

UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



OPTIMIZACION DEL SERVICIO CELULAR DE DATOS 2G-GPRS
MIGRANDO EL PROTOCOLO DE TRANSPORTE DE LA INTERFAZ
GB

INFORME DE SUFICIENCIA
PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:
DAVID ERNESTO RAMIREZ MOTTA

PROMOCIÓN

2009 - I

LIMA – PERÚ

2013

**OPTIMIZACION DEL SERVICIO CELULAR DE DATOS 2G-GPRS MIGRANDO
EL PROTOCOLO DE TRANSPORTE DE LA INTERFAZ GB**

Este informe está dedicado a mi familia, y muy especialmente a mi madre Felicita, la que me ha alentado incansablemente a culminar el informe.

SUMARIO

El servicio general de paquetes vía radio, que proviene del inglés General Packet Radio Service o simplemente GPRS, es una extensión de sistema global para comunicaciones, o simplificado GSM por sus cifras en inglés. Al ser una ampliación de la Red Celular GSM posee características similares, y en parte heredadas de aquella. Esto quiere decir que algunos elementos funcionales de ambas redes se mantienen. Sin embargo se definieron nuevos elementos de red que sirvieron para estructurar la red de paquetes de datos, ante la necesidad de los usuarios de contar con acceso a servicios de datos en los equipos móviles; servicios tales como internet.

Esta nueva definición implicó también la introducción de nuevos protocolos de comunicación entre los elementos de red que tendrían a cargo el tratamiento y transmisión de los paquetes datos. Es así luego que dichos protocolos tuvieron aplicaciones en función a los requerimientos y capacidades de velocidad y hardware que poseía la infraestructura de red del operador de telecomunicaciones. Un ejemplo de tales protocolos son Frame Relay y el protocolo de Internet o simplemente IP. Ambos protocolos son utilizados en la actualidad en la red GPRS por los distintos operadores.

Es este artículo explicaremos las razones de realizar la migración de protocolos, en una red que utiliza el Frame Relay a una red que utilice IP, así como el procedimiento y los resultados, con el objetivo final de optimizar la calidad y rapidez de las mismas.

INDICE

INTRODUCCIÓN	1
---------------------------	----------

CAPITULO I

PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA	2
---	----------

1.1 Descripción del problema.....	2
-----------------------------------	---

1.2 Objetivos del informe	3
---------------------------------	---

1.3 Evaluación del problema	4
-----------------------------------	---

1.4 Limitaciones del informe.....	5
-----------------------------------	---

CAPITULO II

MARCO TEÓRICO CONCEPTUAL	6
---------------------------------------	----------

2.1 Introducción a la red de Telefonía Celular GSM	6
--	---

2.2 Subsistema de Estación Base (BSS).....	6
--	---

2.3 El subsistema de red (NSS).....	9
-------------------------------------	---

2.4 Subsistema de operación (OSS)	10
---	----

2.5 Introducción a la red GPRS.....	10
-------------------------------------	----

2.7 Interfaz Gb.....	12
----------------------	----

2.7.1 BSSGP:.....	13
-------------------	----

2.7.2 NS: Network Service - Servicio de Red.....	14
--	----

2.8 Frame Relay.	16
-----------------------	----

2.8.1 Trama Frame Relay.....	16
------------------------------	----

2.8.2 Direccionamiento	17
------------------------------	----

2.8.3 Mecanismo de Control de Flujo.	18
---	----

2.8.4 Bits Explícitos de Congestión	18
---	----

2.8.5 Elegibilidad de descarte.....	19
-------------------------------------	----

2.8.6 Conmutación en Frame Relay	20
--	----

2.8.7 Bearer Channel	20
----------------------------	----

2.8.8 PVC	21
-----------------	----

2.8.9 Enlace Virtual de Servicio de Red (NSVL)	21
--	----

2.8.10 Conexión Virtual de Servicio de Red (NSVC).....	21
--	----

2.8.11 Network Service Entity.....	22
2.8.12 BSSGP Virtual Connection	23
2.8.13 Direccionamiento en Frame Relay	24
2.9 Protocolo IP	25
2.9.1 Operación del Protocolo IP	25
2.9.2 Direccionamiento	28
2.9.3 Fragmentación	28
2.9.4 Cabecera IP.....	29
2.10 Load Sharing en una Subred Frame Relay	31
2.10.1 Requerimientos de la función Load Sharing.....	31
2.10 Load Sharing en una subred IP.....	32
2.10.2 Selección del IP endpoint remoto	33
2.11 Función de distribución de recursos	33
2.12 Subnetwork Service Protocol	33
2.12.1 Subnetwork Service Protocol en la Red Frame Relay	33
2.12.2 Subnetwork Service Protocol en la Red IP	34
2.12.3 Fragmentación IP.....	34

CAPITULO III

METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA	36
3.1 Introducción.....	36
3.2 Alternativas de Solución	36
3.3 Solución del problema.....	38
3.3.1 Habilitar la nueva red intermedia.	40
3.3.2 Configurar los switchs SWU y routers OSR.	40
3.3.3 Realizar una prueba piloto.....	40
3.3.4 Migración lógica final de la interface Gb, en ventana de mantenimiento.....	40

CAPITULO IV

ANÁLISIS Y PRESENTACIÓN DE RESULTADOS	42
4.1 Introducción.....	42
4.2 Análisis descriptivo.	42
4.2.1 Payload.....	42
4.3 Análisis teórico de los resultados	43
4.4 Presupuesto y tiempo de ejecución	44

CONCLUSIONES Y RECOMENDACIONES	45
ANEXO A	
CONFIGURACION DE IPs EN EL BSC POR BSCU-PCU.....	46
ANEXO B	
COSTO DEL PROYECTO	48
ANEXO C	
DURACION DEL PROYECTO	50
ANEXO D	
GLOSARIOS DE TERMINOS	52
BIBLIOGRAFIA	54

INTRODUCCIÓN

La tecnología y el internet han permitido a los usuarios hacer uso extensivo de nuevos servicios que han cambiado drásticamente la vida de las personas en los últimos años. Hablamos de transacciones bancarias por internet, la difusión de noticias en tiempo real, redes sociales, etc. Es conocido también que el tráfico de datos está creciendo año a año, en contraste al tráfico de voz, que cada vez sufre de la disminución de los abonados.

El uso de un dispositivo móvil en la actualidad está dominado cada vez más por el servicio de internet o de datos que le permita al usuario comunicarse con sus compañeros de trabajo o amigos de manera más novedosa e interesante que hace unos pocos años. Por este motivo, las empresas de telecomunicaciones buscan construir una infraestructura tecnológica que permita proveer el acceso a internet de tal manera que se asegure una mayor velocidad de transferencia, capacidad de usuarios y un mínimo número de rechazos a los intentos de acceder a la red.

Esto permitirá un mayor consumo del servicio de datos lo que generará mayor recaudación para la operadora, y adicionalmente, habrá un mayor nivel de satisfacción en el cliente y por consiguiente la fidelización del mismo hacia la operadora.

El presente informe busca ayudar a comprender la construcción de dicha infraestructura de acceso, en el que el protocolo de transporte de paquetes de datos cumple un rol fundamental. Este protocolo de transporte con el paso de los años ha sido actualizado o remplazado con la aparición de otros nuevos protocolos más efectivos. Así tenemos el uso de los protocolos X.25, Frame Relay e IP. En este informe se abordará el caso de la migración del uso del protocolo Frame Relay al protocolo IP, como protocolo de transporte de datos en la red de acceso

Cabe recalcar que el presente informe se basa en los datos de una de las más grande operadoras de servicios de telecomunicaciones en Latinoamérica, con cerca de 15 años en el sector, que realizó el proceso de migración de éste protocolo en su red.

Finalmente, en este informe se mostrará el diseño, procedimiento y resultados, de la migración del protocolo de transporte de datos de la interface Gb

CAPÍTULO I

PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1 Descripción del problema

Actualmente en el Perú los servicios de datos móviles requieren mayor ancho de banda y calidad de servicio lo que recae, desde el punto de vista del usuario, es una mejor velocidad de descarga. Eso implica que las páginas webs, o las sesiones de datos se visualicen en el explorador de su equipo terminal cada vez más rápido a medida que los servicios ofrecidos brindan mayor contenido multimedia como videos, fotos, chats, etc. Así en un terminal móvil que soporta la denominada tecnología GPRS/EDGE, como el mostrado en la figura 1.1, se puede hacer uso del servicio de datos con velocidades de descarga de hasta 384 Kbps. Y en este servicio la velocidad de transporte de datos en toda la ruta y en especial en la llamada interface Gb de la red GPRS, cumple un papel importante. Sin embargo las redes de acceso de los operadores móviles de telecomunicaciones tienen un ancho de banda que no está distribuido igualmente para todas las zonas de nuestro país. Plasmando esto en nuestra realidad, un terminal móvil descargará datos a mayor velocidad en la ciudad de Lima que en Huaraz o en Tacna, por ejemplo. Esto debido a que la demanda de tráfico de datos en ciertas zonas es mucho mayor, por lo que la planificación de la red tiene como meta mejoras y nuevas configuraciones en la red de acceso, que implica actualizaciones en la mencionada interface Gb. Esto puede llevar a una optimización de los protocolos de transporte, que ya se ha iniciado en determinadas zonas de la capital peruana, y que es lo que se pretende estudiar en el presente estudio.

Debido a lo expuesto en el párrafo anterior, surge un problema para los operadores de telefonía cuando es necesaria la adaptación y optimización de nuevas tecnologías a su red, debido a que esto implica cambiar o utilizar nuevos elementos y sistemas que procesan, transmiten datos.

El cambio de los protocolos es una de las maneras que se utilizan para la optimización de red. Ya veremos luego que la configuración para el cambio de protocolo de transporte de datos, es una operación que implica una interrupción del servicio durante el tiempo que dure las configuraciones necesarias, debe darse en un tiempo prudencial y con

el menor número de errores, ya que está de por medio un servicio público que debe procurarse verse afectado en lo mínimo.



Figura 1.1 Terminales móviles que soportan transferencias de datos GPRS/EDGE

Esto implica también contar con personal capacitado para la operación y mantenimiento de la red de datos. Asimismo los operadores de telecomunicaciones realizan ensayos previos al cambio de protocolos, para de esa manera contar con la garantía que la red se comportará como previamente se ha diseñado. Por este motivo las medidas con que se cuentan para mitigar el riesgo a errores de ejecución o de diseño son tomadas muy en cuenta.

Finalmente, este informe se elaboró sobre los resultados de la migración del protocolo de transporte usando equipos de una reconocida empresa de tecnología en telecomunicaciones de la actualidad.

1.2 Objetivos del informe

- Dar a conocer las ventajas de utilizar el protocolo IP como transporte alternativo al Frame Relay en la transmisión de datos.
- Comparar la eficiencia de ambos protocolos.
- Presentar los resultados de la migración propuesta.

1.3 Evaluación del problema

El fin de las operadoras es brindar mayor calidad y mejor servicio a sus usuarios. En busca de mejorar tales aspectos, algunas de las tareas que se realizan es la mejora de la velocidad de transmisión. La velocidad de transmisión que percibe el usuario final en su equipo móvil es un valor de los servicios. Por ello se busca optimizarla, lo que se traduce en una actualización de software o de protocolo en algunos casos.

Cuando una operadora de telecomunicaciones realiza una actualización en el software o protocolo, proceso al que se conoce como “upgrade”, el área de planificación determina el alcance del trabajo, y el impacto que tendrá sobre la red. Para ello se requiere conocer, los procesos, la infraestructura tecnológica, los recursos humanos que están involucrados en la operación de las tareas. En la Figura 1.2 se muestra el diagrama de red sobre el cual se ubica la Interface Gb sobre la cual se realizará el cambio del protocolo de transporte, y sobre donde se debe diseñar la segmentación de la red de acceso y del core de datos.

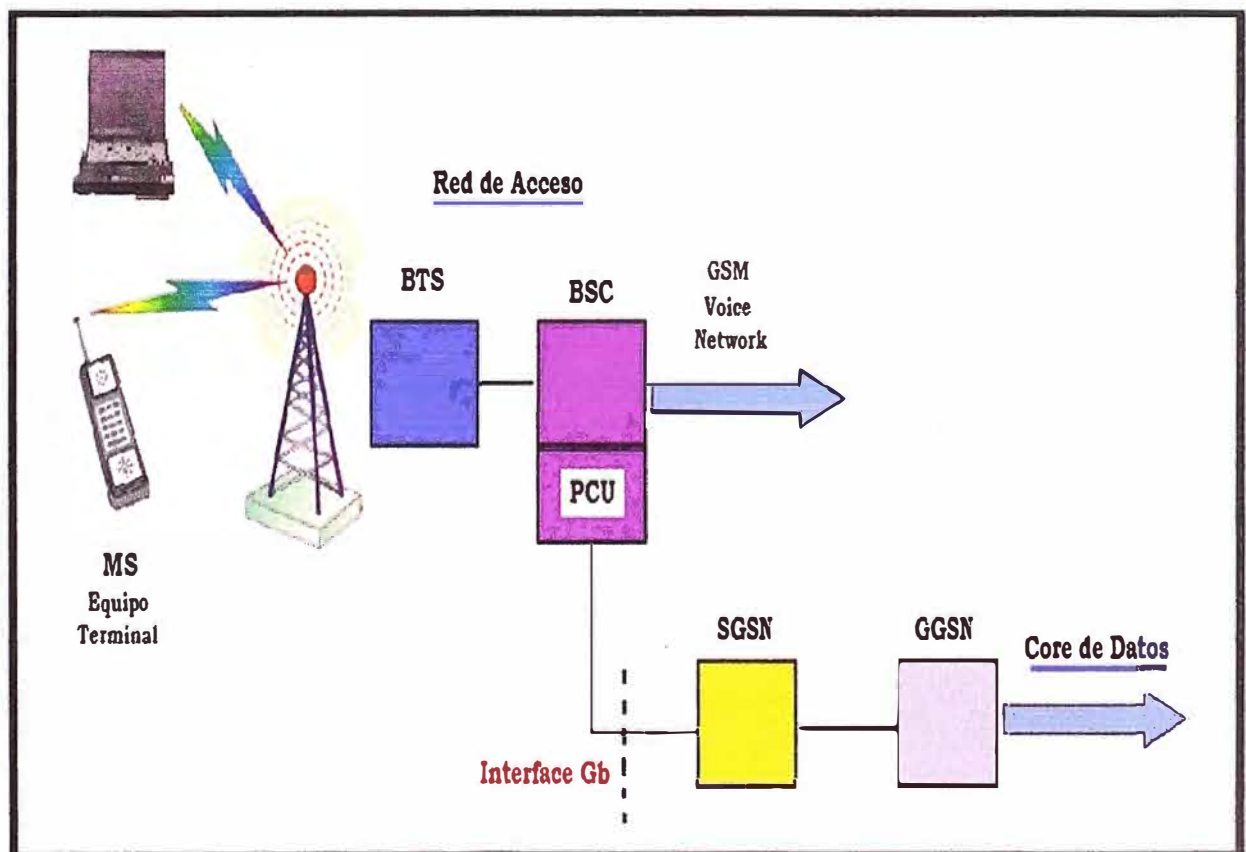


Figura 1.2. Interface Gb.

1.4 Limitaciones del informe.

Según el diagrama de red actual, la implementación de la migración del protocolo de transporte de la Gb a protocolo IP, puede requerir una planificación de ingeniería aun más compleja.

En este informe se desarrollará el proyecto sobre una red física Ethernet y una capa de Red sobre IPv4.

CAPÍTULO II

MARCO TEÓRICO CONCEPTUAL

2.1 Introducción a la red de Telefonía Celular GSM

GSM, acrónimo de Global System for Mobile, fue el primer y el más exitoso sistema celular digital. Su estandarización incluye servicios, interfaces, y arquitectura de protocolos. Es entonces un estándar de telefonía creado para definir la arquitectura la red de telefonía móvil celular de tecnología digital. Los servicios que provee GSM incluyen voz, datos conmutados por circuitos y SMS.

Siendo un sistema de comunicaciones, requiere funcionalidades y componentes que son necesarias para las comunicaciones móviles, tales como:

- Estaciones Base espaciadas regularmente en el área de cobertura.
- Unidades de conmutación para conmutar circuitos y llamadas entre estaciones base y así como también con redes externas.
- Compresión de voz y datos con el fin de maximizar el uso de los limitados recursos de radio.
- Unidades de autenticación que son capaces a autenticar usuarios con el uso de códigos especiales y algoritmos.
- Administración de la localización, a ser usada para realizar llamadas.

La arquitectura GSM está compuesta por 3 subsistemas, sobre los que existen equipos y protocolos con funciones específicas de transmite o recepciona las señales o los paquetes de información. Dichos subsistemas son:

- Subsistema de Estación Base (BSS)
- Subsistema de Red (NSS)
- Subsistema de Operación (OSS)

2.2 Subsistema de Estación Base (BSS)

El subsistema de Estación Base o Base Station Subsystem (BSS) se compone de 2 elementos: la BTS (Base Transceiver Station) localizada generalmente cerca de la torre que

contiene las antenas de transmisión/recepción y el BSC (Base Station Controller). Ambos subsistemas se comunican a través de una interfaz llamada Abis. Un diagrama que grafica los subsistemas se muestra en la Figura N° 2.1

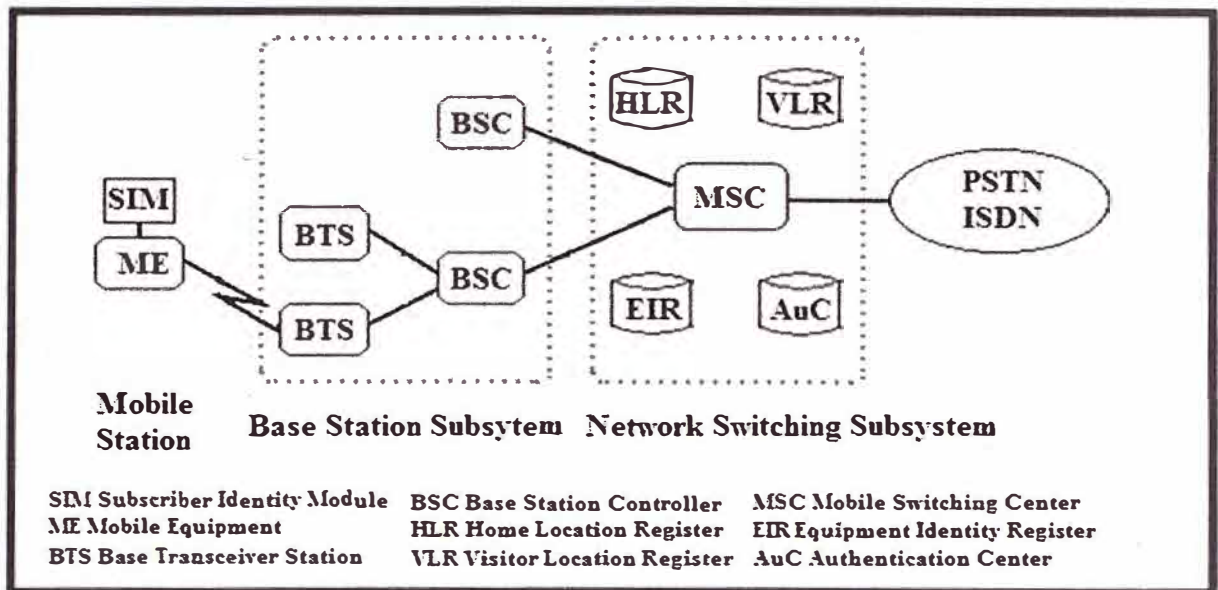


Figura N° 2.1 Subsistemas de la arquitectura GSM.

La BTS contiene a los transceivers de radio, que son dispositivos que manejan las señales de radio y por lo tanto, en conjunción con las antenas permiten brindar cobertura a una zona geográfica. Dicha zona luego se llamaría celda celular, para representar y delimitar el área donde la frecuencia que irradia la antena y el transceiver tiene predominancia. Asimismo estos transceivers tienen la función de manejar los protocolos de la interfaz de radio, enviar y recibir las radiofrecuencias dentro de una zona cercana y brindar cobertura celular a los usuarios. Los transceivers son también llamados TRXs por algunos fabricantes de equipos de telecomunicaciones.

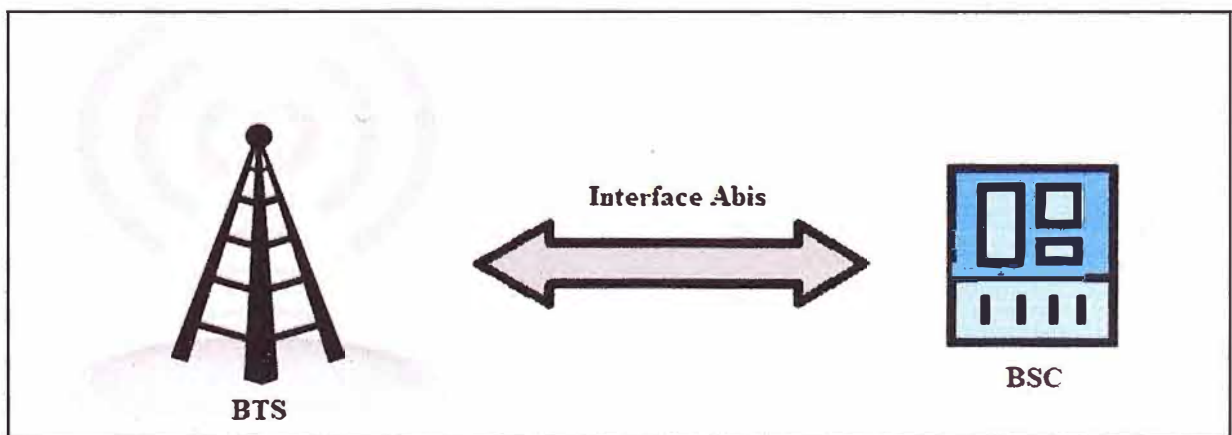


Figura N° 2.2. Interface Abis, ubicada entre el BSC y la BTS

Dichos recursos de radio o frecuencias que se asignan a cada transceiver de cada BTS son gestionadas por el BSC (Base Station Controller), el cual controla la red de radio. Esta gestión se centra en la habilitación de frecuencias que el BSC envía a cada usuario dentro de la cobertura de cada BTS de tal manera que se evite la interferencia y se garantice un aceptable nivel de potencia y calidad a la señal recibida o transmitida. Por tal motivo se dice que el BSC es responsable del control de potencia, que dicho de otra manera es la inteligencia que tiene el software del BSC para enviar señales más potentes a zonas de mucho tráfico o muy alejadas, así como también para trasladar la señal de un usuario en movimiento entre celdas, lo que es conocido como Handover; y finalmente es responsable de agrupar las comunicaciones de los usuarios para trasmitirlas al núcleo o core de la red móvil y así al destino final.

Finalmente el terminal móvil, o simplemente TM, que utiliza el usuario, posee un chip o tarjeta llamado comúnmente tarjeta SIM, de las cifras de Subscriber Identity Module, o SIM Card el cual posee registros compartidos con la central utilizados para la identificación de los subscriptores del servicio móvil. El TM permite a los usuarios cambiar de equipo conservando su número y servicios al solamente cambiar la SIM Card a otro equipo del mismo operador telefónico. Dicha SIM Card almacena además un código llamado IMSI (International Mobil e Subscriber Identity), usado para identificar al suscriptor en el sistema.

Dicho esto, ampliaremos la visión de la arquitectura de red que define GSM, en función del modelo OSI (Open System Interconnection) en la red de Acceso, que es donde el presente informe se desarrolla, para definir los protocolos de comunicación entre los elementos de la red. En la figura 2.3 se muestra las interfaces dentro de la red de acceso.

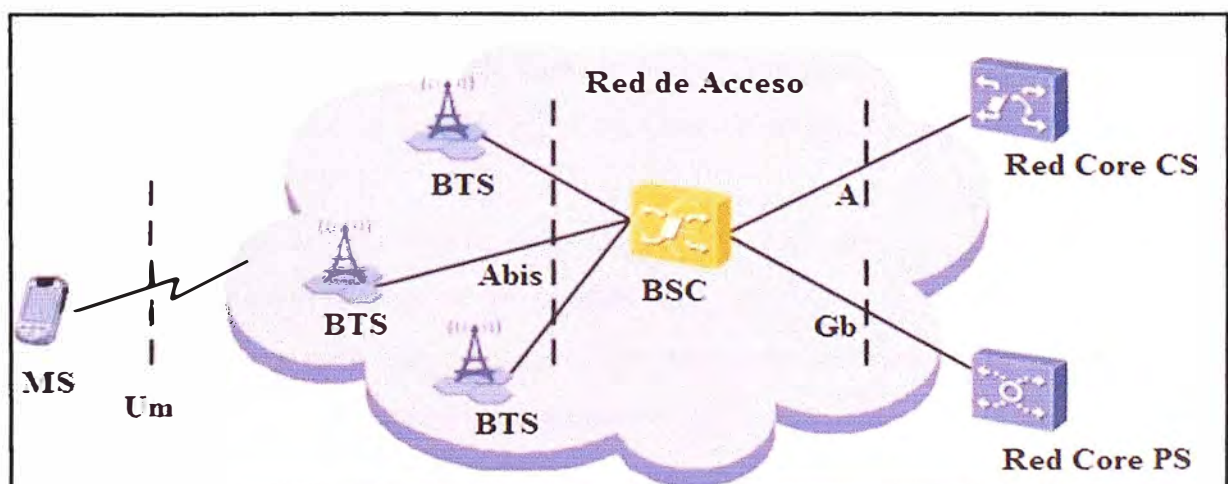


Figura 2.3 Interfaces en la red de Acceso GSM/GPRS.

En la figura 2.4 se muestra otra vista de las interfaces más allá de la red de acceso, propiamente en parte del core de datos teniendo como referencia al SGSN.

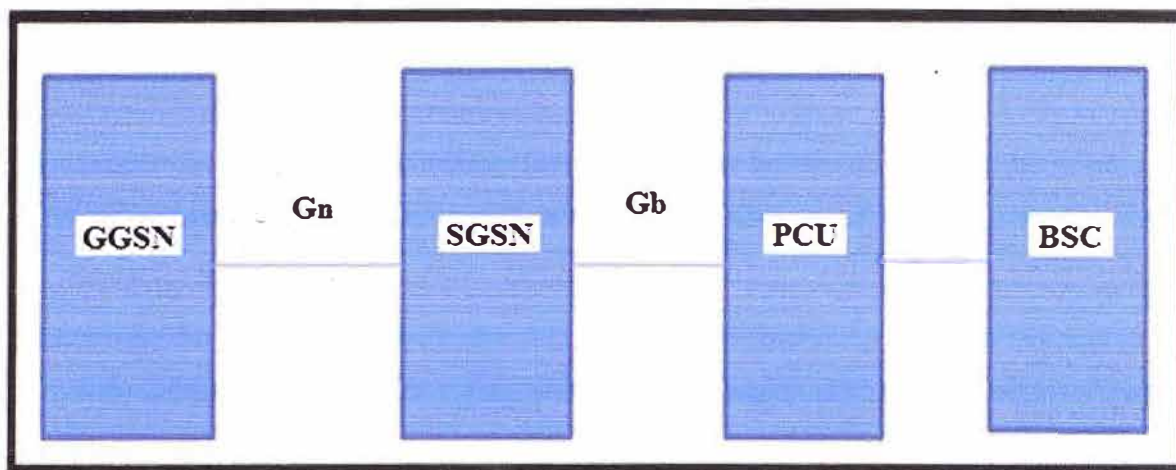


Figura 2.4 Interfaces del SGSN entre elementos del core de datos GSM/GPRS.

Dado que el presente informe se centra en el estudio del protocolo que se maneja en la interface del BSC al SGSN, interface Gb, y no se estudiará las interfaces más allá de la red acceso.

2.3 El subsistema de red (NSS)

Es el subsistema llamado también Core de la Red, ya que concentra los equipos de conmutación y la red inteligente de tarificación. Aquí hay que distinguir el Core de la conmutación de circuitos o de voz, y el core de conmutación de paquetes o de datos. En este documento nos centraremos principalmente en un servicio que atraviesa el core de datos, sin embargo explicaremos brevemente el core de voz.

El elemento principal del core de voz en la central telefónica llamada Mobile services Switching Center (MSC), que se encarga de la conmutación de las llamadas. Esta identifica el origen y el destino de la llamada. El MSC también realiza labores como hand off o desplazamiento de la llamada entre MSCs y de roaming. También provee de una conexión a la red fija PSTN.

En el core de voz asimismo existen otros elementos que cumplen funciones específicas y que están conectados con el MSC:

- HLR (Home Location Register) es el elemento que contiene toda la información administrativa de cada suscriptor registrado en la red GSM con la información de localización, que no necesariamente es la actual, debido a que la función de localización es propia del VLR.

- VLR (Visitor Location Register) contiene información administrativa necesaria para el control de llamada y provisión de servicios al suscriptor en un área geográfica controlada por el VLR.

2.4 Subsistema de operación (OSS)

Entre las funciones del subsistema de operación se encuentran:

- Operación y Mantenimiento de la Red.
- Gestión de Suscripción: precio y tasación.
- Gestión del equipo móvil.

El propósito es la monitorización de elementos de la red. Esto se realiza a través de Workstations conectadas a base de datos que guardan la información de la red. En el presente informe no ahondaremos en la descripción de este subsistema.

2.5 Introducción a la red GPRS

La demanda creciente de los usuarios por acceso a internet ha promovido que los operadores construyan una red sobre la cual transmitir y recibir el flujo de datos. Para servicios de datos que están basados sobre el protocolo IP, tales como e-mail y navegación web, la conmutación por circuitos realizada por GSM es ineficiente. Dichas ineficiencias de GSM se van corrigiendo a través de actualizaciones o publicaciones llamadas Releases. En el Release '97 del GSM se introdujo el General Packet Radio Service (GPRS), el cual mantiene las tecnologías de acceso GSM BSS ofreciendo a la vez servicios de datos de paquetes conmutados al terminal móvil.

2.6 Conexiones de Paquetes Conmutados y Circuitos Conmutados

- **Conexiones de circuitos conmutados:** El standard GSM utiliza conexiones de circuito conmutado (CS). Cada vez que una conexión es requerida entre dos puntos, una conexión es establecida entre ellos, y los recursos de la red son reservados y dedicados para el uso de los suscriptores durante toda la duración de la llamada.
- **Conexiones de paquetes conmutados:** Las redes de datos tales como Internet, X.25 y Frame Relay usan conexiones de paquetes conmutados (PS), donde la data es dividida dentro de paquetes, y cada paquete tiene una dirección o un identificador que es usado por los enrutadores de la red para pasarlos a su destino. GPRS trae conmutación de paquetes a las redes GSM.

El ancho de banda en la red de paquetes conmutados (PS) no se reserva continuamente, como en el caso de los circuitos conmutados. En vez de eso, el ancho de banda de la red es asignado cuando se requiere y liberado cuando no se necesita.

En las conexiones móviles GPRS, los paquetes de diferentes estaciones móviles pueden ser multiplexados en una manera estadística sobre la interface aérea lo cual ofrece uso muy eficiente de los radio canales. Cada canal de radio solamente está ocupado por el usuario cuando hay paquetes de datos para rec-ibir o transmitir.

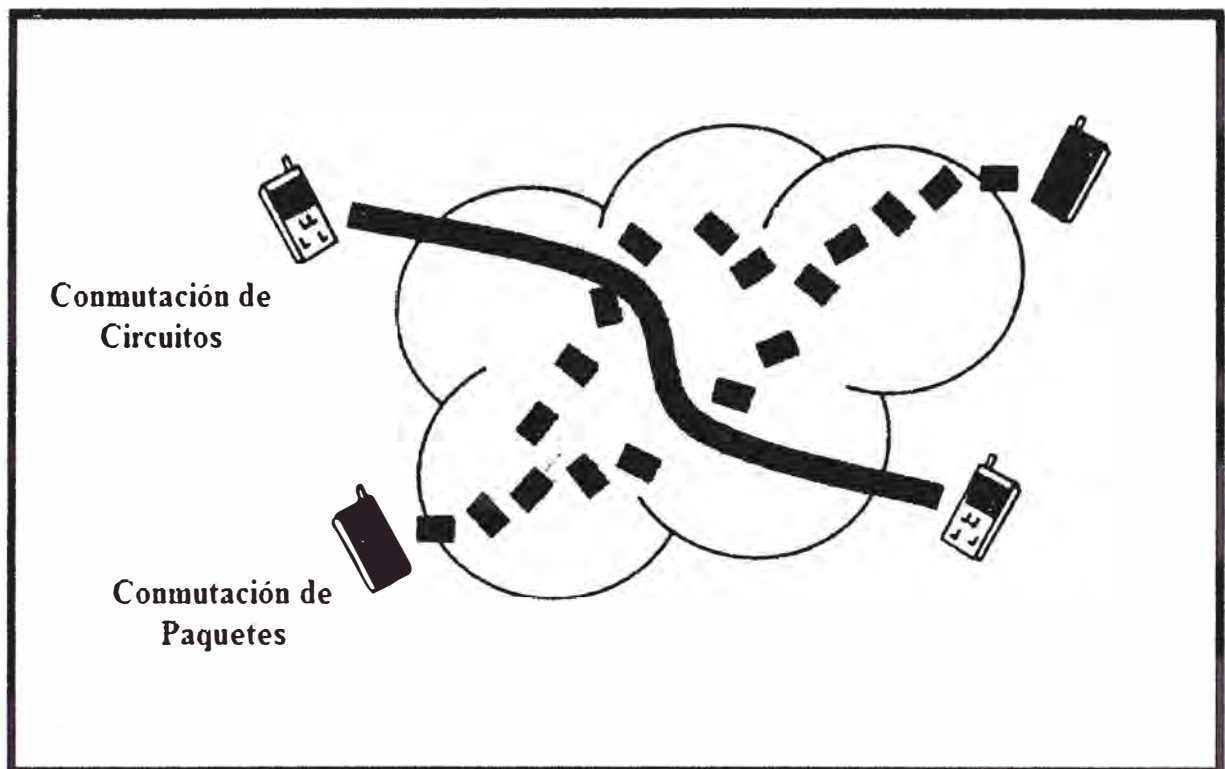


Figura 2.5 Paquetes conmutados y circuitos conmutados

El sistema actual GSM fue originalmente diseñado con un énfasis sobre aplicaciones de voz, el principal objetivo de GPRS es ofrecer acceso a las redes de datos usando protocolos tales como TCP/IP (Transmission Control Protocol) y X.25. Estas redes externas de datos consideran a GPRS simplemente otra subred.

GPRS ofrece transmisiones de paquetes a través de la red en distintas fases. Por ejemplo, una vez que los paquetes de datos han sido transmitidos sobre la interface aérea, los recursos de radio pueden ser liberados para otros usuarios. Los paquetes viajan a su destino a través del backbone GPRS y luego dentro de una red de datos tal como Internet.

Esto hace más eficiente el uso de la red y de los recursos de radio. Si apreciamos en la Figura 2.4 se destacan nuevos elementos en la estructura GPRS: el SGSN y el GGSN.

A continuación detallaremos estos nuevos elementos de la red GSM/GPRS

El nodo **GGSN** (Gateway GPRS Support Node), es el gateway o pasarela entre la red GPRS y la red de datos pública PDN u otras redes GPRS. El GGSN se encarga de las funciones autenticación y gestión de localización, conecta el registro de abonados locales al HLR por medio de la interfaz Gc y cuenta el número de paquetes transmitidos, para facturar a los abonados con exactitud.

El nodo **SGSN** (Serving GPRS Support Node), controla la conexión entre la red y el terminal móvil. El SGSN se encarga de controlar las sesiones y las funciones de gestión de movilidad de GPRS, como radio búsquedas, comandos de enganche o desenganche de la red y trasposos. Se conecta al HLR a través de la interfaz Gr. También cuenta el número de paquetes que encamina.

El BSC contiene la unidad PCU (Packet Control Unit), que se encuentra físicamente dentro del gabinete del BSC. El PCU realiza funciones de conversión de datos desde el formato de paquetes a otro formato que pueda transferirse a través de la interfaz aérea, además de la gestión de los recursos de radio y la implementación de medidas de calidad de servicio. El PCU es una unidad computacional separada de las funciones básicas del BSC, con función exclusiva de manejar los paquetes de datos GPRS o de red evolución de GPRS llamada EDGE (**E**nhanced **D**ata **R**ates for **G**SM **E**volution), por lo cual es conveniente agrupar al BSC y al PCU dentro de un mismo término: BSC-PCU.

Cabe mencionar que el los resultados de este informe, en lo que respecta a la migración del protocolo en la interfaz Gb, es aplicable también a la red EDGE.

Es así que la interfaz de comunicaciones entre el BSC-PCU y el SGSN a la que se denomina Gb, es la que se estudiará en este informe así como los protocolos que en ésta se definen.

2.7 Interfaz Gb.

La Figura 2.6 muestra la posición definida de la interface Gb dentro del modelo de red GPRS. En ésta interface se realiza el intercambio de información de señalización y data de usuarios, y la multiplexación de muchos usuarios sobre el mismo recurso físico. Al ser una interface estandarizada se permite el funcionamiento de diferentes proveedores entre el subsistema BSS y el SGSN.

La figura 2.7 muestra la pila, agrupación o también llamado “stack” de los protocolos utilizados entre el SGSN y el subsistema BSS. En ella se puede apreciar que la

capa NS ha sido dividida en 2 subcapas para conformarse la subcapa NS Control (NSC) independiente de la red de transmisión intermedia, y la capa Subnetwork Service.

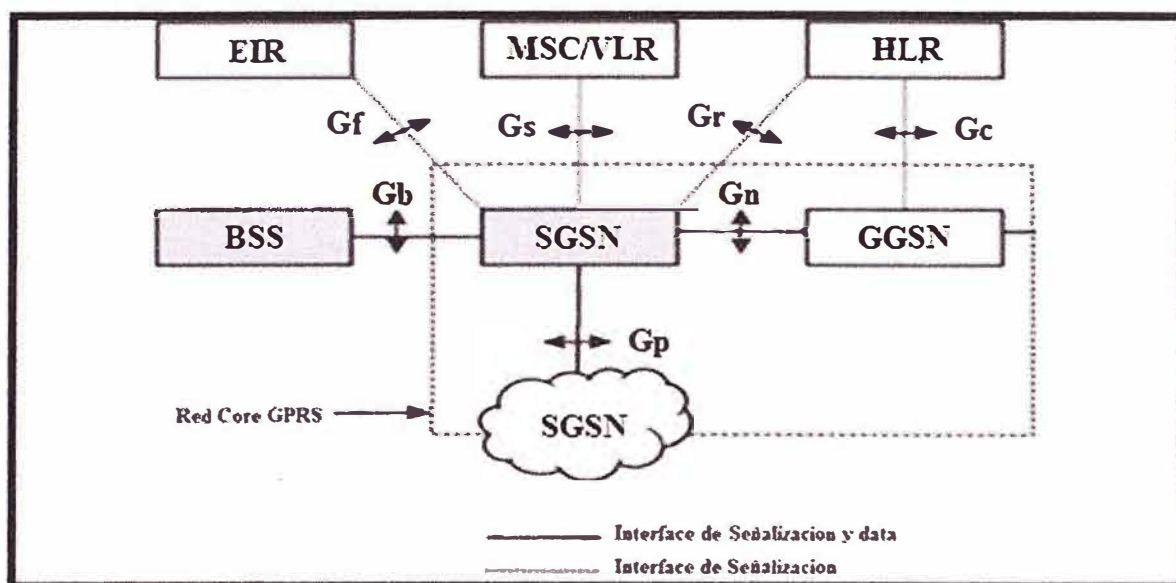


Figura 2.6 Interfaces de conexión en la red GPRS

A continuación se detallan brevemente las funciones de cada una de las capas involucradas.

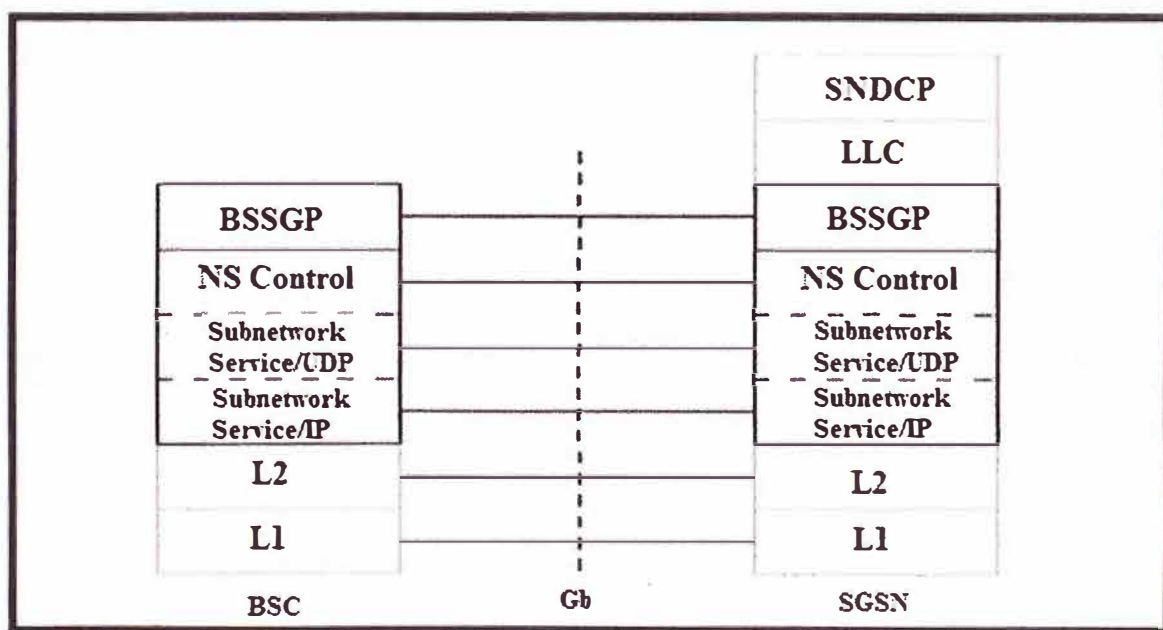


Figura 2.7 Pila de protocolos en la interfaz Gb.

2.7.1 BSSGP: Base Station System GPRS Protocol

Como comentamos anteriormente, se emplea el modelo OSI para realizar un entendimiento del intercambio de información entre el BSC y el SGSN, ósea en la interfaz

Gb. Si exploramos en la capa BSSGP, encontramos que las tareas son la de transferir información de señalización y data de usuarios entre un BSS y un SGSN, asimismo la función de proveer calidad de servicio (QoS), e información de enrutamiento requerida para transmitir data de usuario entre el BSS y el SGSN. Una función secundaria es la de habilitar nodos distintos físicamente, el SGSN y el BSS, para operar con funciones de administración.

El SGSN tiene que habilitar un protocolo BSSGP por cada nodo BSS que tiene a su cargo, por lo tanto hay finalmente una relación uno a uno.

A continuación se resaltan algunas de las principales funciones realizadas en la capa BSSGP:

- Proveer un enlace sin conexión entre el SGSN y el BSS.
- Transferir data en un camino no confirmado entre el SGSN y el BSS.
- Proveer control de flujo bidireccional del flujo de datos entre el SGSN y el BSS.
- Manejar pedidos de paging desde el SGSN hacia el BSS.
- Dar soporte para borrar mensaje antiguos en el BSS, por ejemplo cuando un MS cambia de BSSs.
- Soportar múltiples conexiones de capa 2 entre el SGSN y el BSS.

2.7.2 NS: Network Service - Servicio de Red

En esta capa se realiza la transferencia de datos de paquetes de protocolos de capas superiores que son llamados Network Service SDUs. Los NS SDUs son transferidos a orden del Network Service.

Otra de las funciones es la indicación de congestión de red. Las acciones de control de recuperación de la congestión pueden ser realizadas por el Subservicio de Red (ejemplo Frame Relay). Los mecanismos de reporte de congestión disponibles en la implementación del subservicio de red, deberán ser usados por el Network Service para reportar congestión.

El Network Service está compuesto de una entidad compuesta por una entidad dependiente de la red de transmisión intermedia usada para la interface Gb, el Sub servicio de red (SNS), y de una entidad de control independiente de tal red, la Network Service Control. Hay una relación jerárquica entre ambas entidades. Esto se muestra en la Figura 2.8. Los mecanismos de comunicación detallada entre ambas entidades es materia interna del Network Service y no están estandarizados. El Sub Network Service provee un servicio de comunicación a las entidades correspondientes del Network Service Control.

En otras palabras las entidades del Network Service Control utilizan el Sub Network Service para la comunicación entre cada uno de ellos.

La comunicación uno a uno a través de la interface Gb de entidades remotas del Network Service Control es realizada sobre Network Service Virtual Connections (NS-VCs). Una NS-VC es una ruta de comunicación virtual entre entidades pares del Network Service Control.

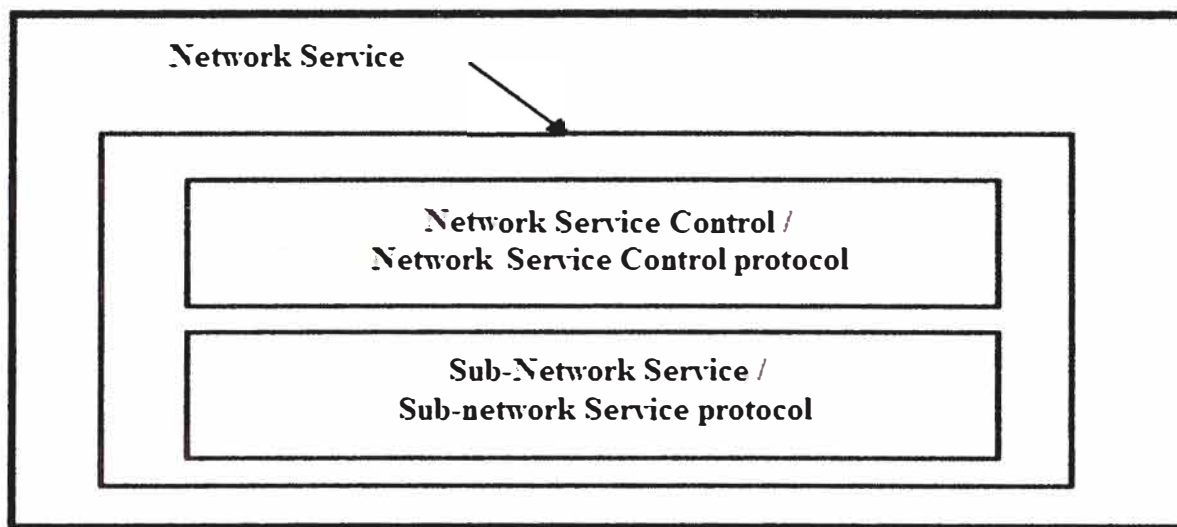


Figura 2.8 Arquitectura interna del Network Service

La entidad Network Service provee un servicio de comunicación entre entidades similares que utilizan el Network Service, así la comunicación par a par entre entidades remotas usuarias del NS es realizada sobre las BSSGP Virtual Connections (BVCs). Un BVC es una ruta virtual de comunicación entre usuarios pares del NS. Un Network Service Entity se comunica sólo con un par Network Service Entity.

La entidad del Network Service Control es responsable de las siguientes funciones:

- La transmisión de NS SDUs. El NS SDU será transmitido sobre el NS-VC. Los NS SDUs están encapsulados dentro Network Service Control PDUs los cuales son a su vez encapsulados en dentro de los Subnetworks Service PDUs.
- Load Sharing o balanceo de carga. La función de load sharing distribuye el tráfico de NS SDUs entre los NS-VCs disponibles de un grupo.
- Administración del NS-VC: Un procedimiento de bloqueo es usado por una entidad NS para informar a la entidad par NS cuando un NS-VC se convierte en no disponible para tráfico de usuarios NS. Existe un procedimiento de desbloqueo para la operación de bloqueo. Un procedimiento de reset es usado entre entidades pares NS para ordenar

configurar a un NS-VC en un determinado estado, después que aparezcan inconsistencias en los estados de los NS-VCs en ambos lados de la interface Gb.

También hay un procedimiento de test para chequear que un NS-VC está operando apropiadamente entre entidades pares NS.

2.8 Frame Relay.

Ahora detallaremos uno de los conceptos más importantes dentro del estudio de este informe, el que está relacionado al protocolo Frame Relay.

Frame relay es un protocolo de red de comunicaciones que define cómo se direccionan las tramas por una red rápida de paquetes a partir del campo de dirección de la trama. Frame relay aprovecha la fiabilidad de las redes de comunicaciones de datos para minimizar la comprobación de errores efectuada por los nodos de red.

Es una evolución de la tecnología de conmutación de paquetes X.25. Está basada en la idea de Circuitos Virtuales (VC). Hay 2 tipos de VC: Permanentes (PVC) que son asignados bajo demanda o los Conmutados (SVC). La interface Gb sólo trabaja con los circuitos permanentes. El PVC está definido como una conexión entre 2 puntos finales. Ésta es una ruta fija, esto significa que no es asignada dinámicamente o cuando ingresa una llamada. A diferencia de X25, Frame Relay elimina todos el procesamiento de la capa 3, y sólo algunas funciones de la capa 2 son usadas, tales como chequeo de validación, trama libre de error pero no hay pedido de retransmisión cuando un error es encontrado. Cuando se recibe una trama Frame Relay errónea ésta es eliminada.

2.8.1 Trama Frame Relay.

Frame Relay usa una estructura de entramado de longitud variable. Esto se muestra en la Figura 2.9. Hay 2 banderas (Flags) que limitan la trama. Una secuencia de chequeo de trama (FCS: Frame Check Sequence) es agregada para protección de la integridad.

El campo de dirección DLCI tiene una longitud variable (6 o 10 bits de longitud). El End Address (EA) es usado para administrar la longitud del campo de dirección. Cuando éste es 0, el siguiente octeto contiene el resto de la dirección, de otra manera, éste indica el último campo de la dirección. El bit C/R indica si la trama es una trama de comando o es una trama de respuesta.

Los bits BECN y FECN son usados para evitar la congestión, cuando una situación de congestión está a punto de ocurrir en una dirección o en la dirección contraria.

La fuente final que recibe esta información reducirá el volumen de información que fluye en la red o también llamado throughput.

El bit DE permite a los nodos de la red indicar cuáles tramas serán eliminadas primero en caso de congestión.

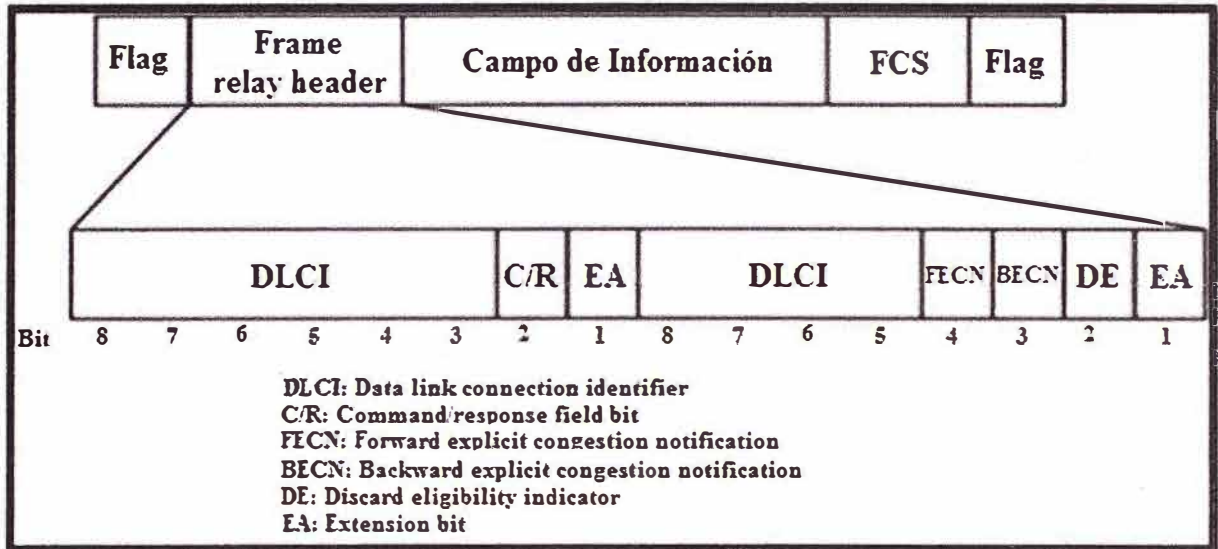


Figura 2.9 Trama Frame Relay

2.8.2 Direccionamiento

La cabecera Frame Relay contiene un campo de 10 bits llamado DLCI (data link connection identifier).

El DLCI es el número de circuito virtual (VC) del Frame Relay con significado local, que corresponde a un destino particular. Este número es usado para distinguir la conexión entre el punto final y el switch Frame Relay entre todas las otras conexiones que son compartidas por el mismo puerto.

El DLCI permite que la data que llega al switch sea enviada a través de la red usando un simple proceso de tres pasos: Primero la integridad de la trama es chequeada con el FCS. Si un error es encontrado, la trama es descartada (la recuperación de error es realizada en una capa más alta). Luego el DLCI entrante es observado en la tabla de enrutamiento. La conexión saliente es identificada, junto con el DLCI saliente. La trama es entonces dirigida hacia su destino al enviarse hacia la dirección especificada en la tabla con el DLCI saliente.

La figura 2.10 ilustra una red imaginaria Frame Relay compuesta de 4 switches. Entre los 2 usuarios finales, un PVC es establecido. El arreglo muestra la conmutación en cada switch y el DLCI asociado con cada conexión usada para definir el PVC. EL número

de DLCI cambia a través de la red de switch a switch, para el mismo PVC. Los DLCIs sólo tienen significado local para cada puerto.

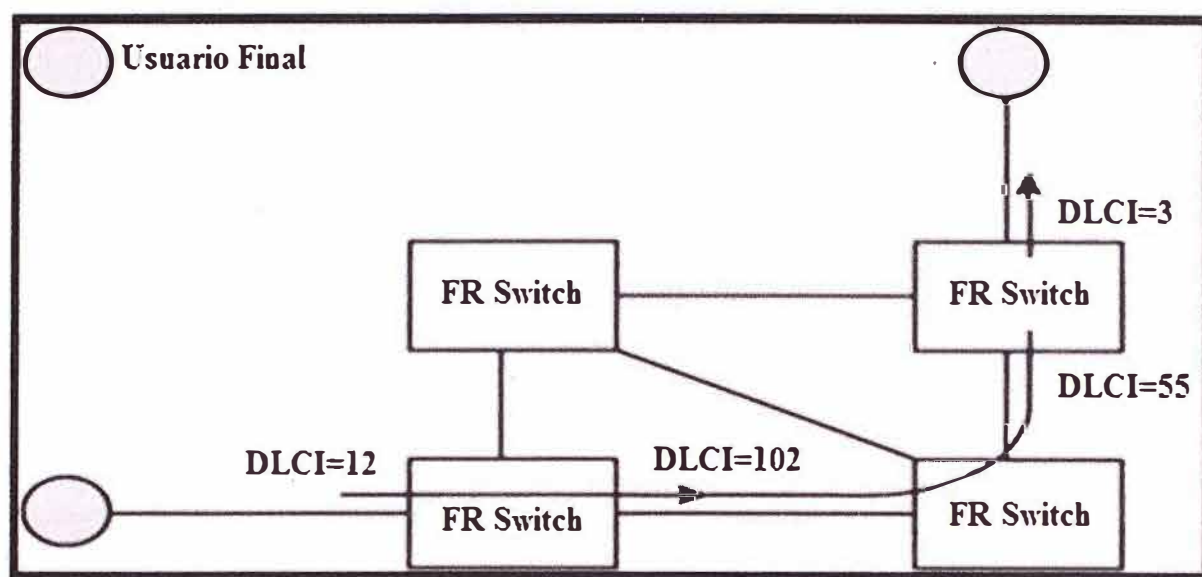


Figura 2.10 Ejemplo de una red Frame Relay

2.8.3 Mecanismo de Control de Flujo.

En congestión severa, todo el flujo de datos de la red puede disminuir, y la única manera de recuperación es la disminución de tráfico del usuario final. Por esta razón varios mecanismos han sido desarrollados para notificar al usuario final la ocurrencia de congestión y así estos usuarios deberían reducir su carga de tráfico.

Hay 2 tipos de mecanismos para minimizar, detectar, y recuperar de situaciones de congestión.

- Notificación de congestión explícita.
- Elegibilidad de descarte.

Estos mecanismos usan bits específicos contenidos en la cabecera de cada trama: FECN, BECN y DE.

2.8.4 Bits Explícitos de Congestión

El primer mecanismo usa 2 bits de notificación de congestión explícita (ECN) en la cabecera de Frame Relay. Ellos son llamados bits BECN y FECN. La figura 2.11 representa el uso de estos bits cuando un switch FR está congestionado.

Supongamos que el switch B en color gris en la figura se acerca a un estado de congestión. Esto puede ser causado por un pico temporal en el tráfico que viene en el nodo

de varias fuentes, o un pico en la cantidad de tráfico entre B y C. En este a notificación de renvío de congestión se produce así:

El switch FR "B" se detecta el inicio de la congestión sobre la base de medidas internas tales como el uso de memoria buffer o longitud de la cola. El switch FR "B" señalaría al switch FR "C" de la congestión, cambiando el FECN contenida dentro de las tramas destinadas al switch FR "C" de 0 a 1.

Todos los nodos intermedios, así como los dispositivos conectados del usuario (fuente y destino) sabrían que la congestión se produce en los DLCI afectados.

A veces es más útil para notificar al origen del tráfico que existe congestión, de modo que la fuente pueda ralentizar hasta que desaparezca la congestión. Esto se llama notificación de congestión hacia atrás.

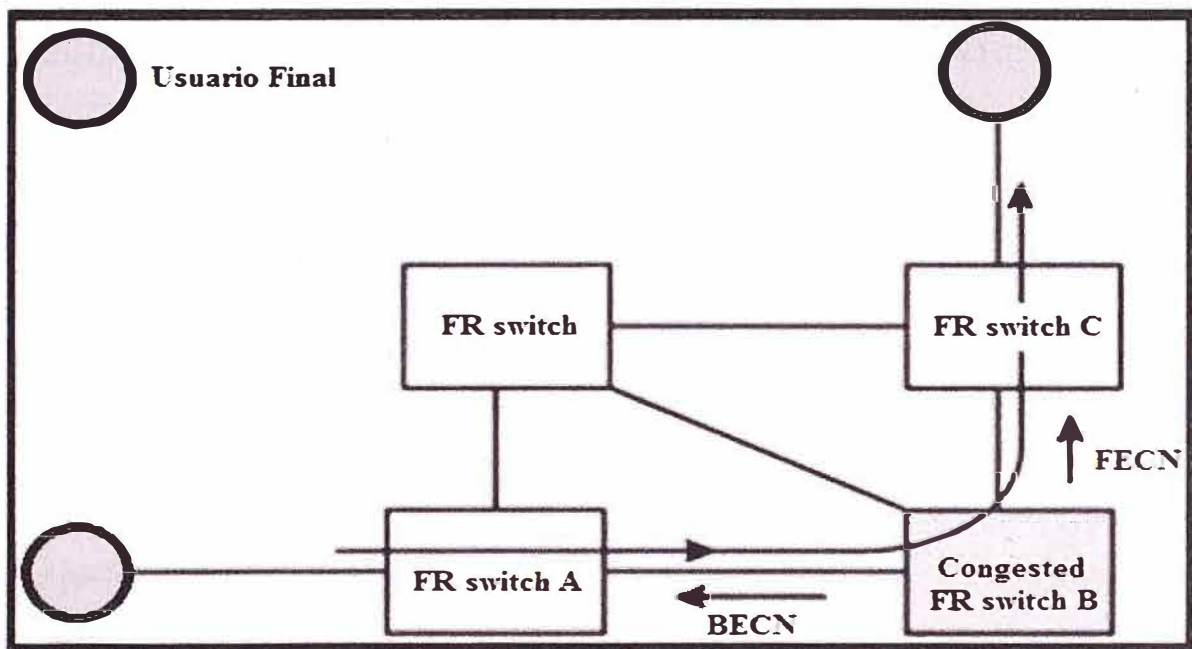


Figura 2.11 Bits de notificación de error

En nuestro ejemplo, el switch FR B mira tramas que vienen en las otras direcciones de la conexión. Se establece el bit BECN dentro de esas tramas para señalar congestión a los nodos de anteriores y al dispositivo de usuario conectado.

2.8.5 Elegibilidad de descarte

Las normas de FR establecen que el dispositivo de usuario debe reducir su tráfico en respuesta a una notificación de congestión. La aplicación de las acciones recomendadas por el dispositivo del usuario se traducirá en una disminución en el tráfico en la red,

reduciendo así la congestión. Sin embargo, si el dispositivo de usuario es incapaz de responder a los mecanismos de señalización, que podría simplemente ignorar la señal de congestión y continuar para transmitir datos a la misma velocidad que antes. Esto llevaría a la congestión constante o al incremento de congestión.

Cuando se produce la congestión, la red debe decidir qué tramas descartar. Esto se hace con el bit DE. Cuando el bit DE se establece en 1, hace que la trama sea elegible para descarte en situaciones de congestión. El bit DE se establece en 1 de los conmutadores Frame Relay cuando la fuente transmite imágenes a una velocidad superior a la tasa contratada.

2.8.6 Conmutación en Frame Relay

El direccionamiento en la interface Gb es realizado sobre conexiones virtuales. En las cap-as NS y BSSGP, cada entidad se comunica con su par a través de este tipo de conexión. El objetivo es explicar la jerarquía entre las diferentes conexiones virtuales e introducir las palabras técnicas que son usadas en la descripción de la interface Gb.

La figura 2.12 muestra una vista de los diferentes niveles de direccionamiento sobre la interface Gb.

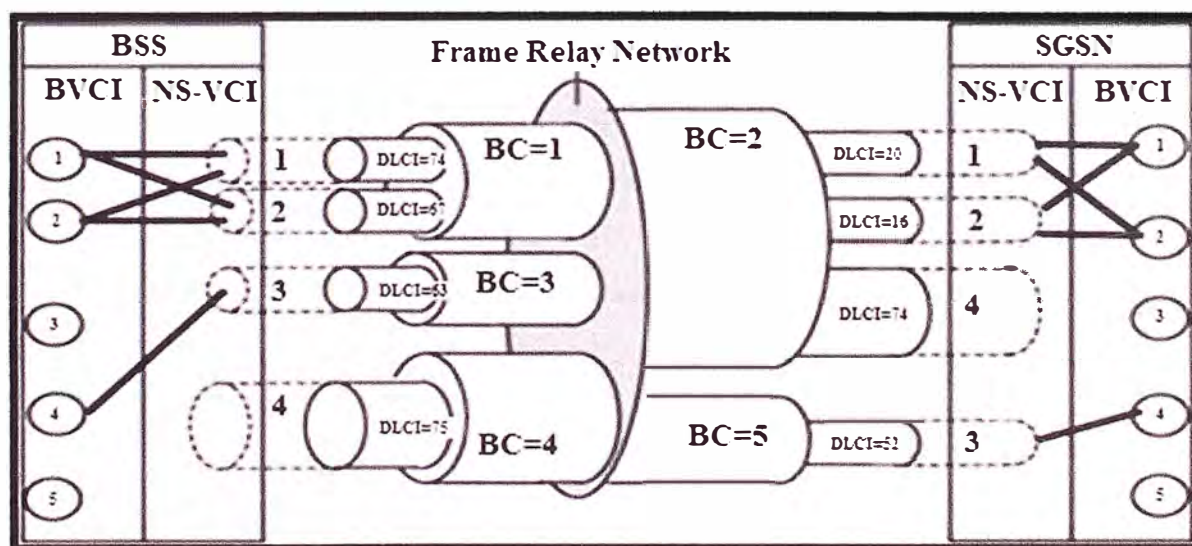


Figura 2.12 Direccionamiento en la interface Gb.

2.8.7 Bearer Channel

Un Bearer Channel (BC) es un canal físico que transporta toda la trama señalización y data de Frame Relay. Un BC podría ser un canal múltiplo de 64 Kbps sobre

un enlace con Modulación por Código de Pulso o también llamado PCM (2,048 Kbps para un enlace Europeo E1, 1544 Kbps para un enlace norteamericano T1). El enlace PCM es el enlace típico de transmisión que se usa en las redes de telecomunicaciones.

2.8.8 PVC

El PVC (Permanent Virtual Connection) permite multiplexar diferentes flujos sobre el Bearer Channel. El BC puede soportar muchos PVCs. En el lado BSS, un DLCI que puede ser diferente del que existe en el lado SGSN, identifica un PVC.

Existe un DLCI, igual a 0, que es usado para propósitos de señalización (administración del enlace). Este DLCI no identifica un PVC.

2.8.9 Enlace Virtual de Servicio de Red (NSVL)

Un SGSN y un BSS pueden estar conectados directamente a través una conexión física o pueden estar conectados indirectamente a través de un equipo de transmisión intermedio o redes de transmisión, donde en cada caso son usados diferentes tipos de conexión. Un SGSN y un BSS pueden a la vez usar diferentes enlaces físicos para conectarse entre ellos.

Cada enlace físico soporta uno o más NSVLs. Cada NSVL es soportado por solo un enlace físico si el Sub Network Frame Relay es empleado. Cuando se utiliza un sub network IP, el NSVL es mapeado a una IP.

El concepto de NSVL es introducido para identificar el enlace definido por un PVC y su BC de soporte. Cada NS-VL es identificado por un NS-VLI (network service virtual link identifier). El significado y estructura exacta de un NSVLI depende de la configuración de la interface Gb y de la red intermedia empleada. Por ejemplo, en el caso de una red Frame Relay, el enlace físico en el Freame relay Bearer Channel (BC). Un NSVLI corresponde a la asociación de un DLCI e identificador de BC.

2.8.10 Conexión Virtual de Servicio de Red (NSVC)

Como se mostró anteriormente la capa de Servicio de Red (NS) ha sido dividida en dos subcapas, SNS y SNC, para tener la subcapa SNC independiente de la red de transmisión intermedia (Frame Relay). Para proveer una conexión punto final a punto final entre el BSS y el SGSN sin necesidad de que haya configuración exacta de la interface Gb y la red de transmisión, el concepto de NSVC, network service virtual connection, ha sido introducida la capa SNC.

Los NSVCs son conexiones virtuales punto a punto en el BSS y SGSN. Cada NSVC está asociado a con un PVC en la capa SNS. En el caso de una subnetwork Frame Relay, en cada lado de la interface Gb, hay una correspondencia uno a uno entre NSVLs y NSVCs. Cuando se emplea una subnetwork IP, un NSVL puede servir a varias NSVCs.

En el caso de la red Frame Relay, el NSVC es la conexión virtual permanente (PVC). Cada NSVC es identificado por un identificador NSVC (NSVCI) que tiene significado punto a punto a través de la interface Gb. NSVC y PVCs están estáticamente configurados por el operador de la red a través de configuraciones de Operación y Mantenimiento. La figura 2.13 muestra la relación entre NSVC y NS-VLs para una subnetwork Frame Relay. La figura muestra la configuración con un solo NSE, pero múltiples NSE entre el BSS y el SGSN están permitidos. En el caso de una red IP, el NSVC está dado por un par de IP finales en el BSS y el SGSN.

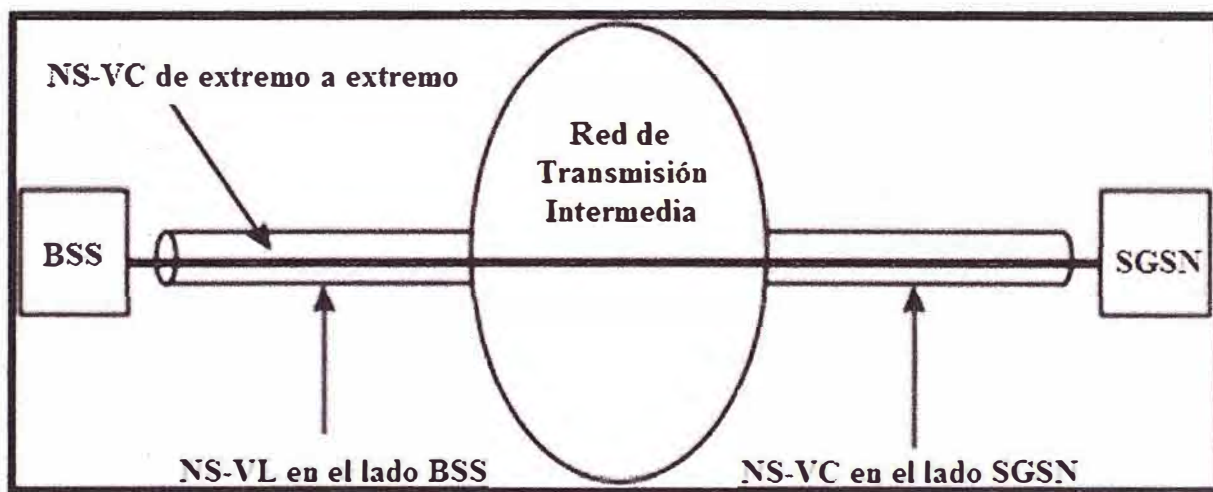


Figura 2.13 Los NS-VCs y NS-VLs

2.8.11 Network Service Entity

Un Network Service Entity el cual está compuesto por un grupo de NSVCs, provee un servicio de comunicación a las entidades pares del servicio de red o NS, es decir entre el SGSN y el BSS. Un Network Service Entity Identifier identifica cada NSE que tiene significado fin a fin a través de la interface Gb. El NSE en cada lado de la interface Gb maneja el tráfico desde o hacia un grupo de celdas.

Un SGSN puede ser enlazado a diferentes BSSs. Los conceptos de NSE y el NSEI pueden ser usados para identificar diferentes BSS conectados al mismo SGSN. Cada BSS es identificado por diferentes NSEIs en el lado del SGSN. Un grupo de NSVCs es definido dentro del NSE identificado por el NSEI para comunicarse con el BSS.

Un NSE y el grupo de NSVCs que lo integran están definidos por el operador de a través del OyM.

La importancia de tener muchos NSVCs dentro de un NSE es distribuir el tráfico desde todas las celdas que pertenecen a éste NSE. En caso de un problema en un NSVC, el tráfico no es interrumpido y es enviado a través de otros enlaces.

2.8.12 BSSGP Virtual Connection

El BVC es una conexión virtual de fin a fin entre el BSS y el SGSN en la capa BSSGP. Un BVC es identificado por un BVCI y tiene significado fin a fin a través de la interface Gb. Un NSEI es asociado con un conjunto de BVCs que son dinámicamente mapeados dentro de sus correspondientes NSVCs.

Dos tipos de BVCs han sido definidos:

- BVCs PTP que están dedicados al tráfico GPRS de una celda (todo el tráfico de señalización dedicado a ésta celda es transmitida vía la correspondiente BVC).
- BVCs de señalización que manejan la señalización del NSE del cual pertenecen.

En el lado del SGSN, la asociación NSEI, BVCI identifica una celda. En el lado del BSS, los BVCI, están estáticamente configurados por razones administrativas. En el lado del SGSN, los BVCI asociados con entidades con funciones PTP está dinámicamente configurados, y BVCI asociados con entidades con funciones de señalización está estáticamente configurados.

En la Figura 2.14 se muestra el uso en la interface Gb, cuando existe una conexión entre nodos de acceso a múltiples nodos de Core. Un Network Service Entity

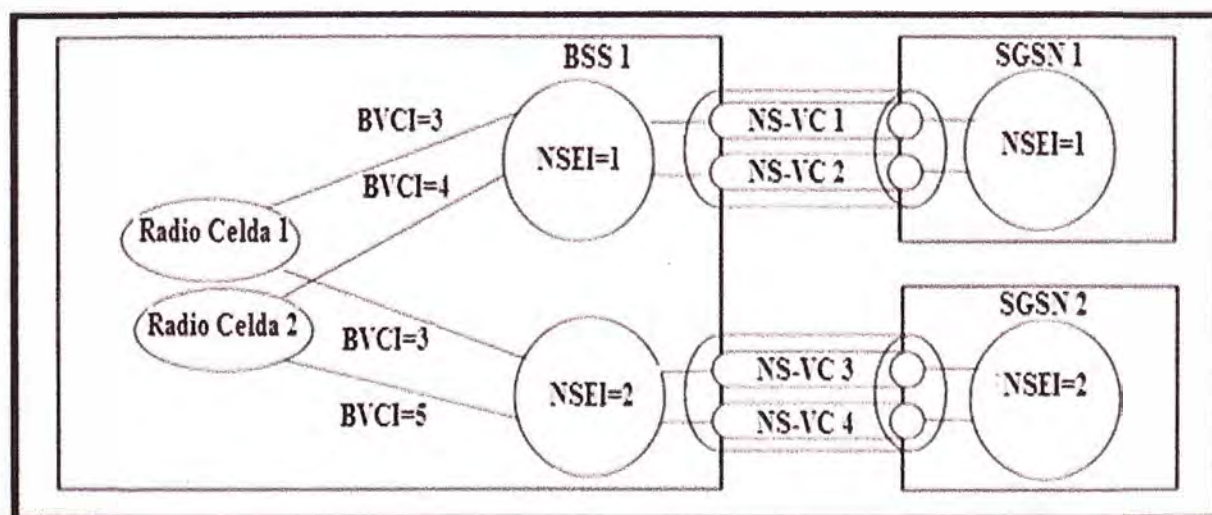


Figura 2.14 Relación entre BVCI, NSEI y NSVC.

2.8.13 Direccionamiento en Frame Relay

La figura 2.14 muestra una referencia de los diferentes elementos presentados en las secciones previas. Específicamente se muestran las celdas 1 y 2 que está diferenciadas por los BVCi 1 y 2, respectivamente. Ellos comparten los dos NSVCs identificados por NVCI 1 y 2.

El NSVCI 1 corresponde al PVC identificado por el DLCI = 74 sobre el BCI = 1 en el lado del BSS y el DLCI = 20 sobre el BC identificado por el BCI = 2 en el lado del SGSN. El NSVC 2 es mapeado sobre el PVC identificado por el DLCI = 67 sobre el BC identificado por el BCI = 1 en el lado del BSS y DLCI = 16 sobre el BC identificado por el BCI = 2 en el lado del SGSN.

Todo el tráfico direccionado a la celda 1 o la celda 2 desde el SGSN o recibida en la celda 1 o en la celda 2 en el BSS es transferida al correspondiente BVC en la capa BSSGP. El tráfico es dinámicamente distribuido sobre los NSVCs identificados por NSVCI = 1 y NSVCI = 2 en la capa SNC.

Un BVC es reservado para propósitos de señalización. Sobre el lado del SGSN, BVCs y NSVCs pertenecientes al mismo BSS están agrupados dentro del mismo NSE. Un NSE es creado para cada BSS. Hay un mapeo uno a uno entre el NSVC y el PVC. En el SGSN, una celda dentro de un BSS está directamente identificada por un BVCi y un NSEI.

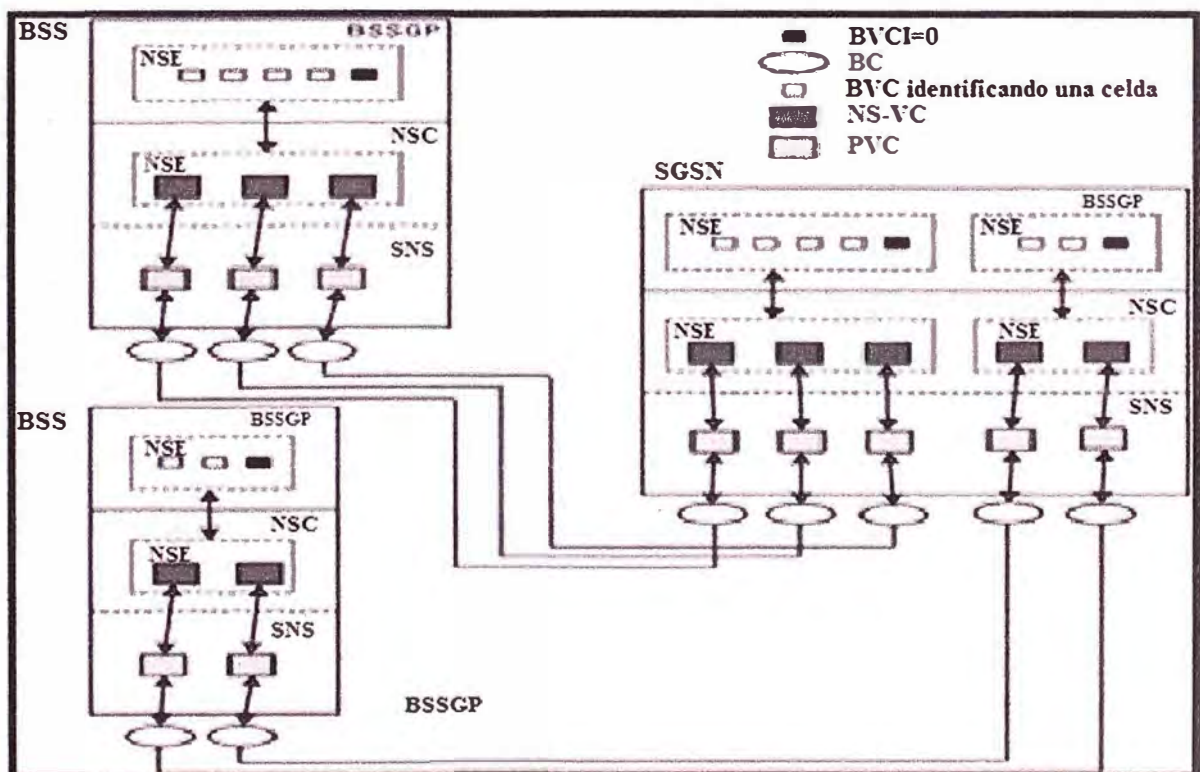


Figura 2.14. Direccionamiento en la interfaz Gb.

2.9 Protocolo IP

De acuerdo al RFC 791, de la IETF (Internet Engineering Task Force), organismo que se encarga de crear notas e informes sobre Internet, se define y se establece los fundamentos de funcionamiento del protocolo IP.

Primeramente definiremos el concepto de protocolo. Se llama protocolo al conjunto de reglas que definen las comunicaciones de data entre entidades. Un protocolo puede definir muchos aspectos de las comunicaciones incluyendo cuál es la naturaleza de las comunicaciones, cómo las entidades se comunicarán, y cuándo las comunicaciones tomarán lugar.

La mayoría de los protocolos pueden ser representados en una arquitectura de capas. En las figuras 2.15 y 2.16 se muestran dos ejemplos. Cada capa realiza distinta función. Cada capa recibe un Protocol Data Unit (PDU) desde la capa superior, realiza algún procesamiento sobre éste, agrega una cabecera al PDU, y envía el PDU resultante a la capa debajo de él. El proceso de agregar cabeceras al PDU se le llama encapsulación.

Actualmente los protocolos TCP/IP son desarrollados y estandarizados por el Engineering Task Force.

En el RFC 791 se sustenta que el Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes, así también proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet también se encarga, si es necesario, de la fragmentación y el re ensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

En el presente informe queremos dar una breve descripción de los conceptos más importantes por los cuales se utiliza el protocolo IP para la encargarse del transporte de datos en la interfaz Gb, sin ahondar en el mismo protocolo.

2.9.1 Operación del Protocolo IP

El protocolo internet implementa dos funciones básicas: direccionamiento y fragmentación.

Los módulos internet usan las direcciones que se encuentran en la cabecera internet para transmitir los datagramas internet hacia sus destinos. La selección de un camino para la transmisión se llama encaminamiento.

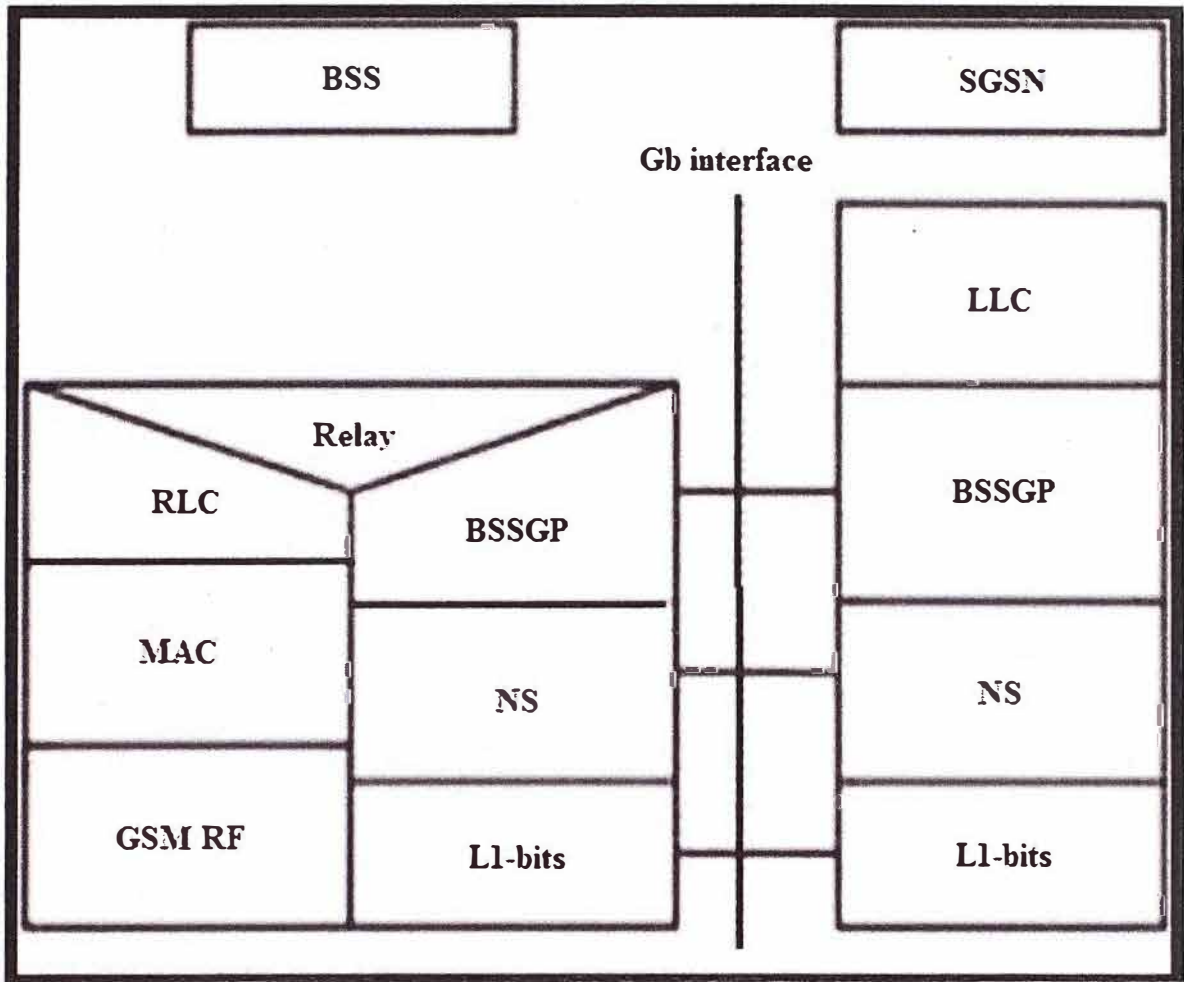


Figura 2.15. Arquitectura de Capas Modelo BSSGP

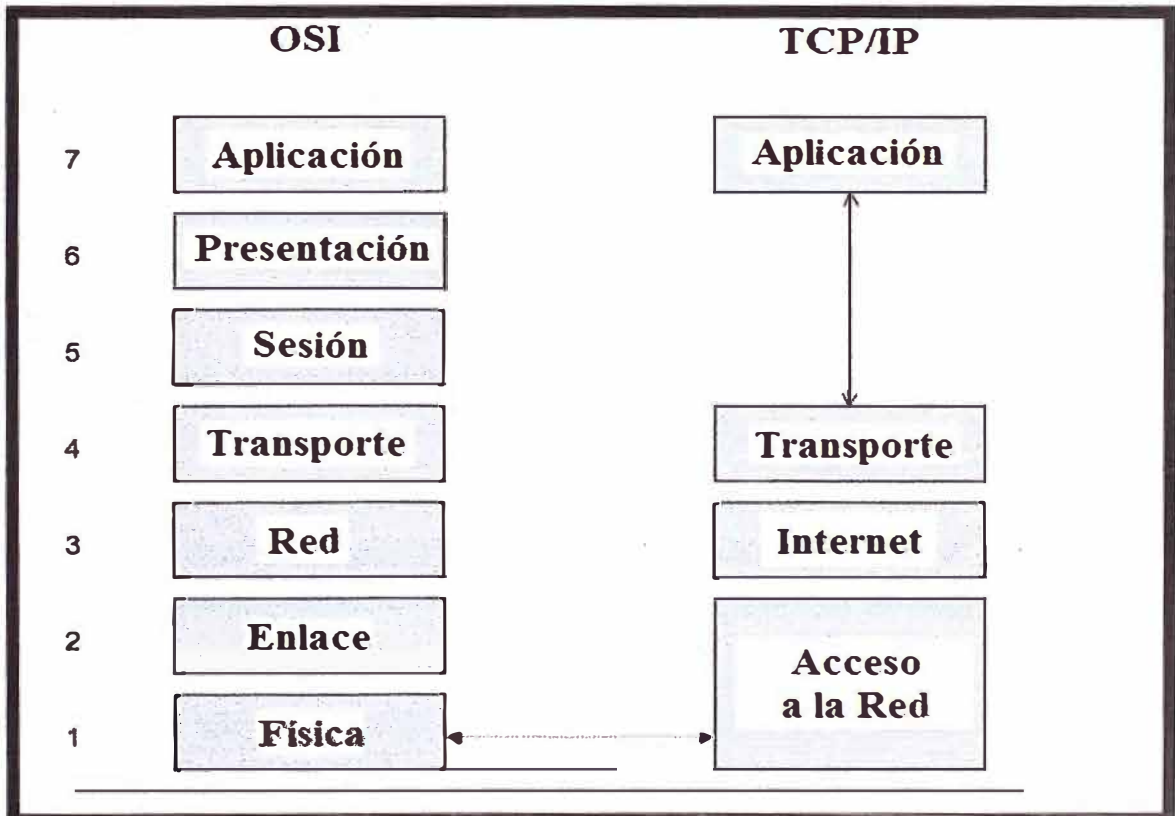


Figura 2.16 Arquitectura de Capas Modelo TCP/IP

Los módulos internet usan campos en la cabecera internet para fragmentar y reensamblar los datagramas internet cuando sea necesario para su transmisión a través de redes de "trama pequeña".

El modelo de operación es que un módulo internet reside en cada host involucrado en la comunicación internet y en cada pasarela que interconecta redes. Estos módulos comparten reglas comunes para interpretar los campos de dirección y para fragmentar y ensamblar datagramas internet. Además, estos módulos (especialmente en las pasarelas) tienen procedimientos para tomar decisiones de encaminamiento y otras funciones.

El protocolo internet utiliza cuatro mecanismos clave para prestar su servicio: Tipo de Servicio, Tiempo de Vida, Opciones, y Suma de Control de Cabecera.

El Tipo de Servicio se utiliza para indicar la calidad del servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet. Esta indicación de tipo de servicio será usada por las pasarelas para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o la siguiente pasarela al encaminar un datagrama internet.

El Tiempo de Vida es una indicación de un límite superior en el periodo de vida de un datagrama internet. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado. Si el tiempo de vida se reduce a cero antes de que el datagrama llegue a su destino, el datagrama internet es destruido. Puede pensarse en el tiempo de vida como en un plazo de autodestrucción.

Las Opciones proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y encaminamiento especial.

La Suma de Control de Cabecera proporciona una verificación de que la información utilizada al procesar el datagrama internet ha sido transmitida correctamente. Los datos pueden contener errores. Si la suma de control de cabecera falla, el datagrama internet es descartado inmediatamente por la entidad que detecta el error.

El protocolo internet no proporciona ningún mecanismo de comunicación fiable. No existen acuses de recibo ni entre extremos ni entre saltos. No hay control de errores para los datos, sólo una suma de control de cabecera. No hay retransmisiones. No existe control de flujo. Los errores detectados pueden ser notificados por medio del Internet Control Message Protocol (ICMP) (Protocolo de Mensajes de Control de Internet) el cual

está implementado en el módulo del protocolo internet. La función o propósito del Protocolo Internet es mover datagramas a través de un conjunto de redes interconectadas. Esto se consigue pasando los datagramas desde un módulo internet a otro hasta que se alcanza el destino.

Los módulos internet residen en hosts y pasarelas en el sistema internet. Los datagramas son encaminados desde un módulo internet a otro a través de redes individuales basándose en la interpretación de una dirección internet. Por eso, un importante mecanismo del protocolo internet es la dirección internet.

En el enrutamiento de mensajes desde un módulo internet a otro, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad se proporciona un mecanismo de fragmentación en el protocolo internet. En la red de Internet no se garantiza cuándo y cómo los paquetes llegarán a su destino. Esto se le conoce como Best Effort o mejor esfuerzo.

2.9.2 Direccionamiento

El protocolo internet maneja principalmente direcciones. Es tarea de los protocolos de mayor nivel (es decir, protocolos host-a-host o entre aplicaciones) hacer corresponder nombres con direcciones. El módulo internet hace corresponder direcciones de internet con direcciones de red local. Es tarea de los procedimientos de menor nivel (es decir, redes locales o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

Las direcciones son de longitud fija de 4 octetos (32 bits). Una dirección comienza por un número de red, seguido de la dirección local (llamada el campo "resto"). Hay 3 formatos o clases de direcciones internet: En la Clase A, el bit más significativo es 0, los 7 bits siguientes son la red, y los 24 bits restantes son la dirección local; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección local; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección local.

2.9.3 Fragmentación

La fragmentación de un datagrama internet es necesaria cuando éste se origina en una red local, la cual permite un tamaño de paquete grande y debe atravesar una red que limita los paquetes a un tamaño inferior para llegar a su destino.

La fragmentación, transmisión y reensamblaje a través de una red local invisible para el módulo del protocolo internet se llama fragmentación intranet y puede ser utilizada.

El procedimiento de fragmentación y reensamblaje en internet tiene que ser capaz de dividir un datagrama en un número casi arbitrario de piezas que puedan ser luego reensambladas. El receptor de los fragmentos utiliza el campo de identificación para asegurarse de que no se mezclan fragmentos de distintos datagramas.

2.9.4 Cabecera IP

A continuación haremos un resumen del contenido de la cabecera IP, campo por campo tal como se muestra en la Figura 2.15.

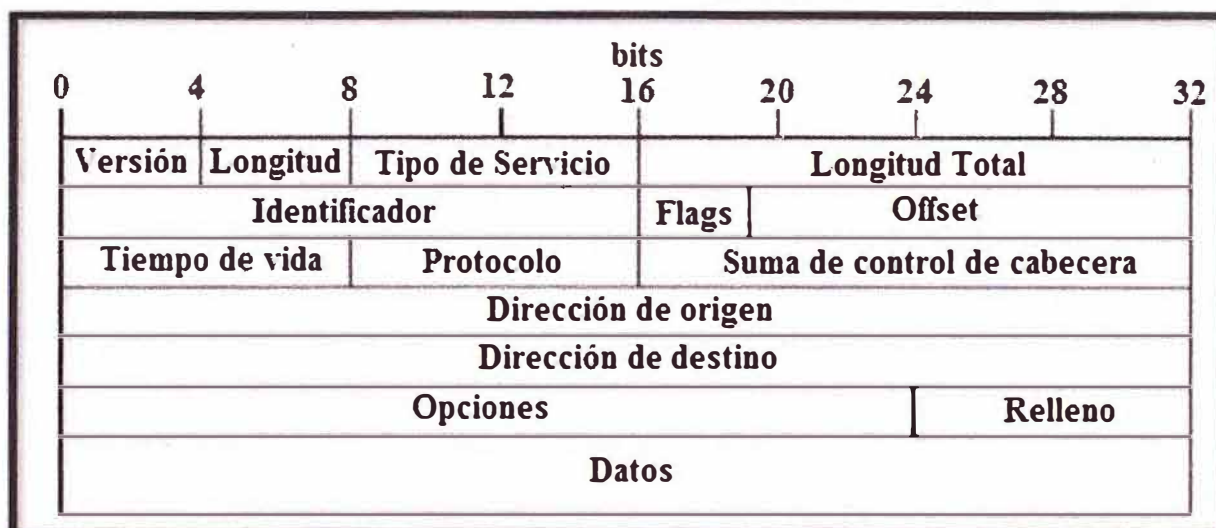


Figura 2.15. Formato de la cabecera del protocolo IP.

- **Versión (4 bits):** El campo Versión describe el formato de la cabecera internet. Este documento describe la versión 4.
- **Longitud (4 bits):** Longitud de la Cabecera Internet (Internet Header Length), es la longitud de la cabecera en palabras de 32 bits, y por tanto apunta al comienzo de los datos. Nótese que el valor mínimo para una cabecera correcta es 5.
- **Tipo de Servicio (8 bits):** El Tipo de Servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada. Estos parámetros se usarán para guiar la selección de los parámetros de servicio reales al transmitir un datagrama a través de una red en particular.
- **Longitud Total (16 bits):** Como su nombre lo dice es la longitud del datagrama, medida en octetos, incluyendo la cabecera y los datos. Este campo permite que la longitud

máxima de un datagrama sea de 65,535 octetos. Los datagramas de tal longitud no son prácticos para la mayoría de hosts y redes. Todos los hosts deben estar preparados para aceptar datagramas de hasta 576 octetos (tanto si llegan completos como en fragmentos). Se recomienda que los hosts envíen datagramas mayores de 576 octetos sólo si tienen la seguridad de que el destinatario está preparado para aceptarlos.

- **Identificación (16 bits):** Es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un datagrama.

- **Flags (3 bits):** Son diversos indicadores de control. A continuación se indica el uso de los bits del flag.

Bit 0: reservado, debe ser cero.

Bit 1: (DF=Don't Fragment) No Fragmentar

0 = puede fragmentarse.

1 = No Fragmentar.

Bit 2: (MF= More Fragments)

0 = Último Fragmento.

1 = Más Fragmentos.

- **Posición del Fragmento (13 bits):** Este campo indica a que parte del datagrama pertenece este fragmento. La posición del fragmento se mide en unidades de 8 octetos (64 bits). El primer fragmento tiene posición 0.

- **Tiempo de Vida (8 bits):** Este campo indica el tiempo máximo que el datagrama tiene permitido permanecer en el sistema internet. Si este campo contiene el valor cero, entonces el datagrama debe ser destruido. Este campo es modificado durante el procesamiento de la cabecera internet. El tiempo es medido en segundos, pero como todo módulo que procese un datagrama debe decrementar el TTL (Time To Live: Tiempo de Vida) al menos en uno, incluso si procesa el datagrama en menos de un segundo, se debe pensar en el TTL sólo como un límite superior del tiempo durante el cual un datagrama puede existir. La intención es hacer que los datagramas imposibles de entregar sean descartados, y limitar el máximo periodo de vida de un datagrama.

- **Protocolo (8 bits):** Este campo indica el protocolo del siguiente nivel usado en la parte de datos del datagrama internet.

- **Suma de Control de Cabecera (16 bits):** Suma de Control de la cabecera solamente. Dado que algunos campos de la cabecera cambian (p. ej. el tiempo de vida), esta suma es recalculada y verificada en cada punto donde la cabecera internet es procesada.

- El campo suma de control es el complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera. A la hora de calcular la suma de control, el valor inicial de este campo es cero.

Esta es una suma de control fácil de calcular y la evidencia experimental indica que es adecuada, pero es provisional y puede ser reemplazada por un procedimiento CRC, dependiendo de la experiencia ulterior.

- Dirección de Origen (32 bits): Es la dirección IP de origen.
- Dirección de Destino (32 bits): Es la dirección IP de destino.
- Opciones (variable): Las opciones pueden o no aparecer en los datagramas. Deben ser implementadas por todos los módulos IP (host y pasarelas). Lo que es opcional es su transmisión en cualquier datagrama en particular, no su implementación.
- Valor de Relleno (variable): El Valor de Relleno se usa para asegurar que la cabecera internet ocupa un múltiplo de 32 bits. El valor de relleno es cero.

Ahora vistos los 2 protocolos analizaremos funciones que se realizan sobre ambos protocolos tales como el Load Sharing o la función de distribución.

2.10 Load Sharing en una Subred Frame Relay

La función Load Sharing distribuye el tráfico de los NS SDU a través de los NSVCs desbloqueados del mismo grupo de la interface Gb.

2.10.1 Requerimientos de la función Load Sharing

Todos los NS SDU a ser transmitidos en la interface Gb son pasados a la función de Load Sharing según el Link Selector Parameter (LSP), el BVCI y el NSEI. El LSP y el BVCI son usados por la entidad NS para seleccionar de entre los NSVCs desbloqueados dentro del grupo, direccionados por medio del NSEI, donde envía el NS SDU. El mapeo entre el LSP y el NSVC está basado sobre una función dependiente de la implementación que implica los siguientes requerimientos:

- Para cada BVCI y NSEI, la entidad NS selecciona el NSVC fuera del grupo basado sobre el LSP. Esta es una materia interna para la entidad NS y esto no es objeto para mayor estandarización.
- Para cada BVC y NSEI, NS SDUs con el mismo Link Selector Parameter deben enviarse sobre el mismo NSVC. La función de Load Sharing garantiza que, para cada BVC, todos los NS SDUs marcados con el mismo valor de LSP deben conservarse.

- Un cambio en NSVCs disponibles para tráfico de usuarios NS (por ejemplo que uno o más NSVCs se bloqueen o desbloqueen) deberá resultar en una reorganización del tráfico NS SDU entre los NSVCs desbloqueados del mismo grupo.
- Las funciones son independientes en el BSS y el SGSN. Por lo tanto el uplink y downlink de NS SDUs para un subscriber puede ser transferidos sobre diferentes NSVCs.
- Para un BVC, cuando no hay ningún NSVC desbloqueado del grupo restante entre el BSS y el SGSN, el tráfico correspondiente es descartado por el NS en el lado que nevía.
- El LSP es usado localmente en el BSS y el SGSN y no será transmitido a través de la interface Gb.

2.11 Load Sharing en una subred IP

La función de Load Sharing distribuye el tráfico de NS SDUs y SNS PDUs entre los disponibles IP endpoints sobre la interface Gb.

La función de Load Sharing para subnetwork IP determina el IP endpoint local y el IP endpoint remoto basado sobre el peso de la información provista por el par NSE. Cada NSE usará una implementación dependiente de la función de Load Sharing para determinar el IP endpoint local asociado con todo el tráfico NS SDU relacionado a un MS (terminal móvil). La IP endpoint remota inicialmente estará determinada por una implementación dependiente de la función de Load Sharing que distribuye el tráfico en igual proporción a los pesos relativos asignados a los endpoints de los NSEs pares. Estos pesos relativos son asignados por el NSE para tanto tráfico de señalización como tráfico de data y será referido como peso de señalización y peso de data respectivamente.

2.11.1 Selección del IP endpoint local

El LSP es usado por una entidad NS para seleccionar entre las IPs endpoints disponibles para un NSEI determinado, desde el cual los NS SDUs son enviados.

- Para cada NS SDU, una entidad NS selecciona un IP endpoint local basado sobre el LSP para enviar NS SDU al NSE par.
- Una vez que el IP endpoint local es seleccionado por el LSP, el NSE debería mantener una conexión entre el LSP y el IP endpoint local así que NS SDUs con el mismo LSP serán enviados desde el mismo IP endpoint local. El NSE puede desasociar el MS del último IP endpoint local usado cuando el MS haga un cambio de celda.
- Selección de un IP endpoint local ocurre localmente en cada NSE.

- Si un IP endpoint local que ha sido mapeado para un LSP es tomado fuera de servicio, un nuevo IP endpoint local deberá ser seleccionado y asociado con el LSP.
- Si no hay IPs endpoint local disponibles, el tráfico correspondiente es descartado por el NS en el lado que envía.

2.11.2 Selección del IP endpoint remoto

Un IP endpoint remoto es una dirección IP y un puerto UDP que el par NSE ha hecho conocido al NSE local (usando un procedimiento de configuración). Además para seleccionar el IP endpoint local, el LSP es también usado por la entidad NS para seleccionar entre los IP endpoints remotos disponibles para un NSEI determinado, para el cual los NS SDUs son enviados. La selección del IP endpoint remoto para un LSP está basado inicialmente en el peso de señalización y peso de data del IP endpoint remoto.

2.12 Función de distribución de recursos

La función de distribución de recursos está solamente disponible para tráfico de data cuando una subred IP es usada. Esta función permite al BSS o al SGSN explícitamente cambiar el IP endpoint en el cual recibe NS SDUs. El BSS o el SGSN pueden escoger no iniciar cualquier pedido para cambiar IP endpoints para alguna sesión del MS y confiar en la función de subcapa del Load Sharing para distribuir tráfico de usuario NS. Sin embargo si el BSS o el SGSN reciben un pedido de cambiar el IP endpoint en el cual los NS SDU son recibidos para un MS, entonces las capas más altas deberán informar de este cambio con una indicación del Link Selector Parameter. Eso es, que si el SGSN o BSS, reciben un pedido para cambiar el IP endpoint remoto de un MS entonces la data subsecuente de downlink o uplink para el móvil serán enviados al IP endpoint remoto indicado por el pedido.

2.13 Subnetwork Service Protocol

En esta sección detallaremos la las funciones del Subnetwork Service bajo los protocolos Frame Relay e Ip.

2.13.1 Subnetwork Service Protocol en la Red Frame Relay

La interface Gb puede consistir de conexiones punto a punto entre el BSS y el SGSN, o una red Frame Relay intermedia entre los puntos finales de la interface Gb.

Otro equipamiento intermedio puede estar atravesado. Varias configuraciones son posibles, pero se considerarán las siguientes para propósitos generales: Conexiones físicas punto a punto o Red Frame Relay intermedia.

Los principios de direccionamiento de la interface Gb serán aplicados como sigue:

- La conexión física es el Frame Relay Bearer Channel.
- El NSVL es el enlace local en un fin (en UNI) del Frame Relay PVC.
- El NSVLI es el Frame Relay DLCI junto con el bearer channel identifier.
- El NSVC es el Frame Relay PVC.
- EL Subnetwork Service entity es el Frame Relay entity.

2.13.2 Subnetwork Service Protocol en la Red IP

El Subnetwork Ip usará el Protocolo IP como se define tanto en la RFC 791 y en la RFC 2460 y Protocolo Datagrama Usuario (UDP) como se define en el RFC 768.

Las conexiones entre el BSS y el SGSN pueden consistir de conexiones punto a punto o de una red IP intermedia. En general se consideran las siguientes características:

- El Subnetwork Service (SNS) puede ser configurado para fines administrativos (ejemplo configuración estática). En el caso de la autoconfiguración el operador asegurará, con anticipación, que cada NSE puede cumplir los requerimientos de su par NSE (máximo número de NSVCs, máximo número de IP endpoints).
- Las configuraciones administrativas suponen la administración de los IP endpoints de los NSE (incluyendo los pesos de data y pesos de señalización)
- En el caso de conexiones punto a punto, la configuración administrativa deberá ser usada. El NSE BSS no tiene conocimiento de la configuración de cualquier otro NSE BSS.
- Los procedimientos de auto configuración son usados para intercambiar información de configuración entre el BSS y el SGSN.
- Los principios de cliente/servidor se aplican. El SGSN es el servidor, el BSS es el cliente. El BSS tendrá conocimiento de al menos un IP endpoint del SGSN.

2.13.3 Fragmentación IP

La fragmentación debería ser evitada en lo posible. Ejemplos de inconvenientes de la fragmentación son:

- La fragmentación es ineficiente, desde que la cabecera IP es duplicada en cada fragmento.

- Si un fragmento es perdido, el paquete completo tiene que ser descartado. La razón es que es posible la retransmisión no selectiva del segmento.

CAPÍTULO III

METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

3.1 Introducción

En la actualidad la gran convergencia de productos y servicios en el internet hace que ciertos estándares sean más populares, tales como redes de área local, web, Ethernet, etc.

En el presente informe utilizaremos las consideraciones realizadas por los proveedores de equipos de telecomunicaciones, el equipo de ingeniería, siguiendo los estándares para realizar operaciones en las redes de Telecomunicaciones.

Cabe mencionar que al ser un trabajo que implica un cambio de sobre las maneras de manejar las rutas de comunicaciones, implica un corte del servicio provisto a los usuario. Por tanto las modificaciones se deberán de realizar en los horarios de menor uso del servicio.

Los servicios basados sobre IP, tales como VPNs, intranets y extranets, son tópicos comunes dentro de la industria. Hay muchas preguntas sobre si IP será una tecnología de remplazo para Frame Relay. Para los servicios basados en IP, los pro incluyen conectividad uno a uno, facilidad de conexión a los socios de negocio, cobertura de servicio e inteligencia general incrementada de la red. Los contras incluyen temas de seguridad, priorización o QoS limitada, y confiabilidad en la entrega de un servicio predecible.

Algunos de las dificultades que aún enfrenta IP son la seguridad, confiabilidad y performance, por lo que algunos creen que aún IP está en las etapas iniciales de su desarrollo.

3.2 Alternativas de Solución

La solución que se usa es la que muestra en la figura 3.1, donde se diagrama una red de transmisión intermedia sobre routers de capa 2 y capa 3. En el gráfico los routers denominados SAR8, manejan datos de capa 2 y aquellos denominados OSR manejan paquetes de capa 3.

Estos OSR serán los que se conecten físicamente a través de cableado UTP hacia la tarjeta correspondiente del SGSN.

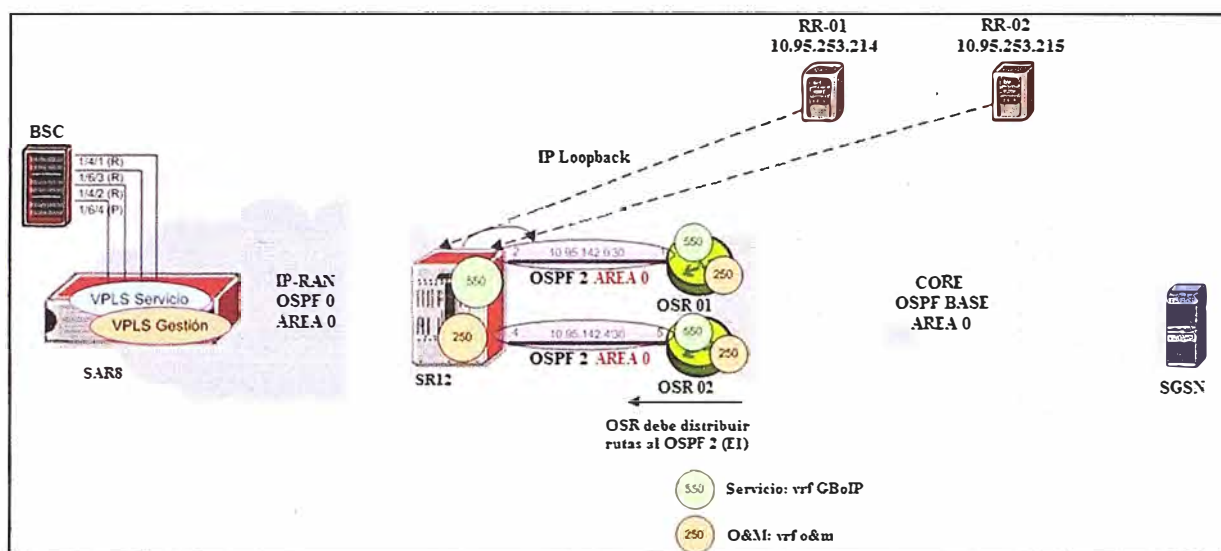


Figura 3.1. Red Transmisión sobre IP.

La red intermedia entre el BSC y el SGSN, que propiamente es la interfaz GB, se compone de nubes IP, en las que existen protocolos de enrutamiento propios. No detallaremos el procedimiento de habilitación de dicha red intermedia. El ancho de banda que se obtenga de la nube IP es el que soportará el protocolo IP de la interfaz Gb.

En el presente informe consideraremos un ancho de banda igual tanto para la red Frame Relay inicial y la red IP final. Sin embargo esto no es requisito indispensable, ya que la migración de protocolos también puede realizarse sobre una red IP final con un ancho de banda superior a la red Inicial, lo cual vendría a ser un upgrade de ancho de banda para aumentar la capacidad de paquetes a transmitir. En la figura 3.2 se muestra una fotografía de un router SAR8.

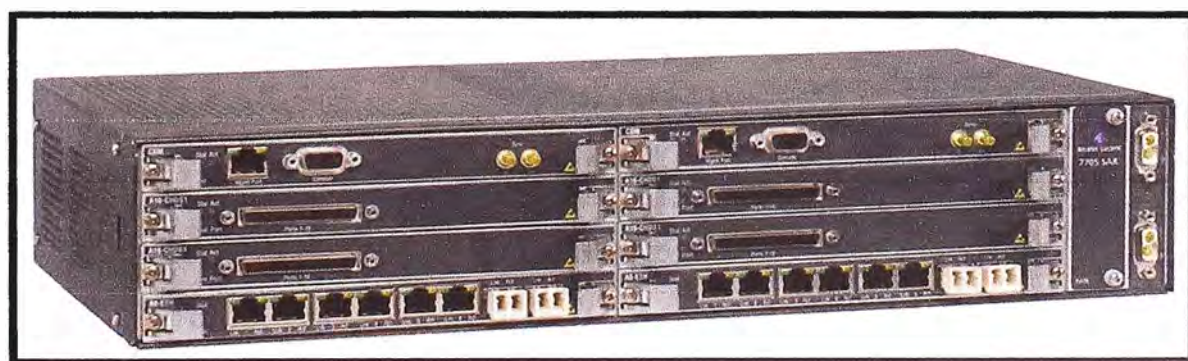


Figura 3.2. Router Alcatel 7705 (SAR8)

3.3 Solución del problema

Empezando desde el BSC, señalaremos aquí la distribución de puertos físicos Ethernet que posee el BSC. Como sabemos el procesamiento de los paquetes de datos se procesan en la PCU. Las conexiones físicas de los enlaces del BSC hacia el SGSN pueden realizarse desde el PCU. Sin embargo en el BSC utilizado en la red del operador de éste informe, existe una unidad computacional intermedia entre la PCU y el BSC llamado switch SWU, que físicamente es una tarjeta integrada al BSC. Este switch ubicado dentro de gabinete del BSC posee los puertos Ethernet donde se conectan físicamente los cables UTP Ethernet. En la figura 3.3 se muestra una fotografía donde se aprecia las tarjetas SWU insertadas en los Slots o ranuras correspondientes en el BSC, y así mismo el cableado UTP que llega a los puertos del mencionado SWU.

Al tener funcionalidad de switch, los SWU pueden manejar enrutamiento por puerto, administración de ancho de banda y configuración de políticas. En el anexo A, se muestra un ejemplo de la configuración utilizada en el SWU. En el anexo B también se muestra la configuración utilizada en el router OSR.

Ahora en el BSC existen conexiones internas físicas y lógicas, que unen los puertos internos de la PCU con los puertos internos del SWU. En la figura 3.4 se observa la topología interna del BSC donde se grafica esto. En ella se muestra dichas conexiones para los SWU.

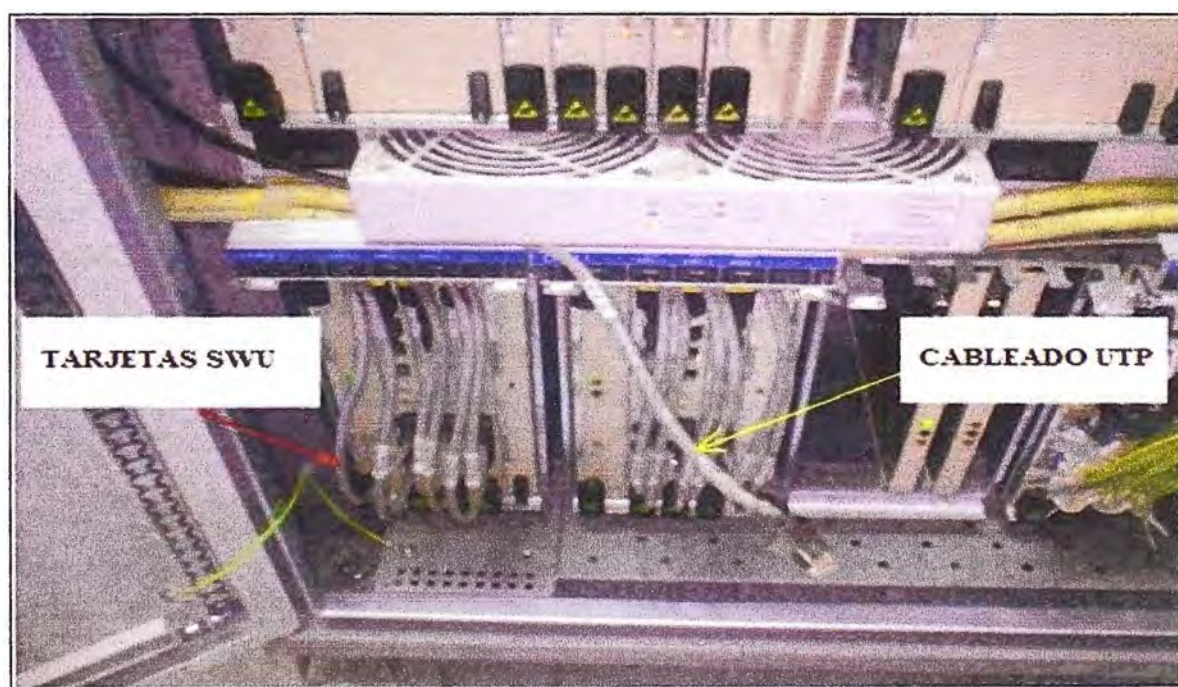


Figura 3.3 Tarjetas SWU dentro del mismo gabinete de un BSC.

En el anexo A, se muestra un ejemplo de la configuración de IPs en un BSC real.

Una vez conectado el cableado UTP Ethernet desde el SWU hacia los routers IP, SAR8 y OSR, y se haya habilitado el ancho de banda de la red intermedia se procederá a realizar migración de protocolos en ventana de mantenimiento, previa prueba piloto que se realiza generalmente un día anterior.

En la migración, los puertos Ethernet de la SWU deben ser configurados signándoseles direcciones IP dentro de la red intermedia. En la figura 3.5 se muestra un la asignación de direcciones IP por puertos de las SWUs.

En el anexo 3 se muestra la configuración que se realiza en el BSC, al cambiar los antiguos parámetros Frame Relay, por los nuevos parámetros IP.

Luego de realizada la migración se procede a monitorear el tráfico de datos desde el BSC, durante las siguientes horas para verificar que el servicio opera con normalidad según lo previsto.

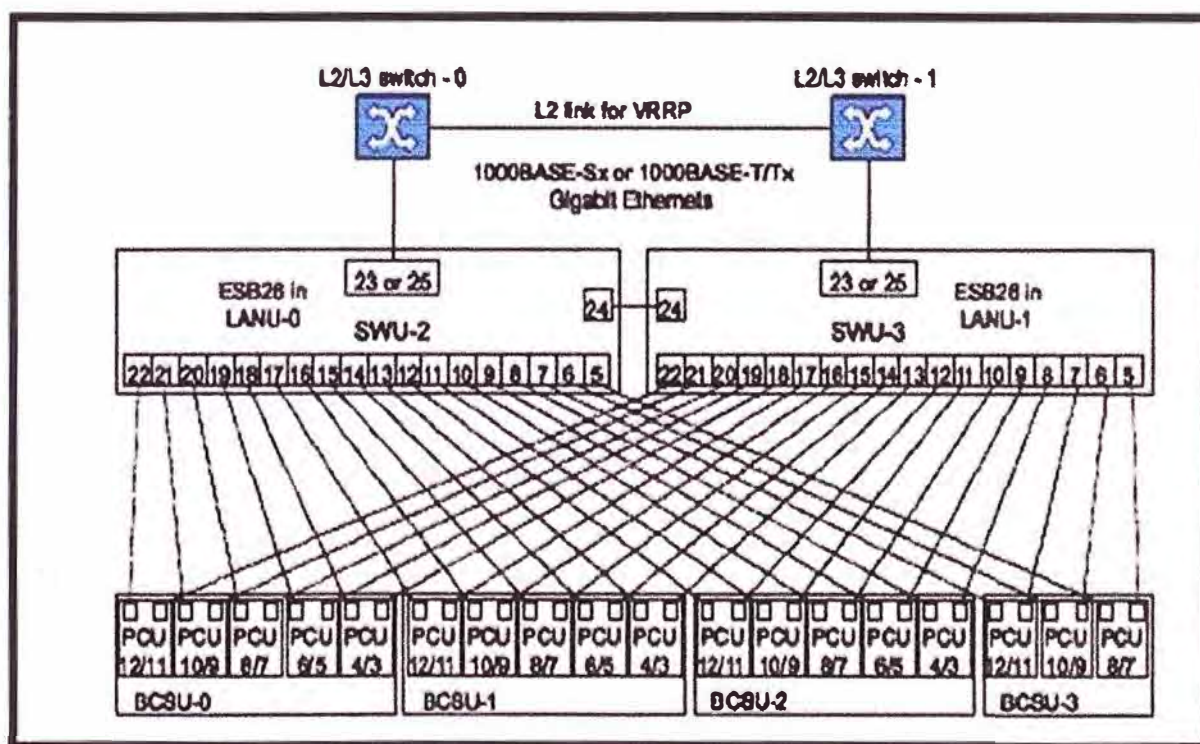


Figura 3.4 Topología PCULAN de un BSC. Fuente: Nokia

A modo de resumen, para realizar la migración utilizaremos las siguientes tareas:

- Habilitar el ancho de banda de la nueva red intermedia.
- Configurar los switches SWU y routers OSR.
- Realizar una prueba piloto.

- Realizar la migración lógica completa de la interface Gb, en ventana de mantenimiento.

3.3.1 Habilitar la nueva red intermedia.

Como pasa a través de routers IP, que tienen capacidad de configurar políticas, ancho de banda, calidad de servicio a cada uno de los puertos que posee.

3.3.2 Configurar los switchs SWU y routers OSR.

Los Router IP SAR8, se conectarán a los router IP OSR del core a través de la red IP. Asimismo estos Router IP del Core se conectarán a las tarjetas manejadoras de tráfico IP en el SGSN a través de cableado Ethernet. Las configuraciones también se realizan en el switch SWU. Una vez realizada la habilitación de la transmisión Ethernet, viene consigo la habilitación de la ruta lógica IP que llevará el tráfico de datos. La habilitación de esta ruta IP es un paso importante y en algunos casos críticos. Estos routers de acceso pueden estar en servicio y llevar tráfico de otros BSCs. La habilitación de un nuevo puerto podría generar, en un diseño de red inicial, bucles o loops de capa 2 que llevarían al router al 100% de su procesamiento y haría reiniciarse router o a las tarjetas lógicas IP del BSC. Es por ello que esta habilitación se realiza en una ventana de mantenimiento, para evitar afectaciones en horas de mucho tráfico.

3.3.3 Realizar una prueba piloto

Esto se realiza luego de que la habilitación de los puertos IP en los routers de acceso se llevó satisfactoriamente. Lo que se realiza en esta prueba piloto es crear un NSEI sobre IP. Se lleva tráfico de algunos sites del BSC sobre este NSEI se revisa los indicadores por un día. Si los indicadores no son favorables, se realiza el roll back y se deshacen todos los cambios hechos.

3.3.4 Migración lógica final de la interface Gb, en ventana de mantenimiento

Luego de la prueba final, se migra la totalidad de la Gb sobre Frame Relay a IP, con el tráfico de todos los sites del BSC. Se realizan pruebas de campo de medición de velocidad y toma de muestras de transacciones entre el móvil y la red para detectar bloqueos o liberaciones de tráfico para futura investigación. En la Figura 3.4 se muestra un diagrama de los grupos de trabajo de ingeniería que trabajaron en este proyecto.

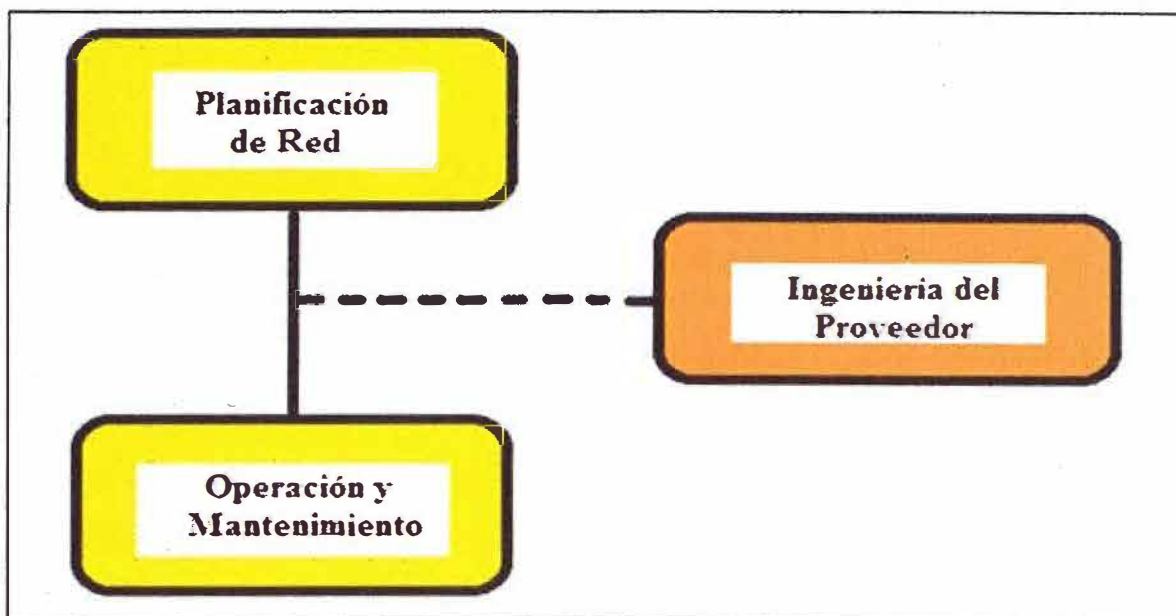


Figura 3.4. Proceso de Migración vista desde las diferentes áreas involucradas.

En la figura 3.5 se muestra un gráfico resumen de la nueva red IP que será el resultado de la migración, y que nos mostrará los resultados tal como veremos en el capítulo 4.

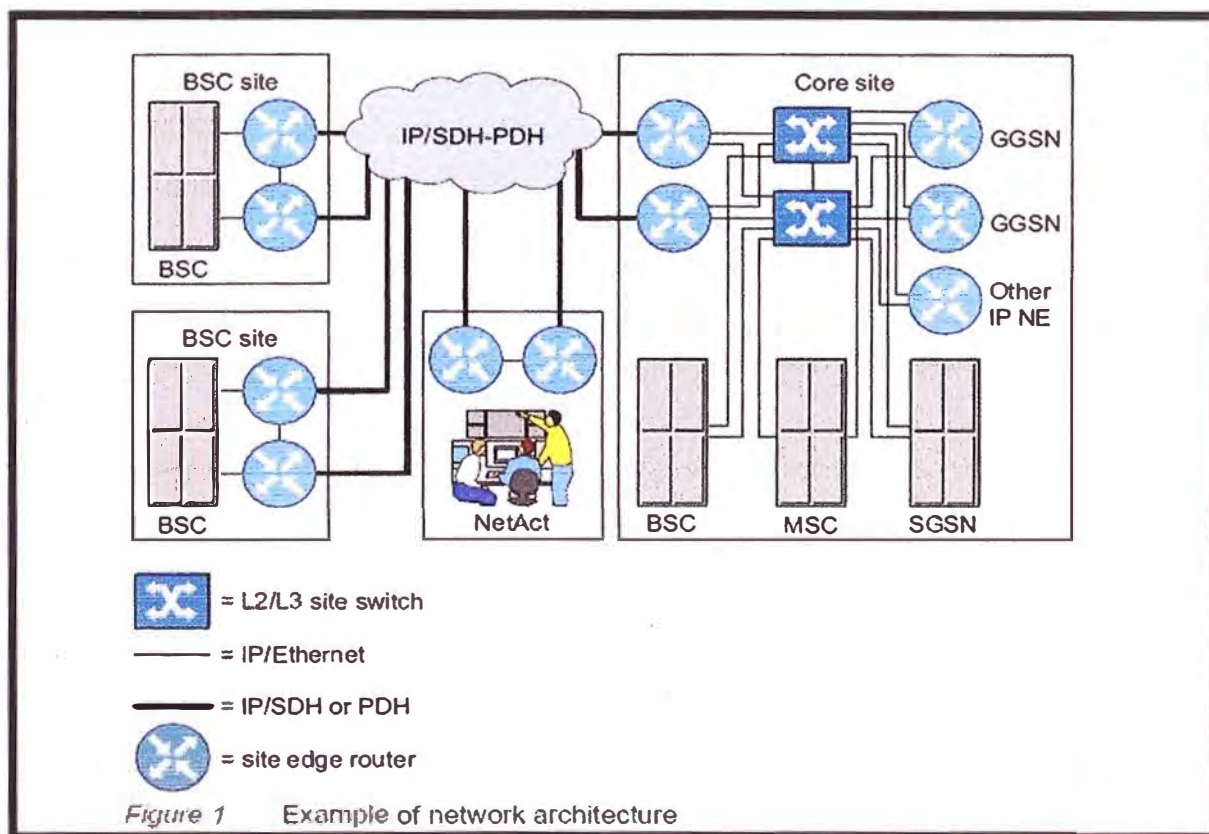


Figura 3.5 Diagrama resumen de la Red de Conectividad IP. Fuente Nokia

CAPÍTULO IV

ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Introducción

La percepción del servicio por parte de los usuarios finales está determinada en la mayoría de los servicios de datos por las interfaces de aplicación. Los usuarios finales sólo perciben los retrasos y rendimientos efectivos.

Los resultados de la migración planteada en éste informe, se observaron a través de una aplicación informática desarrollada por operadora de telecomunicaciones en la cual se realizó el presente trabajo. Esta aplicación maneja la información recibida desde el BSC.

El Base Station Controller (BSC), es capaz de realizar mediciones numéricas de los procesos que ejecuta. Estas mediciones son utilizadas para investigar problemas operativos y para analizar la calidad de los servicios. Las mediciones son diarias, hora por hora. El personal de planificación encargado de utilizar este aplicativo, analizará las mediciones luego de realizada la migración.

Las mediciones numéricas conseguidas desde el BSC se usan para construir indicadores de desempeño de la red, llamados también KPI. Uno de estos indicadores es el llamado Payload, el cual reflejan el tráfico de paquetes al mostrar la cantidad de carga útil transmitida en la red.

La definición de éste concepto se dará en el siguiente subtítulo.

4.2 Análisis descriptivo.

Iniciaremos con la definición de los indicadores a utilizar para describir el comportamiento final de la red.

4.2.1 Payload

Cuando se envían datos a través de Internet, cada unidad de transmisión incluye tanto la información de la cabecera y de los datos que se esté enviando. La cabecera identifica la fuente y el destino del paquete, mientras que los datos reales se conocen como la carga útil o payload.

Debido a que la información de cabecera, o datos de cabecera, sólo se utiliza en el proceso de transmisión, ésta se extrae del paquete cuando llega a su destino. Por lo tanto, la carga útil solamente son los datos recibidos por el sistema de destino.

4.3 Análisis teórico de los resultados

En las figuras 4.1, 4.2, 4.3 y 4.4 se muestra el resultado y el comparativo del indicador Payload de la red antes y después de la migración.

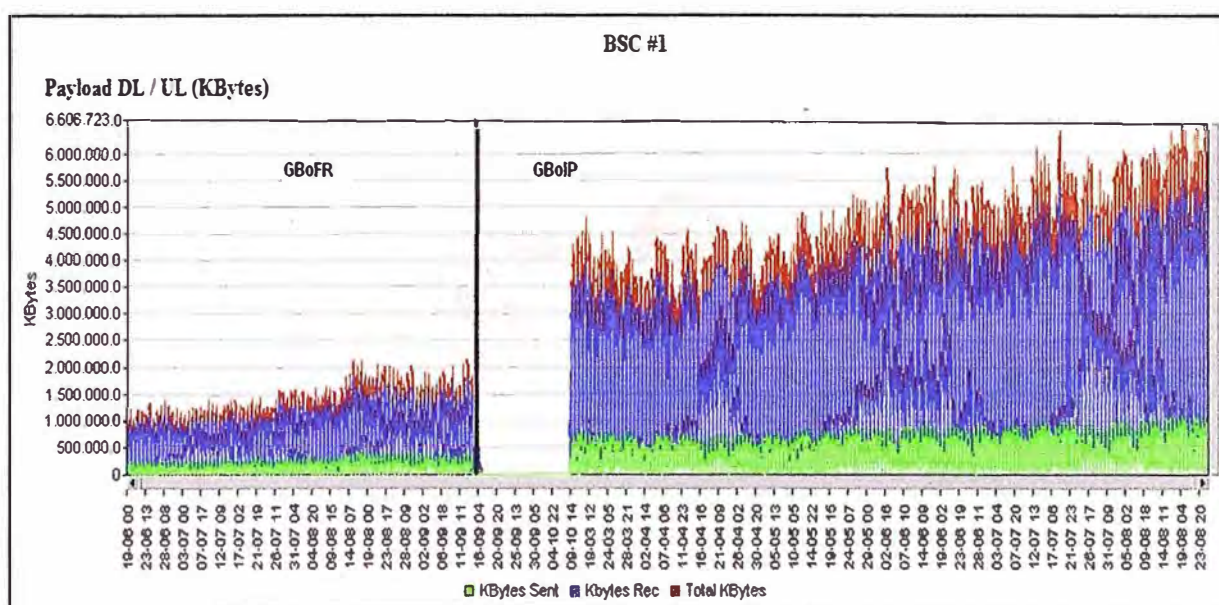


Figura 4.1. Payload DL / UL en Kilobytes después de la migración de protocolos de Frame Relay a IP en un BSC de la ciudad de Lima

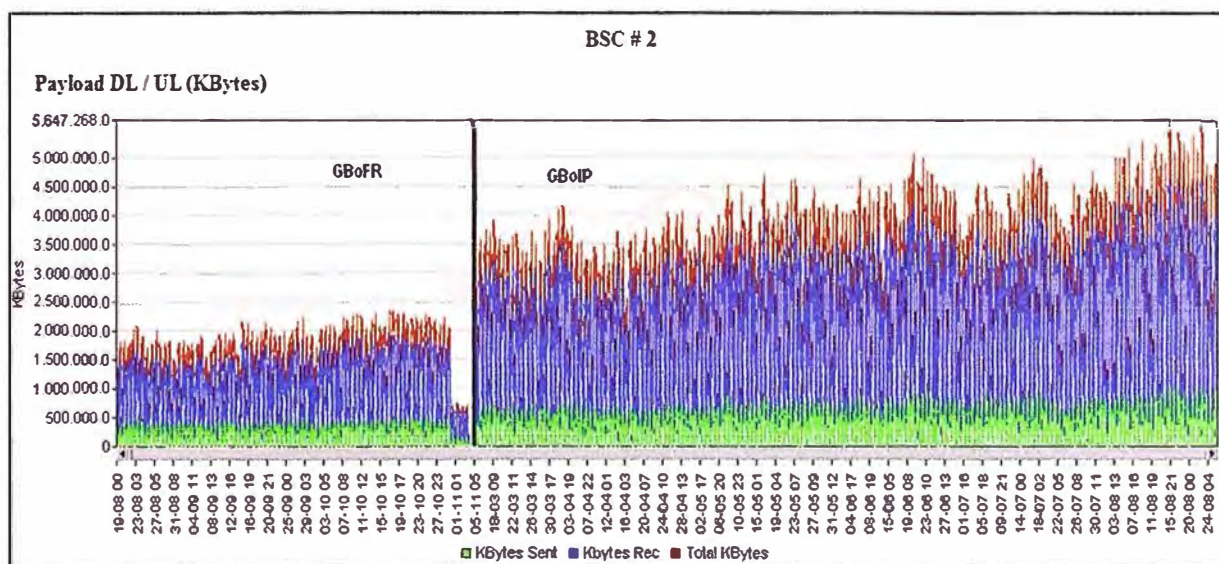


Figura 4.2. Payload DL / UL en Kilobytes después de la migración de protocolos de Frame Relay a IP en un BSC de la ciudad de Trujillo

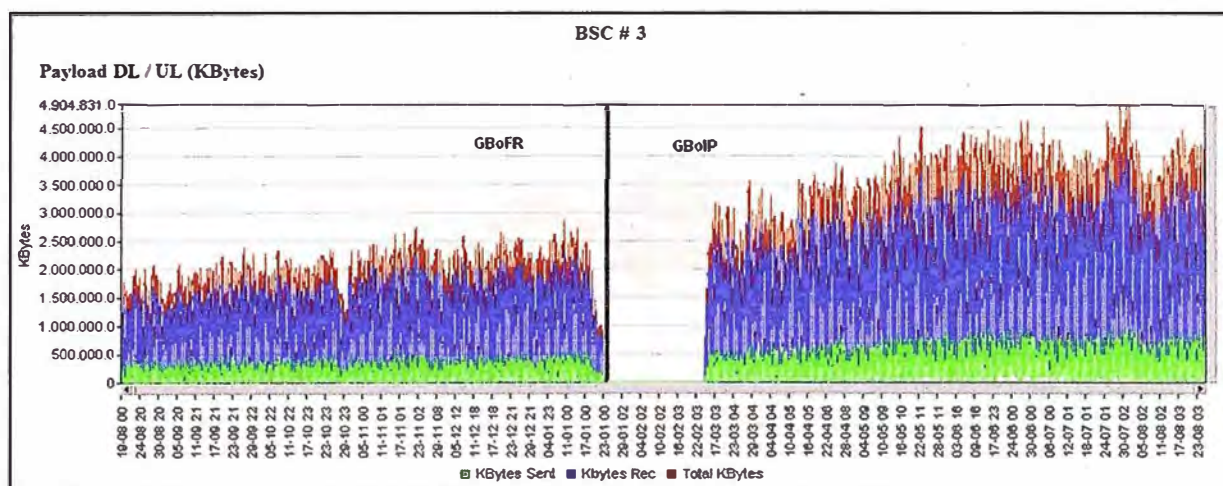


Figura 4.3. Payload DL / UL en Kilobytes después de la migración de protocolos de Frame Relay a IP en otro BSC de la ciudad de Lima

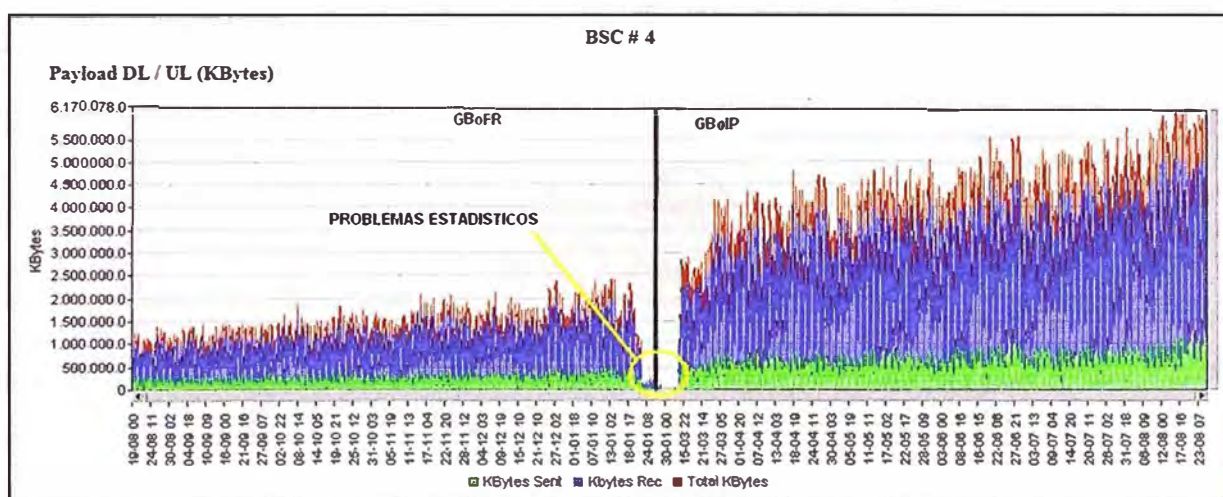


Figura 4.4. Payload DL / UL en Kilobytes después de la migración de protocolos de Frame Relay a IP en un BSC de la ciudad de Arequipa

Como se aprecia, la carga útil transmitida, se incrementa hasta en un 100% en algunos BSC luego de realizada la migración. Esto para el usuario final se traduce en la capacidad de utilizar un mayor ancho de banda de datos para sus distintas aplicaciones.

El tiempo no medido corresponden a las horas en el que no se consiguieron datos del tráfico, debido a que luego del proceso de migración se omitieron activar las mediciones del proceso Gb sobre IP.

4.4 Presupuesto y tiempo de ejecución

El presupuesto se conforma principalmente en equipos routers, switches, cableado UTP necesario para la conectividad. En el anexo 2 se muestran los costos del proyecto y el tiempo necesario para cada pequeña obra.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Las nuevas tecnologías requieren cada vez más ancho de banda para la transmisión de datos, por lo que el mundo está convergiendo al protocolo IP, en parte por su adaptabilidad al protocolo Ethernet, que es casi un estándar en los fabricantes de router, switches, PCs, etc, por su confiabilidad y ancho de banda.
2. La realización de upgrades de las tecnologías o protocolos, requieren una inversión en tiempo y dinero. Sin embargo el mercado y su potencial adquisición rentabilizaran el proyecto.

RECOMENDACIONES

1. El personal deberá estar capacitado para trabajar bajo presión, ya que debido a que el servicio es cortado, si alguna parte del procedimiento falla, deberá encontrar y solucionar la falla en el menor tiempo posible.
2. Las pruebas de campo son necesarias, sin embargo para un área geográfica extensa cubierta por un solo BSC, puede ser demasiado intrincado realizar las pruebas de campo en cada estación base. Por lo tanto las herramientas visuales de tráfico de cada BTS será de gran ayuda, y en determinadas ocasiones pueden ser complementarias.

ANEXO A
CONFIGURACION DE IPs EN EL BSC POR BSCU-PCU


```

BSC31      BSC      2010-06-26 18:36:18
INTERROGATING NETWORK INTERFACE DATA

```

UNIT	NAME	IP ADDRESS	ADDR TYPE	NHL	ASSIGNED	ADM STATE	HTU	PRIOR- RISED
OMU	EL0					UP	1500	NO
	VLAN350	10.96.29.138	L	26	YES	UP	1500	YES
HCMU-0	EL0	10.1.1.1	L I	24	NO	UP	1500	NO
	EL1	10.1.1.1	L I	24	NO	UP	1500	NO
	EMB0	10.1.2.1	L I	27	NO	UP	1500	NO
	EMB1	10.1.3.1	L I	27	NO	UP	1500	NO
HCMU-1	EL0	10.1.1.1	L I	24	YES	UP	1500	NO
	EL1	10.1.1.1	L I	24	NO	UP	1500	NO
	EMB0	10.1.2.1	L I	27	YES	UP	1500	NO
	EMB1	10.1.3.1	L I	27	YES	UP	1500	NO
BSCU-0	-PCU2D- 4	IFETH0 10.103.0.8	L	26	YES	UP	1500	NO
	-PCU2D- 4	IFETH1 10.103.0.8	L	26	NO	UP	1500	NO
BSCU-1	-PCU2D- 3	IFETH0 10.103.0.6	L	26	YES	UP	1500	NO
	-PCU2D- 3	IFETH1 10.103.0.6	L	26	NO	UP	1500	NO
BSCU-2	-PCU2D- 3	IFETH0 10.103.0.9	L	26	YES	UP	1500	NO
	-PCU2D- 3	IFETH1 10.103.0.9	L	26	NO	UP	1500	NO
	-PCU2D- 4	IFETH0 10.103.0.10	L	26	YES	UP	1500	NO
	-PCU2D- 4	IFETH1 10.103.0.10	L	26	NO	UP	1500	NO
BSCU-3	-PCU2D- 3	IFETH0				UP	1500	NO
	-PCU2D- 3	IFETH1				UP	1500	NO
	-PCU2D- 4	IFETH0				UP	1500	NO
	-PCU2D- 4	IFETH1				UP	1500	NO
BSCU-1	-PCU2D- 4	IFETH0 10.103.0.5	L	26	YES	UP	1500	NO
	-PCU2D- 4	IFETH1 10.103.0.5	L	26	NO	UP	1500	NO
BSCU-0	-PCU2D- 3	IFETH0 10.103.0.7	L	26	YES	UP	1500	NO
	-PCU2D- 3	IFETH1 10.103.0.7	L	26	NO	UP	1500	NO

```

COMMAND EXECUTED
TCP/IP STACK DATA HANDLING COMMAND <QR>
< █

```

Figura A.1. Pantalla de consola de BSC que muestra la distribución de IPs por BSCU y PCU.

ANEXO B
COSTO DEL PROYECTO

CONCEPTO		TIPO DE GASTO	PERSONAL	CANTIDAD	COSTO POR UNIDAD US\$	COSTO
ADQUISICION DE TANGIBLES	Cableado, incluye instalacion y medición final de parámetros de calidad del cableado	CAPEX	EXTERNO	4	50	200

Figura B.1. Costos de los elementos tangibles para el proyecto.

CONCEPTO		TIPO DE GASTO	PERSONAL	NRO DE PERSONAS	CANTIDAD DE HORAS	COSTO POR HORA US\$	COSTO
INTANGIBLES	Planificación, configuración y ejecución del trabajo.	OPEX	PROPIO	3	12	30	360
	Pruebas de campo luego del trabajo	OPEX	PROPIO	1	2	60	120

Figura B.2. Costos de los elementos intangibles para el proyecto.

ANEXO C
DURACIÓN DEL PROYECTO

ANEXO D
GLOSARIOS DE TERMINOS

BECN: Backward Explicit Congestion Notification

BSSGP: Base Station System GPRS Protocol

BVC: BSSGP Virtual Connection

BVCI: BSSGP Virtual Connection Identifier

DE: Discard Eligibility

FECN: Forward Explicit Congestion Notification

FR: Frame Relay

IP: Internet Protocol. Es el protocol usado en la internet.

IPv4: Internet Protocol version 4

LLC: Logical Link Control

LSP: Link Selector Parameter

MAC: Medium Access Control

NS: Network Service

NSEI: Network Service Entity Identifier

NS-SAP: Network Service Service Access Point

NS-VC: Network Service Virtual Connection

NS-VCI: Network Service Virtual Connection Identifier

NS-VL: Network Service Virtual Link

NS-VLI: Network Service Virtual Link Identifier

PDU: Protocol Data Unit

PTP: Point-To-Point

PVC: Permanent Virtual Connection

RLC: Radio Link Control

SGSN:Serving GPRS Support Node

SNS: Sub-Network Service

THROUGHPUT: Volumen de información que fluye por la red

BIBLIOGRAFÍA

- [1]. GSM, GPRS and Edge Performance – Timo Halonen, Javier Romero, Juan Melero – Jhon Wiley and Sons Segunda Edicion
- [2]. ETSI Technical Specification 3GPP TS 48.016 – 2011
- [3]. Nokia Training Material SYSTRA GPRS
- [4]. Nokia Documentation Gb over IP - BSC DX 200 – Rel. S12
- [5]. GPRS & EDGE: First steps toward Wireless data-Frederic Michaud-Orange
- [6]. Radio Interface System Planning for GSM/GPRS/UMTS - Lempiäinen, Jukka, Manninen, Matti - 2001
- [7]. RFC 791:IP Protocol-Internet Engineering Task Force
- [8]. RCC 760: UDP Protocol-Internet Engineering Task Force
- [9]. Frame Relay vs IP VPN: White Paper Cisco-Sprint-2002
- [10]. Tendencias en las Reformas de las Telecomunicaciones – Noviembre 2008 - UIT
- [11]. <http://www.techterms.com/definition/payload>
- [12]. <http://en.wikipedia.org/wiki/GPRS>
- [13]. <http://www.etutorials.org/Mobile+devices/gprs+mobile+internet/Chapter+6+Gb+Interface/>