

Nodos de soporte de GPRS

Lars Ekeröth y Per-Martin Hedström

Las telecomunicaciones y la comunicación de datos están convergiendo, debido en una parte no pequeña al papel cada vez más prominente del protocolo de Internet (Internet Protocol - IP). Además, los usuarios quieren acceso a Internet mientras están fuera de sus oficinas y hogares.

Los servicios de conmutación de paquetes presentan nuevas oportunidades para los operadores y usuarios. Permiten a los operadores sacar partido del rápido crecimiento del uso de Internet y situar el servicio celular como acceso móvil a Internet. La introducción del servicio general de paquetes de radio (General Packet Radio Service - GPRS) en las redes celulares de hoy día es un paso clave en la evolución hacia las redes móviles de tercera generación.

GPRS hace móvil a Internet. Permite a los usuarios acceder a intranets corporativas o a proveedores de servicios de Internet (Internet Service Providers - ISP) desde un dispositivo móvil. Sus usuarios pueden permanecer en línea sin ocupar continuamente un canal de radio específico. Cada canal está compartido por varios usuarios y se usa solamente cuando se envían o reciben los paquetes de datos.

En este artículo, los autores describen los nodos de soporte de GPRS (GPRS Support Nodes - GSN) de Ericsson—los nodos de la red nuclear en el corazón de la solución GPRS de Ericsson que proporcionan capacidad de paquetes de datos a las redes celulares GSM, UMTS y TDMA.

Introducción

Nodos de soporte de GPRS

Los nodos de soporte de GPRS constituyen las partes de la red del sistema celular de Ericsson que conmutan los paquetes de datos. Los dos nodos principales son el nodo servidor de soporte de GPRS (Serving GPRS Support Node - SGSN) y el nodo de soporte pasarela de GPRS (Gateway GPRS Support Node - GGSN).

y el nodo de soporte pasarela de GPRS (Gateway GPRS Support Node - GGSN). La Figura 1 muestra un ejemplo de la arquitectura de la solución GPRS de Ericsson en una red celular GSM. Los GSN se usan también para dominios de GPRS dentro de un sistema UMTS ó TDMA.

La plataforma ha sido diseñada con redundancia de hardware y software, lo que permite a los operadores actualizar módulos individuales sin perturbar el tráfico. Toda vez que los dispositivos que transportan la carga útil y los dispositivos de control se mantienen separados en la plataforma, las actualizaciones de software solamente suelen tener un efecto mínimo sobre la transferencia en curso de carga útil del usuario final. Además, la redundancia n+1 de hardware de la plataforma hace posible actualizar la mayor parte de los dispositivos de hardware sin afectar al tráfico.

Funcionalidad

Los SGSN encaminan paquetes a y desde la zona geográfica del SGSN, en tanto que los GGSN hacen interfaz con redes externas de paquetes IP. Los SGSN y los GGSN están físicamente separados de la parte de circuitos conmutados de la red nuclear del sistema celular de Ericsson.

La funcionalidad de los SGSN y los GGSN puede ser combinada en el mismo nodo físico (nodo combinado de soporte de GPRS - Combined GPRS Support Node - CGSN) o residir en diferentes nodos físicos. Tanto el SGSN como el GGSN contienen funciones de encaminamiento de protocolo de red principal GPRS (IP), y pueden ser interconectados con encaminadores IP.

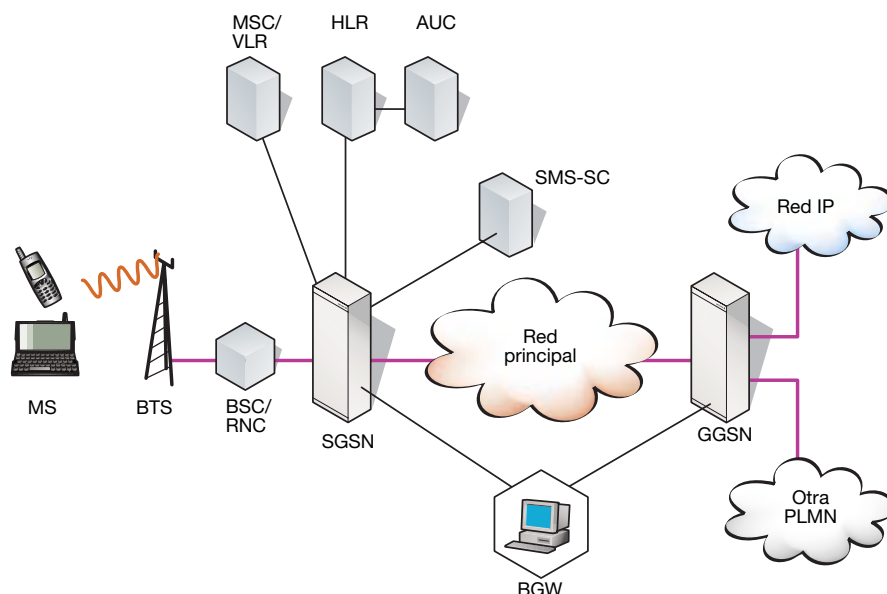
En otros aspectos, la arquitectura de GPRS de Ericsson usa los elementos de red celular existentes, tales como las bases de datos de abonados y los sistemas de transmisión por radio.

Arquitectura

Los GSN están basados en la plataforma inalámbrica de paquetes (Wireless Packet Platform - WPP), una nueva plataforma de conmutación de paquetes de propósito general y altas prestaciones. La WPP, que se usa para GPRS, EDGE y UMTS, combina características usualmente asociadas con las comunicación de datos (tales como su estructura compacta y su alta funcionalidad) con características de las telecomunicaciones (tales como la robustez y la escalabilidad).

La solución de middleware de Ericsson consta de componentes orientados a objetos que usan la arquitectura común de agente de petición de objetos (Common Object-Request Broker Architecture - CORBA) y el lenguaje de definición de Internet (Interface Definition Language - IDL). También se usan CORBA e IDL para hacer interfaz con la capa de aplicación. La solución proporciona un marco para la construcción de aplicaciones robustas de tiempo real para procesar transacciones en entorno multiproce-

Figura 1
Visión de conjunto de la red nuclear de paquetes de datos de Ericsson en un sistema GSM.



sador distribuido usando módulos de software escritos en in C/C++, Java, o Erlang (Figura 2).

Componentes y características de GSN

Nodo servidor de soporte de GPRS

El SGSN es un componente primario de las redes celulares que emplean GPRS. Mediante la red de radio, el SGSN encamina los paquetes IP entrantes y salientes dirigidos a o procedentes de cualquier abonado de GPRS físicamente situado dentro de la zona geográfica a la que da servicio ese SGSN. Cada SGSN proporciona

- cifra (cifrado y descifrado) y autenticación;
- gestión de sesión y preparación de las comunicaciones al abonado móvil;
- gestión de movilidad—esto es, soporte para itinerancia y traspaso dentro de y entre redes móviles;
- gestión del enlace lógico al abonado móvil; y

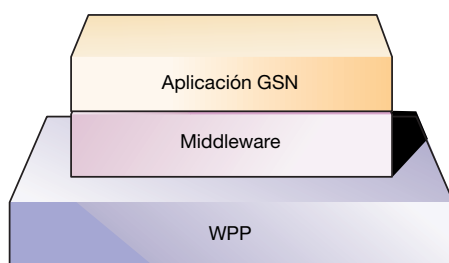


Figura 2
La arquitectura GSN .

CUADRO A, TÉRMINOS Y ACRONIMOS

3GPP	Third-generation Partnership Project	HTML	Hypertext markup language	PASOS	Packet-switched operation support system
AAL5	ATM adaptation layer 5	HTTP	Hypertext transfer protocol	PCI	Peripheral component interconnect
AP	Application processor	IBAM	155 Mbit/s interface for ATM providing a PMC module for multimode fiber	PDCH	Packet data channel
AP/C	Application processor control	IBE1	E1 interface board with a PowerPC processor and E1 PMC modules	PDP	Packet data protocol
APN	Access point name	IBEN	Ethernet interface board with a PowerPC processor and Ethernet PMC modules	PDU	Packet data unit
ASN.1	Abstract syntax notation one	IBT1	E1 interface board with a PowerPC processor and T1 PMC modules	PEB	Power and Ethernet board
ATM	Asynchronous transfer mode	ICMP	Internet control message protocol	PLMN	Public land mobile network
BER	Basic encoding rules	IDL	Interface definition language	PMC	PCI mezzanine card
BG	Border gateway	IIOF	IP-based inter-ORB protocol	PPP	Point-to-point protocol
BGP	Border gateway protocol	IMEI	International mobile equipment identity	PTM	Point-to-multipoint
BNSI	Basic network surveillance interface	IMSI	International mobile subscriber identity	PVC	Permanent virtual circuit
BSC	Base station controller	IP	Internet protocol	PXM	Packet exchange manager
CGF	Charging gateway function	IPsec	IP security protocol	QoS	Quality of service
CGSN	Combined GSN	ISP	Internet service provider	RADIUS	Remote access dial-in user service
CORBA	Common object request broker architecture	L1, L2, L3	Layer 1, layer 2, layer 3	RANAP	Radio access network application part
cPCI	Compact PCI	LCT	Local craft terminal	RD	Resource deployment
DES-CBC	Data Encryption Standard, cipher block chaining (USA)	LDAP	Lightweight directory access protocol	RIP	Routing information protocol
DHCP	Dynamic host configuration protocol	LLF	Link layer forwarding	SCCP	Signaling connection control part
DP	Device processor	MAC	Medium access control	SCF	Software configuration file
DPE	Distributed process environment	MAP	Mobile application part	SGSN	Serving GSN
E1	ETSI 2 Mbit/s interface	MD5	Message digest algorithm 5	SMS	Short message service
E3	ETSI 34 Mbit/s interface	MIB	Management information base	SMS-GMSC	SMS gateway MSC
EIR	Equipment identity register	MSC	Mobile switching center	SMS-IWMSC	SMS interworking MSC
EM	Element manager	MTP	Message transfer part	SNMP	Simple network management protocol
ESP	Encapsulating security payload	NCS	Network control system	SS7	Signaling system no. 7
ETSI	European Telecommunications Standards Institute	NE	Network element	T1	ANSI 1.5 Mbit/s interface
FPGA	Field programmable gate array	NOC	Network object control	T3	ANSI 45 Mbit/s interface
FTP	File transfer protocol	O&M	Operation and maintenance	TC	Traffic control
GGSN	Gateway GSN	ORB	Object request broker	TCAP	Transaction capabilities application part
GMM	GPRS mobility management	OSPF	Open shortest path first	TCP	Transmission control protocol
GPB	General processor board	OTP	Open telecom platform	TDMA	Time-division multiple access
GPRS	General packet radio service			UDP	User datagram protocol
GSN	GPRS support node			UMTS	Universal mobile telecommunications system
GUI	Graphical user interface			WPP	Wireless packet platform
HLR	Home location register				

- conexión a otros nodos (HLR, MSC, BSC, SMS-GMSC, SMS-IW/MSC, GGSN).

El SGSN recopila también los datos de tarificación para cada abonado móvil, tales como el uso real de la red de radio y de los recursos de la red GPRS.

Nodo de soporte pasarela de GPRS

El GGSN es también un componente primario de redes celulares que emplean GPRS. El GGSN sirve de interfaz con las redes externas de paquetes IP, accediendo a funciones externas de ISP tales como encaminadores y servidores de servicio de usuario de marcación con acceso remoto (Remote Access Dial-In User Service - RADIUS). En términos de la red IP externa, el GGSN encamina las direcciones IP de los abonados servidos por la red GPRS, intercambiando información de encaminamiento con la red externa.

En el GGSN de Ericsson, una pasarela fronteriza (Border Gateway - BG) comparte las interfaces físicas de GGSN a redes externas y a la red principal. Una pasarela fronteriza puede manejar múltiples redes terrestres móviles públicas (Public Land Mobile Networks (PLMN)).

La GGSN prepara la comunicación con redes externas y gestiona las sesiones de GPRS. También incluye funciones para asociar abonados con la SGSN apropiada. Para cada abonado móvil, el GGSN recopila también datos de tarificación—uso de la red de datos externos y uso de los recursos de la red GPRS.

Encaminador de IP

Cada GSN de Ericsson tiene un encaminador integrado que

- sirve como encaminador de IP primario o secundario IP en redes IP, aunque solamente de forma temporal—se recomienda encarecidamente un encaminador IP más grande para dirigir a otras redes IP; y
- proporciona redundancia para la interfaz *Gn/Gi*.

El encaminador soporta abrir primero el camino más corto (Open Shortest Path First - OSPF) y el protocolo de pasarela fronteriza (Border Gateway Protocol - BGP), así como otros protocolos de encaminamiento. También puede filtrar paquetes IP en todas las interfaces IP—por ejemplo, desde una PLMN a otra. El filtro, cuyos datos de configuración pueden ser asignados durante la operación y mantenimiento (O&M), aplica a información de cabecera del protocolo de control de transmisión/protocolo de Internet (Transmission Control Protocol/Internet Protocol - TCP/IP), y una combinación de dirección IP de origen, dirección IP de destino, tipo de protocolo, señales TCP, tipo de mensaje del protocolo de mensajes de control de Internet (Internet Control Message Protocol - ICMP), puerto de origen de TCP / protocolo de datagrama de usuario (User Datagram Protocol - UDP), y puerto de destino TCP/UDP e interfaz física.

Tarificación

Como se mencionó anteriormente, tanto el SGSN como el GGSN pueden producir registros de datos de tarificación. Combinado con un dispositivo mediador, tal como la Pasarela de Facturación (Billing Gateway) de Ericsson, esto da a los operadores una amplia abanico de opciones. La tarificación puede estar basada en volumen de datos, duración de la llamada, tipo de servicio, punto de destino, o algún otro factor.

El Instituto Europeo de Estándares de Telecomunicaciones (European Telecommunications Standards Institute - ETSI) ha especificado tanto una alternativa centralizada como una distribuida para la función de pasarela de tarificación (Charging Gateway Function - CGF). En la solución de Ericsson, las CGF básicas están distribuidas y las CGF perfeccionadas están centralizadas.

Las CGF básicas—recopilación, almacenamiento y transferencia de datos de tarificación—están implementadas en los GSN. Los registros de datos de tarificación se almacenan en memorias tampón en los nodos, lo que proporciona una mayor seguridad contra problemas de la red o de transmisión. La salida de datos de tarificación procedente de los SGSN y los GGSN se codifica con la Notación uno de sintaxis abstracta / Reglas básicas de codificación (Abstract Syntax Notation one / Basic Encoding Rules - ASN.1/BER) y se transfiere mediante el protocolo de transferencia de archivos (File Transfer Protocol - FTP) usando un mecanismo o bien de empuje o bien de tirón.

Las CGF perfeccionadas—consolidación, filtrado, preproceso y formateo de los registros de datos de tarificación—están implementadas centralmente en la Pasarela de Facturación de Ericsson. La centralización reduce el número de interfaces al sistema de facturación y proporciona diversas opciones de postproceso. Además, el almacenamiento en medios masivos es mejor que el almacenamiento distribuido en GSNs.

Asignación de direcciones IP

Direcciones IP dinámicas

La asignación de direcciones IP dinámicas permite a los operadores, a los ISP, y a las redes corporativas reutilizar las direcciones IP desde un fondo común asignado a la PLMN o alguna otra red. También reduce de forma significativa el número total de direcciones IP requerido por PLMN.

Una dirección IP dinámica puede ser asignada por un GGSN o a través de él en la red visitada o por un GGSN en la red propia. La dirección IP dinámica puede ser proporcionada por el GGSN mismo o por un servidor RADIUS elegido por el GGSN.

El GGSN contiene un cliente RADIUS que suministra al servidor RADIUS externo información de autenticación procedente del abo-

nado móvil. Por lo tanto, el servidor RADIUS puede devolver una dirección IP si la autenticación es correcta. La configuración puede especificar que el GGSN debe ponerse en contacto con un servidor RADIUS específico para cada nombre del punto de acceso (Access Point Name - APN)—esto es, cada red corporativa o ISP. El servidor RADIUS puede estar situado o bien en el ISP o en un sitio corporativo. El GGSN incluirá también un cliente de protocolo dinámico de configuración de anfitrión (Dynamic Host Configuration Protocol - DHCP). El GSN de Ericsson soporta también la superposición de direcciones IP privadas.

Direcciones IP estáticas

No se recomienda el uso de direcciones IP estáticas, principalmente debido a una escasez de direcciones IP (esta situación cambiará cuando se introduzca IPv6). La dirección IP estática es definida para el abono por el HLR—como opción, se puede contactar con un servidor RADIUS con fine de autenticación. Cuando el terminal está en el estado de conectado, las direcciones IP del abonado se copian al SGSN. De acuerdo con esto, cuando envía una petición de activación de contexto de protocolo de datos en paquetes (Packet Data Protocol - PDP), el terminal

- proporciona una dirección IP—que se comprueba con la información del abono; o
- permite al SGSN asignar la dirección IP—siempre y cuando el abono contenga solamente una dirección IP.

Funciones de seguridad en los GSN

Seguridad en los SGSN

La autenticación se lleva siempre a cabo para la conexión y para actualizaciones de área de encaminamiento entre SGSNs, tanto para los abonados propios como para los visitantes. Se mantiene un registro de anotaciones de intentos de autenticación fallidos. Dicho registro contiene la fecha y la hora, y la identidad internacional de abonado móvil (International Mobile Subscriber Identity - IMSI), la identidad internacional de equipo móvil (International Mobile Equipment Identity - IMEI), la ID de SGSN y la identidad de la célula de los abonados móviles o de los aparatos cuya autenticación falló.

El GSN soporta valores de autenticación selectivos para todos los abonados de la red propia en el nodo. Dichos valores dictan el número de procedimientos de conexión y los procedimientos de actualización de área de encaminamiento entre SGSNs o internos de un SGSN que se pueden producir entre cada procedimiento de autenticación. La autenticación se lleva siempre a cabo para los abonados visitantes.

Las tripletas de seguridad se traen desde el HLR. Sin embargo, para las actualizaciones de área de encaminamiento entre SGSN, se traen

tripletas que no se hayan usado desde el anterior SGSN (si se conoce).

Se pueden proporcionar conexiones seguras en la capa 1 (L1), usando una línea física dedicada; en la capa 2 (L2), usando modo asíncrono de transferencia (Asynchronous Transfer Mode - ATM) circuitos virtuales permanentes (Permanent Virtual Circuits - PVC), PVC de relé de tramas, o el protocolo punto a punto (Point-to-Point Protocol - PPP); y en la capa 3 (L3), usando seguridad de IP (IP security - IPsec). Estas técnicas se pueden usar también en combinación.

Seguridad en los GGSN

El GGSN garantiza que el tráfico para un abonado móvil específico viene del ISP al que dicho abonado móvil estaba conectado durante la ac-

CUADRO B, INTERFACES

Los estándares de ETSI y del Proyecto de Tercera Generación en Colaboración (Third-generation Partnership Project - 3GPP) especifican varias interfaces lógicas a y desde GSNs. Algunas de estas se describen a continuación (ver también la Figura 3).

Interfaz	Usada para
<i>Gn</i> y <i>Gp</i>	señalización de control (para gestión de movilidad y de sesión) entre los SGSNs y los GGSNs, y tunelado de cargas útiles de usuario final en la red principal.
<i>Iu</i>	transporte de tráfico entre la red nuclear y la red de radio. Señalización de control SGSN entre la red de radio y la red nuclear. (El protocolo RANAP, transportado sobre SCCP/MTP3-B/SSCF/SSCOP/AAL5/ATM, se usa sobre esta interfaz para soportar señalización de gestión de movilidad y de sesión entre los terminales móviles y la red nuclear.)
<i>Gb</i>	señalización SGSN con los BSC en redes de acceso de paquetes GSM o TDMA.
<i>Gi</i>	transporte de datos IP de usuario final entre la red móvil y redes IP externas, y señalización de control GGSN con servidores de ISP situados en redes IP (incluyendo autenticación de usuario final y asignación de dirección IP mediante RADIUS).
<i>Gr</i>	señalización MAP para soportar el almacenamiento y recuperación de datos de abonado entre el SGSN y el HLR.
<i>Gd</i>	señalización MAP para soportar el servicio SMS sobre canales de radio de conmutación de paquetes entre el SGSN y el SMS-C.
<i>Gm</i>	señalización entre el PTM-SC, el GGSN, y el SGSN, y transporte de mensajes entre estos nodos después de que haya sido hecha una petición por parte de la aplicación del servidor PTM para enviar datos a un grupo con o sin filtrado geográfico. La interfaz Gm está siendo especificada en la actualidad por el 3GPP.
<i>Gf</i>	señalización MAP para soportar los procedimientos de comprobación de entre los servidores SGSN y EIR cuando un usuario se está conectando.
<i>Gs</i>	El servidor SGSN soporta la interfaz Gs estándar al servidor del MSC, a fin de proporcionar la gestión de movilidad para abonados que están conectados tanto a los canales de conmutación de paquetes como a los conmutación de circuitos. Estos procedimientos combinados cubren, por ejemplo, las actualizaciones de ubicación y los buscapersonas. Para TDMA, esta interfaz sirve para llevar mensajes de señalización ANSI a y desde la red GPRS (para transacciones que incluyen el registro, buscapersonas, e información de portador de teleservicio). La interfaz Gs se usa también para SMS, ya que TDMA no emplea la interfaz Gd.

tivación del contexto de PDP. El GGSN puede acceder a los servidores RADIUS que estén situados en la red de datos externa u operados por un ISP.

El GGSN proporciona una cabecera de autenticación IPv4 IPsec usando el algoritmo 5 de resumen de mensajes (Message Digest Algorithm five - MD5), y carga útil de seguridad de encapsulado (Encapsulating Security Payload - ESP) usando el modo de encadenamiento de bloques de cifra del estándar de cifrado de datos (Data Encryption Standard - Cipher Block Chaining - DES-CBC). El sistema está también preparado para la introducción de nuevos algoritmos de cifrado, tales como un protocolo de autenticación de clave pública asimétrica.

Se dispone de diversas opciones de filtrado de paquetes para proteger al GGSN contra la intrusión o los ataques con denegación de servicio, incluyendo origen, destino, protocolo, y número de puerto.

Seguridad para acceso a mantenimiento

Los comandos de mantenimiento son enviados desde el gestor de elementos a cargo del gestor de intercambio de paquetes (Packet Exchange Manager - PXM). El tunelado de IPsec protege el enlace al PXM.

Para evitar el acceso no autorizado, se asigna a los comandos de gestión para el elemento de red una de entre varias categorías de comandos. Se pueden definir perfiles individuales de ope-

rador con privilegios que operen en una o más categorías de comandos.

Los operadores deben identificarse con una contraseña para tener acceso a un conjunto de categorías de comandos específico preconfigurado. Se anotan todas las peticiones de servicio. Se puede tener acceso de solo lectura desde nodos externos—por ejemplo, para leer alarmas—mediante el protocolo simple de gestión de red (Simple Network Management Protocol - SNMP). El acceso está restringido debido a los fallos de seguridad de SNMP v1 y de la falta de bases de información de gestión (Management Information Bases - MIB) de SNMP estandarizadas para GPRS.

IPsec

IPsec es una característica opcional para las interfaces *Gi*, *Gn*, y *Gp* (Cuadro B). IPsec puede proporcionar una red principal intra-PLMN segura e interfaz a redes externas, tales como ISPs, redes corporativas, y otras PLMNs.

Gestión de la carga útil

Los paquetes se dividen en diferentes clases de retardo de QoS de acuerdo con una prioridad asignada. Dentro de un periodo de tiempo dado, todos los paquetes procedentes de una clase de retardo de QoS con alta prioridad se envían antes que los paquetes de una clase con una prioridad más baja. El tráfico a y desde abonados móviles con la misma clase de retardo de QoS se pueden poner en cola en de manera que el primero que entra es el primero que sale (First-In First-Out - FIFO).

Las situaciones de sobrecarga harán saltar una alarma. El SGSN descarta sistemáticamente las unidades de datos en paquetes (Packet Data Units - PDU) a fin de preservar niveles de QoS comprometidos: las PDU de QoS clase 1 toman precedencia sobre las PDU de clase 2, y así sucesivamente.

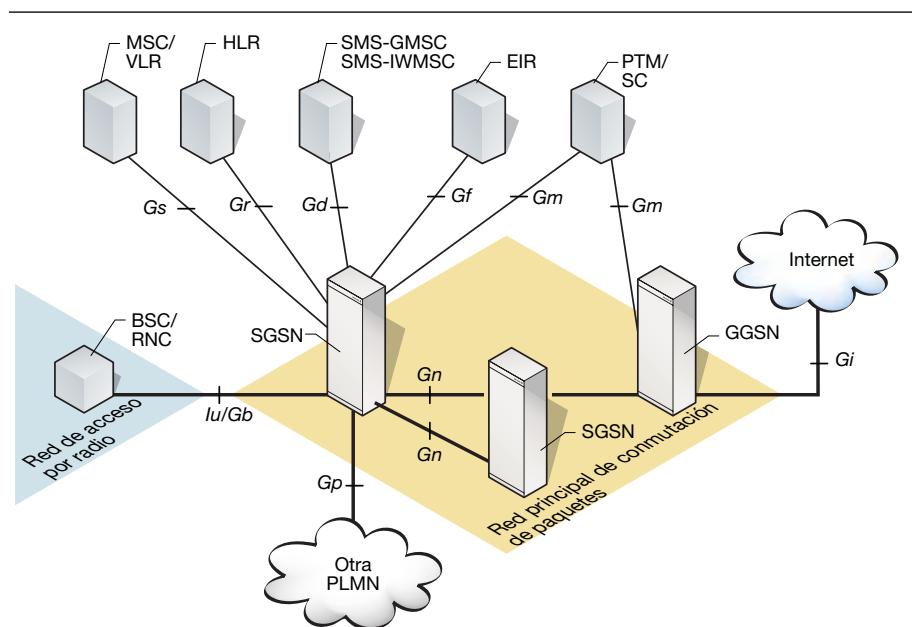
Calidad de servicio

El perfil de QoS de GPRS está basado en el estándar 03.60 de GSM. Sin embargo, solamente se soportan las clases de fiabilidad 2 y 3, porque son adecuadas para datos IP. De forma similar, solamente se soportan las clases de retardo 1 a 4 para datos de abonado.

El SGSN aplica una función de control de admisión a cada petición de activación de contexto de PDP. La función tiene como resultado un procesamiento adicional de la petición, la negociación de la QoS con el abonado móvil, o el rechazo de la petición de activación de contexto de PDP.

El SGSN negocia la QoS con el abonado móvil cuando no se puede dar soporte al nivel solicitado por el abonado o cuando el nivel de QoS negociado desde el anterior SGSN no se puede soportar en una actualización de área de encaminamiento entre SGSNs. La respuesta del abona-

Figura 3
Interfaces de la red nuclear de conmutación de paquetes.



do móvil depende de los datos de abonado almacenados, la QoS solicitada, y el ancho de banda estadísticamente promediado para cada célula.

Una petición de un nivel de QoS específico podría ser rechazada cuando el número de abonados conectados simultáneamente a un SGSN en particular exceda un límite predefinido.

Plataforma inalámbrica de paquetes

El software para el GSN corre en la plataforma inalámbrica de paquetes (Wireless Packet Platform - WPP), que es una plataforma combinada de procesador y comunicaciones diseñada para soportar productos de Internet móvil (Figura 4). El software consta de middleware y de la aplicación GSN.

Descripción general

La WPP está construida en torno a un panel de fondo que proporciona un plano de cableado trasero redundante de Ethernet para la comunicación entre procesadores y una fuente de alimentación duplicada a todas las placas de circuitos. El conmutador de Ethernet redundante proporciona Ethernet totalmente conmutada con un total de 100 Mbit/s a cada posición de placa de circuito.

La distribución de energía del armario proporciona una alimentación de energía duplicada de 48V a cada cajetín. La alimentación de energía a cada posición de placa de circuitos del cajetín es distribuida por dos unidades de placas de energía y Ethernet (Power and Ethernet Board - PEB) a cada lado del cajetín. Cada unidad PEB contiene también un conmutador Ethernet.

Múltiples cajetines pueden ser conectados uno a otro usando un enlace Ethernet de 1 gigabit duplicado. Cada cajetín está equipado con un ventilador para forzar la refrigeración.

Placas de circuitos de la WPP

Las placas de circuitos que se usan en la WPP están diseñadas para acomodar el uso de componentes estándar, incluyendo la mejora de la total redundancia y del soporte de calidad propia de las telecomunicaciones. Cada placa de circuito consta de tres partes: una placa de portadora, una placa de circuitos de módulo de interconexión de componentes periféricos compacta (Compact Peripheral Component Interconnect - cPCI), y módulos de entrapamientos con tarjeta PCI (PCI Mezzanine Card - PMC) (Figura 5). La arquitectura de las placas de circuito permite que se introduzcan múltiples placas fáciles y rápidamente combinando una placa portadora con diferentes placas de circuitos de módulo cPCI y módulos PMC.

La placa portadora proporciona acceso al panel trasero redundante de Ethernet y a la alimentación de energía. Gestiona el acceso duplicado a

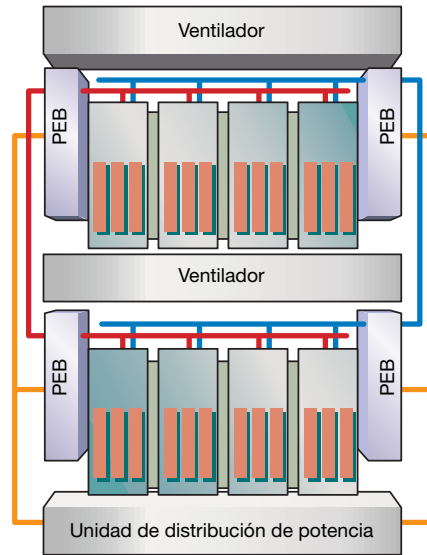


Figura 4
Armario de la WPP — vista esquemática.

Ethernet y oculta esta complejidad de los módulos PMC y de la placa de circuitos del módulo cPCI.

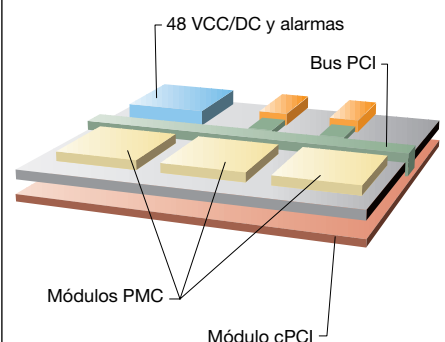
La placa de circuitos del módulo cPCI está montada como una placa hija en la placa portadora— si los volúmenes de producción son lo suficientemente grandes, la placa portadora y la placa de circuitos del módulo cPCI pueden ser también diseñadas como una sola unidad. La cPCI estándar da acceso a muchas placas de circuito confeccionadas.

Un bus cPCI proporciona acceso a la placa de circuito del módulo cPCI y a los módulos PMC. Los PMCs que usan cPCI son comunes en el mercado de los estándares abiertos. Proporcionan diferentes módulos de acceso a enlace y módulos de proceso. Varios módulos PMC pueden ser montados en la placa portadora (con cPCI). Un módulo especial PMC de conjunto de puertas programables sobre el terreno (Field Programmable Gate Array - FPGA) proporciona soporte de cifrado para carga útil móvil de GPRS e IPsec.

En la actualidad, se suministran dos tipos diferentes de placas de circuito en cinco configuraciones diferentes.

- GPB—una placa de procesador general que proporciona un procesador ultraSPARC con una unidad de disco duro en una de las posiciones del módulo PMC;
- IBEN—una placa de interfaz de Ethernet con un procesador PowerPC y módulos Ethernet PMC;
- IBAM—una interfaz de 55 Mbit/s para ATM que proporciona un módulo PMC para fibra multimodo;

Figura 5
Placa de circuito de la WPP—vista esquemática.



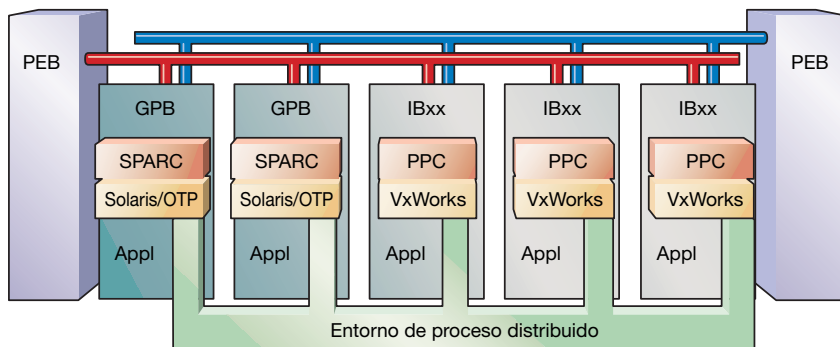


Figura 6
Entorno de Procesos Distribuidos (Distributed Process Environment - DPE).

- IBE1—una placa de interfaz E1 con un procesador PowerPC y módulos PMC E1; y
- IBT1—una placa de interfaz E1 con un procesador PowerPC y módulos PMC T1;

Se pueden agregar nuevos tipos de placas de interfaz cuando se necesiten. Las placas de interfaz que están en la actualidad en desarrollo o en el plan de investigación y desarrollo (Research and Development - R&D) incluyen interfaces para E3/T3, fibra de 155 Mbit/s en modo simple, interfaz eléctrica de 155 Mbit/s, e Ethernet de gigabit.

Todas las placas de circuito actuales requieren dos posiciones. Una nueva placa de interfaz que combina el módulo PowerPC de cPCI con una placa portadora está en desarrollo para proporcionar las mismas características con una sola posición de placa de circuitos.

Software de la WPP

Se suministran tres tipos diferentes de sistema operativo :

- Solaris (en los procesadores UltraSPARC) para tareas de control;
- Plataforma abierta de telecomunicaciones (Open Telecom Platform - OTP), para el soporte de la máquina virtual Erlang; y
- VxWorks (en los procesadores PowerPC), para características de tiempo real.

Además, se está desarrollando soporte de Java para los procesadores UltraSPARC.

Cada aplicación se ejecuta localmente en un procesador local y su sistema operativo. Para crear un sistema, los procesadores débilmente acoplados se mantienen juntos por medio de middleware de entorno de procesos distribuidos (Distributed Process Environment - DPE). El DPE soporta redundancia y la distribución de funciones, detecta fallos de la aplicación, y puede activar aplicaciones redundantes de diferentes maneras.

La plataforma soporta diversos protocolos para proporcionar acceso a redes de telecomunicacio-

nes tradicionales y a redes de comunicación de datos. Sobre las interfaces del nodo, la plataforma soporta el sistema de señalización número 7 (Signaling System No. 7 - SS7), relé de tramas, e IP. Las interfaces IP soportan total redundancia.

El conjunto de funciones de IP proporciona un encaminamiento de tránsito limitado, incluyendo soporte para OSPF, BGP, y el protocolo de información de encaminamiento (Routing Information Protocol - RIP). El acceso de IP a las aplicaciones se proporciona a través del encaminador lógico.

El GGSN requiere conexiones a numerosas intranets y a Internet. Las restricciones de direcciones de las redes IPv4 presentes se gestionan por lo general usando rangos de direcciones privadas con intranets corporativas. En consecuencia, el nodo ha sido diseñado para conectar muchas intranets que usan rangos de direcciones en conflicto.

La plataforma soporta también interfaces básicas de O&M, para proporcionar acceso a redes existentes de telecomunicaciones y comunicación de datos. Se ha implementado un concepto de cliente ligero usando el lenguaje de hipertexto etiquetado (Hypertext Markup Language - HTML) y el protocolo inter-ORB de Internet basado en IP (IP-based Inter-ORB Protocol - IIOP) de CORBA para proporcionar gestión local y remota mediante navegadores de Web estándar y applets de Java.

Un agente SNMP proporciona acceso a sistemas de gestión de comunicaciones de datos estándar. Una interfaz básica de vigilancia de red proporciona acceso a los sistemas de gestión de fallos de Ericsson. Se dispone de una aplicación de gestión de fallos, al igual que de aplicaciones auxiliares que soportan la recopilación y el almacenamiento de datos de desempeño y tarificación .

Soporte de cifrado acelerado por hardware

El uso de las redes públicas de Internet o IP expone a los sistemas a riesgos de seguridad. Además, el uso de sistemas inalámbricos móviles expone a los sistemas a las escuchas furtivas y a riesgos de seguridad en la información. Para neutralizar estos riesgos, la solución obvia parece ser el cifrado, tal vez aumentado mediante la autenticación. IPsec es el estándar de la industria para la transmisión de IP pero requiere procesamiento de alta capacidad tanto para el cifrado como para la autenticación. Para soportar IPsec, se ha desarrollado un módulo especial que contiene un circuito FPGA.

Todas las placas de circuitos de interfaz han sido diseñadas para incluir un módulo FGPA y dos módulos PMC. Para una interfaz de encaminador de IP, el módulo FPGA proporciona seguridad de IPsec. De forma similar, para una interfaz de relé de tramas, proporciona cifrado de abonado móvil—para la interfaz GPRS Gb.

Entorno de procesos distribuidos

Como se mencionó anteriormente, la plataforma inalámbrica de paquetes usa dos tipos de procesadores: el UltraSPARC y el PowerPC. El procesador UltraSPARC funciona con Solaris/OTP—una combinación muy adecuada para las tareas de transacción y control. El procesador PowerPC funciona con VxWorks, un sistema operativo de tiempo real que es muy adecuado para las tareas críticas de tiempo real.

Dependiendo de la arquitectura de las redes móviles futuras, los dos procesadores pueden funcionar al unísono, por ejemplo, en un servidor y nodo pasarela combinados, o aparte, como servidores o pasarelas separados.

El diseño de la aplicación puede ser independiente del número de procesadores diferentes usados en un configuración de nodo específica (Figura 6).

Funciones de middleware de DPE

El middleware de DPE mantiene juntos a los procesadores débilmente acoplados y soporta la aplicación con supervisión de procesos, distribución, redundancia, gestión de hardware, y actualizaciones de software. Todos los procesos son supervisados y un servicio de notificación informa a las aplicaciones de que una determinada aplicación se ha detenido.

El software se distribuye en el nodo por medio del DPE y un sistema de archivo de configuración de software (Software Configuration File - SCF), que emplea cuatro métodos de distribución de acuerdo con

- la placa de circuitos—los módulos de software pueden ser distribuidos a determinadas placas de circuitos. Por ejemplo, las aplicaciones que tienen que ver con el relé de tramas puede ser distribuidas a todas las placas de circuitos configuradas como placas de relé de tramas;
- el número de réplicas (instances)—el módulo de distribución puede especificar que un determinado número de réplicas de una aplicación de software deben ser hechos disponibles en el nodo;
- la posición de la placa de circuitos—los módulos de software pueden ser cargados sobre placas de circuitos que estén ubicadas en una posición particular del cajetín; y
- redundancia—la redundancia puede ser distribuida ya sea por dos casos particulares con una relación de reserva o de acuerdo con la redundancia n+1 con una en reserva para varias aplicaciones similares.

El DPE soporta tres tipos de redundancia. Con una reserva activa hay siempre dos aplicaciones cargadas; una está en activo y una en reserva activa. Hasta un cierto punto limitado, el DPE puede replicar los datos entre las dos aplicaciones. De acuerdo con la redundancia n+1, varias aplicaciones están en funcionamiento, y una aplicación de reserva se activa en el caso de que cualquiera de las aplicaciones falle. Finalmen-

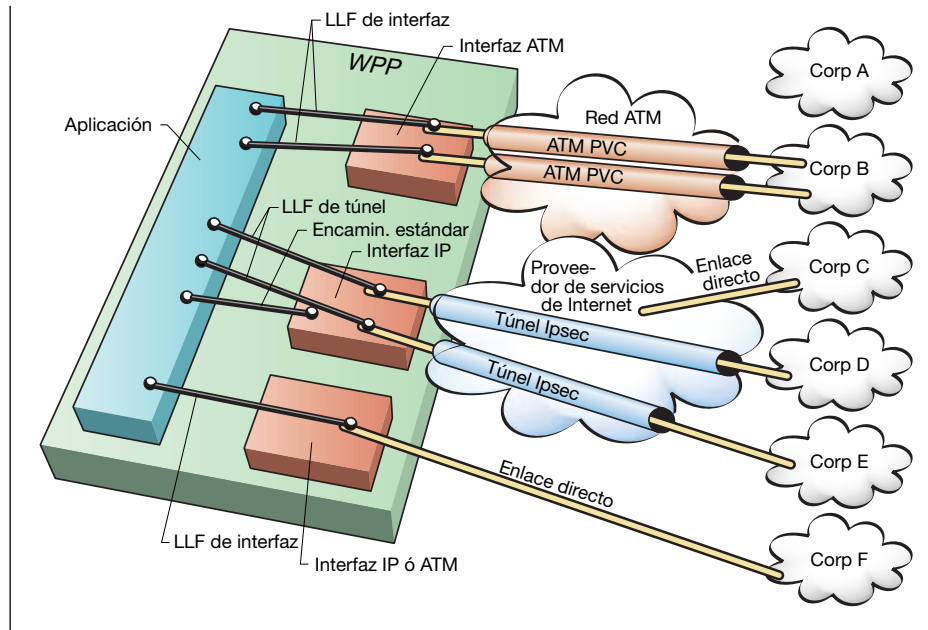


Figura 7
Encaminamiento lógico.

te, la distribución funcional se puede configurar para garantizar que siempre está disponible una réplica de una aplicación. Si falla una aplicación, el DPE activa una nueva réplica de la aplicación.

El DPE gestiona también los equipos, permitiendo la inserción de placas de circuitos “caliente”, y el intercambio de placas de circuitos controlado y sin control. Cualquier cambio en los equipos será causa de que se envíe una notificación a las aplicaciones, que entonces pueden redistribuir las funciones. Las funciones pueden volver a asignar las aplicaciones cuando se quiten las placas o fallen. También soportan plug-and-play, digamos, cuando se agrega una nueva placa de circuitos al nodo o se sustituye un circuito defectuoso por uno nuevo.

El DPE soporta actualizaciones sin complicaciones así como la gestión controlada de parches para correcciones de emergencia. Su soporte a la aplicación es el mismo, independientemente de si la aplicación se ejecuta en un procesador UltraSPARC o PowerPC. Por lo tanto, las aplicaciones no necesitan ser adaptadas a diferentes tamaños de configuraciones de nodos.

Encaminadores lógicos

Los nodos de gestión de paquetes tratan diferentes tipos de aplicaciones que usan IP. Por lo general surgen conflictos de direcciones cuando una plataforma basada en IP se conecta a nu-

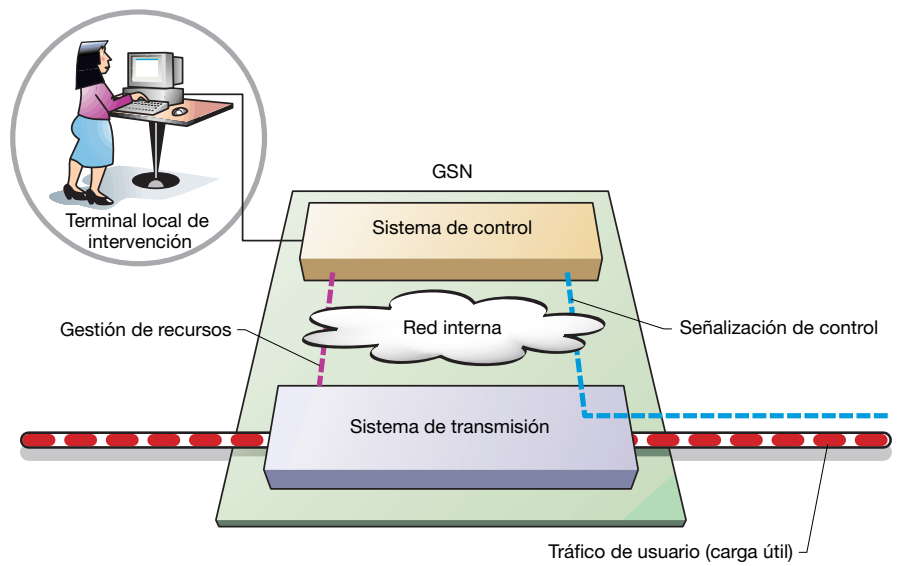
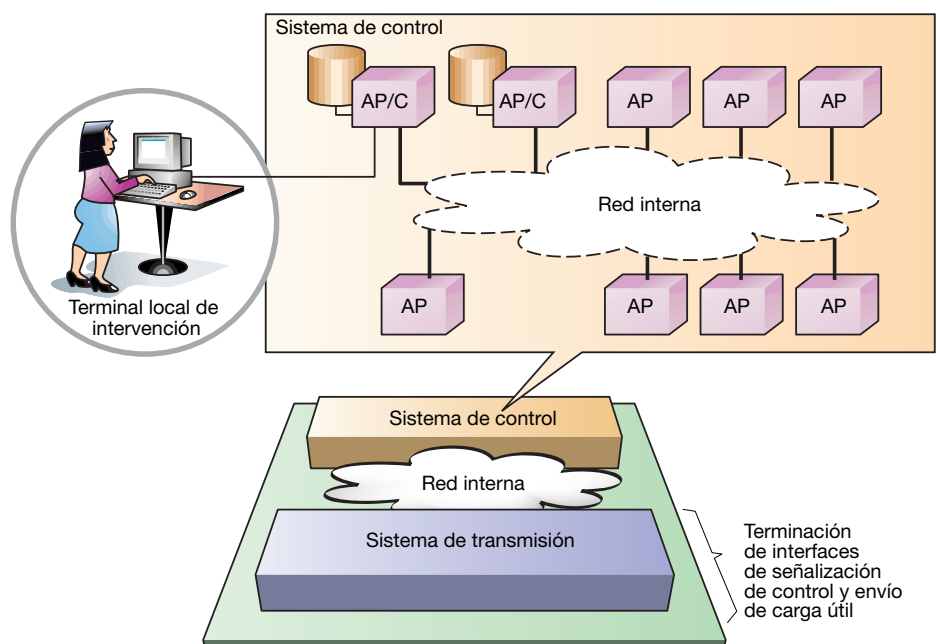


Figura 8
La arquitectura de software de GSN.

merasas redes IP diferentes. Muchas redes no usan normalmente direcciones públicas IP sino más bien uno de los rangos de direcciones privadas apartadas por la sociedad Internet. En consecuencia, el nodo de gestión de paquetes debe poder gestionar los rangos de direcciones conflictivas. Lo hace usando una combinación de métodos (Figura 7):

- encaminamiento ordinario de IP—el nodo puede gestionar una serie de rangos de direcciones y llevar a cabo encaminamiento estándar desde las placas de interfaz hasta la aplicación. Sin embargo, a causa de los conflictos de direcciones, solamente puede existir uno de esos rangos de direcciones en un momento dado;

Figura 9
La arquitectura del sistema de control.



- la función de interfaz de envío de capa de enlace (Link-Layer-Forwarding - LLF) (encaminamiento APN) permite al nodo saltarse el envío de IP y conectar todos los paquetes sobre una interfaz directamente en una aplicación. Los tipos de interfaz pueden ser o bien interfaces físicas, tales como Ethernet y E1, o interfaces lógicas PVC sobre una interfaz ATM; y
- la función LLF de túnel permite al nodo terminar varios túneles IPsec en la interfaz física entrante y hacer que cada terminación de túnel se salte el envío de IP, en vez de conectar todos los paquetes desde el punto final del túnel a una aplicación. El diseño de la LLF permite miles de intranets diferentes y que Internet se conecte al mismo nodo incluso aunque todas usen el mismo rango de direcciones IP.

Arquitectura del software del GSN

Las premisas básicas de la arquitectura del software del GSN son la apertura al hardware y soft-

ware de terceros, la distribución en capas, y la robustez (Figura 8). La gestión está basada en el principio del cliente ligero definida en la WPP, que solamente requiere que el terminal local de intervención (Local Craft Terminal - LCT) soporte una interfaz HTTP/CORBA con el GSN.

La arquitectura del software define dos entidades de computación separadas y débilmente acopladas: el sistema de control (para gestión de movilidad), y el sistema de transmisión (para tráfico de usuario). Una razón para la marcada separación del control y la transmisión es la necesidad de escalamiento flexible e independiente. Otro aspecto importante es el enfoque totalmente diferente de los dos sistemas.

El enfoque principal del sistema de control está en la robustez y en un eficiente entorno de diseño, en tanto que el del sistema de transmisión está en las prestaciones y en unos bajos costes de fabricación. La arquitectura del software del GSN facilita la separación física del SGSN en un nodo servidor, que gestiona las partes de control, y un nodo de pasarela mediática, que gestiona la transmisión de datos.

CUADRO C, COMPONENTES DE NCS

El sistema de control de red (Network Control System - NCS) es un subsistema que implementa la capa de middleware del NOC y algunos servicios que no forman parte del NOC. Un bloque fundamental de construcción de terceros de la plataforma de middleware es Erlang/OTP. Otros componentes de terceros, tal como la WPP, tienen interfaz con unos pocos productos y por lo tanto pueden ser sustituidos por componentes de terceros que ofrezcan la misma funcionalidad.

Redundancia del hardware del sistema de control

Si se avería el AP, el NCS trae un nuevo AP del fondo de reserva pasiva. No se implementa ninguna función de redundancia en la aplicación— toda la redundancia es gestionada por el NCS. Si el fondo de reserva pasiva está agotado, el NCS fusiona el tráfico sobre un AP en funcionamiento.

Redundancia del hardware del sistema de transmisión

Si se avería un procesador de dispositivos (Device Processor - DP), el NCS trae un nuevo DP de un fondo de reserva pasiva apropiado. Bajo condiciones estándar, no se requiere ninguna función de redundancia en la aplicación. Las rellamadas se hacen al módulo de control / módulo de configuración de dispositivo.

Equilibrio de la carga

Cuando se crea una nueva conexión en el sistema, el NCS selecciona el AP y los DP más adecuados.

Arranque / Rearranque

El NCS coordina todos los reanques inclu-

yendo una rellamada a la aplicación activada por la fase de arranque. El NCS gestiona cuatro niveles de reanque: conexión, reanque local menor, reanque menor, y reanque mayor. Los tres primeros niveles de reanque mantienen las conexiones, en tanto que en el nivel de reanque mayor se liberan todas las conexiones. El NCS gestiona también la asociación funcional con los niveles de reanque de la WPP.

Control y supervisión de recursos

El NCS controla y supervisa los AP y DPs que usan cualquier funcionalidad de WPP u OTP disponible. En el caso de un fallo, el NCS adopta las medidas apropiadas (nivel de reanque correcto o redundancia).

Marco del modelo de programación

El NCS define cómo se han de implementar las funciones en Erlang. Se ofrece un importante soporte para el modelo de programación, tal como almacenamiento persistente, gestión de procesos, y la supervisión de acceso de datos.

Protección contra sobrecargas y recuperación

El NCS puede conceder nueva carga en el sistema para evitar reanques debidos a sobrecargas. Sin embargo, si un reanque está causado por una sobrecarga, el NCS podría liberar conexiones a fin de efectuar una recuperación.

Actualizaciones de software

El NCS coordina todas las actividades de actualización del software y lleva a las rellamadas necesarias a la aplicación para convertir las estructu-

ras de datos. Una actualización del software va siempre acompañada de un reanque menor.

Gestor de eventos

Unos gestores de eventos altamente optimizados forman parte de los procesos dinámicos en el sistema de control. Cualquiera puede suscribirse a una vista de evento definida por los proveedores de dicho evento. Hay muchas vistas de eventos, tales como las de tarificación o registro de eventos. Los proveedores del evento están ubicados en el proceso de trabajo de control dinámico del tráfico.

Registro de eventos

La función de registro de eventos permite a los operadores registrar eventos asociados con una aplicación conexión por conexión. La función de registro de eventos se inicia desde un terminal de gestión. Los operadores pueden ver también los eventos anotados desde el terminal de gestión.

Gestión de prestaciones

La WPP ofrece una API central para la gestión de prestaciones. Para soportar un entorno distribuido, el NCS implementa un marco de gestión de prestaciones distribuidas en el sistema de control recopilando contadores distribuidos.

Soporte de tarificación

La WPP ofrece una API central para la expedición transparente de registros de datos de llamada. El NCS implementa un marco distribuido para gestionar los dispositivos de tarificación, los cuales recogen la información de tarificación desde la carga útil y la remiten al AP/C.

Sistema de control

El sistema de control (Figura 9) consta de

- funciones de control de tráfico, tales como la gestión de movilidad de GPRS y protocolos de más alto nivel (MAP);
- funciones de control de objetos, tales como arranque / re arranque, distribución, y comunicación (el middleware de control de objeto de elemento de red (Network-element Object-Control - NOC);
- funciones de O&M; y
- funciones de adaptación (controladores) para el sistema de transmisión.

Las funciones de O&M están escritas en Erlang y Java. El resto del sistema de control está en Erlang.

El principal propósito del sistema de control es procesar protocolos de alto nivel y controlar el encaminamiento de la carga útil al sistema de transmisión. El sistema de control de software no impone ningún requerimiento sobre el entorno de implementación del sistema de transmisión.

El software del sistema de control presenta una arquitectura distribuida que está basada en el OTP. Varios procesadores de aplicaciones (Application Processor - AP) están interconectados mediante una red interna. En este contexto, un AP es cualquier recurso de computación que pueda correr la OTP y la WPP. La red interna está definida por la WPP. En la versión actual, es Ethernet conmutada.

Dos AP, denominados AP/C, están dedicados para funciones centrales de O&M (uno está en reserva). Otro AP tiene asignada la tarea de procesar las funciones de control del tráfico global. Su principal propósito es distribuir trabajos a los AP. Los AP restantes procesan las funciones de control del tráfico local, tales como la gestión de movilidad.

El sistema de control se escala de forma lineal, desde un nodo que solo consta de un AP/C (funciones centrales, globales, y locales), a un nodo que consta de numerosos AP, donde cada AP local es en sí mismo una entidad escalable.

Modelo de distribución

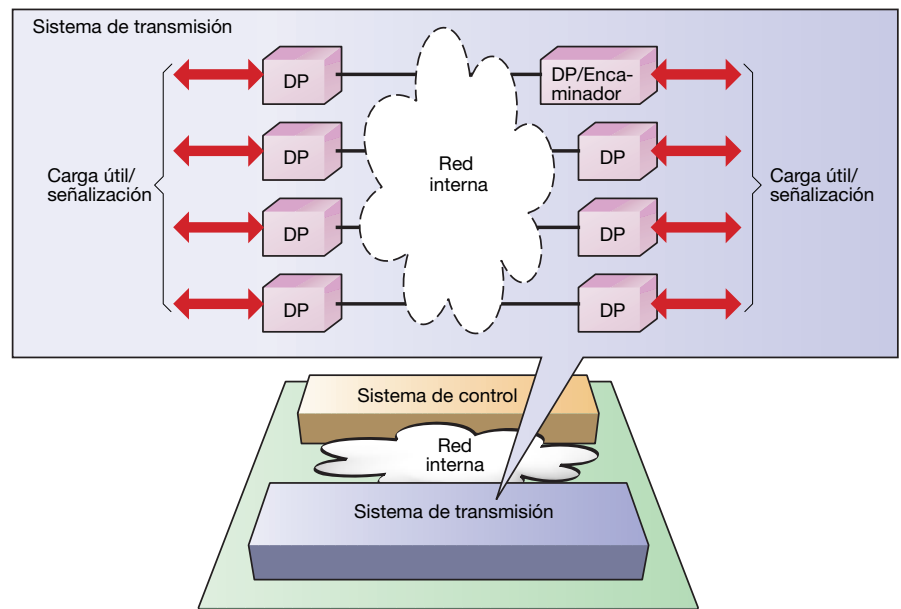
Aparte del AP/C, que contiene software para funciones de nivel de nodo, tales como O&M, cada AP contiene el mismo software. Este software define un modelo de distribución simple en el cual el procesamiento de un contexto es gestionado por un solo AP. Por ejemplo, si hay 70 estaciones móviles en el área cubierta por siete AP (Figura 2), cada AP gestionará el contexto de 10 estaciones móviles. Este procedimiento simplifica el diseño y da como resultado un sistema altamente escalable.

Sistema de transmisión

El sistema de transmisión (Figura 10) consta de

- el transporte, encaminamiento, y procesamiento del tráfico de usuario (carga útil); y

Figura 10
Arquitectura del sistema de transmisión.



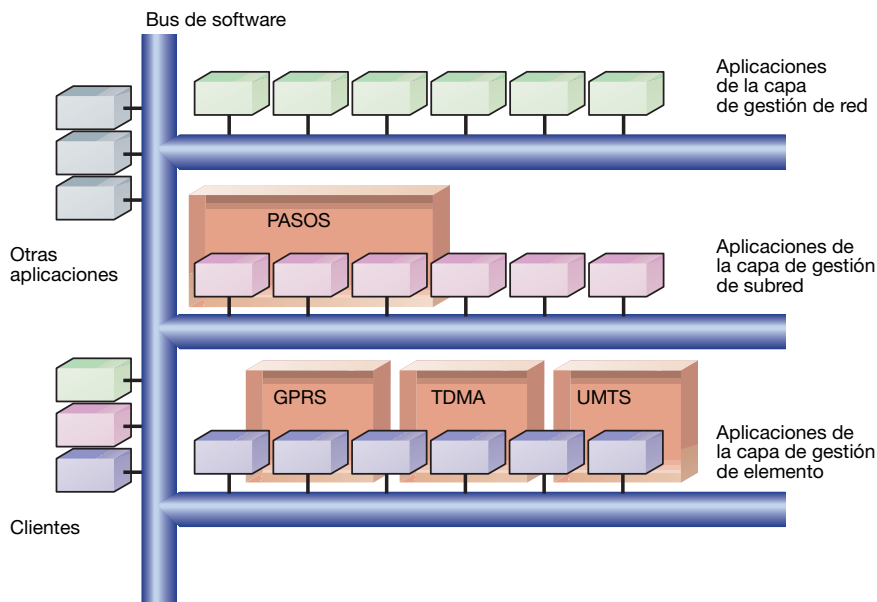


Figura 11
Arquitectura de la gestión lógica.

- la terminación de la capa baja de las pilas del protocolo de señalización, tal como la parte de transferencia de mensaje (Message Transfer Part - MTP), parte de control conexión de señalización (Signaling Connection Control Part - SCCP), y la parte de aplicación de capacidad de transacción (Transaction Capabilities Application Part - TCAP) en SS7.

Aparte de la interfaz de gestión, cada interfaz está terminada por el sistema de transmisión.

Se ha diseñado un marco para el desarrollo de aplicaciones de GPRS para un sistema de transmisión basado en VxWorks/WPP. En este sistema, las pilas del protocolo de carga útil están implementadas en un entorno STREAMS.

Capas de software

El software del GSN está dividido en tres capas que abarcan los sistemas de control y de transmisión:

- la capa de control de tráfico (Traffic Control - TC);
- la capa de control de objetos de elemento de red; y
- la capa de despliegue de recursos (Resource Deployment - RD).

Estas capas facilitan el uso activo de tecnología plug-in, lo que simplifica la adición de nuevos componentes de aplicación.

Las capas de control de tráfico y de despliegue de recursos son capas específicas de aplicación, en las que se implementan los servicios de GPRS, UMTS, y TDMA. Las funciones de aplicación que requieren robustez y soporte extensivo se implementan en la capa de control de tráfico.

De forma similar, las funciones de aplicación que requieren altas prestaciones se implementan en la capa de despliegue de recursos, al igual que las interfaces externas y los protocolos de bajo nivel para señalización.

El NOC es una capa de middleware que soporta capas de control de tráfico y de despliegue de recursos. Es una capa genérica en el sentido de que puede soportar cualquier aplicación de proceso de paquetes y no requiere ninguna modificación. En otras palabras, las aplicaciones se desarrollan en las capas de control de tráfico y de despliegue de recursos; el NOC sirve de canal de comunicación y de unión entre los componentes de la aplicación.

Gestión del GSN

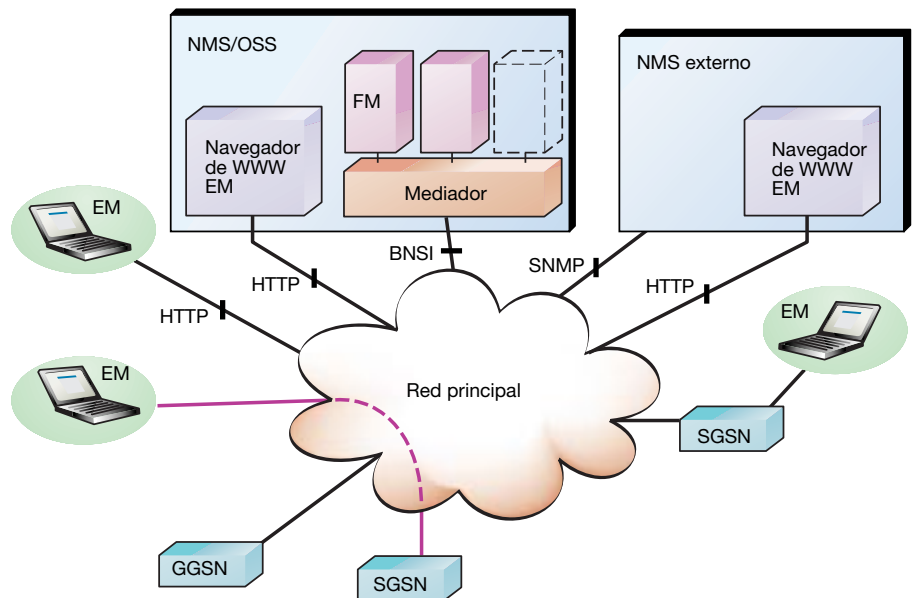
El sistema de gestión (Figura 11) para la red nuclear de conmutación de circuitos está enfocado hacia las necesidades del cliente. La solución está constituida con aplicaciones lógicas a las que se puede acceder mediante cualquier ordenador de sobremesa en el que corra un navegador de Web. Las siguientes aplicaciones de gestión aseguran una clara separación entre la gestión a nivel de elemento, red, y de subred :

- mediación de gestión a nivel de red;
- gestor de subred (PASOS); y
- gestor de elementos (Element Manager - EM) incorporado.

Mediación de gestión de nivel de red

Debido a que soportan interfaces abiertas para gestión de fallos y prestaciones, los GSN de

Figura 12
Gestor de elementos incorporado.



MARCAS REGISTRADAS

PowerPC es una marca registrada de International Business Machines Corporation.

Sun, Sun Microsystems, el Logo Sun, Solaris, y Java son marcas comerciales o marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y otros países. Todas las marcas SPARC se usan bajo licencia y marcas comerciales o marcas registradas de SPARC International, Inc. en los Estados Unidos y otros países. Los productos que llevan las marcas comerciales SPARC están basados en una arquitectura desarrollada por Sun Microsystems, Inc.

VxWorks es una marca registrada de Wind River Systems, Inc.

Ericsson pueden ser migrados a un sistema de gestión de red por medio de

- una solución empaquetada que está integrada en el sistema OSS de GSM;
- un paquete que contiene el sistema de gestión de red para la supervisión de más alto nivel ofrecida por Ericsson; o
- unidades de adaptación para integrar paquetes de gestión de red comunes.

Gestor de subred

El sistema de gestión de subred (denominado el sistema de soporte de operaciones de conmutación de paquetes (Packet-Switched Operation Support System, PASOS) es una aplicación de software portable orientada a tareas cuyo principal papel es gestionar varios nodos con muy pocos comandos. PASOS proporciona al operador aplicaciones de gestión de configuración, gestión de software, y gestión de equipos cuyas potentes posibilidades de plug-and-play garantizan la integridad del software, de las configuraciones, y de los datos. El propósito es mejorar la funcionalidad y la facilidad de uso en tanto que se posibilita una administración de coste eficaz de las configuraciones del GSN de manera clara y consistente.

Los sistemas de gestión proporcionan una interfaz de usuario orientada a tareas que puede

ser operada tanto de manera local como remota. Toda la documentación de gestión está disponible en línea.

Gestor de elementos incorporado

El gestor de elementos incorporado es un componente fundamental del sistema de O&M de la red nuclear de conmutación de paquetes. Todo el software necesario para las tareas de gestión está contenido en los GSN. La solución de gestión de elementos se implementa usando una arquitectura cliente / servidor en la que el cliente puede ser instalado en cualquier ordenador de sobremesa que soporte un navegador de Web y una máquina virtual Java. La parte del servidor se ejecuta en el elemento de red. Los GSN soportan el protocolo de transferencia de hipertexto (HyperText Transfer Protocol - HTTP), SNMP, el protocolo liviano de acceso a directorio (Lightweight Directory Access Protocol - LDAP), IIOP, BNSI, y FTP.

Un gestor de elementos puede ser conectado de forma local o remota desde diferentes entidades (Figura 12). La conexión real al GSN es transparente al usuario.

Gestión de fallos

El software de gestión de fallos proporciona funciones para detectar y aislar un comportamiento indebido dentro de un GSN. El GSN siem-

pre indica la gravedad de una alarma, y proporciona un procedimiento que ayuda a corregir cada fallo. Este procedimiento está automatizado (con enlaces de hipertexto) y permite que se pongan en marcha operaciones de control, o medidas de recuperación desde la aplicación de gestión de fallos.

Gestión de prestaciones

El software de gestión de prestaciones proporciona soporte para la recopilación de estadísticas y eventos generados por el nodo relativas a la calidad y disponibilidad de servicios, la optimización dentro del nodo o la subred, y la planificación. Los grupos de mediciones pueden ser creados, modificados o borrados mediante la interfaz de la aplicación. Un rango de mediciones aplica al análisis de tendencias y a las previsiones.

Gestión de configuración

La gestión de elementos y la gestión de subred se deben configurar a través del servidor LDAP. Esto es, la configuración central de los nodos garantiza la consistencia en la red GSN. No obstante, es posible configurar un nodo remotamente sin usar LDAP, o localmente desde una GUI orientada a tareas a través de la cual pueden ser fijados y modificados los parámetros asociados con el SGSN. La gestión de configuración se aplica a

- gestión de software—por ejemplo, carga, instalación y desinstalación de software, comprobación de configuraciones de software, y gestión de volcados de software;
- gestión de equipos—por ejemplo, listado de equipos con estados administrativos y operacionales, y cambio del estado administrativo (bloqueo o desbloqueo) o el estado operacional (puesta a cero);
- gestión de ejecución—por ejemplo, listado de aplicaciones dentro del nodo y sus estados de ejecución, puesta en marcha, parada, detener, o volver a poner en marcha aplicaciones; y
- fijación de parámetros—por ejemplo, pará-

metros de configuración para SS7, encaminadores, e interfaces físicas.

Gestión de seguridad

La gestión de seguridad al nivel de elemento de red proporciona funciones que protegen los recursos de elementos de red contra la destrucción, tanto si es intencionada como si no. Por lo tanto, incluye funciones comunes de seguridad, tales como la administración de perfiles de usuario final y autorización de acceso de usuario, así como facilidades para la anotación que registran las actividades del usuario y todos los intentos de acceder a los elementos de red.

Soporte multilingüe

La solución de gestión de conmutación de paquetes proporciona a los operadores soporte multilingüe. PASOS soporta documentación, textos de ayuda, y menús en lengua inglesa, japonesa y china.

Sin embargo, la información generada por el sistema, tal como alarmas, eventos, y los nombres de los dispositivos, se dan solamente en inglés.

Conclusión

La solución de Ericsson para introducir GPRS en un sistema GSM—así como los dominios GPRS dentro de un sistema UMTS ó TDMA—se basa en dos nuevos nodos: el SGSN y el GGSN.

Inicialmente, estos nodos pueden ser combinados en el mismo nodo físico. En una etapa posterior, el nodo GPRS centralizado puede ser separado en un SGSN y un GGSN dedicados.

Si la expansión futura comprende otras redes de acceso, los nodos pueden funcionar juntos, usando partes centrales.

La arquitectura permite la fácil separación del SGSN en un nodo servidor y un nodo de pasarela mediática, permitiendo así una asignación de energía más flexible entre el caudal de control y el de datos.

REFERENCIAS

1. Granbohm, H. and Wiklund, J.: GPRS—Servicio general de radio por paquetes. Ericsson Review Vol. 76 (1999):2, páginas 82-88.