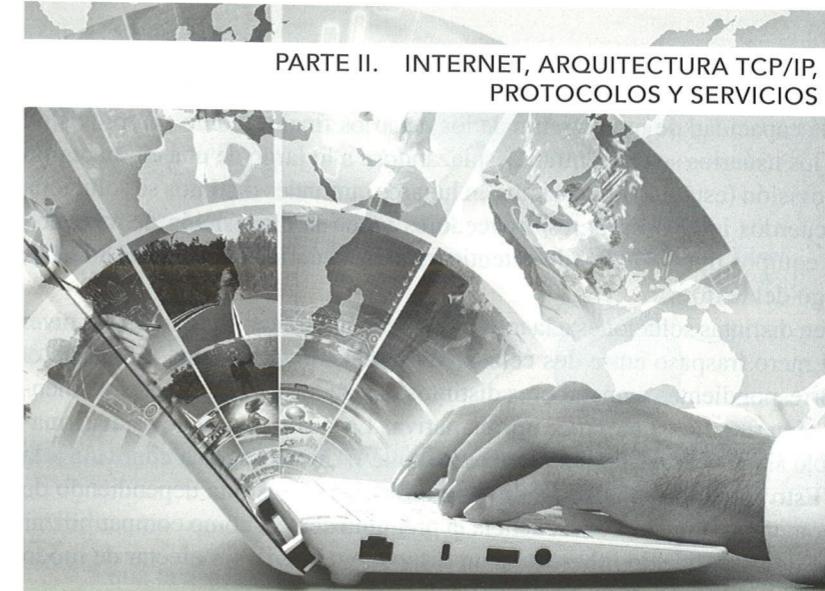


- ITU-T: *La Seguridad de las Telecomunicaciones y las Tecnologías de la Información*. 2006.
- Kaufman, C.: *Internet Key Exchange (IKEv2) Protocol*. RFC 4306. Diciembre, 2005.
- Kent, S.; Seo, K.: *Security Architecture for the Internet Protocol*. RFC 4301. Diciembre, 2005.
- Krawczyk, H.; Bellare, M.; Canetti, R.: *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104. Febrero, 1997.
- Leech, M.; Ganis, M.; Lee, Y.; Kuris, R.; Koblas, D.; Jones, L.: *SOCKS Protocol Version 5*. RFC 1928. Marzo, 1996.
- Lindqvist, U.: *On the Fundamentals of Analysis and Detection of Computer Misuse*. PhD Dissertation, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 1999.
- McCloghrie, K.: *SNMPv2 Management Information Base for the Internet Protocol using SMIV2*. RFC 2011. Noviembre, 1996.
- McCloghrie, K.: *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIV2*. RFC 2012. Noviembre, 1996.
- McCloghrie, K.: *SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2*. RFC 2013. Noviembre, 1996.
- McCloghrie, K.; Rose, M.T.: *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*. RFC 1213. Marzo, 1991.
- Neuman, C.; Yu, T.; Hartman, S.; Raeburn, K.: *The Kerberos Network Authentication Service (V5)*. RFC 4120. Julio, 2005.
- Perkins, C.: *IP Encapsulation within IP*. RFC 2003. Octubre, 1996.
- Perkins, C.: *Minimal Encapsulation within IP*. RFC 2004. Octubre, 1996.
- Ramsdell, B.: *S/MIME Version 3 Certificate Handling*. RFC 2632. Junio, 1999.
- Ramsdell, B.: *S/MIME Version 3 Message Specification*. RFC 2633. Junio, 1999.
- Rigney, C.; Rubens, A.; Simpson, W.; Willens, S.: *Remote Authentication Dial In User Service (RADIUS)*. RFC 2058. Enero, 1997.
- Rivest, R.: *The MD5 Message-Digest Algorithm*. RFC 1321. Abril, 1992.
- Rose, M.T.; McCloghrie, K.: *Concise MIB Definitions*. RFC 1212. Marzo, 1991.
- Rose, M.T.: *The Simple Book: An Introduction to Networking Management*. Ed. Prentice-Hall, 1996.
- Russell, D.; Gangemi, G.T.: *Computer Security Basis*. Ed. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1991.
- Shirey, R.: *Internet Security Glossary, Version 2*. RFC 4949. Agosto, 2007.
- Stallings, W.: *Network and Internetwork Security: Principles and Practice*. Ed. Prentice-Hall, 1995.
- Stallings, W.: *Network Security Essentials. Applications and Standards*. Pearson, 2011.
- Tanenbaum, A.S.; Wetherall, D.J.: *Computer Networks*. Ed. Prentice-Hall, 2011. 5.^a edición.
- Terplan, K.: *Communication Networks Management*. Ed. Prentice-Hall, 1992.
- Townsley, W.; Valencia, A.; Rubens, A.; Pall, G.; Zorn, G.; Palter, B.: *Layer Two Tunneling Protocol «L2TP»*. RFC 2661. Agosto, 1999.
- Turner, S.; Chen, L.: *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*. RFC 6151. Marzo, 2011.
- Valencia, A.; Littlewood, M.; Kolar, T.: *Cisco Layer Two Forwarding (Protocol) «L2F»*. RFC 2341. Mayo, 1998.
- Wijnen, B.; Harrington, D.; Presuhn, R.: *An Architecture for Describing SNMP Management Frameworks*. RFC 2571. Abril, 1999.
- Wijnen, B.; Presuhn, R.; McCloghrie, K.: *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. RFC 2575. Abril, 1999.



GESTIÓN DE LA MOVILIDAD DEL USUARIO

- 13.1. Motivación
- 13.2. Provisión de movilidad en la capa de enlace
- 13.3. Provisión de movilidad en la capa de red: IP móvil
- 13.4. Provisión de movilidad en la capa de transporte
- 13.5. Provisión de movilidad en la capa de aplicación

13.1. Motivación

Hasta este punto hemos tratado de ofrecer una visión general de los procedimientos y protocolos que sustentan las tecnologías de red actuales, en particular en referencia a Internet (esto es, las redes TCP/IP). El estudio aquí realizado está lejos de resultar no ya exhaustivo, sino completo siquiera. Son así numerosos los aspectos, las tecnologías, los protocolos, los servicios que han sido obviados a lo largo del presente texto. Y ello principalmente porque su inclusión superaría con creces los objetivos marcados para este libro, tanto en completitud como en extensión.

No queremos concluir sin embargo la materia aquí tratada sin apuntar aunque sea de forma breve otras cuestiones y tecnologías que, por un lado, evidencien el alcance de lo antes señalado y, por otro, hagan mención expresa a algunos de los aspectos reseñables como complemento a los «fundamentos» hasta ahora expuestos, y sin que ello signifique que estos resultan de mayor relevancia que otros varios también mencionables.

La disponibilidad de tecnologías de transmisión inalámbrica tales como las WLAN o los sistemas de telefonía celular UMTS y 4G, ha potenciado una gran actividad con objeto de garantizar la provisión de servicios a dispositivos móviles de usuario con conexión a Internet. Es de mencionar así la existencia de diversos informes oficiales que señalan la evolución exponencial experimentada por el tráfico móvil en Internet en las últimas fechas. En particular, en el momento de la elaboración del presente documento se apunta que un tercio del tráfico total actual de Internet se refiere a sistemas con movilidad, alcanzándose la cifra de varias decenas de miles de terabytes de este tipo de tráfico al mes en España.

Ello pone de manifiesto el enorme impacto socio-económico que supone la así llamada Internet móvil. Es importante indicar aquí que el término móvil o movilidad (también conocido como *nomadicidad*) no se refiere tanto a la capacidad de movimiento de los usuarios finales, como a la provisión efectiva de servicios mientras los usuarios se encuentran desplazándose a lo largo de una cierta región geográfica. En esta línea, la provisión (estática) de servicios en lugares puntuales distintos se soluciona con la simple definición de acuerdos inter-operadores/proveedores y con la disposición de mecanismos de auto-configuration de equipos tipo DHCP y de autenticación de usuarios como IEEE 802.1X, ambos ya presentados a lo largo del texto.

Aclarado lo anterior, existen distintas soluciones a la movilidad real, dinámica, en función del nivel pretendido para esta: desde el mero traspaso entre dos celdas adyacentes de una misma red, hasta el desplazamiento entre redes correspondientes a operadores distintos. Llegados a este punto es de mencionar que, lamentablemente, ¡Internet no es móvil de forma nativa! La justificación de esta afirmación es fácilmente comprensible si aceptamos, como ya sabemos, que IP identifica una conexión a la red y no un dispositivo en sí. Esto es, un dispositivo tendrá una dirección IP distinta dependiendo de su ubicación exacta en cada momento. Surge en consecuencia la pregunta clave: ¿cómo compatibilizar este hecho con la capacidad de desplazamiento inherente a un dispositivo móvil, sin afectar de modo significativo los servicios proporcionados en cada momento?

Para dar solución al problema de la movilidad en toda su dimensión, la mayor parte de las soluciones disponibles actuales se basan en el empleo de túneles. Si no todas ellas sí las más importantes se presentan a lo largo del resto del capítulo, organizadas en base a la capa en la que operan: enlace (Apartado 13.2), red (Apartado 13.3), transporte (Apartado 13.4) y aplicación (Apartado 13.5).

13.2. Provisión de movilidad en la capa de enlace

El protocolo DHCP no fue diseñado para permitir la movilidad de los *hosts*, pero puede ser utilizado para reconfigurar las comunicaciones cuando se detecta una variación en los puertos Ethernet de un cliente debido a un cambio en su localización. Si tal es el caso se difunde un mensaje DHCP *Request* sobre la red, el cual será retransmitido por los distintos conmutadores dispuestos en la infraestructura. Con ello se consigue que todas las tablas MAC se actualicen con la nueva localización de la dirección del cliente, permitiendo así la movilidad en las capas superiores a través de la capa 2 de enlace.

Para permitir movilidad básica en entornos inalámbricos IEEE 802.11 se definió el *protocolo entre puntos de acceso*, o IAPP («Inter-Access Point Protocol»). Relativo a la recomendación IEEE 802.11f, en IAPP se contempla la difusión de un mensaje de capa 2 (IEEE 802.2 XID Update Response) por parte de un punto de acceso cada vez que se asocia a este un nuevo cliente. Ello permite que cualquier dispositivo de capa 2 actualice su tabla con el puerto correcto para alcanzar la nueva localización del cliente. Obsérvese el paralelismo entre este procedimiento y el antes mencionado para entornos cableados.

Para permitir la gestión rápida de la movilidad entre puntos de acceso (AP), al tiempo que se mantiene un nivel de seguridad adecuado en entornos inalámbricos, IEEE 802.11i contempla un mecanismo de *almacenamiento proactivo de clave*, o PKC («Proactive Key Caching»), el cual permite a una estación cliente almacenar temporalmente la clave PMK («Pairwise Master Keying») derivada durante el proceso de autenticación EAP con un punto de acceso particular. Si, tras haber estado asociado con posterioridad a otro AP distinto, la estación vuelve a estar bajo la cobertura del primero, el cliente puede decidir reutilizar la PMK y así evitar un segundo proceso de autenticación EAP con el mismo AP.

También es de mencionar en esta misma línea el mecanismo de transición rápida contemplado en IEEE 802.11r. En este caso, solo el AP inicial contacta con el servidor de autenticación, de manera

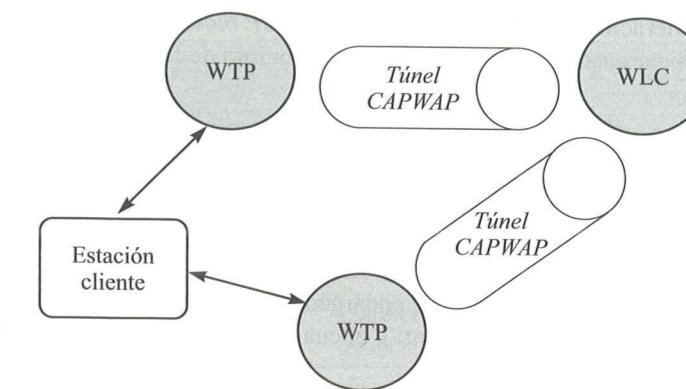


Figura 13.1. Arquitectura CAPWAP.

que la asociación posterior de un cliente dado a otros AP distintos implicaría la interacción de estos con el AP inicial para recuperar el material de claves, y así evitar nuevas interacciones con el servidor.

Si bien las soluciones de movilidad hasta aquí planteadas resultan adecuadas para la gestión de la movilidad de los usuarios en entornos de dimensiones reducidas, no lo son cuando nos referimos a redes más extensas como, por ejemplo, las desplegadas en campus. En tal caso se recurre a soluciones como la relativa a la arquitectura CAPWAP («Configuration and Provisioning for Wireless Access Points»; RFC 3990, 4118) para redes inalámbricas. En esta se centraliza la autenticación de los clientes a través de la disposición de un AP «amplio» compuesto funcionalmente por un WTP («Wireless Termination Point») y un WLC («Wireless LAN Controller»). El primero hace las veces de un AP «ligero», mientras que el WLC se encarga de la autenticación centralizada de un conjunto de AP. Ambas funciones, implementadas en la misma o en distintas subredes, se interconectan a través de un túnel CAPWAP. La ventaja evidente de esta aproximación es que cuando un cliente se mueve entre WTP gestionados por un mismo WLC, este último lleva a cabo de forma sencilla la actualización del estado del cliente sobre el túnel CAPWAP con el nuevo punto de acceso (véase Figura 13.1).

En este punto cabe mencionar que si bien la IETF no especifica la funcionalidad inter-WLC, orientada a posibilitar comunicaciones entre controladores para la gestión de movilidad en topologías de red más complejas, fabricantes como Cisco sí lo hacen a través de la definición de soluciones propietarias.

13.3. Provisión de movilidad en la capa de red: IP móvil

La solución desarrollada por la IETF para dar respuesta al problema de la movilidad en la capa de red tiene como premisa fundamental la transparencia de funcionamiento para el sistema, lo que se traduce en las siguientes consideraciones:

1. Todo dispositivo móvil debe ser capaz de utilizar su dirección IP base en cualquier lugar.
2. Los paquetes destinados al *host* móvil deben recibirse en este sin problemas.
3. No se deben precisar cambios en el software de los *hosts* fijos.
4. No deben ser necesarios cambios en el software de los nodos de encaminamiento ni en las tablas.
5. No debe producirse carga extra cuando el móvil está en su red base.

Con estas consideraciones se desarrolló el protocolo *IP móvil*, o MIP («Mobile IP», ver RFC 3220, 3344 y 5944, actualizaciones del RFC 2002), cuyo principio de funcionamiento se basa en la existencia de tres entidades:

- *Nodo móvil* (MN, «Mobile Node») o de usuario, el cual hace uso de dos direcciones IP:
 - *Base*: dirección IP fija correspondiente a la red a la que pertenece.
 - *Care-of-Address* (CA): dirección variable que identifica al MN en la red que este visita en un momento dado.
- *Agente local* (HA, «Home Agent»), encargado de gestionar la dirección base del MN.
- *Agente externo* (FA, «Foreign Agent»), el cual gestiona la dirección CA asociada al MN en un momento dado.

La interacción de los tres elementos mencionados define la funcionalidad del protocolo IP móvil a través de los siguientes tres procedimientos:

1. *Descubrimiento de la dirección CA*. HA y FA anuncian su presencia de forma periódica, de modo que un MN puede determinar si se encuentra en su red base o en una externa. Si sucede lo segundo, MN obtiene una CA a través del FA, dirección a la que se denomina FACA¹.
2. *Registro de la dirección CA*. Proceso por el que el MN comunica a su HA la CA asociada acordada con el FA.
3. *Envío basado en túnel a la dirección CA*. Realizado el registro, HA intercepta cualquier paquete destinado a MN y lo reenvía a la dirección CA haciendo uso de un esquema de «tunneling». Por su parte, los paquetes enviados por MN no tienen porqué encaminarse por HA.

En los siguientes apartados se detalla cada uno de estos tres procesos.

13.3.1. Descubrimiento de la dirección CA

El descubrimiento de la dirección CA pasa por el conocimiento por parte del MN de la identidad del agente local o externo, dependiendo de si se encuentra en su red base o en una externa. Para ello, los agentes implementan una extensión de los mensajes ICMP *anuncio de router Router Advertisement* (RA, ver RFC 1256), los cuales son difundidos por parte de los nodos de encaminamiento para dar a conocer su existencia a los *hosts* de forma automática. La extensión referida a los mensajes RA se denomina *Mobility Agent Advertisement* (MAA, ver RFC 3220) y tiene las siguientes características reseñables:

- Está incluida en un mensaje RA de ICMP (mensaje tipo 9, véase Apartado 9.2), por lo que el campo *protocolo* del paquete IP sobre el que se encapsula tomará el valor 1 indicativo de dicho protocolo (ver RFC 1700).
- Dicho paquete IP se difunde a todos los sistemas haciendo uso de la dirección *multicast* 224.0.0.1 o de la de difusión 255.255.255.255.
- Puede ir acompañada de un mensaje ICMP de extensión de *longitud de prefijo* (tipo 19), a través del cual se especifica la longitud del prefijo de red de cada una de las direcciones de los nodos de encaminamiento incluidas en el mensaje RA. A través de estos prefijos de red el MN puede deducir si se encuentra en su red base o en una externa.

¹ Frente a FACA aparece el término *co-located CA*, proporcionada por medios externos como es el uso del protocolo DHCP, el cual permite la asignación dinámica de direcciones IP disponibles dentro de un conjunto. No obstante, como ya se ha apuntado, esta solución no resulta adecuada en el contexto que nos ocupa por cuanto que implica el uso de una única dirección IP por parte del móvil, dirección que varía conforme lo hace el área de localización del dispositivo o *host*.

	0	4	8	16	19	24	31
Cabecera IP	Versión	LC	TS			Longitud total paquete IP	
				Identificación	I	Desplazamiento	
	TTL		Protocolo = 1			Comprobación	
				Dirección IP origen			
				Dirección IP destino = 224.0.0.1 o 255.255.255.255			
Mensaje RA de ICMP	Tipo = 9		Código = 0		Comprobación		
	N.direcciones	L.entradas = 2			Tiempo de vida direcciones		
				Dirección router 1			
				Nivel preferencia 1			
				Dirección router 2			
				Nivel preferencia 2			
				...			
Mensaje MAA de ICMP	Tipo = 16	Longitud		Número secuencia			
		Tiempo máximo de vida registros	R B H F M G r T	Reservado			
			Care-of-address 1				
			Care-of-address 2				
			...				
Longitud prefijo (opcional)	Tipo = 19	Longitud	Longitud prefijo 1	Longitud prefijo 2			
			...				

Figura 13.2. Formato y encapsulado del mensaje ICMP *Mobility Agent Advertisement* (MAA).

Los campos que componen explícitamente un mensaje MAA son los siguientes (Figura 13.2):

- *Tipo*: campo de 8 bits a valor 16 a través del que se especifica que se trata de un mensaje ICMP MAA.
- *Longitud*: número de octetos del mensaje MAA, sin contar los dos correspondientes a este campo y al anterior.
- *Número secuencia*: número de mensaje MAA desde que el agente fue inicializado. Dado su carácter monótonamente creciente, este campo se utiliza para detectar duplicaciones en las transmisiones o posibles situaciones de reinicio del agente.
- *Tiempo máximo de vida de los registros*: número máximo de segundos que este agente acepta solicitudes de registro (ver más adelante).
- A continuación sigue una serie de bits a través de los que se señalan ciertas capacidades: registro solicitado (*R*), agente ocupado (*B*), el agente realiza funciones de agente local (*H*) y/o externo (*F*), soporte de encapsulado mínimo (*M*) o GRE (*G*) —ver Apartado 12.3.3—, el agente externo soporta envío mediante túnel en sentido contrario (*T*, ver *envío mediante túnel a CA más adelante*). El bit indicado como *r* significa reservado, sin asignación.
- *Reservado*: campo de 16 bits a valor 0 e ignorado en recepción.
- *Care-of-address i*: lista de direcciones CA disponibles anunciadas por el agente emisor del mensaje MAA.

Alternativamente al anuncio explícito por parte de los agentes, un MN puede enviar un mensaje para descubrir la identidad de estos. Este tipo de mensaje se denomina *Agent Solicitation* (AS)

y es idéntico al de *Router Solicitation* (RS) de ICMP², salvo por el hecho de que el campo TTL del paquete IP sobre el que se encapsula toma el valor 1. En el RFC 1256 se especifica que el mensaje RS de ICMP solo consta de la cabecera ICMP con el campo *tipo* a valor 10 (Figura 9.8), estando dirigido el datagrama IP sobre el que se encapsula AS a la dirección *multicast* 224.0.0.11, de significado «agentes móviles».

13.3.2. Registro de la dirección CA

Conocidas las direcciones CA anunciadas por un agente, un MN debe proceder a obtener una de ellas. Este proceso es el que se conoce como *registro*, el cual consiste básicamente en dos pasos conceptuales:

1. El MN contactará con el agente solicitando una de las CA disponibles anunciadas.
2. La aceptación de esta pasa por el establecimiento de la asociación MN-CA en el HA (véase Apartado 12.3.2 acerca de seguridad en las comunicaciones).

Adicionalmente al proceso anterior, un procedimiento de registro permite a un MN:

- a) Renovar un registro próximo a caducar.
- b) Anular la asociación MN-CA cuando vuelve a su red base. Es el proceso denominado «desregistro».

En consecuencia, un MN lleva a cabo un procedimiento de registro cuando se cumple una de las siguientes circunstancias:

- El bit *R* del mensaje MAA de ICMP está activo (ver apartado anterior).
- Expira el tiempo de vida del CA asociado.
- Se recibe un mensaje MAA con una extensión ICMP de prefijo de red distinto.
- Se detecta el retorno a su red base tras recibir un MAA procedente de su HA.
- Se reinicia su FA, hecho que se constatará tras recibir un mensaje MAA con número de secuencia inferior al último recibido.

Los mensajes involucrados en un proceso de registro son dos: *Registration Request* (RRq) y *Registration Reply* (RRp) —ver RFC 3220—, intercambiándose entre el MN, el HA y el FA como se indica a continuación en función de si el nodo móvil se encuentra en su red base o en una externa:

- Cuando el MN se encuentra en su red base, el procedimiento de registro se lleva a cabo entre el MN y el HA. Los pasos involucrados son:
 1. MN envía un paquete RRq a su HA.
 2. HA responde a este con un mensaje RRp, en el que se especifica la concesión o no de la petición.
- Por su parte, cuando MN se encuentra visitando una red externa el procedimiento de registro se establece con el FA como sigue:
 1. MN envía un paquete RRq al FA.
 2. El FA lo procesa y lo retransmite al HA.
 3. El HA envía a FA un mensaje RRp concediendo o denegando la petición.
 4. El FA lo procesa y lo retransmite al MN.

² Los mensajes ICMP *Router Advertisement* y *Router Solicitation* constituyen los mensajes denominados genéricamente como *Router Discovery* (véase mensajes ICMP en Apartado 9.2 del presente texto).

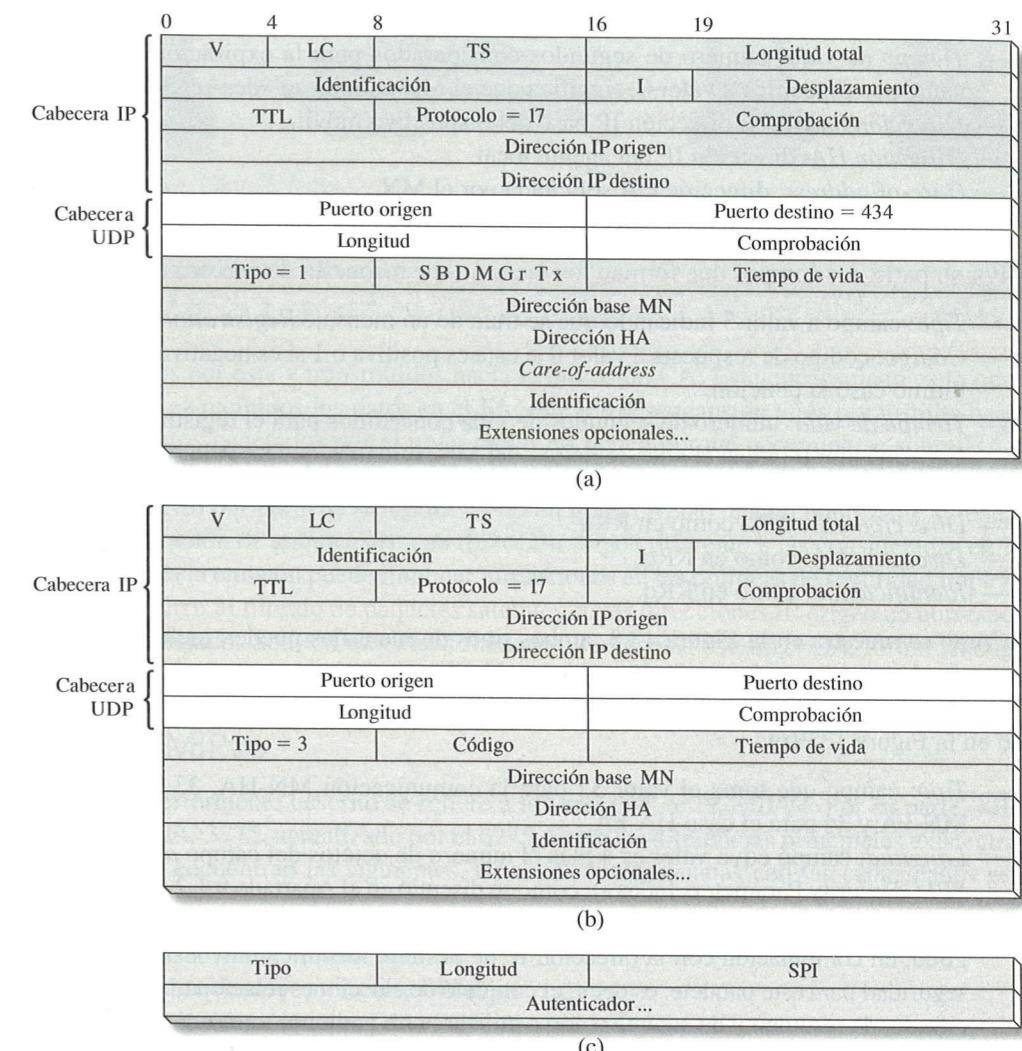


Figura 13.3. Encapsulado de los mensajes *solicitud de registro* (a) y *respuesta de registro* (b). Formato de la extensión de autenticación (c).

En la Figura 13.3 se muestra el formato de los mensajes de solicitud (RRq) y de respuesta (RRp) de registro, los cuales se transmiten encapsulados en datagramas de usuario UDP (protocolo 17 según RFC 1700) destinados al puerto 434. Los campos considerados en los mensajes de solicitud (RRq) son los siguientes:

- *Tipo*: campo de 8 bits a valor 1 en los mensajes *Registration Request*.
- *S*: el MN solicita al HA que mantenga asociaciones simultáneas de CA.
- *B*: si este bit se encuentra activo, el MN solicita al HA la retransmisión de cualquier paquete de difusión transmitido sobre la red base.
- *D*: el MN está utilizando una dirección CA *co-located* en lugar de una FACA.
- *M*: uso de encapsulado mínimo (ver Apartado 12.3.3).
- *G*: uso de encapsulado GRE (ver Apartado 12.3.3).
- *r* y *x*: bits a valor 0 e ignorados en recepción.

- *T*: solicitud de túnel inverso (ver *envío mediante túnel a CA* más adelante).
- *Tiempo de vida*: número de segundos considerados para la expiración del registro. Si este campo se especifica a valor 0, significa que el MN solicita su «des-registro».
- *Dirección base MN*: dirección IP base del dispositivo móvil.
- *Dirección HA*: dirección IP del agente local.
- *Care-of-address*: dirección CA solicitada por el MN.
- *Identificación*: campo de 32 bits para hacer corresponder solicitudes con respuestas.

Por su parte, los campos que forman los mensajes de respuesta de registro (RRp) son:

- *Tipo*: campo a valor 3 indicando que se trata de un mensaje *Registration Reply*.
- *Código*: código de respuesta a valor 0 si esta es positiva o 1 si es negativa, denegándose en este último caso la petición.
- *Tiempo de vida*: número de segundos de vida concedidos para el registro correspondiente a la CA. Un valor 0 indica el «des-registro» del MN, mientras que un valor 0xFFFF en este campo significa un tiempo de vida «infinito».
- *Dirección base MN*: como en RRq.
- *Dirección HA*: como en RRq.
- *Identificación*: como en RRq.

Como se muestra en la Figura 13.3, ambos tipos de mensajes pueden incluir extensiones opcionales, entre las que se encuentra la de *autenticación*. Esta permite una comunicación segura entre las entidades participantes en el proceso de registro. El formato de la extensión de autenticación es el mostrado en la Figura 13.3(c):

- *Tipo*: campo que toma el valor 32 para la comunicación MN-HA, 33 para la comunicación MN-FA y 34 para el caso HA-FA.
- *Longitud*: campo cuyo valor es 4 más el número de octetos del campo *autenticador*.
- *SPI* («Security Parameters Index»): como se discutió en el Apartado 9.1.2 al respecto de las cabeceras AH y ESP, y se volvió a mencionar en el Apartado 12.3.2, el campo SPI, de 32 bits de longitud, en combinación con la dirección IP de destino, identifica únicamente la asociación de seguridad para este paquete; es decir, el conjunto de elecciones relacionadas con los algoritmo de cifrado, de resumen y de autenticación a utilizar entre ambos extremos de la comunicación.
- *Autenticador*: también descrito en el Apartado 9.1.2, este campo es de longitud variable y contiene el valor de comprobación de integridad para el paquete actual.

Una vez finalizado el proceso de registro, el HA dispone de lo que se conoce como *binding*, que no es más que una asociación del tipo *dirección_base_MN + CA + tiempo_vida*.

13.3.3. Envío mediante túnel a CA

Cuando un nodo móvil (MN) se desplaza a una red externa y se ha realizado el proceso de registro comentado anteriormente, el agente local (HA) difunde un mensaje *ARP gratuito* a través del cual permite que todos los nodos asocien espontáneamente la dirección física del agente con la IP base de MN. Simultáneamente, HA implementa el protocolo *ARP promiscuo* a fin de dar respuesta a cualquier consulta ARP acerca de MN. A partir de ahí, HA intercepta todos los mensajes destinados a MN y los envía hacia CA sobre un túnel, concepto este ya presentado en el Apartado 12.3.2.

En la Figura 13.4 se muestra esquemáticamente el uso de un túnel aplicado al contexto que nos ocupa. En ella se observa el proceso seguido en la comunicación HA-MN a través de la CA proporcionada por el FA. Los paquetes destinados a la dirección base de MN y capturados por HA, son

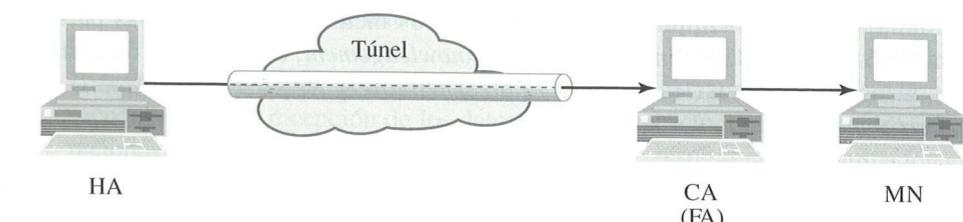


Figura 13.4. Comunicación HA-MN mediante un túnel.

encapsulados por este y transmitidos hacia la dirección CA. Este encapsulado es lo que constituye el túnel. Una vez recibidos los datos en el FA, este los desencapsula y los retransmite hacia MN. Por su parte, los datos generados por el nodo móvil no tienen porqué encaminarse sobre HA, por lo que el túnel en sentido contrario (denominado *túnel inverso*) es menos utilizado. No obstante, hay que señalar que el envío por parte de MN a través de un túnel inverso resulta interesante si tenemos en cuenta que la generación de paquetes IP con dirección origen diferente a las consideradas en la red desde la que se realiza la emisión puede implicar infracciones en las políticas de seguridad implementadas. Así, se suele recurrir al filtrado de paquetes salientes cuyas direcciones IP origen no corresponden a las del entorno manejado. Son los esquemas llamados de «*egress filtering*». De forma análoga, también se suele hacer uso de esquemas «*ingress filtering*» para el control de tráfico entrante.

13.3.4. MIPv6

Todo lo anteriormente descrito se refiere a la versión 4 de IP, MIPv4. Por su parte, MIPv6 está definido en el RFC 3775, actualizado por el 6275. Entre las diferencias principales existentes entre MIPv4 y MIPv6 se encuentran las siguientes, todas ellas relacionadas con las capacidades propias de IPv6 frente a IPv4:

- Integración de optimización de rutas.
- Soporte de nodos «*ingress filtering*».
- No consideración de nodos FA ni encapsulado.
- Uso de descubrimiento de vecinos de IPv6 frente a ARP.

De este modo, la operación MIPv6 es como sigue, supuesto que MN se encuentra desplazado a una red remota:

1. MN solicita una CA mediante el protocolo *Neighbor Discovery* de IPv6 (RFC 4862), a través del cual se posibilita el descubrimiento de nodos, el descubrimiento de prefijo, la autoconfiguración de direcciones (RFC 4862), la resolución de direcciones, la redirección, etc.
2. Obtenida la dirección CA por parte de MN, envía un mensaje *Binding Update* a su agente local, HA.
3. En respuesta, HA enviará un mensaje *Binding Acknowledgement* a MN aceptando la asociación.
4. Formalizada esta, esto es, registrada en HA la localización remota de MN, HA usará mensajes *Proxy Neighbor Advertisement* para capturar los paquetes recibidos en su entorno con destino MN, los cuales serán encapsulados con la cabecera ESP IPv6 y enviados a MN.
5. Por lo que respecta a los envíos inversos, MN usará la opción de destino IPv6 *Home Address* para indicar al receptor del paquete la dirección base del MN aunque se use CA como dirección origen del paquete.

En suma, MIPv6 contempla el empleo de nuevos mensajes y/o cabeceras para su operación: cabecera IPv6 de movilidad (*Binding Update/Acknowledgement*, etc.), opción de destino IPv6 *Home Address*, mensajes ICMPv6 (*Home Agent Address Discovery Request/Reply*, *Mobile Prefix Solicitation/Advertisement*), etc.

13.4. Provisión de movilidad en la capa de transporte

La provisión de seguridad en capas superiores a la de red, en concreto en la de transporte, aporta varios beneficios:

- Optimización inherente de rutas, al evitarse las comunicaciones triangulares implicadas con el empleo de túneles.
- Superación de elementos de seguridad (como los cortafuegos para el filtrado de paquetes), al hacerse uso siempre de direcciones IP «topológicamente correctas».
- Pausado y recuperación de transmisiones, de manera que estas pueden retomarse en el punto en que se quedaron cuando se produjo el cambio de localización del dispositivo, y tras la «reconexión» correspondiente por parte de los elementos de red inferiores a la capa de transporte.
- Capacidad de aplicación de mecanismos de optimización comunes para flujos distintos.

Seguidamente se presentan algunas de las soluciones a la movilidad planteadas en la capa de transporte.

13.4.1. SCTP

El protocolo SCTP («Stream Control Transmission Protocol») se encuentra estandarizado en los RFC 2960 y 4960, y consiste en un protocolo de transporte de propósito general alternativo a TCP y UDP. De forma análoga a TCP, SCTP ofrece un servicio fiable orientado a conexión y lleva a cabo control de congestión.

SCTP define todas las funciones necesarias para establecer y cerrar comunicaciones y transmitir datos. En lugar de hablar de sesiones o conexiones, relativas a comunicaciones entre dos direcciones IP finales, en SCTP se habla de *asociaciones* para referirnos a comunicaciones lógicas entre dos nodos sobre múltiples direcciones IP origen o destino. Una asociación se define, así, como un conjunto de direcciones IP de cada nodo origen o destino y un puerto en cada nodo. El formato de las unidades de datos intercambiados sobre una asociación SCTP se construye concatenando (dependiendo de la funcionalidad requerida) distintos trozos, denominados *chunk*.

SCTP permite también la adaptación de la tasa de transferencia. A pesar de estas similitudes con TCP, existen diferencias significativas:

- SCTP permite *multistreaming*, lo que significa que se posibilita el envío de varias secuencias dentro de una misma asociación entre dos nodos.
- También posibilita *multihoming*, esto es, permite crear y gestionar una asociación sobre múltiples direcciones IP. Esto se traduce en capacidades de adaptación y gestión de movilidad.

A lo largo del tiempo de vida de una asociación, SCTP transita entre tres estados:

- *Inicio*. Frente al proceso de tres pasos seguido en TCP para el establecimiento de conexión, en SCTP son cuatro los pasos contemplados para el inicio: solicitud a través de un mensaje **INIT**, confirmación y solicitud en el otro sentido mediante **INIT-ACK**, construcción del estado del receptor mediante **COOKIE-ECHO** y definición de la configuración mediante **COOKIE-ACK**. Ambos *chunk* de tipo **COOKIE** pueden transportar datos, pues ambos se intercambian una vez que la asociación ha sido validada.

En la Figura 13.5 se muestra una comparativa de los procesos de inicio en TCP y en SCTP.

— *Transferencia de datos*. A diferencia de TCP, donde se hace uso de una única numeración de secuencia para la recepción de los datos en orden estricto, en SCTP se consideran dos numeraciones. Ello es así porque tal requerimiento puede resultar en una limitación en la eficiencia de la comunicación, pues se impide por ejemplo que el cliente pueda visualizar partes de una página web recibida hasta tanto no se reciban otras partes anteriores.

Los dos números de secuencia aludidos son:

- **TSN** («Transmission Sequence Number»), que permite la transmisión de paquetes y la detección de pérdida de estos a nivel de la capa de transporte.
- **SSN** («Stream Sequence Number»), el cual determina la secuencia del envío de los datos y la prioridad del uso del *buffer* a nivel de la capa de aplicación.

En suma, a través del *multistreaming* se posibilita la reordenación parcial de un flujo dado dentro de la asociación SCTP, lo que permite priorizar ciertos flujos. En la Figura 13.6 se muestra una comparativa de los procesos de secuenciación seguidos en TCP y en SCTP.

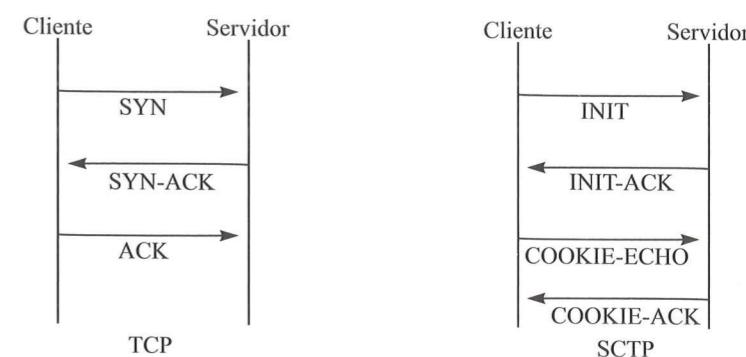


Figura 13.5. Procesos de inicio en TCP y en SCTP.

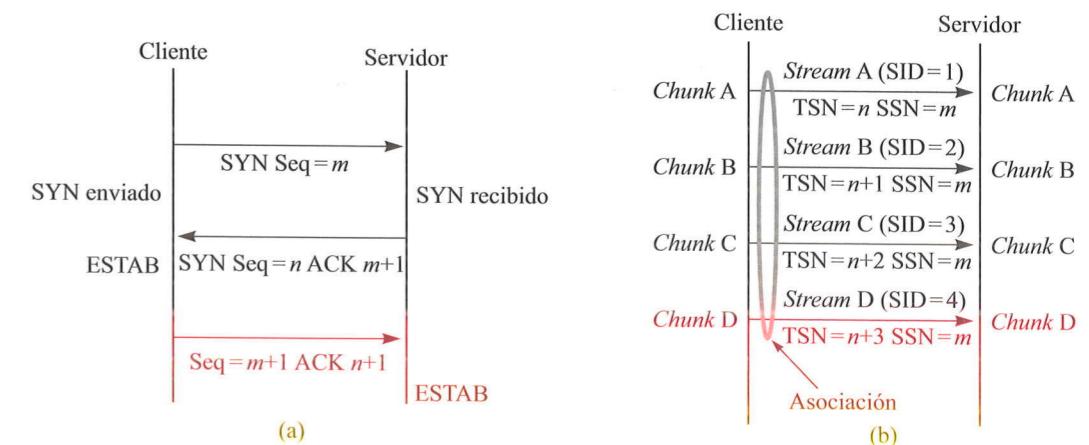


Figura 13.6. Procesos de secuenciación en TCP (a) y en SCTP (b).

Por lo que respecta a la otra característica de SCTP, *multihoming*, a través de ella se proporciona resistencia ante posibles fallos en las interfaces de los nodos en base a la posibilidad de gestionar el envío de datos sobre varias direcciones IP de modo simultáneo (véase Figura 13.7).

- *Cierre*. Para concluir una asociación entre dos nodos, ambas partes deben convenir en ello. Con este fin se intercambian los mensajes SHUTDOWN, SHUTDOWN-ACK y SHUTDOWN COMPLETION como se muestra en la Figura 13.8.

Los mensajes SCTP constan de una cabecera común seguida de una estructura de datos de longitud variable (Figura 13.9). La primera contiene la siguiente información:

- *Puertos origen y destino* que, en combinación con las direcciones IP origen y destino, identifican el receptor SCTP del paquete. Los números de puerto permiten soportar diferentes asociaciones SCTP sobre una misma dirección IP.
- *Comprobación*, correspondiente al empleo de un CRC basado en un polinomio generador de 32 bits.

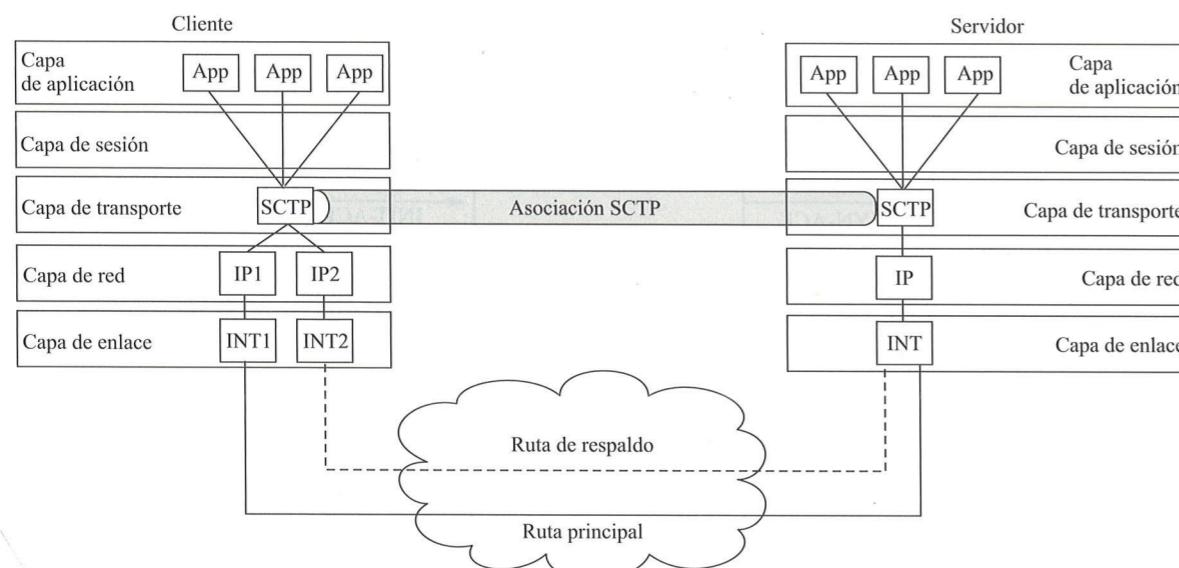


Figura 13.7. Multihoming SCTP.

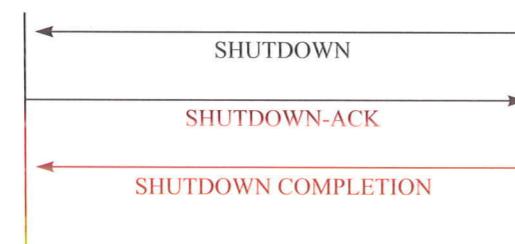


Figura 13.8. Proceso de cierre de asociación en SCTP.

Puerto origen	Puerto destino
Etiqueta verificación	
Comprobación	
Chunk 1	
...	
Chunk N	

Figura 13.9. Formato de mensajes SCTP, con los campos de cabecera sombreados.

- *Etiqueta verificación*, correspondiente al valor inicial intercambiado entre dos *hosts* durante el procedimiento de inicio de cuatro pasos. Este valor debe estar contenido en cada paquete SCTP correspondiente a la asociación, siendo descartado dicho paquete en caso contrario. El objetivo es servir de protección contra paquetes obsoletos correspondientes a asociaciones previas, así como contra ataques de tipo «man-in-the-middle» (MitM).

La parte de datos de los paquetes SCTP que sigue a la cabecera depende, como no puede ser de otro modo, del tipo de mensaje concreto de que se trate: INIT, INIT-ACK, SHUTDOWN, etc. Algunos otros mensajes SCTP adicionales a los ya mencionados con anterioridad son:

- DATA: *chunk* usado para transmitir datos de usuario entre dos entidades pares en una asociación SCTP.
- HEARTBEAT: *chunk* usado para testar la accesibilidad de una dirección IP que forma parte de una asociación.
- ABORT: terminación de una asociación.
- ECNE: valor no definido formalmente por la IETF pero reservado para la notificación explícita de congestión.
- CWR: valor no definido formalmente por la IETF pero reservado para permitir la reducción de la ventana de congestión.
- ERROR: *chunk* para la notificación de errores relativos a una asociación.
- SACK: confirmación selectiva usada para notificar al emisor tanto la recepción como la pérdida de *chunks*.

Adicionalmente a todo lo anteriormente expuesto, en SCTP se contemplan extensiones. En particular, la extensión ADDIP, definida en el RFC 5061 acerca de la reconfiguración dinámica de direcciones, permite el uso de SCTP en entornos de movilidad en base a la consideración de dos nuevos tipos de *chunk*:

- ASCONF: usado por un extremo para notificar cambios de dirección (añadidos, borrados, modificaciones) a una entidad par SCTP.
- ASCONF-ACK: confirmación al *chunk* anterior.

Aunque sobre ADDIP se puede proporcionar movilidad, ha de señalarse que *SCTP móvil* se encuentra actualmente en proceso de definición como *draft* de la IETF para conseguir abordar el reto de la movilidad de forma completa (véase referencia de Riegel en la sección *Bibliografía* al final del tema).

13.4.2. MPTCP

La IETF ha llevado a cabo la modificación del protocolo TCP para ampliar su funcionalidad en una línea similar a SCTP. En esta dirección, MPTCP («MultiPath TCP») permite el uso simultáneo de varias rutas para sesiones TCP, al tiempo que presenta algunas ventajas frente a SCTP:

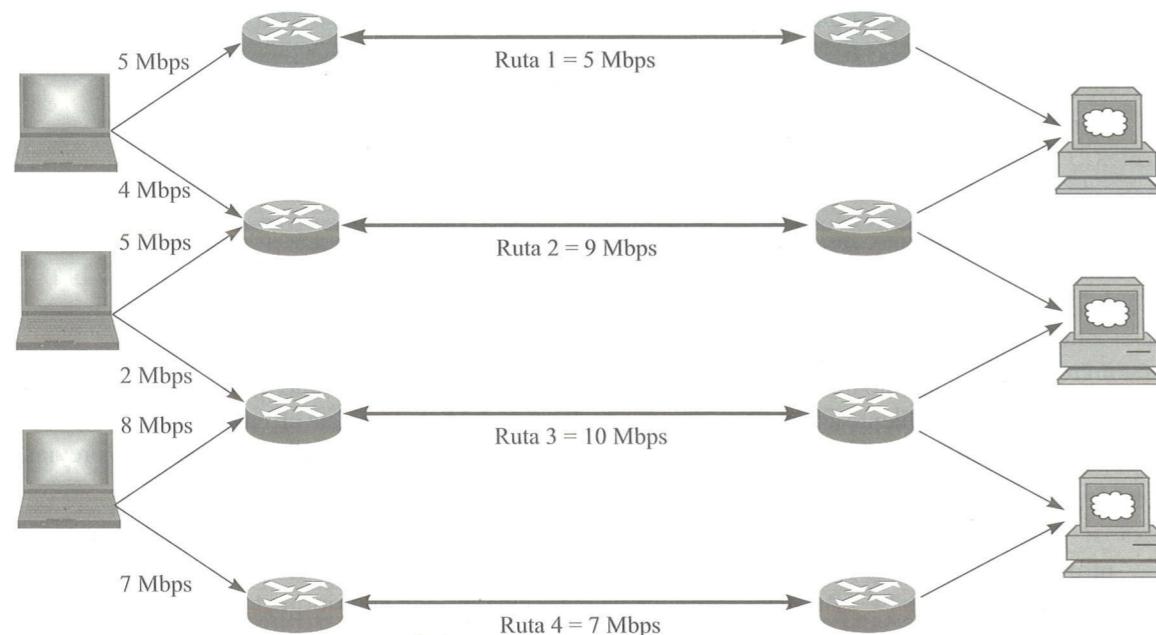


Figura 13.10. Agregación de recursos en la capa de transporte.

- Opera sobre la infraestructura Internet existente.
- Resulta estable sobre un amplio rango de rutas.
- Es transparente para los nodos en las rutas, como los dispositivos NAT.

MPTCP opera sobre un principio de agregación de recursos, de manera que se puede hacer uso concurrente de múltiples interfaces, rutas de red y servidores de aplicación. De este modo, los recursos de la red aparecen con uno solo lógico³. En la Figura 13.10 se muestra cómo esta agregación de recursos permite aumentar la fiabilidad y flexibilidad de la red en base a la distribución del tráfico.

MPTCP está basado en algunos de los principios del proyecto Tng («Transport Next-Generation»), que propone descomponer la capa de transporte en funciones orientadas a aplicación y funciones orientadas a red. La funcionalidad de transporte se distribuye así en cuatro capas lógicas como sigue, las dos primeras orientadas a aplicación y las dos segundas a red:

- *Capa semántica*: hace disponible para todas las aplicaciones las rutas de comunicación, como las sesiones TCP y los *multistream* SCTP.
- *Capa de aislamiento*: proporciona protección y fiabilidad extremo-a-extremo.
- *Capa de flujo*: implementa mecanismos de control de congestión y otras capacidades de gestión.
- *Capa de punto extremo*: implementa mecanismos de identificación de servicios y de extremos para identificar y reforzar las políticas de red.

En base a lo anterior, MPTCP soporta funciones orientadas a aplicación extremo-a-extremo, al tiempo que funciones de red en relación a los nodos dispuestos en las rutas consideradas. Así, frente

³ Otros ejemplos de protocolos mencionados en este texto que siguen una filosofía similar de trabajo son MPLS y VLAN (véase Capítulo 6).

a TCP, donde solo se contemplan las dos capas bajas antes indicadas, MPTCP permite en cambio el control independiente como «sub-flujos» de múltiples sesiones (véase Figura 13.11).

De forma similar a como se estableció para *multihoming* en SCTP (Figura 13.7), MPTCP puede tomar información de la capa de aplicación y distribuir los datos de secuencia sobre varias sesiones TCP disponibles (véase Figura 13.12).

Habida cuenta de la capacidad de MPTCP para añadir, eliminar y modificar direcciones de una sesión y compartir datos sobre múltiples interfaces, este protocolo es susceptible de ser usado también para proporcionar movilidad en las redes de próxima generación. Sin embargo, como sucede con

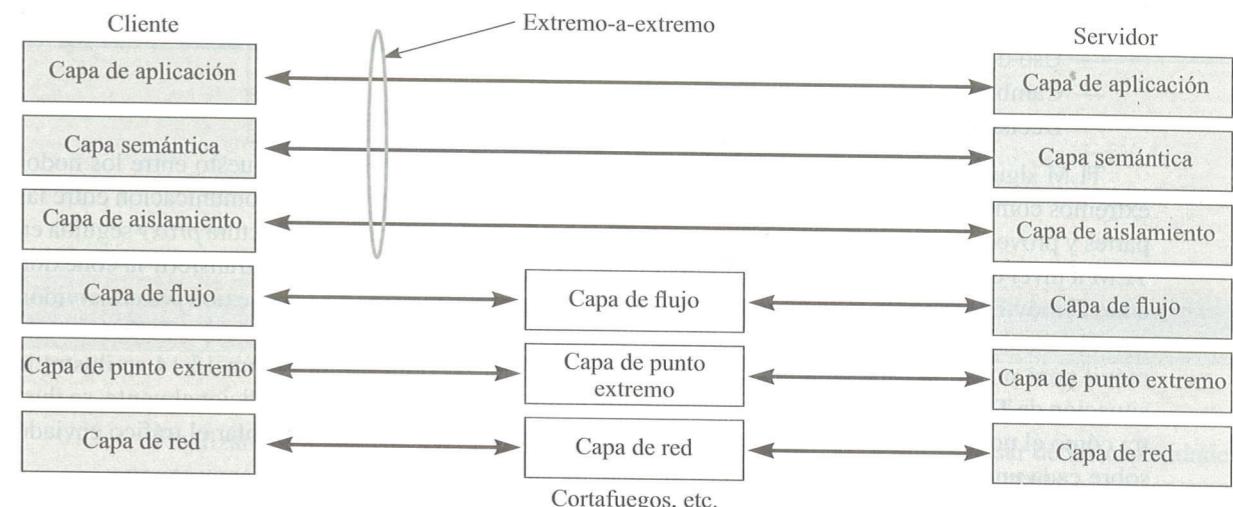


Figura 13.11. Descomposición y operación de la capa de transporte en MPTCP.

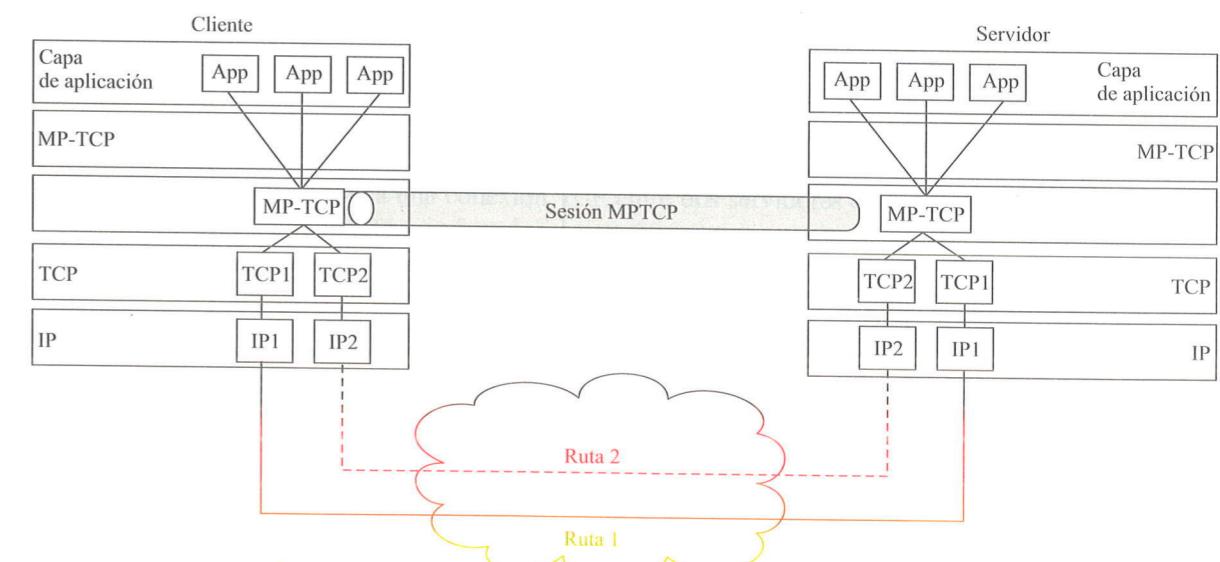


Figura 13.12. Distribución del tráfico en sub-flujos en MPTCP.

SCTCP, MPTCP presenta algunos problemas para abordar con total garantía este fin. Ello pasa, como es también el caso de SCTP, por la necesaria definición de extensiones al protocolo, lo cual constituye una línea de trabajo actual de la IETF.

Para más información sobre MPTCP y sus extensiones, consultese los RFC 6824 y 6897.

13.4.3. MSOCKS

MSOCKS se inició como un proyecto de IBM en el marco del servicio SOCKS ya mencionado en el Capítulo 12 y referente a un cortafuegos de tipo *proxy*. MSOCKS define una arquitectura llamada TLM («Transport Layer Mobility») orientada a dar solución a los siguientes problemas:

- Uso de múltiples interfaces en un mismo nodo móvil.
- Cambio de localización de un dispositivo móvil.
- Decisión acerca de qué flujos de datos utilizan qué interfaz disponible.

TLM sigue una arquitectura *proxy*, en la que un dispositivo intermedio dispuesto entre los nodos extremos comunicantes, y denominado *proxy*, será el encargado de gestionar la comunicación entre las partes y proveer los servicios pertinentes. En la Figura 13.13 se muestra la arquitectura *proxy* seguida en TLM a nivel de transporte, donde se observa la inclusión de un mecanismo para transferir la conexión entre el móvil y el *proxy* a una nueva interfaz mientras permanece inalterada la conexión *proxy-servidor*.

TLM solo precisa la disposición de un *proxy* TLM y la modificación de la capa TCP del nodo móvil pero no así la capa de aplicación, ni del nodo ni del servidor. En la Figura 13.14 se ilustra la situación de TLM en la pila de comunicación entre el nodo móvil y el servidor. Adicionalmente, se ilustra cómo el nodo móvil puede usar simultáneamente varias interfaces IP y controlar el tráfico enviado sobre cada una de ellas.

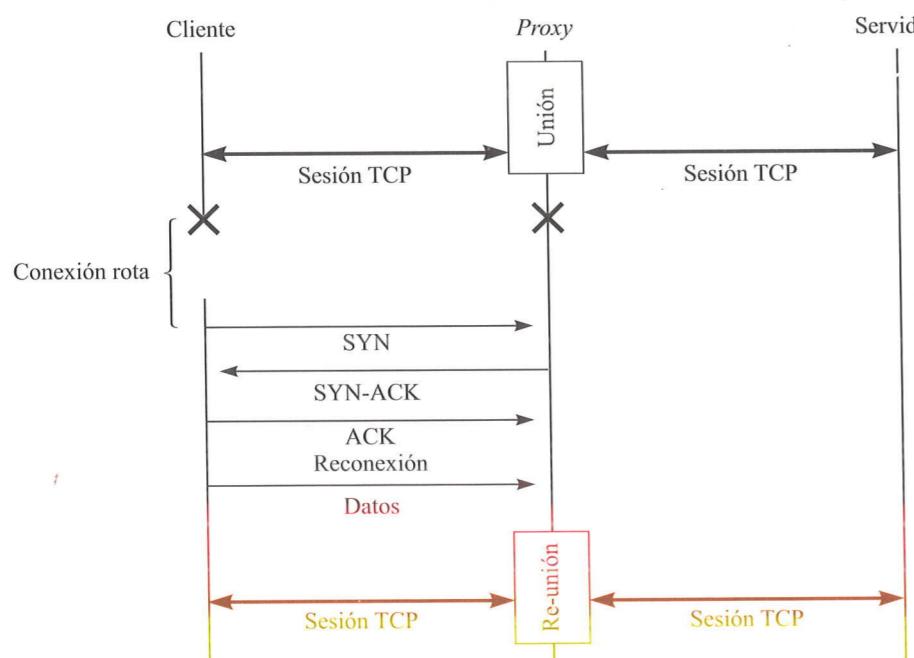


Figura 13.13. Arquitectura proxy TLM.

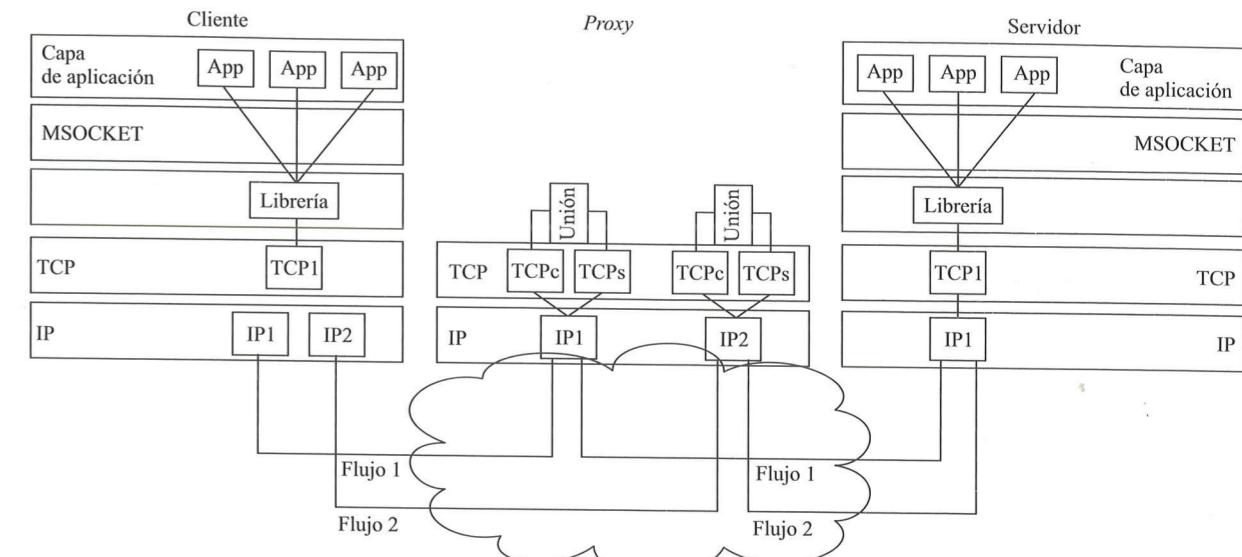


Figura 13.14. Situación de TLM en la pila de comunicación, donde se muestra el control de interfaces permitido al nodo móvil.

Finalizamos la descripción de MSOCKS comentando el hecho de que, a pesar de las capacidades y prestaciones teóricas de este protocolo en relación a la gestión de la movilidad, TLM aún se encuentra en un estado de investigación, con escaso desarrollo real (véase la referencia de Maltz en la sección *Bibliografía* al final del tema).

Para concluir la exposición de soluciones a la movilidad en la capa de transporte, cabe citar algunos otros protocolos desarrollados similares a los ya comentados:

- En el *Migrate Internet Project* del MIT se propone una solución similar a TLM en cuanto a que se sustenta en opciones TCP. Sin embargo, no contempla el uso de un *proxy* y, en consecuencia, tanto el cliente como el servidor deben tener capacidades *Migrate*.
- El protocolo M-TCP («Migratory TCP») también se basa en extensiones TCP, pero en este caso el cliente implica una conexión TCP entre dos servidores en lugar de cambiar una conexión dada a otra interfaz.
- SLM («Session Layer Mobility») es una solución encuadrada en la capa de sesión. Sin recurrir de nuevo al empleo de túneles, y con similitudes con la arquitectura MPTCP y la capacidad *multihoming* de SCTP, SLM hace uso de una entidad de sesión para llevar a cabo el control de conexión entre la capa de aplicación y la de red.

13.5. Provisión de movilidad en la capa de aplicación

A pesar de las numerosas soluciones hasta aquí planteadas, ninguna de ellas resulta definitiva de cara a la gestión completa de la movilidad. En esta línea, seguidamente se describen otras tecnologías alternativas, en este caso implementadas en la capa de aplicación, esto es, centradas en el usuario final.

13.5.1. Movilidad basada en DNS: DDNS

Las entidades en Internet a nivel de aplicación se dirigen mediante su nombre de dominio o FQDN («Fully Qualified Domain Name»), directamente relacionado con el servicio DNS (véase Capítulo 10). DNS implementa una base de datos distribuida y jerárquica para asociar FQDN a direcciones IP, en la cual se definen diferentes registros (RR). Uno de ellos es el de tipo A, para asociar FQDN a direcciones IP; por ejemplo, host.ugra.com A 160.204.251.13. De modo similar, existen los registros PTR para la resolución inversa; por ejemplo, 78.12.225.139 PTR www4.demas.org.

Aunque DNS fue ideado originalmente para la definición estática de asociaciones dirección IP-FQDN, revisiones posteriores (ver RFC 2136) permiten actualizaciones dinámicas de dichas asociaciones. Es el conocido como DNS dinámico, o DDNS («Dynamic DNS»). Este hecho se posibilita través de DHCP como se observa en la Figura 13.15, de acuerdo con el RFC 4702:

- El cliente DHCP emite un mensaje *Request* con su FQDN, la opción 81 y el bit S a valor 0, indicando con ello que desea actualizar su registro A.
- El servidor responde con un mensaje de confirmación *Ack* con el bit S a valor 0, indicando que el servidor DNS acepta el cambio.
- Finalmente, el cliente DHCP envía un mensaje DNS *Update* para completar el procedimiento.

El problema de abordar la movilidad con DDNS es que actualizaciones dinámicas de un nodo involucrado en la comunicación de una aplicación dada provocarán que dicha aplicación falle. En consecuencia, el uso de DDNS se aconseja para entornos con movilidad reducida.

13.5.2. Movilidad mediante SIP

El protocolo SIP («Session Initiation Protocol»), definido inicialmente en el RFC 3261, es un protocolo de aplicación que proporciona señalización para la creación, finalización y modificación de sesiones. Quizás su uso más conocido sea en el servicio VoIP («Voice over IP»).

El establecimiento de los parámetros concretos de una sesión entre dos extremos SIP se lleva a cabo con el protocolo SDP («Session Description Protocol»), embebido en los mensajes SIP. Los datos

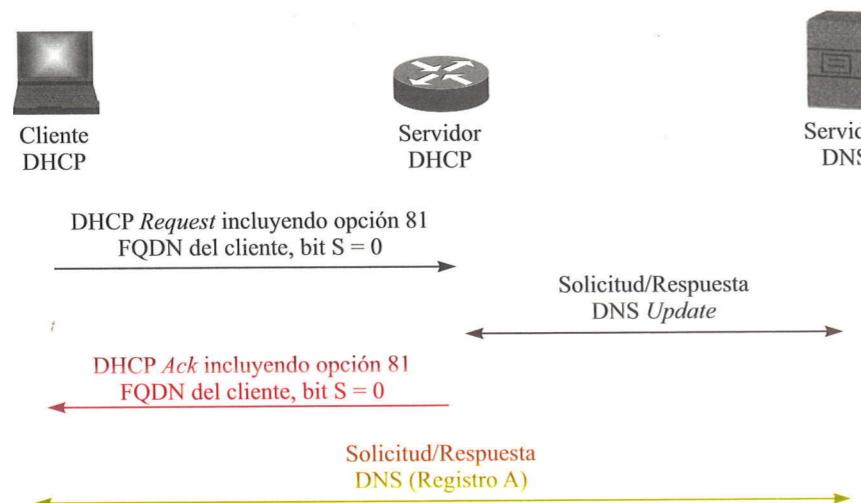


Figura 13.15. Actualización DNS dinámica.

se suelen transmitir mediante RTP («Real Time Protocol»). La funcionalidad SIP se puede resumir en las siguientes tres capacidades:

1. El *direcccionamiento SIP* se basa en el empleo del identificador uniforme de recursos (URI, «Uniform Resource Identifier») SIP. Este tiene la forma *sip:username@host*, donde *username* puede ser un nombre de usuario o de máquina, o una dirección de teléfono. Por su parte, *host* puede ser un nombre de dominio o una dirección de red numérica, como una dirección IP.
2. SIP proporciona un servicio de *registro* que permite asociar una o más direcciones IP a un URI SIP.
3. A través de SIP se posibilita el *control de sesiones*, permitiendo a otro usuario a participar en una sesión dada, modificar esta o terminarla.

Los elementos que componen la arquitectura SIP son (Figura 13.16):

- Agente usuario: el inicio de una sesión se sustenta en un procedimiento cliente-servidor, donde el cliente, UAC («User Agent Client»), envía solicitudes SIP y el servidor, UAS («User Agent Server»), las responde.
- Servidor proxy: el servidor proxy hace de *router* de señalización para los mensajes SIP, recibiendo mensajes SIP de un agente usuario o de otro proxy y encaminándolos hacia el destino.
- Registrador: este elemento acepta registros de usuarios SIP, los cuales son usados para establecer la accesibilidad de un URI SIP, asociándolo a una o más direcciones IP.
- Servidor de redirección: una sesión de cliente puede ser redirigida a otro URI SIP, posibilitando la diversificación de llamadas. El servidor de redirección no retransmite los mensajes a su nueva localización, sino que informa a la entidad origen acerca de ella.
- Servidor de localización: este elemento mantiene una base de datos con la localización de los agentes usuario registrados.

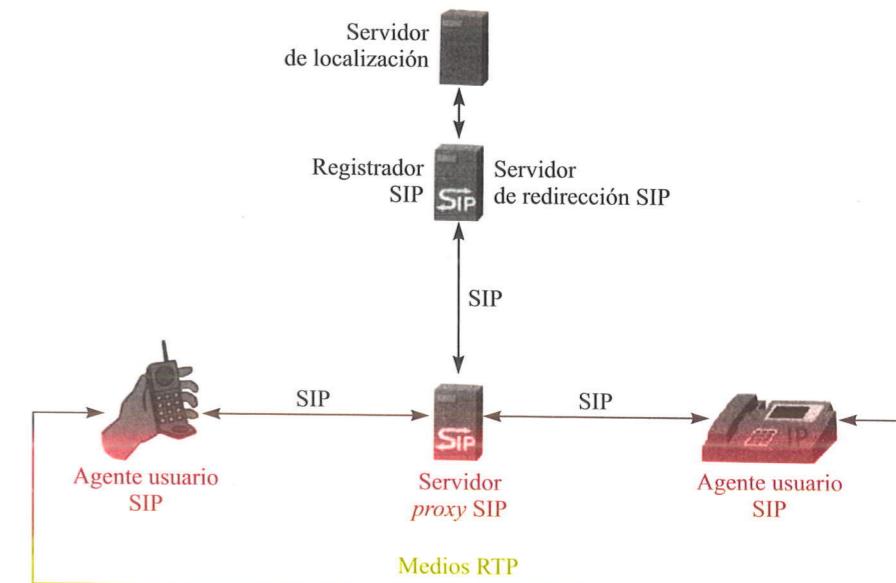


Figura 13.16. Elementos de la arquitectura SIP.

Métodos SIP y formato de mensajes

SIP define seis métodos básicos para el control de llamadas. Estos se refieren a solicitudes/respuestas entre los clientes SIP (o servidores proxy) y se denominan *transacciones*:

- REGISTER, para el registro de información de contacto.
- INVITE, ACK y CANCEL, para el establecimiento de sesiones.
- BYE, para la finalización de sesiones.
- OPTIONS, para determinar las capacidades de un agente usuario SIP.

Adicionalmente a ellos, se ha establecido una serie de extensiones SIP (véase RFC 5411):

- PRACK, para la señalización de confirmaciones provisionales.
- SUBSCRIBE/NOTIFY, para la notificación de eventos a un agente usuario.
- UPDATE, para la modificación de sesiones.
- REFER, para la transferencia de sesiones.
- MESSAGE, para mensajería instantánea.

Al igual que el protocolo HTTP, los mensajes de solicitud SIP comienzan por una *línea de solicitud* y los de respuesta por una *línea de estado*. Ambas líneas están seguidas por campos de cabecera idénticos para solicitudes y respuestas. Ejemplos respectivos de ambos tipos de línea son:

```
INVITE sip:pedro@madan.org SIP/2.0
SIP/2.0 180 ringing
```

donde SIP/2.0 es la versión del protocolo, y 180 y ringing indican el estado de la transacción en formato numérico y texto (legible por una persona), respectivamente.

En cuanto a los campos de cabecera, el RFC 3261 define seis obligatorios:

- *To*: destino de la solicitud de transacción.
- *From*: origen de la solicitud de transacción.
- *Cseq*: número de secuencia y nombre de método.
- *Call-ID*: identificador único para el intercambio de mensaje SIP.
- *Max-forwards*: número máximo de retransmisiones permitidas para el mensaje SIP, de manera que cada vez que un proxy reenvía el mensaje decrementa este valor, siendo descartado el mensaje si se alcanza el valor 0.
- *Via*: para encaminamiento simétrico de los mensajes SIP, un proxy SIP hace uso de esta cabecera en el mensaje de solicitud para asegurar que también gestionará la respuesta.

Tras los campos de cabecera, existe una línea en blanco seguida del cuerpo del mensaje SIP. Como se ha señalado al principio de este subapartado, uno de los tipos de mensaje más usuales se refiere a los mensajes SDP.

Movilidad básica SIP

La provisión de movilidad precisa de tres servicios básicos: registro, autenticación y *rendez-vous* (asociación dirección IP-identificador de aplicación). En la primera fase, registro (Figura 13.17(a)), se realiza el registro del usuario en la red. Tras ello se lleva a cabo su autenticación, la cual es de tipo reto-respuesta y se conoce como *digest authentication* (Figura 13.17(b)). Finalmente se lleva a cabo el inicio de una sesión entre dos usuarios a través del método INVITE (el cual contiene una oferta SDP), se intercambian los datos deseados (mediante RTP) y se termina la sesión con BYE (Figura 13.17(c)).

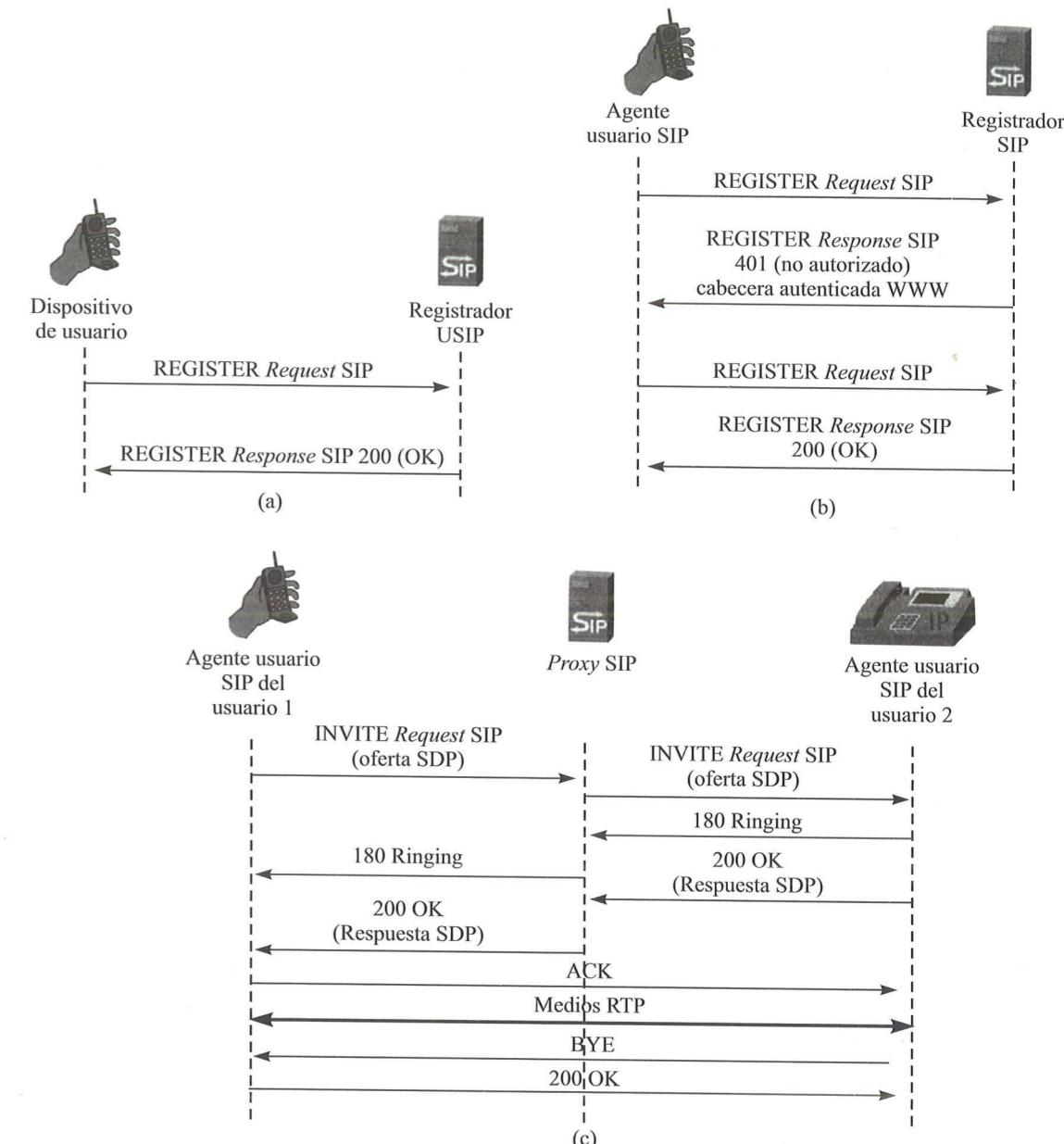


Figura 13.17. Procesos SIP de registro (a), autenticación (b) y rendez-vous (c).

Teniendo lo anterior presente, seguidamente se muestra cómo puede proporcionarse movilidad mediante SIP. El procedimiento es como sigue, para una sesión ya establecida entre dos usuarios (Figura 13.18):

1. En un momento dado, uno de los usuarios cambia de la localización #1 a una nueva #2.
2. En tal caso, dicho usuario procederá a registrar su nueva dirección IP con el registrador SIP.

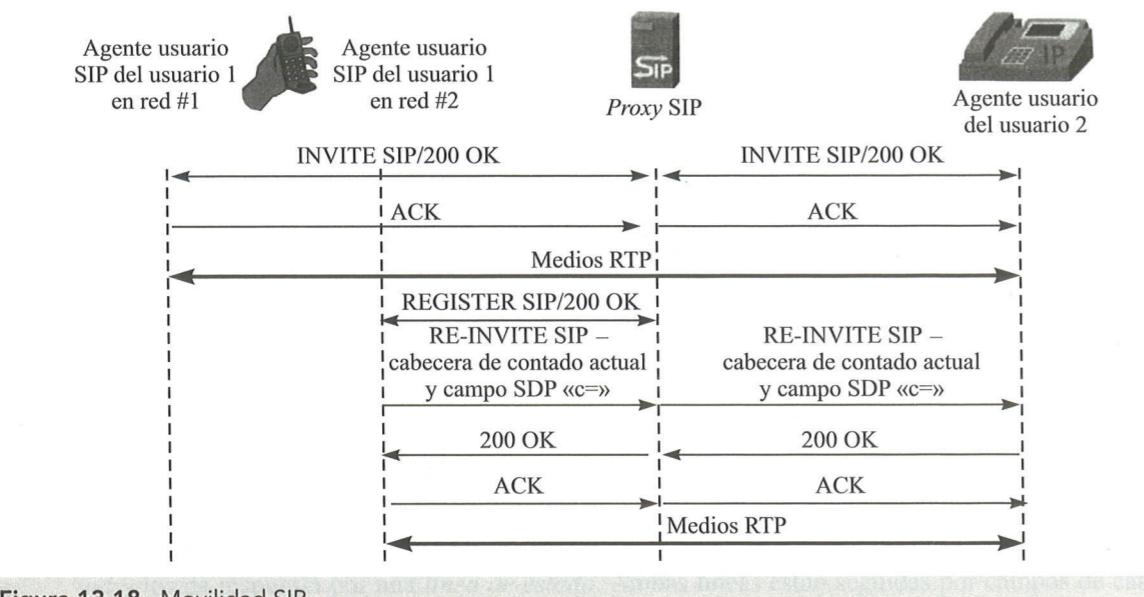


Figura 13.18. Movilidad SIP.

- Hecho ello, enviará un mensaje RE-INVITE al URI SIP del otro extremo, donde indica el *Call-ID* de la llamada original pero con la nueva dirección IP.

Los procesos involucrados, y que tendrán impacto, en la gestión de la movilidad son:

- Adquisición de la nueva dirección IP.
- Indicación de este cambio.
- Registro SIP.
- Señalización SIP.
- Actualización.

Movilidad SIP centrada en el usuario

Las soluciones de movilidad vistas hasta el momento están centradas en los dispositivos más que en el usuario en sí. Sin embargo, se prevé que esta visión debe cambiar en el futuro. Según diversos estudios, se estima que al final de esta década cada usuario disponga de una media de seis dispositivos conectados a Internet de forma simultánea⁴.

La movilidad a nivel de aplicación es adecuada para permitir la movilidad entre dispositivos. Pensemos, por ejemplo, un usuario que inicia una sesión multimedia en el ordenador personal de su hogar pero que a lo largo de su desarrollo decide abandonar la casa y continuar la sesión sobre un dispositivo móvil. SIP permite transferir esta sesión entre ambos dispositivos mediante dos procedimientos alternativos:

- **REFER SIP:** La extensión REFER de SIP (RFC 3515) permite hacer una transferencia de llamada, tal como se observa en la Figura 13.19. En ella se puede ver cómo el dispositivo 1

⁴ Este es también el origen de un nuevo paradigma de comunicaciones denominado *Internet de las cosas* («Internet of Things», IoT), consistente en la interconexión de objetos cotidianos de todo tipo para dar lugar a un mundo totalmente interoperable. No obstante la relevancia creciente de este campo, planteamos aquí su mera referencia y posponemos su estudio a cursos más avanzados.

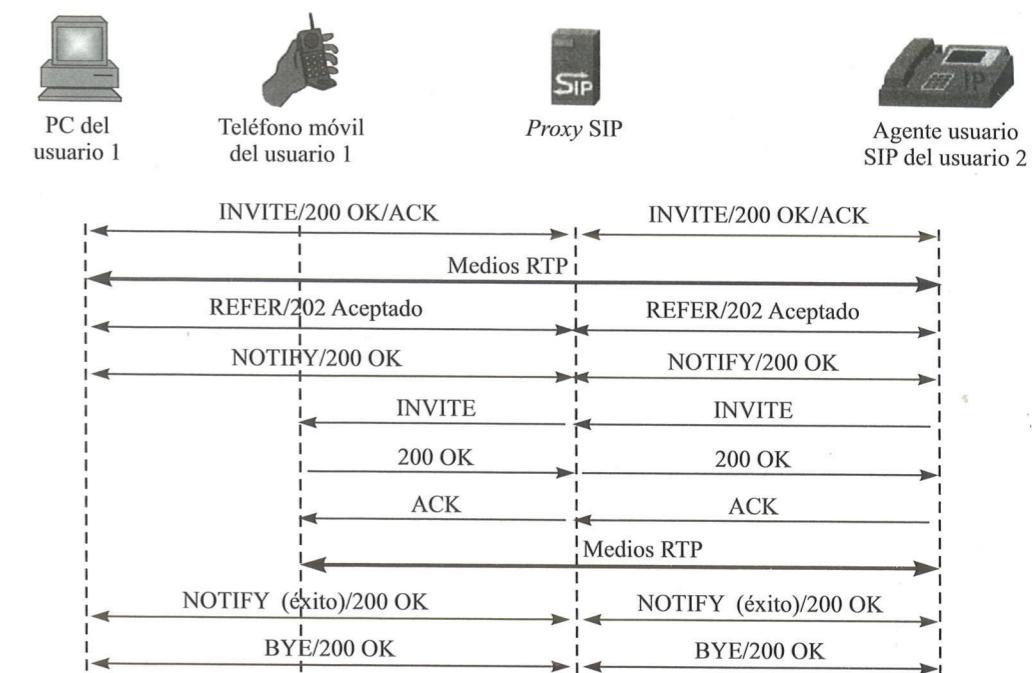


Figura 13.19. Movilidad SIP con REFER.

(PC) envía un método REFER para notificar al otro usuario el nuevo punto de contacto (teléfono móvil).

- Tras ello se establecerá la nueva sesión, lo que implica los métodos INVITE y NOTIFY, cuyo éxito del proceso se notificará oportunamente (NOTIFY) al dispositivo origen.
- **Third-Party Call Control (3PCC):** En la aproximación 3PCC (RFC 3725) se incluye una nueva entidad en la arquitectura SIP: B2BUA («Back-to-Back User Agent»). Como se observa en la Figura 13.20, es este nuevo elemento quien gestiona toda la señalización entre las partes para posibilitar la transferencia de la sesión entre los dispositivos.

Establecidas sendas sesiones SIP con cada uno de los usuarios finales, B2BUA puede llevar a cabo la transferencia de la sesión enviando al otro extremo un RE-INVITE, cuya respuesta retransmite al usuario que desea la transferencia. Una vez aceptado el cambio por las partes, la transferencia de información puede continuar.

Concluimos la descripción de 3PCC indicando que 3GPP ha definido una mejora, denominada *Continuidad de Sesión*, donde se establecen nuevos roles.

Aunque fuera del objetivo de este capítulo, queremos finalizar esta breve introducción realizada al tema de la movilidad de los usuarios mencionando el estudio actual de otras propuestas que van más allá de las capas de la red. En ellas se trata de independizar la localización del usuario para el encañamiento del identificador del extremo final. Es lo que se conoce como LIS («Locator-Identifier Separation»), aproximación que se encuentra actualmente en estudio en el marco del grupo de investigación en routing (RRG, «Routing Research Group») de la IRTF («Internet Research Task Force»). Solo por mencionarlas, algunas de estas soluciones son HIP («Host Identity Protocol»), LISP-MN («Locator-Identifier Separation Protocol-Mobile Node»), NAT66 («Network Address Translation for IPv6 to IPv6») e ILNP («Identifier-Locator Network Protocol»).

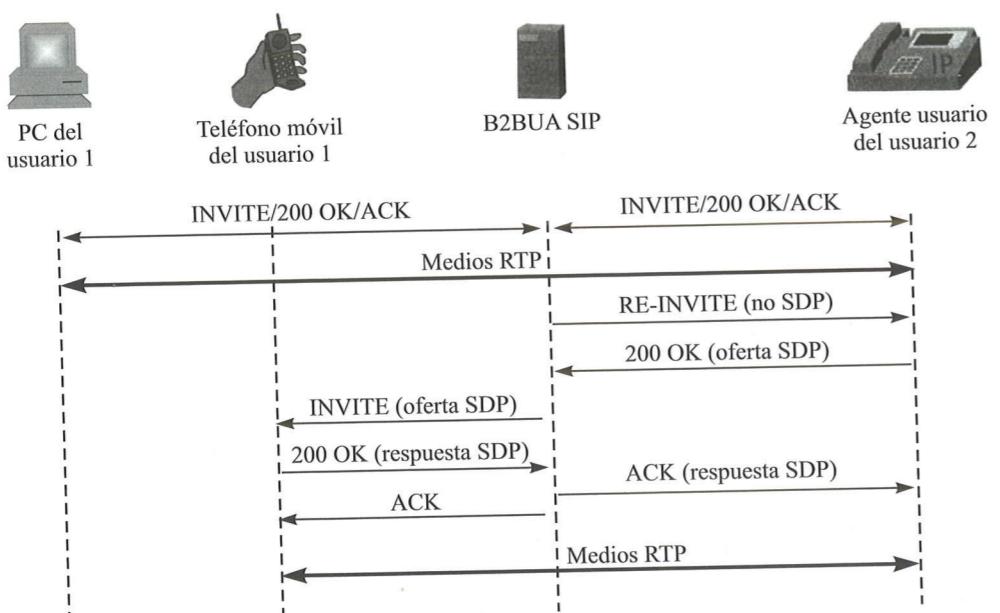


Figura 13.20. Movilidad SIP mediante 3PCC.

RESUMEN

Si bien la amplitud de aspectos tratados a lo largo del texto puede parecer elevada, los campos aún por discutir al respecto de las redes de comunicación son numerosos y, qué duda cabe, de creciente importancia en el despliegue de nuevos sistemas y servicios. Como simple evidencia de ello, en este último tema del libro hemos querido plantear un breve estudio acerca de la posibilidad de movilidad de los usuarios finales en los nuevos entornos de comunicaciones, lo cual constituye una temática de elevado interés debido a la creciente implantación y penetración de nuevas tecnologías como UMTS/4G, WiMAX, etc.

En este marco, se ha discutido la provisión de movilidad desde la perspectiva de las distintas capas en las que puede plantearse la solución. Así, en la capa 2, de enlace, hemos hecho mención a ciertas capacidades del protocolo DHCP en esta línea, así como los esquemas IAPP y CAPWAP para entornos inalámbricos.

En cuanto a la capa de red, se ha introducido el protocolo IP móvil (MIP) tanto en la versión 4 como en la versión 6 de IP. En ambos casos nos hemos referido a la disposición de dispositivos agente locales, los cuales permiten la redirección de la información recibida en la red base hacia la red remota donde se encuentra ubicado el nodo móvil en un momento dado. Además, en el caso de MIPv4 hemos evidenciado el uso habitual de túneles inversos para solventar políticas de filtrado de paquetes.

Por lo que respecta a la provisión de movilidad en la capa de transporte, se han discutido los protocolos SCTP, MPTCP y MSOCKS. A pesar de su posible uso en la línea deseada, ninguno de ellos constituye una solución definitiva al problema de la movilidad del usuario.

Frente a todas las soluciones anteriores, seguidamente se han presentado alternativas situadas en la capa de aplicación. En concreto, dos han sido estas: DNS dinámico y SIP móvil. Frente a todas las anteriores, la ventaja de estas propuestas radica en la posible transferencia dinámica de sesiones entre dispositivos.

EJERCICIOS

1. ¿Cuáles son los pros y los contras de proveer de movilidad en las capas altas de la red frente a las bajas?
2. Discuta los problemas que plantea el uso de DHCP para proveer de capacidad de movilidad al usuario final.
3. ¿Cuáles son las ventajas introducidas por CAPWAP para la gestión de la movilidad de un usuario final?
4. ¿Por qué es necesario el empleo de túnel inverso en MIPv4? ¿Y por qué no lo es en MIPv6?
5. Consulte algunos de los RFC mencionados en el capítulo para explicar por qué podemos obviar el empleo de FA en MIPv6.
6. Compare SCTP y MPTCP en cuanto a la capacidad de cada uno de ellos para la provisión de movilidad a nivel de transporte.
7. Explique la arquitectura funcional de TLM y los procedimientos que afectan a la gestión de la movilidad.
8. Explique cómo funciona DNS dinámico y cuáles son sus limitaciones en la provisión real de movilidad a los usuarios.
9. Describa cómo se proporciona movilidad básica haciendo uso de SIP.
10. Como se ha comentado en el texto, 3GPP ha planteado una solución avanzada en relación a 3PCC SIP. Visite el enlace <http://www.3gpp.org/DynaReport/23237.htm> y discuta esta nueva aproximación en sus líneas generales.
11. Frente a las soluciones planteadas en la capa de aplicación, existen aplicaciones en las que se obvia la movilidad en sí. En ellas, independientemente de si se produce pérdida de conexión o cambio de dirección IP, se abren y cierran conexiones TCP para garantizar la continuidad del flujo de datos. Un ejemplo de ello es el servicio de vídeo streaming. ¿Qué ventajas o inconvenientes plantea esta filosofía de funcionamiento frente a la consideración y desarrollo de soluciones específicas para la gestión de movilidad?

BIBLIOGRAFÍA

- Deering, S.: *ICMP Router Discovery Messages*. RFC 1256. Septiembre, 1991.
- Ford, A.; Raiciu, C.; Handley, M.; Bonaventure, O.: *TCP Extensions for Multipath Operation with Multiple Addresses*. RFC 6824. Enero, 2013.
- Grayson, M.; Shatzkamer, K.; Wierenga, K.: *Building the Mobile Internet*. Cisco Press, 2011.
- Johnson, D.; Perkins, C.; Arkko, J.: *Mobility Support in IPv6*. RFC 3775. Junio, 2004.
- Maltz, D. A.; Bhagwat, P.: *MSOCKS: An Architecture for Transport Layer Mobility*. Disponible en http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=662913&tag=1.
- Narten, T.; Nordmark, E.; Simpson, W.: *Neighbor Discovery for IP Version 6 (IPv6)*. RFC 2461. Diciembre, 1998.
- O'Hara, B.; Calhoun, P.; Kempf, J.: *Configuration and Provisioning for Wireless Access Points (CAPWAP). Problem Statement*. RFC 3990. Febrero, 2005.
- Perkins, C.: *IP Mobility Support*. RFC 2002. Octubre, 1996.
- Perkins, C.: *IP Mobility Support for IPv4*. RFC 3220. Enero, 2002.
- Perkins, C.: *IP Mobility Support for IPv4*. RFC 3344. Agosto, 2002.
- Perkins, C.: *IP Mobility Support for IPv4, Revised*. RFC 5944. Noviembre, 2010.
- Perkins, C.; Johnson, D.; Arkko, J.: *Mobility Support in IPv6*. RFC 6275. Julio, 2011.