

**Centro de Investigación Científica y de
Educación Superior de Ensenada**



**SEÑALIZACION PARA REDES INTELIGENTES
EN COMUNICACIONES INALAMBRICAS**

**TESIS
MAESTRIA EN CIENCIAS**

LUIS ALEJANDRO SERRANO VARGAS

ENSENADA, BAJA CALIFORNIA, MEXICO.

SEPTIEMBRE DE 1997.

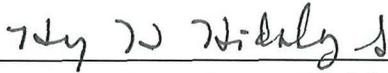
TESIS DEFENDIDA POR
LUIS ALEJANDRO SERRANO VARGAS

Y APROBADA POR EL SIGUIENTE COMITE



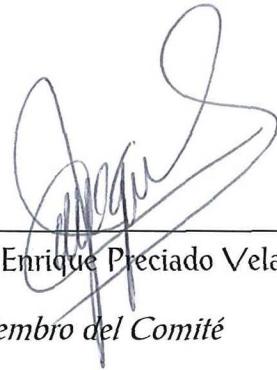
M.C. Ernesto Eduardo Quiroz Morones

Director del Comité



M.C. Hugo Homero Hidalgo Silva

Miembro del Comité



M.C. Jorge Enrique Preciado Velasco

Miembro del Comité



Dr. José Luis Medina Monroy

*Jefe del Departamento de Electrónica y
Telecomunicaciones*

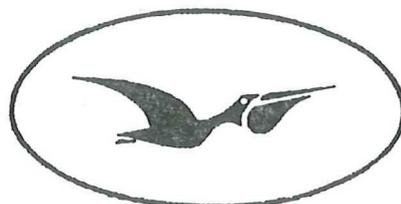


Dr. Federico Graef Ziehl

Director de Estudios de Posgrado

8 de septiembre de 1997

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y
DE EDUCACIÓN SUPERIOR DE ENSENADA



CICESE

DIVISIÓN DE FÍSICA APLICADA

DEPARTAMENTO DE ELECTRÓNICA Y
TELECOMUNICACIONES

**SEÑALIZACIÓN PARA REDES INTELIGENTES EN
COMUNICACIONES INALÁMBRICAS**

TESIS

que para cubrir parcialmente los requisitos necesarios para
obtener el grado de MAESTRO EN CIENCIAS presenta:

LUIS ALEJANDRO SERRANO VARGAS

Ensenada, Baja California; México. Septiembre de 1997

Resumen de la tesis de Luis Alejandro Serrano Vargas, presentada como requisito parcial para la obtención del grado de MAESTRO en CIENCIAS con especialidad en ELECTRÓNICA Y TELECOMUNICACIONES. Ensenada, Baja California; México. Septiembre de 1997.

SEÑALIZACIÓN PARA REDES INTELIGENTES EN COMUNICACIONES INALAMBRICAS

Aprobado por:



M.C. Ernesto E. Quiroz Morones
director de tesis

En este trabajo se evalúa el desempeño de la red de señalización de los Servicios de Comunicación Personal (PCS). Para ello se consideran 3 escenarios actuales o a punto de implementarse. El primero corresponde al caso en donde no se implantan mecanismos de seguridad en la red (privacidad de comunicación y autenticación de usuarios) que corresponde a la situación de las redes PCS actuales. En los otros dos casos, se considera la incorporación de mecanismos de seguridad de acuerdo con las dos diferentes propuestas recientemente adoptadas en el estándar IS-41 C de la TIA/EIA para los PCS americanos: Compartición de los Datos Secretos (SSD) de usuario con el sistema visitado así como la no compartición del SSD con el sistema visitado.

La evaluación del desempeño se realizó mediante simulación utilizando OPNET. El desempeño es medido en términos del retardo extremo a extremo experimentado por los diferentes procedimientos que se tienen que realizar en PCS para proporcionar a los usuarios los servicios suscritos sin importar su actual ubicación dentro de la red, como por ejemplo, registro de terminales, traspaso de llamadas, origen de llamadas, entrega de llamadas, etc. También se identifica a los elementos que limitan la capacidad de la red y se estima su utilización.

Los resultados obtenidos revelan que cuando se implementan mecanismos de seguridad en PCS, la capacidad de la red de señalización se ve notablemente disminuida respecto al caso en que estos mecanismos no se utilizan. Otro resultado notable muestra que a medida que la movilidad de los usuarios de la red se incrementa, la capacidad de la red de señalización para la entrega de llamadas y el origen de llamadas se ve considerablemente reducida. También se encontró que en general, el utilizar la compartición del SSD como mecanismo de seguridad resulta en una mayor capacidad de red respecto al caso en que el SSD no se comparte.

Palabras clave: Señalización, Redes Inteligentes, Servicios de Comunicación Personal.

ABSTRACT of the thesis of Luis Alejandro Serrano Vargas, presented as partial requirement to obtain the MASTER IN SCIENCE grade with specialization in ELECTRONICS AND TELECOMMUNICATIONS. Ensenada, Baja California; México. September 1997.

INTELLIGENT NETWORK SIGNALING FOR WIRELESS COMMUNICATIONS

In this work, we evaluate the performance of the signaling network for Personal Communication Services (PCS). We considerate 3 scenarios implemented already or next to be implemented in these networks. The former corresponding to the actual situation in the PCS networks which is featured by a lack of security mechanisms (privacy and authentication). In the other two situations, we considerate the incorporation of security mechanisms according with the two different proposals recently adopted in the TIA/EIA IS-41 C standards for American PCS: Sharing the Shared Secret Data (SSD) with the visited system as well as no sharing the SSD with the visited system.

Performance evaluation was done by simulation using OPNET. The performance is measured in terms of the end-to-end delay experienced by the different procedures that are necessary in PCS to provide users the subscribed services for example terminal register, hand off, mobile call origination, call delivery, etc. We also identify and estimate the utilization of the elements that limit the network capability.

The results obtained reveal that the implementation of security mechanism in PCS decrease considerably the signaling network capability comparing with the case that these mechanisms are not implemented. Another noticeable result shows that as users mobility increases, the signaling network capability for the call originating and call delivery procedures is strongly diminished. We also found in general that using SSD sharing as security mechanism results in a superior signaling network capability comparing with the case in witch the SSD is not shared.

Keywords: Signaling, Intelligent Network, Personal Communication Services (PCS).

DEDICATORIA

A mis padres:

Luis Serrano Mariaud y Francisca Vargas Bustamante.

Por su cariño, sus invaluable consejos, y ese incondicional apoyo en todas mis decisiones. Les dedico este trabajo por esa confianza que siempre me han tenido, por inspirar en mí el deseo de superación y por toda la libertad con que me han permitido conducir mi vida. Gracias por todos los sacrificios que han realizado en su afán de ayudarme en todo cuanto pueden y por construir con trabajo y esfuerzo la gran familia que algún día soñaron. SON UNOS PADRES EJEMPLARES, LOS QUIERO MUCHO.

A mis hermanos:

Winston, Reynaldo, Rolando, Francisco, Ileana, Marissa, Germán, Tomás y Miguel Angel.

Por todo lo que he vivido con cada uno de ustedes, son muy importantes en mi vida.

A mis tíos:

Lulú, la familia Mondragón y la familia Ponce.

Son parte muy importante en mi familia, siempre los tengo presentes.

A todos mis amigos:

Por todos esos momentos felices que hemos compartido

AGRADECIMIENTOS

A mi director de tesis el **M.C. Eduardo Quiróz** por su valiosa colaboración en este trabajo de tesis. Gracias también por su confianza y el apoyo brindado para que este trabajo se realizara en la Universidad de Ottawa en Canadá.

A los miembros del comité de tesis, por sus comentarios y correcciones al manuscrito. Especialmente al **M.C. Jorge Preciado** quien revisó minuciosamente el manuscrito.

Gracias en especial al **Dr. Luis Orozco** de la Universidad de Ottawa por su desinteresada y valiosa amistad, su dirección para la realización de este trabajo y por poner a mi alcance los recursos y facilidades del MCRLAB y la Universidad de Ottawa.

Gracias también al **Dr. Nicolas Georganas** de la Universidad de Ottawa por abrir cordialmente las puertas del MCRLAB.

A mis amigos y compañeros de la maestría en telecomunicaciones: **Jesús Bedoy, Héctor Félix, Raúl Rivera, Francisco Mora, Raúl Tamayo, Ricardo Solís y Edith García**. Aprecio su sincera amistad, así como todas las experiencias e inolvidables momentos que hemos vivido juntos. He aprendido mucho de ustedes. Cada uno de ustedes significa algo especial para mi.

A **todos los profesores del CICESE** que contribuyeron en mi formación durante mi estancia en el centro de investigación. También agradezco **las atenciones del resto del personal**.

Al **CONACYT** por su apoyo económico siempre tan a tiempo, felicidades por apoyar a los entusiastas estudiantes de posgrado en México.

CONTENIDO

	<u>Página</u>
I. INTRODUCCION	1
I.1 Antecedentes	1
I.2 Planteamiento del problema	2
I.3 Objetivo general	3
I.4 Organización del trabajo	4
II. SISTEMA DE SEÑALIZACION NUMERO 7 PARA REDES INTELIGENTES	6
II.1 Antecedentes	6
II.2 Elementos de la red SS7 y arquitectura funcional	6
II.3 El porqué de la IN	9
II.3.1 Objetivos de la IN	11
II.4 Arquitectura de los protocolos del SS7	12
II.5 Parte de transferencia de mensajes (MTP)	14
II.5.1 MTP-1	15
II.5.2 MTP-2	15
II.5.3 MTP-3	19
II.6 SCCP	21
II.7 ISUP	23
II.7.1 Identificación del usuario que llama	27
II.7.2 Redireccionamiento de llamada	27
II.8 TCAP	28
II.8.1 Ejemplo de servicio de red inteligente	30
III. SERVICIOS DE COMUNICACION PERSONAL (PCS)	32
III.1 Introducción	32
III.2 El concepto celular	33
III.3 Estructura de una red celular	34
III.4 La introducción de la IN en las redes móviles	34
III.5 Arquitectura de una red PCS basada en principios de IN	36
III.6 Estructura de una red PCS típica y manejo de la movilidad de los usuarios	37
III.7 Números en las redes PCS	39
III.8 Fraude en las redes PCS y la manera de erradicarlo	39
III.8.1 Las razones del fraude	39
III.8.2 Puntos vulnerables de la red	40
III.8.3 Fraude en los sistemas de primera generación	40
III.8.4 Listas de usuarios inválidos	40
III.8.5 Validación positiva	41
III.8.6 Réplica de MS	41
III.8.7 Otras medidas contra el fraude	41
III.9 Protocolo IS-41	41
III.9.1 Mecanismos de seguridad en IS-41 (Privacidad y autenticidad)	42

CONTENIDO (continuación)

	<u>Página</u>
III.10 Procedimientos del IS-41 sin compartición del SSD	43
III.10.1 Registro de terminales	43
III.10.2 Origen de llamadas por usuario móvil	45
III.10.3 Entrega de llamadas a usuario móvil:	46
III.10.4 Traspaso de llamada (hand off)	48
III.10.5 Servicios extendidos	50
III.11 Procedimientos del IS-41 con compartición del SSD	53
III.11.1 Registro de terminales	53
III.11.2 Llamadas originadas por usuario móvil	54
III.11.3 Entrega de llamadas a usuario móvil	55
IV. MODELADO DE UNA RED PCS BASADA EN IS-41	56
IV.1 Funcionalidad de SS7 requerida en los diversos elementos de la red	56
IV.2 Modelado de las diferentes capas de la SS7	57
IV.3 Implementación del modelo	62
IV.4 Simplificaciones y limitaciones	62
V. DISEÑO DE LAS CORRIDAS Y PRESENTACION DE RESULTADOS	65
V.1 Comentarios	65
V.2 Comparación entre un sistema con y sin mecanismos de seguridad	66
V.3 Comparación entre compartición y no compartición del SSD	75
V.3.1 Comparación de los mecanismos de seguridad durante el proceso de origen de llamadas	76
V.3.2 Comparación de los Métodos de Seguridad durante el Proceso de Entrega de Llamada	80
V.3.3 Comparación de los métodos de seguridad al variar la movilidad de los usuarios	84
V.3.4 Comparación de los Métodos de Seguridad durante el Proceso de Registro de Terminales	84
VI. CONCLUSIONES, RECOMENDACIONES Y COMENTARIOS	90
VI.1 Conclusiones	90
VI.2 Recomendaciones	92
VI.3 Comentarios	93
LITERATURA CITADA	95
ANEXO: INTRODUCCION A OPNET	98
GLOSARIO	102

LISTA DE FIGURAS

<u>Figura</u>	<u>Página</u>
1. Estructura de una red de telecomunicaciones moderna	7
2. Estructura de los protocolos de la SS7	14
3. Formatos de la unidad de señalización	16
4. Diagrama funcional a bloques de la MTP-2	18
5. Diagrama funcional a bloques de la MTP-3	19
6. Estructura del mensaje de la MTP-3	21
7. Estructura básica de la SCCP	22
8. Formato del mensaje de la SCCP	23
9. Formato del mensaje de la ISUP	24
10. Estructura funcional de la ISUP	24
11. Flujo de mensajes para el establecimiento y liberación de una llamada.	26
12. Estructura de la TCAP y primitivas	29
13. Formato del mensaje de la TCAP y operaciones de las subcapas	30
14. Ejemplo del uso de la TCAP: servicio de números 800's	31
15. Estructura de una red celular	34
16. Arquitectura de una red móvil basada en conceptos de la IN	37
17. Una red PCS típica	38
18. Puntos vulnerables en una red celular	40
19. Registro de terminales	45
20. Origen de llamadas	46
21. Entrega de llamada	47
22. Traspaso de llamada entre celdas de un mismo MSC	49
23. Traspaso de llamadas entre celdas de diferente MSC	50
24. Flujo de mensajes para redireccionamiento incondicional de llamadas	51
25. Redireccionamiento de llamadas cuando la MS no contesta	52
26. Registro de terminales	54
27. Origen de llamadas	55
28. Entrega de llamada	55
29. La red de referencia	56
30. Funcionalidad SS7 en los nodos de la red	57
31. Modelo de colas para la MTP-2	58
32. Modelo de colas para la MTP-3	58
33. Modelo de colas para la SCCP	59
34. Modelo de colas para la ISUP	59
35. Modelo de colas para la TCAP	59
36. Retardo en la red durante el registro de terminales (usuarios en vehículos)	67
37. Utilización del elemento limitante (VLR-1) durante el registro de terminales (usuarios en vehículos)	68
38. Retardo en la red durante el origen de llamadas (usuarios en vehículos)	68

LISTA DE FIGURAS (continuación)

<u>Figura</u>	<u>Página</u>
39. Utilización del elemento limitante (VLR-1) durante el origen de llamadas (usuarios en vehículos)	69
40. Retardo en la red durante la entrega de llamadas (usuarios en vehículos)	70
41. Utilización del elemento limitante (VLR-X) durante la entrega de llamadas (usuarios en vehículos)	70
42. Retardo en la red durante el registro de terminales (usuarios pedestres)	71
43. Utilización del elemento limitante (VLR-1) durante el registro de terminales (usuarios pedestres)	71
44. Retardo en la red durante el origen de llamadas (usuarios pedestres)	72
45. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas (usuarios pedestres)	72
46. Retardo en la red durante la entrega de llamadas (usuarios pedestres)	73
47. Utilización del elemento limitante (VLR-X) durante la entrega de llamadas (usuarios pedestres)	73
48. Respuesta de la red al proceso de origen de llamadas en el caso de usuarios con baja movilidad	76
49. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas en el caso de usuarios con baja movilidad	77
50. Respuesta de la red al proceso de origen de llamadas en el caso de usuarios con mediana movilidad	77
51. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas en el caso de usuarios con mediana movilidad	78
52. Respuesta de la red al proceso de origen de llamadas en el caso de usuarios con alta movilidad	78
53. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas en el caso de usuarios con alta movilidad	79
54. Respuesta de la red al proceso de entrega de llamadas en el caso de usuarios con baja movilidad	80
55. Utilización del elemento limitante (VLR-X) durante el proceso de entrega de llamadas en el caso de usuarios con baja movilidad	81
56. Respuesta de la red al proceso de entrega de llamadas en el caso de usuarios con mediana movilidad	81
57. Utilización del elemento limitante (VLR-X) durante el proceso de entrega de llamadas en el caso de usuarios con mediana movilidad	82
58. Respuesta de la red al proceso de entrega de llamadas en el caso de usuarios con alta movilidad	82
59. Utilización del elemento limitante (VLR-X) durante el proceso de entrega de llamadas en el caso de usuarios con alta movilidad	83
60. Respuesta de la red al proceso de registro de terminales para el caso de usuarios con bajo tráfico de llamadas	86

LISTA DE FIGURAS (continuación)

<u>Figura</u>	<u>Página</u>
61. Utilización del elemento limitante (VLR-1) durante el proceso de registro de terminales en el caso de usuarios con bajo tráfico de llamadas	86
62. Respuesta de la red al proceso de registro de terminales en el caso de usuarios con mediano tráfico de llamadas	87
63. Utilización del elemento limitante (VLR-1) durante el proceso de registro de terminales en el caso de usuarios con mediano tráfico de llamadas	87
64. Respuesta de la red al proceso de registro de terminales en el caso de usuarios con alto tráfico de llamadas	88
65. Utilización del elemento limitante (VLR-1) durante el proceso de registro de terminales en el caso de usuarios con alto tráfico de llamadas	88

LISTA DE TABLAS

<u>Tabla</u>		<u>Página</u>
I.	Algunos mensajes de la ISUP	25
II.	Funcionalidad en las diversas capas de la SS7	58
III.	Tiempo de procesamiento y prioridad para las colas de las capa de la SS7	60
IV.	Otros tiempos de procesamiento considerados	61
V.	Tráfico debido a usuarios en vehículos	66
VI.	Tráfico debido a usuarios pedestres	66
VII.	Tráfico máximo soportado debido a usuarios en vehículos	74
VIII.	Tráfico máximo soportado debido a usuarios en vehículos normalizado	74
IX.	Tráfico máximo soportado debido a usuarios pedestres	74
X.	Tráfico máximo soportado debido a usuarios pedestres normalizado	74
XI.	Tráfico de fondo para la comparación de los mecanismos de seguridad	75
XII.	El tráfico en la red debido a tres condiciones de movilidad distintas	75
XIII.	Tráfico máximo soportado durante el proceso de origen de llamadas para las 3 condiciones de movilidad	79
XIV.	Tráfico máximo soportado durante el proceso de origen de llamadas para las 3 condiciones de movilidad (normalizado)	80
XV.	Tráfico máximo soportado durante el proceso de entrega de llamadas para las 3 condiciones de movilidad	83
XVI.	Tráfico máximo soportado durante el proceso de entrega de llamadas para las 3 condiciones de movilidad (normalizado)	83
XVII.	Efectos de la movilidad sobre el origen de llamadas	84
XVIII.	Efectos de la movilidad sobre la entrega de llamadas	84
XIX.	Tráfico de fondo para evaluar la capacidad de la red al proceso de registro de terminales	85
XX.	Tres condiciones de tráfico para evaluar la capacidad de la red al proceso de registro de terminales	85
XXI.	Tráfico máximo soportado durante el proceso de registro de terminales 3 condiciones de movilidad	89
XXII.	Tráfico máximo soportado durante el proceso de registro de terminales 3 condiciones de movilidad (normalizado)	89

SEÑALIZACIÓN PARA REDES INTELIGENTES EN COMUNICACIONES INALAMBRICAS

I. INTRODUCCION

I.1 Antecedentes

Los sistemas de comunicación celular han pasado ya por las dos primeras etapas de desarrollo. Los sistemas de primera generación se caracterizaron por una baja cantidad de usuarios en la red, el uso de terminales móviles de usuario de gran tamaño, pocos servicios ofrecidos al usuario y una utilización ineficiente del espectro de radio. En los sistemas de segunda generación destaca la utilización de terminales de usuario más ligeras y pequeñas, técnicas digitales de acceso al canal de radio para un mejor uso de los recursos de radio, una mayor densidad de usuarios y una gran variedad de servicios disponibles.

Los Servicios de Comunicación Personal (PCS: Personal Communication Services) corresponden a la fase madura de los sistemas celulares de segunda generación y han sido identificados como el camino a seguir para la implementación de los sistemas de tercera generación, actualmente en proceso de especificación y estandarización mundialmente. Los PCS representan el sector de las telecomunicaciones de mayor crecimiento y uno de los que mayores ingresos económicos generan.

El principal objetivo de los PCS es proporcionar servicios de comunicaciones para todos, en cualquier momento y en cualquier lugar. Esto significa que para los usuarios, el costo del servicio en los PCS debe ser similar al costo del servicio en la red telefónica pública (PSTN: Public Switched Telephone Network). En los PCS los usuarios no se encuentran atados a ninguna conexión física, sino que pueden viajar con sus terminales por toda el área de cobertura de radio de la red, o incluso en las redes de otros proveedores de servicio y, recibir servicio en la manera acostumbrada sin ninguna diferencia apreciable. La red es responsable de seguir la pista de los usuarios a medida que ellos se mueven dentro del área de servicio de la red con el objeto de entregarles llamadas entrantes y para ofrecerles los servicios suscritos en el lugar de su actual ubicación.

Los PCS soportan movilidad terminal, movilidad personal y movilidad de servicios. La movilidad terminal permite a cualquier terminal el obtener acceso a los servicios de la red sin importar su localización dentro de ésta. La movilidad personal permite a cualquier usuario el tener acceso a sus servicios desde cualquier terminal móvil válida en la red. Los usuarios pueden registrarse en la red para utilizar la terminal (ya sea una terminal en la red pública o una terminal en la red móvil) que mejor les convenga en el momento que así lo deseen. La movilidad de servicios permite a los usuarios el tener acceso a los servicios contratados sin importar la terminal de su actual preferencia, esto se logra mediante el manejo de archivos de usuarios, en donde se almacena toda la información relativa a los usuarios (como por ejemplo, privilegios del usuario, servicios contratados, restricciones, etc.).

I.2 Planteamiento del problema

Para lograr el manejo de la movilidad de los usuarios y para soportar la provisión de servicios extendidos, se han introducido recientemente en la arquitectura de los PCS el Sistema de Señalización Número 7 (SS7: Signaling System Number 7) y la arquitectura de la Red Inteligente (IN: Intelligent Network). El SS7 proporcionando el transporte de mensajes de señalización en la red, la IN para la rápida provisión de nuevos servicios, el soporte de servicios extendidos y para consolidar la separación de las funciones de transporte y control de servicios en la red. Ambos conceptos ya han demostrado gran utilidad en la PSTN, pero ahora en un ambiente móvil, los retos impuestos sobre los elementos que conforman la arquitectura de la IN son mayores. Esto se debe a que la movilidad de los usuarios incrementa la cantidad y la complejidad de los procedimientos que son necesarios en la red a fin de proporcionar el servicio a los usuarios. La IN debe soportar las siguientes funciones cuando esta provee comunicaciones personales:

- Registro y seguimiento de usuarios
- Origen de llamadas
- Entrega de llamadas
- Traspaso de llamadas en curso
- Manejo de recursos y archivos de usuario

- Servicios extendidos (llamada en espera, redireccionamiento de llamada, etc.)
- Tarificación

Recientes estudios [Meier-Hellstern Kathleen *et al*, 1992] revelan que la información de señalización que es necesaria en PCS para soportar éstas funciones podría llegar a ser hasta 4-7 veces mayor que en los sistemas celulares y 5-11 veces mayor que en ISDN. Similarmente [Mohan S. y R Jain, 1994] han mostrado que las bases de datos que proporcionan la inteligencia de la red, tendrán sobre sí una carga considerable en el ambiente PCS.

Recientemente se está considerando la introducción de mecanismos de privacidad y autenticación de usuarios no disponibles en las redes PCS actuales. La adopción de éstos mecanismos es la reacción de los proveedores de servicio ante la creciente tasa de fraude que se vive en la industria con el fin de detener el acceso de intrusos a la red. La implementación de estos mecanismos incrementará aún más el tráfico de señalización y presentará carga adicional en las bases de datos de la red.

I.3 Objetivo general

En este trabajo se analizará el impacto que se impone sobre los elementos de la IN cuando esta es incluida en la arquitectura de una red PCS. Principalmente se evaluará el retardo extremo a extremo experimentado por cada uno de los procedimientos asociados con las funciones que la IN debe realizar para proveer PCS; también se identificarán los elementos que limitan la capacidad de la red y se estimará su utilización.

Se estudiará el desempeño de la red de señalización utilizada en PCS bajo tres situaciones distintas: Una en la cuál no se incluirán mecanismos para la privacidad y la verificación de la autenticidad de usuarios en la red (que corresponde a la situación que actualmente se vive en los PCS). En las otras dos situaciones restantes, se incluirán mecanismos de seguridad de acuerdo con las dos propuestas diferentes que han sido estandarizadas recientemente para los PCS americanos [Mohan S, 1996]. Esto permitirá comparar las ventajas y las desventajas que se obtienen en las redes PCS en cada una de éstas tres situaciones.

Para conseguir este objetivo, es necesario establecer y desarrollar modelos de simulación (utilizando el lenguaje de simulación orientado a comunicaciones OPNET) de una red PCS. Se pretende especificar en detalle los diferentes elementos de la red de señalización y se someterá al sistema a diferentes condiciones de tráfico que permitan realizar un análisis de sensibilidad de una red PCS.

I.4 Organización del trabajo

Este trabajo está organizado como sigue. En el capítulo 2 se presenta un estudio del Sistema de Señalización SS7 para la IN. El SS7 es la tecnología emergente que permite el proporcionar servicios de Red Inteligente, Redes Digitales de Servicios Integrados (ISDN: Integrated Services Digital Network) y servicios de Redes Móviles entre otros. La IN es la arquitectura que permite la provisión fácil y rápida de nuevos y variados servicios en las redes de telecomunicaciones modernas, la IN ha demostrado ya utilidad en la red pública, estimulando en los usuarios una mayor utilización de la red y trayendo actualmente se están realizando esfuerzos para emigrar la IN a otras plataformas incluyendo Redes Móviles, ISDN de banda ancha (BISDN: Broadband ISDN), etc. Gran parte de este trabajo se apoya en ambos conceptos, de allí que se dedica un espacio considerable para su estudio.

El capítulo 3 contiene un resumen de los conceptos básicos necesarios para entender el funcionamiento de una red PCS, se evita en lo posible el hablar acerca de la interfaz al canal de radio para no desviar la atención del tema de estudio; se estudia en detalle el protocolo IS-41 de la EIA/TIA quien proporciona la operación entre sistemas de distinto proveedor de servicios para asegurar la provisión de los servicios a los usuarios en los PCS.

En el capítulo 4, se presenta la metodología utilizada para el modelado de una red PCS, una vez que se hayan introducido las bases sobre las cuales se fundamentan dichas redes PCS (La IN y el SS7), podrán establecertse los modelos de simulación.

En el capítulo 5 se presenta el diseño de las corridas de la simulación y se presentan los resultados obtenidos a partir de las simulaciones, incluyendo el análisis de los resultados encontrados.

En el capítulo 6 se presentan las conclusiones del trabajo y se establecen extensiones y mejoras que podrían hacerse a este trabajo en un futuro, así como otros posibles trabajos que podrían ser realizados a partir de los fundamentos teóricos, los modelos y los resultados presentados en este trabajo.

Posteriormente se presentan las referencias a la literatura en la cuál se fundamentó el trabajo. Al final del trabajo está un apéndice que resume las mayores características del lenguaje de simulación orientado a comunicaciones OPNET, que fué utilizado para implementar los modelos de simulación propuestos en este trabajo y por último se incluye un glosario de los términos empleados en el trabajo.

II. SISTEMA DE SEÑALIZACION NUMERO 7 PARA REDES INTELIGENTES

II.1 Antecedentes

La señalización es el intercambio de mensajes que se efectúa entre los diferentes elementos que conforman una Red de Telecomunicaciones (RT) con el propósito de:

- Establecer, mantener y liberar una conexión entre dos o más usuarios de esta red
- Seleccionar la ruta de transporte más conveniente para conectar los usuarios
- Proporcionar información de la situación de los usuarios y recursos
- Realizar las funciones de manejo y operaciones de la red (como por ejemplo, tarificación, reporte de fallas, configuración de la red, etc.).

La señalización en una RT se compone de la señalización de acceso y la señalización de troncal (señalización dentro de la red). La primera permite al usuario expresar su deseo de servicio a la red, así como el tipo y la calidad de éste. La segunda es utilizada dentro de la red misma para establecer las trayectorias de comunicación entre usuarios y para la provisión de servicios avanzados. El tipo de señalización de interés en este trabajo es la señalización de troncal.

Las técnicas de señalización de troncal han evolucionando con el desarrollo de las tecnologías modernas. El tipo de la señalización de troncal que satisface los requerimientos actuales de desempeño, confiabilidad y seguridad de las RT actuales es la Señalización por Canal Común (CCS: Common Channel Signaling). El SS7 definido por la Unión Internacional de Telecomunicaciones (ITU International Telecommunication Union) en sus recomendaciones Q.7XX [CCITT, 1989], es el mayor exponente de los sistemas de CCS actualmente. El SS7 es el principal elemento para soportar un gran número de aplicaciones (gran parte de ellas de reciente aparición) en las RT incluyendo desde el control de llamada en la interconexión de oficinas en una Red Digital de Servicios Integrados, hasta servicios de IN y Telefonía Móvil.

II.2 Elementos de la red SS7 y arquitectura funcional

Un sistema CCS está formado por una red de conmutación de paquetes que es superpuesta (ver la Figura 1) sobre la red troncal (la red de transporte). Es así como las RTs

modernas presentan una estructura en dos planos, uno de ellos el plano de señalización y el otro el plano de transporte. Como ya se ha mencionado, entre otras cosas, el plano de señalización sirve para establecer, mantener y liberar conexiones sobre el plano de transporte.

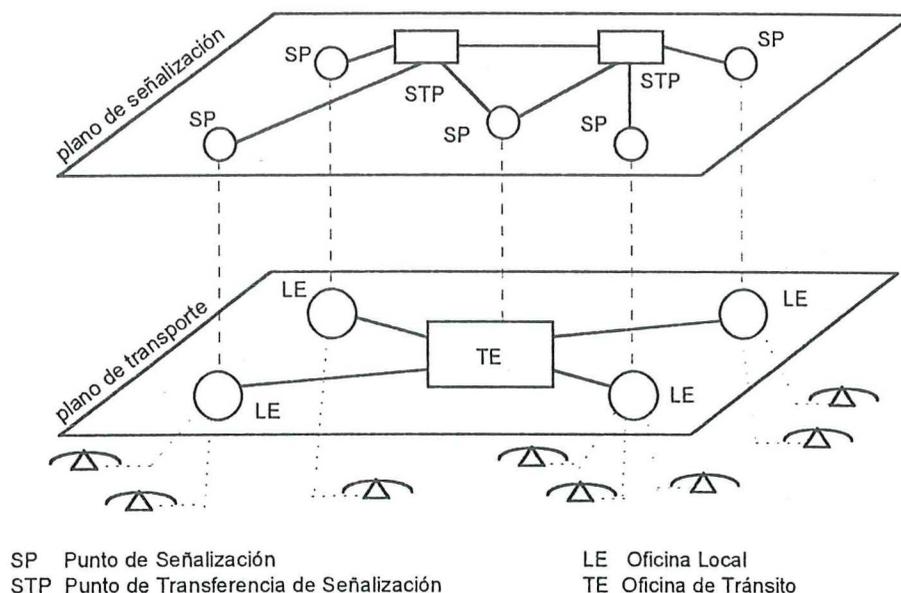


Figura 1. Estructura de una red de telecomunicaciones moderna

En las RTs, el *plano de transporte* está constituido por Oficinas Locales (LE: Local Exchanges), Troncales y Oficinas de Tránsito (TE: Transit Exchanges). Las LEs son las oficinas de conmutación a las cuáles se conectan los usuarios de la red (representados en la figura por medio de aparatos telefónicos), su función es establecer conexiones (o al menos una parte de ellas) entre usuarios (utilizando para ello sus funciones de conmutación). Las LEs se conectan entre si por medio de TEs utilizando como medio de interconexión líneas troncales. Las TEs utilizan sus capacidades de conmutación para establecer rutas de comunicación entre LEs dinámicamente a medida que los usuarios lo demandan.

El *plano de señalización* está formado por Puntos de Señalización (SP: Signaling Point), Puntos de Transferencia de Señalización (STP: Signaling Transfer Point) y Enlaces de Señalización (SL: Signaling Link). Los SPs son los puntos en donde se origina y/o termina la señalización. Los SPs se comunican entre si por medio de los STPs que son

conmutadores de paquetes encargados de encaminar los mensajes de señalización desde el SP en donde se originaron hasta el SP destino. La interconexión entre SPs y STPs se realiza utilizando SLs. El Punto de Control de Servicios (SCP: Service Control Point) (no mostrado en la figura) contiene lógica de servicios y los datos para procesar servicios que requieren procesamiento de red inteligente..

Los oficinas de origen y destino de una conexión en el plano de transporte, establecen rutas de comunicación enlace por enlace, enviando y recibiendo mensajes a través del plano de señalización. Hay bastantes beneficios que se ganan mediante el uso de una red CCS:

- Hay una reducción significativa del tiempo de establecimiento de llamada.
- La existencia de un enlace de señalización separado del enlace de transporte de información de usuario, facilita el control de la llamada antes y durante la conversación a la vez que proporciona capacidad de señalización adicional, flexibilidad y seguridad. Esta capacidad de señalización adicional puede ser utilizada para proporcionar nuevas características de llamada.
- La capacidad de la red de señalización para el transporte de datos (ya que es una red de conmutación de paquetes) puede ser explotada para soportar funciones de manejo, mantenimiento, y tarificación en la red.
- La disponibilidad de un estándar mundial resulta en una más simplificada interconexión de redes internacionales.
- Si se interconectan las bases de datos a la red de señalización se gana la capacidad de introducir una gran cantidad de nuevos servicios (Ejemplos de ellos son servicios de IN y Redes Móviles).

Esta última característica es la base que ha propiciado la introducción de modernos y variados servicios en las RT. Los pormenores de la red inteligente son presentados enseguida.

II.3 El porqué de la IN

La desregulación en el mercado de las telecomunicaciones¹ ha propiciado un ambiente de competencia sin precedentes en ésta industria. Los diversos contendientes en la lucha por el mercado, tratan de atraer nuevos clientes ofreciéndoles servicios novedosos y atractivos, a la vez que con éstos servicios tratan de estimular en sus actuales usuarios una mayor utilización de la red y con ello incrementar sus ganancias. Un factor importante que influye en el éxito de este negocio es el soportar el diseño y la introducción de nuevos servicios en un tiempo reducido. Tradicionalmente la creación de nuevos servicios en las redes de telecomunicaciones tomaba de 2 a 3 años. Era necesario programar el servicio en cada una de las oficinas de conmutación de la red y, debido a la coexistencia de equipo de conmutación de diversos proveedores dentro de la red, este proceso era muy tedioso y demandante en tiempo pues cada equipo de conmutación proveniente de diferente fabricante requería de su propia versión de programa para realizar un servicio. También sucedió que llegó el momento en que la cantidad de servicios programados en cada oficina y los datos necesarios para su ejecución era tan grande que programar un servicio nuevo cada vez era más complicado.

El concepto de Red Inteligente surgió para permitir la rápida creación e introducción de servicios en las redes de telecomunicaciones. El término IN es utilizado para designar a la inteligencia desplegada sobre las redes de telecomunicaciones en la forma de bases de datos de acceso en tiempo real para controlar los servicios ofrecidos en éstas redes; es decir, es la capacidad para proporcionar servicios basados en software desde procesadores externos a los sistemas de conmutación. Una de las principales características de la IN es la utilización del SS7 como mecanismo de transporte de información. Los servicios normalmente son realizados de manera tal que una vez desarrollados, los suscriptores y usuarios del servicio puedan adecuarlos (personalizarlos) a sus requerimientos. Ejemplos de tales servicios son: Servicios de números 800's, redes virtuales privadas, enrutamiento flexible, etc.

¹ El mercado de los E.E.U.U. fué el primero en vivir la desregularización de la industria de las telecomunicaciones, pero muy pronto ésta política fué adoptada por los mercados de otros países y regiones como el Reino Unido, Japón, Australia, la Unión Europea, México, etc.

Antes de analizar los detalles de la SS7 y la IN, es importante ver la diferencia en la manera en que una red digital *no inteligente* y una *inteligente* manejan las llamadas.

En una red no-inteligente el proceso de establecimiento de llamada es a grandes rasgos como sigue:

- La parte que llama marca un número telefónico y la oficina local utiliza su software de procesamiento de llamada para decidir como manejar la llamada. Este rechaza la llamada o trata de establecer una conexión con el abonado llamado.

En una Red Inteligente el procesamiento de una llamada es como sigue:

- La parte que llama marca un número telefónico y la oficina local usa su software de procesamiento de llamada para decidir si manejar ella misma la llamada o pedir ayuda a algún dispositivo externo que contenga lógica de servicio. Si se requiere de ayuda, la oficina local envía un mensaje a algún dispositivo externo apropiado, quien utiliza su lógica de servicio, los datos del abonado llamado y el tipo de servicio solicitado para decidir como puede ser manejada la llamada. Tomada ésta decisión, el dispositivo externo envía una o más instrucciones de control al sistema de conmutación en la oficina local para indicarle como manejar la llamada. El sistema de conmutación entonces rechaza la llamada o trata de establecer una conexión con el abonado llamado tomando en cuenta las instrucciones de la lógica del dispositivo externo.

Esta habilidad de las oficinas locales para acceder lógica de servicio externa es el principio básico detrás del procesamiento de llamada en la IN.

La IN ha sido ya estudiada y estandarizada por los organismos internacionales. En Norteamérica Bellcore ha estandarizado a la IN en su proyecto de Red Inteligente Avanzada (AIN: Advanced Intelligent Network), internacionalmente la ITU-T ha emitido importantes recomendaciones en sus recomendaciones Q.12XX. Ambas organizaciones han producido a la fecha recomendaciones incompatibles, aunque persiguen el mismo objetivo. Se espera que en un futuro cercano (antes del año 2000) ambas versiones de la IN converjan. En este trabajo se hablará acerca de los estándares de la ITU.

II.3.1 Objetivos de la IN

Los objetivos de la IN son permitir la inclusión de capacidades adicionales para hacer más fácil el proporcionar servicios, lograr independencia entre el servicio y la red (es decir el servicio no debe depender de alguna configuración de red específica) y propiciar un ambiente abierto de competencia entre los diversos proveedores de equipo (para ello es necesario que los equipos de diferentes vendedores puedan comunicarse entre si y es donde los estándares juegan un papel importante).

Los objetivos de la ITU-T para ésta arquitectura conceptual son:

- La IN deberá ser aplicable a todas las redes de telecomunicaciones (PSTN, ISDN, Redes Móviles, etc.)
- La IN deberá permitir a los proveedores de servicio el definir sus propios servicios, independientemente de los servicios específicos desarrollados por los proveedores de equipo.
- La IN deberá permitir a los operadores de la red el asignar la funcionalidad, los recursos y los mecanismos adecuados en sus redes para administrarlas de manera eficiente, independientemente de los desarrollos específicos de red hechos por los proveedores de equipo.
- La IN deberá ser introducida a partir de las redes existentes y las recomendaciones actuales de la ITU-T.
- La IN deberá evolucionar para reflejar las experiencias anteriores, las nuevas oportunidades tecnológicas, y la evolución de mercado.

Debido a las necesidades de estandarización y de evolución, la ITU-T ha emprendido un trabajo de estandarización en etapas hacia lo que llama la arquitectura IN final, definiendo para cada etapa un conjunto de capacidades. Cada Conjunto de Capacidades (CS: Capability Set) de la IN pretende estudiar los requerimientos para una o más de las siguientes áreas: La Creación de Servicios, el Manejo y Administración de Servicios, el Procesamiento de Servicios y la Interconexión de Redes (lograr la trascendencia de la IN a nivel global). Este camino en etapas toma en cuenta el hecho que la especificación y desarrollo de las redes que reúnan todos los objetivos de la arquitectura IN final tomará algunos años. A fin de permitir

una evolución gradual hacia la IN final, el conjunto de recomendaciones IN ofrecerá compatibilidad hacia atrás en cada fase evolutiva. La meta de la ITU-T es definir un concepto de arquitectura nuevo que satisfaga las necesidades de los proveedores de servicios.

A la fecha la ITU ha liberado ya los dos primeros conjuntos de capacidades (CS-1 y CS-2) de su proceso evolutivo. El CS-1 y el CS-2 en sí son un subconjunto de la arquitectura IN final. El CS-2 complementa al CS-1, de hecho el texto de CS-2 es en mucho muy similar al de CS-1, pero CS-2 incluye además capacidades para la creación de servicios, el soporte para el manejo de servicios, interconexión de redes de distintos proveedores o países y capacidades para el soporte de movilidad de usuarios, como por ejemplo soportando servicios como Telecomunicaciones Personales Universales (UPT: Universal Personal Telecommunications) y servicios de Redes Móviles. El CS-2 fue liberado en Mayo de 1996.

El lector interesado en conocer más acerca de los servicios actuales que la IN ha hecho posible puede consultar [Berman Roger y Jonh Brewster, 1992; y Robrock, 1991], para mayores detalles en los estándares de la ITU-T para la IN, el lector es referido a [ITU-T, 1993-1996].

En lo que resta del capítulo se introducirá la arquitectura del SS7 que permite proporcionar servicios ISDN, IN y redes móviles. Al final del capítulo se presenta un ejemplo de servicio IN.

La filosofía de la IN en un ambiente de comunicaciones móviles, así como un ejemplo de arquitectura de red móvil con características de IN es introducida en el capítulo III.

II.4 Arquitectura de los protocolos del SS7

El SS7 es esencialmente un sistema de comunicaciones con una estructura en capas, que se distingue de otros sistemas de comunicaciones de datos por su gran desempeño en tiempo real y sus requerimientos de confiabilidad [Abdi Modarressi y Ronald Skoog, 1990; Jabbari Bijan, 1991]. No importa lo complejo que sea el conjunto de las interacciones de la red para establecer una llamada, el tiempo de establecimiento de llamada debe ser menor a 2 segundos (de lo contrario los usuarios de la red se sentirán decepcionados del servicio), esto

impone un estricto control sobre el retardo extremo a extremo de los mensajes de señalización. Respecto a la confiabilidad de la red, los requerimientos (integridad de los mensajes, disponibilidad extremo a extremo, robustez de la red, recuperación ante fallas, etc.) son muy demandantes, por ejemplo el tiempo máximo de indisponibilidad entre un par de nodos arbitrarios en la red de señalización no debe exceder 10 minutos/año, lo cual es por lo menos unos 2 ordenes de magnitud menor que para los nodos de las redes de datos convencionales.

En la Figura 2 se ilustra la arquitectura de los protocolos del SS7 y se relacionan con el modelo de referencia OSI.

La Parte de Transferencia de Mensajes (MTP: Message Transfer Part) (comprendida por las partes MTP-1, MTP-2 y MTP-3) proporciona un servicio confiable (sin pérdida ni duplicaciones) tipo datagrama (es decir, sin conexión) para la transferencia de mensajes de señalización a través de la red desde la fuente (SP de la red en donde el mensaje de señalización se originó) hasta su destino. La MTP por si sola no proporciona toda la funcionalidad de los tres primeros niveles de la OSI, esto se debe a que fue concebida teniendo en mente las necesidades de ejecución en tiempo real de algunas aplicaciones como la telefonía.

Para satisfacer los requerimientos de otras aplicaciones que precisan de toda la funcionalidad del nivel 3 de la OSI (por ejemplo las funciones para el manejo de la red), se creó la Parte de Control de la Conexión de Señalización (SCCP: Signaling Connection Control Part). La SCCP mejora la capacidad de direccionamiento de la MTP y además proporciona el soporte de circuitos virtuales. A la combinación de la MTP y la SCCP se le conoce como Parte de Servicio de Red (NSP: Network Service Part).

La Parte del Usuario ISDN (ISUP: ISDN User Part) proporciona las funciones de las capas 4-7 de la OSI realizando las funciones de señalización necesarias para soportar operaciones relacionadas con el control de llamada y servicios ISDN suplementarios. La expresión "Parte del Usuario ISDN" quiere decir que la ISDN es usuario de los niveles inferiores del SS7 (ya sea MTP ó NSP).

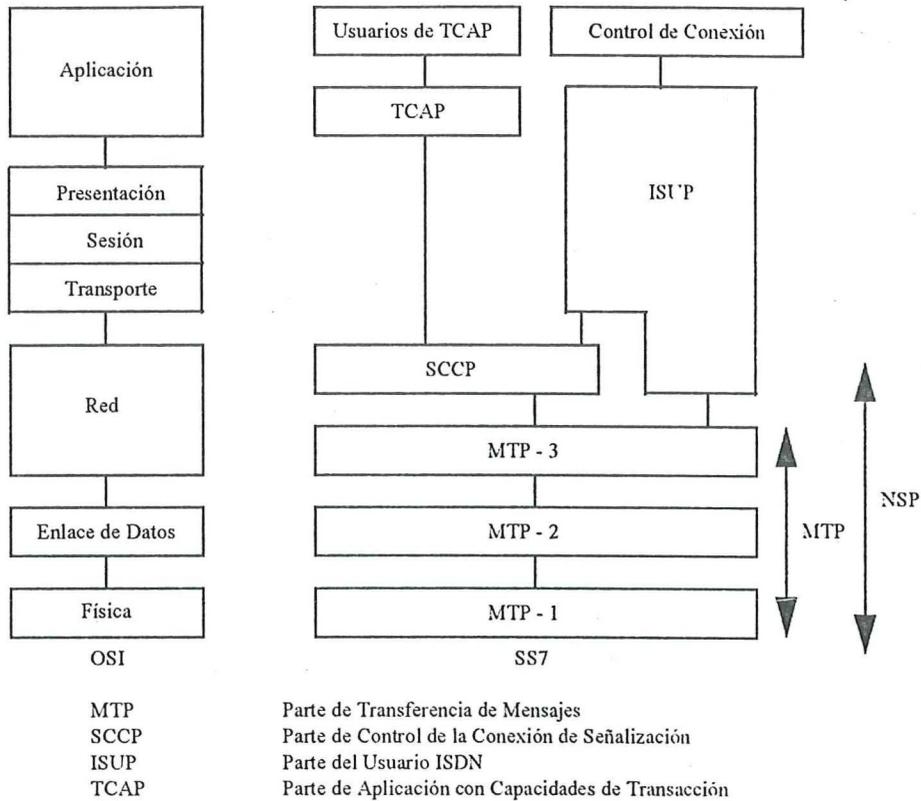


Figura 2. Estructura de los protocolos de la SS7

La Parte de Aplicación con Capacidades de Transacción (TCAP: Transaction Capabilities Application Part), equivale al nivel 7 de la OSI y proporciona un conjunto de operaciones *tipo transacción* que pueden utilizarse por la parte de aplicación en un nodo, para invocar la ejecución de un procedimiento en otro nodo y para comunicar el resultado de tal invocación, ésta característica es pieza clave para la provisión de los servicios de IN.

II.5 Parte de transferencia de mensajes (MTP)

Como ya se ha establecido, la MTP es la base para proporcionar el transporte confiable de mensajes a través de la red de señalización, además proporciona capacidad para el manejo de la red en caso de fallas, ésta característica no está presente en otros protocolos tales como X.25, IP, etc. A continuación se describen los 3 niveles que conforman la MTP.

II.5.1 MTP-1

La MTP-1 especifica las características físicas, eléctricas y funcionales del canal de comunicación que interconecta entre sí los elementos de la red de señalización. Este es un canal digital bidireccional operando a 64 kbps (en la especificación de la ITU) ó 56 kbps (en la especificación de la ANSI) y dedicado exclusivamente para el uso de SS7. Los canales de comunicación pueden ser terrestres o satelitales. Los enlaces son proyectados de modo que sean utilizados [Stallings William, 1995] sólo hasta en un 40% de su capacidad por los mensajes de señalización de usuarios (capas superiores) de manera que ellos puedan manejar el tráfico de otros enlaces en caso de falla. Se pueden agrupar hasta 36 enlaces de señalización entre dos nodos de la red si el tráfico de señalización entre nodos adyacentes así lo amerita [CCITT, 1989].

II.5.2 MTP-2

La MTP-2 realiza las funciones correspondientes a la capa 2 del modelo OSI, se utiliza un protocolo orientado a bit muy similar al HDLC (High-level Data Link Control) para el control del enlace de datos en la transferencia de Unidades de Señalización (SU: Signaling Unit) entre nodos adjuntos de la red (las SUs corresponden a las “tramas” de HDLC), pero a diferencia de éste, en la MTP-2 se establecen funciones para el monitoreo de la calidad de los enlaces que permitan a la red reaccionar en caso de retardos excesivos que llegasen a experimentar los mensajes de señalización y en caso de fallas (ya sea de enlaces o nodos) de la red de señalización. La Figura 3 muestra el formato de las SUs de la MTP-2. Hay 3 clases de SUs: La Unidad de Mensajes de Señalización (MSU: Message Signaling Unit), la Unidad de Estado del Enlace de Señalización (LSSU: Link Status Signaling Unit) y la Unidad de Señalización de Relleno (FISU: Fill-In Signaling Unit).

Las MSUs se encargan del transporte de la información de señalización de los usuarios de la capa MTP-2 (es decir transportan la información de la MTP-3). Las LSSUs transportan información acerca del estado del enlace de señalización. Las FISUs son enviadas cuando no hay MSUs ni LSSUs para enviar, se utilizan para proporcionar reconocimientos de MSUs y para ayudar a determinar la calidad del enlace de

comunicaciones y tomar las acciones necesarias a tiempo (como aislar enlaces, redireccionar tráfico, etc.).

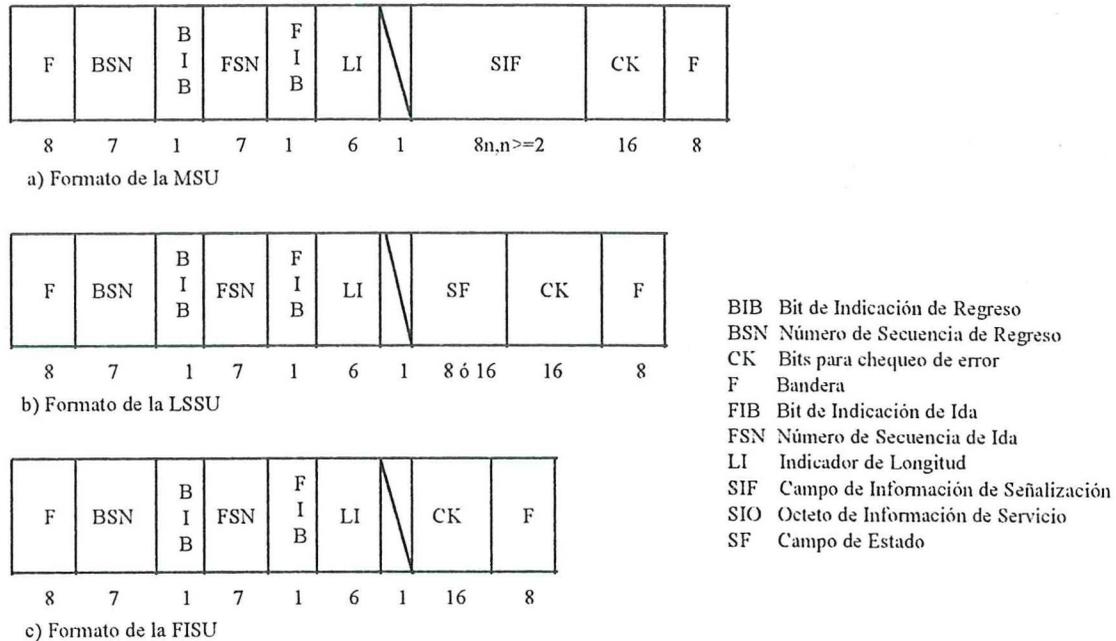


Figura 3. Formatos de la unidad de señalización

Los 3 tipos de SUs tienen en común los siguientes campos:

Banderas (F: Flags). (8 bits) Delimitan el inicio y fin de las SUs por medio de un patrón único (01111110). Para asegurar que no ocurra este patrón dentro de la SU, se utiliza la técnica de inserción "0" donde antes de la transmisión se revisa a la SU de tal modo que inmediatamente después de cualquier ocurrencia de cinco 1's consecutivos en el cuerpo de la SU es insertado un 0. En el receptor luego de haber detectado y removido las banderas, se eliminan los 0's que ocurran luego de cinco 1's consecutivos. De esta manera se logra recuperar la información.

Números de Secuencia de Ida y Regreso (FSN: Forward Sequence Number y BSN: Backward Sequence Number). (7 bits c/u) Ayudan para ejercer el control de flujo y control de error de SUs entre dos nodos que comparten un enlace de datos de señalización entre sí. El FSN representa el número de secuencia de la MSU actualmente transmitida y el BSN representa el número de secuencia de la MSU que está siendo reconocida. Por cada MSU

transmitida (recibida) se incrementa el FSN (BSN) en una unidad utilizando módulo 128. En un instante dado no más de 127 MSUs pueden estar sin ser reconocidas (el tamaño de ventana es 127). Las LSSUs y las FISUs llevan el FSN de la última MSU que se transmitió.

Bits de Indicación de Ida y Regreso. (FIB: Forward Indicator Bit y BIB: Backward Indicator Bit). (1 bit c/u) Sirven para diferenciar una transmisión normal de una retransmisión. Si la SU transmitida es una transmisión normal el FIB es puesto a 0; si se trata de una retransmisión el FIB se pone a 1. Similarmente, cuando se reconoce una SU debida a una transmisión normal el BIB se pone a 0; cuando se reconoce una SU debida a una retransmisión se pone a 1 el BIB.

Indicador de Longitud (LI: Length Indicator). (6 bits) Es el mecanismo utilizado para diferenciar entre los 3 tipos de SUs. Cuando el LI tiene valor de 0 indica una FISU, un valor de 1 ó 2 indica una LSSU y un valor mayor a 2 indica una MSU. Cuando el tamaño del campo SIF de la MSU es mayor a 63 octetos (máximo número que se puede expresar con 6 bits) LI se pone en 63. La máxima longitud del campo de datos de una MSU es 272 octetos, este número fue escogido para evitar largos retardos en la transmisión de los mensajes dada la limitada capacidad de los enlaces (64 ó 56 kbps).

Bits para el Chequeo de Error (CK: Check Bits). (16 bits) Se generan a partir de la SU (utilizando para ello un polinomio generador) y se agregan a ésta en la transmisión antes de insertar las banderas y efectuar la inserción positiva, su propósito es la detección de errores. En el receptor luego de remover las banderas se utiliza el mismo polinomio generador en busca de errores de transmisión.

De manera adicional las MSUs incluyen el Campo de Información de Señalización (SIF: Signaling Information Field) que contiene la información misma de capas superiores (MTP-3), esta información no es procesada por los protocolos de capa 2 sino más bien sólo es transportada.

Las LSUs incluyen un campo denominado Campo de Estado (SF: Status Field) por medio del cuál se pueden reportar diversas fallas como pérdidas de alineamiento, enlaces fuera de servicio, falla de procesador y ocupado.

Un diagrama a bloques que ilustra las funciones realizadas por la MTP-2 es presentado en la Figura 4. Estas funciones son explicadas en seguida.

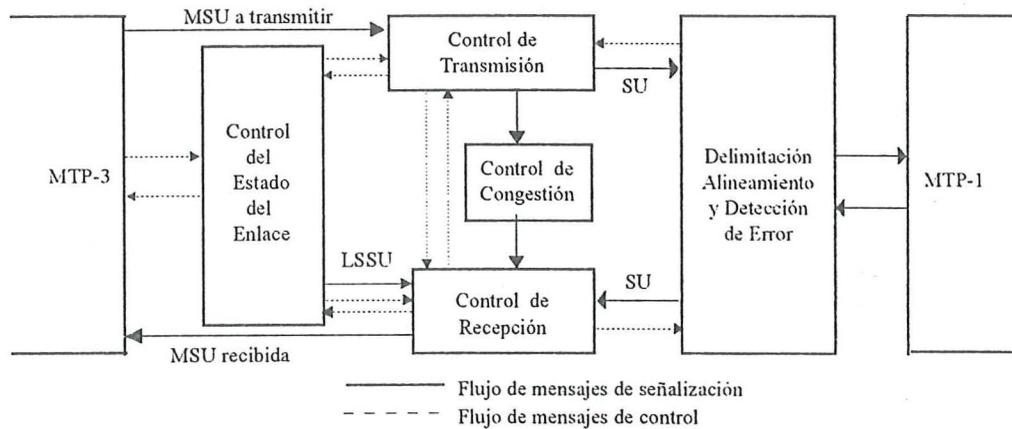


Figura 4. Diagrama funcional a bloques de la MTP-2

Para la *delimitación y alineamiento de tramas* se utilizan las banderas en la forma que ya se ha mencionado. Se considera que se ha perdido alineamiento cuando ocurre en la SU un patrón no permitido (por ejemplo más de cinco 1's consecutivos) ó cuando la longitud de la SU (especificada por el campo LI) no coincide con la longitud de la SU de la trama en cuestión. La *detección de errores* se realiza por medio de los bits para chequeo de error tal y como ya se ha mencionado. El *control de transmisión* y el *control de recepción* implementan la técnica de control de flujo y control de error (basándose en gran medida en los campos FSN, RSN y CK) conocida como *regresa n* (go-back-n); en presencia de errores todas las SUs no reconocidas deben ser retransmitidas. Se utilizan una serie de temporizadores para asegurar que el retardo de las SUs sea menor al máximo permitido. Un nodo puede ejercer control de flujo al detener el envío de reconocimientos de las SUs recibidas. El *control de congestión en enlaces* se ejercita cuando un receptor nota en un enlace alguna condición de congestión, para ello el receptor comienza a transmitir periódicamente Indicaciones de Estado Ocupado (SIB: Status Indication Busy) (usando para ello SUs tipo LSSU) al transmisor a intervalos de (TA) 80-120 ms. La primer SIB recibida activa un temporizador (TB) (3-6 segundos). Si la congestión cesa antes que TB expire, se sigue operando normalmente, de lo contrario se declara el enlace como fallo. El *control del estado del*

enlace se realiza de la siguiente manera, existe un contador que se incrementa en uno cada vez que se recibe una SU con error (es decir una SU que no pasa la prueba de chequeo de error) y se decrementa en uno por cada 256 SUs recibidas correctamente. Si el contador excede un valor “umbral”, entonces se toman las medidas para declarar el enlace como fallo por excesivo número de errores en la transmisión (entre éstas medidas está por ejemplo el informar a las funciones de manejo del enlace de capa 3 de la situación).

II.5.3 MTP-3

La capa MTP-3 realiza 2 funciones importantes (ver la Figura 6), la función de Manejo de los Mensajes de Señalización y la función de Manejo de la Red de Señalización. La primera se encarga del enrutamiento de los mensajes de señalización a través de la red y la segunda realiza funciones de reconfiguración de la red en caso de fallas o congestión.

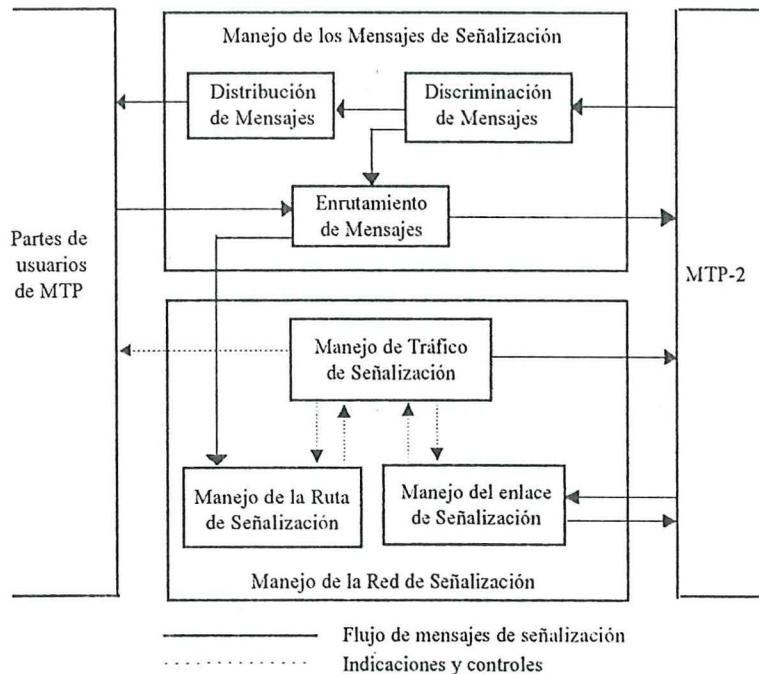


Figura 5. Diagrama funcional a bloques de la MTP-3

La estructura de los mensajes de la capa MTP-3 asociados a éstas funciones es mostrada en la Figura 6. Los aspectos relevantes de ambas figuras son explicados en seguida.

El Manejo de los Mensajes de Señalización: Se realiza por medio de las funciones de enrutamiento, discriminación y distribución de mensajes. Esta función se encarga del transporte de los mensajes de los usuarios de MTP a través de un enlace o una ruta de señalización (enlaces de señalización sucesivos). Para lograrlo, se sirve de los campos Selección del Enlace de Señalización (SLS: Signaling Link Selection), el Código del Punto de Origen (OPC: Originating Point Code), el Código del Punto de Destino (DPC: Destination Point Code) y el Indicador de Servicio (SI: Service Indicator) de la estructura de mensaje de capa MTP-3 (ver la Figura 6). Para enrutar (o enviar) un mensaje sobre un enlace de señalización, el punto de señalización que origina el mensaje forma una etiqueta de enrutamiento utilizando para ello una tabla de enrutamiento, ésta tabla le proporciona al nodo información de todos los enlaces de señalización disponibles para alcanzar a cada Punto de Destino. Normalmente existen una serie de rutas alternas disponibles entre cada Punto de Origen y Cada Punto de destino. El SLS proporciona distribución de carga (load sharing) entre las diversas rutas posibles, que puede ser utilizada para diversificar las rutas de señalización para transacciones sucesivas. Sin embargo para preservar la secuencia de mensajes en una transacción, se debe escoger el mismo SLS. Cuando se recibe un mensaje de señalización en la capa MTP-3 de un nodo, se le examina el DPC, si éste coincide con la dirección del nodo en cuestión, el mensaje es entregado a la función de distribución de mensajes quien, examina a la parte Indicador de Servicio (SI: Service Indicator) del mensaje para decidir la parte de usuario de MTP a quien debe transferir el mensaje. Por el contrario, si no existe una coincidencia y el nodo tiene la capacidad de STP, entonces el mensaje es dirigido a la función de enrutamiento de mensaje

El Manejo de la Red de Señalización: Su propósito es proporcionar la reconfiguración de la red de señalización en el caso de fallas de enlaces o puntos de señalización y proporcionar control de tráfico en caso de congestión o bloqueo. El objetivo es reconfigurar la red en caso de alguna posible falla, evitando la pérdida o duplicación de mensajes y manteniendo el retardo en la entrega de mensajes en niveles aceptables. Han sido definidos procedimientos específicos para cambiar la configuración de la red o recobrar la

configuración normal dada la falla o disponibilidad en los enlaces, rutas o puntos de señalización. El lector interesado en mas detalles puede consultar [Stallings William, 1995] y [CCITT, 1989].

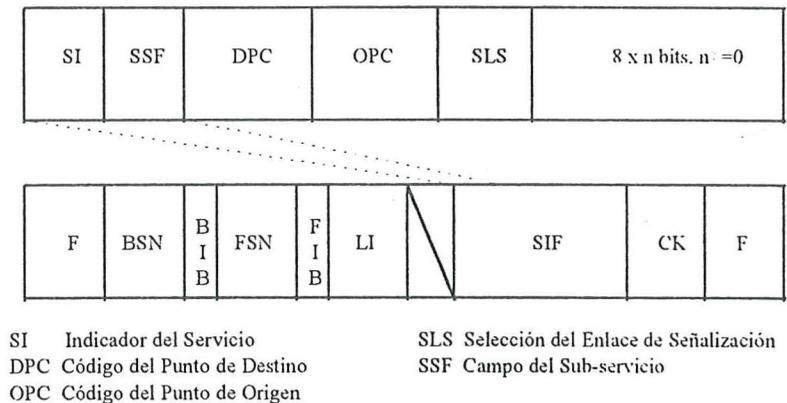


Figura 6. Estructura del mensaje de la MTP-3

II.6 SCCP

La SCCP mejora la funcionalidad ofrecida por la MTP al soportar direccionamiento extendido, permitir direccionar mensajes con título global, proporcionar servicios con y sin conexión y al enriquecer los mecanismos de manejo de red proporcionados por la MTP.

Para proporcionar direccionamiento extendido, la SCCP utiliza además del DPC (ver la Figura 6) Números de Subsistema (SSN: Subsystem Numbers) que, proveen información de direccionamiento local a la SCCP para distinguir entre los usuarios de la SCCP en un nodo.

El direccionamiento de mensajes con título global se realiza de la siguiente manera. Cuando un SP que origina un mensaje no tiene la dirección de red del punto destino, el SP en cuestión construye entonces un mensaje con el DPC de un punto de señalización (típicamente un STP) y un título global. En el STP el título global es convertido a la forma DPC + SNN del nodo al cuál el título global se refiere. Al estar el mensaje en ésta forma, éste podrá ya ser enrutado en la manera convencional. La Figura 7 presenta la estructura básica de la SCCP. La SCCP proporciona a sus usuarios (capas del protocolo SS7 por encima de la SCCP) las siguientes clases de servicios:

- Clase 0 Servicio Orientado a no Conexión Básico
- Clase 1 Servicio Orientado a no Conexión con Secuenciación
- Clase 2 Servicio Orientado a Conexión Básico
- Clase 3 Servicio Orientado a Conexión con Control de Flujo

El servicio clase 0 es un servicio tipo datagrama puro en donde se entregan los mensajes sin secuenciación a los usuarios. En el servicio clase 1 se proporciona secuenciación de mensajes al asignar el mismo SLS (ver la Figura 6) para los mensajes del mismo usuario. En el servicio clase 2 se proporciona secuenciación además de segmentación y ensamble de mensajes cuando los mensajes de usuario excedan la longitud máxima permitida por SCCP. La clase 3 suplementa las capacidades de la clase 2 al incluir control de flujo y en caso de posible pérdida de secuenciación, la conexión puede ser restablecida.

La SCCP proporciona mecanismos para el manejo de la red de señalización por encima de aquellos que la MTP proporciona, incluyendo procedimientos para disminuir el tráfico de mensajes en caso de falla o congestión de la red. Estos procedimientos se aplican tanto a los servicios orientados a conexión como a los servicios orientados a no conexión. La información de manejo hace uso de los servicios sin conexión de SCCP para su transporte.

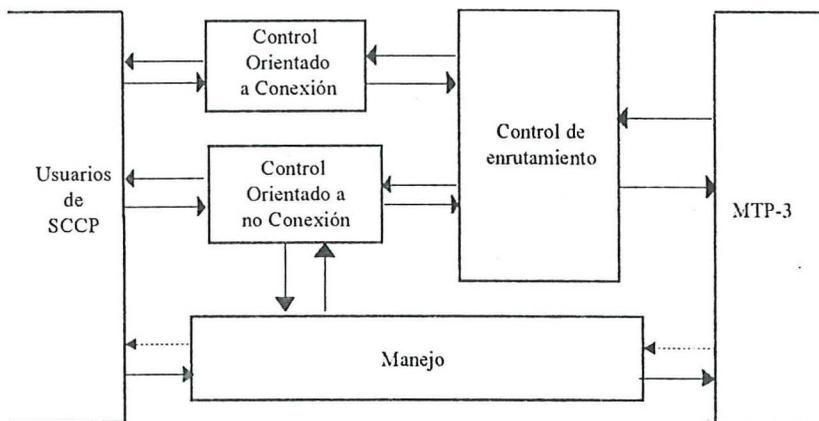


Figura 7. Estructura básica de la SCCP

La Figura 8 presenta el formato del mensaje SCCP. El mensaje consta del código de identificación del tipo de mensaje (Hay 16 mensajes diferentes agrupados en mensajes para servicios orientados a conexión, mensajes para servicios orientados a no conexión y mensajes de manejo), una parte fija obligatoria, una parte variable obligatoria y una parte

opcional (el contenido de éstas partes depende del tipo de mensaje). Para una explicación mas detallada de la operación de SCCP el lector es referido a [Stallings William, 1995] y [CCITT, 1989].

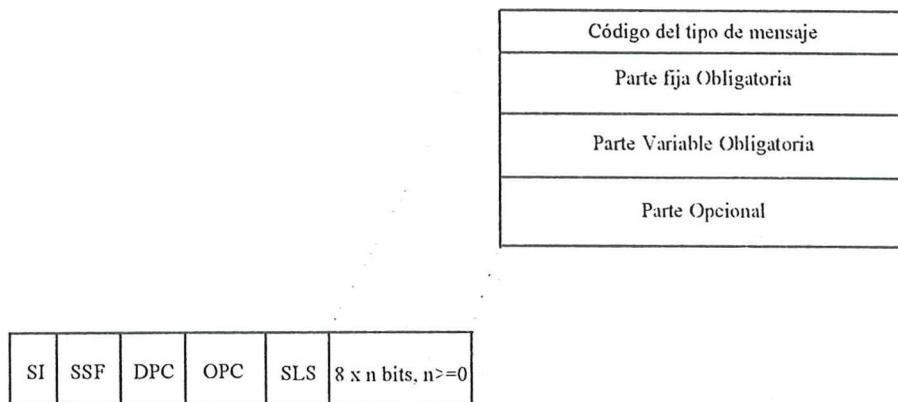


Figura 8. Formato del mensaje de la SCCP

II.7 ISUP

El protocolo de la ISUP proporciona servicios de llamada para el soporte de ISDN. El protocolo cuenta con la funcionalidad para la provisión de servicios básicos y servicios ISDN suplementarios. Para los servicios básicos se incluye el establecimiento, supervisión y liberación de conexiones entre oficinas sobre la red de transporte. Ejemplos de servicios ISDN suplementarios son *Identificación del Abonado que Llama*, *Redireccionamiento de Llamada*, *Señalización de Usuario a Usuario* y *Grupo Cerrado de Usuarios*.

El formato del Mensaje de la ISUP es presentado en la Figura 9 (La ISUP utiliza los servicios de la MTP ó la SCCP, sin embargo la discusión aquí asumirá comunicación con MTP directamente). El mensaje de la ISUP se compone de un código de identificación de circuito (una troncal), el código del tipo de mensaje (los cuales se presentarán posteriormente) que permite distinguir entre los diferentes mensajes, y finalmente hay unas partes fijas y variables obligatorias seguidas de una parte opcional. La información de éstas partes y su longitud depende del tipo de mensaje.

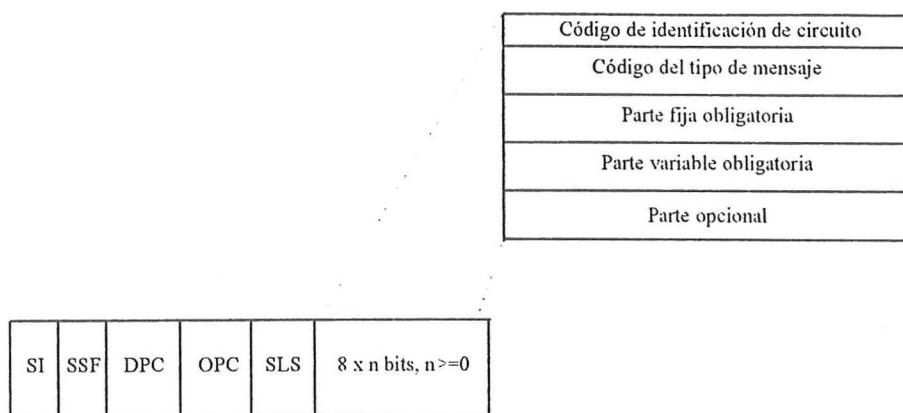


Figura 9. Formato del mensaje de la ISUP

La estructura básica de la ISUP es mostrada en la Figura 10. ISUP se compone de 3 funciones básicas que son el control para procesamiento de llamada, el control para la supervisión de llamadas y el control de envío y distribución de mensajes. La primera parte maneja el control necesario para establecer y liberar circuitos, la segunda asegura la continuidad del enlace una vez que éste ha sido establecido y la tercera se encarga de la interfaz de éstas funciones con la capa inferior (MTP ó SCCP).

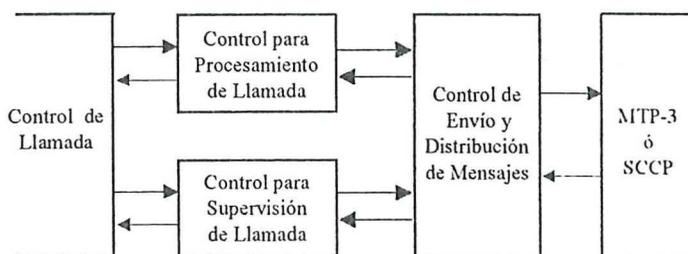


Figura 10. Estructura funcional de la ISUP

Existen una gran cantidad de mensajes ISUP definidos, donde cada mensaje realiza una función específica. La Tabla I proporciona una lista resumida de algunos de ellos que son utilizados para el establecimiento, supervisión y liberación llamadas. (Sólo se incluyen los campos obligatorios de los mensajes).

Tabla I. Algunos mensajes de la ISUP

Mensaje ISUP	Abreviación	Dirección	Propósito	Parámetros (Obligatorios)
Mensaje de Dirección Inicial	IAM	Directa	Para iniciar el establecimiento de llamada reservando una troncal de salida y llevando el código de troncal, el número de destino y otra información para el enrutamiento y manejo de la llamada.	Tipo de mensaje, indicadores de la naturaleza de la conexión, indicador de dirección directa, categoría de la parte que llama, medio de transmisión requerido, número de la parte llamada.
Mensaje de Dirección Completa	ACM	Regreso	Para indicar la recepción de la dirección de la parte llamada en la oficina a la que está conectado el abonado llamado.	Tipo de mensaje, indicador de dirección de regreso.
Mensaje de Contestación	ANM	Regreso	Para indicar que la llamada ha sido contestada.	Tipo de mensaje
Mensaje de Continuidad	COT	Directa	Para verificar la continuidad del enlace de comunicación entre oficinas.	Tipo de mensaje, indicadores de continuidad.
Mensaje de Liberación	REL	Ambas	Para indicar que el circuito debe ser liberado.	Tipo de mensaje, Indicadores de la causa.
Liberación Completa	RLC	Ambas	Para indicar que el circuito ha sido liberado.	Tipo de mensaje.

En la Figura 11 se presenta un ejemplo de llamada utilizando mensajes y procedimientos ISUP². El proceso comienza cuando un abonado conectado a la oficina local LE-1 le indica a ésta su deseo de realizar una llamada por medio del mensaje *establecer* que incluye el número del abonado destino de la llamada, la LE-1 reserva entonces una troncal (por ejemplo la troncal “A”) de salida hacia la oficina de tránsito TE-1 (que representa parte de la mejor ruta para conectar al abonado que llama con el abonado llamado) y construye el Mensaje de Dirección Inicial (IAM: Initial Address Message) que (incluye el identificador de la troncal reservada y el número del abonado llamado entre otras cosas) envía a través de la red de señalización hacia la TE-1. La TE-1 recibe el mensaje y termina de establecer la troncal “A” y reserva la troncal “B” hacia la TE-2 que representa parte de la ruta hacia el abonado llamado. La TE-1 construye un mensaje IAM que incluye el número del abonado llamado y una identificación de la troncal B que acaba de reservar y lo envía a TE-2. Este proceso se repite en TE-2 cuando recibe el mensaje IAM; de ésta manera se va construyendo (parte por parte) el enlace que ha de conectar al abonado que llama con el abonado llamado. Al llegar el mensaje IAM a la LE-2, éste (vía el mensaje *establecer*) informa al abonado

² En la figura se han incluido los mensajes de señalización entre los abonados y la red sólo por dar al lector una idea más clara del proceso de llamada. La señalización entre el usuario y la red se realiza utilizando el protocolo Q.931. Para distinguir a los mensajes Q.931 de los mensajes ISUP utilizaremos para los mensajes Q.931 letras minúsculas.

En cuanto a los servicios suplementarios se hará una breve descripción de 2 de los más difundidos, ellos son identificación del usuario que llama y redireccionamiento de llamada.

II.7.1 Identificación del usuario que llama

La operación de este servicio se compone de presentación y restricción de la identidad de la línea que llama. El servicio de Presentación de la Identidad de la Línea que Llama (CLIP: Call Line Identity Presentation) se utiliza para presentar en la parte llamada el número telefónico de la parte que llama. Si la parte llamada tiene activado el servicio de Restricción de la Identidad de la Línea que Llama (CLIR: Call Line Identity Restriction) se puede prevenir la presentación de la línea que llama en la parte llamada. La transmisión del número de la parte que llama se puede hacer incluyéndolo en el mensaje IAM ó bien bajo petición explícita (por parte de la parte llamada) en un mensaje especial. Si CLIR está activado en la parte que llama, la oficina que sirve a la parte que originó la llamada lo hace saber por medio de un parámetro en el mensaje IAM.

II.7.2 Redireccionamiento de llamada

Este servicio permite la redirección de una llamada bajo 3 diferentes condiciones. La primera es una redirección incondicional, es decir todas las llamadas destinadas para un número que ha activado este servicio serán transferidas a otro número previamente designado. La segunda es un redireccionamiento bajo no contestación, cuando una llamada no es contestada por el usuario que ha contratado este servicio, la llamada es transferida a otro número previamente designado. La tercera es redireccionamiento selectivo, es decir si la llamada entrante proviene de un abonado que no está en un grupo predefinido por el usuario que ha contratado el servicio, entonces la llamada es redireccionada a otro número previamente designado. Una vez que la oficina que alberga a la parte llamada ha decidido efectuar un redireccionamiento de llamada (de cualquiera de los 3 tipos), ésta checa si el número designado para la redirección está en sus dominios. Si es así, la oficina por si misma puede terminar de entregar la llamada. En caso contrario deberá enviar un mensaje IAM a la oficina que alberga al usuario de tal número.

II.8 TCAP

La TCAP constituye el nivel más alto de la estructura de protocolos SS7. La TCAP soporta operaciones para servicios con y sin conexión. Los servicios orientados a conexión pueden ser utilizados por aplicaciones de datos en gran volumen (tolerantes a retardos), mientras que los servicios orientados a no conexión son utilizados normalmente por aplicaciones interactivas (datos cortos sensibles al tiempo) que se ven beneficiados del poco procesamiento y bajos retardos que son característicos a los servicios sin conexión. En este apartado sólo hablaremos de las funciones y procedimientos de la TCAP necesarios para servicios sin conexión, esto debido a que los servicios de Redes Inteligentes y Comunicaciones Móviles hacen uso solamente de los servicios sin conexión debido a sus requerimientos de ejecución en tiempo real. La TCAP no proporciona control de flujo, control de error ni secuenciación de mensajes. Al hacerlo se perdería el poder soportar aplicaciones en tiempo real debido al procesamiento que éste tipo de operaciones requiere.

Esencialmente la TCAP proporciona un conjunto de operaciones que pueden ser utilizadas por la aplicación de un nodo para invocar la ejecución de un procedimiento en otro nodo e informar el resultado de tal invocación. Como tal, éste incluye protocolos y servicios para realizar operaciones remotas. En las redes de telecomunicaciones, las aplicaciones distribuidas que usan la TCAP pueden residir en las oficinas de conmutación ó en las bases de datos de la red. La principal aplicación de la TCAP en éstas redes es para invocar procedimientos remotos para soportar los procedimientos necesarios en los servicios de telefonía móvil y en redes inteligentes (como por ejemplo servicio de números 800's). La TCAP se compone de dos subcapas: La subcapa de componente y la subcapa de transacciones. La subcapa de componente es responsable de la especificación y asociación de unidades de datos (operaciones y respuestas) llamadas componentes. La subcapa de transacción proporciona un eficiente medio para el intercambio de mensajes que contienen a esas componentes al establecer una *pseudoasociación* extremo a extremo entre los dos usuarios de la TCAP. Esta asociación es establecida sin necesidad de intercambiar mensajes

adicionales. El primer mensaje de un diálogo lleva las componentes iniciales y a la vez establece ésta asociación.

El mensaje TCAP está formado por dos partes, una identifica el estado de la transacción (y a la transacción misma) y la otra incluye cada una de las componentes, cada componente está especificada por un tipo de componente y parámetros. Como se puede ver en la Figura 12, el identificador del estado de la transacción puede ser: *Comenzar*, *Continuar*, *Terminar*, *Abortar* y *Unidireccional*. Hay 4 tipos de componentes que son: *Invocar*, *Regresar Resultado*, *Regresar Error* y *Rechazar*. *Invocar* se utiliza para invocar la realización de operación remota, *Regresar Resultado* para comunicar el resultado de tal invocación, *Regresar Error* se usa para notificar la causa por la cuál la operación no pudo realizarse y *Rechazar* se usa para notificar algún error de sintaxis en la petición.

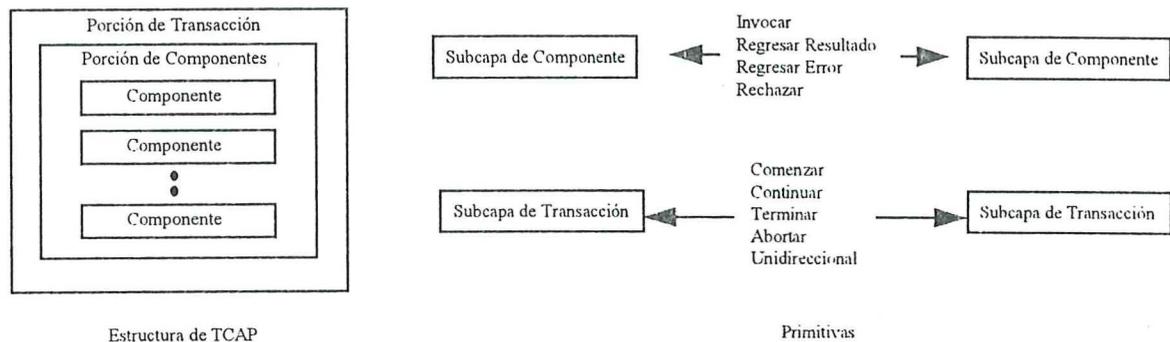


Figura 12. Estructura de la TCAP y primitivas

Los servicios de la TCAP están compuestos de la siguiente secuencia de eventos (ver la Figura 13):

1. El usuario del servicio A especifica las operaciones que el usuario B debe realizar, así como sus parámetros necesarios y pasa éstas componentes a la subcapa de componente. En seguida emite una componente de manejo de diálogo que inicia la transferencia de éstas componentes a la subcapa de transacción.
2. La subcapa de transacción del usuario A reúne éstas peticiones en un sólo mensaje y lo pasa a capas inferiores (capa SCCP). Este mensaje también indica el establecimiento de una asociación entre los dos usuarios.

3. El ejecutor del servicio B, recibe éstas componentes desde su propia subcapa de componente, entonces procede a solicitar operaciones de A o realiza las operaciones solicitadas desde A. Entonces B pasa las componentes que contienen los resultados o las peticiones a la subcapa de componente. Estas componentes son ensambladas en un sólo mensaje por la subcapa de transacción y transmitidos a A cuando el usuario de B expide una componente de manejo de diálogo. Este mensaje podría también especificar la terminación del diálogo si ya no se esperan más mensajes.
4. La subcapa de componente de A recibe éstas componentes, los asocia con la petición que ha hecho con anterioridad y los pasa al usuario A. El usuario A puede solicitar la terminación del diálogo si ya no desea la realización de más operaciones (si B no lo ha hecho ya) o realizar las operaciones que B ha solicitado (si acaso lo ha hecho). Si éste es el caso, todo vuelve a ocurrir a partir del paso 2.

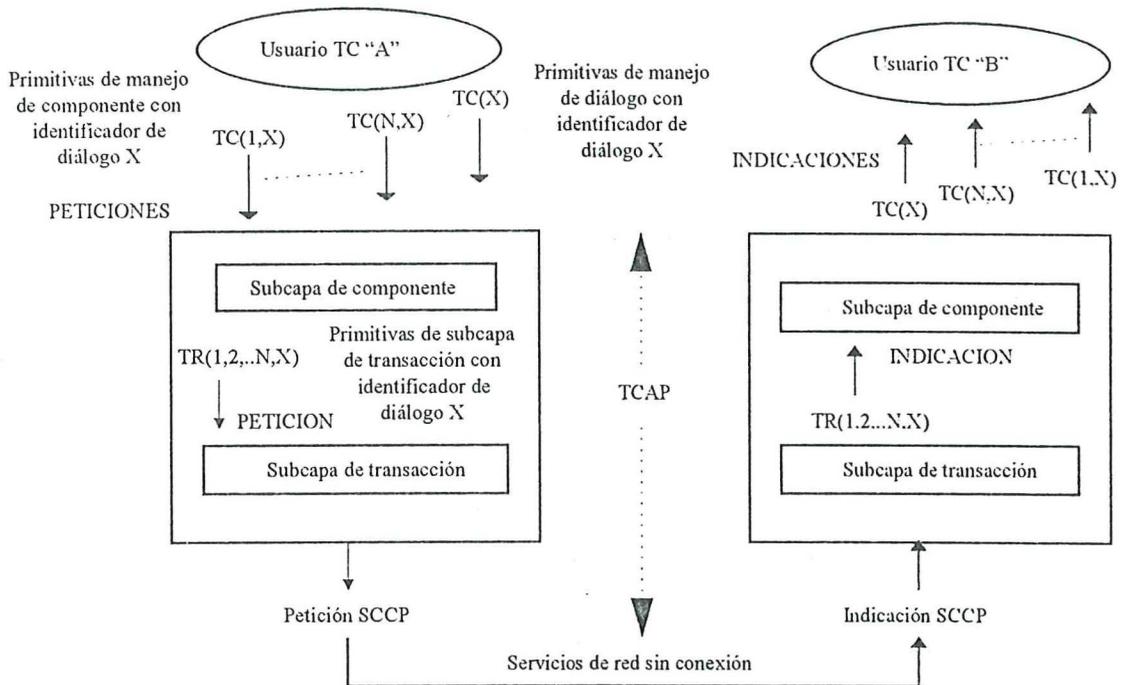


Figura 13. Formato del mensaje de la TCAP y operaciones de las subcapas

II.8.1 Ejemplo de servicio de red inteligente

A modo de ejemplificar los conceptos que se han presentado, se incluye un ejemplo de la operación del protocolo TCAP. Considérese un servicio de números 800 interactivo, una

manera posible de realizarlo se presenta en la Figura 14. La oficina local (LE) de la figura ha recibido una solicitud de llamada desde un usuario de la red. Dado que la LE no sabe el número de directorio (número para enrutamiento) que corresponde a ese número 800, ésta consulta a la base de datos de la red (mensaje *comenzar*) a fin de que ésta realice una conversión de números (a partir de un 800 obtener un número de directorio). A fin de que la base de datos pueda proporcionar el número de directorio equivalente, ésta pide a la LE (primer mensaje *continuar*) que haga un anuncio de voz al usuario que originó la llamada para solicitar al usuario la introducción de dígitos adicionales. Cuando la LE recibe los números adicionales desde el usuario, ésta los envía a la base de datos de la red (segundo mensaje *continuar*) quien utiliza la información recibida para realizar la traducción deseada. La base de datos de la red regresa entonces el número de directorio resultante de la traducción, mismo que envía a la oficina local (mensaje *terminar*). Cuando la oficina local recibe el número de directorio, ésta puede establecer una llamada a ese número utilizando los procedimientos ISUP explicados en la sección II.7.

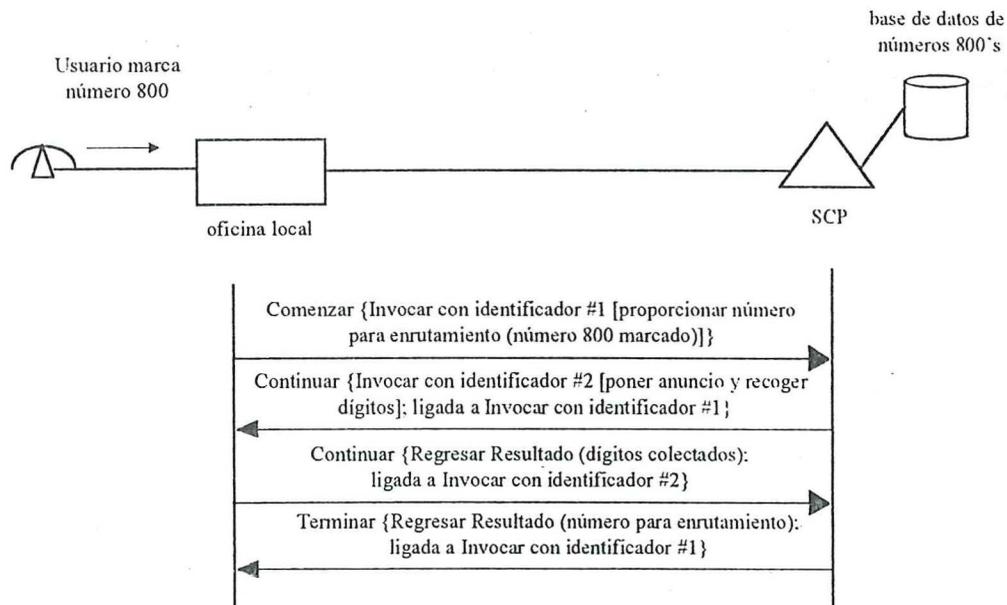


Figura 14. Ejemplo del uso de la TCAP: servicio de números 800's

III. SERVICIOS DE COMUNICACION PERSONAL (PCS)

III.1 Introducción

En los Servicios de Comunicación Personal (PCS: Personal Communication Services) los usuarios son provistos de pequeñas terminales inalámbricas desde las cuales pueden hacer y recibir llamadas en una manera similar a como lo hacen los usuarios de la red pública, sin embargo, a diferencia de ellos los usuarios de los PCSs no se encuentran atados a ninguna conexión física. Esto significa que los usuarios pueden desplazarse libremente con sus terminales por toda el área de radio-cobertura de la red (o incluso en otras redes PCSs que posiblemente sean operadas por otros proveedores de servicio) y tener acceso a los servicios que ellos han contratado independientemente de su ubicación.

El término PCS se aplica a aquellos sistemas que son el fruto de la evolución de los sistemas celulares de segunda generación y se caracterizan por una alta densidad de usuarios, la coexistencia de usuarios con alta y baja movilidad, una gran variedad de servicios y una capacidad superior del sistema de red. Los PCS pretenden permitir además de servicios de telefonía, el intercambio de información multimedia (datos, imágenes, fax y video). Los PCS se perfilan como el camino a seguir para la implementación de los sistemas celulares de tercera generación actualmente en proceso de especificación y estandarización a nivel mundial.

La evolución de los sistemas celulares ha sido posible gracias a los avances logrados en diversas áreas de la electrónica. Los sistemas de primera generación eran analógicos, utilizaban terminales voluminosas y hacían un poco eficiente uso del espectro de radio. Entre los sistemas de primera generación destacan el Sistema Telefónico Móvil Avanzado (AMPS: Advanced Mobile Phone System) utilizado en Norteamérica, el Sistema de Comunicaciones de Acceso Total (TACS: Total Acces Communication System) de la Gran Bretaña, el Sistema Telefónico Móvil Nórdico (NMT: Nordic Mobile Telephone) utilizado en Escandinavia y el Sistema Alemán C450.

Los sistemas de segunda generación surgieron para superar algunas de las limitaciones de los sistemas de primera generación. La premisa fue lograr una mayor capacidad en los

sistemas y con ello reducir los costos. Los sistemas de segunda generación se caracterizan por la utilización de técnicas digitales en diversos subsistemas de transmisión incluyendo una eficiente codificación de la voz, códigos para la detección y corrección de errores y técnicas de modulación digitales eficientes.

En Europa debido a la existencia de varios sistemas de primera generación incompatibles, se vislumbró la oportunidad de introducir un sistema de segunda generación que unificase a los sistemas de primera generación existentes. De hecho, los Europeos proyectaron un sistema digital nuevo e incompatible con los ya existentes para el cuál se asignaron frecuencias específicas. El resultado de todo este proyecto fue la introducción del mayor exponente de los sistemas de segunda generación existentes: El Sistema Global para Comunicaciones Móviles (GSM: Global System for Mobile Communications) que a la fecha ha sido adoptado por más de 50 países en el mundo.

En Norteamérica (México, Estados Unidos y Canadá) debido a la existencia de un mismo sistema de primera generación (el AMPS), no se vivió una fuerte necesidad por un sistema nuevo. Más bien se ha dejado que el mercado sea quien decida el sistema que prevalecerá. Por lo pronto en los EE.UU. existen ya 6 diferentes interfaces de radio incompatibles entre si (utilizando ya sea FDMA, TDMA ó CDMA). Las terminales de usuario son duales, es decir que soportan el manejo de dos interfaces de radio. Una de ellas es el AMPS que aún prevalece en el mercado y la otra es alguna de las 5 interfaces digitales existentes. Esta es una situación indeseable ya que debido a la disimilitud existente entre las diferentes interfaces de radio, se corre el riesgo de no lograr la interoperabilidad de los PCS en América ni siquiera a nivel nacional y podría dejar a muchos clientes frustrados y sin deseos de suscribirse a los PCS a menos que se logre una unificación de éstos sistemas como en Europa.

III.2 El concepto celular

La porción del espectro de radio asignada a los sistemas celulares es limitada (esto es, el número de canales de radio disponibles en PCS es limitado). Para hacer un uso eficiente de este preciado recurso se ha recurrido a una técnica conocida como reuso de frecuencia. Esta

técnica consiste en asignar ciertas frecuencias (canales) a un área geográfica determinada. Se permite a los usuarios dentro de esa área determinada el transmitir con una potencia baja de modo a que a determinada distancia, esos mismos canales puedan ser reutilizados por otros usuarios y que la interferencia resultante sea muy baja.

III.3 Estructura de una red celular

En la Figura 15 se presenta una red con estructura celular [Jabbari Bijan, 1992]. El área de cobertura de la red (área sobre la cuál se ofrece el servicio) es dividida en pequeñas regiones llamadas células (por su forma hexagonal). Hay una Estación Base (BS: Base Station) por cada célula encargada de proporcionar cobertura de radio a la célula (en la figura sólo se muestran algunas de ellas). Los usuarios del servicio son provistos de terminales móviles o portátiles (MS: Mobile Stations) que se pueden instalar en vehículos o traer en sus bolsillos. La comunicación entre la MS (equipo de usuario) y la BS (equipo de red) tiene lugar por medio de canales de radio.

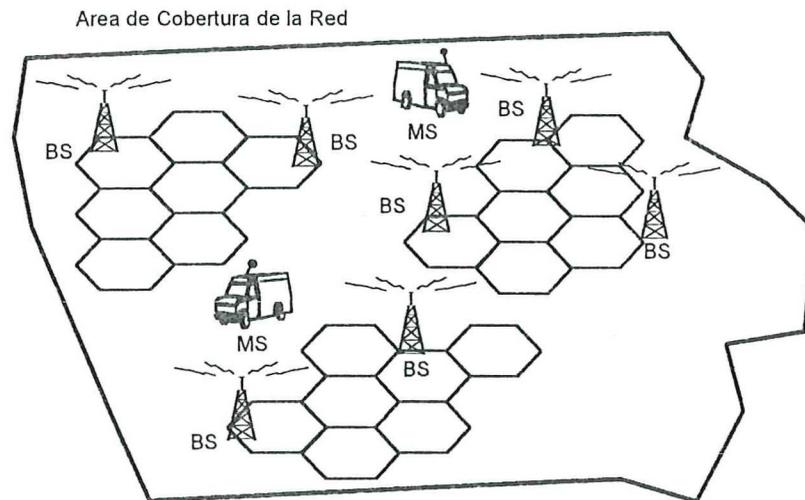


Figura 15. Estructura de una red celular

III.4 La introducción de la IN en las redes móviles

En años recientes, las comunicaciones móviles han experimentado un acelerado crecimiento en número de usuarios. Todo parece indicar que esta tendencia continuará y se vislumbra que en un futuro cercano (tal vez unos 3-7 años) el acceso a las Redes de

Telecomunicaciones será predominantemente inalámbrico. Los proveedores de servicio de las redes móviles en su afán por acaparar parte del mercado, se preocupan por ofrecer una gran cantidad de servicios. El tiempo para la introducción de nuevos servicios es ahora un factor importante. Este tiempo puede definir el éxito o el fracaso de los proveedores de servicio.

La movilidad de los usuarios impone serios retos a la red [Wirth Patricia, 1995], ésta debe ser capaz de seguir la pista de los usuarios a medida que ellos se desplazan a través de la red a fin de entregarles llamadas entrantes a ellos destinadas. Así mismo la red debe de proporcionar a los usuarios acceso a los servicios contratados sin importar el lugar de la red en la que éstos se encuentren. Adicionalmente, la red debe de proporcionar mecanismos para la autenticación de usuarios, estos mecanismos están diseñados para proteger a la red del acceso de MS fraudulentas (como el acceso a la red es por medio de radio, hay posibilidad de que intrusos quieran hacerse pasar por verdaderos usuarios de la red). Similarmente también debe ofrecer mecanismos de privacidad a los usuarios para evitar que algún aficionado provisto de algún equipo de radiocomunicación pueda escuchar la comunicación de algún usuario de la red.

Para enfrentar estos retos los diseñadores de las redes PCS actuales han echado mano de las facilidades que proporcionan el Sistema de Señalización Numero 7 (SS7) y el concepto de Red Inteligente. Estas herramientas ya han sido explotadas exitosamente en la PSTN, sin embargo ahora en un ambiente móvil, el flujo de información necesario para actualizar las bases de datos de la IN a medida que los usuarios se desplazan por la red, reciben u originan llamadas, o tratan de acceder a sus servicios suscritos, impone a las bases de datos de la red (quienes proveen la inteligencia de la red) una mayor carga. Entre las funciones que debe realizar la IN en un ambiente PCS destacan autenticación de usuarios, registro de terminales, entrega de llamadas a terminales, origen de llamadas desde terminales, encriptación (para propósitos de comunicaciones seguras), manejo de archivos de usuario (en donde se encuentra registrada toda la información relativa al usuario), provisión de capacidades para el manejo de servicios suplementarios (como redireccionamiento de

llamada, llamada en espera, bloqueo de llamadas, etc.) y funciones para la creación, introducción y personalización de servicios .

III.5 Arquitectura de una red PCS basada en principios de IN

La arquitectura de una red PCS con estructura de IN se muestra en la Figura 16 [Jabbari Bijan 1992; Jabari Bijan, *et al*, 1995]. Los elementos de la IN más relevantes que constituyen ésta arquitectura y las funciones que desempeñan son:

- *La combinación Ambiente de Creación de Servicios/Sistema de Manejo de Servicios (SCE/SMS)* permite el diseño, creación, prueba, despliegue y manejo de nuevos servicios en la red de una manera rápida y eficiente. También es posible desde aquí el personalizar y modificar servicios ya existentes.
- *La combinación Periférico Inteligente/Nodo de Servicios (IP/SN)* proporciona anuncios de voz personalizados a los usuarios indicándoles acciones a realizar como marcación de nuevos dígitos, causas por las que la llamada o servicio no ha sido completada, etc. También se proporciona el reconocimiento de voz y la colección de dígitos.
- *El Punto de Conmutación de Servicios (SSP)* tiene la capacidad para detectar servicios que requieren procesamiento de red inteligente y se comunica con otros elementos de la red para el procesamiento de éstos servicios.
- *El Punto de Control de Servicios (SCP)* posee programas de servicio lógico y datos para procesar servicios de red inteligente; el SCP también tiene acceso a la base de datos Registro de la Localización de los Usuarios Locales (HLR: Home Location Register) de la red y a la base de datos Autenticación.
- *El Punto de Transferencia de Señalización* es un conmutador de paquetes que forma parte de la SS7 y su función es interconectar diversos SSP con el SCP.
- *El adjunto* cuya funcionalidad es muy similar a la del SCP pero éste se conecta directamente al SSP (es decir no requiere de la SS7). El adjunto tiene acceso a la información de la base de datos Registro de la Localización de Usuarios Visitantes (VLR: Visitor Location Register) de la red.

Los elementos de la IN de esta arquitectura se comunican utilizando las facilidades del SS7.

Los elementos de red móvil más importantes de la arquitectura son:

- *La Estación Móvil (MS: Mobile Station)* que representa al equipo de usuario y puede ser portátil o de mano.
- *La Estación Base (BS: Base Station)* quien proporciona radio comunicaciones con la MS y presenta conectividad con el Centro de Conmutación Móvil (MSC: Mobile Switching Center).
- *El MSC* que realiza funciones de conmutación (muy similares a como lo hacen las oficinas locales de la PSTN) y comunica MSs a través de las BSs. La red presenta interconectividad con otras redes ya sean móviles o fijas.

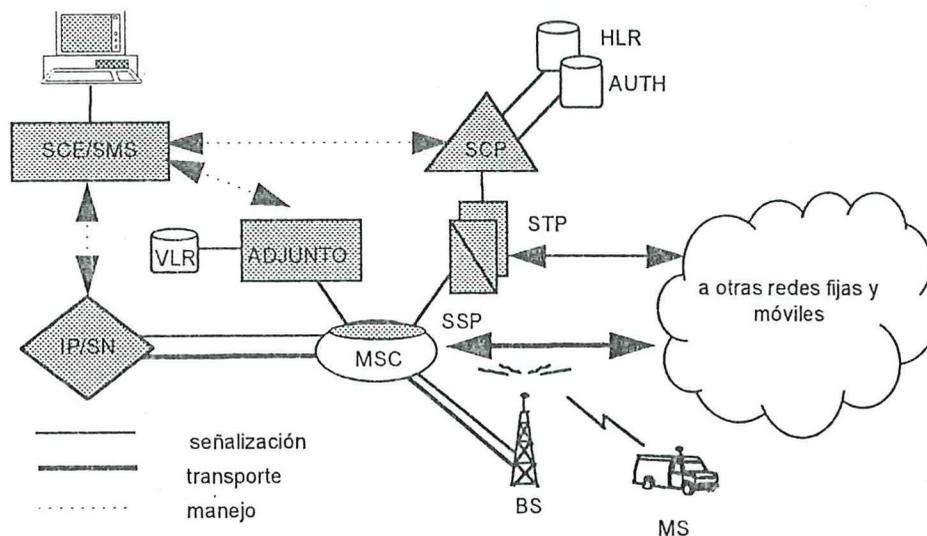


Figura 16. Arquitectura de una red móvil basada en conceptos de la IN

III.6 Estructura de una red PCS típica y manejo de la movilidad de los usuarios

La Figura 17 presenta la estructura de una red PCS típica. Como ya se ha mencionado, el área de cobertura de la red es dividida en pequeñas regiones llamadas células, hay una estación base (BS) por cada célula que proporciona radio comunicaciones a los usuarios que se encuentran dentro de ella. Una célula puede tener entre 100 y 2 000 metros de diámetro. Un grupo de células forman lo que se conoce como Area de Localización (LA: Location

Area). Hay generalmente un MSC y un VLR asociados con una LA. La red presenta conectividad con la PSTN.

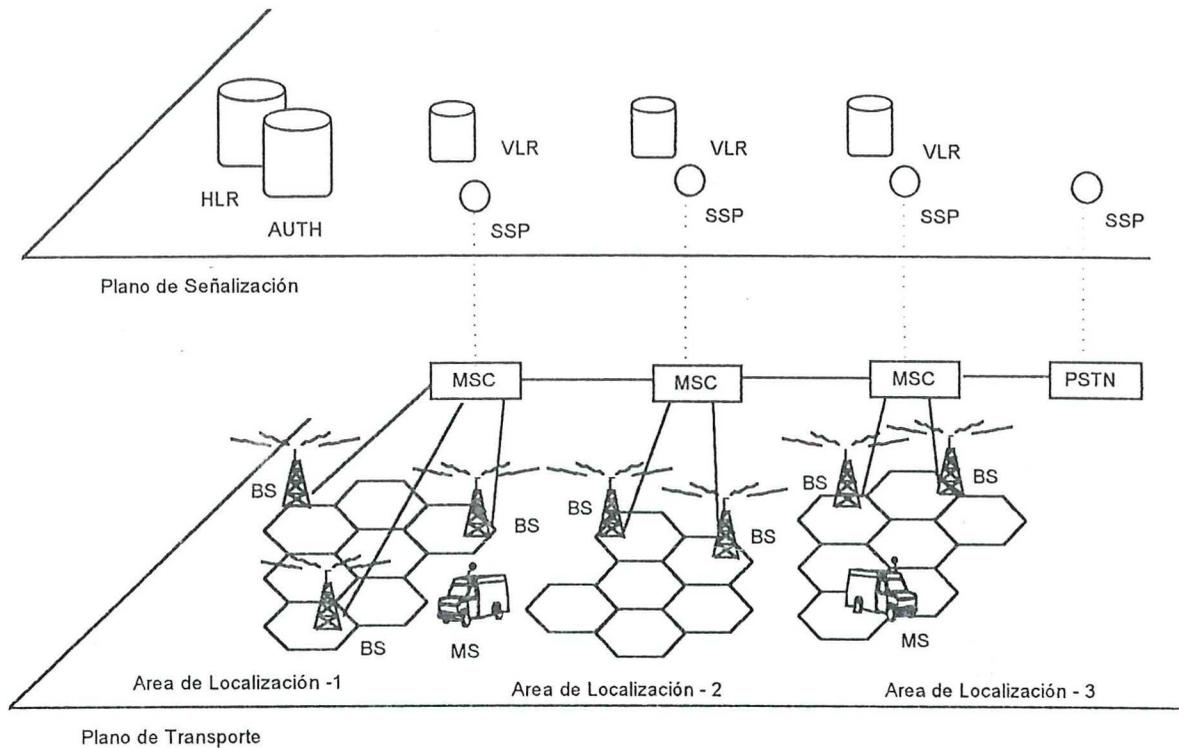


Figura 17. Una red PCS típica

La localización de los usuarios es mantenida por medio de la base de datos HLR. Esta contiene un apuntador hacia la LA actual en la que cada una de las MSs se encuentran actualmente (ya sea dentro de la red de suscripción o incluso en la red de otro proveedor de servicio). El HLR también tiene los datos asignados al momento de suscripción a la red de cada uno de los usuarios. Esta información incluye al número de directorio y el archivo de usuario (donde se especifican los servicios a los que el usuario se ha inscrito)

El VLR es una base de datos que almacena *temporalmente* información selecta recuperada desde el HLR de los usuarios que visitan actualmente su LA asociada. Esa información es utilizada para que el usuario visitante a la LA tenga acceso a los servicios contratados incluso si éste viene de otra red.

El AUTH es una base de datos que contiene claves secretas y otra información requerida para verificar la autenticación de las MSs y para proporcionar privacidad de la información de usuario en el canal de radio (voz, datos, etc.).

III.7 Números en las redes PCS

En PCS existen dos identificadores asociados a cada MS, el primero es denominado Número de Serie Electrónico (ESN: Electronic Serial Number) que es un número único y es asignado a la MS durante su fabricación, este número no se puede modificar sin antes dañar permanentemente a la MS. El otro identificador asociado a una MS es el Número de Identificación Móvil (MIN: Mobile Identification Number) quien contiene al número del plan de numeración americano que es asignado a la MS al tiempo de suscripción y que es el número telefónico que deberá marcarse para llamar al usuario de una MS.

III.8 Fraude en las redes PCS y la manera de erradicarlo

El fraude es uno de los mayores problemas en la industria de las comunicaciones inalámbricas [Cellular Networking Perspectives, 1997]. No sólo es costoso, sino que las medidas tomadas por los proveedores de servicio para contrarrestarlo desalientan en los clientes del sistema el deseo de utilizar el servicio y, además consume tiempo, recursos y energía de parte de los proveedores de servicio en su afán de contrarrestarlo.

El costo debido al fraude tan sólo en E.E.U.U. hasta 1994 era estimado en 1 000 000 dólares Americanos. Actualmente se estima que éste es ya cercano a los 2 000 000 dólares al día.

III.8.1 Las razones del fraude

Hay dos razones principales a las que se les atribuye el fraude. La primera es por el valor del servicio, esto es, el defraudador puede realizar un ilimitado número de llamadas sin costo alguno. La segunda es para propósitos de anonimidad; en este caso el defraudador aprovecha la anonimidad obtenida al introducirse a la red de manera indebida, para realizar comunicaciones destinadas a actividades ilícitas (por ejemplo, venta de drogas, espionaje, etc.), en cuyo caso el obtener el servicio de la red de manera gratuita es tan solo un beneficio adicional.

III.8.2 Puntos vulnerables de la red

Los defraudadores aprovechan ciertas debilidades existentes en diferentes puntos de las redes actuales para introducirse al sistema. Estas son identificadas a partir de la Figura 18.

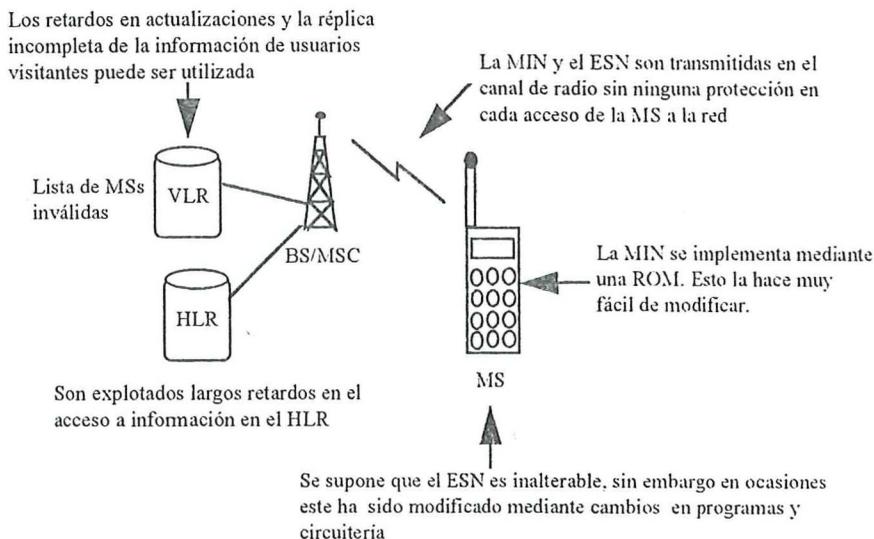


Figura 18. Puntos vulnerables en una red celular

III.8.3 Fraude en los sistemas de primera generación

Los sistemas de primera generación no contaban con mecanismo alguno de protección contra fraude. El fraude era descubierto hasta el momento del intercambio de los registros de cobro entre los proveedores de servicio. Los proveedores encontraban que los intrusos realizaban llamadas desde las áreas visitadas utilizando MSs robadas, MSs con el servicio suspendido ó con el servicio nunca activado.

III.8.4 Listas de usuarios inválidos

Una de las primeras acciones realizadas por los proveedores de servicio para contrarrestar el fraude, fue el mantener una lista de ESNs no permitidas, basándose en el hecho que el ESN a diferencia de la MIN no podía ser modificada. Un ESN asociado con fraude se añadía a la lista del proveedor del servicio, quien a la vez la reportada a todos los demás proveedores y de ésta manera la MS era inutilizada para fraudes posteriores. Este mecanismo es aún utilizado en la actualidad pero su efectividad se ha visto disminuida pues los defraudadores han encontrado formas de modificar el ESN.

III.8.5 Validación positiva

Desde siempre se ha reconocido que la validación en tiempo real de las MSs es necesaria. Sólo cuando la MIN y el ESN de un usuario visitante coincida con un registro en el sistema al cual la MS presumiblemente está suscrita, el sistema que está actualmente dando servicio a la MS podrá estar seguro de ser remunerado por la llamada efectuada. El estándar IS-41 (ver la sección III.9) utiliza ésta técnica.

III.8.6 Réplica de MS

Es la más moderna técnica empleada por los defraudadores. Consiste en la completa duplicación de una MS incluyendo ESN y MIN legítimas.

III.8.7 Otras medidas contra el fraude

Con el paso del tiempo se han sugerido otras soluciones para contrarrestar el fraude. Se ha propuesto desde limitar totalmente o parcialmente las llamadas de usuarios en sistemas visitantes (lo cuál repercute en el desvanecimiento de las ganancias debidas a usuarios visitantes o, en descontento de los usuarios por lo limitado del servicio), hasta análisis computarizados en los patrones de llamada de los usuarios, donde patrones inusuales en el tipo de llamadas, cambio repentino de área de localización de usuarios, etc., conlleva a la terminación de los privilegios de la MS asociada a esa MIN.

La más reciente y efectiva propuesta para erradicar el fraude es mediante autenticación (discutida en la sección III.9.1).

III.9 Protocolo IS-41

El protocolo IS-41 (Inter-System Protocol) ha sido propuesto por la EIA/TIA (Electronic Industry Asociation/Telecommunication Industry Asociation) para lograr la interconectividad e interoperatividad de los diversos sistemas PCS americanos [Husain Syed y James Marochi, 1996; Lin Yi-Bing y Steven Devries, 1995]. Estos procedimientos son independientes de la interfaz de radio utilizada. El IS-41 se implementa por encima de SS7 como usuario de TCAP haciendo pleno uso de las capacidades de la red inteligente. El IS-41 proporciona capacidades y servicios para usuarios visitantes incluyendo:

- Registro automático de terminales en áreas de localización visitadas

- Origen de llamadas por usuario móvil
- Entrega de llamadas a usuario móvil automáticamente
- Traspaso de llamadas en curso (Hand off) entre sistemas
- Servicios Extendidos incluyendo el control de las características del usuario

Para los proveedores de servicio, además de proporcionarles características que mantienen a sus clientes satisfechos, el IS-41 proporciona validación y autenticación de terminales para asegurar que solamente usuarios legítimos tengan acceso a la red.

III.9.1 Mecanismos de seguridad en IS-41 (Privacidad y autenticidad)

Hasta hace muy pocos años en los PCS americanos no se había considerado la adopción de mecanismos de seguridad en la red. Sin embargo recientemente han sido propuestas modificaciones al IS-41 para definir mecanismos para la autenticación de usuarios, privacidad de voz, y encriptación de los mensajes de señalización [Mohan S, 1996] y han sido incorporados en la revisión C del IS-41. Al implementar mecanismos de autenticidad de usuarios, el fraude en los PCS no ocurrirá más. Mediante el uso de mecanismos de privacidad los usuarios podrán realizar comunicaciones seguras pues la información de usuario (voz, datos, fax, etc.) será encriptada. El algoritmo para autenticación, y generación de la máscara para la privacidad de voz y las claves de encriptación para los mensajes de señalización empleadas por el estándar, se basan en técnicas de criptografía por medio de claves privadas en las cuales una clave secreta conocida como Dato Secreto Compartidos (SSD: Shared Secret Data) es compartida entre la MS y la base de datos de Autenticación de la red y es solamente conocida para esas dos entidades.

Hay dos esquemas diferentes que han sido propuestos. En el primero el SSD es compartido únicamente entre la base de datos de Autenticación y la MS. En el otro, el SSD o algún aspecto de éste es también compartido con el sistema visitante.

Debido a la inminente inclusión de los mecanismos de seguridad en PCS, es necesario estudiar en este trabajo los dos esquemas propuestos y comparar su efectividad. Para ello creemos que es beneficioso el explicar el flujo de mensajes en la red debido al esquema en

donde el SSD no se comparte con el sistema visitado y entonces mostrar como éste difiere cuando el SSD es compartido.

Los mecanismos de seguridad pueden ser implantados a discreción a juicio del proveedor de servicios, es común sin embargo invocar éstos mecanismos antes del proceso de registro de terminales y durante el proceso de origen y entrega de llamada. Es probable que los proveedores del servicio decidan introducir éstos mecanismos paulatinamente en sus redes debido al alto impacto que causaría en sus redes el introducirlos repentinamente (ver la sección V.2); paulatinamente significa por ejemplo, que se invoque a los mecanismos de seguridad sólo un porcentaje de las veces que deberían invocar. El valor numérico de este porcentaje y la política de decisión para invocar los mecanismos dependerá de los proveedores de servicios. En este trabajo asumiremos sin embargo que los mecanismos de seguridad son llamados rigurosamente antes del proceso de registro de terminales y durante los procesos de origen y entrega de llamadas.

III.10 Procedimientos del IS-41 sin compartición del SSD

III.10.1 Registro de terminales

Este proceso es invocado automáticamente por una terminal encendida cuando ésta atraviesa los límites de una LA. Por medio de este procedimiento, la MS informa a la red que ha entrado a una nueva LA. En este proceso se debe de redireccionar el apuntador en el HLR asociado con la MS en cuestión para que apunte no a la antigua LA en que el usuario estuvo, sino a la nueva a la cuál ha entrado. Adicionalmente la información de la MS debe ser cargada en el VLR asociado a la nueva LA en la que la MS ha entrado y borrada del VLR asociado a la anterior LA. Este proceso es sumamente útil, y aunque ocurre sin ser percibido por el usuario del servicio, este proceso es quien permite al usuario el recibir llamadas entrantes y tener acceso a los servicios suscritos sin importar su localización en la red (o incluso en otras redes). El flujo de mensajes en la red debido al proceso de registro de terminales es mostrado en la Figura 19 y se explica en seguida.

- a) Una MS determina, basada en la señal transmitida por la BS, que ha entrado a una nueva LA y que requiere registrarse para tener acceso a sus servicios. Entonces

- ejecuta el Algoritmo Celular para Autenticación y Encriptación de Voz (CAVE: Cellular Authentication and Voice Encryption) utilizando el SSD, el ESN, la MIN y un número aleatorio (RAND) obtenido de la BS en ese momento. El algoritmo produce como resultado una clave llamada AUTHR.
- b) La MS solicita registro a la BS proporcionándole la AUTHR, el ESN, el MIN, el RAND y un contador COUNT³ quien mantiene la cuenta de los eventos más significativos (registro, llamadas originadas, entrega de llamadas, etc.) en los que la MS se involucre (Esta misma cuenta es mantenida en la base de datos AUTH).
 - c) La BS hace llegar ésta información a su MSC asociado, en donde a partir de ella se elabora el mensaje IS-41 *AUTHROST* mismo que el MSC envía a su VLR asociado.
 - d) El mensaje *AUTHROST* es así mismo transmitido al SCP y de allí a la base de datos AUT, en donde se utiliza el SSD asociado con la MS y los parámetros recibidos (MIN, ESN, RAND) para producir otra clave, la cuál es comparada con el valor de la clave AUTHR generada por la MS. Si las dos claves coinciden y el contador proporcionado por la MS es igual al contador de la base de datos AUT, entonces la MS es auténtica y se le retorna una clave para encriptar los mensajes de señalización por medio del mensaje *authreqst*.
 - e) Cuando el MSC recibe el mensaje *authreqst*, se inicia el proceso de registro, por medio del mensaje *REGNOT* se registra en el HLR la actual LA a la cuál la MS ha entrado.
 - f) Cuando el HLR recibe el mensaje *REGNOT* a través del SCP, actualiza el valor del apuntador asociado a la MS para que apunte a la LA actual en donde la MS se encuentra y retorna el mensaje *regnot* para confirmar al MSC que se ha registrado a la MSC satisfactoriamente.
 - g) Cuando el mensaje *regnot* llega al SCP, éste lo transmite al VLR de la nueva área de localización y a la vez aprovecha para enviar un mensaje *REGCANC* al VLR de la

³ Al mantener un contador de los eventos significativos tanto en la MS como en la base de datos AUT, la detección de MS impostoras (duplicadas) será fácil.

anterior área de localización para que borre de su base de datos la información de la MS ya que ella ya no se encuentra en su LA asociada. A su vez el VLR hace extensivo el mensaje *REGCANC* a su MSC asociado. Cuando el mensaje *regnot* alcanza al MSC de la nueva LA, el proceso de registro se da por concluido.

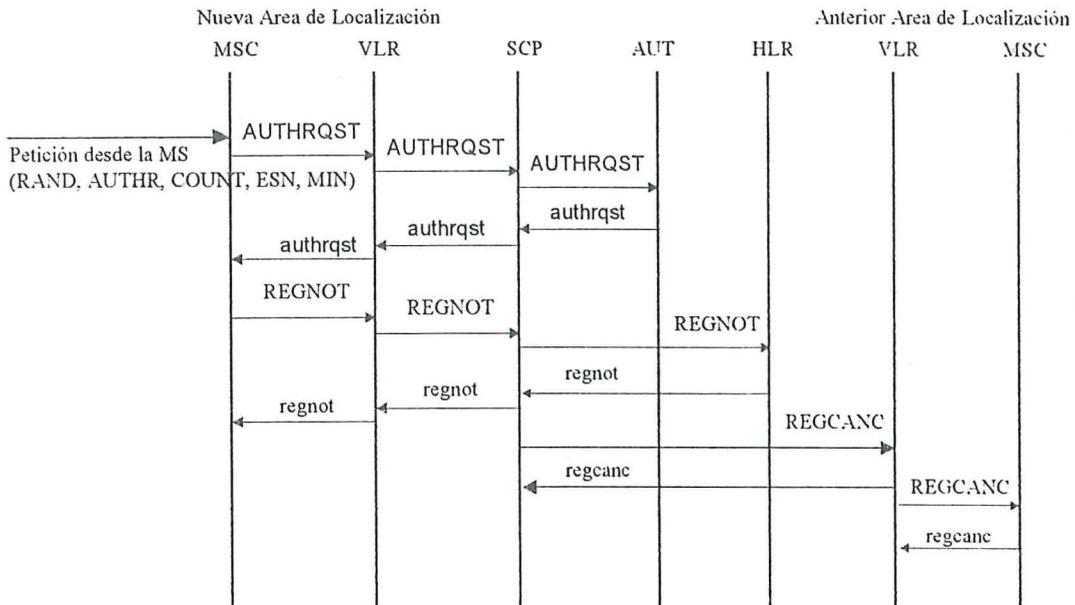


Figura 19. Registro de terminales

III.10.2 Origen de llamadas por usuario móvil

Este proceso permite a un usuario de la red el realizar llamadas a abonados de la PSTN. Para permitir a una MS el realizar una llamada, primero se debe verificar la autenticidad del usuario. Hecho esto, se verifica si el usuario está autorizado para realizar llamadas desde su actual LA. Si este chequeo resulta positivo, entonces la llamada puede ser establecida.

La Figura 20 ilustra el flujo de mensajes generado cuando una MS origina una llamada. El flujo de información es como sigue:

- La MS ejecuta el algoritmo CAVE con los dígitos marcados por el usuario e invoca un proceso para demostrar su autenticidad ante la red. El proceso es similar a como se explicó para el caso de registro de terminales, excepto que en este caso una vez que la base de datos AUT verifica la autenticidad del usuario, devuelve a la MS

además de la clave para encriptación de los mensajes de señalización, una máscara para que en su momento sea empleada para la codificación de voz.

- b) Una vez que la autenticidad del usuario se ha probado, el MSC solicita a su VLR asociado el archivo de usuario por medio del mensaje *PROFREQ*. El MSC precisa del archivo de usuario ya que en éste se almacena toda la información de usuario, incluyendo los servicios suscritos, restricciones, etc.
- c) Si una vez que el MSC ha analizado el archivo de usuario, determina que la llamada puede proceder, entonces utiliza mensajes ISUP para establecer la llamada con la oficina de la PSTN (LE) que corresponde al número marcado por el usuario. Para una explicación de los mensajes ISUP sugerimos al lector consultar la sección II.7.

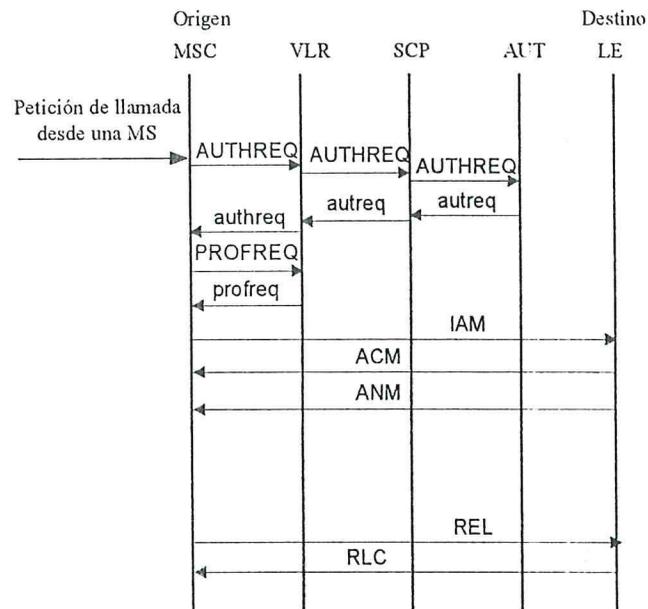


Figura 20. Origen de llamadas

III.10.3 Entrega de llamadas a usuario móvil:

Este proceso permite a una MS el recibir llamadas desde usuarios de la PSTN. Cuando una oficina local (LE) de la PSTN recibe una llamada que tiene como destino una MS, la LE consulta al HLR para saber la LA en la que la MS se encuentra actualmente. Cuando la LE recibe la LA desde el HLR, puede entonces establecer una conexión con el MSC asociado a la LA en la que el usuario se encuentra actualmente. Cuando el MSC mencionado recibe la

solicitud de conexión, realiza un proceso de búsqueda (paging) por todas las celdas que forman la LA para localizar a la MS. Una vez que la MS responde al proceso de búsqueda, el MSC puede entregarle la llamada.

La Figura 21 ilustra el flujo de mensajes entre los elementos de la red debido al proceso de entrega de llamadas a un usuario móvil.

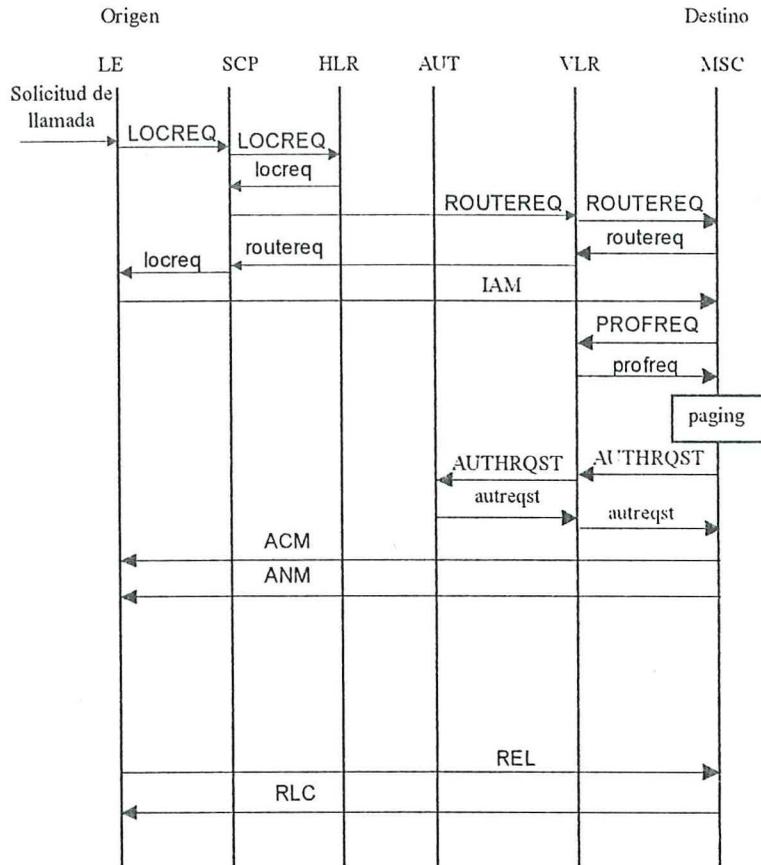


Figura 21. Entrega de llamada

La secuencia de mensajes es como sigue.

- a) Cuando la solicitud de llamada llega a la LE, ésta edita un mensaje *LOCREQ* para solicitarle al HLR (vía el SCP) le proporcione la LA en la que el usuario deseado se encuentra. El HLR devuelve la actual LA del usuario al SCP. El SCP entonces solicita al VLR y al MSC que corresponden a la actual LA del usuario, que asignen a la MS un número telefónico temporal (de aquellos que tienen disponibles y que

- asignan por demanda) a la MS para que pueda recibir una llamada, esto se realiza por medio del mensaje *ROUTEREQ*.
- b) Cuando el VLR y el MSC han asignado el número temporal, lo retornan al SCP usando el mensaje *routereq*. El SCP entonces ya puede responder al mensaje *LOCREQ* de la LE pasándole el número telefónico temporal asignado a la MS en la actual LA visitada.
 - c) La LE de la PSTN ahora inicia una conexión con el MSC que alberga a la MS utilizando el mensaje ISUP *IAM*. Al momento de recibir este mensaje, el MSC inicia un proceso de búsqueda (paging) en todas las celdas de su LA para localizar a la MS.
 - d) Cuando la MS responde al proceso de búsqueda, el MSC inicia un proceso de autenticación para verificar la validez del usuario. Este proceso se realiza de la manera anteriormente explicada.
 - e) Una vez que la autenticidad del usuario ha sido probada, la llamada es establecida.

III.10.4 Traspaso de llamada (hand off)

Hay 2 clases de traspaso de llamada, el primero es traspaso de llamada en un mismo MSC (Intra-MSC) y el segundo es traspaso de llamada de un MSC a otro (inter-MSC). El primero es invocado cuando una MS con una llamada en curso debido a su movimiento, cruza los límites de una celda, su objetivo es permitir a la MS el continuar con una llamada en curso aún en el caso que la MS cruce los límites de una celda. En este proceso la MS reajusta la frecuencia de radio en la que está transmitiendo/recibiendo, a la frecuencia a la cuál la nueva célula a la que ha entrado opera (las células adyacentes manejan diferentes frecuencias). En la Figura 22 se ilustra este proceso. Se supone una comunicación entre un usuario de la PSTN y una MS con una trayectoria de comunicaciones definida por el camino $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow \text{BS-1} \Rightarrow \text{MS}$, que debido al movimiento de la MS debe ser reemplazada por la trayectoria $1 \Rightarrow 2 \Rightarrow 4 \Rightarrow \text{BS-2} \Rightarrow \text{MS}$. Este tipo de traspaso de llamada no contribuye al tráfico de la red de señalización debido a que todo este proceso puede ser manejado localmente por el MSC de esa LA. Por ello, para los objetivos de este trabajo, éste tipo de traspaso de llamada no es importante.

El traspaso de llamada Inter-MS, ocurre cuando una MS con una llamada en curso atraviesa los límites de una LA. Debido a que la MS está pasando más allá del alcance del MSC que actualmente está dando servicio a la llamada en curso, es necesario invocar un cambio de MSC a fin de lograr dar continuidad a la llamada aún en éste caso que la MS ha entrado a los dominios de un nuevo MSC.

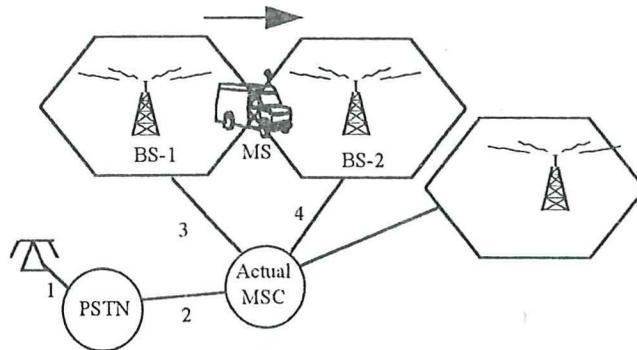


Figura 22. Traspaso de llamada entre celdas de un mismo MSC

La Figura 23 ilustra el proceso de Intrer-MS Hand off. Se supone nuevamente una comunicación existente entre un usuario de la PSTN y una MS, a través del enlace de comunicaciones definido por $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow \text{BS-1} \Rightarrow \text{MS}$, mismo que debido a que la MS está cruzando los dominios del actual MSC que la sirve, debe ser reemplazado por la ruta $1 \Rightarrow 2 \Rightarrow \text{truncal} \Rightarrow 4 \Rightarrow \text{BS-2} \Rightarrow \text{MS}$. El flujo de mensajes necesario para realizar el reemplazo de ruta es como sigue.

- El MSC actual envía un mensaje *HANDOFF MEASUREMENT REQ* al MSC destino.
- Cuando el MSC destino recibe el mensaje, éste selecciona una BS candidata para realizar el traspaso de llamada y se lo hace saber al MSC actual por medio del mensaje *handoff measurement req*.
- El MSC actual solicita a MSC destino la provisión de un canal de voz en la BS candidata por medio del mensaje *FACILITIES DIRECTIVE*. Si el MSC destino puede asignar el canal solicitado entonces responde con *facilities directive* al MSC actual.

- d) Cuando el MSC actual recibe el mensaje *facilities directive*, éste ordena a la MS el realizar el handoff.
- e) Cuando el MSC actual recibe el mensaje *MOBILE ON CHANNEL*, entonces establece una troncal hacia MSC destino y termina la transacción.

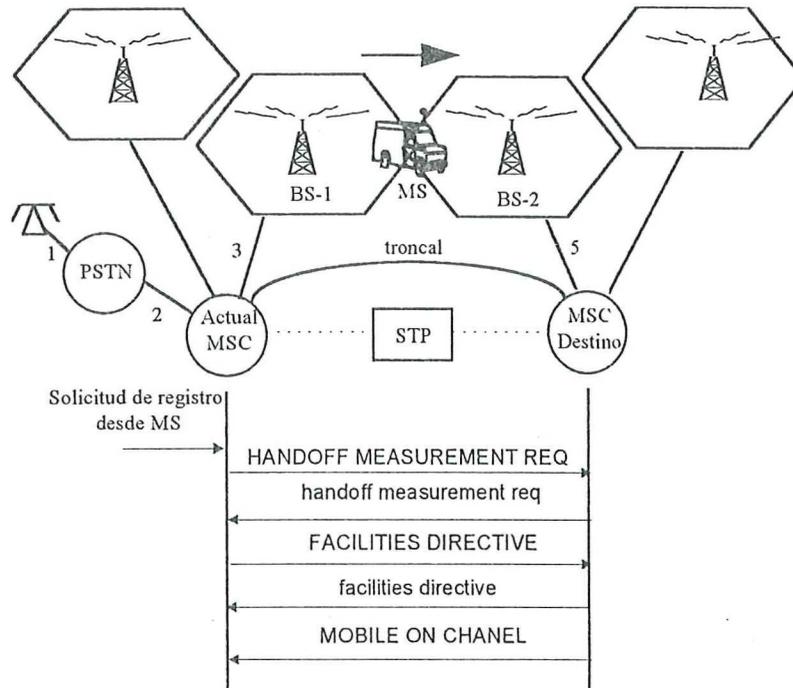


Figura 23. Traspaso de llamadas entre celdas de diferente MSC

III.10.5 Servicios extendidos

Consideraremos en este trabajo sólo dos de los posibles servicios extendidos [Black Uyles, 1996; Garg Vijay y Joseph Wilkes, 1996.] que se pueden concebir con una red como la de la Figura 17.

El primer servicio es Redireccionamiento Incondicional de Llamadas (CFI: Call Forwarding Incondicional) que le permite a un usuario de la red el recibir sus llamadas no en su MS, sino en un número telefónico (por él predeterminado) de la PSTN. Cuando un LE de la PSTN detecta una llamada destinada para una MS, éste consulta al HLR para conocer la LA en donde la MS se encuentra actualmente. Sin embargo el HLR detecta que el usuario tiene habilitado el servicio CFI, por tanto no regresa al LE la identidad de la LA en la que la MS está, sino que le regresa el número telefónico de la PSTN en donde el usuario ha

decidido recibir sus llamadas. Una vez que la LE recibe el número, esta puede establecer la conexión deseada.

El flujo de mensajes para CFI es presentado en la Figura 24 y se resume como sigue:

- a) El LE (origen) origina un mensaje *LOCREQ* para solicitar al HLR le proporcione la actual LA en donde el usuario en cuestión se encuentra.
- b) EL HLR detecta que el usuario tiene habilitado el servicio de redireccionamiento incondicional de llamadas, y entonces devuelve el LE el número telefónico de la PSTN al cuál el usuario ha decidido redireccionar sus llamadas, utilizando el mensaje *locreq*.
- c) Una vez que el LE origen recibe el número telefónico, éste puede establecer una llamada con otro LE (destino) de la forma usual utilizando mensajes ISUP.

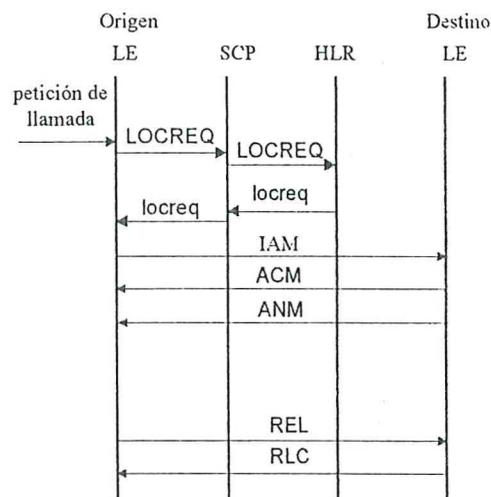


Figura 24. Flujo de mensajes para redireccionamiento incondicional de llamadas

El segundo servicio considerado es Redireccionamiento de Llamadas cuando el usuario no Contesta (CFNA: Call Forwarding Under not Answer). Este servicio es muy similar al de entrega de llamadas a usuario móvil, pero en éste caso, cuando el MSC realiza el proceso de búsqueda de la MS en las celdas que conforman la LA en busca de la MS para entregarle la llamada entrante, por alguna razón la MS no responde al proceso de búsqueda. Si el MSC nota que el usuario tiene activado el servicio CFNA, entonces pide al HLR que le proporcione el número telefónico en la PSTN a donde el usuario ha decidido redireccionar

sus llamadas bajo ésta condición. Cuando el MSC obtiene el número telefónico, puede establecer una llamada con el LE asociado a ese número. El flujo de mensajes es como se ilustra en la Figura 25 y se resume a continuación.

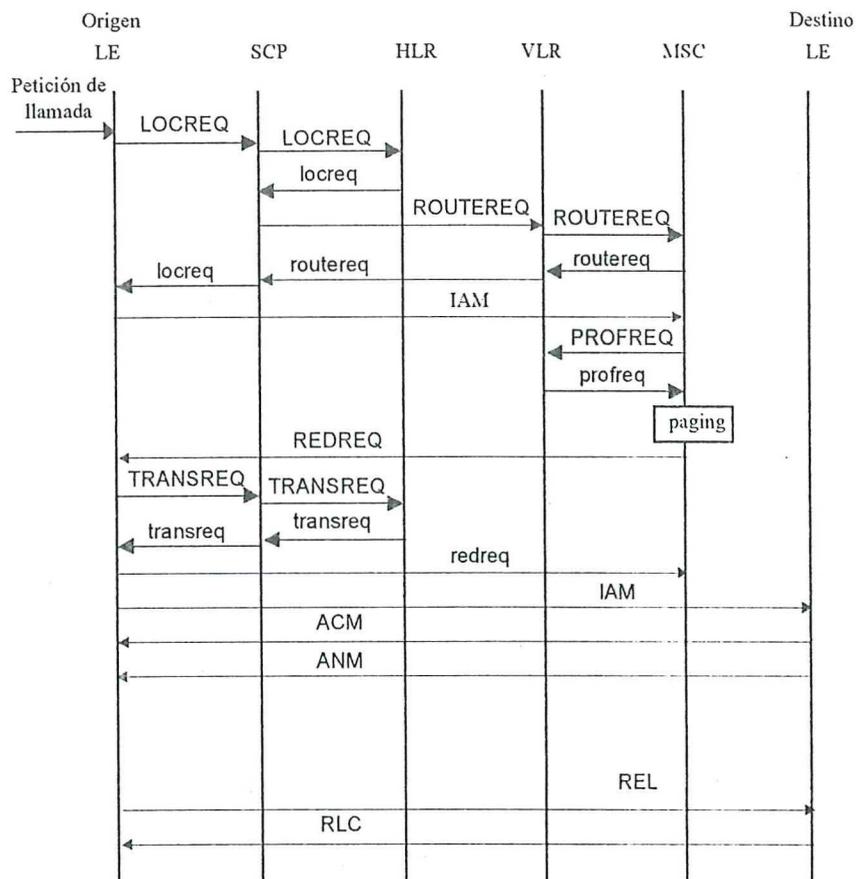


Figura 25. Redireccionamiento de llamadas cuando la MS no contesta

- El proceso es igual que el de entrega de llamadas hasta el proceso de búsqueda (*paging*).
- EL MSC destino nota que la MS no respondió al proceso de búsqueda, pero también nota que el usuario está suscrito al servicio de redireccionamiento de llamadas cuando el usuario no contesta. El MSC destino entonces envía al LE origen un mensaje *REDREQ* indicándole que debe redireccionar la llamada.
- El LE origen solicita al HLR el número en la PSTN al cuál el usuario ha decidido redireccionar sus llamadas bajo esta condición. Esto lo hace por medio del mensaje *TRANSREQ*.

- d) Cuando el LE origen obtiene el número desde el HLR, responde al MSC el mensaje previo *REDREQ* mediante un mensaje *redreq* y también comienza el establecimiento de una llamada con la LE que corresponde con el número predefinido por el usuario.

III.11 Procedimientos del IS-41 con compartición del SSD

Cuando el SSD se comparte con el sistema visitado, el registro de las MSs requiere pasos adicionales comparado con el caso en que el SSD no se comparte. Esto se debe a que el VLR del sistema previo tiene el valor previo del contador COUNT, y por eso la base de datos AUT necesita solicitar el contador al VLR anteriormente visitado. Una vez que la MS ha sido registrada en el nuevo VLR, para todos los accesos al sistema tales como llamadas originadas por usuario móvil, entrega de llamadas a usuario móvil, etc., el VLR puede autenticar a la MS sin tener que enviar la solicitud de autenticación hasta la base de datos AUT. Esto resulta en ahorros substanciales, especialmente cuando la MS se mueve poco comparada con el número de llamadas que hace o recibe.

El flujo de mensajes varía de aquellos presentados en el caso de no compartición del SSD para los procesos de registro de terminales, llamadas originadas por usuario móvil, y entrega de llamadas a usuario móvil. El flujo de mensajes para Hand off y los dos servicios extendidos incluidos es el mismo, esto se debe a que éstos procedimientos no involucran en su estructura mensajes de autenticación.

III.11.1 Registro de terminales

La Figura 26 ilustra el flujo de mensajes durante el proceso de registro cuando el SSD es compartido con el VLR visitado. El flujo de mensajes se explica como sigue.

- a) El flujo de mensajes inicial es similar a aquel explicado para el proceso de registro cuando el SSD no es compartido incluyendo hasta el paso d).
- b) En este caso, la base de datos AUT solicita por medio del SCP al VLR del sistema anterior (anterior área de localización) el valor del contador COUNT por medio del mensaje *COUNTREQ*.

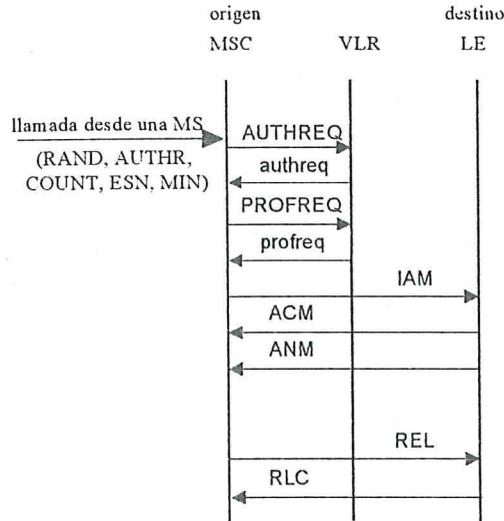


Figura 27. Origen de llamadas

III.11.3 Entrega de llamadas a usuario móvil

La Figura 28 ilustra el flujo de mensajes para el caso de entrega de llamada a usuario móvil. El flujo de mensajes es en casi idéntico que en el caso de entrega de llamadas cuando el SSD no se comparte. Pero en este caso, la autenticación de la MS se realiza en el VLR del sistema visitado sin necesidad de requerir de la intervención de la base de datos AUT.

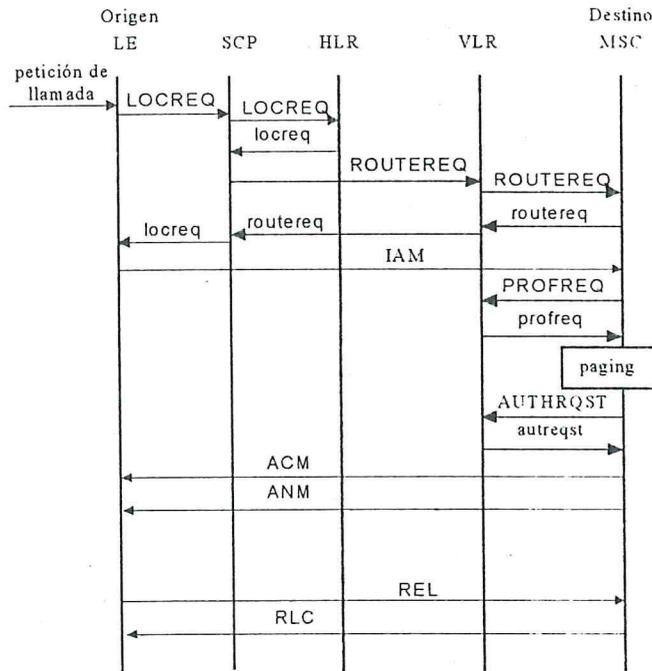


Figura 28. Entrega de llamada

IV. MODELADO DE UNA RED PCS BASADA EN IS-41

En la Figura 29 se representa la red escogida para efectos de la evaluación de su desempeño. Esta red es muy similar a la mostrada en la Figura 17. En esta figura ya se ha omitido a las MSs y BSs ya que sólo estamos interesados en la señalización dentro de la red. Se han incluido en la red cuatro MSCs y sus bases de datos VLR asociadas. Hay dos LEs para representar la interconectividad de la red PCS con la PSTN. Hay una oficina de tránsito (TE), un par de STPs y un SCP con sus respectivas bases de datos HLR y AUT.

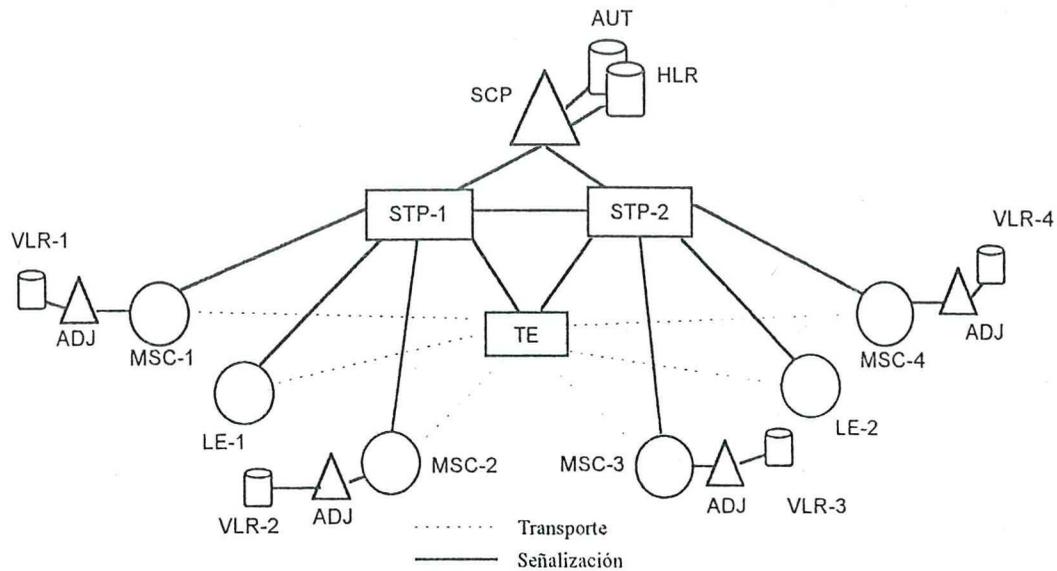


Figura 29. La red de referencia

IV.1 Funcionalidad de SS7 requerida en los diversos elementos de la red

La Figura 30 presenta la funcionalidad del SS7 incluida en los diversos elementos de la red PCS. El STP en su papel de enrutador de paquetes implementa solamente las capas inferiores de SS7 que equivalen a los tres primeros niveles del modelo OSI. La TE requiere ISUP para implementar funciones de control de llamada (por ejemplo establecimiento y liberación de conexiones entre LEs y MSCs). La LE y el MSC requieren de TCAP e ISUP ya que ambos implementan IS-41 y operaciones relacionadas al control de llamada (ver por ejemplo los diagramas IS-41 de la Figura 19 a la Figura 28). El SCP y el Adjunto solamente implementan TCAP ya que ellos no se involucran en operaciones relacionadas al control de llamada.

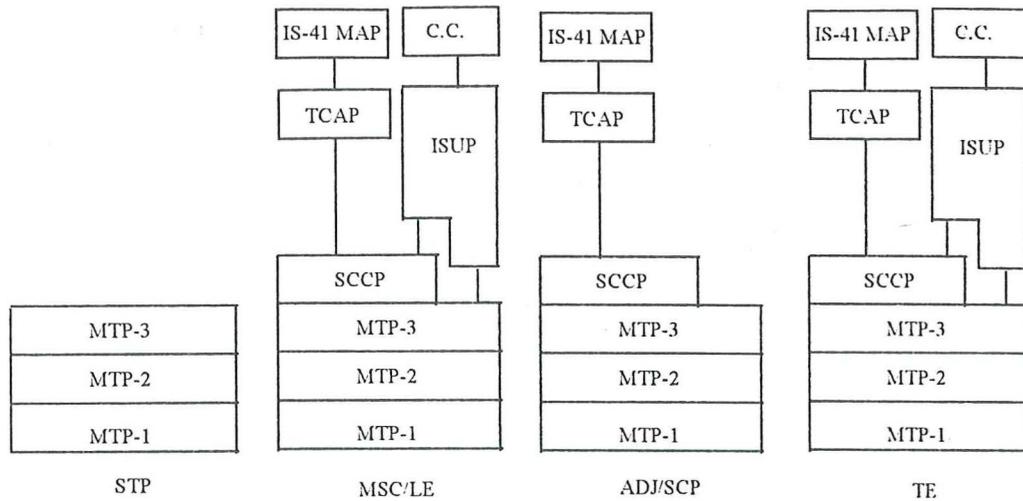


Figura 30. Funcionalidad SS7 en los nodos de la red

IV.2 Modelado de las diferentes capas de la SS7

Se han desarrollado modelos de colas para cada una de las diferentes capas de la SS7 a partir de los bloques funcionales que fueron presentados en las figuras 4, 5, 7, 10, y 12.

Se ha decidido no incluir en los modelos las funciones para el manejo y la administración de la red (tales como funciones de reconfiguración en caso de fallas, funciones para restablecer enlaces o nodos, etc.) como una medida para prevenir que el modelo sea extremadamente complejo. Se considera por conveniencia y sin perder generalidad [Willmann Gert y Paul Kühn, 1990; Bafutto Marcos, *et al*, 1994], que existe un procesador asignado a cada capa de la SS7 encargado de realizar la funcionalidad identificada en cada capa, la Tabla II resume dichas funciones.

De igual manera, la funcionalidad considerada para SCCP no incluye a las funciones de control orientadas a conexión, esto debido a que como ha sido establecido en la sección II.8, en los PCS sólo se utilizan las funciones orientadas a no conexión. Los modelos de colas para cada una de las capas de la SS7 son mostrados en las figuras 31-35. Las colas de cualesquiera de las capas tienen asignada prioridad. Lo que significa que el procesador de la capa dará preferencia a ciertas colas sobre otras. Se ha supuesto que el tiempo de servicio para cada una de las colas de una capa es fijo; esto es razonable ya que para una cola determinada, el procesador realiza exactamente el mismo procesamiento (la misma función).

Tabla II. Funcionalidad en las diversas capas de la SS7

Capa SS7	Proceso	Descripción	Abreviación
TCAP	1	Subcapa de Manejo del Diálogo de Componentes	SMDC
	2	Subcapa Coordinadora de Componentes	SCC
	3	Subcapa de Transacción	ST
ISUP	1	Control para Procesamiento de Llamadas de Llegada	CPLL
	2	Control para Procesamiento de Llamadas de Salida	CPLS
	3	Control de Distribución de Mensajes	CDM
	4	Control de Envío de Mensajes	CEM
SCCP	1	Control Orientado a no Conexión para Recepción	CONCR
	2	Control Orientado a no Conexión para Transmisión	CONCT
	3	Control de Enrutamiento en Recepción	CER
	4	Control de Enrutamiento en Transmisión	CET
MTP-3	1	Discriminación de Mensajes	DISCM
	2	Distribución de Mensajes	DISTM
	3	Enrutamiento de Mensajes	EM
MTP-2	1	Control de Recepción	CR
	2	Control de Transmisión	CT
	3	Delimitación, Alineamiento y Detección de Error en la Recepción	DADER
	4	Delimitación, Alineamiento y Detección de Error en la Transmisión	DADET
MTP-1	-	-	-

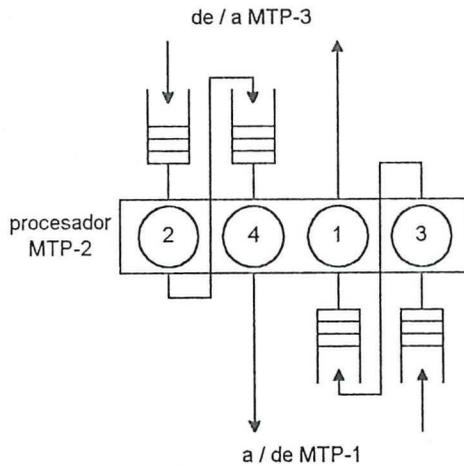


Figura 31. Modelo de colas para la MTP-2

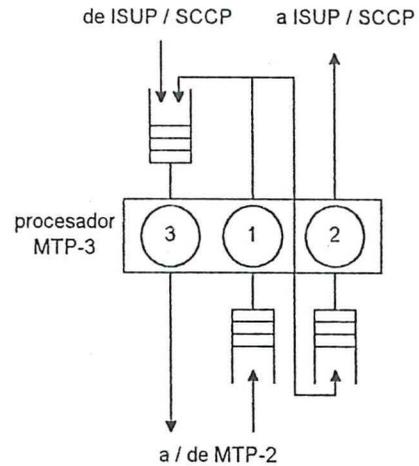


Figura 32. Modelo de colas para la MTP-3

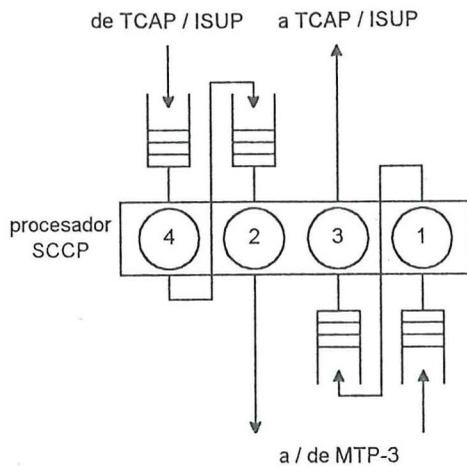


Figura 33. Modelo de colas para la SCCP

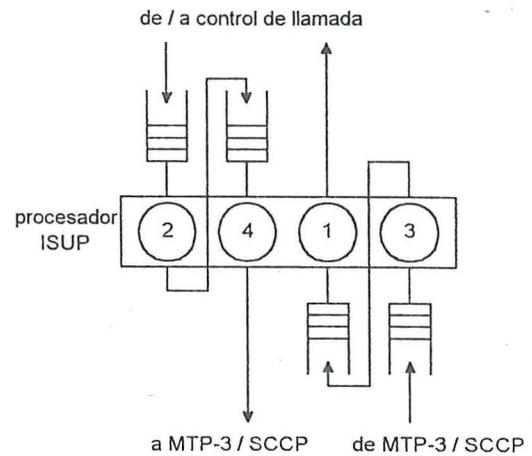


Figura 34. Modelo de colas para la ISUP

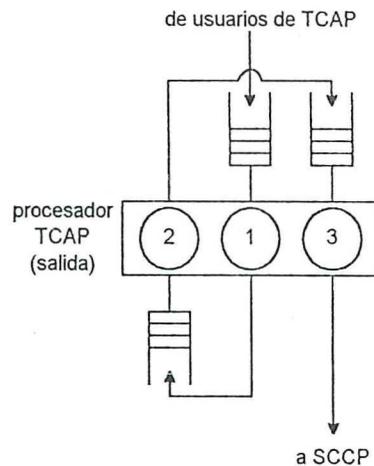
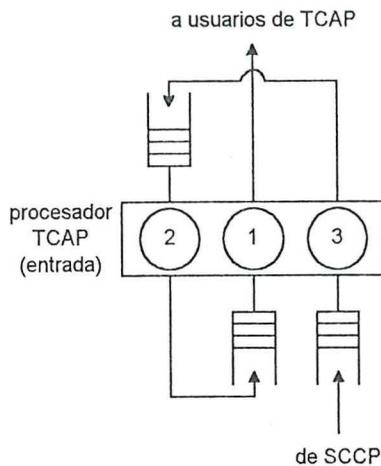


Figura 35. Modelo de colas para la TCAP

La prioridad establecida en cada una de las colas, hace que un mensaje que ingresa a cualquiera de las capas, permanezca en la capa (antes de ser enviado a otra capa) durante un tiempo aleatorio. El modelar éstas colas por simulación es más atractivo que analíticamente. La razón es que éstas son colas de prioridad y con retroalimentación; es decir, en ocasiones, una vez que un mensaje ha recibido servicio por parte del procesador de una capa, el mensaje vuelve a formarse en otra fila para recibir de nuevo servicio por el mismo procesador. En

situaciones como ésta, son muchas las simplificaciones que deben hacerse durante el modelado analítico a fin de obtener una expresión matemática manejable.

La prioridad y el tiempo de procesamiento para cada una de las colas en las diferentes capas se ha resumido en la Tabla III. Ha sido mostrado por [Bafutto Marcos, *et al*, 1996] que cuando la prioridad en las colas es como se indica en la Tabla III, se obtiene el mejor rendimiento de la red de señalización. Adicionalmente los autores proponen valores para el tiempo de procesamiento para los mensajes en cada una de las colas de una capa, éstos valores han sido tomados en cuenta para la proposición de valores para este trabajo, salvo que se ha incluido un orden de magnitud mayor en la capacidad de procesamiento debido a que se ha considerado que desde que se editó ese artículo a la fecha, al menos la capacidad de procesamiento de los microprocesadores se ha incrementado diez veces.

Tabla III. Tiempo de procesamiento y prioridad para las colas de las capas de la SS7

Capa SS7	Proceso	Abreviación	Prioridad	Tiempo de Procesamiento (ms)
TCAP	1	SMDC	2	0.2
	2	SCC	3	0.2
	3	ST	1	0.1
ISUP	1	CPL-L	3	0.2
	2	CPL-S	2	0.2
	3	CDM	4	0.05
	4	CEM	1	0.05
SCCP	1	CONC-R	3	0.1
	2	CONC-T	2	0.1
	3	CE-R	1	0.1
	4	CE-T	4	0.1
MTP-3	1	DISCM	1	0.05
	2	DISTM	2	0.05
	3	EM	3	0.05
MTP-2	1	C-R	4	0.05
	2	C-T	3	0.05
	3	DADE-R	2	0.05
	4	DADE-T	1	0.05

Otros tiempos de procesamiento considerados en el modelo se muestran en la Tabla IV y se resumen en seguida. Los principales parámetros que caracterizan a una base de datos son el número de transacciones por segundo (accesos ya sea para escritura o para lectura de información) que soporta y su capacidad de almacenamiento. Hemos supuesto que las bases de datos HLR, AUT y VLR soportan el mismo número de transacciones por segundo. En general el tiempo para lectura en las bases de datos, es mayor que aquel que se requiere para

su escritura. En este trabajo se ha asumido que el tiempo de procesamiento para la lectura de la base de datos se distribuye exponencialmente y con media 0.00434 segundos, mientras que el tiempo de escritura también se distribuye exponencialmente y con media 0.00582 segundos. Operaciones de lectura en las bases de datos son por ejemplo la solicitud del archivo de usuario (PROFREQ), solicitud de ruta (ROUTEREQ). etc. Ejemplos de operaciones de escritura en las bases de datos son la notificación de registro (REGNOT), cancelación de registro (REGCANC), etc. Si se asume que ambas operaciones son invocadas con la misma probabilidad entonces en promedio cada base de datos soporta 200 transacciones por segundo, cifra que corresponde a los actuales valores soportados por las bases de datos de los sistemas disponibles en el mercado.

Tabla IV. Otros tiempos de procesamiento considerados

Tiempo de Procesamiento en las Bases de Datos (HLR, AUTH y VLR)	
Tiempo de lectura	Distribuido exponencialmente con media 0.00434 (seg.)
Tiempo de escritura	Distribuido exponencialmente con media 0.00582 (seg.)
Tiempo del Proceso de Búsqueda (Paging)	
Cuando la MS responde	Distribuido exponencialmente con media 0.005 (seg.)
Cuando la MS no responde	Distribuido exponencialmente con media 0.010 (seg.)
Tiempo de Conexión	
Tiempo para expedir el mensaje ACM cuando se recibe IAM	Distribuido exponencialmente con media 0.001 (seg.)
Tiempo de Desconexión	
Tiempo para expedir el mensaje RLC cuando se recibe REL	Distribuido exponencialmente con media 0.001 (seg.)

Se ha asumido que el tiempo que se requiere para realizar el proceso de búsqueda de la MS en las celdas que forman la LA durante la entrega de llamada se distribuye exponencialmente con media 5 milisegundos. En el caso que la MS no responde al proceso de búsqueda, la red requiere en promedio de 10 milisegundos distribuidos exponencialmente antes de efectuar un redireccionamiento de llamada.

El tiempo de establecimiento de la conexión representa el tiempo necesario que le toma a un nodo de la red (TEs, MSCs ó LEs) para establecer un circuito sobre la red de transporte una vez que éste ha recibido un mensaje ISUP IAM; se ha asumido que este tiempo sigue una distribución exponencial con una media de 1 milisegundo. De manera similar se ha considerado que el tiempo que toma a un nodo de la red (TEs, MSCs ó LEs) para liberar un

circuito una vez que ha recibido un mensaje ISUP REL se distribuye de manera exponencial con una media de 1 milisegundo.

IV.3 Implementación del modelo

La red de la Figura 29 fue implementada utilizando OPNET. Los diferentes elementos de la SS7 fueron modelados como se mostró en las figuras 32-35, con la funcionalidad, prioridades y tiempos de procesamiento mostrados en la Tabla II-IV. Las bases de datos HLR, AUT y VLR fueron modeladas como colas M/M/1 con tiempos de procesamiento dados por la Tabla IV. El flujo de mensajes IS-41 y los mecanismos para el control de llamada (establecimiento y liberación de llamada) fueron implementados como usuarios de TCAP e ISUP respectivamente. Fué necesario construir las tres de alternativas para IS-41 en modelos separados. Uno correspondiendo al caso donde no hay mecanismos de privacidad y autenticidad⁴ en la red, otro en donde se usa compartición de SSD como alternativa para implementar la seguridad en la red y el otro en donde el SSD no se comparte. Los tres modelos utilizan la misma estructura física de red y la funcionalidad incluida en los nodos de la red es la misma en los tres casos. La diferencia entre los modelos es la versión de IS-41 (usuario de TCAP) que cada uno de ellos implementa.

El lenguaje de simulación orientado a comunicaciones OPNET fue utilizado en este trabajo, debido en parte a su inmediata disponibilidad, y por otra parte debido a que éste representa una de las mejores y más completas herramientas para la evaluación del desempeño de redes de comunicaciones. Como anexo a este trabajo presentamos un resumen de las características más sobresalientes de OPNET.

IV.4 Simplificaciones y limitaciones

En todas las colas del modelo (las colas de cada una de las capas y colas que modelan a las bases de datos) se especificó una capacidad de almacenamiento infinita. De haber considerado colas con una capacidad de almacenamiento limitado, se hubieran producido

⁴ En el caso en donde no hay mecanismos de privacidad y autenticación en la red. el flujo de mensajes es casi idéntico a cualquiera de los 2 mecanismos de autenticación, sólo que en éste caso no se requieren los mensajes AUTHRQST y authreqst durante los procesos de registro, origen y entrega de llamada.

pérdidas de mensajes de señalización cuando la capacidad de alguno de los elementos llegara a excederse; para evitar estas pérdidas, se requiere implementar mecanismos de control de flujo y congestión para controlar la admisión de llamadas en la red [Bedoy Jesús, 1997] para asegurar cierta calidad de servicio a los usuarios. Otro par de simplificaciones importantes que se han hecho en los modelos desarrollados son las siguientes.

La primera de ellas es que no se ha modelado el protocolo de MTP-2, esto es, no se implementó el mecanismo de control de flujo y error de SS7. Hay dos razones importantes para no hacerlo: La primera es que el tiempo necesario para correr una simulación no sería en absoluto trivial debido a las limitantes en los equipos de cómputo y programas de simulación actuales, por ejemplo en [Unger Brian *et al.* 1994] para modelar en detalle a la SS7 requirieron de 200 MB de memoria y 52 horas de simulación en una computadora SUN SPARC 20. En [Gomes Fabian, 1993] se considera el uso de un simulador paralelo (que requiere de una computadora con procesadores múltiples) para acelerar el tiempo de ejecución de un programa de simulación que modela la SS7 en detalle. La segunda razón es que estos mecanismos han sido ya estudiados y modelados en detalle en [Ramaswami V. y Jonathan Wang, 1993; Hou Victor *et al.*, 1994] con anterioridad.

La segunda consideración es que se ha supuesto que la capacidad de los enlaces de comunicación (capa MTP-1) es ilimitada. Esto es, se ha considerado que los enlaces que conectan entre sí a dos elementos adyacentes de la red, son capaces de transportar cualquier cantidad de mensajes de señalización. Esta consideración así mismo puede justificarse por medio de 2 argumentos. El primero es que en las redes SS7 se recomienda que la utilización de los enlaces sea a lo mucho de un 40% [Stallings William, 1995] de su capacidad (debido a los requerimientos de disponibilidad los enlaces se proyectan para soportar el transporte de información cuando algún enlace llegara a fallar). La segunda justificación se debe al hecho que es posible agrupar hasta 36 enlaces de 64 kbps entre dos elementos de la red SS7. Al considerar una capacidad ilimitada en los enlaces de señalización estamos suponiendo que los diseñadores de la red no escatimarán en este recurso. En [Kathleen S. Meier-Hellstern, *et al.*, 1992] se ofrece una serie de cálculos para determinar la capacidad necesaria de los enlaces

entre dos nodos de la SS7 al soportar PCS. Al considerar una capacidad ilimitada en los enlaces de señalización, se consigue que el tamaño de los mensajes de señalización (TCAP ó ISUP) no sea de importancia en el modelo.

V. DISEÑO DE LAS CORRIDAS Y PRESENTACION DE RESULTADOS

V.1 Comentarios

Los siguientes comentarios son extensivos para todas las simulaciones realizadas en este trabajo. No se corrieron simulaciones al variar el tráfico debido a redireccionamiento de llamadas en sus dos modalidades ya que estos servicios no son muy utilizados en la actualidad. En todos los casos considerados, los procesos tienen como destino un nodo escogido aleatoriamente por medio de una distribución uniforme. Por ejemplo, en el proceso de registro de terminales la antigua LA es escogida aleatoriamente; similarmente en el proceso de llamada originada, el LE destino es seleccionado mediante una distribución aleatoria uniforme, etc. Se ha considerado que el tiempo entre llegadas para cada uno de los diferentes procesos sigue una distribución exponencial. Como es bien sabido la distribución exponencial es ampliamente utilizada para modelar tráfico telefónico.

En todas las figuras se presenta un intervalo de confianza del 95%, éste fue obtenido corriendo cinco réplicas de la simulación (utilizando semillas diferentes en cada una). Por ejemplo, para obtener tan sólo la curva dibujada con línea sólida de la Figura 36 se precisó correr 5 veces la simulación para cada uno de los 6 puntos que conforman la curva (5 de los puntos se aprecian en la gráfica, el sexto ya no). Haciendo esto que para la obtención de cada una de las gráficas se requieran unas 15 horas de tiempo de simulación. Todas las figuras en donde el retardo extremo-extremo es la variable dependiente, se caracterizan por retardos intolerables (teóricamente infinitos) una vez que la capacidad de alguno de los elementos de la red ha sido rebasada. Por razones de espacio, en las diversas gráficas se muestran las siguientes abreviaciones cuyo significado es:

- *no autenticación*: no utilización de mecanismos de seguridad como parte de IS-41
- *compartición*: compartición del SSD como mecanismo de seguridad en IS-41
- *no compartición*: no compartición del SSD como mecanismo de seguridad en IS-41

La metodología seguida en este trabajo para determinar al recurso limitante de la red en cada caso, fue la siguiente. Primero se inspeccionaron cada uno de los diagramas de señalización (figuras 19-28), identificando en cada caso al elemento (típicamente a la base de

datos, debido a su alto tiempo de procesamiento) más utilizado, ese tendría que ser el recurso limitante. Esta aseveración, fue confirmada al recabar estadísticas durante las simulaciones para los diferentes elementos de la red.

V.2 Comparación entre un sistema con y sin mecanismos de seguridad

A fin de conocer el desempeño de la red cuando se hace uso y no de mecanismos de seguridad, se probaron dos situaciones diferentes a saber: La situación a) que se caracteriza por la existencia de usuarios que presentan alta movilidad, pero que ofrecen una reducida tasa de llamadas, caso típico cuando los usuarios viajan en autos. En la situación b), los usuarios presentan una baja movilidad y una mayor tasa de llamadas que en el caso anterior; esta situación es característica de usuarios pedestres.

La movilidad de los usuarios es directamente proporcional al número de procesos de traspaso de llamada y registro de terminales. Así mismo, la tasa de llamadas es directamente proporcional al número de procesos de llamadas originadas, entrega de llamadas y redireccionamiento de llamadas en sus dos modalidades. El tráfico considerado para cada una de las dos condiciones es mostrado en la Tabla V y la Tabla VI.

Tabla V. Tráfico debido a usuarios en vehículos

Proceso	Tráfico en MSCs	Tráfico en LEs
Registro	18 solicitudes/seg.	-
Origen de Llamadas	2 llamadas/seg.	-
Entrega de Llamadas	-	2 llamadas/seg.
Traspaso de Llamadas	6 solicitudes/seg.	-
Redireccionamiento Incondicional de Llamadas	-	1 llamada/seg.
Redireccionamiento de Llamadas Cuando el Usuario no Contesta	-	1 llamada/seg.

Tabla VI. Tráfico debido a usuarios pedestres

Proceso	Tráfico en MSCs	Tráfico en LEs
Registro	3 solicitudes/seg.	-
Origen de Llamadas	15 llamadas/seg.	-
Entrega de Llamadas	-	15 llamadas/seg.
Traspaso de Llamadas	1 solicitudes/seg.	-
Redireccionamiento Incondicional de Llamadas	-	2 llamadas/seg.
Redireccionamiento de Llamadas Cuando el Usuario no Contesta	-	2 llamadas/seg.

Primero se introdujo el tráfico mostrado en la Tabla V en los tres modelos de la red implementados (el modelo para el caso de no implementación de mecanismos de seguridad en la red, el modelo para el caso de compartición del SSD y el modelo para el caso de no compartición del SSD). Cuando se varió el tráfico en el MSC-1 debido al proceso de registro de terminales se obtuvieron las gráficas de la Figura 36 y la Figura 37. La Figura 36 muestra el tiempo de respuesta de la red al proceso de registro de terminales, se puede apreciar que en el caso donde no se implementan mecanismos de seguridad, se obtiene el menor tiempo de respuesta de la red. Adicionalmente, el caso en que no se implementan mecanismos de seguridad en la red, esta puede completar muchas más solicitudes de registro de terminales (que en los casos donde esta si se emplea) antes de que el retardo en la red se vuelva inaceptable. La Figura 37 muestra la utilización de la base de datos VLR-1 (base de datos asociada al MSC-1), quien en este caso constituye el recurso limitante para este proceso. Para el tráfico de registro de terminales en el cuál la utilización de la base de datos es mayor a 0.96, el tiempo de respuesta de la red se hace inaceptable. El tiempo de respuesta de la red es siempre menor cuando no se implementan mecanismos de seguridad que cuando si se hace. Esto se debe a que cuando no se implementa la seguridad, se requieren menos accesos a la base de datos VLR que en el caso en que esta si se implementa.

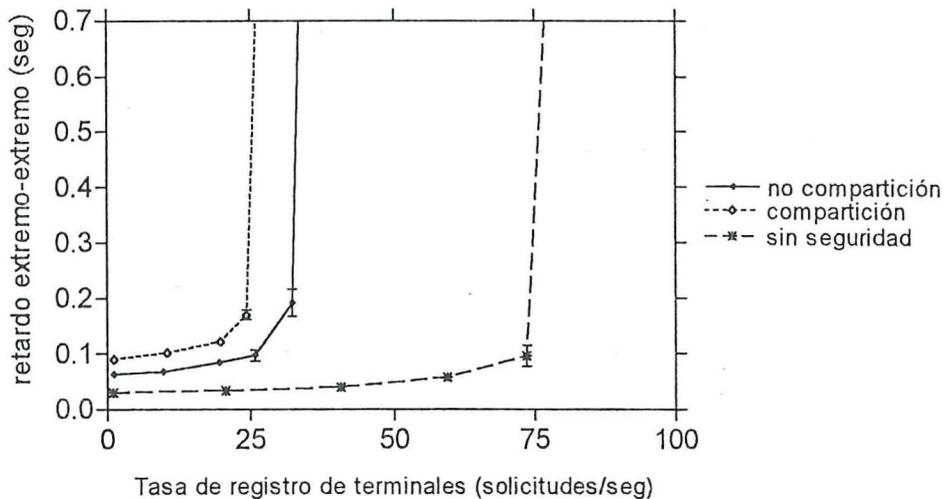


Figura 36. Retardo en la red durante el registro de terminales (usuarios en vehículos)

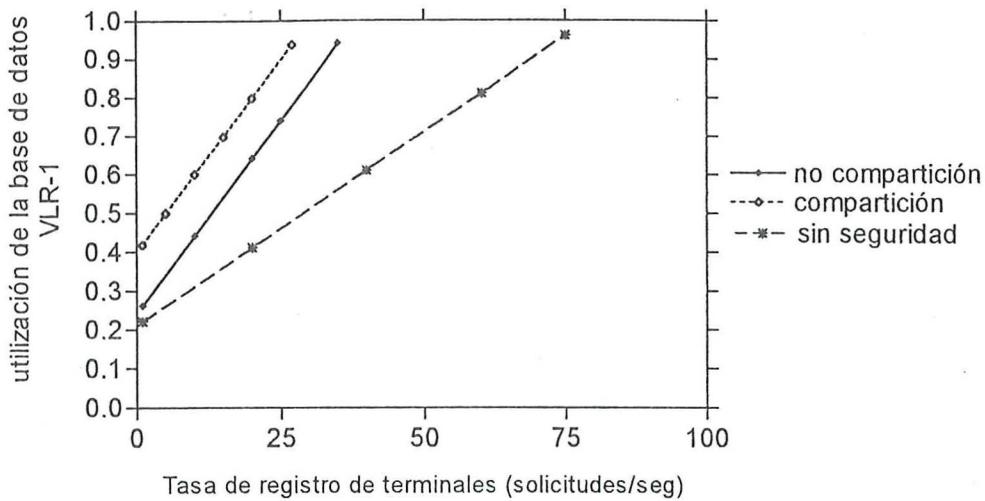


Figura 37. Utilización del elemento limitante (VLR-1) durante el registro de terminales (usuarios en vehículos)

Cuando se varió la tasa de llamadas originadas por usuarios móviles en MSC-1, se obtuvieron las gráficas de la Figura 38 y la Figura 39. La Figura 38 muestra el tiempo de respuesta de la red al proceso de origen de llamadas, la Figura 39 presenta la utilización de la base de datos VLR-1 quien de nuevo resultó ser el recurso que limita la capacidad de la red. La menor utilización de la base de datos VLR cuando no se implementan mecanismos de seguridad (respecto a cuando estos sí se utilizan), hace que el sistema soporte muchas más llamadas que cuando si se implementan estos mecanismos.

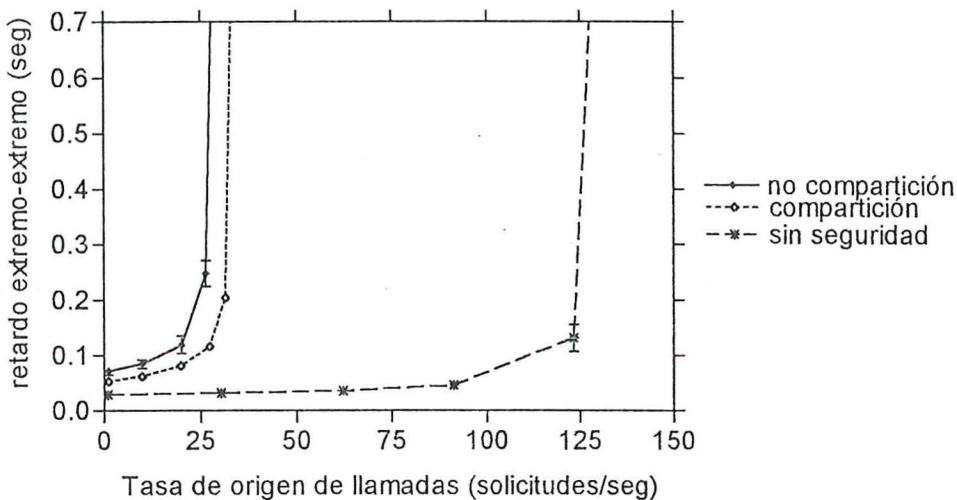


Figura 38. Retardo en la red durante el origen de llamadas (usuarios en vehículos)

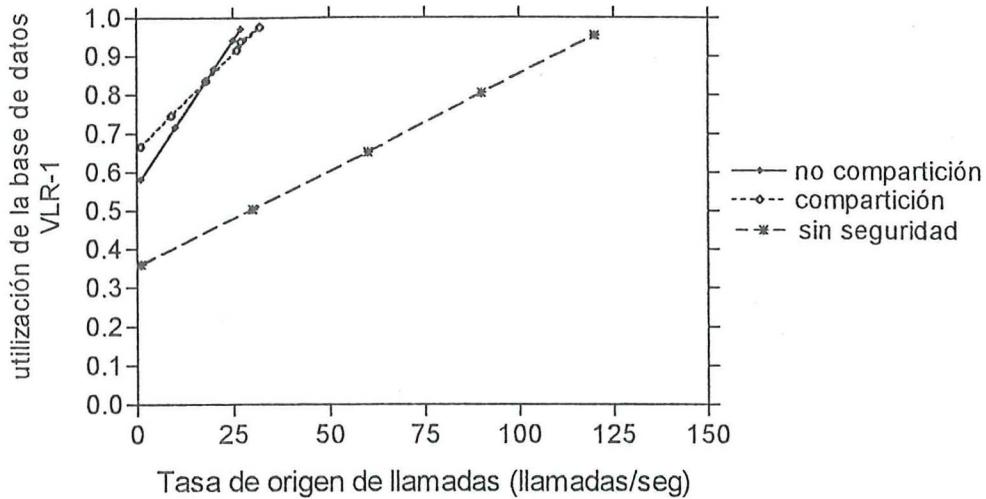


Figura 39 Utilización del elemento limitante (VLR-1) durante el origen de llamadas (usuarios en vehículos)

Cuando se varió el tráfico de entrega de llamadas a usuario móvil en el LE-1, se obtuvieron las gráficas de la Figura 40 y la Figura 41. La Figura 40 corresponde al tiempo de respuesta al proceso de entrega de llamada a usuario móvil. Nuevamente cuando las técnicas de seguridad no se implementan en la red, se logra obtener de la red el mayor número de entrega de llamadas a usuarios móviles que aquellos casos en que la seguridad si se implementa en la red. La Figura 41 ilustra la utilización de las bases de datos VLR-X, donde la "X" indica que todas las bases de datos (no solamente la VLR-1) son el recurso que limita la capacidad de la red. Esto se debe a que en este caso el destino considerado para la entrega de llamada es un destino aleatorio; al considerar un destino aleatorio uniformemente distribuido, el MSC escogido (y por consiguiente el VLR asociado a ese MSC) será aleatorio. Como al largo término, todos los MSCs (y en consecuencia todos los VLRs) recibirán el mismo número de solicitudes de entrega de llamadas, todos ellos serán la limitante del sistema.

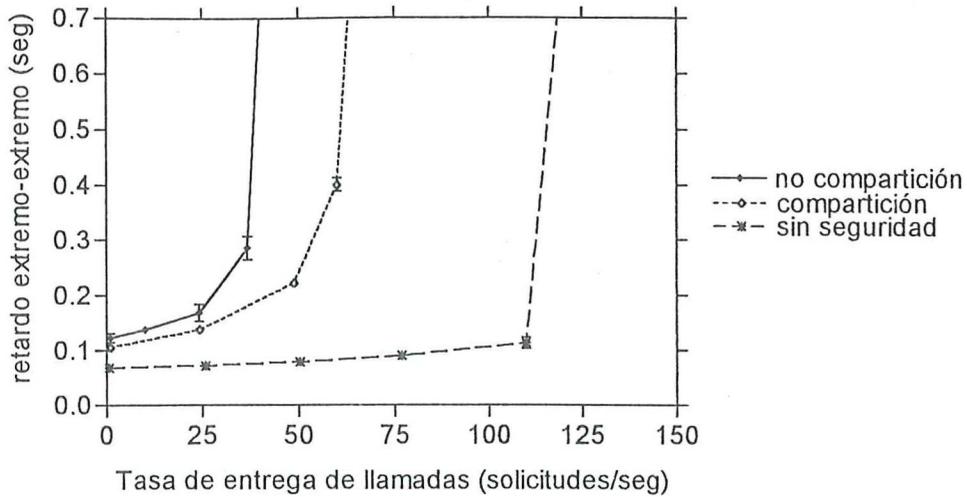


Figura 40. Retardo en la red durante la entrega de llamadas (usuarios en vehículos)

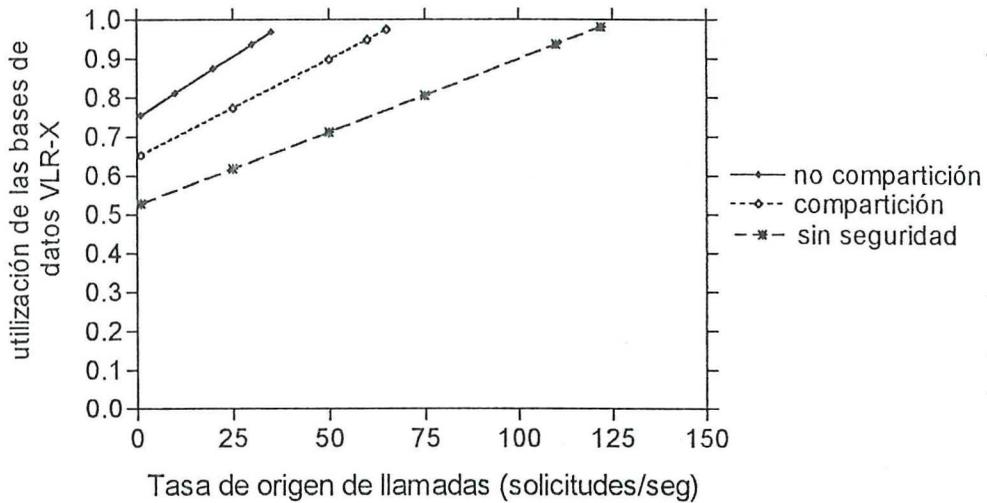


Figura 41. Utilización del elemento limitante (VLR-X) durante la entrega de llamadas (usuarios en vehículos)

Cuando se introdujo en la red el tráfico mostrado en la Tabla IV (tráfico tipo b), se obtuvieron las gráficas que se muestran en las figuras 42-47; en donde los comentarios hechos para las figuras 36-41 se aplican respectivamente.

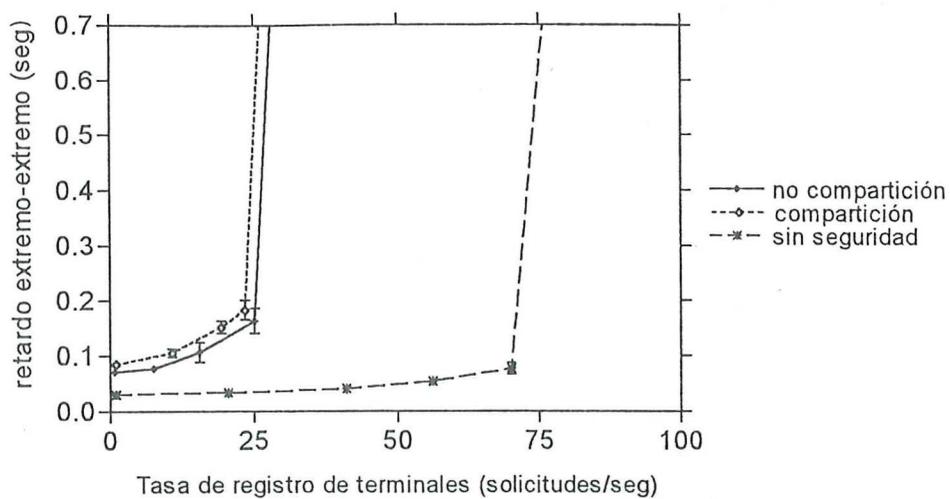


Figura 42. Retardo en la red durante el registro de terminales (usuarios pedestres)

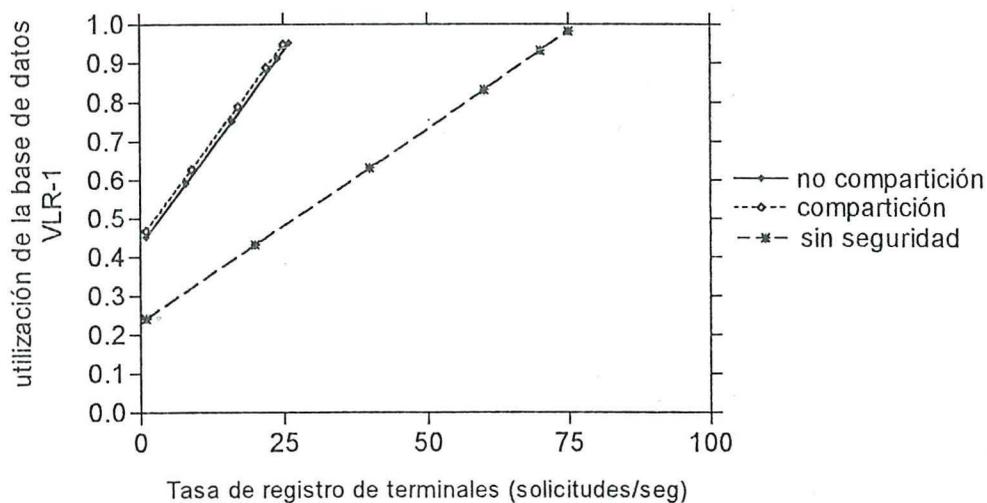


Figura 43. Utilización del elemento limitante (VLR-1) durante el registro de terminales (usuarios pedestres)

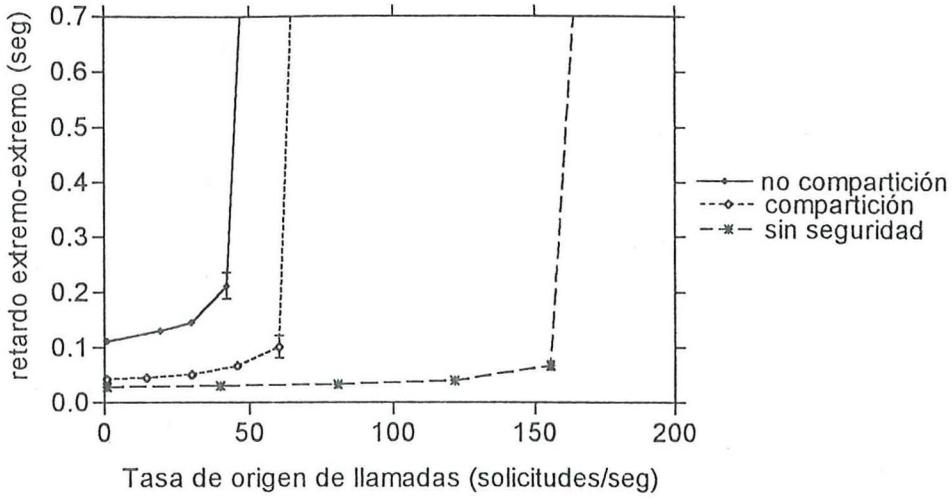


Figura 44. Retardo en la red durante el origen de llamadas (usuarios pedestres)

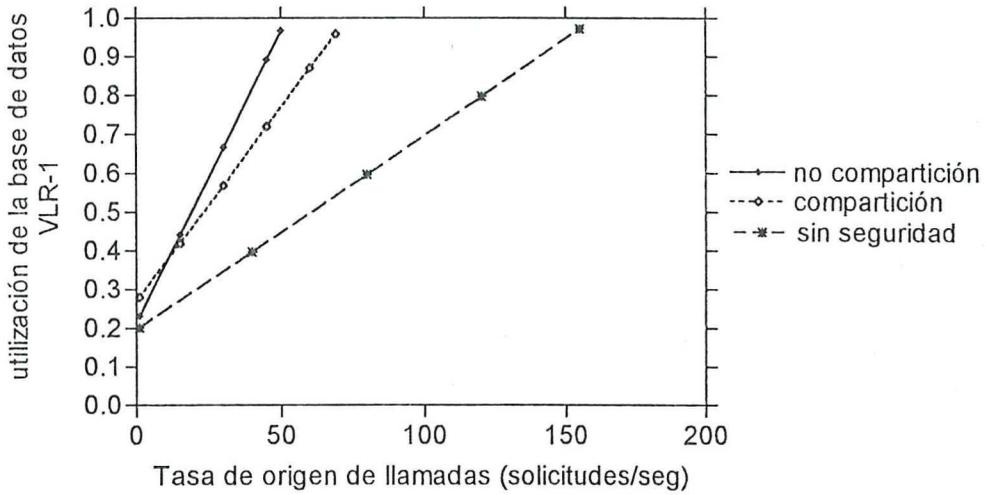


Figura 45. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas (usuarios pedestres)

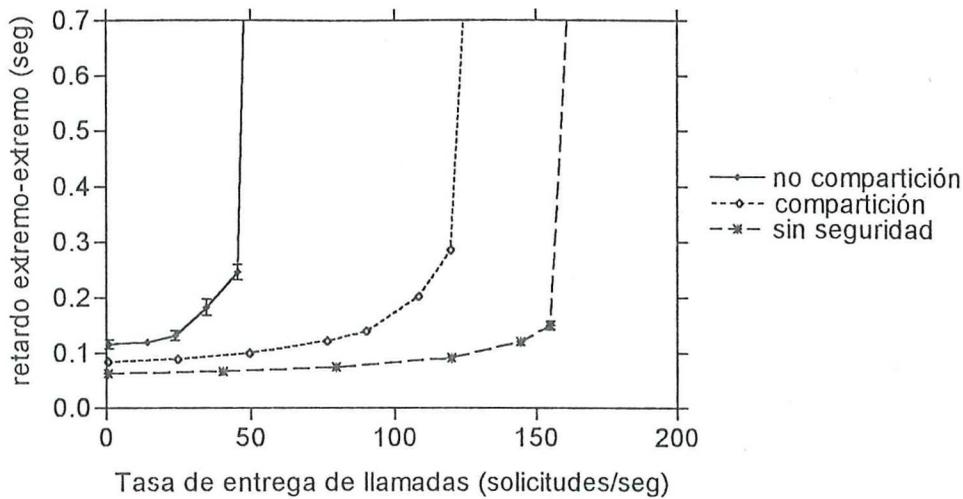


Figura 46. Retardo en la red durante la entrega de llamadas (usuarios pedestres)

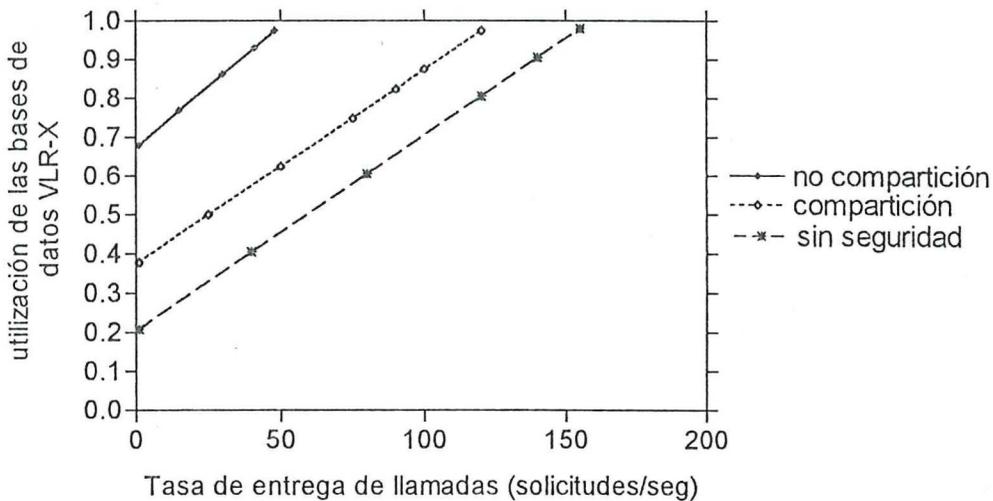


Figura 47. Utilización del elemento limitante (VLR-X) durante la entrega de llamadas (usuarios pedestres)

En la Tabla VII se resume el máximo número de procesos que soporta la red para el caso del tráfico debido a usuarios en vehículos. La Tabla VIII es la versión normalizada⁵ de la Tabla VII, en donde se compara para cada proceso que ocurre en la red, la ventaja de usar la seguridad o no. La información de la Tabla VIII toma sentido cuando se lee horizontalmente.

⁵ Estas versiones normalizadas resultan muy convenientes para propósitos de comparar la efectividad de los métodos. Estas se obtienen al considerar como la unidad al valor más grande ya sea a veces a nivel renglón o a nivel columna de una tabla (según se especifique) los demás porcentajes se obtienen al dividir la cantidad de la celda correspondiente en la tabla original entre ese valor más grande.

Por ejemplo, considérese el caso del proceso de registro de terminales. Cuando no se utilizan técnicas de seguridad en la PCS, se obtiene la mayor capacidad de la red de señalización a este proceso (considerado aquí como la unidad para propósitos de comparación), al utilizar mecanismos de seguridad la red soporta tan sólo 0.33 y 0.42 veces esta capacidad al compartir y no compartir el SSD respectivamente. Los demás renglones de la Tabla VIII se leen de manera similar.

Tabla VII. Tráfico máximo soportado debido a usuarios en vehículos

Proceso	Sin seguridad	Compartición	No compartición
Registro de Terminales	78	26	33
Origen de Llamadas	128	31	27
Entrega de Llamadas	120	61	32

Tabla VIII. Tráfico máximo soportado debido a usuarios en vehículos normalizado

Proceso	Sin seguridad	Compartición	No compartición
Registro de Terminales	1.0	0.33	0.42
Origen de Llamadas	1.0	0.24	0.50
Entrega de Llamadas	1.0	0.50	0.26

Para el caso del tráfico debido a usuarios pedestres, se ha seguido un proceso similar que en el caso debido a usuarios en vehículos. Los resultados son mostrados en la Tabla IX y en la Tabla X.

Tabla IX. Tráfico máximo soportado debido a usuarios pedestres

Proceso	Sin seguridad	Compartición	No compartición
Registro de Terminales	77	26	28
Origen de Llamadas	164	63	47
Entrega de Llamadas	163	120	48

Tabla X. Tráfico máximo soportado debido a usuarios pedestres normalizado

Proceso	Sin seguridad	Compartición	No compartición
Registro de Terminales	1.0	0.33	0.36
Origen de Llamadas	1.0	0.38	0.28
Entrega de Llamadas	1.0	0.73	0.29

Al examinar la Tabla VIII y la Tabla X, resulta ya evidente que los mecanismos de seguridad requieren muchos recursos de la red (tanto en el caso de usuarios en vehículos, como en el caso de usuarios pedestres). Al utilizar estos mecanismos, la capacidad de la red

se ve disminuida severamente. Adicionalmente al observar la Figura 36, la Figura 38, la Figura 40, la Figura 42, la Figura 44, la Figura 46 y la Figura 48 es notorio que cuando no se utilizan mecanismos de seguridad se obtiene el menor retardo para todos los procesos.

Todo esto pone de manifiesto que cuando se utilizan en la red técnicas de autenticidad y privacidad, se gana bastante en cuanto a que se evita la presencia de intrusos en la red. Sin embargo, la capacidad de la red de señalización se ve fuertemente disminuida.

V.3 Comparación entre compartición y no compartición del SSD

Ahora se procede a comparar la eficiencia de los dos mecanismos de privacidad y autenticidad propuestos en los estándares, para ello se probaron tres condiciones distintas en la red determinadas por la movilidad de los usuarios en la red correspondientes a usuarios con baja movilidad, usuarios con mediana movilidad y usuarios con alta movilidad. Para representar de manera realista la operación de la red, se introdujo tráfico de fondo en todos los diferentes nodos de la red como se ilustra en la Tabla XI.

Tabla XI. Tráfico de fondo para la comparación de los mecanismos de seguridad

Proceso	Tráfico en los MSCs	Tráfico en los LEs
Origen de llamadas	10 llamadas/seg.	-
Entrega de llamadas	-	10 llamadas/seg.
Redireccionamiento incondicional de llamadas	-	3 llamadas/seg.
Redireccionamiento de llamadas cuando el usuario no contesta	-	3 llamadas/seg.

Las tres condiciones diferentes de movilidad se representan por medio del tráfico de la Tabla XII.

Tabla XII. El tráfico en la red debido a tres condiciones de movilidad distintas

Movilidad de usuarios	Tráfico en MSCs debido a registro de terminales	Tráfico en MSCs debido a procesos de traspaso de llamadas
Baja	2 solicitudes/seg.	0.5 solicitudes/seg.
Media	10 solicitudes/seg.	2 solicitudes/seg.
Alta	20 solicitudes/seg.	4 solicitudes/seg.

Se realizaron tres corridas distintas de la simulación, la primera introduciendo tráfico en los MSC de la red debido a una condición de baja movilidad de los usuarios, la segunda con tráfico debido a una mediana movilidad en los usuarios y la tercera con tráfico debido a una alta movilidad en los usuarios. El tráfico de fondo permaneció fijo en todos los nodos de la

red, excepto en MSC-1 y LE-1 en donde para cada condición de movilidad, se hizo variar la tasa de origen de llamadas y la tasa de terminación de llamadas respectivamente y de esta manera poder determinar la efectividad de los métodos.

V.3.1 Comparación de los mecanismos de seguridad durante el proceso de origen de llamadas

En la Figura 48 y la Figura 50 y la Figura 52 se muestra el tiempo de respuesta de la red al proceso de origen de llamadas utilizando los dos mecanismos (compartición y no compartición del SSD). La Figura 48 corresponde al caso de usuarios con baja movilidad, la Figura 50 al caso de usuarios con mediana movilidad y la Figura 52 al caso de usuarios con alta movilidad. En la Figura 49, la Figura 51 y la Figura 53 se presenta la utilización del recurso limitante de la capacidad de la red para éste caso, el VLR-1; en estas figuras se observa la manera en que aumenta la utilización de la base de datos VLR-1 al incrementarse la movilidad de los usuarios.

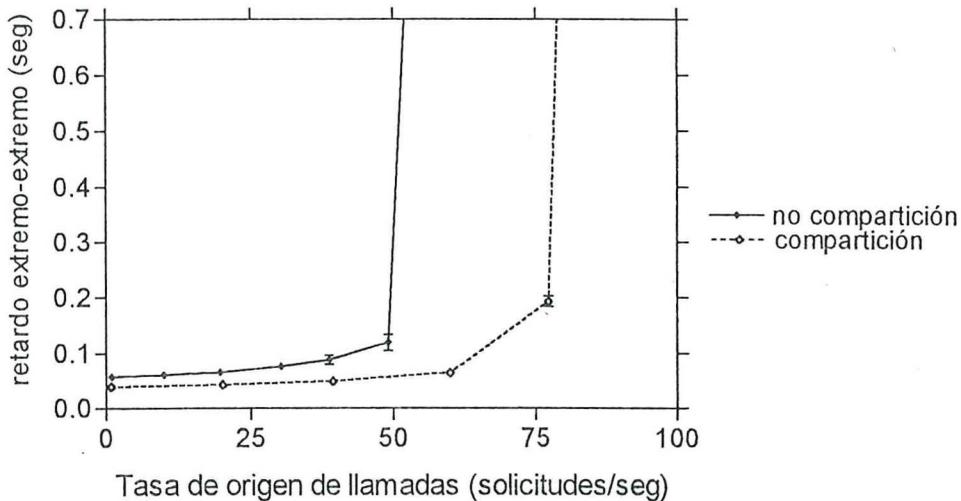


Figura 48. Respuesta de la red al proceso de origen de llamadas en el caso de usuarios con baja movilidad

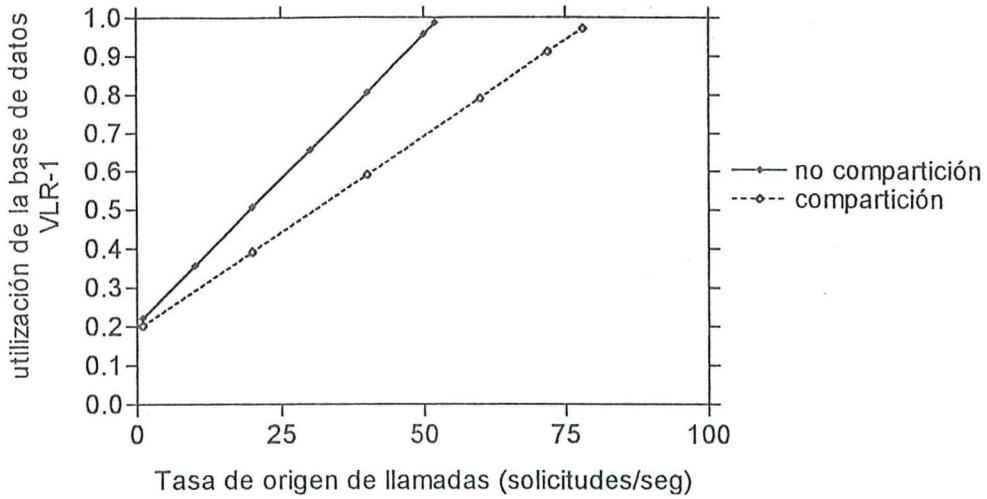


Figura 49. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas en el caso de usuarios con baja movilidad

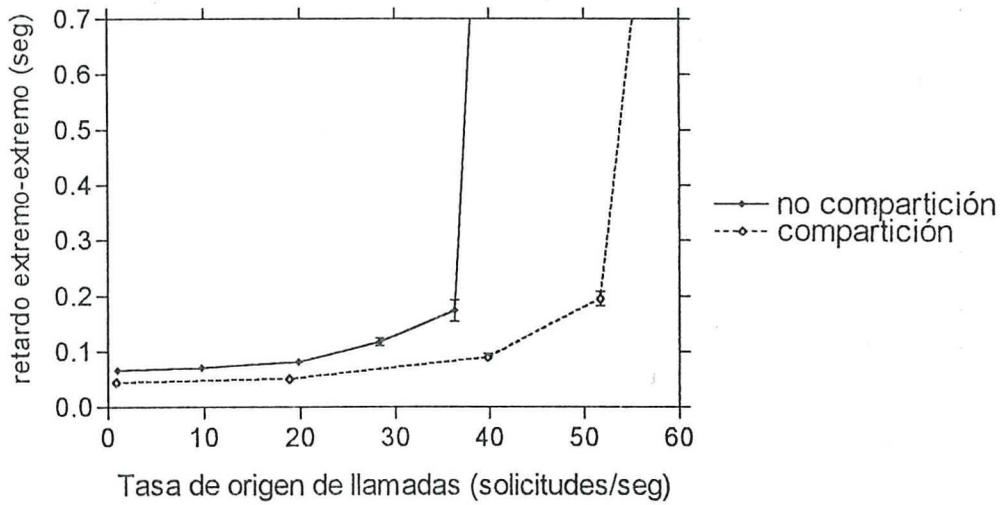


Figura 50. Respuesta de la red al proceso de origen de llamadas en el caso de usuarios con mediana movilidad

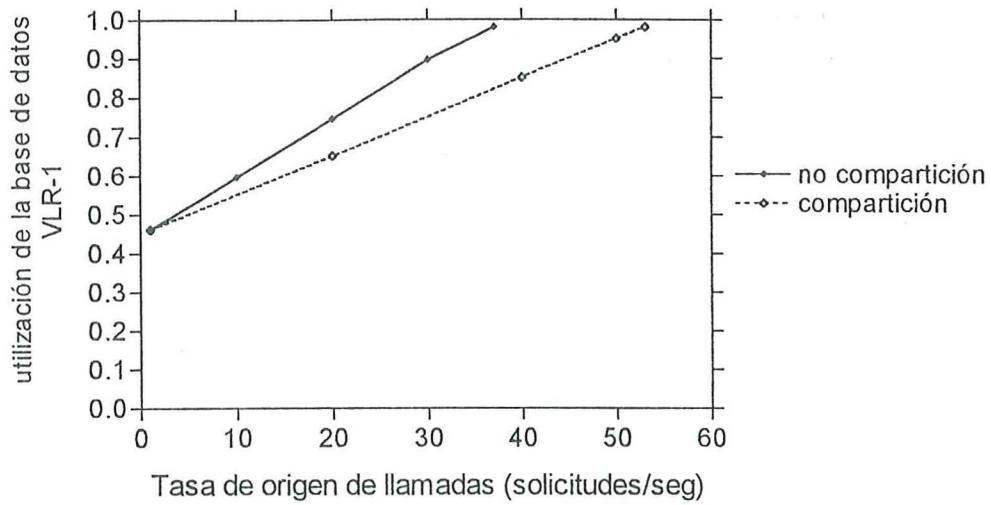


Figura 51. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas en el caso de usuarios con mediana movilidad

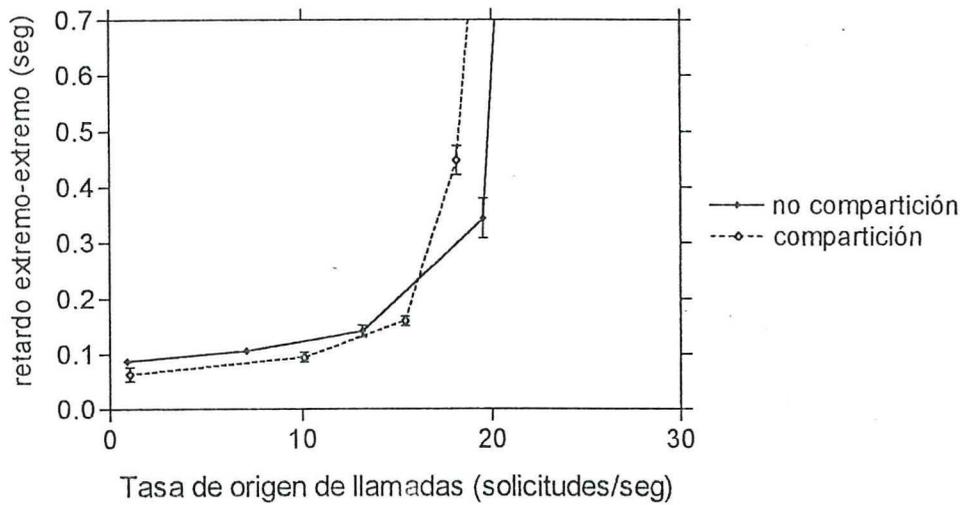


Figura 52. Respuesta de la red al proceso de origen de llamadas en el caso de usuarios con alta movilidad

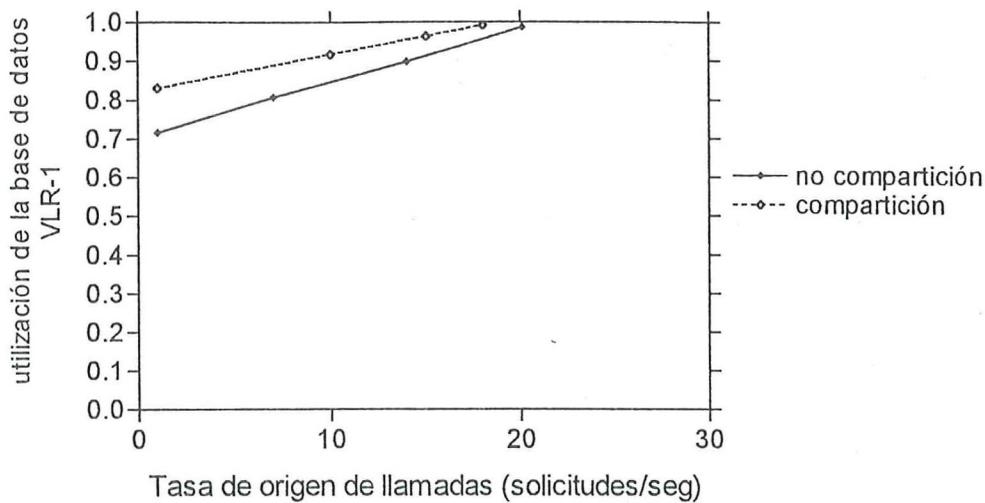


Figura 53. Utilización del elemento limitante (VLR-1) durante el proceso de origen de llamadas en el caso de usuarios con alta movilidad

La Tabla XIII resume el número de llamadas originadas por usuario móvil que la red soporta para las diferentes condiciones de movilidad. La versión normalizada de esta tabla es mostrada en la Tabla XIV para propósitos de comparación. La información de esta última tabla debe leerse verticalmente. Por ejemplo, Para el caso de origen de llamadas cuando la movilidad de los usuarios es baja, el no compartir el SSD resulta en una capacidad de red de apenas el 66.6% respecto al caso en que el SSD se comparte. Las demás columnas se leen en forma similar. A partir de estas tablas y la inspección a las Figura 48, la Figura 50 y la Figura 52 se concluye que para el caso de origen de llamadas el compartir el SSD es más recomendable que el no hacerlo. La capacidad que la red logra es en general mayor y el retardo extremo a extremo es significativamente menor. Sólo en el caso de una alta movilidad de usuarios el compartir el SSD resulta más provechoso.

Tabla XIII. Tráfico máximo soportado durante el proceso de origen de llamadas para las 3 condiciones de movilidad

	Baja Movilidad	Mediana Movilidad	Alta Movilidad
Compartición	78	56	18
No-compartición	52	32	20

Tabla XIV. Tráfico máximo soportado durante el proceso de origen de llamadas para las 3 condiciones de movilidad (normalizado)

	Baja Movilidad	Mediana Movilidad	Alta Movilidad
Compartición	100%	100%	90%
No-compartición	66.6%	57.1%	100%

V.3.2 Comparación de los Métodos de Seguridad durante el Proceso de Entrega de Llamada

En la Figura 54, la Figura 56 y la Figura 58 se presentan los resultados obtenidos para el tiempo de respuesta de la red al proceso de entrega de llamadas. La Figura 54 corresponde al caso de usuarios con baja movilidad, la Figura 56 al caso de usuarios con mediana movilidad y la Figura 58 al caso de usuarios con alta movilidad. La Figura 55, la Figura 57 y la Figura 59 presentan la utilización de los VLR-X identificadas en este caso como el recurso limitante de la capacidad de la red.

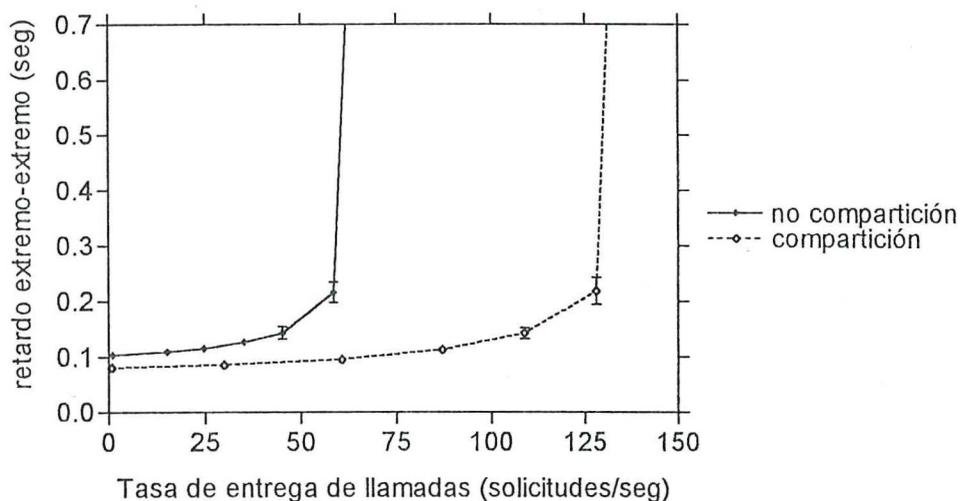


Figura 54. Respuesta de la red al proceso de entrega de llamadas en el caso de usuarios con baja movilidad

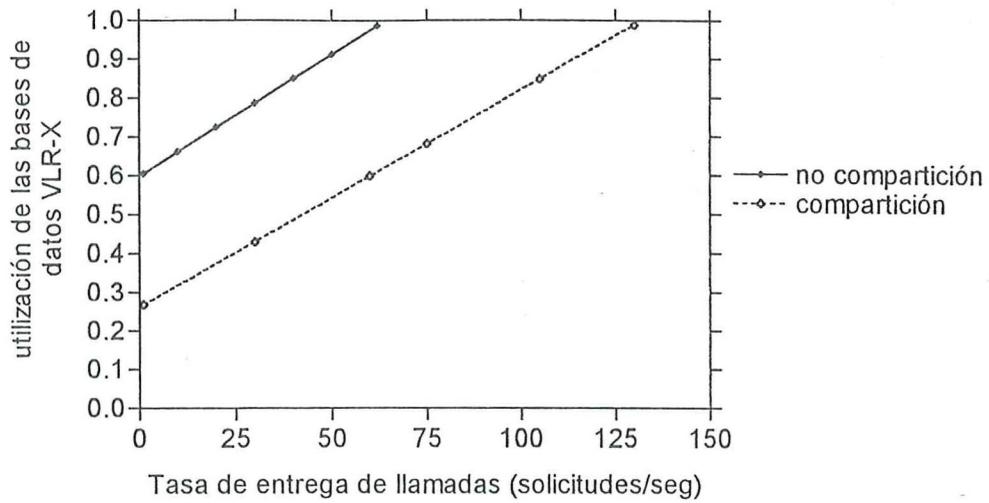


Figura 55. Utilización del elemento limitante (VLR-X) durante el proceso de entrega de llamadas en el caso de usuarios con baja movilidad

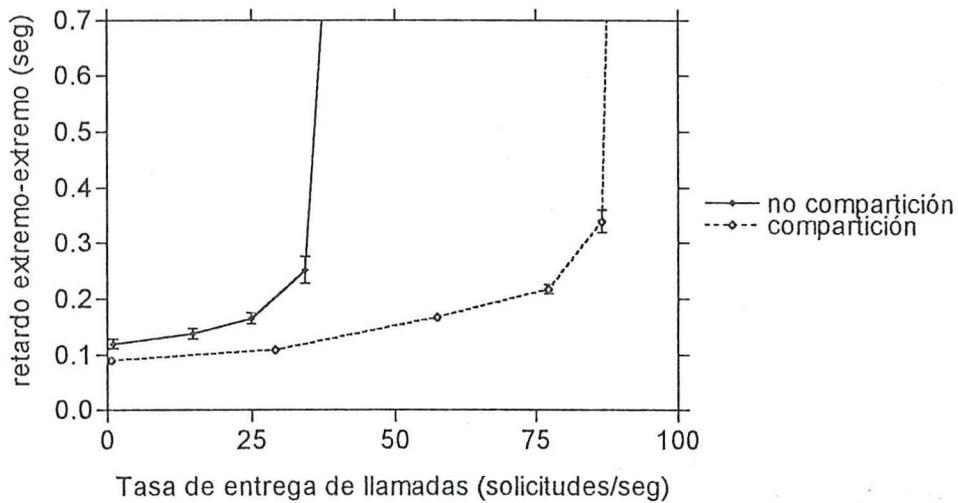


Figura 56. Respuesta de la red al proceso de entrega de llamadas en el caso de usuarios con mediana movilidad

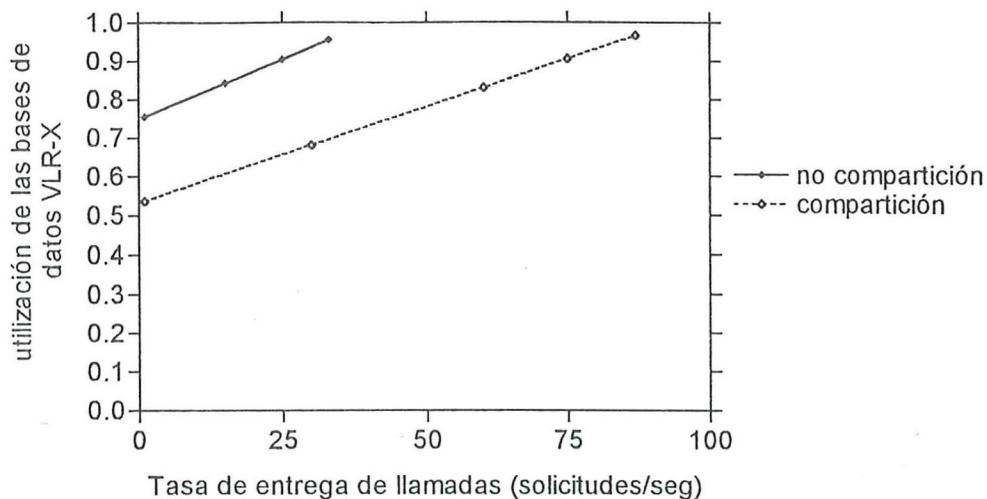


Figura 57. Utilización del elemento limitante (VLR-X) durante el proceso de entrega de llamadas en el caso de usuarios con mediana movilidad

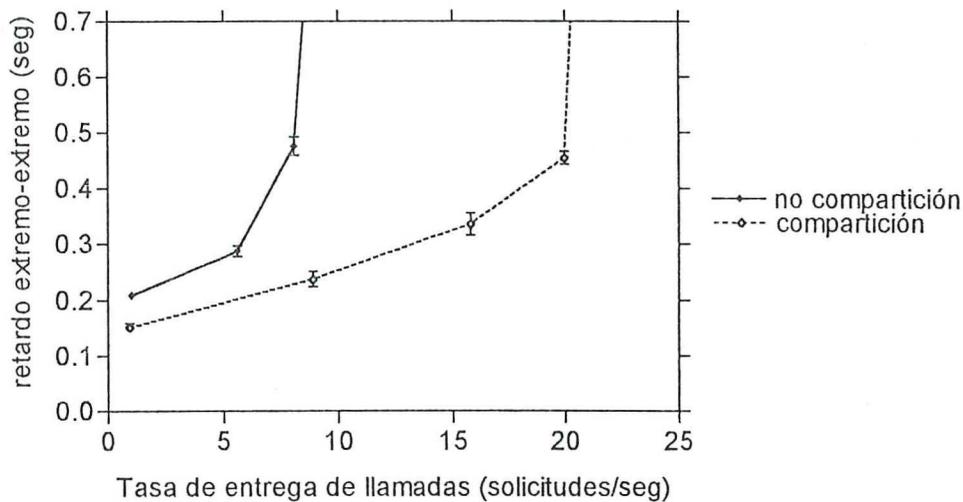


Figura 58. Respuesta de la red al proceso de entrega de llamadas en el caso de usuarios con alta movilidad

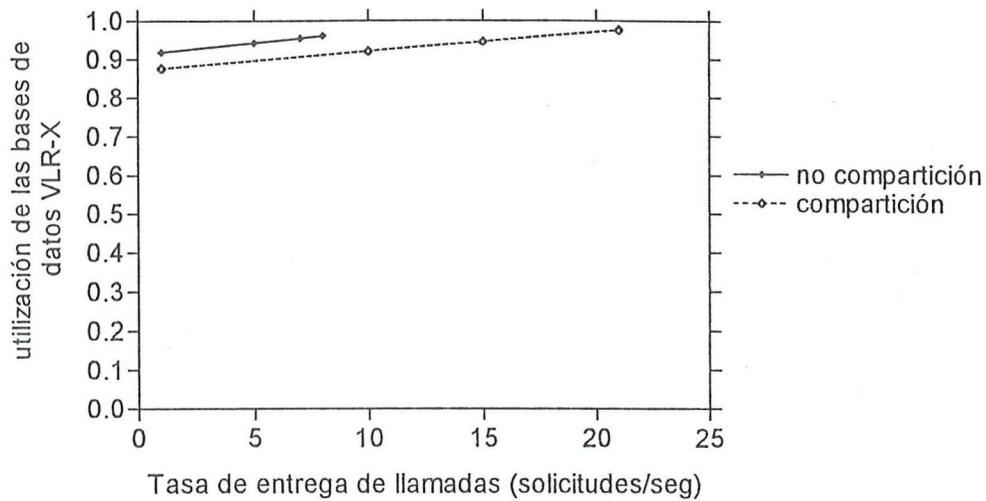


Figura 59. Utilización del elemento limitante (VLR-X) durante el proceso de entrega de llamadas en el caso de usuarios con alta movilidad

En la Tabla XV y la Tabla XVI se resume la capacidad de la red al proceso de entrega de llamadas. La Tabla XVI es la versión normalizada de la Tabla XV. La información de esta última tabla puede leerse de manera vertical. En todos los casos de movilidad (baja, mediana y alta) el no compartir el SSD resulta poco eficiente respecto a cuando éste se comparte. Por ejemplo, cuando la movilidad de los usuarios es alta, la no compartición del SSD logra apenas 0.38 veces la capacidad que se logra cuando el SSD si se comparte.

Tabla XV. Tráfico máximo soportado durante el proceso de entrega de llamadas para las 3 condiciones de movilidad

	Baja Movilidad	Mediana Movilidad	Alta Movilidad
Compartición	130	87	21
No-compartición	62	37	8

Tabla XVI. Tráfico máximo soportado durante el proceso de entrega de llamadas para las 3 condiciones de movilidad (normalizado)

	Baja Movilidad	Mediana Movilidad	Alta Movilidad
Compartición	1	1	1
No-compartición	0.47	0.42	0.38

V.3.3 Comparación de los métodos de seguridad al variar la movilidad de los usuarios

A partir de la Tabla XIII y la Tabla XV es posible comparar la efectividad de compartir el SSD y no compartirlo cuando la movilidad de los usuarios varía. Los resultados se resumen en la Tabla XVII y la Tabla XVIII para los procesos de origen de llamadas y entrega de llamadas respectivamente. La información de las tablas ha sido normalizada para efectos de la comparación. Las tablas deberán leerse horizontalmente. Por ejemplo, considere la Tabla XVII, cuando el SSD se comparte, y la movilidad de los usuarios pasa de ser baja a mediana o alta, la capacidad de la red al proceso de origen de llamadas baja hasta un 0.71 y un 0.23.

Los resultados presentados en esta forma revelan que la movilidad de los usuarios en la red puede llegar a afectar en gran medida la capacidad de llamadas (originadas o entregadas). De allí la importancia de considerar la movilidad de los usuarios durante el diseño de las áreas de localización. A mayor movilidad de usuarios, se deben proyectar las áreas de localización de mayor tamaño para evitar que los procesos de traspaso de llamadas y de registro de terminales sean tan frecuentes, que la capacidad de la red pueda verse seriamente reducida.

Tabla XVII. Efectos de la movilidad sobre el origen de llamadas

	Baja Movilidad	Mediana Movilidad	Alta Movilidad
Compartición	1	0.71	0.23
No-compartición	1	0.61	0.38

Tabla XVIII Efectos de la movilidad sobre la entrega de llamadas

	Baja Movilidad	Mediana Movilidad	Alta Movilidad
Compartición	1	0.62	0.16
No-compartición	1	0.59	0.12

V.3.4 Comparación de los Métodos de Seguridad durante el Proceso de Registro de Terminales

Para una mejor comparación de los mecanismos de privacidad y autenticación, se requiere así mismo, el conocer el número de registros que logra cada uno de los métodos. Para efectos de ésta prueba se han considerado tres clases de usuarios en la red, usuarios con una baja tasa de llamadas, usuarios con mediana tasa de llamadas y usuarios con alta tasa de

llamadas. Para este caso se ha introducido tráfico de fondo en los elementos de la red tal y como se ilustra en la Tabla XIX.

Tabla XIX. Tráfico de fondo para evaluar la capacidad de la red al proceso de registro de terminales

Proceso	Tráfico en los MSCs	Tráfico en los LEs
Registro de terminales	5 solicitudes/seg.	-
Traspaso de llamada	5 solicitudes /seg.	-
Redireccionamiento incondicional de llamadas	-	3 llamadas/seg.
Redireccionamiento de llamadas cuando el usuario no contesta	-	3 llamadas/seg.

Las tres condiciones diferentes de origen de llamadas se representan por medio del tráfico de la Tabla XX.

Tabla XX. Tres condiciones de tráfico para evaluar la capacidad de la red al proceso de registro de terminales

Tráfico de llamadas	Origen de llamadas	Terminación de llamadas
Bajo	2 llamadas/seg.	2 llamadas/seg.
Medio	8 llamadas/seg.	8 llamadas/seg.
Alto	14 llamadas/seg.	14 llamadas/seg.

Se realizaron tres corridas de la simulación, la primera introduciendo tráfico debido a un bajo número de llamadas, la segunda con tráfico debido a un número medio de llamadas y la tercera con tráfico debido a un alto número de llamadas. El tráfico de fondo permaneció fijo en todos los nodos de la red, excepto en MSC-1 en donde para cada condición del tráfico de llamadas se hizo variar la tasa de registros de terminales para checar la efectividad de los métodos. En la Figura 60, la Figura 62 y la Figura 64 se ilustra el tiempo de respuesta de la red al proceso de registro de terminales utilizando los dos mecanismos (compartición y no compartición del SSD), las figuras corresponden al caso de usuarios con bajo tráfico de llamadas, mediano tráfico de llamadas y con alto tráfico de llamadas respectivamente. En la Figura 61, la Figura 63 y la Figura 65 se muestra la utilización del recurso limitante en la capacidad de la red para el caso del proceso de registro de terminales, el VLR-1.

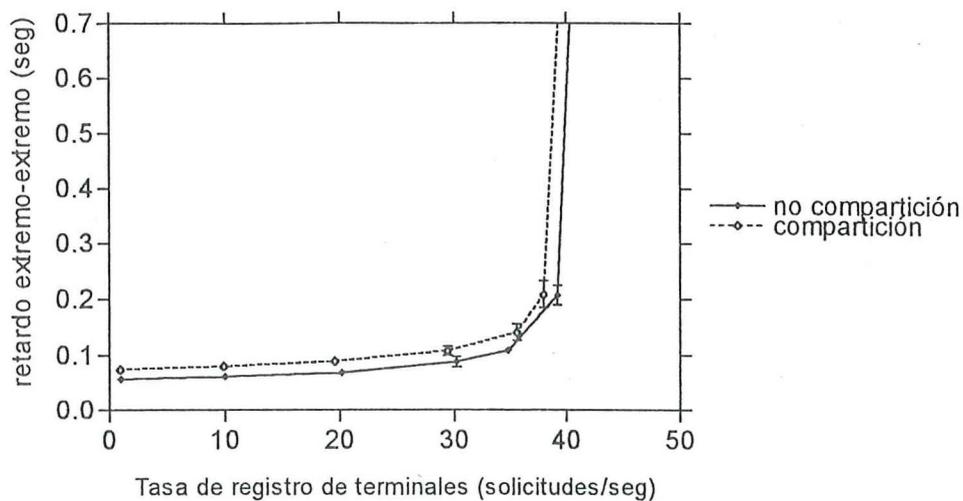


Figura 60. Respuesta de la red al proceso de registro de terminales para el caso de usuarios con bajo tráfico de llamadas

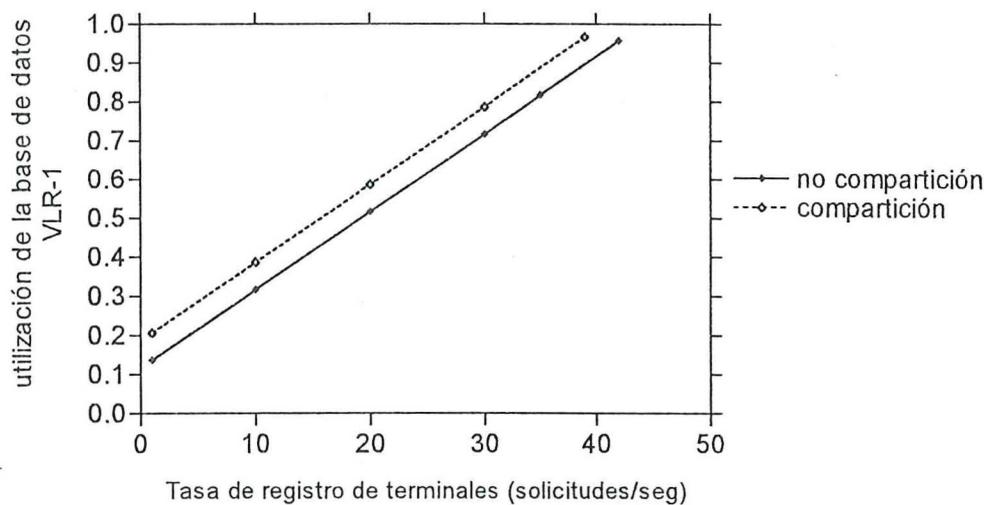


Figura 61. Utilización del elemento limitante (VLR-1) durante el proceso de registro de terminales en el caso de usuarios con bajo tráfico de llamadas

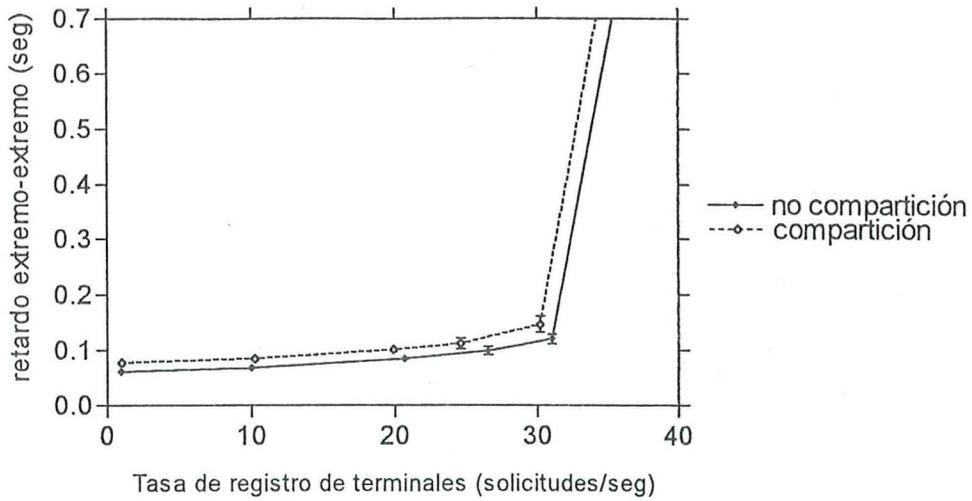


Figura 62. Respuesta de la red al proceso de registro de terminales en el caso de usuarios con mediano tráfico de llamadas

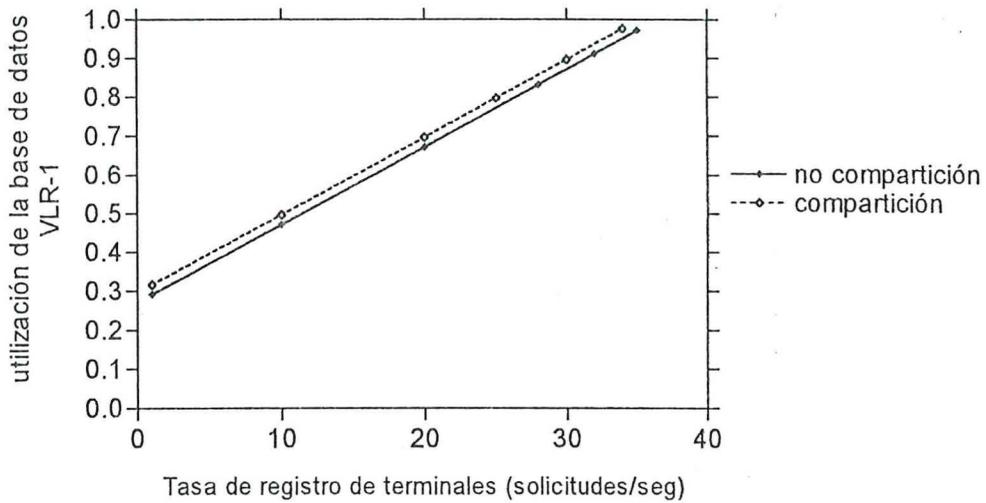


Figura 63. Utilización del elemento limitante (VLR-1) durante el proceso de registro de terminales en el caso de usuarios con mediano tráfico de llamadas

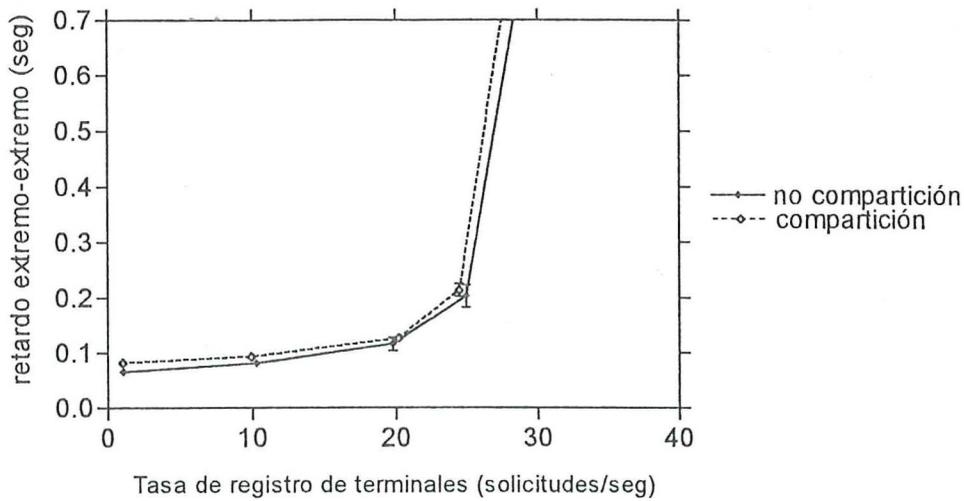


Figura 64. Respuesta de la red al proceso de registro de terminales en el caso de usuarios con alto tráfico de llamadas

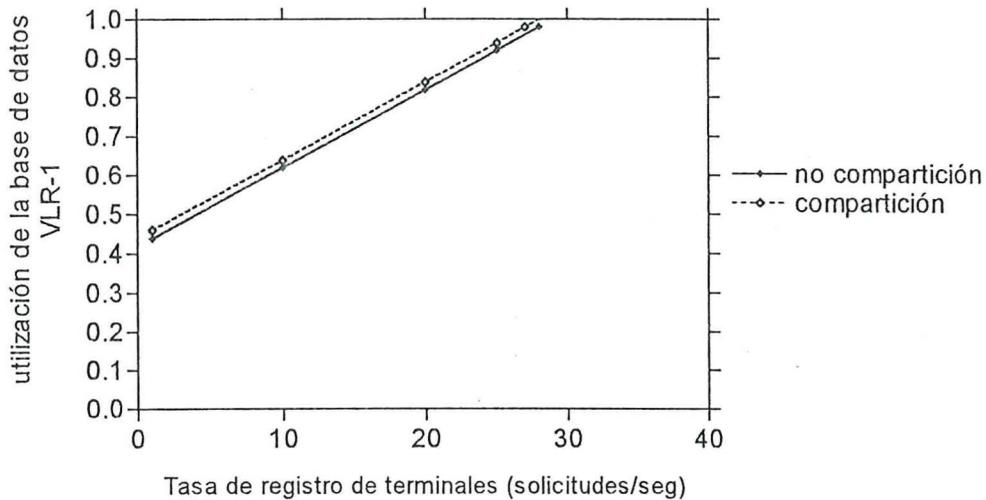


Figura 65. Utilización del elemento limitante (VLR-1) durante el proceso de registro de terminales en el caso de usuarios con alto tráfico de llamadas

En la Tabla XXI y la Tabla XXII se muestra un resumen de la capacidad de la red al proceso de registro de terminales. La Tabla XXII es la versión normalizada de la Tabla XXI. La Tabla XXII puede leerse de manera vertical. En este caso la capacidad de la red es en mucho similar al utilizar o no la compartición del SSD. Sin embargo al observar la Figura 60,

la Figura 62 y la Figura 64, se pone de manifiesto que el compartir el SSD incurre en mayores retardos que el caso en que éste no se comparte.

Tabla XXI. Tráfico máximo soportado durante el proceso de registro de terminales 3 condiciones de movilidad

	Bajo Tráfico	Mediano Tráfico	Alto Tráfico
Compartición	39	34	27
No-compartición	40	35	28

Tabla XXII. Tráfico máximo soportado durante el proceso de registro de terminales 3 condiciones de movilidad (normalizado)

	Bajo Tráfico	Mediano Tráfico	Alto Tráfico
Compartición	0.97	0.97	0.96
No-compartición	1.0	1.0	1.0

VI. CONCLUSIONES, RECOMENDACIONES Y COMENTARIOS

VI.1 Conclusiones

En este trabajo se ha evaluado el desempeño de la red de señalización de los PCS. Esta se basa en el Sistema de Señalización Número 7 (SS7) e incluye a la Red Inteligente (IN) en su estructura.

Para efectos de la evaluación del desempeño se crearon modelos de simulación de una red PCS típica utilizando el lenguaje de simulación orientado a comunicaciones OPNET. OPNET proporciona un completo ambiente de desarrollo que permite el modelado y la evaluación del desempeño de redes de comunicaciones con un gran nivel de detalle, sin imponer restricción alguna en la especificación de los modelos de simulación. Estas características, así como las avanzadas y flexibles herramientas para la colección y el análisis de los resultados arrojados por las simulaciones hacen de OPNET una herramienta atractiva para el modelado.

El desempeño es medido en términos del retardo extremo-extremo que experimentan los procesos que son necesarios en una red PCS para proporcionar servicio a los usuarios, ejemplos de éstos procesos son el registro de terminales, el traspaso de llamadas, el origen de llamadas, la entrega de llamadas y servicios suplementarios de red inteligente como son redireccionamiento incondicional de llamadas y redireccionamiento cuando el usuario no contesta. También se incluye la utilización del dispositivo que en cada proceso limita la capacidad de la red.

Se han evaluado tres diferentes versiones de estos procesos a saber: Una de las versiones se caracteriza por la no implementación de mecanismos de seguridad (autenticidad y privacidad) en la red, esto corresponde a la situación actual en estas redes, en donde la cada vez más alta tasa de usuarios fraudulentos, hace necesaria la introducción de mecanismos de seguridad.

Las otras dos versiones evaluadas corresponden a dos diferentes propuestas estandarizadas recientemente en el estándar IS-41. En una de ellas los datos secretos de

usuario (SSD) (aquellos datos que se requieren para establecer los mecanismos de privacidad y autenticación) son compartidos con el sistema visitado y en la otra no.

Los resultados obtenidos revelan invariablemente que la capacidad de la red se verá afectada seriamente al introducir los mecanismos de privacidad y autenticación respecto del caso en que éstos mecanismos no se utilizan. También el retardo que experimentan los mensajes en la red cuando no se utilizan los mecanismos de seguridad es notoriamente inferior. Esto indica el porque hasta recientemente no se había considerado la autenticación de usuarios en estas redes.

Sin embargo, debido al cada vez mayor costo debido al fraude en los EE.UU. en los PCS, (que ya se estima cercano a los 2 millones de dólares Americanos al día) se hace inminente la inclusión de éstos mecanismos en las redes actuales.

Al evaluar los dos mecanismos de autenticación, ha sido notado que el caso en el que el SSD se comparte con el sistema visitado es en general más provechoso. Cuando el SSD se comparte logra una notoria mayor capacidad en la red y en general el retardo experimentado por los mensajes es menor.

También en éste trabajo ha sido evaluado el impacto de la movilidad de los usuarios sobre la capacidad de la red. Ha sido encontrado que la movilidad de los usuarios puede llegar a afectar en gran medida la capacidad de llamadas. De allí que es importante considerar la movilidad de los usuarios durante el diseño de las áreas de localización de la red. A una mayor movilidad de usuarios, las áreas de localización deben ser proyectadas con un mayor tamaño para evitar que los procesos de traspaso de llamadas y registros de terminales sean tan frecuentes, que la capacidad de la red señalización se vea seriamente reducida.

Para representar a la red de señalización de manera realista, se han modelado en detalle los diferentes elementos de la red de acuerdo a sus características funcionales establecidas por los estándares. Adicionalmente han sido consideradas diferentes cargas de tráfico para modelar diferentes tipos de usuarios en la red.

Los resultados obtenidos en este trabajo pueden ser empleados por la gente que proyecta y diseña sistemas PCS para estimar cuanto impactaría en sus redes el introducir mecanismos de autenticidad y privacidad.

VI.2 Recomendaciones

En seguida se establecen algunas direcciones posibles para trabajo futuro:

Hemos detectado que los procesos para mantener la localización de los usuarios (conocido como método a dos niveles: El HLR y el VLR) en las redes PCS requieren recursos adicionales de la red. En [Akyldiz Ian y Joseph Ho, 1996; Quin Zhigang, *et al*, 1995.] se presenta un compendio de varios métodos alternativos propuestos en investigaciones recientes, que aparentemente resultarían en ahorros substanciales, tanto en el tráfico de señalización necesario para la proporción de los servicios a usuarios, así como en el número de consultas a las bases de datos de la red. Sería conveniente evaluar las diferentes alternativas allí propuestas para ver hasta que medida beneficiaría el introducir en las redes actuales los métodos propuestos.

La carga de tráfico considerada en este trabajo (su intensidad, así como el tipo de distribución de probabilidad que ésta sigue) no corresponde a una situación real en una red PCS en operación, sino más bien, este tráfico ha sido propuesto. Sería conveniente el establecer modelos de tráfico basados en mediciones y estadísticas de una red en operación. En [Lam Derek, *et al*, 1995] se ha establecido una metodología para caracterizar el tráfico producido por usuarios en la PSTN, analizando el patrón del tráfico en la red debido a la movilidad de los usuarios y el perfil de llamadas de diferentes clases de usuarios. Las ideas allí propuestas podrían aplicarse al caso de PCS.

En la red PCS propuesta para este trabajo, se consideraron 4 MSCs y sus respectivas bases de datos VLR asociadas. Sería interesante estudiar el comportamiento de la red cuando no solo 4, sino más (por ejemplo unos 10 ó más) MSCs estuviesen presentes. En este caso, el recurso limitante en los diferentes procesos de la red podrían ya no ser los VLR, sino probablemente el HLR y el AUT debido a son las bases de datos centralizadas de la red. El estudio de esta situación podría proporcionar mayor conocimiento del comportamiento de

estas redes. Sin embargo en este caso se requeriría de equipo de cómputo con mayores capacidades.

Adicionalmente, las colas de los diferentes elementos de la red podrían ser limitadas en longitud para representar la red de manera más realista. Esto requeriría de la implementación de métodos de control de flujo y admisión del tráfico en la red.

Otro posible aspecto a estudiar es la integración y evolución de las redes móviles actuales hacia plataformas como UMTS (Universal Mobile Telecommunication Systems) y UPT (Universal Personal Communications). En [Magendaz T., 1996] se estudian diferentes escenarios posibles para la evolución hacia UMTS. Tanto en UMTS como UPT la red inteligente tiene asegurado un papel importante.

En éstos posibles futuros trabajos vislumbrados, las bases teóricas, los modelos, y la metodología seguida en este trabajo de tesis, serían sin duda de bastante utilidad.

VI.3 Comentarios

Los Sistemas de Comunicación Personal (PCS) representan el sector de las telecomunicaciones con más rápido crecimiento y uno de los que mayores ingresos económicos generan. Aunque pudiese pensarse que gran parte del trabajo en PCS esta hecho ya, aún hay mucho trabajo por hacer. Las redes PCS están evolucionando en todos los aspectos, desde las unidades móviles cada día más pequeñas y portables, incluyendo el acceso al canal de radio soportando más usuarios con mejores técnicas (por ejemplo usando CDMA) que garantizan una mejor calidad de la comunicación, hasta las técnicas en la parte de la red de señalización quien cada vez proporciona mejores y mayores servicios a los usuarios.

Gran parte de las experiencias adquiridas en el despliegue de los PCS son utilizadas para la especificación de los futuros sistemas inalámbricos mundiales. La IN ha sido identificada como un elemento necesario en la arquitectura de las redes de telecomunicaciones del futuro y muy pronto será introducida en las redes de banda amplia soportando servicios multimedia. Los sistemas móviles del futuro (por ejemplo, UMTS) están siendo proyectados utilizando las capacidades de la red inteligente.

Las cada día más demandantes aplicaciones y servicios en las redes de telecomunicaciones hacen necesaria una revisión al Sistema de Señalización Número 7; a pesar que SS7 ha permitido la aparición de tecnologías emergentes como la IN, UPT y Redes Móviles, es un hecho que éste fue proyectado teniendo en mente tecnologías anteriores. Por ejemplo, la velocidad de transmisión de 64 kbps en los enlaces de señalización en pocos años será insuficiente. Adicionalmente, la verificación de errores en cada nodo de la red ya no es necesaria debido a la reciente inclusión de medios de comunicación más libres de error (como por ejemplo las fibras ópticas).

LITERATURA CITADA

Akyldiz Ian y Joseph Ho. 1996. "*On Location Management for Personal Communication Networks*," IEEE Communications Magazine; pp 138-145, September.

Bafutto Marcos, Paul Kühn y Gert Willamann. 1994. "*Capacity and Performance Analysis of Signaling Networks in Multivendor Environments*," IEEE Journal on Selected Areas in Communications. Vol 12, No.3; pp. 490- 500.

Bedoy Jesús. 1997. "*Estudio de Mecanismos de Control de Flujo para la Entrega Eficiente y Robusta de Servicios en la Red Inteligente*". Tesis de Maestría, CICESE Mexico.

Berman Roger y Jonh Brewster. 1992. "*Perspectives on the AIN Architecture*," IEEE Communications Magazine February.

Black Uyles. 1996. "*Mobile and Wireless Networks*," Prentice Hall, USA.

CCITT Specifications of the Signaling System No. 7. 1989. Blue Book, Recommendations Q.700-Q.716. Geneva 1989.

Cellular Networking Perspectives Magazine. 1997. Sampler Edition. Editor David Crowe. Calgary AB T2N 3W1, Alberta Canada.

Garg Vijay and Joseph Wilkes. 1996. "*Wireless and Personal Communications Systems*," Prentice hall, pp 455, USA.

Gomes Fabian 1993 "*Benchmarking SMTW with a SS7 Performance Model Simulation*," Department of Computer Science, the University of Calgary, Calgary Alberta, Canada. Internal Report.

Hou Victor, Kant Krishna y V. Ramaswami. 1994. "*Error Monitoring Issues for Common Channel Signaling*," IEEE Journal on Selected Areas in Communications. Vol 12, No.3; pp. 456- 467. April.

Husain Syed y James Marochi. 1996. "*Intelligent Network: A Key Platform for PCS Interworking and Interoperability*," IEEE Communications Magazine; pp 98-105, September.

ITU-T Reccomendations Q.12XX. Editadas por la ITU 1993-1996.

Jabbari Bijan. 1991. "*Common Channel Signaling System Number 7 for ISDN and Intelligent Networks*". Proceedings of the IEEE, Vol 79, No. 2; pp. 155-169. February

LITERATURA CITADA (continuación)

Jabbari Bijan. 1992. "*Intelligent Networks Concepts in Mobile Communications*," IEEE Communications Magazine; pp. 64-69, February.

Jabbari Bijan, Giovanni Colombo, Akihisa Nakajima y Jayanat Kulkarni. 1995. "*Network Issues for Wireless Communications*," IEEE Communications Magazine; pp 88- 98. January.

Lam Derek, Jan Jannink, Donald Cox, y Jennifer Widom. 1995. "*Modeling Location Management in Personal Communication Services*," Stanford University. Department of Engineering & Computer Science Depts.; pp 27. October 18.

Lin Yi-Bing and Steven Devries. 1995. "*PCS Network Signaling Using SS7*," IEEE Personal Communications; pp. 44-55, June.

Magendaz T. 1996. "*Integration and Evolution of Existing Mobile Telecommunications Systems toward UMTS*," IEEE Communications Magazine; pp 90-98. September.

Meier-Hellstern Kathleen, Eduardo Alonso y Douglas Douglas. 1992. "*The Use of SS7 and GSM to Support High Density Personal Communications*," Proceedings of the ICC; pp 1698-1702.

Modarressi Abdi y Ronald Skoog. 1990. "*Signaling System No. 7: A Tutorial*," IEEE Communications Magazine, Vol 28; pp. 19-35.

Mohan S. y R. Jain. 1994. "*Two Users Location Strategies for Personal Communication Services*," IEEE Personal Communications; pp 42-50, First Quarter.

Mohan S. 1996. "*Privacy and Authentication Protocols for PCS*," IEEE Personal Communications; pp 34-38, October.

OPNET Modeller Manuals. 1993. MIL 3 Inc. USA.

Pollini Gregory. 1994. "*Signaling System No. 7 Messaging in North American Cellular*," Technical Report WINLAB-TR-73, Rutgers University, May.

Quin Zhigang, Malathi Veeraraghavan y Tomas La Porta. 1995. "*An Improved Mobile Tracking and Location Procedure for ATM-Based PCNs*," Proceedings of the ICC 1995"; pp 6-11.

LITERATURA CITADA (continuación)

Ramaswami V. y Jonathan Wang. 1993. "*Analysis of the Link Error Monitoring Protocols in the Common Signaling Network*," IEEE/ACM Transactions on Networking, Vol. 1, No. 1; pp 31-46. February.

Robrock R. 1991. "*The Intelligent Network- Changing the Face of Telecommunications*," Proceedings of the IEEE, Volume 79, No.1, January.

Stallings William. 1995. "*ISDN and Broadband ISDN with Frame Relay and ATM*," Third Edition. Prentice Hall.

Sirovica Dejan y Kamat Purushottam. 1994. "*Experiences with the Development of a Distributed Radio Port Controller Architecture*," International Conference On Universal Personal Communications, San Diego California; pp 286 -290. Sept 27-October 1.

Unger Brian, Douglas Goetz y Maryka Stephen. 1994. "*Simulation of SS7 Common Channel Signaling*," IEEE Communications Magazine; pp 52 -62. March.

Willmann Gert y Paul Kühn. 1990. "*Performance Modeling of Signaling System No. 7*," IEEE Communications Magazine, Vol 28; pp. 44-56, July.

Wirth Patricia. 1995. "*Teletraffic Implications of Database Architectures in Mobile and Personal Communications*," IEEE Communications Magazine; pp 55-59. June.

ANEXO: INTRODUCCION A OPNET

OPNET proporciona un ambiente de desarrollo completo que permite el modelaje y la evaluación del desempeño de sistemas distribuidos y redes de comunicaciones. El comportamiento de los sistemas y su desempeño es obtenido mediante la realización de simulaciones de eventos discretos.

OPNET ofrece un ambiente de simulación orientado a objetos que permite el reuso de módulos. OPNET es una herramienta de simulación orientada a comunicaciones que permite la especificación de modelos de simulación en gran detalle, cuenta con herramientas para la depuración y animación de los modelos.

El paquete consiste de varias herramientas, cada una enfocada en aspectos particulares del modelaje. Estas herramientas pueden agruparse en 3 clases distintas: herramientas para la especificación de los modelos, herramientas para ejecutar la simulación y para la colección de datos (resultados arrojados de las simulaciones) y herramientas de análisis. En seguida se da un panorama acerca de éstas herramientas.

Herramientas para la Especificación del Modelo

OPNET soporta la especificación de modelos por medio de cuatro herramientas o editores que capturan las características del modelo bajo estudio. Estos son: el editor de red, el editor de nodo, el editor de procesos y el editor de parámetros. La especificación del modelo se realiza de una manera jerárquica. Las especificaciones realizadas en el editor de red requieren de elementos especificados en el editor de nodo. A su vez, las especificaciones realizadas en el nivel nodo hacen uso de modelos definidos en el editor de procesos. El editor de parámetros se utiliza para definir modelos de datos (como formatos de paquetes, funciones de densidad de probabilidad, etc.) que son luego utilizados en el nivel de proceso o en el de nodo.

Editor de Red

El editor de red se utiliza para especificar gráficamente la topología de la red de comunicaciones por medio de nodos y enlaces de comunicación. Es posible agrupar

segmentos de red en una subred tal y como se hace realmente en las redes de comunicaciones actuales.

Editor de Nodo

El editor de nodo se utiliza para definir de manera gráfica el flujo de datos entre los módulos que conforman un nodo. Ejemplos de módulos incluyen procesadores, colas y generadores de tráfico entre otros.

Editor de Procesos

El editor de procesos utiliza diagramas de estados, una extensión del lenguaje C conocida como proto-C (C para protocolos) y una librería de más de 300 primitivas para desarrollar protocolos y algoritmos complejos. Las tareas que realizan los módulos del nivel de nodo son llamadas procesos y ellos son definidos por medio del editor de procesos.

OPNET no impone restricción alguna en la complejidad ni el detalle incluidos en la especificación de los modelos de simulación. OPNET soporta el concepto de programación orientada a objetos permitiendo el reuso de modelos. Nuevos modelos pueden ser creados utilizando modelos previamente creados. Esto significa que componentes de cada uno de los niveles pueden ser modificados y/o reutilizados para formar modelos.

Herramientas para Ejecución de la Simulación y Colección de Datos

Mediante la utilización de las herramientas para la especificación del modelo, se puede obtener un programa ejecutable (un programa que no depende de OPNET y que se puede invocar desde la línea de comandos) que incluya en sí mismo las características importantes del modelo bajo estudio. El objetivo que se persigue al realizar simulaciones es el obtener medidas que permitan estimar el desempeño de un sistema o hacer mediciones respecto al comportamiento del sistema. OPNET permite la colección de información de interés en las simulaciones por medio de vectores y escalares de salida. Un vector almacena información relativa a una sola corrida de la simulación, el vector se constituye por pares ordenados donde la primera componente de un par ordenado es una variable independiente (comúnmente el tiempo de simulación) y la segunda es una variable independiente (que puede

ser el número de paquetes, retardo, etc.). Los vectores se van acumulando y almacenando al transcurrir el tiempo de simulación.

Los escalares por otra parte permiten acumular datos de varias corridas de la simulación. Típicamente se corre una vez la simulación durante un tiempo dado y bajo ciertos valores de entrada, obteniendo un valor promedio asociado a esas condiciones de entrada mismo que se almacena en un escalar. Posteriormente se cambian las condiciones de entrada y se vuelve a correr la simulación por el mismo tiempo, obteniéndose otro valor promedio que se acumula en el escalar. Este proceso puede repetirse cuantas veces sea necesario. Los escalares son muy útiles para la generación de curvas que representen el comportamiento de un sistema al variar ciertos parámetros de entrada. Por ejemplo es por medio de escalares como pueden obtenerse curvas como *caudal contra carga ofrecida*, *retardo contra carga ofrecida*, etc.

Herramientas de Análisis

Esas herramientas permiten graficar y manipular los datos (ya sean vectores o escalares) recolectados a lo largo de las simulaciones. OPNET ofrece flexibilidad para el despliegue de gráficas y proporciona herramientas estadísticas y matemáticas para manipular los resultados (como por ejemplo permite calcular intervalos de confianza y funciones de distribución de probabilidad, la aplicación de filtros a los datos, etc.). Adicionalmente OPNET permite un análisis visual del comportamiento de la red por medio de animaciones. Una animación es una representación gráfica dinámica de eventos seleccionados que ocurren durante la simulación. Existe la posibilidad de exportar en formato texto la información contenida en escalares o vectores para su procesamiento en otros paquetes de computo.

En resumen, las principales características que proporciona OPNET incluyen:

- Orientación a Objetos
- Especializado para redes de comunicaciones y sistemas de información
- Modelaje en niveles (jerárquico)
- Ambiente gráfico
- Flexibilidad para desarrollar detallados y personalizados modelos de redes existentes y prototipos

- Generación automática de simulaciones
- Herramientas de Análisis integradas
- Depuración avanzada
- Animación

Al trabajar con OPNET es bueno tener presente que debido al alto nivel de complejidad que se puede especificar en los modelos de simulación, se hacen necesarios recursos de computo sofisticados, además el tiempo de simulación de un modelo de regular complejidad es elevado. El lector interesado en mayor detalles acerca de OPNET puede revisar los manuales del paquete [OPNET, 1993].

GLOSARIO

ACM	Address Complete Message: Mensaje de Dirección Completa
AD	Adjunct: Adjunto
AIN	Advanced Intelligent Network: Red Inteligente Avanzada
AMPS	Advanced Mobile Phone System: Sistema Telefónico Móvil Avanzado
ANM	Answer Message: Mensaje de Contestación
ANSI	American National Standards Institute: Instituto de Estandarización Nacional Americano
AUT	Authentication: Autenticación
Bellcore	Bell Communications Research: Grupo de Investigación en Comunicaciones de los Laboratorios Bell
BIB	Backward Indicator Bit: Bit Indicador de Regreso
BS	Base Station: Estación Base
BSC	Base Station Controller: Controlador de la Estación Base
BSN	Backward Sequence Number: Número de Secuencia de Regreso
CAVE	Cellular Authentication and Voice Encryption: Algoritmo Celular para Autenticación y Encriptación de Voz
CCS	Common Channel Signaling: Señalización por Canal Común
CDM	Control de Distribución de Mensajes
CEM	Control de Envío de Mensajes
CER	Control de Enrutamiento en Recepción
CET	Control de Enrutamiento en Transmisión
CK	Check Bits: Bits para el Chequeo de Error
CLIR	Calling Line Identity Restriction: Restricción de la Identidad de la Línea que Llama
CLIP	Calling Line Identity Presentation: Presentación de la Identidad de la Línea que Llama
CONCR	Control Orientado a no Conexión para Recepción

GLOSARIO (continuación)

CONCT	Control Orientado a no Conexión para Transmisión
COT	Continuity: Continuidad
CPLL	Control para Procesamiento de Llamadas de Llegada
CPLS	Control para Procesamiento de Llamadas de Salida
CR	Control de Recepción
CS	Capability Set: Conjunto de Capacidades
CS-1	Capability Set-1: Conjunto de Capacidades Versión Uno
CS-2	Capability Set-2: Conjunto de Capacidades Versión Dos
CT	Control de Transmisión
DADER	Delimitación, Alineamiento y Detección de Error en la Recepción
DADET	Delimitación, Alineamiento y Detección de Error en la Transmisión
DISCM	Discriminación de Mensajes
DISTM	Distribución de Mensajes
DPC	Destination Point Code: Código del Punto de Destino
EIA	Electronic Industry Association: Asociación de la Industria Electrónica
EM	Enrutamiento de Mensajes
ESN	Electronic Serial Number: Número de Serie Electrónico
ETSI	European Telecommunications Standards Institute: Instituto Europeo de Estandarización en Telecomunicaciones
FE	Functional Entity: Entidad Funcional
FEA	Functional Entity Actions: Acciones de las Entidades Funcionales
FIB	Forward Indicator Bit: Bit de Indicador de Ida
FISU	Fill-In Signal Unit: Unidad de Señalización de Relleno
FPLMTS	Future Public Land Mobile Telecommunication Systems: Sistemas de Telecomunicaciones Públicos Móviles Terrestres del Futuro
FSN	Forward Sequence Number: Número de Secuencia de Ida

GLOSARIO (continuación)

HDLC	High Level Data Link Control: Control del Enlace de Datos de Alto Nivel
GSM	Global System for Mobile Communications: Sistema Global para Comunicaciones Móviles
HLR	Home Location Register: Registro de Localización de Usuarios Locales
IAM	Initial Address Message: Mensaje de Dirección Inicial
IN	Intelligent Network: Red Inteligente
IP	Intelligent Peripheral: Periférico Inteligente
IS-41	Inter-System Protocol: Protocolo para la Interoperabilidad e Interconectividad de Sistemas
ISDN	Integrated Services Digital Network: Red Digital de Servicios Integrados
ISUP	ISDN User Part: Parte del Usuario ISDN
ITU	International Telecommunications Union: Unión Internacional de Telecomunicaciones
ITU-T	ITU-Telecommunications Sector, Sector de Estandarización en Telecomunicaciones
LA	Location Area: Area de Localización
LE	Local Exchange: Oficina Local
LI	Length Indicator: Indicador de Longitud
LSSU	Link Status Signaling Unit: Unidad de Señalización del Estado del Enlace
MIN	Mobile Identification Number: Número de Identificación Móvil
MS	Mobile Station: Estación Móvil
MSC	Mobile Switching Center: Centro de Conmutación Móvil
MSU	Message Signaling Unit: Unidad de Señalización de Mensajes
MTP	Message Transfer Part: Parte de Transferencia de Mensajes
NAP	Network Access Point: Punto de Acceso a la Red

GLOSARIO (continuación)

NMT	Nordic Mobile Telephone: Sistema Telefónico Móvil Nórdico
OPC	Originating Point Code: Código del Punto de Origen
PCS	Personal Communication Services: Servicios de Comunicación Personal
PIN	Personal Identification Number: Número de Identificación Personal
PSTN	Public Switched Telephone Network: Red Telefónica Pública Conmutada
REL	Release: Liberación
RLC	Release Complete: Liberación Completa
RP	Return Point: Punto de Retorno
RT	Redes de Telecomunicaciones
SCC	Subcapa Cordinadora de Componentes
SCCP	Signaling Connection Control Point: Parte de Control de la Señalización de Conexión
SCE	Service Creation Environment: Ambiente de Creación de Servicio
SCP	Service Control Point: Punto de Control de Servicios
SF	Status Field: Campo de Estado
SI	Service Identification: Indicador de Servicio
SIB	Status Identification Busy: Indicación de Estado Ocupado de Servicios
SIF	Signaling Information Field: Campo de Información de Señalización
SLP	Service Logic Programs: Programas de Servicio Lógico
SLS	Signaling Link Selection: Selección del Enlace de Señalización
SL	Signaling Link: Enlace de Señalización
SMDC	Subcapa de Manejo del Diálogo de Componentes
SMS	Service Management System: Sistema de Manejo de Servicio
SN	Service Node: Nodo de Servicio

GLOSARIO (continuación)

SP	Signaling Point: Punto de Señalización
SS7	Signaling System #7: Sistema de Señalización Número 7
SSD	Shared Secret Data: Dato Secreto Compartido
SSN	Sub-System Number: Números de Subsistema
SSP	Service Switching Point: Punto de Conmutación de Servicios
ST	Subcapa de Transacción
STP	Signaling Transfer Point: Punto de Transferencia de Señalización
SU	Signaling Unit: Unidad de Señalización
TACS	Total Acces Communication System: Sistema de Comunicaciones de Acceso Total
TCAP	Transaction Capability Application Part: Parte de Aplicación con Capacidades de Transacción
TE	Transit Exchange: Oficina de Tránsito
TIA	Telecommunication Industry Association: Asociación de la Industria de las Telecomunicaciones
UPT	Universal Personal Telecommunications: Telecomunicaciones Personales Universales
VLR	Visitor Location Register: Registro de Localización de Visitantes
VPN	Virtual Private Network: Red Virtual Privada