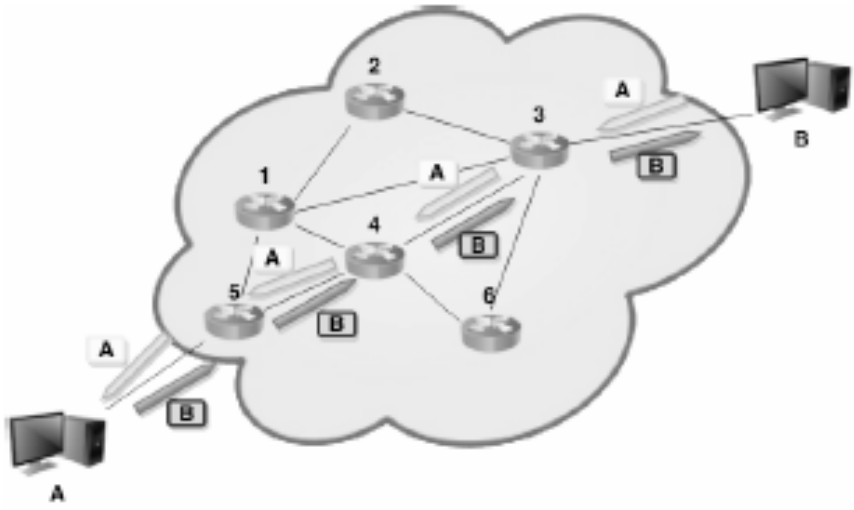

Figura 1.4 - Conmutación de paquetes en modo orientado a la conexión.

1.2.2 Redes de Área Local LAN

En contraste con las redes WAN, las redes LAN ocupan áreas geográficas pequeñas, por ejemplo un edificio o conjunto de edificios. Generalmente se trata de redes cuyo tendido obedece a la necesidad de compartir recursos, tales como impresoras, *scanners* y dispositivos de almacenamiento. Su mantenimiento queda a cargo de administradores, ya sean propietarios de las mismas o contratados para tal efecto.

Las redes LAN de mayor despliegue comercial son las conocidas con el nombre genérico de *Ethernet*. Su tendido se realiza sobre un cable del tipo par trenzado. Se trata de redes de alta velocidad, pudiendo llegar en la actualidad al orden de los *Gbps*. Se caracterizan por interconectar dispositivos tales como computadores personales, repetidores o *hubs*, puentes y conmutadores o *switches*, tal como se presenta en la Fig. 1.5. Generalmente un *router* es el dispositivo de salida de una red LAN a una red WAN.

Un *hub* es un elemento repetidor que ocasiona que la red se comporte como un *bus*, conociéndose con este nombre el caso de las redes LAN cuyos dispositivos comparten un medio, debiéndose establecer algún método de control para el acceso. El *hub* emula este comportamiento, repitiendo sobre todas sus bocas de salida, la señal que recibe por una boca de entrada.

Un *switch* es un dispositivo de mayor inteligencia que el *hub*, repitiendo mensajes entre sus puertos de acuerdo a cierto esquema de direccionamiento especial, propio de las redes LAN.

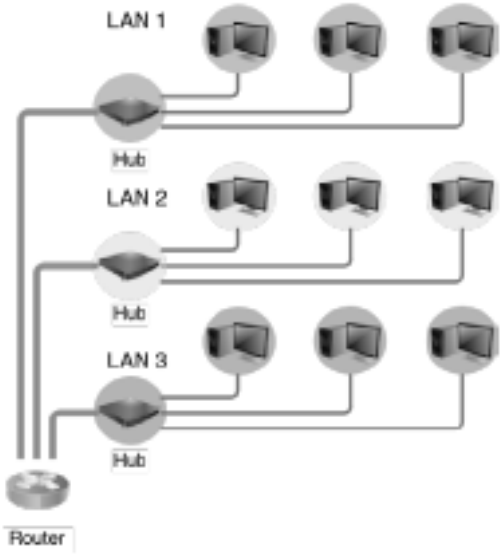

Figura 1.5 - Red LAN cableada.

La Fig. 1.6 presenta un ejemplo de red inalámbrica que cumple con el certificado de Fidelidad Inalámbrica (WiFi, Wireless Fidelity). Es un tipo de red LAN cuyo despliegue ha aumentado de manera sorprendente en los últimos años. Se trata de redes que conectan dispositivos inalámbricos y, en su modo más popular de instalación, poseen un nodo muy especial, conocido como Punto de Acceso (AP, Access Point), a través del cual pasan todas las comunicaciones.

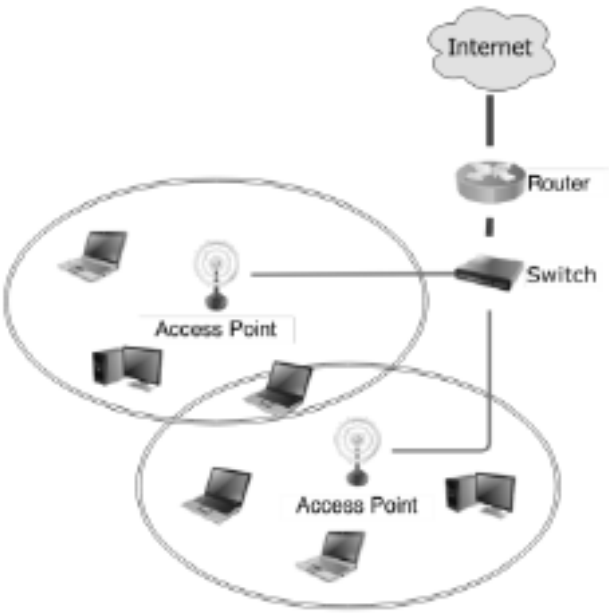

Figura 1.6 - Dos redes LAN WiFi conectadas a través de una LAN cableada.

En el caso de la figura, se puede observar un *switch* conectando ambos AP a través de un soporte cableado, disposición típica de muchas redes de este tipo. Es interesante observar en este ejemplo la disposición del AP como dispositivo de intermediación entre dos tipos de redes LAN. En este caso se dice que el AP realiza la función de un puente, también conocido como *bridge*.

1.2.3 Topologías de Red

La topología de red define su estructura física, o sea la manera en que se disponen los cables o enlaces que interconectan sus diversos elementos.

En general, encontramos las topologías presentadas en la Fig. 1.7, que también pueden servir para otro tipo de clasificación de las redes de datos:

- **Bus**: una de las topologías más sencillas que utiliza un único cable al que se conectan todos los componentes directamente. El cable debe terminarse apropiadamente en ambos extremos para evitar desadaptaciones. Todos los dispositivos comparten el mismo canal, por lo que debe existir una forma apropiada de ingreso al medio, quedando limitada tanto la cantidad de dispositivos como la longitud física de la red. La rotura del cable deja fuera de servicio el sistema.
- Ejemplo: LAN de cable coaxial.

- **Anillo**: conecta un elemento con el siguiente y el último con el primero. En este tipo de red la comunicación depende del paso de un paquete especial, denominado testigo o *token*, que se utiliza para ordenar la comunicación y permitir un acceso equitativo a todos los componentes. Si uno de los componentes falla o uno de los enlaces cae, la red queda fuera de servicio.
- Ejemplo: redes de fibra óptica como columna vertebral o *backbone* de red WAN.

- **Estrella**: conecta todos los cables con un punto central de concentración, por el que pasan todas las comunicaciones. Tiene como ventaja que, si un componente se desconecta o se rompe el cable que lo comunica, sólo ese equipo quedará fuera de la red. Su desventaja es que, si falla el nodo central, cae la red completa.
- Ejemplo: redes LAN tipo *Ethernet* con un conmutador tipo *switch* o un concentrador *hub* como elemento central.

- **Malla**: cada nodo se conecta con todos los demás, de tal manera que es posible llevar los mensajes de un nodo a otro por diferentes caminos. Al estar completamente conectada, se convierte en una red muy confiable en cuanto a una posible interrupción en las comunicaciones. Si la red tipo malla fuera cableada, una desventaja sería el costo, dada la cantidad de cable necesario para su instalación.

- Ejemplo: una red para control de una planta nuclear.

- **Árbol**: se trata de una topología centralizada, desarrollada a partir de un nodo raíz, a partir del cual se van desplegando los demás componentes como ramas. Los elementos de la red se ordenan en una estructura jerárquica, en donde se destaca un elemento predominante o raíz. El resto de los elementos comparte una relación tipo padre-hijo. El encaminamiento de los mensajes de este tipo de redes debe realizarse de tal manera de evitar lazos en la comunicación. Si falla un elemento podrían presentarse complicaciones, quedando parte de la estructura aislada, pero si falla la raíz, la propia red quedaría dividida en dos partes que no podrían comunicarse entre sí.
- Ejemplo: redes de sensores inalámbricos.

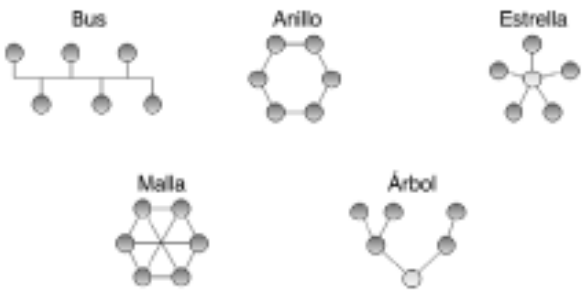

Figura 1.7 - Topologías de red.

1.3 Redes y Protocolos

Habiendo realizado una recorrida por diferentes clases de redes y topologías, conviene realizar una definición formal de red de datos y considerar algunos aspectos relacionados con su correcto funcionamiento.

Se define como **red de datos** a un grupo de dos o más elementos inteligentes que son capaces de comunicarse entre sí a través de algún medio e intercambiar datos de manera cooperativa.

Las redes conectan computadoras y los usuarios que las utilizan. Por ejemplo, en entornos de trabajo, los usuarios comparten recursos de redes LAN y pueden conectarse con otros usuarios, por ejemplo en otra red LAN, a través del acceso a una red WAN. Aparte de compartir datos fácil y rápidamente, pueden compartir dispositivos, tales como impresoras, y aprovechar más mecanismos de comunicación.

Al instalarse una red, primero debe ser planificada desde el punto de vista físico, atendiendo a las necesidades presentes y futuras que deba satisfacer. Una vez instalada físicamente, deberá configurarse para que funcione correctamente. Ya configurada correctamente, interesará que sea monitoreada para poder

anticiparse a posibles problemas de funcionamiento. Todo este trabajo se relaciona con la gestión de la red y es tarea de su administrador.

El uso eficiente de los recursos es una meta importante en cualquier clase de red y, en términos generales, se relaciona con las técnicas seleccionadas para compartir los mismos y los mecanismos utilizados para afrontar situaciones de congestión. De existir fallas, es importante considerar mecanismos de recuperación, sobre todo para evitar posibles pérdidas irreparables. También, dependiendo del tipo de información almacenada o transportada sobre la red, puede ser importante considerar herramientas de seguridad para la protección de los datos.

Por su parte, todo elemento conectado a la red debe contar con una interfaz de acceso apropiada, por ejemplo placas de red, con una antena o conector de red, en el caso de redes LAN.

A su vez, para que los distintos componentes de una red puedan dialogar entre sí de manera eficiente, debe existir una manera de identificarlos, es decir un esquema de direccionamiento apropiado al alcance de la comunicación.

Si se pretende una comunicación fiable, se deberán utilizar técnicas para control de errores. Si los componentes son de diferente capacidad operativa, probablemente utilicen técnicas de control de flujo para acomodar las diferencias en velocidad y/o capacidad de memoria.

Toda esta gestión del intercambio exige reglas de comunicación que deben ser respetadas por todas las partes.

Un **protocolo** define un conjunto de reglas, algoritmos, mensajes y otros mecanismos que habilitan a los elementos de una red a comunicarse de manera eficiente. Detrás de la definición de protocolo, yace la definición de un lenguaje común de entendimiento y la aceptación de un mismo conjunto de parámetros como convención. Por lo tanto, la definición de un protocolo exige el establecimiento de un formato para intercambio de mensajes y la precisión de las reglas que regirán ese intercambio. La elección del mismo debe ser previa a la comunicación y conocida por todas las partes involucradas en la misma.

Se pueden mencionar tres aspectos en la definición de un protocolo: sintáctico, semántico y de sincronismo de la comunicación. La especificación formal de estos tres aspectos es independiente de la implementación, que puede ser en *hardware* o *software*. El aspecto sintáctico se refiere a la especificación de formatos para los mensajes. La semántica se relaciona con la funcionalidad de control para la cual se ha diseñado el protocolo. Por su parte, el sincronismo define la sintonía de velocidades y secuencias particularmente utilizadas en la comunicación.

Para alcanzar un consenso general, un protocolo debe tener una especificación técnica con calidad de estándar. Los estándares son de conocimiento público, se los denomina protocolos abiertos para diferenciarlos de aquellos que no son públicos, conocidos como protocolos propietarios. Un ejemplo de los primeros es el protocolo de red IP. Los protocolos propietarios, en cambio, son protocolos con restricciones de uso, reglamentadas por patentes, y reforzadas por el mantenimiento de cláusulas secretas en cuanto a su implementación. Por ejemplo, un protocolo propietario es el que rige la comunicación por *Skype*.

Un protocolo de red es aquel específicamente diseñado para este tipo de comunicaciones. Su implementación consiste en un módulo de software con interfaces apropiadas para poder comunicarse con un entorno especial implementado en el sistema operativo de la máquina. Es decir que el sistema operativo debe poseer capacidad para comunicación sobre redes.

En general, los sistemas no utilizan un único protocolo, ya que se suele dividir el problema de la comunicación en módulos, para facilitar las tareas. Cada módulo puede tener asociado uno o más protocolos en un entorno de cooperación. Se suele denominar a este conjunto familia de protocolos o conjunto de protocolos. Una de las arquitecturas más conocido es la de TCP/IP.

1.4 Funcionalidad Asociada a Protocolos

Dado que un protocolo debe especificar las reglas que regulan la transmisión, deberá desarrollar varias de las siguientes funcionalidades, aunque no necesariamente todas:

- **Definición del formato de mensajes para el intercambio**: la existencia de un protocolo implica que los mensajes se trasladan de manera encapsulada, concepto que se asocia con la definición de paquete. El protocolo debe definir información adicional a los datos, denominada Información de Control de Protocolo (PCI, Protocol Control Information) o encabezado. El encabezado se asocia unívocamente a un protocolo, consistiendo en una serie de bits divididos en campos, cada uno con un significado particular asignado en su definición. Por otra parte, se denomina Unidad de Datos de Servicio (SDU, Service Data Unit) a la porción de información del mensaje. La SDU más el encabezado definido por el protocolo se denomina Unidad de Datos de Protocolo (PDU, Protocol Data Unit). El hecho de agregar un encabezado a la porción de datos se denomina encapsulado. En la Fig. 1.8 se presenta este concepto.

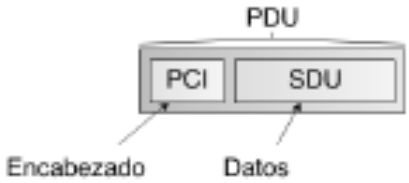

Figura 1.8 - Encapsulado.

- **Direccionamiento**: para poder realizar una comunicación en red se precisan identificadores, también llamados direcciones, tanto para la fuente de la información como para el destino de la misma. El examen de un campo de direcciones en el encabezado de un paquete permite al

elemento que lo procesa, determinar si va dirigido a éste o a otro dispositivo. Si el protocolo posee esta funcionalidad, muy probablemente defina además direcciones especiales. En este sentido, muchos protocolos precisan la dirección correspondiente a todos los bits en "1" como la dirección destino que pertenece a todas las estaciones de una red o dirección de *broadcast*. Esta dirección es de gran utilidad en las redes LAN para avisos de índole operativa, dirigidos a todos los integrantes de la red.
También existen direcciones en distintos niveles y con diferente alcance o significado.
A nivel de de comunicación en una red local, se usan las direcciones de fábrica de las placas de red o direcciones del nivel de Control de Acceso al Medio (MAC, Medium Access Control). Por ejemplo 00:13:49:00:01:02 es una dirección MAC de 48 *bits*.
En cambio, a nivel de red, para que sea posible identificar cada máquina en Internet, se usan direcciones IP del tipo 170.210.36.4, de 32 *bits*, con significado global. A su vez, dentro de un mismo dispositivo, para poder identificar las diferentes aplicaciones que simultáneamente se están comunicando, se utilizan números de puertos. Por ejemplo los servidores web se identifican con los puertos 80 y 8080, de 16 *bits*.

- **Control de errores**: muchos protocolos suelen agregar campos que resultan de la aplicación de algún código para detectar o corregir errores. Uno de los más utilizados es el código que resulta en la generación de bits de Chequeo de Redundancia Cíclica (CRC, Cyclic Redundancy Check). Con este campo adicional se puede trabajar en la detección de errores de transmisión, generando retransmisiones en caso de error.
  Algunos protocolos trabajan en la modalidad confiable, donde cada mensaje recibido sin errores es reconocido mediante el envío de otro mensaje especial a la fuente, conocido como de mensaje de Reconocimiento (ACK, Acknowledgment), distinguible por los valores de los bits de ciertos campos del encabezado. Bajo esta forma de transmisión, al enviar un mensaje y no recibir un ACK dentro de un tiempo determinado, conocido como tiempo de expiración o *timeout*, el transmisor supone que el mensaje no se recibió bien y procede a la retransmisión. Esta estrategia se conoce como de *timeout* y retransmisión.

- **Control de Acceso al Medio**: algunos protocolos se definen para generar un mecanismo de equilibrio de acceso en redes donde el medio es compartido. Algunas topologías que implican la existencia de un medio compartido son las de las redes tipo *bus*, estrella con elemento central tipo *hub*, redes inalámbricas o enlaces punto a punto de comunicación *half duplex*. En estos casos, el control de acceso puede ayudar a detectar o evitar las colisiones entre paquetes transmitidos en simultáneo por más de un dispositivo. Otras formas de ordenar el acceso podrían generarse a

través de un esquema de prioridades o por asignación de canales a cada usuario.

- **Control de Flujo**: es un mecanismo necesario para acomodar interlocutores con diferentes capacidades de procesamiento en cuanto a velocidad y memoria. Para ofrecer este control, muchos protocolos utilizan los propios mensajes de ACK para regular el flujo de la comunicación.
  Uno de los mecanismos más utilizados es el de Parada & Espera (*Stop & Wait*), que se usa en redes WiFi, condicionando la transmisión del cada mensaje a la llegada de un ACK para el mensaje previo.
  Por su parte, TCP usa un control de flujo más complejo, conocido como mecanismo de ventana deslizante, que permite transmitir y mantener en espera más de un mensaje por vez.

- **Control de Orden**: es aplicable en aquellas redes de tipo datagrama, donde los mensajes pueden llegar desordenados, debido a los retardos propios de la red o las diferencias de rutas tomadas por los paquetes en su camino hacia el destino. En respuesta a este problema, muchos protocolos agregan un campo en el encabezado, donde se coloca un número de secuencia que identifica al mensaje. Se debe tener en cuenta que se tratará de un campo con un número de bits limitado, por ejemplo $n\ bits$, razón por la cual sólo permitirá distinguir hasta 2^n mensajes diferentes que se encuentren en tránsito simultáneamente.
  El control de orden también permite distinguir copias de un mismo mensaje, ya que en los casos en los que se usan mecanismos de retransmisión, la pérdida de un ACK podría provocar un retransmisión innecesaria, generando la llegada de un mensaje duplicado, distinguible por la repetición de un número de secuencia.

- **Fragmentación**: en Internet existen redes capaces de transportar mensajes de distintos tamaños. Por ejemplo, una red LAN cableada tipo *Ethernet* puede transportar mensajes de hasta $1500\ bytes$ de datos, en tanto que una red de Modo de Transferencia Asincrónico (ATM, Asynchronous Transfer Mode) transporta mensajes, llamados celdas, de hasta $53\ bytes$. Se denomina Unidad de Transferencia Máxima (MTU, Maximum Transfer Unit) al tamaño máximo de mensaje que una red puede manejar. Teniendo en cuenta que la información debe atravesar una gran variedad de redes, con distintos valores de MTU, algunos protocolos incorporan mecanismos de fragmentación que deben ser complementados con mecanismos de re-ensamble para la recuperación de los datos fragmentados. Con este propósito, se deben adicionar campos especiales en los encabezados. Es de destacar que el mecanismo de fragmentación genera una disminución en el tamaño de la carga de datos, empeorando la relación de incidencia de la longitud del encabezado respecto de la del propio campo de datos.

- **Control de Conexión**: este tipo de control suele encontrarse presente en esquemas del tipo orientado a la conexión, donde se precisan mensajes específicos para el inicio y el cierre de la conexión. Con el propósito de distinguir estos mensajes de control, se incorporan bits especiales en el encabezado.

- **Multiplexado**: en comunicaciones se denomina multiplexor al dispositivo capaz de combinar varios canales en uno solo. Un de-multiplexor realiza la acción contraria, separando a partir un único mensaje, la información correspondiente a cada canal. En temas relacionados con protocolos, el concepto se refiere a la capacidad que posee un protocolo de marcar en su encabezado a cuál otro protocolo debe entregarse el mensaje cuando por encima de éste exista más de una posibilidad.

- **Encaminamiento**: en el caso de la comunicación entre sistemas que no se encuentren directamente conectados, se precisarán dispositivos intermedios a lo largo de la ruta al destino, cuya función es la generación de las acciones apropiadas para el re-envío de los paquetes hacia la dirección apropiada. Para poder cumplir la funcionalidad de encaminar correctamente, estos elementos deben conocer algo de la topología circundante, representada por otros nodos que los puedan ayudar a cumplir con la entrega. Las Tablas de Enrutamiento almacenan esta clase de información, construyéndose a partir del intercambio de mensajes entre nodos. Estos mensajes son generados por protocolos especiales, denominados protocolos de enrutamiento.

1.5 Estándares y su Organización

Toda vez que se enfrente el estudio de redes de datos, se deberán analizar estándares que regulan su funcionalidad y organizaciones que son las responsables de la generación de esos estándares. La necesidad de interconectar equipos con diferentes especificaciones de hardware o software pone en evidencia la importancia de estos estándares, pues ellos describen protocolos y tecnologías.

Se definen como sistemas abiertos, aquellos que son capaces de interactuar con otros de diferente tecnología. Estos sistemas se desarrollan en base a estándares universales, a diferencia de los sistemas propietarios que sólo pueden interactuar con otros sistemas similares. La definición de un estándar universal permite, por ejemplo, que equipos de diferentes fabricantes puedan compartir un entorno.

Para poder desarrollar estándares universales, se precisan organizaciones que coordinen las discusiones y la publicación de la documentación.

A lo largo del texto, se tratarán estándares desarrollados por algunas de las organizaciones mencionadas a continuación:

- **Organización Internacional para Estandarización (ISO,International Organization for Standardization)**: Esta organización no gubernamental fue creada en 1946. Sus miembros son organismos nacionales de máxima representatividad en el tema de estandarización, aceptándose sólo un miembro por país. Por ejemplo, IRAM de Argentina es miembro de la ISO. En este libro se desarrollará un modelo de comunicación en redes ideado por la ISO y conocido como Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI, Open Sistem Interconnection). http://www.iso.org/

- **Instituto Nacional Americano de Estándares (ANSI, American National Standards Institute)**: Responsable de coordinar y publicar los estándares de tecnología de la información y computación en Estados Unidos. Es miembro de la ISO. Por ejemplo, ANSI C es un estándar para el lenguaje de programación C. http://www.ansi.org/

- **Instituto de Ingenieros Electricistas y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers)**: Organización de profesionales de ingeniería eléctrica y electrónica. Uno de los estándares más conocidos de la IEEE es el proyecto IEEE 802, que permitió el desarrollo de tecnologías LAN tipo *Ethernet* y WiFi. http://www.ieee.org/index.html/

- **Alianza de Industrias Electrónicas (EIA, Electronic Industries Alliance)**: Asociación internacional de industrias cuyos estándares más conocidos se refieren al cableado de redes. http://www.eciaonline.org/eiastandards/

- **Unión Internacional de Telecomunicaciones – Sector de Estandarización para Telecomunicaciones (ITU-T, International Telecommunication Union – Telecommunication Standardization Sector)**: Organización internacional para desarrollo de estándares para la industria de las telecomunicaciones.
  http://www.itu.int/en/Pages/default.aspx

1.5.1 Organismos Específicos para Estandarización de Internet

Junto con el crecimiento de Internet, se hizo evidente la necesidad de una estructura formal de organismos para fortalecer cuestiones relacionadas con su arquitectura, estándares, políticas y muchas otras actividades.

En 1992 se creó la Sociedad de Internet (ISOC, Internet Society) para promover la evolución y crecimiento de Internet como estructura global de comunicaciones, y proveer coordinación global de actividades relacionadas con Internet. Se trata de una sociedad de profesionales con más de cien organizaciones y veinte mil miembros en ciento ochenta países. Provee liderazgo en el direccionamiento de cuestiones relativas al presente y futuro de Internet. También es la organización madre para los grupos responsables de los estándares de infraestructura de Internet y se ubica en la intersección del trabajo de grupos de desarrollo, políticas públicas y actividades de educación, tal como se representa en la Fig. 1.9.

La ISOC fiscaliza a la Junta de Arquitectura de Internet (IAB, Internet Architecture Board), que a su vez dirige la Fuerza de Tareas de Ingeniería de Internet (IETF, Internet Engineering Task Force) y la Fuerza de Tareas de Investigación de Internet (IRTF, Internet Research Task Force).

La IETF cumple su trabajo a través de varios grupos, cada uno responsable de desarrollar estándares y tecnologías en áreas tales como Internet, gerenciamiento y operaciones, enrutamiento, seguridad, transporte y aplicaciones en tiempo real. Cada área es manejada por un director, conformando en su conjunto el IESG que, a su vez, reporta ante la IAB.

La IRTF se dedica a las cuestiones relacionadas con el largo plazo para las tecnologías de TCP/IP e Internet. Es una organización más pequeña que la IETF aunque, al igual que ésta, se encuentra conformada por grupos de investigación. La IRTF es supervisada por el IRSG y la IAB.

Por otro lado, la necesidad de estandarizar determinados parámetros, por ejemplo identificadores de protocolos, o recursos globales tales como las direcciones IP, significó el surgimiento de una Autoridad de Asignación de Números de Internet (IANA, Internet Assigned Number Authority), que en 1998 fue sustituido por la Corporación de Internet para Asignación de Nombre y Números (ICANN, Internet Corporation for Assigned Names and Numbers).

IANA opera actualmente bajo ICANN, siendo aún responsable de la asignación de direcciones IP, a través de la entrega de grandes bloques de direcciones a los Registros Regionales de Internet (RIR, Regional Internet Registry) que realizan actividades de asignación a distintos ISP en una región particular del mundo. Existen cuatro de estos registros. APNIC atiende sólo Asia y el Pacífico, en tanto que ARIN se encarga de América del Norte, parte del Caribe y África sub-ecuatorial. Para América Latina y el resto del Caribe, el registro responsable es LACNIC, y para Europa, Medio Oriente, Asia Central, y África al norte del Ecuador, es RIPE NCC.

La asignación de nombres ya no es responsabilidad del IANA, sino que ICANN ha abierto el registro de nombres a muchas organizaciones en el nivel más alto de la jerarquía DNS.

En cuanto a la estandarización de protocolos, al principio se basó en un esquema de consensos: cualquier nueva propuesta se debía plasmar por escrito para ponerla a disposición del resto para su discusión. El objetivo era generar un Requerimiento de Comentarios, por eso estas presentaciones escritas se conocen con las siglas RFC (Requests for Comments). No siempre un RFC describe un

estándar, ya que muchos de estos requerimientos son meramente descriptivos, con el objetivo de clarificar conceptos.

Con la estructura inmensa de Internet actual, este esquema tan informal no daría resultados, aunque los estándares todavía se conocen con sus siglas originales RFC.

Actualmente, la responsabilidad principal de la creación de estándares es de la IETF, cuyos desarrollos se formalizan como un RFC, escritos que son publicados por el Editor de los RFC para su consideración por parte de la comunidad de Internet. Su descarga es gratuita y esta posibilidad se considera uno de los principales motivos de la explosión en el crecimiento de Internet.

No todos los RFC se convierten en estándares, sino que tienen diferentes categorías.

Existen RFC con categoría de estándar propuesto o de borrador, estos últimos conocidos como *draft*, que pueden haberse ya aprobados formalmente como estándares o encontrarse en vías de serlo. Otros son simples recomendaciones o documentos de información general. También existen propuestas en estado experimental.

Antes de que un RFC se pueda considerar estándar, debe publicarse como borrador, bajo ciertos lineamientos de creación que establece la IETF. Generalmente los escriben miembros de los grupos de trabajo de la IETF, aunque cualquier persona podría hacerlo. La revisión queda a consideración de quienes trabajan en otros grupos de trabajo de la IETF. Si la revisión arroja resultados favorables, el documento puede ser candidato a estándar y así pasar a la categoría de estándar propuesto, si el IESG lo dispone.

Aunque sea considerado como tal, estas propuestas deben revisarse mediante pruebas experimentales, probando su aptitud y aceptabilidad para la tecnología vigente. Si se sortean con éxito estas pruebas, el RFC se puede elevar de categoría estándar propuesto a estándar *draft*. Para llegar a alcanzar el estado de Estándar de Internet, la especificación debe ser tecnológicamente madura y ampliamente implementada.

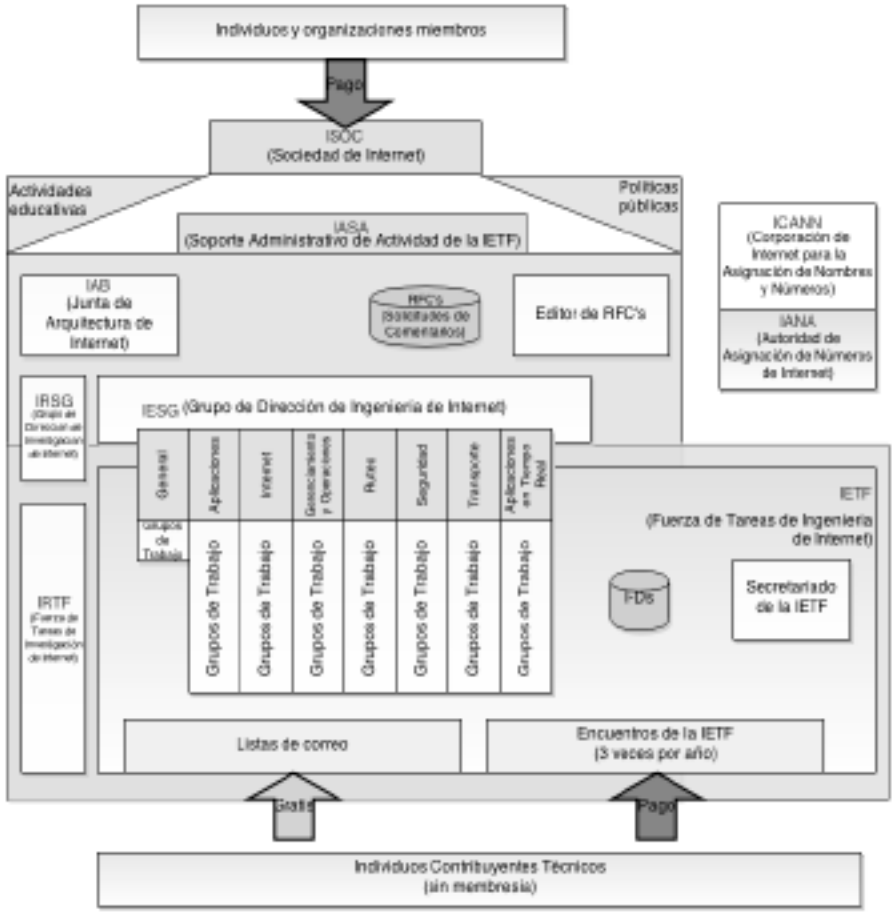

Figura 1.9 - Estructura organizacional de la ISOC.

Bibliografía

1. Tanenbaum, Andrew S., "Redes de Computadoras", Tercera Edición. Prentice Hall Inc., 1996.
2. Stallings, William, "Comunicaciones y Redes de Computadores". Sexta Edición. Prentice Hall Inc., 2000.
3. Commer, Douglas E., "Internetworking with TCP/IP", Vol I Principles, Protocols, and Architecture. Prentice Hall Inc., 1995.
4. Cohen, Danny, "Computer History Museum Exhibits Internet History" http://www.computerhistory.org/internet_history/
5. Leiner, Barry M., Cerf, Vinton G., Clark, David D., Kahn, Robert E., Kleinrock, Leonard, Lynch, Daniel C., Postel, Jon, Roberts, Larry G., Wolff, Stephen, "Brief History of the Internet". http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf
6. Índice de RFC, http://www.ietf.org/rfc/
7. The Internet Engineering Task Force (IETF): http://www.ietf.org/