UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

"ANÁLISIS DE LA SEÑALIZACIÓN EN REDES SS7 APLICANDO EL ACCESS7"

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

NAPOLEÓN TURPO MAMANI

PROMOCIÓN 1997-I

LIMA – PERÚ
2003

Un agradecimiento especial a mi familia por su apoyo en todo momento.

ANÁLISIS DE LA SEÑALIZACIÓN EN REDES SS7 APLICANDO EL ACCESS7

SUMARIO

En los sistemas de telefonía Fija o Móvil se presentan a menudo problemas de señalización N°7 debido a una mala configuración de estos sistemas como pueden ser:

- Mal dimensionamiento de la Rutas, conjunto de E1s entre Centrales Telefónicas, que pueden generar congestión.
- Mala configuración en el Análisis de Dígitos, análisis de lo que digita un abonado, para el enrutamiento de una llamada que puede generar llamadas no terminadas.

A parte de los problemas en los sistemas de telefonía se suelen realizar pruebas de interconexión entre estas para un correcto funcionamiento de las mismas, a través de la Señalización N°7.

Todos estos casos pueden ser solucionados por Sistemas de Monitoreo de Señalización tales como el Acces7. El Acces7 se detallara en el presente informe.

ÍNDICE

PROLOGO

El negocio de la telefonía está cambiando rápidamente en todo el mundo. Las demandas han hecho de nosotros un gestor de la red por los nuevos servicios, las regulaciones cambiantes, y en un mercado más competitivo donde nosotros debemos encontrar las nuevas maneras para manejar la red y tratar con cualquier problema que surja. Hacer las cosas de la misma manera no es el camino.

Un Sistema de Supervisión es lo adecuado para ayudarnos a manejar la red en tiempo real. Estos Sistemas aprovechan la riqueza de datos de la red de Señalización N° 7 para decirnos donde están los lugares de potencial problema y qué problemas presentan nuestros clientes (distintos operadores de Larga Distancia, rural, fijo y celular) antes de que ellos nos lo digan.

¿Por qué supervisar la red de Señalización N° 7?

Los datos derivados de la Red de Señalización N° 7 proporcıonan la única información sobre toda la actividad que tiene lugar en la red. En una red moderna de telecomunicaciones, unos cuantos miles de enlaces de señalización N° 7 controlan cientos de miles de circuitos de tráfico. Monitoreando los enlaces de Señalización nos da acceso inmediato a un rico conjunto de información en la actividad y funcionamiento de la red. Los beneficios resultantes son sustanciales e impactan cada área de la empresa.

En el mercado los productos mas representativos son:

- Sistema de Monitoreo Access7 de Agilent (HP).

- Sistema de Monitoreo Quest7 de GN Nettest

- Sistema de Monitoreo GeoProbe de INET

En este informe se ahondara en información sobre el Sistema AcceSS7 de Agilent ya que cuento con experiencia en el uso de este sistema, mas no dejaremos de comparar sus facilidades con los otros Sistemas existentes. Además el Sistema AcceSS7 esta en la planta de Telefonía Básica de Telefónica y el Sistema GeoProbe esta en la planta de Móviles de Telefónica.

CAPITULO I
RED DE SEÑALIZACIÓN N° 7

En esta sección describiremos la arquitectura de las redes SS7 (Signaling System N° 7 o Sistema de Señalización N° 7) para entender el propósito de los sistemas de monitoreo.

1.1 Señalización por canal común

La señalización por Canal Común o CCS Common Channel Signaling consiste en mensajes en lugar de parecer un arreglo de bits. Así puede transportar mensajes de señalización asociados a un número arbitrario de canales de voz.

Cuando usamos CCS, la voz y los datos de señalización pueden aun ser transportados en el mismo portador y en diferente timeslot. Pero, cuando es necesario, la información de la señalización puede seguir una ruta diferente al de la voz. Los canales de voz son luego portados en un circuito, y los datos de la señalización son portados en otro circuito dedicado (Fig. 1.1).

La CCS tiene las siguientes ventajas:

- El establecimiento y la terminación de una llamada son más rápidos.

- Menos propenso al fraude

- Mejor uso de la capacidad de la red de voz.

- Permite llevar a cabo Servicios de Red Inteligente, donde los circuitos de la señalización necesitan ser independientes de los circuitos de voz.

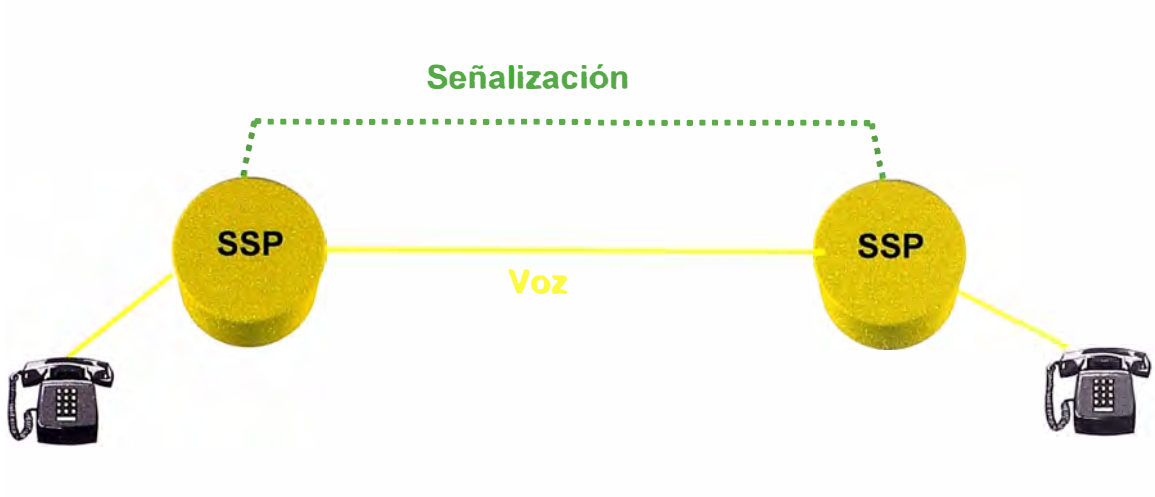


Fig. 1.1 Señalización por Canal Común

1.2 Modos de Señalización

1.2.1 Señalización Asociada

Este es el modo más simple donde el enlace esta directamente en paralelo con las facilidades de voz. Este es usado donde sea mejor conectar dos SSP's (Service Switching Point o Punto de Conmutación de Servicio). Todo mensaje asociado a la conexión de circuitos es enviado a través de este enlace.

1.2.2 Señalización no Asociada

Este moso usa una ruta lógica separada del canal de voz, usando nodos múltiples para alcanzar el destino final. Esto involucra el uso de STP's (Signaling Transfer Point o Punto de Transferencia de Señalización) para alcanzar el intercambio remoto. Usualmente la voz puede ser una ruta directa al destino. Esto no es muy favorable desde que cada nodo introduce un retardo adicional en la entrega del mensaje.

1.2.3 Señalización Cuasi-asociada

Esta usa un numero mínimo de nodos para alcanzar el destino final. Este es el método más favorable de señalización porque, tiene el cuidado en las desventajas de la Señalización Asociada y la Señalización no Asociada.

En general, las redes de señalización pueden usar una combinación de estos métodos, según el tamaño y las condiciones de funcionamiento (Fig. 1.2).

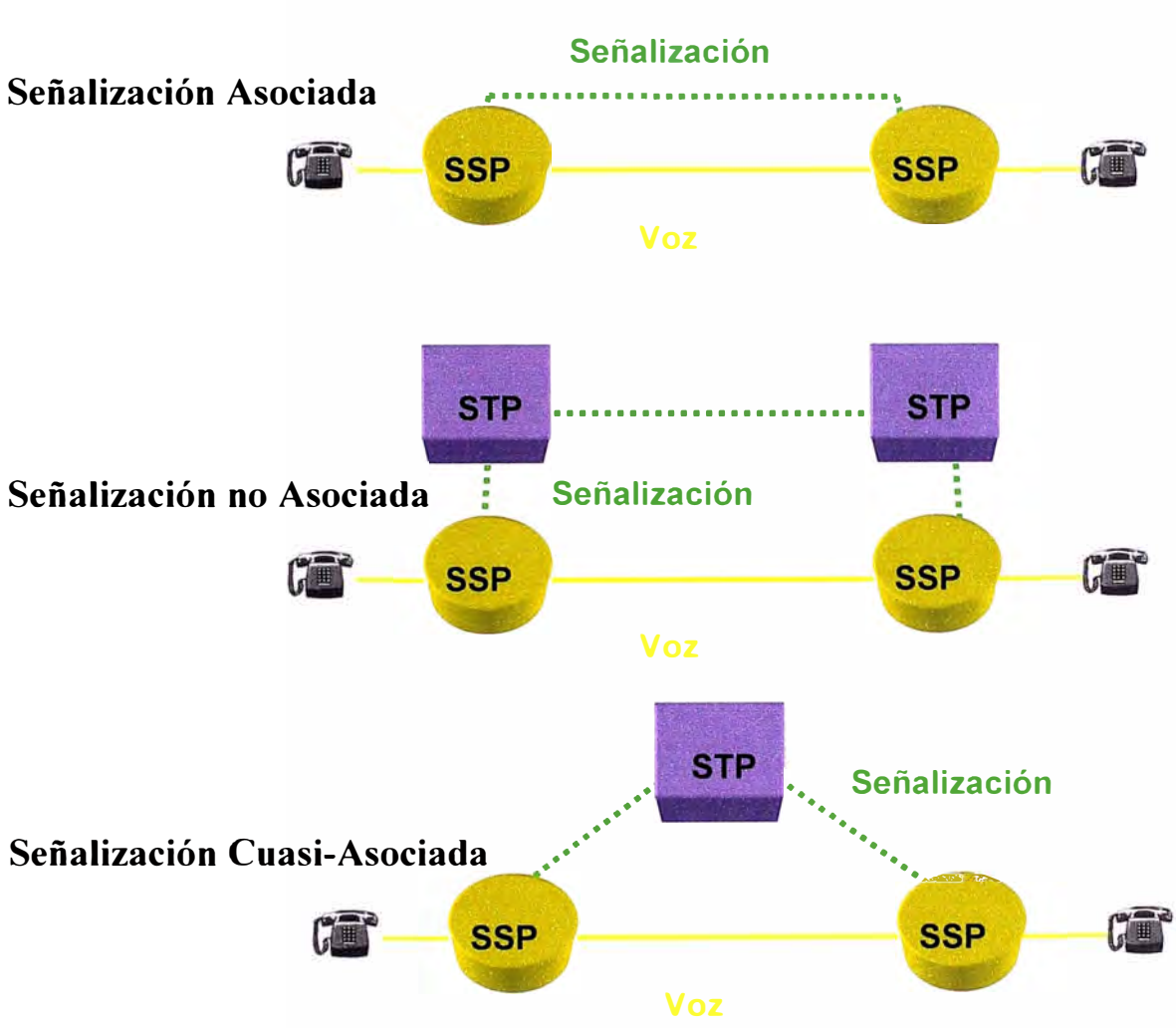


Fig. 1.2 Modos de Señalización

1.3 Configuración de las Redes de Señalización N° 7

Una Red SS7 consiste de procesadores distribuidos los cuáles, en combinación, controlan la Red de Telecomunicaciones. Abajo se muestra un segmento simplificado de una Red SS7 (Fig. 1.3).

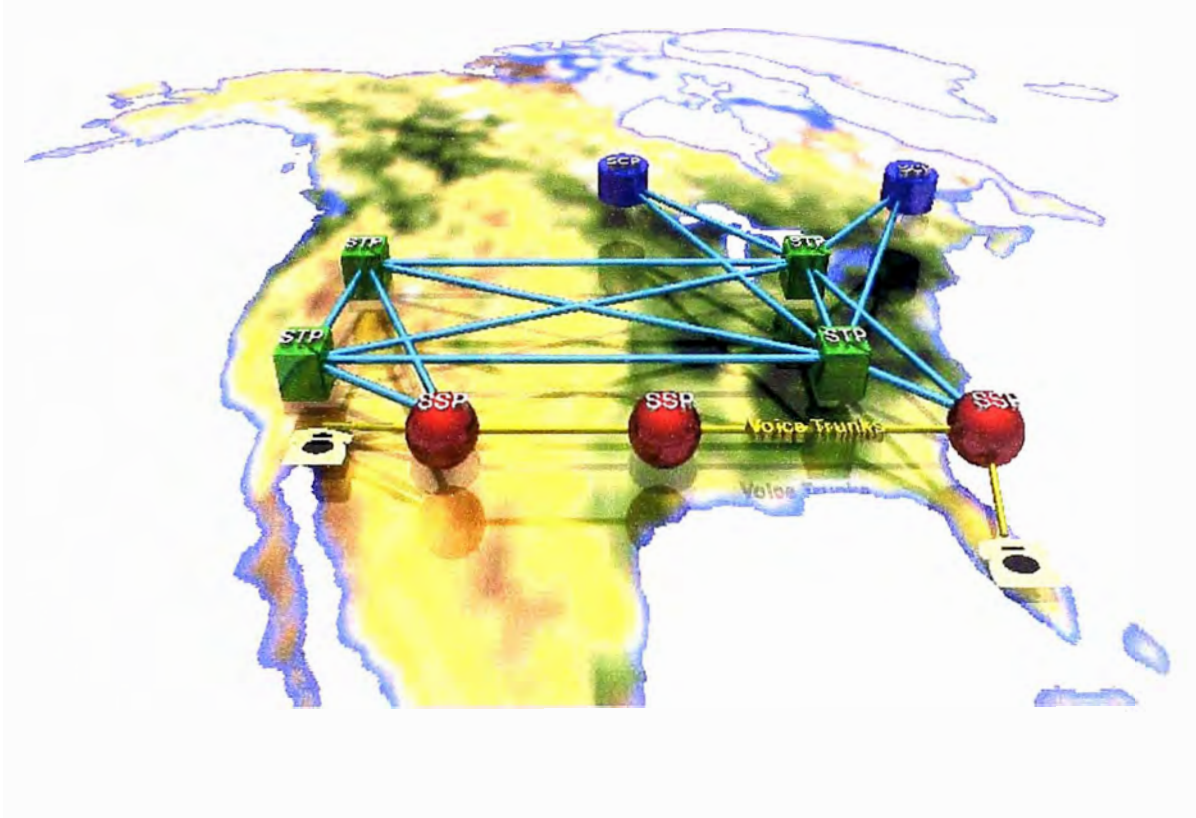


Fig. 1.3 Red SS7

1.3.1 Puntos de Señalización.

Cada Punto de Señalización o Signaling Point (SP) en la Red SS7 está unívocamente identificado por su Point Code (Código de Punto). Los mensajes de señalización llevan códigos de puntos para identificar la fuente y el destino de los mensajes.

Una Red SS7 típicamente consiste de tres tipos principales de SP:

- Punto de Conmutación de Servicio o Service Switching Points (SSPs)
- Puntos de transferencia de Señalización o Signaling Transfer Points (STPs)
- Puntos de Control de Servicio o Service Control Points (SCPs)

1.3.1.1 Puntos de Conmutación de Servicio.

SSPs son centrales tandem ó terminales que tienen capacidad de SS7. Constituyen el origen de los requerimientos de servicios y envían mensajes a la Red de Señalización para establecer las llamadas ó características de acceso de servicio requeridas por un abonado. Las SSPs tienen capacidad TCAP (Transaction Capabilities Application Part)

1.3.1.2 Puntos de Transferencia de Señalización

STPs son centrales grandes de paquetes SS7 y realizan la función de enrutamiento de mensajes dentro de la Red SS7. La central se basa en direcciones MTP (Message Transfer Part) y SCCP (Signaling Connection Control Part) y no conoce nada de las llamadas telefónicas.

En una topología típica en Norte América, ilustrada arriba, cada SSP está conectado a un par de STPs apareados los cuales están conectados a otro par de STPs apareados. La redundancia de esta configuración permite la falla de cualquiera de los STP.

1.3.1.3 Puntos de Control de Servicio

SCPs son sistemas de computación de propósito general que actúan como bases de datos para la Red SS7 al proveer un diálogo de interrogación / respuesta para ciertos servicios. Por ejemplo, una interrogación 800 de un SSP al SCP para trasladar un número 800 a un número telefónico real.

1.3.2 Tipos de enlaces

Las conexiones entre los Signaling Points son llamadas Links (Enlaces) Existen varios tipos de Enlaces, identificados de la 'A ' a la 'F'. Físicamente, todos los Enlaces son lo mismo el nombre del Enlace solo indica su función.

1.3.2.1 Enlaces Tipo 'A'

Los Access Links (Enlaces de Acceso) conectan centrales terminales y o tandems de acceso y SCPs a las STPs. En los EE.UU. se instalan al menos dos Enlaces desde cada SP a su par de STPs apareados, para mayor confiabilidad (Fig. 1.4).

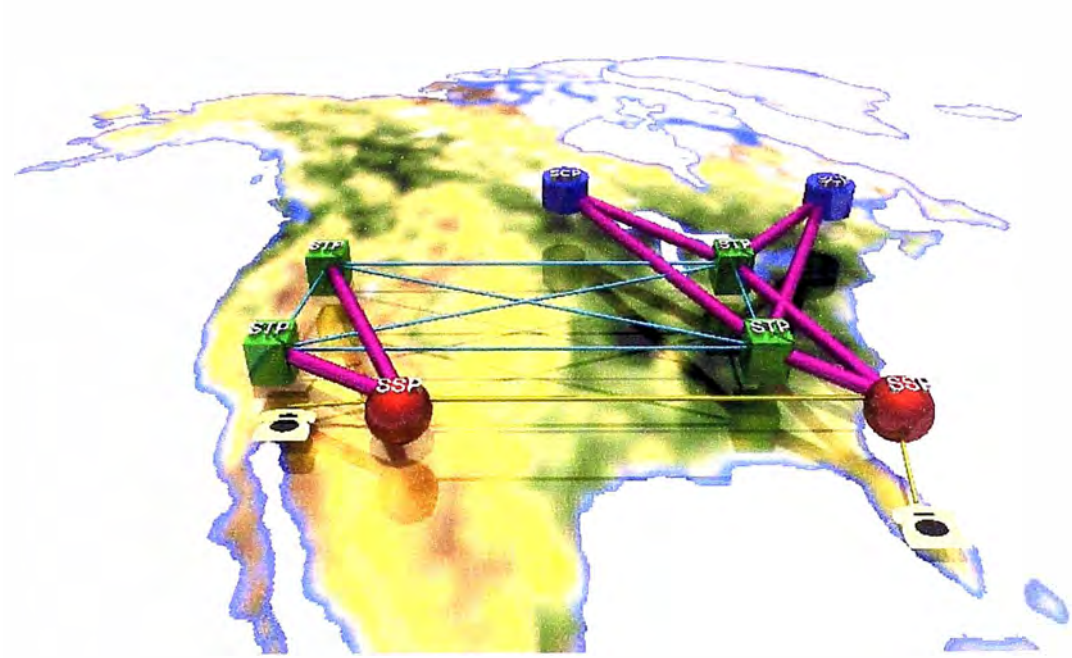


Fig. 1.4 Enlace A

1.3.2.2 Enlaces Tipo 'B'

Bridge Links (Enlaces Puente) conectan pares de STPs apareados en el mismo nivel jerárquico en un arreglo en cuadratura, por ejemplo STPs locales a otros STPs locales, ó STPs regionales a STPs regionales (Fig. 1.5).

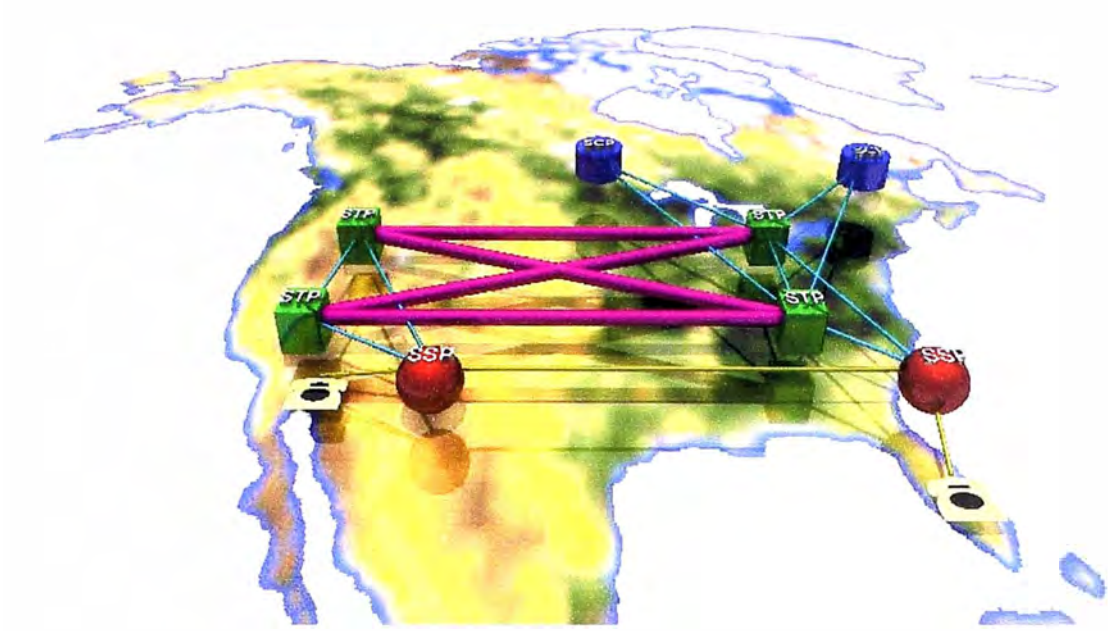


Fig. 1.5 Enlace B

1.3.2.3 Enlaces Tipo 'C'

Los Cross Links (Enlaces Cruzados) conectan pares de STPs apareados. La principal función de un Enlace 'C' es la de pasar mensajes de manejo de la Red entre los STPs apareados. Sí es necesario, por ejemplo, en el caso de fallas, los Enlaces 'C' también pueden ser usados para llevar Señalización (Fig. 1.6)

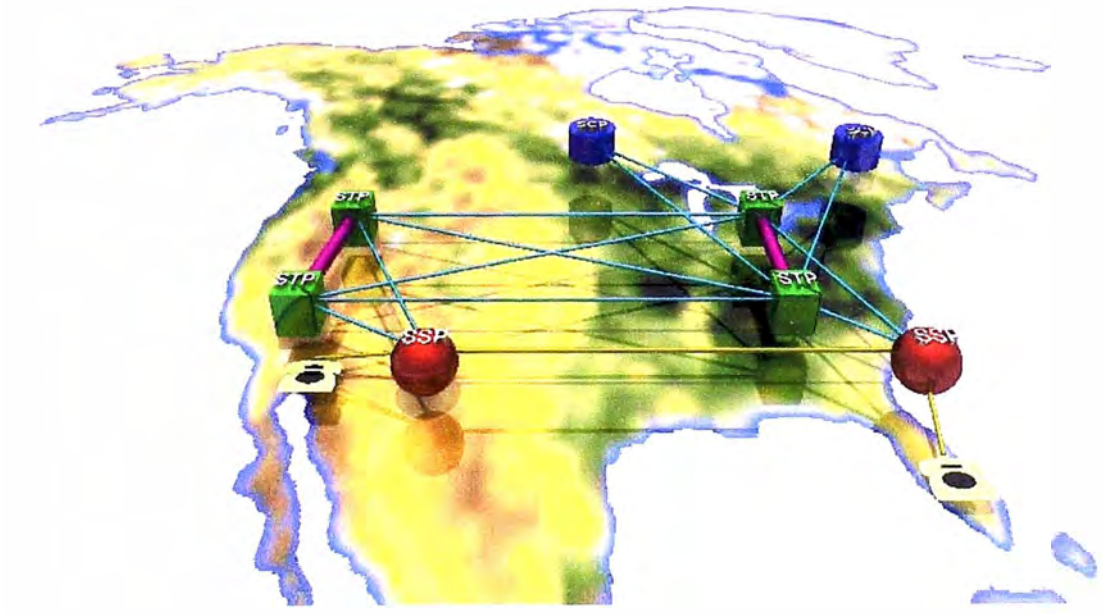


Fig. 1.6 Enlace C

1.3.2.4 Enlaces Tipo 'D'

Los Diagonal Links (Enlaces en Diagonal) son en esencia los mismos Enlaces 'B', excepto que conectan pares de STPs apareados en diferentes niveles jerárquicos, por ejemplo entre STPs regionales y STPs locales (Fig. 1.7).

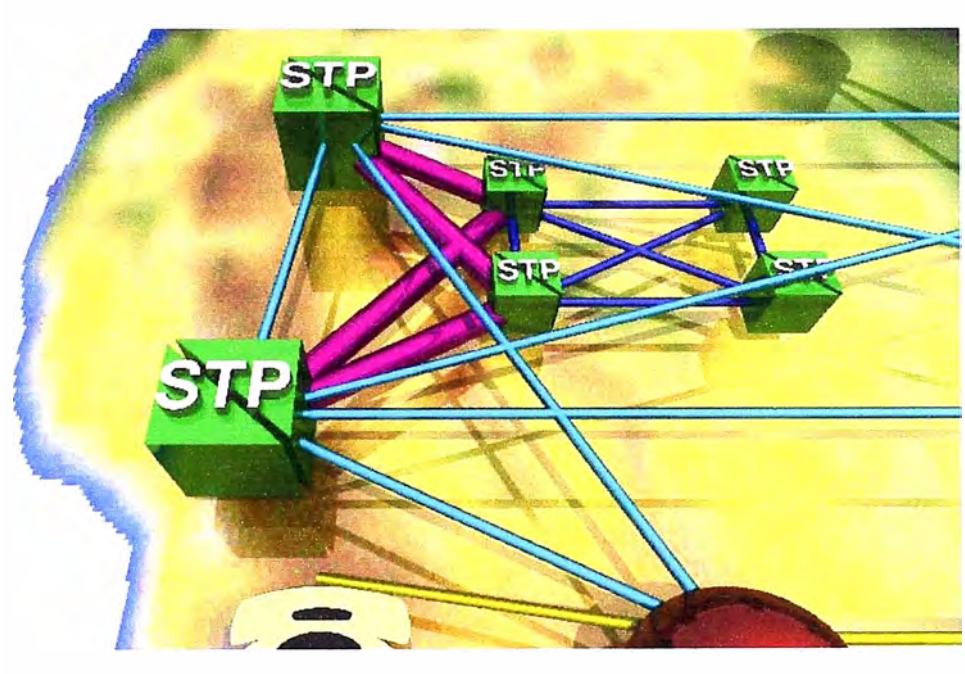


Fig. 1.7 Enlace D

1.3.2.5 Enlaces Tipo 'E'

Los Extended Links (Enlaces Extendidos) conectan SPs a otros STPs diferentes al par de STPs apareados al cuál los SPs están conectados originalmente (Fig. 1.8).

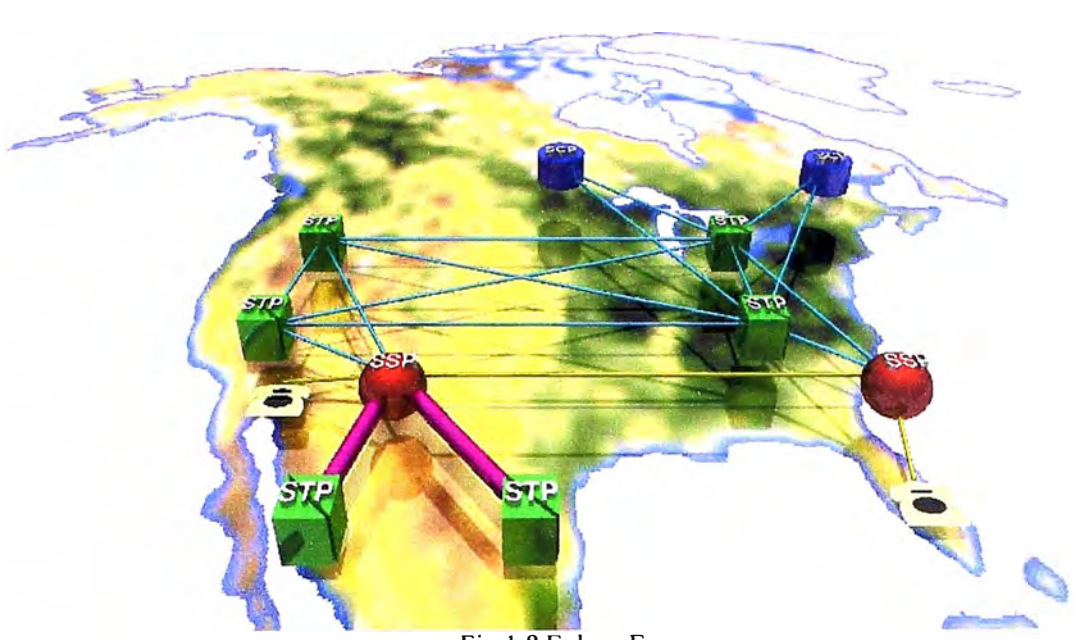


Fig 1.8 Enlace E

1.3.2.6 Enlaces Tipo 'F'

Los Enlaces que conectan SPs sin el uso de un STP se conocen como Fully Associated (Completamente Asociados) Fig. 1.9 .

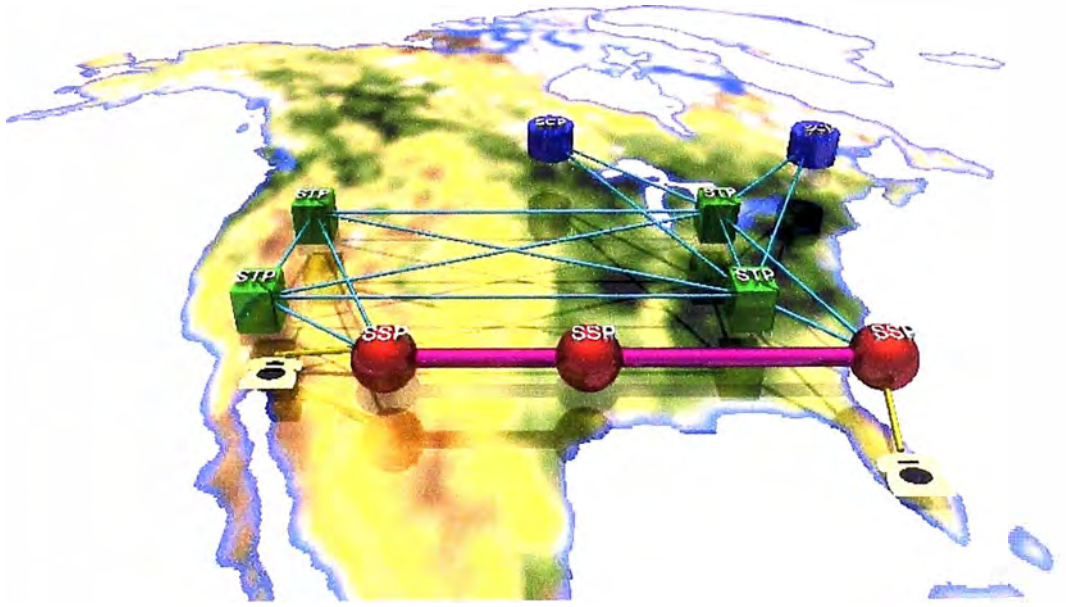


Fig. 1.9 Enlace F

1.3.3 Enlaces y Grupos de enlaces

Los Signaling Points están interconectados por enlaces o Links.

•Cada Link consiste de 2 Canales, uno para cada dirección del flujo de datos.

•Grupos de Links entre un par de Signaling Points se conocen como 'Linksets'.

•Los mensajes SS7 son compartidos igualmente a través de los Links en un Linkset (Fig. 1.10).

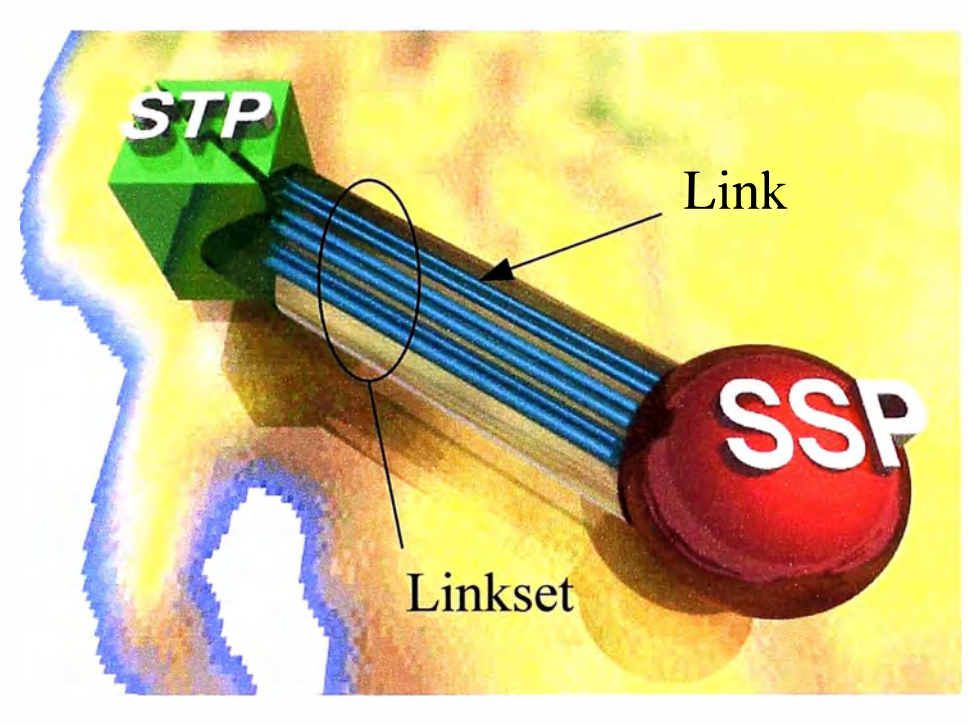


Fig. 1.10 Link & Linkset

La velocidad de transmisión del flujo de datos es normalmente de 56 ó 64 Kbps.

La información es compartida uniformemente a través de los Enlaces en un Linkset. Si un Enlace falla, la carga es transferida a los restantes Enlaces dentro de ese Linkset.

1.4 Estándar del Protocolo de Señalización N° 7

Algunas variantes mayores y menores de la familia del protocolo SS7 son definidas alrededor del mundo. La diferencia mayor esta entre Norte América variaciones (ANSI American National Standards Institute) y el resto del Mundo (ITU-T International Telecommunication Union--Telecommunication Standardization Sector) . Las variaciones ocurren en cada nivel del protocolo.

RECOMENDACIONES ITU-T

Recomendaciones más importantes que convencionalmente describen las normas internacionales:

- MTP	Q.701-704, 706, 707
-TUP	Q.721, 725
-Supp.Serv.	Q.730
-ISUP	Q.711-764, 766, 767
-Data User Part	Q.741
-SCCP	Q.711-714, 716
-TCAP	Q.771-775

1.5 Capas del Protocolo ISO-OSI

En 1977, ISO (International Standards Organization) decidió trabajar en una norma para la interconectividad de sistemas de computo. En 1980, esto condujo al modelo (OSI Open Systems Interconection) ahora una norma de sistema abierto.

El modelo de OSI consiste en siete niveles (Fig. 1.11). Cada nivel ofrece el servicio a un nivel superior y da el servicio a una nivel debajo. Cada nivel del

protocolo es independiente de otro, esto es cualquier nivel puede modificarse sin afectar otro nivel.

1.5.1 El nivel de aplicación:

Proporciona los servicios a la aplicación de los usuarios como los Funcionamientos y Mantenimiento.

1.5.2 El nivel de presentación:

Presenta los datos en la sintaxis usada para la comunicación, que es los cambios de los datos de la sintaxis del usuario a la sintaxis del sistema.

1.5.3 El nivel de sesión:

Controla la sincronización, conexión y desconexión de diálogos entre los niveles de la presentación diferentes.

1.5.4 El nivel de Transporte:

Actúa como una interfaz de transporte para los niveles superiores. Las funciones como la corrección y detección del error y control de flujo se llevan a cabo. También se llevan a cabo las funciones de multiplexado y bifurcación.

1.5.5 El nivel de red:

Establece, mantiene y libera las conexiones entre las entidades de la red y también realiza la asignación de ruta y direccionamiento.

1.5.6 El nivel de enlace:

Envía los mensajes en la secuencia correcta, sin errores ni duplicaciones. También realiza corrección y detección del error y retransmisión de los datos.

1.5.7 El nivel físico:

Proporciona funciones mecánicas, eléctricas para transmitir y recibir bits. Esto convierte los datos en señal.

Fig. 1.11 Modelo OSI

1.6 Arquitectura de la Señalización N° 7

A las capas de SS7 se les llaman "niveles". SS7 precede al modelo OSI, tan así que no se iguala completamente, pero el modelo OSI todavía puede usarse como una trama para clasificar las funciones de SS7 (Fig. 1.12).

1.6.1 Parte de Transferencia de Mensajes o MTP Message Transfer Part

Se usa para enrutar los mensajes alrededor de la red y soporta todas las partes del usuario. MTP constituye las tres capas mas bajas del protocolo:

1.6.1.1 MTP Nivel 1: (Físico)

Fija los niveles de voltaje, los conectores, etc. a través del enlace, se ocupa de datos simplemente como un flujo de bits y no puede descubrir los errores.

1.6.1.2 MTP Nivel 2: (Enlace)

Proporciona instrucción, traslado fiable de datos por un enlace (de su nodo al otro nodo): el control de flujo, la secuencia de mensajes, la comprobación del error.

1.6.1.3 MTP Nivel 3: (Red)

Conoce la existencia de todos los nodos en la red y puede enrutar por la red a través del direccionamiento. Selecciona el enlace apropiado a la ruta al nodo del destino luego proporciona el mensaje a nivel 2 de ese enlace para la transferencia.

1.6.2 Parte de Control de la Conexión de Señalización o SCCP:

El CCITT reconoció que había una deficiencia en las capacidades de direccionamiento de MTP, e introdujo SCCP (Signaling Connection Control Part) para remediarlo. SCCP se localiza a capa 3/4 (la Red / el Transporte) . Proporciona la no-conexión y conexión para transportar data y pueden manejar los nodos y subsistemas de direccionamiento gracias a la interpretación del tratamiento global.

TCAP (Transaction Capability Application Part) y **SCCP** (Signaling Connection and Control Parts) soporta los servicios sin voz (por ejemplo, servicio de base de datos 800 o usuario específico GSM).

1.6.3 Parte de Usuario de la RDSI

Soporta los servicios POTS (Plain Old Telephone Service) e ISDN (Integrated Services Digital Network) para establecer y terminar llamadas. Se usa para asignar y liberar las troncales de voz. En algunos países (Brasil, China), los POTS son a menudo soportados por su propia parte llamada especializada **TUP** (Telephone User Part) .

1.6.4 Mantenimiento

Transporta los mensajes de mantenimiento usados internamente en la red SS7.

1.6.5 Gestión de la Red de Señalización

La Gestión de la Red de Señalización o SNM (Signaling Network Management) transporta mensajes usados para la gestion de la red.

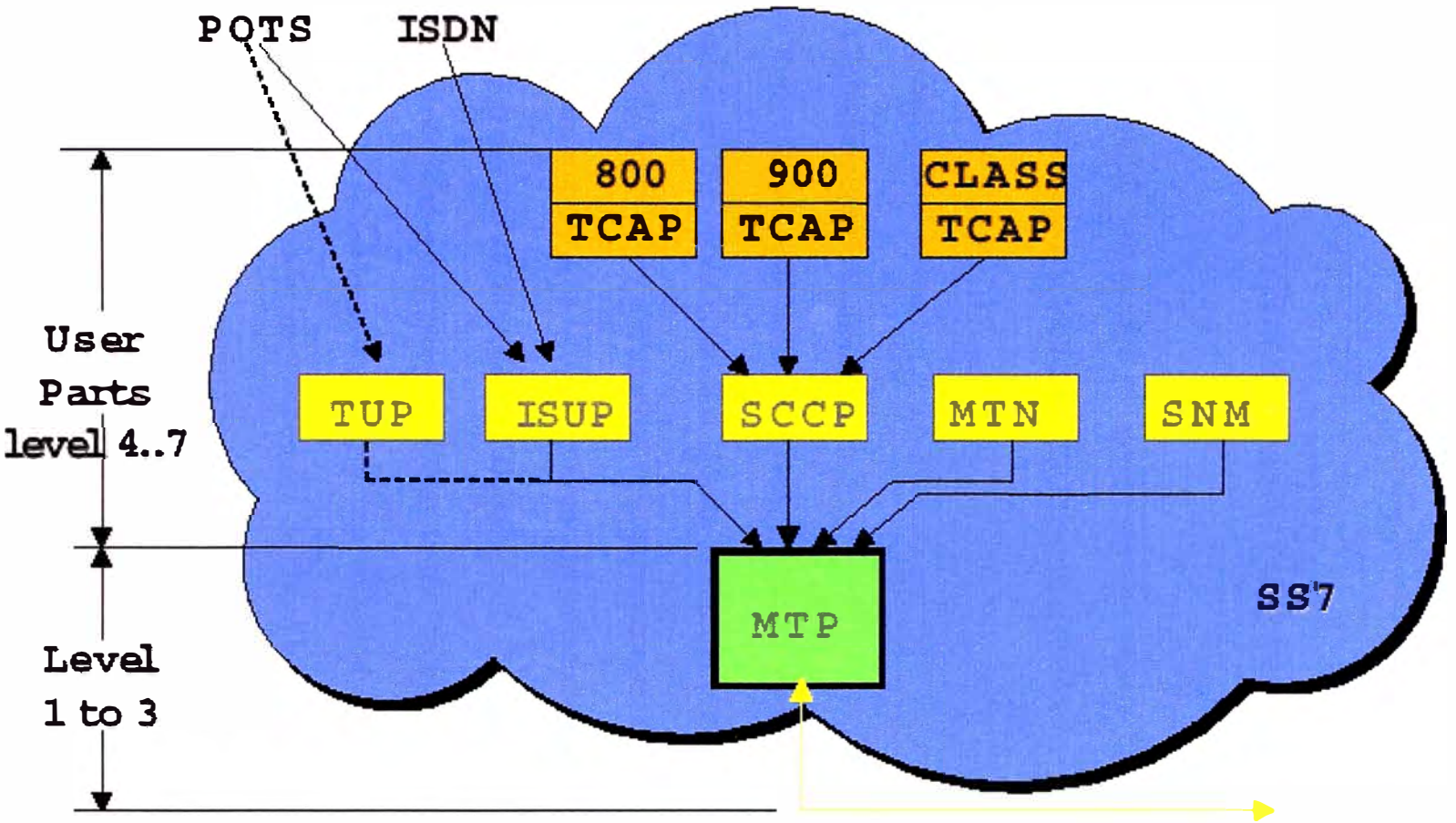


Fig. 1.12 Arquitectura SS7

CAPITULO II
CONFIGURACION DE LOS SISTEMAS DE MONITOREO

El propósito de esta sección es dar una descripción técnica y un acercamiento practico de los Sistemas de Monitoreo que hay en el mercado.

2.1 Arquitectura del Access7

2.1.1 Central Site (Sitio Central)

El Sitio Central es el principal punto de control para un sistema acceSS7. Consiste de un Servidor Central que ejecuta la función principal del software de aplicación de acceSS7 y workstations de usuarios que muestran representaciones gráficas del desempeño de la Red, dependiendo del software de aplicación actual.

2.1.2 Measurement Site (Sitio de Mediciones)

Un Sitio de Mediciones consiste de uno ó más Procesadores de Sitio (hasta un máximo de 10 procesadores de Sitio) y una colección de card cages (hasta un máximo de 20 card cages por procesador de Sitio) conteniendo el hardware de mediciones necesario para capturar el tráfico de SS7 de los Signaling Links. Los Sitios de Mediciones normalmente están ubicados cerca de los STPs en la Red de Señalización para que tengan acceso a una gran concentración de Signaling Links.

Nota:

Las redes LANs en los sitios de Mediciones y en el Sitio Central es provista por el cliente (Fig. 2.1).

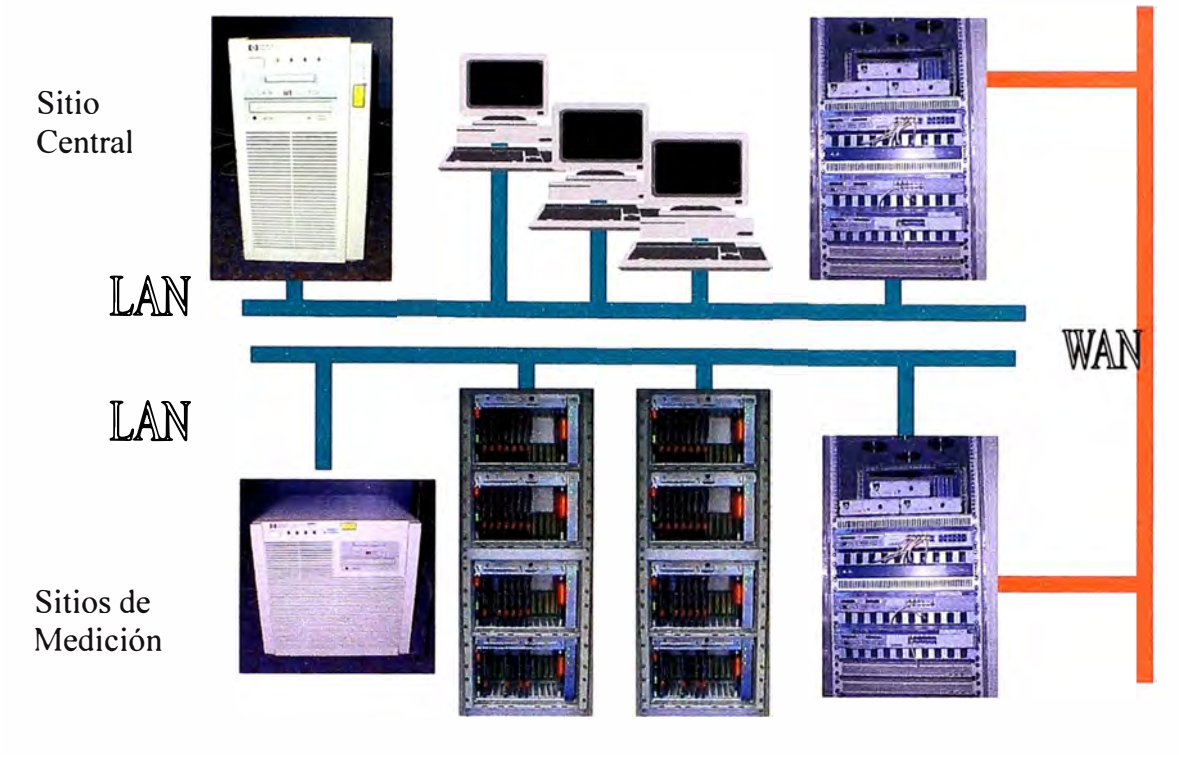


Fig. 2.1 Arquitectura Física.

El acceSS7 Central Site y Measurement Sites están inter-conectados mediante una red ancha TCP/IP Wide Area Network (WAN). Esto le permite a los procesadores de Sitio en los Sitios de medición comunicarse con el servidor central. La red WAN no se suministra como parte del sistema acceSS7, sino que es suministrada por los mismos clientes.

2.1.3 Enlaces Monitoreados

Los Enlaces SS7 que son monitoreados son especificados por el cliente antes de la instalación y son dependientes del tipo de monitoreo que es requerido (Fig. 2.2).

Los Card cages que monitorean los Enlaces para la aplicación de Fraude, por ejemplo, pueden ser restringidos simplemente a una conexión Internacional.

La mayor parte de la supervisión se puede realizar por Card cages situadas en las STPs, sin embargo así se perderá tráfico de los Enlaces 'F' y los Enlaces 'E'.

El uso telefónico se puede monitorear en los Enlaces 'A' y 'B', aún cuando información más detallada acerca del desempeño de la Red se podrá obtener monitoreando también a los Enlaces 'C'.

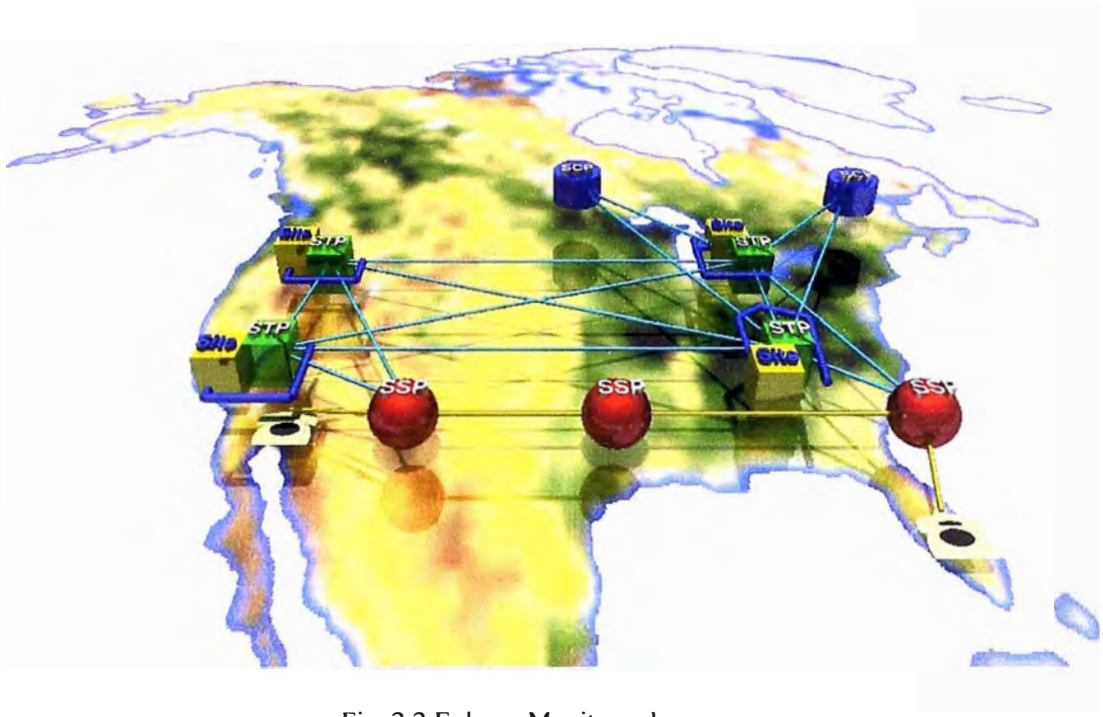


Fig. 2.2 Enlaces Monitoreados

2.1.4 Grupos de area

•Los Grupos de Área se usan para separar el acceso de los usuarios a los Links y Signaling Points en su Red SS7.

•Un Grupo de Área consiste de una lista de SPs, usualmente STPs y sus asociados SCPs, SSPs y CCSSOs (Common Channel Signaling Switching Offices) (Fig. 2.3).

•Signaling Links se considera que pertenecen al Grupo de Área asociado con el SP en el extremo monitoreado del Link.

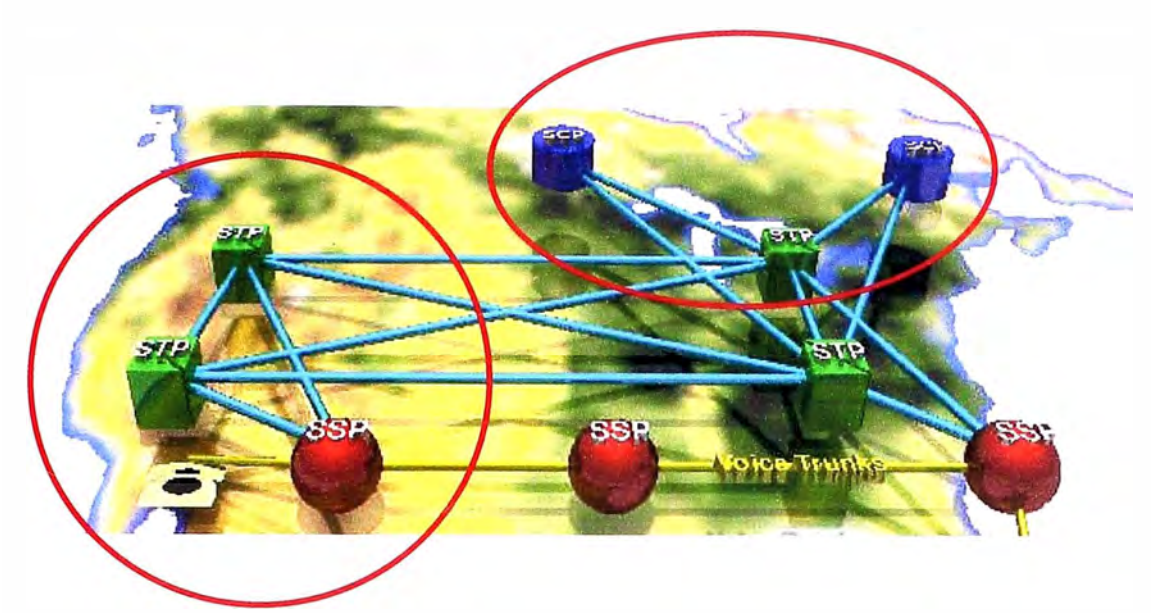


Fig. 2.3 Grupos de Area.

Un Grupo de Área contiene una lista de SPs, usualmente STPs y sus asociados SCPs, SSPs y CCSSOs (Common Channel Signaling Switching Offices). Los usuarios también pueden ver los SPs conectados a los Enlaces monitoreados por los SPs en el Grupo de Área.

Cada usuario de acceSS7 debe pertenecer a solamente un Grupo de Área.

Nota

Las aplicaciones de acceSS7 solo le permitirán monitorear Links y Signaling Points que pertenezcan a su Grupo de Área designado.

Es la responsabilidad del Administrador del Sistema decidir la estructura de los Grupos de Área para las Redes SS7. El acceso de un usuario a los enlaces dentro de su Grupo de Área puede ser restringido si se requiere mediante el utilitario **(p7modauthlinks)**

2.1.5 Sitio central

El Sitio central consta de:

•El Servidor Central

•Los Servidores de Aplicaciones

•Las Workstations de los usuarios

•Los Terminales-X

Los servidores y workstations están conectados mediante una red LAN, y la red LAN está conectada a los Sitios remotos sobre la red WAN.

Nota

Los Servidores de Aplicaciones solo son requeridos cuando cualquiera de las workstations de usuarios son Terminales- X ó no-HP.

2.1.5.1 El servidor Central

•El servidor central es un sistema HP 9000 Series 800 ejecutando un HP-UX (Unix) Operating System.

•El servidor central provee control central del sistema acceSS7.

•Recibe información y estadísticas de los Sitios de mediciones y produce resultados de mediciones completos.

•Estos resultados de mediciones son enviados a las workstations de los usuarios, donde son usados para proveer pantallas casi en tiempo real de la actividad y desempeño de la Red.

El Servidor Central también mantiene la Base de Datos de Configuración de acceSS7 y el Registro de Alarmas Central.

2.1.5.2 El Servidor de Aplicaciones

•El Servidor de Aplicaciones es un Sistema HP 9000 Series 800 System ejecutando un HP-UX Operating System.

•Los Servidores de Aplicaciones solo son requeridos si sus User Workstations no son equipos HP ó X-Terminales.

•El Servidor de Aplicaciones corre el acceSS7 software el cuál produce pantallas gráficas del desempeño de su Red.

•El Servidor de Aplicaciones no tiene ninguna pantalla gráfica directamente conectada, pero exporta las pantallas a los User Workstations y los X-Terminales.

Una Pantalla de Servidor de Aplicaciones se puede configurar para soportar tanto Terminales-X como workstations no-HP ejecutando el software X11.

2.1.5.3 Workstation de Usuario

AcceSS7 soporta 3 tipos diferentes de User Workstation:

1. HP 9000 Series 700 Workstations.
2. no HP workstations.
3. X-terminales.

Los usuarios inician el sistema acceSS7 mediante *logging on* a las User Workstations. Las Workstations proveen pantallas gráficas que permiten a los usuarios monitorear el desempeño de su Red.

2.1.5.3.1 HP 9000 Series 700 Workstations

HP 9000 series 700 Workstations no requieren un Servidor de Aplicaciones - ellas ejecutan el software acceSS7 directamente y muestran la interfase gráfica del usuario de acceSS7. Se comunican con el Servidor Central para requerir los valores de las mediciones que ellas muestran.

2.1.5.3.2 No - HP Workstations

Las no- HP Workstations no ejecutan el software de aplicación de acceSS7 y no hablan directamente al Servidor Central - este es el trabajo del Servidor de Aplicaciones. Ellas operan efectivamente como Terminales-X y muestran la interfase gráfica de usuario para las aplicaciones de acceSS7.

2.1.5.3.3 X-Terminales

Los Terminales -X no ejecutan el software de aplicación de acceSS7 y no hablan directamente al Servidor Central - este es el trabajo del Servidor de Aplicaciones. Su trabajo es solo mostrar la interfase gráfica de usuario para las aplicaciones de acceSS7.

2.1.6 Sitio de Medición

Un Sitio de Medición es responsable de recabar los datos de las mediciones de un grupo de Enlaces SS7 conectados a un SP monitoreado (usualmente un STP) .

La Red SS7 está conectada a los portadores en las Tarjetas de Interfase en los Card Cages.

El Hardware del Sitio de Medición está localizado en ó cerca del Signaling Point desde el cuál se extraen los datos.

Los datos primarios recogidos en el Sitio de Medición son enviados al Servidor Central para un procesamiento adicional.

Un Sitio de Medición Consta de:

•Uno ó más Procesadores de Sitio (hasta un máximo de 10 procesadores de Sitio)

•Card cages conteniendo el hardware de medición (hasta un máximo de 20 card cages por procesador de Sitio)

El procesador y los card cages están conectados juntos mediante una red LAN, la cuál está conectada al Servidor Central y a otros Sitios remotos sobre la red WAN.

2.1.6.1 Card cage para medición

Un card cage de mediciones contiene el hardware que monitorea sus SS7 Signaling Links.

Un card cage consta de 13 ranuras (incluyendo una para la Tarjeta X-Comms) conectadas juntas mediante un plano trasero de inter-conexión (backplane).

El backplane permite que las tarjetas sean colocadas en las ranuras (slots) para comunicarse unas con otras.

Un card cage puede contener:

•Interface Cards (IFs) " *Tarjetas de Interfase*" (mínimo 1, máximo 6)

•Interface Processor Cards (IFPCs) " *Tarjetas de Interfase de Procesador*" (mínimo 1, máximo 8)

•Data Capture Card *"Tarjeta de captura de Datos*" (sólo 1)

•Una Tarjeta de Comunicaciones Externas " External Communications Card" (X-Comms) (obligatoria)

•Fuente de Alimentación "Power Supply" (obligatoria)

La tarjeta X-Comms tiene su propia ranura dedicada además de las 12 ranuras standard disponibles para las tarjetas de Interfase y de Procesador.

Las ranuras del card cage están numeradas (de izquierda a derecha) X-Comms, 0. . . 11.

2.1.6.2 Configuración del Card cage

Cada card cage tiene 12 ranuras - numeradas 0 – 11 (Fig. 2.4).

•Ranuras 0 - 5 están dedicadas a las Interface Processor Cards.

•Ranuras 6 & 7 pueden mantener IFPCs ó Interface Cards ó Data Capture Cards.

•Ranuras 8 - 11 están dedicadas a Interface Cards ó Data Capture Cards.

•La Tarjeta de Comunicaciones Externas tiene su propia ranura dedicada.

Dada la información anterior, esto significa que cada card cage puede soportar un máximo de 8 IFPCs ó 6 Interface Cards - pero no ambas al mismo tiempo.

Con 8 IFPCs y una ó más tarjetas E1 ó DS1 IF, un card cage puede monitorear hasta 64 Enlaces.

Con 6 tarjetas IFPCs y 6 tarjetas DS-0A IF, un card cage puede monitorear hasta 48 Enlaces.

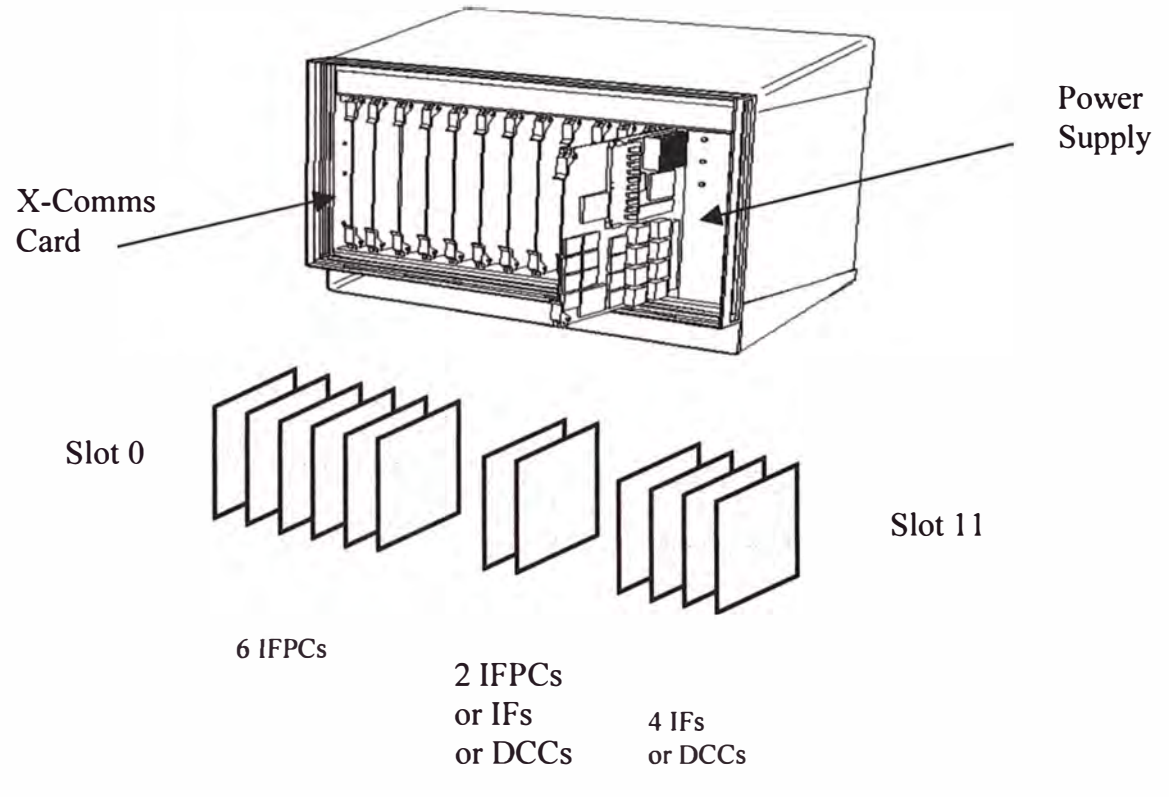


Fig 2.4 Configuración del Card cage

Nota

Una tarjeta DCC no debería ser configurada para monitorear más que 32 Enlaces.

2.1.6.3 Conexión del Card Cage a los SS7 Links

Los Card cages típicamente están conectados a la Red de Señalización SS7 mediante un Puente Aislador (Bridging Isolator) Fig. 2.5 .

El Bridging Isolator asegura que el hardware de mediciones de acceSS7 se conecta sin afectar a los Enlaces SS7.

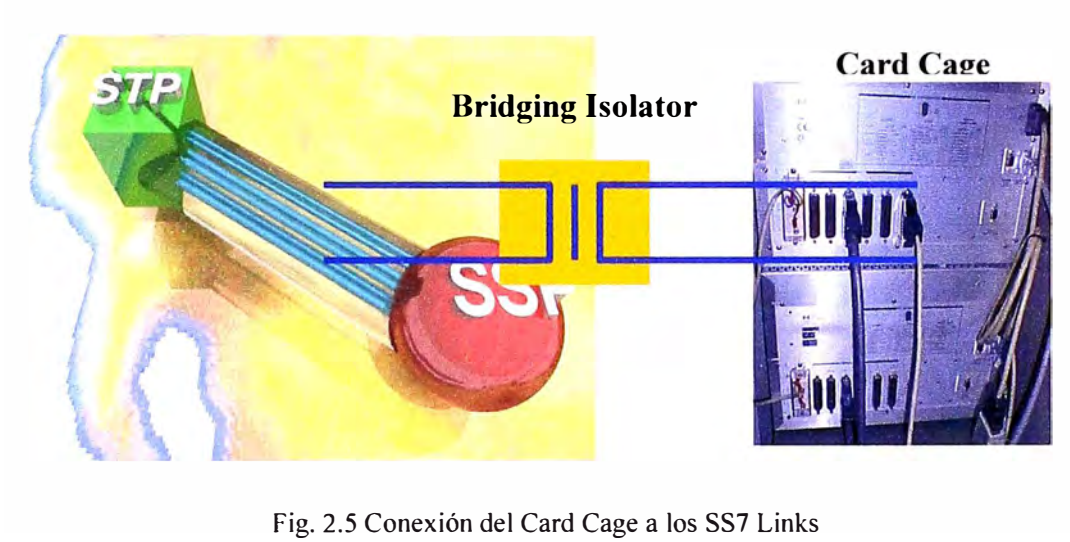


Fig. 2.5 Conexión del Card Cage a los SS7 Links

2.1.7 Procesador de Sitio

•El Procesador(es) de Sitio controla los card cages en un Sitio de medición.

•Es el responsable de adquirir los datos de los card cages y de enviarlos al Servidor del Sitio Central.

•Los Procesadores de Sitio para una pareja de STP se conectan en la WAN para proveer cross-site triggering para algunas de las aplicaciones de software.

El Procesador de Sitio es un servidor HP 9000 Series 800 ejecutando el HP-UX Operating System.

Los procesadores de Sitio usan Capability Codes para reconocer los pares de STP apareados para el disparo en sitio.

Normalmente solo hay un procesador de Sitio en cada Sitio, sin embargo, pueden existir hasta 10 procesadores de Sitio en cada Sitio (controlado por un recurso), hasta un límite de 120 procesadores de Sitio, en todo el sistema.

2.1.8 Arquitectura del software del Access7

La arquitectura del acceSS7 Software (Fig. 2.6a) se puede visualizar como varias capas de software, cada una construida sobre la capa anterior. La capa inferior en la arquitectura del acceSS7 software es el sistema operativo Unix en cada uno de los mayores componentes del hardware. El Servidor del Sitio Central, la workstation del usuario y los procesadores de Sitio usan HP-UX. Las tarjetas IFPC usan VxWorks.

Las workstations de los usuarios ejecutan el software X Windows para proveer la interfase gráfica del usuario para las aplicaciones del software acceSS7, y OpenView también se usa para proveer mapas gráficos de la Red de Señalización.

El Servidor Central usa Informix como un depósito seguro para la información del sistema. La base de datos relacional Oracle también es usada en el Servidor Central para almacenar alarmas para la aplicación de Alarm Manager.

Todos estos paquetes en conjunto constituyen los bloques fundamentales sobre los que se basa el software de aplicación de acceSS7.

Fig. 2.6a Arquitectura del Software

Sobre la capa básica del software, acceSS7 provee un núcleo de infraestructura de funcionalidad el cuál es común a todas las aplicaciones de acceSS7. La infraestructura permite a las aplicaciones configurar el hardware de acceSS7; Obteniendo acceso a las unidades individuales de Señalización SS7; Suministrando capacidades de marcas de tiempo para los mensajes y muchas otras funciones que todas las aplicaciones comparten en común.

Construidas sobre el tope de la infraestructura están las aplicaciones de acceSS7; incluyendo Link Status Monitor, Traffic Monitor, Call Trace, Alarm Manager, Protocol Analysis y Fraud (Fig. 2.6b).

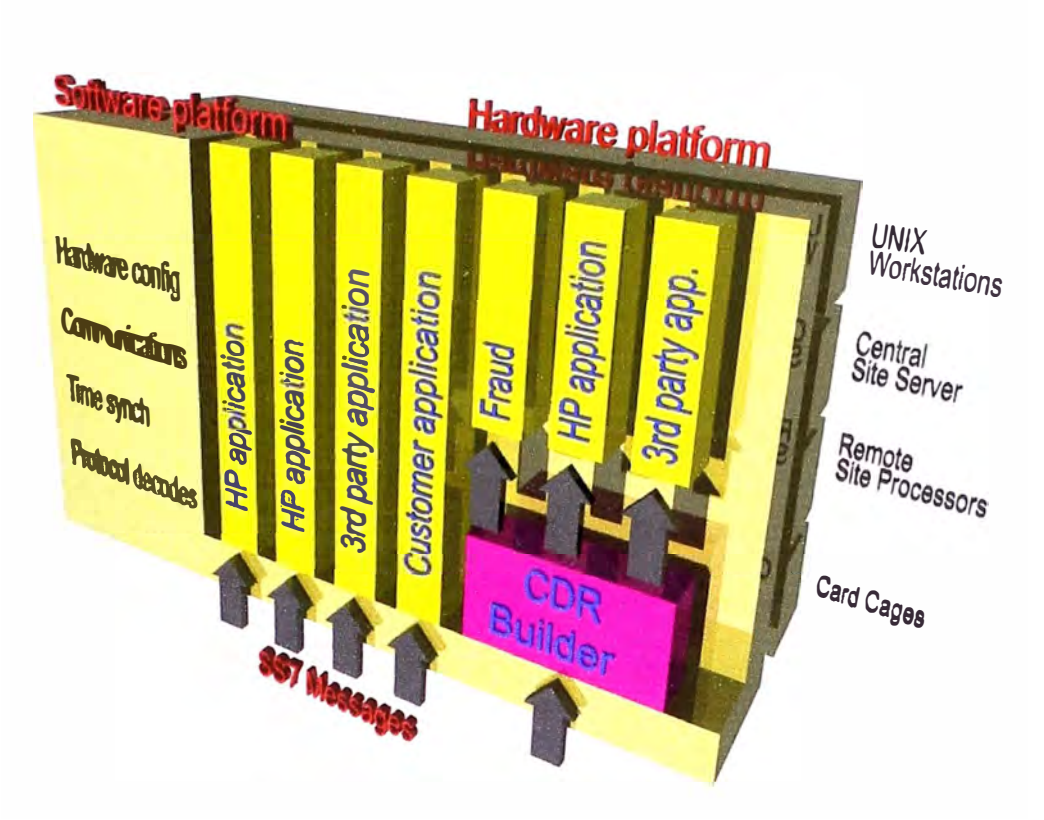


Fig. 2.6b Arquitectura del Software

2.2 Arquitectura del Quest7

QUEST7 es el Sistema de Supervisión SS7 de GN Nettest, esta basado en dos productos GN probados: el Analizador de Protocolos Multicanal (MPA), diseñado específicamente para soportar redes de señalización SS7 y el sistema de gestión QUEST®. Estos productos son transparentes al usuario del sistema de supervisión de señalización SS7 que desea monitorear el funcionamiento de la red.

El MPA es una sonda de monitoreo multi-link para el análisis detallado de la Señalización por Canal Común SS7, incluso los protocolos para las redes fijas, los servicios de RI y GSM. QUEST® es un sistema de gestión que asegura calidad máxima y disponibilidad al costo mínimo. MPA y QUEST® ya están sirviendo satisfactoriamente a los principales operadores y portadores.

2.2.1 Arquitectura del Sistema global

La solución ofrecida esta basado en los componentes estándar de QUEST7:

- La funcionalidad del Centro de Supervisión (la correlación de los datos y el acceso externo a los datos) se entrega a través de componentes de QUEST7 que ejecutan en los Compaq AlphaServers a los Centros de Supervisión Regionales y o Principales. Las interfaces del operador se proporcionan por los workstations con las conexiones de LAN o WAN a los servidores.

- La funcionalidad de MSC/STP (la colección de datos de la medida) se entrega a través de varias sondas de supervisión (MPA 8100) a estos sitios.

Los servidores de Unix pueden localizarse en uno o varios de los sitios anteriores que dependen de la configuración del sistema real y requisitos del cliente.

Los componentes estándares se conectan vía conexiones de WAN o LAN que usan TCP/IP para el transporte (Fig. 2.7). El ancho de banda requerido entre los componentes del sistema también depende de la aplicación real. Los valores típicos están en el rango de 64 KBit/s a 2 MBit/s.

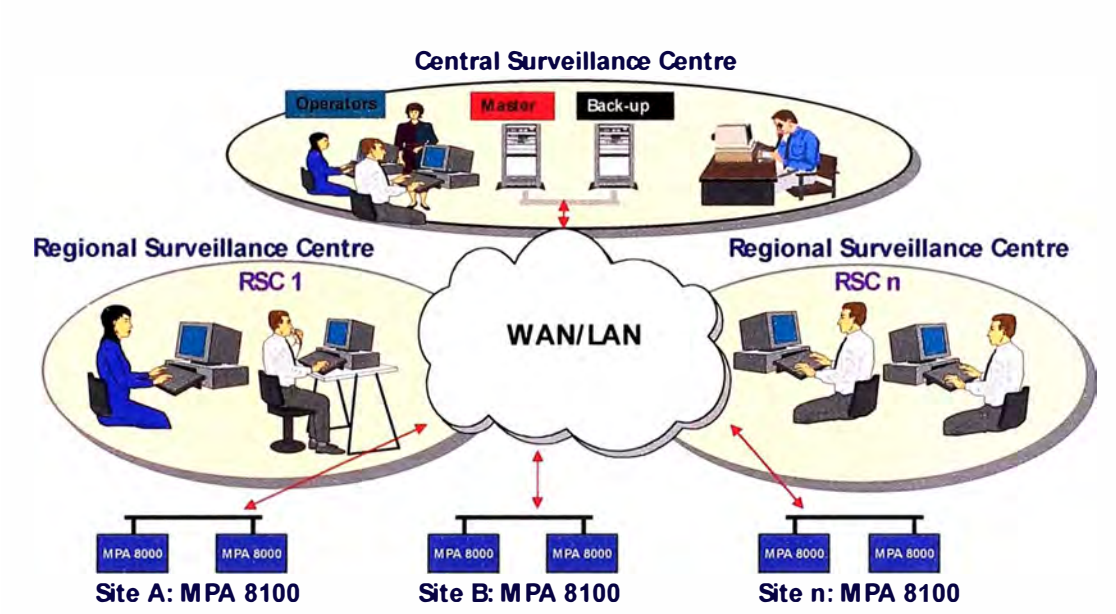


Fig. 2.7 Arquitectura Fisica

2.2.2 Arquitectura de HW

2.2.2.1 Operación Central

El Compaq AlphaServers es usado en el sistema de QUEST7 para organizar las aplicaciones de QUEST7. Externamente los servidores se conectan a una red WAN vía un Router.

Para proporcionar interfase al operador uno mas workstation pueden ser conectados al servidor (vía LAN) . Los Workstation pueden ser Workstation Compaq (en cada caso ellos pueden ejecutar el software nativo MMI) o ellos pueden ser PC

(en cada caso ellos usarán el login remoto para ejecutar el software MMI en el servidor usando X-Windows).

2.2.2.2 Conmutador Central

Cada conmutador central (Fig. 2.8) contiene uno o más sondas de medida MPA 8100. Los MPAs son conectados a un Ethernet LAN que a su vez se conectan al mundo externo vía un router.

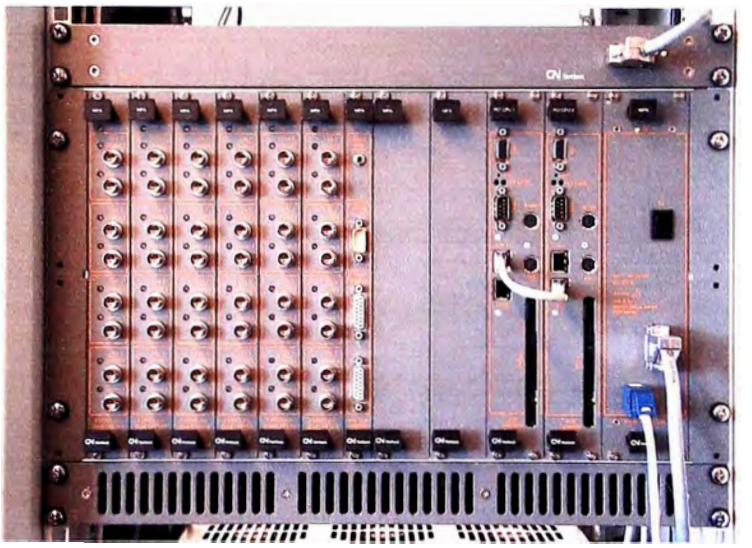


Fig. 2.8 Conmutador Central

Un MPA 8100 consiste de:

· Una Unidad Ventilador

· Un Ducto de Aire

· El MPA básico 8100 sub-rack con

  · Una Unidad Power (PSU)

  · Dos Unidades Controladoras PCI (PCI1, PCI2)

  · Una Unidad Interfaz de Enlace PCI (PLU)

  · Una a seis Unidades de Enlace (LU)

Hasta seis Unidades del Enlace (LU) puede instalarse en el MPA básico 8100, lo cual significa un MPA 8100 totalmente equipado puede manejar un máximo de 24 enlaces de señalización full duplex.

2.2.2.2.1 Fuente de alimentación (PSU)

El módulo de alimentación opera desde voltajes estándares como –48V DC o –60V DC. El consumo de energía máximo del PSU es 325 W.

2.2.2.2.2 Unidad Controlador PCI (PCU)

Cada Unidad Controlador PCI contiene un computador compacto PCI. El MPA 8100 usa dos Unidades Controladoras PCI que son aplicados para los propósitos siguientes:

· Una Unidad Controlador PCI se usa para recolectar eventos de señalización desde las Unidades de enlace y realiza un conteo estadístico y correlación de los mensajes de señalización. Unos 8 Gbyte de disco duro es usado como un buffer cíclico para el almacenamiento de eventos de señalización y CDR's.

· Otra Unidad Controlador PCI se usa para manejar la comunicación entre los MPA 8100 y la aplicación servidor QUEST7 a través de una interfaz de Ethernet. Unos 2 Gbyte de disco duro se usa para el almacenamiento del software MPA 8100 y para el buffer de los datos de comunicación.

2.2.2.2.3 Unidad Interfaz de Enlace PCI (PLU)

Esta Unidad realiza las funciones siguientes:

· Proporciona una interfaz entre las Unidades de Enlace y las Unidades Controladoras PCI.

· Recibe la información cronometrada y la señal sincronizada del GPS.

2.2.2.2.4 Unidad de Enlace (LU)

Los módulos de la Unidad de Enlace LU son usados para unir los enlaces SS7. Cada Unidad del Enlace puede manejar cuatro enlaces de señalización Full dúplex. Los siguientes siete diferentes tipos de Enlace:

Los LU realizan la conversión del reloj, detección de alarmas de transmisión, análisis de trama, verificación de CRC, el tiempo de eventos, estadísticas y filtración de FISU.

2.2.3 Red

Todo los componentes de HW QUEST7 se interconectan vía las combinaciones de LAN y o las redes WAN.

2.2.4 Arquitectura del SW

El sistema de QUEST7 está distribuido en varios componentes que se ejecutan en el AlphaServers en el centro de operación, y varios componentes que se ejecutan en las sondas de monitoreo MPA 8100.

Estos componentes forman la base para las aplicaciones de QUEST7. Cada aplicación usa uno o más componentes para entregar la funcionalidad por una área específica de uso. Las aplicaciones incluyen:

- Surveillance
- Protocol Analysis
- Call Trace
- Statistics
- Call Behaviour Analysis
- Fraud Detection

2.2.5 Estructura de la aplicación genérica

La estructura arquitectónica del software aplicación QUEST7 es basada en un principio del cliente servidor.

2.2.6 Configuración de la Base de datos.

La configuración de Datos para el sistema de QUEST7 es almacenada en una base de datos distribuida (Oracle® o Sybase®)

2.3 Arquitectura del Geoprobe

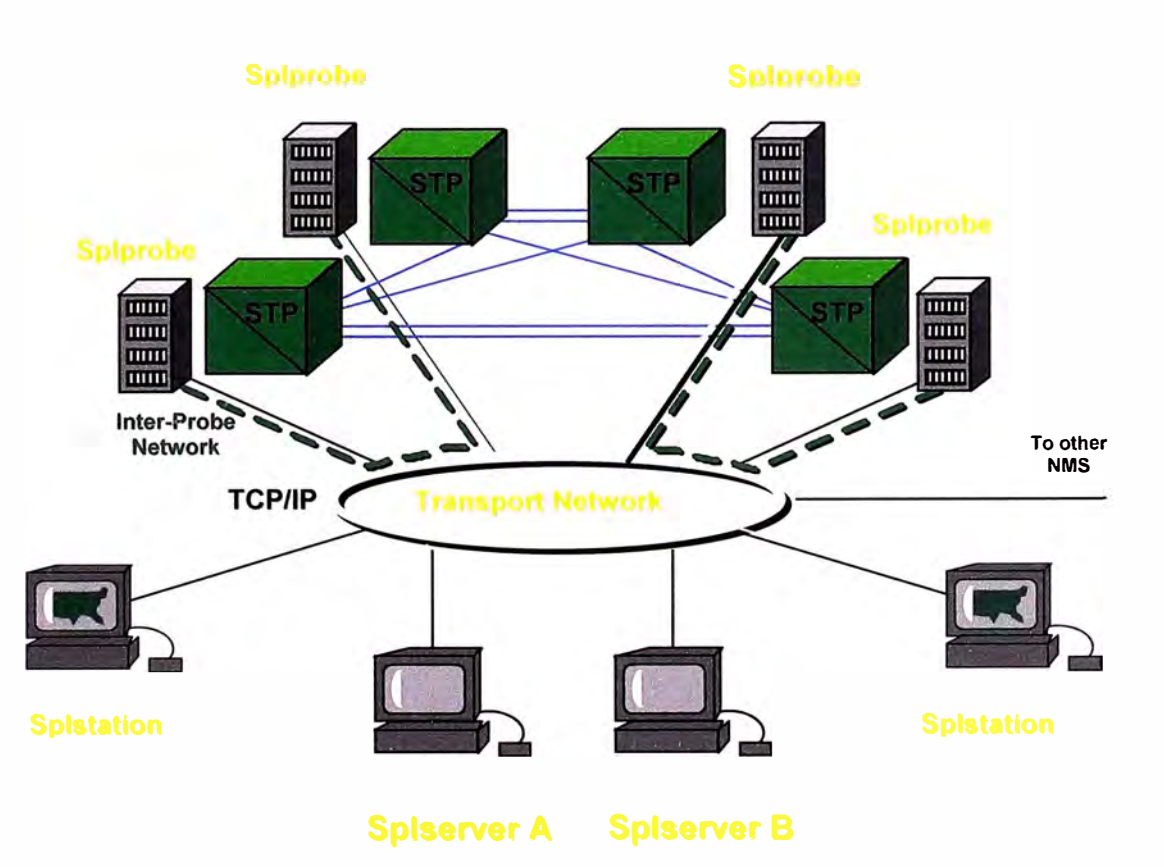


Fig. 2.9 Arquitectura Física

GeoProbe es un Sistema de Supervisión de INET que presenta las siguientes características:

El proceso de Información SS7 es inmediato y en una arquitectura distribuida.

El sistema es redimensionable y ofrece redundancia flexible.

La información es independiente del desarrollador de programas y del proveedor del Switch.

La flexibilidad la demuestra con una configuración par cruzado (Fig. 2.9).

2.3.1 SpIprobe

Es el corazón y cerebro del sistema (Fig. 2.10).

Recoge y Procesa la información SS7 en el Site (lugar donde esta instalado el SpIprobe)

Arquitectura de procesamiento distribuido.

Alberga hasta 18 tarjetas y son una combinación de:

- Interface cards
- Processor cards
- Controller cards

Hasta 192 enlaces de señalización por cada estante.

HW intercambiable.

Diseño integrado y reducido.

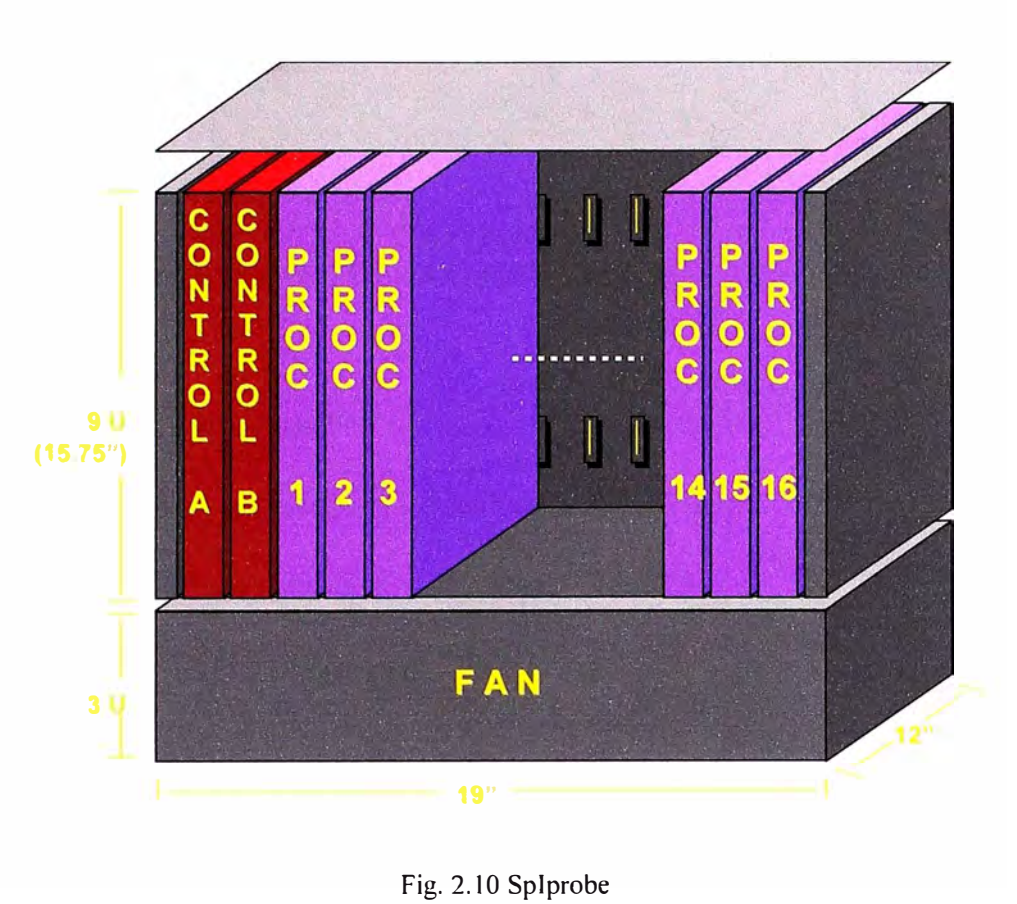


Fig. 2.10 SpIprobe

2.3.2 SpIstation.

Interfase de usuario grafico.

Sun SPARCStation o equivale X11/R5 UNIX workstation

La workstation puede albergar aplicaciones simultaneas.

2.3.3 SpIserver.

Sistema de herramientas de Administración y almacenamiento de Base de Datos.

Procesamiento y presentación continua en los SpIstations y SpIprobes, aun sí el SpIserver esta fuera de servicio.

CAPITULO III
APLICACIONES DE LOS SISTEMAS DE MONITOREO

3.1 Aplicaciones del Access7

Las principales aplicaciones provistas por el access7 son:

•Link Status Monitor

•Traffic Monitor

•Call Trace

•Protocol Analysis

•Network Investigator

•Alarm Manager

•Event Manager

•Datastore

Además hay varias herramientas administrativas:

•System Administration Tool

•Network Configuration Tool

•System Status Tool

También otras aplicaciones:

•Billing

•Fraud

•Business Intelligence

3.1.1 Link Status Monitor

Link Status Monitor (Fig. 3.1) le informa a los usuarios acerca de Enlaces SS7 defectuosos en su Red de Señalización.

El estado de los Enlaces es actualizado casi en tiempo real en un mapa de la Red en HP OpenView.

Link Status Monitor también provee a los usuarios con estadísticas detalladas de sus Enlaces de Señalización SS7.

Se puede ver el estado de los Enlaces de Señalización en su Red.

Se tiene acceso a estadísticas detalladas acerca de los Enlaces de Señalización en su Red. Enlaces de Señalización Defectuosos son rotulados como 'Unhealthy Links', por lo que puede ver de inmediato si existe algún problema relacionado con algún Enlace en su Red.

Las mediciones de status se realizan sobre un período fijo.

Sí dispone del mapa de HP OpenView, la información de status ajusta los colores de los símbolos de los Links, Linksets y Signaling Point en el mapa.

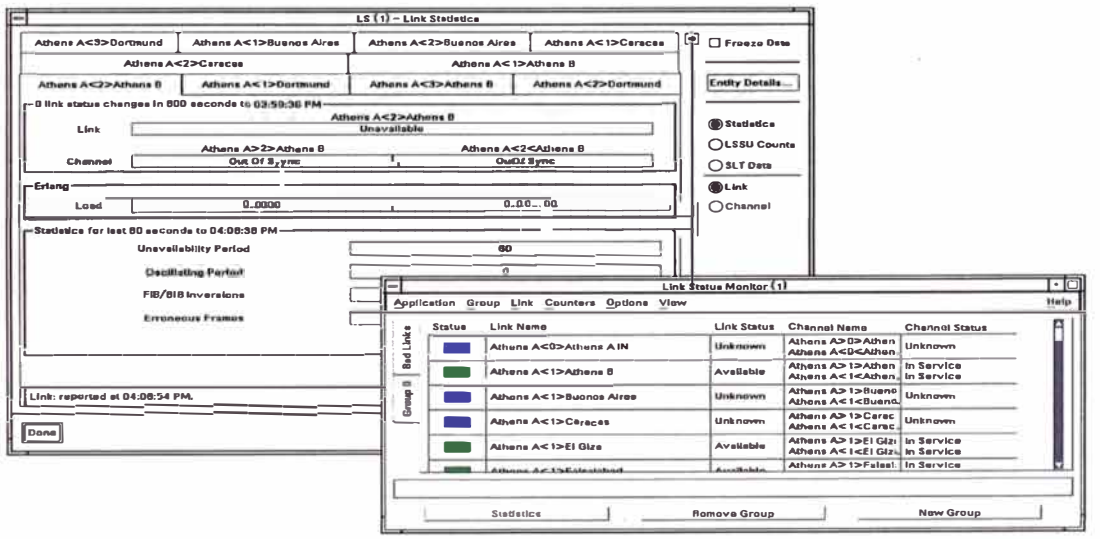


Fig. 3.1 Link Status Monitor

3.1.2 Traffic Monitor

El Traffic Monitor (Fig. 3.2) le permite rápida y fácilmente obtener una visión casi en tiempo real del estado actual de su Red de Señalización SS7.

Realiza mediciones de parámetros claves en su Red y genera datos acerca del desempeño de su Red.

El Traffic Monitor realiza:

•Mediciones relacionadas con Llamadas

•Mediciones de Manejo & Mantenimiento

•Mediciones de Carga

•Mediciones de Aseguramiento del Servicio (opcionales)

•Mediciones de Procedimientos GSM

•Mediciones de Procedimientos IS-41

Traffic Monitor le provee con representaciones gráficas de las estadísticas, fáciles de entender.

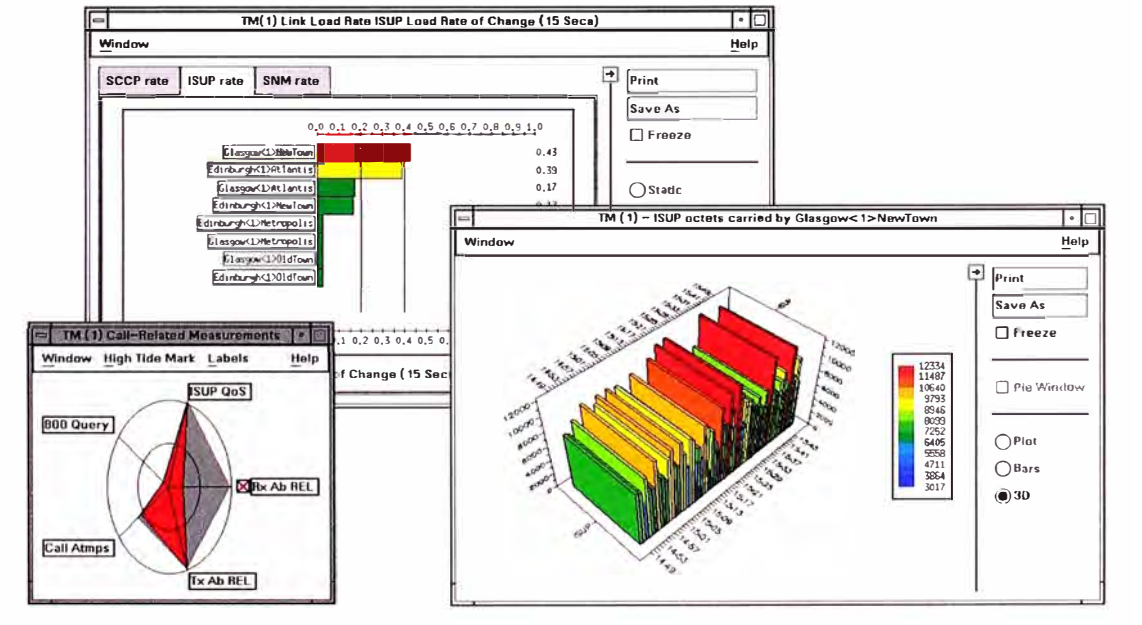


Fig. 3.2 Traffic Monitor

3.1.3 Call Trace

Call Trace (Fig. 3.3) le permite rastrear uno ó más teléfonos, llamadas IS-41 ó GSM a un número, desde un número, entre dos números, cargadas a un número, re-direccionadas a un número (número llamado re-direccionado u original) ó ubicación de ruta del número.

•Puede especificar si quiere rastrear todas las llamadas, ó limitar el rastreo a llamadas Internacionales, Nacionales ó Abonado. Para llamadas IS-41 puede especificar sí quiere rastrear el abonado llamado contra los Dígitos, Mobile Identification Number (MIN), ó Electronic Serial Number (ESN) .

•Para GSM Call Trace puede entrar ó el número telefónico del móvil (MSISDN), un procedimiento relacionado con un teléfono móvil (IMSI, IMEI, LMSI, TMSI) ó una combinación. Estas pueden ser para un teléfono móvil que llama ó es llamado.

•Las llamadas se pueden rastrear casi en tiempo real ó de tráfico SS7 previamente capturado.

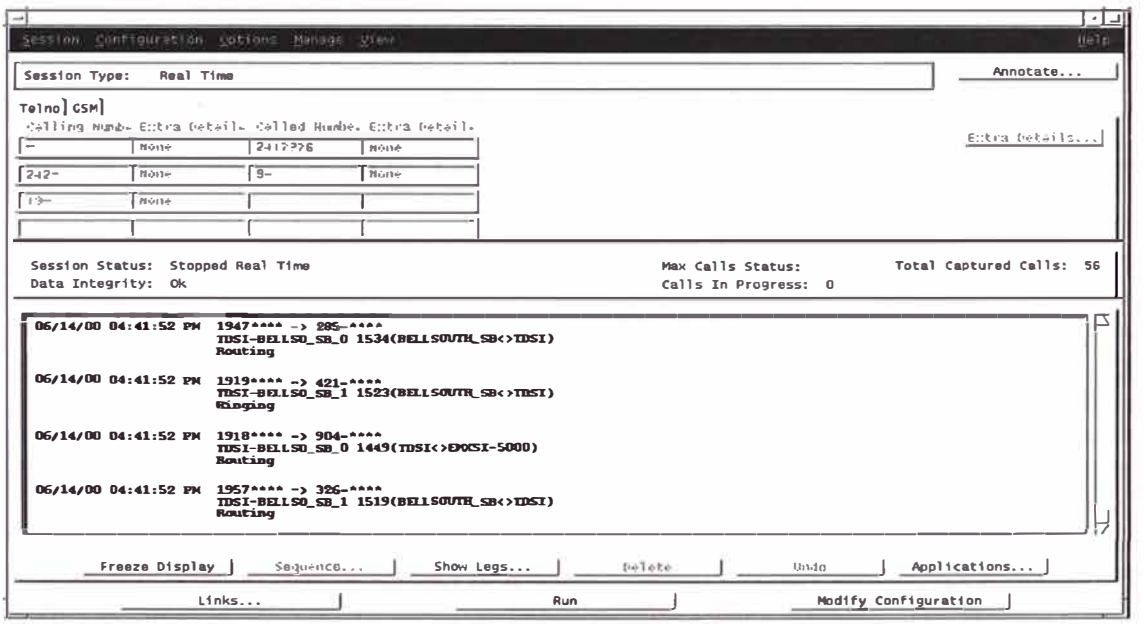


Fig. 3.3 Call Trace

3.1.4 Protocol Analysis

Protocol Analysis (Fig. 3.4) monitorea y analiza los mensajes de Señalización transportados en su Red de Señalización.

En Tiempo- Real

- •monitorea Links ó Linksets casi en tiempo real
- •Captura datos SS7, después de aplicar filtros definidos por el usuario.
- •Inicio / detención controlados por disparos definidos por el usuario.
- •Datos almacenados en disco, mostrados en pantalla.

Post captura

- •aplica filtros, criterios de búsqueda a los datos capturados
- •Decodificación de multi-capas.

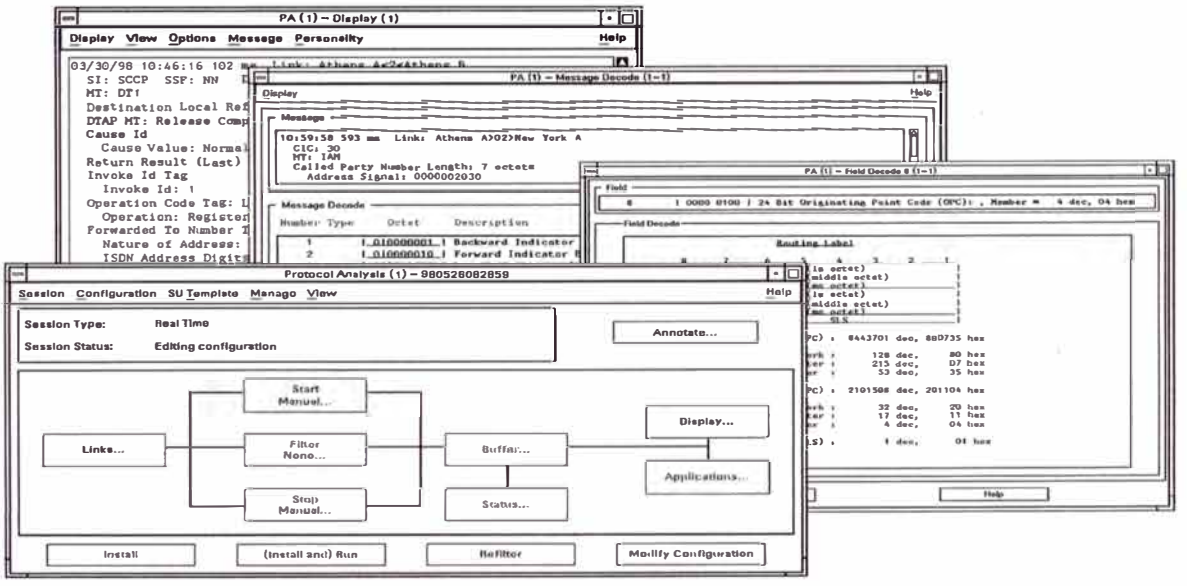


Fig. 3.4 Protocol Analysis

3.1.5 Network Investigator

Su Red SS7 contiene información que se quiere acceder y analizar para que se pueda monitorear el desempeño de los recursos de la Red y medir el impacto de los cambios en la Red. HP acceSS7 Network Investigator le permite hacer esto suministrándole:

•Graphical User Interfaces que le permiten configurar gráficamente los parámetros de medición.

•Monitoreo de desempeño en tiempo real de alarmas y de eventos.

•Grupos de mediciones que le permiten monitorear y controlar mediciones como un grupo antes que individualmente.

•Tipos de Mediciones Standard, incluyendo un número de mediciones de Q.752 y T1.115. Soporta mediciones de conteo de clavijas (peg count) .

•Reportes definibles por el usuario, que le permiten generar resultados de las mediciones en formato gráfico ó tabular. También puede llevar los resultados a aplicaciones externas.

•Umbrales de eventos configurables que significan que se puede definir el límite superior para los eventos generados por una medición. Cuando se excede este límite, se genera una alarma. Además, se muestra el número total de alarmas y de eventos.

3.1.6 Alarm Manager

Las aplicaciones acceSS7 que monitorean su Red de Señalización SS7 pueden generar 'Alarmas de Red'.

Estas Alarmas de Red le notifican que un evento potencialmente importante ha ocurrido en su Red.

Alarm Manager (Fig. 3.5) recolecta y le muestra las Alarmas de Red, permitiéndole manejarlas de una manera consistente.

Registra las alarmas generadas por el Link Status Monitor y el Traffic Monitor.

Puede reconocer y borrar alarmas y también ponerle notas a algunas de ellas.

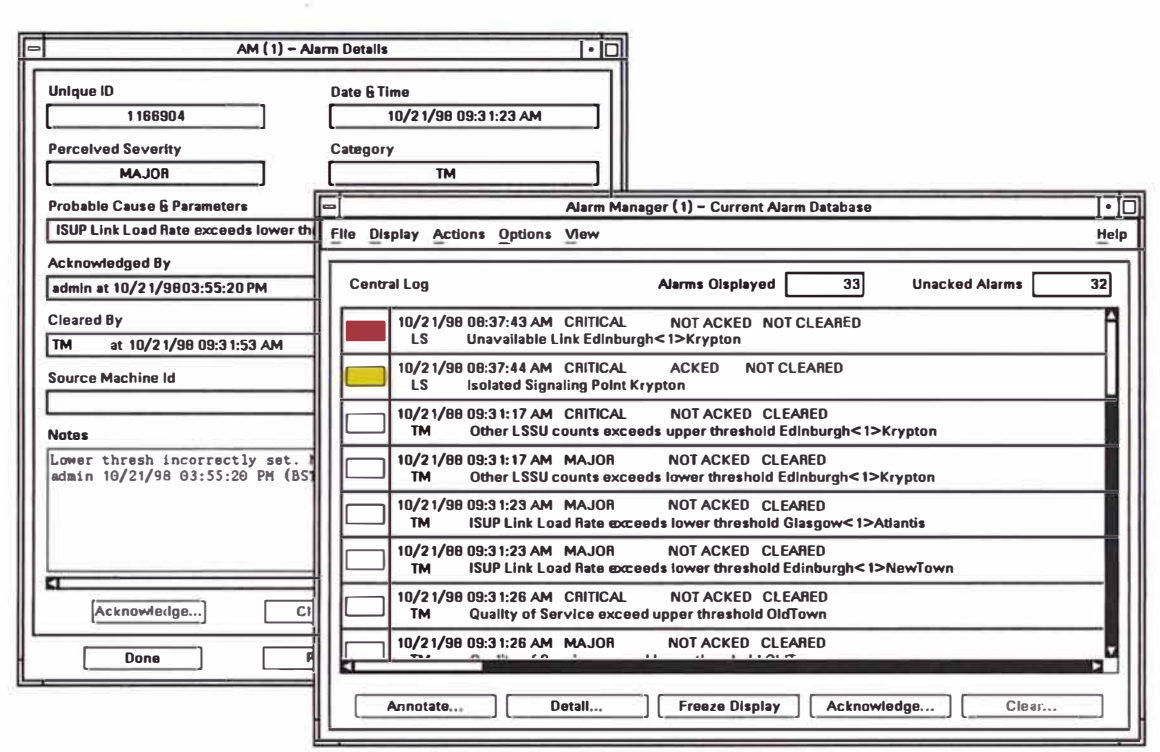


Fig. 3.5 Alarm Manager

3.1.7 Event Manager

Las herramientas GUI le permiten una fácil configuración de las correlaciones de eventos.

Los eventos de LSM, TM, CT y PA son recibidos y procesados en Tiempo Real.

Los eventos son combinados usando lógica AND / OR. Activo para ocurrencia única, con tiempo especificado ó indefinidamente.

Sigue el status de cada correlación

Las sesiones de CT y PA pueden ser iniciadas ó detenidas automáticamente con Event Manager.

Una Alarma se puede registrar con AM cuando una correlación es exitosa.

El Registro de todos los eventos y las correlaciones asociadas son almacenadas para cada usuario.

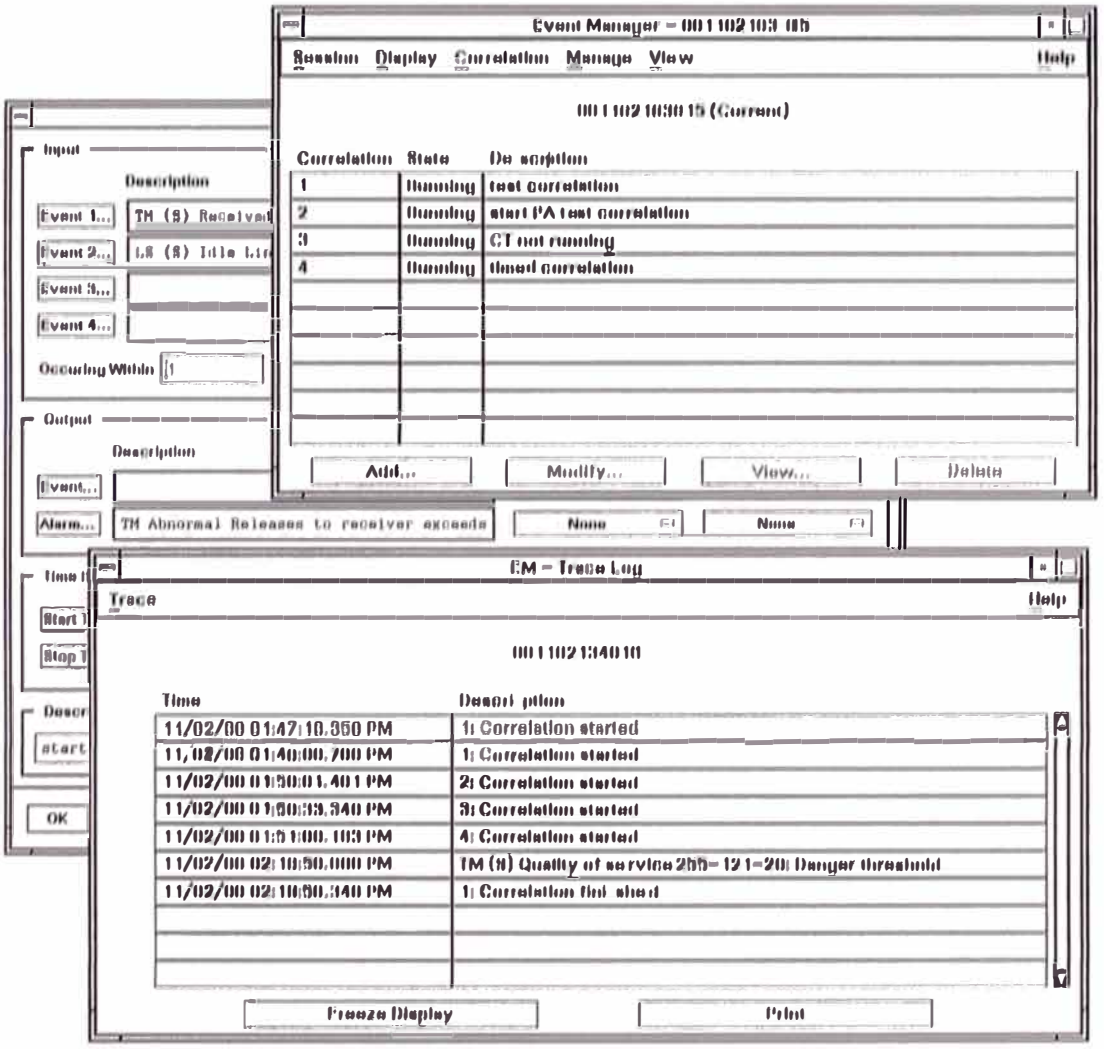


Fig 3.6 Event Mana r

3.1.8 DataStore

DataStore (Fig. 3.7) es una aplicación de acceSS7 que le permite:

•Registro masivo de datos SS7 de una Red activa a un almacenamiento secundario y al mismo tiempo:

•Usar Protocol Analysis ó Call Trace para analizar los datos registrados previamente

DataStore le provee con los datos que necesita para obtener una imagen completa de la actividad de la Red que condujo a un evento significativo en la misma, tal como una caída de la Red.

La operación de DataStore se controla a través de DataStore GUI, ejecutándose en las workstations de usuarios.

DataStore permite registros masivos de datos que posibilitan una exacta y completa imagen de los eventos en la Red. Esto le puede ayudar a Mejorar la Calidad del Servicio mediante:

•Reducción de las Caídas de la Red

•Resolver Asuntos de Integridad de Datos e Interconexión

•Resolver Asuntos de Clientes

Sea que use Protocol Analysis ó Call Trace para analizar problemas actuales en la Red, se usa DataStore para "ir atrás en el tiempo" y analizar problemas y los eventos que los rodean, después que han ocurrido.

DataStore no usa IFPC ó recursos del procesador del Sitio Remoto y potencialmente puede almacenar todos los SUs de todos los Enlaces.

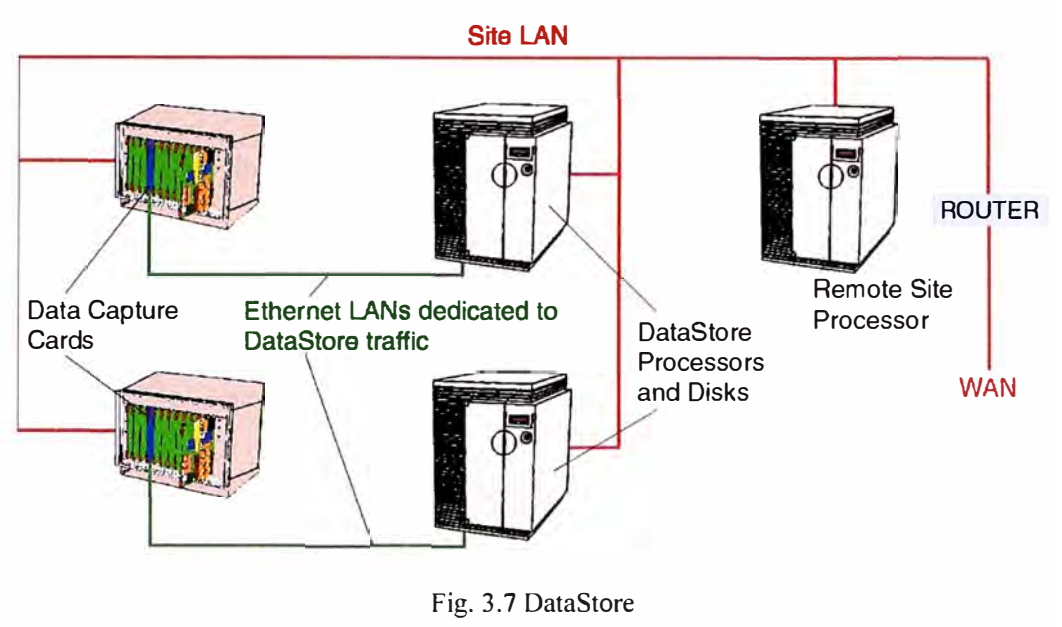


Fig. 3.7 DataStore

3.1.9 Fraude

El HP Fraud Management Toolkit (Fig. 3.8) examina la información de llamadas de ka Red telefónica para identificar fraudes potenciales u otros abusos en el pago.

Las principales actividades son:

Fraud Detection - esta etapa analiza la información de llamadas de la Red telefónica buscando conocidos patrones de llamadas sospechosas, tales como: Llamadas de larga duración a destinos internacionales, llamadas tri-partitas a reconocidas áreas de alto riesgo de fraude en los pagos y así sucesivamente. Este sub-sistema genera Alertas de Fraude (un registro de una ocurrencia sospechosa en una ó más llamadas telefónicas) y luego lo pasa al Case Management.

Case Management esta etapa construye los Casos de Fraude desde las Alertas de Fraude usando un conjunto de claves basadas en los números telefónicos contenidos en las Llamadas. Un Caso de Fraude contiene toda la información de Llamadas y de Alerta relacionadas con un número telefónico dado.

Fraud Investigation - esta etapa provee una interfase de usuario accesada por un equipo de investigadores de fraude. Este es usado para investigar el fraude viendo los Casos, agregando Notas y aplicando Disposiciones a los Casos conforme pasa el tiempo. Finalmente, los investigadores serán requeridos a cerrar los Casos a medida que sus investigaciones son concluidas.

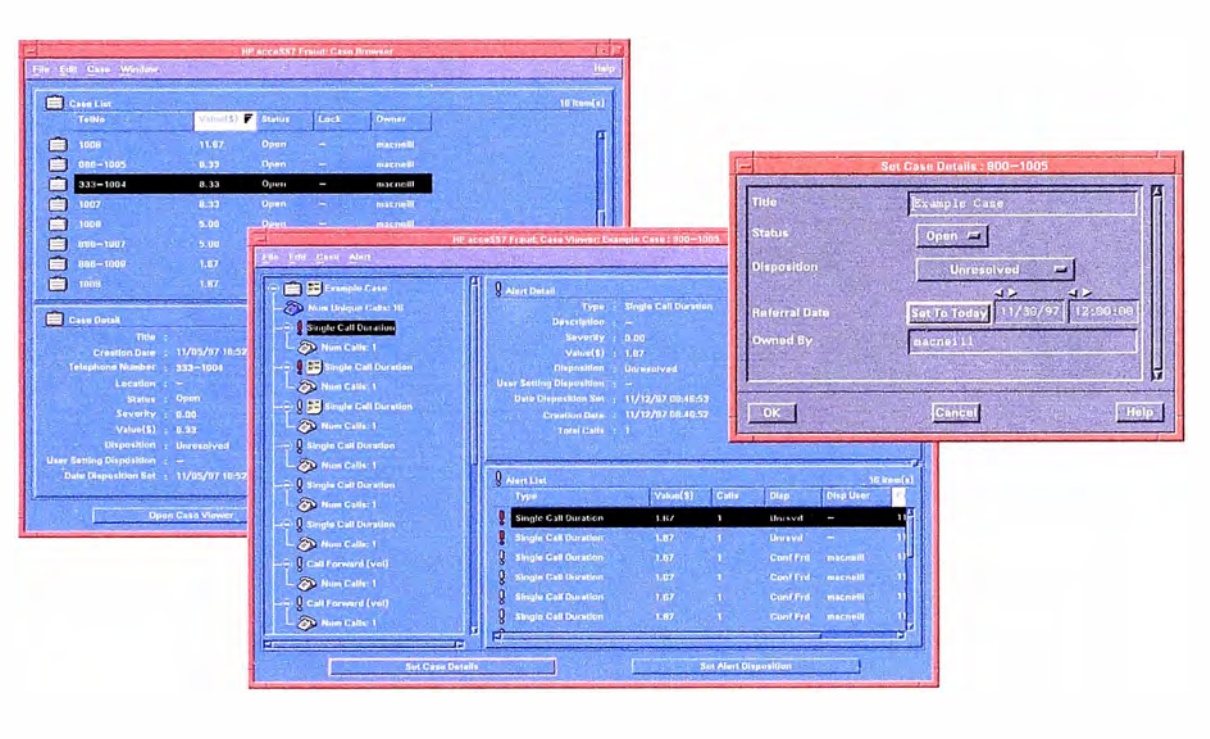


Fig. 3.8 Fraude

3.1.10 Billing CDR7®

(Competitive [access] Detail Recording 7)

CDR7 acumula información e uso para todas las llamadas entre Redes existentes y sub-operadores para propósitos de cobro y aprovisionamiento y lo convierte a un formato utilizable.

Los proveedores de servicio luego usan la información para cobrar a los sub-operadores por el uso de las Redes de conexión existentes y para propósitos de validación de cobro.

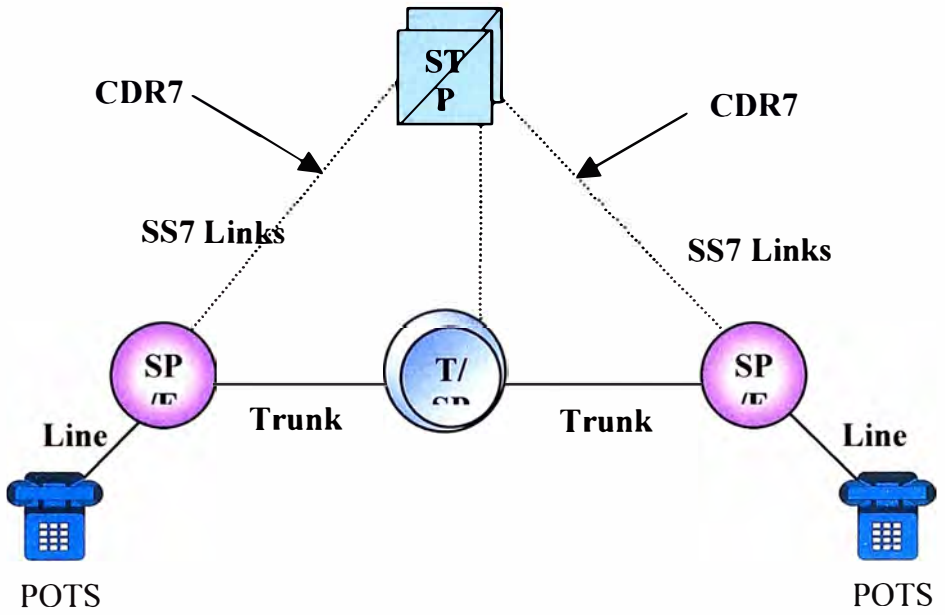


Fig. 3.9 Billing

3.2 Aplicaciones del Quest7

3.2.1 Network Surveillance

El Sistema de Supervisión de Red suministra una flexible y comprensible plataforma para recolectar toda la información de redes fijas e inalámbricas, independientes de los elementos de la red y en tiempo real. El sistema ofrece:

- Visión general jerárquica.
- Demostración grafica con alarmas visuales.
- Configuración según requerimientos organizacionales y geográficos.
- Fácil de usar las alarmas y eventos con amplios filtros

El Network Surveillance es la principal aplicación en QUEST7 ya que las aplicaciones son inicializadas desde aquí, además almacena toda la información de alarmas en objetos orientados a una base de datos Oracle.

3.2.2 SS7 Protocol Análisis

Proporciona una completa colección de decodificadores del paquete de protocolos SS7.

Para asegurar una exacta secuencia y orden en los mensajes estos son grabados por un HW de sondas de monitoreo.

Una sesión es inicializada seleccionando el link a analizar luego el MPA 8100s enviara todos los eventos requeridos por el Protocol Análisis Cliente en tiempo real.

El nivel de detalle de los mensajes pueden ser seleccionados como "general " o "detallado".

3.2.3 Call Trace

Esta aplicación presenta el traceo de las llamadas a lo largo de SS7, GSM/PCS y Redes Inteligentes especificando por ejemplo un numero telefónico (o parte de este).

3.2.4 QUEST7 Statistical Applications

Cuenta con las siguientes aplicaciones:

Link and Message Count statistical application

Performance Statistics (Q.752) application

Call Quality Statistics (E.422) application

La aplicación soporta registro, recuperación y reporte de la data recolectada por la sonda de monitoreo MPA 8100.

3.2.5 Call Data Recording

La aplicación CDR es capaz de recolectar información en cada llamada en la red. Los CDR's son sucesivamente almacenados en una base de datos estándar y hechos disponibles a otras aplicaciones a través de interfaces SQL.

3.2.6 Call Behaviour Análisis

Es un juego de herramientas usadas para analizar informacion generada por el CDR Server. Esta aplicación esta orientado para diferentes usuarios que ejecutan tareas como:

- Operación y mantenimiento de la Red
- Marketing
- Facturación

3.2.7 Basic Fraud Detection

Esta aplicación ayuda al operador a detectar fraude causado por los abonados.

3.3 Aplicaciones del Geoprobe

3.3.1 Network Surveillance

- SS7 Basic Surveillance
- User Call Trace
- MTP and SCCP
- REMON (Remote Monitoring of Protocol Analysis)
- Mass Call Onset Detection
- Signal Unit DataStore (SuDStore)
- Custom or Standard Protocol (MTP, SCCP, ISUP, TCAP, INAP, AIN, IS41, TUP)

3.3.2 Billing

-Usage Measurement

-Call Detail Record (CDR) Generation

-New Service Rollouts

3.3.3 Fraud Management

-Aplicaciones para fraude en lineas fijas e inhalambricas.

-Detección Instantánea

-Chequea Frecuencia, lugar, duración.

3.3.4 Marketing Data

Reportes y estadísticas:

3.3.5 Data Adquisition

MSU Forwarding

CDR Forwarding

SuDStore

3.3.6 Service Quality Assurance

Calidad de Servicio enviado al cliente individualmente

Genera alarmas cuando el funcionamiento cae debajo de estándares.

CAPITULO IV
RESULTADOS Y ANÁLISIS DEL ACCESS7

4.1 Detección temprana de llamadas masivas.

4.1.1 Problema

Si ocurriese un día habitual uno de esos concursos radiales en los cuales se promocionan grandes premios a las primeras llamadas telefónicas, a la emisora. La respuesta del publico es inmediata y podría ser causa de una sobrecarga en la red.

4.1.2 Solución

Para analizar una masiva de llamadas con éxito, necesitamos un sistema de advertencia de tiempo real eficaz. Este debe alertarnos de sobrecargas que ocurren en cualquier parte en la red, mientras se identifica qué partes de la red están involucradas y qué número es el llamado. Una vez obtenida esta información podemos aplicar rápidamente algún procedimiento correctivo para proteger la red, así también causamos una molestia mínima a los clientes (abonados) .

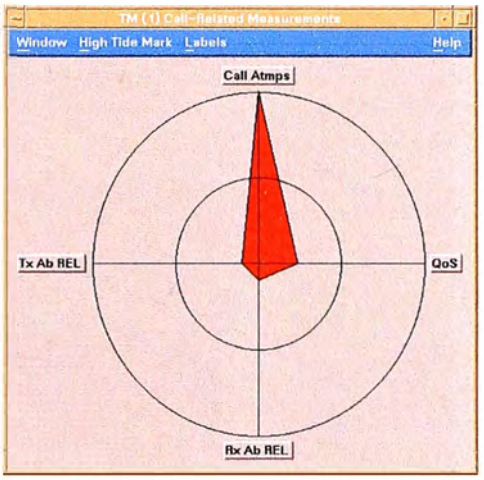
4.1.3 Aplicando acceSS7

El aplicativo Traffic Monitor recolecta y analiza los datos del tiempo real de todas las partes de su red, mientras nos proporciona la advertencia inmediata de una actividad anormal, como llamadas masivas. Podemos configurar el Traffic Monitor para hacer más de 100 medidas en varias categorías diferentes y desplegar los resultados simultáneamente.

1. Dentro de 15 segundos de una sobrecarga causados por las llamadas masiva ocurridas en cualquier parte en su red provocan alarmas en el Monitor de trafico y se torna a color Rojo

Fig. 4.1 Diagrama Radar

2. Diagrama del Radar (Fig. 4.1). Este despliegue en tiempo real se refresca cada 15 segundos y muestra los distintos parámetros monitoreados. El eje en rojo indica un nivel alto de intentos de llamadas en alguna parte en la red.



3. Histograma Activo (Fig. 4.2). Este mapa despliega las 10 situaciones de mayor intento de llamadas en la red. Podemos apreciar inmediatamente en que Código de Punto (por lo tanto Central) se concentra él mas alto Intento de llamadas.

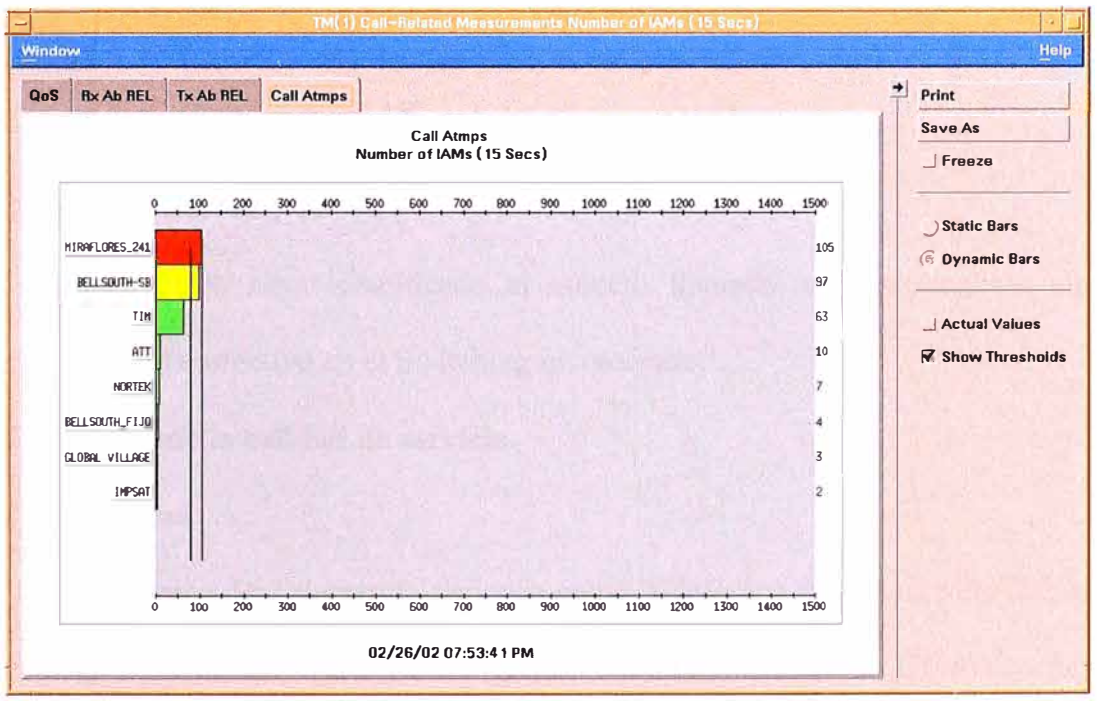


Fig. 4.2 Histograma Activo

4. Histograma de Series de Tiempo (Fig. 4.3). Este despliegue muestra un levantamiento de tráfico durante los 60 minutos anteriores.

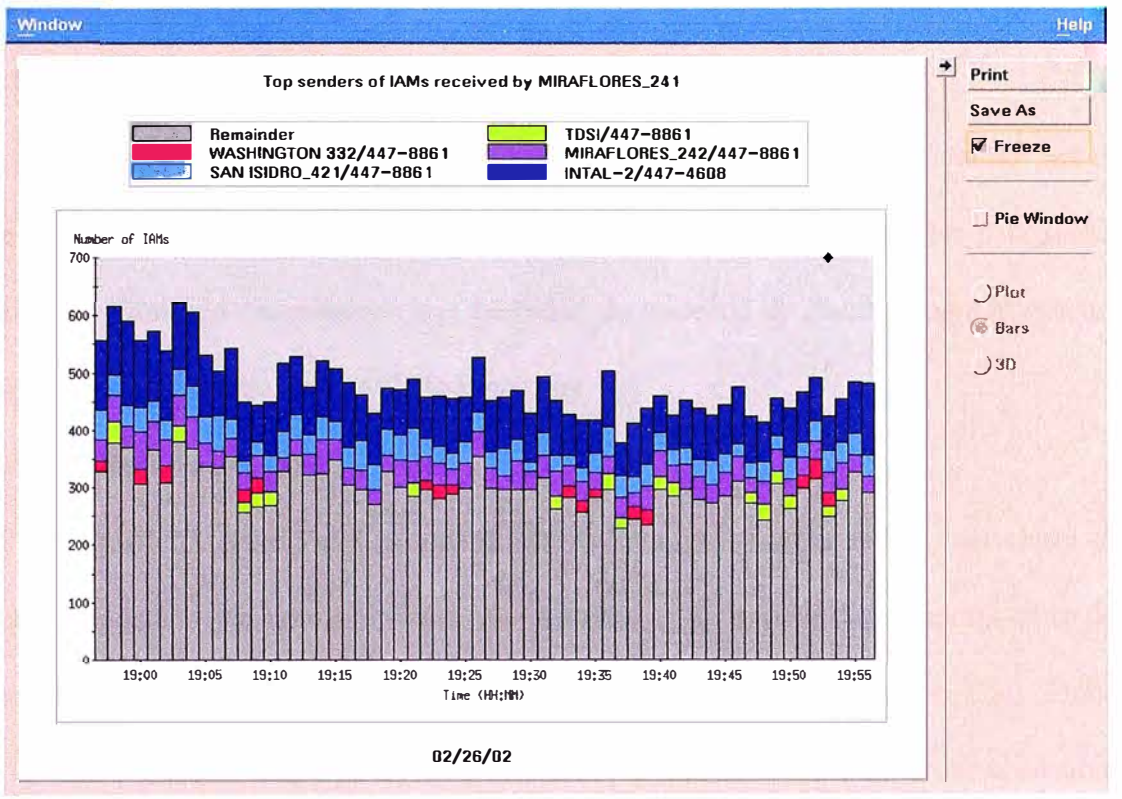


Fig. 4.3 Histograma de Series de Tiempo

4.1.4 Acción Correctiva

Cuando ya se haya identificado al número llamado, debemos aplicar algún procedimiento correctivo en el Switching involucrado.

4.2 Asegurando la calidad de servicio.

4.2.1 Problema

Una Empresa de Telecomunicaciones como Telefónica tiene acuerdos firmados con otros Operadores para que estas realicen transito por la red de Telefónica. En el caso de llamadas de Larga Distancia la competencia es con los Operadores de Larga

Distancia. Para mantenerse competitivo debemos asegurar una alta calidad de servicio, para esto debemos ser capaces de resolver los problemas antes de que estos afecten al cliente (abonado).

4.2.2 Solución

Para mantener una alta calidad de servicio, necesitamos monitorear la red en tiempo real para prevenir cuando los clientes son incapaces de hacer las conexiones exitosas. También necesitamos una facilidad de traceado de llamada para ayudarnos a averiguar por dónde está pasando y por qué.

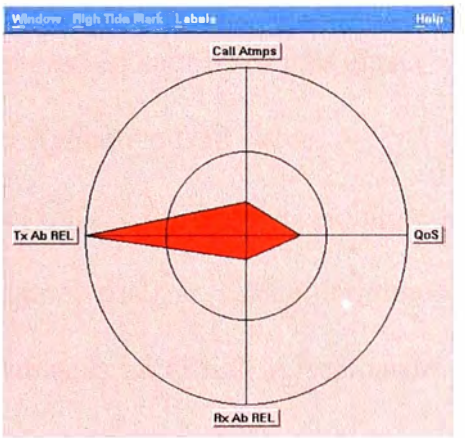
4.2.3 Aplicando acceSS7

El Traffic Monitor realiza un monitoreo continuo de la red y nos alerta de cualquier desviación anormal como las liberaciones al realizar llamadas. Al tanto del problema investigamos la causa y podemos utilizar la aplicación Call Trace, poderoso para descifrar mensajes relacionados a una llamada específica, a un nivel bien detallado.

1. Dentro de 15 segundos es refrescado el Monitor de Trafico y un umbral prefijado si es excedido en cualquier parte en la red se torna en color rojo.

2. Diagrama del Radar (Fig. 4.4). Esto muestra inmediatamente la causa de la alarma, un gran número de mensajes de Liberaciones anormales transmitidas son detectados en alguna parte en la red. Esto significa que muchas llamadas están fallando y los clientes estarán teniendo problemas.

Fig. 4.4 Diagrama Radar



3. Histograma Activo (Fig. 4.5). Este muestra, en el orden descendente, los códigos de punto que transmiten las liberaciones anormales. El Histograma Activo muestra claramente la magnitud relativa del problema.

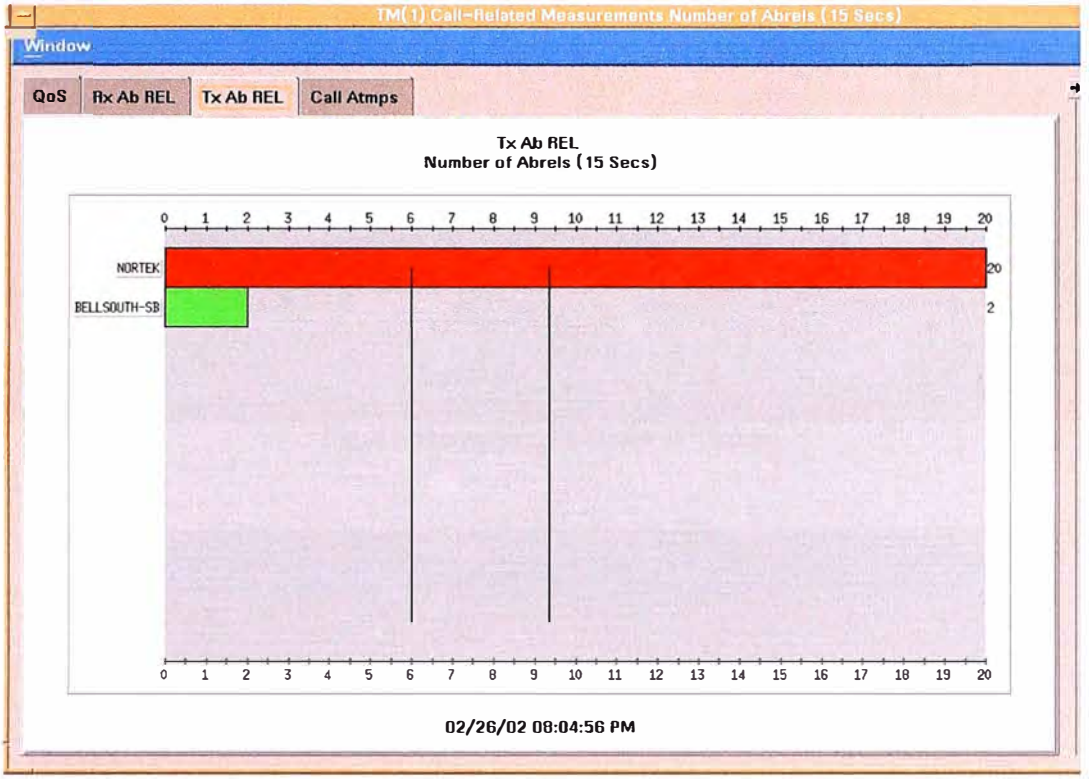


Fig. 4.5 Histograma Activo

4. Histograma de Series de Tiempo (Fig. 4.6). Este muestra la actividad durante la hora anterior. La leyenda muestra los destinos de liberación anormales más altas.

Para realizar un análisis más preciso utilizamos el Aplicativo Call Trace.

5. Call Trace (Fig. 4.7). Primero seleccionamos el Link. Esto limita el monitoreo de la llamada y nos da los datos precisos que necesitamos analizar. Luego definimos como numero llamado "-" para rastrear todas las llamadas en el link seleccionado. Esto displaya las causas de liberación como el tiempo de las llamadas, así podemos notar el factor común de las llamadas anormales.

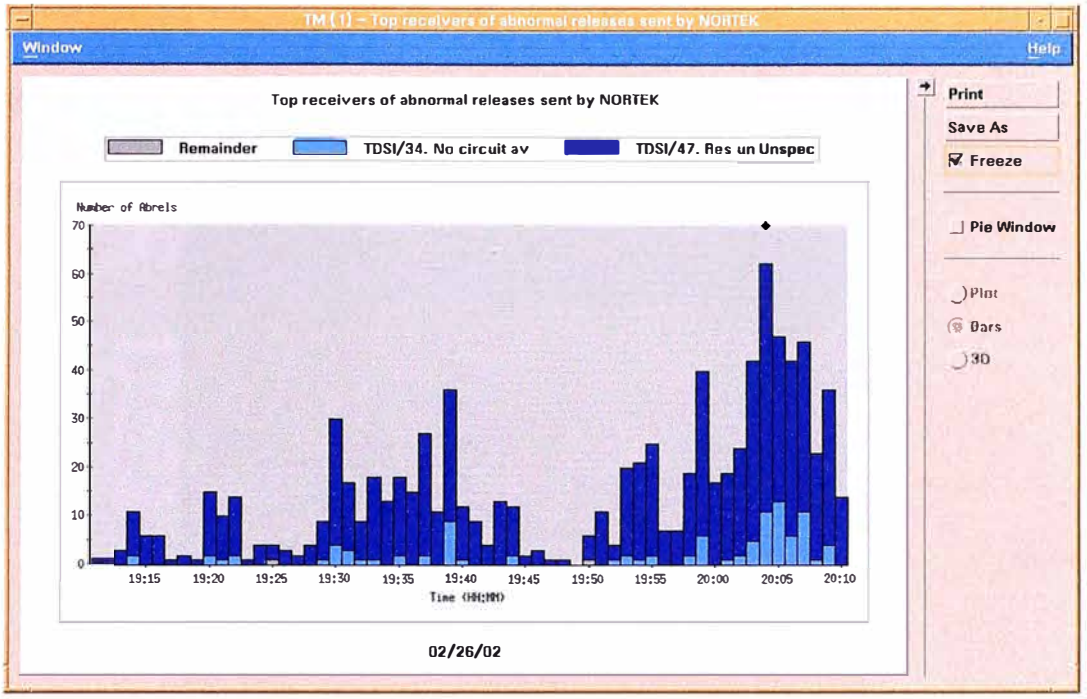


Fig. 4.6 Histograma de Series de Tiempo

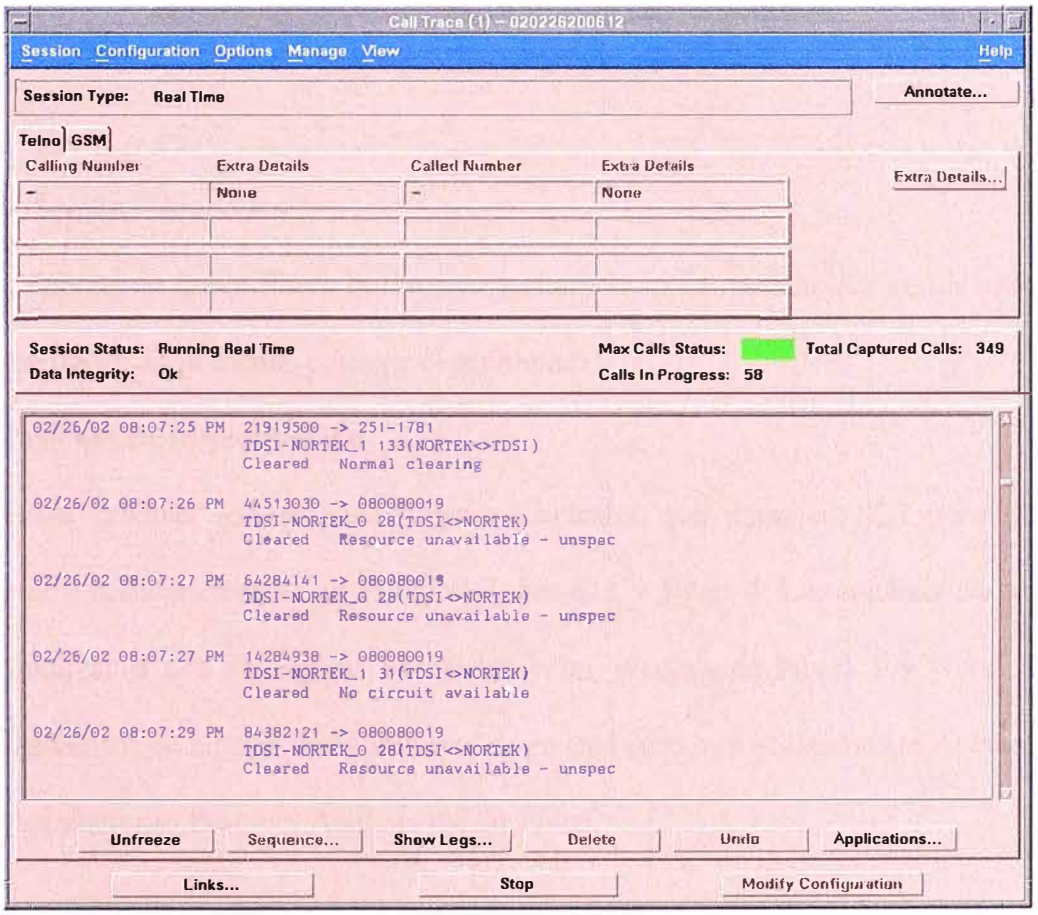


Fig. 4.7 Call Trace

6. Sequence Diagram Display (Fig. 4.8). Esta es la representación gráfica de la llamada y nos muestra quien Libera la llamada.

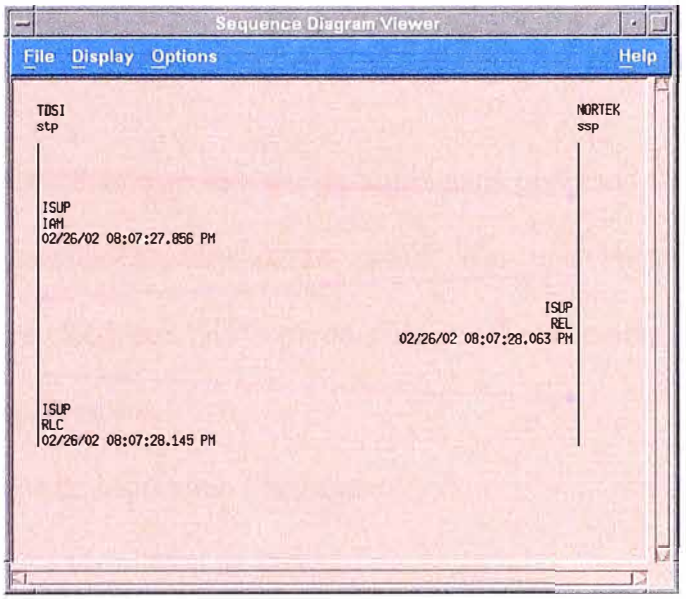


Fig.4.8 Sequence Diagram Display

4.2.4 Acción Correctiva

Conociendo quien libera la llamada y analizando los parámetros en los mensajes de una llamadas podemos corregir el problema.

4.3 Pruebas de interconexión

Estas pruebas son realizadas entre Centrales que manejen SS7 para ello es necesario realizar pruebas en el Nivel 2, Nivel 3 y Nivel 4. Las pruebas de Nivel 2 son realizadas por un equipo Emulador y las pruebas de Nivel 3 y Nivel 4 son realizadas por un equipo de Monitoreo, es en este caso que utilizamos el Access7 con sus Aplicaciones Protocol Análisis y Call Trace.

CONCLUSIONES

Como conclusión de este Informe de Suficiencia podemos añadir que las grandes Redes de Telecomunicaciones deben contar con una buena Configuración de Señalización en su Red, con STP's puros, para poder concentrar la mayor cantidad de links en los Sites Remotos.

Estos sistemas de Monitoreo Facilitan:

- Una completa visibilidad de la Red.

- Presentan relaciones complejas de señalización en formatos amistosos.

- Permiten analizar problemas en la red a través de históricos.

- Entregan valores inmediatos en base a reportes preconfigurados.

- Estos sistemas son independientes ya que están disponibles bajo sobrecarga de red y condiciones de falla de los Switches.

- Estos sistemas ahora soportan el monitoreo de IP y enlaces de alta velocidad.

Por lo tanto el análisis de los resultados de las aplicaciones mejora notablemente la Calidad del Servicio.

ANEXOS

A. ACRÓNIMOS

CCS	Señalización por Canal Común
CCSSO	Oficina de Conmutación con Señalización por Canal Común
CDR	Registro Detallado de Llamada
ESN	Número Serial Electrónico
GPS	Sistema de Posición Global
GSM	Sistema Global para móviles
HP	Hewlett Packard
HP-UX	Sistema Operativo Unix de HP
IMEI	Identificador del equipo Terminal Móvil Internacional
IMSI	Identificador del abonado Móvil Internacional
ISO	Organización Internacional de Estándares
ISUP	Parte de Usuario de RDSI
LAN	Red de Área Local
LMSI	Identificador del Terminal Móvil Local
MIN	Número de Identificación del Móvil
MMI	Interfase Hombre Maquina
MPA	Analizador de Protocolo Multicanal
MSISDN	Terminal Móvil Internacional ISDN
MTP	Parte de Transferencia de Mensajes
OSI	Sistemas de Interconexión Abiertos
PCI	Interconexión de Componentes Periféricos
RI	Red Inteligente
SCCP	Parte de Control de la Conexión de Señalización
SCP	Puntos de Control de Servicio
SNM	Gestión de la Red de Señalización
SP	Punto de Señalización
SS7	Sistema de Señalización N° 7
SSP	Punto de Conmutación de Servicio
STP	Punto de Transferencia de Señalización
TCAP	Parte de Aplicación Orientada a Transacciones
TCP/IP	Protocolo de Control de Transmisión / Protocolo de Internet
TMSI	Identificador del abonado Móvil Temporal
TUP	Parte de Usuario de Telefonía
WAN	Red de Área Extendida

BIBLIOGRAFÍA

[1] **HP acceSS7 Signaling Monitoring System,** (Software release B.06.00)

[2] **QUEST7 Introduction**, NETTEST/QUEST7/SDOC/0010 V. 1.0

[3] **Presentaciones Propietarias (GeoProbe),** INET

[4] **TeleCom Standards Collection T1.2.3,** Information Handling Services

[5] **J.M. Huidobro** - Redes de comunicaciones - Paraninfo, Madrid 1991

[6] **CCITT/UIT-T**
Recomendación Serie I: Red Digital de Servicios Integrados.
Recomendación Serie H: Transmisión de señales no telefónicas.

[7] **M. Schwartz - Telecommunication networks, protocol modeling and analysis** - Addison Wesley 1988 (versión española en Addison Wesley Iberoamericana)

[8] **Telecommunications Protocols (McGraw-Hill Series on Telecommunications)** by Travis Russell

[9] **Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (3th Edition)** by Douglas Comer

Páginas Web de Referencia:

[10] Performance Technologies http://www.pt.com/tutorials/ss7

[11] AcceSS7 http://www.acceSS7.com

[12] Agilent http://www.agilent.com

[13] Inet http://www.inet.com

[14] International Telecommunication Union http://www.itu.int

[15] American National Standards Institute http://www.ansi.org/