



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**Q.1751**

(06/2000)

SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN

Requisitos y protocolos de señalización para IMT-2000

---

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

Recomendación UIT-T Q.1751

(Anteriormente Recomendación del CCITT)

---

RECOMENDACIONES UIT-T DE LA SERIE Q  
**CONMUTACIÓN Y SEÑALIZACIÓN**

SEÑALIZACIÓN EN EL SERVICIO MANUAL INTERNACIONAL	Q.1–Q.3
EXPLOTACIÓN INTERNACIONAL SEMIAUTOMÁTICA Y AUTOMÁTICA	Q.4–Q.59
FUNCIONES Y FLUJOS DE INFORMACIÓN PARA SERVICIOS DE LA RDSI	Q.60–Q.99
CLÁUSULAS APLICABLES A TODOS LOS SISTEMAS NORMALIZADOS DEL UIT-T	Q.100–Q.119
ESPECIFICACIONES DE LOS SISTEMAS DE SEÑALIZACIÓN N.º 4 Y N.º 5	Q.120–Q.249
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.º 6	Q.250–Q.309
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R1	Q.310–Q.399
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R2	Q.400–Q.499
CENTRALES DIGITALES	Q.500–Q.599
INTERFUNCIONAMIENTO DE LOS SISTEMAS DE SEÑALIZACIÓN	Q.600–Q.699
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.º 7	Q.700–Q.849
SISTEMA DE SEÑALIZACIÓN DIGITAL DE ABONADO N.º 1	Q.850–Q.999
RED MÓVIL TERRESTRE PÚBLICA	Q.1000–Q.1099
INTERFUNCIONAMIENTO CON SISTEMAS MÓVILES POR SATÉLITE	Q.1100–Q.1199
RED INTELIGENTE	Q.1200–Q.1699
<b>REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA IMT-2000</b>	<b>Q.1700–Q.1799</b>
RED DIGITAL DE SERVICIOS INTEGRADOS DE BANDA ANCHA (RDSI-BA)	Q.2000–Q.2999

*Para más información, véase la Lista de Recomendaciones del UIT-T.*

## **Recomendación UIT-T Q.1751**

### **Requisitos de la señalización entre redes para el conjunto de capacidades 1 de las telecomunicaciones móviles internacionales-2000 (IMT-2000)**

#### **Resumen**

La presente Recomendación UIT-T contiene los requisitos de señalización para el protocolo de la interfaz red-red (NNI). Los requisitos deberán soportar las capacidades recomendadas en el documento "Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000)" y que se especifican como conjunto de capacidades 1 (CS-1). Esta Recomendación UIT-T abarca requisitos para cuatro grupos de comunicación de la NNI: control de llamada y control de portador; gestión de movilidad, control de servicio de entorno originario virtual (VHE); y servicios de datos por paquetes y control de acceso a Internet. Los requisitos para la seguridad entre redes se describen a alto nivel y su funcionalidad se incorpora a los protocolos de grupo de comunicaciones aplicable. Los requisitos especificados en esta Recomendación UIT-T se refieren al flujo de no información, y pueden ser contemplados como complementarios a los flujos de información de la Recomendación UIT-T Q.1721. Incluyen los requisitos de protocolo NNI generales, los modelos funcionales NNI, los puntos de referencia NNI, los modelos de estados para entidades funcionales selectivas y la selección de varias sucesiones de protocolos.

#### **Orígenes**

La Recomendación UIT-T Q.1751, preparada por la Comisión de Estudio 11 (1997-2000) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la CMNT el 15 de junio de 2000.

#### **Palabras clave**

AMF, BICC, CN, CS-1, IMT-2000, INAP, LMFh, LMFv, MT, NNI, RAN, UIM, VHE.

## PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) 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. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2001

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

## ÍNDICE

### Página

1	Alcance .....	1
2	Referencias.....	1
3	Definiciones .....	2
4	Abreviaturas.....	3
5	Introducción .....	5
6	Requisitos generales.....	6
6.1	Requisitos de la interfaz red-red (NNI).....	6
6.2	Requisitos de control de servicios VHE .....	6
6.2.1	Entorno originario virtual (VHE) basado en la programación a distancia.....	6
6.2.2	Capacidades de servicio.....	6
6.3	Requisitos de almacenamiento de datos de CN para el perfil de abonado (usuario) ..	7
6.4	Requisitos de itinerancia global .....	7
6.5	Agrupaciones de comunicaciones NNI.....	8
6.6	Servicios de Internet .....	9
6.7	Requisitos de seguridad .....	9
6.7.1	Requisitos para el transporte de la autenticación del usuario .....	10
6.7.2	Requisitos de criptación para la interfaz red-red .....	10
6.7.3	Requisitos de gestión de claves para la interfaz red-red .....	10
7	Modelo de interconexión .....	10
8	Interfaz funcional NNI.....	11
8.1	Modelo funcional.....	11
8.2	Puntos de referencia.....	12
8.2.1	Punto de referencia N01 .....	13
8.2.2	Punto de referencia N02 .....	13
8.2.3	Punto de referencia N03 .....	13
8.2.4	Punto de referencia N04 .....	13
8.2.5	Punto de referencia N05 .....	13
8.2.6	Punto de referencia N06 .....	14
8.2.7	Punto de referencia N07 .....	14
8.2.8	Punto de referencia N08 .....	14
8.2.9	Punto de referencia N09 .....	14
8.2.10	Punto de referencia N10 .....	14
8.2.11	Punto de referencia N11 .....	14
8.2.12	Punto de referencia N12 .....	15
8.2.13	Punto de referencia N13 .....	15

8.2.14	Punto de referencia N14 .....	15
8.2.15	Punto de referencia N15 .....	15
8.2.16	Punto de referencia N16 .....	15
8.2.17	Punto de referencia N17 .....	15
8.2.18	Punto de referencia N18 .....	15
8.2.19	Punto de referencia N19 .....	16
8.2.20	Punto de referencia N20 .....	16
8.2.21	Punto de referencia N21 .....	16
9	Requisitos de protocolo para la gestión de la movilidad .....	16
9.1	Activadores del servicio.....	16
9.2	Modos de interacción de la lógica de servicio .....	17
9.3	Modelo de estados LMFv .....	17
9.3.1	State: v_Null .....	18
9.3.2	State: v_Initial_Registration .....	19
9.3.3	State: Proceso de V_Authentication .....	19
9.3.4	State: V_Registration_pending.....	20
9.3.5	State:V_Active_registered.....	20
9.3.6	State: v_Inactive_registered.....	21
9.3.7	State: v_Denied.....	21
9.4	Modelo de estados LMFh .....	21
9.4.1	State H_Location_Unknown .....	22
9.4.2	State H_Registering.....	23
9.4.3	State H_Registered .....	23
9.4.4	State H_Old_Location_Cancelling_and_Registered .....	24
9.4.5	State H_Exception .....	24
9.5	Modelo de estados AMF .....	24
9.5.1	State: A_Null .....	25
9.5.2	State: Authentication_Processing.....	26
9.5.3	State: Awaiting_Challenge_Response.....	26
9.6	Comunicaciones funcionales de la gestión de la movilidad .....	26
9.7	Elección de sucesión de protocolos .....	27
10	Requisitos de protocolo para el control de servicio del VHE.....	28
10.1	Requisitos generales.....	28
10.2	Comunicaciones funcionales de control de servicio.....	28
10.3	Elección de la sucesión de protocolos .....	29
11	Requisitos de protocolo para el control de llamada y de portador.....	30
11.1	Requisitos generales.....	30
11.2	Elección de los principios de conmutación.....	30

	<b>Página</b>
11.3 Comunicaciones funcionales del control de llamada y de portador.....	30
11.4 Elección de la sucesión de protocolos .....	31
11.5 Llamadas multimedios .....	32
11.6 Llamadas pluripartitas.....	32
12 Requisitos de protocolo para el control del servicio de paquetes .....	33
12.1 El protocolo de interfaz PSCF A PSGCF .....	33
12.1.1 Requisitos del plano de usuario .....	34
12.1.2 Requisitos del plano de control .....	34
12.2 El protocolo de interfaz LMFp a LMFp.....	35
Apéndice I – Directriz sobre los conceptos y la utilización de activadores.....	36
I.1 Objetivo .....	36
I.2 Introducción .....	36
I.3 Principios y conceptos .....	36
I.4 Armado dinámico del activador.....	37
I.5 Distribución de activadores.....	38





## Recomendación UIT-T Q.1751

### Requisitos de la señalización entre redes para el conjunto de capacidades 1 de las telecomunicaciones móviles internacionales-2000 (IMT-2000)

#### 1 Alcance

El alcance de la presente Recomendación UIT-T incluye la preparación de los requisitos de señalización entre redes que han de utilizarse para el desarrollo de un protocolo de interfaz red-red (NNI, *network-to-network interface*) común y único. Con contribuciones de las Recomendaciones UIT-T Q.1701 [1], Q.1711 [2], y Q.1721 [3], esta Recomendación UIT-T proporciona requisitos de señalización y protocolo que no son del tipo de flujo de información. Concretamente, esta Recomendación UIT-T incluye los siguientes temas:

- Descripción de las capas de señalización de conformidad con las agrupaciones funcionales para el control de llamada y de portador (CBC, *call and bearer control*), gestión de la movilidad (MM, *mobility management*), control de servicios por paquetes (PSC, *packet services control*), y control del servicio VHE (VSC, *VHE service control*).
- Ejemplares NNI para la itinerancia global y sus puntos de referencia.
- Modelos de estados para diversas entidades funcionales.
- Requisitos de señalización para protocolos NNI.
- Selección de protocolos NNI.

**El interfuncionamiento CN-CN se puede también realizar especificando una función de interfuncionamiento (IWF, *interworking function*) para la conversión de información de protocolo (y de facturación) entre diferentes miembros de la familia. Pero la especificación detallada del interfuncionamiento no es competencia de la UIT.**

**La preparación de la descripción detallada utilizando el "lenguaje de especificación y descripción" (SDL, *specification and description language*), el diseño de la arquitectura de protocolo y la codificación del protocolo caen fuera del alcance de esta Recomendación UIT-T.**

**Los aspectos de OAM entre sistemas miembros de la familia están también fuera del ámbito de esta Recomendación UIT-T.**

#### 2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

- [1] Recomendación UIT-T Q.1701 (1999), *Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000)*.
- [2] Recomendación UIT-T Q.1711 (1999), *Modelo funcional de red para las telecomunicaciones internacionales-2000 (IMT-2000)*.
- [3] Recomendación UIT-T Q.1721 (2000), *Flujos de información para el conjunto de capacidades 1 del IMT-2000*.

- [4] Recomendación UIT-T Q.1901 (2000), *Protocolo de control de llamada independiente del portador*.
- [5] Recomendación UIT-T Q.2630.1 (1999), *Protocolo de señalización de la capa de adaptación del modo de transferencia asíncrono de tipo 2 (conjunto de capacidades 1)*.
- [6] Recomendaciones UIT-T de la serie Q.1238, *Recomendación sobre interfaces para el conjunto de capacidades 3 de la red inteligente*.
- [7] Recomendación UIT-T Q.1290 (1998), *Glosario de términos utilizados en la definición de redes inteligentes*.

### 3 Definiciones

En esta Recomendación UIT-T se definen los términos siguientes.

**3.1 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.

**3.2 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.

**3.3 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).

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

**3.5 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.

**3.6 abonado:** Usuario de un terminal móvil que se ha abonado al servicio.

**3.7 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.

**3.8 usuario:** El usuario de un terminal móvil. Los términos "usuario" y "abonado" se utilizan indistintamente en esta Recomendación UIT-T.

**3.9 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.

Esta Recomendación UIT-T utiliza los términos definidos en la Recomendación UIT-T Q.1701 [1].

– **red medular (o red central).**

Esta Recomendación UIT-T utiliza los términos definidos en la Recomendación UIT-T Q.1290 [7].

– **entidad funcional;**

– **punto de detección;**

– **activador del servicio.**

#### 4 Abreviaturas

En esta Recomendación UIT-T se utilizan las siguientes siglas.

AALx	Capa de aplicación ATM de tipo x ( <i>ATM application layer x</i> )
AC	Centro de autenticación ( <i>authentication center</i> )
ADDS	Servicio de entrega de datos de aplicación ( <i>application data delivery service</i> )
AINI	Interfaz entre redes con modo de transferencia asíncrono ( <i>ATM internetwork interface</i> )
AMF	Función de gestión de autenticación ( <i>authentication management function</i> )
ATM	Modo de transferencia asíncrono ( <i>asynchronous transfer mode</i> )
BICC	Control de llamada independiente del portador ( <i>bearer independent call control</i> )
CBC	Control de llamada y de portador ( <i>call and bearer control</i> )
CC	Control de llamada ( <i>call control</i> )
CCAF'	Función de agente de control de llamada ( <i>call control agent function</i> ) (mejorada, como se describe en la Recomendación UIT-T Q.1711 [2])
CCF	Función de control de llamada ( <i>call control function</i> )
CCF'	Función de control de llamada ( <i>call control function</i> ) (mejorada, como se describe en la Recomendación UIT-T Q.1711 [2])
CLI	Identificación de la línea llamante ( <i>calling line ID</i> )
CN	Red medular ( <i>core network</i> )
CNa	Red medular (de anclaje) [ <i>core network (anchored)</i> ]
CnCAF	Función de agente de control de conexión ( <i>connection control agent function</i> )
CnCF	Función de control de conexión ( <i>connection control function</i> )
CNh	Red medular (originaria) [ <i>core network (home)</i> ]
CNpv	Red medular (previamente visitada) [ <i>core network (previous visited)</i> ]
CNsn	Red medular (soporte) [ <i>core network (supporting)</i> ]
CNv	Red medular (visitada) [ <i>core network (visited)</i> ]
CS-X	Conjunto de capacidades X ( <i>capability set X</i> )
DFP	Plano funcional distribuido ( <i>distributed functional plane</i> )
DP	Punto de detección ( <i>detection point</i> )
FE	Entidad funcional ( <i>functional entity</i> )
FT	Terminal fijo ( <i>fixed terminal</i> )
GPCF	Función de control de posición geográfica ( <i>geographic position control function</i> )
GPF	Función de posición geográfica ( <i>geographic position function</i> )
ID	Identidad
IF	Flujo de información ( <i>information flow</i> )
IMDN	Número de directorio móvil internacional/IMT-2000 ( <i>IMT-2000/international mobile directory number</i> )

IMT-2000	Telecomunicaciones móviles internacionales-2000 ( <i>International Mobile Telecommunications-2000</i> )
IMUI	Identidad de usuario móvil internacional/IMT-2000 ( <i>IMT-2000/international mobile user identity</i> )
INAP	Protocolo de aplicación de red inteligente ( <i>intelligent network application protocol</i> )
IP	Protocolo Internet ( <i>Internet protocol</i> )
ISP	Proveedor de servicio Internet ( <i>Internet service provider</i> )
IWF	Función de interfuncionamiento ( <i>interworking function</i> )
LAI	Identidad de zona de posición ( <i>location area identity</i> )
LMF	Función de gestión de ubicaciones ( <i>location management function</i> )
MCF	Función de control móvil ( <i>mobile control function</i> )
MGPF	Función de posición geográfica móvil ( <i>mobile geographic position function</i> )
MM	Gestión de la movilidad ( <i>mobility management</i> )
MRTR	Transmisión y recepción radioeléctrica móvil ( <i>mobile radio transmission and reception</i> )
MSC	Centro de conmutación de servicios móviles ( <i>mobile switching centre</i> )
MT	Terminal móvil ( <i>mobile terminal</i> )
NAI	Identificador de acceso de red ( <i>network access identifier</i> )
NNI	Interfaz red-red ( <i>network-to-network interface</i> )
Nxx	Punto de referencia Nxx
PIAM	Punto en la gestión de autenticación ( <i>point in authentication management</i> )
PIN	Número de identificación personal ( <i>personal identification number</i> )
PNNI	Interfaz red-red privada ( <i>private network-to-network interface</i> )
PSC	Control de servicio por paquetes ( <i>packet services control</i> )
PSCAF	Función de agente de control de servicio por paquetes ( <i>packet service control agent function</i> )
PSCF	Función de control de servicio por paquetes ( <i>packet service control function</i> )
PSGCF	Función de control de pasarela de servicio por paquetes ( <i>packet service gateway control function</i> )
PU-RDSI	Parte usuario de la RDSI ( <i>ISDN user protocol</i> )
PU-RDSI-BA	Parte usuario de la RDSI de banda ancha
PU-RDSI-BE	Parte usuario de la RDSI de banda estrecha
QoS	Calidad de servicio ( <i>quality of service</i> )
RACAF	Función de agente de control de acceso radioeléctrico ( <i>radio access control agent function</i> )
RAN	Red de acceso radioeléctrico ( <i>radio access network</i> )
RDSI	Red digital de servicios integrados
RF	Radiofrecuencia

RFTR	Transmisión y recepción en radiofrecuencia ( <i>radio frequency transmission and reception</i> )
RI	Red inteligente
RNC	Controlador de red radioeléctrica ( <i>radio network controller</i> )
RPD	Red de datos por paquetes
RTPC	Red telefónica pública conmutada
SACF	Función de control de acceso al servicio ( <i>service access control function</i> )
SCF	Función de control de servicio ( <i>service control function</i> )
SCP	Punto de control de servicio ( <i>service control point</i> )
SDF	Función de datos de servicio ( <i>service data function</i> )
SDP	Punto de datos de servicio ( <i>service data point</i> )
SIBF	Función de difusión de información de acceso al sistema ( <i>system access information broadcast function</i> )
SLP	Programa lógico de servicio ( <i>service logic program</i> )
SMF	Función de gestión de servicio ( <i>service management function</i> )
SMS	Servicio de mensajes cortos ( <i>short message service</i> )
SRF	Función de recursos especializados ( <i>specialized resource function</i> )
SSD	Dato secreto compartido ( <i>shared secret data</i> )
TMUI	Identificador temporal de usuario móvil ( <i>temporary mobile user identifier</i> )
TTG	Traducción del título global
UDP	Protocolo de datagrama de usuario ( <i>user datagram protocol</i> )
UIM	Modulo de identidad de usuario ( <i>user identity module</i> )
UIMF	Función de gestión de identificación de usuario ( <i>user identification management function</i> )
UPT	Telecomunicaciones personales universales ( <i>universal personal telecommunications</i> )
VHE	Entorno originario virtual ( <i>virtual home environment</i> )
VSC	Control de servicios de entorno originario virtual ( <i>VHE services control</i> )

## 5 Introducción

Los entornos de señalización NNI presentados en esta Recomendación UIT-T constituyen una ayuda para los diseñadores de protocolo en el desarrollo de los protocolos específicos que gobiernan las interacciones entre redes centrales de la familia de sistemas IMT-2000. Estos requisitos se dividen en dos partes, aplicaciones y protocolos, y se organizan en 12 cláusulas como se muestra en adelante. Las cláusulas 1 a 5 son requisitos de documentación generales que proporcionan una descripción del alcance de esta Recomendación UIT-T, un resumen breve del contenido de esta Recomendación UIT-T, referencias, abreviaturas, definiciones y terminología, y la presente introducción. La cláusula 6 contiene todos los requisitos generales y relativos a la aplicación, incluidos los requisitos de capacidades de servicios, almacenamiento de datos y perfil de abonado. Estudia también todos los aspectos de la modelización funcional de la NNI. La cláusula 7 identifica y describe todos los puntos de referencia FE-FE relativos al protocolo. En esa cláusula se examinan un total de 20 puntos

de referencia. Las cláusulas 8 a 12 se refieren a los requisitos de protocolo de la movilidad, el control de servicios VHE y RI, el control del servicio por paquetes y del servicio Internet y el intercambio entre redes modulares de información y datos de seguridad.

## 6 Requisitos generales

### 6.1 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.

El conjunto de requisitos NNI numerados siguiente proporciona el punto de arranque para la construcción de un conjunto completo en las secciones sucesivas. Los requisitos están deliberadamente orientados al único objetivo de posibilitar un seguimiento fácil y eficaz.

- 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).

### 6.2 Requisitos de control de servicios VHE

El entorno originario virtual debe proveerse de acuerdo con los escenarios identificados, en la Recomendación UIT-T Q.1711 [2]. En esta Recomendación UIT-T se identifican dos escenarios:

**Instrucción originaria directa:** Este escenario exige la invocación de la lógica de servicio para pedir instrucción/información a la SCFsn. En este escenario el preacuerdo entre las redes soporte y originaria o entre las redes soporte y visitada puede tener que precisar la selección de capacidades de activación de la invocación.

**Control de servicio de repetición:** Este escenario solicita la invocación de la lógica del servicio vía la SCFh o la SCFv para pedir una instrucción/información a la SCFsn. En este escenario el preacuerdo entre las redes soporte y originaria o entre las redes soporte y visitada abarca desde las capacidades de repetición, seguridad/selección a la lógica de servicio compartida.

#### 6.2.1 Entorno originario virtual (VHE) basado en la programación a distancia

Soporte de VHE mediante telecarga de la lógica del servicio y de los datos relativos al servicio desde la red originaria a la red sirviente y al UIM.

#### 6.2.2 Capacidades de servicio

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

---

<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.

**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.

### 6.3 Requisitos de almacenamiento de datos de CN para el perfil de abonado (usuario)

Los siguientes elementos de información son almacenados en la red originaria del abonado, así como el sujeto de la información de abonado y las actividades de gestión del perfil:

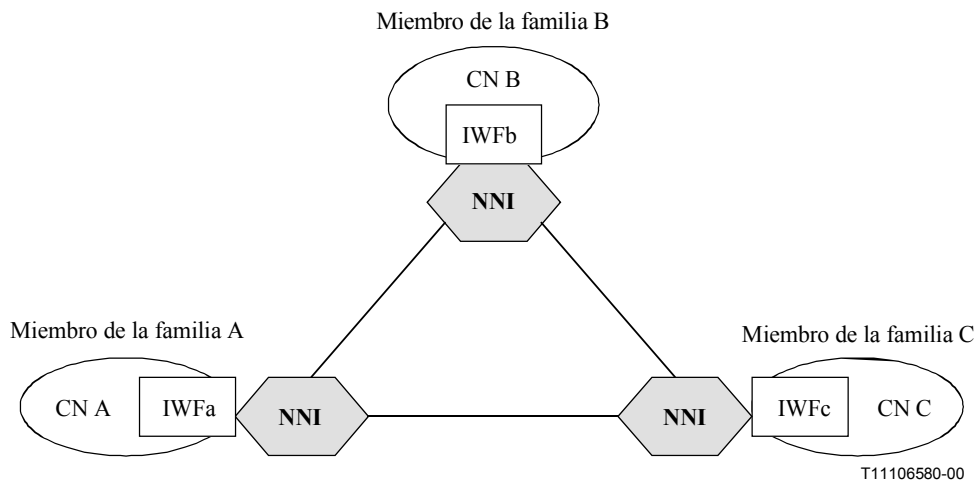
- número de directorio móvil IMT-2000 (IMDN, *IMT-2000 mobile directory number*), por ejemplo, un número "marcable",
- ID de usuario móvil IMT-2000 (IMUI, *IMT-2000 mobile user ID*),
- ID de usuario móvil temporal IMT-2000 (TMUI, *IMT-2000 temporary mobile user ID*),
- estado del terminal,
- información 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 y,
- datos de abono VHE.

### 6.4 Requisitos de itinerancia global

La interfaz red-red (NNI) es un protocolo común y único de interfaz red central-red central que soporta la capacidad de itinerancia global de las 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 6-1 se representa el cometido que puede desempeñar 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 6-1 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 (en desarrollo en el UIT-T).
- Eficacia: Se necesita una 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.

Mientras que el desarrollo del protocolo NNI corresponde al UIT-T, el desarrollo de la IWF es competencia de cada miembro de la familia.



**Figura 6-1/Q.1751 – Modelo de interconexión de redes IMT-2000**

## 6.5 Agrupaciones de comunicaciones NNI

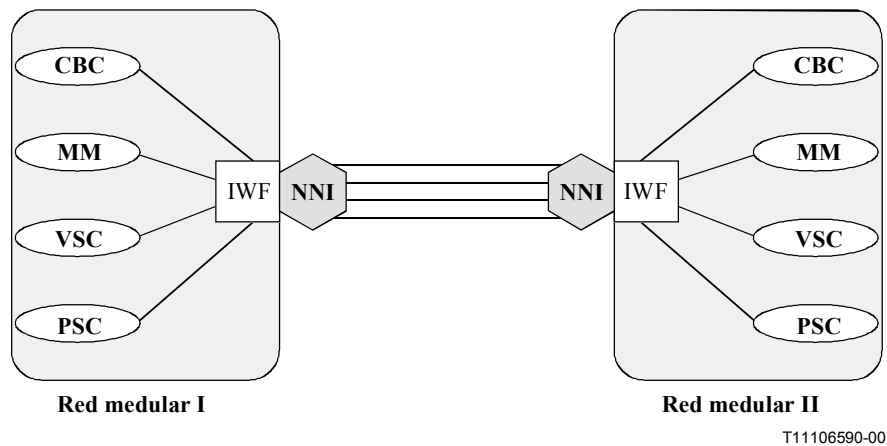
Se reconocen cuatro agrupaciones principales y distintas de comunicaciones en operaciones de CN transversales IMT-2000. La distinción se deriva de la naturaleza de las operaciones que ellas soportan mediante la constitución de un protocolo de aplicación NNI único y común. Estos grupos de comunicaciones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

Dentro del contexto de un protocolo NNI común y único descrito en 6.4, estas agrupaciones se ilustran con más detalle la figura 6-2 a continuación:





**Figura 6-2/Q.1751 – 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 7 que se ilustra en la figura 7-1.

## 6.6 Servicios de Internet

- 1) El abonado de datos por paquetes itinerante debe ser capaz de acceder a la red pública Internet, a un proveedor de servicios Internet (ISP) originario o a una red privada desde múltiples proveedores de servicio IMT-2000, aunque mantenga una relación cliente-vendedor con un solo proveedor del servicio IMT-2000.
- 2) El abonado debe indicar explícitamente qué acceso de servicio de datos (esto es, acceso a servicios públicos Internet, a un ISP originario a una red privada) está solicitando.
- 3) El abonado debe poder establecer sesiones de datos simultáneas a la Internet pública, a un ISP originario o a una red privada y disponer de diferentes direcciones IP e identificadores de acceso de red (NAI, *network access identifier*) para los respectivos servicios de acceso. La red de datos por paquetes puede utilizar la dirección IP de destino o el NAI, que puede incluirse en la petición de registro de sesión para determinar el destino de la sesión de datos por paquetes.
- 4) La NNI debe poder soportar la calidad de servicio (QoS, *quality of service*) mediante la asignación del tráfico de usuario a una clase de servicio diferenciada y específica, paquete a paquete, para el transporte por Internet. La NNI debe poder también asignar el tráfico de todos los usuarios a una clase de servicio específica destino por destino.

## 6.7 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 6-1). La NNI transportará información sobre los usuarios (por ejemplo, posición, autorización, autenticación y claves de criptación) y las redes (es decir, señalización y control); esta información debe guardarse protegida contra los intrusos. Esta Recomendación UIT-T trata los aspectos de seguridad del transporte de la información.

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

### **6.7.1 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 criptación y privacidad puede formar parte del procedimiento de autenticación.
- El compromiso de un móvil individual no deberá comprometer la seguridad de la red global.

### **6.7.2 Requisitos de criptación para la interfaz red-red**

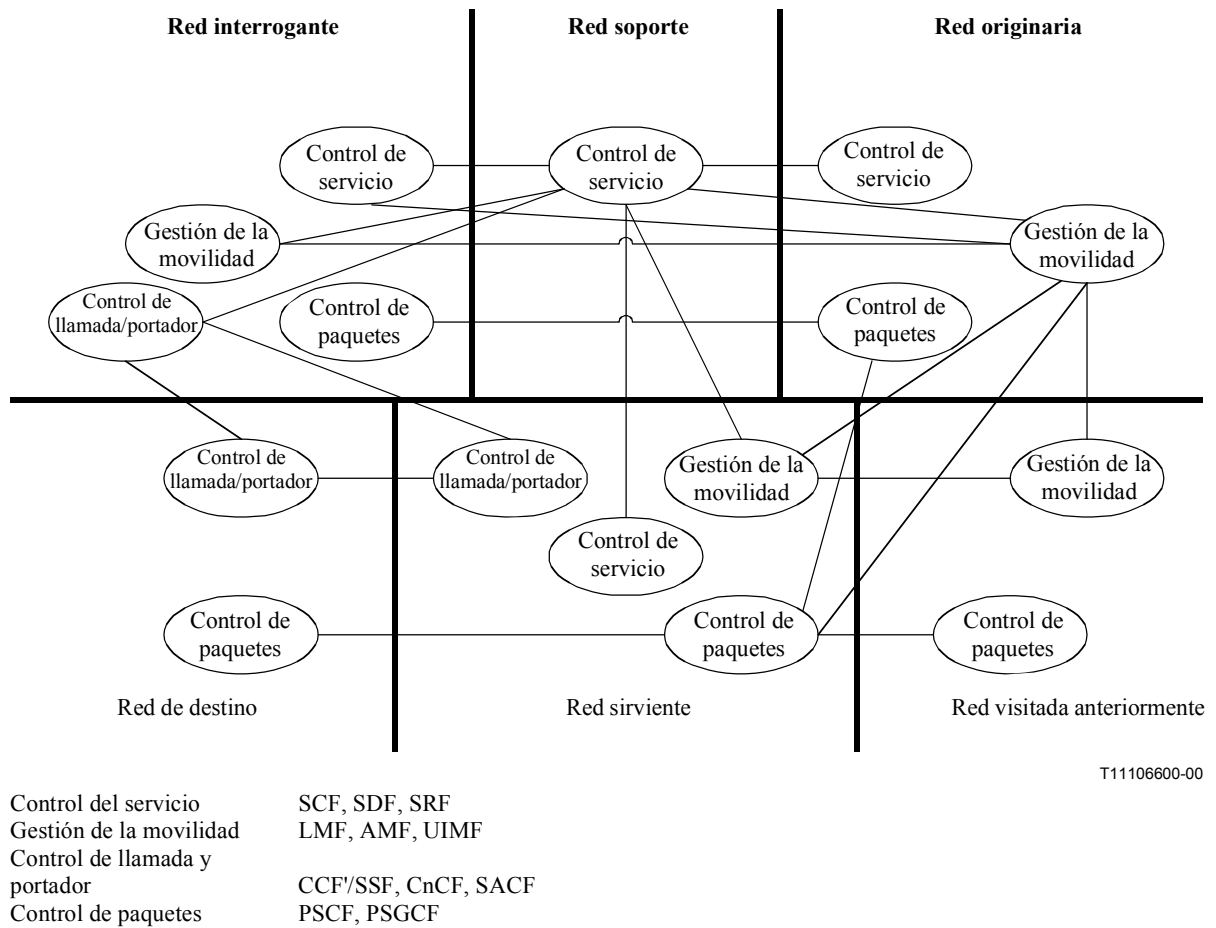
- Los mecanismos de criptación de la NNI deben cumplir los requisitos legales impuestos por los organismos reguladores (por ejemplo, controles de exportación, interceptación legal).
- Los mecanismos de criptación de la NNI deben ser capaces de criptar a velocidades de multimegabits por segundo, sin ningún compromiso para la seguridad.
- La seguridad de NNI deberá poder proporcionar la autenticación mutua entre los elementos de red.

### **6.7.3 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 criptación 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).

## **7 Modelo de interconexión**

En la figura 7-1 a continuación se ilustran las relaciones que habrá de soportar la NNI para soportar las CS-1 IMT-2000. Todas las entidades funcionales contenidas en cada red no se muestran necesariamente aquí (por ejemplo, la red originaria puede contener SCF y SDF, la red previamente visitada puede contener PSGCF). Más bien la diferenciación al atravesar las fronteras pretende mostrar cuales son las entidades funcionales pertinentes a la función de red particular a efectos de interoperabilidad NNI. Con el fin de evitar la confusión de la figura, no se muestran en la misma las relaciones intrared.

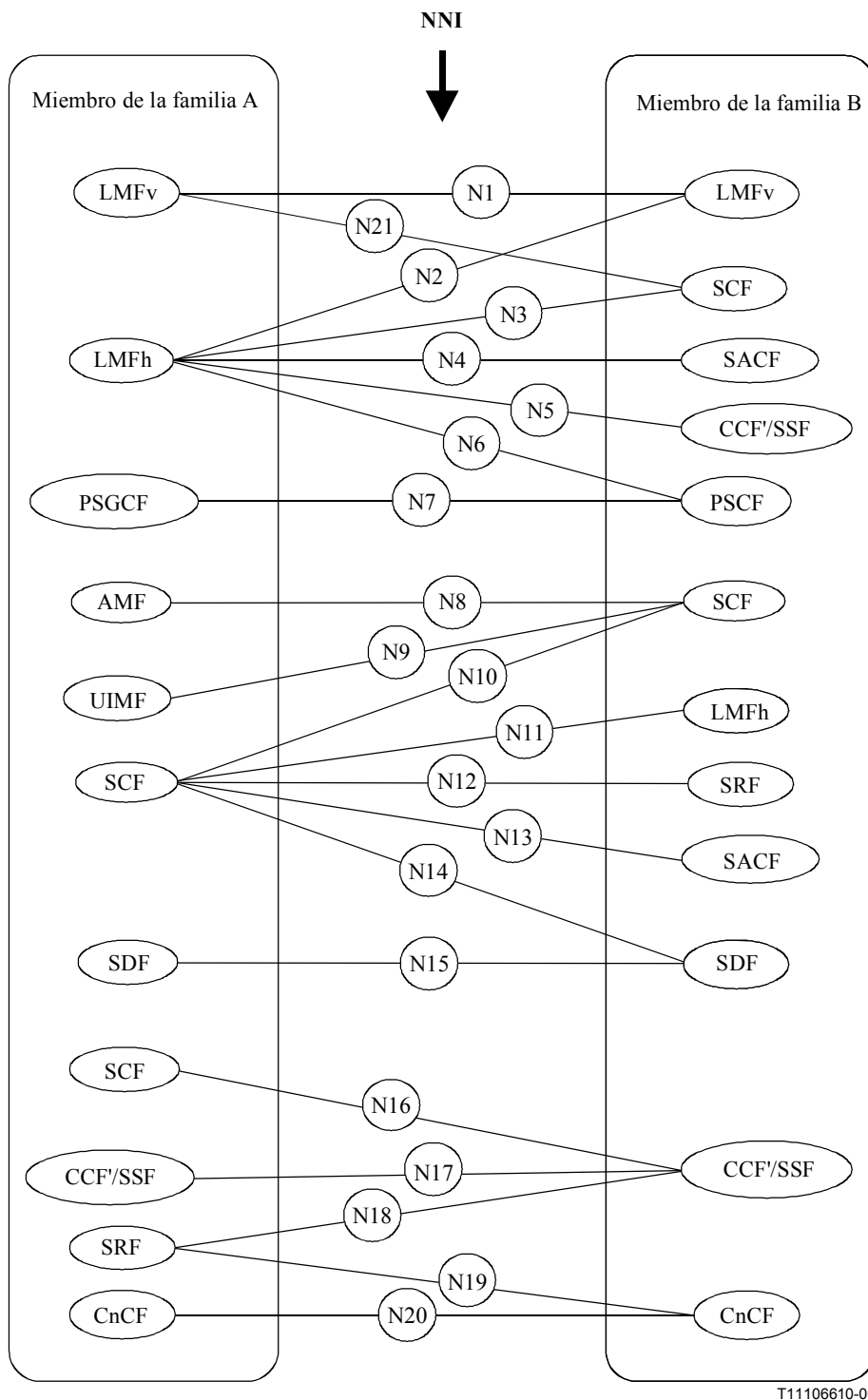


**Figura 7-1/Q.1751 – Modelo de interconexión de red IMT-2000**

## 8 Interfaz funcional NNI

### 8.1 Modelo funcional

La figura 8-1 muestra el "Modelo de interfaz funcional NNI". Su propósito es centrar la presente Recomendación UIT-T solamente en aquellas interfaces que pertenecen a la NNI en un nivel funcional. La figura 7-1 "Modelo de interconexión de red IMT-2000" (NIM, *IMT-2000 network interconnection model*) y la figura 8-1 "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 8-1/Q.1751 – Modelo de interfaz funcional NNI**

## 8.2 Puntos de referencia

Los puntos de referencia (Nxx), que se muestran en la figura 8-1, 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>).

<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.

Obsérvese 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.

### **8.2.1 Punto de referencia N01**

El punto de referencia N01 es la interfaz funcional LMFv a LMFv. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la gestión de la información de abonado [por ejemplo, la recuperación de la IMUI basada en el identificador de usuario móvil temporal (TMUD)].

### **8.2.2 Punto de referencia N02**

El punto de referencia N02 es la interfaz funcional LMFh a LMFv. Por ejemplo, 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.

### **8.2.3 Punto de referencia N03**

El punto de referencia N03 es la interfaz funcional LMFh a SCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- los servicios de RI relacionados con la gestión de posiciones.

### **8.2.4 Punto de referencia N04**

El punto de referencia N04 es la interfaz funcional LMFh a SACF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la transferencia de información de encaminamiento para el establecimiento de las comunicaciones;
- la transferencia de peticiones relativas a la autenticación;
- la gestión de información de movilidad básica, tal como:
  - 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:
  - mensajes SMS;
  - 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.

### **8.2.5 Punto de referencia N05**

El punto de referencia N05 es la interfaz funcional LMFh a CCF'/SSF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la transferencia de información de encaminamiento para el establecimiento de las comunicaciones;
- la transferencia de información de perfil incluidas capacidades de servicio, como:
  - información de protocolo;
  - información de portador.

### **8.2.6 Punto de referencia N06**

El punto de referencia N06 es la interfaz funcional LMFh a PSCF. Por ejemplo, la mensajería NNI por esta interfaz funcional 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.

### **8.2.7 Punto de referencia N07**

El punto de referencia N07 es la interfaz funcional PSGCF a PSCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- 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.

### **8.2.8 Punto de referencia N08**

El punto de referencia N08 es la interfaz funcional AMF a SCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- los servicios de RI relativos a la autenticación del usuario.

### **8.2.9 Punto de referencia N09**

El punto de referencia N09 es la interfaz funcional UIMF a SCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la transferencia de los datos/lógica del servicio;
- la modificación del perfil del servicio;
- el intercambio de información de aplicación.

### **8.2.10 Punto de referencia N10**

El punto de referencia N10 es la interfaz funcional SCF a SCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la adquisición y manipulación de datos asegurados;
- el control de servicio distribuido;
- notificaciones de servicio no solicitadas.

### **8.2.11 Punto de referencia N11**

El punto de referencia N11 es la interfaz funcional SCF a LMFh. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- que la LMFh proporcione la posición del MT y el estatus del abonado a la SCF.

### **8.2.12 Punto de referencia N12**

El punto de referencia N12 es la interfaz funcional SCF a SRF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la provisión de recursos especializados para los servicios RI.

### **8.2.13 Punto de referencia N13**

El punto de referencia N13 es la interfaz funcional SCF a SACF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- los servicios de RI basados en eventos de gestión de movilidad, tales como:
  - la gestión de posiciones;
  - la autenticación del usuario;
- servicios de RI no relacionados con la llamada.

### **8.2.14 Punto de referencia N14**

El punto de referencia N14 es la interfaz funcional SCF a SDF. Por ejemplo, la mensajería NNI por esta interfaz funcional 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.

### **8.2.15 Punto de referencia N15**

El punto de referencia N15 es la interfaz funcional SDF a SDF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- el intercambio de datos de servicio.

### **8.2.16 Punto de referencia N16**

El punto de referencia N16 es la interfaz funcional SCF a CCF'/SSF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- los servicios de RI relativos a la llamada.

### **8.2.17 Punto de referencia N17**

El punto de referencia N17 es la interfaz funcional CCF'/SSF a CCF'/SSF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

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

### **8.2.18 Punto de referencia N18**

El punto de referencia N18 es la interfaz funcional SRF a CCF'/SSF, cuando el control de llamada y de conexión están integrados. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- el control de portadores a SRF para servicios de RI, en relación con:
  - el establecimiento;
  - el mantenimiento;

- 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.

### 8.2.19 Punto de referencia N19

El punto de referencia N19 es la interfaz funcional SRF a CnCF, cuando el control de llamada y de conexión están integrados. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- el control de portadores a la SRF para servicios de RI, en relación con:
  - el establecimiento;
  - el mantenimiento;
  - la liberación.

### 8.2.20 Punto de referencia N20

El punto de referencia N20 es la interfaz funcional CnCF a CnCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- la gestión de instancias de conexión, en relación con:
  - el establecimiento;
  - el mantenimiento;
  - la modificación;
  - la liberación;
- la gestión de las asociaciones de control de portador, en relación con:
  - el establecimiento;
  - el mantenimiento;
  - la liberación.

### 8.2.21 Punto de referencia N21

El punto de referencia N21 es la interfaz funcional LMFv a SCF. Por ejemplo, la mensajería NNI por esta interfaz funcional posibilita:

- los servicios de RI relativos a la gestión de posiciones.

## 9 Requisitos de protocolo para la gestión de la movilidad

### 9.1 Activadores del servicio

Los siguientes activadores de servicio de RI se detallan más adelante en esta Recomendación UIT-T, y 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.

## 9.2 Modos de interacción de la lógica de servicio

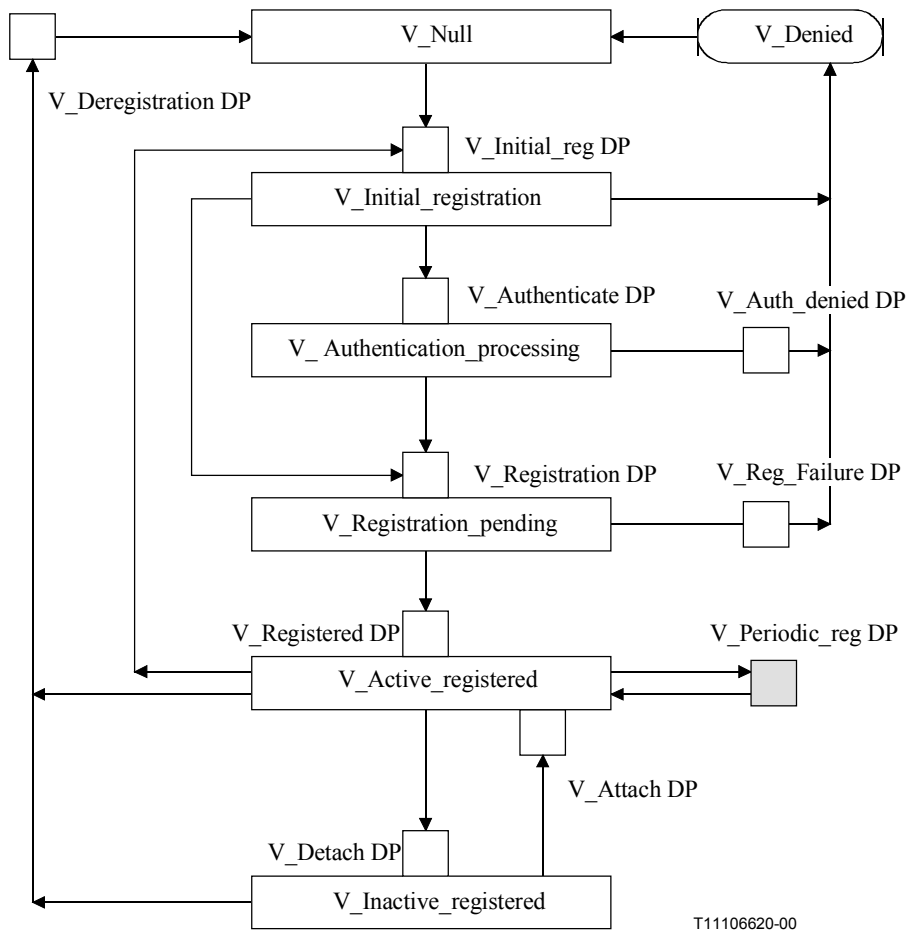
Entre las características del servicio detalladas en 9.1, la lógica de servicio que controla el proceso de gestión de movilidad puede clasificarse en los dos tipos siguientes:

- **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.

## 9.3 Modelo de estados LMFv

La figura 9-1 es una representación esquemática del modelo de estados LMFv que muestra varios estados posibles del terminal móvil en la red visitada. Incluye la identificación de todos los puntos de detección (DP, *detection points*) de entrada y salida para cada estado. Estos estados y los DP son descritos con más detalle a continuación.

Los DP con activadores de servicio no identificados se muestran en gris. En el futuro, estos DP pueden eliminarse si no se proporciona una justificación del servicio. La supresión de estos DP no repercutirá en la validez del modelo (incluidos estados, eventos, transiciones de estados y acciones).



**Figura 9-1/Q.1751 – Modelo de estado LMFv**

### 9.3.1 State: v\_Null

#### Descripción

Estado inicial (el usuario móvil no es conocido en la LMFv) y LMFv espera petición de registro.

#### Eventos de entrada

- Recepción de cancelación de posición del MT (DP: v\_Deregistration).
- Completado el tratamiento de autorización o registro denegado para el MT. (Transición de v\_Denied.)

#### Acciones

- Suprime el perfil de abonado si está presente y libera los demás recursos asignados al MT.

#### Eventos de salida

- Se recibe una petición de registro para el MT (DP: v\_Initial\_reg).

### 9.3.2 State: v\_Initial\_Registration

#### Descripción

Se inicia el registro de usuario y se adopta una decisión sobre el proceso de autenticación.

#### Eventos de entrada<sup>3</sup>

- Se recibe una petición de registro para el MT (DP: v\_Initial\_reg).
- Se recibe una petición de registro para el MT para una nueva zona de posición (mientras está en el estado activo) (DP: v\_Initial\_reg).

#### Acciones

- Inicia el registro del usuario y reúne información sobre el usuario (por ejemplo, información de autenticación e identidad de usuario de la red visitada anterior).
- Decide si se realizará o no la autenticación. El modo de adoptar esta decisión es específico del operador.

#### Eventos de salida

- Se efectuará la autenticación: autenticar (DP: v\_Authenticate).
- No se efectuará la autenticación: no autenticar (DP: v\_Registration).
- El registro falla (Transición a v\_Denied).

### 9.3.3 State: Proceso de V\_Authentication

#### Descripción

Se procesa la autenticación.

#### Eventos de entrada<sup>3</sup>

- La autenticación es necesaria (DP: v\_Authenticate).

#### Acciones

- Recupera nuevos parámetros de autenticación si no hay ninguno disponible.
- Procesa la autenticación.

#### Eventos de salida

- La autenticación tiene éxito (DP: v\_Registration).
- La autenticación falla (DP: v\_Auth\_denied).

<sup>3</sup> Considerando los requisitos en tiempo real en la red, estos DP se deben implementar para notificación sin suspender el procesamiento de la gestión de posiciones (equivalente a TDP-N).

### 9.3.4 State: V\_Registration\_pending

#### Descripción

Se procesa el registro para el MT.

#### Eventos de entrada<sup>3</sup>

- El MT ha sido autenticado satisfactoriamente (DP: v\_Registration)
- La autenticación no habrá de efectuarse: no autenticar (DP: v\_Registration).

#### Acciones

- Tratamiento de registro para el MT.
- Un registro de abonado es llenado y actualizado con información de posición del MT y con el periodo de autorización y otras informaciones.
- Se recupera el perfil del abonado.

#### Eventos de salida

- El registro se efectúa con éxito (DP: v\_Registered).
- El registro falla (DP: v\_Reg\_Failure).

### 9.3.5 State:V\_Active\_registered

#### Descripción

El MT está registrado y se supone que es alcanzable.

#### Eventos de entrada

- El registro se ha efectuado con éxito (DP: v\_Registered).
- Se recibe una petición de registro de un MT independiente (DP:v\_ Attach).
- Se recibe una petición de registro para el MT en la misma zona de posición (DP: v\_Periodic\_reg).

#### Acciones

- Mantiene el puntero de posición del MT y fija el estatus de MT a activo.
- Si se solicita, proporciona una dirección de encaminamiento para el establecimiento de un trayecto de intercambio de información (por ejemplo, entrega de llamada, entrega de mensaje corto). Solicita radiobúsqueda antes de devolver una dirección de encaminamiento [ésta es una opción de la red visitada].
- Si se solicita, proporciona una notificación de que el MT ha sido registrado con éxito y se encuentra activo.
- Si se solicita, proporciona información basada en el perfil de servicio del abonado.

#### Eventos de salida

- Se recibe una petición de registro para el MT en la misma zona de posición (DP: v\_Periodic\_reg).
- Se recibe una petición independiente para el MT (DP: v\_Detach).
- Se recibe una petición de cancelación de registro para el MT (DP: v\_Deregistration).
- Se recibe una petición de registro para el MT en una zona de posición nueva. (DP: v\_Inital\_reg).

### 9.3.6 State: v\_Inactive\_registered

#### Descripción

El MT está registrado, pero no es alcanzable. Los datos de usuario y el perfil de servicio están todavía retenidos en la red visitante.

#### Eventos de entrada

- **Se recibe una petición independiente para el MT (DP: v\_Detach).**

#### Acciones

- Mantiene el puntero de posición del MT y fija el estatus del MT a inactivo.
- Si se solicita, informa de que el MT está inactivo.

#### Eventos de salida

- Se recibe una petición de registro del MT independiente (DP: v\_Attach).
- Se recibe una petición de cancelación de registro para el MT (DP: v\_Deregistration).

### 9.3.7 State: v\_Denied

#### Descripción

Tratamiento de fallo y denegación de la autenticación y registro.

#### Eventos de entrada

- El registro es denegado durante la autenticación (DP: v\_Auth\_denied) o el registro de posición (DP: v\_Reg\_failure).

#### Acciones

- Proporciona información sobre la denegación de autenticación o registro para el MT.
- Fija el temporizador de excepción.

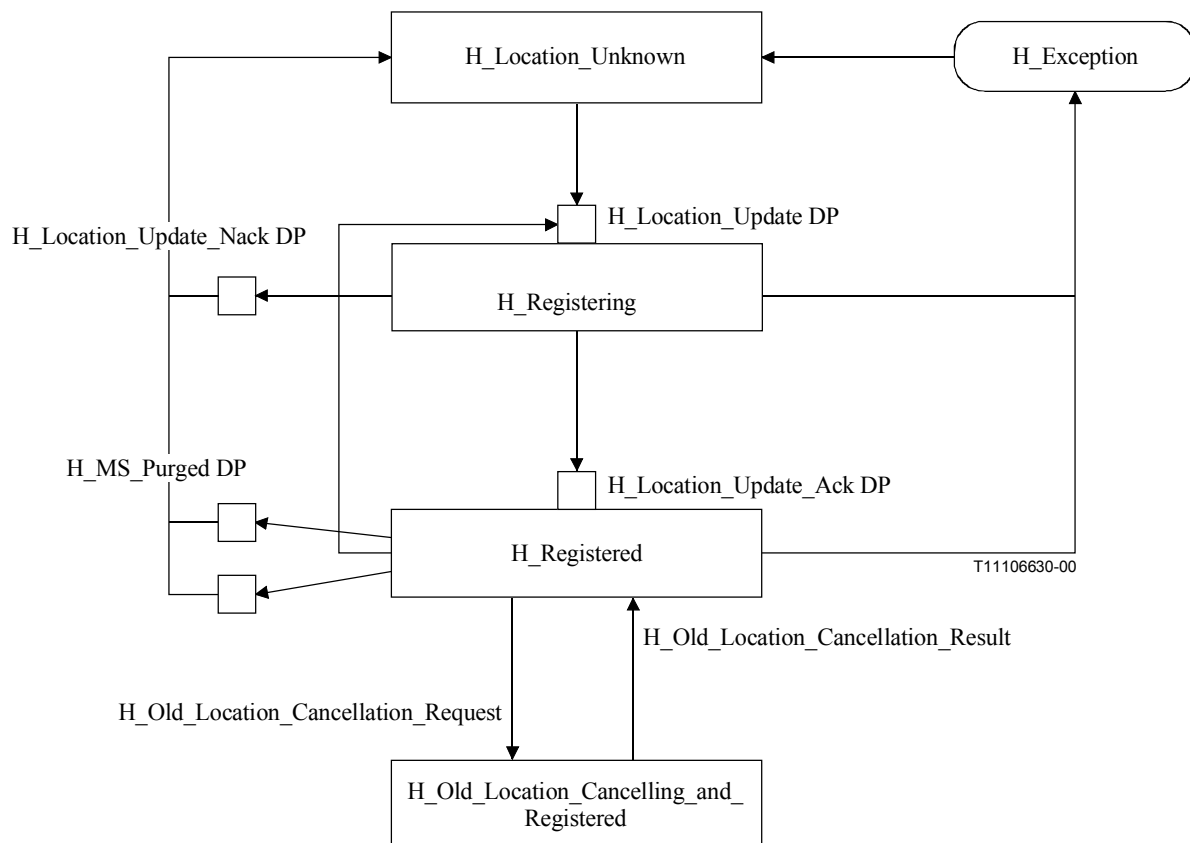
#### Eventos de salida

- El temporizador de excepción expira (Transition to v\_Null).

## 9.4 Modelo de estados LMFh

Esta subcláusula proporciona una descripción de alto nivel del modelo de estados de gestión de posiciones para la LMFh (función de gestión de posiciones), mostrando puntos en la gestión de posiciones (PILM, *points in location management*) y puntos de detección (DP). Se ilustran todas las transiciones posibles DP a PILM y PILM a DP.

En el futuro, estos DP pueden eliminarse si no se proporciona una justificación del servicio. La supresión de estos DP no repercutirá sobre la validez del modelo (incluidos estados, eventos, transiciones de estados y acciones).



**Figura 9-2/Q.1751 – Modelo de estados de gestión de posiciones para la LMFh**

#### 9.4.1 State H\_Location\_Unknown

##### Descripción

Se desconoce la posición del abonado móvil y los servicios de terminación (por ejemplo, terminación de llamadas móviles, terminación SMS, etc.) no pueden ser tratados.

##### Eventos de entrada

- Abonado móvil purgado (DP: H\_MS\_Purged).
- Registro de abonado móvil en el dominio visitado cancelado por LMFh (DP: H\_present\_location\_cancelled).
- Se produce una excepción (PILM: H\_Exception).

##### Acciones

- Ninguna.

##### Eventos de salida

- Abonado móvil registrado a la red móvil (DP: H\_Location\_Update, observando las restricciones descritas en el estado H\_Registering).

## 9.4.2 State H\_Registering

### Descripción

El abonado móvil que ha cambiado de entre zonas de servicio, o se ha ligado a una zona, dentro de la red móvil, ha de transferir su perfil de servicio a la zona de servicio, y ha de actualizarse la información de posición del abonado.

### Eventos de entrada<sup>4</sup>

- El abonado móvil registrado a la red móvil (DP: H\_Location\_Update).
- El abonado móvil ha estado itinerante entre zonas de servicio (DP: H\_Location\_Update).

### Acciones

- Comprobar si el abonado es conocido dentro de la base de datos.
- Autorizar el acceso a la red del abonado móvil.
- Transferir el perfil del abonado móvil a la nueva zona de servicio.
- Actualizar la información de posición del abonado móvil dentro de la base de datos.

### Eventos de salida

- Respuesta negativa a la petición de actualización de posición (es decir, tal como abonado desconocido, abonado rechazado, etc.) (DP: H\_Location\_Update\_Nack).
- Respuestas positiva a la petición de actualización de posición (DP: Location\_Update\_Ack).
- Se produce una excepción (PILM: H\_Exception).

## 9.4.3 State H\_Registered

### Descripción

La posición del abonado móvil es conocida y los servicios de terminación (es decir, terminación de llamadas móviles, terminación SMS, etc) pueden ser tratados.

### Eventos de entrada

- Actualización exitosa de la posición (DP: H\_Location\_Update\_Ack).
- Cancelación exitosa o no de la posición en la LMFv antigua (PILM: H\_old\_registration\_cancellation\_result).

### Acciones

- Tratar peticiones de posición para servicios de terminación.
- Tratar las actualización de perfil de servicio en la LMF visitada. Estas actualizaciones de perfil no tendrán repercusión en las llamadas en curso o en otros servicios en curso.

### Eventos de salida

- Decisión de cancelar el registro (DP: H\_present\_location\_cancelled).
- Decisión de suprimir el abonado en la LMFv antigua (PILM: H\_old\_location\_cancellation\_request).
- Indicación de la LMFv de que el MS ha sido purgado (DP: H\_MS\_Purged)
- El abonado móvil se desplazó a otra zona de servicio (DP: Location\_Update, observando las restricciones descritas en el estado H\_Registering).
- Se produce una excepción (PILM: Exception).

<sup>4</sup> Considerando los requisitos en tiempo real en la red, estos DP se deben implementar para notificación sin suspender el procesamiento de la gestión de posiciones (equivalente a TDP-N).

#### 9.4.4 State H\_Old\_Location\_Cancelling\_and\_Registered

##### Descripción

Se cancela el registro de abonado en la LMFv antigua.

##### Eventos de entrada

- Decisión por la LMFh de cancelar la posición en la LMFv (PILM: H\_Old\_Location\_Cancellation\_Request).

##### Acciones

- Interactuar con la LMFv antigua para cancelar la posición.
- Actualizar la información de posición del abonado móvil dentro de la base de datos.

##### Eventos de salida

- Cancelación exitosa o no de la posición (PILM: H\_Old\_Location\_Cancellation\_Result).

#### 9.4.5 State H\_Exception

##### Descripción

Tratamiento de los fallos y excepciones.

##### Eventos de entrada

Las excepciones HLR ocurren durante el proceso de los estados H\_registered y H\_registering.

##### Acciones

- Tratamiento de excepciones para un abonado móvil específico.

##### Eventos de salida

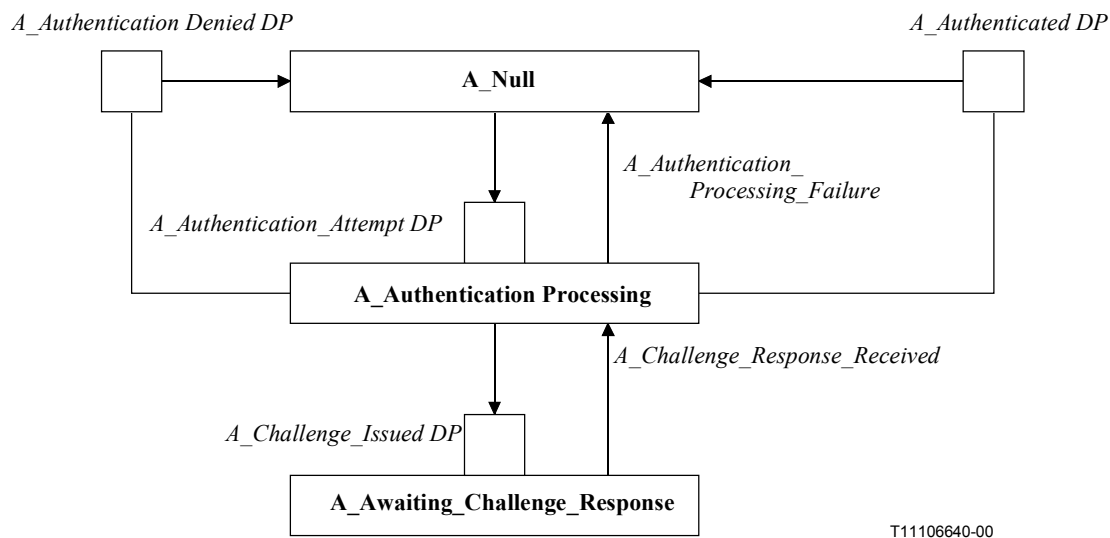
Tratamiento de excepción completado (transición a H\_Location\_Unknown).

#### 9.5 Modelo de estados AMF

Esta subcláusula proporciona una descripción alto nivel del modelo de estados función de gestión de autenticación (AMF, *authentication management function*) (véase la figura 9-3) mostrando puntos en la gestión de autenticación (PIAM, *points in authentication management*) y puntos de detección (DP). Se ilustran todas las transiciones posibles DP a PIAM y PIAM a DP. Este modelo de estados AMF (AFM SM) se aplica a las situaciones de red originaria y red visitada. Se crea un ejemplar de modelo de estados de autenticación en la AMF en la cual se procesa la autenticación. Esto excluye el proceso en que se generan los parámetros de autenticación. Dependiendo de la implementación, está ubicado en la red originaria o en la red visitada. La utilización de la AMF propia o de la AMF visitada es una decisión del operador.

En el futuro, estos DP pueden eliminarse si no se proporciona una justificación del servicio. La supresión de estos DP no repercutirá en la validez del modelo (incluidos estados, eventos, transiciones de estados y acciones).





**Figura 9-3/Q.1751 – Modelo de estados AMF**

### 9.5.1 State: A\_Null

#### Descripción

Estado inicial (la AMF espera una petición de autenticación del usuario móvil).

#### Eventos de entrada

- Se produce el fallo del proceso de autenticación. (PIAM: A\_Authentication\_Processing\_Failure).
- La autenticación es denegada. (DP: A\_Authentication\_Denied DP).
- La autenticación tiene éxito (DP: A\_Authenticated DP).

#### Acciones

- Ninguna.

#### Eventos de salida

- Se recibe una petición de autenticación (DP: A\_Authentication\_Attempt).

### 9.5.2 State: Authentication\_Processing

#### Descripción

Tiene lugar el proceso de autenticación del usuario.

#### Eventos de entrada

- Se recibe una petición de autenticación (DP: A\_Authentication\_Attempt DP).
- Se recibe el resultado de la Awaiting\_Challenge\_Response (PIAM: A\_Challenge\_Response\_Received).

#### Acciones

- Se actualiza la cuenta de llamadas si es necesario.
- Se generan, en caso necesario, las claves de privacidad.
- Se realiza el tratamiento de autenticación y, dependiendo del resultados del estado A\_Awaiting\_Challenge\_Response, bien la autenticación tiene éxito o bien es denegada.

#### Eventos de salida

- Se produce el fallo del tratamiento de autenticación (PIAM: A\_Null).
- Se emite una puesta a prueba de autenticación (el tratamiento SCF puede ocurrir en este punto) (DP: A\_Challenge\_Issued DP).
- La autenticación tiene éxito. (DP: A\_Authenticated).
- La autenticación es denegada. (DP: A\_Authentication\_Denied).

### 9.5.3 State: Awaiting\_Challenge\_Response

#### Descripción

La AMF espera una respuesta a la puesta a prueba de autenticación.

#### Eventos de entrada

- Se ha emitido una puesta a prueba de autenticación (DP: A\_Challenge\_Issued DP).

#### Acciones

- Ninguna.

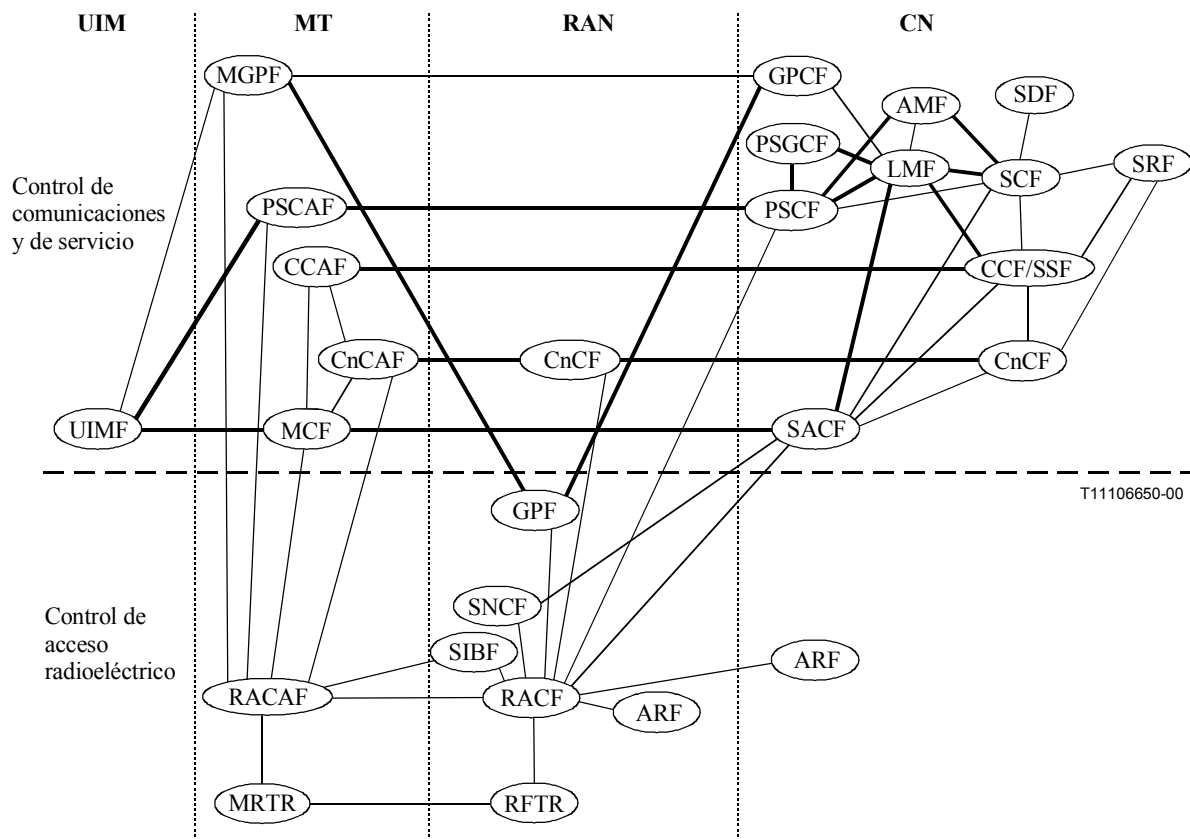
#### Eventos de salida

- La AMF recibe una respuesta a la puesta a prueba de autenticación. (PIAM: A\_Challenge\_Response\_Received).
- Se produce el fallo del tratamiento de autenticación (PIAM: A\_Null).

## 9.6 Comunicaciones funcionales de la gestión de la movilidad

La figura 9-4 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 9-4/Q.1751 – Modelo funcional (gestión de la movilidad) de IMT-2000**

### 9.7 Elección de sucesión de protocolos

Existen ya varios protocolos de movilidad para sistemas 2G, tales como GSM MAP y IS-41. Estos protocolos han sido específicamente concebidos y optimizados para estas 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 (es decir, la sintaxis y la semántica de argumentos y los resultados de estas operaciones de gestión de la movilidad están fuertemente asociadas con la arquitectura y servicios 2G correspondientes).

Los protocolos 2G deben mejorarse para soportar la itinerancia interfamilias entre los diferentes miembros de sistemas IMT-2000. Por consiguiente, el desafío de realizar el protocolo NNI 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 la tecnología de acceso radioeléctrico. En otras palabras, debe ser suficientemente genérico para adecuarse a los diferentes miembros/sistemas de IMT-2000 desde la perspectiva NNI. 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.

## **10 Requisitos de protocolo para el control de servicio del VHE**

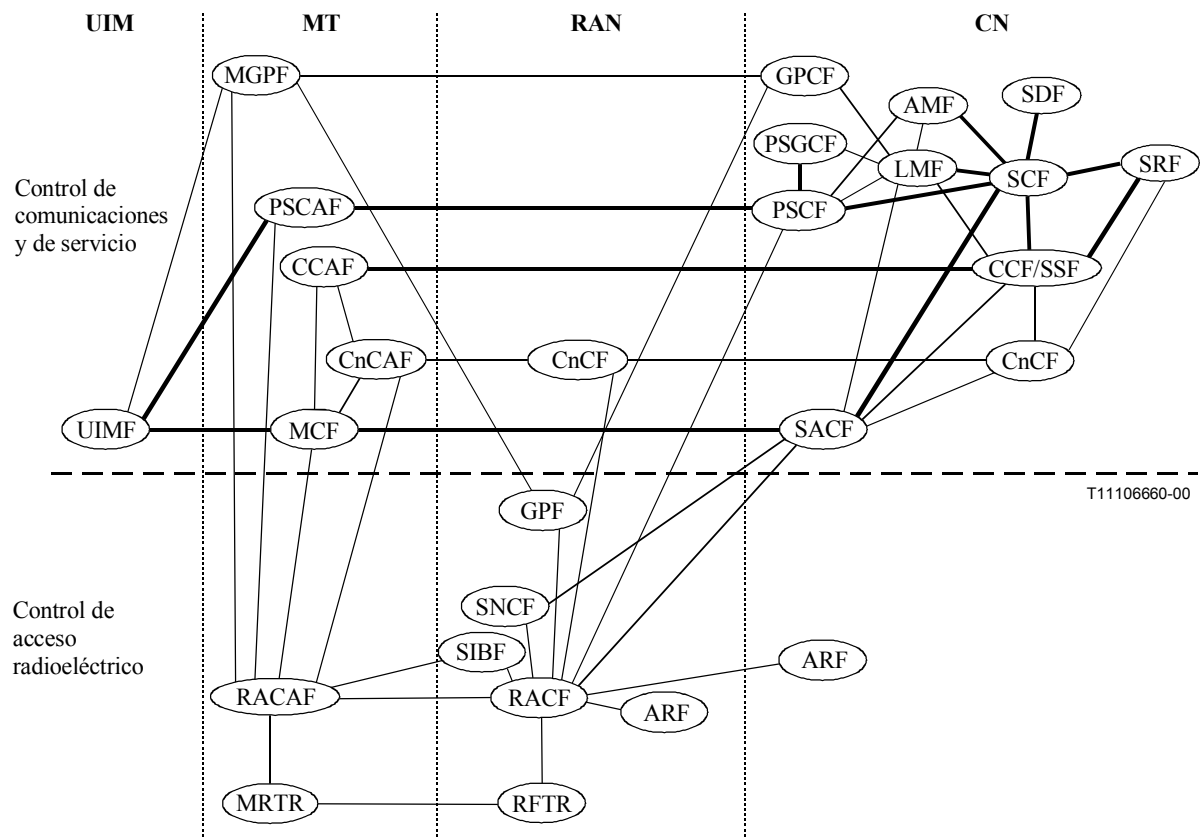
### **10.1 Requisitos generales**

- 1) Para la invocación del servicio de VHE, se recomienda la adición de los siguientes elementos de información a las definiciones de operación pertinentes del INAP (protocolo de aplicación de RI):
  - el abonado es un abonado móvil;
  - identidad del abonado móvil (por ejemplo, IMUI);
  - capacidades del terminal (por ejemplo, voz, datos, etc.);
  - información de posición (por ejemplo, latitud & longitud, emplazamiento de la célula, elevación, precisión, etc.).
- 2) El perfil de activadores que se sitúa geográficamente y de modo dinámico, ha de incluir, además de la identificación de los activadores, criterios de activadores y direcciones de lógica de servicio asociadas con los activadores, la información de versión de protocolo que se utilizará en el programa de lógica de servicio indicado. La versión de protocolo es necesario para asegurar que el mensaje enviado al SLP que es de una versión no superior a la que el SLP puede reconocer y tratar en virtud de su equipamiento.
- 3) Para los flujos de información de servicio VHE que implican el uso de un recurso especializado, estos flujos de información deben estar alineados con las especificaciones de RI.
- 4) Para la provisión del servicio VHE, la SCF y la SRF en la "red soporte" pueden estar situadas en cualquier parte. Por ello se requieren mecanismos de direccionamiento apropiados. Las capacidades de direccionamiento del protocolo INAP para este aspecto deben ser revisadas con el fin de asegurar su adecuación.

### **10.2 Comunicaciones funcionales de control de servicio**

La figura 10.1 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.



**Figura 10-1/Q.1751 – Modelo funcional (control de servicio) de IMT-2000**

### 10.3 Elección de la sucesión de protocolos

Relación	Propuesta de protocolo inicial
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>

## 11 Requisitos de protocolo para el control de llamada y de portador

### 11.1 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.

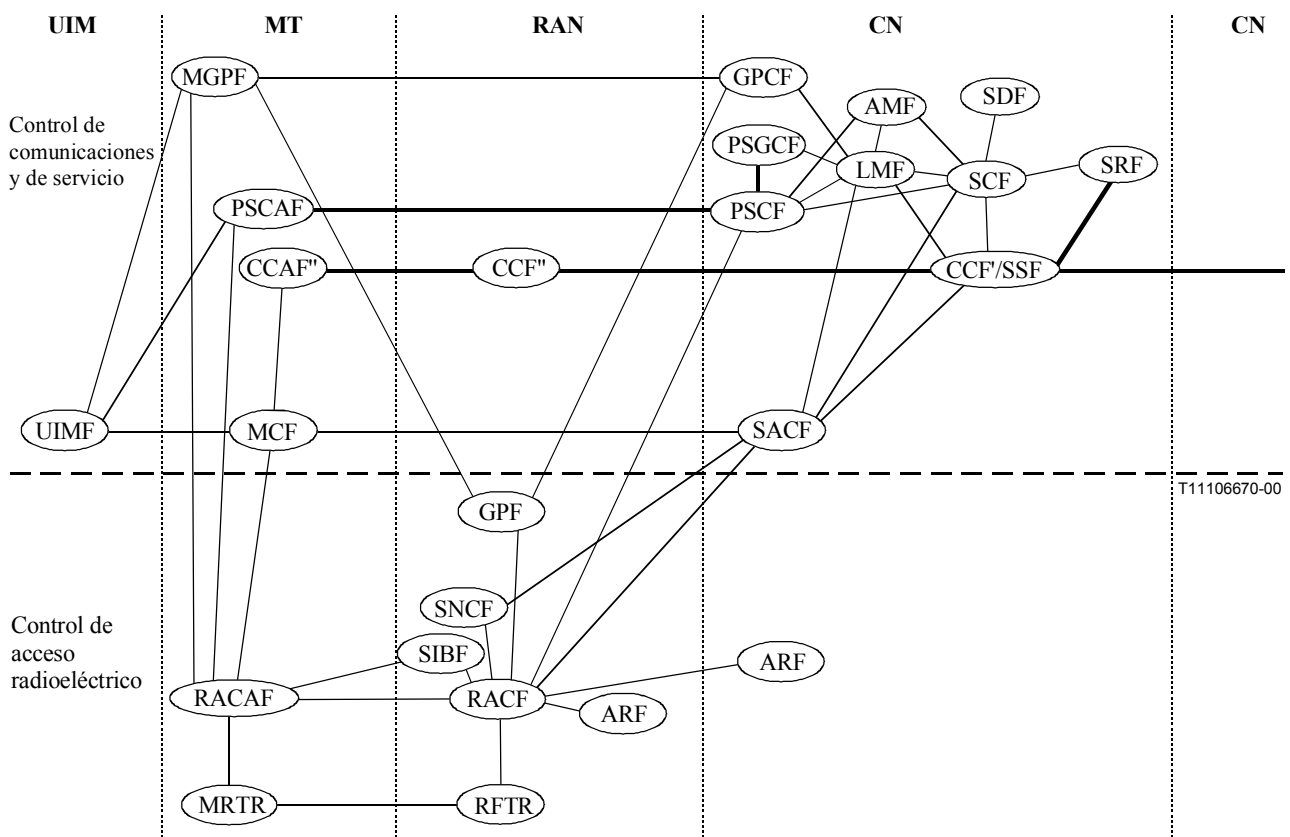
### 11.2 Elección de los principios de conmutación

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

### 11.3 Comunicaciones funcionales del control de llamada y de portador

Las figuras 11-1 y 11-2 se han tomado de la Recomendación UIT-T Q.1711, y se han ampliado para mostrar la interfaz red-red.

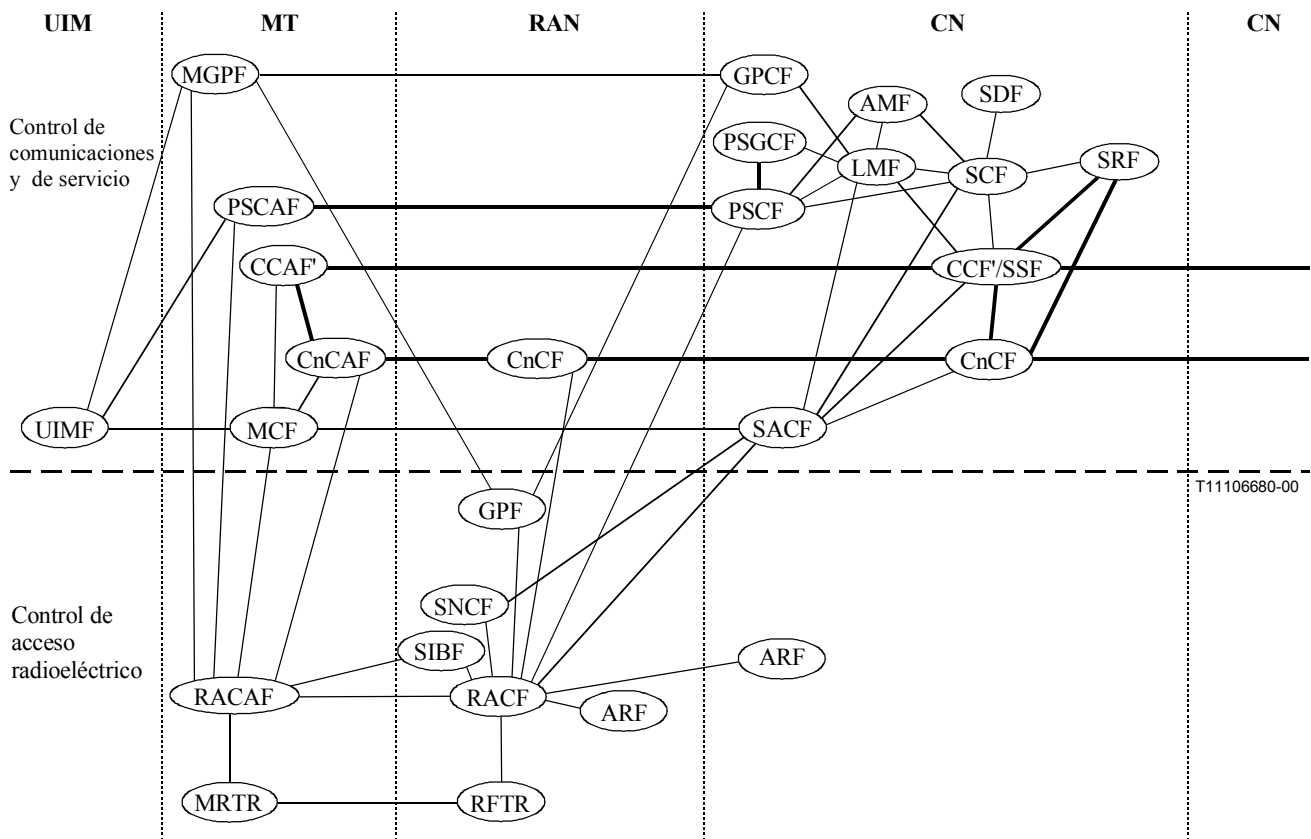
Las relaciones señaladas en línea gruesa caen – total o parcialmente – dentro del ámbito de la señalización de control de llamada y de portador.



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 11-1/Q.1751 – Modelo funcional de IMT-2000**

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



**Figura 11-2/Q.1751 – Modelo funcional de IMT-2000  
Alternativa 2: Entidades funcionales control de conexión y control de llamada separadas**

#### 11.4 Elección de la sucesión de protocolos

Se pueden utilizar los siguientes protocolos para CS-1 de IMT-2000:

Relación funcional	Propuesta de protocolo
CCF'-CCF'	BICC PU-RDSI-BE para STM
CnCF-CnCF	Q.AAL2 para ATM AAL2 PU-RDSI-BA para ATM AAL1  NOTA – No se excluyen otros protocolos análogos a PNNI/ATM o AINI/ATM.

Debido a las constricciones de temporización, se ha asignado a las siguientes relaciones funcionales una prioridad inferior dentro de la trama de tiempo de CS-1 de IMT-2000.

Relación funcional	Propuesta de Protocolo
CCAF'-CCF'	Protocolo específico del miembro de familia dentro de la trama de tiempo de CS-1 IMT-2000
CnCAF-CnCF	
CnCF-CnCF	
PSCAF-PSCF	
PSCF-PSGCF	

Hay que distinguir dos dominios, el dominio RTPC/RDSI y el dominio de datos por paquetes, que pertenecen a los siguientes protocolos:

- 1) *Dominio de servicios RDSI/RTPC*
  - a) Control de llamada: BICC, PU-RDSI-BE para STM
  - b) Control de portador: PU-RDSI-BA para ATM AAL1, Q.AAL2 para ATM AAL2

Es necesario que haya flexibilidad con respecto a la tecnología de transporte IMT-2000 para satisfacer los requisitos de un mercado dinámico y no regulado.

- 2) *Dominio de servicios de datos por paquetes*
  - a) Control de llamada: No se necesita
  - b) Control de portador: Portador ATM AAL5.
  - c) Capa de red: Protocolo Internet (IP).

Es necesario que exista flexibilidad con respecto a la tecnología de transporte IMT-2000 para satisfacer los requisitos de un mercado dinámico y no regulado. Por consiguiente, deberán permitirse diferentes tipos de portador en CS-1 IMT-2000.

### 11.5 Llamadas multimedios

Los requisitos de las llamadas multimedios IMT-2000 incluyen la capacidad de combinar los trenes de los medios en una sola conexión. Los medios se contemplan como tipos diferentes de trenes de datos (por ejemplo, voz, datos, imagen, etc). Estos medios pueden ser multiplexados en una sola conexión y ser controlados (por ejemplo, adición, sustracción de medios) en virtud de Recomendaciones UIT-T existentes (por ejemplo, H.323, H.245, H.248) que operan "en banda" dentro de la conexión de portador. El requisito para CS-2 AAL2 es que la anchura de banda de la conexión AAL2 debe ser susceptible de modificación. Este requisito es tratado por la CS-2 de señalización AAL2.

### 11.6 Llamadas pluripartitas

Las capacidades partes adición/sustracción requieren solamente configuraciones de comunicaciones punto a punto a un servidor o puente (configuración 6), que puede simular las configuraciones 2, 3, 4 y 5 desde el punto de vista del usuario. Esta configuración de tipo 6 es una configuración de comunicación que incluye un nodo servidor [por ejemplo, unidad de comunicación multipunto, MCU, *multipoint communication unit*] dentro de la red que puede conectar múltiples conexiones punto a punto. Proporcionará al usuario de extremo la posibilidad de comunicaciones multipunto a multipunto. Las configuraciones de comunicaciones de tipo 1 y 6 todavía tienen en cuenta partes adición/sustracción iniciadas por la raíz, hoja o un tercero, (véase TRQ 2001).

Además, la capacidad de llamadas pluripartitas incluye solamente la capacidad parte adición/sustracción iniciada por la raíz u hoja. No se requiere ninguna capacidad parte adición/sustracción 3ª parte para CS-1 IMT-2000. Además de esto, es necesario incluir la



señalización de notificación raíz cuando ocurre un evento de parte adición/sustracción iniciado por la hoja.

## 12 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 10-1. Esta cláusula identifica un conjunto de requisitos que pertenecen a la NNI que soporta los servicios de datos por paquetes.

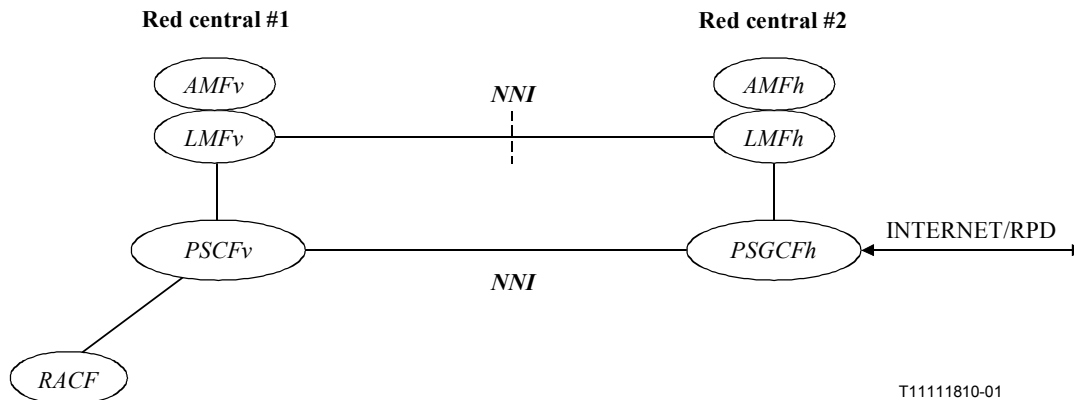


Figura 12-1/Q.1751 – Interfaces red-red de datos por paquetes

### 12.1 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, y
- 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*) 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 esta 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 e, 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 identificados de número de sesión asociado para identificar inequívocamente cada sesión de servicio individual.

#### **12.1.1 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 mecanismos 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.

#### **12.1.2 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 criptación de datos y la autenticación y comprobación de integridad de los mensajes de control.

## 12.2 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 criptación 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 criptación 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.

## APÉNDICE I

### Directriz sobre los conceptos y la utilización de activadores

#### I.1 Objetivo

El propósito de este apéndice informativo es proporcionar una orientación sobre la utilización de activadores a través de un examen informal de algunos elementos esenciales del armado y procesamiento de un activador en IMT-2000. Se espera que estas directrices básicas serán posteriormente mejoradas y optimizadas para satisfacer los requisitos específicos (por ejemplo, las necesidades operacionales) de los diferentes miembros de la familia IMT-2000.

#### I.2 Introducción

Este apéndice se inicia con el examen de algunos principios y conceptos. Se desarrollan a continuación directrices sobre el uso y aplicación del activador basadas en estos principios y conceptos. Hay que señalar que los principios y conceptos, si bien están basados en el modelo de estados de llamada básica (BCSM) relativo a la llamada, son también aplicables a los modelos de estados de gestión de posiciones y autenticación. Las subcláusulas restantes de este apéndice, que estudian el armado del activador dinámico y la distribución de activadores, requieren un estudio adicional para determinar si estas directrices son apropiadas para la activación de servicios de gestión de posiciones y gestión de autenticación.

Véanse las Recomendaciones UIT-T Q.1231 y Q.1238 (Partes 1 y 2) sobre la RI para un examen más detallado de la activación y de los principios de modelado de llamada BCSM en que se basan las subcláusulas siguientes.

#### I.3 Principios y conceptos

- 1) Los activadores y su independencia del servicio:  
Un concepto fundamental de la activación es que los activadores son independientes del servicio. Esto significa que cuando se encuentra un activador armado y sus criterios cumplidos, el centro de conmutación de servicios móviles (MSC, *mobile switching centre*) no conoce cual es el servicio o servicios que serán invocados como resultado del mensaje que éste envía al programa lógico de servicio (SLP, *service logic program*) en la SCF.
- 2) Los activadores incluyen información de dirección de la lógica de servicio:  
En el caso de abonados inalámbricos, los activadores de servicio, que implícitamente indican la SCF que ha de consultarse, están ubicados con el perfil de servicio de abonados situado en la LMFh.

- 3) El SLP responderá con una instrucción ejecutable:  
El MSC espera que la SCF (SLP) responda con una instrucción apropiada sobre el modo de procesar la llamada. El MSC debe examinar la instrucción recibida para determinar la conveniencia de considerar su visión actual de la llamada. En algunas circunstancias, los eventos relativos a la llamada pueden haber ocurrido en el intervalo entre la consulta a la SCF (SLP) y la respuesta de la SCF que hace la instrucción recibida inapropiada. Un ejemplo es el abandono de la llamada.
- 4) Solamente se actúa sobre los activadores cuando se encuentran en el BCSM (modelo de estados de llamada básica):  
Algunas circunstancias proporcionan información antes de que el BCSM la busque. Es el caso de la notificación de la condición de ocupado como resultado de un procedimiento de gestión de la movilidad (por ejemplo, petición de posición). El modelo O-BCSM no reconoce esta condición de ocupado hasta que el tratamiento de la llamada ha progresado hasta un punto en el que un modelo T-BCSM es ejemplificado y el T-BCSM ha progresado hasta el punto en que encuentra el DP T\_Busy. Si el estado de ocupado no se consume, el T-BCSM lo propaga hacia atrás al O-BCSM par su posible uso en éste.  
Obsérvese que el examen que aquí se hace describe el modelado de RI (véase la serie Q.1238 de las Recomendaciones UIT-T). Una implementación puede examinar libremente la información de ocupado tan pronto como esta información se encuentre disponible con el fin de optimizar su calidad de funcionamiento, pero debe ser consciente de la posibilidad de que sean invocados otros servicios entre el momento en que la información de ocupado se recibe y el momento en el que el modelado indica que éste debe ser considerado.
- 5) Los activadores siguen un orden de precedencia: abonado, grupo, central:  
Esta secuencia permite que los proveedores del servicio puedan ofrecer a abonados seleccionados prestaciones de servicios que no se encuentran a disposición de todos los abonados en general. Por ejemplo, el acceso a servicios mejorados, como la comunicación conferencia, etc. Análogamente, este orden de precedencia de los activadores permite a los proveedores del servicio denegar a abonados seleccionados servicios disponibles para los abonados en general. Por ejemplo, la restricción de partes llamantes a determinados distintivos de zona, etc.
- 6) Cada activador se examina totalmente antes del siguiente activador:  
Los activadores se enumeran por orden de precedencia. Este principio indica que un tipo de activador determinado es examinado en relación con su aplicabilidad al abonado, grupo o central, antes de continuar con el siguiente tipo de activador en el orden de precedencia.  
Se pueden perfeccionar ulteriormente los puntos 5) y 6) para tomar en consideración la precedencia y la secuenciación de los criterios de los activadores, pero esto depende del servicio específico y de los requisitos operacionales del miembro concreto de la familia IMT-2000. Por ejemplo, la compatibilidad hacia atrás con sistemas 2G existentes puede exigir un tratamiento específico de los activadores de servicios cuando operan en el contexto del entorno 3G.

#### **I.4 Armado dinámico del activador**

El perfil de un activador de abonado se almacena con otra información relativa al servicio en la LMFh. Este perfil de activador se considera "estático" porque cambia lentamente, si lo hace. Esto es, se mantiene el mismo perfil a menos que el abonado añada o suprima un servicio activado desde el perfil, o encienda o apague o modifique uno de los servicios a los que está abonado. Es este perfil "estático" el que se sitúa geográficamente de modo dinámico a medida que el abonado está itinerante y es servido por diferentes MSC.

Un perfil de activador de abonado puede ser modificado para un ejemplar de llamada determinada sin que afecte al perfil "estático". Estas modificaciones del perfil no sobrevivirán después de la llamada vigente. Al liberarse la llamada, todas estas modificaciones desaparecen. Esto se denomina armado "dinámico" del activador.

El armado dinámico del activador es una capacidad potente, pero que puede también ser fácilmente utilizada de modo incorrecto. Incumbe a los proveedores del servicio que utilicen esta capacidad conocer y tratar los posibles efectos colaterales del empleo de la misma. Por ejemplo, cuando hay múltiples puntos SCP que prestan servicios, el uso inadecuado de la capacidad de armado dinámico del activador puede producir interacciones o fallos del servicio no deseados desde el punto de vista del usuario de extremo. Si no está bien coordinado, un programa lógico de servicio en un SCP puede sobrescribir los activadores armados para una programa lógico de servicio en otro SCP. Esto puede hacer que falle otro servicio, o que no se ejecute en absoluto o que lo haga incorrectamente. Cuando están afectados varios proveedores del servicio, ellos probablemente no tendrán conocimiento de la serie completa de servicios suscritos y de los efectos que pueden producirse en estos otros servicios desconocidos para ellos.

## **I.5 Distribución de activadores**

Puesto que los abonados inalámbricos son intrínsecamente móviles, es necesario considerar el modo en que deben distribuirse los activadores para sus servicios. La originación o terminación de una llamada móvil puede ocurrir en cualquier lugar y el abonado itinerante puede encontrarse en cualquier sitio de las zonas de itinerancia a las que el abonado itinerante pueda ser llamado, por lo que es necesario distribuir el procesamiento del servicio de una manera óptima. Se supone que cuando un proveedor de servicios ofrece un conjunto de servicios a un abonado, debe asegurar que los servicios constituyen un conjunto adecuado, coherente e internamente consistente, y cada uno de ellos interactuará con los demás del modo deseado por el abonado.

Las opciones del emplazamiento geográfico dinámico de los activadores de origen y terminación armados estadísticamente se encuentran en el MSC de origen, de terminación o pasarela. Si se colocan perfiles de activador idénticos en el MSC de origen, de terminación o de pasarela, puede ocurrir que algunos servicios se ejecuten dos veces, lo que producirá resultados no deseables. Puesto que no deben colocarse perfiles de activador idénticos en cualquier emplazamiento, es necesario disponer de criterios utilizables en la decisión sobre el emplazamiento de los activadores.

Los criterios a continuación se suministran como ayuda en el proceso de toma de decisión para determinar la ubicación de los activadores de servicio.

Para optimizar los recursos de red, los activadores de origen de llamadas salientes deben situarse lo más cerca posible del abonado llamante. Por lo general, esto implica que los activadores de origen del abonado deben situarse en el MSC de origen cuando se registra el abonado móvil (MS).

En las llamadas a un abonado, para asegurar una utilización óptima de los recursos de conexión de portadores de red, es deseable colocar los activadores para servicios que pueden impedir la compleción de la llamada lo más cerca posible del punto de origen de la llamada. Por tanto, puede colocarse un conjunto de activadores de terminación en el MSC de origen o de pasarela para su utilización en un BCSM que se está ejecutando como un sustituto del abonado llamado. Estos activadores deben indicarse en la información devuelta con la petición de encaminamiento (o actualización de posición). Sin embargo, debe señalarse que la colocación de perfiles de activadores en las centrales locales (MSC) tiene un coste superior y compromete a los proveedores de servicios de red con un despliegue del servicio de coste más elevado antes de que se haya demostrado la existencia de un mercado para el servicio. Generalmente, salvo que el servicio requiera una alta disponibilidad (utilización elevada o tiempos de respuesta bajos) o que requiera un despliegue de centrales locales (MSC) por razones técnicas, deben considerarse las ventajas en cuanto al coste del despliegue de centrales de tránsito o de pasarelas de interrogación.

Si la llamada puede ser reflejada a otro destino, ello deberá efectuarse lo más cerca posible de la fuente de la llamada (por ejemplo, MSC de origen o de pasarela). Un ejemplo de servicio es el reenvío de llamada a un servicio de correo vocal.

La seguridad de la señalización puede hacer necesario que los activadores sean desplegados en un nodo de tránsito o pasarela. Por ello, si la SSF se encuentra en una red y el SCP en una red diferente, se necesitarán STPs y GTT en el nivel de transporte de señalización. El empleo de STPs y GTT reducirá la velocidad de la señalización y requerirá una seguridad extra de los proveedores de servicios para asegurar sus contextos de protocolo.

El uso elevado de un servicio requiere que éste sea desplegado en el MSC visitado, de origen o de terminación.

La necesidad de tiempos de respuesta muy cortos requiere que sea desplegado en el MSC visitado, de origen o de terminación.

Las redes que utilizan el encaminamiento óptimo pueden necesitar el despliegue de activadores en el MSC visitado, de origen o de terminación, ya que la activación en el nodo de interrogante (tránsito) puede provocar un encaminamiento complejo, por ejemplo, tramos con efecto trombón.

Las temporizaciones de la señalización pueden requerir que se instalen activadores de origen en el MSC de origen y que los activadores de terminación se instalen en el MSC de terminación. Puesto que el MSC necesita que se cumplan varias condiciones específicas para reiniciar las temporizaciones cortas RDSI en el acceso de red cuando el SCP está procesando la aplicación, esto puede realizarse en otras centrales.

El acceso a la información de zona de posición puede requerir que los activadores de origen se ubiquen en el MSC de origen y los activadores de terminación en el MSC de terminación. Este requisito puede ser suavizado por los futuros sistema de señalización, que permiten que la información de zona de posición (LAI, *location area identity*) sea repetida en el trayecto de la llamada como la CLI puede serlo hoy. Sin embargo, la selección de tales parámetros en las fronteras de red pueden hacer que la señalización resulte ineficaz.

La tasación aplicada a la red originaria puede precisar que los activadores sean desplegados en un nodo de tránsito o pasarela, puesto que la SSF se encuentra en una red y el SCP en otra diferente. La red originaria no puede nunca recibir la llamada. En efecto, puede ser retirada del trayecto de llamada y de este modo no puede asegurar la tasación aplicada a la llamada. Otros métodos de tasación pueden exigir que los activadores de servicio sean también desplegados lo más cerca posible de la parte llamada. Por ejemplo, los servicios que requieren un conocimiento específico de los parámetros de la interfaz radioeléctrica utilizados, como el ID de célula, el número de canales radioeléctricos empleados, etc, para garantizar el cálculo exacto de las tasas. Otros ejemplos de servicio incluyen el aviso de tasación y prepago de terminación móvil.

Los servicios de área local requerirán que los activadores de origen se ubiquen en el MSC de origen y que los activadores de terminación se sitúen en el MSC de terminación. Por ejemplo, los privilegios y la exclusión de usuario en una estación de base. Esto puede ser equivalente a los servicios alámbricos de la red fija.







## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
<b>Serie Q</b>	<b>Conmutación y señalización</b>
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación