

## TABLA DE CONTENIDO

	<b>Pág</b>
<b>ANEXO B</b>	<b>1</b>
B-1. INTERFAZ RED A RED PARA IMT – 2000	1
B-1.1. INTRODUCCIÓN	1
B-1.2. REQUISITOS GENERALES	2
B-1.2.1. Requisitos de la interfaz red-red (NNI)	2
B-1.2.2. Capacidades de servicio	2
B- 1.2.3. Requisitos de almacenamiento de datos de CN para el perfil de abonado (usuario)	3
B-1.2.4. Requisitos de itinerancia global	4
<b>B-1.2.5. Agrupaciones de comunicaciones NNI</b>	<b>5</b>
B-1.2.6. Requisitos de seguridad	5
B-1.3. Modelo de interconexión	8
B-1.4. Interfaz funcional NNI	9
B-1.4.1. Modelo funcional	9
<b>B-1.4.2. Puntos de referencia</b>	<b>11</b>
<b>B-1.5. Requisitos de protocolo para la gestión de la movilidad</b>	<b>15</b>
B-1.5.1. Activadores del servicio	15
B-1.5.2. Modos de interacción de la lógica de servicio	16
B-1.5.3. Comunicaciones funcionales de la gestión de la movilidad	16
B-1.5.4. Comunicaciones funcionales de control de servicio	17

<b>B-1.6. Requisitos de protocolo para el control de llamada y de portador</b>	<b>19</b>
B-1.6.1. Requisitos generales	19
B-1.6.2. Elección de los principios de conmutación	20
B-1.6.3. Comunicaciones funcionales del control de llamada y de portador	20
B-1.7. Requisitos de protocolo para el control del servicio de paquetes	22
<b>B-1.7.1. El protocolo de interfaz PSCF A PSGCF</b>	<b>23</b>
B-1.7.2. El protocolo de interfaz LMFp a LMFp	26
<b>B-1.7.2. Definiciones</b>	<b>28</b>
<b>B-1.7.3. Abreviaturas</b>	<b>29</b>

## LISTA DE FIGURAS

	Pag.
Figura B-1 – Modelo de interconexión de redes IMT-2000	5
Figura B-2– Agrupación de comunicaciones NNI	6
Figura B-3– Modelo de interconexión de red IMT-2000	9
Figura B-4– Modelo de interfaz funcional NNI	10
Figura B-5 – Modelo funcional (gestión de la movilidad) de IMT-2000	17
Figura B-6 – Modelo funcional (control de servicio) de IMT-2000	18
Figura B-7 – Modelo funcional de IMT-2000	21
Figura B-8 – Modelo funcional de IMT-2000	22
Figura B-9– Interfaces red-red de datos por paquetes	23

## LISTA DE TABLAS

	<b>Pag.</b>
Tabla B-1. Elección de la sucesión de protocolos	19

## ANEXO B

### B-1. INTERFAZ RED A RED PARA IMT – 2000

#### B-1.1. INTRODUCCIÓN

Como ya se ha explicado, existen varios protocolos de movilidad para sistemas 2G, los dos más importantes o empleados a nivel mundial son el GSM MAP e IS-41. Estos protocolos han sido concebidos y optimizados específicamente para capacidades de servicio y sistemas 2G. Sin embargo, el principal inconveniente que presentan estos protocolos es que no pueden soportar fácilmente la comunicación entre familias por su naturaleza y diseño específicos, esto significa que la sintaxis y la semántica de los argumentos y los resultados de éstas operaciones de gestión de la movilidad están fuertemente asociadas con la arquitectura y servicios de segunda generación.

Se entiende entonces, que los protocolos de señalización deben mejorarse para soportar la itinerancia interfamilias entre los diferentes miembros de sistemas IMT-2000. Por consiguiente, el desafío de realizar un protocolo NNI (Network to Network Interface - Interfaz Red a Red) común para la gestión de la movilidad que sea válido para la itinerancia interfamilias depende principalmente de la creación de elementos de protocolo que no deben quedar restringidos a un servicio móvil particular y a una tecnología de acceso radioeléctrico. En otras palabras, debe ser lo suficientemente genérico para adecuarse a los diferentes miembros/sistemas de IMT-2000. Un modo de progresar en esta dirección es obtener operaciones genéricas basadas en parámetros comunes para servicios IMT-2000 que serán utilizadas por estos diferentes miembros. Debe prestarse también atención a conseguir que el trayecto que siga la evolución desde los sistemas 2G existentes a la NNI común 3G sea lo más suave posible con el fin de prevenir un impacto negativo en las actuales redes y servicios, además de minimizar el riesgo económico y financiero para usuarios y operadores.

En éste anexo se presenta la propuesta de la interfaz red-red hecha por la UIT (Unión Internacional de Telecomunicaciones) y que es requerida para la comunicaciones de tercera generación en el entorno de IMT-2000. Se han tomado como base las recomendaciones UIT-T Q.1701 (*Marco para las redes de las telecomunicaciones móviles internacionales - 2000*), Q.1711 (*Modelo funcional de red para las telecomunicaciones internacionales - 2000*), Q.1721 (*Flujos de información para el*

*conjunto de capacidades 1 del IMT-2000) y Q.1751 (Requisitos de la señalización entre redes para el conjunto de capacidades 1 de las telecomunicaciones móviles internacionales-2000).*

La UIT es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT el cual estudia los aspectos técnicos, de explotación, tarificación y publica las recomendaciones pertinentes sobre los mismos, con miras a la normalización de las telecomunicaciones a nivel mundial.

## **B-1.2. REQUISITOS GENERALES**

### **B-1.2.1. Requisitos de la interfaz red-red (NNI)**

La interfaz red-red (NNI) deberá soportar el conjunto de características y capacidades de red/servicio CS-1 de IMT-2000 que aseguran la compatibilidad hacia atrás con los sistemas de la segunda generación. Los requisitos generales son:

- 1) La NNI debe suministrar una indagación o encaminamiento óptimo, por ejemplo, para evitar el efecto "trombón"<sup>1</sup>.
- 2) La NNI debe soportar la transferencia de registros de detalles de las llamadas (CDR, *call detail record*) como las etiquetas de referencia de las llamadas, los datos de tarificación, el aviso de tasación y otras informaciones CDR necesarias para temas de reglamentación.
- 3) La NNI debe soportar servicios de mensajería (por ejemplo: notificación de correo vocales, ADDS).

---

<sup>1</sup> En sistemas de segunda generación, el efecto "trombón" hace que una llamada terminada móvil sea encaminada hacia atrás al sistema doméstico del abonado móvil llamado, incluso si la parte llamada se encuentra en la vecindad de la parte llamante. En especial en un situación de itinerancia global, sería muy beneficioso evitar el efecto trombón, con lo que se impediría el despilfarro de recursos troncales de larga distancia.

### **B-1.2.2. Capacidades de servicio**

**Tarificación:** Los procedimientos de tarificación se utilizan para proporcionar la documentación de la llamada y la duración de la llamada.

**Gestión de red:** Los procedimientos de gestión de red dan protección a la red originaria contra la sobrecarga.

**Interacción del llamante y tratamiento de los recursos especializados:** Procedimientos que tienen en cuenta la puesta en marcha de anuncios, avisos y recogida de información posmarcación procedente del usuario (por ejemplo, PIN para llamadas con tarjeta de crédito).

**Asistencia y traspaso:** Procedimientos que permiten solicitar asistencia a un equipo exterior (por ejemplo, IP) para poner en marcha anuncios, avisos y recogida de información.

### **B- 1.2.3. Requisitos de almacenamiento de datos de CN para el perfil de abonado (usuario)**

En el entorno IMT-2000 se hará necesario almacenar los siguientes elementos de información en la red originaria del abonado, así como el sujeto de la información de abonado y las actividades de gestión del perfil para tener la capacidad de prestar servicios con itinerancia global:

- Número de directorio móvil IMT-2000 (IMDN, *IMT-2000 mobile directory number*), por ejemplo, un número "marcable"
- ID de usuario móvil IMT-2000 (IMUI, *IMT-2000 mobile user ID*)
- ID de usuario móvil temporal IMT-2000 (*TMUI, IMT-2000 temporary mobile user ID*)
- Estado del terminal
- Información de posición del usuario/terminal
- Datos de servicios básicos (por ejemplo, servicios portadores del abonado)
- Teleservicios (por ejemplo, difusión y datos de suscripción de llamada a grupos)
- Datos de servicios suplementarios
- Características/servicios determinados por el operador (por ejemplo, datos de prohibición de llamadas)

- Características/servicios determinados por el abonado (por ejemplo, datos de selección de llamadas)
- Datos de restricción de la itinerancia
- Datos de abono regional
- Datos de abono VHE

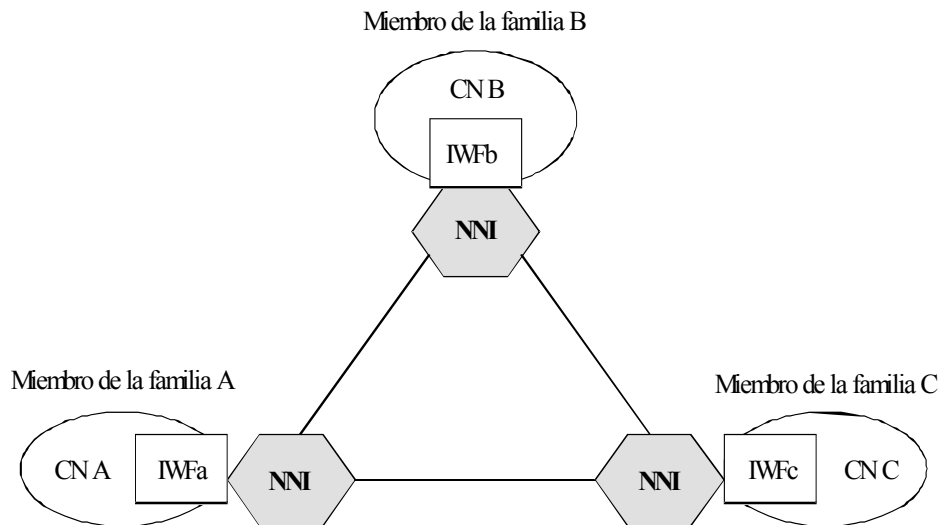
#### **B-1.2.4. Requisitos de itinerancia global**

La interfaz red-red (NNI) es un protocolo común y único de interfaz red central a red central que soporta la capacidad de itinerancia global para IMT-2000 y proporciona un entorno de servicio originario a los usuarios itinerantes a lo largo de dos o más redes miembros de la familia IMT-2000. En la figura B-1 se representa la función esperada para la NNI común, junto con varias IWF de miembros de la familia, para facilitar la interoperabilidad entre las redes y soportar la itinerancia global mediante la provisión de un entorno de servicio originario a los usuarios itinerantes. La implementación de la interoperabilidad y la configuración de itinerancia global que se muestra en la figura B-1 tiene las siguientes características diferentes con respecto a la implementación de funciones IWF para cada pareja de redes medulares.

- **Interfaz abierta:** Solamente habrá una NNI común y única (actualmente se encuentra en desarrollo en el UIT-T).
- **Eficacia:** Se necesita una única función IWF (en contraposición a N-1 IWF bilaterales) por miembro de familia para una familia IMT-2000 de N miembros. Esto es válido para que cada miembro de la familia pueda interfuncionar con los demás miembros de la misma.
- **Transparencia:** Los cambios en las especificaciones de red de un miembro de la familia no afectarán a las funciones IWF de otros miembros.
- **Prueba de futuro:** Se pueden acomodar fácilmente nuevos miembros dentro de la familia.

Se debe tener en cuenta que el desarrollo del protocolo NNI corresponde al UIT-T, mientras que el desarrollo de la IWF es competencia de cada miembro de la familia.





**Figura B-1 – Modelo de interconexión de redes IMT-2000**

#### **B-1.2.5. Agrupaciones de comunicaciones NNI**

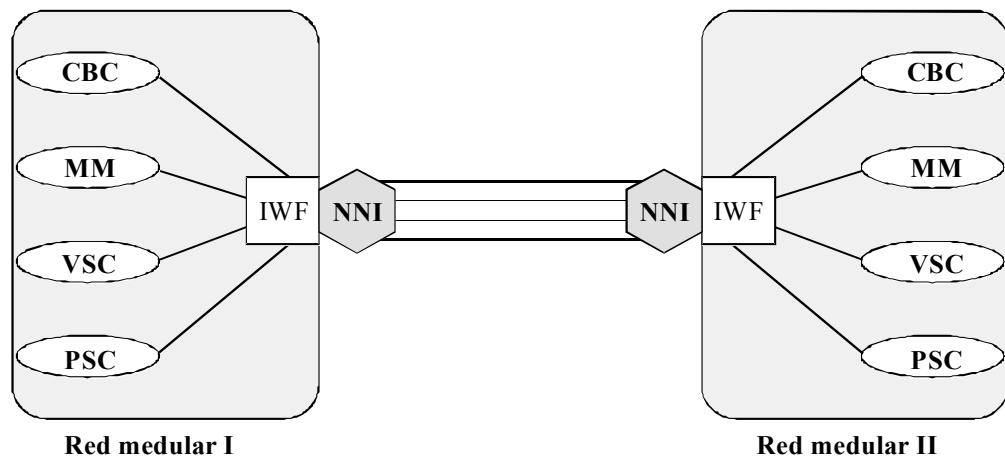
Se reconocen cuatro agrupaciones principales y distintas de comunicaciones en operaciones de CN transversales IMT-2000. La distinción se deriva de la naturaleza de las operaciones que ellas soportan mediante la constitución de un protocolo de aplicación NNI único y común. Estos grupos de comunicaciones son:

- **Control de llamada y de portador (CBC):** Esta agrupación de comunicaciones incluye todos los intercambios de información CN transversales relacionados con el control de los servicios con conexión y servicios sin conexión, incluidos los servicios básicos y los servicios suplementarios estándar.
- **Gestión de la movilidad (MM):** Esta agrupación de comunicaciones incluye todos los intercambios de información CN transversales relativos a la gestión de la movilidad (por ejemplo, registro, autenticación y gestión de información de posición).

- **Control de servicio VHE (VSC):** Esta agrupación de comunicaciones incluye todos los intercambios de información CN transversales relativos al control de los servicios de red originaria accesibles desde las redes visitadas.

- **Control de servicio por paquetes (PSC):** Incluye todos los intercambios de información CN transversales relativos al control de los servicios por paquetes (por ejemplo, voz, imagen y datos).

Los requisitos para la seguridad entre redes se describen a alto nivel y su funcionalidad se incorpora en los protocolos de grupo de comunicaciones aplicables. A continuación se ilustran las agrupaciones de comunicaciones y el protocolo red a red común.



**Figura B-2– Agrupación de comunicaciones NNI**

Para establecer una comunicación y/o transportar un servicio sobre un protocolo que interconecta dos redes medulares, deberán establecerse una o más de estas agrupaciones de comunicaciones, directa o indirectamente, entre dos o más redes medulares. El esquema de interconexiones para transportar las comunicaciones requeridas sigue el modelo de interconectividad de redes IMT-2000 de la cláusula 1.3 que se ilustra en la figura B-3.

#### **B-1.2.6. Requisitos de seguridad**

La NNI es el punto de interfaz de una red medular del sistema IMT-2000 con otras redes centrales. La NNI interactúa con otras redes para proporcionar comunicaciones de extremo a extremo entre

usuarios (véase la figura B-1). La NNI transportará información sobre los usuarios (por ejemplo, posición, autorización, autenticación y claves de encriptación) y las redes (es decir, señalización y control); esta información debe guardarse protegida contra los intrusos.

Los requisitos de seguridad para la NNI pueden dividirse en tres partes. Requisitos de autenticación (que incluyen la privacidad), requisitos de encriptación y requisitos de gestión de claves para la NNI. Estas partes se detallan a continuación.

#### **Requisitos para el transporte de la autenticación del usuario:**

- Las normas de NNI deben concebirse para tener en cuenta la posible introducción de nuevos algoritmos de autenticación, tamaños de claves y métodos de autenticación facultativos durante la vigencia esperada de las normas.
- Los mecanismos de seguridad de la NNI deben hacer mínima la repercusión en el tráfico de red (por ejemplo, permitiendo opcionalmente la compartición de datos secretos entre la entidad originaria y la entidad sirviente).
- Los mecanismos de seguridad de NNI deben soportar puestas a prueba únicas de terminales en canales (portador y de señalización) dedicados.
- Los mecanismos de seguridad NNI deben soportar un mecanismo de puesta a prueba global, la difusión en un canal de señalización global, el requerimiento a un terminal para que responda correctamente a una puesta a prueba de red antes de que sean asignados canales dedicados.
- Los mecanismos de seguridad de NNI deben ser capaces de detectar y comunicar las violaciones de la seguridad, y disponer de mecanismos de recuperación para restablecer el sistema a un estado protegido.
- La provisión o la generación de claves de encriptación y privacidad puede formar parte del procedimiento de autenticación.
- El compromiso de un móvil individual no deberá comprometer la seguridad de la red global.

#### **Requisitos de encriptación para la interfaz red-red :**

- Los mecanismos de encriptación de la NNI deben cumplir los requisitos legales impuestos por los organismos reguladores (por ejemplo, controles de exportación, interceptación legal).

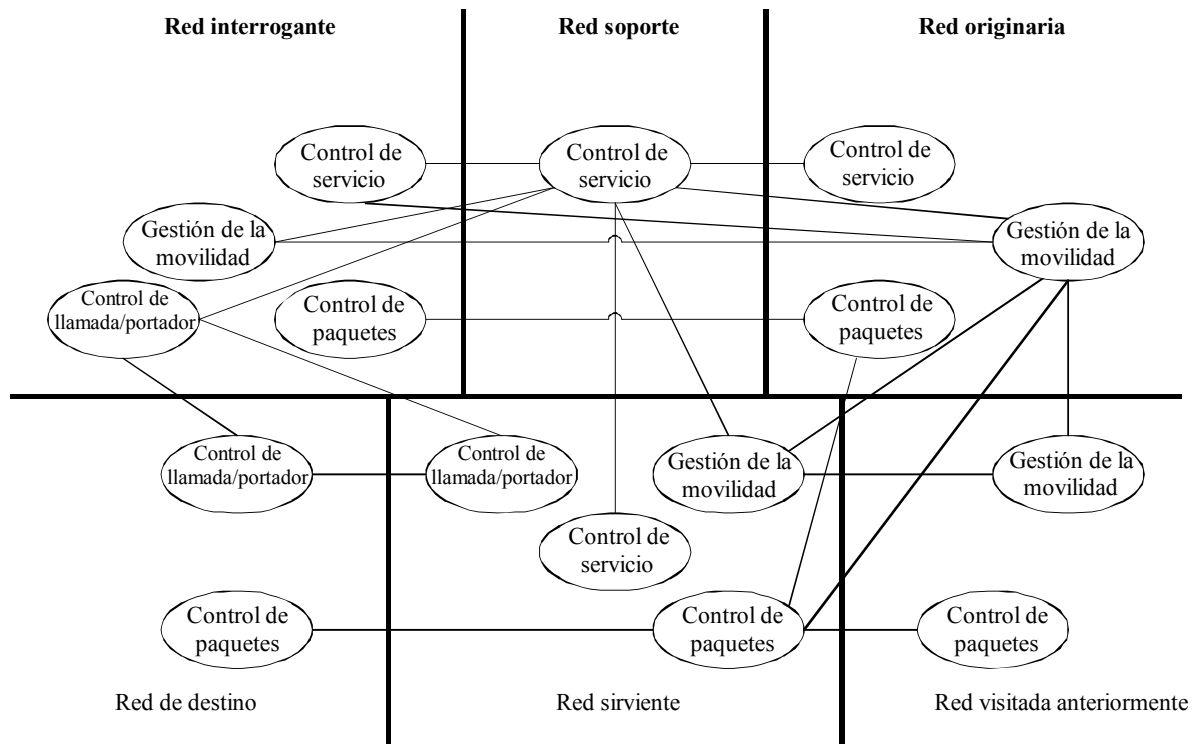
- Los mecanismos de encriptación de la NNI deben ser capaces de encriptar a velocidades de multimegabits por segundo, sin que la seguridad se vea afectada.
- La seguridad de NNI deberá poder proporcionar la autenticación mutua entre los elementos de red.

#### **Requisitos de gestión de claves para la interfaz red-red:**

- El compromiso de una clave de privacidad no debe comprometer la autenticación.
- Las claves para la privacidad de los datos pueden basarse en la misma clave raíz de autenticación.
- Los mecanismos de encriptación de la NNI deben soportar la gestión de claves relativa a la llamada, por ejemplo, la creación, distribución, modificación o revocación de claves criptográficas.
- La NNI no deberá soportar modificaciones de la clave (o claves) raíz de autenticación almacenada en un UIM y en el centro de autenticación originario (AMFh).

#### **B-1.3. Modelo de interconexión**

A continuación la figura B-3 ilustra las relaciones que habrá de tener la NNI para soportar las CS-1 IMT-2000. No se muestra la totalidad de las entidades funcionales contenidas en cada red (por ejemplo, la red originaria puede contener SCF y SDF, la red previamente visitada puede contener PSGCF) con el fin de evitar la confusión en la figura. Más bien la diferenciación al atravesar las fronteras pretende mostrar cuales son las entidades funcionales pertinentes a la función de red particular para efectos de interoperabilidad NNI. Por el mismo motivo, tampoco se muestran las relaciones intrared.



Control del servicio SCF, SDF, SRF  
 Gestión de la movilidad LMF, AMF, UIMF  
 Control de llamada y portador CCF/SSF, CnCF, SACF  
 Control de paquetes PSCF, PSGCF

**Figura B-3– Modelo de interconexión de red IMT-2000**

#### **B-1.4. Interfaz funcional NNI**

##### **B-1.4.1. Modelo funcional**

La figura B-4 muestra el "Modelo de interfaz funcional NNI". Se enfoca solamente en aquellas interfaces que pertenecen a la NNI en un nivel funcional. La figura B-3 "Modelo de interconexión de red IMT-2000" (NIM, *IMT-2000 network interconnection model*) y la figura B-4 "Modelo de interfaz funcional NNI" (FIM, *NNI functional interface model*) proporcionan juntas el marco para identificar las relaciones de señalización NNI y la base para la definición del protocolo.

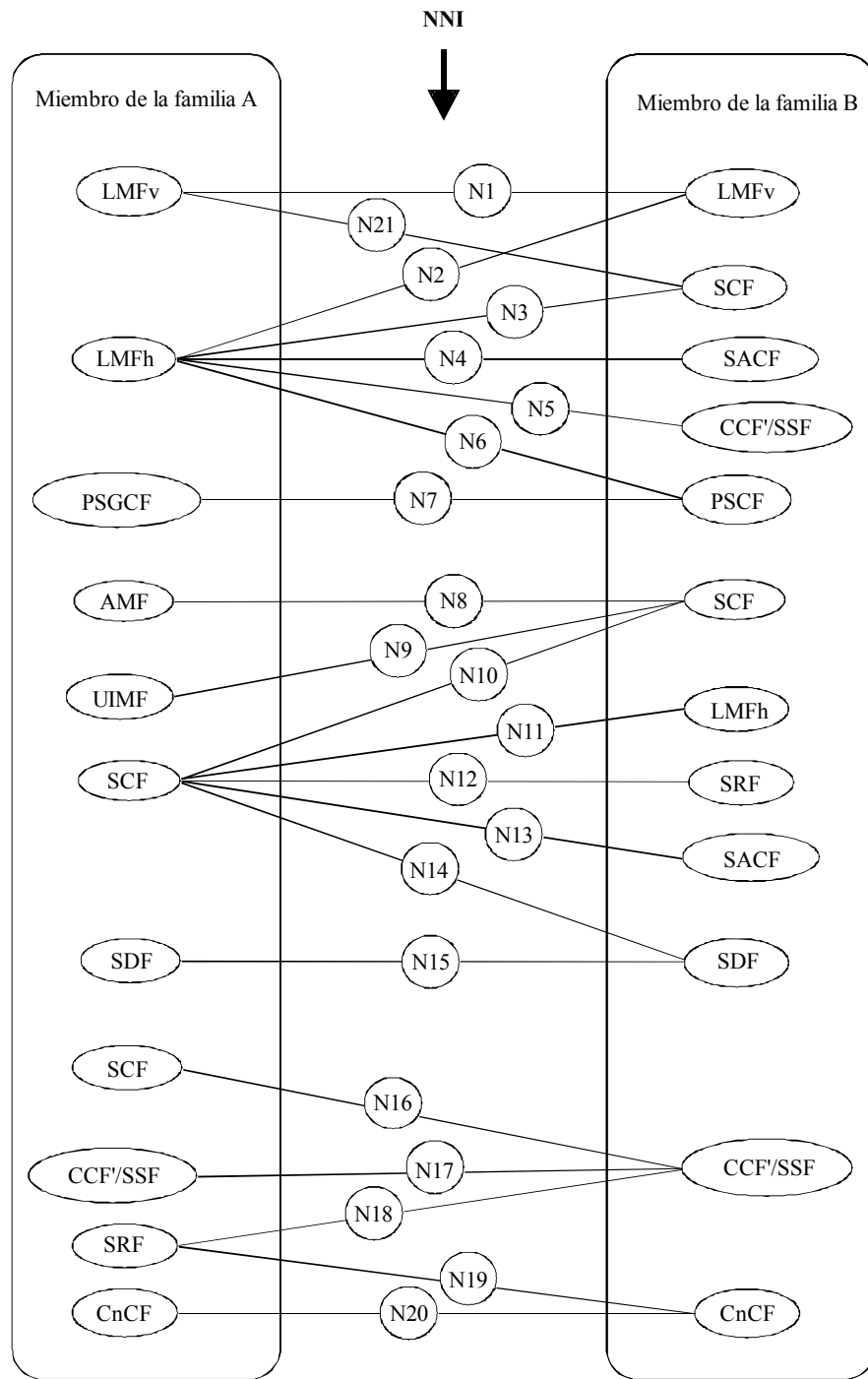


Figura B-4– Modelo de interfaz funcional NNI

### **B-1.4.2. Puntos de referencia**

Los puntos de referencia (Nxx), que se muestran en la figura B-4 se describen a continuación con ejemplos ilustrativos de la mensajería NNI (extraídos de la cláusula 5 "The IMT-2000 Functional Models – Modelos funcionales IMT-2000" de la Recomendación UIT-T Q.1711<sup>2</sup>).

Nótese que para soportar los requisitos de servicio IMT-2000 han de ampliarse los medios de identificación de los abonados para que incluyan la identificación de usuario móvil internacional (IMUI) y otras. Este requisito es general y aplicable a las interfaces de RI existentes.

**Punto de referencia N01** : Es la interfaz funcional LMFv a LMFv en cada miembro de familia. La mensajería NNI por medio de ésta interfaz funcional posibilita la gestión de la información de abonado como es la recuperación de la IMUI basada en el identificador de usuario móvil temporal (TMUI).

**Punto de referencia N02** : Es la interfaz funcional LMFh a LMFv. La mensajería NNI por esta interfaz funcional posibilita:

- El registro
- La cancelación del registro (originario a previamente visitado)
- La transferencia del perfil de servicio
- La transferencia de la información de encaminamiento para el establecimiento de las comunicaciones.
- La gestión de la información de abonado
- El control de los servicios suplementarios

**Punto de referencia N03** : Es la interfaz funcional LMFh a SCF. La mensajería NNI por medio de ésta interfaz funcional posibilita los servicios de RI relacionados con la gestión de posiciones.

**Punto de referencia N04** : Es la interfaz funcional LMFh a SACF. Por medio de ésta interfaz es posible obtener:

---

<sup>2</sup> Algunas de las relaciones no pueden ser cubiertas en la cláusula 7/Q.1711 [2], "Itinerancia global y escenarios de interfuncionamiento", debido posiblemente a que no son completas.

- La gestión de información de movilidad básica como lo es la posición, estatus e identidad del terminal móvil (MT)
- La compartición de información sobre estrategias de radiobúsqueda
- El control de los servicios suplementarios
- La entrega de mensajes, como lo son los mensajes SMS y mensajes ADDS
- La gestión de las actividades de puesta a prueba aleatoria global
- La gestión de las actividades de puesta a prueba de autenticación única

**Punto de referencia N05 :** Es la interfaz funcional LMFh a CCF'/SSF. La mensajería NNI por esta interfaz funcional hace posible:

- La transferencia de información de encaminamiento para el establecimiento de las comunicaciones
- La transferencia de información de perfil incluidas capacidades de servicio, como lo son la información de protocolo y la información de portador

**Punto de referencia N06 :** Es la interfaz funcional LMFh a PSCF. Por medio de ésta interfaz funcional se posibilita:

- El acceso y actualización de los datos referentes al abonado
- La actualización de la información del servicio por paquetes
- La actualización de la información de encaminamiento de paquetes

**Punto de referencia N07 :** Es la interfaz funcional PSGCF a PSCF. La mensajería NNI por esta interfaz funcional hace posible:

- La actualización de la información del servicio de datos por paquetes del MT
- La actualización de la asociación de contextos de encaminamiento del MT
- La transferencia de datos de usuario entre un MT y una red de paquetes

**Punto de referencia N08 :** Es la interfaz funcional AMF a SCF. Por medio de ésta interfaz funcional se hacen posible los servicios de RI relativos a la autenticación del usuario.



**Punto de referencia N09** : Es la interfaz funcional UIMF a SCF. La mensajería NNI por medio de ésta interfaz funcional posibilita:

- La transferencia de los datos/lógica del servicio
- La modificación del perfil del servicio
- El intercambio de información de aplicación

**Punto de referencia N10** : Es la interfaz funcional SCF a SCF. Esta hace posible:

- La adquisición y manipulación de datos asegurados
- El control de servicio distribuido
- Notificaciones de servicio no solicitadas

**Punto de referencia N11** : Es la interfaz funcional SCF a LMFh. Esta interfaz funcional posibilita que la LMFh proporcione la posición del MT y el estatus del abonado a la SCF.

**Punto de referencia N12** : Es la interfaz funcional SCF a SRF. La mensajería NNI por medio de ésta interfaz funcional posibilita la provisión de recursos especializados para los servicios RI.

**Punto de referencia N13** : Es la interfaz funcional SCF a SACF. Esta hace posible:

- Los servicios de RI basados en eventos de gestión de movilidad, tales como la gestión de posiciones y la autenticación del usuario
- Servicios de RI no relacionados con la llamada

**Punto de referencia N14** : Es la interfaz funcional SCF a SDF. Mediante mensajería NNI en ésta interfaz funcional se posibilita:

- Que la SDF proporcione a la SCF una visión lógica de los datos de abonado
- Que la SCF y la SDF gestionen y actualicen los datos de servicio

**Punto de referencia N15** : Es la interfaz funcional SDF a SDF. La mensajería NNI por esta interfaz funcional posibilita el intercambio de datos de servicio.

**Punto de referencia N16** : Es la interfaz funcional SCF a CCF'/SSF. Esta interfaz funcional posibilita los servicios de RI relativos a la llamada.

**Punto de referencia N17** : Es la interfaz funcional CCF'/SSF a CCF'/SSF. Esta interfaz funcional hace posible:

- La gestión de los ejemplares de llamada en relación con el establecimiento, el mantenimiento y la liberación
- La gestión de servicios basados en CCF', incluidas las interacciones CCF'-CCF' (por ejemplo, petición de redirección)

**Punto de referencia N18** : Es la interfaz funcional SRF a CCF'/SSF, cuando el control de llamada y de conexión están integrados. La mensajería NNI por medio de ésta interfaz funcional hace posible el control de portadores a SRF para servicios de RI, en relación con el establecimiento, el mantenimiento y la liberación.

Obsérvese que opcionalmente puede también utilizarse el protocolo control de llamada independiente del portador (BICC, *bearer independent call control*) a través de este punto de referencia.

**Punto de referencia N19** : Es la interfaz funcional SRF a CnCF, cuando el control de llamada y de conexión están integrados. La mensajería NNI empleando ésta interfaz funcional posibilita el control de portadores a la SRF para servicios de RI, en relación con el establecimiento, el mantenimiento y la liberación.

**Punto de referencia N20** : Es la interfaz funcional CnCF a CnCF. Esta interfaz funcional posibilita:

- La gestión de instancias de conexión, en relación con el establecimiento, el mantenimiento, la modificación y la liberación
- La gestión de las asociaciones de control de portador, relacionadas con el establecimiento, el mantenimiento y la liberación

**Punto de referencia N21** : Es la interfaz funcional LMFv a SCF. La mensajería NNI empleando ésta interfaz funcional posibilita los servicios de RI relacionados con la gestión de posiciones.

### **B-1.5. Requisitos de protocolo para la gestión de la movilidad**

#### **B-1.5.1. Activadores del servicio**

Los siguientes activadores de servicio de RI se utilizan como ejemplo de servicios de RI basados en eventos de movilidad:

1) **Comprobación del crédito**: el abonado puede ver rechazado su registro cuando se encuentra en itinerancia si no dispone de más crédito. De un modo similar, puede ser avisado cuando su factura ha alcanzado un umbral predeterminado. Finalmente, puede ser autorizado a registrarse sólo para un conjunto de servicios restringido si se ha alcanzado determinado umbral.

2) **Control de posición de autenticación**: el abonado puede ver rechazado sus registro si se ha detectado un fraude. Se comprueba la coherencia entre sucesivas posiciones de registro: por ejemplo, el abonado se ha registrado en Berlín, y 15 minutos más tarde en Chicago. La comprobación de posiciones de autenticación ayuda a detectar este fraude.

3) **UPT**: el IMT-2000 debe soportar las UPT. Aquí se supone que un usuario UPT está autorizado para registrarse en un terminal móvil desde este terminal: el registro UPT se basa en un número IMT-2000, es decir, un abonado móvil debe ser registrado en el terminal antes de que el usuario UPT arranque el registro por sí mismo. Para lograr un encaminamiento eficaz, la SCF de UPT debe ser avisada cuando el terminal es activado o desactivado a fin de encaminar la llamada al destino apropiado (por ejemplo, al correo vocal UPT cuando el terminal está desactivado,). De manera análoga, el servicio UPT puede incluir restricciones de servicio cuando el terminal móvil se encuentra itinerante: la SCF de UPT debe ser avisada cuando el terminal se registra en una red visitada para comprobar la autorización de itinerancia del usuario UPT y aplicar una tasación específica tanto para las llamadas entrantes como salientes.

4) **Avisos locales:** cuando se registra el abonado móvil, se pueden visualizar algunos anuncios para proporcionarle alguna información local, por ejemplo, la previsión meteorológica. Estos anuncios locales dependen de los elementos del servicio a los se ha abonado el usuario.

5) **Filtrado dinámico basado en la posición del usuario:** cuando está itinerante, el abonado puede desear que se realice un filtrado de sus llamadas entrantes, en el caso de que se aplique la tarificación dividida. El filtrado dinámico se activa cuando el usuario se registra en una red visitada en el extranjero (usuario itinerante) y en tanto en cuanto el terminal se encuentre activado.

### **B-1.5.2. Modos de interacción de la lógica de servicio**

Entre las características del servicio detalladas en 1.5.1, la lógica de servicio que controla el proceso de gestión de movilidad puede clasificarse en los dos tipos siguientes:

- **Notificación:** La SCF solamente recibe notificación de la LMF de que ha ocurrido un evento de movilidad. Los avisos locales y el filtrado UPT se consideran de este tipo. La SCF no influye en el resultado del procedimiento de movilidad, a pesar de que el servicio RI es prestado al usuario. En el ejemplo, bien se preste un servicio de mensajería o bien se preste cualquier otro servicio, relativo o no al abonado, tal servicio es notificado.
- **Control:** La SCF es capaz de modificar el resultado del procedimiento de movilidad, por ejemplo denegando o cancelando la autenticación o el registro. La comprobación del crédito y el control de posición de autenticación son ejemplos de tales servicios.

### **B-1.5.3. Comunicaciones funcionales de la gestión de la movilidad**

La figura B-5 se ha tomado de la Recomendación UIT-T Q.1711, y se ha ampliado para mostrar la interfaz red-red. Las relaciones señaladas en línea gruesa caen – total o parcialmente – dentro del ámbito de la gestión de la movilidad.

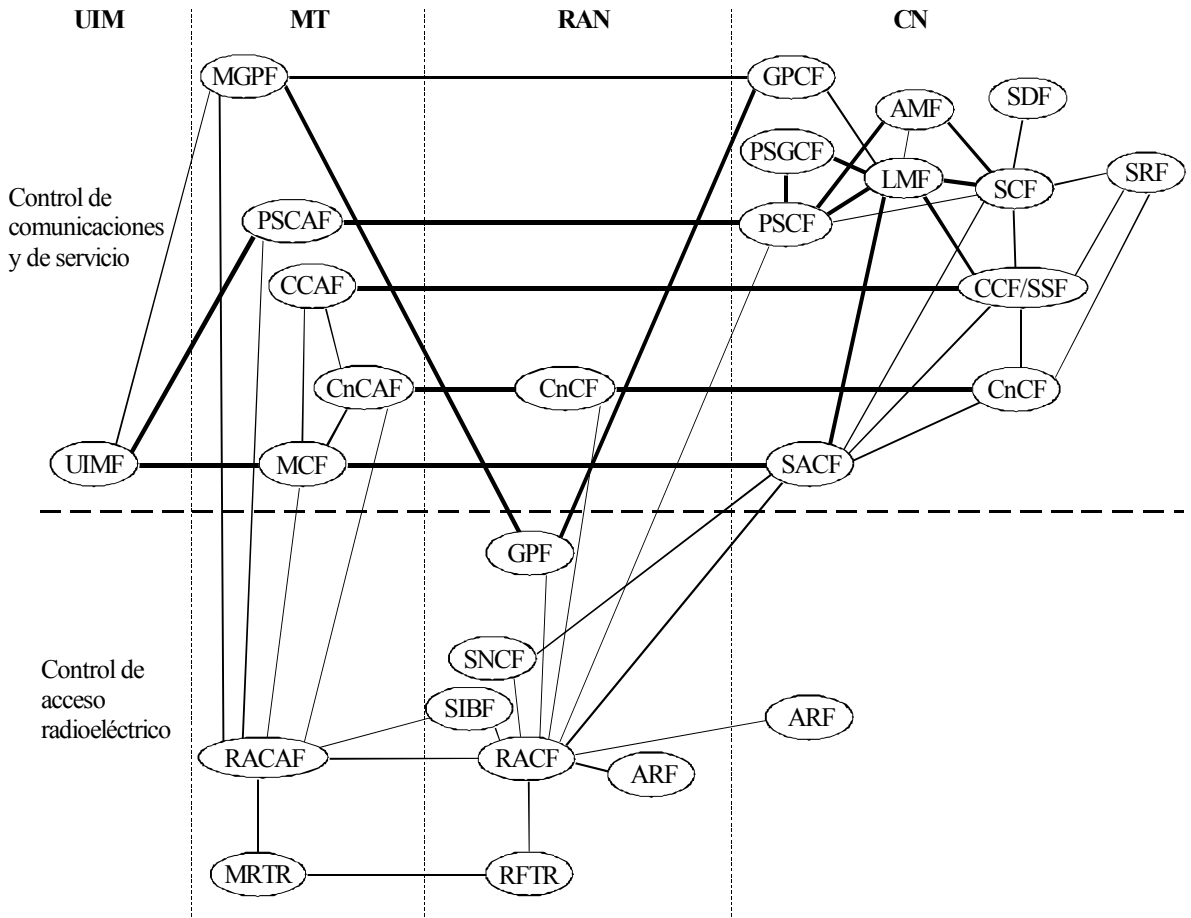


Figura B-5 – Modelo funcional (gestión de la movilidad) de IMT-2000

**B-1.5.4. Comunicaciones funcionales de control de servicio**

La figura B-6 se ha tomado de la Recomendación UIT-T Q.1711. En este caso se ha ampliado para mostrar la interfaz red-red en la capacidad de control de servicio. Las relaciones señaladas en línea gruesa caen –total o parcialmente– dentro del ámbito de la señalización de control de servicio.



<b>Relación</b>	<b>Propuesta de protocolo inicial</b>
SCF-SDF	INAP + extensiones para movilidad.
SCF-SRF	INAP + extensiones para movilidad.
SCF-CCF/SSF	INAP + extensiones para movilidad.
SCF-AMF	Análogo a INAP basado en modelo de estados AMF. Véase la cláusula 9/Q.1721 para flujos de información.
SCF-LMF	Análogo a INAP basado en modelo de estados LMF, pendiente de definir.
SRF-CCF/SSF	Protocolo de control de portador apropiado.
SCF – UIMF (paquetes, vía PSCF, PSCAF)	El transporte se proporcionará vía IPv4 con posibilidad de evolución a IPv6.
SCF-UIMF (circuitos, vía SACF, MCF)	Opciones identificadas: <ul style="list-style-type: none"> <li>• Se utilizará el servicio suplementario USSD de RDSI para soportar el intercambio del diálogo servicio/usuario. Véase la cláusula 11/Q.1721 para flujos de información.</li> <li>• Capacidad CS-2 de RI OCCRUI que utiliza APM ISUP y mecanismo de transporte GAT DSS1.</li> </ul>

**Tabla B-1. Elección de la sucesión de protocolos**

### **B-1.6. Requisitos de protocolo para el control de llamada y de portador**

#### **B-1.6.1. Requisitos generales**

*Registro detallado de la llamada (CDR):* Este procedimiento permite transferir datos CDR desde la red sirviente a la red originaria. Además, debe proveerse la transferencia CDR en tiempo real. Sin embargo, para hacer mínima la transferencia de datos, sólo se transferirán las etiquetas de referencia de la llamada y los datos necesarios para el tratamiento de la llamada.

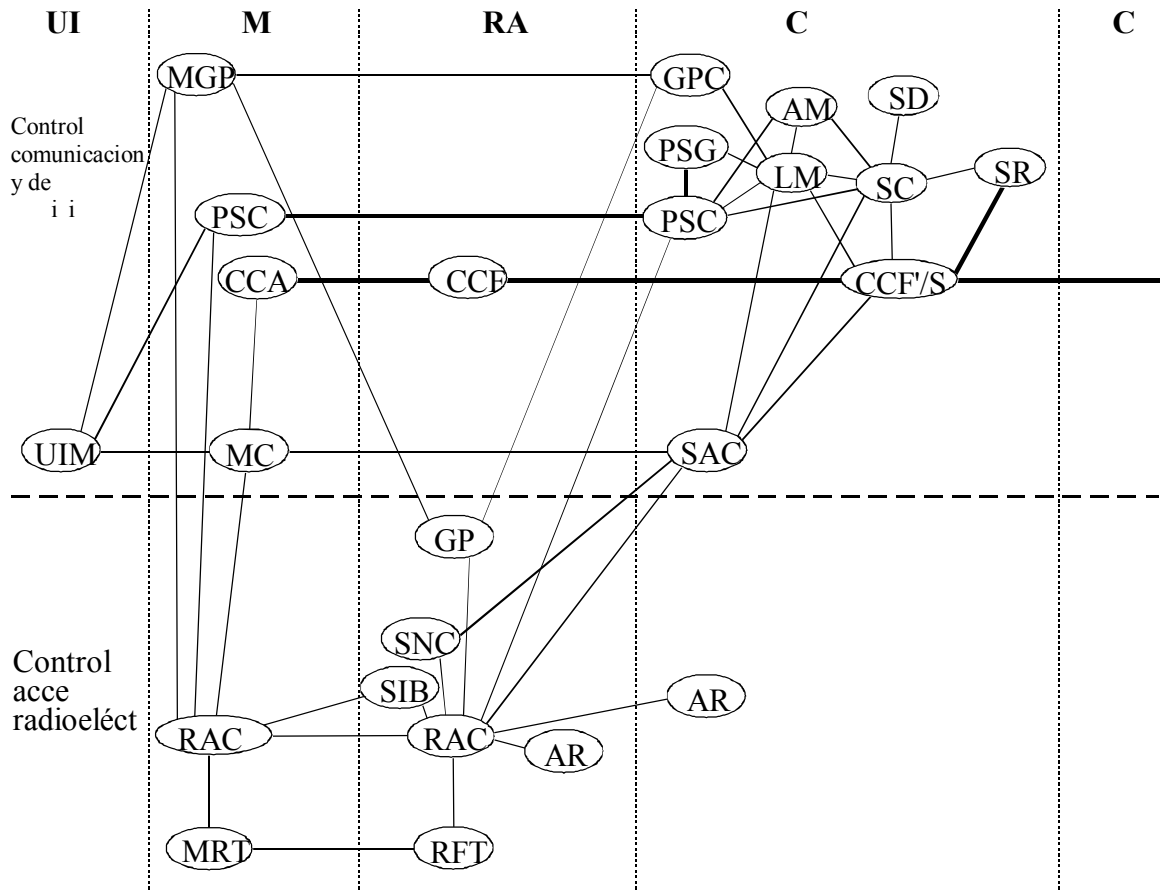
**B-1.6.2. Elección de los principios de conmutación**

Las tecnologías de conmutación (circuitos conmutados, ATM, AAL2, retransmisión de tramas) deben ser elegidas por el operador o el proveedor del servicio.

**B-1.6.3. Comunicaciones funcionales del control de llamada y de portador**

Las figuras B-7 y B-8 se han tomado de la Recomendación UIT-T Q.1711, y se han ampliado para mostrar la interfaz red-red. Las relaciones señaladas en línea gruesa caen – total o parcialmente – dentro del ámbito de la señalización de control de llamada y de portador.

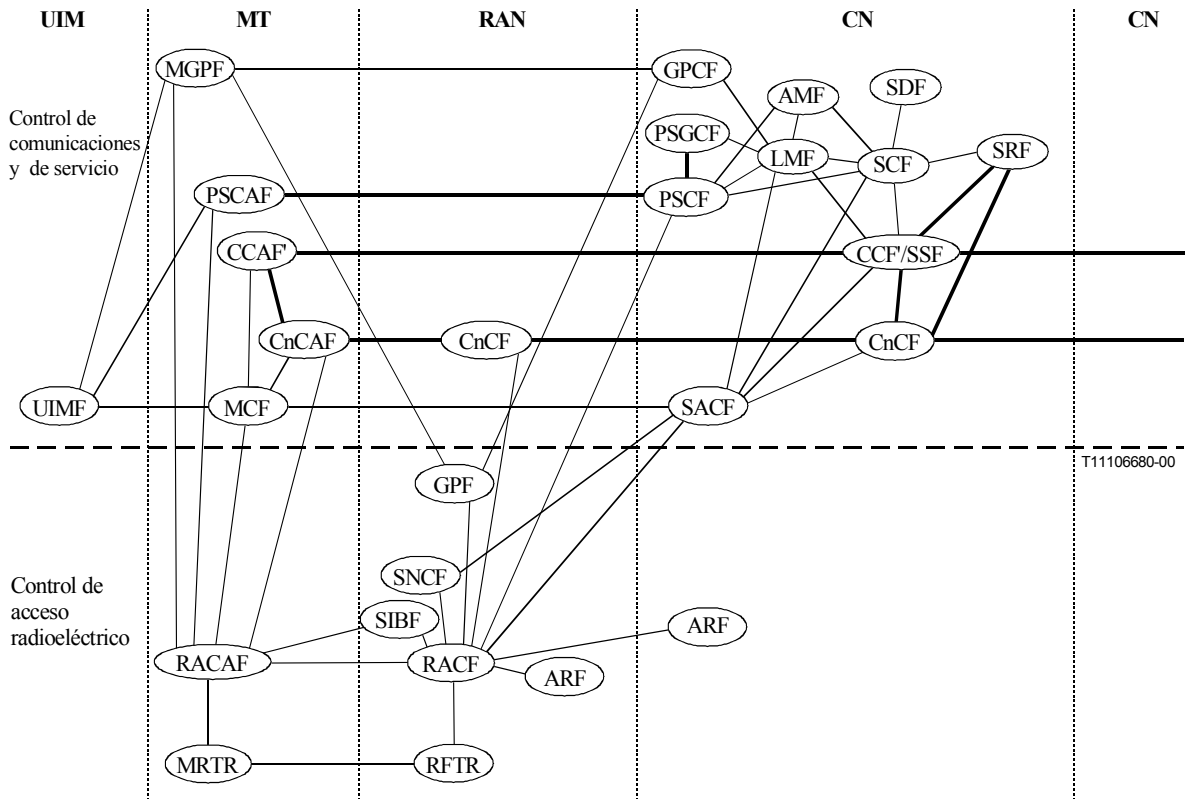




NOTA – CCF" se introduce para efectuar las funciones de conversión de protocolo (relativas al control de llamada y de portador) entre las interfaces MT-RAN y RAN-CN.

**Figura B-7 – Modelo funcional de IMT-2000**

**Alternativa 1: Entidades funcionales control de conexión y control de llamada integradas**

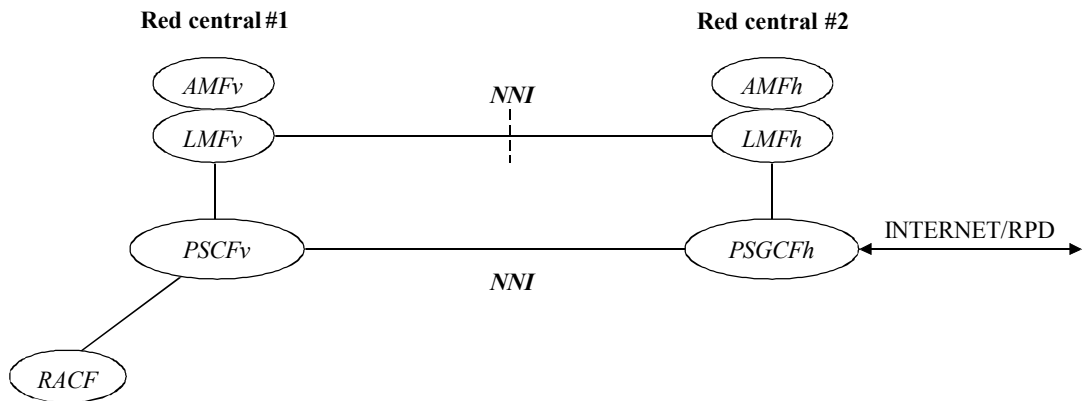


**Figura B-8 – Modelo funcional de IMT-2000**

**Alternativa 2: Entidades funcionales control de conexión y control de llamada separadas**

**B-1.7. Requisitos de protocolo para el control del servicio de paquetes**

Los elementos funcionales que soportarán servicios de datos por paquetes y sus relaciones a través de fronteras de redes centrales (CN) se muestran en la figura B-9. Esta cláusula identifica un conjunto de requisitos que pertenecen a la NNI que soporta los servicios de datos por paquetes.



**Figura B-9– Interfaces red-red de datos por paquetes**

#### **B-1.7.1. El protocolo de interfaz PSCF A PSGCF**

La PSCF y la PSGCF proporcionarán las dos capacidades funcionales siguientes:

- 1) La transferencia de datos de usuario entre estas dos entidades.
- 2) La interacción entre estas dos entidades para actualizar el servicio de paquetes y los contextos de encaminamiento.

Estas dos funciones y el flujo de información asociado pertenecen a dos planos lógicos disjuntos, el plano de usuario y el plano de control. La primera función identificada anteriormente pertenece al plano de usuario, mientras que la segunda función pertenece al plano de control. Los requisitos funcionales enumerados a continuación pertenecen a ambos planos, de usuario y de control, cuando la PSCF y la PSGCF residen en dos redes medulares (CN - Core Networks – Núcleo de Red) diferentes.

- 1) Cuando la PSCF y la PSGCF residen en dos CN diferentes, estas dos entidades deben interconectarse sobre una red IP.

- 2) Cuando la PSCF y la PSGCF son conectadas sobre la red Internet pública, debe haber una asociación de seguridad entre la PSCF y la PSGCF.
- 3) Cuando la CN originaria autoriza a un terminal móvil (MT, *mobile terminal*) para servicios de datos en una CN visitada, la CN originaria debe dar una instrucción a la CN visitada para que seleccione una PSGCF específica o que proponga la asignación de una PSGCF local en la CN visitada para tratar una sesión de servicio de datos.
- 4) Cuando la sesión de servicio de datos ha sido establecida, la PSGCF asignada debe ser fijada durante la duración total de la sesión de servicio de datos. La red medular visitada en la que reside la PSGCF, viene a ser la red medular de anclaje, CNa, para la sesión de datos.
- 5) Cuando el MT inicia una sesión de servicio de datos, la PSCF debe ser asignada por la CN en la que se ha iniciado la sesión de servicio de datos.
- 6) Cuando el MT se encuentra itinerante en el interior de una CN visitada durante una sesión de servicio establecida, la CN visitada debe asignar dinámicamente una nueva PSCF para tratar la sesión de servicio respectiva. Se puede asignar una sucesión de funciones PSCF al MT cuando está itinerante dentro de la CN visitada (durante la itinerancia intrared).
- 7) La IMSI o el NAI pueden utilizarse como un identificador de servicio único en todas las transacciones de protocolo. Si el MT soporta varias sesiones de servicio simultáneas, debe utilizarse un identificador de número de sesión asociado para identificar inequívocamente cada sesión de servicio individual.

**Requisitos del plano de usuario:**

- 1) La PSCF y la PSGCF deben transferir la información de usuario por una red IP empleando un túnel IP bidireccional.

- 2) El plano de usuario puede incorporar un mecanismo que soportará la existencia concurrente de una multiplicidad de conexiones túnel bidireccionales dentro del túnel IP que conecta la PSCF y la PSGCF.
- 3) El plano de usuario debe incorporar un mecanismo opcional (por ejemplo, un esquema de encapsulado) que impedirá las entregas fuera de secuencia de unidades de datos por paquetes de usuario a través de la conexión túnel.
- 4) En un momento dado, cada conexión túnel entre la PSCF y la PSGCF debe tener una duración de vida específica. El tiempo de vida de una conexión túnel debe ser ampliable. Cuando expira el tiempo de vida de una conexión túnel determinada, la conexión túnel respectiva debe ser liberada.

**Requisitos del plano de control:**

- 1) El protocolo del plano de control entre la PSCF y la PSGCF debe ser capaz de establecer conexiones túnel individuales, ampliar el tiempo de vida de las conexiones túnel establecidas y liberar las conexiones túnel establecidas.
- 2) La PSCF y la PSGCF deben emplear el protocolo de datagramas de usuario (UDP, *user datagram protocol*) para intercambiar mensajes de control. Estos mensajes pueden ser protegidos por un túnel de seguridad IP.
- 3) Un puerto UDP dedicado y perfectamente conocido en la PSGCF debe terminar un canal de control sobre el cual deben intercambiarse los mensajes de control entre la PSCF y la PSGCF.
- 4) La PSCF y la PSGCF deben aplicar un protocolo de toma de contacto bidireccional (es decir, dos mensajes) al establecer una conexión túnel o ampliar el tiempo de vida de una conexión túnel establecida. El protocolo unidireccional debe utilizarse para liberar una conexión túnel establecida.

- 5) La PSCF y la PSGCF deben ser capaces de establecer una asociación de seguridad con la otra, y realizar la encriptación de datos y la autenticación y comprobación de integridad de los mensajes de control.

#### **B-1.7.2. El protocolo de interfaz LMFp a LMFp**

Para acceder a los servicios de datos por paquetes, el MT itinerante se registrará con la red IMT-2000 visitante mediante procedimientos comunes de autenticación y registro de terminal, y pedirá acceso a las facilidades de datos por paquetes. Puede mantenerse un registro de facturación asociado para registrar la utilización de los recursos de datos por paquetes. La arquitectura CN debe tener en cuenta la separación de capacidades LMF (y AMF asociada) que pertenecen a facilidades de acceso y capacidades LMFp (y AMFp asociada) que pertenecen a los servicios de datos por paquetes. Los requisitos enumerados a continuación se refieren a la interacción entre las LMFp visitada y originaria que residen en dos CN diferentes e incorporan solamente las capacidades de datos por paquetes.

- 1) Cuando se intercambia información perteneciente a servicios de datos por paquetes, la LMFp visitante y la LMFp originaria deben ser capaces de transportar la información respectiva sobre una red IP.
- 2) Debe existir una asociación de seguridad entre una LMFp visitante y una LMFp originaria antes de que se pueda intercambiar información entre estas dos entidades. La asociación de seguridad puede establecerse automáticamente o acordarse previamente, o bien una LMFp visitante y una LMFp originaria pueden comunicar a través de un tercero de confianza (por ejemplo, un agente) con aquellos con los que tengan, respectivamente una asociación de seguridad.
- 3) El protocolo entre la LMFp visitante (y AMFp asociada) y la LMFp originaria (y AMFp asociada) debe posibilitar que la CN visitada autentique y autorice al MT visitante para que utilice los servicios de datos por paquetes en la red CN visitada.

- 4) Si la LMFp originaria falla en la autenticación del MT, la CN visitada no permitirá el servicio de datos por paquetes. La CN visitada asumirá un acuerdo de tasación si la red originaria autoriza el servicio.
- 5) Cuando se utilizan servicios de datos por paquetes, el MT visitado puede identificar por sí mismo a la red de datos por paquetes solamente con su NAI. La LMFp visitada debe poder identificar y localizar la LMFp originaria basándose en el NAI.
- 6) La LMFp visitada debe poder solicitar, y la LMFp originaria debe poder identificar, la PSGCF que la CN visitada debe utilizar para la sesión de datos por paquetes respectiva.
- 7) La LMFp visitada debe poder solicitar, y la LMFp originaria debe poder suministrar, una dirección IP que será utilizada por el MT durante la sesión de datos por paquetes respectiva.
- 8) El protocolo entre LMFp pares debe proporcionar un mecanismo de transporte de la información de facturación a través de esta interfaz.
- 9) Las LMFp pares deben utilizar un identificador de sesión (ID de sesión) único para cada sesión de datos por paquetes que ellas tratan mutuamente.
- 10) Las LMFp pares deben emplear un conjunto de códigos de respuesta que han de incluirse en cada mensaje de respuesta. El código de respuesta proporcionará copia de la información relativa a la petición (por ejemplo, servicio denegado, condición de error y contraseña no correcta) al par solicitante.

Para los servicios de datos por paquetes, la red IMT-2000 proporcionará dos niveles de seguridad – la seguridad de la red de acceso y la seguridad de la red de datos por paquetes. La seguridad de la red de acceso incluye la encriptación de la señal radioeléctrica y la gestión de claves del acceso radioeléctrico para la autenticación del MT. La seguridad de la red de datos por paquetes incluye la encriptación y tunelización de paquetes sobre la red Internet pública y la autenticación del MT con la red IMT-2000 utilizando un clave secreta. Los requisitos de interfaz LMFp a LMFp enumerados a continuación pertenecen a la seguridad de la red de datos por paquetes.

- 1) A fines de autenticación y autorización del servicio, la CN originaria puede ser capaz de proporcionar información de seguridad relacionada con el MT a la CN visitada.
- 2) Debe existir un mecanismo mediante el cual la LMFp visitada será capaz de transportar a la LMFp originaria los valores de puesta a prueba y respuesta de puesta a prueba. El valor de puesta a prueba contendrá el valor que la CN visitada transfirió al MT visitante, La respuesta de puesta a prueba contendrá el valor que el MT visitante ha generado utilizando el valor de puesta a prueba y el secreto que el MT visitante comparte con su CN originaria.
- 3) Debe existir un mecanismo de seguridad mediante el cual la LMFp visitada y la LMFp originaria serán capaces de intercambiar parámetros de seguridad (por ejemplo, SPI y claves de seguridad). Los parámetros de seguridad que hayan sido recibidos de la LMFp originaria posibilitarán que la CN visitada establezca una asociación de seguridad bidireccional con el MT visitante, y entre la PSCF en la CN visitada y la PSGCF en la CN originaria.

### **B-1.7.2. Definiciones**

En este anexo se emplean los siguientes términos:

**Red medular de anclaje:** en un entorno de itinerancia de sesión de datos, la red medular anclada es la red en la que se inicia la sesión de datos y se asigna una pasarela del servicio por paquetes al terminal móvil. La red medular de anclaje puede ser una red originaria o una red visitada.

**Punto de referencia:** en un modelo funcional entre redes e intrared, el punto de referencia está referido a la relación entre dos entidades funcionales para el intercambio de mensajes de señalización y transacciones de operaciones.

**Aplicación de servicio:** provisión de servicios mediante capacidades de uso general, tales como las capacidades de red inteligente aplicadas en la posición originaria o en una posición visitada como parte de un entorno originario virtual (VHE).

**Control de servicio:** funciones que establecen o modifican el contexto en el cual son establecidos, modificados y liberados los portadores y llamadas básicas.



**Modelo de estados:** el modelo de estados para una entidad funcional es una representación esquemática de los estados de la entidad en relación con un procedimiento de señalización entre redes. Incluye la identificación de todos los puntos de detección (DP) de entrada y salida para cada estado.

**Abonado:** usuario de un terminal móvil que se ha abonado al servicio.

**Aplicación de servicio suplementario:** provisión de un servicio suplementario específico, típicamente mediante el uso de capacidades específicas de servicio, sea en la posición originaria o en la posición visitada como parte de un entorno originario virtual.

**Usuario:** el usuario de un terminal móvil. Los términos "usuario" y "abonado" se utilizan indistintamente en este anexo.

**Entorno originario virtual:** provisión de unas condiciones de servicio al abonado visitante idénticas, o lo más similar posibles, a las condiciones de servicio de que gozó el abonado cuando ha operado en su posición originaria.

### B-1.7.3. Abreviaturas

AALx.	ATM Application Layer x - Capa de Aplicación ATM del Nivel x
AC.	Authentication Center - Centro de autenticación
AINI.	ATM Internetwork Interface - Interfaz entre Redes con Modo de Transferencia Asíncrono
AMF.	Authentication Management Function - Función de Gestión de Autenticación
ATM.	Asynchronous Transfer Mode - Modo de Transferencia Asíncrono
BICC.	Bearer Independent Call Control - Control de Llamada Independiente del Portador
CBC.	Call and Bearer Control - Control de Llamada y de Portador
CC.	Call Control - Control de llamada
CCAF'.	Call Control Agent Function - Función de Agente de Control de Llamada
CCF.	Call Control Function - Función de Control de Llamada
CCF'.	Call Control Function - Función de Control de Llamada
CLI.	Calling Line ID - Identificación de la Línea Llamante

CN.	Core Network - Red Medular
Cna.	Core Network anchored - Red Medular de anclaje
CnCAF.	Connection Control Agent Function - Función de Agente de Control de Conexión
CnCF.	Connection Control Function - Función de Control de Conexión
CNh.	Core Network home - Red Medular originaria
CNpv.	Core Network previous visited - Red Medular previamente visitada
CNsn.	Core Network supporting - Red Medular soporte
CNv.	Core Network visited - Red Medular visitada
CS-X.	Capability Set X - Conjunto de Capacidades X
DAS.	Application Data Delivery Service - Servicio de Entrega de Datos de Aplicación
DFP.	Distributed Functional Plane - Plano Funcional Distribuido
DP.	Detection Point - Punto de Detección
FE.	Functional Entity - Entidad Funcional
FT.	Fixed Terminal - Terminal Fijo
GPCF.	Geographic Position Control Function - Función de Control de Posición Geográfica
GPF.	Geographic Position Function - Función de Posición Geográfica
ID.	Identity - Identidad
IF.	Information Flow - Flujo de Información
IMDN.	IMT-2000/International Mobile Directory Number - Número de Directorio Móvil Internacional/IMT-2000
IMT-2000.	International Mobile Telecommunications-2000 -Telecomunicaciones móviles internacionales-2000
IMUI.	IMT-2000/International Mobile User Identity - Identidad de Usuario Móvil Internacional/IMT-2000
INAP.	Intelligent Network Application Protocol - Protocolo de Aplicación de Red Inteligente
IP.	Internet Protocol - Protocolo Internet
ISP.	Internet Service Provider - Proveedor de Servicio Internet
IWF.	Interworking Function - Función de Interoperabilidad
LAI.	Location Area Identity - Identidad de Zona de Posición
LMF.	Location Management Function - Función de Gestión de Ubicaciones
MCF.	Mobile Control Function - Función de Control Móvil
MGPF.	Mobile Geographic Position Function - Función de Posición Geográfica Móvil
MM.	Mobility Management - Gestión de la Movilidad
MRTR.	Mobile Radio Transmission and Reception - Transmisión y Recepción Radioeléctrica Móvil
MSC.	Mobile Switching Centre - Centro de Conmutación de Servicios Móviles

MT.	Mobile Terminal - Terminal Móvil
NAI.	Network Access Identifier - Identificador de Acceso de Red
NNI.	Network-to-Network interface Interfaz Red-Red
Nxx.	Punto de Referencia
PIAM.	Point in Authentication Management - Punto en la gestión de autenticación
PIN.	Personal Identification Number - Número de Identificación Personal
PNNI.	Private Network-to-Network - Interfaz Interfaz Red-Red Privada
PSC.	Packet Services Control - Control de Servicio por Paquetes
PSCAF.	Packet Service Control Agent Function - Función de Agente de Control de Servicio por Paquetes
PSCF.	Packet Service Control Function - Función de Control de Servicio por Paquetes
PSGCF.	Packet Service Gateway Control Function - Función de Control de Pasarela de Servicio por Paquetes
PU-RDSI.	ISDN User Protocol - Parte Usuario de RDSI
PU-RDSI-BA.	Parte Usuario de RDSI de Banda Ancha
PU-RDSI-BE.	Parte Usuario de RDSI de Banda Estrecha
QoS.	Quality of Service - Calidad de Servicio
RACAF.	Radio Access Control Agent Function - Función de Agente de Control de Acceso Radioeléctrico
RAN.	Radio Access Network - Red de Acceso Radioeléctrico
RDSI.	Red digital de servicios integrados
RF.	Radiofrecuencia
RFTR.	Radio Frequency Transmission and Reception - Transmisión y Recepción en Radiofrecuencia
RI.	Red inteligente
RNC.	Radio Network Controller - Controlador de Red Radioeléctrica
RPD.	Red de Datos por Paquetes
RTPC.	Red Telefónica Pública Conmutada
SACF.	Service Access Control Function - Función de Control de Acceso al Servicio
SCF.	Service Control Function - Función de Control de Servicio
SCP.	Service Control Point - Punto de Control de Servicio
SDF.	Service Data Function - Función de Datos de Servicio
SDP.	Service Data Point - Punto de Datos de Servicio
SIBF.	System Access Information Broadcast Function - Función de Difusión de Información de Acceso al Sistema
SLP.	Service Logic Program - Programa Lógico de Servicio

SMF.	Service Management Function - Función de Gestión de Servicio
SMS.	Short Message Service - Servicio de Mensajes Cortos
SRF.	Specialized Resource Function - Función de Recursos Especializados
SSD.	Shared Secret Data Datos Secretos Compartidos
TMUI.	Temporary Mobile User Identifier - Identificador Temporal de Usuario Móvil
TTG.	Traducción del Título Global
UDP.	User Datagram Protocol - Protocolo de Datagrama de Usuario
UIM.	User Identity Module - Modulo de Identidad de Usuario
UIMF.	User Identification Management Function - Función de Gestión de Identificación de Usuario
UPT.	Universal Personal Telecommunications - Telecomunicaciones Personales Universales
VHE.	Virtual Home Environment - Entorno Originario Virtual
VSC.	VHE Services Control - Control de Servicios de Entorno Originario Virtual