UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

INTEGRACIÓN DE LOS ELEMENTOS DE RED DE TELEFONÍA CELULAR A UN SISTEMA DE ADMINISTRACIÓN DE RED

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

CHRISTIAN MIGUEL AGUILAR VARGAS

PROMOCIÓN
2001 - I

LIMA – PERÚ
2007

INTEGRACIÓN DE LOS ELEMENTOS DE RED DE TELEFONÍA CELULAR A UN SISTEMA DE ADMINISTRACIÓN DE RED

Dedico el presente trabajo a mis
padres por su soporte y estímulo
durante el periodo de mis estudios.

SUMARIO

El presente proyecto detalla la administración de los elementos de red de Telefonía celular enfocado desde el punto de vista de ingeniería. El sistema de administración de red ha sido desarrollado por NOKIA y es utilizado por los operadores móviles para el mantenimiento de sus redes. A continuación se detalla un resumen del contenido del presente documento:

Capítulo I: Arquitectura GSM, GPRS y UMTS
El presente capítulo explica la arquitectura de la red móvil de circuitos conmutados (GSM) y de paquetes (GPRS) así como una introducción a las redes móviles de 3G.

Capítulo II: Descripción del sistema de administración de red
El presente capítulo explica cada uno de los componentes del sistema de administración de red, que se encargará de la gestión de los elementos de red.

Capítulo III: Diseño de la red de comunicación de datos
El presente capítulo explica el detalle del diseño y funcionamiento de la red de comunicación de datos. Así como los protocolos utilizados.

Capítulo IV: Descripción de los elementos de la red de telefonía celular
El presente capítulo detalla la arquitectura de los elementos de red de NOKIA que pertenecen a cada subsistema, BSS y NSS, así como a la red de paquetes GPRS.

Capítulo V: Integración de los elementos de red al sistema de administración de red
El presente capítulo explica el proceso de integración de los elementos de red de cada subsistema al sistema de administración de red.

Capítulo VI: Aplicaciones prácticas e implementación
El presente capítulo muestra el detalle de algunas implementaciones con las respectivas configuraciones para lograr que los elementos de red puedan ser gestionados.

INDICE

CAPITULO II

DESCRIPCIÓN DEL SISTEMA DE ADMINISTRACIÓN DE RED

CAPITULO III

DISEÑO DE LA RED DE COMUNICACIÓN DE DATOS

CAPITULO VI

APLICACIONES PRÁCTICAS E IMPLEMENTACIÓN

PRÓLOGO

El mercado de la tecnología inalámbrica ha experimentado un crecimiento fenomenal desde la segunda generación de las redes celulares digitales, basadas en la tecnología GSM. Desde entonces, GSM ha llegado a ser el estándar dominante global de acceso de radio 2G. Este crecimiento ha tomado lugar simultáneamente con la expansión del acceso a la Internet y los servicios multimedia.

Los operadores celulares hacen frente al desafío de desarrollar sus redes para soportar eficientemente la demanda de los servicios multimedia basados en Internet. Para hacer esto, ellos necesitan realizar una rápida evolución tecnológica hacia la tercera generación de tecnología de acceso de radio, capaz de entregar tales servicios en una manera competitiva y a un costo efectivo.

Sin embargo, el desarrollo de éstas redes deben ser soportadas por un sistema de administración que permita manejar de manera centralizada la red y sus servicios, lo cual significa que el operador pueda gestionar las fallas de los elementos de red, los indicadores de calidad de servicio y el tráfico que cursa sobre toda la red.

El sistema de administración de red es una parte esencial de las redes celulares que proporciona las herramientas operacionales al operador para manejar eficientemente la red, convirtiéndose en un framework de administración de red y de servicio que direcciona los desafíos del operador a manejar más elementos de red, redes más grandes, de mayor complejidad y un crecimiento explosivo en el tráfico y los datos esperados en las redes futuras.

El sistema Nokia NetAct OSS, cumple con todos los requerimientos necesarios para cumplir éstas expectativas. La capacidad de recolectar, integrar y utilizar la información acerca del estado y performance de los elementos de red y de servicios es el core del Nokia NetAct OSS. El manejo de alarmas, las capacidades de los reportes así como la funcionalidad de la optimización de la red, reducen al mínimo la congestión en la red y optimiza la capacidad de la misma creando las bases para las operaciones eficientes de la red.

CAPITULO I

ARQUITECTURA GSM, GPRS y UMTS

1.1 Arquitectura GSM

1.1.1 Estación Móvil (MS)

En GSM, el teléfono móvil es llamado Estación móvil (MS). La estación móvil es una combinación del equipo terminal y los datos del abonado. El equipo terminal como tal es llamado Equipo móvil (ME) y los datos del abonado son almacenados en un dispositivo llamado Módulo de identidad del abonado (SIM).

Estación Móvil = Equipo Móvil (ME) + Módulo de Identidad del Abonado (SIM)

La unidad SIM es la base de datos usada en una red GSM, el cual es un pequeño dispositivo de memoria que contiene la información específica del abonado. Esta contiene los números de identificación del usuario y una lista de redes disponibles. La tarjeta SIM también contiene herramientas necesarias para la autenticación y codificación (ciphering).

1.1.2 Subsistemas y elementos de una red GSM

La red GSM es llamada Red móvil pública terrestre (PLMN), y está organizada en 3 subsistemas:

Subsistema de Estación Base (BSS: Base Station Subsystem).
Subsistema de Conmutación de Red (NSS: Network Switching Subsystem).
Subsistema de Administración de Red (NMS: Network Management Subsystem).

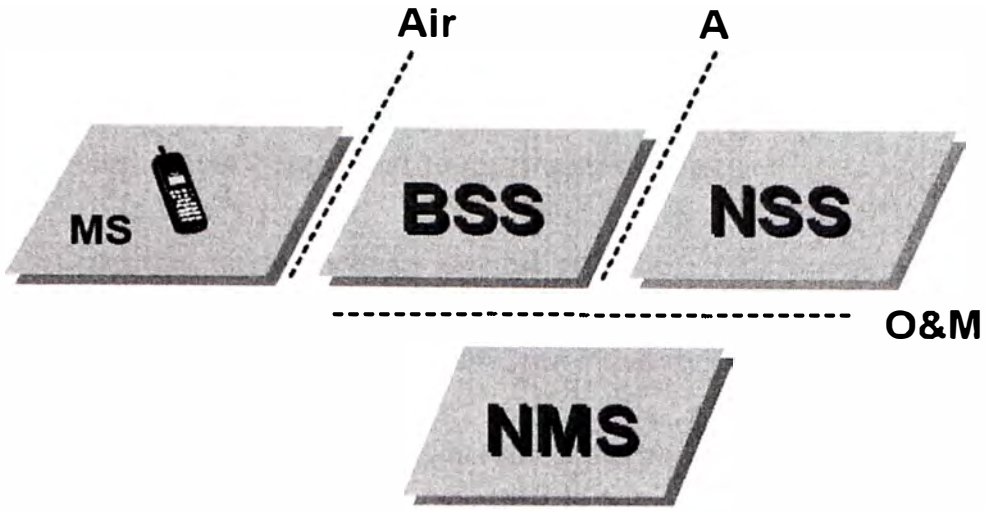


Figura 1.1: Red Móvil Pública Terrestre - PLMN

a) Subsistema de Conmutación de Red (NSS)

El Subsistema de Conmutación de Red contiene básicamente los siguientes elementos de red:

- Central de Conmutación de Servicios Móviles (MSC).
- Gateway de la Central de Conmutación de Servicios Móviles (GMSC).
- Registro de Ubicación Visitante (VLR).
- Registro de Ubicación Local (HLR).
- Centro de Autenticación (AC).
- Registro de Identidad del Equipo Móvil (EIR).

Funciones:

Control de llamada: Identifica al abonado, establece la llamada y libera la conexión después que la conversación finaliza.

Charging (cargo): Se recolecta la información de charging (cargo) de una llamada (los números de los abonados llamante y llamado, el tiempo, tipo de transacción, etc.) y los transfiere al Centro de facturación (Billing Center).

Administración de movilidad: Mantiene la información de la ubicación del abonado.

Señalización: Se aplica a interfases con el Subsistema de estación base (BSS) y la Red conmutada de telefonía pública (PSTN).

Manejo de datos del abonado: Se da tanto en el almacenamiento de los datos permanentes en el Registro de Ubicación Local (HLR) como el almacenamiento temporal de datos relevantes en el Registro de Ubicación Visitante (VLR).

Central de Conmutación de Servicios Móviles (MSC)

La MSC es responsable del control de llamadas en la Red de Telefonía Móvil. Identifica el origen y destino de una llamada, sea una estación móvil o teléfono fijo, así como el tipo de llamada.

La MSC es responsable de las siguientes tareas más importantes:

Control de llamada: La MSC identifica el tipo, el origen y el destino de una llamada, así como el establecimiento, supervisión y finalización de la misma.

Iniciación de paging: El paging es el proceso de ubicar una estación móvil en particular en caso de la finalización de una llamada (llamada a una estación móvil).

Recolección de los datos de charging: La MSC genera los Registros de datos de charging (CDR: Charging Data Records), el cual contiene información acerca del uso de la red por parte del abonado.

Gateway de la Central de Conmutación de Servicios Móviles (GMSC)

El GMSC cumple las mismas funciones que la MSC, excepto el Paging. Este elemento de red es necesario en caso de Llamadas terminadas en el móvil (MTC: Mobile Terminated Call). En GSM, la MSC, la cual está sirviendo a la estación móvil, cambia con la movilidad del abonado. Por lo tanto, en una llamada terminada en el móvil, la llamada es establecida a un equipo definido (central de conmutación) en la red local del abonado (PLMN).

Este equipo es llamado GMSC. El GMSC interactúa con la base de datos del Registro de ubicación local (HLR), el cual mantiene la información de la MSC que está actualmente sirviendo a la estación móvil. Es decir, el GMSC consulta la información de rutas desde el HLR si la llamada es establecida a la estación móvil. Dada la información acerca de la MSC que está sirviendo a la estación móvil, el GMSC continúa el proceso de establecimiento de llamada.

En las implementaciones actuales las funcionalidades de la MSC y el GMSC son implementadas en el mismo equipo, la cual es llamada MSC. También, algunos operadores utilizan el GMSC como salida a redes externas como la PSTN.

Registro de Ubicación Visitante (VLR)

El VLR es una base de datos que contiene la información de los abonados que actualmente se encuentran en el área de servicio de la MSC. Esta información está relacionada a:

Identificación de los números del abonado.
Seguridad de información para la autenticación de la tarjeta SIM y para la codificación.
Servicios que el abonado puede usar.

El VLR lleva a cabo los registros de ubicación y las actualizaciones respectivas. Cuando una estación móvil viene a un nuevo MSC (área de servicio), éste debe registrarlo en el VLR, es decir realizar una Actualización de ubicación (Location Update). En otras palabras, el abonado debe siempre estar registrado en el VLR para usar los servicios de la red. También, las estaciones móviles ubicadas en su propia red están siempre registradas en el VLR.

La base de datos del VLR es temporal, sin embargo los datos son mantenidos siempre y cuando el abonado se encuentre dentro de su área de servicio. Este también contiene la dirección de cada HLR del abonado.

En implementaciones de NOKIA, el VLR está integrado al gabinete de la MSC.

Registro de Ubicación Local (HLR)

El HLR mantiene el registro permanente de los abonados. Los números de identidad del abonado y los servicios suscritos son encontrados aquí. En adición a los datos permanentes, el HLR también mantiene la ruta de la ubicación actual de sus abonados.

Centro de Autenticación (AC)

El AC proporciona la seguridad de información a la red, verifica las tarjetas SIM (autenticación entre la estación móvil y el VLR y codifica la información transmitida en la interfase Air). El AC soporta el trabajo del VLR.

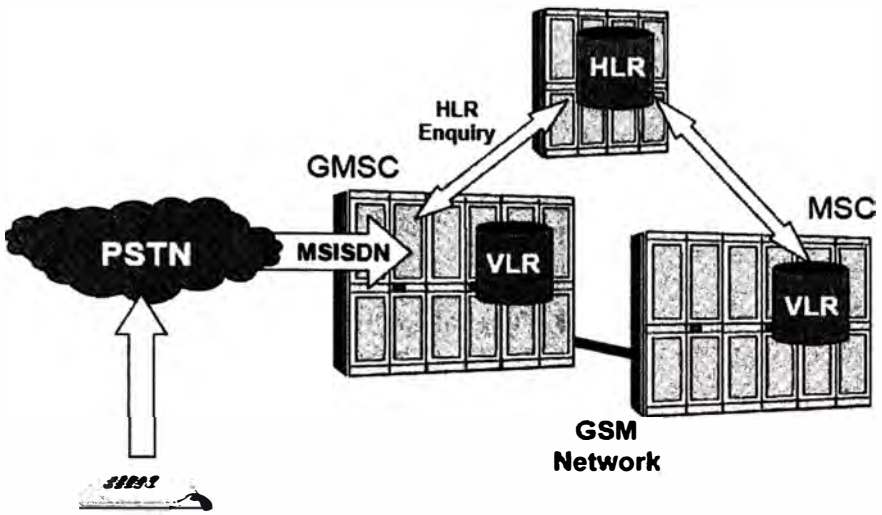


Figura 1.2: Enrutamiento de la llamada dentro de la red GSM

Registro de Identidad del Equipo Móvil (EIR)

Al igual que el AC, el EIR es utilizado para razones de seguridad. Pero mientras el AC provee información para verificar las tarjetas SIM, el EIR es responsable de verificar la validez del equipo móvil con el número IMEI (Internacional Mobile Equipment Identity) o Identidad internacional móvil del equipo.

Cuando este elemento de red opcional está en uso, la estación móvil es requerida a proporcionar el número IMEI.

El EIR contiene 3 listas:

- Lista Blanca: En la cual el equipo móvil es permitido a operar normalmente.
- Lista Gris: Sí existe sospecha que un equipo móvil está defectuoso, se puede monitorear su uso ubicándolo en ésta lista.
- Lista Negra: Sí el equipo móvil es reportado como robado, o no permitido a operar en la red, entonces es ubicado en ésta lista.

En la implementación NOKIA, los elementos de Red AC y EIR están ubicados en el HLR.

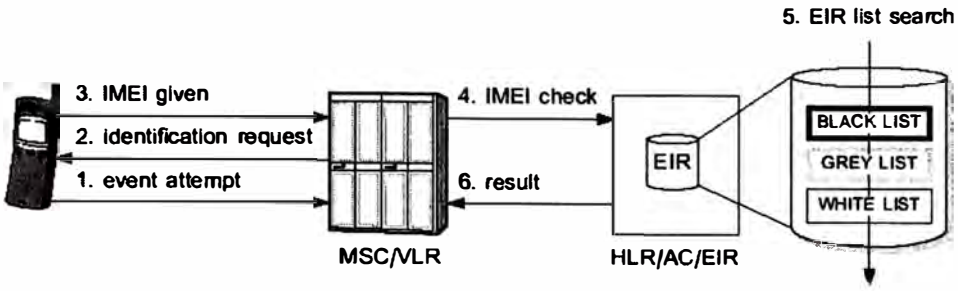


Figura 1.3: Verificación del estado del IMEI desde el EIR

Core de la red de circuitos conmutados (UMTS release 4)

La red GSM comparte un core en común con la red UMTS (3G: Universal Mobile Telecommunications System), lo cual conduce a considerables actualizaciones de las funciones del core de la red debido a que el plan es ofrecer un amplio rango de Servicios Multimedia. Como una consecuencia de éste conjunto más amplio de servicios para el abonado, los servicios bearer de la red deben llegar a ser más flexibles y eficientes.

El bearer es la trayectoria de transmisión de capacidad definida que va a través de los diferentes elementos de red y es llevado sobre las distintas interfases de red. Una variedad más amplia de bearers debe estar disponible en el core y en la red de acceso de radio para hacer que los nuevos servicios estén disponibles para los abonados.

Una MSC tradicional, es responsable de:

- Control y administración de servicios bearer.
- Control de llamada.
- Aprovisionamiento de servicio.

Con el UMTS release 4, el control de llamadas y el control y administración de servicios bearer están separados. Los elementos de red con UMTS release 99 MSC, VLR y GMSC son sustituidos por las entidades de red: MSC-Server, GMSC-Server y CS-MGW (Circuit Switched – Función Gateway Multimedia), lo cual permite eficiencia mucho más alta y soluciones bearer mucho más flexibles.

Servidor MSC (MSS)

El MSC-Server es responsable de las tareas de control de llamadas del MSC y VLR. Estas tareas incluyen:

Control de llamadas originadas y terminadas en el móvil en el dominio de la red de circuitos conmutados.

- La funcionalidad del VLR: Para todos los abonados en el área del MSC-Server, éste almacena temporalmente los perfiles, información de ubicación, identidades, etc. de cada abonado.
- Interacción con el CS-MGW (Circuit Switched Multimedia GateWay): El MSC-Server determina los parámetros de la calidad de servicio requeridos para la aplicación del abonado, por lo que es responsabilidad del CS-MGW hacer que el bearer esté disponible. La interacción entre el MSC-Server y el CS-MGW es hecho vía una interfase abierta basada en el estándar ITU-T H.248
- Terminación de la señalización equipo de abonado – red y red – red. La señalización equipo de abonado – red es hecho vía la interfase Iu-CS. Para la señalización red – red, los protocolos de señalización tales como el BICC (Bearer Independent Call Control) pueden ser usados.
- Recolección de los CDRs (Charging Data Records).

Servidor GMSC (GMSCS)

El GMSC-Server adopta las tareas de control de llamadas del GMSC. Estas tareas incluyen:

- Interrogación del HLR.
- Terminación de la Señalización red-red.
- Interacción con el CS-MGW.
- Recolección de los registros de datos de charging.
- Interacción con el CSE, que es una entidad lógica el cual procesa las actividades relacionadas a los servicios específicos del operador.

Gateway Multimedia – Circuitos Conmutados (CS-MGW)

El CS-MGW es responsable del control del bearer. Estas funciones incluyen:

Control del bearer: Los requerimientos para el control del bearer están configurados en el (G)MSC-Server. El CS-MGW obtiene ésta información vía una interfase abierta. El CS-MGW debe determinar, sí se puede hacer que los bearers estén disponibles de acuerdo al conjunto de parámetros de calidad y servicio.

Terminación de canal del bearer: Diferentes tecnologías de transmisión pueden estar en uso: ATM e IP sobre Ethernet. El bearer ATM finaliza en el MGW y el bearer IP empieza en el MGW para transporte de datos del usuario.

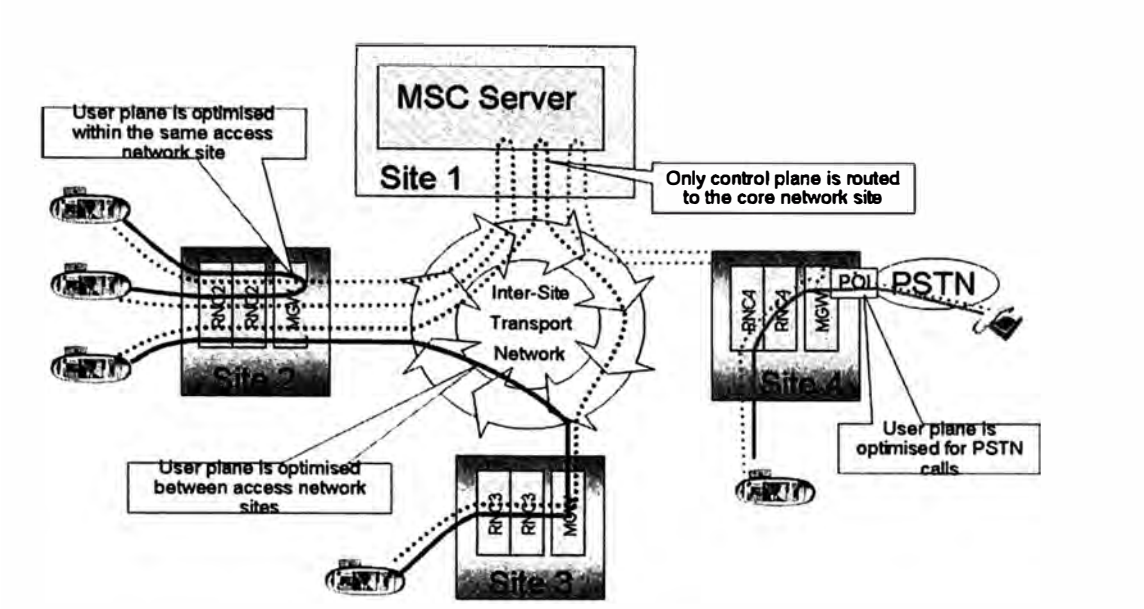


Figura 1.4: Separación del tráfico de control y usuario

Conversión del medio y procesamiento de carga útil: Si el CS-MGW está interactuando con la Red de Acceso Universal Radioeléctrico Terrestre (UTRAN), la información de voz debe ser procesada, por ejemplo, la voz puede ser transmitida con 64kbps en el core de la red, pero para la interfase de radio, 12.2kbps de voz (speech) es requerido. El Codec de Voz específico del UMTS es encontrado en el MGW, así como también los canceladores de eco, dispositivos para conferencias, etc.

Funciones móviles: Un CS-MGW debe soportar funciones específicas de Movilidad, tales como los procedimientos de handover y reubicación del Servidor RNC (SRNC).

A continuación se detallan las interfases de conexión en el Gateway Multimedia (MGW).

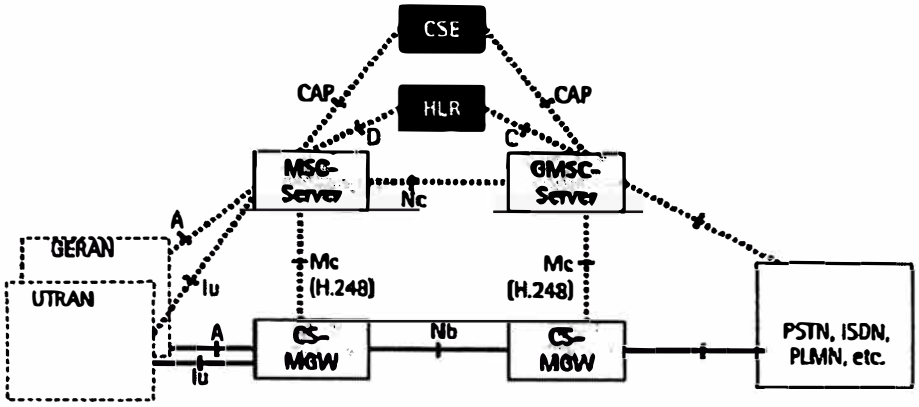


Figura 1.5: Interfases en el Gateway Multimedia

Nc:

Interfase entre el MSC-Server y GMSC-Server

La señalización red-red se lleva a cabo a través de ésta interfase. Sí se usa ATM o IP para establecer los bearers, entonces el protocolo usado en el punto de referencia de ésta interfase debe ser independiente del bearer. La Asociación del Proyecto de 3G (3GPP) no especifica ningún protocolo, así que los proveedores pueden implementar diferentes protocolos de señalización, tal como el BICC.

Mc:

Interfase entre (G)MSC-Server y CS-MGW

El protocolo de control ITU-T H.248 es utilizado aquí.

Nb:

Interfase entre CS-MGW y CS-MGW

El transporte de los bearers da énfasis al transporte por IP o ATM. Como consecuencia, diferentes opciones para la señalización de control y transporte del bearer existen.

b) Subsistema de Estación Base (BSS)

El subsistema de estación base es responsable del manejo de la red de radio, y es controlado por una MSC. Típicamente una MSC contiene varios BSSs. Un BSS puede cubrir un área geográfica considerablemente grande, consistiendo de muchas celdas (una celda se refiere a un área cubierta por uno o más recursos de frecuencia). El BSS consiste de los siguientes elementos:

Controlador de Estación Base (BSC)
Transceptor (Tx/Rx) de la Estación Base (BTS)
Unidad Transcoder y Adaptadora de Velocidad (TRAU) o frecuentemente llamado Transcoder (TC)

Funciones:

Control de la ruta de radio: En la red GSM, el subsistema de estación base es la parte de la red que se encarga de los recursos de radio, es decir, la asignación de los canales de radio y la calidad de la conexión de radio.

Sincronización: El subsistema de estación base usa sincronización jerárquica, lo cual significa que la MSC sincroniza al BSC y el BSC sincroniza las BTSs asociadas a dicho BSC. Dentro del BSS, la sincronización es controlada por el BSC. La sincronización es un asunto crítico en la red GSM debido a la naturaleza de la información transferida. Sí la cadena de sincronización no está trabajando correctamente, las llamadas pueden ser cortadas o la calidad de la llamada puede no ser la mejor posible, o en el peor de lo casos, incluso puede ser imposible el establecimiento de la llamada.

Señalización de la interfase A y Air: Para establecer una llamada, la estación móvil debe tener una conexión a través del BSS.

Establecimiento de la conexión entre la estación móvil y el subsistema NSS: El BSS está ubicado entre 2 interfases, la interfase A y la interfase Air. La estación móvil debe tener una conexión a través de éstas 2 interfases antes que una llamada sea establecida. Ésta conexión puede ser una conexión de Señalización o una conexión de tráfico.

Administración de movilidad y transcodificación de voz: La transcodificación consiste en convertir la voz de un formato de codificación digital a otro y viceversa. La administración de la Movilidad en el BSS cubre los diferentes casos de handovers.

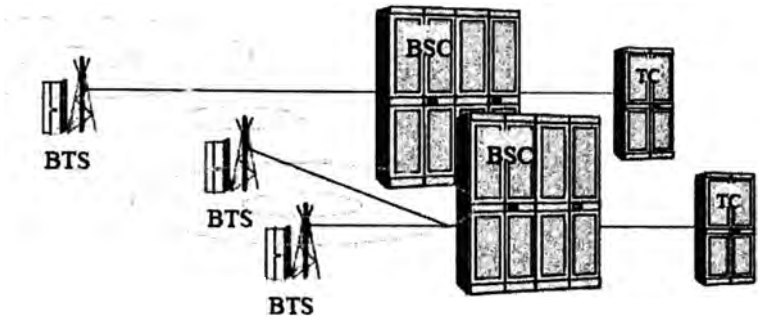


Figura 1.6: Subsistema de estación base - BSS

Controlador de Estación Base (BSC)

El BSC es el elemento central del subsistema de estación base y controla la red de radio. Este elemento tiene varias tareas importantes, entre las cuales tenemos:

Establecimiento de la conexión entre la estación móvil y el subsistema NSS: Todas las llamadas hacia y desde la estación móvil son conectadas a través de la funcionalidad de conmutación (switching) del BSC.

Administración de movilidad: El BSC es responsable de la iniciación de los handovers, y hace la decisión del handover basado en los reportes de medición enviados por la estación móvil durante una llamada.

Recolección de datos estadísticos: La información desde las BTSs, transcoders y BSC son recolectadas en el controlador de estación base (BSC) y enviadas vía la Red de comunicación de datos (DCN) al sistema de administración de red, donde son post procesados para las estadísticas y de allí se obtiene la calidad y el estado de la red.

Soporte de señalización de las interfases Air y A: En la interfase A, el Sistema de señalización número 7 (SS7) es usado como lenguaje de señalización, mientras el entorno en la interfase Air permite el uso de un protocolo adaptado de los estándares ISDN, llamado LAPDm. Entre la BTS y el BSC (Interfase Abis), es usado un protocolo más estandarizado llamado LAPD. El BSC también habilita la conexión de señalización transparente necesaria entre la MSC/VLR y la estación móvil.

Control de la BTS y el transcoder: Dentro del subsistema BSS, todas las BTSs y los transcoders están conectados al BSC. El BSC mantiene a las BTSs, es decir, el BSC es capaz de separar una BTS de la red y recolectar la información de alarmas.

Los transcoders son también mantenidos por el BSC, es decir el BSC también recolecta alarmas relacionadas a los transcoders.

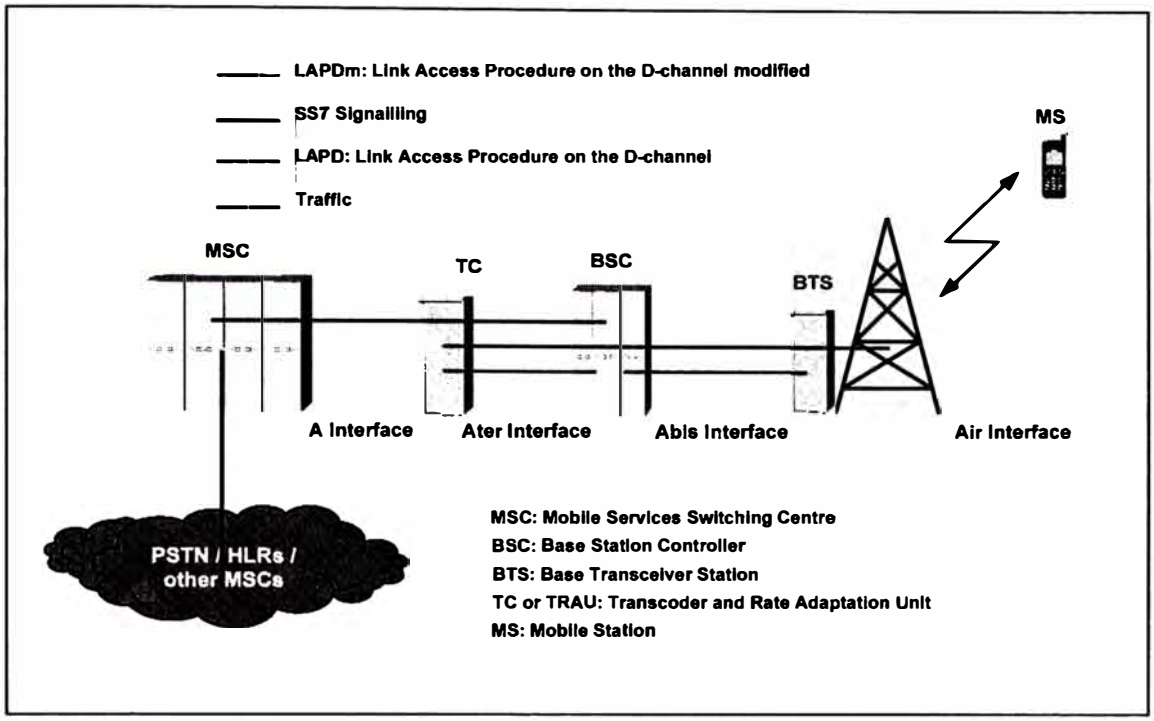


Figura 1.7: Interfases en una red GSM

Transceptor de la Estación Base (BTS)

La BTS es el elemento de red responsable del mantenimiento de la interfase Air y de minimizar los problemas de transmisión (la interfase Air es muy sensitiva a los distubios). Esta tarea es realizada con la ayuda de unos 120 parámetros. Estos parámetros definen exactamente que clase de BTS está en consulta y como las estaciones móviles pueden "ver" la red cuando se mueven en el área de ésta BTS.

Los parámetros de la BTS manejan: Clases de handovers (cuándo y porqué), organización de paging, control del nivel de potencia de radio e identificación de BTSs. La BTS tiene varias tareas muy importantes, las cuales son presentadas a continuación:

Señalización de la interfase Air: Muchas de las llamadas relacionadas a la señalización deben ser realizadas para que el sistema trabaje. Un ejemplo es que cuando la estación móvil es encendida por primera vez, éste necesita enviar/recibir información hacia/desde la red (más precisamente con el VLR) antes que se hagan y reciban llamadas telefónicas.

Otro ejemplo es la señalización requerida para establecer llamadas originadas y terminadas en el móvil. Una tercera señalización muy importante en redes móviles es la necesidad de informar a la estación móvil cuando un handover se realizará y luego

cuando la estación móvil envía un mensaje en la dirección de subida (uplink) diciendo a la red que el handover ha sido completado.

Codificación: La BTS y la estación móvil deben ser capaces de codificar y descifrar la información para proteger la voz y los datos transmitidos en la interfase Air.

Procesamiento de la voz: El procesamiento de la voz se refiere a todas las funciones que la BTS realiza para garantizar una conexión libre de error entre la estación móvil y la BTS. Esto incluye tareas como codificación de la voz (digital a analógica en la dirección de bajada (downlink) y viceversa), codificación de canal (para protección de error), interpolación (para habilitar una transmisión segura) y burst formatting (adición de información a la voz/datos codificados para alcanzar una transmisión organizada y segura).

Modulación y Demodulación: En GSM, el GMSK es aplicado como técnica de modulación. La estación base puede contener varios TRXs (Transceivers), cada uno soportando un par de frecuencias para transmitir y recibir información. La BTS también tiene una o más antenas, las cuales son capaces de transmitir y recibir información hacia/desde uno o más TRXs. Las antenas son omnidireccionales o sectorizadas. Este también tiene funciones de control para Operación y Mantenimiento (O&M), sincronización y alarmas externas, etc.

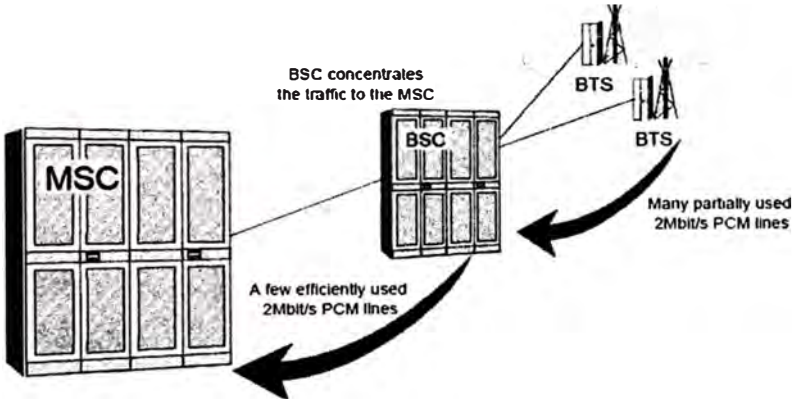


Figura 1.8: Conexión BTS - BSC - MSC

Unidad Transcoder y Adaptadora de Velocidad (TRAU o TC)

En la interfase Air (entre la estación móvil y la BTS), el medio que transporta el tráfico es una frecuencia de radio. Para habilitar una eficiente transmisión de información de la voz digital sobre la interfase Air, la señal de la voz digital es comprimida. Sin embargo, debemos también ser capaces de comunicarnos con y hacia la Red de telefonía fija, donde el formato de la compresión de voz es diferente. Así entre la BTS y la PSTN, se tiene que convertir desde un formato de compresión de la voz a otro, y es allí en donde interviene el transcoder.

Para la transmisión sobre la interfase Air, la señal de voz es comprimida por la estación móvil a 13kbps (full rate y enhanced full rate), 5.6kbps (half rate) o 12.2kbps (enhanced full rate). Sin embargo, la tasa estándar para la voz en la PSTN es 64kbps. La técnica de modulación es llamada Modulación por codificación de pulsos (PCM). Esto requiere que la red GSM realice la adaptación de la voz.

Así, la TRAU maneja el cambio de una velocidad a otra. Si el transcoder es ubicado tan cerca posible a la MSC con líneas PCM estándar conectadas a los elementos de red, en teoría se podrán multiplexar 4 canales de tráfico en un canal PCM. Esto incrementa la eficiencia de las líneas PCM, y disminuye los costos para el operador.

Cuando nos conectamos a la MSC, las líneas multiplexadas tienen que ser demultiplexadas, por esa razón, la solución de NOKIA de la TRAU es llamada Submultiplexor Transcoder (TCSM). Otra tarea del TRAU es habilitar la Transmisión discontinua (DTX), el cual es usado durante una llamada cuando no existe nada para transmitir. Esto es habilitado para reducir la interferencia y ahorrar la batería de la estación móvil.

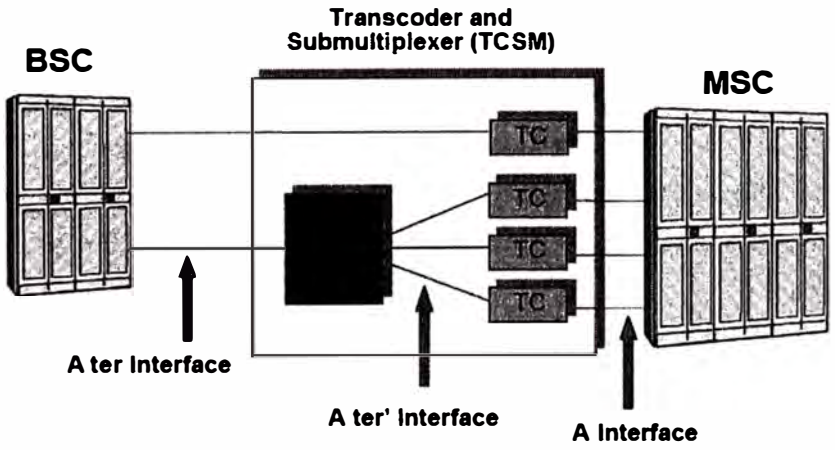


Figura 1.9: Ubicación del transcoder y el multiplexor

c) Subsistema de Administración de Red (NMS)

El tercer subsistema de la red GSM tiene como principal tarea monitorear las funciones de los elementos de red. Ésta tarea puede ser dividida en 3 categorías:

- Administración de Fallas de Red (FM)
- Administración de Configuración de Red (CM)
- Administración del Desempeño de la red (PM)

Estas funciones cubren de manera completa los elementos de la red GSM desde el nivel de BTSs hasta los MSCs y HLRs.

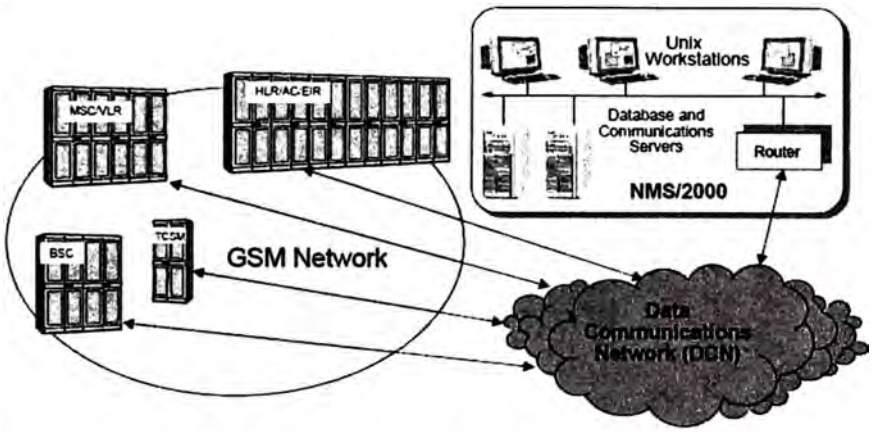


Figura 1.10: El subsistema de administración de red y la red GSM

Administración de Fallas (FM)

Tiene como propósito asegurar la adecuada operación de la red y la rápida corrección de cualquier clase de problemas que son detectados. La administración de fallas provee al operador de red información acerca del estado actual de los eventos de alarma y mantiene una base de datos histórica de alarmas.

Las alarmas son almacenadas en la base de datos del Subsistema de administración de red y ésta puede ser consultada de acuerdo a un criterio especificado por el operador de red.

Administración de Configuración (CM)

Tiene como propósito mantener actualizada la información acerca de la operación y el estado de configuración de los elementos de red. Las funciones de configuración

específicas incluyen la administración de la red de radio, administración de software y hardware de los elementos de red, sincronización del tiempo y operaciones de seguridad.

Administración del Desempeño (PM)

Tiene como propósito la recolección de los datos de mediciones de los elementos de red de forma individual y los almacena en la base de datos. Sobre ésta información, el operador de red es capaz de comparar el desempeño actual de la red con el desempeño planeado y detectar el desempeño dentro de la red.

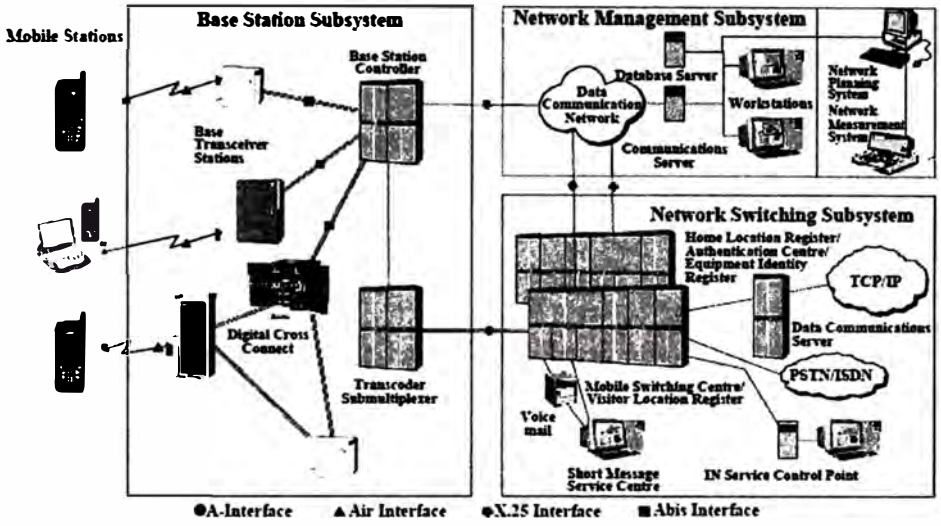


Figura 1.11: Arquitectura de la red GSM – Implementación NOKIA

1.1.3 Interfases GSM

Uno de los principales propósitos en las especificaciones GSM es definir varias interfases abiertas, el cual limita ciertas partes del sistema GSM. Debido a estas interfases, el mantenimiento de la red puede ser obtenida de diferentes proveedores de red GSM. Con una interfase abierta, también se define que está sucediendo a través de la interfase y también definir que clase de acciones / procedimientos / funciones pueden ser implementadas entre las interfases. Las especificaciones definen 2 interfaces abiertas dentro de la red GSM:

La primera está entre la estación móvil y la estación base. Esta interfase es llamada Um, y es una interfase abierta dado que los teléfonos móviles (de cualquier operador) deben ser capaces de comunicarse con las Redes GSM de diferentes proveedores.

La segunda interfase está ubicada entre la MSC y el BSC. Esta interfase es llamada interfase A.

Existen otras interfases dentro del subsistema BSS, las cuales no son totalmente abiertas.

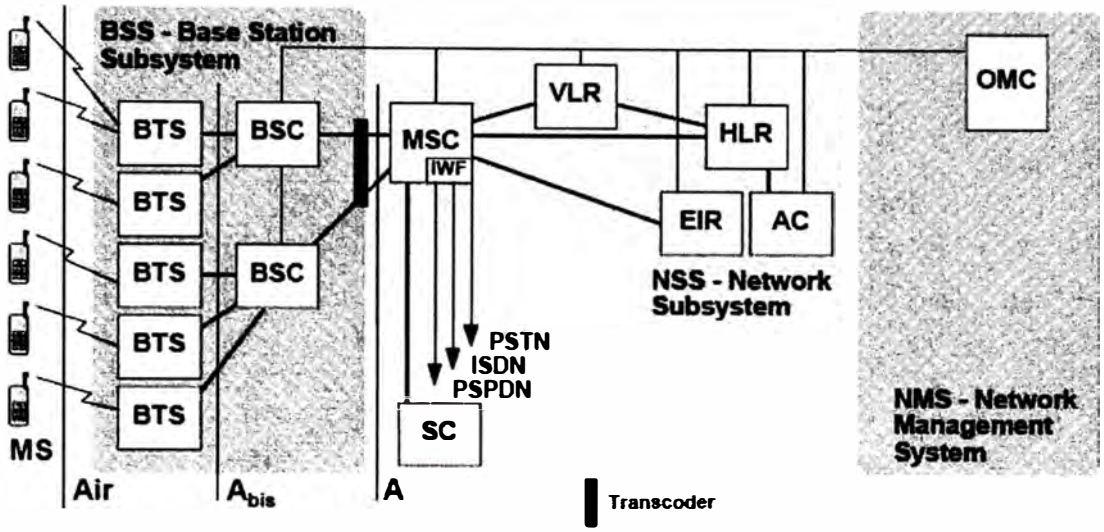


Figura 1.12: Interfases en una red GSM

Air: Interfase Um (Interfase de radio o aire)

Abis: Interfase entre el BSC y la BTS (Interfase propietaria)

A: Interfase entre la MSC y el BSC

1.2 Administración del tráfico en una red GSM

1.2.1 Ubicación de un abonado

a) Registro y base de datos

Desde que un abonado enciende su teléfono, éste se conecta a la red sobre un enlace de radio inalámbrico. Una conexión a través de la red móvil es posible sólo si existe una conexión punto a punto entre la persona llamante y la persona quién es llamada.

Por lo tanto, es absolutamente necesario que la red conozca de la ubicación del abonado. La red mantiene el rastro de la ubicación del abonado con la ayuda de varias bases de datos, más precisamente la SIM, VLR y HLR.

El abonado conmuta (su teléfono) en un área en donde un operador local provee el servicio de red. El área es conectada a través de una interfase de aire al VLR, el cual está integrado en la MSC.

El operador local del abonado también necesita conocer la ubicación del abonado. Por lo tanto, éste se mantiene en otro registro, el HLR.

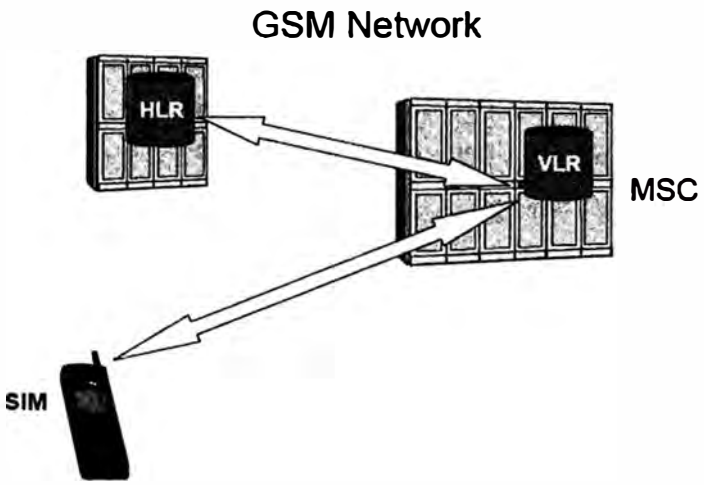


Figura 1.13: Bases de datos en una red GSM

El HLR almacena los datos básicos del abonado sobre una base permanente. La única información variable en el HLR es la ubicación actual del abonado (dirección VLR).

La dirección del VLR es necesaria, porque el HLR necesita conocer desde que MSC/VLR preguntar para el encaminamiento de la información en el caso de una llamada terminada en el móvil (llamada a la estación móvil). Cuando el abonado se mueve a otra área VLR, sus datos son borrados del antiguo VLR y almacenados en el nuevo VLR.

b) Actualización de ubicación – Primera vez

El punto básico de las redes móviles es la capacidad de los usuarios para moverse a diferentes áreas de cobertura. Sí permitimos a un usuario moverse de un lugar a otro, la red debe ser capaz de ubicar al usuario en cualquier tiempo en que exista una llamada terminada en el móvil.

Para conectar una llamada a un móvil es necesario determinar donde está el teléfono móvil. Esta información de ubicación permite a la red formar una conexión punto a punto a un teléfono móvil. La transacción que permite a la red mantener el rastro del abonado es llamado Actualización de ubicación (Location Update).

El teléfono móvil recibe constantemente información enviada por la red. Esta información incluye identificación del área VLR en el cual el móvil está actualmente ubicado. Para mantener el rastro de la ubicación, el móvil almacena la identificación del área en el cual está actualmente registrado. Cada vez que la red difunde la identificación del área, el móvil compara ésta información con la identificación almacenada en su memoria. Cuando las 2 identificaciones no son ampliamente las mismas, el móvil envía una petición a la red, es decir, una consulta del registro al área a la cual ha entrado.

Esta petición puede ser realizada para registrarse en una nueva área bajo el VLR actualmente usado o éste puede ser enviado a un nuevo VLR dependiendo de la situación. En aquellos casos en donde el VLR es cambiado, la red recibe la petición y registra al móvil en la nueva área del VLR. Simultáneamente, el HLR del abonado es informado acerca de la nueva ubicación del VLR y los datos concernientes al abonado son limpiados del VLR anterior.

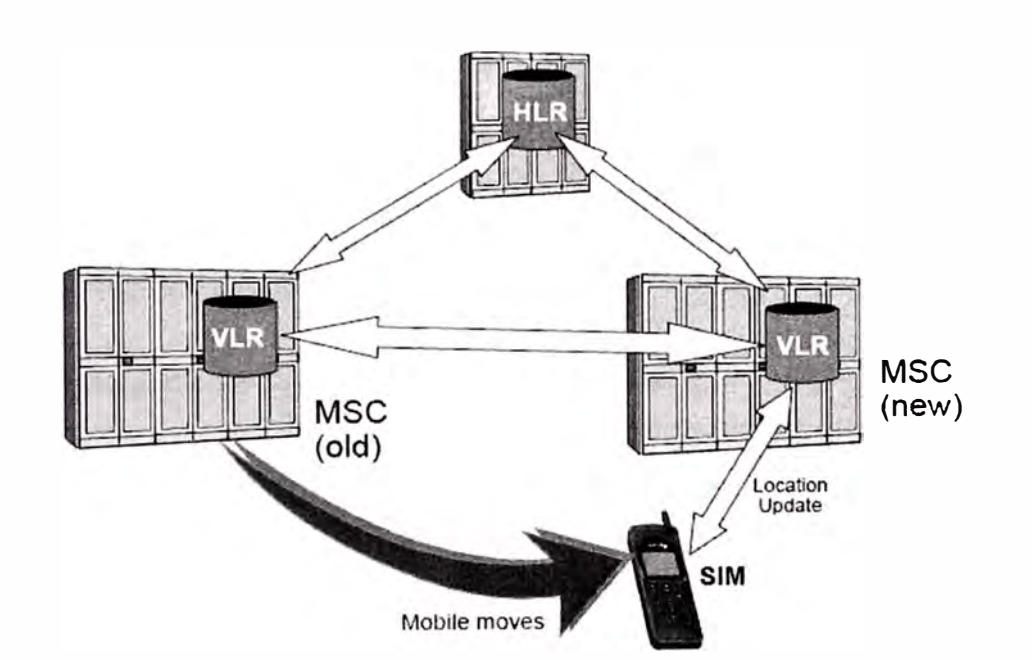


Figura 1.14: Elementos involucrados en el Location Update

En la siguiente figura, se describe brevemente los tipos de mensajes que son intercambiados en la primera vez que un abonado hace un Location Update, es decir, la primera vez que una estación móvil es encendida con la tarjeta SIM insertada.

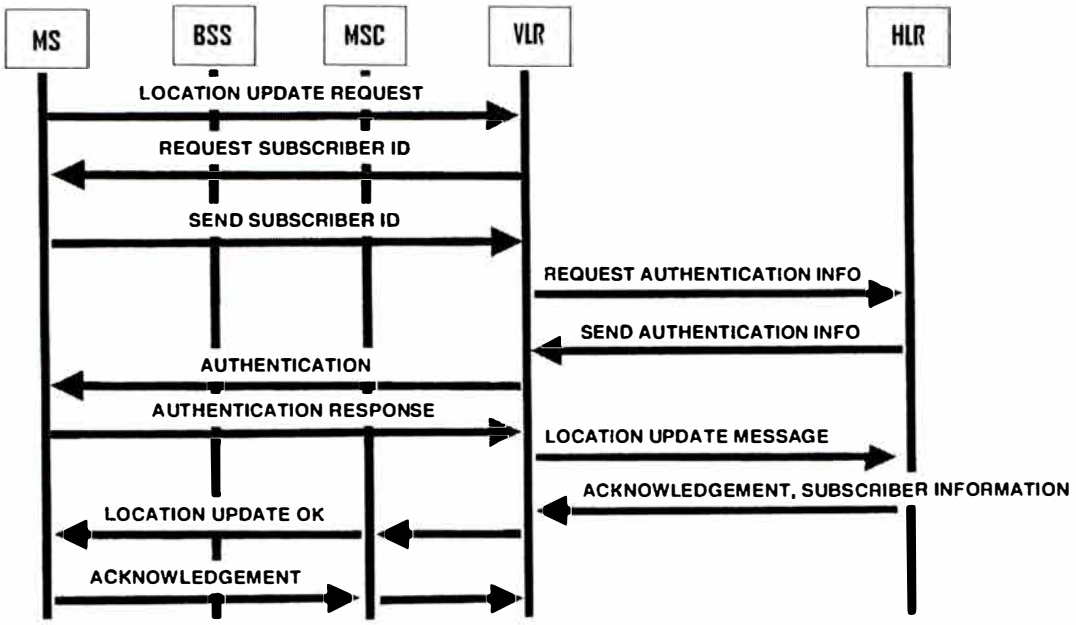


Figura 1.15: Procedimientos en la actualización de ubicación

El procedimiento de ubicación, registration/IMSI attach, permite a la red mantener el rastro del abonado todo el tiempo. El seguimiento de la ubicación es solo una función básica que permite a otros mecanismos de red a operar. Esto llega a ser más complicado cuando sea necesario establecer una llamada.

1.2.2 Establecimiento de la llamada en una red GSM

Es posible presentar 2 casos básicos de establecimiento de llamada. Estos casos pueden variar para diferentes situaciones. La primera es originada en la red PSTN o llamada terminada en el móvil, y la segunda es una llamada originada en el móvil o llamada terminada en la red PSTN.

El establecimiento de una llamada consiste de un considerable número de operaciones. Estas operaciones incluyen señalización entre centrales de conmutación, identificación y localización del abonado quién está siendo llamado, decisiones de encaminamiento y conexiones de tráfico, etc.

a) Establecimiento de la llamada originada en la red PSTN – llamada terminada en el móvil

Este es el establecimiento de una llamada entre un teléfono en una red de telefonía fija y una estación móvil GSM.

1.- Un abonado en una red de telefonía fija marca el número de una estación móvil. Esta llamada puede ser nacional o internacional. Un ejemplo de un número nacional es:

040 2207959

Un ejemplo de un número internacional es:

+358 40 2207959

El número marcado es llamado Número ISDN internacional móvil del abonado (MSISDN: Mobile Subscriber Internacional ISDN Number), el cual contiene los siguiente elementos:

MSISDN = CC + NDC + SN

CC (Country Code): Código de pais (358 es Finlandia)

NDC (Nacional Destination Code): Código nacional de destino

SN (Subscriber Number): Número de abonado

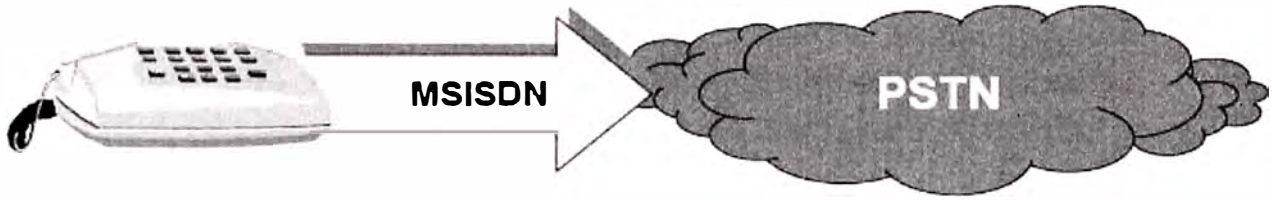


Figura 1.16: La llamada es originada en la red PSTN

2.- La red PSTN analiza el número marcado. El resultado del análisis es la información de encaminamiento requerida para encontrar la red móvil PLMN en la cual el abonado llamado ha hecho su inscripción. La red PSTN identifica la red móvil con el NDC, después éste accesa a la red móvil vía el GMSC más cercano.

3.- El GMSC analiza el MSISDN de la misma forma como lo hizo la red PSTN. Como resultado del análisis, éste obtiene la dirección del HLR, que es el elemento en donde el abonado está permanentemente registrado. Notar que el GMSC no tiene información acerca de la ubicación del abonado llamado. La ubicación del abonado puede solo ser determinada por las 2 bases de datos HLR y VLR. En ésta etapa el GMSC solo conoce la dirección del HLR, así que éste envía un mensaje (conteniendo el MSISDN) al HLR.

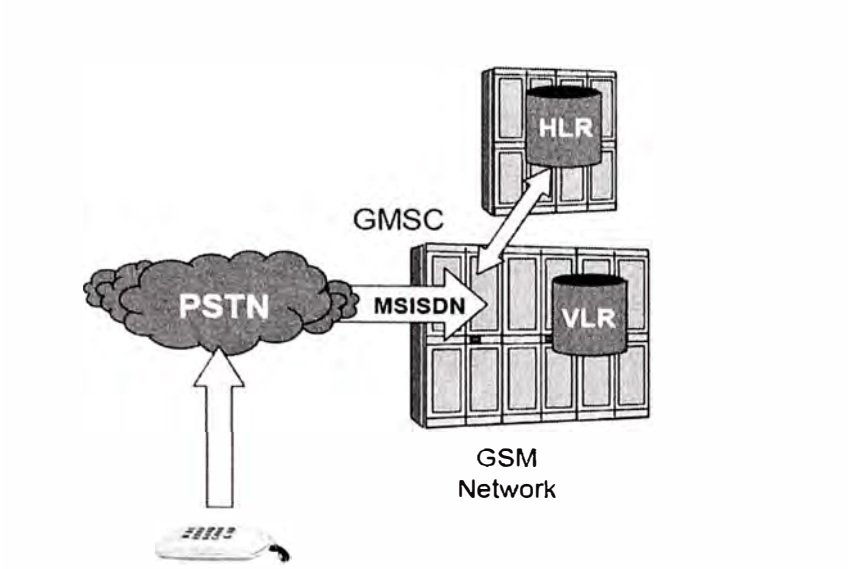


Figura 1.17: Llamada entrante desde la red PSTN a la red móvil

En la práctica éste mensaje es una solicitud para buscar al abonado llamado para el establecimiento de llamada. Esto es llamado Consulta al HLR (HLR Enquiry). Muchas redes soportan una función adicional llamada Portabilidad del número móvil, en el cual se hace el uso de un elemento de red llamado Registro del servicio de encaminamiento (SRR). El SRR sirve como un punto de conexión de señalización y todos los establecimientos de llamadas terminadas en el móvil son analizados aquí. Si existe un valor para un MSISDN, éste apuntará al HLR en donde el abonado está actualmente registrado.

4.- El HLR analiza el mensaje. Este identifica al abonado llamado en base del MSISDN y luego verifica su base de datos para determinar la ubicación del abonado. Como se sabe, el HLR es informado cada vez que el abonado se mueve de un área VLR a otra, es decir, el HLR siempre conoce en cual área VLR el abonado está actualmente registrado.

El HLR no maneja todo el tráfico de la red. Una conexión de tráfico requiere 2 elementos de red que sean capaces de proveer conexiones de voz. Una conexión de voz es un servicio de red y solo puede ser manejado por la MSC.

Por lo tanto, al habilitar la conexión de tráfico quizás 2 MSCs tendrán que estar conectadas. La primera MSC es el Gateway MSC (GMSC), el cual está contactado a la PSTN. El HLR actúa como un coordinador para establecer la conexión entre el Gateway MSC y la MSC destino (el cual también pudo ser el GMSC).

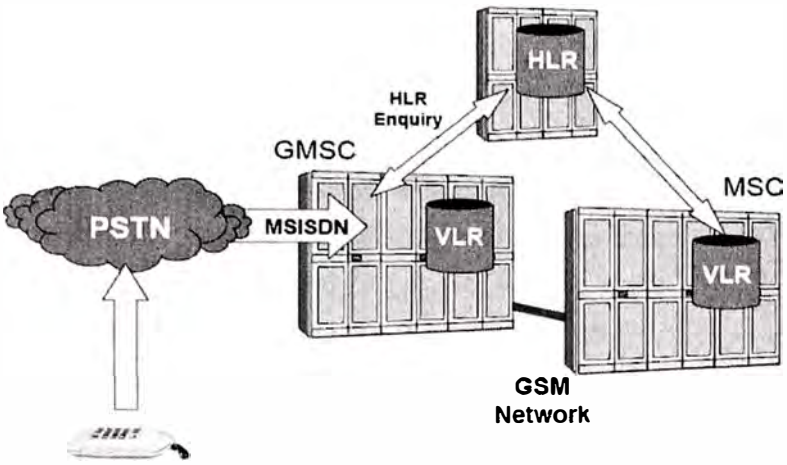


Figura 1.18: Encaminamiento de la llamada dentro de la red GSM

Ejemplo:

Usaremos un abonado italiano como ejemplo:

HLR:

MSISDN: 39 347 220759

IMSI: 222 10 1234567890

Dirección VLR: xyz

Datos de abonado: servicios, etc.

Como se puede ver, el primer campo contiene números de identidad del abonado. El propósito del número de Identidad internacional móvil del abonado (IMSI) es identificar al abonado en la red móvil. La longitud total del abonado es hasta 15 dígitos y contiene los siguientes elementos:

IMSI = MCC + MNC + MSIN

MCC (Mobile Country Code): Código móvil de país (3 dígitos)

MNC (Mobile Network Code): Código móvil de red (2 dígitos)

MSIN (Mobile Subscriber Identification Number): Número de identificación móvil del abonado (hasta 10 dígitos)

El número IMSI es usado para registrar un usuario en la red PLMN. Para ubicar un abonado y habilitar la conexión de tráfico, el HLR tiene que asociar el MSISDN con la IMSI del abonado móvil.

5.- Ahora el HLR interroga al MSC/VLR que está actualmente sirviendo al abonado llamado. Pero, ¿porqué necesitamos interrogar en vez de conectar directamente? Primero, el estado actual de la estación móvil es almacenado en la base de datos del VLR y necesitamos conocer el estado para evitar el establecimiento de una llamada a un abonado cuyo teléfono está apagado. Segundo, necesitamos tener alguna clase de información que permita al GMSC encaminar la llamada al MSC objetivo, esto puede ser en cualquier parte del mundo.

6.- En términos de enrutamiento de llamada, el MSC/VLR que está sirviendo al abonado es el destino de la llamada. Esto significa que debemos dirigir la llamada a éste usando el siguiente procedimiento: Después de recibir el mensaje del HLR, el MSC/VLR que está sirviendo al abonado genera un Número roaming de la estación móvil (MSRN) temporal y lo asocia con la IMSI. El número roaming es usado para iniciar la conexión y tiene la siguiente estructura:

MSRN = CC + NDC + SN

CC (Country Code): Código de país (del país visitado)

NDC (Nacional Destination Code): Código Nacional de Destino (de la red que está sirviendo al abonado)

SN (Subscriber Number): Número de abonado

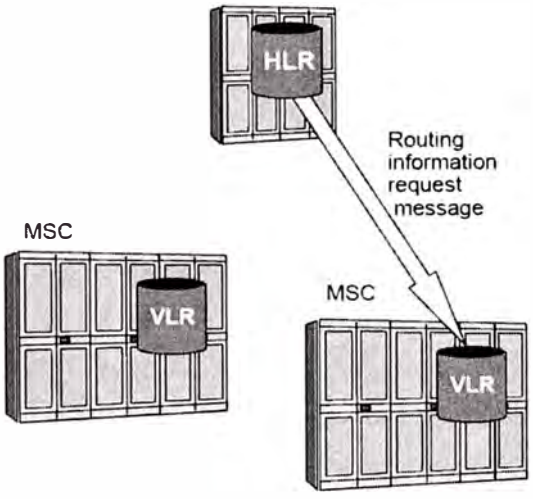


Figura 1.19: Solicitud del MSRN desde el HLR a la MSC que ésta sirviendo al abonado

Si comparamos el MSRN y el MSISDN, notamos que ellos tienen la misma estructura, aunque son usados para diferentes propósitos. El MSISDN es usado para interrogar al HLR, mientras que el MSRN es la respuesta dada por el MSC/VLR que está sirviendo al abonado y es usado para encaminar la llamada. El campo del número de abonado del MSRN es un número interno que está temporalmente asociado con la IMSI.

Dado que el número roaming es temporal, éste está disponible para el establecimiento de otra conexión de tráfico después que la llamada ha sido establecida. En esencia, el SN en el MSISDN apunta a una entrada de la base de datos en el HLR, y el SN del MSRN apunta a una entrada de la base de datos en el VLR.

7.- El MSC/VLR envía el número roaming al HLR. El HLR no analiza el número roaming, porque el MSRN es usado para transacciones de tráfico solamente y el HLR no maneja tráfico, es solo una base de datos que ayuda a la ubicación de los abonados y coordina el establecimiento de llamada. Por lo tanto, el HLR simplemente desvía el MSRN al Gateway MSC (GMSC) que originalmente inició el proceso.

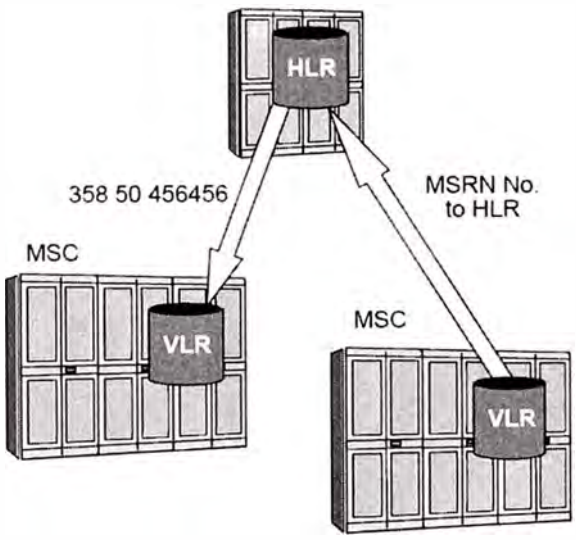


Figura 1.20: El MSRN es enviado al GMSC vía el HLR

8.- Cuando el GMSC recibe el mensaje conteniendo el MSRN, éste analiza el mensaje. El número roaming identifica la ubicación del abonado llamado, así el resultado de éste análisis es un proceso de enrutamiento, el cual identifica el destino de la llamada que es el MSC/VLR que está sirviendo al abonado.

9.- La fase final del proceso de enrutamiento es realizado por el MSC/VLR que está dando el servicio. Este MSC/VLR también tiene que recibir el número roaming así

sabrá que no es una llamada nueva, sino una llamada que está yendo a terminar allí, es decir, una llamada a la cual ya se le asignó un MSRN.

Ahora el enrutamiento de la llamada es hecho hacia la MSC/VLR destino, y es tiempo para que la MSC inicie el proceso paging.

Ubicación y paging del abonado

Con lo anterior, el GMSC/VLR y el MSC/VLR han sido conectados vía un canal de señalización y tráfico y el establecimiento de llamada ha sido casi completado. El abonado que llama está conectado a la red PSTN, la red PSTN está conectada al GMSC, el GMSC está conectado al MSC/VLR que está sirviendo al abonado llamado, pero aún no hemos establecido una conexión al abonado llamado. Para establecer la conexión, primero tenemos que entender como ubicar al abonado.

Como no conocemos la ubicación exacta del abonado, parece como si debemos buscar por él en toda el área de servicio del VLR, lo cual requeriría mucho trabajo para el MSC/VLR. Podemos por lo tanto definir geográficamente áreas limitadas donde podamos buscar un abonado. Estas son las Áreas de ubicación (Location Areas) y son manejadas por el MSC/VLR.

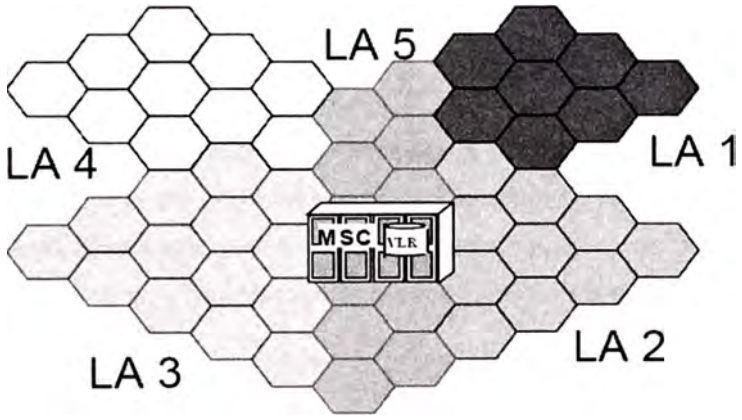


Figura 1.21: Áreas de ubicación bajo un MSC/VLR

Cada MSC/VLR contiene muchas áreas de ubicación. Podemos definir un área de ubicación como aquel en el cual podemos buscar al abonado en caso exista una llamada para él.

Los datos en el VLR para establecer la llamada con el abonado llamado son:

VLR:
IMSI: 222 10 1234567890
LAC: 262 15 0987
Datos:abc ....
MSRN: 358 50 456456

Cada área de ubicación es identificada por un número de Identidad de área de ubicación (LAI) y tiene la siguiente estructura:

LAI = MCC + MNC + LAC

MCC (Mobile Country Code): Código móvil de ciudad (del país visitado)

MNC (Mobile Network Code): Código móvil de red (de la red PLMN que está dando el servicio)

LAC (Location Area Code): Código de área de ubicación

Ahora que conocemos el área de ubicación del abonado, podemos empezar su búsqueda. Para ubicar al abonado, el proceso paging es iniciado en el área de ubicación. El Paging es una señal que es transmitida por todas las celdas en el área de ubicación. Este contiene la identificación del abonado. La identificación es llamada TMSI y es una identidad única temporalmente asignada por el VLR a los abonados móviles visitantes.

Incluso si la señal de paging es recibida por varias estaciones móviles en el área de ubicación, solo uno de ellos reconoce la identificación y responde a éste. Como consecuencia de ésta respuesta, una conexión punto a punto es establecida. Ahora los 2 abonados están conectados, y el tráfico puede ser llevado a través de la red.

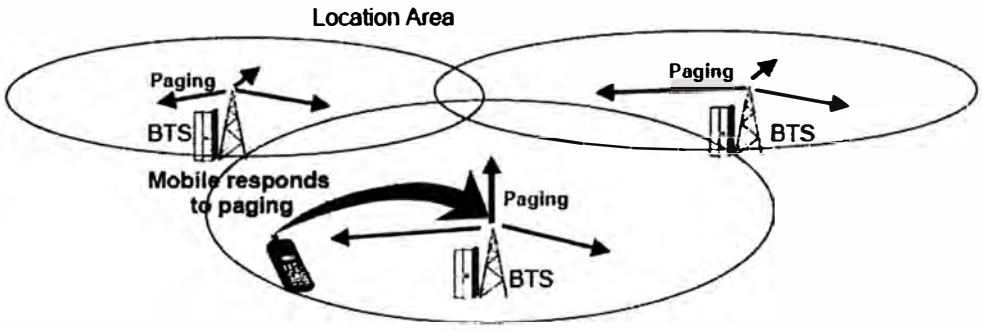


Figura 1.22: El proceso de PAGING

Llamada originada en la red PSTN – Proceso de establecimiento de llamada terminada en el móvil

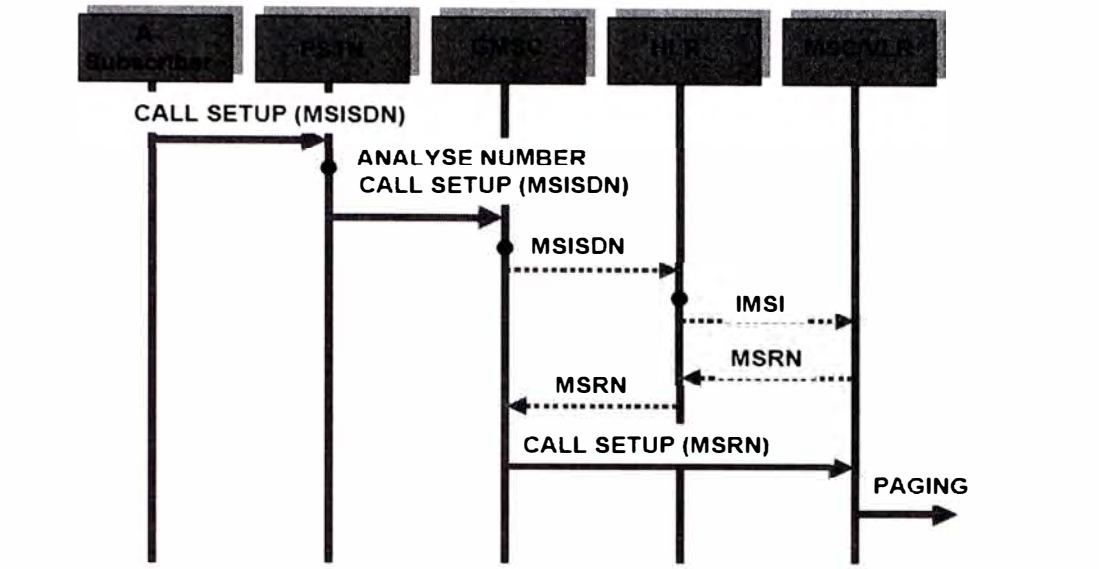


Figura 1.23: Pasos simplificados en el establecimiento de una llamada

1. Un abonado de la red de telefonía fija marca un número a un teléfono móvil (MSISDN).
2. Le red PSTN analiza el número y contacta al Gateway MSC (GMSC).
3. El GMSC analiza el MSISDN y envía un mensaje al HLR.
4. El HLR verifica su base de datos para determinar la actual ubicación del abonado llamado.
5. El HLR interroga al MSC/VLR que está actualmente sirviendo al abonado llamado.
6. El MSC/VLR que está sirviendo al abonado genera un MSRN temporal.
7. El MSC/VLR envía el MSRN al HLR y el HLR desvía el MSRN al GMSC.
8. El GMSC identifica el MSC/VLR que está sirviendo al abonado como el destino para encaminar la llamada.
9. El MSC/VLR destino recibe el MSRN. Este identifica el número que es llamado y rastrea al abonado llamado.
10. El MSC/VLR destino inicia un proceso paging en el área de ubicación para ubicar al abonado llamado. El teléfono móvil del abonado llamado reconoce la señal paging y responde a éste.

b) Llamada originada por el móvil

Este caso trata acerca de la conexión establecida cuando la llamada es iniciada por un abonado móvil.

El abonado móvil marca un número. En otras palabras, el abonado realiza una solicitud de servicio a la red en la cual él está actualmente registrado como un visitante. Después de recibir la petición, la red analiza los datos del abonado llamante para:

- Autorizar o denegar el uso de la red.
- Activar el servicio solicitado.
- Encaminar la llamada.

La llamada puede tener 2 tipos de destino: Una estación móvil o un teléfono en una red de telefonía fija. Si la llamada es direccionada a un teléfono en una red de telefonía fija, es encaminada a la red PSTN, el cual lo encamina al destino. Si el número llamado es otra estación móvil en la misma red, el MSC inicia el procedimiento de interrogar al HLR (HLR Enquiry), el cual es procesado de la misma manera como en el ejemplo de la llamada originada en la red PSTN.

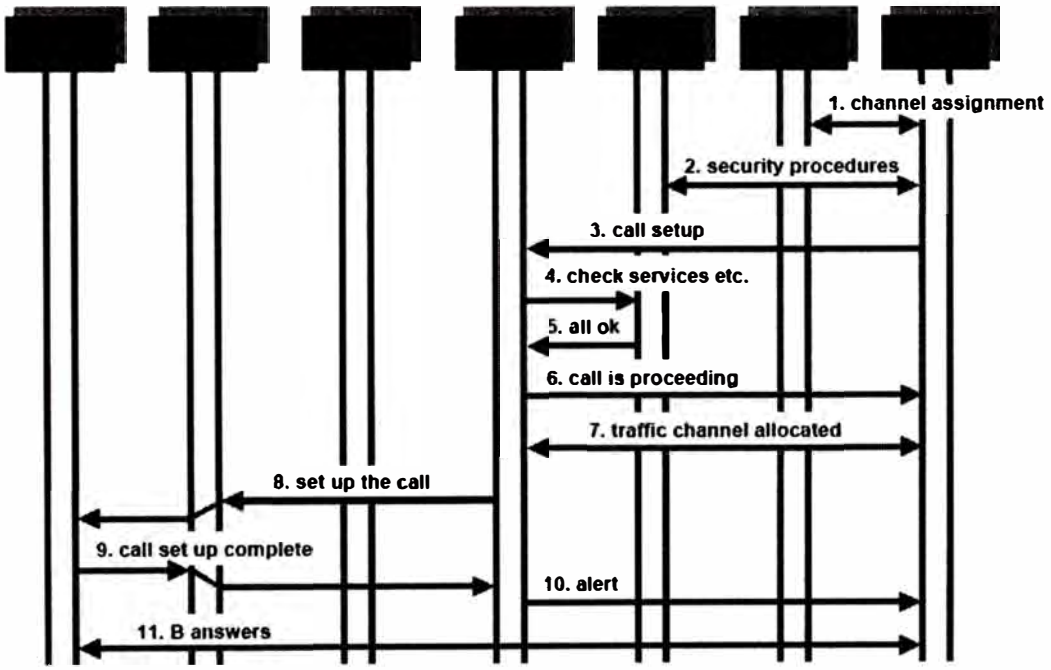


Figura 1.24: Procedimiento de llamada originada en el móvil

Dos pre-condiciones claves para el establecimiento de una conexión punto-punto son IDENTIFICAR y LOCALIZAR al abonado. El MSISDN cumple el propósito de identificación, pero la localización requiere un rápido y comprensivo sistema para mantener el rastreo del abonado. Si la red no tiene la información actualizada acerca de la ubicación actual del abonado, el establecimiento de una llamada significaría hacer paging en una gran área de red para encontrar al abonado y sería una tarea compleja y consumiría mucho tiempo. Para evitar esto, la red GSM monitorea y registra el movimiento de los abonados todo el tiempo. Este proceso es llamado Actualización de ubicación (Location Update).

1.2.3 Actualización de ubicación (Location Update)

a) Tipos de Location Update

En la práctica existen 3 tipos de Actualización de Ubicación (Location Update):

Registro de ubicación (encendido).
Genérico.
Periódico.

El registro de ubicación toma lugar cuando una estación móvil es encendida. Esto también se conoce como IMSI Attach, porqué tan pronto la estación móvil es encendida, ésta informa al VLR que ha vuelto al servicio y es capaz de recibir llamadas. Como resultado de un registro satisfactorio, la red envía a la estación móvil 2 números que son almacenados en la tarjeta SIM de la estación móvil.

Estos números son la Identidad del área de ubicación (LAI) y la Identidad temporal móvil del abonado (TMSI). La red envía el número LAI vía los canales de control de la interfase Air. El número TMSI es usado para propósitos de seguridad, así que el número IMSI del abonado no tiene que ser transmitido sobre la interfase Air. El número TMSI es una identidad temporal que cambia regularmente.

Una Identidad del área de ubicación (LAI) es un número único globalmente.
El Código de área local (LAC) es único en una red particular.

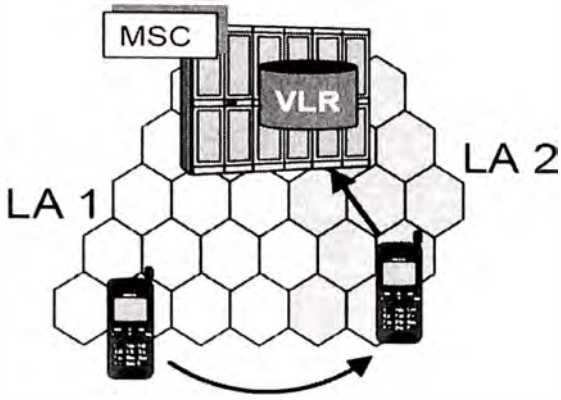


Figura 1.25: Registro de Ubicación

Cada vez que el móvil recibe datos a través de los canales de control, éste lee el número LAI y lo compara con el que está almacenado en la tarjeta SIM. Una Actualización de ubicación genérica es realizada si son diferentes. El móvil inicia un proceso de actualización de ubicación accesando al MSC/VLR que envío los datos de ubicación.

Un mensaje de solicitud de canal es enviado el cual contiene la identidad del abonado (es decir IMSI/TMSI) y el número LAI almacenado en la tarjeta SIM. Cuando el MSC/VLR objetivo recibe la solicitud, éste lee el antiguo número LAI, el cual identifica el MSC/VLR que sirvió al teléfono hasta ese punto. Una conexión de señalización es establecida entre ambos MSC/VLRs y el número IMSI del abonado es transferido desde la MSC antigua a la nueva MSC. Usando este IMSI, la nueva MSC actualiza el VLR y el HLR después de una autenticación exitosa. Este también recibe los datos del abonado desde el HLR.

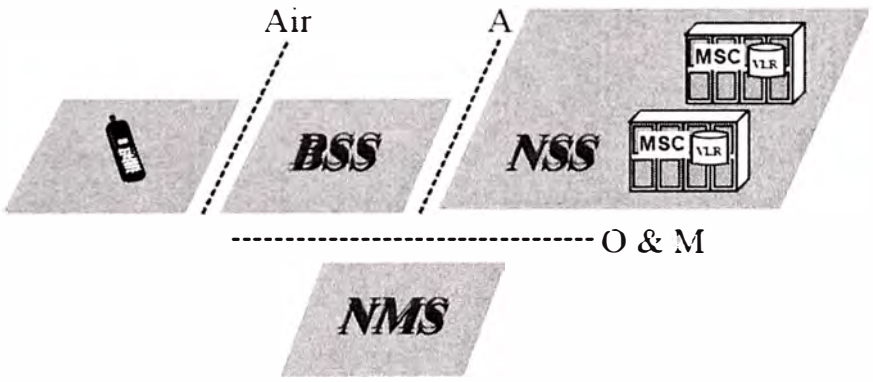


Figura 1.26: Elementos de red involucrados en la Actualización de Ubicación Genérica

La actualización de ubicación periódica es llevada a cabo cuando la red no recibe alguna solicitud de actualización de ubicación desde el móvil en un tiempo específico. Tal situación es creada cuando un móvil es encendido, pero el tráfico no es llevado a cabo, en el cual el teléfono móvil está solo leyendo y midiendo la información enviada por la red. Si el abonado se está moviendo dentro de un área de ubicación (Location Area), no hay necesidad de enviar una solicitud de Actualización de ubicación (Location Update).

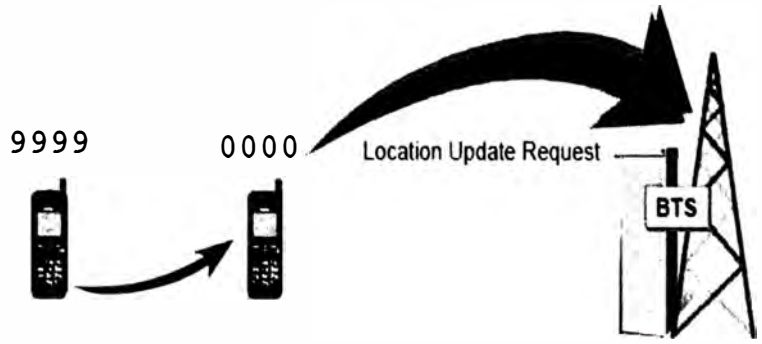


Figura 1.27: Ejemplo de una Actualización de Ubicación Periódica

El timer controla las actualizaciones periódicas, y el operador del VLR fija el valor del timer. La red difunde éste valor del timer y así la estación móvil conoce los valores del timer de la actualización de ubicación periódica. Por lo tanto, cuando el tiempo es establecido, la estación móvil inicia un proceso de registro enviando una señal de solicitud de Actualización de ubicación. El VLR recibe la solicitud y confirma el registro del móvil en la misma área de ubicación. Si la estación móvil no sigue éste procedimiento, puede ser que las baterías del móvil estén agotadas o el abonado está en un área donde no existe cobertura de red. En tal caso, el VLR cambia los datos de ubicación de la estación móvil a "no conocido".

b) Procedimientos

La siguiente figura describe brevemente el proceso de Actualización de ubicación cuando el abonado se mueve desde un área de ubicación bajo un MSC/VLR a otra área de ubicación bajo un nuevo MSC/VLR.

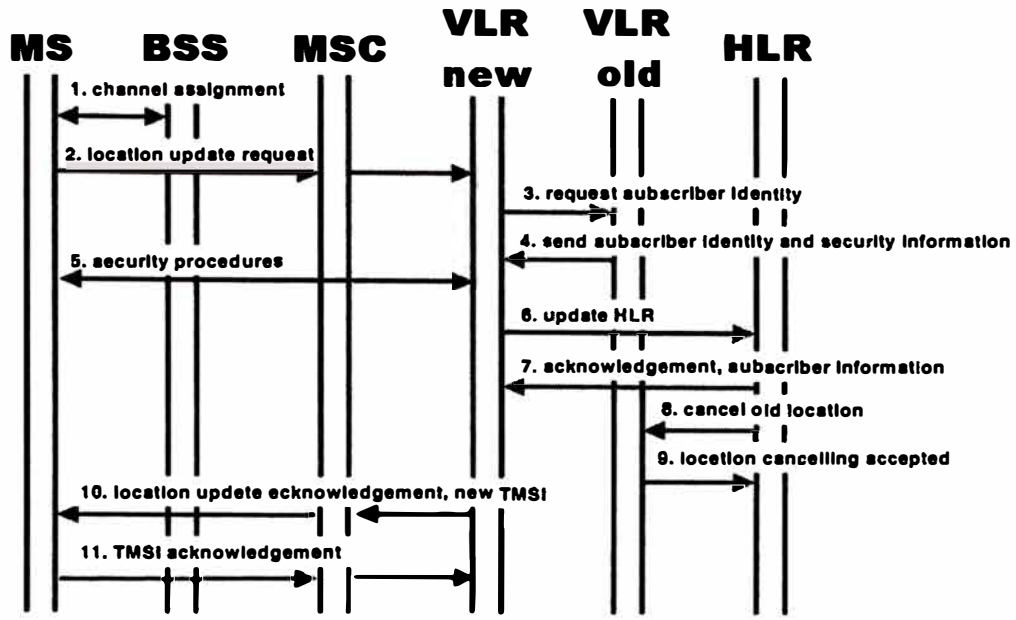


Figura 1.28: Procedimiento detallado en la actualización de ubicación

1.2.4 Handover

En una red de comunicaciones móviles, el abonado puede moverse alrededor de ésta. ¿Como se puede mantener la conexión en éste caso? Para comprender esto, tenemos que estudiar el proceso de Handover de llamadas.

Mantener la conexión del tráfico con un abonado en movimiento es hecho posible con la ayuda de la función handover. El concepto básico es simple: Cuando el abonado se mueve desde el área de cobertura de una celda a otra, una nueva conexión con la nueva celda tiene que ser establecida y la conexión con la antigua celda debe ser liberada. Existen 2 razones para realizar un handover:

El Handover debido a las mediciones, ocurre cuando la calidad o la fuerza de la señal de radio cae debajo de ciertos parámetros especificados en el BSC. El deterioro de la señal es detectado por la medición constante de la misma llevada a cabo por la estación móvil y la BTS. Como una consecuencia, la conexión es llevada a una celda con señal más fuerte.

El Handover debido a razones de tráfico, ocurre cuando la capacidad de tráfico de una celda ha alcanzado su valor máximo o se está aproximando a éste. En tal caso, las estaciones móviles cerca de los bordes de la celda pueden ser llevadas a las celdas vecinas con menos carga de tráfico.

La decisión de realizar un handover es realizada siempre por el BSC que está sirviendo al abonado, excepto el handover por razones de tráfico. En el último caso, la decisión es realizada por la MSC.

Existen 5 tipos diferentes de handover, y la mejor manera de analizarlos es siguiendo el movimiento del abonado:

a) Handover Intra Celda – Intra BSC

El más pequeño de los handovers es el intra-celda, en donde el abonado es llevado a otro canal de tráfico (generalmente a otra frecuencia) dentro de la misma celda. En éste caso, el BSC que controla la celda toma la decisión de realizar el handover.

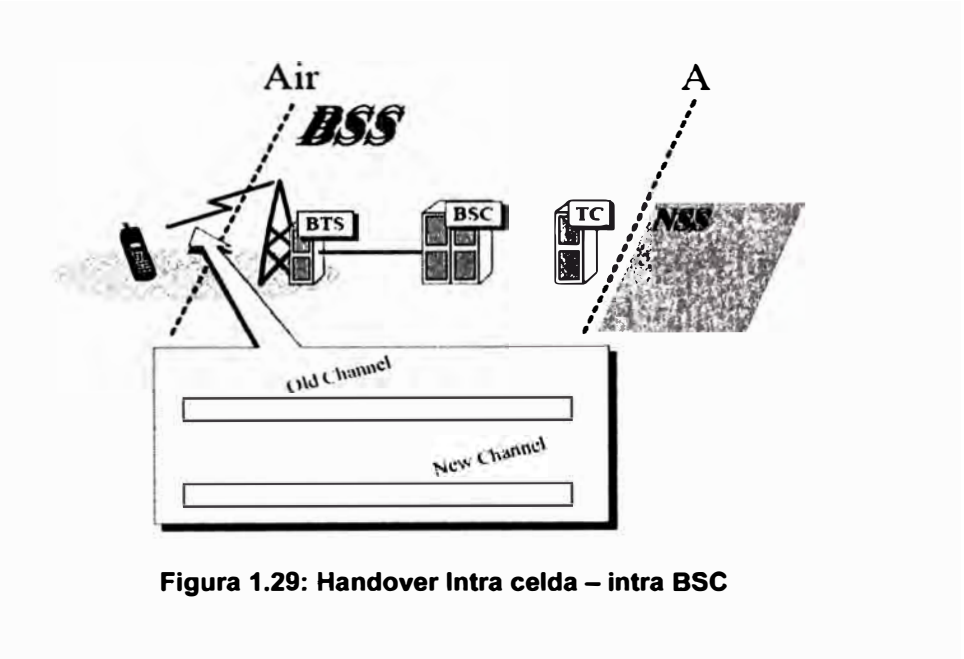


Figura 1.29: Handover Intra celda – intra BSC

b) Handover Inter Celda – Intra BSC

El abonado se mueve desde una celda 1 a una celda 2. En éste caso, el proceso de handover es controlado por el BSC. La conexión de tráfico con la celda 1 es liberada cuando la conexión con la celda 2 es establecida satisfactoriamente.

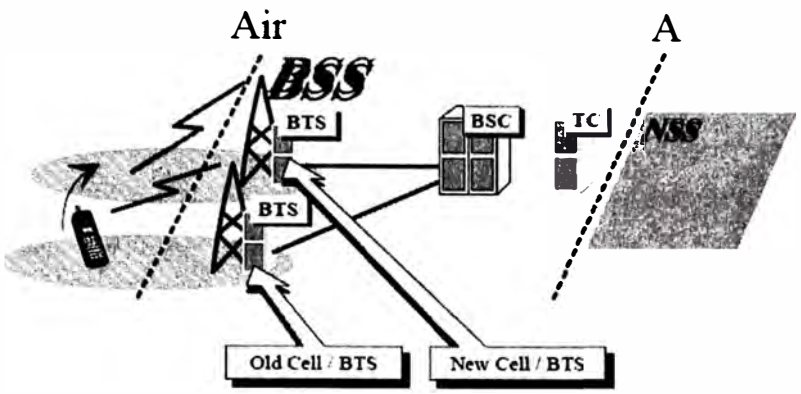


Figura 1.30: Handover Inter celda – intra BSC

c) Handover Inter Celda – Inter BSC

El abonado se mueve desde una celda 2 a una celda 3, el cual es servido por otro BSC. En éste caso, el proceso de handover es llevado a cabo por la MSC, pero la decisión de hacer el handover es aún hecho por el primer BSC. La conexión con el primer BSC (y BTS) es liberada cuando la conexión con el nuevo BSC (y BTS) es establecida satisfactoriamente.

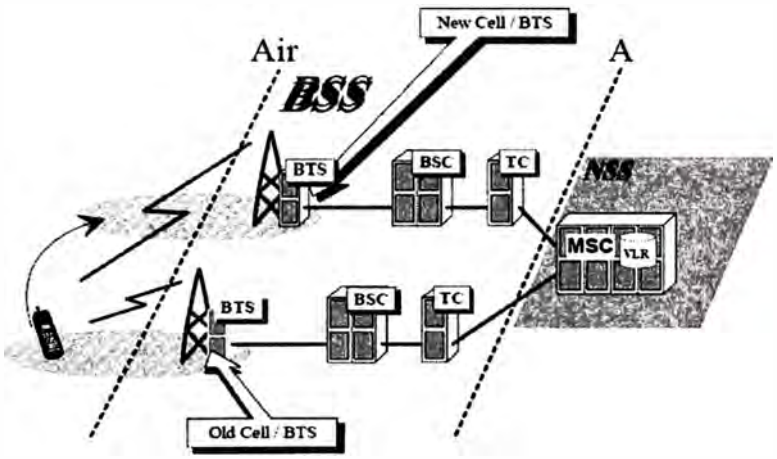


Figura 1.31: Handover Inter celda – inter BSC

d) Handover Inter MSC

El abonado se mueve desde una celda controlada por un MSC/VLR a una celda en el dominio de otro MSC/VLR. Este caso es un poco más complicado. Considerando que el primer MSC/VLR está conectado al GMSC vía un enlace que pasa a través de las líneas de la red PSTN, es evidente que el segundo MSC/VLR no puede asumir el control del primero.

El MSC/VLR que está actualmente sirviendo al abonado (MSC ancla) contacta al MSC/VLR nuevo y la conexión de tráfico es transferida a éste nuevo MSC/VLR. Como ambas MSCs son parte de la misma red, la conexión es establecida "suavemente". Es importante notar sin embargo, que la nueva MSC y la MSC origen son 2 centrales telefónicas. La llamada puede ser transferida entre 2 centrales solo si existe un número telefónico identificando a la nueva MSC.

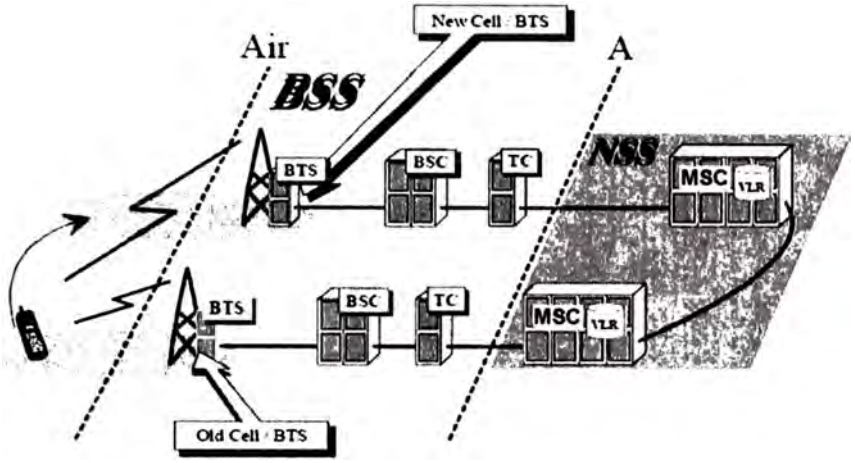


Figura 1.32: Handover Inter celda – Inter MSC

Tal situación hace necesario generar un nuevo número, el número de handover (HON). La MSC ancla recibe la información de handover desde el BSS. Este reconoce que el destino está dentro del dominio de otro MSC y envía una solicitud de handover (Handover Request) a la nueva MSC vía la red de señalización. La nueva MSC responde generando un HON y envía éste a la MSC origen (MSC ancla), la cual realiza un análisis digital para obtener la información necesaria de enrutamiento. Esta información permite a la MSC que está sirviendo al abonado a conectarse con la nueva MSC. Cuando ambas MSCs están conectadas, la llamada es transferida a una nueva ruta.

En la práctica, el número de handover es similar al número de roaming. El número de abonado identifica a la MSC que lo está sirviendo y está solo en uso temporal durante el handover. Más aún, el número de roaming y el número de handover tienen un propósito similar, conectar ambas MSCs. La estructura del número handover es:

$$HON = CC + NDC + SN$$

CC (Country Code): Código de País

NDC (Nacional Destination Code): Código nacional de destino

SN (Subscriber Number): Número de abonado

La llamada no durará para siempre y la conexión tiene que ser liberada lo más pronto posible. Para entender el proceso de liberación de conexión, debemos considerar: ¿Quién paga por la llamada?, ¿que central se encarga de la operación del charging (cargo)? y ¿donde están almacenados los datos del abonado?

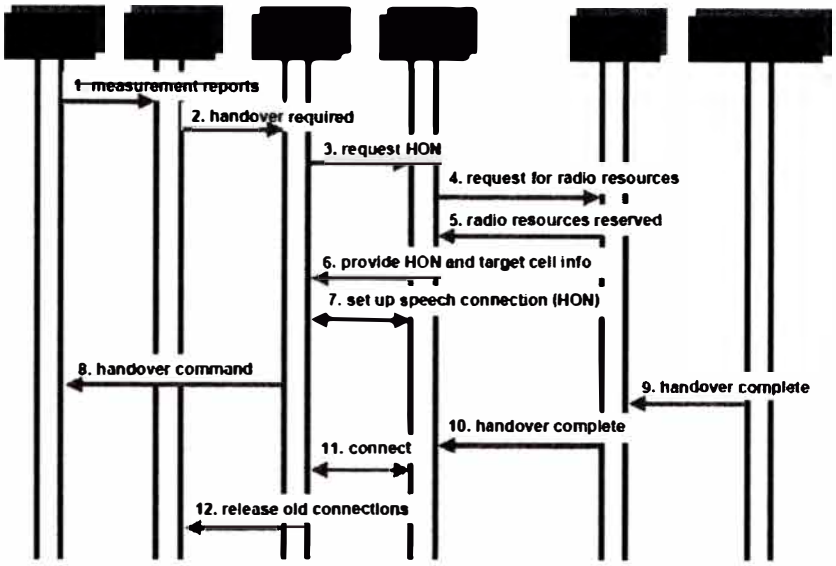


Figura 1.33: Procedimiento Handover Inter MSC

e) Handover Inter Sistemas GSM – UMTS

Las redes GSM/UMTS soportan handovers entre sistemas. Esto es importante por razones de cobertura dado que las redes UMTS son esperadas a incrementar la cobertura gradualmente. El handover inter sistemas es algunas veces realizado basado en la activación de servicio del abonado y debe ser dependiente de la aplicación usada. Este tipo de funciones además, permite a los operadores a mejorar los servicios del abonado de la red móvil.

Existen 2 tipos de handover inter sistemas en redes GSM/UMTS. Es posible realizar un handover desde el subsistema BSS de la red GSM a la red UTRAN o viceversa. Comparado a otros tipos de handovers, éste introduce nuevos desafíos dado que el handover es realizado entre 2 tecnologías de redes sustancialmente diferentes. Si una estación móvil necesita realizar un handover desde la red UTRAN a la red GSM (BSS), éste debe recibir información de la celda vecina. La información es necesaria para

medir celdas GSM candidatas. Basado en los reportes de medición el Controlador de la red de radio (RNC) de la red UTRAN hace la decisión de handover. Los recursos son reservados en el subsistema BSS y los mensajes son enviados al equipo del usuario conteniendo los comandos de handover. El equipo del abonado conmuta usando la funcionalidad GSM.

Un handover puede también ser realizado desde la red GSM a la red UTRAN y la función es similar a la descrita anteriormente. El equipo del abonado recibe los parámetros de la celda vecina para la red UTRAN en mensajes downlink desde el subsistema BSS. Basado en los reportes de medición para el subsistema BSS y la red UTRAN, el BSC hace la decisión de handover. Los recursos son reservados en la red UTRAN y el equipo de abonado recibe los parámetros necesarios para conmutar a la funcionalidad UTRAN.

1.2.5 Cargo del servicio (Charging)

El cargo del servicio en una red GSM sigue los principios similares que en la red de telefonía fija. En adición a un pago estándar, los abonados tienen que pagar por las llamadas que ellos hacen y los servicios que ellos usan. Sin embargo, existen algunas diferencias en como los costos son calculados y quién está obligado a pagarlos.

Cuando una persona adquiere el servicio, ésta recibe una tarjeta SIM personal del operador de red y su información básica (número de teléfono, tipo de servicio ordenado, etc.) es almacenada en las bases de datos de la red tal como el HLR. Para cubrir los costos de estas operaciones, los operadores de red frecuentemente cargan un costo inicial de suscripción.

Después que la suscripción es hecha y el suscrito ha llegado a ser un abonado de una red particular, está disponible para los servicios de red y los derechos a usarlos. Esto es un pago regular, el cual es cargado si el abonado hace o no la llamada. Esta clase de cargo es conocido como renta de servicio de la red.

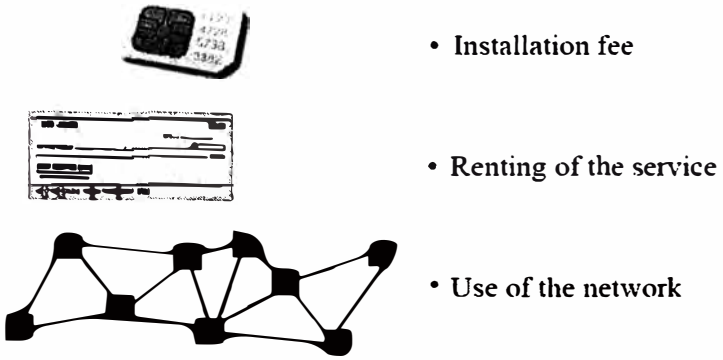


Figura 1.34: Diferentes maneras de cargo de servicio de un abonado (charging)

a) Cargo por el uso de la red (Charging)

El tercer tipo de cargo es aplicado al uso de la red en base de llamada por llamada. Existen muchos factores que afectan en cuanto el abonado tiene que pagar por hacer (y algunas veces recibir) una llamada. Los parámetros que pueden ser usados para facturar el servicio al abonado son las siguientes:

Tipo de servicio, por ejemplo, voz, SMS.

Duración de la llamada.

Tiempo en el día cuando la llamada es hecha, por ejemplo, horas de trabajo, tarde, noche.

Destino de la llamada (a quién se está llamado).

Origen de la llamada (desde donde hacemos la llamada), por ejemplo una cierta celda.

Uso de la red, por ejemplo la red PSTN.

Uso de servicios suplementarios tales como desvío y bloqueo de llamadas, servicios de red inteligente, etc.

Uso de los recursos de radio (cuando se realizan los handovers).

Roaming internacional.

El desvío de llamadas y el roaming son factores que no solo afectan el pago del servicio, sino que también se tiene que tener en cuenta de quién está obligado a pagar.

b) A quién cargar el pago del servicio

Demos un vistazo cercano del número marcado por el abonado llamante. El número incluye el código de destino nacional, el cual identifica la red local del abonado. Si el abonado quién es llamado está registrado en un área que pertenece a su red local, la conexión es establecida y el abonado que llama paga por la llamada.

Sin embargo, si el abonado quién es llamado está fuera del área de servicio de su red local (en otro país) y está conectado a otra red, entonces la llamada tiene que ser encaminada a él usando el servicio de una o más redes foráneas. En ese caso hablamos del roaming internacional, el cual se refiere a la conexión entre la red local y el abonado vía una red foránea. En tal caso, el cargo de la llamada será compartida de acuerdo a los siguientes principios:

El abonado llamante paga por la conexión al número marcado (MSISDN)

El abonado llamado paga por el roaming internacional

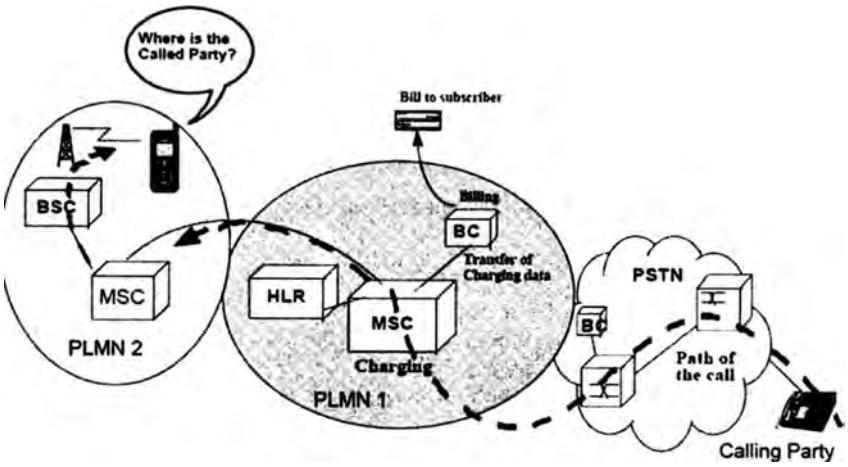


Figura 1.35: Enrutamiento de una llamada PSTN – GSM

El mismo principio es aplicado cuando el abonado móvil ha desviado las llamadas entrantes a otro número. El abonado llamante es solo responsable por los costos de las llamadas hasta la estación móvil del abonado llamado, y el usuario móvil paga por el desvío de las llamadas. Es decir, el abonado llamante no necesariamente conoce la ubicación del abonado llamado o los servicios y conexiones que son requeridos para acceder a él. El abonado llamante solo conoce que está marcando un número en una cierta red móvil, y por lo tanto él puede solo ser requerido a pagar por los servicios de los cuales él es consciente. El abonado llamado conoce si él está usando los servicios de una red foránea o algún servicio de cargo suplementario de su red local, y por lo tanto él está obligado a pagar por ellos.

La llamada Collect es el tercer caso en el cual el abonado llamado paga por la llamada. Una llamada Collect en una red GSM es similar a una llamada Collect en una red fija. Primero, el abonado llamado tiene que aceptar la llamada, el cual es responsable por todos los costos.

c) Procedimiento de charging en GSM

En la red de telefonía fija, el charging es normalmente determinado por la colección de pulsos de medición, por la cual la central de conmutación puede calcular el precio de la llamada. Este método es llamado tiempo de cargo de servicio (time charging). El abonado llamante (abonado A) es normalmente quién paga por la llamada. En la red móvil, el abonado llamado (abonado B) es normalmente requerido ha pagar parte del servicio con el uso de roaming, porque el abonado A no necesariamente conoce donde se encuentra ubicado el abonado B.

En una red GSM existen diferentes maneras para definir el charging que es sensible a crear un registro en el MSC o/y HLR acerca de cada evento que puede ser una base para el charging. Estos eventos pueden ser los casos de llamada definida u otros eventos de cargos posibles, tales como la Actualización de ubicación (location update). El registro conteniendo la información acerca de un evento de cargo es llamado Registro de datos de cargo o charging (CDR) o el "boleto de peaje" (TT).

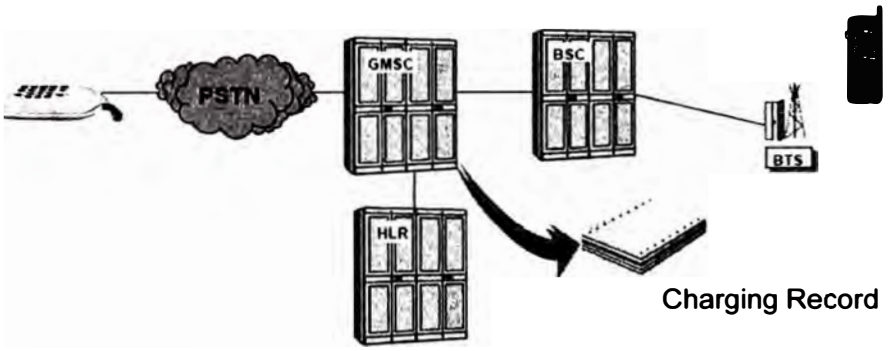


Figura 1.36: El GMSC es responsable de la creación de registros de charging

Estos registros son almacenados primariamente como archivos de charging en la MSC o HLR, y luego los archivos son transferidos a un centro de facturación separado. El operador que está dando el servicio controla todo el proceso de charging. El proceso comienza cuando una llamada es establecida y en el mismo tiempo, un registro de charging es abierto en el MSC/VLR que esta dando el servicio.

En general, la primera y última MSC involucradas en un establecimiento de llamada recolectan el registro de charging.

Conforme la llamada continúa, el abonado se mueve en el área de servicio del operador e ingresa al área de servicio de otro MSC/VLR, y así es realizado un handover inter MSC. El registro de charging no es transferido a la nueva MSC durante el handover. En vez de ésto, la MSC mantiene el registro de la llamada mientras dura.

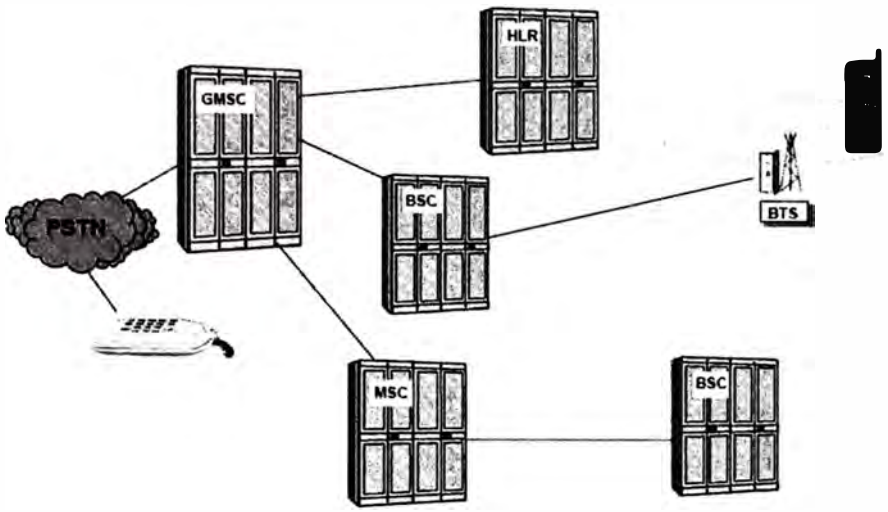


Figura 1.37: Elementos involucrados en el manejo de una llamada

Cuando la llamada ha sido liberada, el registro de charging es cerrado. Cuando un número suficiente de registros de charging ha sido acumulado, éstos son enviados a un Centro de facturación vía conexión X25 o Ethernet.

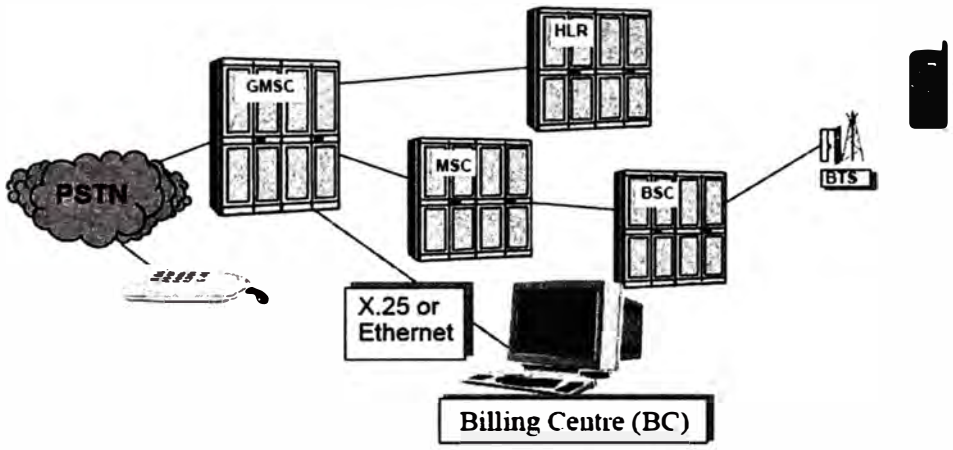


Figura 1.38: Transferencia de datos de charging al centro de facturación

Como el actual charging es afectado por una variedad de factores, el registro de charging contiene todos los eventos que pueden ser usados para determinar el cargo del servicio. La información para un abonado es recolectado desde varios MSCs y Centros de facturación que el móvil ha visitado.

d) Cargo de servicio distribuido

Para producir los cargos del servicio (billing) de cada abonado, los centros de facturación deben recolectar datos de charging detallados desde todos los MSCs dentro de la PLMN. Con el roaming internacional, ésta operación debe ser extendida para cubrir todas las PLMNs donde existe un contrato de roaming. La información de charging debe ser recolectada desde los Centros de facturación (BC) de todas las redes que han sido visitadas por el abonado, y pasados al centro de facturación de la red local.

Figura 1.39: Cargo de servicio distribuido

Cuando 2 operadores GSM firman un "contrato de roaming", ellos acuerdan cuan frecuentemente trasferirán los datos de charging entre ellos. El centro de facturación local analiza la información de charging recolectada desde todas las redes donde existe un contrato de roaming, y genera la facturación para el abonado.

e) Servicio prepago

El principio básico del servicio prepago es que un abonado pague una cierta cantidad de dinero por adelantado a una cuenta prepago. Con éste pago, el abonado es permitido ha realizar llamadas telefónicas. Cada vez que el abonado hace una llamada, el dinero de la cuenta prepago es deducido en tiempo real de acuerdo a la tarifa aplicada.

Cuando el límite de la cuenta es alcanzada, las llamadas pueden ser barridas, continuadas como normal o encaminadas a un número especial, donde el abonado es capaz de recargar dinero a su cuenta otra vez. Las suscripciones del servicio prepago no necesariamente involucran pagos de conexión o mensuales, pero la carga por minuto de las llamadas es usualmente más alta que las llamadas postpagos.

Este servicio ofrece muchos beneficios al operador. El abonado deposita un cierto crédito por adelantado, así los operadores pueden estar seguros que las llamadas son pagadas y el dinero no necesitaría ser recolectado luego. El operador puede controlar el uso del servicio estableciendo límites a las llamadas. Las configuraciones de los límites de llamadas significan que el número de llamadas que el abonado hace durante un cierto periodo puede ser configurado. En adición, el periodo de tiempo cuando el servicio está activo puede ser configurado.

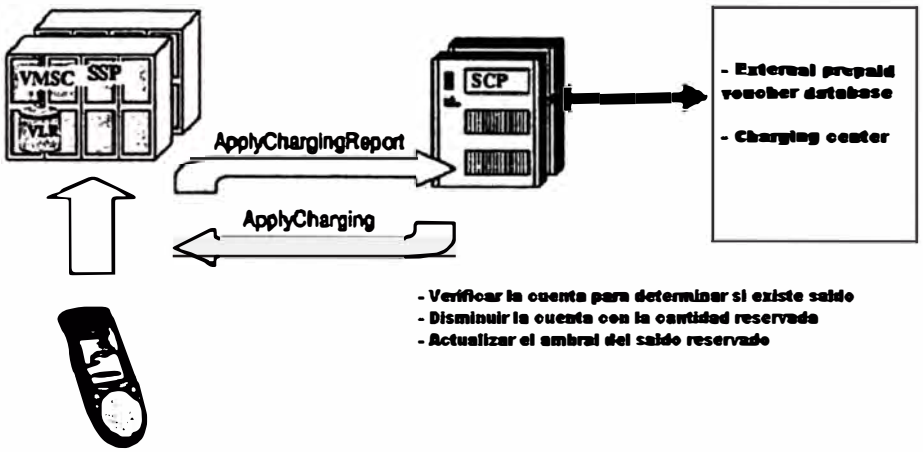


Figura 1.40: Arquitectura prepago

El servicio prepago está disponible para llamadas de voz tradicionales y para datos, fax y servicio SMS. También los métodos de charging y tarificación han sido mejorados y además son desarrollados para reunir los requerimientos del futuro (El charging del GPRS basado en contenido, volumen, punto de acceso o calidad de servicio; el manejo del charging en situaciones de roaming complejas, charging del servicio multimensaje). Puede ser anticipado para el futuro que el servicio prepago puede ser considerado como un método de pago en vez de un servicio como tal. Así, el objetivo es tener todos los servicios prepagos cumplidos. Una cuenta prepago por suscripción debe estar disponible para cargos independientes del servicio.

1.3 Señalización SS7

1.3.1 Introducción

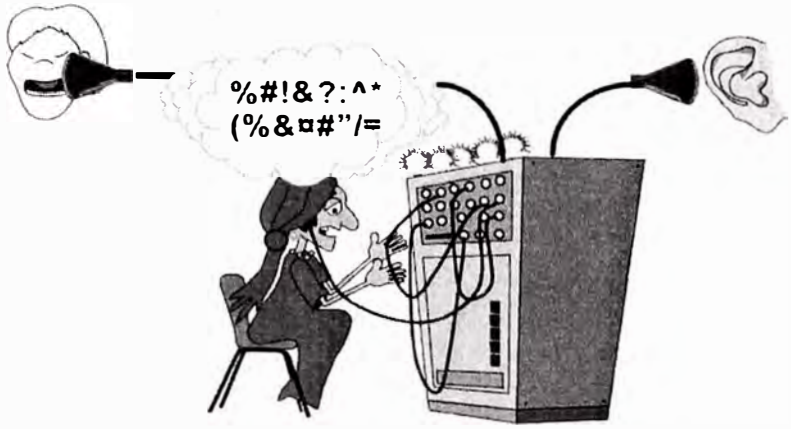


Figura 1.41: La señalización en tiempo antiguo

El siguiente diagrama muestra los pasos básicos para el establecimiento de la llamada:

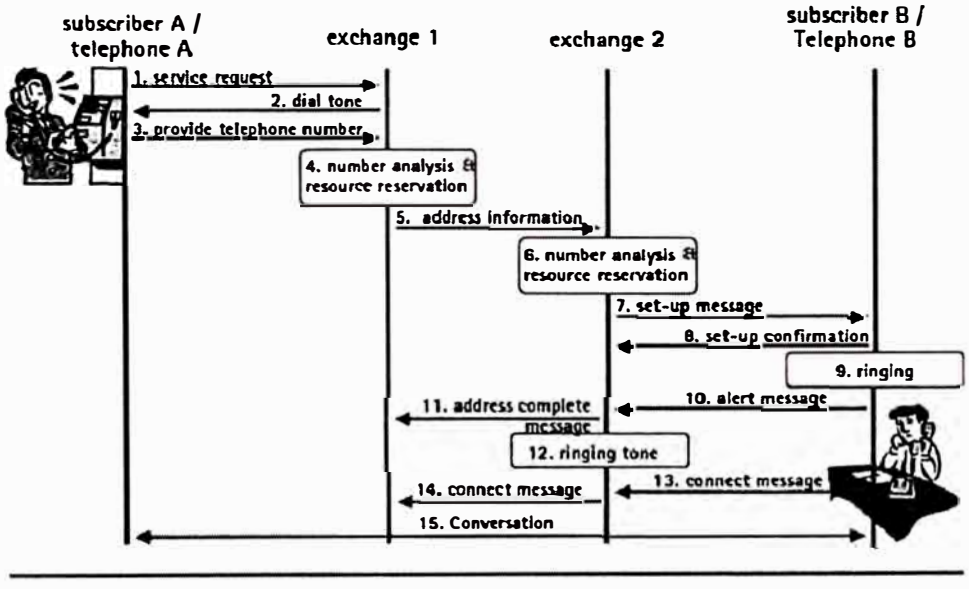


Figura 1.42: Operaciones de la señalización

Los teléfonos y las centrales realizan el intercambio de mensajes para una llamada en proceso. Por ejemplo, entre las centrales 1 y 2 existen recursos de transmisión. Ellos intercambian mensajes para llevar a cabo la información entre los

abonados A y B, en donde los recursos disponibles de transmisión son asignados a ésta llamada específica. Sino, una central liberaría los recursos de transmisión, mientras el otro los bloquea. Esto ya indica la importancia del intercambio de mensajes entre elementos de red de una red de telecomunicaciones.

Estos mensajes son llamados Mensajes de Control y Señalización. Un sistema de señalización representa un conjunto de reglas específicas sobre como los elementos de red tienen que intercambiar información de señalización y control. Cada sistema de señalización debe soportar mensajes para:

Establecimiento de llamada.
Supervisión de llamada.
Terminación de llamada y
Manejo de alguna situación anormal.

En Europa, el Sistema de señalización digital de abonado número 1 (E-DSS1) es frecuentemente usado entre centrales de conmutación y teléfonos. Entre centrales de conmutación, el Sistema de señalización de canal común número 7 (CCS#7, CS#7, SS#7, SS7) es el protocolo más usado. Este también ha sido adoptado para GSM.

1.3.2 Implementación y evolución

La señalización en los sistemas de Telecomunicaciones es básicamente un conjunto de mensajes usados para establecimiento, supervisión y liberación de la llamada. Muchos factores han conducido a una variedad de sistemas de señalización que están siendo desarrollados en las redes de telecomunicaciones. Los diferentes estándares de señalización fueron desarrollados en diferentes partes del mundo. Ellos hacen la misma tarea, pero en diferentes maneras. Esto significaría que cuando una llamada es originada en una red con un tipo de implementación de señalización y termina en otra red con otro tipo de sistema de señalización, tendría que ser usado algún tipo de adaptación.

Debido a estas diferencias el Comité consultivo internacional telegráfico y telefónico (CCITT) ahora Unión internacional de telecomunicaciones (ITU), recomendó el Sistema de señalización de canal asociado como un estándar. En el CAS, los mensajes de señalización y la voz/datos de usuario son transmitidos en el mismo recurso de transmisión.

a) Señalización de Canal Asociado (CAS)

Es el método en el cual la información de señalización que relaciona al tráfico llevado por un solo canal es transmitido en el mismo canal o en un canal permanentemente acosiado con éste.

Como un sistema de señalización para el establecimiento de llamadas, el CAS fue un buen sistema que funcionó bastante bien. Un gran número de centrales telefónicas en el mundo están todavía usando éste sistema, pero su implementación es solo adecuada para casos en donde el tráfico es bajo. Otro problema con el CAS es que no es posible enviar mensajes de señalización en la ausencia de una llamada.

b) Señalización de Canal Común (CCS)

La CCITT (ahora ITU) dio una nueva recomendación para el sistema de señalización el cual fue el sistema de señalización de canal común número 7. Una de las principales ventajas del sistema fue que la señalización no tiene que ir a lo largo del mismo canal que la voz.

El SS7 fue desarrollado a comienzos de 1980 y es un sistema de señalización de canal común (CCS) con un ancho de banda del canal de señalización de 64kbits/s. El término "Señalización de Canal Común" indica, que la información de señalización y datos de usuario son transmitidos vía recursos separados. Los mensajes de señalización son transmitidos vía recursos de transmisión, los cuales son usados por varios cientos hasta miles de llamadas.

El SS7 es orientado a paquetes, es decir los mensajes de señalización son enviados como paquetes de manera similar que lo paquetes IP en la Internet. La carga de señalización es baja en comparación al tráfico de datos de usuario. Existe necesidad de recursos de señalización durante el establecimiento de llamada y la fase de terminación de la misma. El uso de recursos comunes resulta en una eficiencia bastante alta para los recursos de señalización.

Los puntos finales de los mensajes de señalización SS7 son las centrales de conmutación, tales como la MSC, pero también los elementos de registro como el HLR. Dentro del SS7, el generador y el receptor de los mensajes de señalización SS7 son llamados Puntos de señalización (SP). Depende del operador si los puntos de servicio pueden intercambiar directamente mensajes SS7. Frecuentemente, el encaminamiento de los mensajes SS7 es hecho vía Puntos de transferencia de señalización (STP). Un punto de transferencia de señalización recibe mensajes SS7, analiza la dirección de destino del mensaje SS7, luego desvía el mensaje, siguiendo el conjunto de reglas

establecidas por el operador en las tablas de encaminamiento del punto de transferencia de señalización.

1.3.3 Sistema de Señalización de Canal Común número 7 (SS7)

Originalmente, el Sistema de señalización de canal común número 7 (SS7) consistió de 2 partes: La primera parte fue responsable de la transferencia del mensaje dentro de una red de señalización. La segunda parte fue el usuario de estos mensajes. Es decir:

Parte de transferencia de mensajes (MTP): Responsable de la transferencia de mensajes.

Parte de usuario de telefonía (TUP): Usuario de los mensajes.

a) Parte de Transferencia de Mensajes (MTP)

Hemos establecido hasta ahora que la señalización es usada para el establecimiento de llamada, y que existen sistemas estándares de mensajes, los cuales son enviados hacia delante y hacia atrás para ayudar a facilitarlo. La parte responsable de tomar estos mensajes desde un elemento de red a otro es conocida como la Parte de transferencia de mensajes (MTP). El SS7 es construido sobre el fundamento del MTP, el cual consiste de 3 subcapas, como siguen:

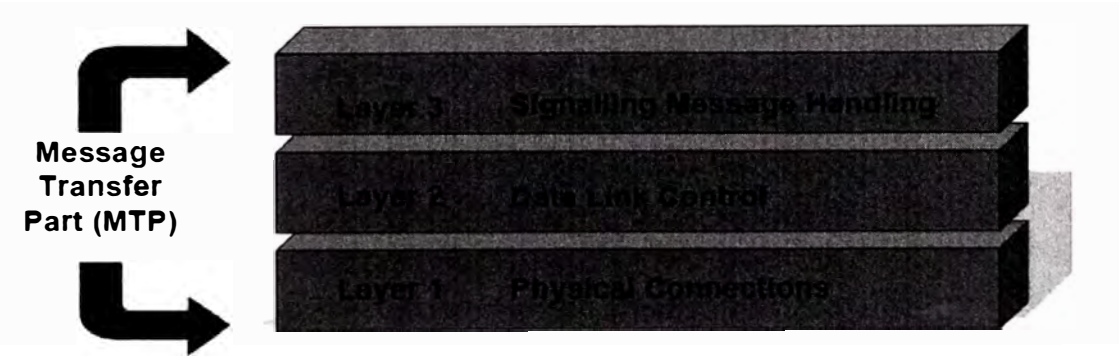


Figura 1.43: Capas de la parte de transferencia de mensajes

El nivel más bajo, capa 1 del MTP (Conexiones físicas), define las características eléctricas y físicas. La capa 2 del MTP (Control de enlaces de datos), ayuda en la transmisión libre de errores de los mensajes de señalización entre elementos adyacentes. La capa 3 del MTP (Capa de red) es responsable de tomar el mensaje desde cualquier elemento en una red de señalización a cualquier otro elemento dentro de la misma red.

b) Parte de Usuario de Telefonía (TUP)

¿Quién es el usuario quién recibe, envía y actúa sobre éstos mensajes (MTP)? La respuesta es la parte de usuario de telefonía. Aquellos sistemas estándares de mensajes mencionados previamente son los mensajes estándares TUP que ayudan al establecimiento de llamadas, a la supervisión y liberación de ésta.

Para muchos el SS7 en la red de telefonía fija consistió de solo 2 partes, el MTP y el TUP. El CCITT (ahora ITU) permitió variaciones en los mensajes llamadas Parte de usuario nacional (NUP).

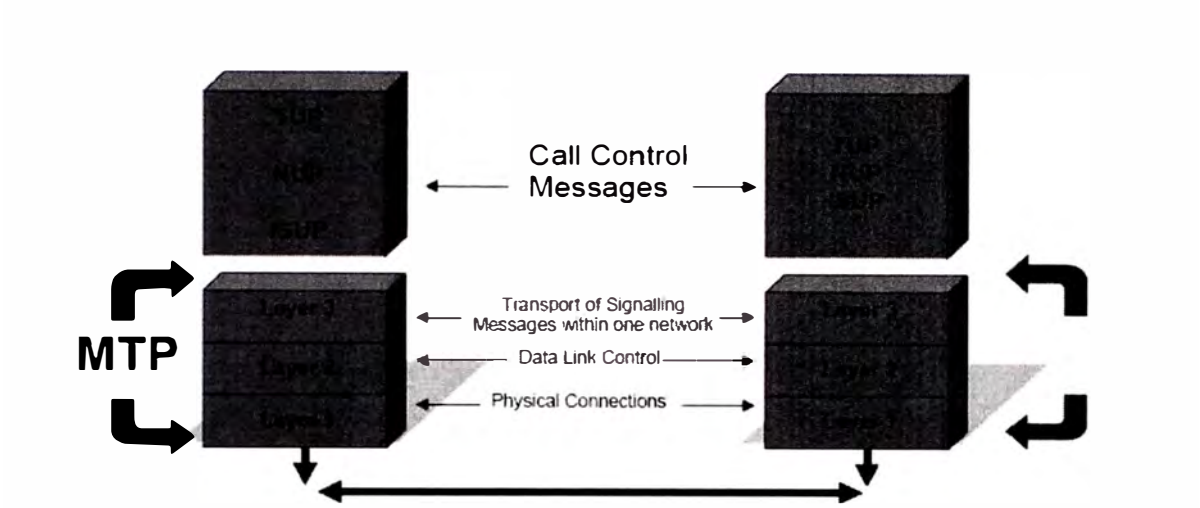


Figura 1.44: Grupo de protocolos MTP y TUP/NUP/ISUP

Con la introducción de la Red digital de servicios integrados (ISDN), la cual tiene una capacidad más amplia que la PSTN, algunos mensajes adicionales son requeridos. Estos han llegado a ser conocidos como la Parte de usuario ISDN (ISUP). El TUP, NUP e ISUP hacen el mismo trabajo de ayudar en el establecimiento de la llamada.

c) Parte de Control y Conexión de Señalización (SCCP)

La estructura del SS7 con TUP/NUP/ISUP encima del MTP fue bastante satisfactoria para el manejo de la llamada de voz. Sin embargo, conforme pasaba el tiempo se fue dando el desarrollo de tecnología nueva y más avanzada, los requerimientos de señalización también empezaron a ser más rigurosos y demandantes.

Fue observado que solo la combinación de TUP/MTP no fue suficiente cuando las conexiones virtuales llegan a ser necesarias. El MTP garantiza la transferencia de mensajes desde cualquier "punto de señalización" en la red de señalización a cualquier otro "punto de señalización", de manera segura y confiable. Sin embargo cada mensaje, puede alcanzar el punto de señalización destino usando diferentes trayectorias. Esto

puede causar que las situaciones donde el orden de los mensajes que son recibidos, son diferentes que la secuencia original. Cuando el orden es importante, existe la necesidad de establecer una conexión virtual.

Las conexiones virtuales usan un protocolo orientado a conexión que provee números de secuencia para permitir que los mensajes sean ubicados en el correcto orden en la distancia final. Otro ejemplo acerca de que la estructura TUP/MTP es ineficiente se da cuando un mensaje de señalización tiene que ser enviado a lo largo de múltiples redes en ausencia de una llamada. El MTP es capaz de encaminar un mensaje dentro de una sola red.

El caso de establecer una llamada a lo largo de múltiples redes no es el mismo que la señalización a lo largo de la misma red. La señalización va etapa por etapa de acuerdo a la llamada. Pero en ausencia de una llamada, el MTP no puede encaminar un mensaje de señalización a lo largo de redes múltiples.

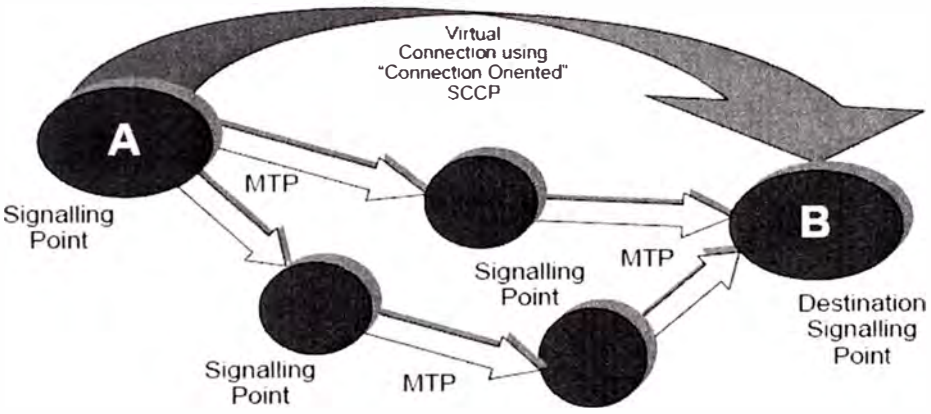


Figura 1.45: Conexiones virtuales

La solución a estos problemas fue la creación de otra capa de protocolos por encima del MTP que fue llamado Parte de control y conexión de señalización (SCCP). El SCCP se encarga de las conexiones virtuales y la señalización sin conexión. Las tareas del TUP y el SCCP son diferentes y así ellos son paralelos el uno al otro, pero ambos usan los servicios del MTP.

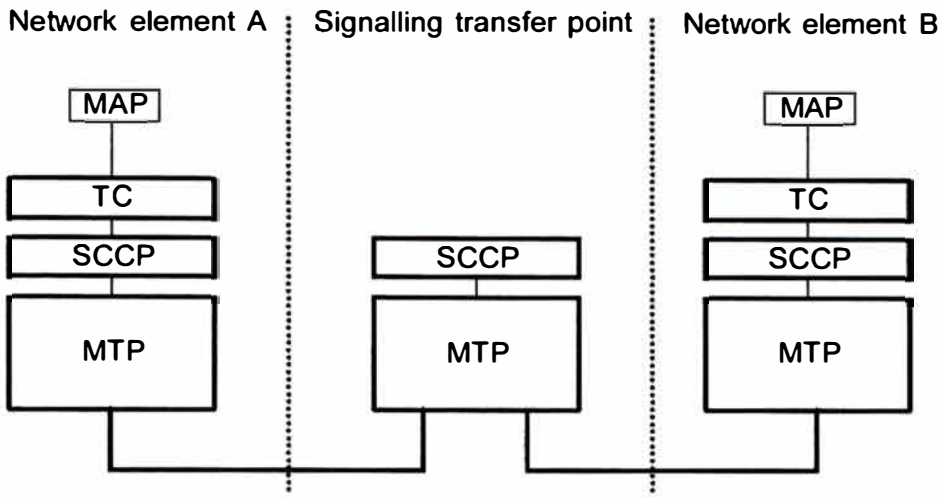


Figura 1.46: Señalización entre 2 elementos de red y un STP

1.3.4 Protocolos SS7 adicionales en redes GSM

En redes GSM, la señalización no es tan simple como en la red PSTN. Existen otros requerimientos de señalización en la red GSM debido a diferentes arquitecturas de la red que requieren una gran cantidad de señalización no relacionado a llamadas. Por ejemplo, el abonado siempre es móvil (está en movimiento), mientras que en la red PSTN el abonado siempre está en un mismo lugar. Por lo tanto, es requerido un continuo seguimiento de la estación móvil, el cual resulta en el procedimiento de Actualización de Ubicación (Location Update).

Este procedimiento es un ejemplo de señalización no relacionado a una llamada, donde el teléfono móvil y la red se están comunicando, pero la llamada no ocurre. Esto requiere mensajes estándares adicionales para satisfacer los requerimientos de señalización de la red GSM.

Estas capas de protocolos adicionales son:

Parte de aplicación del subsistema de estación base (BSSAP).

Parte de aplicación móvil (MAP).

Parte de aplicación de capacidades de transacción (TCAP).

a) Parte de Aplicación del Subsistema de Estación Base (BSSAP)

Esta capa es usada cuando una MSC se comunica con el BSC y la estación móvil. Dado que la estación móvil y la MSC tienen que comunicarse vía el BSC, debe haber una conexión virtual; por lo tanto el servicio del SCCP es también necesario.

El procedimiento de verificación de autenticación y asignación de una nueva Identidad de abonado móvil temporal (TMSI) toman lugar con los mensajes estándares del BSSAP. La comunicación entre la MSC y el BSC también usa la capa de protocolo BSSAP. Por lo tanto, el BSSAP sirve para 2 propósitos:

- Señalización MSC – BSC.
- Señalización MSC – Estación móvil.

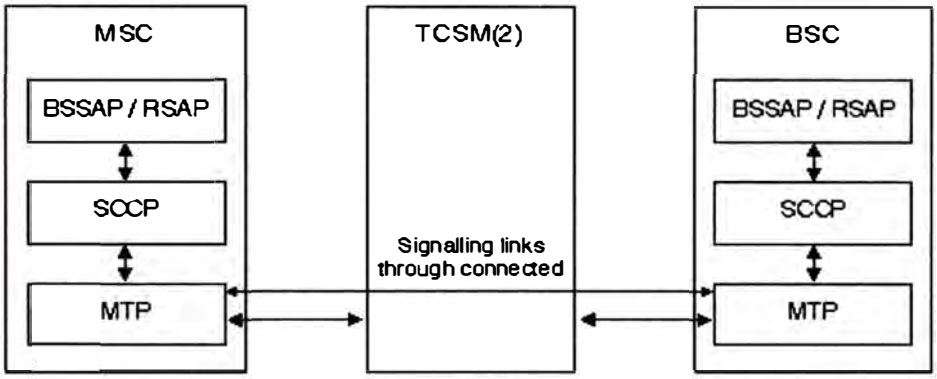


Figura 1.47: Las 3 capas de señalización CCS7/SS7 entre la MSC y el BSC

b) Parte de aplicación móvil (MAP)

El procedimiento de Actualización de ubicación (location update) no está confinado solo a la sección MSC – BSC, éste ocupa múltiples PLMNs. En caso de un location update por primera vez por un abonado con roaming internacional (él no está en su red local), el VLR tiene que obtener los datos del HLR del abonado vía el GMSC de la red local del abonado.

Mientras una llamada terminada en el móvil está siendo manejada, el número roaming de la estación móvil (MSRN) tiene que ser solicitado del HLR sin encaminar la llamada al mismo. Por lo tanto, para estos casos otra capa de protocolo fue adicionada al SS7 llamada Parte de aplicación móvil (MAP), el cual es usado para comunicación de señalización entre elementos NSS.

c) Parte de Aplicación de Capacidades de Transacción (TCAP)

En la señalización MAP, una MSC envía un mensaje a un HLR, y ese mensaje requiere un cierto resultado. El HLR retorna un mensaje, el cual puede ser el resultado final u otros mensajes también podrán seguir (o podrá no ser el último resultado). Estas invocaciones y resultados que son enviados y retornados entre múltiples elementos usando MAP necesitan alguna clase de "secretaria" para manejar las transacciones. Esta "secretaria" es llamada TCAP.

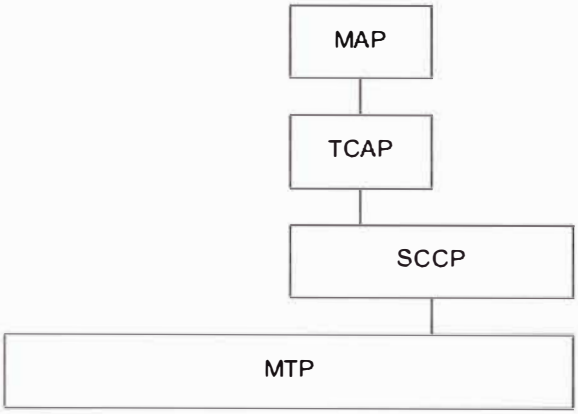


Figura 1.48: Protocolos de soporte de MAP

1.3.5 Otros protocolos de señalización en redes GSM

Como ya fue visto, los elementos de red del core GSM usan SS7 para intercambiar mensajes de señalización entre ellos.

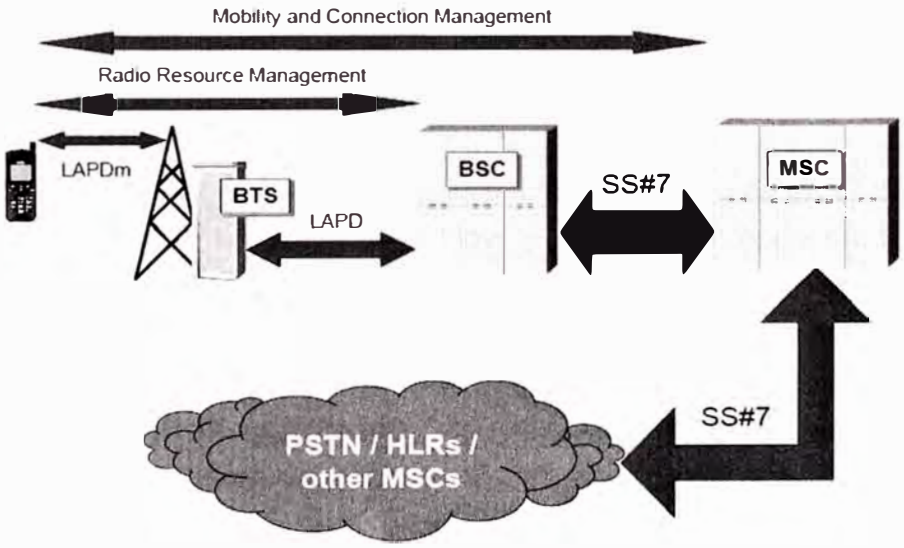


Figura 1.49: Señalización en GSM

Entre el BSC y la BTS, se utiliza un protocolo de señalización conocido como Prcedimiento de acceso al enlace en el canal D ISDN (LAPD). Este es el mismo protocolo que es usado en las redes ISDN entre el abonado y la red. Este protocolo es también usado en los intercambios de solicitudes y respuestas entre el BSC y el TRAU (Transcoder). Entre la estación móvil y la BTS, es usado el LAPD con pequeñas modificaciones que hacen frente a las características del medio de transmisión de radio.

Este protocolo es conocido como LAPDm donde "m" significa modificado. La estructura del mensaje LAPD es similar al SS7, pero no soporta capacidades de networking, por lo tanto, es usado para conexiones punto a punto.

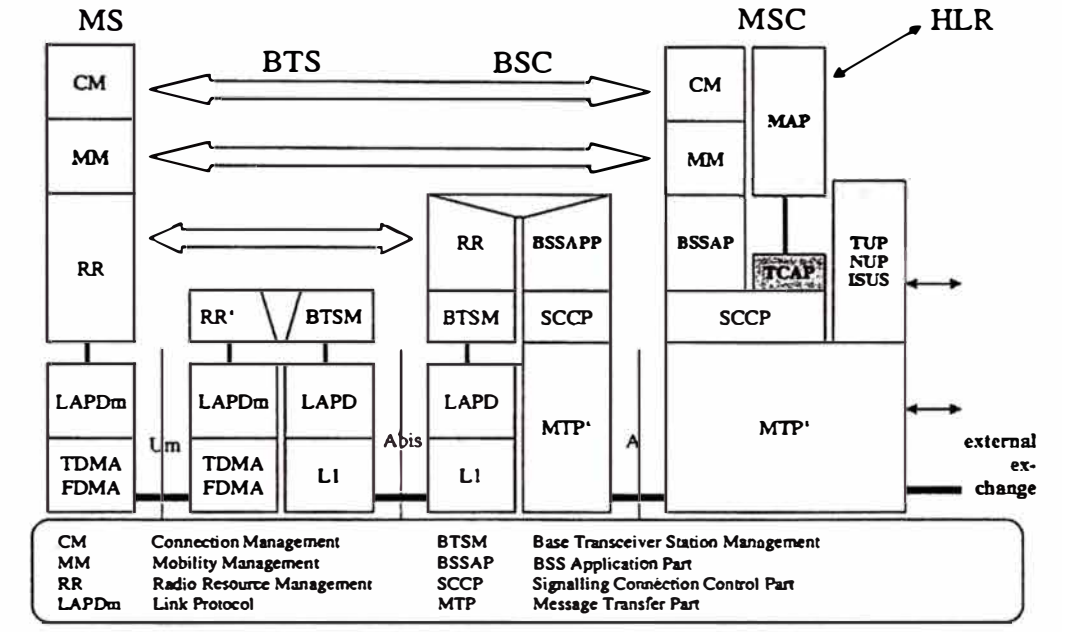


Figura 1.50: Señalización en GSM

Como puede ser visto en la figura anterior, un protocolo de señalización es requerido para negociar los recursos de radio que serán usados para la señalización dedicada y el transporte de datos de usuario. El protocolo es llamado protocolo de administración del Recurso de radio (RR), y sus mensajes son intercambiados entre la estación móvil y el BSC vía LAPDm y LAPD. El protocolo RR' en la figura anterior indica que algunas tareas de la administración del recurso de radio puede ser directamente realizado entre la estación móvil y la BTS.

La BTS determina que recursos de la interfase de radio están asignados a la estación móvil para tráfico dedicado, pero la BTS también debe ser informada. Esto es la

causa de la existencia del protocolo de Administración de BTS, BTSM (BTS Management).

¿Qué hay acerca de la Administración de movilidad (mobility management)? La administración de movilidad (MM) comprime las tareas tales como la actualización de ubicación (location update) y la autenticación. Existen mensajes que son intercambiados directamente entre la estación móvil y el MSC/VLR. Como puede ser visto, existen otros elementos de red en la transmisión de los mensajes de mobility management tales como la BTS y el BSC. Pero estos elementos de red transmiten transparentemente los mensajes de la capa de mobility management más altos. Similar al STP en el SS7, ellos toman el mensaje de señalización, y lo desvían a la siguiente entidad. La estación móvil y el MSC/VLR son entidades de los mensajes de mobility management.

Lo mismo se repite para los mensajes de Administración de conexión (CxM). La administración de conexión incluye mensajes de establecimiento de llamada, mensajes de alerta, etc., es decir los mensajes necesarios para el control de la llamada. También el Servicio de mensajes cortos (SMS) y los servicios suplementarios son manejados con la ayuda de la administración de conexión.

1.4 Arquitectura GPRS

1.4.1 Introducción

Los sistemas GSM se desarrollan progresivamente hacia el Sistema Universal de Telecomunicaciones Móviles (UMTS) introduciendo nuevas técnicas que proporcionan anchos de banda más amplios. Estas etapas son:

Circuito conmutado de datos de alta velocidad (HSCSD).
Servicio General de Paquetes por Radio (GPRS).
Tasa de Datos Mejorada para la Evolución GSM (EDGE).

Las redes GSM existentes están basadas en técnicas de circuitos conmutados. Para los servicios de datos que están basados en el protocolo IP tales como el e-mail y el web browsing, la red GSM de circuitos conmutados es ineficiente.

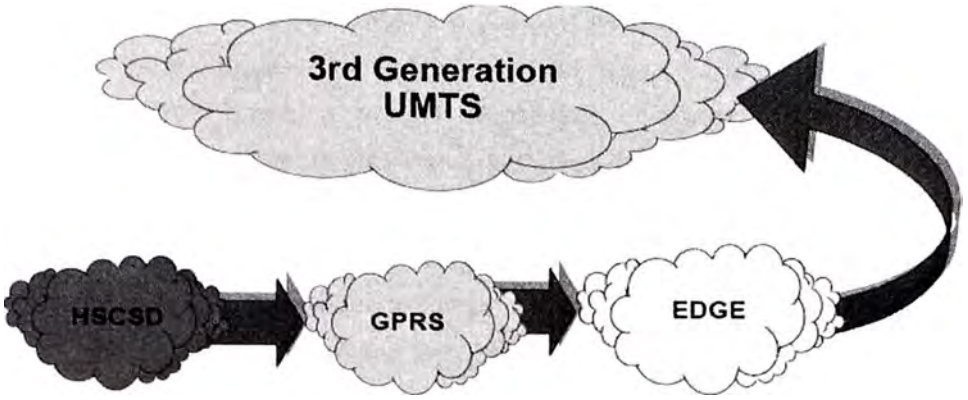


Figura 1.51: La evolución con GSM

El release 97 del GSM ha introducido el Servicio General de Paquetes por Radio (GPRS) el cual mantiene las tecnologías de acceso BSS de la red GSM pero proporciona servicios de datos de paquetes conmutados a la estación móvil.

a) Conmutación de Circuitos y Paquetes

Conexiones de circuitos conmutados:

El GSM estándar utiliza conexiones de circuitos conmutados. Cada vez que una conexión es requerida entre 2 puntos, un enlace es establecido entre ellos, y los recursos de red son reservados y dedicados al uso de un abonado para la duración de la llamada. Las conexiones de circuitos conmutados tienen relativamente, bajo retardo en la red y han sido utilizados tradicionalmente en redes fijas y móviles para voz y datos.

Conexiones de paquetes conmutados:

Las redes de datos, tales como Internet, Frame Relay y X25, utilizan conexiones de paquetes conmutados. Con la conmutación de paquetes, los datos del usuario son organizados en paquetes (datagramas), cada paquete tiene un identificador o dirección que es usado por los elementos de conmutación en la red para pasar los paquetes a su destino propuesto.

Por este medio, cada paquete es encaminado individualmente. GPRS proporciona las técnicas de paquetes conmutados en las redes GSM.

Una conexión de paquetes conmutados puede ser orientada o no orientada a conexión:

- **Servicio de red orientado a conexión (CONS):** Un servicio es orientado a conexión cuando la señalización toma lugar para establecer una conexión punto a punto, mantenerla y liberarla. La información de señalización es usada por los puntos de transmisión para acordar en como la transmisión tiene que llevarse a cabo. Por ejemplo, el protocolo de transporte TCP (Transfer Control Protocol) ofrece servicio de red orientado a conexión a los protocolos de capas más altas, tales como http, SMTP. TCP proporciona la conexión confiable y bien organizada.

- **Servicio de red no orientado a conexión (CLNS):** En un servicio no orientado a conexión cada paquete es transmitido independientemente. No existe acuerdo mutuo entre los puntos de transmisión en como organizar la transferencia de datos del usuario. IP es el mejor ejemplo conocido de un servicio de red no orientado a conexión.

A continuación se muestra la comparación entre las soluciones de red de circuitos conmutados y la red de paquetes conmutados:

Circuito conmutado: Circuitos físicos PCM-TSL (CONS)

- Establecimiento de conexión punto a punto (end to end)
- Los recursos dedicados (PCM - TSL) para un usuario son reservados durante el establecimiento de llamada.
- Solo el 30% - 40% de los recursos son efectivamente usados para transferencia de voz.
- La voz es transferida en tiempo real.
- La voz no acepta retardos.
- Los errores en la transmisión no son críticos para la voz.
- El charging es basado en tiempo.

Paquete conmutado:

Circuitos virtuales (CONS) – Circuitos no virtuales (CLNS)

- Los recursos son compartidos entre diferentes sesiones de usuario, es decir no es dedicado.
- Los recursos son solicitados en demanda, es decir es más eficiente.
- Los paquetes no son enviados en tiempo real, por lo tanto existe retardo y buffering.

- Posible corrección y detección de error.
- El charging está basado en el volumen, es decir en el número de paquetes.

1.4.2 Descripción y arquitectura GPRS

GPRS proporciona el acceso de los usuarios móviles a los servicios de Protocolo de aplicación inalámbrica (WAP) de valor agregado y a las redes externas de paquetes conmutados.

La parte BSS de la red GSM proporciona la interfase de radio y la red core de GPRS maneja la movilidad y el acceso a los servicios y las redes externas de paquetes.

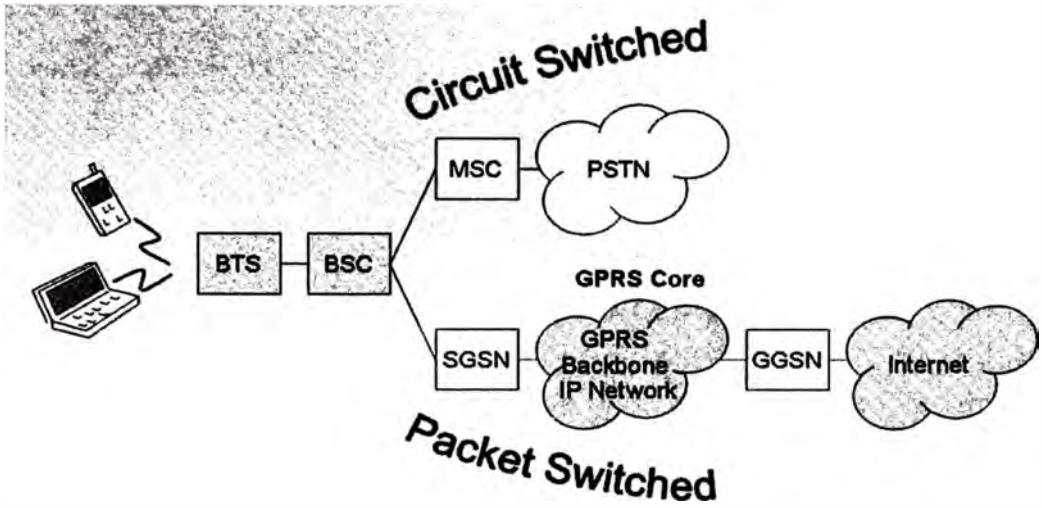


Figura 1.52: Descripción – Red GPRS

La red GPRS actúa en paralelo con la red GSM, proporcionando conexiones de paquetes conmutados a las redes externas. Los requerimientos de una red GPRS son:

- La red GPRS debe usar la infraestructura GSM existente
- Dado que un usuario GPRS puede tener una o más sesiones de datos, GPRS debe ser capaz de soportar una o más conexiones de paquetes conmutados
- Para soportar la carga de varios usuarios GPRS, éste debe ser capaz de soportar diferentes suscripciones de calidad de servicio (QoS) del usuario
- La arquitectura de la red GPRS tiene que ser compatible con los futuros sistemas de comunicaciones móviles de 3ra y 4ta generación
- Debe ser capaz de soportar conexiones de datos punto a punto y punto a multipunto
- Debe proporcionar accesos seguros a redes externas

La red GPRS debe proporcionar toda la funcionalidad de una red GSM hacia las redes conmutadas de paquetes.

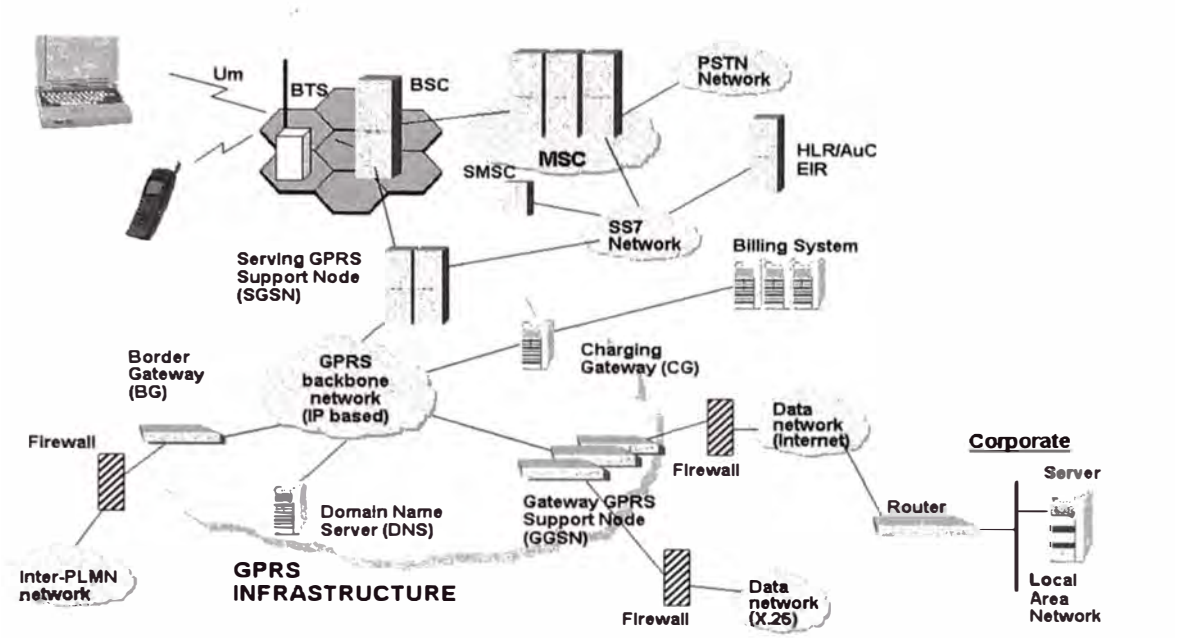


Figura 1.53: Arquitectura de una red GPRS

La red GPRS trae nuevos elementos de red a la red GSM. Los más importantes son el Nodo de soporte de Servicio GPRS (SGSN) y el Nodo de soporte de gateway GPRS (GGSN). El Gateway de borde (BG) es necesario para razones de seguridad y está situado en la conexión a la red backbone inter-PLMN.

El SGSN 2G de NOKIA es un elemento esencial requerido para implementar el GPRS en una red GSM. Junto con el GGSN, el SGSN es necesario para los servicios basados en conexiones de paquetes conmutados. GPRS trae el acceso rápido de datos combinado con el beneficio de estar continuamente conectado. La arquitectura distribuida del SGSN 2G de NOKIA está implementada con un sistema multiprocesador redundante y de alta capacidad: La plataforma DX 200.

El SGSN 3G de NOKIA soporta comunicación de paquetes hacia una red de accesos. Es responsable de la administración de movilidad (Mobility Management) que está relacionada a la actualizaciones de áreas de encaminamiento (routing area update), packet paging y mecanismos de control de seguridad relacionado a comunicación de paquetes. Este elemento de red actúa como un enlace entre la Red de acceso de radio 3G (3G RAN) y la red core de paquetes y realiza funciones de control y manejo de tráfico de paquetes conmutados en un sistema 3G.

El GGSN de NOKIA es el elemento de red dentro de una infraestructura GPRS que proporciona interacción con las redes de datos externas, habilitando a los abonados GPRS el acceso a varios servicios de datos. El GGSN conecta las redes GPRS y 3G a la Internet, Proveedores de servicio de Internet (ISPs) e intranets corporativas.

1.5 Tráfico en GPRS

La Administración de movilidad (Mobility Management) y la Administración de conexión (Connection Management) son pre-requisitos en GSM para ofrecer servicios móviles. Lo mismo sucede en GPRS. Es por eso que la administración de movilidad es llamada Administración de movilidad GPRS (GMM) y la administración de conexión es llamada Administración de sesión (SM). GMM y SM forman 2 categorías de procedimientos de administración de tráfico. Los mensajes que son enviados entre varios componentes de la red GPRS son colectivamente conocidos como Tráfico GPRS.

1.5.1 Información del abonado

Cuando los mensajes GPRS son enviados, existe la necesidad de dar la información del abonado GPRS y otros parámetros dentro del mensaje. La información acerca de un usuario GPRS en los diferentes elementos de red cae dentro de 4 categorías:

Identidad: Se hace a través del IMSI, TMSI, P-TMSI, TLLI y la dirección IP.

Ubicación: Se realiza a través de la Ubicación de área, área de enrutamiento, SGSN y MSC.

Servicios: Servicios a lo cual el abonado está permitido a acceder.

Autenticación de datos: Se realiza a través de técnicas de encriptación y algoritmos de autenticación para la transferencia de datos entre el SGSN y la estación móvil.

1.5.2 Administración de Movilidad GPRS (GMM)

Los procedimientos acerca de la movilidad del usuario son llamados Administración de movilidad GPRS (GMM). Los procedimientos GMM son similares a la administración de movilidad para los usuarios de redes conmutadas de circuitos. Un ejemplo de un procedimiento GMM es el GPRS Attach.

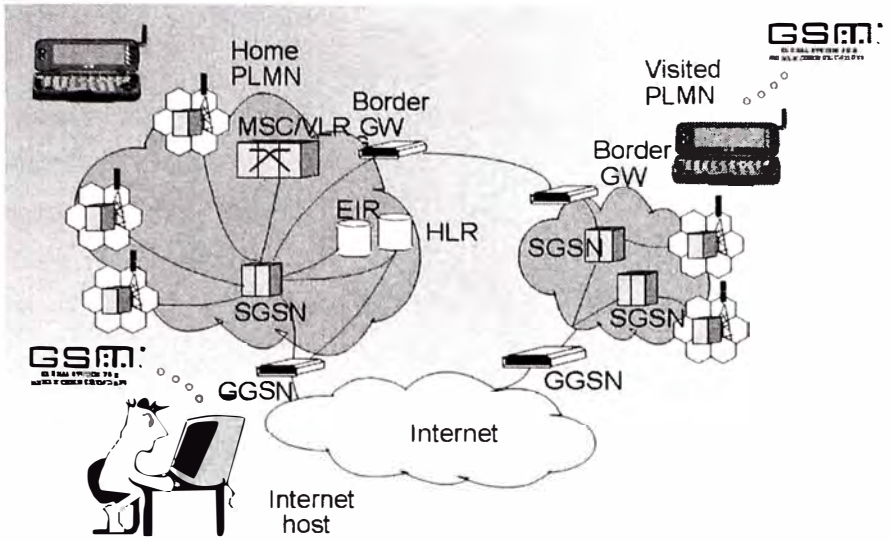


Figura 1.54: Componentes de una red GPRS

Cuando un terminal GPRS es encendido, éste envía un mensaje 'attach' a la red. El SGSN autentica al usuario antes de conectar el terminal a la red GPRS. Una vez que un abonado es conectado a la red, la conexión lógica es establecida entre la estación móvil, el SGSN y el HLR.

El área de cobertura está dividida en celdas, y cada celda o grupo de celdas son servidos por una o más estaciones base. Cuando un abonado móvil se mueve de una celda a otra, el handover toma lugar. En GSM, se usa el concepto de Área de ubicación (LA) para ubicar (page) a los abonados GSM, mientras que GPRS tiene un nuevo concepto de ubicación conocido como Área de enrutamiento (RA).

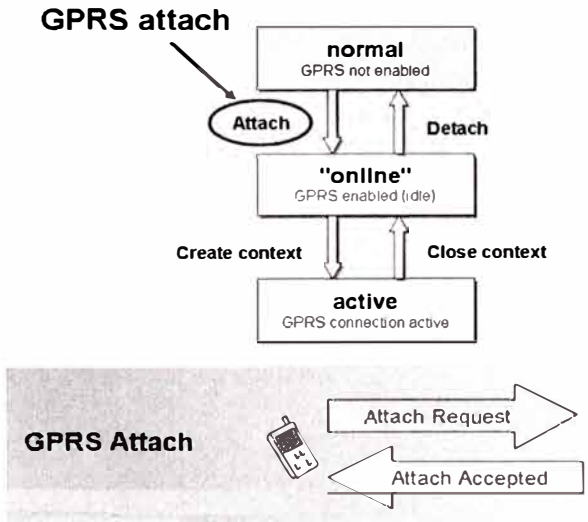


Figura 1.55: El GPRS attach

El attach, habilita el GPRS, el cual corresponde al login en la red. El GPRS attach es hecho tan pronto el usuario enciende su teléfono.

La función del GPRS Attach es similar al IMSI attach:

- Autentica el móvil.
- Genera las claves de encriptación.
- Habilita la encriptación.
- Asigna la identidad temporal (TLLI).
- Copia el perfil del abonado desde el HLR al SGSN.

Después del GPRS attach:

- La ubicación del móvil es rastreada.
- La comunicación entre la estación móvil y el SGSN es segura.
- La información de charging es recolectada.
- El SGSN conoce lo que el abonado puede hacer en la red.
- El HLR conoce la ubicación de la estación móvil en relación al SGSN.

1.5.3 Administración de Sesión (SM)

La administración de sesión se refiere a un conjunto de procedimientos para la activación, desactivación y modificación de una sesión de datos entre la estación móvil y una red externa. Para establecer sesiones de datos, el sistema GPRS proporciona un grupo de funciones para asociar una estación móvil con una dirección IP y liberar ésta asociación. Esas funciones son llamadas Contextos PDP (PDP context). El contexto PDP resultante puede ser modificado. La estación móvil puede usar el contexto PDP solo cuando está en estado ready o standby.

La estación móvil puede usar varias clases de direcciones IP. El operador de red puede asignar una dirección IP estática a una estación móvil permanentemente. Otra opción para los operadores es asignar direcciones IP dinámicas a una estación móvil durante la activación del contexto PDP. La conexión es establecida entre la estación móvil y el GGSN a través del SGSN.

El contexto PDP permite la conexión, es decir el protocolo IP es activado. Este es creado tan pronto el servicio GPRS es iniciado.

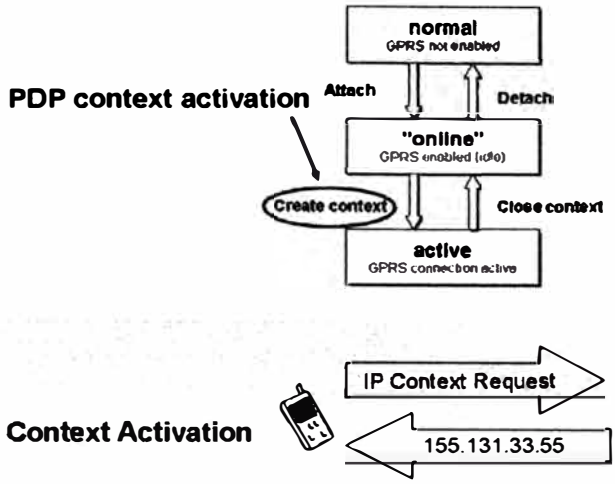


Figura 1.56: Activación del contexto PDP

Cuando el GPRS activa el contexto PDP:

- El usuario pueda activar cada una de las direcciones PDP suscritas, separadamente.
- El usuario puede tener varios contextos PDP.
- La transmisión de datos no es posible antes que la dirección PDP es activada.
- El HLR no está involucrado en la activación del contexto PDP.
- La red puede solicitar la activación del contexto PDP.

Cuando el contexto PDP es activado:

- El SGSN tiene un túnel lógico bidireccional entre la estación móvil y el GGSN.
- El GGSN tiene una dirección PDP activada.
- El GGSN ubica a la estación móvil en relación al SGSN.
- La estación móvil ahora puede transferir datos usando su dirección PDP.

1.5.4 Transferencia de datos en GPRS

La transferencia de datos es siempre a través del GGSN, incluso si la comunicación es móvil a móvil. El GGSN conoce cual SGSN está dando el servicio al móvil.

En la transferencia de datos, el SGSN realiza las siguientes funciones:

- No interpreta los datos del usuario, pero puede realizar la compresión de la cabecera TCP/IP.
- No interpreta las direcciones origen o destino.
- Envía todos los paquetes al GGSN que maneja el contexto PDP.

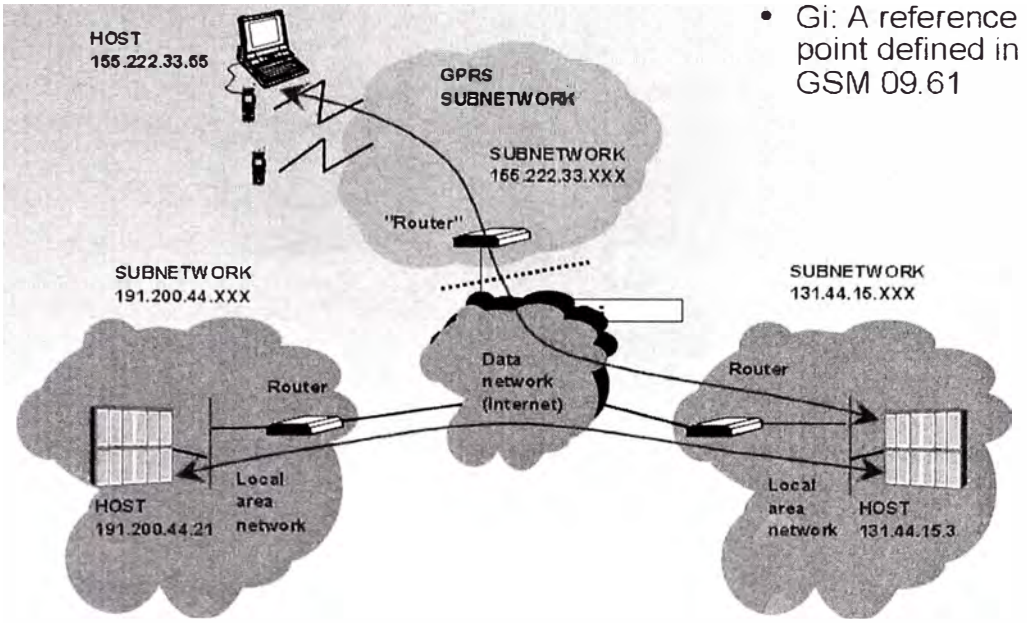


Figura 1.57: Conexiones externas de red

Por otro lado, el GGSN realiza las siguientes funciones:

Realiza opciones de filtrado.

Decide donde y como encaminar los paquetes.

Todos los datos de usuario están encapsulados o encriptados.

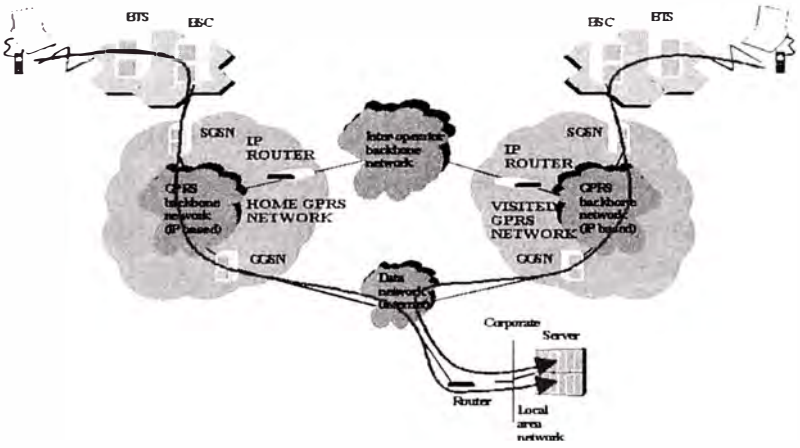


Figura 1.58: Transferencia de datos: La conexión de datos se origina en el móvil (MO data)

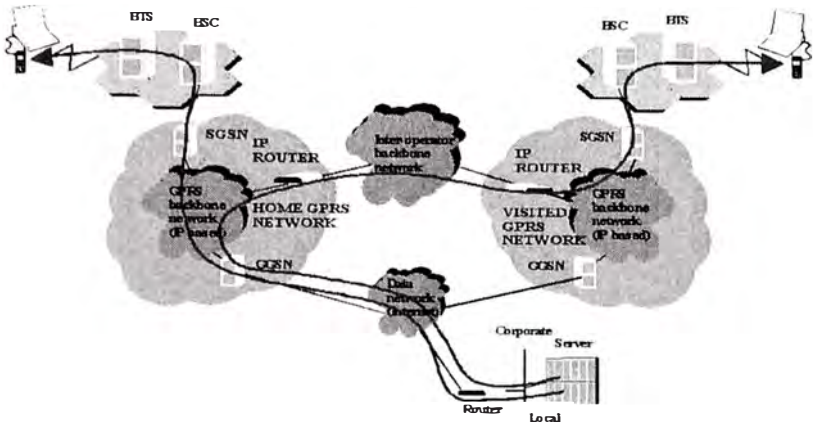


Figura 1.59: Transferencia de datos: La conexión de datos termina en el móvil (MT data)

1.5.5 Charging (Facturación)

El SGSN y GGSN que están sirviendo a la estación móvil recolectan la información de charging acerca del uso del servicio GPRS. La información que el operador utiliza para generar la facturación de un abonado es específica. Cada operador GPRS procesa su propia información de facturación:

El SGSN genera información de charging sobre el uso de la red de radio.

El GGSN genera información de charging sobre el uso de la red externa de datos.

El SGSN y GGSN generan información de charging sobre el uso de los recursos de la red GPRS.

La información de charging (CDR) es generada por el SGSN y GGSN y luego son entregadas al Gateway de facturación (CG) usando una transferencia en tiempo real: Protocolo GTP mejorado (Enhanced GTP). La interfase Ga es usada entre el SGSN y el CG. Desde el CG, la información es transferida al Centro de facturación (BC).

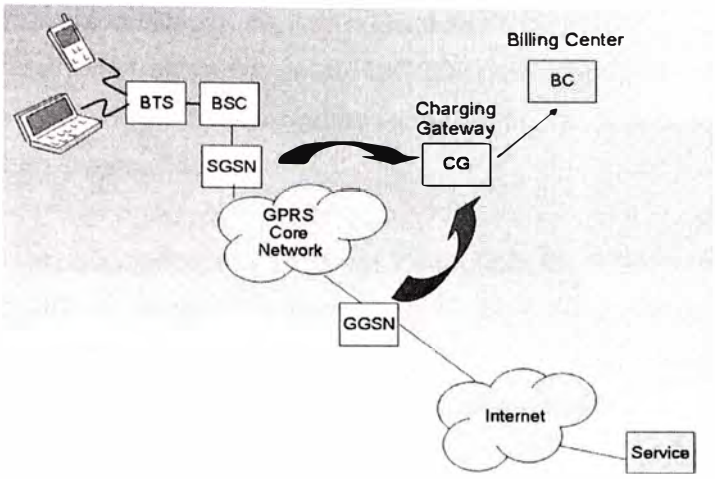


Figura 1.60: Charging. Estadísticas recolectadas

1.6 Evolución del GSM a las redes de tercera generación

1.6.1 Introducción

GSM ha sido diseñado, por encima de todo, para comunicación de voz (speech). Aunque el estándar ofrece servicios de datos, sus posibilidades son limitadas a una tasa de datos de 9.6kbps. Para reunir la creciente demanda del incremento complejo de aplicaciones de datos, es decir la multimedia o el Internet, los datos de alta velocidad son necesarios. Por lo tanto, la capacidad del sistema está siendo constantemente mejorada.

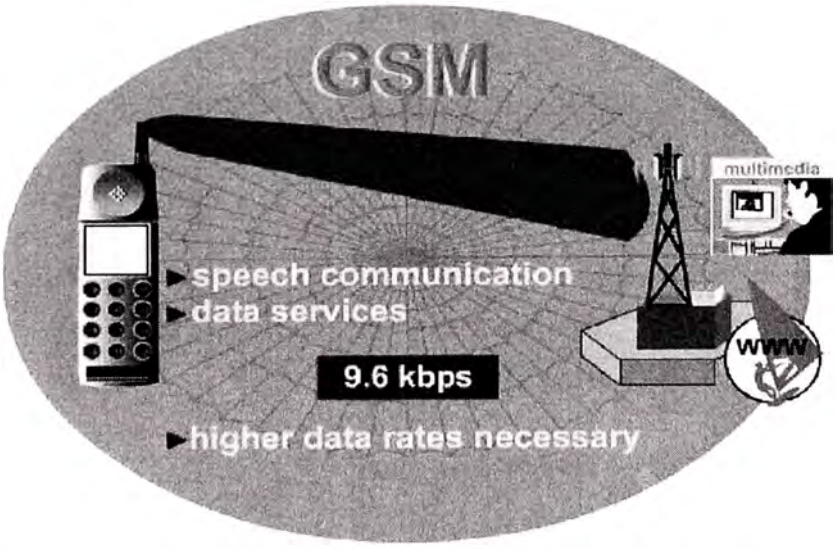


Figura 1.61: GSM

1.6.2 Circuito Conmutado de Datos de Alta Velocidad (HSCSD)

Una extensión del GSM estándar es el HSCSD. Esta innovación da a la tasa de bits un enorme valor. El HSCSD es circuito conmutado y optimiza las tasas de transmisión existentes en 2 aspectos:

Un nuevo método de codificación de canal, disponible en GSM fase 2+ en un solo circuito conmutado de datos, que incrementa la tasa de datos desde 9.6kbps a 14.4kbps.

El grupo de hasta 4 intervalos de tiempo (TSL) puede incrementar la tasa de datos del usuario a 57.6kbps.

Esto permite por ejemplo, la transferencia rápida de correos electrónicos y archivos así como una rápida y barata descarga de datos desde la Internet. Como la mayoría de servicios usados requieren tasas de datos más altas en el enlace de bajada (downlink) que en el enlace de subida (uplink), el HSCSD muestra una implementación asimétrica, por ejemplo, 3 intervalos de tiempo en el downlink y 1 en el uplink. Esto también facilita el diseño de la estación móvil y evita problemas de capacidad de la batería.

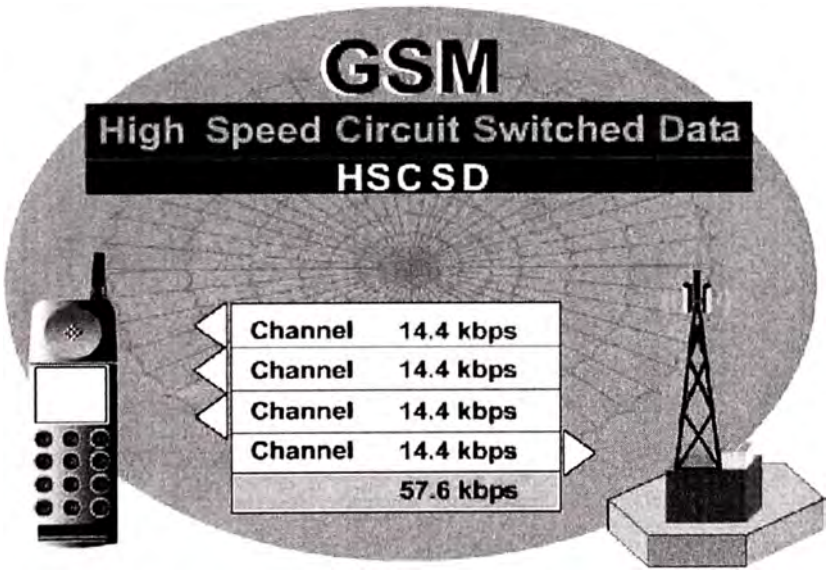


Figura 1.62: HSCSD

1.6.3 Servicio General de Paquetes por Radio (GPRS)

En contraste al HSCSD, el GPRS es paquete conmutado en vez de circuito conmutado. Los recursos de la red de radio son solo usados si los datos están siendo transmitidos.

Así, la facturación no está basada en la duración de la llamada, sino en la cantidad de datos transmitidos. Adicionalmente, el tipo de servicio de datos puede ser cargado, por ejemplo web browsing o acceso WAP.

Agrupando hasta 8 canales, una tasa de datos puede ser de hasta 171.2kbps, con hasta 8 abonados por canal. A más usuarios que transmiten datos dentro de una celda, la disponibilidad de la tasa de datos para cada usuario será reducida. GPRS requiere algunas modificaciones para la infraestructura GSM existente.

El HSCSD y el GPRS, juntos, son el siguiente paso hacia la multimedia móvil.

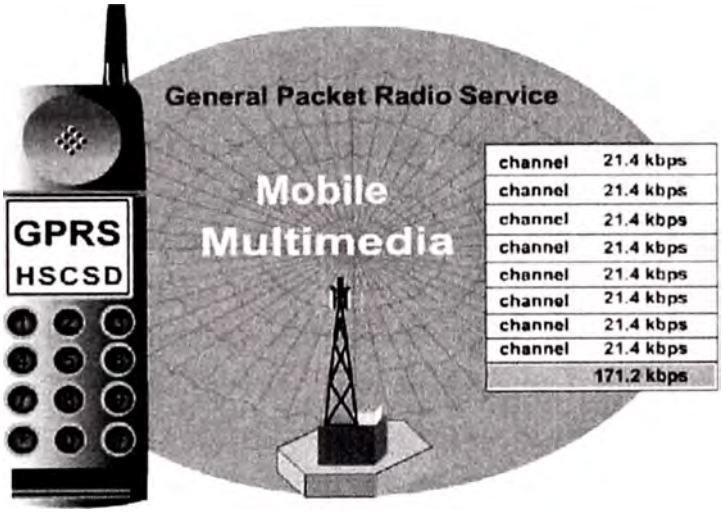


Figura 1.63: GPRS

1.6.4 Tasa de Datos Mejorada para la Evolución GSM (EDGE)

EDGE es una tecnología que se concentra en la interfase air entre el móvil y la estación base. Está basado en un nuevo proceso de modulación, Modulación por desplazamiento de fase de 8 estados (8 Phase Shift Keying) o 8-PSK. Con ésta modulación, EDGE alcanza 3 veces la tasa de datos del HSCSD y GPRS en la interfase air. Además, con EDGE, el abonado puede usar los 8 intervalos de tiempo en la interfase air. A diferencia del GSM, la unidad de datos digital en la interfase air, un símbolo, no es solo un bit, sino 3 bits.

Esta tecnología permite tasas de datos de casi 474kbps por usuario. Por otro lado, EDGE es muy sensitivo al error de bit y requiere de cuidado en la planificación y un número adecuado de estaciones bases.

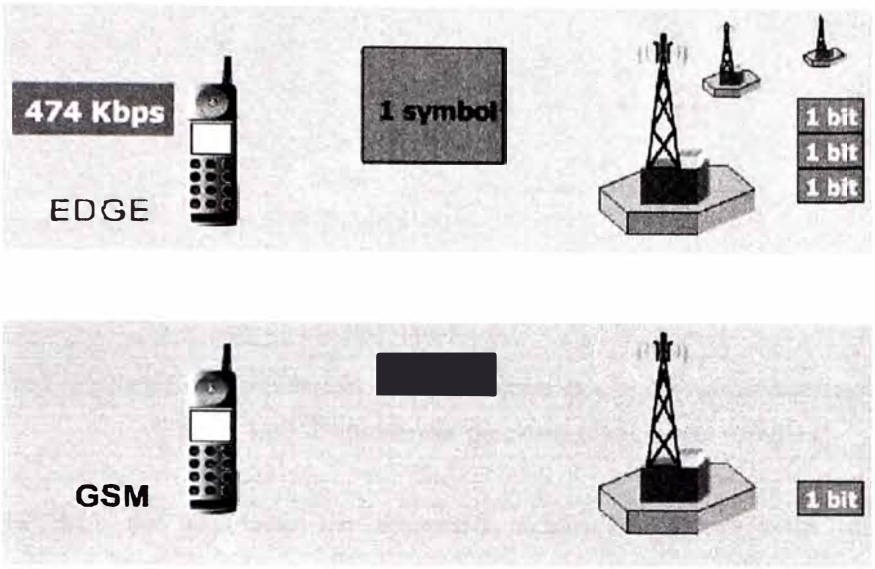


Figura 1.64: EDGE

1.6.5 Sistema Universal de Telecomunicaciones Móviles (UMTS)

UMTS representa la tercera generación de las comunicaciones móviles. Este alcanza una tasa de hasta 2Mbps si el móvil es estático y otro usuario no está transfiriendo datos. En situaciones reales puede alcanzar un máximo de 144 o 384 kbps.

La introducción de UMTS no significa que GSM sea innecesario. Los servicios simples como la voz serán tratados por GSM en el futuro, mientras que la alta tasa de datos de servicios multimedia y aplicaciones móviles serán manejadas por UMTS.

UMTS principalmente afecta la interfase air, donde un método de transmisión de banda ancha alcanza altas velocidades. Esto requiere cambios considerables en la arquitectura de red. Así, especialmente en el comienzo, una cooperación cercana con la estructura de red GSM existente es necesaria para garantizar que los servicios serán proveídos de manera amplia.

El Sistema universal de telecomunicaciones móviles (UMTS) es a GSM como el Acceso múltiple por división de códigos de banda ancha (WCDMA) es al FDMA/TDMA en la interfase air.

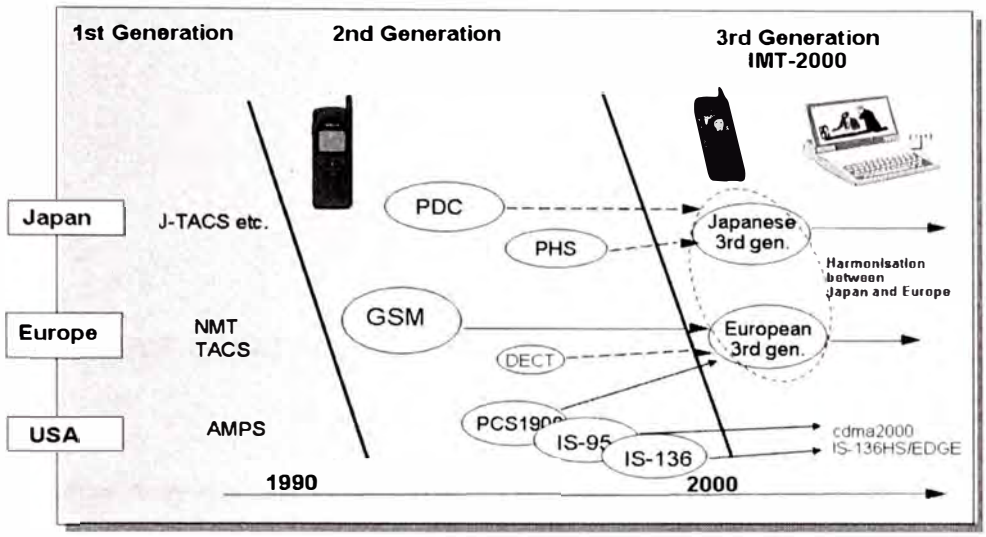


Figura 1.65: Estándares de comunicaciones móviles

El WCDMA es sinónimo de espectro expandido y presenta las siguientes características:

- Resistencia a la interferencia de señal desde múltiples puntos de transmisión (interferencia multipath).
- Permite el acceso al canal de comunicación común (acceso múltiple).
- Resistencia a la interferencia o congestión.
- Manejo flexible de tasa de datos variables.

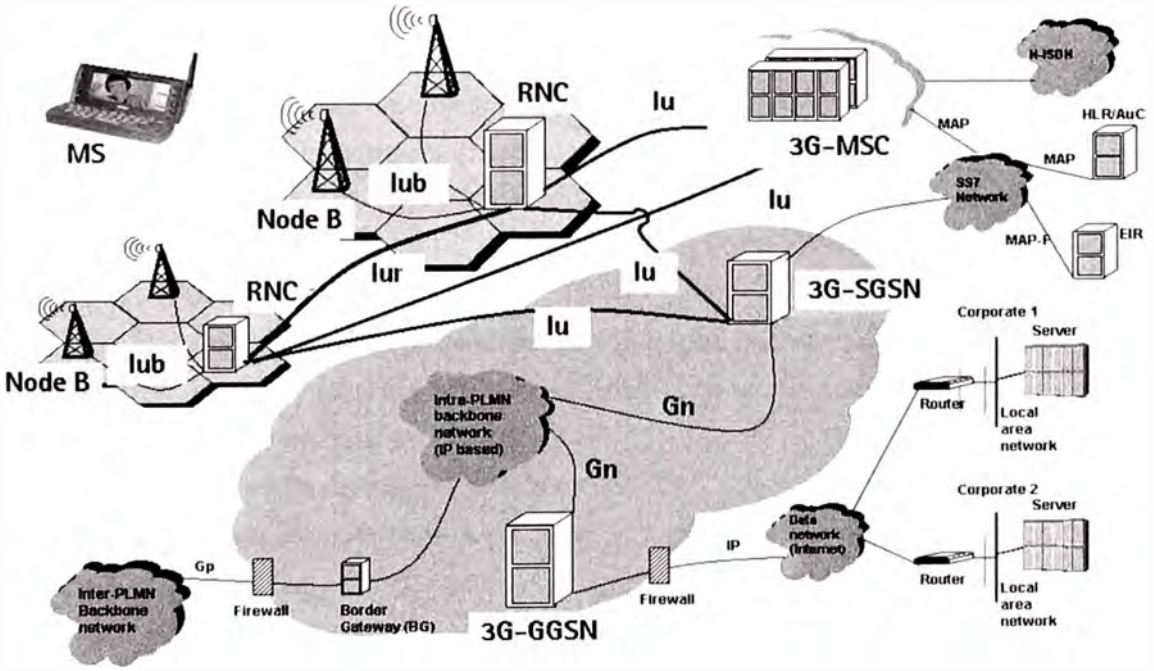


Figura 1.66: Arquitectura de la red UMTS

CAPITULO II

DESCRIPCIÓN DEL SISTEMA DE ADMINISTRACIÓN DE RED

2.1 Principios de diseño

El sistema de administración de red propuesto, presenta un marco de trabajo (framework) de administración de servicio y red modular que ayuda a los operadores a manejar sus redes en un entorno de soporte multitecnológico, multiservicio y multiproveedor.

El framework consiste de componentes del sistema y una capa de mediación y adaptación unificada (UMA). La UMA actúa como una capa de aplicación común sobre interfases a varios elementos de red y diferentes tecnologías. El sistema de administración de red de NOKIA es llamado NetAct OSS, el cual presenta los siguientes aspectos claves:

Modularidad:

Módulos de procesos plug-in.

No muestra una complejidad de red.

Permite una fácil interoperabilidad con otros sistemas.

Los componentes del sistema tienen sus propias actualizaciones.

Escalabilidad:

Nuevas tecnologías pueden ser desplegadas con el mismo sistema.

El número de clusters, servidores, hosts, puede ser adicionado o reducido.

Servidores en clusters HP-UX.

Servidores de aplicación Windows (WAS).

Servidores de aplicación Unix (UAS).

Sistema Abierto:

- Fácil adaptabilidad e integración con otros sistemas.
- Flexibilidad para desarrollar y adicionar nuevas aplicaciones.
- Integración de productos de terceros (HP, Cisco, EMC2, etc.).

Alta disponibilidad:

- Componentes redundantes (discos, LAN, fuentes de alimentación, etc.).
- Clusters HP-UX (MC/Service Guard).

Modelo de Autenticación:

- Servidores HP-UX: Servicio de información de red (NIS).
- Windows 2000 servers: Servicio Active Directory + Protocolo de Acceso a Directorios Livianos (LDAP).

Almacenamiento:

- Concepto de Red de almacenamiento (SAN).
- Arreglo de discos de acuerdo a la red de almacenamiento.

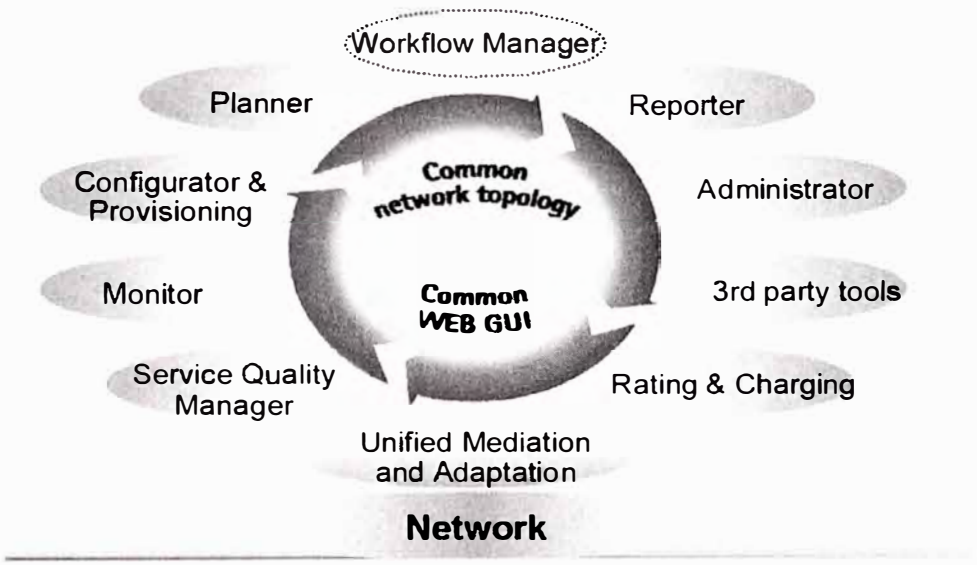


Figura 2.1: Framework del sistema NOKIA NetAct OSS

Cada sistema contiene un número definido de servidores HP-UX (UNIX de Hewlett Packard) en configuración predefinida. Como tal, el sistema es capaz de manejar un cierto número de usuarios y elementos de red. Los servidores pueden ser repotenciados adicionando CPUs y memoria RAM.

Si uno de los servidores dentro del cluster tiene que proveer capacidad adicional, otro servidor de cluster debe ser integrado al sistema, dado que el servidor puede manejar tráfico de red así como la carga causada por los usuarios al mismo tiempo. Naturalmente, este paso está basado en la suposición (la razón más probable) de conectar más usuarios al sistema ante un crecimiento de red.

2.2 Descripción de la plataforma

2.2.1 Arquitectura general

La arquitectura general del sistema de administración de red comprende diferentes componentes de sistema:

a) Cluster global (GC)

Es un cluster que ofrece una vista general de la red completa, cubriendo todas las áreas y tecnologías de red. El cluster global es necesario para aplicaciones que realizan, por ejemplo, configuraciones amplias y operaciones de monitoreo de red.

El cluster global de un sistema de administración de red comprende módulos de monitoreo, reportes, administración, calidad de servicio, planificación y charging.

b) Cluster Regional (RC)

Es un cluster que ofrece una vista a un área particular o tecnología de red. El cluster regional contiene el sistema de soporte de operación para una región.

El cluster regional de un sistema de administración de red comprende módulos de monitoreo, reportes, administración, configuración y aprovisionamiento, planificación y calidad de servicio.

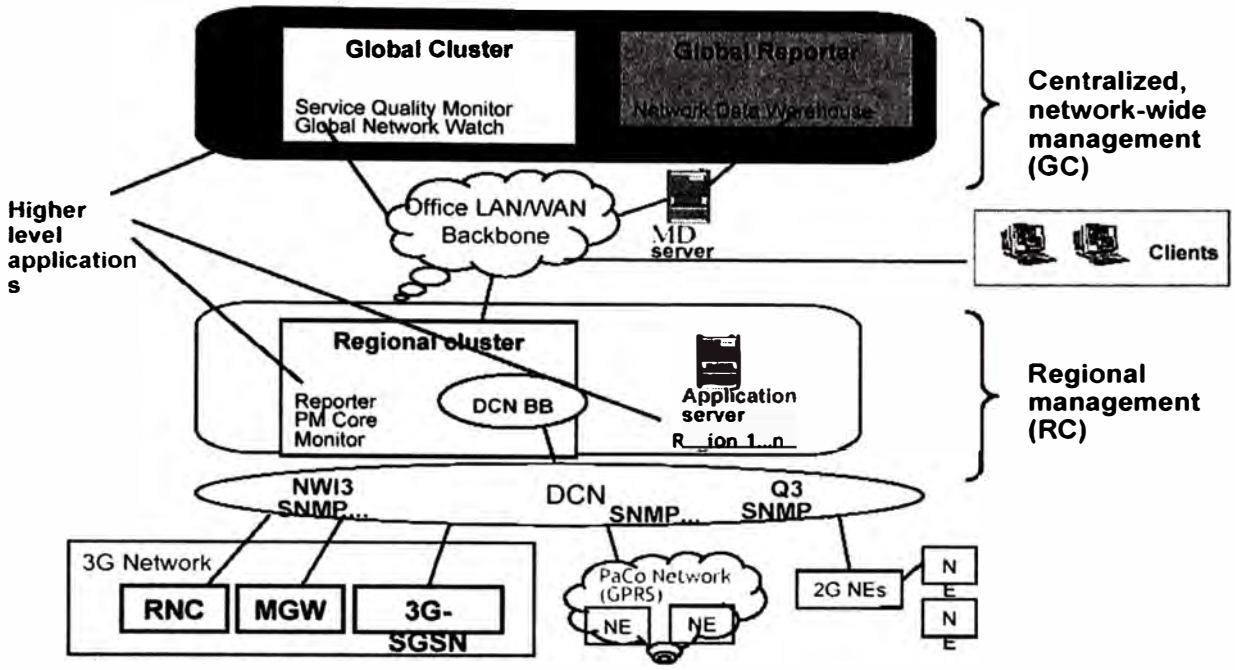


Figura 2.2: Arquitectura general del sistema de administración de red de NOKIA

2.2.2 Vista general de la red

La descripción general de la red comprende la conexión del sistema de administración NetAct OSS de NOKIA con los diferentes tipos de elementos de red y los sitios de operación remota.

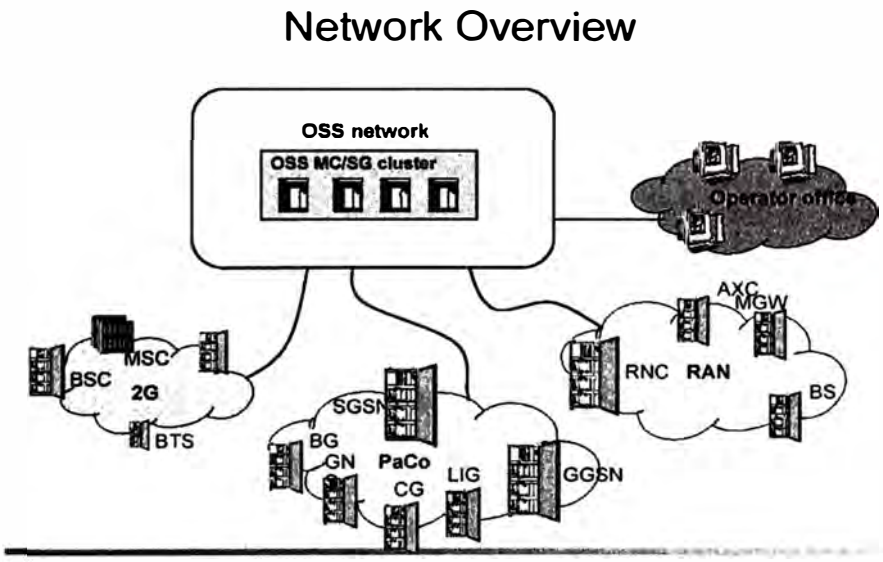


Figura 2.3: Vista general de la red del sistema de administración de red

Red de Acceso de Radio (RAN: Radio Access Network)

AXC: Conexión cruzada ATM (dentro de una estación base).

BS: Estación base.

RNC: Controlador de la red de radio.

MGW: Gateway multimedia (previo al módulo ATM).

Red de paquetes (PaCo: Packet Core)

BG: Gateway de borde.

CG: Gateway de facturación.

GNS: Servidor de nombres de GPRS.

GGSN: Nodo de soporte del gateway GPRS.

SGSN: Nodo de soporte del servicio GPRS.

Red GSM – 2G

MGW: Gateway multimedia (entre el MSC y RNC).

BTS: Estación transmisor-receptor base.

BSC: Controlador de estación base.

MSC: Central de Conmutación de Servicios Móviles.

2.2.3 Mediación y Adaptación Unificada (UMA)

a) Concepto general de UMA

La mediación y adaptación unificada es la capa de software, la cual se encarga de la recolección de datos (como alarmas y mediciones) desde la red y la descarga de datos (como los parámetros de la red de radio) a ésta capa. La UMA proporciona una vista amplia de red desde las capa más altas del sistema.

La adaptación y mediación unificada se conecta a la red para administrar y proporcionar la recolección de datos para los niveles más altos del sistema y así realizar una amplia administración de red.

La UMA interactúa con otras áreas funcionales a través de un conjunto de Puntos referencia de integración bien definidos (IRPs: Integration Reference Points). La UMA es una entidad lógica.

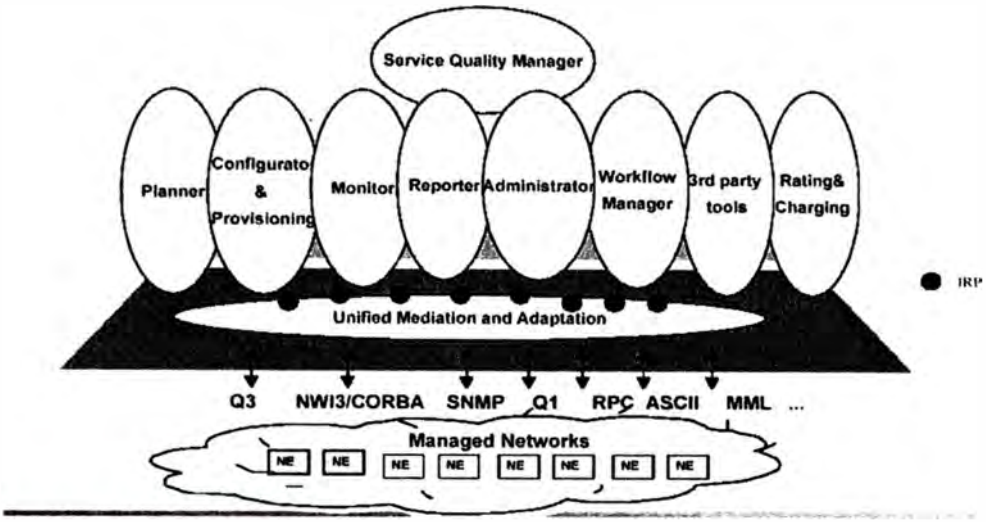


Figura 2.4: Concepto general de UMA

Las ventajas que se obtienen de la UMA son:

- Administración independiente de la tecnología.
- Las aplicaciones de usuarios están separadas de la adaptación tecnológica.
- Rápida adaptación a nuevas tecnologías.
- La complejidad de red es oculta.
- Se proporciona todas las funcionalidades de administración de los elementos de red.
- Soporte de la administración unificada de múltiples tecnologías.

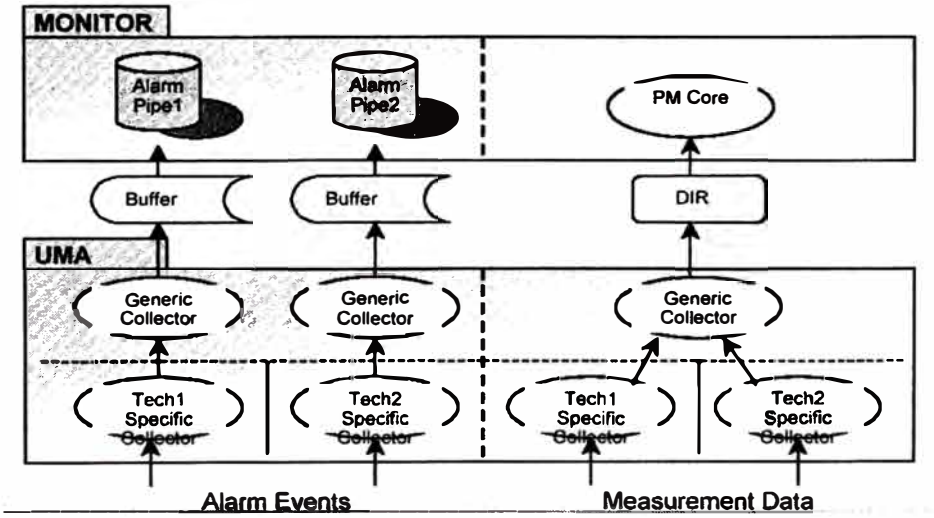


Figura 2.5: Ejemplo de UMA

En el ejemplo, las alarmas y las mediciones son recolectadas desde los elementos de red por los colectores de una específica tecnología. Las alarmas son enviadas a un buffer a través de colectores generales. Los procesadores de alarmas en el sistema monitor obtienen la alarma leyendo los buffers.

Las mediciones son escritas en un archivo, de donde los componentes del sistema del módulo de performance las obtienen para su respectivo procesamiento.

2.3 Arquitectura de hardware

El hardware del sistema de administración de red está diseñado en función de los siguientes principios:

Alta disponibilidad:

Comprende componentes redundantes tales como discos, controladores de red, fuentes de poder, etc.

Soporte en cluster HP, MC/Service Guard.

Escalabilidad:

Servidores en cluster, dependiendo de la configuración y el nivel de protección de datos.

Servidores de aplicación Windows.

Los servidores pertenecientes al sistema pueden ser escalados adicionando memoria y CPU.

Almacenamiento consolidado:

La red de área de almacenamiento (SAN) como solución para el arreglo de discos.

2.3.1 Componentes del sistema

El sistema cuenta con los siguientes componentes:

Servidor de base de datos (DS): Servidor en el cluster MC/Service Guard que corre el paquete de base de datos.

Modelos de servidores (HP): K380, K580, L2000/rp5450, L3000/rp5470 y rp4440.

Servidor de sistema (SS): Servidor en el cluster MC/Service Guard que corre los paquetes de sistema y aplicación.

Modelos de servidores (HP): K380, K580, L2000/rp5450, L3000/rp5470 y rp4440.

Servidor componente del sistema (SCS): Servidores en cluster, en el cual cada uno corre otros paquetes de aplicación.

Modelos de servidores (HP): K380, K580, L2000/rp5450, L3000/rp5470 y rp4440.

Nodo failover de la base de datos (DFN): Nodo adoptivo diseñado para el paquete de la base de datos. El DFN debe ser del mismo modelo de servidor del DS y debe ser idénticamente dimensionado. El DFN puede ser el SCS o SS.

Modelos de servidores (HP): K380, K580, L2000/rp5450, L3000/rp5470 y rp4440.

Servidor de aplicación Windows (WAS): Servidores que corren aplicaciones de interfase de usuarios. Sirven como punto de acceso para las conexiones de usuario.

Modelos de servidores (HP): DL580, DL380G2, DL360G3 y DL360G4

2.3.2 Configuraciones de los servidores del sistema

a) Configuración de un servidor

La configuración con un servidor consiste de un servidor de base de datos y sistema combinados en un solo servidor (SDS) y servidores de aplicación windows, dependiendo de las necesidades de usuarios. El almacenamiento es en arreglo de discos conectados a un SAN o módulo de arreglo de discos.

Esta configuración es solo para clusters regionales.

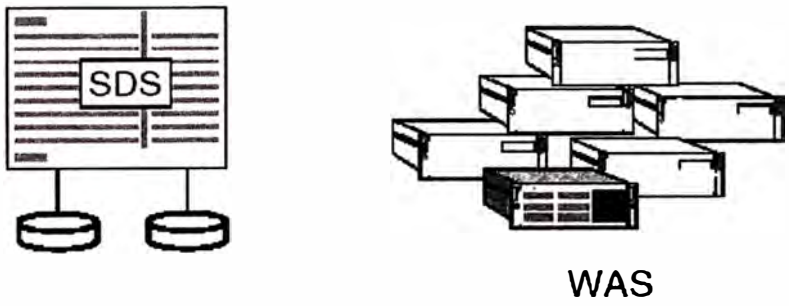


Figura 2.6: Configuración de 1 servidor

b) Configuración de 2 servidores

La configuración con 2 servidores (como el sistema propuesto) consiste de un Servidor de sistema (SS) y un Servidor de base de datos (DS). En adición, existen también servidores de aplicación Windows, dependiendo de las necesidades de usuarios. El almacenamiento es realizado en arreglo de discos conectados a un SAN.

Esta configuración puede ser utilizada en un cluster regional o global.

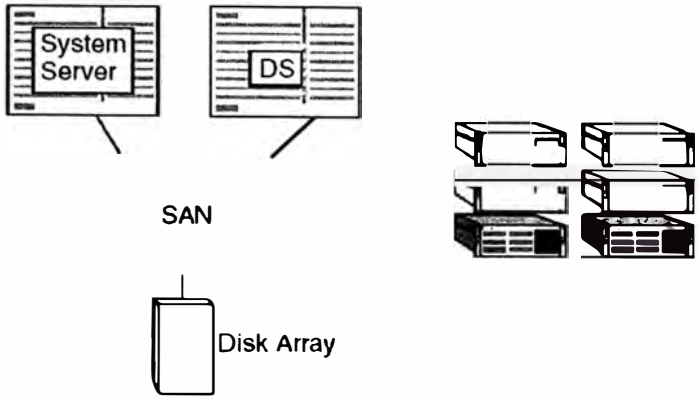


Figura 2.7: Configuración de 2 servidores

c) Configuración de 3 a 5 servidores

La configuración de 3 a 5 servidores consiste de un Servidor de sistema, un Servidor de base de datos y uno o más Servidores componentes de sistema. Uno de los servidores componentes de sistema actúa como el Nodo failover de la base de datos.

Son también usados los servidores de aplicación Windows y la información es almacenada en un SAN. Esta configuración es adecuada para los clusters regionales y globales.

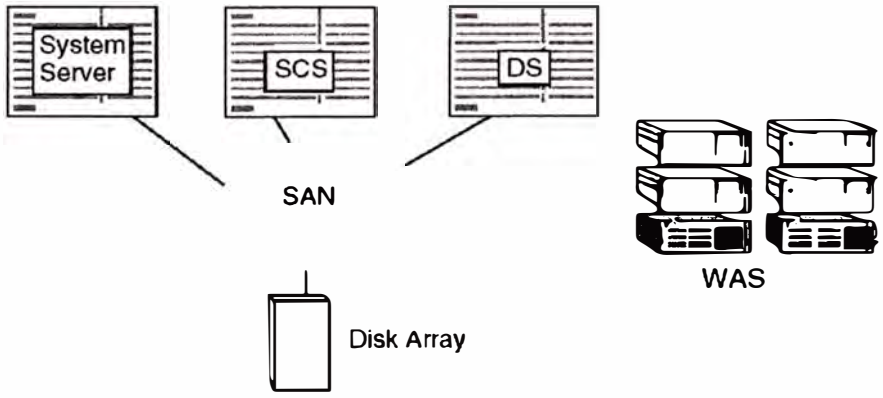


Figura 2.8: Configuración de 3 a 5 servidores

2.3.3 Solución de Almacenamiento

a) SAN y arreglo de discos

La solución de almacenamiento consiste de 2 partes independientes: La Red de área de almacenamiento (SAN) y el arreglo de discos.

La red de área de almacenamiento es una infraestructura de conmutación (switching) inteligente entre los hosts (servidores y workstations) y dispositivos conectados, tales como discos, arreglos de discos y librerías de cintas de almacenamiento. En otras palabras, SAN es una red dedicada al tráfico de entrada y salida (Input/output) de discos.

La solución SAN consiste de 2 switches de canal de fibra por cluster constituyendo una SAN Fabric redundante.

b) Agrupamiento de discos (Disk enclosures)

La solución básica de almacenamiento usando agrupamiento de discos puede ser usado en configuraciones de 1 o 2 servidores con drives de discos duros y fuentes de poder redundantes.

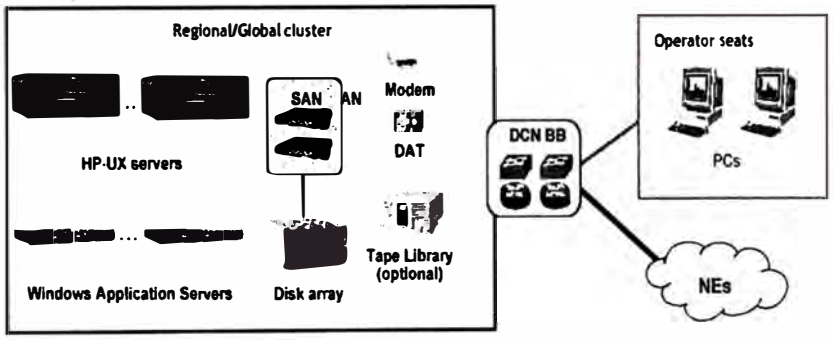


Figura 2.9: Solución general del hardware

2.3.4 Arquitectura de los servidores Windows

Los clusters del sistema de administración de red de NOKIA son una combinación de los servidores UNIX HP-UX y los servidores de aplicación Windows. Esto aplica para el cluster regional y global.

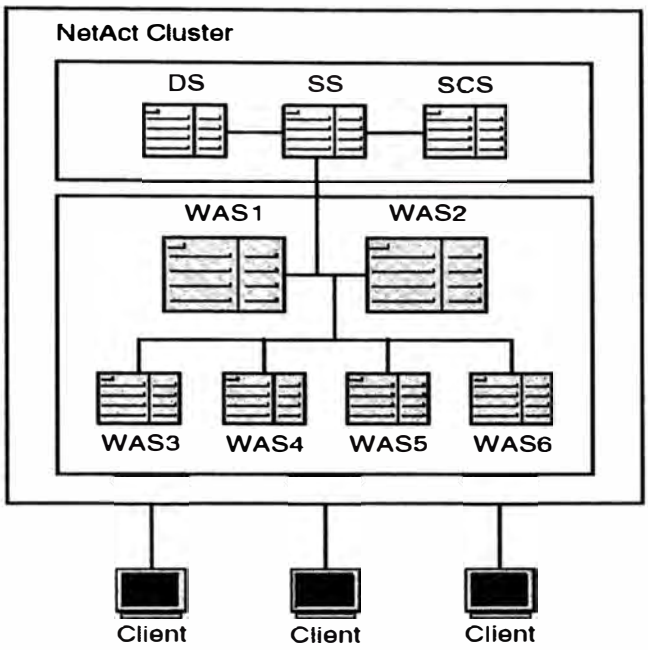


Figura 2.10: Arquitectura del cluster del sistema de administración de red con los servidores WAS

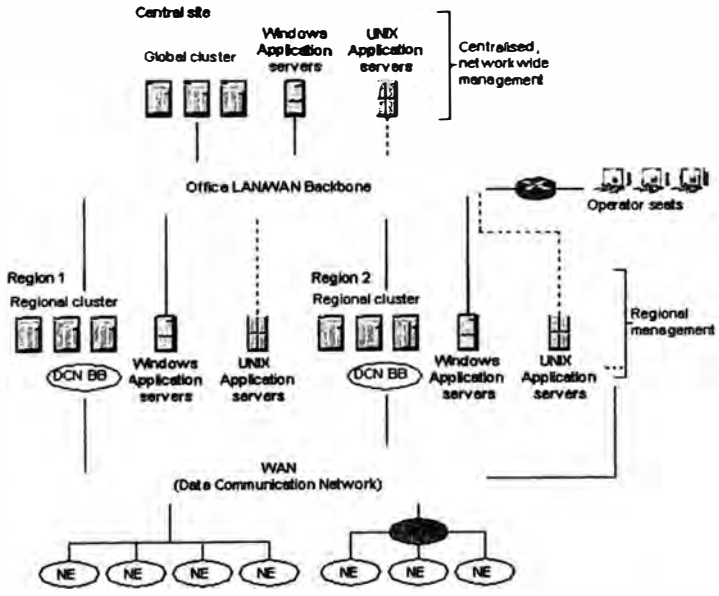


Figura 2.11: Arquitectura de hardware del NOKIA NetAct OSS

2.4 Arquitectura de software

2.4.1 Tipos de software

El sistema de administración de red de NOKIA, consiste de los siguientes softwares instalados en los diferentes tipos de servidores:

Los servidores de sistema (SS) y los servidores componentes del sistema (SCS) corren la funcionalidad del NMS en el cluster MC/Service Guard. El servidor de sistema existe en cada instalación del NMS; en la configuración de un servidor también corre la base de datos. El servidor componente de sistema soporta la carga del sistema y mejora la performance.

Versión de software: Sistema operativo Unix HP-UX versión 11.0 o 11i
Versión de la aplicación NOKIA: OSS 3.1 ED3

El servidor más potente es el servidor de base de datos (DS), el cual bajo circunstancias normales, corre las instancias de la base de datos. Si la base datos falla, la aplicación MC/Service Guard mueve el paquete de base de datos al nodo failover de la base de datos (SCS/DFN) predefinido.

El SCS/DFN es un servidor componente de sistema que está dimensionado idénticamente al servidor de base de datos, corre la funcionalidad del NMS y está diseñado para correr la base de datos si el servidor de base de datos falla.

Versión de software: Sistema operativo Unix HP-UX versión 11.0 o 11i
Versión de la aplicación NOKIA: OSS 3.1 ED3
Versión de base de datos: Oracle 8i

Los servidores de aplicación Windows (WAS) corren las aplicaciones de interfases de usuarios. El número de servidores WAS puede variar de acuerdo al número de aplicaciones a ejecutar y al número de usuarios que accedan a las aplicaciones.

Los usuarios son conectados a uno de los servidores WAS predefinidos usando el software cliente Citrix instalado en las estaciones de trabajo. Este software proporciona servicios similares para los entornos Windows como la emulación X lo proporciona para el UNIX. Múltiples usuarios pueden operar una o más aplicaciones al mismo tiempo. Debido al software de emulación X, los usuarios pueden extender sus sesiones desde los servidores WAS a cualquier servidor UNIX.

Aplicaciones: Java GUis, Web GUIs, aplicaciones EJB, emulaciones X Exceed y Oracle cliente.

Versión de sistema operativo: Windows 2000 server.

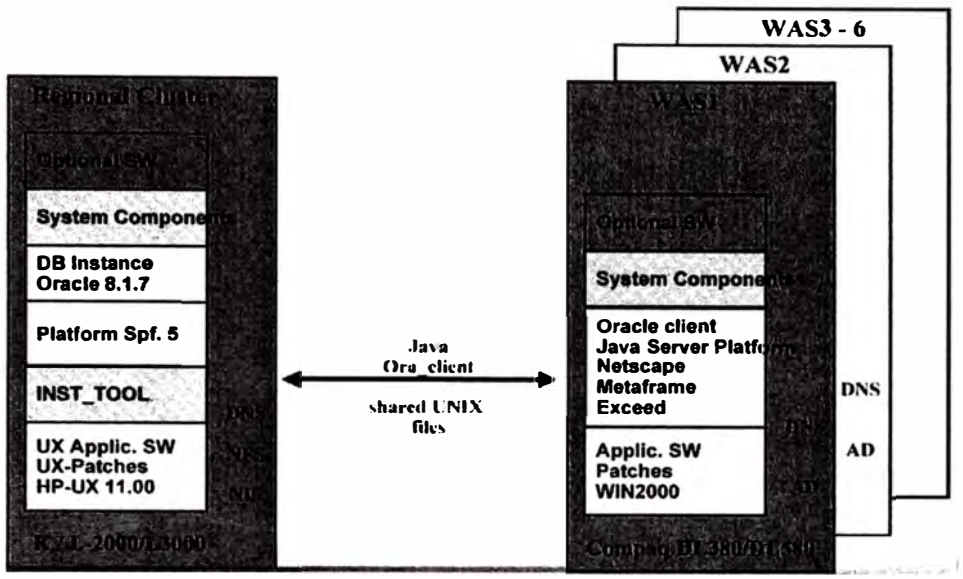


Figura 2.12: Arquitectura de software del sistema de administración de red NetAct OSS

2.4.2 Componentes de software para la disponibilidad del sistema

El sistema NMS de NOKIA utiliza varios componentes de alta disponibilidad para proteger constantemente las aplicaciones de una amplia variedad de fallas de hardware y software. Sin embargo, el principal componente es el MC/Services Guard.

El MC/Service Guard monitorea el funcionamiento del NMS y su base de datos, así como algunos componentes de hardware de la red del mismo. El MSC/Service Guard puede ser configurado para responder a las fallas en los procesadores del sistema, memoria del sistema, procesos del sistema, hardware de la red LAN y procesos de la aplicación.

a) Servidores del NetAct OSS y MC/Service Guard

La implementación NOKIA del MC/Service Guard consiste de nodos HP los cuales forman el cluster de alta disponibilidad. Cada servidor corre uno o más de los siguientes paquetes:

- El paquete del sistema, que posee el disco global y exporta éste a otros servidores usando Sistema de archivos de red (NFS). Cada cluster debe tener un solo paquete de sistema.
- El paquete de base de datos, el cual contiene los procesos oracle y posee los discos de la base de datos. Cada cluster debe tener el paquete de base de datos.
- Los paquetes de aplicación, el cual puede ser uno o más. Los paquetes de aplicación contienen uno o más computadores virtuales corriendo las aplicaciones del NMS de NOKIA.

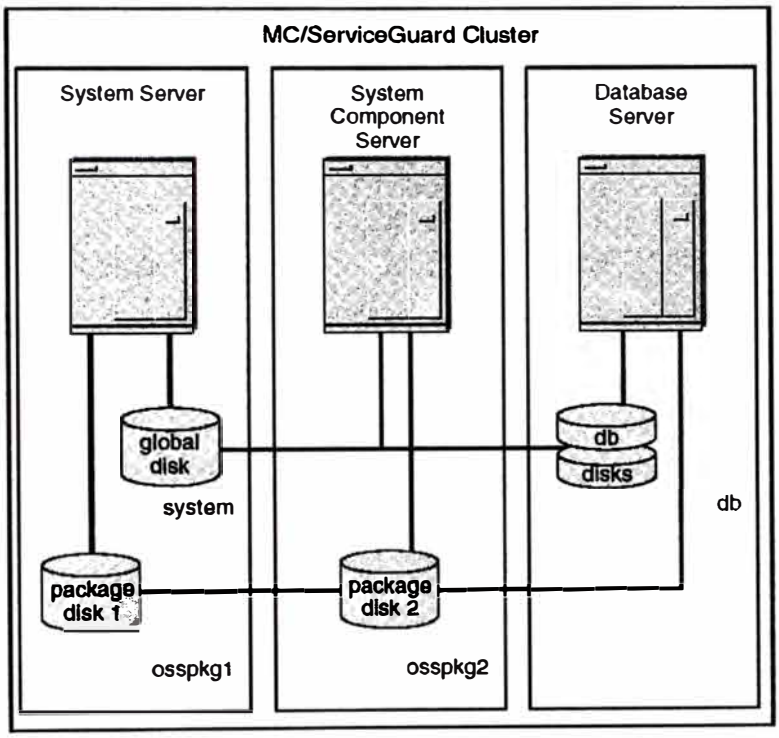


Figura 2.13: MC/Service Guard en una configuración de 3 nodos

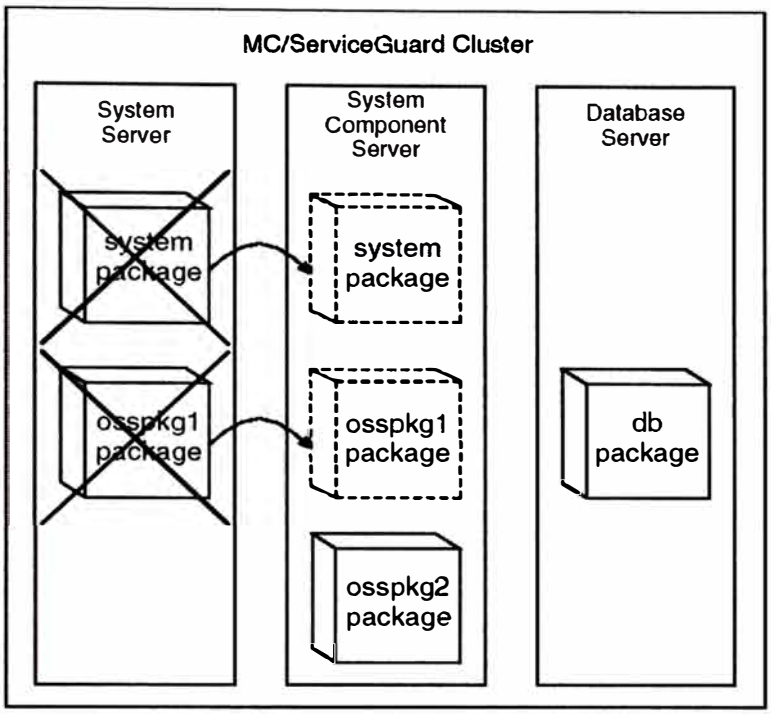


Figura 2.14: Falla del servidor de sistema en una configuración de 3 nodos

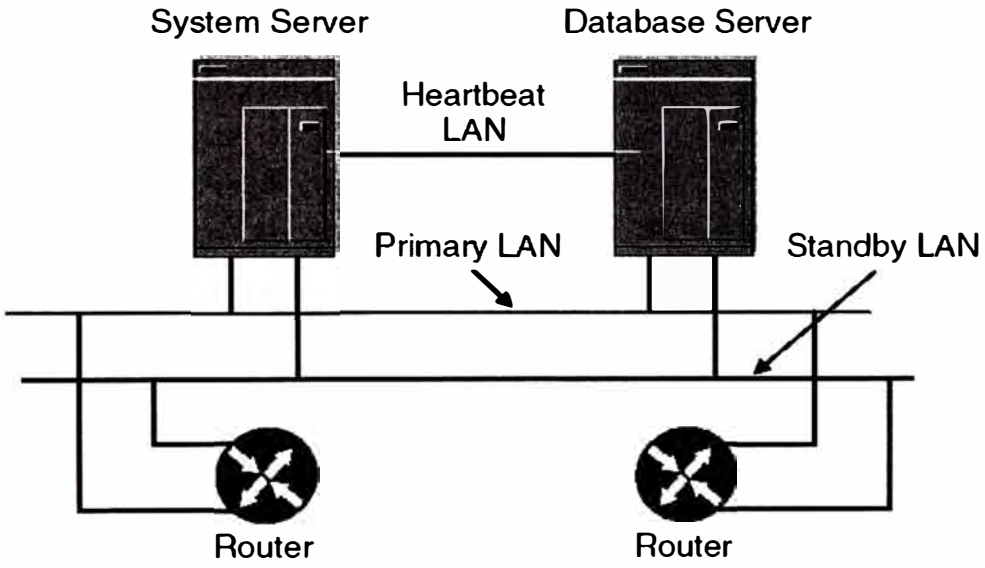


Figura 2.15: Supervisión de la conexión LAN

CAPITULO III

DISEÑO DE LA RED DE COMUNICACIÓN DE DATOS

3.1 Principios de diseño

La solución para el diseño de la red de comunicación de datos deberá proveer las siguientes características y funcionalidades:

Escalabilidad: El backbone de la red de comunicación de datos (DCN) debe ser capaz de adaptar cambios futuros en el uso de la red.

Disponibilidad: El backbone de la DCN debe proveer redundancia sin punto de falla.

Performance: El backbone de la DCN debe manejar el tráfico causado por las aplicaciones del sistema de administración hacia las redes gestionadas y los otros clusters del sistema de administración de red.

Seguridad: El backbone de la DCN debe proveer la posibilidad de integrar una solución de seguridad al sistema de administración para prevenir o proteger el tráfico.

Flexiblidad: El backbone de la DCN debe ser manejado desde el sistema de administración de red usando protocolos de comunicación. El sistema de administración de red provee plantillas de configuración descargables para los switches y routers con las LAN virtuales (VLANs) y los puertos predefinidos. Los usuarios serán requeridos a adicionar direcciones IP o ISO IP de acuerdo al plan de direccionamiento local.

Adaptabilidad: El diseño del backbone DCN debe tener una estructura modular la cual lo hace flexible en caso de cambios en las tecnologías WAN y LAN así como en los protocolos de enrutamiento.

Productividad: El diseño modular del backbone DCN permite el uso de equipamiento DCN existente. También es posible incrementar la performance sin grandes inversiones en nuevo hardware.

3.1.1 Planeamiento de le red

Cuando se requiere planificar la implementación de una red de comunicación de datos, se debe asegurar que todo el equipamiento, los nombres de host y las direcciones están disponibles y apropiadamente documentados. Esta información es necesaria para el planeamiento, integración y troubleshooting de la red de comunicación de datos (DCN).

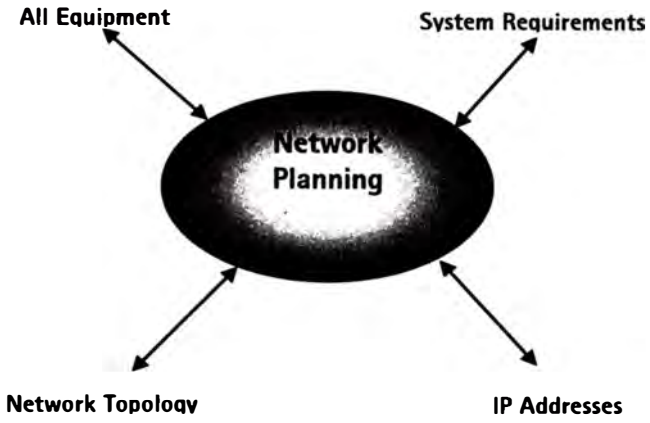


Figura 3.1: Planeamiento de red

Es aconsejable no cambiar la configuración actual de la DCN durante el proceso de instalación e integración. Cualquier cambio en la DCN debe ser hecho durante el planeamiento de la red.

3.1.2 Descripción de la Red de Comunicación de Datos (DCN)

La red de comunicación de datos (DCN) conecta los elementos de red al sistema de administración así como los diferentes sitios (sistema de administración). Las áreas del sistema de administración de red están divididas en clusters regionales y un cluster global. Un cluster global puede manejar varios clusters regionales. Por lo tanto, es posible combinar los clusters regionales y global en un solo sitio usando la misma solución de la red de comunicación de datos.

El backbone DCN provee una solución WAN y LAN integrada y redundante. La DCN provee conexiones a las redes 2G/GSM (ISO IP), 3G y redes de paquetes (Packet Core). Las partes WAN y LAN del backbone DCN pueden ser expandidas independientemente una de la otra.

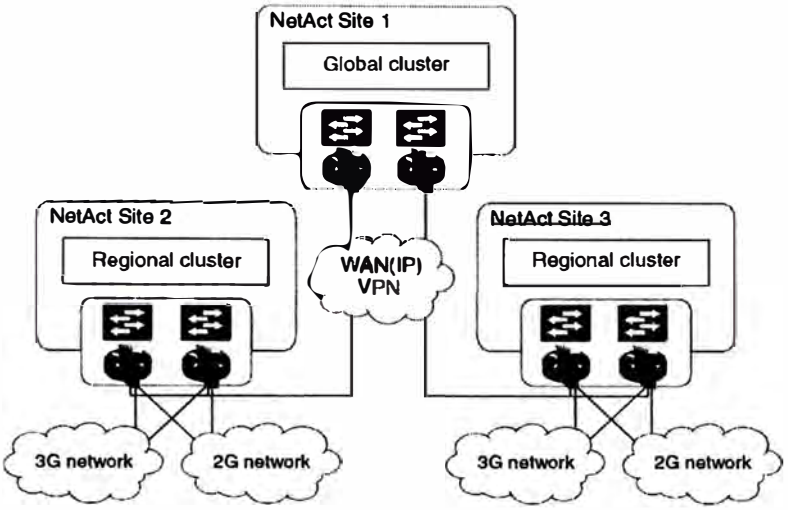


Figura 3.2: Descripción de la red de comunicación de datos (DCN)

La parte WAN provee las interfases para conexiones de Operación y Mantenimiento a los elementos de red 2G/3G y Packet Core, así como las conexiones entre clusters y conexiones backup y dial-up.

La siguiente lista describe el tipo de información requerida en un diagrama de red:
Hardware: Lista el fabricante de los equipos y su número de modelo. Por ejemplo: Servidor HP RP 4440, Router Cisco 3640 o equipos NOKIA DX 200.
Rol: Lista la función del hardware. Por ejemplo: Servidor del sistema, Servidor de base de datos, Servidor de aplicaciones, router, switch, MSC, HLR o BSC.
Software: Lista las versiones de software de todos los equipos.
Nombres de hosts: Lista los nombres de hosts de todos los equipos.
Direcciones: Lista las direcciones IP o X121 de todos los equipos.
Direcciones del Punto de acceso del servicio de red (NSAP): Lista las direcciones NSAP de todos los servidores y elementos de red.
Números C (C-Numbe): Lista los C-Numbers de todos los elementos de la red.

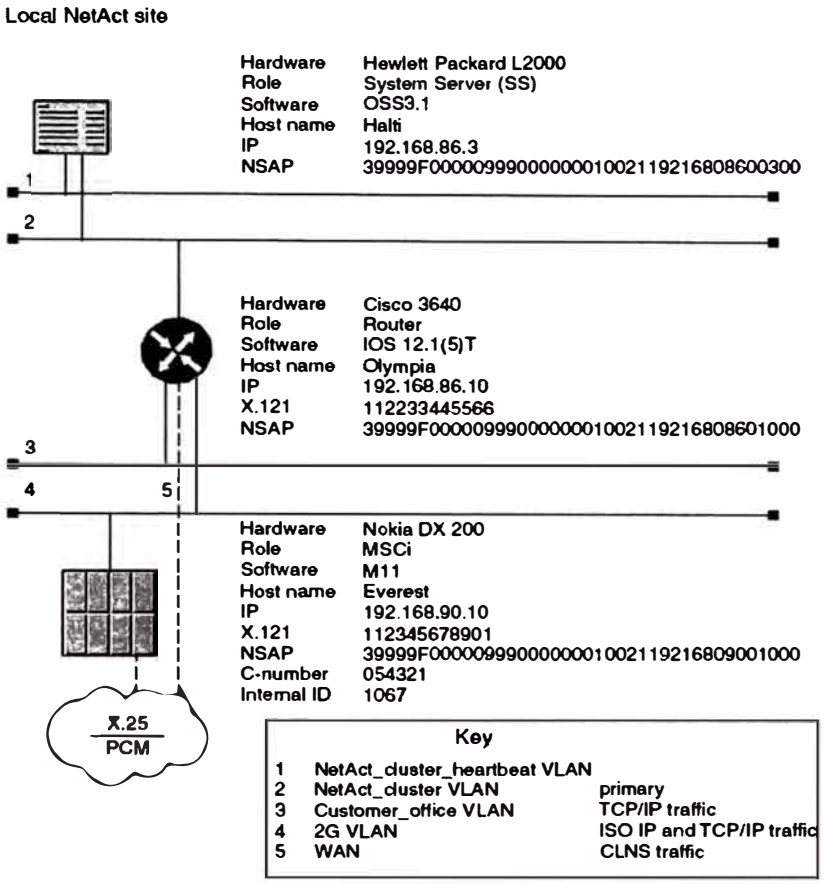


Figura 3.3: Ejemplo de un mapa de red

3.1.3 Principios de operación del backbone DCN

Las diferentes partes (lógicas) de la red están divididas en LAN virtuales (VLANs), por ejemplo, definición de LAN virtuales para los servidores del sistema de administración de red y los elementos de red local. Los routers son usados para encaminar los paquetes entre las diferentes VLANs.

Las plantillas de configuración pueden ser usadas en los switches y routers para simplificar y acelerar el proceso de comisionamiento. Conforme todas las principales VLANs están predefinidas en las plantillas de configuración, el usuario solo necesitará proveer las direcciones IP de acuerdo al plan de direccionamiento local.

Todos los componentes del backbone DCN son manejados desde el sistema de administración de red usando SNMP. Los traps SNMP enviados por los routers y switches del backbone DCN son almacenados en la base de datos del sistema de administración de red para luego ser vistos por las aplicaciones respectivas.

Conforme al requerimiento, el sistema de administración puede estar aislado de la red. El aislamiento es hecho por firewalls ubicados entre el sistema de administración de red y la red externa.

a) Conexiones lógicas en el backbone DCN

La solución del backbone DCN consiste de switches y routers, los cuales tienen la capacidad de definición de VLANs y enrutamiento IP respectivamente. Esto permite la alta disponibilidad del enrutamiento/conmutación (routing/switching) de los paquetes IP entre las diferentes VLANs de los switches. Los routers también están dedicados a propósitos de enrutamiento WAN.

Los switches son hardwares redundantes, lo cual significa que los hosts que están conectados a los switches se recuperan si uno de los switches falla. Sin embargo, los hosts deben tener un software especial para ser capaz de recuperarse de éste tipo de fallas (por ejemplo, MC/Service Guard en el Unix de Hewlett Packard).

El protocolo HSRP es utilizado para proveer la disponibilidad de un default gateway IP y para hacer que los cambios en la topología de red sean transparentes a los hosts. El HSRP debe ser configurado en cualquier VLAN donde los hosts IP están presentes.

Los switches y routers WAN están interconectados vía una VLAN dedicada e intercambian dinámicamente la información de enrutamiento utilizando el protocolo OSPF.

El tráfico entre la WAN y las VLANs del sistema de administración de red está redireccionado por los routers. El principal rol del router es proveer conexiones a los elementos de red 2G/3G, Packet Core e interconexiones WAN entre los diferentes sitios del sistema de administración de red.

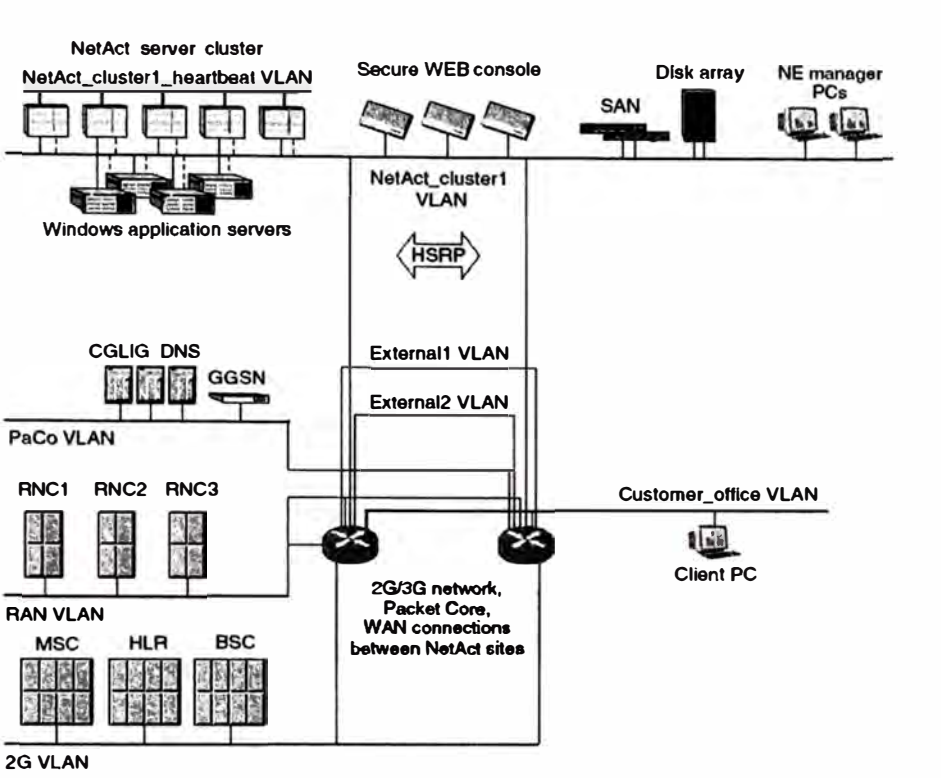


Figura 3.4: Diagrama lógico de la red

b) Conexiones físicas en el backbone DCN

Todos los hosts en los diferentes sitios del sistema de administración de red están conectados a los puertos 10/100Mbits de los switches. El software MC/Service Guard en HP-UX provee la redundancia para los servidores del NMS en el cluster en caso de una falla en el enlace. Los elementos de la red local, los servidores de aplicación y las estaciones de trabajo de operación están también interconectados a los switches.

Los switches están interconectados por medio de Canal fast ethernet (FEC). El FEC, provee hasta 800/400 Mbits (4 o 2 enlaces full duplex fast Ethernet) de ancho de banda agregado entre los switches.

Los routers están interconectados a los switches vía enlaces Fast Ethernet. Dado que los routers son redundantes, la falla de un switch no interrumpe la comunicación normal entre el sistema de administración de red y las redes gestionadas. El protocolo OSPF y los protocolos IS-IS distribuyen dinámicamente los cambios que ocurren en la topología de red entre los routers.

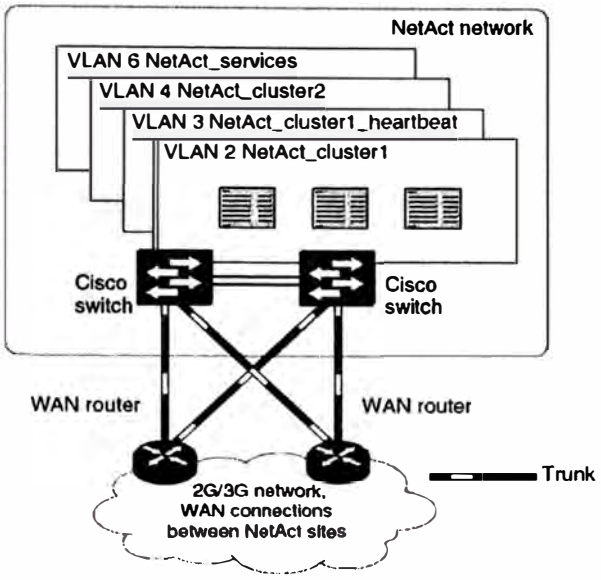


Figura 3.5: Conexiones físicas en el backbone DCN

El enlace fast ethernet que conecta al router y el switch está configurado como una VLAN trunk (ISL o 802.1Q). Es necesario configurar el trunk porque los routers redireccionan los paquetes ISO IP con los paquetes IP. Los paquetes ISO IP no pueden ser encaminados en los switches, por lo tanto, ellos deben ser redireccionados directamente a la VLAN ISO IP.

3.1.4 Soluciones DCN

Las soluciones del backbone DCN deben estar diseñadas para ser fácilmente modificables y soportar la administración de redes separadas. Como solución del backbone DCN, se propone el uso de routers y switches, con una solución de firewall entre el sistema de administración y las redes manejadas, y una interfase a la red del operador.

NOKIA provee varias soluciones de red que están agrupadas en las siguientes categorías:

Redes de área local (LAN).

Redes de área amplia (WAN).

También es posible combinar diferentes tipos de soluciones de red dentro de una DCN.

Los siguientes factores afectan la disponibilidad de la solución DCN:

- Capacidad requerida
- Costo de equipamiento y/o enlaces
- Configuración actual
- Distancia entre el Sistema de administración y sus elementos de red
- Facilidad de configuración y mantenimiento
- Calidad de servicio

a) Redes de área local (LAN)

Las redes de área local son redes de alta velocidad con bajo error de datos que cubren un área geográfica pequeña (algunos miles de metros). Estas redes conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo lugar u otra área limitada geográficamente.

Debido a las características físicas del envío de datos a altas velocidades, el rango de una red LAN está limitado a 2.5Km usando repetidores (10Base5).

IEEE 802.3

Las soluciones DCN ofrecidas por NOKIA soportan redes LAN IEEE 802.3. Este estándar especifica la capa física (capa 1) y la parte de canal de acceso de la capa de enlace de datos (capa 2). Las redes LAN IEEE 802.3 no definen el protocolo de control de enlace lógico. Este protocolo es definido en IEEE 802.2. Los siguientes tipos de redes LAN 802.3 están disponibles:

Tabla 3.1: Diferentes tipos de redes LAN IEEE 802.3

IEEE 802.3	-	-	-
	10Base2	10BaseT	100BaseT
Data rate (Mbps)	10	10	100
Signalling method	Baseband	Baseband	Baseband
Maximum segment length	185 metres	100 metres	150 metres
Media	50-ohm coax (thin)	Unshielded twisted-pair wire	Unshielded twisted-pair wire (category 5)
Topology	Bus	Star	Star

La red LAN IEEE 802.3 es la actual solución con alta performance, en la que el sistema de administración de red es conectado indirectamente a un elemento de red usando un dispositivo de enrutamiento. Esto permite a los operadores de red a construir un nivel adicional de redundancia entre los servidores de la red de administración de datos, dispositivos de enrutamiento y redes físicas.

Las conexiones LAN para comunicación de datos tienen las siguientes ventajas:

Facilidad de configuración: Debido a la naturaleza dinámica de la topología de red ES-IS, las redes LAN son fáciles de configurar usando la aplicación de Servicios de Transporte OSI (Solución NOKIA: HP).

Amplia capacidad: Desde el punto de vista de performance, la solución LAN provee la capacidad más alta debido a la amplia potencialidad del ancho de banda de una red LAN.

Redundancia: Debido a que las redes LAN son fáciles de configurar e instalar, dividiendo el tráfico IP por sus roles (heartbeat, comunicaciones, redundancia, oficina y DCN) permite a los operadores de red crear un nivel adicional de redundancia en la capa física.

Capacidades de enrutamiento: Debido a que las redes LAN requieren que los paquetes completos de datos sean enviados a sus destinos (incluyendo información de dirección), la capa de red puede elegir los métodos de enrutamiento más eficientes para la información. Alternativamente, esto "refresca" la red y minimiza el efecto de fallas de línea.

Sin embargo, las conexiones LAN presenta la siguiente desventaja:

Límites de distancia: Para mantener un nivel aceptable de los costos de implementación, se recomienda que el sistema de administración de red y los elementos de red estén ubicados dentro de un área geográfica razonablemente pequeña, como en el mismo lugar.

A continuación se muestra la implementación de una conexión LAN IEEE 802.3:

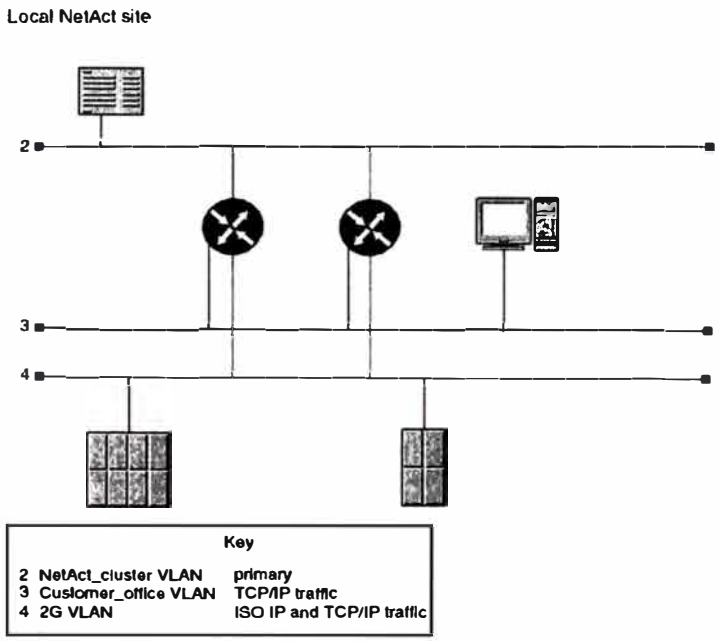


Figura 3.6: Usando una conexión LAN IEEE 802.3

b) Redes de área amplia (WAN)

Una red WAN es una red de comunicación de datos que sirve a los usuarios a través de un área geográfica amplia y frecuentemente usa dispositivos de transmisión proveídos por portadores comunes (carriers).

X25 sobre PCM

La Modulación por Códificación de Pulsos (PCM) es un proceso en el cual una señal es muestreada y cada muestra es cuantificada independientemente de las otras y convertida por codificación a una señal digital. (ITU-T, G.701). De aquí que el X25 sobre PCM es también referido como X25 digital. En la solución de NOKIA, cuando se usa X25 sobre PCM, el Sistema de administración de red, NOKIA NetAct OSS, es conectado a un elemento de red (NE).

Un router, equipado con una tarjeta E1, actúa como un sistema intermedio (IS) entre el Sistema de administración de red (NetAct OSS) y el elemento de red (ES – IS – ES).

Las interfases E1 son usadas para proveer conexiones X25 sobre PCM usando el estándar G703. Esta interfase tiene la capacidad de transmitir y recibir datos en el E1 a una velocidad de 2.048 Mbps a través de un cable serial canalizado.

Cuando se usa X25 sobre PCM, el sistema de administración de red debe ser conectado a un sistema intermedio (IS) usando una red LAN IEEE 802.3. La configuración de una red usando X25 sobre PCM requiere:

- Una conexión LAN al sistema de administración de red.
- Una conexión PCM desde el router al elemento de red remoto.

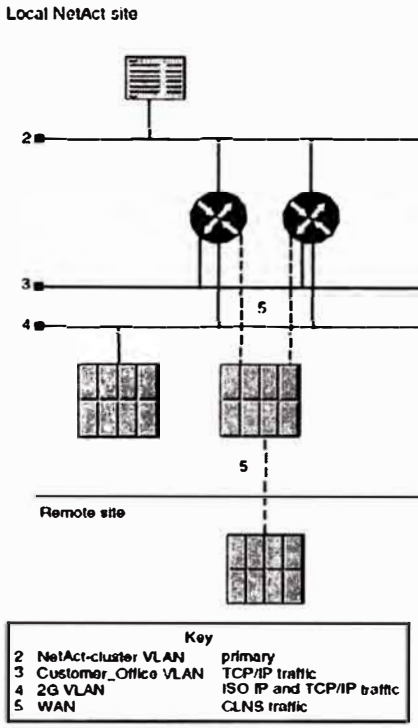


Figura 3.7: Implementación X25 sobre PCM usando un sistema intermedio

El uso de X25 sobre PCM para una red de comunicación de datos tiene las siguientes ventajas:

Bajo costo: La implementación rápida y de bajo costo es posible porque el X25 sobre PCM es una parte vital e integral de una red de telecomunicaciones.

Confiabilidad y seguridad: Debido a su naturaleza punto a punto, las conexiones PCM son muy confiables y seguras.

El uso de las conexiones PCM para la red de comunicación de datos tiene las siguientes desventajas:

Pérdida de la capacidad de telecomunicaciones: El uso de las conexiones PCM para tareas de administración de red elimina la capacidad PCM de los canales de voz.

Tasa de transmisión: La tasa de transmisión de una conexión PCM es típicamente más baja que una LAN.

Cuando el PCM es usado, las estaciones de trabajo de la red del sistema de administración son conectadas a un router en una LAN.

c) Routers redundantes

Para un nivel adicional de tolerancia de fallas, los routers redundantes son usados entre el sistema de administración de red y un sistema final. Un router redundante (secundario) permite que el tráfico sea redireccionado automáticamente a través de una conexión activa en caso que el router primario falle. Esta redundancia previene que un sistema intermedio sea el único punto de falla. Para alcanzar el nivel de tolerancia de falla, ambos routers deben ser interconectados a través de 2 segmentos LAN IEEE 802.3. En una falla de conexión, el router primario redireccionará los paquetes a su destino vía la interfase secundaria (activa). El protocolo utilizado para conectar los routers del sitio local a los routers del sitio remoto pueden ser HDLC o PPP.

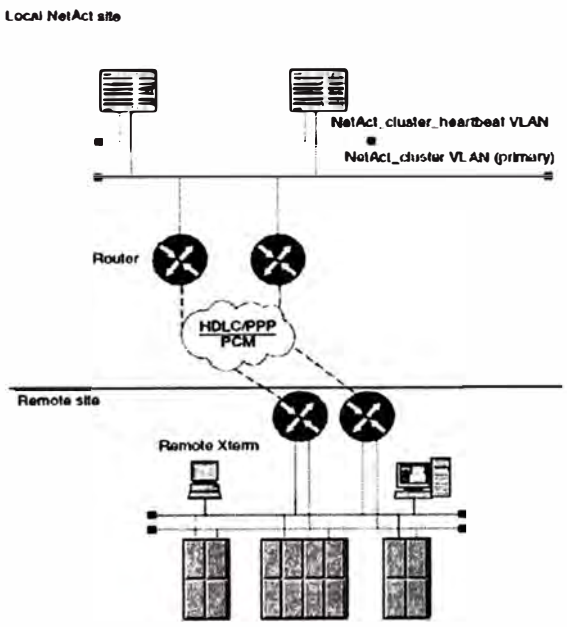


Figura 3.8: Usando routers redundantes en una solución DCN

d) Tarjetas de red

La subred (X25 o LAN) determina que tarjeta de red es requerida. Las diferentes tarjetas de red son descritas a continuación:

Tabla 3.2: Tipos de tarjetas de red

Network cards	Subnetwork	Interface(s)
COCEN (CP-523A, CPSSO-B)	IEEE 802.3 LAN with the LLC1 data link transfer protocol	• coaxial interface (10Base2) • attachment unit interface (10Base5) • twisted pair interface (10BaseT)
AC25-S AC25-A	X.25 • support for both DTE and DCE device types	• restricted V.24 • V.24 • V.35 • V.36 • X.21
AS7-U AS7-V AS7-A AS7-B	X.25 over PCM	G.703

Cuando se utiliza las tarjetas AC25-S o AS7-U, los canales físicos están definidos por las propiedades de la tarjeta de red con los parámetros X25.

Por ejemplo: Tarjeta de red + parámetros = Canal físico

La información asociada con la unidad plug-in X25 define la información específica del hardware tales como los datos de la unidad y los posibles tipos de interfase.

El canal define los atributos dinámicos del equipo terminal X25, tal como el método de comunicación, velocidad y la parte DTE del equipo Terminal.

Cuando se usan las tarjetas COCEN, el protocolo ISO IP es usado para implementar una conexión LAN como parte de la solución DCN. Las tarjetas COCEN están solo asociadas con los objetos de enlace CLNS. Sin embargo, cuando se usa CLNS sobre X25, la tarjeta X25 está asociada con objetos de enlace CLNS.

3.1.5 Soluciones de seguridad

Con la solución de seguridad, el operador puede monitorear y regular el tráfico entre el sistema de administración de red y las redes externas. La solución de seguridad de la red de comunicación de datos consiste del firewall que controla el acceso al NMS y encripta el tráfico de administración de red.

a) Principios de seguridad de la red de comunicación de datos (DCN)

El framework del sistema de administración está basado en servidores y sistemas operativos que permiten los principios de seguridad genéricos. En adición a ésta

seguridad genérica, la solución del sistema de administración tiene un rol más amplio para garantizar la seguridad de la red del operador.

La solución de la seguridad de la DCN debe estar basada en mecanismos estandarizados y abiertos, tales como IPSec, 3DES, SHA-1, MD5, PKI y SSH.

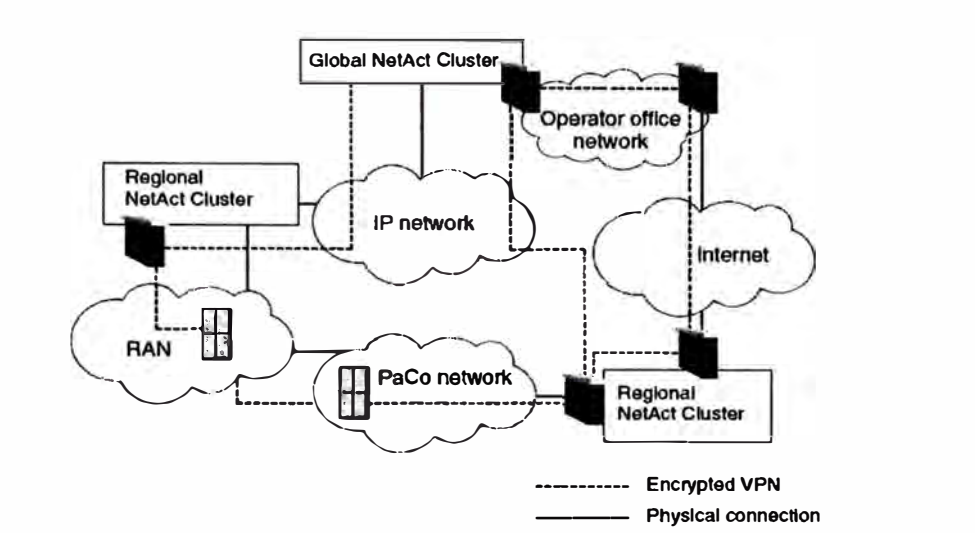


Figura 3.9: Una red de comunicación de datos segura

La solución de seguridad de la DCN tiene las siguientes características y capacidades:

Permitir la comunicación intra-cluster: El cluster está ubicado dentro de un solo sitio y solo personas autorizadas pueden accesar a éste. No existe necesidad para la encriptación o autenticación entre aplicaciones dentro de un cluster.

Encriptación de la comunicación inter-cluster: Es posible encriptar todo el tráfico entre los clusters del sistema de administración de red.

Acceso al cluster del sistema de administración: Con la solución del firewall, es posible controlar el tráfico desde los clientes que accedan al sistema de administración desde fuera de la red. Todo el tráfico es autenticado.

Encriptación de las conexiones de los elementos de red

Separación de la red de administración de la DCN con un firewall

Construyendo la política de seguridad

La política de seguridad define los protocolos de comunicación y las reglas necesarias para las conexiones de administración de red. Sin embargo, los administradores tienen que producir su propia política de seguridad extensiva para un

sistema completo de administración de red, tal como los clusters del NMS, autenticación de usuarios, etc.

La política de seguridad se observa en una tabla que contiene las reglas asignadas a cada elemento de red. Las reglas definen cual tráfico puede pasar a través del firewall y cual es rechazada. El firewall compara los paquetes en las primeras 3 columnas (Origen, Destino y Servicio). Cada paquete inicia en la regla superior y se mueve hacia abajo hasta encontrar su regla adecuada. Todo el tráfico (puerto tcp/udp < 1023) es rechazado a menos que esté permitido explícitamente.

Todo el tráfico (tcp > 1023) es permitido a menos que esté denegado explícitamente. En la última regla, cualquier tráfico (Origen-any, Destination-any y Service-any) es también descartado.

Los gateways VPN proporcionan transmisión segura de la información sensitiva sobre redes no protegidas. Todo el tráfico es encriptado y solo la entidad receptora puede desencriptar los datos. Las VPNs pueden ser usadas cuando existen conexiones a los otros clusters del NMS y elementos de red basados en IP.

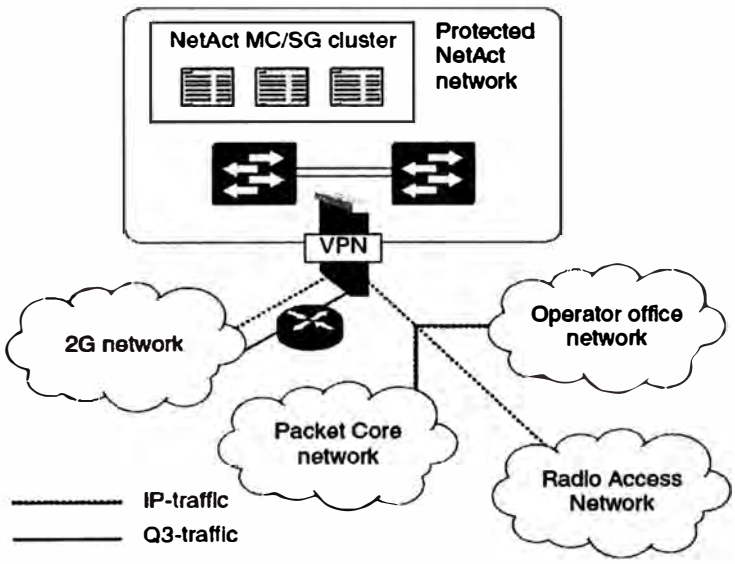


Figura 3.10: Configuración con Firewall

Los objetos de red incluyen las estaciones de trabajo, gateways, routers, redes, switches, servidores, gateway clusters y dominios. Antes de incluir un objeto de red en una regla, se debe definir éste y sus propiedades. Los objetos de red puede ser organizados en grupos jerárquicos para formar objetos del más alto nivel y reglas más leíbles.

Amenazas de seguridad

Las amenazas de seguridad pueden ser divididas en amenazas internas y externas.

Amenazas de seguridad externas:

La solución de seguridad se concentra en proteger la red IP del NMS de amenazas externas limitando el acceso a la red y autenticando y auditando la comunicación a y desde el NMS. La siguiente tabla lista algunas amenazas de seguridad externas:

Tabla 3.3: Amenazas de seguridad externas

Security threat	Counter-measure
Unauthorised access	NetAct Framework security policy, protected by the firewall
Traffic hijacking	Protected by the VPN solution
IP spoofing	Detected by the firewall
Denial of service	Detected and protected by the firewall
Modification of messages	Protected by the VPN solution

Amenazas de seguridad internas:

Las amenazas de seguridad internas son manejadas con la característica de administración centralizada de usuarios del sistema de administración de red.

b) Solución firewall integrado y VPN

Esta solución es utilizada para la seguridad de la red IP del sistema de administración de red y provee seguridad para la transmisión de datos sobre redes no protegidas.

Funcionalidades y características

Los firewalls proveen los medios para controlar el tráfico IP entre 2 redes o servidores. La solución de Firewall de NOKIA, basada en plataforma de seguridad de redes IP y software CheckPoint Firewall, provee un medio para controlar y monitorear el tráfico IP originado desde o destinado a una red protegida por el NMS. Los paquetes IP son redireccionados dinámicamente basados en el conjunto de reglas configuradas.

Los gateways VPN proveen un medio de encriptación selectiva del tráfico de datos entre los sitios que están separados de las redes en donde la seguridad de las

conexiones no pueden ser controladas (por ejemplo, servicios WAN públicos e Internet). DES y 3DES son los estándares de tecnología de criptografía más populares utilizados en los gateways VPN IPSec.

En adición a la solución Firewall y VPN, NOKIA provee una política de seguridad para el site del NMS el cual permite solo conexiones necesarias entre los componentes del NMS y los hosts IP externos (no protegidos), tales como los elementos de red y las PC clientes.

La solución integrada de Firewall y VPN de NOKIA provee las siguientes características:

- Solución única que provee seguridad en la comunicación de redes y control de acceso
- Alta disponibilidad y distribución de carga con el VRRP (Virtual Router Redundancy Protocol)
- Consola de administración remota y centralizada para la política de configuración del firewall y la VPN
- Administración del sitio del NMS y sitios remotos dentro de la misma solución
- Enrutamiento de alta performance en la plataforma optimizada de seguridad de NOKIA:

  Enrutamiento dinámico.

  Rendimiento IPSec hasta 200Mbps.

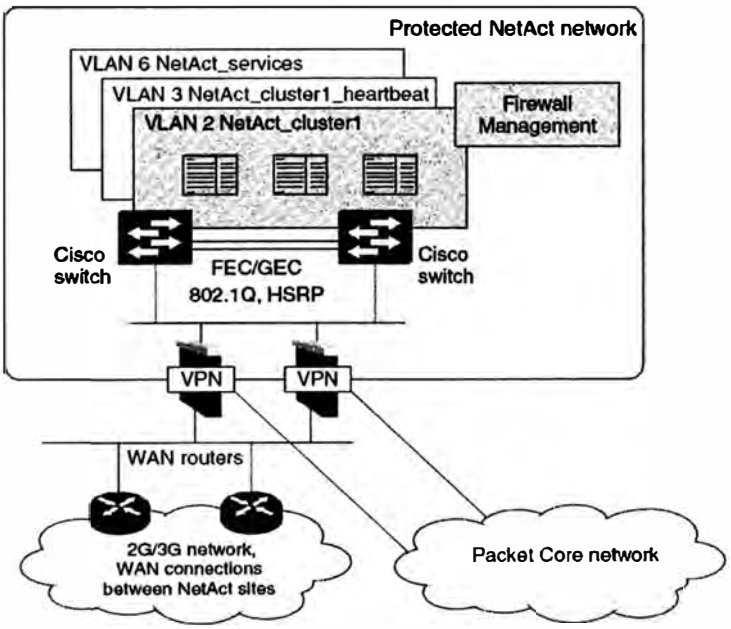


Figura 3.11: Solución Firewall Integrado y VPN

3.2 Arquitectura de red

3.2.1 Introducción

La solución propuesta para el diseño de la red de comunicación de datos, constituye una propuesta que permitirá una alta disponibilidad del diseño.

El core de la arquitectura de la red de comunicación de datos (DCN) en cada sitio, forma un backbone DCN, una solución flexible, redundante y unificada que puede ser utilizada tanto en clusters globales como en clusters regionales. El backbone DCN provee conexiones a redes 2G GSM, 3G y Packet Core. Las conexiones entre los clusters son protegidas por Redes privadas virtuales (VPNs).

Las interfases de administración a las redes GSM, Packet Core y 3G son proveídas por el backbone DCN. Ambas conexiones LAN y WAN son soportadas: los elementos locales pueden ser conectados a los switches (VLANs) del backbone, mientras que las conexiones WAN son proveídas por los routers del backbone.

Las soluciones del backbone DCN propuestos pueden ser divididos en soluciones Mini y estándar (con switches de capa 2) y de alta performance (con switches de capa 3).

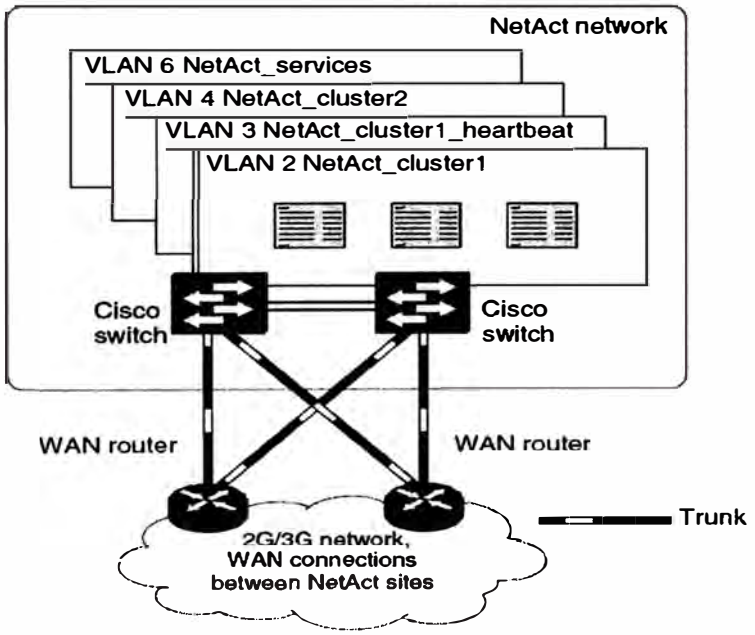


Figura 3.12: Arquitectura de backbone DCN

Las soluciones son listadas de la siguiente manera:

Backbone Mini DCN:

Por ejemplo, un servidor Unix HP, un MSC y un RNC o un BSC

1 Router de acceso Cisco 3640: Ruteo IP (IP Routing) y WAN (WAN Routing).

1 Switch de capa 2 Cisco Catalyst 2950: Los hosts locales son conectados al Switch.

Backbone DCN Estándar:

2 Routers de acceso Cisco 3640: Enrutamiento IP (IP Routing) y WAN (WAN Routing).

2 Switches de capa 2 Cisco Catalyst 2950: Los hosts locales son conectados al Switch.

Backbone DCN de Alta Performance:

2 Routers de acceso Cisco 3640: Enrutamiento IP (IP Routing) y WAN (WAN Routing).

2 Switches de capa 3 Cisco Catalyst 3550: Los hosts locales son conectados al Switch y para enrutamiento IP (IP Routing).

Un tercer switch es necesario para los dispositivos de Red de almacenamiento (SAN), consolas web (Unix HP) y el heartbeat (El heartbeat es una señal entre 2 nodos o procesos para verificar la operación en la comunicación). Este switch también provee interfases extras usada para otros componentes del sistema de administración, sistemas de tráfico, etc.

Las soluciones de capas 2 están más limitadas en capacidad y escalabilidad que la solución de capa 3. Por otro lado, las soluciones de capa 2 son menos costosas y permiten el uso del equipamiento existente.

3.2.2 Topologías de red

El procedimiento para el planeamiento de una DCN es determinado por la Topología de red usada. La topología de red define si se conectará un elemento de red directamente al sistema de administración de red o indirectamente usando routers. En esencia, las topologías de red definen la capa del cableado de red.

Una vez que la topología de red es definida, se procede a identificar los servicios de red (CLNS) y protocolos que serán usados (X25, ISO/IP y otros).

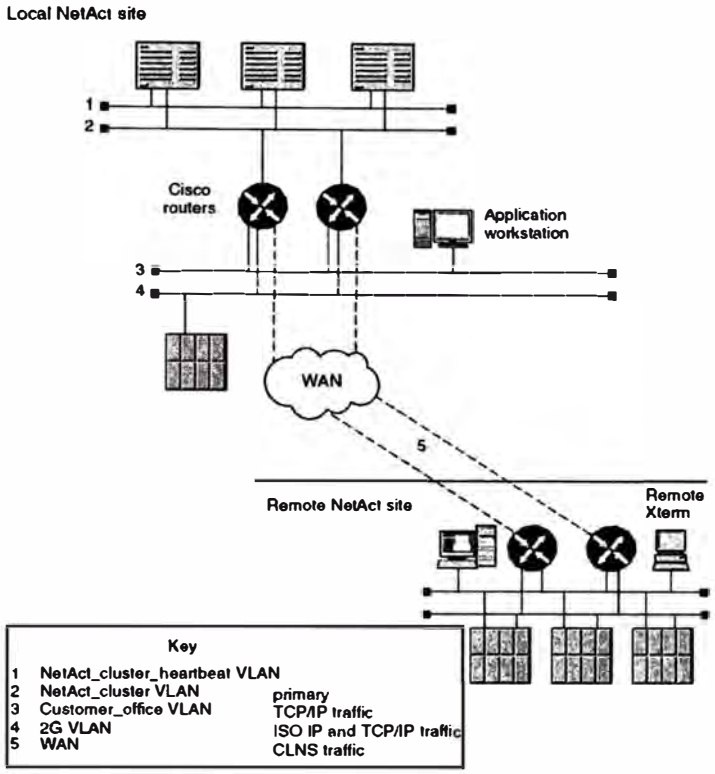


Figura 3.13: Ejemplo de una mapa de topología de red (sites locales y remotos)

3.2.3 Servicios de red

Los servicios de red permiten la transferencia de datos entre la capa de transporte OSI y la capa de red. Después de determinar que elementos de red son necesarios en la topología, se debe resolver el tema de la subred seleccionando el apropiado servicio de red. Por ejemplo, en el sistema de administración de red de NOKIA (NetAct OSS), el servicio de red sin conexión es soportado.

a) Servicio de red sin conexión (CLNS)

El CLNS envía independientemente paquetes de datos a su destino. Cada paquete contiene la dirección destino del sistema remoto. Una vez que el paquete es identificado, el servicio de enrutamiento selecciona la mejor ruta para entregar el paquete.

Por lo tanto, cada paquete es manejado y encaminado a su destino de manera individual. Esto da lugar a que los paquetes viajen sobre una variedad de trayectorias físicas a su destino final. Una vez que la información de dirección es encapsulada dentro del paquete, no se requiere una conexión dedicada entre sistemas finales.

El CLNS usa la capa de transporte OSI para establecer y terminar la conexión. Dentro del enfoque del CLNS, la capa de transporte también provee detección y

corrección de errores. Debido a que el CLNS consiste de una sola fase, transferencia de datos, CLNS no provee conexiones punto a punto.

El CLNS es comúnmente usado cuando existen varios elementos de red, incluyendo sistemas intermedios, en una subred LAN IEEE 802.3 o X25. El CLNS también permite que los elementos de red reconozcan un sistema intermedio en la misma subred. Debido al mecanismo de enrutamiento del CLNS, el efecto de las fallas es minimizado porque la carga de la red es distribuida más eficientemente que en un servicio de red orientado a conexión.

Un servicio de red sin conexión es requerido cuando la solución de red tiene:

- LAN IEEE 803.2.
- Sistemas intermedios (routers).

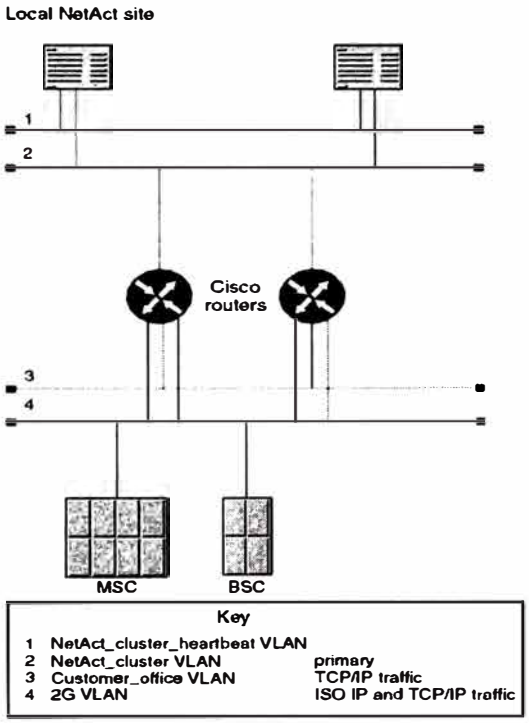


Figura 3.14: Servicio de red sin conexión en una red de comunicación NOKIA

Enrutamiento CLNS

El grupo de protocolos OSI incluye varios protocolos de enrutamiento y un protocolo de descubrimiento.

Los sistemas en la red están divididos en 2 diferentes categorías:

Sistemas finales (ES): Un sistema final se refiere a un elemento de red que no realiza enrutamiento. Los ejemplos de un sistema final en una red de

comunicación de datos son: Elementos de red (BSCs, HLRs, MSCs), servidores (del sistema de administración de red) e impresoras.

- Sistemas intermedios (IS): Un sistema intermedio se refiere a un sistema inteligente que distribuye o tiene la capacidad de encaminar información. Los ejemplos de un sistema intermedio en una red de comunicación de datos son: Los routers de un sistema third-party.

Dependiendo de la configuración de red, los siguientes protocolos de enrutamiento OSI son usados:

- Protocolo de descubrimiento (router) de sistema final a sistema intermedio (ES-IS) (ISO/IEC, 9542).
- Protocolo de enrutamiento intra-domain de sistema intermedio a sistema intermedio (IS-IS) (ISO/IEC, 10589).
- Protocolo de enrutamiento inter-domain de sistema intermedio a sistema intermedio (IS-IS) (ISO/IEC, 10747).

El protocolo de enrutamiento intra-domain IS-IS (ISO/IEC, 10589) es particionado en dominios de enrutamiento. Un dominio de enrutamiento es una colección de sistemas finales y sistemas intermedios que operan protocolos de enrutamiento comunes bajo el control de una sola administración. Los límites (enlaces exteriores) del dominio de enrutamiento son establecidos por la administración de red. Si un enlace es marcado como exterior (inter-domain), los mensajes de enrutamiento IS-IS no son enviados a ese enlace.

El enrutamiento IS-IS usa 2 áreas de enrutamiento jerárquico:

- Enrutamiento de nivel uno (intra-área).
- Enrutamiento de nivel dos (inter-área).

El enrutamiento de nivel uno (intra-área) permite la distribución de información dentro del área local de todos los sistemas intermedios. Los routers del nivel uno conocen la topología de su área, incluyendo todas las áreas y hosts. Debido a que los routers del nivel uno no conocen la identidad de los routers o destinos fuera de su área, éstos routers deben desviar todo el tráfico fuera de su área a un router del nivel dos.

El enrutamiento de nivel dos (inter-área) intercambia paquetes de datos o información de enrutamiento directamente con routers ubicados fuera de su área o dominio de enrutamiento. Los routers de nivel dos no necesitan conocer la topología de un área de nivel uno con la excepción de la ubicación del router de nivel dos en ésta área.

3.2.4 Conexiones a través de sistemas finales

a) Conexiones OSI remotas desde el DX200

En una red bien planificada, las conexiones OSI remotas desde el elemento de red DX 200 son configuradas usando varias rutas alternativas a un sistema destino. Si una falla de comunicación ocurre en una ruta, otra ruta alternativa puede ser abierta y usada para enviar los datos al destino.

El uso de rutas alternativas requiere la replicación de tarjetas de red. El método de replicación depende de la estructura de la subred OSI y el tipo de interfase disponible en el sistema remoto.

Cuando se usa CLNS, se deben crear el objeto CLNS y los objetos que intervienen en el enlace (linkage objects). Los linkage objects deben ser creados por cada interfase X25 o LAN. Las direcciones de red y NSAP son utilizados para asociar los servicios (CLNS) con un elemento de red. Una aplicación OSI es alcanzable a través de varios NSAPs.

Debido a que las aplicaciones OSI no están directamente asociadas con las direcciones NSAP, las direcciones de red son usadas para crear ésta asociación. Estas asociaciones (o direcciones de red) pueden contener varias direcciones NSAP.

Una vez que una dirección NSAP es mapeada (unida) a una dirección de red, se ha establecido que el enrutamiento está basado en CLNS.

Protocolo CLNS

Cuando se utiliza CLNS, las direcciones NSAP para el CLNS permiten que los datos sean encaminados usando protocolos IS-IS y sean resueltos usando protocolos ES-IS.

Estos protocolos enlazan dinámicamente el costo de información a cada tarjeta de red proveyendo una ruta a un sistema remoto identificado por la dirección NSAP. Esto hace posible seleccionar automáticamente el enlace más favorable.

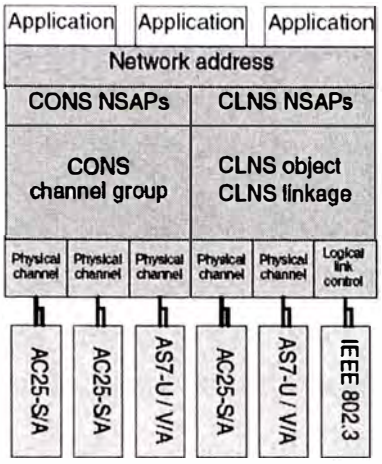


Figura 3.15: Interfase CLNS

Configuración de la conexión del servidor de software

El servidor de conexión del Sistema de administración de red de NOKIA es una aplicación de software distribuido a través de varias estaciones de trabajo en el mismo sistema. El servidor de conexión es usado para establecer conexiones de Lenguaje hombre-máquina (MML) desde la interfase de usuario (TLUI) a un elemento de red.

El MML es un lenguaje de comandos basado en texto, con una estructura estandarizada, diseñada para facilitar el control directo del usuario de un sistema.

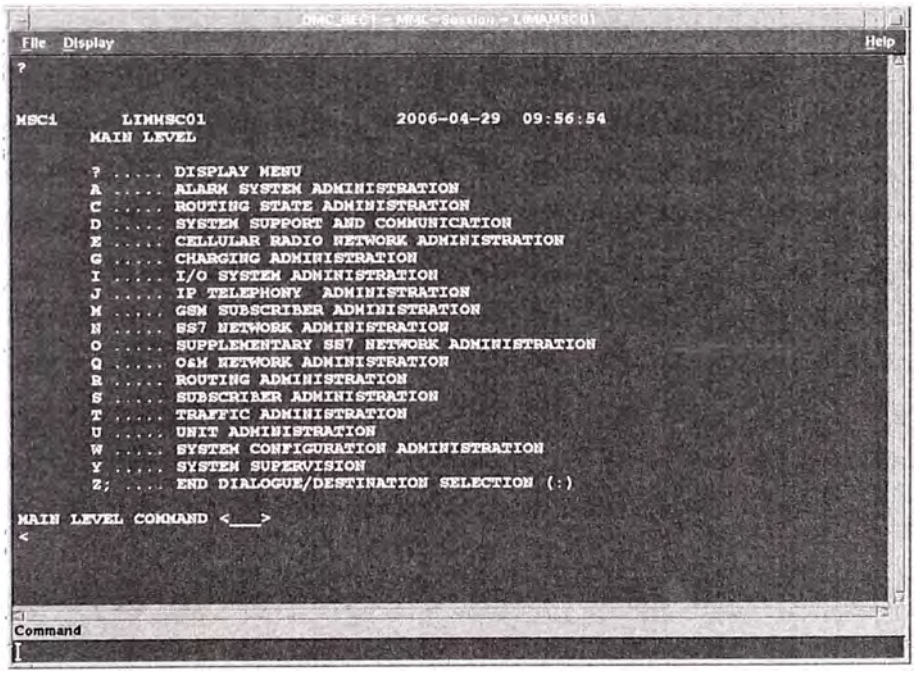


Figura 3.16: Interfase MML de conexión

3.2.5 Direccionamiento NSAP

La dirección NSAP permite a los equipos de telecomunicaciones comunicarse en un entorno multivendor "abierto". La dirección NSAP identifica un sistema, cada dispositivo capaz de usar la capa de transporte OSI y la ubicación geográfica basada en los códigos de datos (país) de esos ítems.

a) Direcciones NSAP

Las direcciones del Punto de acceso al servicio de red (NSAP) especifican la ubicación donde los usuarios tienen acceso a las capacidades de comunicación de la capa de red OSI.

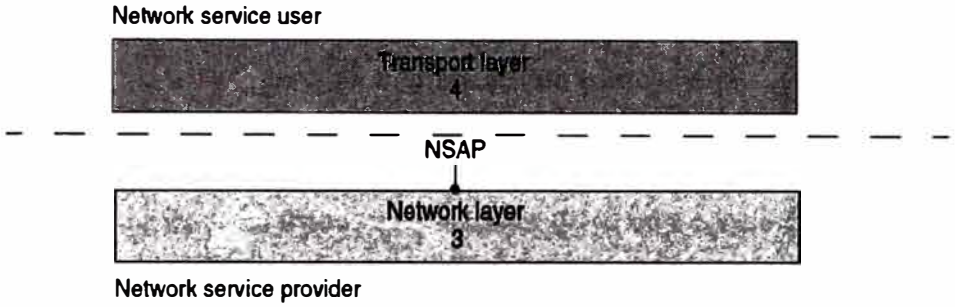


Figura 3.17: Ubicación del Punto de Acceso al Servicio de Red

Las direcciones NSAP son publicadas por los respectivos institutos de estándares de cada país. Después que una compañia recibe su identificador organizacional, ellos pueden asignar las direcciones NSAP dentro de su rango de direcciones.

Si un operador no ha recibido su identificador organizacional y tienen una red cerrada (sin acceso a la red pública de datos), el operador puede generar su propio identificador organizacional.

Desde un punto de vista práctico, las direcciones NSAP son encapsuladas en la información de control del protocolo. Esa información, la cual reside en la capa de red, es implementada por la Información de dirección del protocolo de red (NPAI) en la forma de una unidad de datos del protocolo de red.

La sintaxis y codificación de las direcciones NSAP son preservadas en la NPAI y son transportadas en las apropiadas Unidades de datos de protocolo (PDUs)

Estructura NSAP CLNS

La estructura CLNS NSAP puede ser vista desde 2 perspectivas, la información de enrutamiento y la información de administración de dirección. Aunque ambas

perspectivas usan la misma información, ellas son agrupadas de manera diferente. Por ejemplo, el protocolo de enrutamiento requiere la misma dirección de área para todos los elementos de red dentro de un área de enrutamiento.

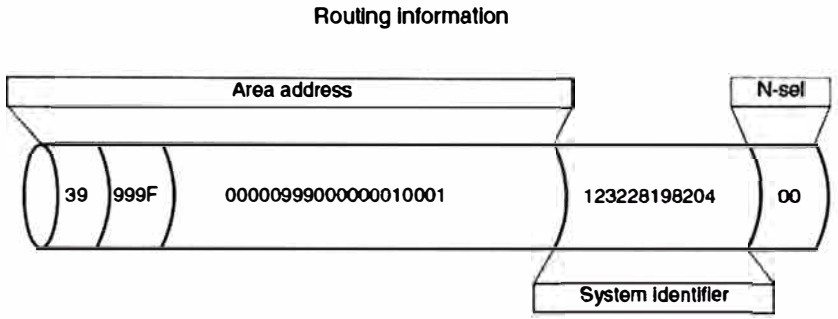


Figura 3.18: Información de enrutamiento

El identificador del sistema debe ser único porque éste identifica un específico elemento de red dentro de un área de enrutamiento. En lo que concierne al protocolo de enrutamiento, solo la parte del área de la dirección NSAP es significante.

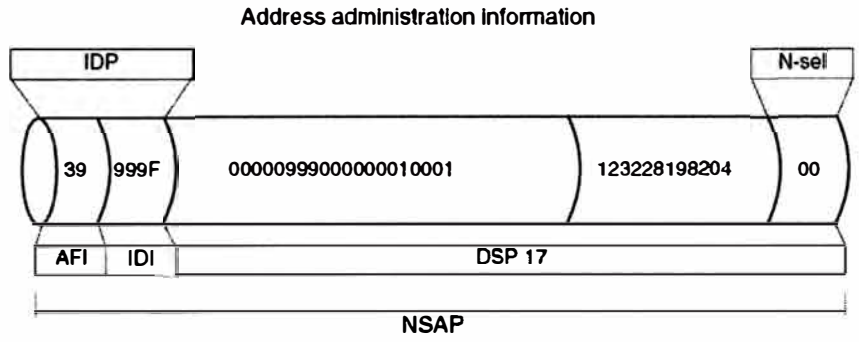


Figura 3.19: Información de administración de dirección

La red de comunicación de datos del Sistema de Administración de red de NOKIA, NetAct DCN, soporta los siguientes formatos de direcciones:

Código de datos NSAP del país

Designador internacional del código NSAP

Código de datos NSAP del país

El Código de datos NSAP del país (DCC) define la asignación de dirección geográfica de acuerdo a ISO, 3166.

PAKISTAN	PK	PAK	586
PALAU	PW	PLW	585
PALESTINIAN TERRITORY, Occupied	PS	PSE	275
PANAMA	PA	PAN	591
PAPUA NEW GUINEA	PG	PNG	598
PARAGUAY	PY	PRY	600
PERU	PE	PER	604
PHILIPPINES	PH	PHL	608
PITCAIRN	PN	PCN	612
POLAND	PL	POL	616
PORTUGAL	PT	PRT	620
PUERTO RICO	PR	PRI	630

Figura 3.20: Código del Perú, según el ISO 3166

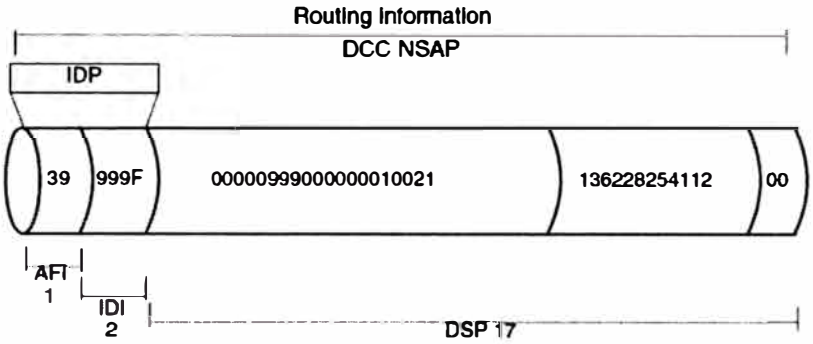


Figura 3.21: Estructura DCC NSAP

Tabla 3.4: Formato del Código de datos NSAP del país

NSAP part	Size in octets	Explanation
IDP	3	Initial Domain Part. Identifies the organisation designated as the addressing authority. The IDP consists of two parts. • AFI • IDI
AFI	1	Authority and Format Identifier • Identifies the authority responsible for allocating IDI values • specifies the format of the IDI(ISO DCC, ISO ICD, and X.121) • specifies the syntax of the DSP (binary or decimal) The value 39 indicates a DCC NSAP.
IDI	2	Initial Domain Identifier • identifies the subdomain that DSP values are allocated • identifies the authority responsible for the structure and assignment of DSP values • also referred to as the data country code
DSP	17	Domain-specific Part

La parte específica del dominio (DSP) es una combinación de la información topológica y administrativa. Los componentes del DSP son:

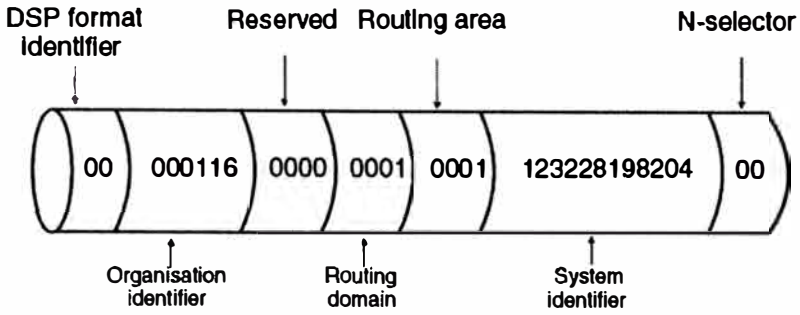


Figura 3.22: Estructura DSP

Tabla 3.5: Formato del DSP para un DCC NSAP

DSP field	Size in octets	Explanation
DSP format identifier	1	Defines the structure and administrative requirements for the rest of the DSP. Any value can be used. 00 is recommended.
Organisation identifier	3	Identifies the authority responsible for the organisation of ESs and ISs. Also known as the: • organisation code (DCC) • administrative authority identity (ICD) These codes are controlled by national authorities.
Reserved	2	Not used
Routing domain	2	Identification of the routing domain within the administrative domain
Routing area	2	Identification of the subdomain within the routing domain
System identifier	6	Identifies the end or intermediate system. We recommend using the C number of a network element or the IP address of a router/server.
N-selector	1	Identifies the user of the network layer transport service.Interpreted locally (not part of the routing information).

Designador internacional del código NSAP (ICD)

El formato común para el Designador del código internacional (ICD) NSAP que define la asignación de la dirección geográfica se realiza de acuerdo al ISO 6523.

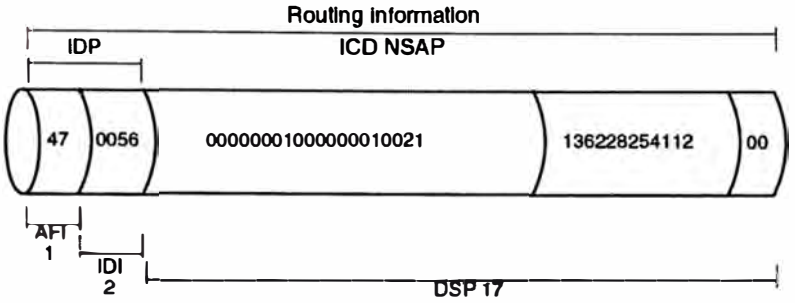


Figura 3.23: Estructura ICD NSAP

b) Uso de las direcciones NSAP en el Sistema de administración de red

En la práctica, el sistema de administración de red de NOKIA, utilizará 2 tipos diferentes de direcciones NSAP: Direcciones NSAP física y del paquete (en el sistema será llamado osspkg). La dirección NSAP física identifica los sistemas de cómputo (servidores) y sus interfases. La dirección NSAP del paquete identifica al paquete Service Guard de Hewlett Packard (osspkg). El Sistema de gestión de red utiliza la estructura DCC NSAP para identificar las direcciones física y del paquete.

Uso de conexiones LAN

El sistema de administración de red de utiliza solo conexiones LAN en el entorno local. La siguiente figura ilustra el uso de las conexiones LAN sobre CLNS:

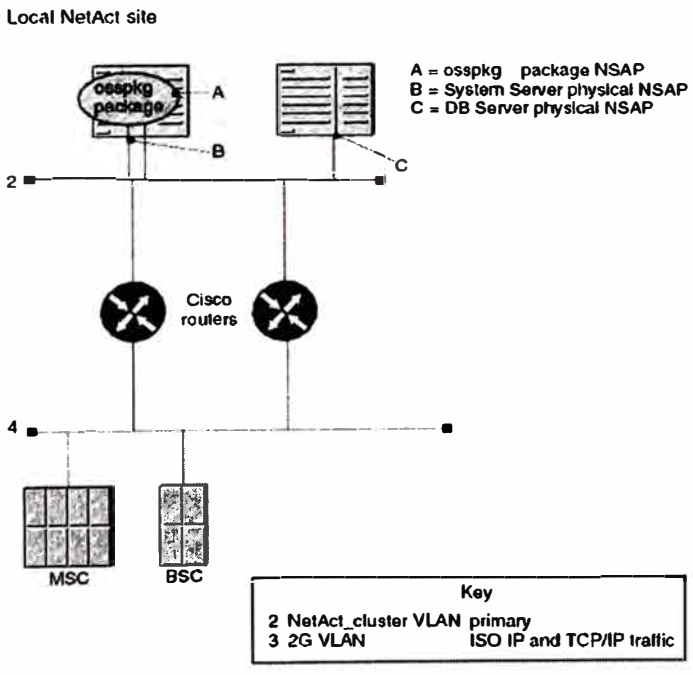


Figura 3.24: Usando CLNS sobre LAN

Selectores OSI

Existen 3 capas encima de la capa de red OSI que requieren información de direccionamiento: Transporte, Sesión y Presentación. En la terminología OSI éstas direcciones son llamadas Selectores N, donde N = Una capa OSI. Los selectores correspondientes son llamados T, S y P. En un sistema abierto, la combinación de estos selectores únicamente identifica una Entidad de aplicación (AE).

Los selectores N son usados para encaminar conexiones a través de las capas OSI. La dirección NSAP junto con los selectores T, S y P constituyen un Punto de acceso al servicio de presentación (PSAP) o dirección de presentación. La siguiente figura ilustra el uso de selectores en el enrutamiento OSI:

Figura 3.25: Usando CLNS sobre LAN

Después que las direcciones NSAP son asignadas, se deben distinguir todos los elementos del servicio OSI que usan una dirección NSAP común asignando valores únicos de selector.

La identificación de aplicación está usualmente basada en el Punto de acceso al servicio de presentación (PSAP), pero es también posible usar información de identificación adicional. Si varias aplicaciones están identificadas con una dirección de presentación común, la actual selección está basada en los Títulos de entidad de aplicación (AETs).

Un AET consiste de una Título de proceso de aplicación (APT) y un Calificador de entidad de aplicación (AEQ). La estructura del APT puede ser un nombre de directorio o un identificador de objeto. En los sistemas DX200, una aplicación local es siempre identificada con una dirección de presentación. Solo las aplicaciones remotas pueden requerir valores AET.

3.3 Principios de Networking

El procedimiento para el planeamiento de una red de comunicación de datos es determinado por la topología de red. Las topologías de red definen la capa de cableado para la red. En el sistema de administración propuesto, es recomendado que los elementos de red local estén conectados a dicho sistema con LAN.

Existen varios métodos para establecer las conexiones WAN:

- Conexiones a sitios remotos sobre línea serial usando el protocolo de Control de enlace de datos de alto nivel (HDLC) o el Protocolo punto a punto (PPP).
- Tunnelling ISO IP sobre TCP/IP entre los sitios remotos y locales.
- Conexión ATM (usando IMA o STM-1) a los elementos de red RAN (Radio Access Network – 3G).
- Conexión X25 a los elementos de red GSM (PCM / PSN).

Una vez que la topología de red es definida, se tiene que identificar los servicios y protocolos de red a ser usados.

Interfases de red:

Las interfases proveídas por el backbone DCN son las siguientes:

- Interfases LAN:
  IEEE 802.3 10/100 Mbps
- Interfases WAN:
  E1
  ATM IMA 4 puertos E1
  ATM STM-1 multimodo o monomodo
  Serial síncrono

3.3.1 Protocolos e interfases de administración

a) Interfases de administración

A continuación se lista los protocolos utilizados para manejar las diferentes partes de la red.

Administración del backbone DCN:

SNMP, Telnet, http y FTP.

Administración de red GSM:

Q3, MML, Q1, RPC y XML sobre HTTP.

Administración de la red de paquetes:

Q3, SNMP, Telnet, SSH, FTP y HTTP.

Administración de red 3G:

CORBA, Q1 (transmisión), Telnet, SSH, FTP, HTTP y XML sobre HTTP.

b) Protocolos

Los siguientes protocolos son soportados por la solución del backbone de la red de comunicación de datos:

Protocolos de red:

TCP/IP e ISO IP.

Protocolos WAN:

HDLC (entro routers Cisco), PPP, X25 y ATM.

Protocolos de enrutamiento:

OSPF e IS-IS.

TCP/IP

El protocolo IP consiste de un conjunto de protocolos de comunicación. Entre éstos, los más populares son el Protocolo de control de transmisión (TCP), Protocolo de datagrama de usuario (UDP) y el Protocolo de Internet (IP).

Protocolo de resolución de dirección (ARP):

El ARP permite a 2 hosts IP, ubicados en una subred IP dada, a comunicarse el uno con el otro. ARP permite a los hosts IP a determinar dinámicamente las direcciones MAC de los otros hosts para que la comunicación sea posible.

Protocolo de control de mensajes de Internet (ICMP):

El ICMP es un protocolo de capa de red que reporta errores y es usado para control y administración de red.

Protocolo de control de Transmisión (TCP):

El TCP es un protocolo de capa de transporte que provee transmisión orientada a conexión confiable de datos entre hosts IP. Los principales servicios proveídos por el TCP son:

Transferencia de datos stream
Confiabilidad
Control de flujo
Operación full duplex
Multiplexación

Protocolo de datagrama de usuario (UDP):

El UDP es un protocolo de capa de transporte no orientado a conexión. Es el opuesto al TCP en el sentido que no garantiza que la entrega de datos esté libre de errores. El UDP confía de los protocolos de capas más altas cuando los errores ocurren durante la transmisión de datos.

Protocolo de capa de aplicación IP:

El protocolo TCP/IP tiene un rango amplio de protocolos de capa de aplicación el cual incluye lo siguiente:

- Protocolo de transferencia de archivos (FTP): Usado para la transferencia de archivos entre hosts IP.
- Protocolo de administración de red simple (SNMP): Usado para manejar y monitorear los nodos en la red IP.
- Telnet: Protocolo de emulación de Terminal que provee servicios de conexión de terminal remoto.
- Sistema de archivos de red (NFS): Protocolo distribuido para el compartimiento de archivos de sistema.
- Llamada de procedimiento remoto (RPC): Conjunto de procedimientos para implementación de arquitectura cliente / servidor en programación distribuida.
- Sistema de nombres de dominio (DNS): Usado para trasladar los nombres de nodos de red a direcciones de red.

3.3.2 Enrutamiento (Routing)

El routing es el movimiento de información a lo largo de una red desde un origen hacia un destino. A lo largo del trayecto, al menos un nodo intermedio es típicamente encontrado. La decisión de la correcta ruta es hecha en cada nodo basado en la dirección IP del paquete.

a) Procedimiento de entrega del paquete IP

El procedimiento de entrega del paquete IP depende de la ubicación del transmisor y del receptor. Si ambos están ubicados en la misma red de área local (LAN), no existe necesidad de la funcionalidad de enrutamiento IP. En la misma LAN, el paquete puede ser enviado directamente al receptor usando la dirección ethernet del receptor. El protocolo de resolución de dirección (ARP) es usado para encontrar la dirección ethernet de un receptor en la misma LAN.

Si el origen y el destino están ubicados en diferentes LANs, se necesita una funcionalidad de enrutamiento externo para transferir paquetes IP desde el transmisor al receptor. El paquete IP es enviado al router, el cual encamina el paquete a su destino correcto.

La decisión del destino correcto está basada en la información de la tabla de enrutamiento. Cada fila de la tabla de enrutamiento IP contiene una entrada para cada red que es conocida por el router que está almacenando ésta tabla. Las tablas de enrutamiento son configuradas manualmente por el administrador del sistema o automáticamente usando un adecuado protocolo de enrutamiento.

b) Enrutamiento estático

El enrutamiento estático es realizado usando una tabla de enrutamiento preconfigurada. Las tablas de enrutamiento estático son configuradas manualmente, usualmente por un administrador de sistema. Este es la forma más básica de enrutamiento. Usualmente se requiere que todos los dispositivos tengan configuración de dirección estática.

Un requerimiento adicional es que todos los dispositivos permanezcan en sus respectivas redes. Sino, las tablas de enrutamiento tienen que ser alteradas manualmente en uno o más dispositivos para reflejar los cambios en la topología de red o direccionamiento.

c) Enrutamiento dinámico

El enrutamiento dinámico utiliza protocolos de enrutamiento de información especial para actualizar automáticamente la tabla de enrutamiento con rutas conocidas por los routers. El protocolo de enrutamiento, es el método usado por los routers para intercambiar información, forma la base para proveer una conexión a través de una red.
Los protocolos de enrutamiento pueden ser divididos en 2 categorías: Protocolos de acceso interior (IGP) y los protocolos de acceso exterior (EGP).

Los protocolos de acceso interior son usados para distribuir información de enrutamiento dentro de un Sistema autónomo (AS).

Un sistema autónomo es un conjunto de routers dentro de un dominio administrado por una autoridad. Los ejemplos de IGPs son los protocolos OSPF y el RIP.

Los protocolos de acceso exterior, tales como el BGP, son usados para enrutamiento inter-AS. Con los EGPs, cada sistema autónomo (AS) puede alcanzar otros sistemas autónomos a través de las redes.

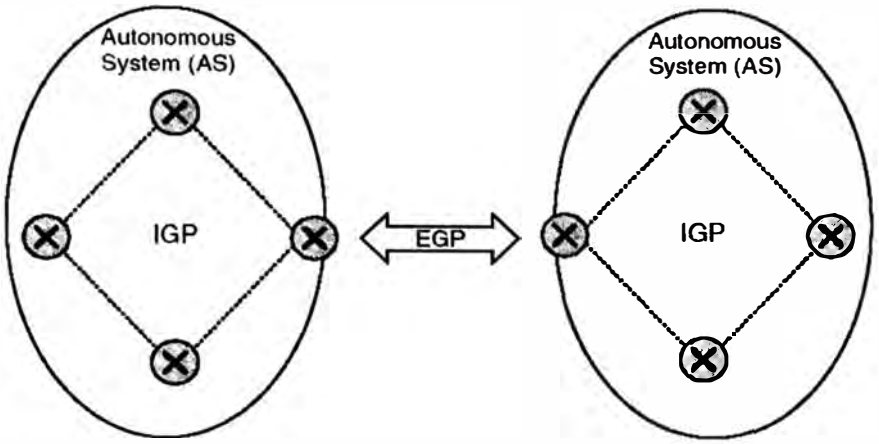


Figura 3.26: Protocolos IGPs y EGPs

d) Enrutamiento OSPF

El OSPF es un protocolo de enrutamiento que envía mensajes del estado de conexión (LSAs) a otros routers dentro de la misma área jerárquica. Los LSAs OSPF incluyen información sobre interfases conectadas, métricas usadas y otras variables. Cuando los routers con OSPF acumulan información del estado de conexión, ellos usan el algoritmo SPF (Shortest Path First) para calcular la ruta más corta a cada nodo.

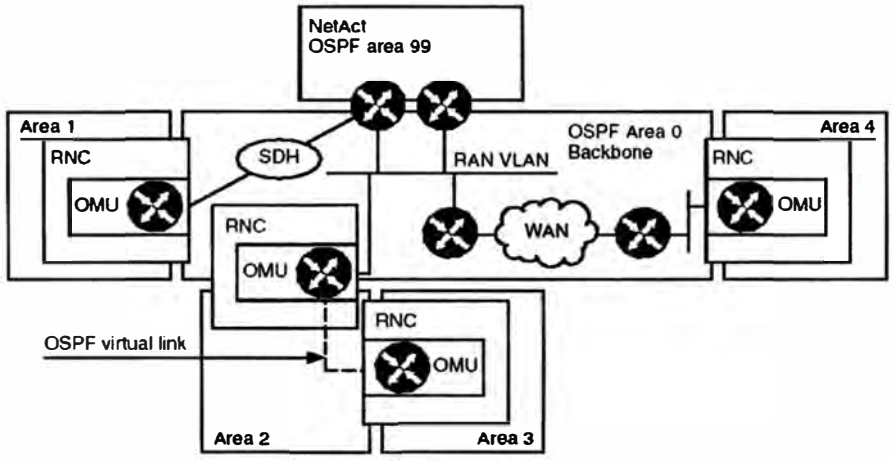


Figura 3.27: Enrutamiento OSPF en el backbone DCN

e) Diferentes routers con OSPF

Router interno: Dentro de un área, el router mantiene una base de datos precisa y actual de cada subred dentro del área y desvía los datos a otras redes por la ruta más corta. Las actualizaciones de los enrutamientos serán confinados al área.

Router backbone: El diseño de las reglas para OSPF requiere que todas las áreas sean conectadas a través de una sola área conocida como el área backbone o área O. Un router dentro de ésta área es referido como router backbone. Este puede también ser un router interno o un router de borde de área (area border router).

Router de borde de área (ABR): Este router es responsable de conectar 2 o más áreas. Este mantiene una base de datos completamente topológica por cada área que ésta conectada a éste, y envía las actualizaciones de los Mensajes de estado de conexión (LSAs) entre áreas. Estas actualizaciones de LSAs son resúmenes de actualización de las subredes dentro de un área.

La sumarización o resumen para el OSPF debe ser configurada como área de borde (border area), porqué es donde los LSAs hacen uso de las actualizaciones de enrutamiento reducidas para minimizar la sobrecarga del enrutamiento en las redes y routers.

Router de frontera del sistema autónomo (ASBR): Los ASBRs son usados para conectarse al mundo externo, o a cualquier otro protocolo de enrutamiento.

f) Diferentes tipos de áreas

Área ordinaria o estándar: Esta área se conecta al backbone y es vista como una entidad independiente. Cada router conoce acerca de cada red en el área y cada router tiene la misma base de datos topológica.

Área stub: Es un área que no acepta rutas externas (LSA tipo 5). Este tipo de rutas no pueden ser anunciadas en el área o no pueden ser generadas desde las áreas de los routers. Si los routers alcanzan redes externas, ellos dependerán de la ruta por defecto.

Área totally stub: Esta área no acepta rutas internas (LSA tipo 5) ni externas (LSA tipo 3 y 4). Si los routers alcanzan un destino fuera del área, ellos dependerán de la ruta por defecto.

Enlace virtual: Si la nueva área no puede conectarse directamente al área backbone, un router es configurado para conectarse a un área que tiene conectividad directa.

3.3.3 Interconexión de Sistemas Abiertos (OSI)

La interconexión de Sistemas abiertos representa una familia de protocolos y estándares creados por la Organización internacional para la Estandarización (ISO). Estos protocolos son usados para conectar diferentes sistemas de red.

El propósito del OSI es proveer una base común para la coordinación del desarrollo de estándares para la interconexión de sistemas. Debido a que OSI está enfocado al intercambio de información entre sistemas abiertos, los otros aspectos no relacionados a la interconexión están fuera del enfoque de OSI.

El término "abierto" se refiere a los sistemas que usan, desarrollan y soportan herramientas de interconectividad basados en los estándares establecidos por ISO y la ITU-T (formalmente la CCITT).

a) Modelo de referencia y capas OSI

El modelo de referencia OSI define un grupo de protocolos de 7 capas para la comunicación entre aplicaciones OSI. Este modelo incluye protocolos de aplicación estandarizados para varios servicios y modos de comunicación.

Aunque el enfoque del modelo de referencia OSI es muy amplio, éste modelo es enfocado primariamente a sistemas que tienen terminales, computadoras y dispositivos que transfieren información entre sistemas abiertos. Las redes de comunicación de datos deben seguir el modelo de referencia OSI para las aplicaciones ITU-T como se estipula en ITU-T, M.3010.

La siguiente figura ilustra las 7 capas del modelo de referencia OSI:

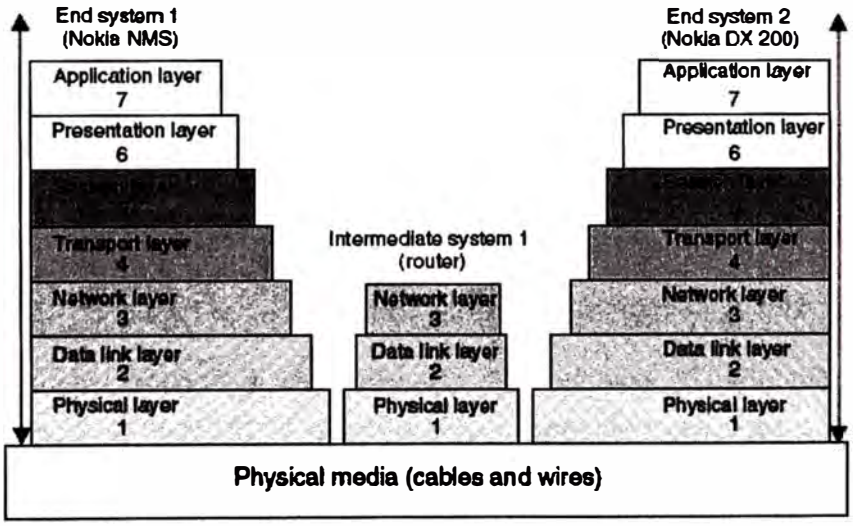


Figura 3.28: Modelo de referencia OSI – 7 capas

Cada objeto en el modelo de referencia OSI está dividido en 7 capas jerárquicas. Aunque cada capa es distinta, ellas dependen de la capa (N-1) para realizar funciones que son prerequisitos para llevar a cabo sus tareas.

Capa de Aplicación

La capa de Aplicación provee acceso al entorno OSI. Esta capa provee los servicios requeridos para que una aplicación que corre en un sistema pueda interactuar con otra aplicación que corre en otro sistema. Las funciones realizadas en ésta capa incluyen el establecimiento del contacto entre procesos y condiciones de interacción.

La implementación de NOKIA acerca del modelo de referencia OSI se refiere primariamente a los elementos del servicio de aplicación que están ubicados en la capa de aplicación.

Elemento del servicio de aplicación (ASE): Los ASEs fueron diseñados para ayudar a las aplicaciones individuales a llevar a cabo tareas específicas. Aunque otros ASEs han sido definidos, la familia de productos de NOKIA, DX200, usa los siguientes elementos:

Elemento del servicio de información de administración común (CMISE): El CMISE es responsable de la transferencia de datos de administración de red entre el sistema de administración de red (MANAGER) y los elementos de red (AGENTES) usando el Servicio de red OSI sin conexión (CLNS). Las operaciones del CMISE son usadas:

Para recolectar estadísticas considerando mediciones, performance y otros factores que afectan la calidad de la red (Interfase del sistema de administración de red).

Para el manejo de alarmas. Los eventos de alarmas son enviados desde el elemento de red al sistema de administración de red para el monitoreo, filtrado y clasificación (Interfase del sistema de administración de red).

Para la administración del usuario.

Administración, acceso y transferencia de archivos (FTAM): El FTAM es responsable de proveer la facilidad de administración y transferencia de archivos sobre el servicio de red sin conexión (CLNS). La familia de productos DX200 y el sistema de administración de red de NOKIA pueden ser los que inician o los que responden a una

operación FTAM. Se requiere conocer acerca de la estructura del archivo y el lugar de almacenamiento. Las operaciones de FTAM son usadas:

Entre las mediciones y las aplicaciones de administración de software (Interfase del sistema de administración de red).
Entre las aplicaciones de charging (Interfase del centro de facturación).
Entre las aplicaciones del Registro de Identidad del Equipo Móvil (EIR) (Interfase de la central del Registro de Identidad del Equipo Móvil).

Terminal Virtual (VT): VT es responsable de proveer capacidades de conexión remota sobre un Servicio de red sin conexión (CLNS). Un elemento de red DX200 puede solo actuar como un equipo que responde en una conexión VT.

Capa de Presentación

La capa de presentación es responsable de convertir la información enviada por la capa de aplicación. Esta también es responsable del mantenimiento de la sintaxis y estructura de los datos.

Capa de Sesión

La capa de sesión establece y mantiene las conexiones entre las aplicaciones y maneja el diálogo entre ellas. Esta capa determina que lado está "hablando" y cual está "escuchando" en un momento dado, para asegurar que la interacción proceda de una manera ordenada.

Capa de Transporte

La capa de transporte es responsable de la comunicación punto a punto (end to end) entre sistemas, sin considerar sus características de red. La capa de transporte entrega información desde un proceso de aplicación a otro y enmascara cualquier falla de los servicios de red subyacentes. Los protocolos tales como el TP4 (Protocolo de transporte de clase 4) son usados en la capa de transporte.

Capa de Red

La capa de red es la primera capa que controla la comunicación entre computadoras más que los procesos. Es el responsable de la ubicación del dispositivo y donde un proceso remoto está ubicado. La capa de red es responsable del enrutamiento,

direccionamiento y control de flujo. Protocolos tales como el CLNP son usados en ésta capa.

Capa de Enlace de Datos

La capa de enlace de datos es responsable de la transmisión de datos sobre un enlace mientras se lleva a cabo la detección / corrección de error, control de flujo, secuencia de enlace y mantenimiento de la integridad del enlace. Los protocolos tales como el ethernet y el X.25 son usados en ésta capa.

Capa Física

La capa física establece como los bits son movidos desde un punto a otro sobre un medio físico. Esto incluye las especificaciones eléctricas o características de la señal óptica, conectores, codificación de señales digitales y sincronización. La característica de la capa física va más allá de los atributos físicos de las conexiones y el cableado. También se incluye el intercambio de los mensajes de control y procedimientos de "handshaking" (Donde una señal enviada debido a una función recibe una señal de respuesta).

La siguiente figura ilustra las aplicaciones y protocolos usados en un elemento de red DX200 (Familia de productos de Hardware NOKIA). Los protocolos usados en la capa física son por ejemplo: V.35, PCM E1, 10/100 Base T.

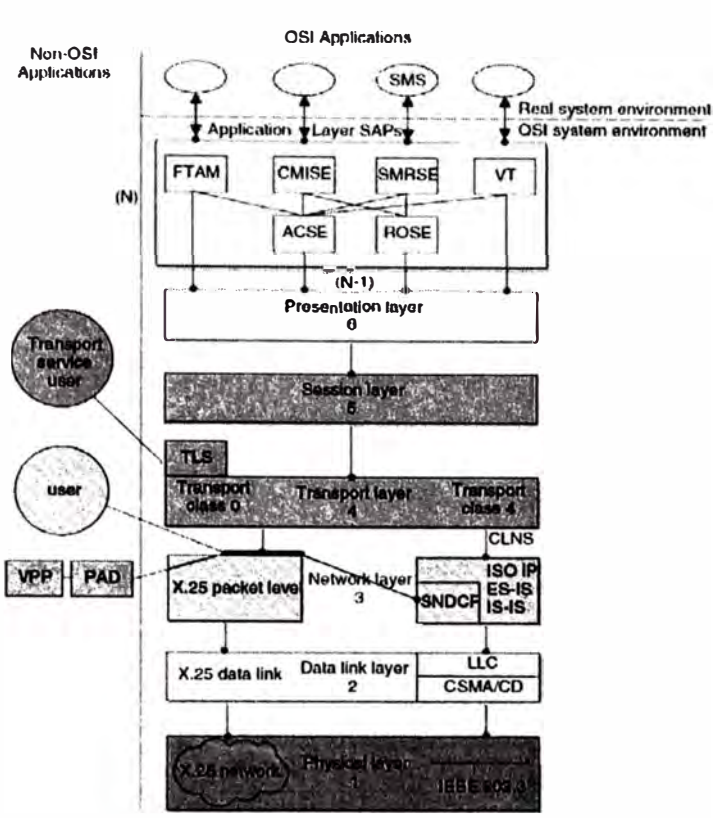


Figura 3.29: El Modelo OSI: Como funciona en un elemento de red DX200

b) Servicios OSI

Los elementos de red basados en DX 200 ofrecen un amplio rango de servicios OSI que proveen una variedad de soluciones de comunicación.

Servicio de capa de transporte (TLS)

El servicio TLS provee acceso a los servicios de la capa de transporte. Las aplicaciones definidas de usuario, como la transmisión celular vía la interfase Q1, pueden usar directamente los servicios de transferencia para la comunicación entre procesos.

El TLS también es usado con un Proveedor de transporte (TPP). El TPP provee aplicaciones con la capacidad para llevar a cabo conexiones punto a punto (end to end), independientemente de cualquier capa de protocolo de red, en la capa de transporte.

Este servicio corresponde al Servicio OSI de capa de transporte orientado a conexión (COTS).

Los usuarios TPP pueden solo iniciar una conexión vía X25 o LAN IEEE 802.3. Las conexiones no pueden ser hechas usando TCP/IP.

c) Interoperabilidad de protocolos OSI

Para asegurar una satisfactoria operación de la red, se debe evaluar todo el equipamiento de comunicación (Hardware y Software) y verificar que la comunicación punto a punto pueda ser establecida entre elementos de red.

Cuando se considera una transferencia FTAM desde el sistema A al sistema B, se debe asegurar que:

- Ambos sistemas tienen una implementación FTAM mutuamente compatible.
- La comunicación de red entre los sistemas A y B soportan comunicación de datos OSI. El servicio de red proveído es sin conexión (CLNS).
- Los permisos necesarios para la transferencia de archivos están en orden.

La siguiente tabla lista las aplicaciones OSI más comunes y sus equivalentes TCP/IP:

Tabla 3.6: Términos TCP/IP y sus equivalentes OSI

TCP/IP	OSI	Explanation
Host	ES	End System
Router	IS	Intermediate System
OSPF	IS-IS	Intermediate System to Intermediate System
SNMP	CMISE	Common Management Information Service Element
FTP	FTAM	File Transfer, Access, and Management
Telnet	VT	Virtual Terminal
RPC	ROSE	Remote Operation Service Element

d) Servicios de Transporte OSI (OTS)

En el diseño se considerará los servicios de transporte OSI de HP (Hewlett Packard) para servidores HP 9000. Los servicios de transporte OSI de HP son paquetes de software de red que incluyen los siguientes componentes:

- Elemento del servicio de control de asociación (ACSE).
- Elemento del servicio de operación remota (ROSE).
- Capa de presentación OSI.
- Capa de sesión OSI.
- Capa de transporte OSI.
- Capa de red OSI.
- Servicio de red sin conexión (CLNS).

El OTS/9000 provee servicios de capa de red OSI sobre enlaces X25 o LAN. Estas capas suministran los fundamentos necesarios para correr servicios OSI como FTAM o CMIP (CMIP).

CAPITULO IV

DESCRIPCIÓN DE LOS ELEMENTOS DE LA RED DE TELEFONÍA CELULAR

4.1 Descripción de los elementos de red BSS

4.1.1 Descripción del Controlador de Estación Base (BSC)

El subsistema de estación base de NOKIA consiste del Controlador de estación base (BSC), submultiplexor transcoder (TCSM), la estación base (BTS), transmisión celular (CT) y planeamiento de red.

El Controlador de estación base (BSC) está diseñado para el eficiente uso de los recursos de radio, fácil operatividad y mantenimiento. También está diseñado para reunir y transmitir información completa acerca de la calidad de servicio. Además de ser un producto maduro y estable de alta confiabilidad y funcionalidad variable, el BSC de NOKIA es de costo eficiente y tiene alta capacidad.

El BSC de NOKIA proporciona la conexión entre la MSC, las BTSs y el SGSN. La principal función del BSC es controlar y manejar los canales de radio y el subsistema de estación base. Este transfiere información de señalización hacia y desde el equipo móvil y maneja los handovers entre celdas.

El BSC está basado en las estructuras modulares de software y hardware. La arquitectura distribuida del BSC está implementada por un sistema multiprocesador. En un sistema multiprocesador, la capacidad del procesamiento de datos está dividida entre varias unidades de computadoras (unidades funcionales), en donde cada una posee su propia microcomputadora.

Como la capacidad del manejo de llamadas del BSC depende del número de unidades de computadoras para el control de llamadas, el sistema puede ser flexiblemente dimensionado de acuerdo a la capacidad de demanda del operador. Y cuando existe necesidad para expandir la capacidad, el sistema puede ser fácilmente expandido adicionando nuevas unidades a la configuración existente.

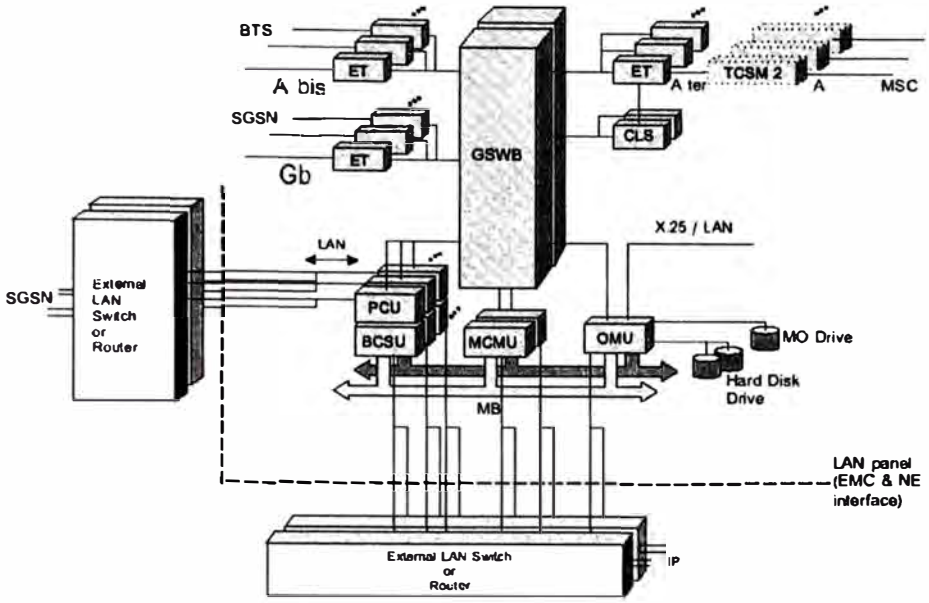


Figura 4.1: Diagrama de bloques del BSC DX200

El BSC es un elemento de red en el subsistema de estación base (BSS) tolerante para redes GSM800, GSM900, GSM1800 y GSM1900. Este elemento de red es conectado a los elementos de red circundantes con interfases PCM estándar y ofrece flexibilidad y eficiencia de costo en la transmisión. El BSC tiene una conexión X.25 y LAN hacia el sistema de administración de red llamada interfase Q3. La interfase Q3 es usada para la transferencia de datos entre el BSC y el sistema de administración de red.

a) Unidades funcionales del BSC

Las unidades funcionales están compuestas de módulos individuales de software y hardware. Estas son las siguientes:

El switch de grupo (GSWB) transmite el tráfico que pasa a través del BSC y los circuitos troncales. El switch de grupo también establece las conexiones necesarias a las unidades de señalización y los canales internos de transmisión de datos, y es responsable de las funciones de submultiplexación del BSC. El switch de grupo conmuta a un nivel de 8, 16, 32 y 64 kbit/s.

La unidad de señalización del controlador de estación base (BCSU) maneja las funciones de señalización del BSC. También es responsable de las siguientes tareas:

- Realizar las funciones distribuidas de la parte de transferencia de mensajes (MTP) y la parte de control de conexión de señalización (SCCP) de SS7.
- Controlar la señalización del móvil y la estación base (Parte de aplicación del Subsistema de estación base (BSSAP)).
- Realizar el manejo de mensajes y funciones de procesamiento de los canales de señalización conectados a éste.

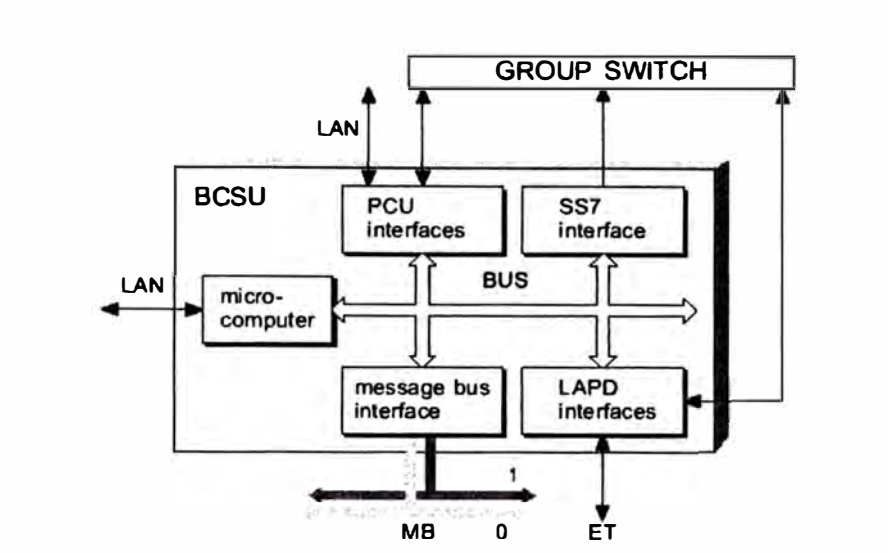


Figura 4.2: Estructura de la unidad BCSU

El marcador y unidad de administración celular (MCMU) controla y supervisa el GSWB e implementa funciones de administración de los recursos de radio (RRM), siendo responsable de las celdas y canales de radio. El MCMU también actúa como una unidad de mantenimiento de sistema en caso que la OMU falle (BSC SYM). Esta unidad está conectada a otras unidades de computadoras de la central, la OMU y el BCSU, a través del bus de mensajes. También realiza las funciones de control de la matriz de conmutación y las funciones de administración específicas del BSC de los recursos de radio.

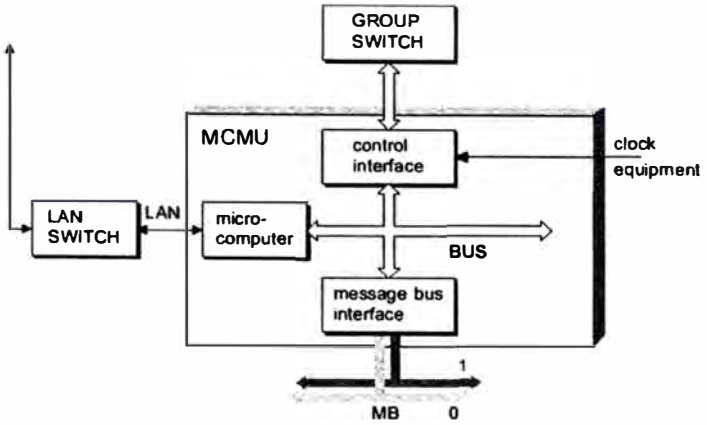


Figura 4.3: Estructura de la unidad MCMU

La unidad de control de paquete (PCU) tal como su nombre lo indica, maneja las funciones de control de paquetes en el BSC. La PCU realiza las tareas de procesamiento de datos que están relacionadas al tráfico (E)GPRS, es decir, maneja las funciones del control de paquetes GPRS en el BSC. Otras funciones principales son la administración de los recursos de radio del tráfico GPRS como por ejemplo, establecimiento y administración de conexión, asignación de recursos, transferencia de datos, control de potencia del enlace de subida (uplink) de la estación móvil, compartir la carga de la unidad Gb (uplink) y control de flujo (downlink).

La unidad de operación y mantenimiento (OMU) sirve como una interfase entre el usuario y el BSC, pero también supervisa automáticamente al BSC.

El bus de mensajes de alta velocidad (MB) interconecta las computadoras del control de llamadas y la OMU.

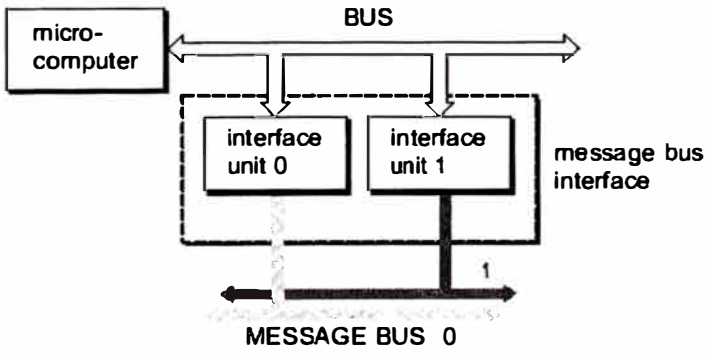


Figura 4.4: Estructura del bus de mensajes

Las terminales de intercambio (ET) conectan los sistemas de transmisión al GSWB. La terminal de intercambio realiza la sincronización eléctrica y la adaptación de líneas PCM externas. También realiza la codificación y decodificación HDB3, B8ZS o AMI, inserta bits de alarma en la dirección saliente y produce la estructura PCM.

Todas las interfases de 2.048 Mbit/s (ETSI) o 1.544 Mbit/s (ANSI) para la MSC, el SGSN y las BTSs están conectadas a las terminales de intercambio (ET). La ET adapta los circuitos PCM externos al Switch de Grupo y los sincroniza al reloj del sistema.

En la dirección entrante, la ET decodifica la señal de 2.048 Mbit/s (ETSI) o 1.544 Mbit/s (ANSI) de un circuito en señales de datos. El decoder realiza la decodificación del código de línea (HDB3 en el entorno ETSI, B8ZS o AMI en el entorno ANSI) en forma binaria. Al mismo tiempo, la ET es sincronizada a la tasa en bits de la señal entrante.

En la dirección saliente, la ET recibe una señal binaria PCM de la red de conmutación y genera el frame con la estructura PCM. La señal resultante es convertida en código de línea (HDB3 (ETSI), B8ZS o AMI (ANSI)) y se transmite en un circuito a 2.048 Mbit/s (ETSI) o 1.544 Mbit/s (ANSI).

La unidad de reloj y sincronización (CLS) distribuye las señales de referencia de sincronización a las unidades funcionales del BSC. Este puede operar plesiócronamente o sincrónicamente con las referencias de sincronización que recibe de las troncales digitales PCM. El oscilador del CLS es normalmente sincronizado a un origen externo, usualmente una MSC, a través de una línea PCM.

El transcoder TCSM2, aunque es un elemento de red separado el cual es usualmente instalado en el lado de la MSC, es normalmente visto como una unidad funcional del BSC.

Las unidades de conmutación (SWU) LAN, las cuales están conectadas a las interfases (CPUs y PCUs) con la subred ethernet interna establecida con conexiones duplicadas de cable. El switch LAN proporciona acceso a la red IP del operador en un primer nivel de switch LAN. Proporciona interfaces de enlace de subida (uplink) a la red IP.

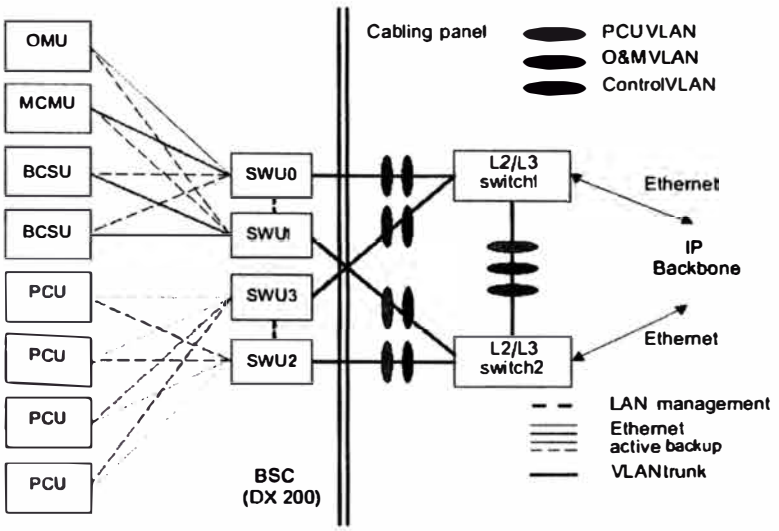


Figura 4.5: Ejemplo de conexiones LAN en el BSC

En el BSC GSM/EDGE, las funciones de control de llamadas son realizadas por microcomputadoras, llamadas Computadoras de control de llamadas. Estas computadoras tienen una Unidad central de procesamiento (CPU), la cual está basada en microprocesadores INTEL.

La unidad central de procesamiento (CPU) contiene un microprocesador y la Memoria de acceso aleatorio (RAM). Cada computadora de control de llamadas también contiene unidades adicionales que son requeridas para realizar tareas específicas.

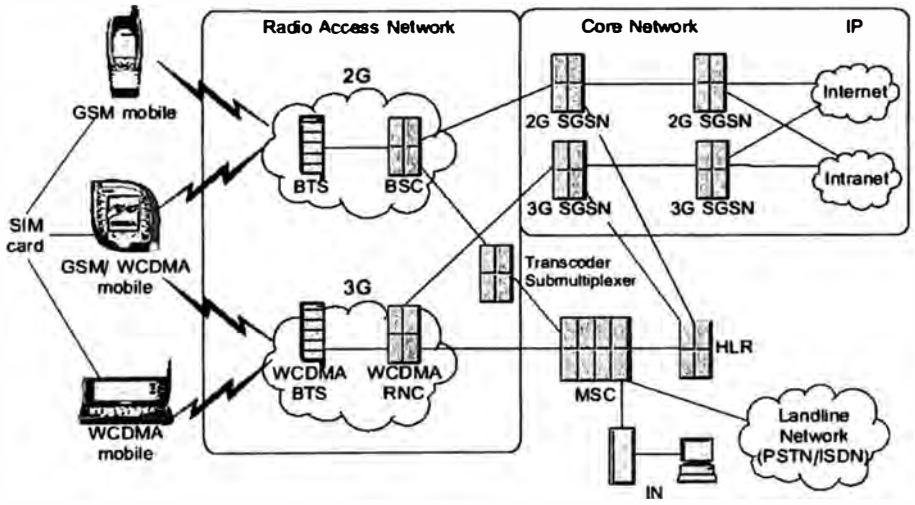


Figura 4.6: Descripción de la red GSM 1800/1900

El controlador de estación base (BSC) hace referencia a la familia de productos BSC GSM/EDGE, que proporcionan al operador el medio para el control de canales de radio. Ellos también controlan la señalización a las BTSs.

b) Características de la plataforma BSC de NOKIA

Las principales características del BSC son:

Plataforma confiable

- Procesamiento distribuido.
- Estructura modular.
- Tolerancia a fallas.
- Procesadores actualizables.

Fácil operatividad

- Buena operatividad en línea.
- Modelo de protocolos OSI para funciones de operación y mantenimiento.
- Amigable interfase MML de acuerdo a las recomendaciones ITU-T.

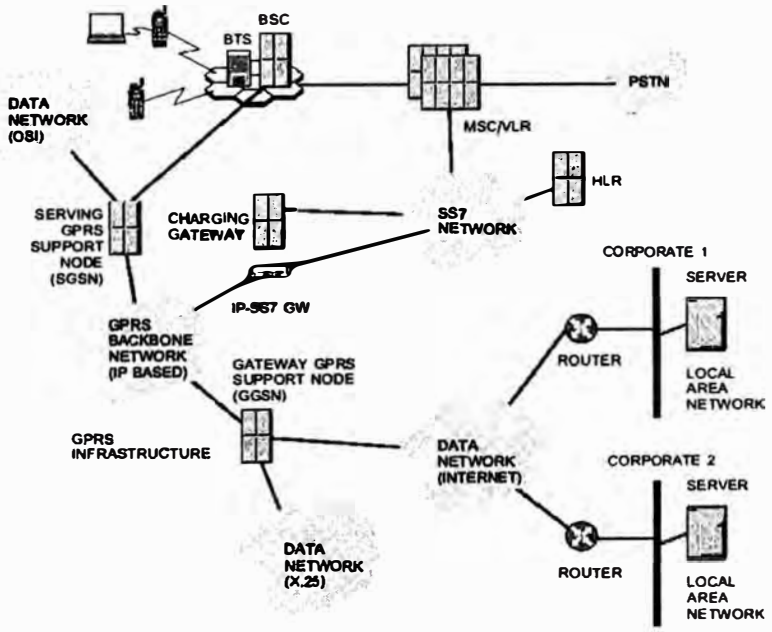


Figura 4.7: Descripción del BSC en una red GPRS

Configuración flexible

- Expansión de TRXs en configuraciones del BSC de alta capacidad.
- La arquitectura modular permite construir sistemas de conmutación económicamente dimensionados de acuerdo a las necesidades.

Sin requerimientos especiales de sitio

- Los BSCs son pequeños y compactos con bajo consumo de potencia.
- El enfriamiento del BSC es implementado por medio de convección natural.

c) Funcionalidades del BSC

Administración de canales terrestres

- Indicación del bloqueo de los canales de la interfase A entre el BSC y la MSC.
- Asignación de canales de tráfico entre el BSC y las BTSs.
- Soporte para los circuitos de la interfase A.
- Soporte para la asignación flexible de canales, por ejemplo, half rate y high speed en circuitos conmutados de datos.

Administración de los canales de radio

- Administración de las configuraciones de los canales, es decir, cuantos canales de tráfico y canales de señalización pueden ser usados en el subsistema de estación base. Esto es hecho en conexión con la configuración de la red de radio.
- Administración de los canales de tráfico (TCH) y canales de control dedicado stand-alone (SDCCH). Esta función puede ser dividida en las siguientes tareas: Administración de recursos, asignación de canales, supervisión de enlaces, liberación de canales y control de potencia.
- Administración de los canales de control de broadcast (BCCH) y canales de control común (CCCH). Esta función puede ser subdividida en las siguientes tareas: Administración de canales, acceso random, paging, etc.
- Administración del salto de frecuencia (frecuency hopping). El BSC está a cargo de la administración del salto de frecuencia el cual permite el uso efectivo de los recursos de radio y la calidad de voz mejorada para un abonado GSM.

- Handovers. La frecuencia del móvil es cambiada en conexión con los handovers, los cuales son ejecutados y controlados por el BSC. Los handovers pueden ser uno de los siguientes tipos:
  - Intra BSC, intra celda: El cual significa que el handover toma lugar dentro de un área controlada por el BSC y el móvil permanece en la misma celda
  - Intra BSC, inter celda: El cual significa que el móvil permanece en la misma área del BSC pero se mueve de una celda a otra
  - Inter BSC entrante y saliente: El cual significa que el móvil se mueve en un área de otro BSC

Administración de los canales de señalización entre el BSC y las BTSs

- El BSC supervisa las conexiones permanentes (punto a punto) de señalización LAPD de 16, 32 o 64kbps, que consiste de una conexión por unidad de transceiver (TRX) y de operación y mantenimiento de la BTS (OMU).

Mantenimiento

- El BSC ofrece los siguientes procedimientos de mantenimiento: Localización de falla del BSC, reconfiguración del BSC, soporte de reconfiguración de la BTS y actualización del software en el BSC, TCSM2 y BTS.

Operación

- Durante la operación normal, el BSC ofrece varias posibilidades para el operador: Modificación de los parámetros del BSC y la BTS, modificación de los parámetros de la red de radio, configuración del hardware del BSC y administración del equipamiento del BSC.

Interfase de usuario

- El BSC tiene una interfase de usuario amigable con mensajes en texto y comandos, los cuales son fácil de aprender y usar. La interfase de usuario cumple con las recomendaciones de la ITU-T.

Mediciones y observaciones

- Para minimizar los costos y maximizar la calidad de servicio hacia el abonado, se necesita información acerca de la performance y nivel de servicio en la BSC y la red de radio. La información usual, es por ejemplo, cuanto tráfico llevan las diferentes celdas, si existe congestión en los canales SDCCH o TCH

y cuantos handovers son satisfactorios y cuantos fallan. Las mediciones de tráfico proporcionan ésta información.

d) Unidad de operación y mantenimiento

La unidad de operación y mantenimiento (OMU) es una interfase entre el BSC y el sistema de administración de red como el NOKIA NetAct y/o el usuario. La OMU recibe indicaciones de falla (alarmas) desde el BSC. También puede producir alarmas locales y enviar las alarmas de fallas del BSC hacia el sistema de administración de red. En un evento de falla, la OMU activa automáticamente la recuperación apropiada y los procedimientos de diagnóstico dentro del BSC. La recuperación puede también ser activada por la MCMU en caso que la OMU falle.

Las tareas de la unidad de operación y mantenimiento pueden ser divididas en 4 grupos:

- Funciones de control de tráfico.
- Funciones de mantenimiento.
- Funciones de administración de la configuración del sistema.
- Funciones de administración del sistema.

La OMU consiste de microcomputadoras, de manera similar a las computadoras de control de llamadas. En adición, la OMU contiene interfases de entrada y salida (I/O) para operación local.

La OMU consiste de los siguientes módulos:

- Microcomputadora.
- Interfase de alarmas.
- Interfase del bus de mensajes.
- Interfase de dispositivo periférico.
- Interfase X25 analógica opcional (MODEM).
- Interfase X25 digital opcional (interfase de operación y mantenimiento basado en intervalos de tiempo).
- Interfase ethernet.

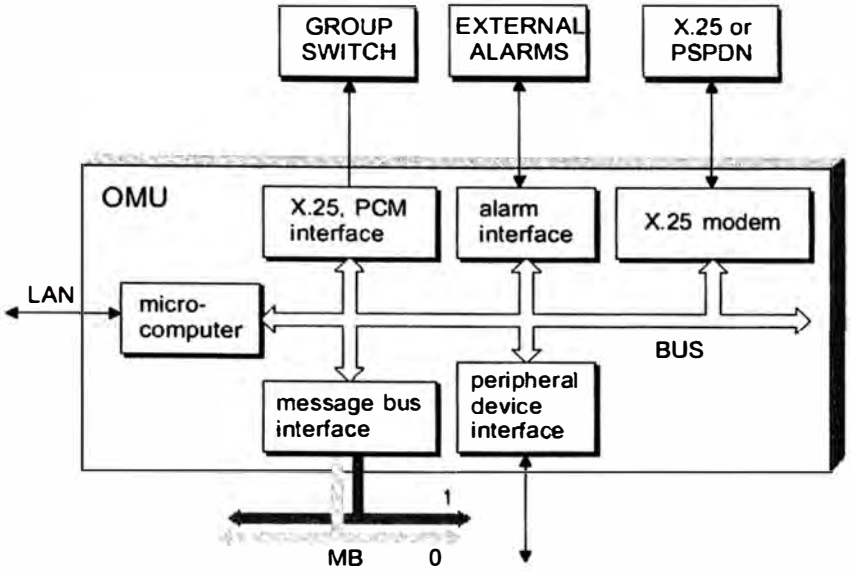


Figura 4.8: Estructura de la unidad OMU

El módulo de interfase de alarmas conecta las alarmas internas a la OMU desde la fuente de energía eléctrica, equipo de aire acondicionado, etc. del BSC. Este módulo proporciona interfases de entrada y salida para las alarmas externas hacia el sistema de administración de red. La OMU se comunica con las computadoras de control de llamadas vía el bus de mensajes.

La unidad central de procesamiento controla el módulo interfase del dispositivo periférico, el cual es usado para conectar las unidades de disco, unidades de display e impresora a la OMU. Existe redundancia en las unidades de disco duro y disco magneto óptica los cuales son controlados por la OMU.

La interfase de modem X25 analógica proporciona una interfase DTE X25 para la red conmutada de paquetes con una capa física V24, V35 o X21.

El módulo de la interfase de operación y mantenimiento X25 digital basado en PCM es utilizado para las interfases de la administración de red implementados en intervalos de tiempo. Este módulo proporciona una conexión X25 vía el intervalo de tiempo de la interfase A.

La interfase LAN proporciona una interfase ethernet de acuerdo al estándar IEEE 802.3. Estas interfases están ubicadas en las tarjetas de las CPUs.

4.1.2 Descripción del Transcoder y Submultiplexor (TCSM)

El TCSM2 es el término general de la segunda generación del elemento de red Transcoder y Submultiplexor. TCSM2A es la versión del TCSM para ANSI (USA) y el TCSM2E para ETSI (Europa).

Las unidades del TCSM son responsables de transcodificar (convertir señales digitales en un código a las señales correspondientes en un código diferente) y submultiplexar (mapear un número de sub canales en un solo canal usado para la transmisión de datos de usuario) canales de tráfico llevados por un solo circuito PCM (T1 o E1) entre el BSC y el sitio de transcodificación.

Las unidades del TCSM son unidades funcionales del BSC, pero ellos pueden ser ubicados en el sitio del BSC o la MSC. Cuando están ubicadas en el sitio de la MSC, la capacidad de transmisión entre el BSC y la MSC es ahorrada, porque la señal es transmitida hasta la MSC de manera transcodificada.

El TCSM proporciona transcodificación de canales de tráfico en la red digital celular GSM900/GSM1800/GSM1900. Esta función está ubicada en el subsistema de estación base (BSS).

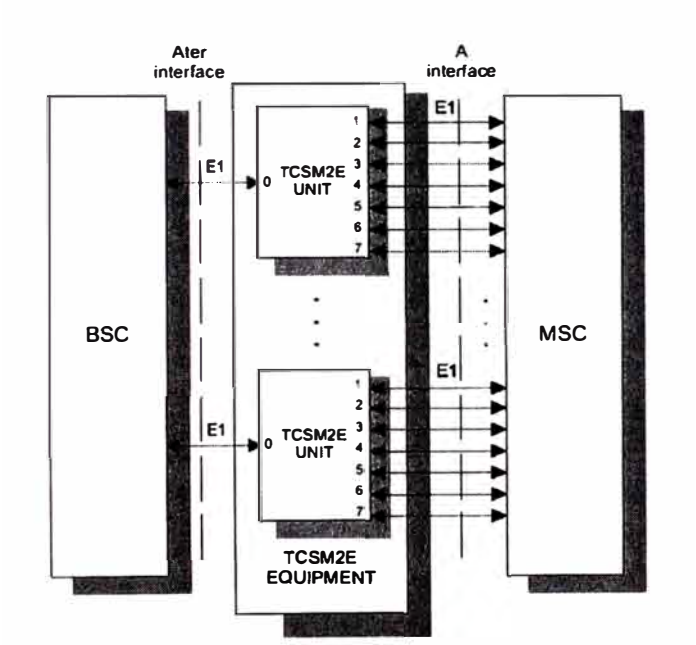


Figura 4.9: Entorno operativo del TCSM ETSI

a) Funciones del TCSM

Cada bloque de canal de tráfico del TCSM es una Unidad Transcoder y Adaptadora de Velocidad (TRAU). La TRAU convierte los 64 kbit/s de los canales de tráfico que vienen de la MSC en canales de 8 kbit/s, 16 kbit/s, 32 kbit/s o 64 kbit/s y

multiplexa estos canales para adaptar los intervalos de tiempo de la línea PCM (circuito digital para la transferencia de señales PCM) que van hacia el BSC. El mismo principio se aplica hacia la otra dirección (BSC a MSC) en viceversa, es decir, conversión de 8, 16, 32 o 64 kbit/s a 64 kbit/s.

Una unidad TCSM2A puede manejar hasta 7 líneas T1 (DS-1) de la MSC. Una unidad TCSM2E puede manejar hasta 7 troncales PCM (2048 kbit/s) de la MSC. Las funciones de operación y mantenimiento del TCSM son coordinados usando el BSC.

Las funciones de telecomunicaciones del TCSM son los siguientes:

Transcodificación y adaptación de los canales de tráfico llevados entre la BTS y la TRAU.

Submultiplexación de 8, 16, 32 y 64 kbit/s de la capacidad de TRAU en intervalos de tiempo de 64 kbit/s.

Conexión a través de los intervalos de tiempo seleccionados.

Proporciona funciones de interfase para las líneas PCM.

Recepción de la sincronización de reloj de las líneas T1 en la dirección de la MSC o líneas PCM y son parte de la cadena de sincronización que se extiende hacia las BTSs.

b) Arquitectura del TCSM

El TCSM2A consiste de 4 bloques principales:

La unidad controladora plug-in, TRCO (TRanscoder COntroller).

Hasta 14 unidades trandcoders plug-in, TR12-T.

La unidad PSC1 plug-in que suministra voltajes operativos de +5V o -5V a la TRCo y TR12Ts.

Hasta 4 unidades plug-in ET2A.

El TRCO incorpora una microcomputadora que controla y supervisa la operación del TCSM2A. El TCSM2A tiene 7 interfases de línea PCM hacia la MSC y una interfase de línea T1 hacia el BSC. Las funciones relacionadas a las interfases de línea T1 son manejadas por la unidad plug-in ET2A.

El TCSM2E consiste de 4 bloques principales:

Unidades plug-in controladoras del transcoder (TRCO).

Hasta 14 unidades transcoders plug-in (TR16-S).

- La unidad plug-in PCS1 como fuente de energía que administra voltajes operativos de +5V o -5V a la TRCO y TR16-Ss.
- Unidades plug-in de terminales de intercambio (ET2E).

El TRCO incorpora una microcomputadora que controla y supervisa la operación del TCSM2E. El TCSM2E tiene hasta 7 interfases de línea PCM hacia la MSC y una interfase de línea PCM hacia el BSC. Las funciones relacionadas a las interfases de línea son manejadas por la unidad plug-in ET2E.

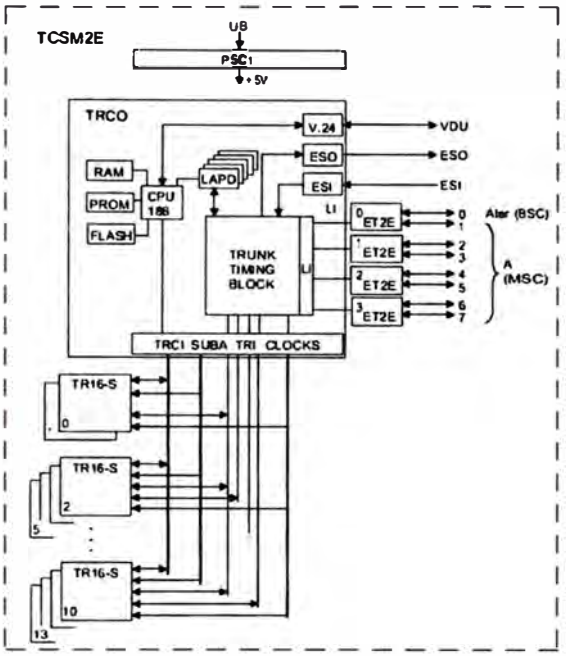


Figura 4.10: Diagrama de bloques del TCSM2E

c) Descripción de las unidades plug-in del TCSM

Unidad plug-in controladora del transcoder (TRCO)

El TRCO controla las funciones del TCSM2A y TCSM2E. Este proporciona una ruta para las señales troncales (trunk) al ET2A/ET2E, y las unidades plug-in TR12-T (TCSM2A) o al ET2E y las unidades plug-in TR16-S (TCSM2E). Estas señales troncales internas son llamadas interfases transcoder (TRI) y señales de interfase de línea (LI). Estas tienen una tasa de bit de 4096 kbit/s y llenan los intervalos de tiempo de dos troncales PCM.

El BSC controla las unidades TCSM2A y TCSM2E sobre el enlace de operación y mantenimiento LAPD. El TRCO incluye 5 funciones LAPD, 4 de los cuales controlan las unidades plug-in ET2A/ET2E y uno de los cuales se comunica con el BSC.

Unidades plug-in de terminales de intercambio (ET2A)

La unidad ET2A tiene 2 puertos DS-1. Los puertos del primer ET2A son compartidos, así que el primer puerto DS-1 está a cargo de la dirección del BSC y el segundo de la dirección de la MSC.

La unidad ET2A está a cargo de la conversión entre las tasas de bits 1544 kbit/s y 2048 kbit/s. Las señales internas de O&M entre el TRCO y cada ET2A son transportadas sobre un intervalo de tiempo dedicado de la señal de interfase de línea.

Unidades plug-in de terminales de intercambio (ET2E)

En el TCSM2E, cada unidad plug-in ET2E tiene 2 interfases de línea PCM. Las interfases PCM del primer ET2E están a cargo de la dirección del BSC y la MSC respectivamente.

Las señales internas de O&M entre el TRCO y cada ET2E son transportadas sobre un intervalo de tiempo dedicado de la señal de interfase de línea.

Unidad plug-in transcoder (TR12-T y TR16-S)

Los canales de tráfico y los intervalos de tiempo son manejados por las unidades plug-in TR12-T y TR16-S. Cada bloque TRAU tiene un procesador digital de señales (DSP), el cual realiza las funciones de transcodificación y adaptación de las velocidades (rates) de transmisión en ambas direcciones. Un DSP puede realizar alternativamente la conmutación de un intervalo de tiempo de 64 kbit/s entre el lado del BSC y las líneas T1 del lado de la MSC.

Unidad plug-in de la fuente de alimentación (PSC1)

Esta fuente de alimentación tiene una capacidad de +5V/24A y -5V/7.5A. Otra variante de la fuente de alimentación es la PSC1-S y puede entregar +5V/40A y -5V/7.5A.

4.1.3 Descripción del Transceptor de la Estación Base (BTS)

La BTS EDGE de NOKIA soporta configuraciones omnidireccionales y sectorizadas para aplicaciones de voz y datos. La BTS puede ser usada en sistemas GSM/EDGE 800, 900, 1800 o 1900MHz. Con la adición de la tecnología EDGE/GPRS, la BTS ofrece una velocidad de datos máxima de más de 400 kbit/s con múltiples intervalos de tiempo, comparado a los 100 kbit/s con múltiples intervalos de tiempo para GSM/GPRS.

a) Operación de la BTS

La BTS realiza las funciones de radio del subsistema de estación base (BSS). La BTS recibe y envía las señales a través de:

Interfase Air: Frecuencias que conectan la BTS a la estación móvil (MS).

Interfase Abis: Cable o enlace de radio que conecta la BTS al controlador de estación base (BSC).

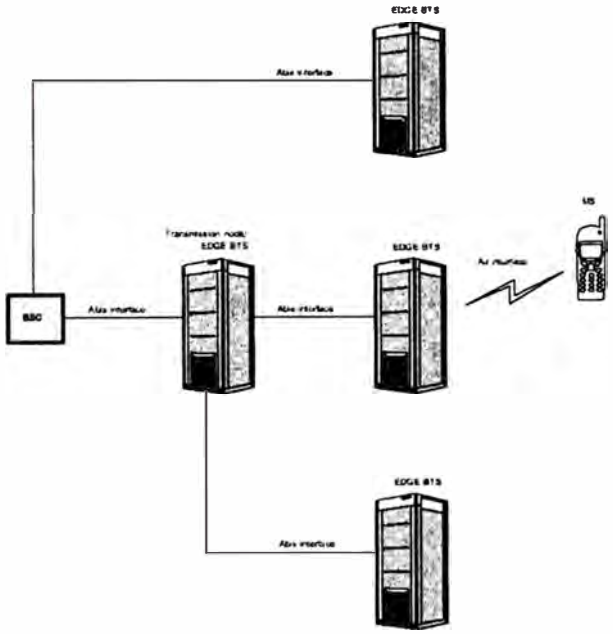


Figura 4.11: Interfases de la BTS

Señalización de los enlaces de subida (uplink) y bajada (downlink)

En la trayectoria del enlace de subida, la BTS recibe las señales de la estación móvil. En la trayectoria del enlace de bajada, la BTS envía las señales a la estación móvil. Las señales de uplink y downlink viajan a través de la interfase Air a diferentes frecuencias, con la frecuencia más alta transportando las señales downlink.

La trayectoria de la señal uplink involucra las siguientes acciones:

- La antena recoje la señal de la estación móvil a través de la interfase Air.
- La antena pasa la señal al Amplificador Masthead (MNxx) y las unidades Bias Tee (BPxx) o a la unidad de filtro Dual Band Diplex (DU2A).
- La señal pasa a través del filtro Dual Variable Gain Duplex (DVxx) o la unidad Remote Tune Combiner (RTxx) al Multiacoplador Receptor (M2xA o M6xA) y las unidades transceptoras de radio frecuencia (TSxx).
- El módulo transceptor (TRX) en la unidad TSxx convierte la señal recibida a los niveles de frecuencia intermedia y filtra la señal.
- Luego la unidad TSxx envía la señal a la unidad transceptora banda base (BB2x) para el procesamiento digital de la señal.
- La unidad BB2x envía la señal procesada a la unidad de transmisión (VXxx), la cual transmite la señal al BSC usando tecnologías de transmisión estándar.

La trayectoria de la señal downlink involucra las siguientes acciones:

- El BSC recibe la señal desde el core de la red y envía la señal a la unidad VXxx utilizando tecnologías de transmisión estándar.
- La unidad VXxx pasa la señal a la unidad BB2x para el procesamiento digital de la señal.
- La unidad BB2x envía la señal procesada a la unidad TSxx
- El módulo TRX en la unidad TSxx filtra la señal, incrementa ésta a la frecuencia portadora y la amplifica.
- La unidad TSxx luego envía la señal a la unidad RTxx o a través de la unidad Wideband Combiner (WCxA) a la unidad DVxx.
- La unidad DVxx o RTxx envía la señal a través de la unidad DU2A o BPxx y MNxx a la entena, el cual pasa la señal a la estación móvil a través de la interfase Air.

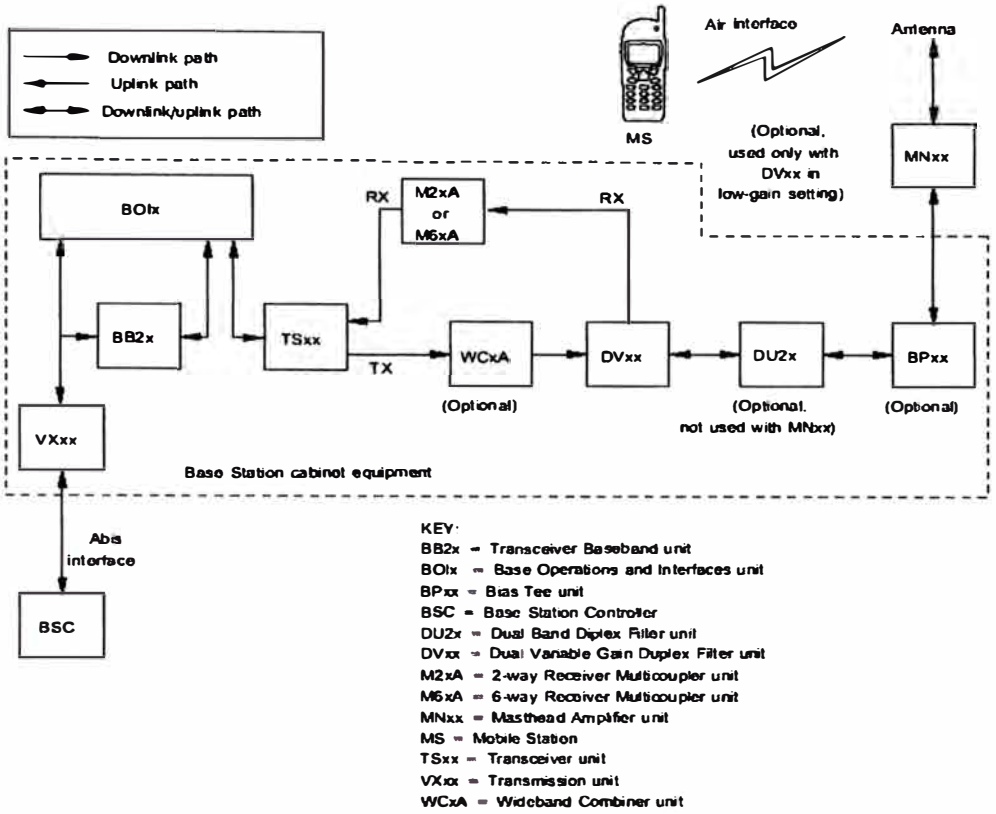


Figura 4.12: Trayectorias de la señal uplink y downlink

b) Transmisión

La BTS proporciona transmisión escalable y de alta capacidad de acceso para las redes de gran capacidad y servicios de datos. La BTS soporta señalización de 16, 32 y 64 kbit/s a través de la interfase Abis. La velocidad de señalización de operación y mantenimiento puede ser de 16, 32 o 64kbit/s.

La BTS soporta los medios de transmisiones de radio enlaces y cable. Las señales son multiplexadas y cross-conectadas a un nivel de 8 kbit/s en la BTS usando la Jerarquía Digital Plesiócrona (PDH).

c) Configuraciones

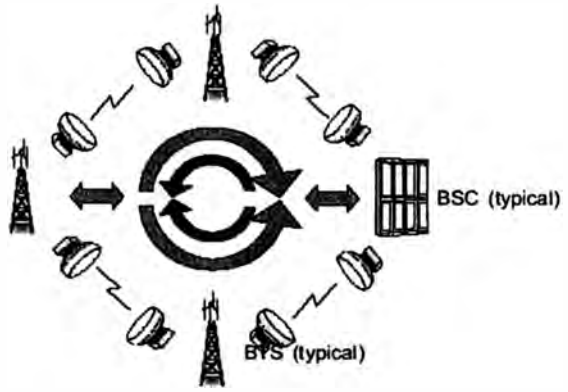


Figura 4.13: Configuración en loop de la BTS

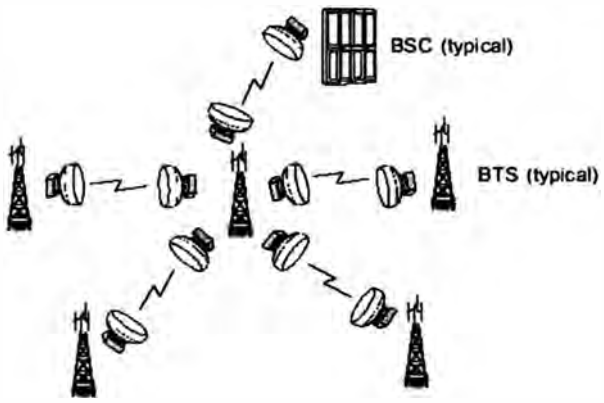


Figura 4.14: Configuración en estrella de la BTS

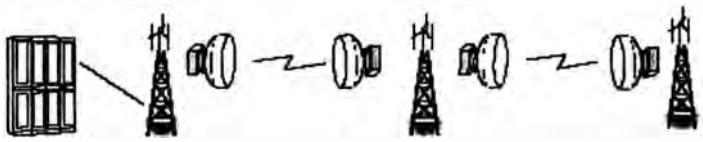


Figura 4.15: Configuración en cadena de la BTS

4.2 Descripción de los elementos de red NSS

4.2.1 Descripción de la Central de Conmutación de Servicios Móviles (MSC)

La central de conmutación de servicios móviles (MSC) es la unidad central en las redes móviles. La MSC realiza la mayoría de funcionalidades en el core de la red de circuitos conmutados. Maneja tareas como señalización, recolección de información de charging, registro de ubicación y paging y administración de tráfico. La MSC es capaz de servir al Subsistema de estación base GSM (BSS) y a la Red de acceso de radio WCDMA (RAN) simultáneamente debido a que tiene las interfases A (hacia BSS) y Iu-CS (hacia RAN). Adicionalmente, puede ser configurada para soportar EDGE.

La MSC soporta:

- La interfase Iu-CS usando transmisión ATM hacia la RAN WCDMA.
- Adaptación del plano de usuario (user plane) a los servicios de datos de circuitos conmutados.
- Transcodificación del servicio de voz.

Los enlaces tradicionales IP y PCM pueden ser usados para la transmisión hacia otras centrales (switches) en la MSC.

a) Plataforma MSC

La MSC realiza las funciones de conmutación en su área de operación y controla el intercambio de mensajes con otras redes. Esta consiste de un número de unidades funcionales, cada una con su propio procesador y un backup que facilita llevar a cabo un número de tareas.

Estas unidades funcionales tienen tareas independientes, pero se comunican cuando usan el bus común de mensajes.

La confiabilidad está asegurada por un backup de los módulos: el módulo de hardware o software está duplicado (2n) o un repuesto está en standby (n+1).

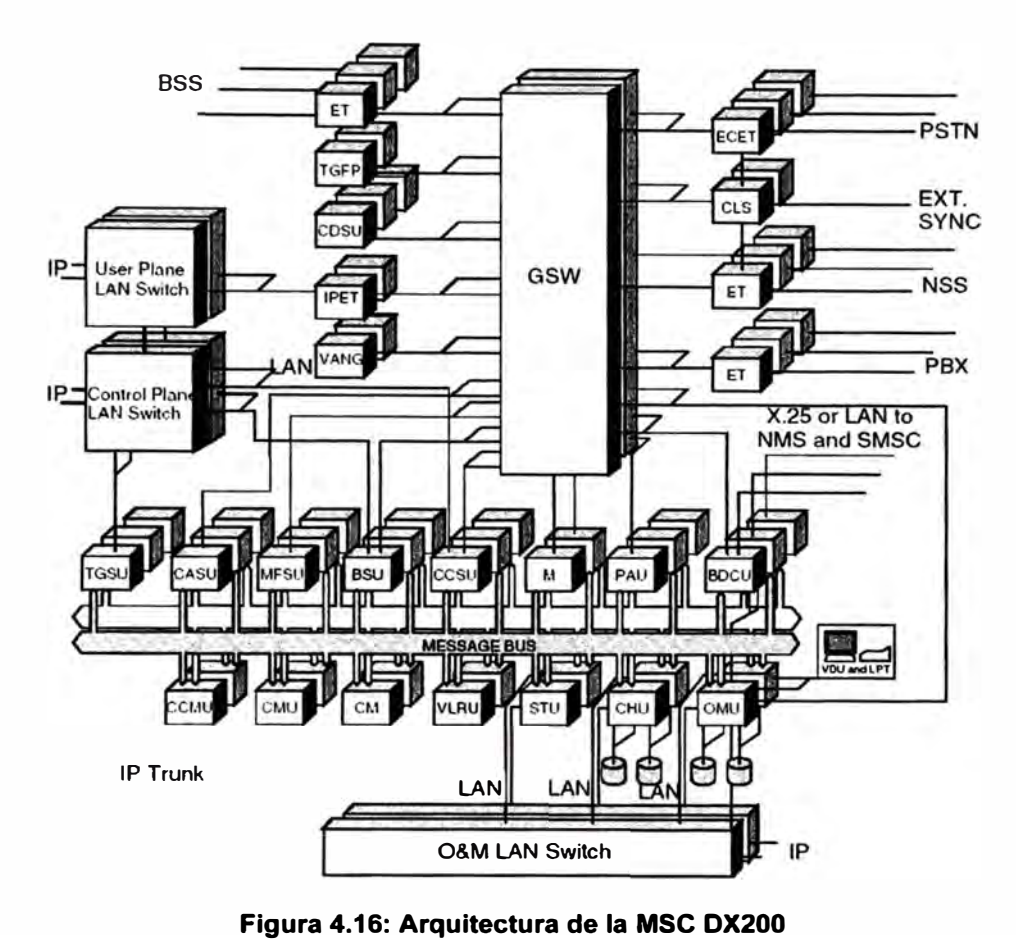


Figura 4.16: Arquitectura de la MSC DX200

A continuación se muestra el detalle de cada una de las unidades funcionales:

La unidad básica de comunicación de datos (BDCU) controla la transferencia de datos y proporciona una interfase X.25 o LAN al Sistema de administración de red y al Sistema de facturación.

La unidad de señalización de la estación base (BSU) controla las funciones de señalización entre la MSC y el BSC, y los PCMs enlazados hacia el subsistema BSS.

La unidad de señalización de canal asociado (CASU) maneja las funciones relacionadas a los métodos de señalización de canal asociado.

La unidad de administración de señalización de canal común (CCMU) contiene información centralizada relacionada a la señalización de canal común (CSS7) y control de red del MTP, SCCP y TCAP. Esta unidad contiene unidades plug-

in responsables de las funciones del Generador de Voz para anuncios (VANG).

- La unidad de señalización de canal común (CCSU) se encarga de las funciones descentralizadas del MTP en el sistema de señalización, del manejo de los mensajes de señalización y las funciones relacionadas al canal de señalización.

- La unidad de servicio compacto de datos (CDSU) proporciona el equipamiento para el intercambio de los servicios de datos (MODEM).

- La unidad de charging (CHU) recolecta los datos de charging, mantiene los contadores y produce registros detallados de charging.

- La unidad de sistema de reloj (CLS) genera las señales de reloj necesarias para sincronizar las funciones de la MSC y transmitirlos a las otras unidades.

- La memoria central (CM) contiene la información del sistema de tarificación, señalización, enrutamiento y configuración.

- La unidad de administración celular (CMU) proporciona el control de la red de radio y la administración centralizada de las transacciones.

- Las terminales de intercambio (ET) son conectadas a las líneas PCM de 2 Mbit/s en el core de la red y realizan la sincronización eléctrica y la adaptación de circuitos externos de 2 Mbit/s a la central (switch).

- El switch de grupo (GSW) conmuta las llamadas. También conmuta los tonos audibles para el anuncio, y las conexiones necesarias por las unidades de señalización y multifrecuencia.

- La terminal de intercambio IP (IPET) convierte los frames de voz TDM que vienen de la matriz del switch en paquetes IP y los desvía a la red IP. Cada IPET tiene una dirección IP individual el cual es definido en el establecimiento de la llamada.

- Los switches LAN pueden ser configurados en diferentes unidades dependiendo del propósito para el que son usados.

- El marcador (M) controla y supervisa la matriz de conmutación realizando las funciones de conexión y liberación del switch de grupo.

- El bus de mensajes (MB) es la conexión física entre las unidades de computadoras.

- La unidad de señalización multifrecuencia (MFSU) es responsable de la verificación del canal de voz, establecimiento de la conferencia de llamadas y recepción del marcado entrante.

  La unidad de operación y mantenimiento (OMU) actúa como una interfase entre el usuario y el sistema y puede ser usado para operaciones locales y con propósitos de mantenimiento, para controlar la configuración de aplicaciones y archivos del sistema así como las mediciones de tráfico.

- La unidad de acceso a la PBX (PAU) contiene las funciones de control para las interfaces de señalización hacia la PBX tales como la señalización DPNSS1 y PRA.

- La unidad de estadísticas (STU) recolecta las mediciones de tráfico, supervisa la carga de la central, mantiene los contadores y produce reportes estadísticos.

- El campo programable generador de tonos (TGFP) genera los tonos audibles necesarios en la MSC. Este también genera las señales estándar y las señales de prueba requeridas por la central (switch).

- La unidad de señalización Trunk Gateway (TGSU) maneja las funciones de señalización del control de llamadas sobre la red IP vía LAN. La TGSU negocia las direcciones IPs para las IPETs al comienzo de cada establecimiento de llamada.

La unidad del registro de ubicación visitante (VLRU) es responsable de la actualización, supresión y lectura de los datos del abonado visitante.

b) Registro de Ubicación Visitante (VLR)

El VLR se encuentra ubicado en la MSC y almacena la información de todos los abonados móviles que están usando la red controlada por dicha MSC. La comunicación entre la MSC y el VLR es completamente una señalización interna.

El VLR también soporta administración de movilidad y participa en las siguientes funciones del procesamiento de llamadas:

Llamadas originadas y terminadas en el móvil.

Soporte para servicios suplementarios.

Soporte para mensajes cortos originados y terminados en el móvil (SMS-MT, SMS-MO).

Las funciones de administración de movilidad soportadas por el VLR incluyen los registros de ubicación y el uso del TMSI e IMSI en los procesos attach (fijación) y detach (separación).

c) Gateway Multimedia para la MSC (MGW)

La implementación del Gateway Multimedia (MGW) es la diferencia más significante entre las redes 2G y 3G. El principal propósito del MGW es proporcionar intercambio de mensajes RAN WCDMA con la MSC implementando la interfase Iu. La interfase Iu tiene 2 partes: La Iu de paquetes conmutados (Iu-PS: Iu Packet Switched) entre el RNC y el SGSN y la Iu de circuitos conmutados (Iu-CS: Iu Circuit Switched) entre el RNC y la MSC. Ambas están basadas en ATM.

En adición al soporte de la interfase Iu, el MGW para la MSC proporciona:

Transcodificación de servicios de voz.

Transmisión TDM hacia la MSC.

Adaptación del plano de usuario para servicios de datos de circuitos conmutados.

Conversión de protocolos de 3ra generación a protocolos de 2da generación (WCDMA RANAP y GSM BSSAP).

La capacidad del MGW para la MSC depende del número de unidades de transcodificación (TCU).

El Gateway Multimedia para la MSC está basado en la plataforma ATM IPA2800. La plataforma tiene una arquitectura modular que hace fácil la operación y el mantenimiento.

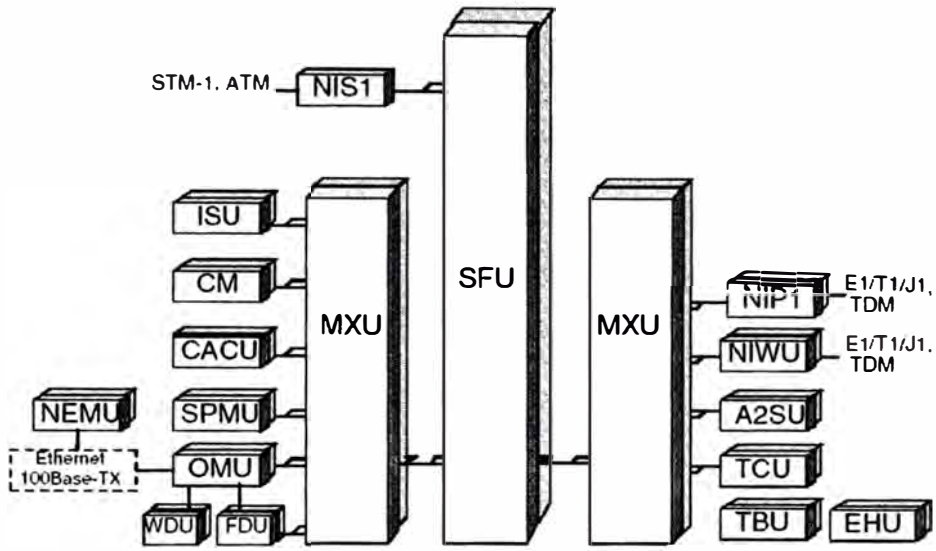


Figura 4.17: Arquitectura del MGW para la MSC

A continuación se muestra el detalle de cada una de las unidades funcionales:

Las computadoras de control distribuido (CACU, CM, SPMU, ISU) consisten de hardware común y sistema de software.

La unidad de alarmas externas de Hardware (EHU) proporciona la posibilidad de encaminar las alarmas externas (desde otros elementos de red) vía la OMU hacia el sistema de manejo de alarmas internas.

La unidad de operación y mantenimiento (OMU) es utilizado para funciones básicas de mantenimiento del sistema. Los dispositivos periféricos son también conectados a la OMU.

La unidad de procesamiento distribuido de señal (TCU) proporciona soporte para la transcodificación de la voz y procesamiento de datos de circuitos conmutados.

- La unidad de interfase de red (NIP, NIS) conecta el elemento de red al sistema de transmisión (ATM sobre STM-1 o E1/T1/JT1).

- La unidad de intercambio de red (NIWU) conecta el elemento de red a sistemas de transmisión basados en PCM (E1, T1 o JT1).

- La unidad multiplexadora y unidad fabric de conmutación ATM (MXU, SFU) son utilizados para conmutación de canales de datos de circuitos conmutados, canales de señalización y comunicaciones internas del sistema.

- La unidad de conmutación AAL tipo 2 (A2SU) realiza la funcionalidad de conmutación de minipaquetes.

- La unidad de bus de administración de sincronización y hardware (TBU) es utilizado para sincronización y propósitos de mantenimiento del sistema.

El MGW también contiene la Unidad de Administración del Elemento de Red (NEMU). La NEMU es una unidad de computadora que proporciona una plataforma de cómputo estándar para aplicaciones que no tienen requerimientos estrictos en tiempo real. La implementación del software de la NEMU del MGW está basada en el Sistema operativo Windows. La NEMU contiene sus propios discos, interfases para el teclado y display para propósito de debug, una interfase serial, una interfase USB y una interfase LAN (100 Mbit Ethernet).

4.2.2 Descripción del Sistema Servidor MSC (MSS)

El sistema MSS es un desarrollo de la MSC. Así como el Gateway Multimedia (MGW) con la MSC tiene un mejor desarrollo en el MGW para MSS. El MSS ofrece una red común IP y ATM para el tráfico 2G o 3G del abonado.

Los operadores son libres de elegir la tecnología a utilizar en la capa de transporte en sus redes (TDM, ATM o IP). Con el MGW para MSS el operador tiene la libertad de separar el plano de control (control plane) y el plano de usuario (user plane) y seleccionar la mejor combinación de los protocolos de transporte utilizados. El sistema MSS permite el uso de red de transporte común para el core de circuitos y core de paquetes.

El plano de control (Control Plane) es la capa que realiza las funciones de señalización necesarias para el establecimiento, supervisión y liberación de llamadas y conexiones.

El plano de usuario (User Plane) es la capa en la cual los datos o voz del usuario que vienen de la red de radio son convertidos a datos PCM del usuario.

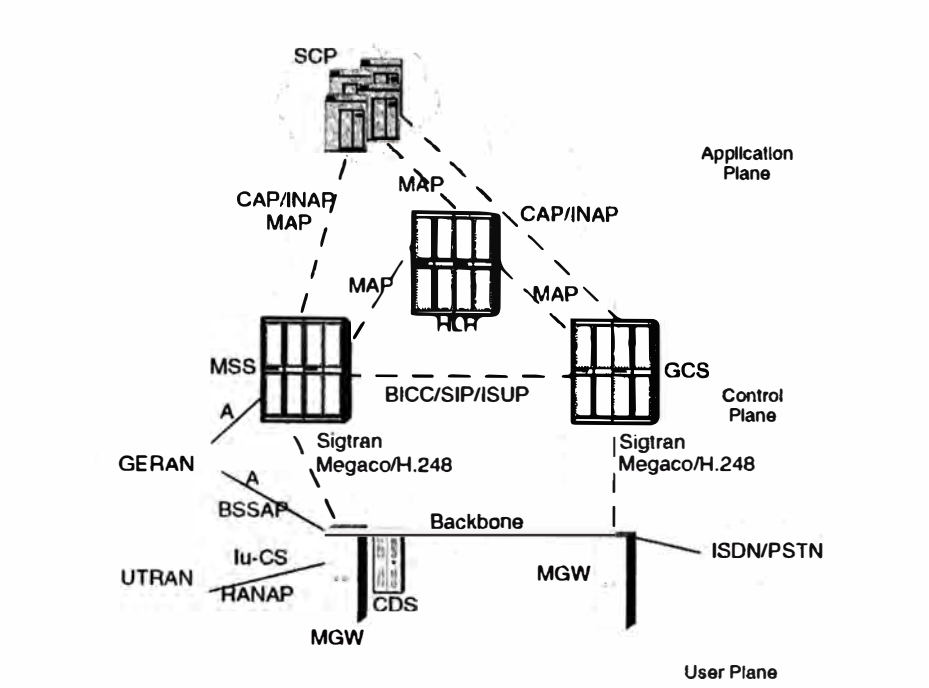


Figura 4.18: Separación de los planos de control y de usuario en el core de la red

El sistema MSS proporciona la continuidad del servicio GSM. El sistema MSS es la manera más rápida y segura hacia los servicios y otras ventajas IP Multimedia.

a) Servidor MSC (MSS)

El MSS comprende principalmente los elementos de control de llamadas y control de movilidad de una MSC tradicional. Este es responsable del control de las llamadas originadas y terminadas en el móvil de una red de circuitos conmutados así mismo, el MSS se encarga de terminar la señalización usuario – red y trasladar ésta a la señalización red – red. El MSS contiene también un VLR para mantener los datos del servicio de los abonados móviles y los datos relacionados a las Aplicaciones Personalizadas para la Lógica Mejorada de la Red Móvil (CAMEL). Además, el Punto del servicio de conmutación (SSP) está incluido en el MSS.

La funcionalidad del MSS puede ser dividida en 2 roles: Solo como MSS y Servidor de Control Gateway (GCS). El GCS es un equipo que incluye la funcionalidad de servidor GMSC.

Para operadores quienes tienen una PLMN operacional, es posible integrar la funcionalidad del Servidor MSC (MSS) a la MSC actualizando el software y hardware. La red basada en PCM puede co-existir con el backbone IP/ATM y el MSS y el Servidor de Control Gateway (GCS) son capaces de utilizar ambas redes.

El operador puede definir el tipo y la cantidad de tráfico transportado vía el backbone IP/ATM y la red PCM. Las líneas PCM de la GERAN pueden ser conectadas en el MSS integrado o el MGW y, similarmente, las líneas PCM de las red PSTN/ISDN pueden ser conectadas al GCS o al MGW.

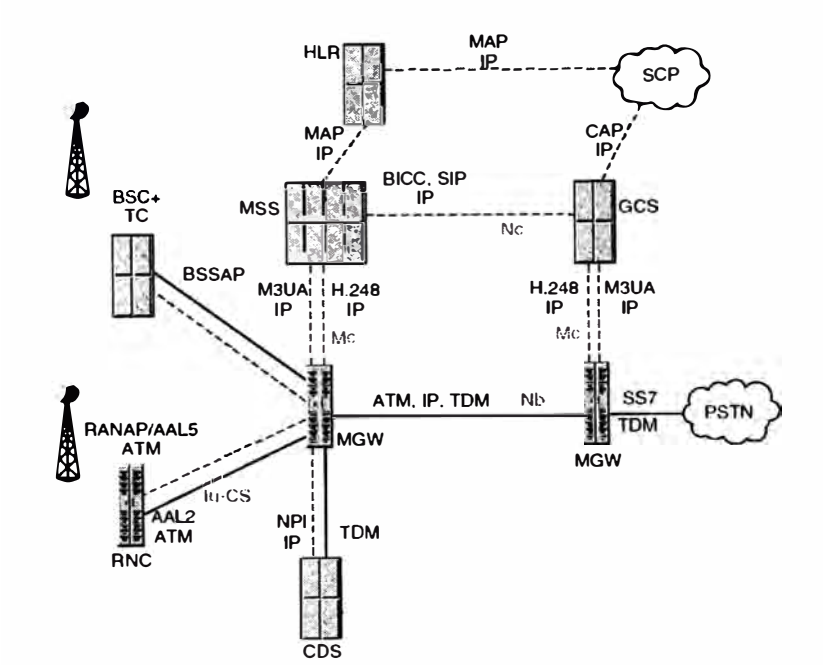


Figura 4.19: Solución NOKIA del core de la red conmutada de circuitos

A continuación se muestra la arquitectura de hardware del MSS integrado. La unidad de señalización Trunk Gateway (TGSU) es una nueva unidad funcional en el concepto IP Trunk y proporciona las funciones de señalización necesarias en la red de transmisión IP.

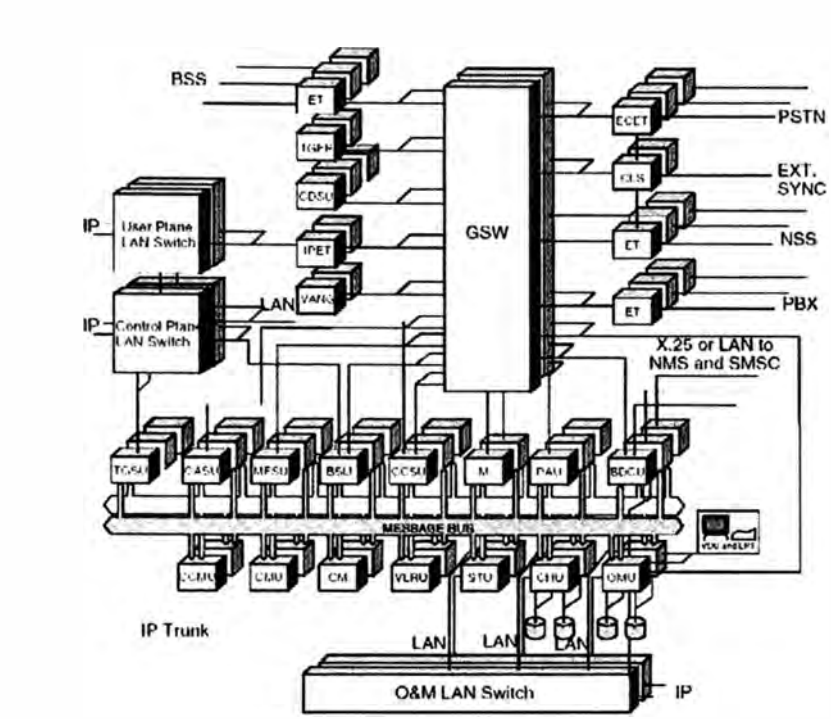


Figura 4.20: Arquitectura del MSS integrado

El MSS independiente (stand-alone) ofrece la funcionalidad en la cual el plano de control (control plane) está destinado al MSS y el transporte y procesamiento del plano de usuario (user plane) es hecho solamente en el MGW. El MSS es un elemento de red con conexiones basadas en IP.

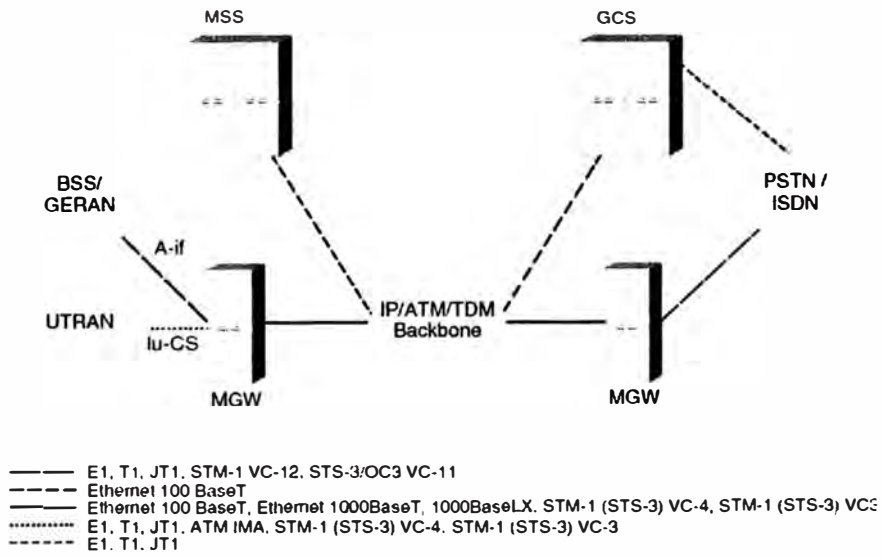


Figura 4.21: Entorno de red de un MSS independiente

El MSS independiente no tiene Switch de Grupo (GSW) para la conmutación de canales a 64kbit/s sino un pequeño GSW que puede ser opcionalmente incluido en la configuración si los propósitos de señalización C7 son requeridos.

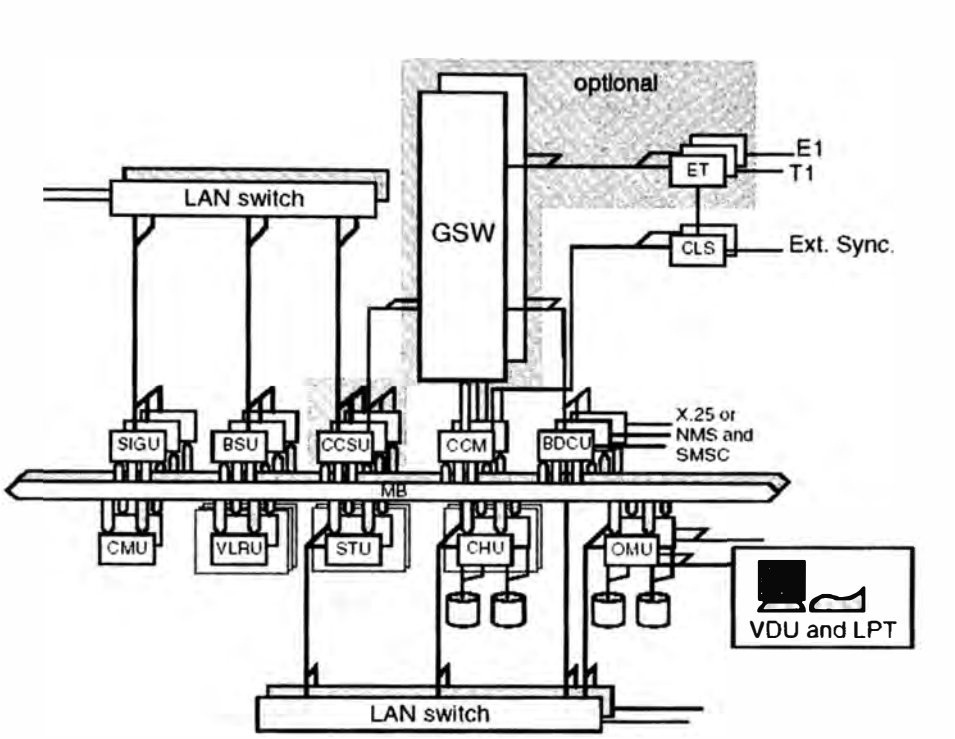


Figura 4.22: Arquitectura del MSS independiente

El marcador y memoria central (CMM) contiene las funcionalidades de memoria central en la misma unidad funcional y está incluida solo en el modelo MSS independiente. Otra unidad usada en el MSS independiente pero no en el integrado, es la unidad de señalización SIGU. Este tiene las funcionalidades de la unidad CCSU excepto que la SIGU puede utilizar solo SS7 basado en IP mientras que la unidad CCSU puede utilizar SS7 basado en TDM o IP. Las otras unidades funcionales son las mismas que la de una MSC.

El Servidor de Control Gateway (GCS) tiene todas las funcionalidades de gateway del MSS. El GCS es utilizado en el sistema Servidor MSC (MSS) para controlar los Gateways Multimedia (MGWs) que realizan intercambio de datos entre las redes PSTN/ISDN, IP y ATM.

En redes IP multimedia, el GCS puede ser usado para controlar los MGWs que son usados para intercambio de datos entre las redes de circuitos conmutados y el subsistema IP multimedia (IMS).

b) Gateway Multimedia (MGW) para MSS

El Gateway Multimedia en el entorno MSS convierte el medio proporcionado por un tipo de red al formato requerido en otro tipo de red. El MGW termina los canales bearer (canal utilizado para transmisión de datos de abonado) TDM del subsistema BSS (interfase A) y la PSTN, ATM o IP de la red de acceso de radio RAN (interfase Iu) y el backbone. El MGW puede proporcionar servicios, como por ejemplo, transcodificación, generación de tonos, para un media stream. El MGW es controlado por el MSS o GCS. Un MSS/GCS puede controlar varios MGWs, y equivalentemente, un MGW puede proporcionar interfase de plano de usuario y recursos de procesamiento para varios elementos MSS/GCS.

En el entorno del Servidor MSS, el MGW de NOKIA implementa el Gateway Multimedia (MGW) y las entidades funcionales del Gateway de Señalización (SGW).

La funcionalidad del Gateway Multimedia es terminar los canales bearer de la red de circuitos conmutados y los media streams de la red backbone (RTP) en una red IP o conexiones AAL2/ATM en un backbone ATM), y realizar la conversión entre éstas terminaciones. Además, para la terminación e intercambio de datos de diferentes tecnologías de interfase, el MGW proporciona capacidades avanzadas para procesamiento de media.

El Gateway de Señalización (SGW) convierte la capa de transporte SS7 del Método de Transporte IP (SIGTRAN). Este es usado principalmente por el protocolo de control de llamada (ISUP), pero puede ser usado también para transmitir cualquier protocolo basado en SS7 sobre la capa de transporte IP y viceversa.

Utilizando el MGW, los operadores son libres de separar la capa de transporte y la capa de control de llamadas y seleccionar la combinación preferida de los protocolos de transporte utilizados.

La funcionalidad está distribuida en un conjunto de unidades funcionales capaces de realizar propósitos especiales. Las unidades están conectadas a la Matriz de Conmutación basada en ATM (SFU) ya sea directamente en el caso que las unidades tengan alta capacidad de tráfico, o vía la Unidad Multiplexadora (MXU) en el caso que las unidades tengan baja capacidad de tráfico.

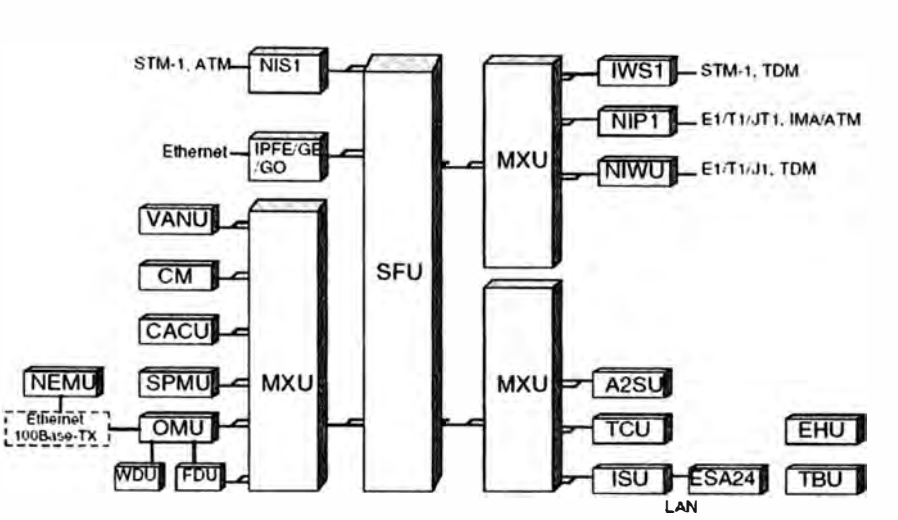


Figura 4.23: Arquitectura del MGW para MSS

La mayoría de las unidades funcionales en el MGW para MSS son las mismas que en el MGW para MSC. Las unidades nuevas en el MGW para MSS son:

El switch ethernet (ESA24: Ethernet Switch) agrupa las interfases Ethernet de las unidades ISU y OMU, y luego proporciona la conectividad Ethernet a otros elementos.

La unidad de interfase de red IP (IPNIU) proporciona las interfases externas para conexiones de plano de usuario IP vía la interfase ethernet de 100 Mbit/s o 1 Gbit/s.

La unidad de anuncio de voz (VANU) contiene anuncios proporcionados por el MGW para el plano de usuario.

4.2.3 Descripción del Registro de Ubicación Local (HLR)

El HLR está integrado con el Centro de Autenticación (AC) y el Registro de Identidad del Equipo (EIR) y soporta servicios GSM y 3G. El HLR proporciona almacenamiento de base de datos y modificación de:

Datos del perfil del abonado.
Datos de autenticación.
Datos de identidad del equipo móvil especificando la lista blanca, negra o gris.

Los datos del abonado son almacenados en el HLR de la misma manera que en el VLR, pero el HLR es la base de datos permanente. El HLR soporta protocolo Parte de aplicación móvil (MAP) sobre SS7 o IP hacia el MSC/MSS y SGSN. Además, el HLR participa en las siguientes funciones de procesamiento:

- Consultas de encaminamiento para las llamadas terminadas en el móvil y mensajes cortos.
- Servicio suplementario de activación/desactivación de terminales móviles.
- Soporte para los servicios de llamada entrante, servicios de desvío de llamadas, etc.

La arquitectura del HLR es notoriamente similar a la MSC. Las especificaciones exactas de las interfases hace posible adicionar funciones sin cambiar la arquitectura del sistema y permitir al sistema a permanecer actualizado a lo largo de su vida operacional.

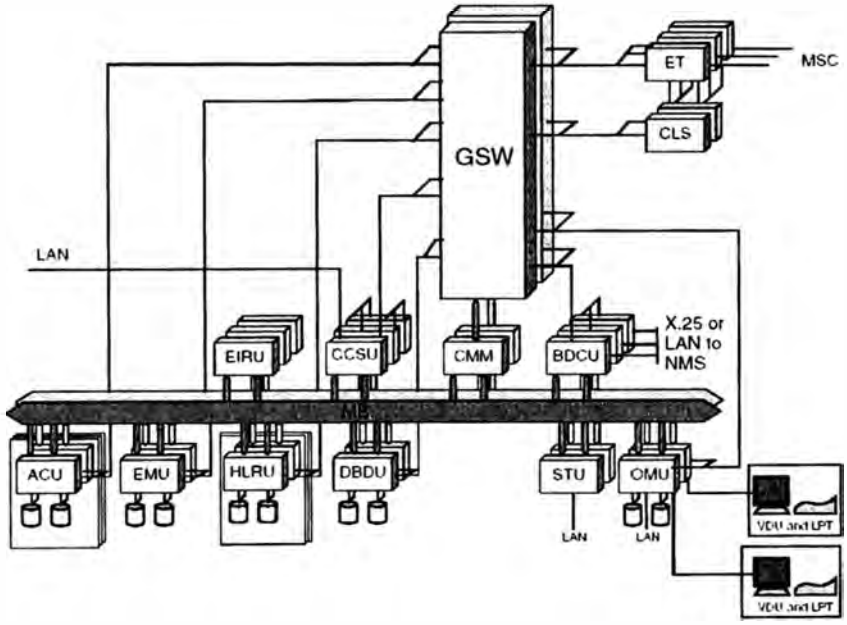


Figura 4.24: Arquitectura del HLR DX200

A continuación se muestra el detalle de cada una de las unidades funcionales:

La unidad del centro de autenticación (ACU) es responsable del almacenamiento de los datos de autenticación, generando números aleatorios y ejecutando algoritmos de seguridad.

- La unidad básica de comunicación de datos (BDCU) controla la transferencia de datos GSM. Proporciona una interfase X25 o LAN al sistema de administración de red y al sistema de facturación.

- La unidad de sistema de reloj (CLS) genera las señales de reloj necesarias para sincronizar las funciones del HLR y transmitirlos a las otras unidades.

- La unidad de señalización de canal común (CCSU) se encarga de las funciones descentralizadas del MTP en el sistema de señalización, del manejo de los mensajes de señalización y las funciones relacionadas al canal de señalización.

- El Marcador y Memoria Central (CMM) es una combinación de la memoria central y la unidad marker.

- La unidad distribuidora de base de datos (DBDU) distribuye los datos del HLR/AUC relacionados al abonado a la unidad correcta.

- La unidad principal del equipo (EMU) es responsable de la administración del EIR y la administración de la interfase CEIR-EIR, es decir, la transferencia entre el EIR y el CEIR.

- La terminal de intercambio (ET) realiza la sincronización eléctrica y adaptación externa de los circuitos de 2 Mbit/s a la central.

- El switch de grupo (GSW) conmuta las llamadas así como los tonos audibles, anuncios, y conexiones necesarias por las unidades de señalización y multifrecuencia.

- La unidad del registro de ubicación local (HLRU) es responsable de la actualización, supresión y recuperación de los datos del abonado.

- La unidad de operación y mantenimiento (OMU) actúa como una unidad entre el usuario y el sistema. Esta unidad puede ser usada para operaciones locales y propósitos de mantenimiento así como la recolección de indicadores de fallas de la central y enviarlos al sistema de administración de red.

La unidad de estadísticas (STU) recolecta las mediciones de tráfico, supervisa la carga de la central, mantiene los contadores y produce los reportes estadísticos.

a) Centro de Autenticación

El Centro de Autenticación (AuC) maneja la administración de la seguridad de datos para la autenticación del abonado. El AuC está integrado en el HLR de NOKIA. El VLR solicita la autenticación de vectores (vectores de parámetros) desde el AuC, almacena los vectores recibidos y ejecuta el procedimiento de autenticación. En GSM, el procedimiento de autenticación es realizado para validar la tarjeta SIM del abonado y prevenir una tarjeta falsa de acceso a la red.

Para UMTS, nuevos procedimientos de autenticación han sido introducidos para asegurar la Seguridad en 3G. Nuevos algoritmos han sido adicionados, los quintetos de autenticación son generados (Código de autenticación de mensaje (MAC), Respuesta esperada (XRES), Clave de cifrado (CK), Clave de integridad (IK) y Clave anónima (AK)), las conversiones de 2G a 3G son habilitadas en el Sistema 3G para el cifrado y la autenticación.

b) Registro de Identidad del Equipo

El EIR integrado en el HLR de NOKIA contiene las bases de datos y mantiene los registros de la base de datos de los números IMEI. Estos números IMEI son almacenados en 3 listas: blanca, gris y negra, indicando el estado actual del equipo móvil. La verificación del IMEI es realizada para asegurar que el equipo móvil no está en la lista negra.

Cuando el EIR recibe una solicitud del MSC/MSS y SGSN, éste busca en su base de datos para determinar en cual lista el IMEI está ubicado. Después de eso, éste devuelve la información a la MSC, el cual actúa de acuerdo a la información recibida. La MSC puede, por ejemplo, terminar una llamada si el IMEI es encontrado en la lista negra.

4.3 Descripción de los elementos de red GPRS

4.3.1 Descripción del Nodo de Soporte de Servicio GPRS (SGSN)

a) SGSN 2G

El SGSN de segunda generación (SGSN 2G) conecta la red de radio 2G al core de la red de paquetes 2G y 3G. Actúa como un enlace entre la red de circuitos conmutados 2G (con los elementos de red de BSS y NSS) y el core de la red de paquetes conmutados, encargándose de la administración de la movilidad, encriptación y compresión, así como la generación de información estadística y de charging.

Las conexiones de datos son creadas hacia el GGSN, y soporta IPV6 en el plano de usuario (user plane). Las funciones del SGSN 2G son las siguientes:

Administración de sesión y movilidad.
Autenticación de abonado y terminal.
Estadísticas y charging.
Encriptación y compresión.
Operación y mantenimiento.
Calidad de servicio (QoS).
Prepago.
Administración de datos del abonado.
Mantenimiento del sistema.
Manejo de parámetros.
Entrega del SMS vía GPRS.
Traces.
Control de sobrecarga.

El SGSN 2G es implementado como un nodo independiente, significando que éste puede ser ubicado en la posición óptima considerando las necesidades de operación, mantenimiento y transmisión.

b) SGSN 3G

El SGSN 3G es parte del core de la red de paquetes de 3ra generación. Este actúa como un enlace entre la Red de Acceso de Radio 3G (RAN) y el core de la red de paquetes, realizando funciones de control y manejo de tráfico para la parte del dominio de paquetes conmutados del core de la red 3G.

En éste rol, el SGSN 3G es responsable de las siguientes funciones:

- Administración de sesión y movilidad.
- Supervisión de los recursos y servicios de la red 3G.
- Tunnelling GTP y enrutamiento (routing) de los datos de usuario del GGSN.
- Autorización y autenticación del abonado.
- Recolección de los datos de charging y estadísticas de tráfico y entrega de ésta información al Gateway de facturación (CG) y el sistema de administración de red.
- Soporte de charging prepago, hot billing, tarifa plana y remoción de CDRs duplicados.
- Entrega de mensajes cortos.

El SGSN 3G soporta IPv6, calidad de servicio, IPSec (IP Security), servicio prepago y múltiple contextos PDP (asociación de la estación móvil a múltiples PDPs) por dirección IP. En 3G, la característica acerca de la señalización SS7 sobre IP proporciona una posibilidad de comunicar el tráfico SS7 sobre el protocolo IP usando ethernet.

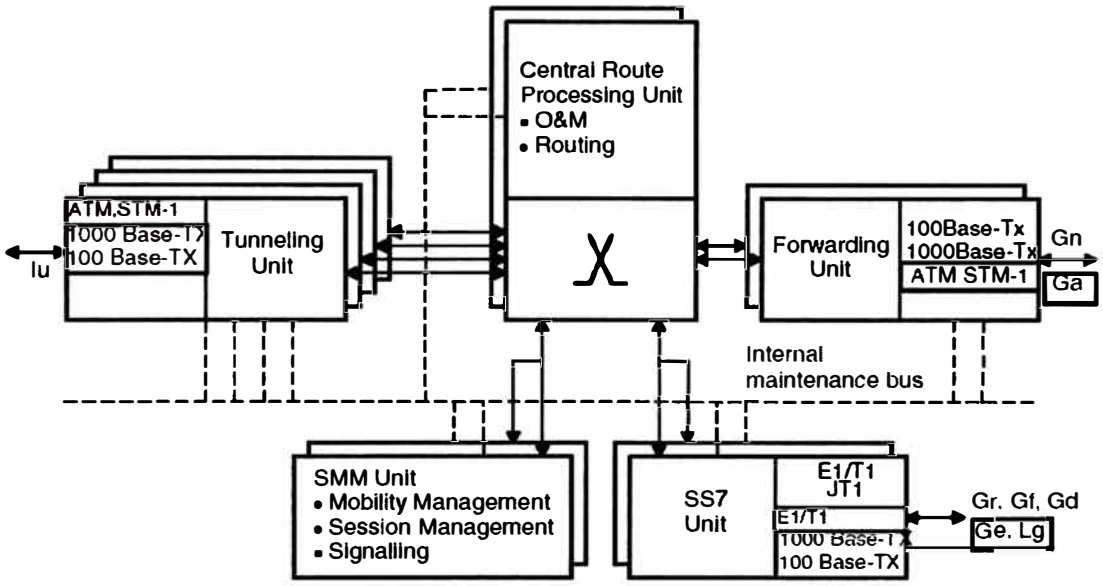


Figura 4.25: Arquitectura del SGSN

El SGSN 3G está basado en una plataforma de enrutamiento (routing) multiprocesador y consiste de unidades, cada una con un CPU, memoria, slots para tarjetas interfases PCI y una conexión de alta velocidad al switch fabric.

A continuación se describen las unidades funcionales:

- El procesador central de enrutamiento (CRP) ejecuta los protocolos de enrutamiento, maneja la operación y mantenimiento del sistema, es decir, se encarga de la administración de fallas, administración de performance y administración de configuración y de aquí, proporciona las interfases hacia el sistema de administración de red.

- La unidad de administración de movilidad y señalización (SMMU) mantiene la información de los recursos del sistema y los abonados conectados. Esta unidad también maneja todas las aplicaciones de la capa de señalización (RANAP, MAP y CAP) y se encarga del control de admisión, es decir, acepta o rechaza las solicitudes para nuevas conexiones.

- Las unidades de tunnelling (TU) manejan el procesamiento de los datos del usuario final, los cuales se encapsulan en túneles para el transporte sobre la red backbone IP. Los procesos de tunnelling son distribuidos entre varias unidades para una alta performance y redundancia de interfase.

- Las unidades de desviación (FU) se implementan en la interfase Gn, lo cual significa que ellos conectan el SGSN al backbone de red y consecuentemente a otros GSNs.

- Las unidades SS7 (SS7U) proporcionan la conexión de señalización al HLR, EIR y SMSC.

4.3.2 Descripción del Nodo de Soporte de Gateway GPRS (GGSN)

La funcionalidad del GGSN es parte del nodo de servicios inteligentes. El GGSN actúa como una interfase entre las redes GPRS o externas (Internet o intranets corporativas).

El GGSN habilita el GPRS en los abonados móviles para acceder a varios servicios de datos. Desde el punto de vista de redes externas, el GGSN es simplemente un router a una subred. El mismo GGSN puede servir para abonados GPRS y 3G al mismo tiempo.

Soporta los protocolos de routing más comunes: RIPv1, RIPv2, OSPF, IGRP, BGP4 DVMPR y enrutamiento estático así como GRE e IP.

El GGSN participa en las siguientes funciones:

- Tunnelling GTP, el cual retarda los paquetes de datos entre las redes 3G o GPRS y redes externas de paquetes de datos.
- Señalización GPRS/UMTS, el cual maneja los contextos PDP y también asigna direcciones IP dinámicas.
- IPv6 en el plano de usuario (user plane), ofreciendo una solución más durable para el direccionamiento IP siendo también compatible con las redes basadas en IPv4.
- Calidad de servicio.
- Soporte de charging para servicios prepago, hot billing, tarifa plana y remoción de CDRs duplicados.
- Recolección de datos de charging y estadísticas de tráfico y entrega de ellos al Charging Gateway y el sistema de administración de red.

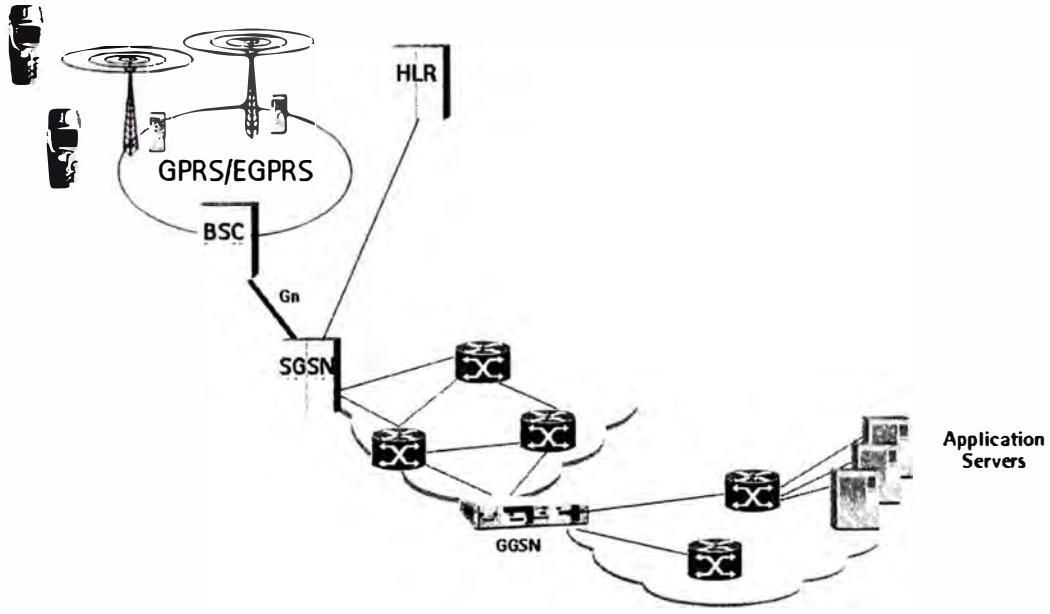


Figura 4.26: Implementación GPRS/EGPRS

El GGSN de NOKIA soporta los siguientes protocolos de enrutamiento:

- Protocolo de Información de Enrutamiento (RIP)
- Protocolo de Apertura de Ruta de Acceso más Corta (OSPF)
- Protocolo de Gateway de Borde (BGP)
- Enrutamiento estático

También, este soporta los siguientes protocolos de tunnelling:

Encapsulación Genérica de Ruta

IP en IP

Protocolo de Tunnelling de capa 2 (L2TP)

VLAN trunk

CAPITULO V

INTEGRACIÓN DE LOS ELEMENTOS DE RED AL SISTEMA DE ADMINISTRACIÓN DE RED

5.1 Integración de la Red de Comunicación de Datos (DCN)

La red de comunicación de datos proporciona las conexiones hacia los elementos de red que usan protocolo IP para la administración de operación y mantenimiento y también hacia aquellos elementos que usan protocolo ISO IP.

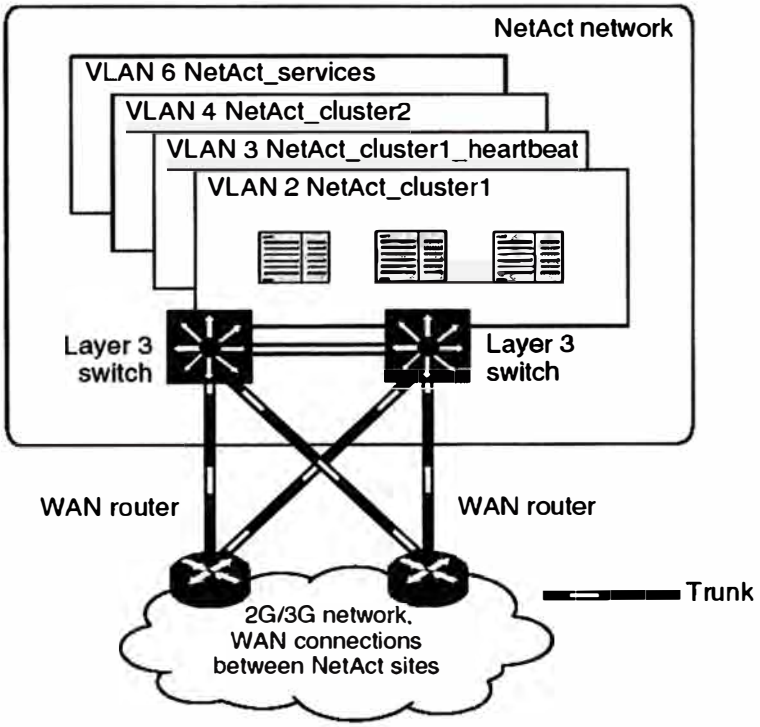


Figura 5.1: Conexiones físicas desde la red de comunicación de datos al sistema de administración de red

La solución propuesta es estándar, utilizando switches Cisco de capa 2. El enrutamiento IP es llevado a cabo por routers Cisco.

En el diseño de la red de comunicación de datos, se utilizan como protocolos de enrutamiento al OSPF e ISIS y como protocolos enrutables al TCP/IP e ISO IP.

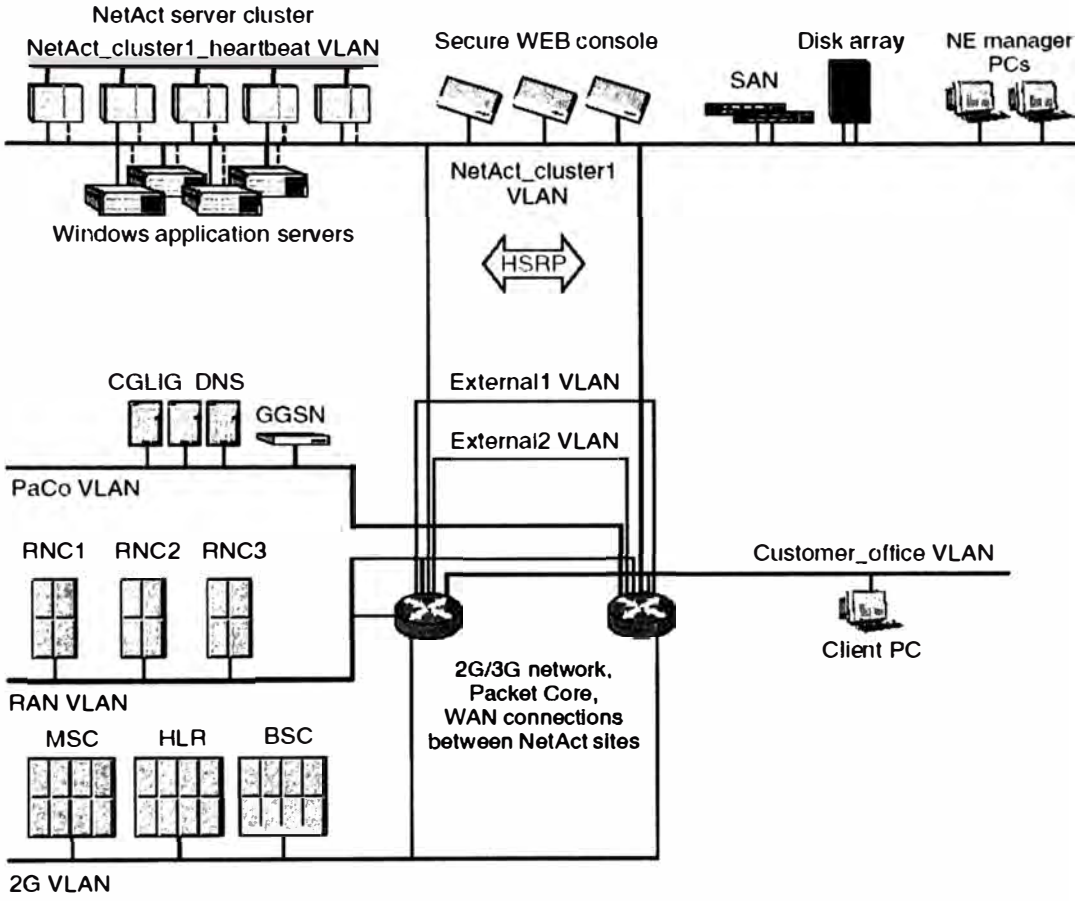


Figura 5.2: Solución estándar del backbone de la red de comunicación de datos

5.1.1 Definición de VLANs en el Sistema de Administración de Red

La red del sistema de administración de red está dividida en varias VLANs (LAN Virtuales) separadas para proporcionar una mejor estructura. A continuación se muestra un ejemplo de las VLANs definidas:

Tabla 5.1: Ejemplo de la definición de VLANs

VLAN	Descripción
VLAN A	Definida para los servidores del sistema de gestión de red que forman parte del cluster1
VLAN B	Definida para las conexiones de heartbeat entre los servidores del cluster1
VLAN C	Definida para los servidores del sistema de gestión de red que forman parte del cluster2
VLAN D	Definida para las conexiones de heartbeat entre los servidores del cluster2
VLAN E	Definida para los componentes del arreglo de discos, switches SAN y otros servicios
VLAN F	Definida para los elementos de red GSM
VLAN G	Definida para los elementos de red de paquetes
VLAN H	Definida para las conexiones hacia la red del operador
VLAN I	Definida hacia las interfases del firewall

En términos de direccionamiento IP, cada VLAN forma una subred. Se debe tomar en cuenta el número de hosts en cada subred, el cual definirá el tamaño de la VLAN. Se recomienda la reserva de direcciones IP para una posible expansión futura.

Para la parte de subredes, es recomendable utilizar las Máscaras de Subred de Longitud Variable (VLSM), el cual es un concepto para la asignación de recursos de direccionamiento IP a subredes de acuerdo a las necesidades individuales y no a una regla general de red. Es decir, el concepto de VLSM se convierte en un medio para especificar una diferente máscara de subred para la misma red en diferentes subredes. Con el VLSM, se puede utilizar una máscara grande en redes con pocos hosts y una máscara corta en subredes con muchos hosts. El protocolo de enrutamiento debe soportar VLSM.

Los siguientes protocolos de enrutamiento IP soportan VLSM:
OSPF, Dual IS-IS, BGP-4 y EIGRP.

Se debe tener en cuenta el número de direcciones IP para las subredes:

Direcciones IP de todos los hosts.

Direcciones IP del paquete MC/Service Guard.

Direcciones IP para los switches y routers.

5.1.2 Procedimiento de integración

a) Tareas previas

Obtención de la información del sistema

Para la integración de la red de comunicación de datos (DCN), se debe asegurar que todo el equipamiento, nombres de hosts y direcciones IP están documentadas sobre un mapa de red. Con el mapa de red, se proporciona información necesaria para la planificación, integración y tareas de mantenimiento para la DCN.

A continuación se muestra el tipo de información que se debe considerar en un mapa de red:

Hardware: Fabricantes y modelos del hardware a utilizar.

Role y función de los componentes del hardware, como base datos, servidor de aplicaciones, etc.

Versión de software a utilizar en el equipamiento.

Nombres de los hosts.

Direcciones IP y X.121.

Direcciones NSAP de los servidores y elementos de red.

Número C (C-number) de los elementos de red.

ID internos para los elementos de red.

Comunidad SNMP.

Revisión de los requerimientos del sistema

Administración de la estación de trabajo

Para configurar un router o switch Cisco, la estación de trabajo, consola o PC debe reunir los siguientes requerimientos:

El TCP/IP está funcional.

El Telnet está funcional.

El software de emulación de Terminal debe estar instalado en la PC a su vez éste software permite la transferencia xmodem.

Routers Cisco

El router debe tener una versión de IOS 12.2 o superior.

128MB de DRAM.

32MB de memoria flash.

Debe existir backups disponibles para todas las configuraciones de los routers.

Switches Cisco

Switch Cisco 2950-24 con IOS 12.1(6)EA2b

Switch Cisco 3750-24TS-E1u con IOS 12.2.20.SE1

Switch Cisco 3750-48TS-S con IOS 12.2.20.SE1

b) Configuración de los servidores del sistema de administración de red

Adición de objetos al DNS

El DNS es un sistema de base de datos distribuido que contiene información de nombres acerca de los elementos de red. El sistema proporciona el servicio de convertir los nombres de hosts en direcciones IP y viceversa.

c) Configuración del router y switch Cisco

Configuración inicial del router o switch Cisco

La configuración inicial del switch y router Cisco involucra los siguientes pasos:

Conexión al puerto de consola

Usando el conector RJ-45 y el apropiado adaptador podremos conectar la consola o PC al router/switch de Cisco. La interfase de línea de comandos nos permitirá configurar y monitorear el switch/router. Seguidamente, la configuración de la Terminal de Aplicación con las características físicas por defecto: Tasa de 9600 baudios, 8 bits de datos, sin paridad y sin control de flujo.

Configuración de passwords

a) Ingresar al modo privilegiado

```
routerTest> enable
```

b) Ingresar al modo de configuración global

```
routerTest# configure terminal
```

c) Configurar los passwords

```
routerTest(config)# enable secret <password>
```

Configuración del router y switch para el acceso por telnet

a) Desde el modo de configuración global, ingresar al modo de configuración de línea

```
routerTest(config)# line vty 0 4
```

b) Habilitar la autenticación de la línea

```
routerTest(config-line)# login
```

c) Ingresar el password que será utilizado para el telnet

```
routerTest(config-line)# password <password>
```

d) Retornar al modo de configuración global

```
routerTest(config-line)# exit
```

Proveer la configuración por defecto con un template de configuración

a) Se puede construir un archivo de plantilla para acelerar el procedimiento de configuración de los routers y switches

b) Luego de construirlo se puede copiar y pegar el contenido en la configuración global

```
routerTest# configure terminal
routerTest(config)# <pegar el contenido de la plantilla>
routerTest(config)# [CTRL]+Z
```

c) Por razones de seguridad, cambiar el password de la consola preconfigurada

```
routerTest(config)# line con 0
routerTest(config-line)# password <password>
```

d) Salvar la configuración

```
routerTest# copy running-config startup-config
```

Para descargar una base de datos de las VLAN al switch, se debe realizar lo siguiente:

a) En el modo enable

```
switchTest# copy xmodem flash
```

b) Ingresar el nombre del archivo de destino y confirmar la sobre escritura

```
Destination filename []? vlan_database.dat
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
```

c) Iniciar la transferencia xmodem en el terminal de aplicación

d) Reiniciar el switch

```
switchTest# reload
Proceed with reload? [confirm]
```

Activación de las interfases del switch

Después de realizar la configuración con el archivo de plantilla, activar solo aquellas interfases las cuales serán usadas en la configuración de la red de comunicación de datos.

a) Desde el modo de configuración global, ingresar al modo de configuración de interfase

```
switchTest(config)# interfase fastethernet <number>
```

b) Activar la interfase

```
switchTest(config-if)# no shutdown
```

c) Realizar los pasos a) y b) para las demás interfases

d) Salir del modo de configuración de interfase

```
switchTest(config-if)# exit
```

La solución a utilizar en la red de comunicación de datos será Estándar

Asignación de un puerto del switch a la VLAN

a) Desde el modo de configuración global, ingresar la configuración de la interfase

```
switchTest(config)# interface fastethernet 0/<int_number>
```

b) Asignar la interfase a la VLAN

```
switchTest(config-if)# switchport access vlan <number>
```

c) Si el dispositivo conectado al puerto no es un switch sino un MSC, HLR, PC u otro router que no participa en el proceso spanning tree, deshabilitar el spanning tree en el puerto como sigue

```
switchTest(config-if)# spanning-tree portfast
```

d) Habilitar la interfase

```
switchTest(config-if)# no shutdown
```

e) Salir del modo de configuración de interfase

```
switchTest(config-if)# exit
```

Configuración de las direcciones IP

Tabla 5.2: Requerimientos IP del backbone de la red de comunicación de datos

Equipo	Interfase	VLAN	Número de VLAN	IP	HSRP	OSPF	Observación
router1 de la dcn	FastEthernet 0/0.A	VLAN A	A	Yes	Yes	No	
	FastEthernet 0/0.F	VLAN F	F	Yes	Yes	No	Si los elementos de red 2G usan TCP/IP
	FastEthernet 0/0.G	VLAN G	G	Yes	Yes	No	HSRP es necesario si los hosts IP están presentes
	FastEthernet 0/0.H	VLAN H	H	Yes	Yes	No	HSRP es necesario si los hosts IP están presentes
	FastEthernet 0/0.I	VLAN I	I	Yes	No	Yes	
router2 de la dcn	FastEthernet 0/0.A	VLAN A	A	Yes	Yes	No	
	FastEthernet 0/0.F	VLAN F	F	Yes	Yes	No	Si los elementos de red 2G usan TCP/IP
	FastEthernet 0/0.G	VLAN G	G	Yes	Yes	No	HSRP es necesario si los hosts IP están presentes
	FastEthernet 0/0.H	VLAN H	H	Yes	Yes	No	HSRP es necesario si los hosts IP están presentes
	FastEthernet 0/0.I	VLAN I	I	Yes	No	Yes	
switch1 de la dcn	VLAN A	VLAN A	A	Yes	No	No	
switch2 de la dcn	VLAN A	VLAN A	A	Yes	No	No	

Para configurar las direcciones IP, se deben seguir los siguientes pasos

a) Desde el modo de configuración global, ingresar al modo de configuración de interfase

```
routerTest(config)# interface <int_name> <int_index>
```

b) Configurar la dirección IP de la interfase

```
routerTest(config-if)# ip address <ip_address> <net_mask>
```

c) Salir del modo de configuración

```
routerTest(config-if)# exit
```

Donde:

<password> : Password a configurar

<number> o <int_number> : Número de la interfase

<int_name> : Interfase (FastEthernet en el router y VLAN para el switch)

<ip_address> : Dirección IP para asignar

<int_index> : Indice de la interfase

<net_mask> : Máscara de red

Configuración del HSRP

El HSRP es un protocolo propietario de Cisco. Es usado en el backbone DCN para proporcionar un backup a un router en el caso de una falla. Los routers del backbone DCN que usan el HSRP trabajan juntos para presentar la apariencia de un solo router virtual en una LAN virtual (VLAN) en particular. Los routers comparten las mismas direcciones virtuales IP y MAC que los hosts deben usar como gateway por defecto. Si un router falla, los hosts son capaces de continuar el envío de los paquetes a una dirección IP y MAC, el cual será movido automáticamente a otro router. El proceso de transferencia de las responsabilidades de enrutamiento de un dispositivo a otro es transparente para el usuario final.

Este protocolo es configurado para proporcionar un gateway por defecto redundante para los hosts IP y por lo tanto es configurado solo para aquellas interfases donde existen hosts IP presentes.

Para configurar la dirección IP standby:

a) Ingresar al modo de configuración de la interfase

```
routerTest(config)# interface <int_name> <int index>
```

b) Configurar la dirección IP standby

```
routerTest(config-if)# standby <group> ip <ip_address>
```

c) Especificar la prioridad standby de la interfase

```
routerTest(config-if)# standby <group> priority <priority>
routerTest(config-if)# standby <group> preempt
```

Donde:

<priority> : Prioridad de la interfase usada cuando se selecciona un router activo

<group> : Número de grupo standby

El comando de configuración de la interfase, standby IP, habilita el HSRP y establece la dirección IP del router virtual. Los routers comparten la misma dirección IP virtual. La configuración de por lo menos uno de los routers en el grupo standby debe especificar la dirección IP del router virtual, la especificación de la dirección IP del otro router es opcional para los otros routers en el mismo grupo standby.

El comando de configuración de la interfase, standby priority, establece la prioridad HSRP del router. La configuración del router que incluya éste comando, hará que ese router sea el router activo por defecto.

El comando de configuración de la interfase, standby preempt, permite al router llegar a ser el router activo cuando su prioridad es más alta que los otros routers configurados con HSRP en el grupo standby. Cada router puede ser el router standby para el otro router. Si no se usa el comando, standby preempt, en la configuración de un router, ese router no llega a ser el router activo.

d) Retornar al modo de configuración global

```
routerTest(config-if)# exit
```

Configuración del protocolo OSPF

Para mantener la redundancia del enrutamiento IP dentro del backbone DCN se utiliza el protocolo OSPF, el cual es un protocolo de enrutamiento dinámico que proporciona una rápida convergencia, alta escalabilidad y requiere menos ancho de banda de red para las actualizaciones. Si una falla ocurre en la trayectoria del encaminamiento, el OSPF actualiza inmediatamente las tablas de enrutamiento, así los paquetes IP son reencaminados sobre enlaces backup.

Para definir las redes que participarán en el OSPF:

a) Desde el modo de configuración global, ingresar al modo de configuración del OSPF

```
routerTest(config)# router ospf <process-id>
```

b) Configurar las redes que participaran en OSPF

```
routerTest(config-router)# network <interface_IP> 0.0.0.0
area <area_number>
```

c) Habilitar la publicación de las subredes conectadas sobre el sistema autónomo OSPF

```
routerTest(config-router)# redistribute connected subnets
```

d) Salir del modo configuración del router

```
routerTest(config-router)# exit
```

Donde:

<process_id> : Identificador del proceso OSPF

<interface_IP> : Dirección IP de la interfase

<area_number> : Número de área

El comando, router ospf process-id, crea un proceso OSPF en el router.

El comando, network area, habilita al OSPF a operar en una interfase.

El comando, redistribute, permite redistribuir las rutas desde un dominio de enrutamiento a otro.

Opcional - Configuración del SNMP

Los routers y switches pueden ser configurados para enviar los traps SNMP al sistema de administración de red cuando ocurren ciertos eventos.

Para configurar los traps SNMP en el router Cisco:

a) Definir la cadena de acceso de la comunidad SNMP

```
routerTest(config)# snmp-server community <string> ro
```

b) Definir la interfase cuya dirección IP será usada como una dirección origen cuando se envían los traps SNMP al sistema de administración de red

```
routerTest(config)# snmp-server trap-source <interface>
```

c) Definir el host que recibirá los traps SNMP

```
routerTest(config)# snmp-server host <address> <string>
```

d) Habilitar el envío de los traps SNMP

```
routerTest(config)# snmp-server enable traps
```

Para configurar los traps SNMP en el switch Cisco:

a) Definir la cadena de acceso de la comunidad SNMP

```
switchTest(config)# snmp-server community <string> ro
```

b) Definir el host que recibirá los traps SNMP

```
switchTest(config)# snmp-server host <address> traps
<host_community>
```

Donde:

<string> : Cadena de la comunidad local SNMP

<interface> : Interfase cuya dirección IP fue usada al definir el objeto de red en el sistema de administración de red

<address> : Dirección IP del paquete del sistema de administración de red

Opcional - Configuración del NTP y TZ

Los routers y switches Cisco tienen sus propios relojes internos. Esto les permite simplificar los eventos de rastreo (tracking) asignando información de tiempo en los mensajes (debug) y traps SNMP. El NTP es utilizado para proporcionar un tiempo de referencia desde el sistema de administración de red.

Para configurar el NTP y el TZ:

a) Ingresar el siguiente comando en el modo de configuración global

```
routerTest(config)# ntp Server <ip_address>
```

b) Configurar la zona de tiempo local

```
routerTest(config)# clock timezone <timezone> <offset>
```

Donde:

<ip_address> : Es la dirección IP del nodo en donde el paquete del sistema está corriendo

<timezone> : Cadena de texto de la zona de tiempo local

<offset> : Desfasaje de tiempo del GMT

Opcional - Mensajes de logs del sistema

El router envía las salidas de los comandos debug y mensajes de error del sistema al terminal de consola. Se puede utilizar cualquier servidor del sistema de administración de red como un servidor de logs para recibir los mensajes desde los switches y routers.

Para redireccionar los mensajes de logging al servidor del sistema de administración de red:

a) Ingresar el siguiente comando en el modo de configuración global

```
routerTest(config)# logging <ip_address>
```

b) Definir el nivel de detalle de los mensajes de log

```
routerTest(config)# logging trap <level>
```

Debido a que estos eventos utilizan recursos de CPU, es recomendable deshabilitarlo a menos que sea utilizado para monitorear eventos de error.

```
routerTest(config)# no logging console
routerTest(config)# show logging
```

Donde:

<ip_address> : Es la dirección IP del servidor del sistema de administración de red

<level> : Nivel del detalle de información

Salvar la configuración actual a la memoria RAM no volátil (NVRAM)

Para salvar la configuración a la NVRAM:

```
routerTest# copy running-config startup-config
```

d) Configuración de parámetros ISO IP

Configuración del enrutamiento dinámico IS-IS

El IS-IS es otro protocolo de enrutamiento dinámico que es usado en el backbone DCN para el enrutamiento CLNS. Sus características son similares al OSPF. El IS-IS utiliza el proceso de enrutamiento para recolectar las direcciones destinos disponibles y construir las tablas de enrutamiento. Esto ocurre cada vez que ocurra un cambio en la topología de la red o en el tráfico.

Para configurar el enrutamiento dinámico IS-IS:

a) Ingresar al modo de configuración global

```
routerTest# configure terminal
```

b) Habilitar el enrutamiento IS-IS e ingresar al modo configuración del router

```
routerTest(config)# router isis dcn
```

c) Configurar la entidad de red (NET: Network Entity Title) para el proceso de enrutamiento

```
routerTest(config-router)# net <NET>
```

d) Salir del modo configuración del router

```
routerTest(config-router)# exit
```

e) Salir de los modo de configuración global y configuración de la interfase

Presionar: [CTRL] + Z

Donde:

<NET> : Network Entity title. También conocida como la NSAP del router

Configuración de las conexiones a los elementos de red

Una vez que la configuración del router está completa, determinar las interfases a configurar.

Interfase Lógica LAN o serial: Tarjeta de los elementos de red o Interfase serial

Configuración de las interfases seriales

Las interfases seriales permiten la conexión a una red pública de paquetes usando X25.

Interfase Lógica: Serial

Interfase Física: Serial Síncrona o E1-G.703

Configuración de las interfases seriales sincrónicas

Para configurar la interfase serial síncrona:

a) Ingresar al modo de configuración global

```
routerTest# configure terminal
```

b) Configurar los parámetros seriales síncronos

```
routerTest(config)# interfase serial <slot>/<port>
routerTest(config-if)# shutdown
routerTest(config-if)# encapsulation x25 dce
routerTest(config-if)# clock rate <clock_rate>
routerTest(config-if)# x25 address <rp_x121>
routerTest(config-if)# x25 htc 16
routerTest(config-if)# x25 map clns <ne_x121> broadcast
routerTest(config-if)# clns router isis dcn
routerTest(config-if)# no shutdown
```

Donde:

<slot> :	Número de slot del router
<port> :	Número del puerto asignado a un elemento de red
<clock_rate> :	Velocidad de la interfase
<rp_x121> :	Dirección X121 del puerto del router
<ne_x121> :	Dirección X121 del elemento de red

Normalmente, los routers son asignados como Equipo de comunicación de datos DCE y los elementos de red como Equipos terminales de datos DTE.

c) Salir de los modos de configuración de interfase y global, con [CTRL] + Z

d) Verificar la configuración:

```
routerTest# show running-config
```

Para incrementar el tamaño de paquete y ventana X25, ingresar los siguientes comandos:

```
routerTest(config-if)# x25 ips bytes
routerTest(config-if)# x25 ops bytes
routerTest(config-if)# x25 win packets
routerTest(config-if)# x25 wout packets
```

El parámetro htc (x25 htc channel) establece el canal bidireccional más alto (HTC: Highest Two-ways Channel). El canal (channel) es un número desde 1 a 4095.

Las redes usan tamaños de paquete máximo de entrada y salida. El parámetro ips especifica el tamaño de paquete de entrada y ops especifica el tamaño de paquete de salida. Estos parámetros están dados en bytes en el rango de 128 y 1024.

El parámetro win especifica el límite superior del número de paquetes no reconocidos en la ventana de entrada. Mientras que el parámetro wout especifica el límite superior de paquetes no reconocidos en la ventana de salida.

El mismo tamaño de paquete y tamaño de ventana X25 debe ser configurado en todos los switches x25 en la ruta entre el router y el elemento de red y en el mismo elemento de red.

Configuración de las interfases E1

Las interfases E1 son utilizadas para proporcionar conexiones X25 sobre PCM usando el estándar G.703. La interfase en el elemento de red tiene la capacidad para transmitir y recibir datos a la velocidad de 2.048 Mbps a través de un cable serial canalizado.

Para configurar las interfases E1:

a) Ingresar al modo de configuración global

```
routerTest# configure terminal
```

b) Configurar el tipo de tarjeta

```
routerTest(config)# card type e1 <slot>
```

c) Ingresar al modo de configuración del controlador

```
routerTest(config)# controller e1 <slot/port>
```

d) Definir el código de línea

```
routerTest(config-controller)# linecode <format>
```

e) Seleccionar el reloj del origen

```
routerTest(config-controller)# clock source line
```

f) Seleccionar la terminación de línea

```
routerTest(config-controller)# line termination { 75 ohms
120 ohms }
```

g) Configurar el frame

```
routerTest(config-controller)# framing <type>
```

h) Configurar el resto de parámetros de la interfase E1

```
routerTest(config-controller)# channel-group <grp>
timeslots <TSL>
```

```
routerTest(config-controller)# interface serial
<slot/port>:<grp>
routerTest(config-if)# shutdown
routerTest(config-if)# encapsulation x25 dce
routerTest(config-if)# x25 address <router_x121>
routerTest(config-if)# x25 htc 16
routerTest(config-if)# x25 map clns <ne_x121> broadcast
routerTest(config-if)# clns router isis dcn
routerTest(config-if)# no shutdown
```

i) Salir del modo conficuración global y de interfase con [CTRL] + Z

j) Verificar la configuración

```
routerTest# show running-config
```

Donde:

<format> : Formato del código de línea. Como b8zs, hdb3, etc

<type> : Tipo de frame. Como crc4

<slot> : Número de slot

<grp> : Número de grupo de canal a asignar

<TSL> : Intervalo de tiempo usado por el grupo de canal

<slot/port> : Número de la interfase lógica asignada al controlador E1

<router_x121> : Dirección X121 del router

<ne_x121> : Dirección X121 del elemento de red

El comando, linecode, configura el formato del código de línea a la codificación AMI (Alternate Mark Inversion) o HDB3 (High-Density Bipolar 3), etc. para el enlace E1.

El comando, framing, configura el formato de frame para el enlace E1 con CRC (Cyclic Redundancy Check) (crc4).

El comando, clock source line, configura el controlador E1 para obtener la fuente de reloj del router desde un dispositivo conectado de la red.

El comando, line termination, especifica la impedancia para la terminación E1. Los niveles de impedancia son mantenidos para evitar corrupción en los datos sobre enlaces a grandes distancias.

El comando, channel group timeslot, define los intervalos de tiempo (timeslots) para cada circuito E1. El número del grupo de canal depende si la línea de datos es T1 (valores del 0 al 23) o E1 (valores del 0 al 30). El rango de timeslots pertenece al grupo de canal. Para el controlador T1, el rango de timeslots va desde el 1 al 24. Para el controlador E1, el rango va desde el 1 al 31.

El enrutamiento CLNS es habilitado por defecto en el router cuando se configura el enrutamiento dinámico IS-IS. El comando, clns router isis, especifica las interfases que deben estar enlutando activamente el IS-IS.

Salvar la configuración del router

Para salvar la configuración del router:

```
routerTest# copy running-config startup-config
```

5.2 Integración del elemento de red del subsistema BSS

Los enlaces de comunicación (LAN o X.25) desde el BSC hacia el sistema de administración de red son establecidos a través de las unidades funcionales y unidades plug-in de hardware. El procedimiento correcto de configuración depende de la topología de red, el servicio de red utilizado y el hardware en el BSC.

5.2.1 Hardware

El hardware involucrado en la integración del BSC cubre los siguientes tópicos:

Tarjetas de red

Sistemas Intermedios

a) Tarjetas de red

Las tarjetas de red para la integración están ubicadas en la Unidad de operación y mantenimiento del BSC. El modelo de la tarjeta de red usada depende del tipo de BSC y el tipo de conexión.

La tarjeta AC25-S/A permite la conexión de canales de transmisión de datos síncronos siguiendo el protocolo HDLC. Estas tarjetas son utilizadas para conexiones X.25 en el DX200.

La tarjeta AS7-B/U/V es un terminal multicanal usado para controlar canales de señalización LAPD. Estas tarjetas son también usadas para conexiones X25 sobre PCM.

La tarjeta CP6LX es una unidad plug-in que está ubicada en la OMU del BSC y tiene una interfase ethernet 10/100 Mbit.

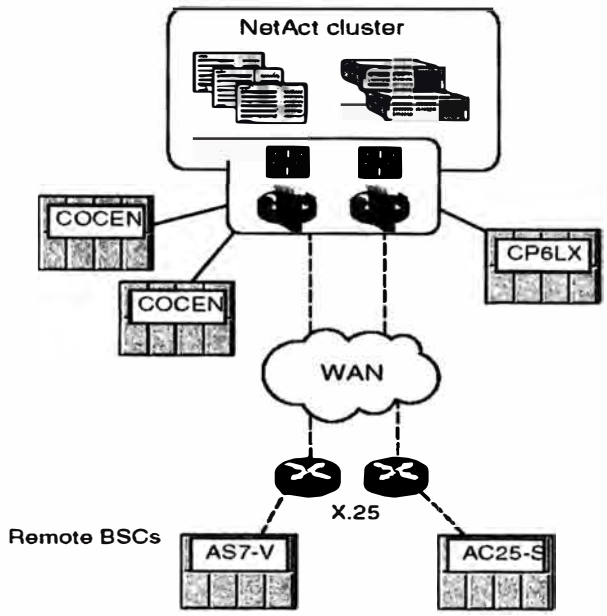


Figura 5.3: Tarjetas de red en el BSC

- La tarjeta COCEN es utilizada para conexiones LAN IEEE 802.3. Estas tarjetas son conectadas usando cable 10Base2 (Coaxial), 10Base5 (AUI) o 10BaseT.

b) Sistemas Intermedios

Debido a la configuración de red existente, pueden existir sistemas intermedios (IS) en la red. Para mantener la estructura de ésta red, el uso de un sistema intermedio encamina los datos desde un elemento de red al sistema de administración de red.

5.2.2 Tareas preliminares

a) Obtención de la información del sistema

Antes de realizar la integración, se debe asegurar la obtención de información del sistema:

- Servidores del Sistema de administración de red: Hardware, rol de cada servidor, versiones de la aplicación y documentación, nombres de hosts, passwords, direcciones IP de todas las interfases y direcciones NSAP.
- Elementos de red: Hardware, rol, versión de software, nombres de hosts, passwords, direcciones IPs, dirección NSAP y el número C.

b) Revisión de los requerimientos del sistema

Sistema de Administración de Red

- Verificación de la versión del sistema de administración de red.

Disponibilidad del password para los usuarios bases del sistema de administración de red: SYSOP (Usuario para acceso al sistema) y TRAFADM (Usuario para la transferencia de archivos).

Elemento de red

BSC

Verificación de la versión del software instalado en el BSC.

Verificación de la activación de parámetros de configuración.

c) Creación de los objetos a ser supervisados en el sistema de administración de red

Antes que el sistema de administración de red pueda recibir y almacenar datos del elemento de red, se debe crear el objeto que será manejado en el sistema de administración. Esto consiste en crear un objeto en una vista general para la supervisión y cuyos parámetros de configuración serán almacenados en la Base de Datos del sistema de administración de red.

d) Creación y modificación del usuario administrador en el BSC

El perfil del usuario administrador es necesario por la aplicación del sistema de administración de red para la creación, modificación y control de los perfiles de grupos de usuarios.

Para crear o modificar el perfil de grupo del usuario administrador:

Se debe iniciar una sesión de lenguaje hombre-máquina MML en el BSC.

El perfil de grupo del usuario administrador debe tener los altos niveles de autorización definidos en el BSC.

Crear el identificador del grupo del usuario administrador.

5.2.3 Configuración de los servidores del Sistema de Administración de Red

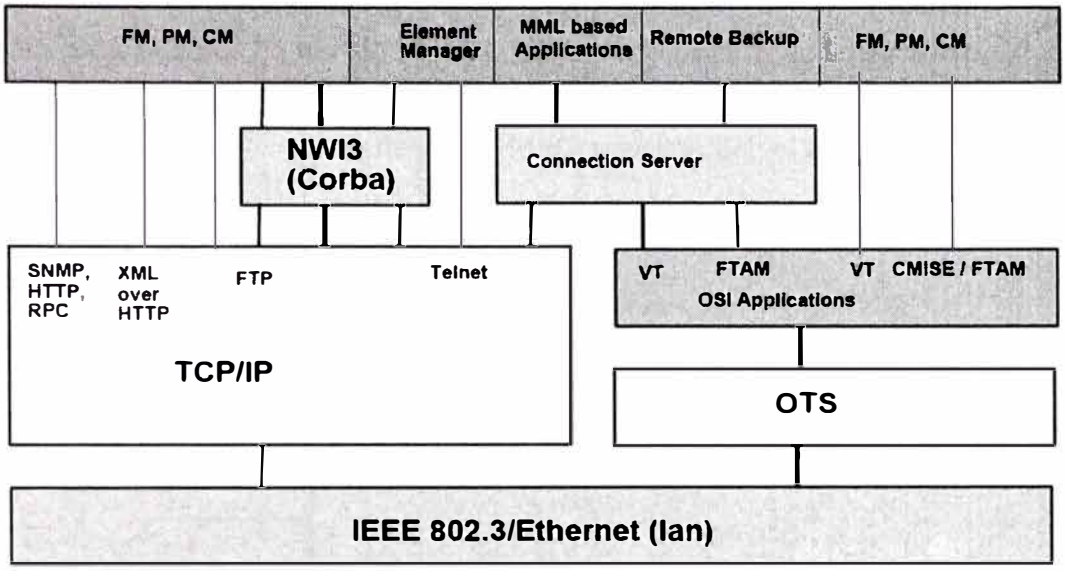


Figura 5.4: Modelo de las aplicaciones en los servidores del NMS

En el servidor extremo del sistema de administración de red, se utiliza el TCP/IP e ISO IP sobre LAN.

a) OTS

OTS provee servicios de capa de red sobre el cual corren las aplicaciones OSI. Estas aplicaciones son usadas por los elementos de red de segunda generación (2G).

b) Aplicaciones OSI

Las aplicaciones OSI proveen servicios para:

Transferencia de Archivos

FTAM: Mediciones (tráfico) y recarga de alarmas.

Eventos

CMISE: Alarmas, eventos de la red de radio, notificaciones de transferencia de mediciones.

VT: Proporciona la conexión terminal a los elementos de red.

TCP/IP

Las aplicaciones basadas en TCP/IP son usadas principalmente para integraciones de elementos de red de tercera generación (3G) y PaCo (Packet Core), excepto para los elementos de red NSS en un determinado nivel de software que pueden usar OSI o TCP/IP y SGSN de segunda generación (2G) que usa OSI. OSI (FTAM/VT) y TCP/IP (telnet) pueden usar Servidor de conexión (Connection Server).

c) Direccionamiento IP en los servidores UNIX

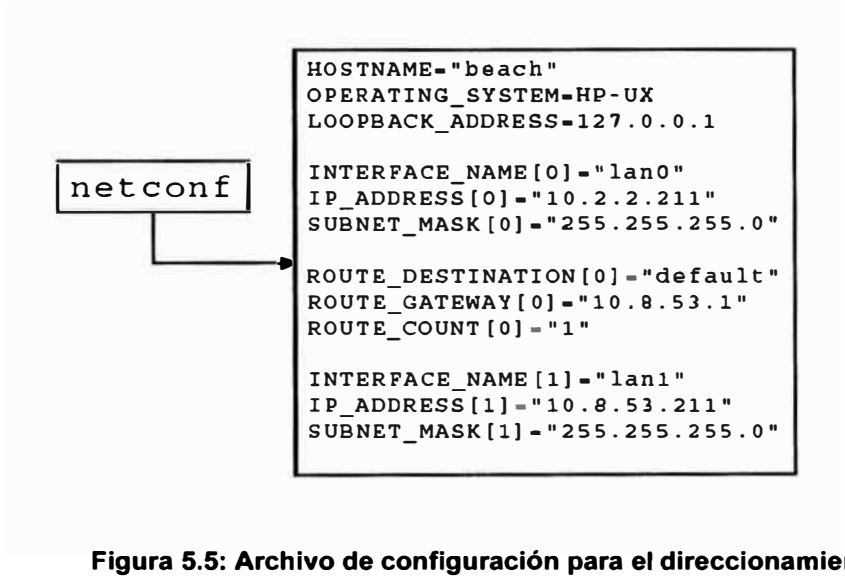


Figura 5.5: Archivo de configuración para el direccionamiento IP

El direccionamiento IP de los servidores unix está definido en el archivo netconf. Las direcciones IP para las interfases físicas se encuentran definidas en éste archivo.

La configuración por defecto de las direcciones IP del sistema de administración de red, NetAct, está definida por una interfase de heartbeat (lan0) y la interfase de comunicación (lan1). De la misma manera, la información de enrutamiento que está definida en éste archivo significa el gateway por defecto.

d) Direccionamiento OSI en los servidores UNIX

El direccionamiento OSI está definido separadamente del direccionamiento TCP/IP, sin embargo las mismas interfases físicas son usadas.

ots_subnets

```
snet_clns_8023              clnslan1
snet_local_net_address      39246F000001160000000100250100080532l100
.
.
.
snet_query_subnet           1   #    0    1    0
.
.
.
snet_if_name                lan1  # 802.3 device interface name
```

Figura 5.6: Archivo ots_subnets

La dirección OSI (NSAP) para los servidores unix está definido en el archivo ots_subnets. En adición a la propia dirección NSAP del servidor, el archivo también tiene información acerca del nombre de la subred CLNS snet_clns_8023 y el parámetro snet_query_subnet. La interfase física de red usada para las conexiones OSI está definida en la variable snet_if_name.

ots_routes

```
route_id            00      # hexadecimal number
route_id_mask       00      # hexadecimal bitmask
route_out_subnet    clnslan1
route_primary       39246F000001160000000100250100080530020O
```

Figura 5.7: Archivo ots_routes

El gateway por defecto de las conexiones OSI para el servidor unix está definido en el archivo ots_routes. El archivo contiene también el nombre de la subred route_out_subnet. Este debe ser igual al nombre de la subred en ots_subnets. El valor 00 para route_id y route_id_mask define que la ruta es una ruta por defecto.

El paquete tiene también una dirección NSAP que es definido durante la instalación en el archivo arch1_conf.cfg. Durante el inicio del cluster Service Guard, la dirección NSAP es leída y activada por el sistema. Cuando el cluster es parado, el NSAP del paquete es desactivado y los servicios OTS también son parados.

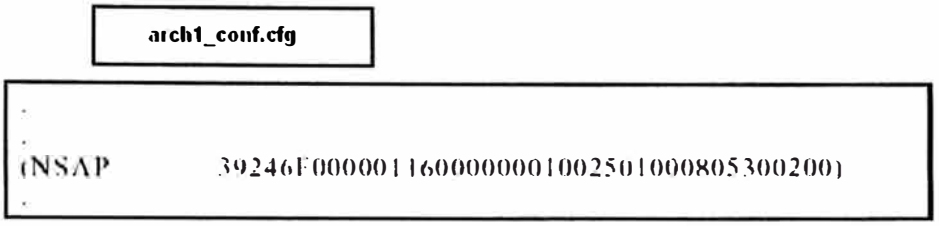


Figura 5.8: Archivo arch1_conf.cfg

e) Configuración de las aplicaciones OSI

El direccionamiento de la conexión hacia el elemento de red está definido en el archivo arch2_conf.cfg. La variable psap define los selectores y la dirección NSAP para un elemento de red, es decir, la dirección NSAP debe ser la dirección del elemento de red.

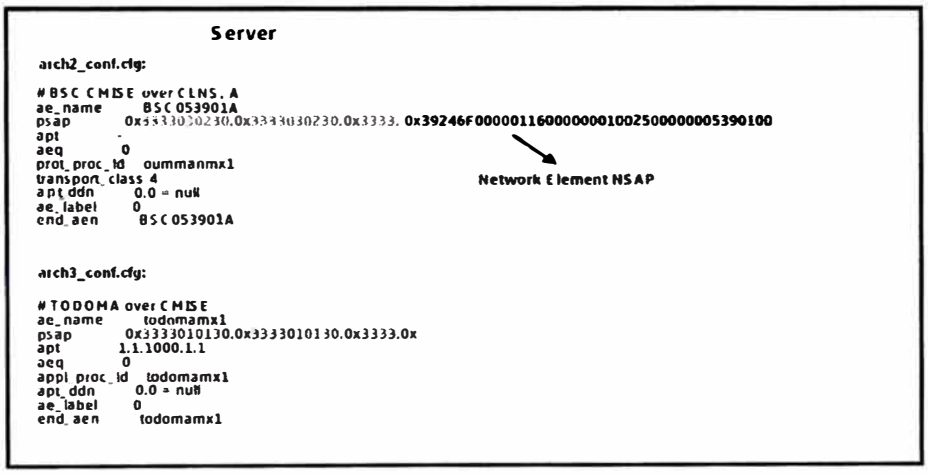


Figura 5.9: Archivos arch2_conf.cfg y arch3_conf.cfg

Los selectores son parámetros que definen las conexiones de las aplicaciones a través del nivel OSI. En el ejemplo, el selector de la capa de presentación P es 3333030230, el selector de la capa de sesión S es 3333030230 y el selector de la capa de transporte T es el 3333. Cada aplicación tiene sus propios selectores.

Las aplicaciones OSI locales para los servidores del sistema de administración de red son definidos en el archivo arch3_conf.cfg.

f) Servidor de conexión

El servidor de conexión es usado principalmente para tomar las sesiones del terminal remoto a los elementos de red con la aplicación VT, pero también puede ser configurado para usar FTAM para el backup remoto de los elementos de red o sesiones telnet.

```
(arcName "A_SSRV_APPL_PROTOCOL_XYNEABCD"
(maxConns                          "N#")
(address                           "NE_12345APPL")
(connChannel                       "processA")
(loginSeqFileName                  "script1.cfg")
(logoutSeqFileName                 "script2.cfg")
)
(routeName "R_SSRV_APPL_PROTOCOL_XYNEABCD"
(arcs          "A_SSRV_APPL_PROTOCOL_XYNEABCD")
(host          "testbed")
(port          "WXYZ")
(checkScript   "")
(commandLine   "script3.cfg")
)
(Id "67"
(tecName       "XYNEABCD")
(maxMMLConns   "N#")
(maxFileConns  "N#")
(maxSpontConns "N#")
(totalMaxConns "18")
(edMMLConns    "Y")
(edFileConns   "Y")
(edSpontConns  "Y")
(edAllConns                        "Y")
(edMMLLog                          "N")
(edFileLog                         "N")
(edSpontLog    "N")
(edAllLog                          "N")
(users ""
               (groups "prueba"
                                   (connTypes "MML_HUMAN,MML_MACHINE"
               (routes"R_SSRV_APPL_PROTOCOL_XYNEABCD")
                                   )
               )
)
```

Figura 5.10: Archivo arch_princ.cfg

Existen 3 partes principales para definir una conexión a un elemento de red: arc, route (ruta) y node (nodo). El admin route, es usado para la supervisión de las conexiones del servidor de conexión y la creación de las alarmas en caso de problemas de conexión.

Un arc define que aplicaciones y los scripts de login que son usados para la conexión. El arc está definido para un elemento de red integrado por OSI usando la aplicación VT (APPL). Por ejemplo, en caso de una conexión telnet, la dirección es el nombre del elemento de red (para el cual una dirección IP es definida en el DNS) y el connChannel sería telnet.

En route (ruta), el arc en uso es definido con el nombre del paquete del service guard y el puerto usado para la conexión.

El node (nodo) define la conexión para el objeto en la base de datos del sistema de administración de red. Este mapeo es hecho en la variable id que debe tener el id interno del objeto en la base de datos.

La definición del nodo también contiene información acerca del usuario quién toma la conexión. En la variable groups el grupo de usuarios UNIX es definido y todos los usuarios que pertenecen a éste grupo son permitidos a tomar la conexión. El grupo UNIX es mapeado a un usuario del elemento de red en la base de datos del sistema de administración de red.

5.2.4 Configuración del elemento de red

a) Configuración de la conexión física

Usando LAN

Las tareas que se deben realizar cuando se utiliza LAN, son las siguientes:

Instalación y configuración de las tarjetas y switches en el elemento de red.
Configuración del objeto CLNS.
Configuración del objeto de enlace (linkage object).
Creación de las direcciones NSAP local y remota.
Creación de las direcciones de red local y remota.
Conexión de las direcciones NSAP a las direcciones de red.
Configuración de las aplicaciones locales y remotas.

Usando X.25

La configuración de la conexión física usando X.25 requiere las siguientes tareas:

Instalación y configuración de la tarjeta de comunicaciones en el elemento de red.
Creación de la terminal de datos.
En ésta parte se define el tipos de interfase: V24, V35 o V36.
Creación y modificación de los parámetros X.25.
Creación del canal físico.
Configuración del objeto CLNS.
Configuración del objeto de enlace.
Creación de las direcciones NSAP local y remota.

- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAP a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.
- Verificación de la conexión física

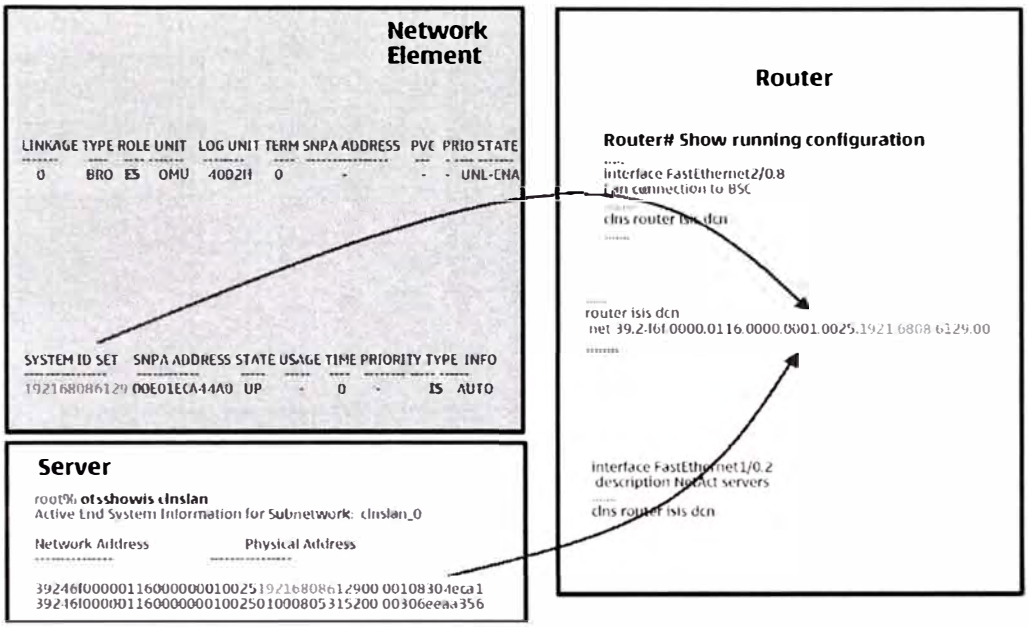


Figura 5.11: Verificando las conexiones OSI con LAN

Usando X.25 sobre PCM

Las tareas requeridas para la configuración de las conexiones físicas para el X.25 sobre PCM son las siguientes:

- Instalación y configuración de la tarjeta en el elemento de red.
  En éste punto se debe crear la conexión PCM para la unidad funcional.
- Instalación y configuración en la Terminal de Intercambio (ET).
  En éste punto también se debe crear una conexión PCM.
- Configuración de las conexiones semipermanentes.
  La comunicación hacia la MSC/HLR se hace configurando una conexión semipermanente entre los intervalos de tiempo en la línea PCM al BSC y los dispositivos de enrutamiento. Las líneas PCM externas son conectadas de manera semipermanente al Switch Group del MSC/HLR.
- Creación y modificación de los parámetros X.25 (para conexiones digitales).
- Creación del canal físico.
- Creación del objeto CLNS.
- Creación del objeto de enlace.

- Creación de las direcciones NSAP local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAP a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.
- Verificación de la conexión física.

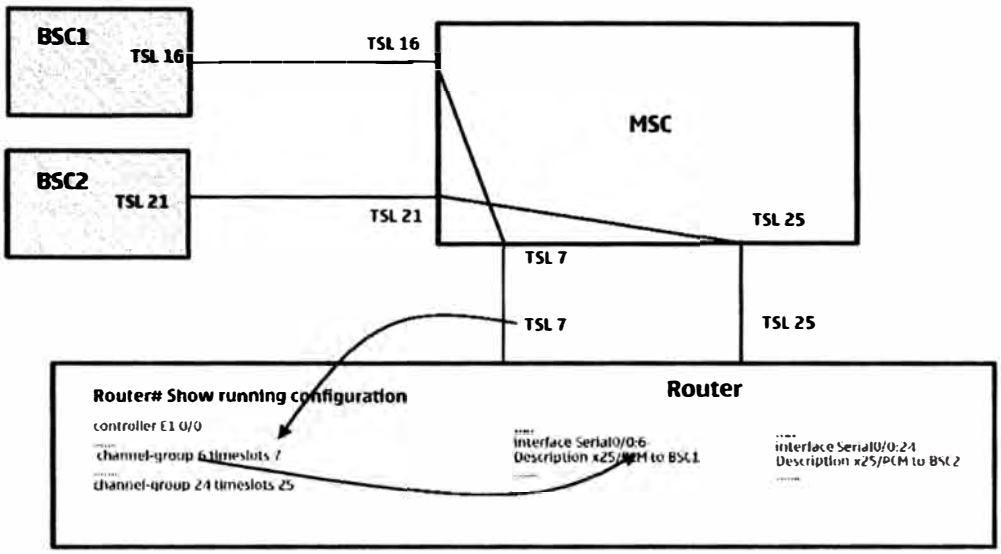


Figura 5.12: Conexiones semipermanentes PCM

b) Configuración de la subred OSI

Configuración del objeto CLNS

- Verificación de la existencia de otro objeto CLNS, de no existir, crear un nuevo objeto.
- Desbloqueo del objeto CLNS creado.
- Inicialización del objeto CLNS.

Configuración del objeto de enlace

- Si se utiliza CLNS sobre X.25, crear un objeto de enlace X.25 para cada tarjeta. Si se utiliza LAN, crear un objeto de enlace broadcast.
- Desbloqueo del objeto de enlace creado.
- Reinicialización del objeto CLNS.

Creación de las direcciones NSAP y direcciones de red

Las direcciones NSAP y las direcciones de red son utilizadas para asociar los servicios con los elementos de red. Antes de establecer una conexión desde el sistema de administración de red al elemento de red, las direcciones NSAP y direcciones de red deben ser creadas en todos los elementos de red.

Para crear las direcciones de red y NSAP, se deben realizar las siguientes tareas:

- Definición de los parámetros por defecto de la dirección de área.
- Creación de la dirección NSAP local.
- Creación de la dirección NSAP remota.
- Creación de la dirección NSAP del paquete del sistema.
- Creación de la dirección de red local.
- Creación de la dirección de red remota.

Conexión de las direcciones NSAP a las direcciones de red

- Conexión de la dirección de red local a la dirección NSAP local.
- Conexión de la dirección de red remota a la dirección NSAP remota.
- Desbloqueo de las direcciones NSAP remota y local.
- Creación de conexiones redundantes, a través de nuevas direcciones de red y NSAP.

c) Configuración de las aplicaciones y direcciones OSI

Creación de las aplicaciones OSI locales

- Creación de la aplicación local en el elemento de red.

En éste punto se definen los selectores de transporte, sesión y presentación.

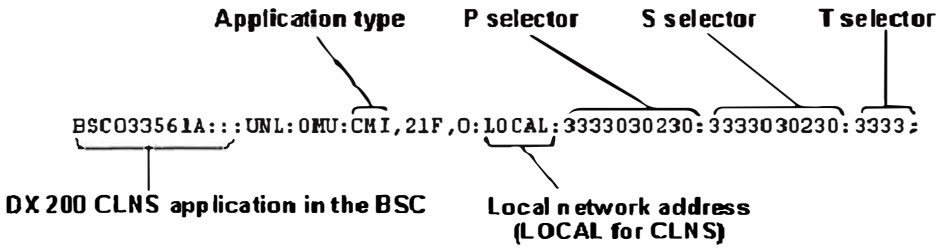


Figura 5.13: Parámetros para la aplicación CLNS local en el BSC

Asegurar que los estados estén en el modo desbloqueado.

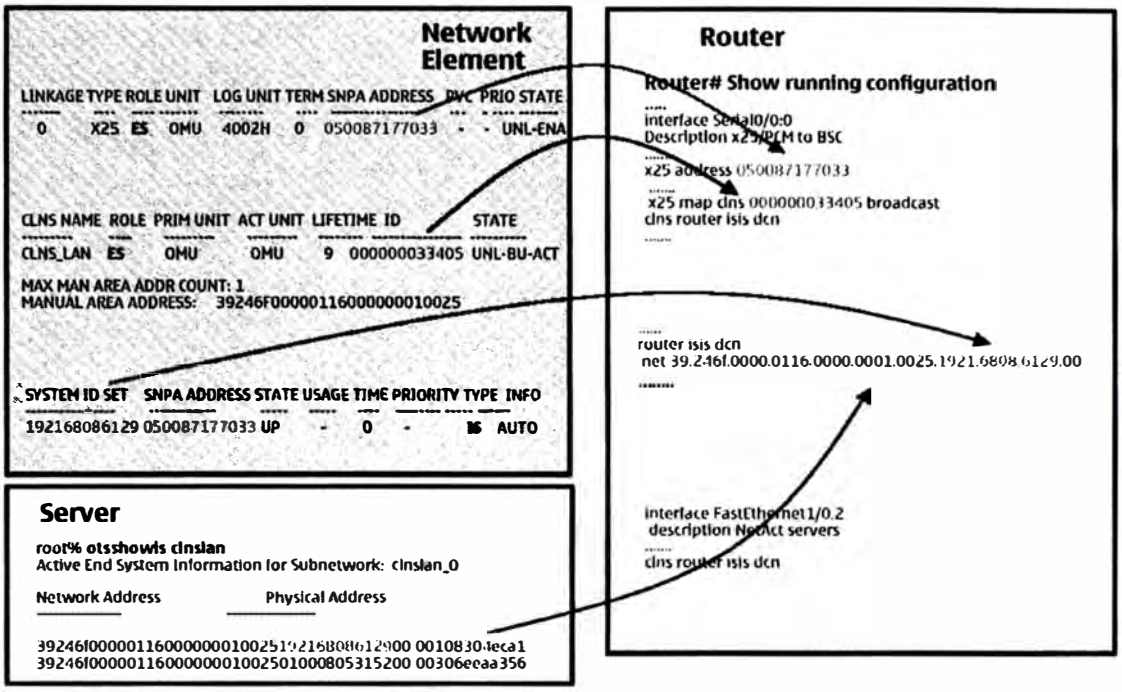


Figura 5.14: Verificación de las conexiones OSI con X.25

Adición del perfil de servicio CMISE

Después de crear todas las aplicaciones locales en el elemento de red, adicionar el perfil de servicio CMISE para la aplicación. Esta aplicación permite que un elemento de red envíe datos al sistema de administración de red usando CMISE.

Para adicionar éste perfil, se deben seguir las siguientes tareas:

- Asegurar que la aplicación CMISE está en el modo bloqueado.
- Adicionar el perfil de servicio CMISE.
- Cambiar el estado del CMISE al modo desbloqueado.
- Interrogar el perfil del servicio CMISE y asegurar que los valores están correctos.

Creación de las aplicaciones OSI remotas

Antes de establecer una conexión desde el elemento de red al sistema de administración de red, las aplicaciones remotas deben ser especificadas en el elemento de red.

Para crear las aplicaciones OSI remotas, se deben realizar las siguientes tareas:

- Creación de la aplicación remota en el elemento de red.

  En éste punto se definen los selectores de transporte, sesión y presentación.

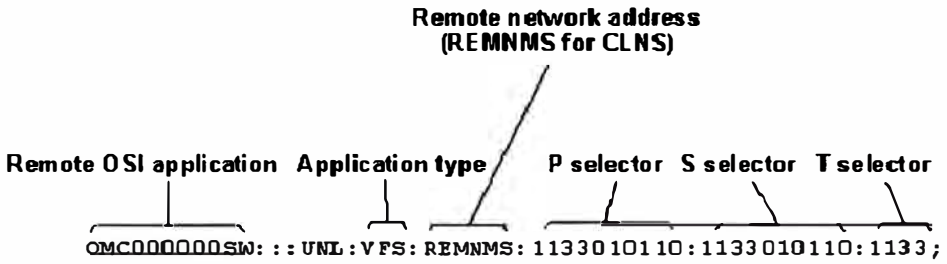


Figura 5.15: Parámetros para la aplicación OSI remota en el BSC

- Asegurar que los estados estén en el modo desbloqueado

5.2.5 Configuración de los Sistemas Intermedios (IS)

La configuración de los sistemas intermedios en el backbone DCN, se realiza de acuerdo a las tareas descritas en la sección 5.1, Integración de la red de comunicación de datos.

5.2.6 Configuración de los usuarios en la red

Los usuarios que se podrán conectar a los elementos de red, serán creados y actualizados en el sistema de administración de red. Los elementos de red están divididos en Regiones de Mantenimiento, de acuerdo al tipo, función o ubicación de cada uno de ellos.

5.3 Integración de los elementos de red del subsistema NSS

Las unidades funcionales involucradas en el procedimiento de integración de los elementos del subsistema de conmutación de red (HLR, MSC/MSS), son las Unidades de operación y mantenimiento (OMU) y la Unidad básica de comunicación de datos (BDCU).

La OMU maneja toda la supervisión centralizada del elemento de red, alarmas y funciones de recuperación, así como las conexiones hacia la interfase de usuarios. Esta unidad debe ser redundante.

La BDCU controla las interfases X.25 e incluye las funciones del enlace X.25 y la capa de paquetes. La BDCU contiene los enlaces de comunicación (tarjetas de red) hacia el sistema de administración de red.

El Gateway Multimedia (MGW) está basado en la arquitectura IPA2800, cuyo principal propósito es conectar una MSC de segunda generación a una red de acceso de radio de tercera generación (RAN). El Gateway Multimedia es manejado desde el sistema de administración de red a través de las siguientes unidades:

- La Unidad de administración del elemento de red (NEMU) proporciona una interfase de administración local y una interfase hacia el sistema de administración de red. También proporciona algunas funciones de post procesamiento de operación y mantenimiento.
- La Unidad de operación y mantenimiento (OMU) realiza las funciones al más alto nivel de mantenimiento del sistema y sirve como una interfase entre la NEMU y las otras unidades en el MGW.
- La Unidad ESA12 es un switch ethernet de 12 puertos, el cual interconecta la OMU y NEMU. Proporciona conexiones ethernet 10/100Mbps hacia el sistema de administración de red.

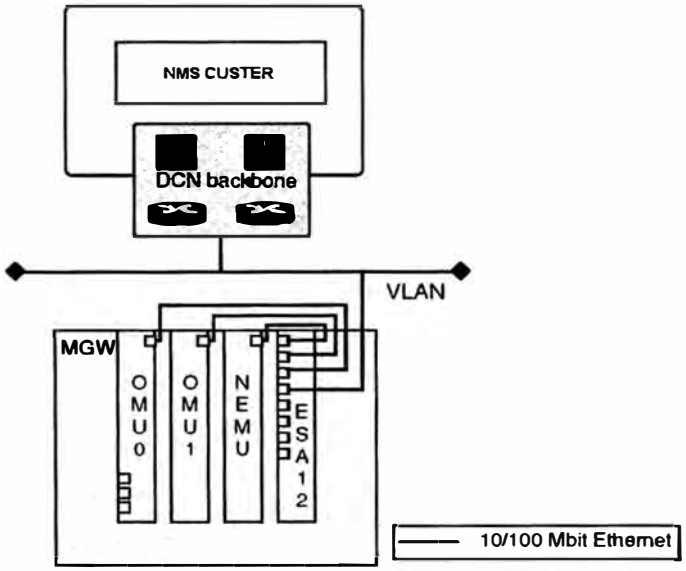


Figura 5.16: Conexiones de operación y mantenimiento entre el NMS y el MGW

La interfase de administración de red entre el NMS y la NEMU utiliza IP como el protocolo de transporte. Otro protocolo es utilizado entre la NEMU y la OMU en el MGW, el cual también está basado en IP.

5.3.1 Hardware

El hardware involucrado en la integración de los elementos de red NSS cubre los siguientes tópicos:

- Tarjetas de red en los elementos DX200 (MSC/MSS y HLR).
- Interfases de red en el MGW.
- Sistemas Intermedios.

a) Interfases de red en el elemento de red DX200

Las tarjetas de red para la integración, están ubicadas en la Unidad básica de comunicación de datos (BDCU) del elemento de red NSS. Estas son las siguientes:

- La tarjeta AC25-S/A permite la conexión de canales de transmisión de datos síncronos siguiendo el protocolo HDLC. Estas tarjetas son utilizadas para conexiones X.25 en el elemento DX200.

- La tarjeta AS7-A/B/U es un terminal multicanal usado para controlar canales de señalización LAPD. Estas tarjetas son también usadas para conexiones X25 sobre PCM.

- Las unidades plug-in CP523-A y CP550-B son unidades centrales de procesamiento en el MSC y HLR, los cuales poseen un controlador ethernet 10/100 Mbit.

- La tarjeta COCEN es utilizada para conexiones LAN IEEE 802.3. Estas tarjetas son conectadas usando cable 10Base2 (Coaxial), 10Base5 (AUI) o 10BaseT.

b) Interfases de red en el MGW

Las unidades OMU y NEMU tienen interfases ethernet de 10/100Mbit, las cuales son utilizadas para las conexiones de operación y mantenimiento.

c) Sistemas Intermedios

Debido a la configuración de red existente, pueden existir sistemas intermedios (IS) en la red. Para mantener la estructura de ésta red, el uso de un sistema intermedio encamina los datos desde un elemento de red al sistema de administración de red.

5.3.2 Tareas preliminares

a) Obtención de la información del sistema

Antes de realizar la integración, se debe asegurar la obtención de información del sistema:

Servidores del Sistema de administración de red: Hardware, rol de cada servidor, versiones de la aplicación y documentación, nombres de hosts, passwords, direcciones IP de todas las interfases y direcciones NSAP.

Elementos de red: Hardware, rol, versión de software, nombres de hosts, passwords, direcciones IP, dirección NSAP y el número C.

b) Revisión de los requerimientos del sistema

Sistema de administración de red

Verificación de la versión del sistema de administración de red.

Disponibilidad del password para los usuarios bases del sistema de administración de red: SYSOP (Usuario para acceso al sistema) y TRAFADM (Usuario para la transferencia de archivos).

Para configurar la NEMU, se debe asegurar asegurar que el número id del MGW que será integrado está disponible.

Elementos de red

DX200 (MSC/MSS y HLR):

Si la integración del elemento de red está basado en IP, asegurar la disponibilidad de los datos de red.

Verificación de la versión del software instalado en los elementos DX200.

Verificación de la activación de los parámetros de configuración necesarios para la integración, como los parámetros de la interfase Q3 en el elemento de red.

Adición de los parámetros IP, como dirección y nombre del elemento de red al DNS.

MGW:

Verificar el software instalado en el elemento de red.

Disponibilidad de las direcciones de red para la OMU y la NEMU.

El número C que identifica al elemento de red.

Adición de los parámetros IP, como dirección y nombre del elemento de red al DNS.

c) Creación de objetos a ser supervisados en el sistema de administración de red

Antes que el sistema de administración de red pueda recibir y almacenar datos del elemento de red, se debe crear el objeto que será manejado en el sistema de administración de red. Esto consiste en crear un objeto en una vista general para la supervisión y cuyos parámetros de configuración serán almacenados en la Base de Datos del sistema de administración de red.

d) Creación y modificación del usuario administrador en el elemento de red

El perfil del usuario administrador es necesario por la aplicación del sistema de administración de red para la creación, modificación y control de los perfiles de grupos de usuarios.

Para crear o modificar el perfil de grupo del usuario administrador:

Se debe iniciar una sesión de lenguaje hombre-máquina (MML) en el elemento de red.

El perfil de grupo del usuario administrador debe tener los altos niveles de autorización definidos en el elemento de red.

Crear el identificador del grupo del usuario administrador.

Los usuarios con funciones de administración y conexión por FTP deben ser creados en los elementos DX200 cuya integración está basada en IP así como en el MGW.

5.3.3 Configuración del Gateway Multimedia (MGW)

a) Configuración de la interfase LAN en la OMU

La interfase ethernet 10/100Mbit en la OMU del MGW es utilizado para la comunicación entre el MGW y la NEMU así como entre el MGW y el sistema de administración de red. El protocolo IP es utilizado para el transporte del tráfico de operación y mantenimiento.

Configuración de las direcciones IP en la unidades OMU

Asignación de la dirección IP a cada una de las unidades OMU: 0 y 1.

Asignación de la dirección IP al par de la unidad OMU.

Configuración de los parámetros IP

Asignación de los parámetros IP a la OMU del MGW como el nombre de host (hostname).

b) Configuración de la ruta estática

La ruta estática es configurada en el MGW para definir el gateway por defecto para las conexiones IP.

Configuración de la ruta estática

Configurar una ruta estática entre el MGW y la red de destino. Los parámetros para tal configuración son los índices de las OMUs así como la dirección IP del router de la DCN el cual será el gateway por defecto.

c) Configuración de las conexiones de operación y mantenimiento de la NEMU

La asignación de direcciones IP a las interfases ethernet de la NEMU deben ser asignadas durante el comisionamiento del elemento de red. Luego que la información acerca de la dirección IP ha sido verificada, se tiene que configurar la conexión entre la NEMU y el MGW así como entre la NEMU y el sistema de administración de red.

Verificación de la información acerca de la dirección IP en la NEMU

Para habilitar las conexiones desde la NEMU al MGW y al sistema de administración de red, primero se debe verificar si las interfases ethernet en la NEMU tienen dirección IP.

La asignación y verificación acerca de la información de la dirección IP se realiza a través de las propiedades de las interfases ethernet. La NEMU es una microcomputadora con sistema operativo Windows instalado.

Configuración del registro de la NEMU para las conexiones del MGW y la recolección de datos

Para configurar las conexiones del MGW, se necesita configurar el registro (regedit) de la NEMU con la dirección IP de la OMU y el id del usuario en el MGW y el password. Para la recolección de datos, existe una aplicación instalada en la NEMU encargada de ésta tarea.

Configuración de la interfase del sistema de administración de red en la NEMU

- Los procesos para la administración de sesión y el CORBA (Common Object Request broker Architecture) deben estar corriendo en la NEMU como pre-requisitos.
- El identificador del sistema del elemento de red debe estar configurado en un archivo de configuración en el sistema operativo de la NEMU.
- Transferencia del objeto de referencia IOR desde el sistema de administración de red a la NEMU a través del FTP. El objeto IOR es obtenido desde el CORBA que está corriendo en el sistema de administración de red.

Configuración de los servicios de NTP

Se realiza a través de comandos MML en el MGW.

5.3.4 Configuración de los servidores del Sistema de administración de red

En éste sección se describe el procedimiento para la configuración de los servidores del sistema de administración de red para las comunicaciones OSI.

a) Configuración de la subred OSI

Para habilitar la comunicación ISO OSI entre el sistema de administración de red y el elemento de red, la subred OSI debe ser configurada para cada interfase del servidor.

Adición de la subred CLNS para una LAN

- Iniciar sesión al servidor del sistema de administración de red como usuario administrador (root).
- Iniciar la utilidad osiadmin (para la configuración del OTS).
- Configurar el OTS (OSI Transport Services).
- Seleccionar las subredes.
- Seleccionar el CLNS sobre 802.3.
- Configuración del archivo ots_subnets.

Los parámetros necesarios para ésta configuración son: Nombre de la subred, id de red, dirección NSAP local y nombre de la interfase de red.

Verificación de la dirección NSAP del paquete del sistema

Los recursos de hardware, servicios de aplicación (procesos del unix HP-UX, NMS y base de datos) son agrupados en paquetes. Los paquetes están asociados a un nodo específico y una dirección NSAP. Cunado se realiza la integración de la red de comunicación de datos DCN, el Servidor del Sistema (SS) actúa como el nodo primario que forma el cluster de alta disponibilidad y utiliza una dirección para identificar el paquete del Service Guard.

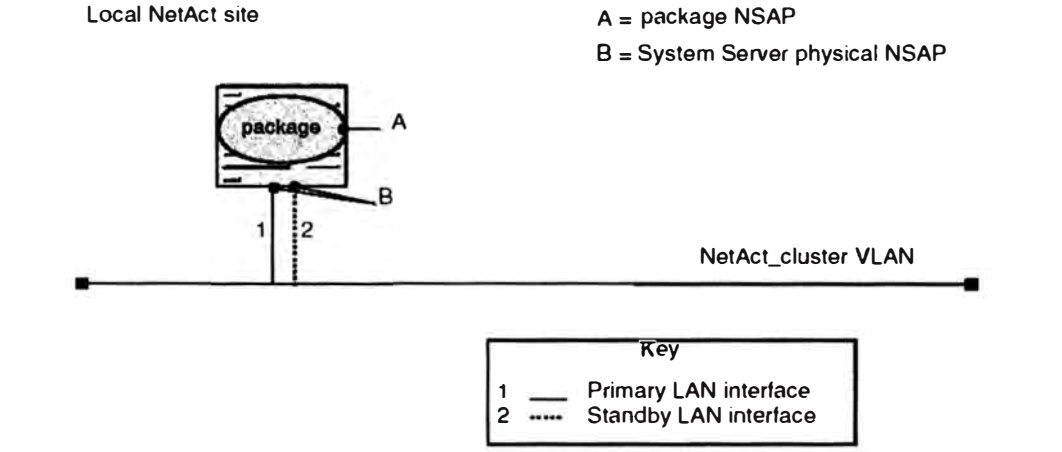


Figura 5.17: Direcciones NSAP

Para configurar la dirección NSAP del paquete del sistema, se debe utilizar las direcciones NSAP designada por la autoridad nacional responsable.

La dirección del paquete es configurada en el archivo de configuración arch1_conf.cfg ubicado en el servidor del sistema.

Adición de la ruta por defecto

Una ruta por defecto es utilizada para direccionar el tráfico a un router redundante. Usualmente, el tráfico ISO IP es direccionado al segundo router.

Para verificar que la configuración fue satisfactoria, ejecutar el comando del unix-hp osiconfchk en el servidor del sistema.

b) Configuración de las aplicaciones OSI remotas

Antes que el sistema de administración de red envíe los datos a los elementos de red, las aplicaciones OSI remotas usadas para la comunicación, deben ser configuradas en los servidores del sistema de administración de red.

Las aplicaciones OSI remotas se configuran en el archivo de configuración arch2_conf.cfg.

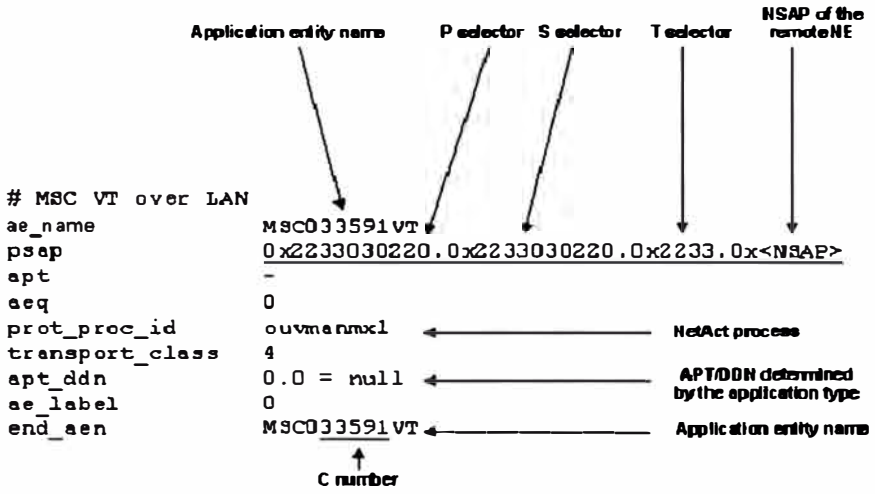


Figura 5.18: Aplicaciones OSI remotas en el archivo arch2_conf.cfg

c) Configuración para el soporte de reportes de mediciones binarias

Los elementos de red pueden crear reportes de medición binaria y reportes de medición por XML. Ambos formatos de reporte son soportados en el sistema de administración de red.

5.3.5 Configuración del elemento DX200 para la conexión DCN basada en OSI

a) Configuración de la conexión física

Usando una LAN

Las tareas que se deben realizar cuando se utiliza LAN, son las siguientes:

- Instalación y configuración de las tarjetas y switches en el elemento de red.
- Configuración del objeto CLNS.
- Configuración del objeto de enlace (linkage object).
- Creación de las direcciones NSAP local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAP a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.

Usando X.25

La configuración de la conexión física usando X.25 requiere las siguientes tareas:

- Instalación y configuración de la tarjeta de comunicaciones en el elemento de red.
- Creación de la terminal de datos.
  En ésta parte se define el tipos de interfase: V24, V35 o V36.
- Creación y modificación de los parámetros X.25.
- Creación del canal físico.
- Configuración del objeto CLNS.
- Configuración del objeto de enlace.
- Creación de las direcciones NSAP local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAP a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.
- Verificación de la conexión física.

Usando X.25 sobre PCM

Las tareas requeridas para la configuración de las conexiones físicas para el X.25 sobre PCM son las siguientes:

- Instalación y configuración de la tarjeta en el elemento de red.
  En éste punto se debe crear la conexión PCM para la unidad funcional.
- Instalación y configuración en la Terminal de Intercambio (ET).
  En éste punto también se debe crear una conexión PCM.
- Configuración de las conexiones semipermanentes.
  La comunicación a través del MSC/MSS o HLR se hace configurando una conexión semipermanente entre los intervalos de tiempo en la línea PCM hacia el BSC y los dispositivos de enrutamiento. Las líneas PCM externas son conectadas de manera semipermanente al Switch Group del MSC/HLR.
- Creación y modificación de los parámetros X.25 (para conexiones digitales).
- Creación del canal físico.
- Creación del objeto CLNS.
- Creación del objeto de enlace.
- Creación de las direcciones NSAP local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAP a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.
- Verificación de la conexión física.

b) Configuración de la subred OSI

Configuración del objeto CLNS

- Verificación de la existencia de otro objeto CLNS, de no existir, crear un nuevo objeto.
- Desbloqueo del objeto CLNS creado.
- Inicialización del objeto CLNS.

Configuración del objeto de enlace

- Si se utiliza CLNS sobre X.25, crear un objeto de enlace X.25 para cada tarjeta. Si se utiliza LAN, crear un objeto de enlace broadcast.
- Desbloqueo del objeto de enlace creado.
- Reinicialización del objeto CLNS.

Creación de las direcciones NSAP y direcciones de red

Las direcciones NSAP y las direcciones de red son utilizadas para asociar los servicios con los elementos de red. Antes de establecer una conexión desde el sistema de administración de red al elemento de red, las direcciones NSAP y direcciones de red deben ser creadas en todos los elementos de red.

Para crear las direcciones de red y NSAP, se deben realizar las siguientes tareas:

- Definición de los parámetros por defecto de la dirección de área.
- Creación de la dirección NSAP local.
- Creación de la dirección NSAP remota.
- Creación de la dirección NSAP del paquete del sistema.
- Creación de la dirección de red local.
- Creación de la dirección de red remota.

Conexión de las direcciones NSAP a las direcciones de red

- Conexión de la dirección de red local a la dirección NSAP local.
- Conexión de la dirección de red remota a la dirección NSAP remota.
- Desbloqueo de las direcciones NSAP remota y local.
- Creación de conexiones redundante, a través de nuevas direcciones de red y NSAP.

c) Configuración de las aplicaciones y direcciones OSI

Creación de las aplicaciones OSI locales

- Creación de la aplicación local en el elemento de red.

  En éste punto se definen los selectores de transporte, sesión y presentación.

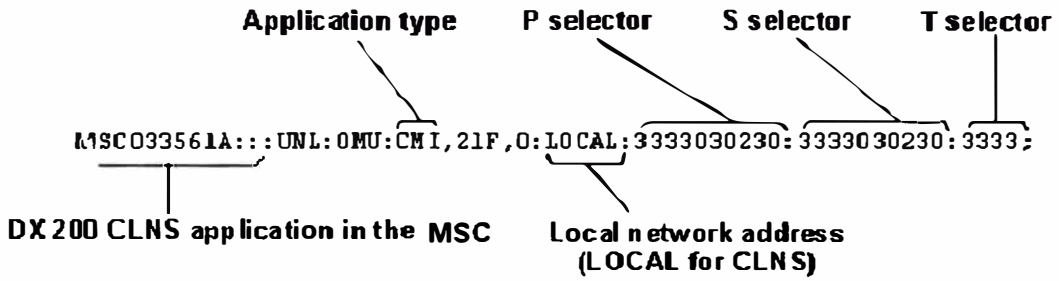


Figura 5.19: Parámetros para la aplicación CLNS local en el elemento de red

- Asegurar que los estados estén en el modo desbloqueado

Adición del perfil de servicio CMISE

Después de crear todas las aplicaciones locales en el elemento de red, adicionar el perfil de servicio CMISE para la aplicación. Esta aplicación permite que un elemento de red envíe datos al sistema de administración de red usando CMISE.

Para adicionar éste perfil, se deben seguir las siguientes tareas:

- Asegurar que la aplicación CMISE está en el modo bloqueado.
- Adicionar el perfil de servicio CMISE.
- Cambiar el estado del CMISE al modo desbloqueado.
- Interrogar el perfil del servicio CMISE y asegurar que los valores están correctos.

Creación de las aplicaciones OSI remotas

Antes de establecer una conexión desde el elemento de red al sistema de administración de red, las aplicaciones remotas deben ser especificadas en el elemento de red.

Para crear las aplicaciones OSI remotas, se deben realizar las siguientes tareas:

Creación de la aplicación remota en el elemento de red.

En éste punto se definen los selectores de transporte, sesión y presentación.

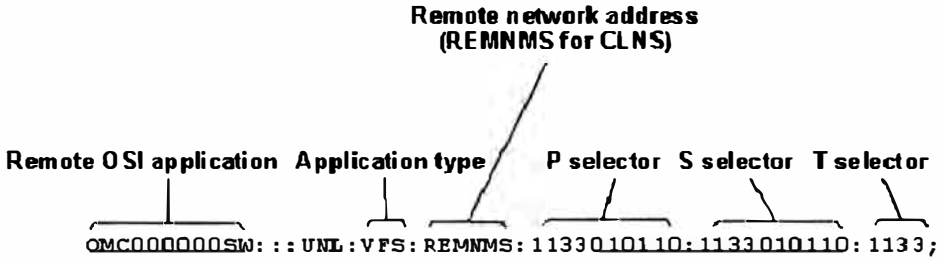


Figura 5.20: Parámetros para la aplicación OSI remota en el elemento de red

- Asegurar que los estados estén en el modo desbloqueado

Configuración de la interfase Q3

La interfase Q3 debe ser configurada para permitir la transferencia de datos entre el elemento de red DX200 basado en OSI y el sistema de administración de red.

Los pasos a seguir son los siguientes:

- Verificar si la interfase Q3 se encuentra activada en el elemento de red.
- De ser necesario, configurar la interfase Q3 del elemento de red y reiniciar el sistema.

5.3.6 Configuración del elemento DX200 para la conexión DCN basada en IP

a) Configuración de la Interfase LAN en la OMU

La interfase ethernet 10/100Mbit en la OMU del MSC/MSS y HLR es utilizada para la comunicación entre el elemento de red y el sistema de administración de red usando IP. Para habilitar la comunicación, las unidades OMU en el elemento de red tienen asignadas direcciones IP: Una dirección IP es asignada a cada unidad OMU y una tercera dirección IP es asignada a las unidades como un par (dirección IP lógica).

Para configurar las direcciones IP en la OMU:

- Asignar una dirección IP a cada unidad OMU: 0 y 1.
  Dirección IP, máscara de red y estado.
- Asignar una dirección a la unidad OMU como un par.
  Dirección IP, máscara de red y estado.

Para configurar los parámetros IP en la OMU:

- Asignar los parámetros IP a la OMU del MSC/MSS o HLR.
  Indice de la unidad y nombre de host.

b) Configuración de la ruta estática

La ruta estática es configurada en el MSC/MSS y HLR para definir un gateway por defecto para las conexiones IP.

Para configurar la ruta estática:

- Verificar si la ruta estática se encuentra ya definida, sino proceder a crearla.
- Configurar la ruta estática.
  Indice de la unidad y dirección IP del gateway.

c) Configuración de la interfase XML sobre HTTP (OMU)

La interfase XML sobre http asegura la transferencia de datos en formato XML entre los elementos de red basados en IP y el sistema de administración de red.

Configuración de los archivos de configuración XML

Estos archivos de configuración XML contienen la parte TCP/IP, HTTP, XML y otros parámetros relacionados a la transferencia de datos.

Para configurar los archivos XML:

- Editar los archivos de configuración para la transferencia utilizando un browser web.
- Configurar los parámetros de transferencia, como: puerto, estado de administración, dirección IP del sistema de administración de red, proceso, tiempo de notificación del heartbeat y tipo de evento.
- Activar los archivos de configuración.
- Reiniciar la unidad OMU.

Configuración de la interfase XML sobre HTTP

Para configurar la interfase XML sobre HTTP:

- Verificar sí la interfase IP se encuentra activada.
- Si es necesario, configurar la interfase IP.
- Reiniciar el sistema.

d) Configuración de la interfase XML sobre HTTP (NEMU)

Las interfases ethernet de la NEMU tienen asignadas una dirección IP cada una durante el comisionamiento inicial del elemento de red. Después que la información de la dirección IP ha sido verificada, se procede a la configuración de la conexión entre la NEMU y el elemento de red basado en IP, así como entre la NEMU y el sistema de administración de red.

Configuración del sistema de alarmas en la NEMU

La configuración se realiza desde la NEMU hacia el sistema de administración de red utilizando una solución de NOKIA llamada Solución RPC. Esta solución proporciona una interfase de evento de alarmas para que otro proceso desvíe las alarmas desde la NEMU al sistema de alarmas del sistema de administración de red.

El desvío de alarmas soporta el almacenamiento (buffering) en caso de algún tipo de falla en la conexión con el sistema de administración de red. Las alarmas serán nuevamente enviadas desde la NEMU una vez que la conexión es re-establecida.

El proceso que realiza el desvío de las alarmas hacia el sistema de administración de red es supervisado por la NEMU.

5.3.7 Configuración de los Sistemas Intermedios (IS)

La configuración de los sistemas intermedios en el backbone DCN, se realiza de acuerdo a las tareas descritas en la sección 5.1, Integración de la red de comunicación de datos.

5.3.8 Configuración de los usuarios en la red

Los usuarios que se podrán conectar a los elementos de red, serán creados y actualizados en el sistema de administración de red. Los elementos de red están divididos en Regiones de mantenimiento, de acuerdo al tipo, función o ubicación de cada uno de ellos.

5.4 Integración de los elementos de red GPRS

5.4.1 Integración del SGSN 2G

Una vez que la integración del SGSN 2G es finalizada, el sistema de administración de red será capaz de realizar las funciones administración de fallas y configuración desde una ubicación centralizada.

a) Principios de integración

Se recomienda que la integración del SGSN hacia el sistema de administración de red sea realizada a través de LAN. El SGSN es configurado usando CLNS y TCP/IP.

El TCP/IP es utilizado por el sistema de administración de red para establecer conexiones IP hacia los elementos de red del backbone GPRS.

El SGSN, elemento de red de la familia DX200, es parte de la solución de NOKIA para el sistema de transmisión de datos GPRS entre la red GSM y la red de paquetes de datos, como la Internet. El SGSN es un elemento core de la red GPRS como lo es el MSC en la red GSM. El SGSN maneja el enrutamiento de las llamadas, administración de movilidad y funciones de charging y actúa como el gateway entre la red GPRS y el Subsistema de estación base (BSS). Las unidades funcionales del SGSN involucradas en la integración del SGSN son la MCHU y OMU.

La MCHU consiste de 2 unidades funcionales separadas, la unidad CHU y la unidad M. La MCHU también maneja las conexiones desde la OMU hacia el sistema de administración de red. Tanto la MCHU como la OMU son redundantes.

Los enlaces de comunicación (tarjetas de red) del SGSN hacia el sistema de administración de red son los siguientes:

CP550-B para conexiones LAN/Ethernet.
AS7-B para conexiones X.25 digital.
AC25-A para conexiones X.25 analógica.

b) Hardware

Las tarjetas de red AC25-A y AS7-B para la integración, se encuentran localizadas en la unidad MCHU. Las conexiones LAN ISO/IP siempre van a través de la unidad OMU.

La tarjeta AC25-A permite la conexión de canales de transmisión de datos síncronos siguiendo el protocolo LAPB. Estas tarjetas son utilizadas para conexiones X.25 en el DX200.

La tarjeta AS7-B es una terminal multicanal usada para controlar canales de señalización LAPD. Estas tarjetas son también usadas para conexiones X25 sobre PCM.

La unidad plug-in CP550-B es una unidad central de procesamiento en el SGSN, la cual posee un controlador ethernet 10/100 Mbit.

c) Tareas Preliminares

Obtención de la información del sistema

Antes de realizar la integración, se debe asegurar la obtención de información del sistema:

- Servidores del Sistema de administración de red: Hardware, rol de cada servidor, versiones de la aplicación y documentación, nombres de hosts, passwords, direcciones IP de todas las interfases y direcciones NSAP.
- Elementos de red: Hardware, rol, versión de software, nombres de hosts, passwords, direcciones IPs, dirección NSAP y el número C.

Revisión de los requerimientos del sistema

Sistema de Administración de Red

- Verificación de la versión del sistema de administración de red.
- Disponibilidad del password para los usuarios bases del sistema de administración de red: SYSOP (Usuario para acceso al sistema) y TRAFADM (Usuario para la transferencia de archivos).

Elementos de red

- Verificar la disponibilidad de las direcciones IP de las unidades MCHU y OMU.
- Versión de software a nivel de paquetes del elemento de red.
- Adición de los parámetros IP, como dirección y nombre del elemento de red al DNS.

Creación de objetos a ser supervisados en el sistema de administración de red

Antes que el sistema de administración de red pueda recibir y almacenar datos del elemento de red, se debe crear el objeto que será manejado en el sistema de administración de red. Esto consiste en crear un objeto en una vista general para la supervisión y cuyos parámetros de configuración serán almacenados en la Base de Datos del sistema administración de red.

Creación y modificación del usuario administrador en el elemento de red

El perfil del usuario administrador es necesario por la aplicación del sistema de administración de red para la creación, modificación y control de los perfiles de grupos de usuarios.

Para crear o modificar el perfil de grupo del usuario administrador:

- Se debe iniciar una sesión de lenguaje hombre-máquina (MML) en el elemento de red.
- El perfil de grupo del usuario administrador debe tener los altos niveles de autorización definidos en el elemento de red.
- Crear el identificador del grupo del usuario administrador.

d) Configuración de los servidores del Sistema de Administración de Red

En éste sección se describe el procedimiento para la configuración de los servidores del sistema de administración de red para las comunicaciones OSI. El procedimiento es el mismo que la sección 5.3.4.

e) Configuración del SGSN

Configuración de la conexión física

Usando X.25

La configuración de la conexión física usando X.25 requiere las siguientes tareas:

- Instalación y configuración de la tarjeta de comunicaciones en el elemento de red.
- Creación de la terminal de datos.
  En ésta parte se define el tipos de interfase: V24, V35 o V36.
- Creación y modificación de los parámetros X.25.
- Creación del canal físico.
- Configuración del objeto CLNS.
- Configuración del objeto de enlace.
- Creación de las direcciones NSAPs local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAPs a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.
- Verificación de la conexión física.

Usando X.25 sobre PCM

Las tareas requeridas para la configuración de las conexiones físicas para el X.25 sobre PCM son las siguientes:

- Instalación y configuración de la tarjeta en el elemento de red.
  En éste punto se debe crear la conexión PCM para la unidad funcional.

- Instalación y configuración en la Terminal de Intercambio (ET).
  En éste punto también se debe crear una conexión PCM.
- Configuración de las conexiones semipermanentes.
  La comunicación a través del SGSN se hace configurando una conexión semipermanente entre los intervalos de tiempo en la línea PCM hacia el BSC y los dispositivos de enrutamiento.
  Las conexiones semipermanentes son utilizadas para multiplexar los intervalos de tiempo (time slots) PCM. Luego que la conexión semipermanente es creada en el BSC, el Switch de Grupo (GSW) multiplexará los intervalos de tiempo entrantes y los enviará a la Terminal de Intercambio (ET).
- Creación y modificación de los parámetros X.25 (para conexiones digitales).
- Creación del canal físico.
- Creación del objeto CLNS.
- Creación del objeto de enlace.
- Creación de las direcciones NSAPs local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAPs a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.
- Verificación de la conexión física.

Usando LAN

Las tareas que se deben realizar cuando se utiliza LAN, son las siguientes:

- Instalación y configuración de las tarjetas y switches en el elemento de red.
- Configuración del objeto CLNS.
- Configuración del objeto de enlace (linkage object).
- Creación de las direcciones NSAPs local y remota.
- Creación de las direcciones de red local y remota.
- Conexión de las direcciones NSAPs a las direcciones de red.
- Configuración de las aplicaciones locales y remotas.

Configuración de la subred OSI

Configuración del objeto CLNS

- Verificación de la existencia de otro objeto CLNS, de no existir, crear un nuevo objeto.
- Desbloqueo del objeto CLNS creado.
- Inicialización del objeto CLNS.

Configuración del objeto de enlace

- Si se utiliza CLNS sobre X.25, crear un objeto de enlace X.25 para cada tarjeta. Si se utiliza LAN, crear un objeto de enlace broadcast.
- Desbloqueo del objeto de enlace creado.
- Reinicialización del objeto CLNS.

Creación de las direcciones NSAPs y direcciones de red

Las direcciones NSAP y las direcciones de red son utilizadas para asociar los servicios con los elementos de red. Antes de establecer una conexión desde el sistema de administración de red al elemento de red, las direcciones NSAP y direcciones de red deben ser creadas en todos los elementos de red.

Para crear las direcciones de red y NSAP, se deben realizar las siguientes tareas:

- Definición de los parámetros por defecto de la dirección de área.
- Creación de la dirección NSAP local.
- Creación de la dirección NSAP remota.
- Creación de la dirección NSAP del paquete del sistema.
- Creación de la dirección de red local.
- Creación de la dirección de red remota.

Conexión de las direcciones NSAPs a las direcciones de red

- Conexión de la dirección de red local a la dirección NSAP local.
- Conexión de la dirección de red remota a la dirección NSAP remota.
- Desbloqueo de las direcciones NSAP remota y local.
- Creación de conexiones redundante, a través de nuevas direcciones de red y NSAP.

Configuración de las aplicaciones y direcciones OSI

Creación de las aplicaciones OSI locales

- Creación de la aplicación local en el elemento de red.
  En éste punto se definen los selectores de transporte, sesión y presentación.
- Asegurar que los estados estén en el modo desbloqueado.

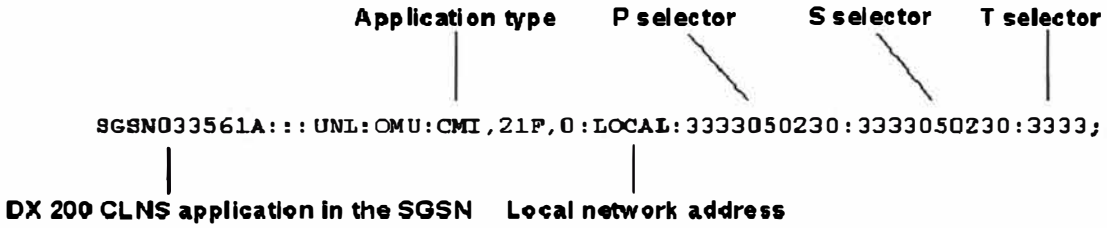


Figura 5.21: Creación de las aplicaciones CLNS locales en el SGSN

Adición del perfil de servicio CMISE

Después de crear todas las aplicaciones locales en el elemento de red, adicionar el perfil de servicio CMISE para la aplicación. Esta aplicación permite que un elemento de red envíe datos al sistema de administración de red usando CMISE.

Para adicionar éste perfil, se deben seguir las siguientes tareas:

- Asegurar que la aplicación CMISE está en el modo bloqueado.
- Adicionar el perfil de servicio CMISE.
- Cambiar el estado del CMISE al modo desbloqueado.
- Interrogar el perfil del servicio CMISE y asegurar que los valores están correctos.

Creación de las aplicaciones OSI remotas

Antes de establecer una conexión desde el elemento de red al sistema de administración de red, las aplicaciones remotas deben ser especificadas en el elemento de red.

Para crear las aplicaciones OSI remotas, se deben realizar las siguientes tareas:

- Creación de la aplicación remota en el elemento de red.

  En éste punto se definen los selectores de transporte, sesión y presentación.

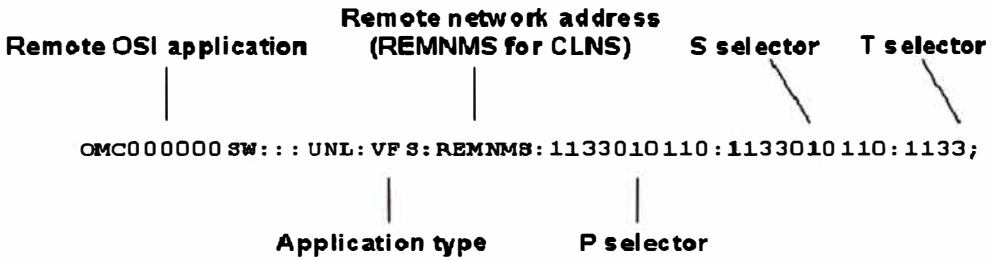


Figura 5.22: Creación de las aplicaciones OSI remotas en el SGSN

- Asegurar que los estados estén en el modo desbloqueado.

Configuración de las aplicaciones TCP/IP

Antes que el SGSN pueda enviar los datos utilizando TCP/IP, las interfases de red y las aplicaciones deben ser configuradas dependiendo de la versión de software que está corriendo en el SGSN.

Para crear una interfase de red para datos TCP/IP:

- Crear las interfases de red.
  Tipo de interfase, dirección IP, máscara de red y estado de la interfase.
- Crear la ruta por defecto desde la OMU al router de la DCN.

f) Configuración de los usuarios de red

Los usuarios que se podrán conectar a los elementos de red, serán creados y actualizados en el sistema de administración de red. Los elementos de red están divididos en Regiones de Mantenimiento, de acuerdo al tipo, función o ubicación de cada uno de ellos.

5.4.2 Integración del GGSN

a) Principios de Integración

El GGSN actúa como una interfase entre la red GPRS y las redes externas. El GGSN está conectado al sistema de administración de red a través del backbone de la red IP del core de paquetes.

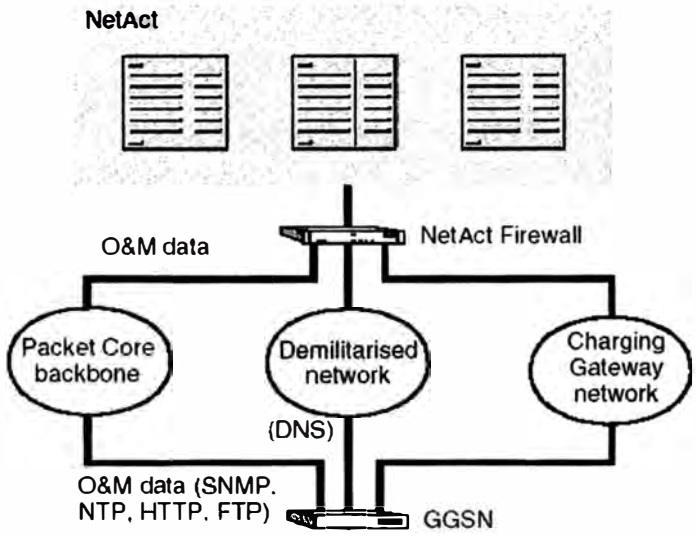


Figura 5.23: Conexiones GGSN al sistema de administración de red

b) Procedimiento de Integración

La integración del GGSN consiste en completar un conjunto de tareas preliminares y luego configurar los servicios NTP, SNMP y DNS.

c) Tareas preliminares

Revisión de los requerimientos del sistema

Sistema de Administración de Red

- Verificación de la versión del sistema de administración de red.
- Disponibilidad de las direcciones IP de los servidores del sistema de administración de red.
- Creación del usuario con perfil para el acceso por FTP.
- Disponibilidad de los passwords del GGSN y del usuario administrador de la región de mantenimiento a la cual pertenece el elemento de red.

Elementos de red

- Verificar que el GGSN ha sido integrado a la red IP del core de paquetes.
- Verificar que dirección IP del GGSN ha sido reservado en el DNS.
- Usuario y password para el acceso al GGSN a través de la aplicación web.
- Versión de software a nivel de paquetes del elemento de red.

d) Configuración de los servidores del sistema de administración de red

En ésta sección se describe el procedimiento para la configuración de los servidores del sistema de administración de red para las comunicaciones IP. El procedimiento es el mismo que la sección 5.3.4.

e) Creación del objeto a ser supervisado en el sistema de administración de red

Antes que el sistema de administración de red pueda recibir y almacenar datos del elemento de red, se debe crear el objeto que será manejado en el sistema de gestión. Esto consiste en crear un objeto en una vista general para la supervisión y cuyos parámetros de configuración serán almacenados en la Base de Datos del sistema de administración de red.

f) Configuración del GGSN

La configuración de la unidad se realiza utilizando la aplicación web del GGSN en el sistema de administración de red. Los parámetros a configurar son los siguientes:

- Configuración IP del GGSN.
- Configuración del enrutamiento OSPF.
- Configuración del NTP (Network Time Protocol).

  El NTP es un protocolo de administración de tiempo basado en TCP/IP utilizado para sincronizar los relojes de los servidores IP con un reloj externo utilizado como referencia (tal como un GPS).

  El sistema de administración de red recibe el tiempo de referencia del GPS y lo distribuye a los otros elementos de red.
- Configuración del SNMP.

  El SNMP es utilizado para recolectar los datos de administración de performance (PM) y recibir las alarmas desde el GGSN.
- Verificar la configuración del DNS en el GGSN.

El DNS es utilizado para resolver nombres de hosts IP a direcciones IP.

CAPITULO VI

APLICACIONES PRÁCTICAS E IMPLEMENTACIÓN

6.1 Configuración en el Sistema de Administración de Red

A continuación detallaremos la configuración del lado del sistema de administración de red, el cual permitirá la integración de los elementos de red a éste.
Los elementos de red considerados para la integración al sistema de administración de red son los siguientes:

BSC_TEST_X25: BSC que será integrado usando X25 sobre PCM.
BSC_TEST_LAN: BSC que sera integrado usando LAN.
MSC_TEST_LAN: MSC que será integrada usando LAN.
MSS_TEST_IP: MSS que sera integrada usando IP.

6.1.1 Configuración de los servidores UNIX del Sistema de Administración de Red

a) Direccionamiento IP en los servidores UNIX

La configuración para el direccionamiento IP se detalla en el archivo netconf del sistema operativo UNIX:

SERVIDOR COMPONENTE DEL SISTEMA (SCS)

```
HOSTNAME="rc_scs"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

INTERFACE_NAME[0]="lan0"
IP_ADDRESS[0]="170.29.4.172"
SUBNET_MASK[0]="255.255.255.248"
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0
```

```
ROUTE_DESTINATION[0]="default"
ROUTE_MASK[0]=""
ROUTE_GATEWAY[0]="170.29.4.1"
ROUTE_COUNT[0]="1"
ROUTE_ARGS[0]=""

INTERFACE_NAME[1]="lan1"
IP_ADDRESS[1]="170.29.4.11"
SUBNET_MASK[1]="255.255.255.128"
DHCP_ENABLE[1]=0
```

SERVIDOR DE BASE DE DATOS (DBS)

```
HOSTNAME="rc_dbs"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

INTERFACE_NAME[0]="lan0"
IP_ADDRESS[0]="170.29.4.173"
SUBNET_MASK[0]="255.255.255.248"
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0

ROUTE_DESTINATION[0]="default"
ROUTE_MASK[0]=""
ROUTE_GATEWAY[0]="170.29.4.1"
ROUTE_COUNT[0]="1"
ROUTE_ARGS[0]=""

INTERFACE_NAME[1]="lan1"
IP_ADDRESS[1]="170.29.4.12"
SUBNET_MASK[1]="255.255.255.128"
DHCP_ENABLE[1]=0
```

b) Direccionamiento OSI en los servidores UNIX

El direccionamiento OSI está definido separadamente del direccionamiento TCP/IP, sin embargo se utilizan las mismas interfases físicas. La dirección OSI (NSAP) para los servidores unix está definido en el archivo ots_subnets:

```
snet_clns_8023                  nms_net
snet local net_address          39604F000000000000000010001170029004012 00
snet_if_name                    lan1
```

El gateway por defecto de las conexiones OSI para el servidor unix está definido en el archivo ots_routes.

```
route_id                        00
route_id_mask                   00    # hexadecimal bitmask
route_out_subnet                nms_net
route_primary                   39604F000000000000000010001700290040030 0
```

El valor 00 para route_id y route_id_mask define que la ruta es por defecto. El paquete tiene también una dirección NSAP que es definido en el archivo arch1_conf.cfg:

```
...
( NSAP "39604F000000000000000010001700290040150 0" )
...
```

Las direcciones locales NSAP configuradas en OTS (OSI Transport Services) para el servicio de red CLNS son las siguientes:

```
rc_scs:/ (100) root% otsshownsaps CLNS
---------------------------------
    Current local OTS NSaps:
---------------------------------
 Nsap [ Alias ] [I/F Name ] Type
---------------------------------

CLNS:
 39604f000000000000000010001700290040120 0  dynamic
 39604f000000000000000010001700290040150 0  dynamic
```

Los sistemas intermedios encontrados en la configuración OTS son los siguientes:

```
rc_scs: (118) root% otsshowis nms_net
 Active Intermediate System Information for Subnetwork:  nms2000snet

   Network Address                          Physical Address
   ---------------                          ----------------

  39604f000000000000000010001700290040040 0 0001b7db9a21
  39604f000000000000000010001700290040030 0 000486472c08
  39604f000000000000000010001700290040020 0 000686477008
```

c) Configuración de las aplicaciones locales OSI

Archivo arch3_conf.cfg:

```
# ProcessA over CMISE
ae_name          processAmx1
psap             0x3333010130.0x3333010130.0x3333.0x
apt              1.1.1000.1.1
aeq              0
appl_proc_id     processAmx1
apt_ddn          0.0 = null
ae_label         0
end_aen          processAmx1

# VT (Process B)
ae_name          vt_initiator
psap             0x2233010120.0x2233010120.0x2233.0x
apt              1.1.1000.3.1
aeq              0
appl_proc_id     processBmx1
apt_ddn          0.0 = null
ae_label         0
end_aen          vt_initiator

# CM over FTAM
ae_name          OMC000000SW
psap             0x1133010110.0x1133010110.0x1133.0x
apt              1.1.1000.2.1
aeq              0
appl_proc_id     processCmx1
apt_ddn          1 = OMC000000SW
ae_label         0
end_aen          OMC000000SW
```

Archivo arch2_conf.cfg:

Para BSC_TEST_X25 (Número C: 123456)

```
# KK CMISE , A
ae_name          BSC123456A
psap
0x3333030230.0x3333030230.0x3333.0x39604F0000000000000001000100000123456
00
apt              -
aeq              0
prot_proc_id     processAmx1
transport_class 4
```

```
apt_ddn          0.0 = null
ae_label         0
end_aen          BSC123456A

# VT
ae_name          BSC123456VT
psap
0x2233030220.0x2233030220.0x2233.0x39604F0000000000000001000100000000123456
00
apt              -
aeq              0
prot_proc_id     processBmx1
transport_class  4
apt_ddn          0.0 = null
ae_label         0
end_aen          BSC123456VT

# KK FTAM
ae_name          BSC123456F
psap
0x1133030210.0x1133030210.0x1133.0x39604F0000000000000001000100000000123456
00
apt              -
aeq              0
prot_proc_id     processCmx1
transport_class  4
apt_ddn          1 = BSC123456F
ae_label         0
end_aen          BSC123456F
```

Para BSC_TEST_LAN (Número C: 234567)

```
# KK CMISE , A
ae_name          BSC234567A
psap
0x3333030230.0x3333030230.0x3333.0x39604F0000000000000001000100000000234567
00
apt              -
aeq              0
prot_proc_id     processAmx1
transport_class  4
apt_ddn          0.0 = null
ae_label         0
end_aen          BSC234567A
```

```
# VT
ae_name          BSC234567VT
psap
0x2233030220.0x2233030220.0x2233.0x39604F00000000000000010001000000234567
00
apt              -
aeq              0
prot_proc_id     processBmx1
transport_class  4
apt_ddn          0.0 = null
ae_label         0
end_aen          BSC234567VT

# KK FTAM
ae_name          BSC234567F
psap
0x1133030210.0x1133030210.0x1133.0x39604F00000000000000010001000000234567
00
apt              -
aeq              0
prot_proc_id     processCmx1
transport_class  4
apt_ddn          1 = BSC234567F
ae_label         0
end_aen          BSC234567F
```

Para MSC_TEST_LAN (Número C: 345678)

```
# KK CMISE , A
ae_name          MSC345678A
psap
0x3333040230.0x3333040230.0x3333.0x39604F00000000000000010001000000345678
00
apt              -
aeq              0
prot_proc_id     processAmx1
transport_class  4
apt_ddn          0.0 = null
ae_label         0
end_aen          MSC345678A

# VT
ae_name          MSC345678VT
psap
0x2233040220.0x2233040220.0x2233.0x39604F00000000000000010001000000345678
00
```

```
apt             -
aeq             0
prot_proc_id    processBmx1
transport_class 4
apt_ddn         0.0 = null
ae_label        0
end_aen         MSC345678VT

# KK FTAM
ae_name         MSC345678FO
psap
0x1133040210.0x1133040210.0x1133.0x39604F00000000000000010001000000345678
00
apt             -
aeq             0
prot_proc_id    processCmx1
transport_class 4
apt_ddn         1 = MSC345678FO
ae_label        0
end_aen         MSC345678FO
```

Para MSS_TEST_IP (Número C: 456789)

Cuando la integración se realiza utilizando IP, no se necesita la configuración CLNS. Por lo tanto los parámetros para éste elemento en éste archivo de configuración no son necesarios.

d) Servidor de conexión (Connection Server)

Archivo arch_princ.cfg:

Para BSC_TEST_X25 (Número C: 123456)

```
(arcName    "A_CSRV_VT_ISOIP_BSC_TEST_X25"
    (maxConns              "16")
    (address               "BSC123456VT")
    (connChannel           "processmx")
    (loginSeqFileName      "archconfloginmx.cf")
    (logoutSeqFileName     "archconflogoutmx.cf")
)
(arcName    "A_CSRV_FTAM_BSC_TEST_X25"
    (maxConns              "16")
    (address               "BSC123456F")
    (connChannel           "OMC000000SW")
    (loginSeqFileName      "archconfloginmx.cf")
    (logoutSeqFileName     "archconflogoutmx.cf")
```

```
(routeName    "R_CSRV_VT_ISOIP_BSC_TEST_X25"
    (arcs                 "A_CSRV_VT_ISOIP_BSC_TEST_X25")
    (host                 "rc_scs")
    (port                 "7654")
    (checkScript          "")
    (commandLine          "archconfvtmx.cf")
)
(routeName    "R_CSRV_FTAM_BSC_TEST_X25"
    (arcs                 "A_CSRV_FTAM_BSC_TEST_X25")
    (host                 "rc_scs")
    (port                 "6543")
    (checkScript          "")
    (commandLine          "")
)
(id    "987654"
    (tecName              "BSC_TEST_X25")
    (maxMMLConns          "10")
    (maxFileConns         "6")
    (maxSpontConns        "6")
    (totalMaxConns        "18")
    (edMMLConns           "Y")
    (edFileConns          "Y")
    (edSpontConns         "Y")
    (edAllConns           "Y")
    (edMMLLog             "N")
    (edFileLog            "Y")
    (edSpontLog           "Y")
    (edAllLog             "Y")
    (users                 ""
       (groups                "prueba"
            (connTypes             "XFER"
                (routes                "R_CSRV_FTAM_BSC_TEST_X25")
            )
            (connTypes             "MML_HUMAN,MML_MACHINE"
                (routes                "R_CSRV_VT_ISOIP_BSC_TEST_X25")
                )
        )
    )
)
```

Para BSC_TEST_LAN (Número C: 234567)

```
(arcName    "A_CSRV_VT_ISOIP_BSC_TEST_LAN"
    (maxConns             "16")
    (address              "BSC234567VT")
    (connChannel          "processmx")
    (loginSeqFileName     "archconfloginmx.cf")
    (logoutSeqFileName    "archconflogoutmx.cf")
)
(arcName    "A_CSRV_FTAM_BSC_TEST_LAN"
    (maxConns             "16")
```

```
    (address                "BSC234567F")
    (connChannel            "OMC000000SW")
    (loginSeqFileName       "archconfloginmx.cf")
    (logoutSeqFileName      "archconflogoutmx.cf")
)
(routeName     "R_CSRV_VT_ISOIP_BSC_TEST_LAN"
    (arcs                   "A_CSRV_VT_ISOIP_BSC_TEST_LAN")
    (host                   "rc_scs")
    (port                   "7654")
    (checkScript            "")
    (commandLine            "archconfvtmx.cf")
)
(routeName     "R_CSRV_FTAM_BSC_TEST_LAN"
    (arcs                   "A_CSRV_FTAM_BSC_TEST_LAN")
    (host                   "rc_scs")
    (port                   "6543")
    (checkScript            "")
    (commandLine            "")
)
(id     "876543"
    (tecName                "BSC_TEST_LAN")
    (maxMMLConns            "10")
    (maxFileConns           "6")
    (maxSpontConns          "6")
    (totalMaxConns          "18")
    (edMMLConns             "Y")
    (edFileConns            "Y")
    (edSpontConns           "Y")
    (edAllConns             "Y")
    (edMMLLog               "N")
    (edFileLog              "Y")
    (edSpontLog             "Y")
    (edAllLog               "Y")
    (users                   ""
       (groups                  "prueba"
            (connTypes               "XFER"
                (routes                  "R_CSRV_FTAM_BSC_TEST_LAN")
            )
            (connTypes               "MML_HUMAN,MML_MACHINE"
                (routes                  "R_CSRV_VT_ISOIP_BSC_TEST_LAN")
                )
        )
    )
)
```

Para MSC_TEST_LAN (Número C: 345678)

```
(arcName     "A_CSRV_VT_ISOIP_MSC_TEST_LAN"
    (maxConns               "10")
    (address                "MSC345678VT")
    (connChannel            "processmx")
```

```
    (loginSeqFileName      "archconfloginmx.cf")
    (logoutSeqFileName     "archconflogoutmx.cf")
)
(arcName    "A_CSRV_FTAM_MSC_TEST_LAN"
    (maxConns              "20")
    (address               "MSC345678FO")
    (connChannel           "OMC000000SW")
    (loginSeqFileName      "archconfloginmx.cf")
    (logoutSeqFileName     "archconflogoutmx.cf")
)
(routeName    "R_CSRV_VT_ISOIP_MSC_TEST_LAN"
    (arcs                  "A_CSRV_VT_ISOIP_MSC_TEST_LAN")
    (host                  "rc_scs")
    (port                  "7654")
    (checkScript           "")
    (commandLine           "archconfvtmx.cf")
)
(routeName    "R_CSRV_FTAM_MSC_TEST_LAN"
    (arcs                  "A_CSRV_FTAM_MSC_TEST_LAN")
    (host                  "rc_scs")
    (port                  "6543")
    (checkScript           "")
    (commandLine           "")
)
(id    "765432"
    (tecName               "MSC_TEST_LAN")
    (maxMMLConns           "10")
    (maxFileConns          "6")
    (maxSpontConns         "6")
    (totalMaxConns         "18")
    (edMMLConns            "Y")
    (edFileConns           "Y")
    (edSpontConns          "Y")
    (edAllConns            "Y")
    (edMMLLog              "N")
    (edFileLog             "Y")
    (edSpontLog            "Y")
    (edAllLog              "Y")
    (users                  ""
       (groups                 "prueba"
            (connTypes              "XFER"
                (routes                 "R_CSRV_FTAM_MSC_TEST_LAN")
            )
            (connTypes              "MML_HUMAN,MML_MACHINE"
                (routes                 "R_CSRV_VT_ISOIP_MSC_TEST_LAN")
                )
        )
    )
)
```

Para MSS_TEST_IP (Número C: 456789)

```
(arcName "A_SSRV_TELNET_TCPIP_MSS_TEST_IP"
        (maxConns "22")
        (address "170.29.4.144") # OMU IP Address
        (connChannel "telnet")
        (loginSeqFileName "archconfloginmx.cf")
        (logoutSeqFileName "archconflogoutmx.cf")
)
# Route definitions
(routeName "R_SSRV_TELNET_TCPIP_MSS_TEST_IP"
        (arcs "A_SSRV_TELNET_TCPIP_MSS_TEST_IP")
        (host "rc01oss1")
        (port "7654")
        (checkScript "")
        (commandLine "archconfvtmx.cf")
)
#Node definitions
(id "654321"
        (tecName "MSS_TEST_IP")
        (maxMMLConns "16")
        (maxFileConns "6")
        (maxSpontConns "6")
        (totalMaxConns "22")
        (edMMLConns "Y")
        (edFileConns "Y")
        (edSpontConns "Y")
        (edAllConns "Y")
        (edMMLLog "N")
        (edFileLog "N")
        (edSpontLog "N")
        (edAllLog "Y")
        (users ""
                (groups     "prueba"
                        (connTypes "MML_HUMAN,MML_MACHINE"
                                (routes "R_SSRV_TELNET_TCPIP_MSS_TEST_IP")
                        )
                )
        )
)
```

6.2 Configuración en la Red de Comunicación de Datos (DCN)

Los equipos de red a utilizar en la red de comunicación de datos son los siguientes:

2 Routers Cisco 7206 con versión de IOS 12.2(15)T5

```
rc_rtr1#show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.2(15)T5, RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 11-Jun-03 20:54 by user
Image text-base: 0x60008954, data-base: 0x61F7C000

ROM: System Bootstrap, Version 12.2(4r)B2, RELEASE SOFTWARE (fc2)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.2(15)T5, RELEASE
SOFTWARE (fc1)

rc_rtr1 uptime is 8 weeks, 6 days, 10 hours, 22 minutes
System returned to ROM by bus error at PC 0x606F8204, address 0x300
System restarted at 05:42:33 sat5 Wed May 17 2006
System image file is "disk0:c7200-js-mz.122-15.T5.bin"

cisco 7206VXR (NPE400) processor (revision A) with 491520K/32768K bytes
of memory.
Processor board ID 29740897
R7000 CPU at 350Mhz, Implementation 39, Rev 3.3, 256KB L2, 4096KB L3
Cache
6 slot VXR midplane, Version 2.7

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.1.
Basic Rate ISDN software, Version 1.1.
Channelized E1, Version 1.0.
4 FastEthernet/IEEE 802.3 interface(s)
29 Serial network interface(s)
8 ISDN Basic Rate interface(s)
8 Channelized E1/PRI port(s)
125K bytes of non-volatile configuration memory.

125952K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
31360K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
```

3 Switches Cisco 2950 con versión de IOS 12.1(22) EA4a

```
rc_sw1#show version
Cisco Internetwork Operating System Software
IOS(tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4a, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 16-Sep-05 10:46 by user
Image text-base: 0x80010000, data-base: 0x80562000

ROM: Bootstrap program is C2950 boot loader

rc_sw1 uptime is 23 weeks, 4 hours, 19 minutes
System returned to ROM by power-on
System restarted at 11:37:30 SAT Tue Feb 7 2006
System image file is "flash:/c2950-i6q4l2-mz.121-22.EA4a.bin"

cisco WS-C2950-24 (RC32300) processor (revision R0) with 21039K bytes of
memory.
Processor board ID FCZ0946X1RM
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:15:FA:9B:B2:C0
Motherboard assembly number: 73-5781-13
Power supply part number: 34-0965-01
Motherboard serial number: FOC09431UXT
Power supply serial number: DAB09146NFW
Model revision number: R0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FCZ0946X1RM

Configuration register is 0xF
```

6.2.1 Definición de las VLANs en el Sistema de Administración de Red

Dirección de Red a utilizar:	170.29.4.0
Máscara de Red:	255.255.255.0

Número de hosts requeridos:

Subnet A: 126 hosts

Subnet B: 14 hosts

Subnet C: 6 hosts

Subnet D: 6 hosts

Subnet E: 6 hosts

Subnet F: 6 hosts

Subnet G: 6 hosts

Subnet H: 30 hosts

Subnet I: 6 hosts

Red Clase C: 170.29.4.0 / 24

Usando VLSM (Variable Length Subnet Mask), podemos definir cada subred como sigue:

Subred A (126 hosts):

11111111.11111111.11111111.10000000 : /25 = 255.255.255.128

Subred B (14 hosts):

11111111.11111111.11111111.11110000 : /28 = 255.255.255.240

Subred C, D, E, F, G, I (6 hosts):

11111111.11111111.11111111.11111000 : /29 = 255.255.255.248

Subred H (30 hosts):

11111111.11111111.11111111.11100000 : /27 = 255.255.255.224

Tabla 6.1: Definición de VLANs

Nombre de VLAN	Número de VLAN	Número de hosts	Dirección de Red / Máscara	Direcciones IPs disponibles	Broadcast	Máscara de subred
NMS_Cluster1 (A)	2	126	170.29.4.0/25	.1 - .126	170.29.4.127	255.255.255.128
NMS_Servicios (B)	6	14	170.29.4.128/28	.129 - .142	170.29.4.143	255.255.255.240
NE 2G locales (C)	8	6	170.29.4.144/29	.145 - .150	170.29.4.151	255.255.255.248
Red_Interna (D)	11	6	170.29.4.152/29	.153 - .158	170.29.4.159	255.255.255.248
Red_Externa1 (E)	12	6	170.29.4.160/29	.161 - .166	170.29.4.167	255.255.255.248
Red_Externa2 (F)	13	6	170.29.4.168/29	.169 - .174	170.29.4.175	255.255.255.248
Acceso 3G (G)	7	6	170.29.4.176/29	.177 - .182	170.29.4.183	255.255.255.248
Red_Operador (H)	10	30	170.29.4.192/27	.193 - .222	170.29.4.223	255.255.255.224
Red_Externa3 (I)	14	6	170.29.4.248/29	.249 - 254	170.29.4.255	255.255.255.248

Donde:

NE (Network Element): Elementos de red

NMS (Network Management System): Sistema de administración de red

6.2.2 Procedimiento de integración

a) Tareas previas

Obtención de la información del sistema

A continuación se muestra el tipo de información que se debe considerar en un mapa de red:

Hardware

Sistema de Administración de red:

2 Servidores HP RP4440 con Sistema Operativo Unix HP 11i

rc_scs: Servidor SCS (System Component Server) – 170.29.4.11

rc_dbs: Servidor DBS (Database Server) – 170.29.4.12

2 Servidores HP Proliant DL360 G4p (Servidores de Aplicación Windows) con Sistema Operativo Windows 2000 Server

rc_was1: Servidor WAS 1 (Windows Application Server) – 170.29.4.21

rc_was2: Servidor WAS 1 (Windows Application Server) – 170.29.4.22

Arreglo de discos EMC CX500 con 2x15x73GB de capacidad de almacenamiento

spa: Procesador de Almacenamiento A (Storage Processor) – 170.29.4.132

spb: Procesador de Almacenamiento B (Storage Processor) – 170.29.4.133

2 switches de fibra óptica para la interconexión del arreglo de discos hacia los servidores unix

fb_sw1: Switch SAN (Storage Area Network) – 170.29.4.138

fb_sw2: Switch SAN (Storage Area Network) – 170.29.4.139

Red de Comunicación de Datos:

2 Routers Cisco 7206

VLAN 1: Vlan Nativa

VLAN 2:
Dirección IP de HSRP – rc_rtr: 170.29.4.1
rc_rtr1: 170.29.4.2
rc_rtr2: 170.29.4.3

VLAN 6:
Dirección IP de HSRP – rc_rtr: 170.29.4.129
rc_rtr1: 170.29.4.130
rc_rtr2: 170.29.4.131

VLAN 8:
Dirección IP de HSRP – rc_rtr: 170.29.4.145
rc_rtr1: 170.29.4.146
rc_rtr2: 170.29.4.147

VLAN 10:
Dirección IP de HSRP – rc_rtr: 170.29.4.193
rc_rtr1: 170.29.4.194
rc_rtr2: 170.29.4.195

VLAN 11:
Dirección IP de HSRP – rc_rtr: 170.29.4.153
rc_rtr1: 170.29.4.154
rc_rtr2: 170.29.4.155

VLAN 12:
Dirección IP de HSRP – rc_rtr: 170.29.4.161
rc_rtr1: 170.29.4.162
rc_rtr2: 170.29.4.163

VLAN 13 (Heartbeat):
rcscs_hb: 170.29.4.172
rcdbs_hb: 170.29.4.173

VLAN 14:

Dirección IP de HSRP – rc_rtr: 170.29.4.249

rc_rtr1: 170.29.4.250

rc_rtr2: 170.29.4.251

3 Switches Cisco 2950

VLAN 2:

rc_sw1: 170.29.4.5

rc_sw2: 170.29.4.6

rc_sw3: 170.29.4.7

Revisión de los requerimientos del sistema

Administración de la estación de trabajo

El TCP/IP está funcional: Conectividad hacia los servidores que forman parte del cluster:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\prueba> ping 170.29.4.11
Pinging 170.29.4.11 with 32 bytes of data:

Reply from 170.29.4.11: bytes=32 time=2ms TTL=128
Reply from 170.29.4.11: bytes=32 time=7ms TTL=128
Reply from 170.29.4.11: bytes=32 time=7ms TTL=128
Reply from 170.29.4.11: bytes=32 time=2ms TTL=128

Ping statistics for 170.29.4.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 7ms, Average = 4ms
```

Verificar que el Telnet está funcional:

```
C:\Documents and Settings\prueba> telnet 170.29.4.11
Telnet escape character is '^@'.
Trying 170.29.4.11...
Connected to 170.29.4.11.
Escape character is '^@'.

HP-UX rc_scs B.11.11 U 9000/800 (ta)

login:
```

b) Configuración de los servidores del sistema de administración de red

Adición de objetos al DNS

En el DNS:

```
rc_scs:/var/named (106) root% more db.r01.netact.operadora.com
$ORIGIN r01.netact.operadora.com. $TTL 3600
; Please type the following three lines into same line
r01.netact.operadora.com. IN SOA rc_scs.r01.netact.operadora.com.
root.rc_scs.r01.netact.operadora.com. (
   2006020907 ; serial number
   28800      ; refresh after 8 hours
   1200       ; retry after 20 minutes
   604800     ; expire after 1 week
   3600       ; default TTL 1 hour
   )
        NS rc_scs.r01.netact.operadora.com.
        NS rc_dbs.r01.netact.operadora.com.

$ORIGIN      w2k.r01.netact.operadora.com.
; Delegations to the Windows application servers:
w2k     NS      rc_was1.w2k.r01.netact.operadora.com.
        NS      rc_was2.w2k.r01.netact.operadora.com.

; A-records for the Windows nameservers necessary for delegation
rc_was1         A       170.29.4.21
rc_was2         A       170.29.4.22

$ORIGIN r03.netact.operadora.com.

; A-records for the SG packages in this cluster
syspkg          A       170.29.4.15
dbpkg           A       170.29.4.14
osspkg          A       170.29.4.13

; Aliases (=canonical names) for all the SG packages
; example alias
; osspkg        CNAME   rc1oss1.r01.netact.nokia.com.
system  CNAME syspkg.r01.netact.operadora.com.
db      CNAME dbpkg.r01.netact.operadora.com.
osspkg  CNAME osspkg.r01.netact.operadora.com.

; A-records for all other hostnames
localhost       A       127.0.0.1
rc_scs          A       170.29.4.11
rc_dbs          A       170.29.4.12
```

En el archivo /etc/hosts:

```
rc_scs:/m/home/omc (102) omc% cat /etc/hosts
# @(#)B.11.11_LRhosts $Revision: 1.9.214.1 $ $Date: 96/10/08 13:20:01 $
#
# The form for each entry is:
# <internet address>    <official hostname> <aliases>
#
# For example:
# 192.1.2.34    hpfcrm  loghost
#
# See the hosts(4) manual page for more information.
# Note: The entries cannot be preceded by a space.
#       The format described in this file is the correct format.
#       The original Berkeley manual page contains an error in
#       the format description.
#

127.0.0.1       localhost  localhost.r01.netact.operadora.com     loopback
170.29.4.11     rc_scs.r01.netact.operadora.com                   rc_scs
170.29.4.12     rcdbs.r01.netact.operadora.com                    rc_dbs
170.29.4.15     syspkg.r01.netact.operadora.com                   syspkg
170.29.4.14     dbpkg.r01.netact.operadora.com                    dbpkg
170.29.4.13     osspkg.r01.netact.operadora.com                   osspkg
170.29.4.21     rc_was1.w2k.r01.netact.operadora.com              rc_was1
170.29.4.22     rc_was2.w2k.r01.netact.operadora.com              rc_was2

170.29.4.132    spa
170.29.4.133    spb
```

c) Configuración del router y switch Cisco

Configuración inicial del router o switch Cisco

La configuración inicial del switch y router Cisco involucra los siguientes pasos:

Conexión al puerto de consola

La configuración de la terminal de aplicación con las características físicas por defecto: Tasa de 9600 baudios, 8 bits de datos, sin paridad y sin control de flujo.

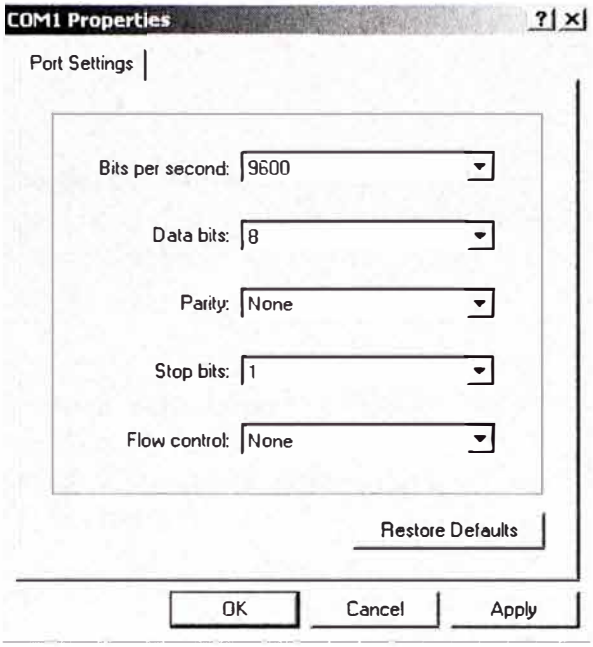


Figura 6.1: configuración de la terminal de aplicación

Configuración de passwords

ROUTER (en rc_rtr1 y rc_rtr2):

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname rc_rtr1
!
boot system flash disk0:c7200-js-mz.122-15.T5.bin
card type e1 0
logging queue-limit 100
enable password 7 052E044B711E4F081A
!
clock timezone sat5 -5
aaa new-model
!
```

SWITCH (en rc_sw1, rc_sw2 y rc_sw3):

```
!
version 12.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname rc_sw1
!
logging buffered 10000 debugging
logging console critical
enable secret 5 $1$P0U/$Q9JRWWz.acKOKbjDU93b..
enable password 7 044904091B
!
clock timezone SAT -5
```

Configuración del router y switch para el acceso por telnet

ROUTER (en rc_rtr1 y rc_rtr2):

```
!
line con 0
line aux 0
line vty 0 4
 password nokia
 login
!
```

SWITCH (en rc_sw1, rc_sw2 y rc_sw3):

```
!
line con 0
line vty 0 4
 password 7 082F43450018
 login
line vty 5 15
 password 7 082F43450018
 login
!
```

Proveer la configuración por defecto con un template de configuración

ROUTER:

```
rc_rtr1# configure terminal
rc_rtr1(config)# <pegar el contenido del archivo template>
rc_rtr1(config)# [CTRL]+Z
rc_rtr1# copy running-config startup-config
```

SWITCH:

```
rc_sw1# copy xmodem flash
Destination filename []? vlan_database.dat
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

rc_sw1# reload
Proceed with reload? [confirm]
```

La solución a utilizar es la SOLUCIÓN ESTÁNDAR

Asignación de un puerto del switch a la VLAN

Configuración en el switch rc_sw1

```
!
interface FastEthernet0/1
 description nms_rc_scs_lan1
 switchport access vlan 2
 speed 100
 duplex full
 spanning-tree portfast
!
interface FastEthernet0/2
 description nms_rc_dbs_lan1
 switchport access vlan 2
 speed 100
 duplex full
 spanning-tree portfast
!
interface FastEthernet0/5
 description nms_rc_was1_lan1
 switchport access vlan 2
 speed 100
 duplex full
 spanning-tree portfast
!
```

```
interface FastEthernet0/6
 description nms_rc_was2_lan1
 switchport access vlan 2
 speed 100
 duplex full
 spanning-tree portfast
!
……
!
interface FastEthernet0/11
 description EMC_SPA
 switchport access vlan 6
 speed 100
 duplex full
 spanning-tree portfast
!
interface FastEthernet0/12
 description EMC_SAN_1
 switchport access vlan 6
 speed 100
 duplex full
 spanning-tree portfast
!
!
interface FastEthernet0/17
 description rc_rtr1_FE0/0
 switchport mode trunk
 speed 100
 duplex full
!
interface FastEthernet0/18
 description rc_rtr2_FE0/1
 switchport mode trunk
 speed 100
 duplex full
!
interface FastEthernet0/19
 description red_externa3
 switchport access vlan 14
 speed 100
 duplex full
!
interface FastEthernet0/21
 description FEC_to_rc_sw3
 switchport mode trunk
 speed 100
```

```
 duplex full
 channel-group 3 mode on
!
interface FastEthernet0/22
 description FEC_to_rc_sw3
 switchport mode trunk
 speed 100
 duplex full
 channel-group 3 mode on
!
interface FastEthernet0/23
 description FEC_to_rc_sw2
 switchport mode trunk
 speed 100
 duplex full
 channel-group 1 mode on
!
interface FastEthernet0/24
 description FEC_to_rc_sw2
 switchport mode trunk
 speed 100
 duplex full
 channel-group 1 mode on
!
interface Vlan1
 no ip address
 no ip proxy-arp
 no ip route-cache
 shutdown
!
interface Vlan2
 ip address 170.29.4.5 255.255.255.128
 no ip route-cache
!
……
!
ip default-gateway 170.29.4.1
ip http server
!
……
!
line con 0
line vty 0 4
 password 7 082F43450018
 login
line vty 5 15
```

```
 password 7 082F43450018
 login
!
ntp clock-period 17179839
ntp server 170.29.4.15
!
end
```

Configuración de las direcciones IP en el router rc_rtr1

```
!
interface FastEthernet0/0
 no ip address
 no ip proxy-arp
 speed 100
 full-duplex
!
interface FastEthernet0/0.1
 description vlan_nativa
 encapsulation dot1Q 1 native
 no ip proxy-arp
 no snmp trap link-status
!
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.2 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 200
 standby 2 preempt
!
.....
!
interface FastEthernet0/0.6
 description nms_servicios
 encapsulation dot1Q 6
 ip address 170.29.4.130 255.255.255.240
 no ip proxy-arp
 no snmp trap link-status
 standby 6 ip 170.29.4.129
 standby 6 priority 200
 standby 6 preempt
!
```

```
interface FastEthernet0/0.7
 description acceso_3g
 encapsulation dot1Q 7
 no ip proxy-arp
 no snmp trap link-status
!
interface FastEthernet0/0.11
 description red_interna
 encapsulation dot1Q 11
 ip address 170.29.4.154 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 standby 11 ip 170.29.4.153
 standby 11 priority 200
 standby 11 preempt
!
……
!
interface FastEthernet0/1
 no ip address
 no ip proxy-arp
 speed 100
 full-duplex
!
interface FastEthernet0/1.8
 description ne2G_locales
 encapsulation dot1Q 8
 ip address 170.29.4.146 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 8 ip 170.29.4.145
 standby 8 priority 200
 standby 8 preempt
!
interface FastEthernet0/1.10
 description red_operador
 encapsulation dot1Q 10
 ip address 170.29.4.194 255.255.255.224
 no ip proxy-arp
 no snmp trap link-status
 standby 10 ip 170.29.4.193
 standby 10 priority 200
 standby 10 preempt
!
```

```
interface FastEthernet0/1.12
 description red_externa1
 encapsulation dot1Q 12
 ip address 170.29.4.162 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 12 ip 170.29.4.161
 standby 12 priority 200
 standby 12 preempt
!
interface FastEthernet0/1.13
 description red_externa2_heartbeat
 encapsulation dot1Q 13
 no ip proxy-arp
 no snmp trap link-status
!
interface FastEthernet0/1.14
 description red_externa3
 encapsulation dot1Q 14
 ip address 170.29.4.250 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 14 ip 170.29.4.249
 standby 14 priority 200
 standby 14 preempt
!
.....
!
```

Configuración del protocolo HSRP

En el router rc_rtr1:

```
!
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.2 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 200
 standby 2 preempt
!
```

En el router rc_rtr2:

```
!
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.3 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 150
 standby 2 preempt
!
```

Configuración del protocolo OSPF

```
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 170.29.4.0 0.0.0.255 area 2
 network 170.26.1.1 0.0.0.0 area 2
 network 170.26.1.129 0.0.0.0 area 2
!
```

Configuración del SNMP

ROUTER:

```
!
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source FastEthernet0/0.2
snmp-server host 170.29.4.13 public
!
```

SWITCH:

```
!
snmp-server community public RO
snmp-server trap-source Vlan2
snmp-server host 170.29.4.13 public
!
```

Opcional - Configuración del NTP y TZ

ROUTER:

```
ntp clock-period 17180197
ntp server 170.29.4.15
```

SWITCH:

```
ntp clock-period 17179839
ntp server 170.29.4.15
```

Configuración en los switches

Interconexión entre switches

En el switch rc_sw1:

```
interface FastEthernet0/21
 description FEC_to_rc_sw3
 switchport mode trunk
 speed 100
 duplex full
 channel-group 3 mode on

interface FastEthernet0/22
 description FEC_to_rc_sw3
 switchport mode trunk
 speed 100
 duplex full
 channel-group 3 mode on

interface FastEthernet0/23
 description FEC_to_rc_sw2
 switchport mode trunk
 speed 100
 duplex full
 channel-group 2 mode on

interface FastEthernet0/24
 description FEC_to_rc_sw2
 switchport mode trunk
 speed 100
 duplex full
 channel-group 2 mode on
```

En el switch rc_sw2:

```
interface FastEthernet0/21
 description FEC_to_rc_sw1
 switchport mode trunk
 speed 100
 duplex full
 channel-group 1 mode on

interface FastEthernet0/22
 description FEC_to_rc_sw1
 switchport mode trunk
 speed 100
 duplex full
 channel-group 1 mode on

interface FastEthernet0/23
 description FEC_to_rc_sw3
 switchport mode trunk
 speed 100
 duplex full
 channel-group 3 mode on

interface FastEthernet0/24
 description FEC_to_rc_sw3
 switchport mode trunk
 speed 100
 duplex full
 channel-group 3 mode on
```

En el switch rc_sw3:

```
interface FastEthernet0/21
 description FEC_to_rc_sw2
 switchport mode trunk
 speed 100
 duplex full
 channel-group 2 mode on

interface FastEthernet0/22
 description FEC_to_rc_sw2
 switchport mode trunk
 speed 100
 duplex full
```

```
 channel-group 2 mode on

interface FastEthernet0/23
 description FEC_to_rc_sw1
 switchport mode trunk
 speed 100
 duplex full
 channel-group 1 mode on

interface FastEthernet0/24
 description FEC_to_rc_sw1
 switchport mode trunk
 speed 100
 duplex full
 channel-group 1 mode on
```

Interconexión hacia los routers y elementos de red

En el switch rc_sw1:

```
interface FastEthernet0/7
 description ne2G_to_MSC_TEST_LAN
 switchport access vlan 8
 speed 100
 duplex full

interface FastEthernet0/17
 description rc_rtr1_FE0/0
 switchport mode trunk
 speed 100
 duplex full

interface FastEthernet0/18
 description rc_rtr2_FE0/1
 switchport mode trunk
 speed 100
 duplex full

interface FastEthernet0/19
 description red_externa3
 switchport access vlan 14
 speed 100
 duplex full
```

En el switch rc_sw2:

```
interface FastEthernet0/7
 description ne2G_to_MSS_TEST_IP
 switchport access vlan 8
 speed 100
 duplex full

interface FastEthernet0/17
 description rc_rtr1_FE0/1
 switchport mode trunk
 speed 100
 duplex full

interface FastEthernet0/18
 description rc_rtr2_FE0/0
 switchport mode trunk
 speed 100
 duplex full

interface FastEthernet0/19
 description red_externa3
 switchport access vlan 14
 speed 100
 duplex full
```

Configuración de los parámetros ISO IP

Configuración del enrutamiento dinámico IS-IS

```
clns routing
```

```
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.2 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 200
 standby 2 preempt
```

```
interface FastEthernet0/1.8
 description ne2G_locales
 encapsulation dot1Q 8
 ip address 170.29.4.146 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 8 ip 170.29.4.145
 standby 8 priority 200
 standby 8 preempt


interface FastEthernet0/1.12
 description red_externa1
 encapsulation dot1Q 12
 ip address 170.29.4.162 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 12 ip 170.29.4.161
 standby 12 priority 200
 standby 12 preempt


interface FastEthernet0/1.14
 description red_externa3
 encapsulation dot1Q 14
 ip address 170.29.4.250 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 14 ip 170.29.4.249
 standby 14 priority 200
 standby 14 preempt
```

En el router rc_rtr1:

```
router isis dcn
net 39.604f.0000.0000.0000.0001.0001.1700.2900.4002.00
 log-adjacency-changes
```

En el router rc_rtr2:

```
!
router isis dcn
net 39.604f.0000.0000.0000.0001.0001.1700.2900.4003.00
 log-adjacency-changes
!
```

Configuración de las interfases E1:

```
!
controller E1 0/0
 channel-group 0 timeslots 1
 channel-group 1 timeslots 2
 channel-group 2 timeslots 7-8
 channel-group 3 timeslots 5-6
.
.
.
!
```

Configuración de las interfases seriales sincrónicas:

```
!
x25 routing
!
.....
!
interface Serial0/0:2
 description X.25 NE_NAME
 no ip address
 encapsulation x25 dce
 no ip route-cache
 x25 address 17002900400207
 x25 htc 16
 x25 map clns 000000123456 broadcast
 clns router isis dcn
 isis circuit-type level-1
 isis hello-interval 65535
!
.....
!
x25 route ^000000123456$ interface Serial0/0:2
x25 host NE_NAME 000000123456
```

```
Serial0/0:2 is up, line protocol is up
  Hardware is PA-MC-8TE1 Plus
  Description: X.25 NE_NAME
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation X25, crc 16, loopback not set
  X.25 DCE, address 17002900400207, state R1, modulo 8, timer 0
      Defaults: idle VC timeout 0
        cisco encapsulation
        input/output window sizes 2/2, packet sizes 128/128
      Timers: T10 60, T11 180, T12 60, T13 60
      Channels: Incoming-only none, Two-way 1-16, Outgoing-only
none
      RESTARTs 7/0 CALLs 8+4/0+26/0+0 DIAGs 0/0
  LAPB DCE, state CONNECT, modulo 8, k 7, N1 12056, N2 20
      T1 3000, T2 0, interface outage (partial T3) 0, T4 0
      VS 0, VR 5, tx NR 5, Remote VR 0, Retransmissions 0
      Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
      IFRAMEs 216710/407435 RNRs 0/0 REJs 0/1 SABM/Es 111/5 FRMRs
0/0 DISCs 0/0
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters 8w6d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     624157 packets input, 11807077 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 7 giants, 0 throttles
     1788 input errors, 1666 CRC, 0 frame, 0 overrun, 0 ignored,
110 abort
     510998 packets output, 5189401 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     7 carrier transitions   no alarm present
  Timeslot(s) Used:7-8, subrate: 64Kb/s, transmit delay is 0
flags
```

6.3 Integración del elemento de red del subsistema BSS

A continuación se muestra la aplicación de los modelos de integración a los elementos del subsistema de estación base (BSS). Los tipos de de integración a utilizar son: Integración por LAN y X25 sobre PCM.

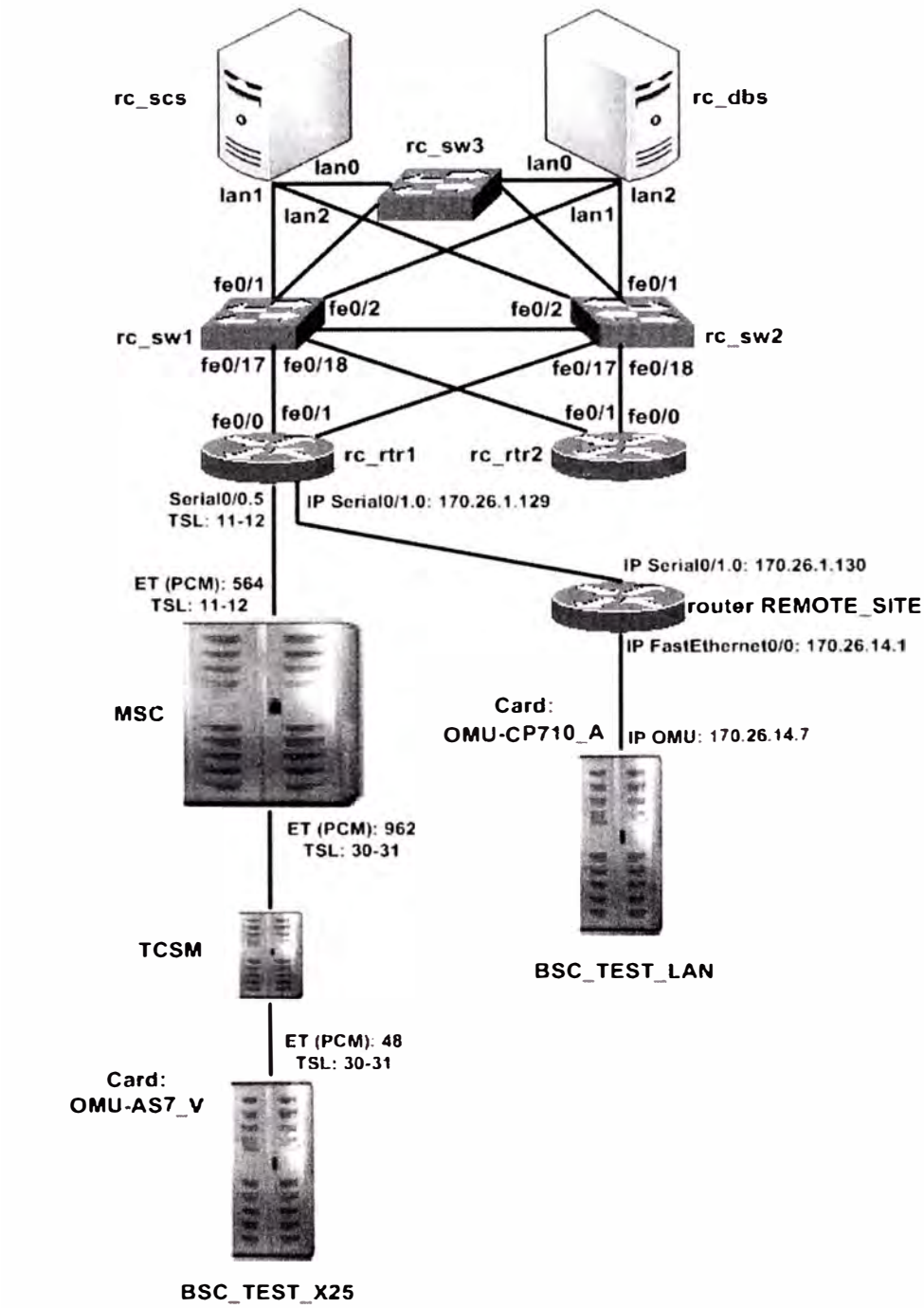


Figura 6.2: Topología de la integración del BSC usando X25 sobre PCM y LAN

6.3.1 Configuración en los routers rc_rtr1 y rc_rtr2

```
!
hostname rc_rtr1
!
!
username nokia privilege 15 password 7 1128124147410A0D00
clock timezone sat5 -5
no aaa new-model
ip subnet-zero
ip cef
!
!
ip ftp username user
ip ftp password 7 0334504F565C204D4A
ip host rc_scs 170.29.4.11
ip host rc_dbs 170.29.4.12
ip host rc_sw1 170.29.4.5
ip host rc_sw2 170.29.4.6
ip host rc_sw3 170.29.4.7
!
!
clns routing
!
……
!
x25 routing
!
……
!
controller E1 0/0
……
 channel-group 5 timeslots 11-12
……
!
……
!
controller E1 0/1
 channel-group 0 timeslots 1-31
 description Conexion WAN - REMOTE_SITE
!
!
interface Loopback0
 ip address 170.26.1.1 255.255.255.252
 clns router isis dcn
!
```

```
!
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.2 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 200
 standby 2 preempt
!
……
!
interface Serial0/0:5
 description x.25 link to BSC_TEST_X25
 no ip address
 encapsulation x25 dce
 no ip route-cache
 x25 address 170029004002 11
 x25 htc 16
 x25 map clns 000000123456 broadcast
 clns router isis dcn
 isis circuit-type level-1
 isis hello-interval 65535
!
……
!
interface Serial0/1:0
 description BSC-REMOTE_SITE
 ip address 170.26.1.129 255.255.255.252
 clns router isis dcn
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 170.29.4.0 0.0.0.255 area 2
 network 170.26.1.1 0.0.0.0 area 2
 network 170.26.1.129 0.0.0.0 area 2
!
!
router isis dcn
 net 39.604f.0000.0000.0000.0001.0001.1700.2900.4002.00
log-adjacency-changes
!
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 170.29.4.254
!
ip http server
no ip http secure-server
!
……
!
x25 route ^000000123456$ interface Serial2/0:5
x25 host BSC_TEST_X25 000000123456
!
……
!
ntp clock-period 17179630
ntp server 170.29.4.15
!
```

6.3.2 Configuración en el router REMOTE_SITE

```
!
hostname REMOTE_SITE
!
enable secret 5 $1$Jtyu$Lfu5megCxXa4kUOG00Q5P.
!
username backup privilege 15 password 7 1502000F06242A34
aaa new-model
!
!
ip subnet-zero
!
……
!
clns routing
!
……
!
controller E1 0/1
 channel-group 0 timeslots 1-31
!
……
!
interface FastEthernet0/0
 ip address 170.26.14.1 255.255.255.224
 duplex auto
 speed auto
 clns router isis dcn
!
……
```

```
!
interface Serial0/1:0
 ip address 170.26.1.130 255.255.255.252
 clns router isis dcn
!
router ospf 1
 log-adjacency-changes
 network 170.26.1.130 0.0.0.0 area 2
 network 170.26.14.1 0.0.0.0 area 2
!
router isis dcn
 net 39.604f.0000.0000.0000.0001.0001.1700.2600.1129.00
 log-adjacency-changes
!
.....
!
ip classless
ip route 0.0.0.0 0.0.0.0 170.26.1.129
ip http server
!
```

6.3.3 Configuración en el BSC

a) Utilizando X25 sobre PCM

Tarjeta de red del elemento de red

La tarjeta de red utilizada para la integración, está ubicada en la Unidad de operación y mantenimiento (OMU) del BSC.

La tarjeta a utilizar para la integración es la unidad AS7-V, la cual es utilizada para conexiones X25 sobre PCM.

```
OMU          IN LOC  1A058-27

  AS7_V    2  TRACK:  7
   MS:80300000  ME:803FFFFF   IS:      IE:
   INT:26H      SW:06490012
                                    TSLS 30        20        10         0
   X25             4M   PCM:    1     B  00000000000000000000000000000011
                                      R  00000000000000000000000000000011
```

Tareas Preliminares

Elementos de red:

Hardware: BSC2i NOKIA

Versión de software: Software versión 11.0

Nombre del elemento de red: BSC_TEST_X25

Número C: 123456

CLNS:

Dirección de área: 39604F00000000000000010001

Identificador del sistema: 000000123456

Revisión de los requerimientos del sistema

Sistema de Administración de Red

SYSOP:

```
BSC2i     BSC_TEST_X25                  2005-11-09  16:37:50
USER ID:  SYSOP
PROFILE NAME: SYSOP
COMMAND CLASS AUTHORITIES:

 A=250 B=250 C=250 D=250 E=250   F=250 G=250 H=250 I=250 J=250
 K=250 L=250 M=250 N=250 O=250   P=250 Q=250 R=250 S=250 T=250
 U=250 V=250 W=250 X=250 Y=250

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: COMPLETE
UNIQUE PROFILE: YES
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: NO
NETWORK USE ALLOWED: YES
```

TRAFADM:

```
BSC2i     BSC_TEST_X25                  2005-11-09  16:37:50
USER ID:  TRAFADM
PROFILE NAME: TRAFADM
COMMAND CLASS AUTHORITIES:

 A=1 B=1 C=1 D=1 E=1   F=1 G=1 H=1 I=1 J=1
 K=1 L=1 M=1 N=1 O=1   P=1 Q=1 R=1 S=1 T=1
 U=1 V=1 W=1 X=1 Y=1

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: LIMITED
UNIQUE PROFILE: YES
```

```
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: WRITE
NETWORK USE ALLOWED: YES
```

Creación de objetos a ser supervisados en el sistema de administración de red

El objeto es creado en el Sistema de administración de red. Con la creación, los parámetros necesarios para la administración del elemento de red serán almacenados en la Base de Datos del sistema.

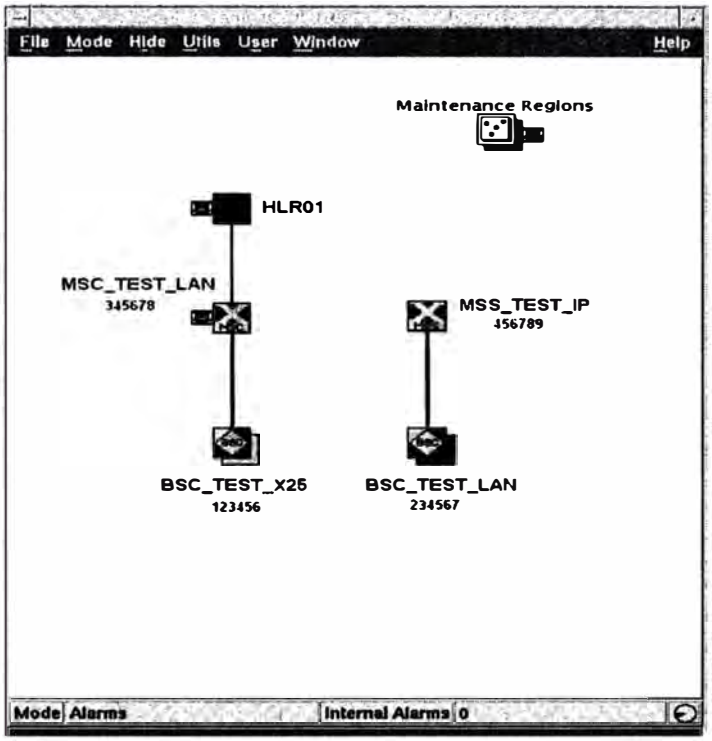


Figura 6.3: Creación de objetos en el sistema de administración de red

Configuración en el elemento de red

Configuración de la conexión física

Instalación y configuración de la tarjeta en el elemento de red

```
OMU          IN LOC  1A058-27

 AS7_V    2  TRACK:  7
  MS:80300000  ME:803FFFFF   IS:      IE:
  INT:26H      SW:06490012
                                TSLS 30        20        10         0
  X25            4M   PCM:    1    B  00000000000000000000000000000011
                                   R  00000000000000000000000000000011
```

Instalación y configuración en la Terminal de Intercambio (ET)

```
ET-48         IN LOC  1A030-01

  ET2E_SC  0  TRACK:  4
   MS:          ME:           IS:       IE:
   INT:         SW:0649001D
                                    TSLS 30        20        10         0
   ETT00           4M   PCM:   48     B  00000000000000000000000000000001
                                       R  00000000000000000000000000000001

TOTAL OF     1  UNITS,      1  PLUG-IN UNITS AND      1  FUNCTIONS
```

Configuración de las conexiones semipermanentes

En el BSC:

```
PHYSICAL CHANNELS THROUGH DIGITAL TERMINAL

                                        DTE X.25       EXTERNAL      INTERNAL
CHANNEL SNPA-ADDRESS   UNIT  TERM DCE PARAM SET PCM  TSL TSL PCM  TSL TSL
------- -------------- ----- ---- --- --------- ------------ ------------
     0  000000123456   OMU     2  DTE OPDEF      48  30 31     1  00 01
```

En la MSC:

```
SEMIPERMANENT CIRCUIT TRUNK TO TRUNK
    CRCT (PCM - TSL)          CRCT (PCM - TSL)
          ......
       962 - 30                  564 - 11
       962 - 31                  564 - 12
          ......
```

Configuración y modificación de los parámetros X.25 (conexiones digitales)

```
PARAMETER SET NAME: OPDEF
==================

MAXIMUM NETWORK SERVICE DATA UNIT LENGTH:  2048 BYTES
L2 CONNECTION MODE: INITIATED AFTER START UP
```

```
LEVEL 2 PARAMETERS:
-------------------
L2 TIMER T1:    6 SECONDS                L2 BITS IN FRAME:    1024 BITS
L2 TIMER T2:  NOT IN USE                 L2 RETRY COUNT:        10 TIMES
L2 TIMER T3:  NOT IN USE                 L2 WINDOW:              7 FRAMES
L2 INTERFRAME FILL:   01111110              L2 LINE DOWN TIMER:    20 (NOT
SUPPORTED)

LEVEL 3 PARAMETERS:
-------------------
L3 USER DATA SIZE:   128 BYTES
L3 SEND WINDOW SIZE:   2 FRAMES
L3 MODULO:   8

L3 TIMER T20:    180 SECONDS
L3 TIMER T21:    200 SECONDS
L3 TIMER T22:    180 SECONDS             L3 RESET RETRY COUNT:    5 TIMES
L3 TIMER T23:    180 SECONDS             L3 CLEAR RETRY COUNT:    5 TIMES

L3 FIRST PVC:      0 (= NOT IN USE)      L3 LAST PVC:      0 (= NOT IN USE)
L3 LIC:            0 (NOT SUPPORTED)     L3 HIC:           0 (NOT SUPPORTED)
L3 LTC:            1                     L3 HTC:          16
L3 LOC:            0 (NOT SUPPORTED)     L3 HOC:           0 (NOT SUPPORTED)

USER FACILITIES:
----------------
NO USER FACILITIES
```

Creación y configuración del canal físico

```
PHYSICAL CHANNELS THROUGH DIGITAL TERMINAL

                                        DTE X.25       EXTERNAL      INTERNAL
CHANNEL SNPA-ADDRESS  UNIT    TERM DCE PARAM SET PCM  TSL TSL PCM  TSL TSL
------- ----------- -------- ---- --- --------- ------------ ------------
   0  000000123456     OMU       2  DTE OPDEF      48  30 31     1  00 01
```

Creación y configuración del objeto CLNS

```
INTERROGATING CLNS
NODE IN ES ROLE

                  NS USER     NS USER     MAX PDU   SYSTEM
CLNS NAME  ROLE   PRIM UNIT   ACT UNIT    LIFETIME  ID                STATE
---------  ----   ---------   ---------   --------  ------------  ----------
ES          ES    OMU         OMU          9     000000123456      UNL-BU-ACT

MAX MAN AREA ADDR COUNT: 2
MANUAL AREA ADDRESS:     39604F00000000000000010001
```

Creación y configuración del objeto de enlace

```
INTERROGATING LINKAGE DATA
NODE IN ES ROLE
LINKAGE TYPE ROLE UNIT     LOG UNIT TERM SNPA ADDRESS     PVC  PRIO STATE
------- ---- ---- -------- -------- ---- --------------- ---- ---- -------
   1   X.25  ES   OMU      4002H      2  170029004002 11    -    -  UNL-ENA
```

Creación y configuración de las direcciones NSAP local y remota

```
INTERROGATING NETWORK ADDRESS DATA
NET ADDR  ROLE     NSAP NR PRIO NSAP NR PRIO
--------  ------   ------- ---- ------- ----
LOCAL     LOCAL          1    -
REMNMS    REMOTE         2  100       3   75
```

Creación y configuración de las direcciones de red local y remota y la conexión de las direcciones NSAPs a las direcciones de red

```
INTERROGATED NSAP DATA

LOCAL N-SELECTOR
NBR   ROLE    STATE   SEL
----- ------ ------- ---
    1 LOCAL  UNL-ENA 00
```

```
ISO DCC/ISO 6253-ICD NSAP
NBR   ROLE    STATE  AFI IDI   DFI ORG    RESERVED AREA END SYSTEM   SEL
----- ------ ------- --- ---- --- ------ -------- ---- ------------ ---
    2 REMOTE UNL-ENA 39  604F 00  000000 00000001 0001 170029004015 00
    3 REMOTE UNL-ENA 39  604F 00  000000 00000001 0001 170029004012 00
```

Creación y configuración de las aplicaciones locales y remotas

```
LOCAL OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE   UNIT        FAM ID PROC ID
---------------- ------ -------- ------- ---------- ------- -------
BSC123456F       VFS    LOCAL    UNL-ENA OMU
BSC123456VT      VTP    LOCAL    UNL-ENA OMU
BSC123456A       CMISE  LOCAL    UNL-ENA OMU          021FH   0000H
BSC123456EHA     CMISE  LOCAL    UNL-ENA OMU          02B1H   0000H
BSC123456NOD     TPU    LOCAL    UNL-ENA OMU          02AFH   0000H

REMOTE OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE
---------------- ------ -------- -------
OMC000000D1      CMISE  REMNMS   UNL-ENA
OMC000000BP      CMISE  REMNMS   UNL-ENA
OMC000000FP      VFS    REMNMS   UNL-ENA
OMC000000SW      VFS    REMNMS   UNL-ENA
```

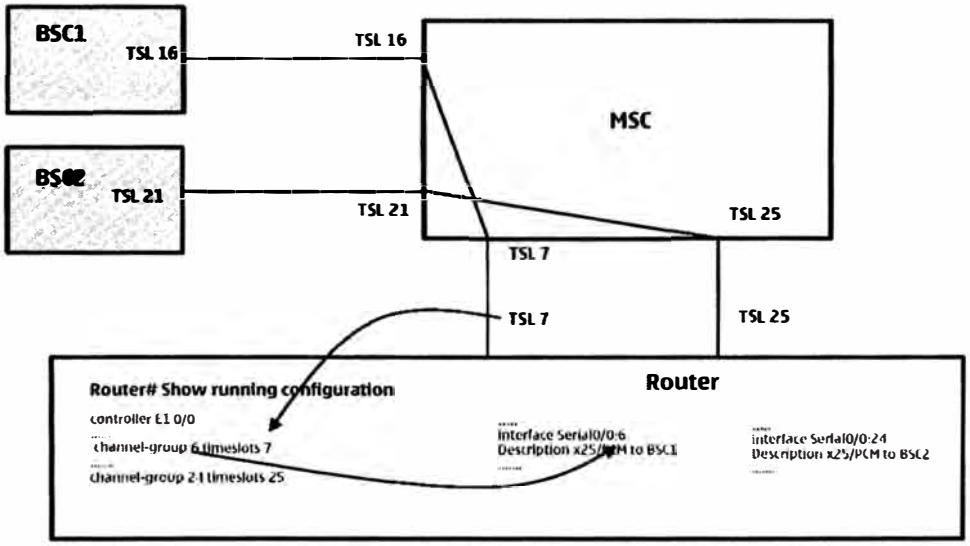


Figura 6.4: Conexiones semipermanentes PCM

Configuración del servicio y perfil CMISE

```
LOCAL OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE   UNIT        FAM ID PROC ID
---------------- ------ -------- -------  ---------- ------- -------
BSC123456A       CMISE  LOCAL    UNL-ENA  OMU          021FH   0000H

AP_TYPE    : NOT IN USE
AP_TITLE   :
AEQ        :

P-SELECTOR: 3333030230
S-SELECTOR: 3333030230
T-SELECTOR: 3333


INTERROGATING SERVICE PROFILE DATA

AE-NAME           SERVICE PROFILE TYPE
----------------  ------------------------------
BSC123456A        CMISE

MULTIPLE OBJECT SELECTION = YES  FILTER SUPPORT   = YES
MULTIPLE REPLYS           = YES  EXTENDED SERVICE = NO
CANCEL GET OPERATION      = YES  CMISE VERSION    = 1 AND 2
```

b) Utilizando LAN

Tarjeta de red del elemento de red

```
OMU          IN LOC  1A002-06

  CP710_A  0  TRACK: 10
   MS:          ME:           IS:  0   IE: 3FF
   INT:         SW:
```

Tareas Preliminares

Elementos de red:

Hardware: BSC3i NOKIA

Versión de software: Software versión 11.0

Nombre del elemento de red: BSC_TEST_LAN

Número C: 234567

CLNS:

Dirección de área: 39604F00000000000000010001

Identificador del sistema: 000000234567

Revisión de los requerimientos del sistema

Sistema de Administración de Red

SYSOP:

```
BSC3i     BSC_TEST_LAN                  2005-11-09  17:37:50
USER ID:  SYSOP
PROFILE NAME: SYSOP
COMMAND CLASS AUTHORITIES:

 A=250 B=250 C=250 D=250 E=250   F=250 G=250 H=250 I=250 J=250
 K=250 L=250 M=250 N=250 O=250   P=250 Q=250 R=250 S=250 T=250
 U=250 V=250 W=250 X=250 Y=250

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: COMPLETE
UNIQUE PROFILE: YES
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: NO
NETWORK USE ALLOWED: YES
```

TRAFADM:

```
BSC3i     BSC_TEST_LAN                  2005-11-09  17:37:50
USER ID:  TRAFADM
PROFILE NAME: TRAFADM
COMMAND CLASS AUTHORITIES:

 A=1 B=1 C=1 D=1 E=1   F=1 G=1 H=1 I=1 J=1
 K=1 L=1 M=1 N=1 O=1   P=1 Q=1 R=1 S=1 T=1
 U=1 V=1 W=1 X=1 Y=1

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: LIMITED
UNIQUE PROFILE: YES
```

```
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: WRITE
NETWORK USE ALLOWED: YES
```

Creación de objetos a ser supervisados en el sistema de administración de red

El objeto es creado en el Sistema de administración de red. Con la creación, los parámetros necesarios para la administración del elemento de red serán almacenados en la Base de Datos del sistema.

Configuración en el elemento de red

Configuración de la conexión física

Instalación y configuración de las tarjetas en el elemento de red

```
OMU           IN LOC  1A002-06

  CP710_A  0  TRACK: 10
   MS:           ME:            IS:  0    IE: 3FF
   INT:          SW:
```

Creación y configuración del objeto CLNS

```
INTERROGATING CLNS
NODE IN ES ROLE
                 NS USER     NS USER     MAX PDU   SYSTEM
CLNS NAME  ROLE  PRIM UNIT   ACT UNIT    LIFETIME  ID                STATE
---------  ----  ---------  ---------   --------  ------------  -----------
ES          ES   OMU        OMU         9         000000234567   UNL-BU-ACT

MAX MAN AREA ADDR COUNT: 3
MANUAL AREA ADDRESS:     39604F00000000000000010001
```

Creación y configuración del objeto de enlace (linkage object)

```
INTERROGATING LINKAGE DATA
NODE IN ES ROLE
LINKAGE TYPE ROLE UNIT    LOG UNIT TERM SNPA ADDRESS     PVC  PRIO STATE
------- ---- ---- ------- -------- ---- ---------------- ---- ---- ------
   0    BRO   ES  OMU     4002H      0      -              -    -  UNL-ENA
```

Creación y configuración de las direcciones NSAPs local y remota

```
INTERROGATING NETWORK ADDRESS DATA
NET ADDR  ROLE    NSAP NR PRIO NSAP NR PRIO
--------  ------  ------- ---- ------- ----
LOCAL     LOCAL         1    -
REMNMS    REMOTE        2  100       3   75
```

Creación de las direcciones de red local y remota y la conexión de las direcciones NSAPs a las direcciones de red

```
INTERROGATED NSAP DATA

LOCAL N-SELECTOR

NBR   ROLE    STATE  SEL
----- ------ ------- ---
    1 LOCAL  UNL-ENA 00

ISO DCC/ISO 6253-ICD NSAP

NBR   ROLE    STATE  AFI IDI  DFI ORG    RESERVED AREA END SYSTEM   SEL
----- ------ ------- --- ---- --- ------ -------- ---- ------------ ---
    2 REMOTE UNL-ENA 39  604F 00  000000 00000001 0001 170029004015 00
    3 REMOTE UNL-ENA 39  604F 00  000000 00000001 0001 170029004012 00
```

Configuración de las aplicaciones locales y remotas

```
LOCAL OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE   UNIT        FAM ID PROC ID
---------------- ------ -------- ------- ---------- ------- -------
BSC234567F       VFS    LOCAL    UNL-ENA  OMU
BSC234567VT      VTP    LOCAL    UNL-ENA  OMU
BSC234567A       CMISE  LOCAL    UNL-ENA  OMU          021FH   0000H
BSC234567EHA     CMISE  LOCAL    UNL-ENA  OMU          02B1H   0000H
BSC234567NOD     TPU    LOCAL    UNL-ENA  OMU          02AFH   0000H

REMOTE OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE
---------------- ------ -------- -------
OMC000000D1      CMISE  REMNMS   UNL-ENA
OMC000000BP      CMISE  REMNMS   UNL-ENA
```

```
OMC000000FP       VFS     REMNMS    UNL-ENA
OMC000000SW       VFS     REMNMS    UNL-ENA
```

Configuración del servicio y perfil CMISE

```
LOCAL OSI APPLICATION DATA

AE-NAME           APPL    NET ADDR  STATE    UNIT         FAM ID PROC ID
---------------- ------ -------- -------  ---------- ------- -------
BSC234567EHA      CMISE   LOCAL     UNL-ENA  OMU           02B1H   0000H

AP_TYPE     : NOT IN USE
AP_TITLE    :
AEQ         :

P-SELECTOR: 3333030231
S-SELECTOR: 3333030231
T-SELECTOR: 3333


INTERROGATING SERVICE PROFILE DATA

AE-NAME           SERVICE PROFILE TYPE
----------------  ------------------------------
BSC234567A        CMISE

MULTIPLE OBJECT SELECTION = YES  FILTER SUPPORT    = YES
MULTIPLE REPLYS           = YES  EXTENDED SERVICE = NO
CANCEL GET OPERATION      = YES  CMISE VERSION    = 1 AND 2
```

Configuración de la unidad de operación y mantenimiento (OMU)

```
INTERROGATING NETWORK INTERFACE DATA
                                          ADDR                ADM    PRIO-
UNIT                NAME    IP ADDRESS    TYPE NML ASSIGNED STATE RISED
------------------ ------ --------------- ---- --- -------- ----- -----
OMU                 EL0     170.26.14.7     L     24 YES      UP    NO

INTERROGATED ROUTE DATA
                                    NEXT ADDR
UNIT              DESTINATION       HOP  TYPE ADDRESS                NBR
--------------- ------------------ ---- ---- -------------------- -----
OMU             DEFAULT ROUTE      GW   IP   170.26.14.1              1
```

6.4 Integración del elemento de red del subsistema NSS

A continuación se muestra la aplicación de los modelos de integración a los elementos del subsistema de conmutación de red (NSS). Los tipos de de integración a utilizar son: Integración por LAN e IP.

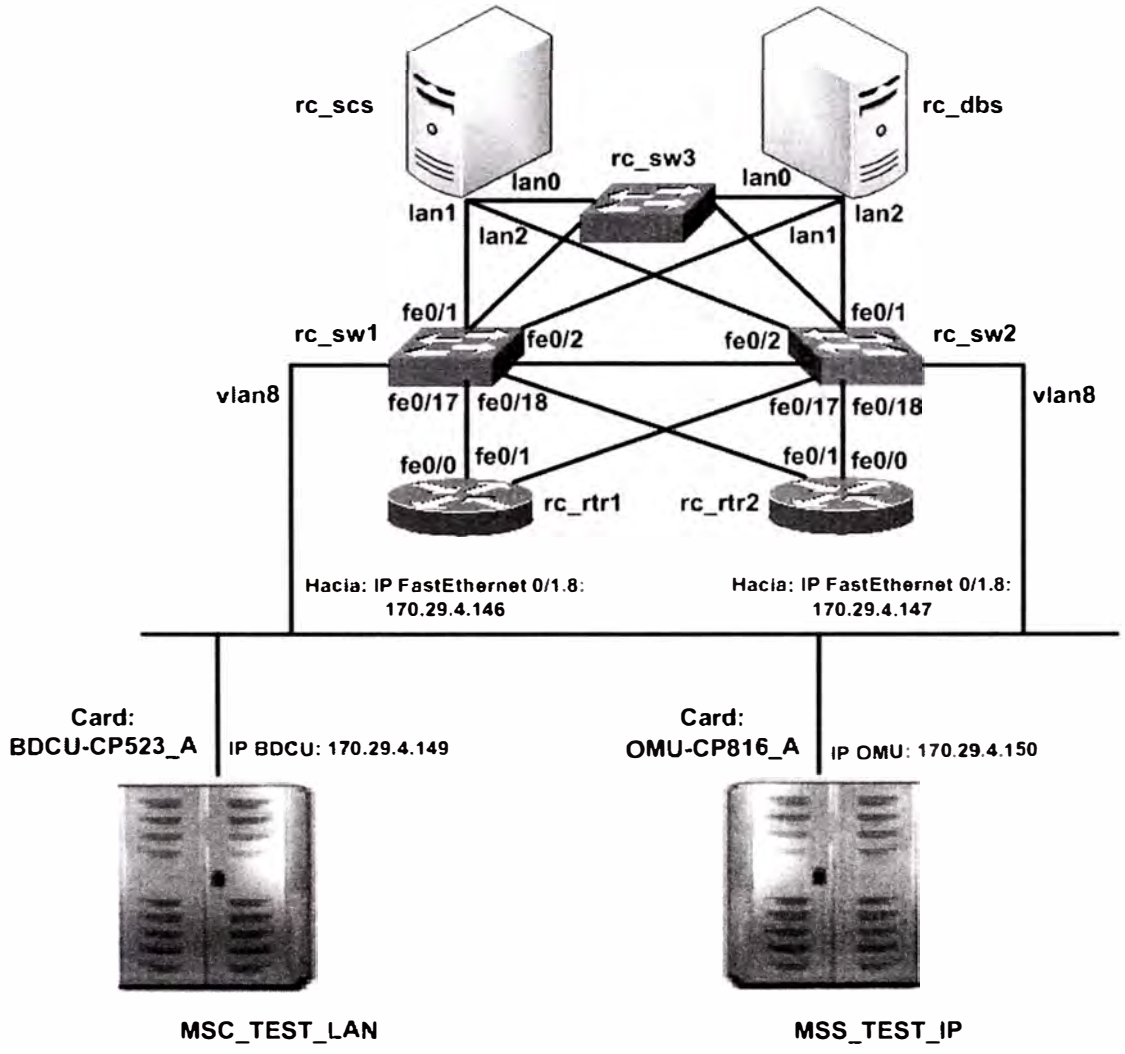


Figura 6.5: Topología de la integración de la MSC usando LAN e IP

6.4.1 Configuración en los routers rc_rtr1 y rc_rtr2

En el router rc_rtr1:

```
!
hostname rc_rtr1
!
username nokia privilege 15 password 7 1128124147410A0D00
clock timezone sat5 -5
no aaa new-model
ip subnet-zero
ip cef
!
!
ip ftp username user
ip ftp password 7 0334504F565C204D4A
ip host rc_scs 170.29.4.11
ip host rc_dbs 170.29.4.12
ip host rc_sw1 170.29.4.5
ip host rc_sw2 170.29.4.6
ip host rc_sw3 170.29.4.7
!
clns routing
!
.....
!
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.2 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 200
 standby 2 preempt
!
.....
!
interface FastEthernet0/1.8
 description ne2G_locales
 encapsulation dot1Q 8
 ip address 170.29.4.146 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 8 ip 170.29.4.145
```

```
 standby 8 priority 200
 standby 8 preempt
!
……
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 170.29.4.0 0.0.0.255 area 2
 network 170.26.1.1 0.0.0.0 area 2
 network 170.26.1.129 0.0.0.0 area 2
!
……
!
router isis dcn
 net 39.604f.0000.0000.0000.0001.0001.1700.2900.4002.00
 log-adjacency-changes
!
……
!
ip classless
ip route 0.0.0.0 0.0.0.0 170.29.4.254
!
ip http server
no ip http secure-server
!
……
!
ntp clock-period 17179630
ntp server 170.29.4.15
!
```

En el router rc_rtr2:

```
!
hostname rc_rtr2
!
username nokia privilege 15 password 7 1128124147410A0D00
clock timezone sat5 -5
no aaa new-model
ip subnet-zero
ip cef
!
!
```

```
ip ftp username user
ip ftp password 7 0334504F565C204D4A
ip host rc_scs 170.29.4.11
ip host rc_dbs 170.29.4.12
ip host rc_sw1 170.29.4.5
ip host rc_sw2 170.29.4.6
ip host rc_sw3 170.29.4.7
!
clns routing
!
……
!
interface FastEthernet0/0.2
 description nms_cluster1
 encapsulation dot1Q 2
 ip address 170.29.4.3 255.255.255.128
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 2 ip 170.29.4.1
 standby 2 priority 200
 standby 2 preempt
!
……
!
interface FastEthernet0/1.8
 description ne2G_locales
 encapsulation dot1Q 8
 ip address 170.29.4.147 255.255.255.248
 no ip proxy-arp
 no snmp trap link-status
 clns router isis dcn
 standby 8 ip 170.29.4.145
 standby 8 priority 200
 standby 8 preempt
!
……
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 170.29.4.0 0.0.0.255 area 2
 network 170.26.1.1 0.0.0.0 area 2
 network 170.26.1.129 0.0.0.0 area 2
!
……
```

```
!
router isis dcn
 net 39.604f.0000.0000.0000.0001.0001.1700.2900.4003.00
 log-adjacency-changes
!
.....
!
ip classless
ip route 0.0.0.0 0.0.0.0 170.29.4.254
!
ip http server
no ip http secure-server
!
.....
!
ntp clock-period 17179630
ntp server 170.29.4.15
!
```

6.4.2 Configuración del DNS

Se procede a la configuración del elemento de red que será integrado utilizando IP en los archivos de configuración de zonas del DNS.

```
$ORIGIN .
$TTL 3600       ; 1 hour
nss.netact.operadora.com  IN SOA  rc_scs.r01.netact.operadora.com.
root.rc_scs.r01.netact.operadora.com. (
   2005120620 ; serial
   28800      ; refresh (8 hours)
   1200       ; retry (20 minutes)
   604800     ; expire (1 week)
   3600       ; minimum (1 hour)
   )
         NS      rc_scs.r01.netact.operadora.com.
         NS      rc_dbs.r01.netact.operadora.com.
$ORIGIN nss.netact.operadora.com.

MSC_TEST_IP               CNAME   msc_test_ip-omu
msc_test_ip-omu           A       170.29.4.149
```

6.4.3 Configuración en la MSC

a) Utilizando LAN

Tarjeta de red del elemento de red

La tarjeta de red utilizada para la integración, está ubicada en la Unidad Básica de Comunicación de Datos (BDCU) del MSC:

```
BDCU-0        IN LOC  1A005-08

  CP523_A  0  TRACK: 10
   MS:           ME:           IS:  0    IE: 3FF
   INT:          SW:
```

Tareas Preliminares

Elementos de red:

Hardware: MSCi NOKIA

Versión de software: Software versión 13.0

Nombre del elemento de red: MSC_TEST_LAN

Número C: 345678

CLNS:

Dirección de área: 39604F00000000000000010001

Identificador del sistema: 000000345678

Revisión de los requerimientos del sistema

Sistema de Administración de Red

SYSOP:

```
MSCi     MSC_TEST_LAN                  2005-11-19  16:37:50
USER ID:  SYSOP
PROFILE NAME: SYSOP
COMMAND CLASS AUTHORITIES:

 A=250 B=250 C=250 D=250 E=250   F=250 G=250 H=250 I=250 J=250
 K=250 L=250 M=250 N=250 O=250   P=250 Q=250 R=250 S=250 T=250
 U=250 V=250 W=250 X=250 Y=250

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: COMPLETE
UNIQUE PROFILE: YES
```

```
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: NO
NETWORK USE ALLOWED: YES
```

TRAFADM:

```
MSCi      MSC_TEST_LAN                  2005-11-19  16:37:50
USER ID:  TRAFADM
PROFILE NAME: TRAFADM
COMMAND CLASS AUTHORITIES:

 A=1 B=1 C=1 D=1 E=1    F=1 G=1 H=1 I=1 J=1
 K=1 L=1 M=1 N=1 O=1    P=1 Q=1 R=1 S=1 T=1
 U=1 V=1 W=1 X=1 Y=1

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: LIMITED
UNIQUE PROFILE: YES
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: WRITE
NETWORK USE ALLOWED: YES
```

Creación de objetos a ser supervisados en el sistema de administración de red

El objeto es creado en el Sistema de Administración de red. Con la creación, los parámetros necesarios para la administración del elemento de red serán almacenados en la Base de Datos del sistema.

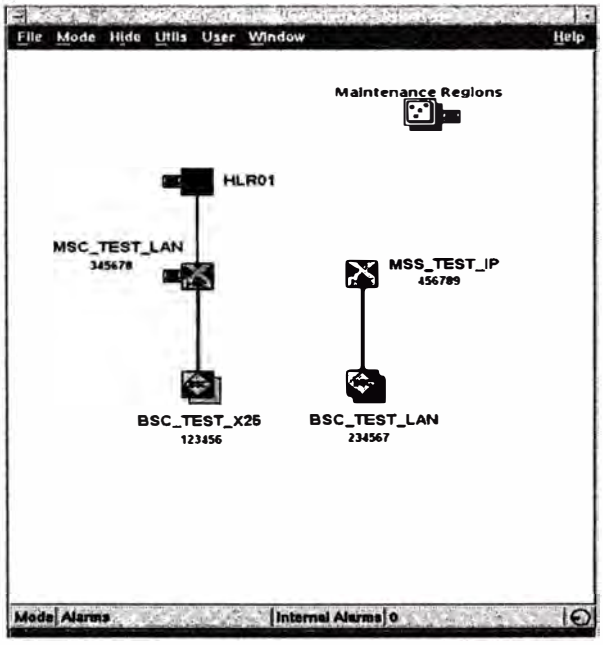


Figura 6.6: Creación de objetos en el sistema de administración de red

Configuración en el elemento de red

Configuración de la conexión física

Instalación y configuración de la tarjeta en el elemento de red

```
BDCU-0        IN LOC  1A005-08
  CP523_A  0  TRACK: 10
   MS:           ME:            IS:  0   IE: 3FF
   INT:          SW:
```

Creación y configuración del objeto CLNS

```
INTERROGATING CLNS
NODE IN ES ROLE
                 NS USER     NS USER     MAX PDU   SYSTEM
CLNS NAME  ROLE  PRIM UNIT   ACT UNIT    LIFETIME  ID              STATE
---------  ----  ---------  ------- -------  ------------  ----------
ESX         ES   BDCU-0     BDCU-0      9    000000345678      UNL-BU-ACT

MAX MAN AREA ADDR COUNT: 1
MANUAL AREA ADDRESS:     39604F00000000000000010001
```

Creación y configuración del objeto de enlace (linkage object)

```
INTERROGATING LINKAGE DATA

NODE IN ES ROLE

LINKAGE TYPE ROLE UNIT    LOG UNIT TERM SNPA ADDRESS     PVC  PRIO STATE
------- ---- ---- ------- -------- ---- --------------- ---- ---- -------
    0   BRO   ES  BDCU-0  4121H      0      -             -    -  UNL-ENA
```

Creación y configuración de las direcciones NSAPs local y remota

```
INTERROGATING NETWORK ADDRESS DATA

NET ADDR  ROLE    NSAP NR PRIO NSAP NR PRIO
--------  ------  ------- ---- ------- ----
LOCALNMS  LOCAL         1    -
REMNMS    REMOTE        5  100       6   75
```

Creación de las direcciones de red local y remota y la conexión de las direcciones NSAP a las direcciones de red

```
INTERROGATED NSAP DATA
LOCAL N-SELECTOR

NBR   ROLE    STATE  SEL
----- ------ ------- ---
    1 LOCAL  UNL-ENA 00

ISO DCC/ISO 6253-ICD NSAP

NBR   ROLE    STATE  AFI IDI  DFI ORG    RESERVED AREA END SYSTEM   SEL
----- ------ ------- --- ---- --- ------ -------- ---- ------------ ---
    5 REMOTE UNL-ENA 39  604F 00  000000 00000001 0001 170029004015 00
    6 REMOTE UNL-ENA 39  604F 00  000000 00000001 0001 170029004012 00
```

Configuración de las aplicaciones locales y remotas

```
LOCAL OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE   UNIT        FAM ID PROC ID
---------------- ------ -------- ------- ---------- ------- -------
MSC345678FO      VFS    LOCALNMS UNL-ENA  OMU
MSC345678VT      VTP    LOCALNMS UNL-ENA  OMU
MSC345678A       CMISE  LOCALNMS UNL-ENA  OMU          021FH   0000H
MSC345678EHA     CMISE  LOCALNMS UNL-ENA  OMU          02B1H   0000H

REMOTE OSI APPLICATION DATA

AE-NAME          APPL   NET ADDR  STATE
---------------- ------ -------- -------
OMC000000D1      CMISE  REMNMS   UNL-ENA
OMC000000BP      CMISE  REMNMS   UNL-ENA
OMC000000FP      VFS    REMNMS   UNL-ENA
OMC000000SW      VFS    REMNMS   UNL-ENA
```

Configuración del servicio y perfil CMISE

```
LOCAL OSI APPLICATION DATA

AE-NAME           APPL   NET ADDR  STATE   UNIT         FAM ID PROC ID
----------------- ------ -------- -------  ---------- ------- -------
MSC345678EHA      CMISE  LOCALNMS UNL-ENA  OMU           02B1H   0000H

AP_TYPE     : NOT IN USE
AP_TITLE    :
AEQ         :

P-SELECTOR: 3333040231
S-SELECTOR: 3333040231
T-SELECTOR: 3333
```

Configuración de la unidad básica de comunicación de datos (BDCU)

```
INTERROGATING NETWORK INTERFACE DATA
                                          ADDR                ADM    PRIO-
UNIT                NAME    IP ADDRESS    TYPE NML ASSIGNED STATE RISED
------------------- ------ --------------- ---- --- -------- ----- -----
BDCU-0              EL0     170.29.4.149     P     24 YES      UP    NO


INTERROGATED ROUTE DATA
                                    NEXT ADDR
UNIT              DESTINATION       HOP  TYPE ADDRESS                 NBR
--------------- ------------------ ---- ---- ---------------------- -----
BDCU-0            DEFAULT ROUTE     GW   IP   170.29.4.146             5
```

b) Utilizando IP

Tarjeta de red del elemento de red

```
OMU-0        IN LOC  1A004-00

  CP816_A  0  TRACK:  7
   MS:          ME:          IS:C000  IE:C3FF
   INT:         SW:
```

Tareas Preliminares

Elementos de red:

Hardware: MSS NOKIA

Versión de software: Software versión 13.0

Nombre del elemento de red: MSS_TEST_IP

Número C: 456789

CLNS:

Dirección de área: 39604F00000000000000010001

Identificador del sistema: 000000456789

Revisión de los requerimientos del sistema

Sistema de Administración de Red

SYSOP:

```
MSCi     MSS_TEST_IP                  2005-11-29  17:37:50
USER ID:  SYSOP
PROFILE NAME: SYSOP
COMMAND CLASS AUTHORITIES:

 A=250 B=250 C=250 D=250 E=250   F=250 G=250 H=250 I=250 J=250
 K=250 L=250 M=250 N=250 O=250   P=250 Q=250 R=250 S=250 T=250
 U=250 V=250 W=250 X=250 Y=250

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: COMPLETE
UNIQUE PROFILE: YES
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: NO
NETWORK USE ALLOWED: YES
```

TRAFADM:

```
MSCi     MSS_TEST_IP                  2005-11-29  17:37:50
USER ID:  TRAFADM
PROFILE NAME: TRAFADM
COMMAND CLASS AUTHORITIES:

 A=1 B=1 C=1 D=1 E=1   F=1 G=1 H=1 I=1 J=1
 K=1 L=1 M=1 N=1 O=1   P=1 Q=1 R=1 S=1 T=1
 U=1 V=1 W=1 X=1 Y=1

PARALLEL PASSWORD EXISTENCE: NO
PASSWORD VALIDITY TIME LEFT: PASSWORD NEVER EXPIRES
MML COMMAND LOG ACCESSIBILITY: LIMITED
UNIQUE PROFILE: YES
```

```
MML SESSION IDLE TIME LIMIT: 15 MIN(S)
FTP ACCESSIBILITY: WRITE
NETWORK USE ALLOWED: YES
```

Creación de objetos a ser supervisados en el sistema de administración de red

El objeto es creado en el Sistema de administración de red. Con la creación, los parámetros necesarios para la administración del elemento de red serán almacenados en la Base de Datos del sistema.

Configuración en el elemento de red

Configuración de los parámetros IP

```
INTERROGATING NETWORK INTERFACE DATA
                                          ADDR                ADM    PRIO-
UNIT                NAME   IP ADDRESS     TYPE NML ASSIGNED   STATE  RISED
------------------- ------ -------------- ---- --- -------- ------ -----
OMU-0               EL0    170.29.4.150    L     28 YES      UP     NO
                    EL1    170.29.4.150    L     28 NO       UP     NO
OMU-1               EL0    170.29.4.150    L     28 NO       UP     NO
                    EL1    170.29.4.150    L     28 NO       UP     NO

INTERROGATED ROUTE DATA
                                  NEXT ADDR
UNIT            DESTINATION       HOP  TYPE ADDRESS                 NBR
--------------- ----------------- ---- ---- --------------------- -----
OMU-0          DEFAULT ROUTE      GW   IP   170.29.4.147               1
OMU-1          DEFAULT ROUTE      GW   IP   170.29.4.147               2


INTERROGATED TCP/IP PARAMETER DATA
UNIT      IP FORW TTL SNL HOST NAME
--------- ------- --- --- ----------------------------------------------
---
OMU-0     NO      64  YES MSC_TEST_IP-OMU
OMU-1     NO      64  YES MSC_TEST_IP-OMU
```

CONCLUSIONES Y RECOMENDACIONES

Conclusión 1.

A continuación se muestran los resultados obtenidos al realizar una traza a nivel de CLNS en el router de la red de comunicación de datos al realizar una recarga de alarmas del elemento de red BSC_TEST_LAN desde el sistema de administración NOKIA NetAct OSS.

Eventos en el router rc_rtr1 al realizar la recarga de alarmas en el elemento de red:

```
rc_rtr1#debug clns packets
CLNS packets debugging is on
rc_rtr1#ter mon
Aug  1 23:14:15.812: CLNS: Forwarding packet size 87
Aug  1 23:14:15.812:       from 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:15.812:       to 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:15.812:       via REMOTE_SITE (Serial0/1:0 *HDLC*)
Aug  1 23:14:15.820: CLNS: Forwarding packet size 278
Aug  1 23:14:15.820:       from 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:15.820:       to 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:15.820:       via REMOTE_SITE (Serial0/1:0 *HDLC*)
Aug  1 23:14:15.828: CLNS: Forwarding packet size 87
Aug  1 23:14:15.828:       from 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:15.828:       to 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:15.828:       via REMOTE_SITE (Serial0/1:0 *HDLC*)
Aug  1 23:14:15.860: CLNS: Forwarding packet size 125
Aug  1 23:14:15.860:       from 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:15.860:       to 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:15.860:       via REMOTE_SITE (Serial0/1:0 *HDLC*)
Aug  1 23:14:15.860: CLNS: Forwarding packet size 125
```

```
Aug  1 23:14:15.860:       from 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:15.860:       to 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:15.860:       via REMOTE_SITE (Serial0/1:0 *HDLC*)
```

Eventos en el router rc_rtr1 al recibir las alarmas del elemento de red:

```
Aug  1 23:14:49.875: CLNS: Forwarding packet size 115
Aug  1 23:14:49.875:       from 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:49.875:       to 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:49.875:       via 1700.2900.4012 (FastEthernet0/0.2 0013.21bd.0de8)
Aug  1 23:14:49.875: CLNS: Forwarding packet size 115
Aug  1 23:14:49.875:       from 39.604f.0000.0000.0000.0001.0001.0000.0023.4567.00
Aug  1 23:14:49.875:       to 39.604f.0000.0000.0000.0001.0001.1700.2900.4015.00
Aug  1 23:14:49.875:       via 1700.2900.4012 (FastEthernet0/0.2 0013.21bd.0de8)
```

Eventos en el elemento de red BSC_TEST_LAN:

```
LOADING PROGRAM

BSC     BSC_TEST_LAN                  2006-08-01  23:14:57

INTERROGATING LINKAGE ADJACENCY INFORMATION

NODE IN ES ROLE

LINKAGE TYPE ROLE UNIT    LOG UNIT TERM SNPA ADDRESS     PVC  PRIO STATE
------- ---- ---- ------- -------- ---- ---------------- ---- ---- -------
    0   BRO   ES  OMU     4002H      0      -              -    -  UNL-ENA

ADJACENCY DATA

SYSTEM ID SET    SNPA ADDRESS STATE USAGE TIME PRIORITY TYPE  INFO
---------------- ------------ ----- ----- ---- -------- ----- ------
170026001129     000C3044E280 UP      -      0     -    IS    AUTO

AREA ADDRESS : -

SYSTEM ID SET    SNPA ADDRESS STATE USAGE TIME PRIORITY TYPE  INFO
---------------- ------------ ----- ----- ---- -------- ----- ------
000000234567     0000501F762F UP      -     -      -    ES    AUTO

AREA ADDRESS : -

COMMAND EXECUTED
```

Con lo anterior, se determinó que el CLNS envía independientemente paquetes de datos a su destino. Cada paquete contiene la dirección destino del sistema remoto. Una vez que el paquete es identificado, el servicio de enrutamiento selecciona la mejor ruta para entregar el paquete.

Por lo tanto, cada paquete es manejado y encaminado a su destino de manera individual. Esto da lugar a que los paquetes viajen sobre una variedad de trayectorias físicas a su destino final. Una vez que la información de dirección es encapsulada dentro del paquete, no se requiere una conexión dedicada entre sistemas finales.

El CLNS usa la capa de transporte OSI para establecer y terminar la conexión. Dentro del enfoque del CLNS, la capa de transporte también provee detección y corrección de errores.

Conclusión 2.

La tecnología de paquetes conmutados X.25, si bien es cierto es muy antígua, continua siendo utilizada por los operadores móviles en el proceso de transportar datos que se traducen en información de fallas, desempeño y configuración.

Tal es el caso del BSC (BSC_TEST_X25) que está integrado al sistema de administración de red usando éste protocolo.

LINKAGE	TYPE	ROLE	UNIT	LOG UNIT	TERM	SNPA ADDRESS	PVC	PRIO	STATE
1	X.25	ES	OMU	4002H	2	17002900400211	-	-	UNL-ENA

Conclusión 3.

El sistema de administración propuesto está orientado a gestionar en un futuro muy cercano, elementos de red de tercera generación, en los 3 aspectos que caracterizan a la administración de red: Administración de Fallas, administración de desempeño y administración de configuración.

El diseño para la factibilidad y hacer que el sistema sea abierto (bajos los estándares), hace que nuevas tecnologías y nuevos servicios puedan ser soportados de manera efectiva.

Recomendación 1.

Por la experiencia en el tema, se observa con mucha frecuencia problemas en la conectividad de red del operador, que provoca un serio retardo en el arrivo de alarmas y mediciones desde los elementos de red gestionados al sistema de administración de red.

Por lo que se recomienda monitorear y dar el correcto mantenimiento a los equipos de comunicaciones que se encuentran en el trayecto por donde pasan los datos (fallas, mediciones y comandos remotos) para tener una rápida respuesta en el caso que algún elemento en la red presente un problema crítico.

Recomendación 2.

Los respaldos (backups) de información base del sistema como el Sistema Operativo, base de datos, etc deben estar siempre disponibles en caso el sistema colapse.

Recomendación 3.

El correcto mantenimiento preventivo a los elementos de red, desde el sistema de administración es la mejor herramienta en conjunto que asegurará un alto desempeño de la red.

Recomendación 4.

La integración de los elementos de red utilizando LAN muestra una mayor flexibilidad en las configuraciones, por lo cual es recomendable el uso de la misma en la integración de los elementos de red. En el futuro, el uso de IP en las integraciones de los elementos de red, será el más utilizado ya que las tecnologías actuales están orientadas a IP.

ANEXO A

RED OSS: 170.29.4.0 MASCARA DE RED: 255.255.255.0

Nombre de VLAN	Número de VLAN	Número de hosts	Dirección de Red / Máscara	Direcciones IPs disponibles	Broadcast	Máscara de subred
NMS_cluster1	2	126	170.29.4.0/25	.1 - .126	170.29.4.127	255.255.255.128
NMS_Servicios	6	14	170.29.4.128/28	.129 - .142	170.29.4.143	255.255.255.240
NE 2G locales	8	6	170.29.4.144/29	.145 - .150	170.29.4.151	255.255.255.248
Red_Interna	11	6	170.29.4.152/29	.153 - .158	170.29.4.159	255.255.255.248
Red_Externa1	12	6	170.29.4.160/29	.161 - .166	170.29.4.167	255.255.255.248
Red_Externa2	13	6	170.29.4.168/29	.169 - .174	170.29.4.175	255.255.255.248
Acceso 3G	7	6	170.29.4.176/29	.177 - .182	170.29.4.183	255.255.255.248
Red_Operador	10	30	170.29.4.192/27	.193 - .222	170.29.4.223	255.255.255.224
Red_Externa3	14	6	170.29.4.248/29	.249 - 254	170.29.4.255	255.255.255.248

VLAN 2 - NMS_CLUSTER1	
170.29.4.1	rc_rtr
170.29.4.2	rc_rtr1
170.29.4.3	rc_rtr2
170.29.4.4	
170.29.4.5	rc_sw1
170.29.4.6	rc_sw2
170.29.4.7	rc_sw3
170.29.4.8	
170.29.4.9	
170.29.4.10	
170.29.4.11	rc_scs
170.29.4.12	rc_dbs
170.29.4.13	ossPkg1
170.29.4.14	dbpkg
170.29.4.15	syspkg
170.29.4.16	
170.29.4.17	
170.29.4.18	
170.29.4.19	
170.29.4.20	
170.29.4.21	rc_was1
170.29.4.22	rc_was2
170.29.4.23	
170.29.4.24	
170.29.4.25	
170.29.4.26	
170.29.4.27	
170.29.4.28	svr_bck
170.29.4.29	svr_bck_console
170.29.4.30	
170.29.4.31	
170.29.4.32	
170.29.4.33	
170.29.4.34	
170.29.4.35	
170.29.4.36	
170.29.4.37	rc_was1console
170.29.4.38	rc_was2console
170.29.4.39	rc_scsconsole
170.29.4.40	rc_dbsconsole
170.29.4.41	
170.29.4.42	
170.29.4.43	
170.29.4.44	
170.29.4.45	
170.29.4.46	
170.29.4.47	
170.29.4.48	
170.29.4.49	
170.29.4.50	
170.29.4.51	
170.29.4.52	
170.29.4.53	
170.29.4.54	
170.29.4.55	
o	
o	
o	
o	
o	
o	
170.29.4.126	

VLAN 6 - NMS_SERVICIOS	
170.29.4.129	rc_rtr
170.29.4.130	rc_rtr1
170.29.4.131	rc_rtr2
170.29.4.132	spa
170.29.4.133	spb
170.29.4.134	fb_sw1console
170.29.4.135	fb_sw2console
170.29.4.136	spaconsole
170.29.4.137	spbconsole
170.29.4.138	fb_sw1
170.29.4.139	fb_sw2
170.29.4.140	
170.29.4.141	
170.29.4.142	

VLAN 8 - NE_2G_LOCALES	
170.29.4.145	rc_rtr
170.29.4.146	rc_rtr1
170.29.4.147	rc_rtr2
170.29.4.148	
170.29.4.149	
170.29.4.150	

VLAN 10 - RED_OPERADOR	
170.29.4.193	rc_rtr
170.29.4.194	rc_rtr1
170.29.4.195	rc_rtr2
170.29.4.196	
170.29.4.197	
170.29.4.198	
170.29.4.199	
170.29.4.200	rc_client
170.29.4.201	
170.29.4.202	
170.29.4.203	
170.29.4.204	
170.29.4.205	
170.29.4.206	
170.29.4.207	
170.29.4.208	
170.29.4.209	
170.29.4.210	
170.29.4.211	
170.29.4.212	
170.29.4.213	
170.29.4.214	
170.29.4.215	
170.29.4.216	
170.29.4.217	
170.29.4.218	
170.29.4.219	
170.29.4.220	
170.29.4.221	
170.29.4.222	

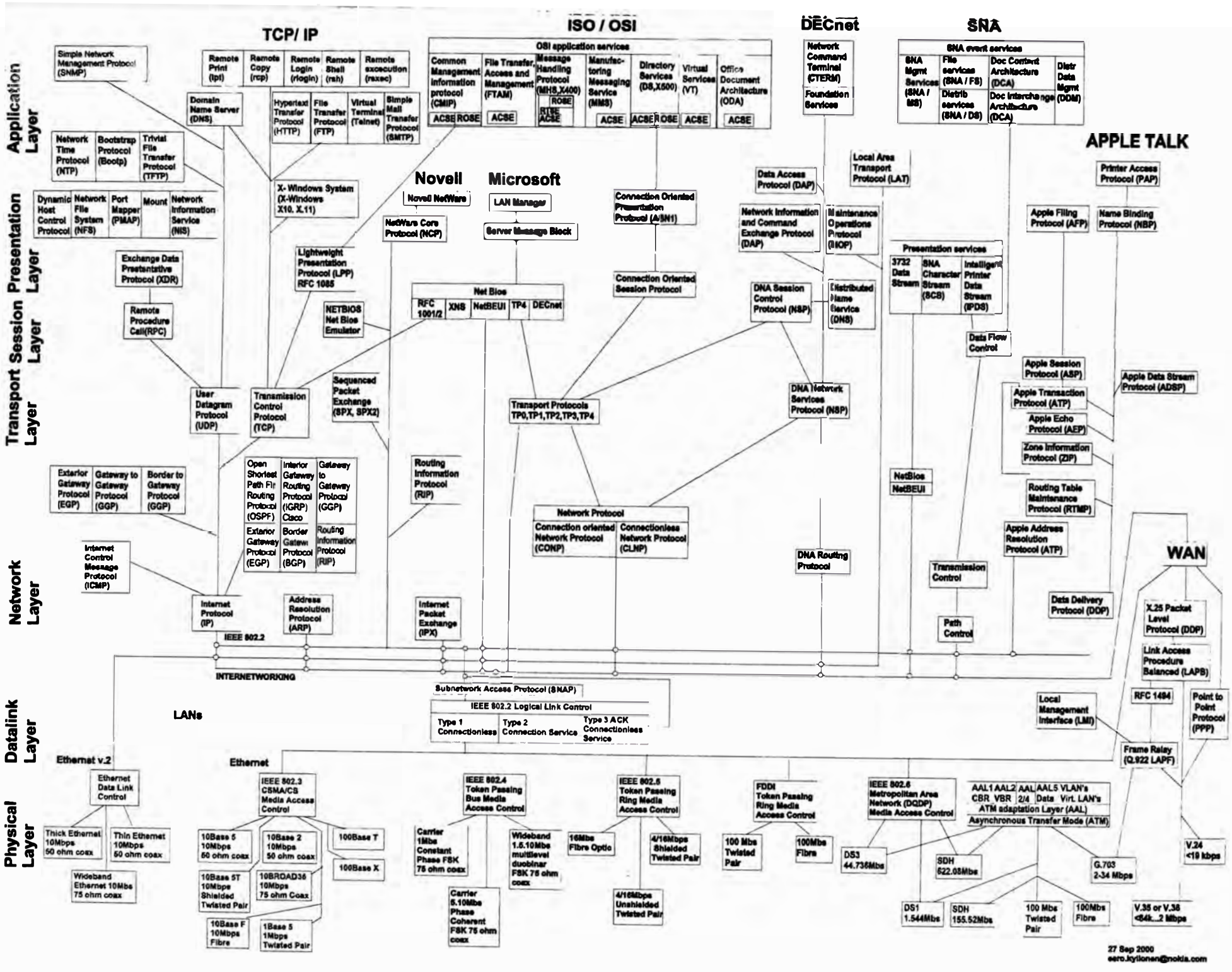
VLAN 11 - RED_INTERNA	
170.29.4.153	rc_rtr
170.29.4.154	rc_rtr1
170.29.4.155	rc_rtr2
170.29.4.156	
170.29.4.157	svr_adm_cisco
170.29.4.158	

VLAN 12 - RED_EXTERNA1	
170.29.4.161	rc_rtr
170.29.4.162	rc_rtr1
170.29.4.163	rc_rtr2
170.29.4.164	
170.29.4.165	
170.29.4.166	

VLAN 13 - RED_ EXTERNA2 (heartbeat)	
170.29.4.169	
170.29.4.170	
170.29.4.171	
170.29.4.172	rcscs_hb
170.29.4.173	rcdbs_hb
170.29.4.174	

VLAN 14 - RED_EXTERNA3	
170.29.4.249	Nokia_OSS_HSRP
170.29.4.250	Nokia_OSS_rtr1
170.29.4.251	Nokia_OSS_rtr2
170.29.4.252	Firewall_Operador
170.29.4.253	Firewall_Operador
170.29.4.254	Firewall_Operador

PLANEAMIENTO DE LAS DIRECCIONES IP


TCP/ IP
ISO / OSI
DECnet
SNA
APPLE TALK
Novell
Microsoft
WAN
LANs
INTERNETWORKING
Application Layer
Presentation Layer
Transport Session Layer
Network Layer
Datalink Layer
Physical Layer
Simple Network Management Protocol (SNMP)
Remote Print (lpt)
Remote Copy (rcp)
Remote Login (rlogin)
Remote Shell (rsh)
Remote execution (rexec)
Domain Name Server (DNS)
Hypertext Transfer Protocol (HTTP)
File Transfer Protocol (FTP)
Virtual Terminal (Telnet)
Simple Mail Transfer Protocol (SMTP)
Network Time Protocol (NTP)
Bootstrap Protocol (Bootp)
Trivial File Transfer Protocol (TFTP)
Dynamic Host Control Protocol
Network File System (NFS)
Port Mapper (PMAP)
Mount
Network Information Service (NIS)
Exchange Data Presentative Protocol (XDR)
Remote Procedure Call(RPC)
X- Windows System (X-Windows X10. X.11)
Lightweight Presentation Protocol (LPP) RFC 1085
NETBIOS Net Bios Emulator
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
Sequenced Packet Exchange (SPX, SPX2)
Exterior Gateway Protocol (EGP)
Gateway to Gateway Protocol (GGP)
Border to Gateway Protocol (GGP)
Open Shortest Path Flr Routing Protocol (OSPF)
Interior Gateway Routing Protocol (IGRP) Cisco
Gateway to Gateway Protocol (GGP)
Exterior Gateway Protocol (EGP)
Border Gatew Protocol (BGP)
Routing Information Protocol (RIP)
Internet Control Message Protocol (ICMP)
Internet Protocol (IP)
Address Resolution Protocol (ARP)
IEEE 802.2
OSI application services
Common Management information protocol (CMIP)
File Transfer, Access and Management (FTAM)
Message Handling Protocol (MHS,X400)
Manufac-turing Messaging Service (MMS)
Directory Services (DS,X500)
Virtual Services (VT)
Office Document Architecture (ODA)
ACSE
ROSE
RTSE
Novell NetWare
NetWare Core Protocol (NCP)
LAN Manager
Server Message Block
Net Bios
RFC 1001/2
XNS
NetBEUI
TP4
DECnet
Routing Information Protocol (RIP)
Transport Protocols TP0,TP1,TP2,TP3,TP4
Network Protocol
Connection oriented Network Protocol (CONP)
Connectionless Network Protocol (CLNP)
Connection Oriented Presentation Protocol (AISN1)
Connection Oriented Session Protocol
Internet Packet Exchange (IPX)
Network Command Terminal (CTERM)
Foundation Services
Data Access Protocol (DAP)
Network Information and Command Exchange Protocol (DAP)
Maintenance Operations Protocol (MOP)
DNA Session Control Protocol (NSP)
Distributed Name Service (DNS)
DNA Network Services Protocol (NSP)
DNA Routing Protocol
SNA event services
SNA Mgmt Services (SNA / MS)
File services (SNA / FS)
Doc Content Architecture (DCA)
Distrib services (SNA / DS)
Doc Interchange Architecture (DCA)
Distr Data Mgmt (DDM)
Local Area Transport Protocol (LAT)
Presentation services
3732 Data Stream
SNA Character Stream (SCS)
Intelligent Printer Data Stream (IPDS)
Data Flow Control
NetBios
NetBEUI
Transmission Control
Path Control
Printer Access Protocol (PAP)
Apple Filing Protocol (AFP)
Name Binding Protocol (NBP)
Apple Session Protocol (ASP)
Apple Data Stream Protocol (ADSP)
Apple Transaction Protocol (ATP)
Apple Echo Protocol (AEP)
Zone Information Protocol (ZIP)
Routing Table Maintenance Protocol (RTMP)
Apple Address Resolution Protocol (ATP)
Data Delivery Protocol (DDP)
X.25 Packet Level Protocol (DDP)
Link Access Procedure Balanced (LAPB)
RFC 1484
Point to Point Protocol (PPP)
Frame Relay (Q.922 LAPF)
Local Management Interface (LMI)
Subnetwork Access Protocol (SNAP)
IEEE 802.2 Logical Link Control
Type 1 Connectionless
Type 2 Connection Service
Type 3 ACK Connectionless Service
Ethernet v.2
Ethernet Data Link Control
Thick Ethernet 10Mbps 50 ohm coax
Thin Ethernet 10Mbps 50 ohm coax
Wideband Ethernet 10Mbs 75 ohm coax
Ethernet
IEEE 802.3 CSMA/CS Media Access Control
10Base 5 10Mbps 50 ohm coax
10Base 2 10Mbps 50 ohm coax
100Base T
100Base X
10Base 5T 10Mbps Shielded Twisted Pair
10BROAD36 10Mbps 75 ohm Coax
10Base F 10Mbps Fibre
1Base 5 1Mbps Twisted Pair
IEEE 802.4 Token Passing Bus Media Access Control
Carrier 1Mbs Constant Phase FSK 75 ohm coax
Carrier 5.10Mbs Phase Coherent FSK 75 ohm coax
Wideband 1.5.10Mbs multilevel duobinar FSK 75 ohm coax
IEEE 802.5 Token Passing Ring Media Access Control
16Mbs Fibre Optic
4/16Mbps Shielded Twisted Pair
4/16Mbps Unshielded Twisted Pair
FDDI Token Passing Ring Media Access Control
100 Mbs Twisted Pair
100Mbs Fibre
IEEE 802.6 Metropolitan Area Network (DQDP) Media Access Control
AAL1 AAL2 CBR VBR
AAL 2/4
AAL5 VLAN's Data Virt. LAN's
ATM adaptation Layer (AAL)
Asynchronous Transfer Mode (ATM)
DS3 44.736Mbs
SDH 622.08Mbs
G.703 2-34 Mbps
V.24 <19 kbps
DS1 1.544Mbs
SDH 155.52Mbs
100 Mbs Twisted Pair
100Mbs Fibre
V.35 or V.36 <64k...2 Mbps
27 Sep 2000
eero.kyllonen@nokia.com

ANEXO B

GLOSARIO

2G: Segunda Generación
3G: Tercera Generación
3GPP (3G Partnership Project): Asociación del Proyecto de 3G
A2SU (AAL type 2 Switching Unit): Unidad de Conmutación AAL tipo 2
ABR (Area Border Router): Router de Borde de Área
AC (Autenthication Centre): Centro de Autenticación
ACSE (Association Control Service Element): Elemento del Servicio de Control de Asociación
ACU (Authentication Centre Unit): Unidad del Centro de Autenticación
AE (Application Entity): Entidad de Aplicación
AEQ (Application Entity Qualifier): Calificador de Entidad de Aplicación
AET (Application Entity Title): Título de Entidad de Aplicación
AFI (Authority and Format Identifier): Identificador de la Autoridad y del Formato
ANSI (American Nacional Standards Institute): Instituto Americano de Estándares Nacionales
APT (Application Process Title): Título de Proceso de Aplicación
ARP (Address Resolution Protocol): Protocolo de Resolución de Dirección
AS (Autonomous System): Sistema Autónomo
ASBR (Autonomous System Boundary Router): Router de Frontera del Sistema Autónomo
ASE (Application Service Element): Elemento del Servicio de Aplicación
ATM (Asynchronous Transfer Mode): Modo de Transferencia Asíncrona
AuC (Authentication Centre): Centro de Autenticación
AXC (ATM Cross-Connection): Conexión Cruzada ATM
BC (Billing Centre): Centro de Facturación
BCCH (Broadcast Control CHannel): Canal de Control de Broadcast
BCSU (Base Station Controller Signalling Unit): Unidad de Señalización del Controlador de Estación Base
BDCU (Basic Data Communication Unit): Unidad Básica de Comunicación de Datos
BG (Border Gateway): Gateway de Borde
BGP (Border Gateway Protocol): Protocolo EGP que domina internet
BICC (Bearer Independent Call Control): Control de Llamada Independiente del Bearer
BS (Base Station): Estación Base
BSC (Base Satation Controller): Controlador de Estación Base

BSS (Base Station Subsystem): Subsistema de Estación Base

BSSAP (Base Station Subsystem Application Part): Parte de Aplicación del Subsistema de Estación Base

BSU (Base Station Signalling Unit): Unidad de Señalización de la Estación Base

BTS (Base Transceiver Station): Transceptor de la Estación Base

BTSM (BTS Management): Administración de BTS

C-Number: Número de entrega de los equipos NOKIA entre 0 y 999999

CAMEL (Customised Applications for Mobile Network Enhanced Logic): Aplicaciones Personalizadas para la Lógica Mejorada de la Red Móvil

CAP (CAMEL Application Part): Parte de Aplicación CAMEL

CAS (Channel Associated Signalling): Señalización de Canal Asociado

CASU (Channel Associated Signalling Unit): Unidad de Señalización de Canal Asociado

CC (Country Code): Código de País

CCCH (Common Control CHannel): Canal de Control Común

CCITT (Consultative Committee for International Telegraphy and Telephony): Comité Consultivo Internacional Telegráfico y Telefónico

CCMU (Common Channel Signalling Management Unit): Unidad de Administración de Señalización de Canal Común

CCS (Common Channel Signalling): Señalización de Canal Común

CCSU (Common Channel Signalling Unit): Unidad de Señalización de Canal Común

CDR (Charging Data Record): Registro de Datos de Charging

CDSU (Compact Data Service Unit): Unidad de Servicio Compacto de Datos

CEIR (Central Equipment Identity Register): Registro Central de Identidad del Equipo

CG (Charging Gateway): Gateway de Facturación

CHU (CHarging Unit): Unidad de Charging

CLNP (ConnectionLess Network Protocol): Protocolo de Red no Orientado a Conexión

CLNS (ConnectionLess Network Service): Servicio de Red no Orientado a Conexión

CLS (Clock and Synchronisation Unit): Unidad de Reloj y Sincronización

CM (Configuration Management): Administración de Configuración

CM (Central Memory): Memoria Central

CMIP (Common Management Information Protocol): Protocolo de Información de Administración Común

CMISE (Common Management Information Service Element): Elemento del Servicio de Información de Administración Común

CMM (Central Memory and Marker): Marcador y Memoria Central

CMU (Cellular Management Unit): Unidad de Administración Celular

COCEN (Communication Controller for Ethernet): Controlador de comunicación para Ethernet

CONS (Connection Oriented Network Service): Servicio de Red Orientado a Conexión

CORBA (Common Object Request Broker Architecture): Estándar general y abierto para el trabajo con objetos distribuidos

COTS (Connection-Oriented Transport Layer Service): Servicio OSI de Capa de Transporte Orientado a Conexión

CPU (Central Processing Unit): Unidad Central de Procesamiento

CRC (Cyclic Redundancy Check): Verificación de Redundancia Cíclica

CRP (Central Routing Processor): Procesador Central de Enrutamiento

CS – MGW (Circuit Switched – MGW): Gateway Multimedia – Circuitos Conmutados

CT (Cellular Transmission): Transmisión Celular

CxM (Connection Management): Administración de Conexión

DBDU (DataBase Distributor Unit): Unidad Distribuidora de Base de Datos

DCC (Data Country Code): Código de Datos NSAP del País

DCE (Data Communication Equipment): Equipo de Comunicación de Datos

DCN (Data Communication Network): Red de Comunicación de Datos

DES (Data Encryption Standard): Estándar de Encriptación de Datos

DFN (Database Failover Node): Nodo Failover de la Base de Datos

DNS (Domain Name System): Sistema de Nombres de Dominio

DPNSS1 (Digital Private Network Signalling System number 1): Sistema Digital de Señalización de Red Privada número 1

DRAM (Dynamic RAM): Memoria de Acceso Alatorio Dinámico

DS (Database Server): Servidor de Base de Datos

DSP (Domain – Specific Part): Parte Específica de Dominio

DSP (Digital Signal Processor): Procesador Digital de Señales

DTE (Data Terminal Equipment): Equipo Terminal de Datos. El identificador del DTE es utilizado como la dirección X.121 del elemento de red

DTX (Discontinuous Transmission): Transmisión Discontinua

E-DSS1 (European – Digital Subscriber Signalling System number 1): Sistema Europeo de Señalización Digital de Abonado número 1

EDGE (Enhanced Data rates GSM Evolution): Tasa de Datos Mejorada para la Evolución GSM

EGP (Exterior Gateway Protocol): Protocolo de Acceso Exterior

EHU (External Hardware Alarm Unit): Unidad de Alarmas Externas de Hardware

EIR (Equipment Identity Register): Registro de Identidad del Equipo Móvil

EMU (Equipment Main Unit): Unidad Principal del Equipo
ES (End System): Sistema Final
ET (Exchange Terminal): Terminal de Intercambio
ETSI (European Telecommunications Standards Institute): Instituto Europeo de Estándares de Telecomunicaciones
FDMA (Frequency Division Multiple Access): Acceso Múltiple por División de Frecuencias
FEC (Fast Ethernet Channel): Canal Fast Ethernet
FM (Fault Management): Administración de Fallas
FTAM (File Transfer, Access and Management): Administración, Acceso y Transferencia de archivos
FTP (File Transfer Protocol): Protocolo de Transferencia de Archivos
FU (Forwarding Unit): Unidad de Desviación
GC (Global Cluster): Cluster Global
GCS (Gateway Control Server): Servidor de Control Gateway
GERAN (GSM EDGE Radio Access Network): Red de Acceso de Radio GSM EDGE
GGSN (Gateway GPRS Support Node): Nodo de Soporte de Gateway GPRS
GMM (GPRS Mobility Management): Administración de Movilidad GPRS
GMSC (Gateway MSC): Gateway de la Central de Conmutación de Servicios Móviles
GMSCS (GMSC – Server): Servidor GMSC
GMSK (Gaussian Minimum Shift Keying): Desplazamiento de Frecuencia Mínima Gausiana
GNS (GPRS Name Server): Servidor de Nombres de GPRS
GPRS (General Packet Radio Service): Servicio General de Paquetes por Radio
GPS (Global Positioning System): Sistema de Posicionamiento Global
GRE (Generic Routing Encapsulation): Encapsulación de Enrutamiento Genérico
GSM (Global System for Mobile Communications): Sistema Global para Comunicaciones Móviles
GSWB o GSW (Group Switch): Switch de Grupo
GTP (GPRS Tunnelling Protocol): Protocolo de Túnel de GPRS
HDLC (High-Level Data Link Control): Protocolo de Control de Enlace de Datos de Alto Nivel
HLR (Home Location Register): Registro de Ubicación Local
HLRU (Home Location Register Unit): Unidad del Registro de Ubicación Local
HON (HandOver Number): Número de Handover
HP-UX: Sistema Operativo Unix de Hewlett Packard

HSCSD (High Speed Circuit Switched Data): Circuito Conmutado de Datos de Alta Velocidad

HSRP (Hot Standby Router Protocol): Protocolo que crea un grupo de routers en standby. Es un protocolo propietario de Cisco

HTTP (HyperText Transfer Protocol): Protocolo de Transferencia de HiperTexto

ICD (International Code Designator): Entidad que designa el Código Internacional

ICMP (Internet Control Message Protocol): Protocolo de Control de Mensajes de Internet

IDI (Initial Domain Identifier): Identificador Inicial de Dominio

IDP (Initial Domain Part): Parte Inicial de Dominio

IEEE (Institute of Electrical and Electronics Engineers): Instituto de Ingenieros Eléctricos y Electrónicos

IGP (Interior Gateway Protocol): Protocolo de Acceso Interior

IGRP (Interior Gateway Routing Protocol): Protocolo IGP diseñado por Cisco para enrutamiento en un sistema autónomo

IMA (Inversing Multiplexing ATM): Multiplexación Inversa ATM

IMEI (International Mobile Equipment Identity): Identidad Internacional Móvil del Equipo

IMS (IP Multimedia Subsystem): Subsistema Multimedia IP

IMSI (International Mobile Subscriber Identity): Identidad Internacional Móvil del Abonado

IOR (Interoperable Object Reference): Objeto de Referencia Interoperable

IOS (Internetwork Operating system): Software que ejecuta los procesos de enrutamiento y conmutación en los routers y switches respectivamente

IP (Internet Protocol): Protocolo de Internet

IPET (IP Exchange Terminal): Terminal de Intercambio IP

IPNIU (IP Network Interface Unit): Unidad de Interfase de Red IP

IPSec (IP Security): Protocolo de Seguridad de Internet

IRP (Integration Reference Point): Punto Referencia de Integración

ISDN (Integrated Services Digital Network): Red Digital de Servicios Integrados

IS (Intermediate System): Sistema Intermedio

IS-IS (Intermediate system to Intermediate System): Protocolo EGP usado para enrutamiento no orientado a conexión

ISO (International Organization for Standardization): Organización Internacional para la Estandarización

ISP (Internet Service Provider): Proveedor de Servicio de Internet

ISUP (ISDN User Part): Parte de Usuario ISDN

ITU (International Telecommunication Union): Unión Internacional de Telecomunicaciones

L2TP (Layer 2 Tunnelling Protocol): Protocolo de Túnel de Capa 2

LA (Location Area): Área de Ubicación
LAC (Location Area Code): Código de Área de Ubicación
LAI (Location Area Identity): Identidad de Área de Ubicación
LAPB (Link Access Procedure on the B-channel): Procedimiento de Acceso al Enlace en el canal B
LAPD (Link Access Procedure on the D-channel): Procedimiento de Acceso al Enlace en el canal D
LAPDm (Link Access Procedure on the D-channel, modified): LAPD modificado
LDAP (Lightweight Directory Access Protocol): Protocolo de Acceso a Directorios Livianos
LSA (Link Status Advertisement): Mensajes de Estado de Enlace o Conexión
MAP (Mobile Application Part): Parte de Aplicación Móvil
MB (Message Bus): Bus de Mensajes de alta velocidad
MCC (Mobile Country Code): Código Móvil de País
MCHU (Marker and Charging Unit): Marcador y Unidad de Charging
MCMU (Marker and Cellular Management Unit): Marcador y Unidad de Administración Celular
MFSU (MultiFrequency Signalling Unit): Unidad de Señalización Multifrecuencia
MGW (Multimedia Gateway): Gateway Multimedia
MM (Mobility Management): Administración de Movilidad
MML (Man-Machine Language): Lenguaje Hombre – Máquina
MNC (Móbile Network Code): Código Móvil de Red
MOC (Móbile Originated Call): Llamada Originada en el Móvil
MS (Mobile Station): Estación Móvil
MSC (Mobile Services Switching Centre): Central de Conmutación de Servicios Móviles
MSIN (Mobile Subscriber Identification Number): Número de Identificación Móvil del Abonado
MSISDN (Mobile Subscriber International ISDN): Número ISDN Internacional Móvil del Abonado
MSRN (Mobile Station Roaming Number): Número Roaming de la Estación Móvil
MSS (MSC – Server): Servidor MSC
MTC (Mobile Terminated Call): Llamada Terminada en el Móvil
MTP (Message Transfer Part): Parte de Transferencia de Mensajes
MXU (Multiplexer Unit): Unidad Multiplexadora
NDC (National Destination Code): Código Nacional de Destino
NE (Network Element): Elemento de Red

NEMU (Network Element Management Unit): Unidad de Administración del Elemento de Red

NetAct: Producto de NOKIA para Administración de Red

NFS (Network File System): Sistema de Archivos de Red

NIS (Network Information Service): Servicio de Información de Red

NIWU (Network InterWorking Unit): Unidad de Intercambio de Red

NMS (Network Management Subsystem): Subsistema de Administración de Red

NPAI (Network Protocol Address Information): Información de Dirección del Protocolo de Red

NSAP (Network Service Access Point): Punto de Acceso del Servicio de Red

NSS (Network Switching Subsystem): Subsistema de Conmutación de Red

NTP (Network Time Protocol): Protocolo utilizado para proporcionar un tiempo de referencia

NUP (National User Part): Parte de Usuario Nacional

NVRAM (Non-Volatile Random Access Memory): Memoria RAM no Volátil

O&M (Operation and Maintenance): Operación y Mantenimiento

OMC (Operation and Maintenance Centre): Centro de Operación y Mantenimiento

OMU (Operation and Maintenance Unit): Unidad de Operación y Mantenimiento

OSI (Open Systems Interconnection): Interconexión de Sistemas Abiertos

OSPF (Open Shortest Path First): Protocolo de ruteo IP dentro de un sistema autónomo, estandarizado en RFC 1247

OSS (Operation and Support Subsystem): Subsistema de Soporte y Operación

OTS (OSI Transport Services): Servicios de Transporte OSI

P-TMSI (Packet - TMSI): TMSI de Paquetes

PaCo (Packet Core): Red de Paquetes

PAU (PBX Access Unit): Unidad de Acceso a la PBX

PCM (Pulse Code Modulation): Modulación por Codificación de Pulsos

PCU (Packet Control Unit): Unidad de Control de Paquete

PDH (Plesiochronous Digital Hierarchy): Jerarquía Digital Plesiócrona

PDP (Packet Data Protocol): Protocolo de Paquete de Datos

PDU (Protocol Data Unit): Unidad de Datos de Protocolo

PKI (Public Key Infraestructure): Infraestructura de Clave Pública

PLMN (Public Land Mobile Network): Red Móvil Pública Terrestre

PM (Performance Management): Administración de Desempeño

PPP (Point to Point Protocol): Protocolo Punto a Punto

PRA (Primaty Rate Access): Acceso Primario

PSAP (Presentation Service Access Point): Punto de Acceso al Servicio de Presentación
PSN (Packet Switched Network): Red de Paquetes Conmutados
PSTN (Public Switched Telephone Network): Red Conmutada de Telefonía Pública
Q3: Conjunto de definiciones estándar OSI para la transferencia de información de administración
QoS (Quality of Service): Calidad de Servicio
RA (Routing Area): Área de Enrutamiento
RAM (Random Access Memory): Memoria de Acceso Alatorio
RAN (Radio Access Network): Red de Acceso de Radio
RANAP (Radio Access Network Application Part): Parte de Aplicación de la Red de Acceso de Radio
RC (Regional Cluster): Cluster Regional
RFC (Request for Comments): Documento formal escrito por miembros de la IETF
RIP (Routing Information Protocol): Protocolo de ruteo estándar documentado en RFC 1058
RNC (Radio Network Controller): Controlador de la Red de Radio
ROSE (Remote Operation Service Element): Elemento del Servicio de Operación Remota
RPC (Remote Procedure Call): Llamada de Procedimiento Remoto
RR (Radio Resource): Recurso de Radio
RRM (Radio Resource Management): Administración del Recurso de Radio
RTP (Real-Time Transport Protocol): Protocolo de Transporte en Tiempo Real
SAN (Storage Area Network): Red de Área de Almacenamiento
SCCP (Signalling Connection and Control Part): Parte de Control y Conexión de Señalización
SCP (Service Control Point): Punto de Control del Servicio
SCS (System Component Server): Servidor Componente del Sistema
SDCCH (Stand-alone Dedicated Control Channel): Canal de Control Dedicado
SDH (Synchronous Digital Hierarchy): Jerarquía Digital Síncrona
SDS (System and Databse Server): Servidor de Sistema y Base de Datos
SFU (Switch Fabric Unit): Unidad Fabric de Conmutación
SGSN (Serving GPRS Support Node): Nodo de Soporte de Servicio GPRS
SGW (Signalling Gateway): Gateway de Señalización
SHA-1 (Secure Hash Algorithm 1): Algoritmo de Hash Seguro número 1
SIGTRAN (SIGnalling TRANsmission): Transmisión de Señalización
SIM (Subscriber Identity Module): Módulo de Identidad del Abonado
SM (Session Management): Administración de Sesión

SMMU (Signalling and Mobility Management Unit): Unidad de Administración de Movilidad y Señalización
SMS (Short Message Service): Servicio de Mensajes Cortos
SN (Subscriber Number): Número de Abonado
SNMP (Simple Network Management Protocol): Protocolo de Administración de Red Simple
SP (Signalling Point): Punto de Señalización
SRR (Service Routing Register): Registro del Servicio de Encaminamiento
SS (System Server): Servidor de Sistema
SS7 (Signalling System number 7): Sistema de Señalización número 7
SS7U (SS7 Unit): Unidad SS7
SSH (Secure Shell): Protocolo de Shell Seguro
SSP (Service Switching Point): Punto del Servicio de Conmutación
STP (Signalling Transfer Point): Punto de Transferencia de Señalización
STU (Statistical Unit): Unidad de Estadísticas
SWU (Switch Unit): Unidad de Conmutación LAN
TBU (Timing and Hardware Management Bus Unit): Unidad de Bus de Administración de Sincronización y Hardware
TC o TRAU (Transcoder and Rate Adaptation Unit): Unidad Transcoder y Adaptadora de Velocidad
TCAP (Transaction Capabilities Application Part): Parte de Aplicación de Capacidades de Transacción
TCH (Traffic Channel): Canal de Tráfico
TCP (Transmission Control Protocol): Protocolo de Control de Transmisión
TCSM (Transcoder Submultiplexer): Submultiplexor Transcoder
TCU (Transcoding Unit): Unidad de Transcodificación
TCU (Distributed Signal Processing Unit): Unidad de Procesamiento Distribuido de Señal
TDMA (Time Division Multiple Access): Acceso Múltiple por División de Tiempo
TGFP (Tone Generator Field Programmable): Campo Programable Generador de Tonos
TGSU (Trunk Gateway Signalling Unit): Unidad de señalización Trunk Gateway
TLLI (Temporary Logical Link Identity): Identidad Temporal de Enlace Lógico
TLS (Transport Layer Service): Servicio de Capa de Transporte
TLUI (Top-Level User Interface): Interfase de Usuario de Alto Nivel
TMSI (Temporary Mobile Subscriber Identity): Identidad Temporal Móvil del Abonado
TPP (Transport Pipe Provider): Proveedor de Transporte
TRCO (TRanscoder COntroller): Controlador de Transcoder

TRX (Transceiver): Transceptor (Receptor / Transmisor)
TSL (Time SLot): Intervalo de tiempo
TT (Toll Ticket): Expresión "Boleto de Peaje"
TU (Tunneling Unit): Unidad de Tunneling
TUP (Telephone User Part): Parte de Usuario de Telefonía
TZ (Time zone): Zona Horaria
UAS (Unix Application Server): Servidor de Aplicación Unix
UDP (User Datagram Protocol): Protocolo de Datagrama de Usuario
UMA (Unified Mediation and Adaptation): Capa de Mediación y Adaptación Unificada
UMTS (Universal Mobile Telecommunications System): Sistema Universal de Telecomunicaciones Móviles
UTRAN (Universal Terrestrial Radio Access Network): Red de Acceso Universal Radioeléctrico Terrestre
VANG (Voice Announcement Generador): Generador de Voz para Anuncios
VANU (Voice Announcement Unit): Unidad de Anuncio de Voz
VLAN (Virtual Local Area Network): Red de Area Local Virtual
VLR (Visitor Location Register): Registro de Ubicación Vistante
VLRU (Visitor Location Register Unit): Unidad del Registro de Ubicación Visitante
VLSM (Variable Length Subnet Mask): Máscara de Subred de Longitud Variable
VPN (Virtual Private Network): Red Privada virtual
VRRP (Virtual Router Redundancy Protocol): Protocolo de Redundancia de Router Virtual
VT (Virtual Terminal): Terminal Virtual
WAN (Wide Area Network): Red de Área Amplia
WAP (Wireless Application Protocol): Protocolo de Aplicación Inalámbrica
WAS (Windows Application Server): Servidor de Aplicación Windows
WCDMA (Wideband Code Division Multiple Access): Acceso Múltiple por División de Códigos de Banda Ancha
X.121: Plan de numeración internacional para redes públicas de datos
XML (eXtensible Markup Language): Lenguaje Extensible

BIBLIOGRAFÍA

1. Timo Halonen, "GSM, GPRS and EDGE Performance – Evolution towards 3G/UMTS", England - 2003
2. Nokia Learning - Center Network, "Gprssys Systra Training Handbook", Finland – 2004.
3. Nokia Learning - Center Network, "OSS DCN Overview Training Handbook", Finland – 2005.
4. Nokia Corporation, "Integrating 2G/3G Circuit Switched Core NEs to NMS", Finland – 2005
5. Nokia Corporation, "Integrating 2G BSS to NMS", Finland – 2005.
6. Cisco System, "Interconnecting Cisco Network Devices version 2.3" (Vol 1 y 2), USA – 2006.