

PROTOCOLO DEL GRUPO TRABAJO SIGTRAN (SIGNALING TRANSPORT)
PARA EL TRANSPORTE DE SEÑALIZACIÓN SS7 SOBRE REDES IP

MOYLEE JAY PATRÓN
JESÚS DAVID SEGURA GUTIERREZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
CARTAGENA DE INDIAS, D. C.

2006

1



PROTOCOLO DEL GRUPO TRABAJO SIGTRAN (SIGNALING TRANSPORT)
PARA EL TRANSPORTE DE SEÑALIZACIÓN SS7 SOBRE REDES IP

MOYLEE JAY PATRÓN
JESÚS DAVID SEGURA GUTIERREZ

Monografía de grado para optar el título de
Ingeniero Electrónico

Director

GONZALO LOPEZ VERGARA

Ing. Electrónico

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
CARTAGENA DE INDIAS, D.C.

2006

2



Cartagena de Indias, 29 de junio de 2006

Señores:

COMITÉ DE PROYECTO DE GRADO

Facultad de Ingeniería Eléctrica, Electrónica y Mecatronica.

Universidad Tecnológica de Bolívar

L.C.

Apreciados Señores:

Por medio de la presente me permito hacer la entrega formal de la monografía de grado titulado “PROTOCOLO DEL GRUPO TRABAJO SIGTRAN (SIGNALING TRANSPORT) PARA EL TRANSPORTE DE SEÑALIZACIÓN SS7 SOBRE REDES IP” que será presentado por los estudiantes MOYLEE JAY PATRÓN y JESÚS DAVID SEGURA GUTIERREZ, el cual estuvo bajo mi supervisión como asesor del mismo para optar el titulo de INGENIERO ELECTRÓNICO.

Atentamente,

Ingeniero Electrónico

Director



Cartagena de Indias, 29 de junio de 2006

Señores:

COMITÉ DE PROYECTO DE GRADO

Facultad de Ingeniería Eléctrica, Electrónica y Mecatronica.

Universidad Tecnológica de Bolívar

L.C.

Apreciados Señores:

Hacemos entrega formal de nuestra monografía de grado titulado "PROTOCOLO DEL GRUPO TRABAJO SIGTRAN (SIGNALING TRANSPORT) PARA EL TRANSPORTE DE SEÑALIZACIÓN SS7 SOBRE REDES IP", como requisito para optar el título de INGENIERO ELECTRÓNICO.

Esperamos que éste cumpla con las normas y requerimientos exigidos por la facultad.

Atentamente,

MOYLEE JAY PATRÓN

JESÚS DAVID SEGURA GUTIERREZ



Nota de Aceptación

Presidente del Jurado

Jurado

Cartagena de Indias, 29 de junio de 2006



Dedicado a mis padres, por su grandioso y reconfortante apoyo en todos los pasos que seguí; A mis hermanos que me acompañaron anímicamente en todo momento; y especialmente a mi novia que estuvo en las buenas y en las malas, apoyándome y ayudándome incondicionalmente hasta la culminación de mí grado.



Dedicado a mis padres, por su grandioso y reconfortante apoyo en todos los pasos que seguí; A mis hermanos que me acompañaron anímicamente en todo momento; y especialmente a mi novia que estuvo en las buenas y en las malas, apoyándome y ayudándome incondicionalmente hasta la culminación de mí grado.



JESÚS DAVID SEGURA GUTIÉRREZ

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Gonzalo López Vergara, Ingeniero Electrónico y Director del proyecto, por su constante ayuda y apoyo incondicional.

A los Ingenieros (profesores) que nos colaboraron en el transcurso del mainor, por su invaluable colaboración a lo largo de la ardua ejecución del presente proyecto. Por brindar sus conocimientos sin restricciones y su inestimable esfuerzo porque este proyecto se llevar a feliz termino.

Todos los que participaron con su ayuda tanto material como moral. Que con su apoyo y ánimo no permitieron que decayera. Y a muchos de los que aportaron un poquito con su experiencia, trabajo y conocimiento.



CONTENIDO

	Pág.
JUSTIFICACIÓN	
INTRODUCCIÓN	
1. OBJETIVOS	1
1.1 OBJETIVO GENERAL	1
1.2 OBJETIVOS ESPECÍFICOS	1
2. SEÑALIZACIÓN SS7	2
2.1 ARQUITECTURA DE PROTOCOLO SS7	4
2.2 TIPOS DE NODOS SS7	8
2.3 ENLACES DE SEÑALIZACIÓN SS7	11
3. TELEFONÍA IP	14
3.1 IMPORTANCIA DE LA TELEFONÍA IP	15
3.2 PROBLEMAS QUE ENFRENTA LA TELEFONÍA IP	18
3.3 COMPARACIÓN ENTRE LA TELEFONÍA IP Y LA TRADICIONAL	18
3.4 SEÑALIZACIÓN EN LA TELEFONÍA IP	22
4. SIGTRAN	24
4.1 FUNCIONALIDADES DE LOS PROTOCOLOS SIGTRAN	25
4.2 LIMITACIONES DE TCP Y UDP	26
4.3 ARQUITECTURA SIGTRAN	26
5. SCTP	29
5.1 COMPARACIÓN ENTRE SCTP Y LOS PROTOCOLOS TCP	31
5.2 PRINCIPALES CARACTERÍSTICAS DE SCTP	34
5.3 PAQUETE SCTP	41



5.3.1 Cabecera Común	43
5.3.2 Tipos de Chunks	43
5.3.3 Etiqueta de Verificación	47
5.3.4 Datos de usuario	47
5.3.5 Checksum	47
6. CAPAS DE ADAPTACIÓN SIGTRAN	48
6.1 M2UA	48
6.2 M2PA	49
6.3 M3UA	50
6.4 SUA	51
6.5 IUA	52
CONCLUSIONES	53
GLOSARIO	57
BIBLIOGRAFÍA	
ANEXO1.	



LISTA DE FIGURAS

	Pág.
Figura 1. Señalización dentro de banda	3
Figura 2. Señalización fuera de banda	3
Figura 3. Arquitectura de Protocolo SS7	5
Figura 4. Nodos de la red SS7	8
Figura 5. Tipo de Enlaces SS7	12
Figura 6. Red Telefónica Tradicional	14
Figura 7. Red Telefónica IP	15
Figura 8. Incremento de ingresos y trafico en el periodo 1998—2002	17
Figura 9. Arquitectura Sistemas Multimedia del IETF	20
Figura 10. Arquitectura de protocolo SIGTRAN	27
Figura 11. Arquitectura detallada de Protocolo SIGTRAN	28
Figura 12. SCTP orientado a mensaje Vs TCP orientado a bits.	33
Figura 13. Multihoming en SCTP	38
Figura 14 Multistreaming en SCTP	42
Figura 15 Iniciación SCTP y TCP	42
Figura 16 Estructura generalizada de paquete SCTP	
Figura 17 Estructura detallada de Paquete SCTP	



Figura 18	Arquitectura M2UA	48
Figura 19.	Transporte de MTP3 a MTP2 remoto, mediante M2UA.	48
Figura 20.	Arquitectura M2UA	50
Figura 21.	Arquitectura M3UA.	51
Figura 22.	Arquitectura acostumbrada de SUA.	52



LISTA DE TABLAS

	Pág.
Tabla 1. Comparación telefonía IP Vs Telefonía tradicional	18
Tabla 2. Comparación entre SCTP, TCP y UDP	34
Tabla 3. Resumen Características del Protocolo SCTP	40
Tabla 4. Tipos de chunks definidos en SCTP	44



ARTICULO 105 DEL REGLAMENTO ACADÉMICO

La institución se reserva el derecho de propiedad intelectual de todos los Trabajos y Monografías de Grado Aprobados, los cuales no pueden ser explotados comercialmente sin su autorización.



JUSTIFICACIÓN

Cada vez se hace mayor la necesidad de integrar las redes de voz y datos, es por eso que el crecimiento del tráfico de datos en el mundo es mucho mayor que el crecimiento del tráfico de voz. Esto conlleva a que dentro de muy poco tiempo el tráfico de voz será insignificante comparado con el volumen de datos que se transporta en la red. Sin embargo cerca del 80% de los ingresos de las empresas de telecomunicaciones provienen de servicios de voz.* (GRUPO YANKEE). Esta situación realza aun más la importancia y la necesidad de la telefonía sobre las redes IP, por consiguiente cualquier proveedor que tenga aplicaciones sobre el Internet puede ofrecer a sus usuarios el servicio de telefonía de larga distancia sobre IP, utilizando las redes ya existentes.

Aunque la telefonía IP aun no constituye un porcentaje muy convincente o sustancial del volumen de tráfico telefónico en todo el mundo, este se esta expandiendo rápidamente debido a los beneficios que contribuiría la implementación de este tipo de tecnologías, al utilizar una misma red para transmitir voz y datos, las empresas de telecomunicaciones reducen sustancialmente los costos de funcionamiento, mantenimiento y a futuro los costos de implementación. Además de hacer un uso más eficiente de estas redes, se vería reflejado en una disminución bastante considerable en las tarifas que pagan los usuarios. Por este motivo es de crucial importancia conocer y estudiar las nuevas tecnologías encaminadas a permitir la integración de las redes de voz y datos, los protocolos que se han implementado y los que pueden ser implementados en el futuro.



El gran reto de la telefonía IP es brindar una calidad de servicio similar a la ofrecida por las redes telefónicas convencionales, siendo la señalización uno de los aspectos más cruciales e importantes para alcanzar este objetivo. Teniendo en cuenta que la señalización más utilizada en las redes actuales de la telefonía de voz conmutada es el protocolo SS7, por todas sus características que lo hacen un protocolo de señalización confiable. Por eso es imprescindible el desarrollo de estándares que permitan implementar este protocolo de señalización sobre redes IP, como un protocolo de señalización para la telefonía IP, igualmente es importante conocer y estudiar los diferentes protocolos y estándares desarrollados para este fin.



INTRODUCCIÓN

Se puede ver claramente que la red telefónica actual es el sistema más complejo que dispone el hombre, el cual permite hacer una llamada instantáneamente desde cualquier parte del planeta a otro pero el surgimiento de los datos creo una red mucho mas gigantesca y por ello surgió la necesidad de integrar las redes telefónicas y las redes de computadores. Desde este momento comienza a cobrar importancia la convergencia de voz en las redes de datos, estas redes son capaces de transportar información de diferente índole, como la voz digitalizada, mensajes, email, música, video en tiempo real, transacciones bancarias, compras, etc. En realidad infinidad de operaciones en base a datos propiamente dichos.

La posibilidad de tener una sola red para trasportar voz y datos, beneficia a los operadores de telefonía por que reducen los costos en sus operaciones de administración, mantenimiento y el manejo de la información. El protocolo de tecnología IP se presenta como la plataforma idónea para la convergencia de todas tecnologías de transmisión de voz y datos, debido a los avances agigantados de la demanda de mejores servicios y la masificación de la Internet.

Para un servicio de voz sobre redes IP, es muy importante mantener la misma calidad y disponibilidad de la telefonía tradicional conmutada. Para esto es importante un elemento que hace posible mantener esta condición, el cual no es más que la señalización de la telefonía tradicional el proveedor. La



señalización ha existido desde el principio de la telefonía, y es tan importante como la conmutación misma y el transporte de la voz.

El grupo de trabajo de señalización (Signaling Transport, SIGTRAN), de La Fuerza de Trabajo Transporte de Ingeniería de Internet (Internet Engineering Task Force, IETF) es el encargado de producir los estándares necesarios para hacer posible la integración de las redes de voz y datos. El propósito fundamental de este grupo es encargarse del transporte de señalización de Redes Públicas Telefónicas Conmutadas (Public Switched Telephone Networks, PSTN) basadas en conmutación de paquetes sobre redes IP, teniendo en cuenta las características fundamentales para el transporte de dicha señalización.

El objetivo de esta investigación es ofrecer una completa descripción de las características generales, alcance y fundamentos de los protocolos del grupo de trabajo SIGTRAN, para el transporte de la señalización SS7 sobre redes IP.

En esta monografía se hará un repaso por los conceptos básicos de las redes telefónicas, su evolución y su respectiva señalización.

Lo más importante en una red de transporte de señalización es la fiabilidad y calidad de transmisión. Dado que esta red transporta y controla de todas las comunicaciones actuales, un fallo en ella podría suponer la indisponibilidad de gran parte de la red mundial y pérdidas económicas sustanciales que no competen a las que produciría un fallo en un nodo de transporte de tráfico de un país.

Seguidamente se aborda el tema principal de esta tesis, el Protocolo de Transmisión de Flujo de Control (Stream Control Transmission Protocol, SCTP). Es un protocolo de capa de transporte definido por IETF, se estudiarán sus funciones, características y componentes. Además se sustentan las razones por la cual se hizo necesario la creación de dicho protocolo, haciendo una comparación



con otros protocolos de capa de transporte como el TCP y UDP utilizados para el transporte de datos en Internet.

También se discute sobre la forma en que SCTP realiza la transmisión de los datos, así mismo se estudia el mecanismo que SCTP utiliza para evitar la congestión en la red, la forma en que SCTP realiza los cálculos de la Máxima Unida de Transferencia (Maximun Transfer unit, MTU), el Tiempo de Espera de Retransmisión (Retransmission Time-Out).

Y por ultimo se hablara sobre las aplicaciones que utiliza el protocolo de trasporte SCTP, y los cambios en las especificaciones que puede tener este SCTP



1. OBJETIVOS

1.1 OBJETIVO GENERAL

Brindar una descripción detallada de los nuevos protocolos y estándares desarrollados por el grupo de trabajo SIGTRAN para el transporte de información de señalización SS7 sobre redes IP, con el fin de conocer y entender los conceptos fundamentales y diferencias significativas entre los protocolos de transporte SCTP y TCP/UDP. Para que la comunidad académica tenga un complemento académico con respecto al estudio de las nuevas tecnologías para la implementación de telefonía IP.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar una investigación en las diferentes fuentes de información acerca del tema en todos los medios disponibles. Con el fin de seleccionar los aspectos mas importantes para su descripción y análisis.
- Elaborar un documento donde se consigne las principales características encontradas sobre los protocolos y estándares del grupo de trabajo SIGTRAN.
- Realizar un estudio detallado de los aspectos principales del protocolo de transporte SCTP, para lograr una completa comprensión del mismo.



- Realizar un análisis de las tendencias futuras en la utilización del protocolo SCTP como protocolo de transporte para nuevos servicios. Sobre redes IP.

2. SEÑALIZACIÓN SS7.

La señalización ha existido desde el principio de la historia del teléfono y se utiliza para establecer, mantener y colgar una llamada telefónica, así como información que permita la tarificación y servicios especiales como identificador de llamadas, numero gratuitos 01800, etc.

Los protocolos de Señalización por Canal Común No.7 fueron desarrollados por AT&T a partir del año 1975 y definido como estándar por la UIT- T (Unión Internacional de Telecomunicaciones-Sector de normalización de telecomunicaciones.) en 1981 en la serie de recomendaciones Q.7xxx del UIT-T.

El Sistema de Señalización SS7 es un medio que utilizan los elementos de la red de conmutación para intercambiar información. Esta información se transporta en forma de mensajes. Los mensajes SS7 transportan información relativa a establecimiento y liberación de llamadas. Además, en las redes de telefonía móvil también transportan información de localización del usuario, así como mensajes de texto de usuario (SMS).

Actualmente el sistema de señalización No. 7 (SS7) es el estándar internacional de la señalización telefónica. Este fue emitido por el Comité Internacional Consultivo de Telegrafía y Telecomunicaciones (UIT-T) y el Comité Consultivo Internacional



Télégraphique et Téléphonique, CCITT) in 1980, con una revisión cada cuatro años.

SS7 se diseña para ser una norma de señalización de canal común abierta que pueda ser utilizada para trabajar en una gran variedad de redes digitales. Su propósito global es proporcionar un sistema de señalización de canal común de uso general estandarizado internacionalmente con las siguientes características: Mantiene un medio fiable para el transporte de información sin pérdida ni duplicación de datos. Perfeccionado para el uso en comunicaciones digitales con canales de 64Kbps, sin embargo también es conveniente para trabajar con canales analógico. Fue diseñado para cumplir con requerimientos presentes y futuros de transferencia de información de control.

Antes de la señalización No.7 existieron otros tipo de señalización en la cual se utilizaba el mismo canal para la información de control y la señal de voz, esto se llamaba señalización dentro de banda o señalización por canal asociado, ya que la información del establecimiento de la llamada eran enviadas a través de de tonos especiales por las líneas telefónicas, esto ocasionaba una gran cantidad de problemas de seguridad. En la figura 1 se muestra una grafica de este tipo de señalización.



Figura 1. Señalización dentro de banda



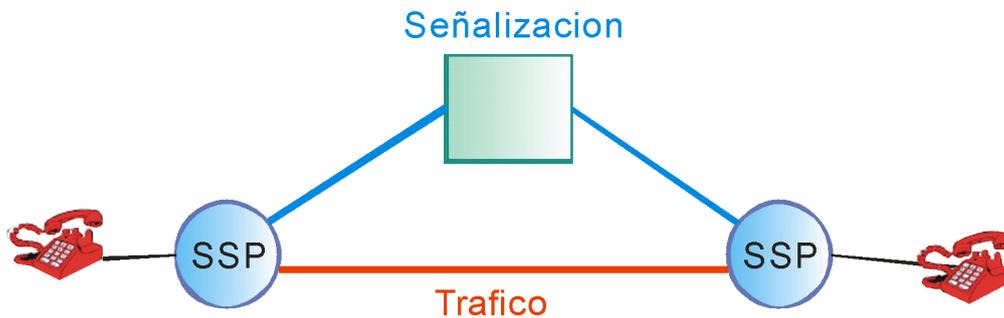


Figura 2. Señalización fuera de banda

SS7 trabaja con señalización fuera de banda, utilizando un canal de señalización separado del canal de voz y es clasificado como señalización por canal común (CCS) o Common Channel Interoffice Signalling Systems (CCIS) ya que separan la señal de señalización de los canales portadores. Este requiere de un canal separado dedicado exclusivamente a señalización, como se muestra en la figura 2.

SS7 fue diseñada para redes digitales y centrales con control por programa almacenado, para aplicaciones como la red de telefonía fija, red de telefonía móvil y red inteligente.

El sistema SS7 consiste básicamente en una red de transporte de mensajes cuyos usuarios son nodos de conmutación. Esta red de transporte de señalización es paralela a la red de conmutación que forman los nodos que la utilizan, y su topología es, en general, completamente diferente.

2.1 ARQUITECTURA DEL PROTOCOLO SS7

El protocolo SS7 se divide en capas y guarda similitud con el modelo de referencia OSI, alguna de las funciones requeridas en el modelo OSI no tienen ningún propósito en la red SS7 ya que este protocolo fue creado para requerimientos específicos, por esta razón existen muchas diferencias entre los dos modelos. Los



tres niveles mas bajos del modelo SS7 se ocupan de la Parte de Transferencia de Mensaje (Message Transfer Part, MTP), estos se encargan de llevar de forma fiable un mensaje desde el origen al destino, a través de la red SS7, realiza las funciones de transporte de las capas inferiores, selección del enlace de señalización, detección y corrección de errores, conexión física. Las MTP guardan mucha similitud con las tres primeras capas del modelo OSI, sin embargo no proporciona todas las funciones y servicios especificados en las capas 1, 2 y 3 del modelo OSI. Esta arquitectura se muestra en la figura 3.

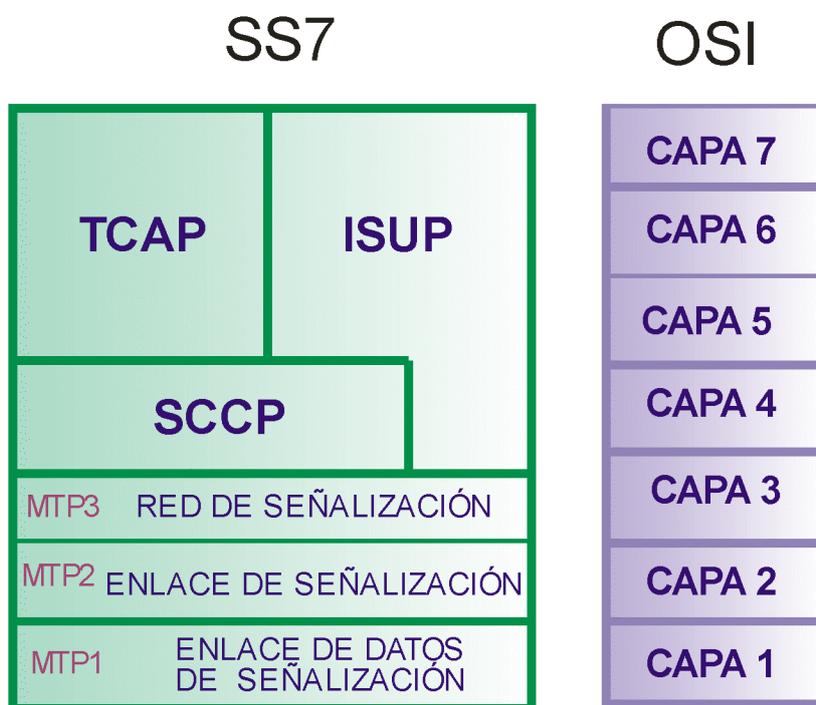


Figura 3. Arquitectura de Protocolo SS7.

MTP Nivel 1 (MTP1). Es el nivel físico de SS7, en general, en las redes SS7 tradicionales los enlaces de señalización se implementan mediante transmisión TDM (Multiplexación por División en el Tiempo) utilizando canales de 64 kbps dentro de tramas punto a punto de 2 Mbps (E1 normalizados).



Entre dos nodos de una red SS7 se pueden definir como máximo 16 canales, pero en la práctica no se suelen implementar más de 8.

MTP de nivel 2 (MTP2). Esta capa se encarga de todas las tareas de nivel de enlace, de forma que se asegura que entre los dos extremos de un enlace de señalización se pueden intercambiar mensajes de forma fiable. Estas tareas son:

- Sincronismo de enlace.
- Monitorización de tasa de errores.
- Generación y comprobación de códigos de redundancia cíclica (CRC) y números de secuencia de MSUs.
- Gestión de colas de entrada y salida de MSUs y monitorización de congestión.
- Transmisión, recepción y reenvío en caso de error de MSUs.

MTP nivel 3 (MTP3). Este es el nivel mas importante de la red SS7. El MTP3 es el encargado de proveer conectividad entre todos los nodos de la red, de forma que asegura que dos nodos puedan intercambiar mensajes de señalización, independientemente de si están directamente conectados o no. Las funciones de este nivel son:

- Identificación de todos los nodos de la red.
- Encaminamiento y reenvío de mensajes, y reparto de carga entre varios enlaces.



- Gestión del estado de enlaces.

El nivel cuatro de SS7 se encuentra la Parte de Control de Conexión de Señalización (Signaling Connection Control Part, SCCP). El SCCP y el MTP juntos forman la Parte de Servicio de Red (Network Service Part, NSP).

SCCP contiene funciones de transporte de alto nivel necesarias para soportar partes de aplicación de alto nivel. Proporciona funciones de encaminamiento, servicios orientados a conexión y no orientados a conexión. También se ocupa de la gestión de bases de datos duplicadas. Permite que los mensajes sean utilizados por subsistemas, que son aplicaciones independientes dentro de un nodo, por ejemplo llamadas 018000, llamadas con tarjetas y redes inteligentes avanzadas. Tiene la capacidad de discriminar aplicaciones dentro de un nodo con un único punto de señalización.

Mas arriban de SCCP se encuentra la Parte de Aplicación de Capacidades de Transacción (Transaction Capabilities Application Part, TCAP) y Integrated Services Digital Network - User Part (ISDN-UP).

TCAP soporta la transferencia de información que no está asociada con el circuito de control, por ejemplo la petición/respuesta de la base de datos tipo 01800. Esta define los mensajes y el protocolo utilizado en los nodos para comunicarse entre aplicaciones.

ISUP se encarga del establecimiento y liberación de llamadas de voz y datos sobre redes de conmutación de circuitos de 64 kbps. Para ello gestiona en cada tramo de la llamada la toma de enlace, y su correspondiente liberación posterior, dentro de las tramas disponibles entre centrales de conmutación de voz. Los mensajes ISUP se transportan directamente sobre el MTP-3.



El protocolo OMAP (Operations Maintenance Administration Part) se ocupa de las prestaciones, monitorización, encaminamiento y verificaciones. Esta capa es paralela a todas las demás capas SS7.

Además de los protocolos antes mencionados también se encuentran otros protocolos que hacen parte de SS7, como Telephone User Part (TUP), Broadband ISDN User Part (BISUP), Data User Part (DUP).

2.2 TIPOS DE NODOS SS7

La arquitectura de la red SS7 esta formada por nodos y diversos tipos de enlaces de señalización (Signaling Link, SL) que están configurados de forma que aporten la máxima confiabilidad al sistema. Cada uno de los nodos se conoce como Punto de Señalización (Signaling Point, SP) y es identificado por una o más direcciones o Códigos de Punto de Señalización (Signaling Point Code, SPC) de 14 bits . Estos puntos de señalización se interconectan entre si por enlaces de transmisión.

Existen tres niveles de redes de señalización: red de señalización internacional, nacional e interna.

La arquitectura de red SS7 consiste en un conjunto interconectados que intercambian información de señalización. Existen diferentes tipos de nodos y puntos de señalización, los cuales se muestran en la figura



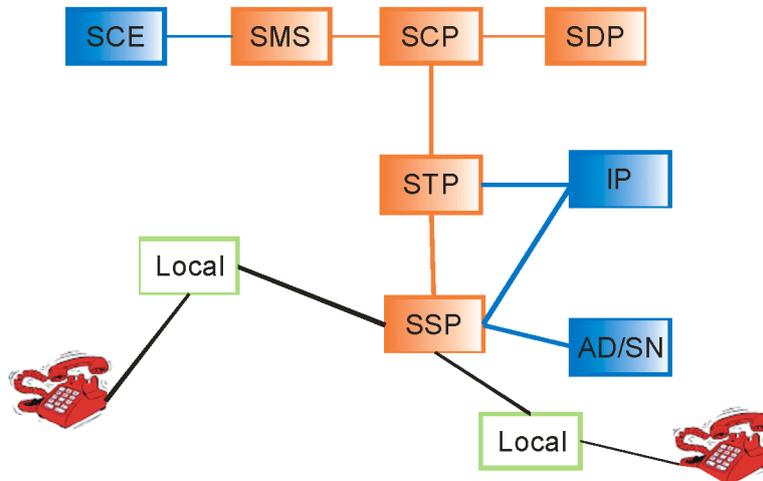


Figura 4. Nodos de la red SS7.

- Punto de Transferencia de Señal (Signal Transfer Point, STP): Proporciona servicio de enrutamiento en la red de forma ininterrumpida. Estos se encargan de recibir y dirigir los mensajes de señalización hacia el destino correcto basándose en la información del propio mensaje o bien en información almacenada en tablas de enrutamiento. Los STPs siempre se configuran en parejas exactamente iguales. Todos los nodos que se conectan a un STP, también se conectan al otro STP de la pareja, formando una red redundante. Pueden realizar funciones de gateway para transferir mensajes de señalización a otras redes de señalización SS7. También son responsables del acceso a bases de datos. Cada número concreto accede a un servicio diferente. Existe una tabla en cada STP que indica para cada número el SCP y el enlace que se debe utilizar para enviar el mensaje.

- Punto de Conmutación de Servicio (Service Switching Point, SSP). Dispone de software especial para proporcionar servicios de red inteligente (Advanced Intelligent Network, AIN). Son centros de conmutación equipados para manipular señalización troncal así como señalización de servicios o servicios de



transacciones con las bases de datos dentro y fuera de la red. También transfieren mensajes SS7 a otros puntos de señalización dentro de la red.

- Punto de Control de Servicio (Service Control Point, SCP). Tienen capacidades para tomar decisiones. Los SCPs contienen programas lógicos de servicios que reflejan los servicios de clientes y que interactúan con SSP para gestionar decisiones en el procesado de llamadas. Por lo tanto mediante los SCP se implementan los servicios de telefonía que necesiten un procesamiento avanzado de las llamadas. En otras palabras son bases de datos multifuncionales, centralizadas, on-line, que almacenan datos de clientes y lógica de servicio para responder a peticiones procedentes de SSPs. Estos nodos intercambian señalización de control de llamada con las centrales de conmutación, y en ellos se implementa la lógica del servicio. Este tipo de servicios se conoce también con el nombre de Red Inteligente. Dependiendo de la importancia del servicio al que atienden, los SCPs se pueden configurar como parejas redundantes, del mismo modo que los STPs.

- Punto de datos del servicio (Service Data Point, SDP): son nodos independientes que contienen base de datos común para los diferentes SCP utilizados para implementación de servicios de red inteligentes de forma masiva. Este tipo de servicios se distribuye entre diferentes SCP, para distribuir la carga total del proceso y utilizan una base de datos común.

La base de datos del SDP se puede distribuir físicamente en varios nodos en forma de bases de datos de millones de registros y frecuencias de acceso elevadas para mayor facilidad de implementación.

Además de los nodos mencionados también se encuentran otros elementos en una red SS7, como son:



- Sistema de Gestión de Servicio (Service Management System SMS). Realiza funciones de mantenimiento, administrativas y de provisión para los SCPs. También realiza la función de creación de servicios.

- Periférico inteligente (Intelligent peripheral, IP). Añaden funciones de comprensión a la red tales como reconocimiento de voz, síntesis y anuncios de voz específicos.

- Entorno de creación de servicios (Service Creation Environment SCE).

- Adjunto. (Adjunct AD). Son nodos que se conectan a los SSPs y que realizan las mismas funciones que SCPs.

- Nodo de servicios (Services Node, SN).

2.3 ENLACES DE SEÑALIZACIÓN SS7.

Los enlaces de señalización (SL) conectan todos los nodos de la red SS7. Cada enlace se administra de forma diferente según los nodos a los que conecta. Son enlaces síncronos bidireccionales a 64 Kbps (56 Kbps en U.S.)

En SS7 cada enlace de su grupo de enlaces se identifica con un Código de Enlace de Señalización (Signaling Link Code, SLC).



Los enlaces de señalización se clasifican de acuerdo a la función que realizan en la red telefónica, básicamente existen en laces A, B, C, D, E y F, los cuales se muestran en la figura 5.

Los enlaces A también se denominan Enlaces de Acceso, estos se refieren a los enlaces que unen puntos terminales de señalización, conectan centrales entre sí y/o tándems de acceso y SCPs. Cada nodo se conecta como mínimo con un par de nodos jerárquicos (superiores e inferiores) para mayor fiabilidad.

Cada SCP suele tener un mínimo de tres enlaces y un máximo de cinco enlaces a cada par de STPs a los que está conectado.

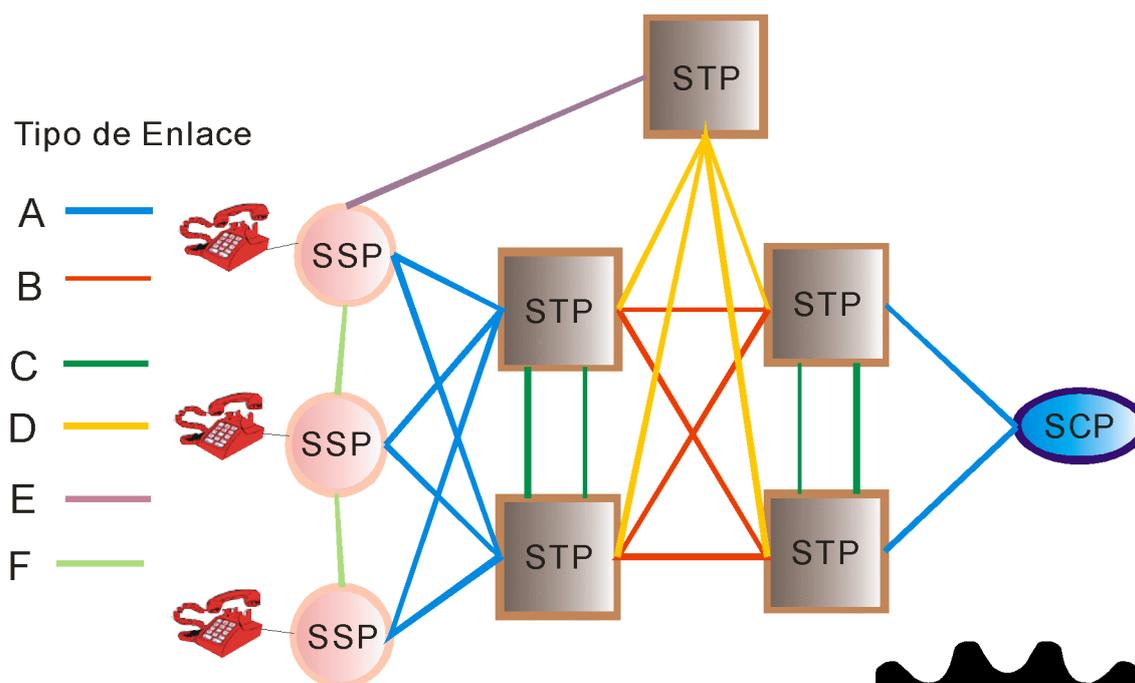


Figura 5. Tipo de Enlaces en SS7

Los enlaces B (o enlaces puente) se establecen entre pares de STPs en el mismo nivel jerárquico. Estos tienen como función llevar los mensajes de señalización



mas allá del área descrita por su red. Este tipo de enlace forma un puente entre dos STPs que no forman un par.

Los enlaces C o Enlace Cruzado (Cross Links), son los que conectan pares de STPs juntos o sea STPs que forman un par. La principal función de los enlaces C es llevar mensajes de gestión de red. Se utilizan para garantizar la fiabilidad de la arquitectura, en el caso en que uno o más enlaces de otro tipo no se encuentren disponibles.

Los enlaces D o Enlaces en diagonal conectan STPs de diferentes niveles jerárquicos. Generalmente se disponen con al menos tres rutas alternativas. Cada conjunto de enlaces tiene un máximo de ocho enlaces.

Los enlaces E o Enlaces Extendido (Extended Linls) conectan SSPs a STPs diferentes del par asociado originariamente. Un mínimo de uno y un máximo de 16 enlaces E se utilizan desde cada SP/SSP para conectar a sus compañeros STPs en una nueva área de servicio.

Los enlaces F o Enlaces Totalmente Asociados (fully associated links) se conectan directamente entre SSPs siempre que no hayan STPs. Permiten únicamente una señalización asociada. Como máximo se utilizan 16 enlaces y no hay conexión a nodos inteligentes de la red.



3. TELEFONÍA IP

Los sistemas de comunicaciones y computadores han evolucionado muy rápidamente, siendo el servicio de telefonía fundamental en el desarrollo del vivir cotidiano de cualquier compañía. Debido a todos los desarrollos de los sistemas informáticos y del Internet, se ha llegado a la convergencia entre las redes de computadores y las redes de telefonía. Aprovechando la estructura del protocolo de Internet y los bajos costos de las comunicaciones a través de Internet se plantea la conveniencia de utilizar el Internet como plataforma para la transmisión de voz, como soporte a las comunicaciones telefónicas, tanto la telefonía fija como la telefonía móvil.

Para tener éxito las redes telefónicas IP debe adaptarse a las redes telefónicas tradicionales. En la figura 6 se muestra la arquitectura básica de una red telefónica tradicional, basada en centrales de conmutación de circuitos. En la figura 7 se muestra la arquitectura básica de una red telefónica basada en IP, donde se utilizan Gateway como interfaces entre las centrales de conmutación de circuito y la red IP.

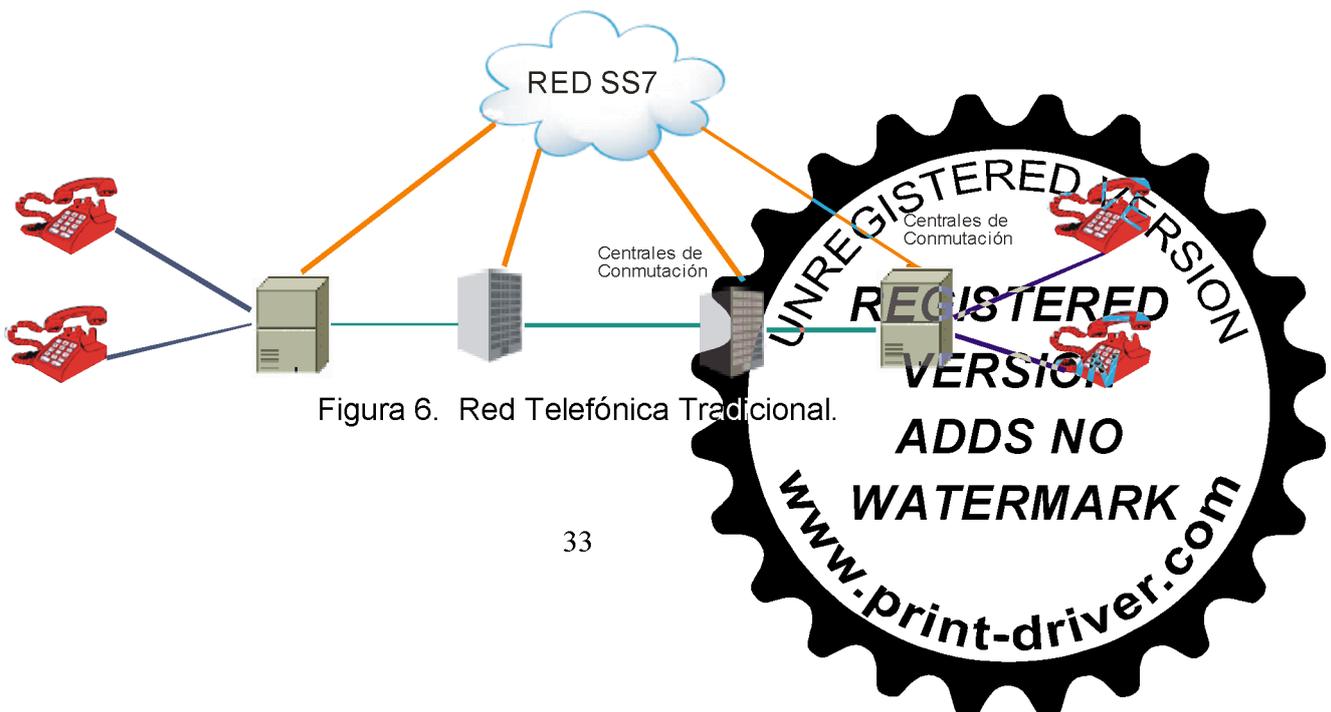


Figura 6. Red Telefónica Tradicional.

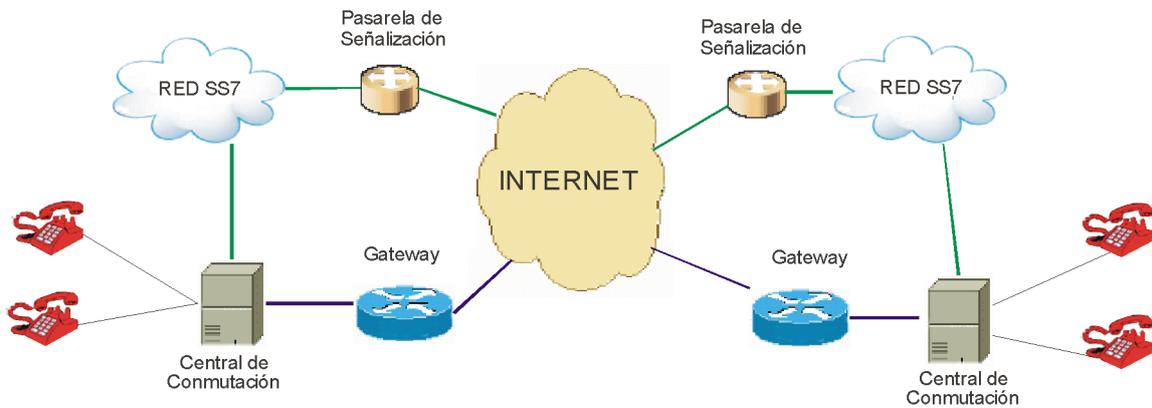


Figura 7. Red Telefónica IP.

3.1 IMPORTANCIA DE LA TELEFONÍA IP

Durante los últimos años la telefonía sobre IP (VoIP), se ha convertido un tema de mucho interés y debates. La proporción del número global de llamadas telefónicas por IP está aumentando significativamente. Este interés se debe a diferentes factores como son:

- La red con conmutación de circuitos se diseñó y optimizó con el objetivo de ofrecer un solo producto, canales de voz dúplex entre puntos con conmutación de 4 kHz (canales digitales de 64 kbit/s).
- Las ráfagas de datos pueden ser transportadas de una manera más eficaz utilizando paquetes de información que pueden intercalarse en función del tiempo en una red con otros paquetes que estén siendo transportados entre otras fuentes y destinos.

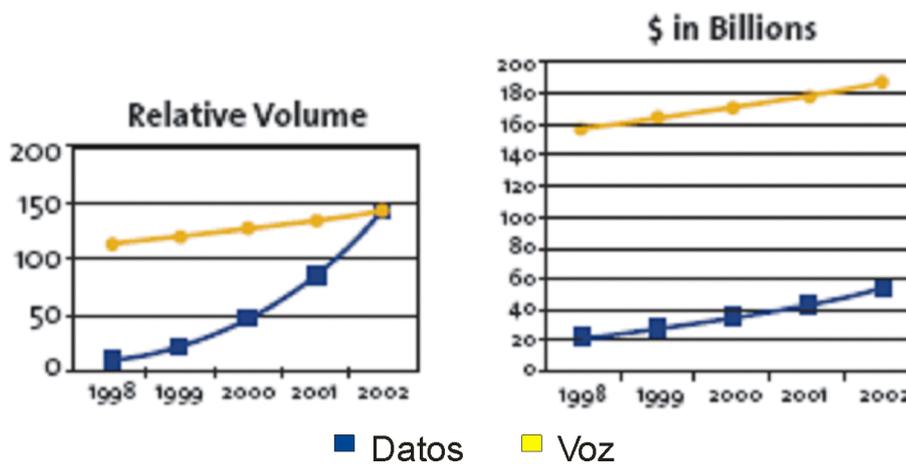


- El Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force, IETF) y otros organismos han realizado trabajos importantes orientados a ofrecer capacidades en tiempo real o casi real utilizando el protocolo IP, que permite transportar la voz por este protocolo empleando la gama de codificación vocal. Los operadores han estado introduciendo productos que integran estos protocolos y que cumplen la calidad de servicio necesaria para satisfacer a sus clientes.
- La flexibilidad para transportar una diversidad de trenes de información de usuario, es decir, velocidades binarias constantes y variables, distintas velocidades, etc., permite que las redes con conmutación de paquetes evolucionen hacia una red integrada para una amplia gama de aplicaciones. Una red integrada (con conmutación de paquetes) puede reducir los costos de funcionamiento y mantenimiento con respecto a los costos asociados con varias redes superpuestas.
- Las redes basadas en IP pueden aprovechar las mismas facilidades de transporte de capas más bajas subyacentes, es decir, pares metálicos trenzados, cable, medios inalámbricos, fibra óptica o satélite.
- La evolución a las redes basadas en IP puede lograrse de una forma económica mediante la instalación de conmutadores de paquetes basados en IP que pueden conectarse mediante las facilidades de transporte existentes.

Todos estos factores hacen que las empresas de telefonía basadas en IP puedan ofrecer un servicio a costos considerablemente menores a los que se pueden permitir al utilizar las redes telefónicas convencionales.



Además, según datos estadísticos el tráfico de datos es mayor que el tráfico de voz, así mismo crece exponencialmente mientras que el tráfico de voz crece de forma lineal (esto se muestra en la grafica de la figura 8). Esta situación contrasta con el hecho de que las principales ganancias económicas de las empresas de telecomunicaciones provienen en su gran mayoría del tráfico de voz, generando un interés especial en la integración de voz sobre la infraestructura ya existente, lo cual permitiría mejores servicios a sus clientes y mayores ingresos para las empresas. Esto se muestra en la grafica de la figura 8, presentada por The Yankee Group, donde se muestra el incremento del tráfico de Datos y voz contra los ingresos generados por cada uno de estos a nivel mundial.



Fuente: The Yankee Group

Figura 8. Incremento de ingresos y tráfico en el período 1998-2002

Los beneficios que implica la implementación de redes de telefonía sobre IP no solo son favorables a las redes alámbricas sino que también favorecen a redes móviles inalámbricas, donde el advenimiento de la tercera generación implica la transición de la conmutación de circuitos a la conmutación de paquetes para convergencia de servicios.



3.2 PROBLEMAS QUE ENFRENTA LA TELEFONÍA IP

El mayor problema al cual se enfrenta la telefonía sobre IP, es que no puede ofrecer la misma calidad de servicio de la Red Publica Conmutada (Public Switched Telephone Network, PSTN). En el sistema de telefonía tradicional cuando se establece una llamada telefónica se reserva un circuito exclusivo para una llamada específica, durante el tiempo de duración de la llamada. La telefonía IP no hace una reserva exclusiva de cualquier recurso, esta enlaza la llamada a través de la red como un simple flujo de datos.

En la telefonía IP el portador de larga distancia es remplazado por una red IP como Internet, convirtiendo una llamada de larga distancia en dos llamadas locales, así el proveedor de servicio de telefonía IP (IP Telephony Service Provider, ITSP) puede ofrecer el servicio a costos mucho mas bajos, ya que el costo de transportar la voz por IP son mucho mas baratos que con la PSTN.

3.3 COMPARACIÓN ENTRE LA TELEFONÍA IP Y LA TRADICIONAL

Existen algunas diferencias entre la telefonía IP y las PSTN, las cuales dificultan el uso de redes IP como medio para transportar voz.

Descripción	PSTN	Internet
Diseñado para	Solo Voz	Paquetes de datos
Ancho de Banda designado	64Kbps dedicado	Ancho de banda totalmente utilizado durante un periodo de tiempo.



Entrega	Garantizada	No garantizada
Retrazo	Depende de la distancia	No predecible (normalmente mayor que en PSTN)
Coste del servicio	Cargo por minuto: la llamada de larga distancia genera facturación mensual.	Un solo cargo mensual
Calidad de la Voz	Alta calidad	Depende mucho del equipo y la conexión del cliente
Calidad del servicio	Entrega en tiempo real	No hay entrega en tiempo real.
servicio	especializado	Multiservicio
Inteligencia	En la red	Mayor inteligencia en los equipos terminales
Inclusión de nuevos servicios	La tecnología condiciona la introducción de nuevos servicios	Tecnología subordinada al servicio

Tabla 1. Comparación telefonía IP vs telefonía tradicional

Una de las mayores diferencias es la calidad del servicio (QoS) que se proporciona. Mientras que las PSTN se diseñó para ser una red muy confiable en el que rara vez se presenta pérdida de información o retardos. El QoS ofrecido por VoIP es muy dependiente de la congestión de la red y surge de las consideraciones técnicas específicas de la transferencia de datos en el modo de las redes IP y, por otro lado, de las consideraciones relacionadas con la organización y el modo de prestación del servicio por las redes de datos en general y por la red IP en particular.



Cuando se trata con la QoS para el servicio de voz, el interés principal tiende a ser en el tren de portadores, ya que esto es lo que generalmente afectará a un abonado. Los demás componentes como la señalización y control o la OAM son igualmente importantes en lo que toca a la QoS general del servicio. Pero no todos estos componentes del servicio de voz IP requieren la misma QoS ya que cada uno puede tener diferentes necesidades de servicio de datos. De allí que el IETF enunció el paradigma de Servicios Diferenciados en el marco IP Diff-Serv ((IETF RFC 2475) (Informativo).

El IETF y otros organismos han realizado trabajos y esfuerzos importantes orientados a ofrecer capacidades de comunicación en tiempo real sobre redes IP. El IETF ha trabajado en la creación de protocolos que garanticen un adecuado QoS de manera equivalente a la de la PSTN.

La arquitectura del IETF, para sistemas multimedia, se constituye de un grupo de protocolos independientes, y cada uno funciones complementarias. La figura 9 muestra los protocolos que hacen parte de esta arquitectura.

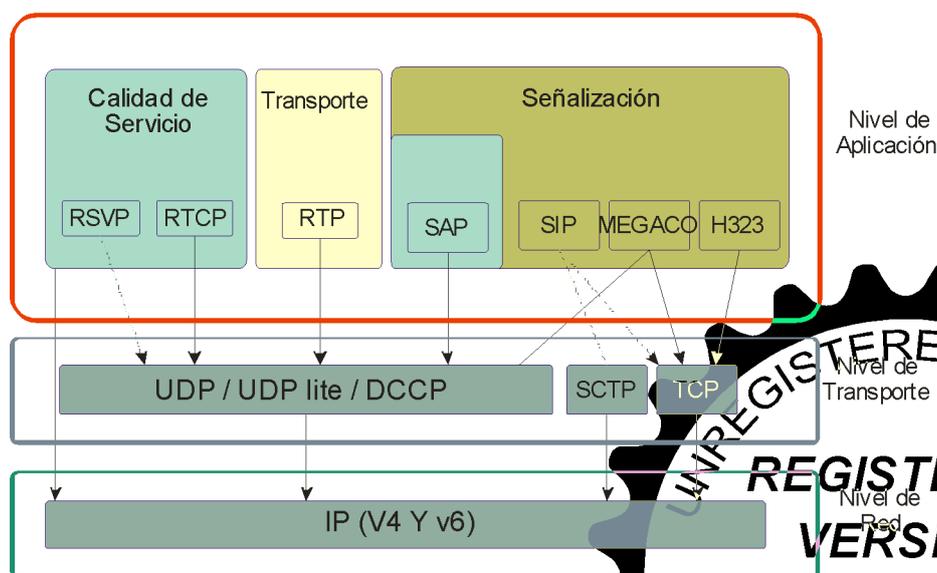
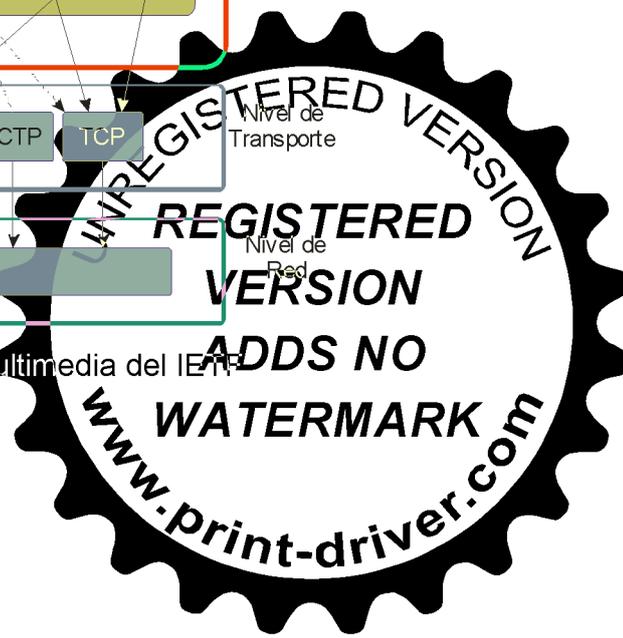


Figura 9. Arquitectura Sistemas Multimedia del IETF



Entre los protocolos y métodos definidos por la IETF para tal fin se encuentran:

- Sobre aprovisionamiento de red para LAN conmutadas corporativas puede no ser económicamente viable.
- Refuerzo de la calidad (PSTN del IETF), centrada en la aplicación, sin repercusión en la red, gestión de control de admisión/tráfico.
- Prioridades (por ejemplo, en la cola de los recursos, DiffServ).
- Reservación de recursos (RSVP, IntServ).
- Ingeniería de tráfico.

Otro problema que se presenta para la implementación de la telefonía IP es que el actual protocolo Internet Ipv4 trabaja con hasta 4.000 millones de direcciones con un espacio de direcciones de 32 bits. Si bien 4.000.000 es mucho más que el número actual estimado de 2.500.000 de direcciones en uso por varios cientos de millones de usuarios de la Internet, en la práctica el Ipv4 trabaja con un número mucho menor. Eso se debe a que las direcciones no se usan muy eficientemente, son atribuidas en bloques regionales, y hay un exceso de oferta en ciertas regiones del mundo, mientras que otras (Asia, Europa y Latinoamérica) están próximas a quedarse sin direcciones. Al índice actual de eficiencia del 60%, las direcciones IP se acabarán en algún momento en el futuro, por lo que es uno de los temas de trabajo del IETF para la próxima generación de Internet (IEN07) creó el Ipv6 (RFC 2460) (Proyecto de norma). El formato de direcciones de 128 bits del Ipv6 admite 340.232.366.920.938.463.374.607.431.768.5156 direcciones.

Además de una gama de direcciones de 128 bits, el conjunto de protocolo Ipv6 ofrece otras características, tales como seguridad obligatoria y movilidad, facilidad



de administración y funciones de autoconfiguración, QoS integral, y un encaminamiento más variable, así como mayor solidez, para mencionar unas pocas.

3.4 SEÑALIZACIÓN EN LA TELEFONÍA IP

Uno de los elementos más importantes dentro de los sistemas de telefonía es la señalización, tanto en las PSTN como en telefonía sobre IP. Lo más importante en una red de transporte de señalización es la fiabilidad. Dado que esta red transporta el control de todas las comunicaciones, un fallo en ella podría suponer la indisponibilidad de gran parte de la red y pérdidas económicas mucho mayores que las que produciría un fallo equivalente en un nodo de transporte de tráfico de usuario.

El sistema SS7 surgió dentro del entorno de la telefonía fija. Fue necesario crear un nuevo protocolo para añadirle las funcionalidades requeridas por las redes de telefonía IP.

Para el transporte de la señalización en la telefonía sobre IP hay dos opciones: la propuesta por IETF (SIGTRAN) y la de ITU -T (RDSI-BA/SS7).

El protocolo definido por la UIT-T para la transmisión de señalización de la señalización de la PSTN basadas en paquetes por las redes IP es el protocolo BICC (Control de Llamada de Portador Independiente). El protocolo SS7 y se especifica en la recomendación Q.1901 de U

El grupo de trabajo Transporte de Señalización (Signaling Transport, SIGTRAN) fue creado por IETF en 1999, y fue encargado de producir los estándares necesarios para hacer posible la integración las redes de datos y las redes



telefónicas. El propósito principal de este grupo de trabajo es encargarse de definir una arquitectura y protocolos para el transporte de señalización en tiempo-real sobre redes IP, también se encarga de definir una serie de protocolos para transportar SS7 y mensajes de ISDN sobre IP, teniendo en cuenta las funciones y prestaciones requeridas para el transporte de dicha señalización.



4. SIGTRAN

TRANSMISIÓN DE SEÑALIZACIÓN (SIGNALING TRANSPORT) SIGTRAN es un conjunto de protocolos y niveles de adaptación usados para transportar información de señalización sobre redes IP. Este conjunto de protocolos permiten la convergencia entre las redes telefónicas de conmutación de circuitos y las redes telefónicas basadas en IP.

La meta específica del grupo de trabajo SIGTRAN es la de producir una propuesta de estándares o normas, que den lugar a un RFC informativo que identifique funcionalidad y requisitos de desempeño para apoyar el envío de señalización telefónica sobre redes IP. Esta propuesta debe identificar los métodos de encapsulación de diferentes protocolos de señalización, las diferencias entre los diferentes protocolos de transportes y que componentes se transportan, se traducen o se terminan al gateway de señalización (SG). Se debe resaltar la seguridad. Este trabajo se realizó junto con otro grupo de trabajo de la IETF que trabajan sobre problemas similares.

4.1 FUNCIONALIDADES DE LOS PROTOCOLOS SIGTRAN

Los protocolos de Sigtran proveen todas las funcionalidades que se describen a continuación:

- Control de flujo.
- Identificación de puntos de señalización de origen y destino.



- Identificación del canal de voz.
- Detección de errores y retransmisión.
- Control de congestión en Internet.
- Detección de estado de la entidad par.
- Soporte de seguridad para información de señalización.
- Transporte de la señalización entre un gateway de señalización y media gateway o media gateway control.
- El transporte de Parte de Aplicación de Capacidades de Transacción (Transaction Capabilities Application, TCAP) entre un gateway de señalización y nodos IP.

El grupo de trabajo SIGTRAN requería un protocolo de transporte que se adecuara a los requerimientos para el transporte de la información de señalización SS7 sobre redes IP. Los protocolos TCP y UDP presentan una serie de limitaciones, que hacen que estos no sean adecuados como protocolo de transporte de información de señalización sobre redes IP.

4.2 LIMITACIONES DE TCP Y UDP

Los protocolos de transporte sobre IP, TCP y UDP, diseñados con propósito de propósito general, y presentan ciertas limitaciones que les hacen inadecuados para transportar señalización SS7, debido a las características de este tráfico.



Por ejemplo el protocolo UDP, no soporta acuse de recibo de los mensajes (ACK); no garantiza entrega ordenada de los mensajes; no incorpora mecanismos de seguridad. El protocolo TCP no tiene en cuenta el origen de los datos, ni diferencia unos datos de otros; TCP es muy sensible a retardos provocados por un fallo de transmisión en algún mensaje TCP, cuando esto ocurre TCP no envía mas datos hasta que se confirma la entrega correcta del mensaje que se transmitió con errores, así si se transmite un mensaje de una llamada concreta con error entre dos centrales de conmutación, todos los mensaje ISUP de todas las llamadas tendrían que esperar hasta que se retransmitiera correctamente el mensaje erróneo; la duración de temporizadores utilizados en TCP como (time-out) pueden ocasionar retardos no aceptables en un establecimiento de llamada; además TCP es muy vulnerable a ataques de negación de servicio.

Todas las limitaciones que presentan TCP y UDP los hacen inadecuados para el transporte de señalización de PSTN sobre redes IP. Por esto el grupo de trabajo SIGTRAN, genero el protocolo de Transmisión de Flujo de Control SCTP.

4.3 ARQUITECTURA SIGTRAN

La arquitectura del protocolo SIGTRAN se define por RFC2719 y consta de tres componentes básicos:

- IP estándar como protocolo de red.
- Un protocolo común de transporte de señalización. Los protocolos definidos por el Sigtran se basan en un nuevo protocolo de transporte sobre IP, el Protocolo de Transmisión de Flujo de Control SCTP (Stream Control Transmission Protocol).



- Capas de adaptación específicas para cada capa de la torre SS7 que se necesite transportar.

En la figura 10 se presenta la arquitectura SIGTRAN generalizada, mientras que en la figura 11 se presenta la arquitectura SIGTRAN detallando los protocolos y capas de adaptación que lo conforman.



Figura 10. Arquitectura de protocolo SIGTRAN

Los protocolos de la suite SIGTRAN han creado un nuevo protocolo de transporte, el SCTP y un conjunto de capas de Adaptación de Usuario (UA), capas que pueden emular los servicios de las capas inferiores de SS7 y ISDN.

Capa de adaptación del usuario, RFC 3057 (norma propuesta) que define un protocolo para el retroceso de los mensajes del usuario de RDSI sobre IP usando SCTP.

En total SIGTRAN actualmente define las siguientes capas de adaptación: M2UA, M2PA, M3UA, SUA y IUA.



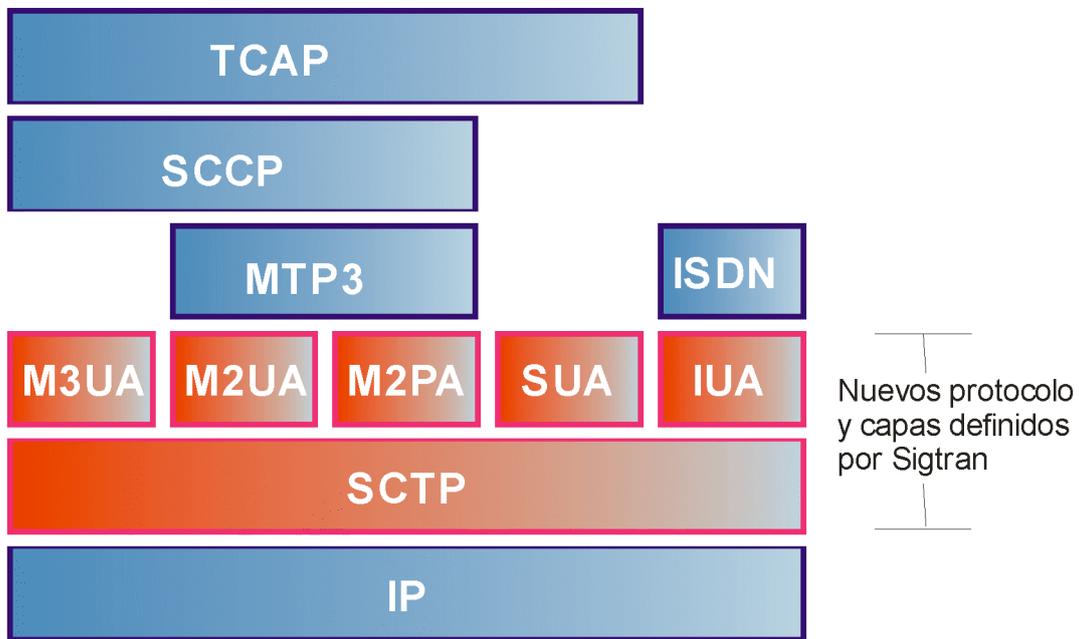


Figura 11. Arquitectura detallada de Protocolo SIGTRAN

Las capas de adaptación de sigtran todas sirven para un numero común de propósitos:

- Para llevar los Protocolos de Señalización de capa superiores encima de un transporte basado en IP.
- Para proporcionar la misma clase de servicio ofrecida a la interfaz equivalente de las PSTN. Por ejemplo M3UA debe proporcionar el mismo aspecto y los usuarios deben sentirla como MTP3.
- Para ser transparente: El usuario del servicio debe estar inadvertido de que la capa de adaptación ha reemplazado el protocolo original.



5. SCTP

Protocolo de Transmisión de Flujo de Control (Stream Control Transmission Protocol). Es un protocolo de comunicación de capa de transporte. Fue diseñado inicialmente para transportar señalización telefónica SS7 sobre redes IP. La intención fue proveer en IP algunos de las características de confiabilidad de SS7. Luego se propuso utilizarlo en otras áreas debido a su gran versatilidad.

La primera versión de SCTP se basó en un protocolo llamado Protocolo de Transmisión de Datagramas Multi-Red (Multi-Network Datagram Transmission Protocol, MDTP), el cual en su etapa inicial se basaba ampliamente en el protocolo TCP. De hecho MDTP comenzó a diseñarse antes de la creación de SIGTRAN y su objetivo original era subsanar algunos de los problemas encontrados al usar TCP. Al crearse SIGTRAN y comenzar a buscar el protocolo que más se adaptase a sus requerimientos, encontraron que MDTP era lo más parecido a aquello que andaban buscando. Durante su fase de diseño, la estructura inicial de MDTP cambió mucho. Había que adaptarlo a las necesidades específicas de SIGTRAN, el transporte de señalización de las redes telefónicas, en especial de la red SS7. La primera versión del SCTP se generó en septiembre de 1999, y desde entonces ha habido muchas modificaciones, así la estructura de este protocolo se fue formando a partir de una gran cantidad de cambios y se realizaban las modificaciones en consenso, hasta que fue anunciado una Petición de Comentarios (Request For Comments, RFC) número 2960 a finales de octubre de 2000 y la RFC3286 brinda una introducción al mismo. SCTP incluye muchas mejoras sobre TCP que lo hacen más apropiado para el transporte de señalización, e incluso puede competir con él como protocolo de transporte fiable general en Internet.



Como protocolo de transporte, podría considerársele equivalente a TCP o UDP pues es capaz de operar en modo confiable o no confiable. En el modo confiable provee servicios similares a TCP, es decir, asegura la entrega confiable y ordenada de los mensajes, incluyendo control de congestión. Pero a diferencia de TCP, SCTP está orientado al mensaje y no al byte. SCTP es más parecido a TCP que a UDP, sin embargo presenta prestaciones superiores a TCP apoyado en muchas de las funcionalidades de este.

Por su diseño SCTP, es muy adecuado para protocolos de señalización de sistemas de tiempo real. Este presenta varias ventajas frente a UDP en el contexto de los sistemas en tiempo real, derivadas fundamentalmente del hecho de que es un protocolo orientado a la conexión.

En el modelo de referencia TCP/IP, SCTP se encuentra en la capa de transporte, junto a TCP y UDP. La capa de transporte se ocupa de comunicación entre los programas en una red. Esto involucra aceptar los datos de la capa de la aplicación, y fragmentarlos para que pueda pasarse a la capa de la red. Además la capa de transporte también asegurará que los datos llega correctamente al nodo destino. Un protocolo de transporte en el ser es un juego de reglas que gobiernan cómo los datos se envía entre los nodos.

SCTP presenta entre otras las siguientes funciones: transferencia de datos fiable, definición de múltiples flujos para una misma conexión, posibilidad de seleccionar entrega ordenada o desordenada por separado para cada flujo, monitorización, fragmentación y reunificación de datos, y control de congestión, que comparte con TCP. Asimismo, contempla funciones adicionales de seguridad, como protección contra ataques por denegación de servicio y enmascaramiento.

SCTP es un protocolo muy abierto que ha sido diseñado para que sea extensible por naturaleza. SCTP contiene una serie de funciones básicas, que han sido



para que toda aquella característica adicional que quiera ser añadida en el futuro, pueda incluirse con gran facilidad.

5.1 COMPARACIÓN ENTRE SCTP Y EL PROTOCOLO TCP.

SCTP y TCP tienen algunas diferencias y también muchas similitudes. Entre sus similitudes se encuentran:

- **Iniciación:** para establecer una asociación entre dos nodos, tanto TCP como SCTP intercambiarán una serie de mensajes. Hay diferencias de la manera en que estos mensajes se intercambian y su formato, pero ellos tienen el mismo propósito, que es preparar una conexión de extremo a extremo (asociación o conexión). Mientras que TCP completa la iniciación de una conexión en tres pasos, SCTP completa en ambos lados después del intercambio de cuatro mensajes. El proceso se muestra en la gráfica (figura 13).

- **Fiabilidad y Ordenamiento:** SCTP y TCP llevan a cabo los mecanismos para garantizar la entrega exitosa de datagramas del usuario.

- **Manejo de Congestión:** SCTP y TCP sostienen el mismo mecanismo de manejo de congestión; el Aumento Aditivo, la Disminución Multiplicativa (AIMD) y el administrador de ventanas de congestión.

- **Cierre de la Asociación:** A pesar de que TCP y SCTP tienen básicamente los mismos mecanismos para el cierre, hay una ligera diferencia. TCP permite lo que se conoce como el estado entreabierto donde un punto final se encuentra abierto mientras el otro punto final se encuentra cerrado. SCTP no permite esto, ambos puntos finales deben cerrar cuando se emite la primitiva de cierre. Una razón para



no poner el estado entreabierto en SCTP era la falta de uso de él, muy pocas aplicaciones lo requieren.

- Seguridad en la Iniciación: tanto SCTP como TCP llevan a cabo un intercambio de mensajes para establecer una conexión de fin a fin. Sin embargo la manera que estos mensajes se envían es diferente. Mientras TCP utiliza un protocolo de establecimiento de asociaciones en tres pasos, SCTP emplea un protocolo de establecimiento de asociaciones en cuatro pasos. Esto le permite a los servidores el autenticar la dirección IP fuente del datagrama que tiene la bandera SYN fijada antes de reservar ningún recurso y así imposibilitar ataques de negación de servicio, en otras palabras SCTP utiliza un procedimiento de inicialización basado en cookies, para proporcionar protección frente a este tipo de ataques de negación de servicio tipo SYN.

Un ataque de negación de servicio es cuando los recursos se atan en el lado del servidor para que sea imposible responder para legitimar las conexiones. El atacante emite inmensas cantidades de demanda de SYN (un mensaje que pide estructuración de una conexión) al servidor y cuando recibe el SYN, lo desecha simplemente, no preocupándose por responder con un ACK. Esto causa que el servidor retenga el estado parcial que se asigno después de la petición del SYN, y si lleva a cabo esto repetidamente provocara un desbordamiento y llevara a un rechazo de servicio.

- SCTP es orientado a mensaje como UDP, en cambio TCP maneja el concepto de mensaje y lo que transporta se ve como un simple flujo de bytes, no existe diferenciación entre un mensaje u otro. Esto hace que las aplicaciones deben proporcionar sus propias marcas para distinguir mensajes diferentes enviados a través una conexión TCP. Como se muestra en la figura 12, diferentes mensajes son enviados desde el origen, en SCTP cada uno de esos mensajes



llega por separado, mientras que en una conexión TCP estos llegan como un solo flujo de bits, y no hay diferenciación entre ellos.

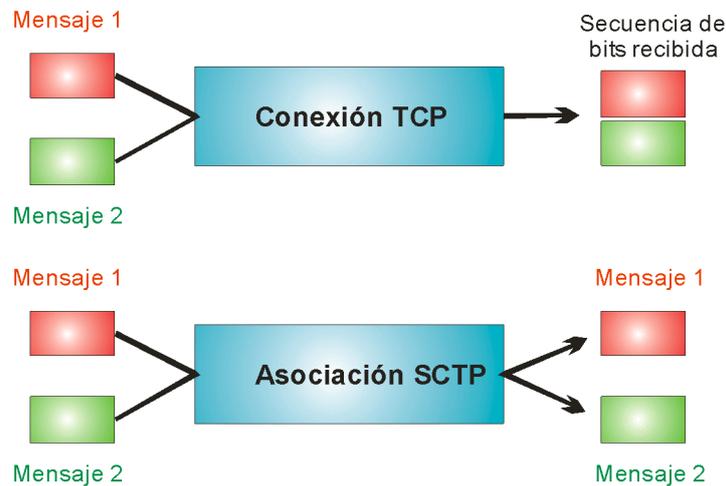


Figura 12. SCTP orientado a mensaje Vs TCP orientado a bits.

De todas las diferencias existentes entre SCTP Y TCP se encuentran dos características en SCTP que definen realmente la mayor diferencia entre estos dos protocolos. Estas son las funciones Multihoming y Multistreaming del SCTP, que se explicaran mas adelante.

En la tabla 2 se muestra un resumen de la comparación entre los tres protocolos de transporte sobre IP más importantes TCP, UDP y SCTP.

Servicio /Característica	SCTP	TCP	UDP
Transmisión Full-Duplex.	si	si	si
Orientado a Conexión	si	si	No
Transferencia de datos Confiable	si	si	No
Transferencia de datos parcialmente confiable	opcional	No	No
Entrega ordenada de datos	si	si	No



Entrega de datos no ordenada	si	no	Si
Control de flujo o congestión	si	si	No
Acks selectivo	si	opcional	Si
Multistreaming	si	no	No
Multihoming	si	no	No
Protección contra ataque de inundación de SYN	si	no	n/a
Conexión parcialmente cerrada	no	si	n/a

Tabla 2. Comparación entre SCTP, TCP y UDP.

5.2 PRINCIPALES CARACTERÍSTICAS DE SCTP.

Entre las características de SCTP se encuentran dos que mayormente hacen la diferencia entre este y los otros protocolos de transporte sobre redes IP, estos son el multihoming y multistreaming que posee SCTP.

- **Multihoming:** propiedad en la cual uno (o dos) de los extremos de una conexión pueden tener más de una dirección IP. Esto permite reaccionar en forma transparente ante fallas en la red. esta propiedad hace a los nodos más tolerantes contra fallas de la red física y otros problemas de ese tipo.

Una conexión TCP se identifica por la dirección IP y puerto tanto del cliente como del servidor. Así si una máquina posee diferentes tarjetas de red con sus respectivas direcciones IP asociadas, no puede usar más que una para establecer una conexión TCP con otra máquina. En SCTP una asociación se identifica por una serie de direcciones IP y un puerto del cliente, y el conjunto de direcciones IP del servidor y su puerto. De esta manera, en caso de que una de las direcciones IP deje de funcionar, siempre se puede seguir utilizando cualquiera de las otras. En la figura 13 se muestra una conexión SCTP con dos interfaces (ej.



tarjetas de red) cada una con su propia dirección IP, en ambos puntos de la asociación.



Figura 13. Multihoming.

A pesar que con SCTP se puede tener varias direcciones IP (multihoming) tanto en el cliente como en el servidor, tan solo se utiliza una de ellas para enviar los datos, la dirección primaria (primary address). El resto se reserva y sólo se utilizan en caso de que la dirección primaria falle. Por ello, para saber el estado en que se encuentran dichas direcciones IP de reserva, SCTP tiene el llamado mecanismo de latidos de corazón (heartbeat mechanism), el cual consiste en enviar mensajes a las direcciones IP que no estén siendo utilizadas para enviar datos. Dichos mensajes, o latidos, se deben responder, de manera que al recibir la respuesta se sabe que esas direcciones siguen activas.

- **Multistreaming:** Entrega de los datos en trozos que forman parte de flujos independientes y paralelos dentro de una asociación, de manera que datagramas dirigidos a flujos distintos se tratan independientemente, eliminando así el problema conocido como Bloqueo del principio de la Línea (head of the line blocking) que sufre TCP, con la posibilidad de seleccionar entrega ordenada o desordenada por separado para cada flujo. El beneficio de tener los flujos de datos independientes es que mientras que un flujo se bloquea por pérdida de un paquete esperando su retransmisión el resto de flujo pueden continuar enviando los datos.



En TCP si un paquete se pierde, la comunicación se detiene hasta que retransmita el dato perdido.

La posibilidad de establecer múltiples flujos de datos (streams) entre dos aplicaciones permite que exista un proceso de nivel de aplicación de SCTP que gestione la señalización. Los mensajes asociados a una llamada se envían por un streams concreto. Si un mensaje no se entrega correctamente y es necesario retransmitirlo, el resto de streams no se ven afectados por el retardo. Si las llamadas se transmitieran mediante TCP, un fallo en un mensaje de una llamada retrasaría la entrega de los mensajes del resto de llamadas innecesariamente.

El fenómeno de Bloqueo del Principio de la Línea es cuando los paquetes son bloqueados por un paquete delante que ha se ha perdido. Esto se explica en la figura 14.

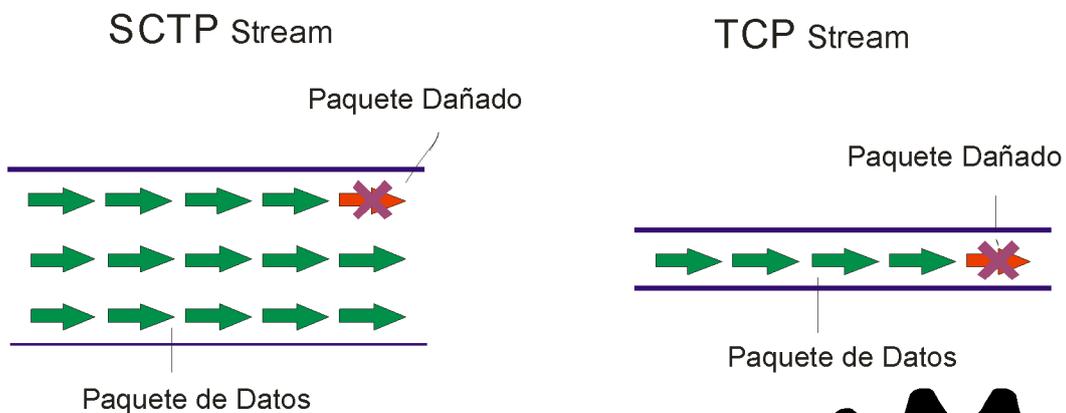


Figura 14. Multistreaming en SCTP.

El número de streams que se enviarán a través de una asociación se define en el establecimiento de la misma, de forma negociada entre ambos extremos de la comunicación. Los streams son unidireccionales, de forma que para una



comunicación bidireccional se deberán definir al menos dos streams en una asociación SCTP.

El Multistreaming se puede lograrse en TCP, pero involucraría la apertura de conexiones de TCP múltiples que cada acto como un stream para enviar datos. Esto difiere del multistreaming en SCTP dónde todos los flujos residen en una sola asociación. Para esto se requeriría en TCP un mayor ancho de bando.

• **Inicio de asociación en SCTP:** SCTP protege contra el ataque de rechazo de servicio con el uso de cookie [RFC2522]. Para iniciar una asociación, el servidor recibe un INIT (mensaje para petición de Iniciación). El servidor analiza los datos contenidos en este mensaje y genera los valores necesarios para establecer una asociación y genera un despiece seguro de estos valores y genera una llave secreta, entonces se colocan estos datos en un Cookie de llamado, junto con el código de autenticación de mensaje derivado (MAC). Este cookie he devuelto al remitente en un INIT-ACK (Reconocimiento de Inicio), el servidor permanece en estado cerrado y se olvida del INIT recibido. Una vez el receptor recibe el INIT-ACK del servidor genera un COOKIE-ECHO (que contiene el cookie de la estructura de los datos) y lo envía al servidor, al recibirlo el servido desempaqueta los datos contenido en este cookie y usa un nuevo MAC para verificar si este si es el cookie creado por el servidor, en este caso envía un COOKIE-ACK (reconocimiento de cookie) al cliente y establece la asociación. Puesto el servidor no reconoce la asociación, hasta que el cliente responde con un COOKIE-ECHO, se vuelve resistente al rechazo de servicios de servicio. Dicho proceso se muestra en la figura 15.



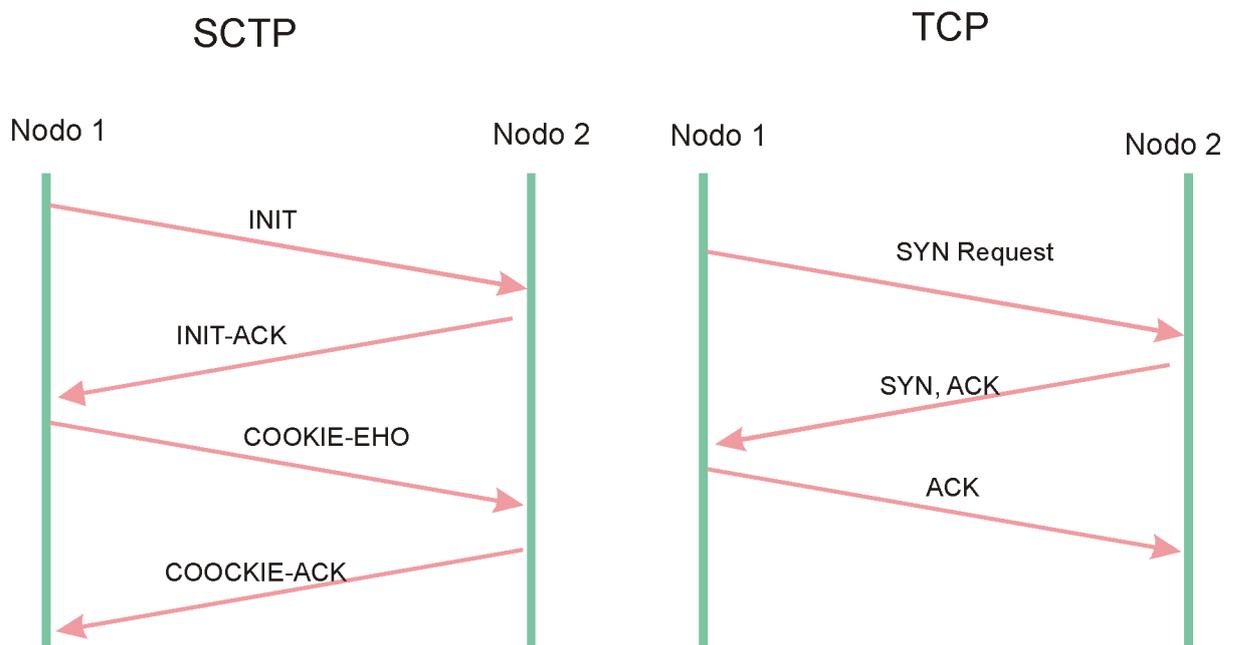


Figura 15. Iniciación en SCTP y TCP.

- **Gestión de Conexiones:** La función de gestión de conexiones de SCTP escoge la dirección de transporte destino para cada paquete SCTP que se envía, basándose en las instrucciones del usuario de SCTP y en las direcciones disponibles alcanzables para ese destino SCTP.

En periodos de inactividad, la función de gestión de conexiones monitoriza la disponibilidad de los extremos de la comunicación mediante mensajes de comprobación (heartbeats). Si SCTP percibe algún extremo como inalcanzable informa a su usuario de nivel superior. En el establecimiento de la asociación, se define un camino primario para cada extremo SCTP, que es el que se usa en el envío normal de paquetes.



En el extremo receptor, la gestión de conexiones se encarga de comprobar la existencia de una asociación SCTP válida a la que pertenece cada paquete SCTP recibido.

- **Fragmentación de los datos de usuario:** SCTP posee mecanismos de fragmentación y re-ensamblado de mensajes de usuario para adecuarlos al tamaño requerido por el nivel inferior (IP en el caso de SS7 sobre IP).

- **Mensajes de Error:** una máquina que tiene una asociación SCTP con otra, puede enviarle mensajes de error, de manera que ciertos errores a nivel del protocolo de transporte pueden resolverse sin afectar al usuario. Estos mensajes de error sirven también para negociar el uso de funciones opcionales, de manera que versiones antiguas de SCTP que no soporten dicha función nueva tengan una manera de expresar dicha carencia enviando el mensaje de error apropiado.

- **Entrega Ordenada y no ordenada de mensajes:** Los mensajes de usuario se asocian a flujos determinados, de forma que el extremo receptor SCTP entrega al nivel superior todos los mensajes de un mismo flujo en el mismo orden en que se enviaron. Sin embargo, no existen restricciones de entrega ordenada entre mensajes de distintos flujos de la misma asociación. De esta forma, los mensajes de un flujo se pueden seguir entregando aunque otro esté bloqueado esperando el siguiente mensaje. Adicionalmente, SCTP proporciona un mecanismo para no utilizar el servicio de entrega ordenada de mensajes, de forma que los mensajes enviados mediante dicho mecanismo se entregan al nivel superior al mismo ritmo SCTP tan pronto como se reciben.

En la tabla 3 se presenta un resumen de las características del protocolo SCTP.



Es un protocolo Punto a extremo conocido.
Define tiempos de reintento (time-outs) mucho menores que los de TCP.
Proporciona mecanismos de validación y asentimiento como protección ante ataques por inundación, proveyendo notificación de trozos de datos duplicados o perdidos.
Es capaz de seleccionar y monitorizar caminos, seleccionando un camino "primario" y verificando constantemente la conectividad de cada uno de los caminos alternativos.
Se adapta a la tasa de transferencia, disminuyendo la velocidad de envío de datos en caso de congestión en la red.
Permite compactar varios mensajes de señalización en un mismo mensaje SCTP. A su vez, permite fragmentar los mensajes de señalización, de forma que un mismo mensaje se divida en varios mensajes SCTP.
Está orientado a mensajes y no a bits como TCP, que define tramas de datos estructurados.
Los datos se pueden dividir en múltiples flujos (streams), cada uno con un orden de entrega de mensajes independiente.
Ofrece monitorización, fragmentación y reunificación de datos, y control de congestión y flujo compatibles con TCP.
Proporciona mecanismos para retransmitir con rapidez segmentos perdidos y control de congestión.
Fragmentación de nivel de transporte. En aquellas situaciones en las que la MTU es menor que el tamaño de un mensaje, no se recurre a fragmentación IP, mejorando la tasa de pérdidas y el comportamiento ante cortafuegos y traductores de direcciones de red.

Tabla 3. Resumen de Características del protocolo SCTP.



5.3 PAQUETE SCTP

El datagrama SCTP consiste en un encabezamiento común seguido por uno o más segmentos de datos. Este ha cambiado completamente desde sus primeras versiones, sus rasgos han sido mejorados y se han resuelto muchos errores. Este es una evolución del Protocolo MDTP, el cual en su diseño inicial se basó en TCP.

Los paquetes de SCTP se conocen como Unidad de Paquete de Protocolo (Protocol Data Units, PDU).

Un paquete SCTP está compuesto por una cabecera común y una serie de unidades de información, denominadas chunks. Un chunk puede contener información de control o datos de usuario. Los múltiples chunks pueden ser multiplexados en paquetes dimensionados encima de una ruta MTU.

Los chunks tienen estructura propia, y presentan una serie de campos, dependiendo del tipo de chunk que sean.

SCTP permite transportar varios mensajes de usuario en un único mensaje SCTP, mediante el uso de distintos chunks de datos dentro del mismo mensaje.

La estructura del paquete SCTP se muestra en las siguientes gráficas (figuras 16 y 17.)



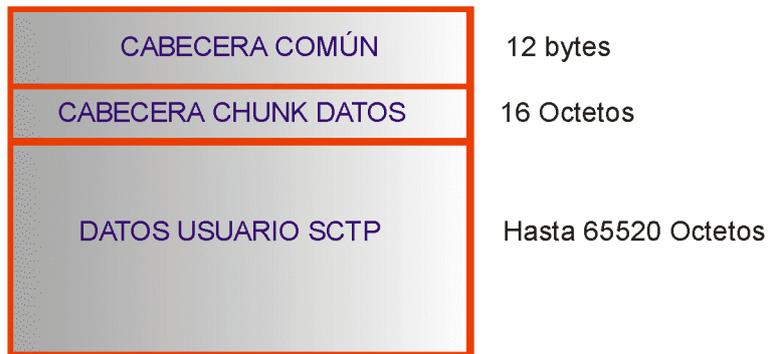


Figura 16. Estructura generalizada de paquete SCTP.

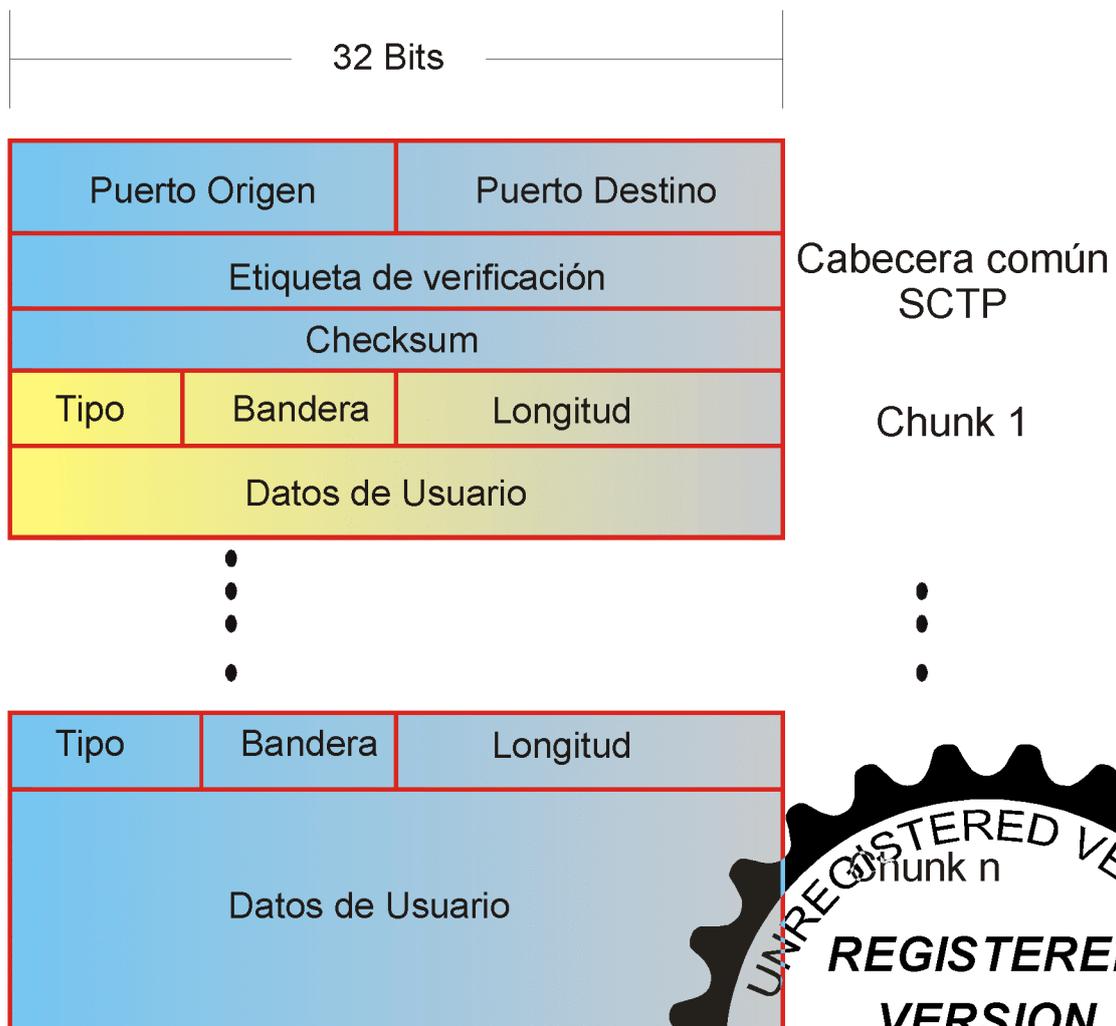


Figura 17. Estructura detallada de Paquete SCTP



Cuando SCTP fue modificado para trabajar directamente encima de IP, también fue convenido que todos los puertos de TCP usados para aplicaciones bien conocidas serían automáticamente reservados en espacio de dirección de puertos en SCTP. Eso no sólo haría más fácil la migración de aplicación de TCP a SCTP.

5.3.1 Cabecera Común

La cabecera común esta compuesta por 12 bytes. Para la identificación de una asociación SCTP usa el mismo concepto de puerto como TCP y UDP. Para el descubrimiento de errores en la transmisión, cada paquete de SCTP es protegido por un Cheksum de 32 bits (algoritmo Adler-32) que es más robusto que los checksum de 16 bits de TCP y UDP. Los paquetes SCTP con un checksum no valido son silenciosamente descartados. La cabecera común también tiene un pedazo de 32 bits llamado etiqueta de comprobación. La etiqueta de comprobación es una asociación específica, y se intercambia entre el punto final el inicio de la asociación. Hay dos valores de etiqueta utilizados en esta asociación.

5.3.2 Tipos de Chunks

Cada chunks empieza con un campo de tipo de chunks, que se usa para distinguir los chunks de los datos y los tipos diferentes de chunks de control. Cada chunk específico de la bandera y un chunks de longitud de campo, necesarios porque los chunks tienen una longitud variable. El campo contiene la carga útil real del chunks.



Hasta ahora existen 13 tipos de chunks, definidos para uso estándar, los cuales se muestran en la tabla 4.

ID	Tipo de Chunks
0	Carga útil de datos - Payload Data (DATA)
1	Iniciación - Initiation (INIT): se usa para comenzar una asociación de SCTP entre dos puntos finales.
2	Reconocimiento de la asociación - Initiation Acknowledgement (INIT ACK): se usa para reconocer la iniciación de una asociación de SCTP. La parte del parámetro de INIT ACK se estructura semejantemente al chunk de INIT. Usa dos parámetros inconstantes extras: el cppkie de estado y el Parámetro no reconocido:
3	Reconocimiento de selección - Selective Acknowledgement (SACK): se envía al punto final del par para reconocer los chunk de los DATOS recibidos.
4	Latido del corazón - Heartbeat Request (HEARTBEAT): Un punto final debe enviar este chunk a su punto final par para sondear el estado de una IP en particular definida en la asociación presente. El campo del parámetro contiene la Información del Latido del corazón que es una longitud inconstante la estructura de los datos opaca sólo entendida por el remitente.
5	Reconocimiento de latido del corazón - Heartbeat Acknowledgement (HEARTBEAT ACK): Un endpoint debe enviar este chunk a su endpoint par como una contestación a un chunk HEARTBEAT. Un HEARTBEAT ACK siempre se envía a la fuente que IP se dirigen del datagrama de IP que contiene el chunk del HEARTBEAT a que este ACK está respondiendo.
6	Aborto - Abort (ABORT): se envía al par de una asociación para



	<p>cerrar la asociación. El chunk ABORT puede contener los Parámetros de la Causa para informarle la razón de la interrupción al receptor. No deben atarse los chunk de los DATOS con la el chunk ABORT. Los chunk de control (salvo INIT, INIT ACK y CIERRE COMPLETO) puede atarse con un chunk ABORT pero ellos deben ponerse antes del ABORT en el paquete de SCTP, o ellos son ignorarán por el receptor.</p>
7	<p>Cierre - Shutdown (SHUTDOWN): Un endpoint en una asociación debe usar este chunk para comenzar un cierre elegante de la asociación con su par.</p>
8	<p>Reconocimiento de Cierre - Shutdown Acknowledgement (SHUTDOWN ACK): Este chunk debe usarse para reconocer el recibo del chunk Shutdown.</p>
9	<p>Error de funcionamiento - Operation Error (ERROR): Un endpoint envía este chunk a su endpoint del par notificarlo de ciertas condiciones del error. Contiene uno o más causas del error. Un Error del Funcionamiento no es considerado en si mismo fatal, pero puede usarse con un chunk error para informar una condición fatal. Cada causa del error puede llevar su propio juego de parámetros. Las causas del error que se han definido son:</p> <ul style="list-style-type: none"> - 1. Identificador de Stream invalido. - 2. Parámetro obligatorio perdido. - 3. Cookie de error viejo. - 4. Fuera de medio. - 5. Dirección Irresoluble. - 6. Tipo de chunk irreconocible. - 7. Parámetro obligatorio invalido. - 8. Parámetro desconocido. - 9. Ningún DATO de usuario.



	- 10. Recepción de Cookie durante el cierre.
10	Cookie de Estado - State Cookie (COOKIE ECHO): Este CHUNK sólo se usa durante la inicialización de una asociación. Se envía por el iniciador de una asociación a su par para completar el proceso de la inicialización. Este chunk debe preceder cualquier chunk de DATOS enviado dentro de la asociación, pero puede atarse con uno o más chunk de DATOS en el mismo paquete.
11	Cookie de Reconocimiento - Cookie Acknowledgement (COOKIE ACK): Este chunk sólo se usa durante la inicialización de una asociación. Se usa para reconocer el recibo de un chunk COOKIE ECHO. Este chunk debe preceder cualquier DATOS o pedazo corto y grueso del SACK enviados dentro de la asociación, pero puede atarse con uno o más pedazos cortos y gruesos de los DATOS o pedazo corto y grueso del SACK en el mismo paquete de SCTP.
12	Reservado para la notificación de congestión de eco - Reserved for Explicit Congestion Notification Echo (ECNE)
13	Reserva para congestión de ventana reducida - Reserved for Congestion Window Reduced (CWR)
14	Cierre completo - Shutdown Complete (SHUTDOWN COMPLETE): Este chunk debe usarse para reconocer el recibo del chunk SHUTDOWN ACK a la realización del proceso del cierre. El chunk SHUTDOWN COMPLETE no tiene ningún parámetro.
15 a 52	Reservado por IETF - reserved by IETF
53	Definido por la IETF para extensión de chunks - IETF defined Chunk Extensions
54 - 126	Reservado por IETF - reserved by IETF

Tabla 4. Tipos de chunks definidos en SCTP



5.3.3 Etiqueta de Verificación

Esta formada por 32 bits enteros, escogidos al azar e intercambiada en la fase del establecimiento. Esta no tiene modificaciones durante toda la vigencia de la asociación para validar los datagramas entrantes como realmente fueron enviados por el punto final del par y no por un atacante. De esta forma se consigue más protección frente a comunicaciones con suplantación de identidad. El valor de este campo lo decide el extremo de la comunicación SCTP en el establecimiento de la asociación.

5.3.4 Datos de usuario

La cabecera de un chunk de datos de usuario mide 16 octetos, y pueden contener hasta 65520 octetos de información del nivel superior. Esto significa que, en principio, cualquier mensaje de cualquier operación cabe en un chunk de datos SCTP, incluyendo las cabeceras de los protocolos de adaptación intermedios.

5.3.5 Checksum

Después de largas discusiones se convenido que el Chequeo de Redundancia Cíclico de 32 bits (CRC-32) estandarizado por ITU-T ([ITU-T 967] se usará en SCTP. Un código cíclico es aquel en el que cualquier rotación cíclica (lo que sale por un lado, entra por el otro) de una palabra código produce otra palabra código válida. Los códigos cíclicos son una familia de códigos bloque-lineales que son especialmente fáciles y eficientes de generar y verificar.



6. CAPAS DE ADAPTACIÓN SIGTRAN

6.1 M2UA, (MTP2 User Adaptation.): El protocolo M2UA, al igual que M2PA, adapta MTP3 a SCTP, e igualmente gestiona asociaciones SCTP en lugar de enlaces MTP3. M2UA permite el intercambio de mensajes MTP3 entre dos puntos de señalización IP o entre un punto de señalización IP y Gateway. En otras palabras M2UA proporciona los servicios de MTP2 en una situación de cliente servidor. Se publico bajo la normativa RFC 3331.

En caso de que la comunicación se realice entre dos puntos de señalización IP, sin gateway de señalización intermedio M2UA es un protocolo entre pares, como se muestra en la figura 18.

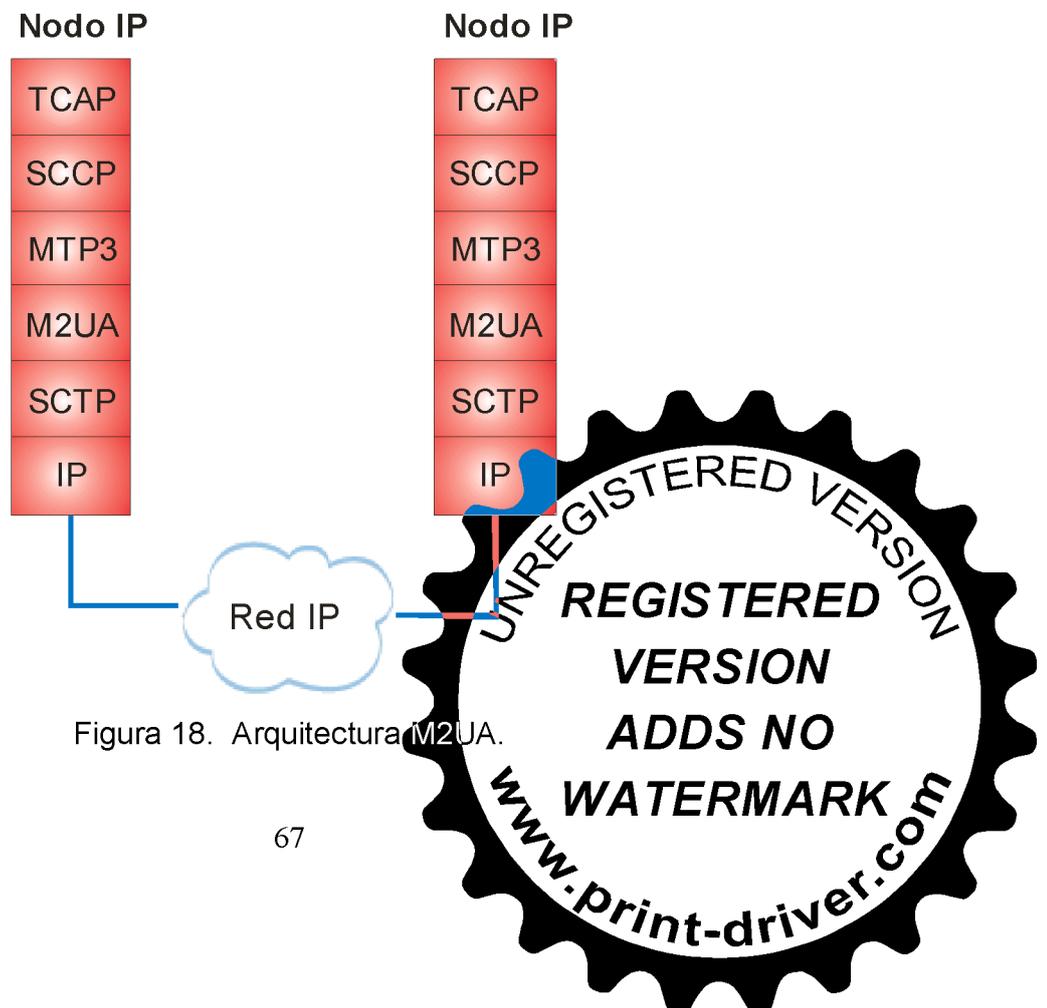


Figura 18. Arquitectura M2UA.

Cuando se implementa M2UA en un gateway de señalización, no es un protocolo entre pares, entonces M2UA no procesa las ordenes que le llegan desde la capa superior (MTP3), sino que la envía tal cual hacia un nodo remoto, mediante SCTP, en este caso se debe entender M2UA como un medio que comunica la capa MTP3 de un nodo IP con la MTP2 de un gateway de señalización, como se muestra en la figura 19.

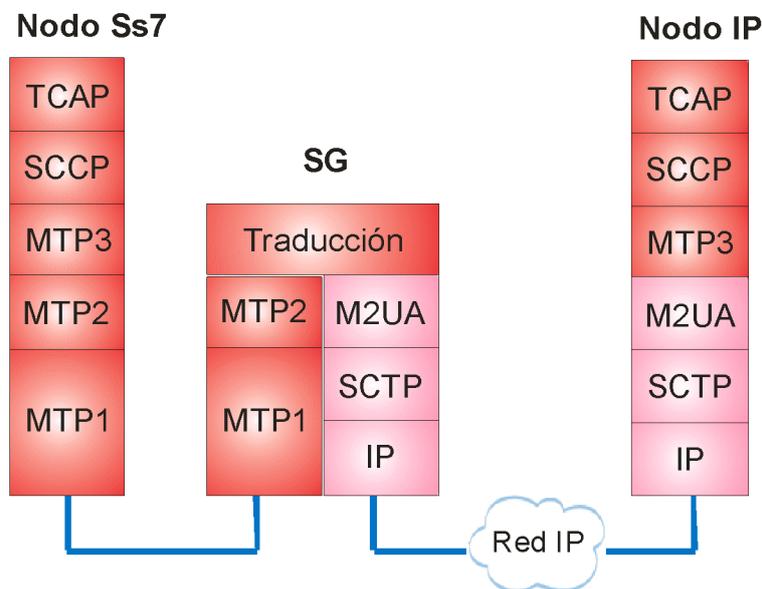


Figura 19. Transporte de MTP3 a MTP2 Remoto, Mediante M2UA.

6.2 M2PA (MTP2-user peer-to-peer adaptation.): proporciona los servicios de MTP2 en una situación del punto a punto, como las conexiones SG a SG. Su usuario sería MTP3. M2PA es el equivalente punto a punto de M2UA. En lugar de proporcionar un eslabón entre MTP2 remotamente localizados y la instancia MTP3, reemplaza un eslabón de MTP2 bajo el usuario de MTP3. En otras palabras un mensaje MTP3 enviado por M2PA tiene como destino otra capa MTP3 de un nodo con capa M2PA, y todas las órdenes, o primitivas, de MTP3 las procesa la capa M2PA del mismo nodo, tal como



haría MTP2. este proceso se muestra en la figura 20. Debido a la presencia de MTP3, cada SG requerirían su propio Código de Punto de SS7.

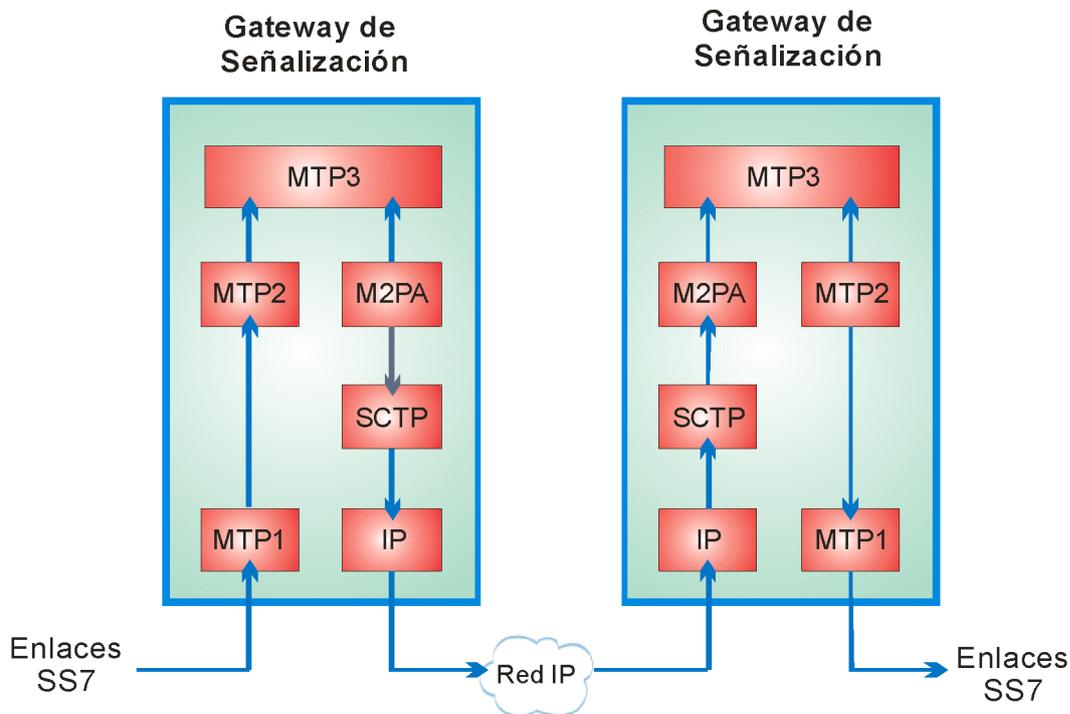


Figura 20. Arquitectura M2UA.

Al ser un protocolo entre pares, es el protocolo más adecuado para transportar señalización entre dos nodos SS7 puros (sin capa IP) a través de una red IP, ya que reemplaza completamente la capa MTP2, y permite comunicación entre SGs.

6.3 M3UA (MTP3-User Adaptation). Este protocolo transporta mensajes procedentes de un usuario de MTP3 (ISUP, TUP o SCCP) a través de una red SCTP/IP hasta un nodo remoto, como se muestra en la figura 21. M3UA está presente en cada SG para proporcionar la asignación de ruta y dirección del MTP2/M2PA.



Es similar a M2UA, M3UA simplemente transporta los mensajes hasta el destino, pero no realiza por sí mismo las funciones de la capa MTP3. Esto significa que M3UA no dispone de tablas de enrutamiento basadas en puntos de señalización, ni realiza ninguna otra función propia de MTP3.

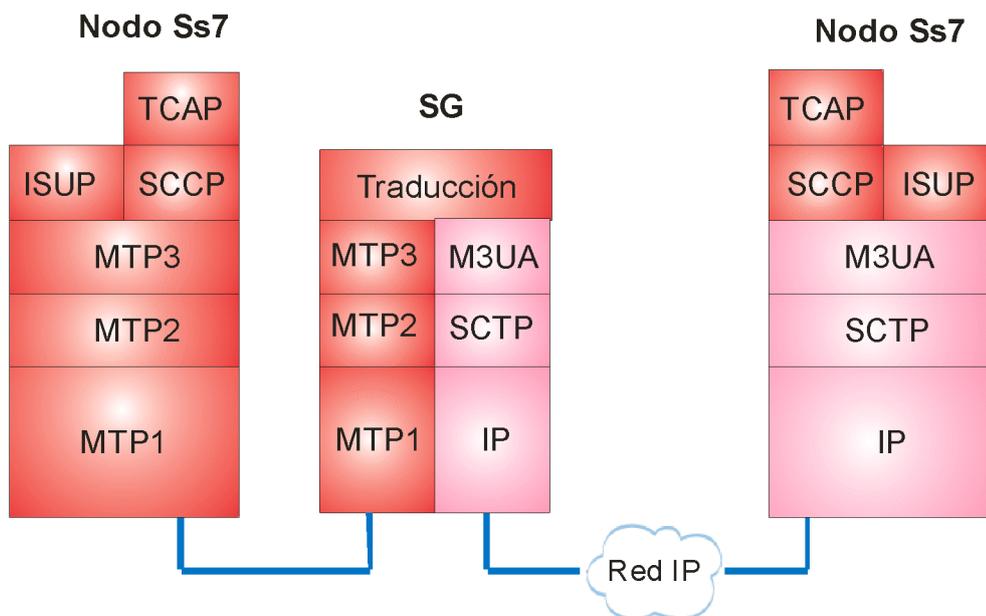


Figura 21. Arquitectura M3UA.

6.4 SUA proporciona los servicios de SCCP en una arquitectura punto a punto, como SG a IP SCP. Su usuario sería TCAP. SUA proporciona un medio para que una parte de la Aplicación (como TCAP) en un IP SCP pueda alcanzar un SG. La arquitectura de la red asociada con SUA le permite a SCPs tener múltiples IP en un mismo SG. La arquitectura de SUA se muestra en la figura 22.



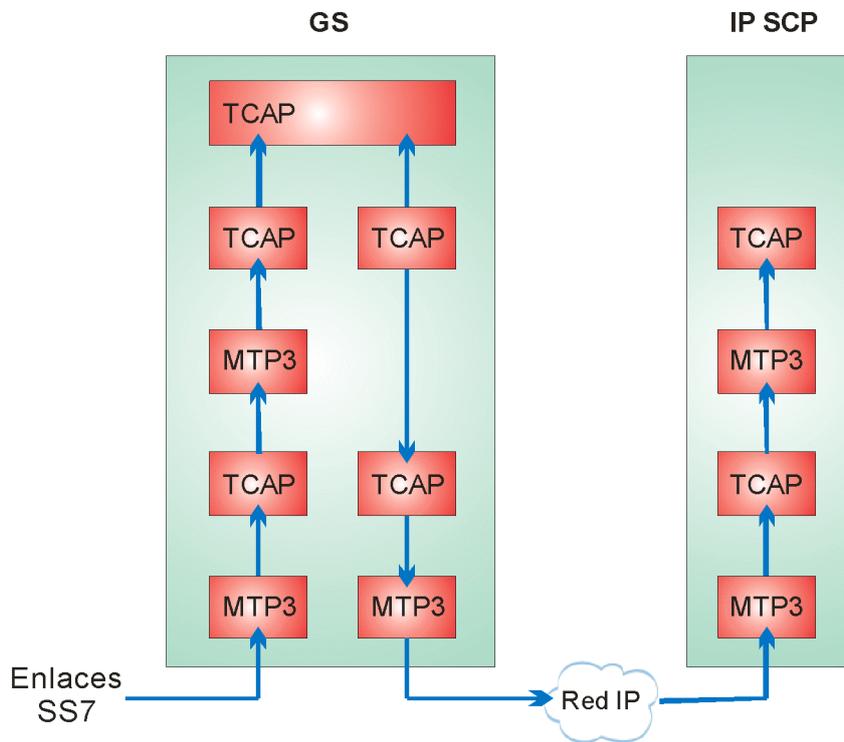


Figura 22. Arquitectura acostumbrada de SUA.

6.5 IUA proporciona los servicios a la capa de enlace de datos ISDN (LAPD.) Su usuario sería un ISDN Capa 3.

Todavía se está trabajando en el protocolo SIGTRAN. La RFC2719 (informativo) proporciona el marco arquitectónico para la transmisión de la señalización, y en la RFC3257 (informativo) se describe la aplicabilidad de SCTP.



7. CONCLUSIONES

En la actualidad SCTP todavía no es muy conocido y se podría decir que todavía esta bajo desarrollo. Hoy en día no son muchas las aplicaciones prácticas que lo utilizan, pero mirando sus características se puede estar seguro que este será un éxito y tendrá muchas otras aplicaciones además del transporte de información de señalización.

El grupo SIGTRAN inicialmente pensó en un protocolo relativamente simple, con características específicas para el transporte de información de señalización, pero debido a las propuestas hechas en los diferentes foros hicieron que este se estructurara hasta el punto de convertirse en un protocolo robusto, con características que lo hacen ideal no solo para el transporte de información de señalización sino que podría competir en otras aplicaciones con TCP.

SCTP posee varias características que lo hacen más conveniente que TCP para el transporte de información de aplicaciones comunes en Internet. Uno de los puntos mas débiles de TCP es su vulnerabilidad ante el ataque de SYN. Mientras que SCTP es inmune a este tipo de ataque por la utilización de cookies en el inicio de una asociación.

La propiedad Multistreaming de SCTP es particularmente conveniente para su uso en los servidores de HTTP. actualmente, cuando se transmite una página web, una conexión de TCP debe prepararse para cada elemento gráfico que contiene, así como para sonido o video. SCTP usando el servidor podría abrir tantos streams simplemente como se necesiten para el transporte de esos cuadros y envía la información que considera cada uno usando un stream



independiente. Un efecto práctico de esto es que si hay 20 usuarios que acceden un servidor de HTTP por ejemplo, 19 de ellos que transmiten páginas que contienen sólo texto (usando una sola conexión de TCP así), y uno de ellos que pide una página que contiene 19 cuadros (qué requeriría 20 conexiones de TCP), este último usuario consumirá en total tanto ancho de banda del servidor HTTP y tiempo de procesamiento como los otros 19 usuarios. Usando SCTP, los 20 usuarios recibirían la misma porción de recursos.

La propiedad Multihoming no la posee ningún otro protocolo de transporte anterior a SCTP, esta propiedad es bastante útil para servidores que tienen una alta demanda de tráfico, utilizando varias tarjetas de red, esta propiedad asegura que la conexión no se pierde en caso que una de las tarjetas quede fuera de funcionamiento, además da la posibilidad de desviar el tráfico de los caminos congestionados.

SCTP es orientado a mensaje como UDP. TCP no tiene el concepto de mensaje y lo que transporta se ve como un flujo simple de bytes. Esto hace que las aplicaciones deben proporcionar sus propias marcas para separar mensajes diferentes enviados a través una conexión TCP. Pero UDP es inestable y no ofrece muchos de los rasgos que tiene TCP. En SCTP los mensajes del usuario se identifican por su SSN y eso hace posible identificar porciones específicas de los datos transportados. Aplicado a nuestro ejemplo anterior de un servidor de HTTP, podrían transferirse las partes diferentes de una página web como mensajes diferentes que harían más fácil su identificación al lado del receptor cuando solo se un solo flujo de datos.

TCP confía en ICMP para informar sobre los problemas. Los problemas informados por ICMP siempre están en el nivel de IP y el propio TCP no tiene manera alguna de informar sobre los problemas a nivel de transporte. SCTP tiene



la posibilidad de utilizar chunk Error para informar al par de ciertas condiciones de error, así el otro par puede actual de forma más consistente.

SCTP esta inspirado en TCP, esto es bueno ya que TCP ha demostrado ser un protocolo robusto, usado durante mucho tiempo. La propiedad de manejo de congestión se tomo directamente de TCP y algunos otros rasgos que son operativos en TCP se colocaron por defectos en cualquier aplicación SCTP. Entre ellos se podrían mencionar el uso de reconocimientos selectivos, la habilidad de decir sobre el recibo de TSNs doble, soporte para ECN o el mecanismo de latido del corazón.

SCTP tiene las capacidades de extensibilidad mucho mayor que TCP. En TCP, el espacio restringido que puede usarse para incluir las opciones los hace casi inútil. Los pocos pedazos que son reservado en el título de TCP son un muy escaso, y cualquier nuevo rasgo que se agregue a TCP tuviera que hacer uso de cualquiera de esos pedazos reservados debe adaptarse como sea posible a estos espacios vacíos. En SCTP que agrega un nuevo rasgo es fácil y los diseñadores no tienen que estar preocupándose por el espacio disponible para las extensiones, ellos apenas definen nuevos chunks o los nuevos parámetros e incluyen en ellos la tanta información como sea necesario. La cantidad disponible de chunks indefinidos y parámetros es bastante grande para posibles extensiones en el futuro.

Existe una cantidad bastante grande de aplicaciones que utilizan TCP y todavía debe pasar algún tiempo para que se cambien a SCTP.

En general SCTP posee características que hacen que este tenga muchas ventajas sobre TCP y muy pocas desventajas, por lo que se puede esperar que SCTP sea utilizado en aplicaciones distintas al transporte de información de



señalización. Se espera que en el futuro SCTP reemplace a TCP en Internet, sin embargo esto no pasara de la noche a la mañana. Tendría una evolución similar a IPv6.

Se espera que en el futuro la arquitectura TCP/IP sea remplazada por la arquitectura SCTP/IPv6.



GLOSARIO

ACK	Mensaje de asentimiento a otro mensaje enviado previamente.
AGW	Access Gateway. Pasarela de acceso
AN	Access Node. Nodo de acceso
Chunk	Unidad de información en la que se divide un paquete del protocolo SCTP.
CIC	Circuit Identification Code. Código identificador de un circuito de voz entre dos nodos de conmutación.
CRC	Cyclic redundancy check. Comprobación de Redundancia Cíclica.
Diffserv	Método de caracterización de tráfico IP basado en diferenciación por servicios.
DPC	Destination Point Code. Código de punto de señalización destino.
DSL	Digital Subscriber Line. Línea de abonado digital
IETF	Internet Engineering Task Force. Grupo de Trabajo de ingeniería de Internet.
IP	Internet Protocol. Protocolo de Internet
ISPC	International Signalling Point Code. Código de señalización nacional
ISUP	Integrated Services User Part. Parte de usuario de servicios integrados.
IUA	ISDN Q.921-User Adaptation Layer. Capa de adaptación del usuario del protocolo Q.921 de la Red Digital de Servicios Integrados.



Linkset	Conjunto de enlaces de señalización entre dos nodos adyacentes.
M2PA	MTP2-User Peer-to-Peer Adaptation Layer. Capa de adaptación entre pares de usuario de MTP2.
M2UA	MTP2-User Adaptation Layer. Capa de adaptación de usuario de MTP2.
M3UA	MTP3-User Adaptation Layer. Capa de adaptación de usuario de MTP3.
MGC	Media Gateway Controller.
MSU	Message Signal Unit. Unidad de señalización de mensaje.
MTP	Message Transfer Protocol. Protocolo de transferencia de mensajes de señalización.
MTP3	Message Transfer Protocol layer 3. Capa de red del protocolo de transferencia de mensajes de señalización
OPC	Originating Point Code. Código de punto de señalización origen.
OSI	Open System Interconnection. Interconexión de sistemas abiertos.
PABX	Private Automatic Branch Exchange. Centralita automática privada
PBX	Private Branch Exchange. Centralita privada
PSTN	Public-Switched Telephone Network. Red Telefónica Pública Conmutada.
QoS	Quality of Service. Calidad del servicio
RDSI	Red digital de servicios integrados
RTCP	Real-time Transport Control Protocol. Protocolo de control de transporte en tiempo real.
RTP	Real-time Transport Protocol. Protocolo de transporte en tiempo real
RTPC	Public-Switched Telephone Network. Red Telefónica



	Pública Conmutada.
SCCP	Signalling Connection Control Part. Parte de control de conexión de señalización.
SCP	Service Control Point. Punto de control de servicios.
SCTP	Stream Control Transmission Protocol. Protocolo de transmisión de flujos de control.
SDP	Service Data Point. Punto de datos del servicio.
SG	Signalling Gateway. Pasarela de señalización.
SI	Service Indicator. Indicador de servicio
SIGTRAN	Signalling Transport. Transporte de señalización.
SIP	Session Initiation Protocol. Protocolo de iniciación de sesión.
SLC	Signalling link code. Código de enlace de señalización.
SLS	Signalling link selection. Selección de enlace de señalización.
SPC	Signalling Point Code. Código de punto de señalización.
SS7	Sistema de señalización número siete.
STP	Signalling Transfer Point. Punto de transferencia de señalización.
Stream	Secuencia de mensajes de usuario de SCTP que debe entregarse al nivel superior de forma ordenada.
SUA	SCCP-User Adaptation Layer. Capa de adaptación de usuarios de SCCP.
TCAP	Transaction Capabilities Application Part. Parte de aplicación de capacidades de transacción.
TCP	Transmission Control Protocol. Protocolo de control de transmisión.
TDM	Time division multiplexation. Multiplexación por división en el tiempo.
TUA	TCAP User Adaptation Layer. Capa de adaptación de



usuarios de TCAP.

UDP

User Datagram Protocol. Protocolo de datagramas de usuario.

UIT-T

Unión Internacional de Telecomunicaciones-Sector de normalización de telecomunicaciones.



BIBLIOGRAFÍA

La última versión de la Aplicación de la Referencia SCTP.

<http://www.sctp.org/>

Información sobre todos los RFCs publicados por la IETF.

<http://www.ietf.org>

Todo sobre el grupo de trabajo SIGTRAN.

<http://www.sigtran.org>

Información sobre SIGTRAN y la IETF.

<http://www.ietf.org/html.charters/sigtran-charter.html>

Información sobre señalización SS7.

<http://www.openss7.org/>

Informe al Secretario General y el Informe del Presidente al tercer Foro Mundial de Política de las Telecomunicaciones (WTPF-01)

<http://www.itu.int/osg/spu/wtpf/wtpf2001/index.html>

Redes de datos y comunicaciones de sistemas abiertos»

<http://www.itu.int/ITU-T/studygroups/com07/index.html>

Requisitos y protocolos de señalización» [CE rectora sobre redes inteligentes]

<http://www.itu.int/ITU-T/studygroups/com11/index.html>

