reciba un valor de ventana distinto.

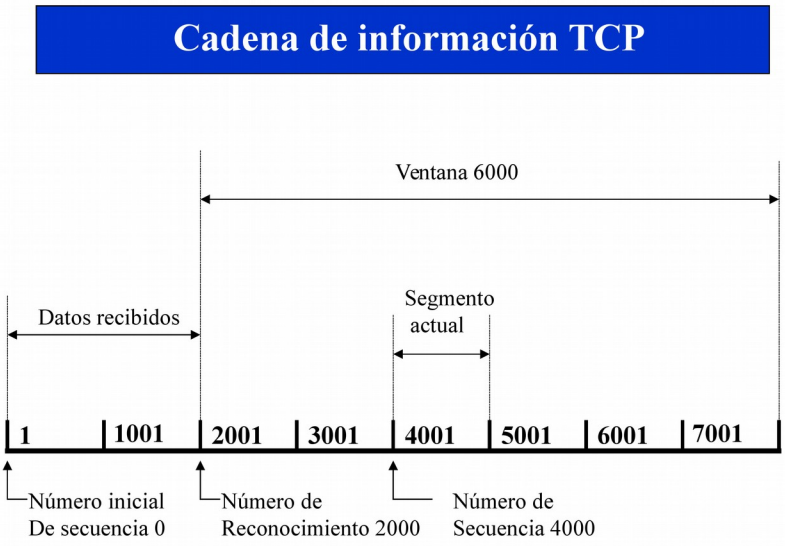
La figura a continuación muestra una cadena de datos TCP que comienza con un Número Inicial de Secuencia 0. El sistema ha recibido y reconocido 2000 bytes, por lo que el Número de reconocimiento actual es 2000. El receptor tiene también un límite de espacio suficiente para otros 6000 bytes, por lo que ha anunciado una ventana de 6000. El emisor actualmente está enviando un segmento de 1000 bytes iniciado con el número de secuencia 4001. El emisor no ha recibido reconocimiento para los bytes del 2001 en adelante, pero continúa enviando información siempre que quepa en la ventana. Si el emisor llena ésta y no recibe reconocimiento de la información enviada previamente, enviará la información de nuevo, después de un lapso de espera apropiado, comenzando desde el primer byte no reconocido. En el ejemplo de la figura, la retransmisión comenzaría desde el byte 2001 si no se recibieran reconocimientos posteriores. Este proceso asegura que la información se reciba de modo confiable en el extremo remoto de la red.

Negociación en tres sentidos



TCP se encarga también de enviar información recibida desde IP hacia la aplicación correcta. La aplicación a la que se dirige la información se identifica por un número de 16 bits llamado número de puerto. El Puerto fuente y el Puerto destino están contenidos en la primera palabra del segmento.

Cadena de información TCP



CAPÍTULO 5 NIVEL DE APLICACIÓN

En la parte superior de la arquitectura TCP/IP está el nivel de aplicación. Hay muchos protocolos de aplicación, (*Telnet*, FTP, HTTP, DNS, RIP, NFS,..) la mayoría de ellos proporcionan servicios de usuario, y continuamente se están agregando nuevos servicios a este nivel. Interactúan con uno o más protocolos de transporte para enviar o recibir datos, en forma de mensajes o bien en forma de flujos de bytes.

El uso de algunos protocolos, como *Telnet* y FTP, requiere que el usuario tenga algún conocimiento de la red. Otros protocolos, como RIP, se ejecutan sin que el usuario sepa siquiera que existen.

Los protocolos FTP, *Telnet* y SMTP se basan, principalmente, en TCP; mientras que NFS, DNS y RIP se basan, principalmente, en UDP. Algunos protocolos de tipo de aplicación, como el Protocolo de Compuerta de Acceso Exterior (EGP, *Exterior Gateway Protocol*), otro protocolo

de enrutamiento, no usan servicios del nivel de transporte; usan directamente los servicios del IP.

Para enviar información entre dos anfitriones es necesario moverla a través de la red al anfitrión correcto, y dentro de ese anfitrión al proceso correcto, para ello TCP/IP usa tres esquemas:

- Direccionamiento, las direcciones IP se utilizan para enviar la información al anfitrión correcto.
- Enrutamiento, las compuertas de acceso envían la información a la red correcta.
- Multiplexaje, los números de protocolo y de puerto sirven para enviar la información al módulo de software correcto dentro del anfitrión.

Para enviar la información entre dos aplicaciones cooperativas a través de Internet, son necesarias las funciones de: direccionamiento entre anfitriones, enrutamiento entre redes y multiplexaje entre niveles.

CAPÍTULO 6 PROTOCOLOS, PUERTOS Y SOCKETS

Una vez que la información se enruta a través de la red y se envía a un anfitrión específico, debe mandarse al usuario o proceso correcto. Conforme la información sube o baja por los niveles de TCP/IP, se necesita un mecanismo para enviarla a los protocolos correctos en cada nivel. El sistema debe poder combinar la información de varias aplicaciones un unos cuantos protocolos de transporte y de éstos hacia IP. El combinar varias fuentes de información en una sola cadena de información se llama multiplexaje. La información que llega desde la red debe ser demultiplexada, esto es, dividida para entregarla a varios procesos. Para hacer esto, IP utiliza números de protocolo para identificar los protocolos de transporte, y éstos, a su vez, usan números de puerto para identificar las aplicaciones.

Algunos números de protocolo y puerto están reservados para identificar servicios bien conocidos. Los números de protocolo y los números de puerto adjudicados a los servicios bien conocidos se documentan en la RFC Números asignados, que se actualiza cada vez que recibe un nuevo número de la RFC.

6.1. NÚMEROS DE PROTOCOLO

El número de protocolo se indica en un byte de la tercera palabra del encabezado del datagrama. El valor identifica el protocolo del nivel encima del de IP al cual debe pasarse la información.

En un sistema UNIX, los números de protocolo se definen en el archivo */etc/protocols*. Este archivo es una tabla donde cada registro o línea contiene el nombre oficial del protocolo, el número de protocolo asociado a ese nombre y el “alias” del nombre del protocolo, todos ellos

separados por un blanco. Los comentarios en la tabla comienzan con #. A continuación se muestra, como ejemplo, el contenido de un archivo */etc/protocol*.

```
% cat    /etc/protocols
#
# @ (#) protocols 1.8  88/02/07  SMI
#
# Protocolos de Internet (IP)  #
ip              0       IP      # protocolo de Internet, número de pseudo protocolo
icmp            1       ICMP    # protocolo Internet de Mensajes de Control
igmp            2       IGMP    # protocolo de grupo multicast de Internet
ggp             3       GGP     # protocolo de compuerta a compuerta
tcp             6       TCP     # protocolo de control de transmisión
pup             12      PUP     # protocolo de paquete universal PARC
udp             17      UDP     # protocolo de datagrama de usuario
```

Un sistema sólo necesita incluir los números de los protocolos que realmente emplea.

Cuando un datagrama llega y su dirección destino coincide con la dirección IP local, el nivel IP sabe que el datagrama debe ser enviado a uno de los protocolos de transporte superiores. Para decidir qué protocolo debe recibir el datagrama, IP consulta esta tabla y de acuerdo con el número lo envía al protocolo correspondiente. O sea, si el número de protocolo del datagrama es 6, IP lo envía a TCP. Si el número de protocolo es 17, IP lo envía a UDP. TCP y UDP son los dos servicios más importantes de nivel de transporte, aunque también el resto de los protocolos mostrados en la tabla usan directamente el servicio de envío de datagramas IP. ICMP y GGP ya se han comentado, IGMP es una extensión de IP para *multicast* explicado en la RFC 988, y PUP es un protocolo de paquete similar a UDP.

6.2. NÚMEROS DE PUERTO

Después de que IP pasa la información de entrada al protocolo de transporte (TCP o UDP), este último la pasa al proceso de aplicación correcto. Los procesos de aplicación (también llamados servicios de red) se identifican por números de puerto, los cuales son valores de 16 bits. El número de puerto fuente, identifica el proceso que envió la información, y el número de puerto destino, identifica el proceso que recibirá la información, ambos están contenidos en la primera palabra del encabezado de cada segmento de TCP y paquete de UDP.

Hay muchas más aplicaciones de red que protocolos de nivel de transporte. Los números de puerto debajo de 1024 están reservados para servicios bien conocidos (como FTP y *Telnet*) y se definen en la RFC Números asignados.

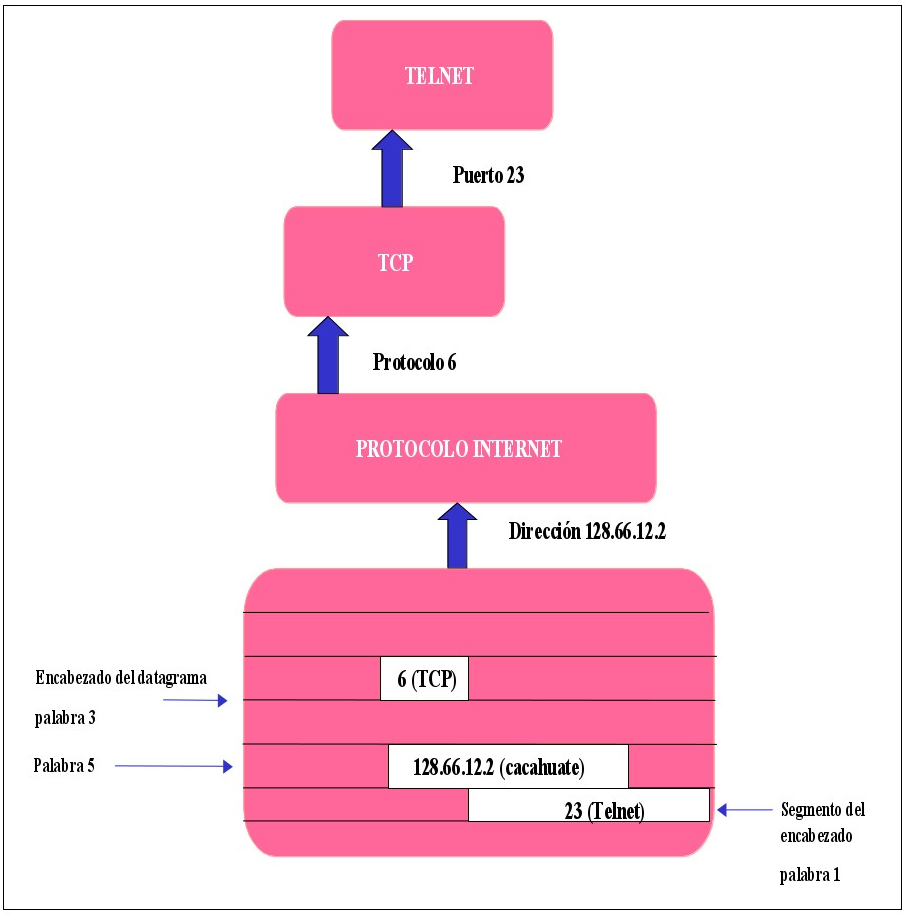
Los números de puerto no son únicos entre los protocolos de nivel de transporte; son únicos sólo dentro de un protocolo de transporte específico. En otras palabras, TCP y UDP pueden tener, y tienen, asignados los mismos números de puerto. Es la combinación de números de puerto y protocolo la que identifica de modo único el proceso específico al que debe ser enviada la información.

En los sistemas UNIX, los números de puerto se definen en el archivo */etc/services*. El formato del archivo */etc/services* es similar al del archivo */etc/protocols*. Cada registro de una sola línea

empieza con el nombre oficial del servicio, separado por un espacio en blanco de la pareja número de puerto/protocolo asociado a ese servicio. A continuación de la pareja número de puerto/protocolo se puede indicar un alias del nombre oficial del servicio.

```
Cacahuete %  cat  /etc/services
#
#  @ (#)9 services  1.12  88/02/07  SMI
#
#  Servicios de red,   estilo Internet
#
echo            7/udp
echo            7/tcp
ftp-dat         20/tcp
ftp             21/tcp
telnet          23/tcp
smtp            25/tcp
time            37/tcp
time            37/udp
domain 53/ucp
domain 53/tcp
#
#  Funciones específicas de anfitrión
#
finger          79/tcp
nntp            119/tcp         usenet          # Transferencia de noticias de red
ntp             123/tcp                         # Protocolo de tiempo de red
#
#  Servicios específicos de UNIX
#
exec            512/tcp
login           513/tcp
shell           514/tcp         cmd     # Sin usar contraseña de acceso
biff            512/udp                 comsat
who             513/udp                 whod
syslog          514/udp
talk            517/udp
route           520/udp                 router  routed
```

Esta tabla combinada con la tabla */etc/protocols*, proporciona toda la información necesaria para enviar la información a la aplicación correcta. Un datagrama llega a su destino basado en la dirección destino de la quinta palabra del encabezado del datagrama. IP usa el número de protocolo de la tercera palabra del encabezado del datagrama, para enviar la información de este último al protocolo del nivel de transporte apropiado. La primera palabra de la información enviada al protocolo de transporte contiene el número de puerto destino que le dice el protocolo que mande la información a una aplicación específica. La Figura a conitnuación muestra este proceso de envío.



6.3. SOCKETS

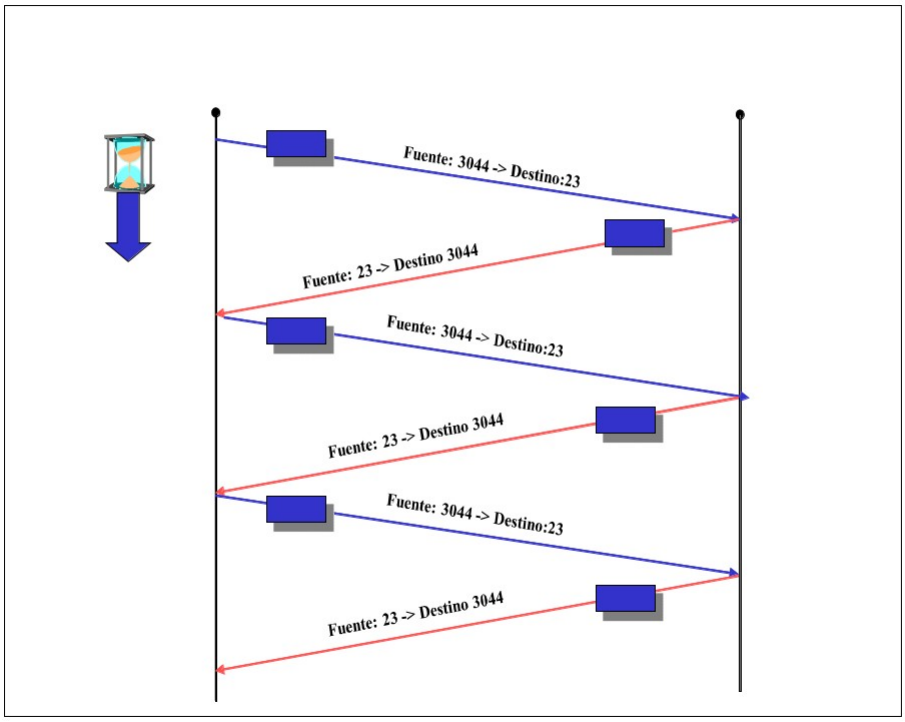
Los puertos bien conocidos son números de puerto estándar que permiten que los ordenadores remotos sepan a qué puerto conectarse para un servicio de red específico, lo cual simplifica el proceso de conexión porque tanto el emisor como el receptor saben por adelantado que la información destinada a un proceso específico usará un puerto específico. Por ejemplo, todos los sistemas que ofrece *Telnet* lo hacen en el puerto 23.

Hay un segundo tipo de número de puerto llamado puerto asignado dinámicamente, que se asignan a los procesos cuando se requiere. El sistema garantiza que no se asigne el mismo número de puerto a dos procesos y que los números asignados estén por encima del rango de números de puerto estándar.

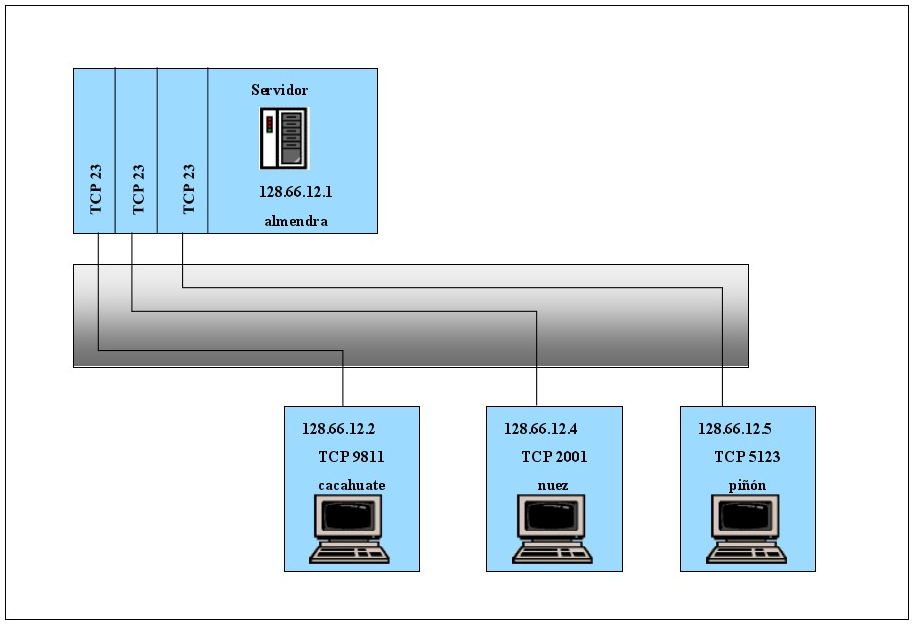
Los puertos asignados dinámicamente ofrecen la flexibilidad necesaria para soportar a varios usuarios. Para identificar de forma única cada conexión, al puerto fuente se le asigna un número de puerto asignado dinámicamente y se usa el número de puerto bien conocido para el puerto destino.

Por ejemplo con *Telnet*, al primer usuario se le da un número de puerto fuente al azar y el número de puerto destino 23 (*Telnet)*. Al segundo usuario se le da un número de puerto fuente al azar distinto y el mismo puerto destino. El par de números de puerto, fuente y destino, identifican de forma única cada conexión de red. El anfitrión destino conoce el puerto fuente porque va en el encabezado del segmento TCP o del paquete UDP. Ambos anfitriones conocen el puerto destino porque es un puerto bien conocido.

La combinación de una dirección IP y un número de puerto se llama *socket*. Un *socket* identifica de modo único un solo proceso de red dentro de toda Internet. Un par de *sockets*, uno del anfitrión receptor y otro del emisor, definen la conexión de los protocolos orientados a conexión, como TCP.



La Figura a continuación muestra cómo pueden conectarse clientes en diversas máquinas al mismo puerto de un solo servidor. El servidor puede distinguir la diferencia entre las conexiones porque cada una de ellas involucra diferentes direcciones IP. Aun si las conexiones vinieran todas de la misma máquina remota el servidor puede identificarlas porque cada una usa un número de puerto distinto en la máquina remota.


Servidor
TCP 23
TCP 23
TCP 23
128.66.12.1
almendra
128.66.12.2
TCP 9811
cacahuate
128.66.12.4
TCP 2001
nuez
128.66.12.5
TCP 5123
piñón