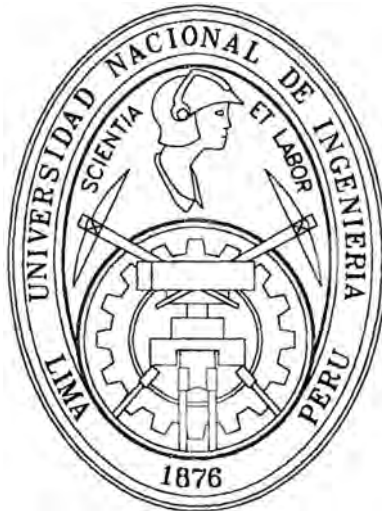


UNIVERSIDAD NACIONAL DE INGENIERÍA
Facultad de Ingeniería Industrial y de Sistemas



**IMPLANTACIÓN DE UNA SOLUCIÓN
INTERNET EN LA BANCA**

INFORME DE INGENIERÍA

Para Optar el Título Profesional de:

INGENIERO DE SISTEMAS

ALDO MANUEL ALFREDO MONTES MONFORTE

LIMA – PERU
2002

Este trabajo está dedicado a mis padres Alfredo y Rosario, a mi esposa Choqui y a mis hijos Andrea y Giancarlo a quienes descuido por dedicarme mucho al trabajo, a mis hermanos Giovanni y Gino y para ti también Erick que siempre te tengo presente a pesar de la distancia

Implantación de una Solución Internet en la Banca

Quiero agradecer a la Universidad Nacional de Ingeniería, mi “Alma Mater” por darme la oportunidad de ser un profesional al servicio de los demás

<u>Indice</u>	<u>Pág.</u>
Descriptores Temáticos	8
Sumario	10
I. Introducción	
I.1 Antecedentes	12
I.2 Reseña Histórica	20
I.3 Organigrama	22
I.4 Equipos de Trabajo	22
II. Soporte Técnico	
II.1 Conceptos Básicos	30
II.2 Networking	45
II.3 Modelo OSI de Comunicaciones	48
II.4 Arquitectura TCP/IP	50
II.5 Protocolos	62
II.6 Esquema general de la solución	62
II.7 Evolución	64

III. Desarrollo de Informática

III.1 Aplicación 66

III.2 Evolución 90

IV. Proveedores

IV.1 Herramientas de Monitoreo 93

V. Aspectos Críticos

V.1 Seguridad 97

V.2 Ambientes 101

V.3 Tiempos de Respuesta 102

V.4 Homogenización de Ambientes 103

V.5 Conciliación de Base de Datos 104

V.6 Pases de Versiones 104

V.7 Backups 105

V.8 Simuladores 105

V.9 Herramientas de Gestión 106

V.10 Controles Internos y Externos 106

V.11 Distribución Física 107

VI. Actividades de Apoyo

VI.1 Comité de Cambios	108
VI.2 Reuniones de Seguimiento	108
VI.3 Reportes de Incidencias y Disponibilidad	109
VI.4 Procedimiento de Crisis	109

VII. Expectativas

VII.1 Tienda Virtual	112
VII.2 Currículum Web	112
VII.3 Portal Inmobiliario	112
VII.4 WAP	113
VII.5 Intranet	115
VII.6 Negocios digitales y Comercio Electrónico	115

VIII. Otros

VIII.1 Capacitación	117
---------------------	-----

IX. Conclusiones y Recomendaciones

IX.1 Conclusiones	119
IX.2 Recomendaciones	121

X. Bibliografía	122
------------------------	-----

XI. Anexos	124
-------------------	-----

Descriptorios Temáticos

- ◆ Acl
- ◆ Hipertexto
- ◆ Plug – in
- ◆ Applets
- ◆ Host
- ◆ Protocolo
- ◆ Datagrama
- ◆ Interfaz
- ◆ Proxy Inverso
- ◆ DNS
- ◆ Internet
- ◆ Routers
- ◆ E-Mail
- ◆ Internauta
- ◆ Scripts
- ◆ FTP
- ◆ Intranet

Implantación de una Solución Internet en la Banca

- ◆ Servlets
- ◆ HACMP
- ◆ IP
- ◆ Socket
- ◆ Hacker
- ◆ Modems
- ◆ Switches
- ◆ Hipermedia
- ◆ Perl
- ◆ Telnet
- ◆ Verónica

Sumario

Este trabajo tiene por objeto presentar de una manera simple y sencilla lo que significa implementar una solución Internet en un medio tan competitivo como resulta ser la Banca.

Por razones de ética y para no defraudar la confianza que la Institución donde laboro me dio al proponerme en este proyecto, en este trabajo no mencionaré el nombre de la institución ni proporcionaré ninguna información confidencial que pueda poner en riesgo la confidencialidad y la seguridad de mi institución, por lo que solicito la comprensión que el caso amerita.

He tenido la oportunidad de recibir capacitación en el exterior sobre esta nueva tecnología con el propósito de poder implantar la solución corporativa en nuestro país y que una vez implantado pueda mejorarse incluyendo servicios que sean prioritarios y necesarios en nuestro medio.

El trabajo puede dividirse dependiendo del enfoque que se le de, inicialmente participé en el equipo de Desarrollo de Informática que tenía el encargo de implantar el software aplicativo, software recibido en una etapa inicial y que habría de personalizarse necesariamente en América Latina, es por eso que explicaré lo que desde el punto de vista del programador ha significado y significa aún esta experiencia considerada como un reto por ser algo totalmente nuevo en la institución. Posteriormente pasé a formar parte del equipo de Soporte Técnico a Internet por lo que tuve que familiarizarme con el aspecto de Hardware de la solución, con la

Implantación de una Solución Internet en la Banca

experiencia de los dos frentes me atrevo a presentar este trabajo que de alguna manera resume todo el esfuerzo personal por hacer que esta solución se convierta en una realidad y servir de guía para todos aquellos que de alguna manera u otra tengan que enfrentarse a este reto.

I. Introducción:

I.1 Antecedentes

Este trabajo tiene por objeto mostrar lo que significa implantar una aplicación Internet en un entorno tan complejo como resulta ser la Banca y puede servir de guía para aquellos que tengan en mente instalar una solución de gran envergadura. La solución tomada fue importada de Europa.

De alguna manera trataré de enfatizar aquellos aspectos que pueden resultar cruciales y que se deben tomar en cuenta en una implantación de esta naturaleza. Claramente es sabido que la tecnología apunta a Internet de forma acelerada y es de esperar que en un futuro no muy lejano, no solamente las aplicaciones bancarias sino aquellas que corresponden a la vida cotidiana estén definidas bajo un entorno Internet. La posibilidad de poder acceder a cualquier tipo de información no importando en que servidor remoto se encuentre, es un paso gigantesco que estamos seguros sabremos aprovechar en su verdadera magnitud. Este trabajo es un resumen, por supuesto muy breve, de lo que significó y significa actualmente implantar una solución Internet en una empresa financiera de características multinacionales; no he ahondado el tema en cada Servidor o en cada Producto ya que cada uno de ellos encierra una cantidad de conocimientos que tranquilamente podría ocuparnos meses, he pretendido de una manera somera pero paladina evidenciar aquellos aspectos en donde fue necesario ponerse a pensar que camino tomar ante cada uno de los tramos de este singular pero dantesco reto.

Implantación de una Solución Internet en la Banca

El trabajo fue desarrollado en un banco de características transnacionales, como lo mencioné anteriormente, esta entidad financiera o mejor dicho la sucursal nacional donde laboro no tenía experiencia en el tema de Internet, resultaba un tema novedoso y al mismo tiempo amenazante. Inicialmente se pensó en un desarrollo centralizado a cargo de la Casa Matriz, de esa manera los países satélites de la corporación recibirían los productos terminados con lo que su labor se limitaría a la instalación y seguimiento del mismo. Las modificaciones y adecuaciones propias de cada país serían canalizadas y entregadas como pendientes a la Casa Matriz quien en un período determinado cumpliría con el requerimiento sin perder de vista al producto final como un producto corporativo, vale decir incorporando las peticiones de cada país satélite dentro de un producto único válido para toda la corporación, una vez recopilados todos los cambios la versión sería transmitida a los países satélites con lo que habría uniformidad a nivel de países de América, uno de los fundamentos o estilos de la Corporación.

La idiosincrasia de cada país de América Latina resulta ser muy variada, hay algunos en donde se da más importancia a algunos aspectos financieros que en otros, la complejidad de los requerimientos de uno u otro país podría complicar el desarrollo centralizado desde varias ópticas, una de ellas podría ser la prisa en el cumplimiento de una petición y otra podría ser la cantidad de recursos tanto físicos como lógicos necesarios para cumplir con una petición de un país satélite en la Casa Matriz, por lo que comenzó a evaluarse la posibilidad de realizar desarrollo en los países satélites, este cambio daría origen a la aventura de especialistas peruanos en una solución europea; una de las premisas sería de que todos los países partirían de un producto único y corporativo y que cada modificación o adecuación debería de notificarse a Europa para su registro en una versión única, válida para la Corporación, es decir no se podría implantar algún cambio sin que sea del conocimiento de la Casa Matriz, pero finalmente se decidió por una opción, el núcleo de producto sería invariablemente el mismo en todos los países pero los nuevos desarrollos se harían en segmentos de código independientes y asignables a cada país en cuestión; así por ejemplo Perú podría tener sub-proyectos dentro del producto de software de desarrollo muy propios y que no necesariamente

tendría que tener México, si el producto resulta bueno en un país, la política sería exportarlo a los otros con la condición de incluir el segmento de código como parte de la solución Corporativa, es decir, que el núcleo del producto sea invariablemente el mismo en todos los países y que los nuevos desarrollos se hagan en segmentos de código independientes y asignables a cada país en cuestión; finalmente se decidió hacer un desarrollo básico con la participación de los países satélites.

Internet, a pesar de no ser un tema muy nuevo en América Latina, aún sigue sin explotarse en la misma dimensión como se hace en los países altamente industrializados, sin embargo la expectativa es grande, en muchos centros educativos o de formación de Informática el tema de Internet y derivados se ha convertido en algo de primerísima importancia, podría llamarse el “boom” de este siglo.

Luego de realizar profundos análisis de costo-beneficio, la Casa Matriz decidió que el desarrollo se haga descentralizadamente como ya se precisó en párrafos anteriores, pero sólo luego de recibir el programa “piloto base” que sería desarrollado por los especialistas seleccionados de cada país para ese propósito, en conclusión cada país recibiría una copia del programa “piloto” producto del trabajo tripartito de especialistas de la Casa Matriz, especialistas de los Proveedores y adicionalmente los especialistas seleccionados de América Latina para conocer, entender y estar en capacidad de modificar la aplicación “base” una vez estén de vuelta en sus respectivos países; enfatizando lo expresado anteriormente, la dirección corporativa para América Latina vio conveniente seleccionar dos personas de cada país satélite (siendo yo uno de ellos por el Perú) para recibir capacitación en la nueva aplicación que involucraría conocer la Arquitectura y estar en capacidad de poder desarrollar nuevas aplicaciones bajo el entorno corporativo.

En este trabajo trataré de volcar todo lo que sé fruto de la participación que tuve y tengo en el proyecto, objetivo que inicié y finalmente vi en ejecución.

Es importante recordar que cuando uno trabaja en corporaciones muy grandes se toma mucho tiempo en las decisiones de compras, ya que estas tienen que ser aprobadas en la Casa Matriz luego de una cantidad de documentación que justifique la adquisición, sin embargo no solo en ese aspecto es relevante la influencia de la Casa Matriz, si se quiere instalar un Producto, se espera que este haya sido probado en casi todo el mundo antes de pensar en la alternativa de instalarlo o simplemente se espera colocar un producto que aún no siendo el último resulte ser más seguro, el tema de la “Confiabledad en el Producto” es crucial y está por encima de cómo vaya el mundo de costado. La corporación por ejemplo escogió para el tema de Internet una arquitectura que no es la última pero que si ha sido hartamente probada en todo el mundo, basta con que el proveedor esté en capacidad de asegurar que con ese producto no se tendrá absolutamente ningún problema. Profesionalmente hablando resulta un poco desalentador para un especialista tener que trabajar con algo que él no considera que sea lo mejor o que solamente exista en su corporación, no siendo comercial el producto y es ahí donde uno entiende que los intereses de la corporación están por encima de los intereses individuales por mantener un esquema de trabajo distinto que puede traer resultados pero que no se ajusta a los estándares de la corporación.

La capacitación tomó un tiempo de 4 a 5 meses en la casa matriz, no solo de vieron aspectos técnicos sino también se revisaron temas referentes a las estrategias a aplicar en América Latina al momento de la implementación, como resultado de fin de curso, cada uno de los especialistas de los países que intervinieron, deberían personalizar la aplicación dependiendo las costumbres y modos de cada país, luego llevarían la aplicación a su país de origen.

Al retornar a nuestros países de origen habríamos de iniciar el largo camino de la implementación de la solución en la que habríamos de apoyar no sólo con el tema del software sino también con el tema de la configuración de equipos.

Implantación de una Solución Internet en la Banca

Estando en la Casa Matriz, desarrollé todo el esquema básico para el manejo de las Consultas de Saldos y de Movimientos de Tarjetas de Débito y Crédito, así como modificaciones al Estado Resumen (Posición) del cliente en donde aparecerían todas sus cuentas, saldos y movimientos.

En resumen, luego de la capacitación en la Casa Matriz debíamos estar en capacidad de:

- ◆ Implementar la solución en nuestro país de origen.
- ◆ Personalizar la solución hasta un nivel que signifique la aprobación de las áreas comerciales.
- ◆ Incluir sub-proyectos a la solución haciendo uso de programación.

Características Generales:

La solución optada se basaría en equipos IBM ya que la Casa Matriz en tal sentido escogió esta firma como el Proveedor principal y responsable general de la implantación de la solución desde el punto de vista de equipos y software base, todo esto bajo contrato.

Las plataformas a ser consideradas en la solución corresponden a:

- ◆ RS/6000
- ◆ Netfinity
- ◆ Sun

El Software o Aplicativos soportados en la Operación de Servicio serían:

- ◆ AIX
Es el software base de los servidores RS-6000
- ◆ HAMCP
Software orientado a la alta disponibilidad que se usará en diferentes componentes de la Arquitectura.

Implantación de una Solución Internet en la Banca

- ◆ **CBTF**
Software, núcleo de la solución Internet
- ◆ **Sun Solaris**
Software, sistema operativo para los Firewalls
- ◆ **CheckPoint**
Software de Firewall
- ◆ **StoneBeat**
Software alta disponibilidad de Firewalls
- ◆ **Real Secure**
Software para el manejo del monitoreo y seguridad de la red
- ◆ **DB2 Enterprise Edition para AIX**
Manejador de la base de datos
- ◆ **DB2 for NT Workgroup Edition**
Manejador de la base de datos
- ◆ **IBM e-Network Communication Server**
SNA del RS-6000
- ◆ **MQ-Series**
Manejador de mensajes entre el RS-6000 y el Host
- ◆ **Norton Antivirus**
Detector de Virus

Implantación de una Solución Internet en la Banca

- ◆ Policy Director
Manejador del esquema de Seguridad
- ◆ LDAP
Manejador de la Base de Datos para el esquema de Seguridad
- ◆ Tivoli Framework
Herramienta de monitoreo
- ◆ Tivoli Distributed Monitoring
Herramienta de monitoreo
- ◆ Tivoli Netview
Herramienta de monitoreo
- ◆ Webseal
Web Server de la Solución
- ◆ Websphere Application Server
Conocido como WAS, la Aplicación
- ◆ Websphere Performance Pack (Network Dispatcher)
Balanceador de carga a nivel de Webseal
- ◆ Windows NT
Sistema Operativo Microsoft
- ◆ Cisco Works
Software de monitoreo de elementos de red

Implantación de una Solución Internet en la Banca

- ◆ Internet Explorer
Navegador
- ◆ Crystal Reports
Reporteador que explotando cualquier archivo fuente permite manejar la salida de diferentes formas.
- ◆ La Aplicación propiamente dicha bajo Visual-Age for Java

Viéndolo desde la perspectiva de Servidor-Producto se tiene:

- ◆ Consola de Firewall
Checkpoint, Norton Antivirus, StoneBeat, WebTrends, WindowsNT
- ◆ Consola de Detector de Intrusión
Cristal Reports, Real Secure, Windows NT
- ◆ Detector de Intrusión
Real Secure, Windows NT
- ◆ Firewall
Firewall 1 Checkpoint, StoneBeat, Sun Solaris
- ◆ Ldap
AIX, DB2 Enterprise, HACMP, Java Run Time, Ldap, Policy Director
- ◆ Monitor Cisco Works
Cisco Works, Windows 98

- ◆ Policy Director
AIX, DB2 Enterprise, DCE, HACMP, Java Run Time,
Ldap, Policy Direct

- ◆ Portal
AIX, HTTP Server, Java Run Time, Ldap, Policy Director

- ◆ Tivoli
AIX, DB2 for AIX Workgroup Edition, Tivoli Netview

- ◆ Was
AIX, Ca-XCOM, CBTF, SNA, DB2 HACMP, Java Run
Time, MQSeries, Netscape Enterprise Server, WebSphere
Application Server

- ◆ WebSeal
AIX, DCE, Java Run Time, Network Dispatcher, Policy
Director

I.2 Reseña Histórica

Como he mencionado anteriormente, la empresa donde se ha instalado la solución corresponde al sector de la Banca, tiene cincuenta años de antigüedad y a lo largo de su historia ha cambiado de estilo de dirección muchas veces, ha pertenecido inicialmente a la Banca Privada para luego ser nacionalizada y posteriormente vendida a capital extranjero.

La institución siempre le ha brindado vital importancia al desarrollo tecnológico prueba de ello es que a lo largo de su vigencia se ha distinguido por estar a la vanguardia en los adelantos y novedades tecnológicas de su época.

Inicialmente estuvo en manos de capital Americano, específicamente el Chess Manhattan Bank tuvo mucha influencia en los estilos y modos de manejar los asuntos bancarios en nuestro país, posteriormente la institución habría de pasar a manos del gobierno y con ello su estilo cambiaría radicalmente, tengo la suerte de trabajar en esta institución por más de 20 años y he podido percibir de manera directa como la administración principal puede influir directamente en el logro de los objetivos de la institución.

Específicamente en el Área de Informática, no solo se tuvieron cambios de nombre ya que en otros momentos se llamó Sistemas sino que cambiamos en repetidas oportunidades de orientación en cuanto a los procesos informáticos, en algún momento los procesos se hicieron totalmente centralizados, ya que se trata de una empresa que tiene sucursales en diferentes puntos del país, todos los procesos hechos en las sucursales debía de ser traído a Lima y posteriormente en reportes distribuir la información de retorno con los procesos efectuados, esto se hizo durante muchos años, posteriormente se tomó la idea de descentralizar los procesos, lo que obligó a abrir puestos de trabajo en las diferentes sucursales, Lima seguiría recibiendo la información centralizada pero en detalle, mucho personal fue enviado a Trujillo, Arequipa, etc..., posteriormente y con la privatización de la institución se volvió a pensar en la Centralización, con ello se eliminaron los puestos en provincias y algunos sobrevivientes tuvieron que buscar un cupo en nuestra ciudad capital, la Privatización generó un cambio radical, la institución forma parte de una corporación mundial y podría decirse que a nivel global es una de las instituciones financieras más poderosas del mundo, la institución tiene parte capital nacional y parte capital extranjero (europeo), una de las primeras cosas que se hizo en la institución fue eliminar la burocracia exagerada que se había heredado del manejo gubernamental así como puestos de trabajo que para la nueva administración no eran justificados, esto generó un clima de tensión ya que más de dos mil empleados tuvieron que abandonar la institución en un período no mayor de dos años, desde el punto de vista informático y a pesar de poseer sistemas buenos y bien calificados por el mercado éstos fueron reemplazados por los estándares europeos, la administración de la institución estaría a cargo del socio extranjero que tiene experiencia en el tema, el

socio peruano participaría de otra forma, más tarde se dieron los cambios, muchas ejecutivos salieron o fueron bajados de sus cargos y reemplazados por ejecutivos venidos de Europa, en Informática también se dieron cambios, los sistemas principales debían de ser removidos para lo que se crearon equipos de trabajo, las metas, la presión y el tiempo comenzaron a ser temas cruciales y continuos de ahí en adelante, se trabaja muy duro, mucho más que antes, muchos han terminado enfermos, otros no resisten y otros se han tenido que adaptar al cambio, se ha perdido mucho de calor y se ha reemplazado por un esquema más práctico en donde los resultados y el logro de los objetivos son lo más importante, he tenido la suerte de participar en casi todos los proyectos importantes de la institución, proyectos como el cambio del esquema del Teleproceso, cambios en el manejo de los servicios de atención automática a los clientes, en el manejo de los documentos digitalizados, etc.

I.3 Organigrama



I.4 Equipos de Trabajo

Como mencioné inicialmente, solo fuimos dos personas a ver el software, a entenderlo y a recibir la capacitación como para poder modificarlo y adaptarlo a las necesidades, hubieron otras personas que viajaron también a la Casa Matriz, pero estas fueron del Hardware, ellos pertenecían al Proveedor Principal que por razones contractuales habría de tener la responsabilidad de la instalación y puesta en marcha de la solución así como el soporte en materia de software base.

Las personas que viajamos, formamos parte del Área de Desarrollo de Informática que como se ha podido apreciar en el organigrama, se divide en tres grandes grupos: Producción y Soporte Técnico, Desarrollo de Sistemas y Calidad de Informática, ésta última, un área especializada en velar por la integridad de los

Implantación de una Solución Internet en la Banca

sistemas y el pase adecuado de los módulos de un ambiente de desarrollo al final que es el de Producción, sin embargo inicialmente este grupo no formaría parte fundamental del proyecto, hasta después en que la aplicación estuviera más sólida.

Por un lado estaba Desarrollo de Sistemas encargado del desarrollo, el equipo de Soporte como intermediario entre el Proveedor y Desarrollo y el equipo del proveedor propiamente dicho.

Mi trabajo inicialmente consistió en instalar las herramientas y el software básico para poder implementar el software que habíamos traído desde la Casa Matriz, se nos facilitaron las máquinas mejor equipadas de la Institución de manera que no tuviéramos problemas para poder realizar la instalación y desarrollo del producto, paralelamente brindábamos apoyo al área de Soporte en materia de comprensión de la aplicación y como es que ésta finalmente habría de funcionar interactuando con la Aplicación, no puedo negar que hubieron muchas imprecisiones que fueron aclarándose a medida que el tiempo pasara y nuestros conocimientos se consolidaran, porque una de las cosas que más preocupó todo el tiempo fueron las fechas compromisos adquiridas por la Gerencia General de la institución hacia el universo de clientes.

El Software elegido por la casa Matriz fue el “Visual-Age for Java” que para propósito de Desarrollo habría de montarse en una máquina con Sistema Operativo Windows NT.

La instalación de este producto no fue nada sencilla, de hecho a pesar de contar con máquinas de una gran capacidad, no podíamos lograr el éxito esperado, se escogieron 5 máquinas y a cinco personas incluyendo a los dos que fuimos a la capacitación de la casa matriz, quienes teníamos idea de lo que íbamos a hacer mientras que los demás estarían aprendiendo de nosotros.

Implantación de una Solución Internet en la Banca

Inicialmente habríamos de trabajar en modo aislado, vale decir, cada uno habría de modificar sus “clases” (Segmentos de código en lenguajes orientados a objetos) pero tendríamos que finalmente pasar las modificaciones a una “máquina final”, desafortunadamente terminamos haciendo el trabajo solo los dos que viajamos ya que por la premura del tiempo las personas del grupo asignadas solo pudieron ser aprovechadas para cosas muy puntuales, una característica esencial que se tuvo en el proyecto fue la lucha desesperada contra el tiempo.

Posteriormente habría de instalarse una facilidad que permitiría que las clases modificadas no se alojen en una sola máquina final o resultante o para ese único propósito específico sino que más bien se trabajara en “equipo”, es decir el repositorio (archivo de gran tamaño) en donde se deja y se toma el código fuente habría de ser único, ya no sería uno por máquina sino que sería compartido por todos, así mientras alguien modificaba una clase otro si quería utilizarla también tendría que esperar que el anterior termine para recién tomar acción, en la actualidad ya es un estándar de trabajo.

El Visual-Age tiene la característica de poder facilitar el desarrollo de aplicaciones web con una alta facilidad pudiendo usarse una sofisticada interfase gráfica.

La estructura organizativa del Visual-Age es jerárquica y va de arriba hacia abajo de la siguiente forma, primero se tiene el concepto de Proyectos y dentro de estos el de Paquetes y bajo éstos, las famosas clases, para finalmente caer en el detalle que es el “objeto” en sí, un objeto es “instanciado” y la clase es “referenciada”.

Inicialmente habríamos de tener un solo proyecto con varios paquetes, la Casa Matriz nos proporcionó el software que se montaría en cada una de las máquinas instaladas con el nombre de “ivj.dat”, algunas “clases” estarían disponibles, es decir podría verse su código sin embargo otras por razones de seguridad o de confidencialidad no podrían ser vistas solo referenciadas, esto debe

interpretarse como que algunas cosas que atañen a las comunicaciones o interfases con el sistema operativo habrían de ser controladas solo por la Casa Matriz, lo que marcaría una diferencia entre lo que es la Arquitectura o clases propias de la Arquitectura y las clases de la Aplicación que si estaríamos en capacidad de modificar o de crear según nuestros requerimientos.

Estructura para el desarrollo de Visual-Age

(Ver Anexo "2")

Esta experiencia fue verdaderamente muy interesante, no sólo por la necesidad de conocer algo nuevo sino también por la obligación de que algo nuevo se ponga operativo con tiempos bastante ajustados.

Las funcionalidades básicas fueron.

- Inscripción de Usuarios
- La Posición General del Cliente (Todas sus cuentas)
- Consulta y Movimiento de Cuentas Personales
- Transferencia a Cuentas Propias
- Cambio de Clave de Acceso

Posteriormente habría de personalizarse estas funcionalidades dotándolas de particularidades propias de nuestro medio, se incluirían otras funcionalidades como la de "Pago de Servicios" en su modalidad de pago de Agua, luz, telefonía (básica, cable, Internet...) algo que personalmente diseñé y programé, adicionalmente Consultas de Tipo de Cambio Monetario, Desconexión del Sistema, Implementación del Portal, Internet Empresarial, etc..

Paralelamente se hacían los ajustes a fin de montar la infraestructura para que lo que se venía trabajando aisladamente pueda hacer efecto en los ambientes donde finalmente habrían de residir. Una cosa es el desarrollo u otra hacer que lo que

se ha desarrollado pueda instalarse en un ambiente que sea el que finalmente de la cara al público.

El sistema operativo sobre el que finalmente habría de correr la aplicación montada sería el AIX, versión mejorada por así decirlo del famoso UNÍX y que estaría corriendo en un Servidor RS-6000 de IBM, los servidores RS-6000 se utilizarán no solo para montar la aplicación sino también para los elementos de Seguridad. Habría de montarse el Websphere Application Server en esta máquina pero necesitaríamos de contar con otras para alojar el software de seguridad, para lo cual necesitaríamos contar con un producto de IBM denominado Policy Director que contendría al Webseal que no es más que un publicador de páginas y el LDAP que es la base de datos del Policy en donde en principio radicarían todos los usuarios con acceso al sistema.

Habrían de hacerse muchas modificaciones al sistema, de hecho tendríamos que alojar el producto del desarrollo que en esta caso se denominaría “jar” en rutas permisibles en el WAS a fin de que pueda gestionarse la aplicación, la definición de las rutas también fue un trabajo interesante, la aplicación cuenta con htmls, gif, jpgs, jars, etc... y cada uno debe estar en una ruta específica, en el WAS existe un motor JAVA con jar que contendría proyectos que a su vez serían ejecutados una vez se haga el requerimiento desde el usuario.

No debería existir una aplicación Internet que no requiera del uso de Firewalls, si pretende asegurarse estar libre del ataque de intrusos, hay gente que está constantemente bombardeando con direcciones IP la solución con el propósito de ver si pueden acceder a algunos de nuestros componentes y así realizar algún hecho delictivo que redunde en un perjuicio para la institución, es por eso que se requiere del apoyo de los Firewalls que con sus reglas evitan el acceso de intrusos a la red protegiendo de esta forma la integridad de la solución, el esquema empleado por el Banco es el de contar con una zona insegura y con otra zona totalmente segura y con cuatro Firewalls colocados al ingreso de cada zona.

Asimismo, las reglas habrían de revisarse y seguir con las recomendadas por la Casa Matriz, la creación de las reglas y el entendimiento del funcionamiento de los Firewalls también fue cosa de tiempo, en la actualidad sabemos que Microsoft está recomendando el uso del “ISA-SERVER” con el Windows 2000 pero nuestra institución lo desestimó, toda la Arquitectura Física fue estudiada y analizada en la Casa Matriz, fue allí donde se decidió con que equipos contar y aún más la Casa matriz se encargaría de hacer la compra de los equipos y con los contratos con los proveedores para América Latina. Para el caso de los Firewalls la Casa Matriz decidió que se contara con el StoneBeat.

El usuario o internauta (el que navega por Internet) puede solicitar la página de la corporación introduciéndola a través de un “browser (navegador)” que sea de su preferencia, sin embargo nosotros tuvimos especial cuidado en recomendar a los usuarios el uso de la solución con navegadores a partir de ciertas versiones tanto para el I-Explorer como para el NetScape.

No se tenía una idea clara de que funcionara la conectividad para lo cual se armó un ambiente de Pruebas, un ambiente no pensado inicialmente ya que como mencioné en ningún momento se pensó en la necesidad de hacer desarrollo en América Latina, pero el requerimiento se dio y tuvimos que hacer lo posible para contar con equipos hasta que en la Casa Matriz autorizaran la compra de los mismos, una alternativa fue sacrificar la Alta Disponibilidad en el ambiente de Producción haciendo que de los dos equipos planteados en cada punto solo funcionara uno de ellos y el otro pasara conformar nuestros ambientes de Pruebas

La certificación tuvo que ser adquirida de manera que pudiéramos contar con un nombre para nuestro “Site”, esa fue una negociación con Verisign (sede en Argentina).

Implantación de una Solución Internet en la Banca

El Websphere instalado en cada máquina de desarrollo permitía emular el comportamiento de nuestra solución en Producción, en el ambiente de desarrollo contábamos afortunadamente con la opción de “debugg” que permitía poder hacer un seguimiento a lo que estábamos haciendo con nuestro código Java.

No solamente se conformaron equipos de trabajo de los grupos de Informática, sino que también intervinieron otras áreas como, Organización y Métodos cuya actividad principal estaría orientada a la verificación y prueba del software a pasarse a Producción, E-Business cuya función sería la de calibrar los requerimientos del mercado y su trabajo estaría más en función de la gente de las áreas comerciales y Marketing y Promoción. Como su nombre lo indica, esta última área se encargaría de la promoción del producto y sus bondades con los clientes.

Así todos reunidos inicialmente dos veces por semana y luego una vez hasta que el proyecto estuviera en Producción, cada una de las áreas aportaba lo necesario de manera que no quedara ningún punto sin tomar en cuenta antes del gran “debut” que podría significar el éxito o el fracaso del proyecto y por ende la imagen de la institución.

Informática, evaluaría la factibilidad de los requerimientos y propondría la fecha de culminación, la Gerencia General haría el seguimiento de detalle de cada uno de los requerimientos así como de los compromisos tomados.

Las reuniones con estos grupos finalmente ya no serían celebradas sino reemplazadas por reuniones de coordinación y seguimiento una vez por semana y lideradas por el Jefe de Informática con el apoyo de los grupos de Informática y de Organización y Métodos.

Los tres grandes grupos amén de los otros que he mencionado a lo largo de este punto son Desarrollo de Informática, Soporte Técnico en Internet y los Proveedores, de los cuales he formado parte del primero haciendo las primeras aplicaciones de la solución, para lo cual me interesé profundamente en el manejo del

Implantación de una Solución Internet en la Banca

Visual-Age, posteriormente formé parte del grupo de Soporte Técnico y tuve que profundizar aún más en temas de Comunicaciones y Conectividad, mi relación con el Proveedor se volvió muy estrecha ya que serví como nexo entre los Proveedores y la Institución, sobre todo para el seguimiento de incidencias, instalación de productos y nuevas versiones de los mismos así como el monitoreo de la Solución.

II. Soporte Técnico:

II.1 Conceptos Básicos

La solución final a la que deberíamos de llegar contempla varios aspectos, uno de ellos es el de contar con dos equipos similares en cada punto de la solución con lo que estaríamos resolviendo el tema de la “Alta Disponibilidad” que luego adquiriría una importancia grande en el proyecto por su marcada complejidad, Alta Disponibilidad significa que si un equipo no funciona otro similar puede asumir su función de manera inmediata, inicialmente el paso de la operatividad de un equipo a otro se hacía manualmente, posteriormente se harían esfuerzos para que este “cambio” se de en forma automática, otro aspecto importante dentro de la solución es el conocido como “Balanceo de Carga”, este permite que no se sature el uso de un equipo teniendo otro con disponibilidad, es decir, si partimos del principio que siempre son dos los equipos en cada nivel hay que lograr que los equipos estén proporcionalmente compartidos lo que redundará en la consistencia y manejabilidad del sistema permitiendo que el usuario tenga una adecuada respuesta a su requerimiento. Otro aspecto es la resistencia de la solución a las “Pruebas de Esfuerzo”, mediante la cual podemos tener una idea de cuan vulnerable puede ser el sistema ante una gran demanda del Producto, es decir, como es que podría comportarse el sistema si simultáneamente muchos usuarios intentan ingresar a la misma dirección Web, la solución debe de garantizar un adecuado “Tiempo de Respuesta”.

Internet:

La red Internet es hoy en día, la red de computadoras más extensa del planeta, para ser más precisos, Internet es una red que enlaza centenares de miles de redes locales heterogéneas.

Se dice que Internet es “la red de redes”, lo que quiere decir es que Internet está conformado por millones de redes en todo el mundo, las cuales se comunican entre ellas a través de un protocolo denominado TCP/IP (Protocolo de Control de Transmisión(Protocolo Internet).

En 1990, Tim Berners-Lee, un joven estudiante del Laboratorio Europeo de Partículas (CERN) situado en Suiza, desarrolló un nuevo sistema de distribución de información en Internet basado en páginas hipertexto, al que denominó World Wide Web (La “telaraña mundial”). La revolución de la Web había comenzado.

Realmente el concepto de hipertexto no es nuevo: fue introducido por Ted Nelson en 1965 y básicamente se puede definir como texto de recorrido no secuencial. Clicando en las palabras con enlaces (linkS) se puede acceder al documento al que apuntan, que normalmente contiene una información más detallada sobre el concepto representado por las palabras de enlace.

De ordinario, las palabras del enlace aparecen subrayadas y de un color diferente del resto del documento, para que puedan diferenciarse fácilmente. Una vez que han sido clicadas cambian de color, para indicar que el documento al que apuntan ya ha sido visitado. Lo realmente novedoso de la Web es la aplicación del concepto de **hipertexto** a la inmensa base de información accesible a través de Internet.

Por otra parte, lo que inicialmente se había concebido como un sistema de páginas hipertexto, se ha convertido posteriormente en un verdadero sistema **hipermedia**, en el que las páginas permiten acceder a imágenes, sonidos, videos, etc. Ello ha incrementado aún más el atractivo de la Web.

Además de Internet, existen en la actualidad numerosas Intranet, es decir redes basadas en los mismos conceptos de hipertexto e hipermedia y en las mismas tecnologías de Internet, pero con un ámbito mucho más limitado. Por lo general, las Intranets se reducen al marco de una empresa, de una institución, de un centro educativo, etc... en general carecen de interés para otros usuarios del exterior, por el tipo de información que ofrecen.

Durante mucho tiempo ha estado limitado el uso comercial de Internet, esto se debe a que la red está sostenida casi en su totalidad por fondos gubernamentales ya que su propósito era estrictamente académico. Las políticas que restringían el uso de la red han empezado a cambiar, lo cual es beneficioso para los negocios pequeños que no cuentan con los recursos necesarios para mantener una red nacional privada como lo hacen las grandes corporaciones. Gradualmente se irán eliminando las políticas restrictivas, permitiendo así dar un apoyo a las industrias que aprovechen esta ventaja además de incrementar los servicios que se ofrecen en la red. También se reducirán los costos, y la gente podrá comprar este servicio a precios accesibles.

Las tecnologías se mejoran para adaptarse a la enorme demanda que se espera en los próximos años, el incremento en la velocidad de transmisión y la reducción en los precios ampliarán la gama de servicios existentes y permitirán otros servicios que hoy no son factibles.

Al mismo tiempo que ocurra la comercialización se dará también la privatización. Durante años la comunidad Internet ha solicitado a las compañías telefónicas que provean conexiones IP de la misma forma que dan líneas telefónicas, pero esto parecía no importarles, ahora que las empresas comienzan a interesarse en

Implantación de una Solución Internet en la Banca

Internet, las compañías telefónicas han visto un gran negocio y van a presionar para que el gobierno reduzca los subsidios y sean ellas las que den el servicio. Esto significa que las instituciones comerciales o educativas tendrán que pagar la parte que les corresponde por estar en Internet y el apoyo del gobierno se retirará gradualmente.

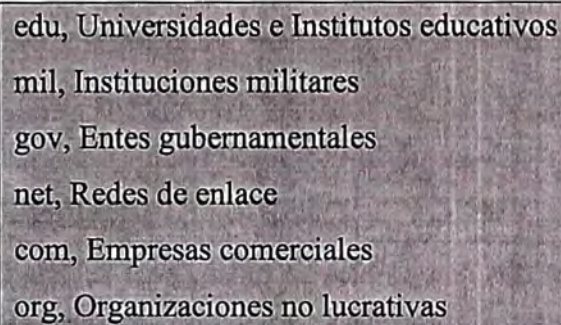
Esto es justo para las empresas que obtengan una utilidad, pero puede ser perjudicial para las universidades que dependen de los apoyos gubernamentales.

Finalmente se dará una fusión entre las tecnologías de telecomunicaciones para crear un nuevo tipo de redes que incluya a las compañías telefónica, televisoras y de servicios informativos, para que juntas conformen a lo que se conoce con el nombre de supercarreteras de información.

Para poder utilizar cualquier servicio dentro de Internet se va a tener que especificar al menos una dirección. Todas las computadoras conectadas a Internet tienen una dirección numérica e irrepitable llamada dirección IP (132.248.54.10), la cual sirve para identificar con quien o que te vas a conectar.

Evidentemente resulta mucho más sencillo recordar una cadena de palabras que asocian un significado que una cadena de números, es por esto que se creó el DNS (Domain Name System) el cual consiste en una base de datos que contiene las equivalencias entre las palabras y los números.

La terminación de las direcciones puede dar una idea de la naturaleza del organismo que la posee:



edu, Universidades e Institutos educativos
mil, Instituciones militares
gov, Entes gubernamentales
net, Redes de enlace
com, Empresas comerciales
org, Organizaciones no lucrativas

Correo electrónico

Millones de personas leen su correo electrónico (e-mail) diariamente. El e-mail se usa a través de una aplicación que te permite enviar y recibir cartas y archivos a una o varias personas que posean una cuenta en Internet, o inclusive a sistemas capaces de procesar la información enviada.

Las listas de correos fueron creadas para que las personas con interese comunes puedan discutir sobre un tópico específico a través del correo electrónico.

FTP:

File Transfer Protocol, permite conectarse a un sistema remoto y transferir archivos a tu computadora (download) o de tu computadora al servicio remoto (upload). Muchos de los sitios de FTP permiten ser accesados de forma anónima, es decir que no necesitas una cuenta para poder entrar.

Telnet:

Herramienta creada para establecer sesiones remotas en otras máquinas.

Archie:

Es un sistema de búsqueda de archivos para los servidores de FTP anónimos.

Gopher:

Significa topo o algo parecido a una ardilla, es el primer programa que fue hecho para facilitar la navegación en Internet.

IRC:

Es un sistema que permite “platicar” interactivamente con varias personas a la vez, sin importar que éstas se encuentren al otro lado del mundo.

Finger:

Permite ver quienes están conectados en un momento determinado a la red.

Verónica:

Es un servicio de búsqueda por palabras dentro de los títulos de los menús en todos los servidores Gopher del mundo, es para Gopher lo que Archie es para FTP.

WWW.

Es la telaraña de cobertura mundial, no existe un centro que administre esta red de información, está basado en un modelo de cliente-servidor, utilizando el protocolo http.

Los componentes básicos son:

1. El usuario Internet:

Que puede estar en su casa, en una cabina o en cualquier ambiente pero que debe contar con las especificaciones mínimas necesarias como para que el sistema funcione.

La solución se ha orientado básicamente a usuarios que poseen navegadores tipo Netscape y Explorer, específicamente versiones iguales o superiores a Internet Explorer 4.0 y Netscape 4.5.

2. Telefónica:

Los enlaces son importantes en este punto, la caída de los circuitos digitales o la mala calidad de la línea en algún tramo de la comunicación puede incidir grandemente en el tiempo de respuesta de la aplicación al cliente o usuario final. Este proveedor juega un papel importante en la disponibilidad del servicio y es responsable de la solución, sobre todo desde que el usuario externo solicita el requerimiento es dirigido hacia algunas de sus centrales, ya sea Washington o San Isidro y desde allí enlazadas a "Modems" que se comunicarán cada uno con "Routers" que finalmente también se comunicarán con "Switches" ya en el interior de nuestra instalación. La responsabilidad de este proveedor va desde la salida de los usuarios hasta los "Routers".

El proveedor ha designado un equipo de trabajo que permanece en nuestras instalaciones de manera permanente, no sólo para ver el tema de Internet sino todos aquellos en que la comunicación a través de Telefónica se da.

3. Routers:

Estos dispositivos son importantes porque permiten la interpretación de los protocolos provenientes del exterior a la red interna del banco, la funcionalidad de los “Routers” no se está explotando de manera total ya que en principio reciben un protocolo IP y lo vuelcan a otro protocolo IP con lo que no existe conversión sino simplemente interpretación, eso no quita que en el futuro sin ningún costo adicional podamos comunicar desde el exterior protocolos diferentes al IP y convertirlos a IP para su ingreso a la red interna.

Como mencionara anteriormente, hay una comunicación desde la nube de Internet específicamente desde las centrales de Telefónica, Washington y San Isidro hacia los dos “Routers” vía MODEM.

El ancho de Banda entre la Nube (“Modems”) y los “Routers” es de 512K.

Los usuarios internos, es decir aquellos que forman parte de la corporación, no necesitan ir hasta la nube para consultar las páginas que se almacenan en nuestro WAS, para lo cual se ha diseñado un circuito especial que permite que a través del “Back-Bone” (Red de Anillos) las peticiones de los usuarios se dirijan directamente a estos “Routers” sin salir a la nube de Internet, con el consiguiente ahorro en los tiempos de respuesta.

4. Firewalls Externos:

Hago hincapié de que se tratan de firewalls externos para diferenciarlos de los internos, su importancia es vital porque al estar contenido de reglas sólo dejan pasar direcciones que son aceptables por el sistema (Filtrado), evitando el ingreso de intrusos, para los que en especial también se cuentan con “detectores de intrusión”.

5. Switches:

Son las unidades de conexión entre redes. Para el diseño, se han considerado switches para la parte insegura, segura, monitoreo y control.

A diferencia de los simples “Hubs”, estos Switches permiten en cada puerto la conectividad de redes, es decir, cada puerto puede comportarse como un anillo autónomo.

En la zona insegura, la nube se comunica con nuestras instalaciones a través de los “Routers”, de ahí, de los “Routers” como se mencionó anteriormente la comunicación es hacia cada uno de los “Switches”. La idea es tener los “Switches” de a dos es para que puedan hacer frente al tema de la “Alta Disponibilidad”, conectados a estos primeros “Switches” están el primer par de “Firewalls” que son componentes de filtrado. Los componentes no pueden comunicarse entre sí si no es a través de los “Switches”.

Inmediatamente después de pasar por los “Firewalls”, se hará uso de otro par de “Switches” y en este nivel se pueden comunicar el “Portal”, los “Webseals”, el Detector de Intrusión y el otro juego de “Firewalls” (Firewalls Internos).

También hay otro juego de “Switches” que están en la zona segura y que permiten la conectividad entre los “Firewalls Internos”, el “Policy Director”, Los “Web Application Server” y el “Host”.

Adicionalmente hay otro juego de “Switches” que permiten comunicar los “Firewalls Internos”, y las “Consolas de Firewalls”, el “Tívoli”, la “Consola de Operación” y una impresora de uso de operaciones.

6. Servidor Webseal (Policy Director):

El concepto de “Gabinete” (mueble en donde se alojan los equipos) es importante porque permite entender cómo no solamente la “Alta Disponibilidad” puede darse sino cómo contribuir para que ésta efectivamente se de, los diferentes componentes en principio no deberían estar en el mismo gabinete ya que si éste se quemara por mucho que haya alta disponibilidad por el hecho de estar juntos, ambos componentes, el original dañado y el alternado, no podrían trabajar ya que resultarían dañados.

El “Network Dispatcher” es un componente lógico instalado en el Servidor donde también se encuentra alojado el “Webseal” cuya función principal es el Balanceo de Carga y la Alta Disponibilidad, el “Network Dispatcher” es el que se comunica con el “Webseal” en última instancia pero mantiene una comunicación viva con el otro “Network Dispatcher” del otro servidor ya que trabaja bajo la modalidad de imagen. Si solo hubiera un “Webseal”, no sería necesario contar con un “Network Dispatcher”.

El “Webseal” es un web-Server que forma parte del producto “Policy Director”, cuando las solicitudes del cliente llega al nivel de “Network Dispatcher” el “Policy” ya distribuyó información necesaria para la administración a los respectivos “Webseals” de manera que éstos no tengan necesidad de ir al “Policy” a requerir de información. En el “Policy” se encuentran los permisos (“ACLs”), los grupos y los usuarios en cuanto a perfiles. Es el gran administrador del sistema de Seguridad del sistema.

En un primer momento los “Webseals” solicitan información al “Policy Director” en su primera descarga, de ahí en adelante el “Policy Director” cada cierto tiempo que puede ser programado y en general no supera los 5 o 10 minutos o cuando hay un cambio a nivel de definición de “Policy”, refresca la información en los respectivos “Webseals” de manera que estos tengan los últimos detalles o modificaciones y no tengan que ir a leerlos del “Policy”.

La comunicación “Policy Director—Webseal” es a través del protocolo “DCE”.

El “Webseal”, dependiendo del tipo de requerimiento, si se trata de una página protegida o no, buscará la información del “Policy” que tiene grabada en su propio servidor y requerirá de conversar directamente con el “LDAP” que es el otro componente que administra el directorio de usuarios cuyo contenido tampoco se encuentra en la misma máquina sino externamente a fin de poder aplicar el concepto de la “Alta Disponibilidad”, con sus respectivas claves e información adicional, una vez solicitado su concurso devolverá un código de error que a su vez permitirá que el “Webseal” decida si pasar o cancelar la transacción.

Cuando menciono el hecho de pasar o cancelar, quiero hacer referencia a un concepto que es muy mencionado pero pocas veces entendido, el “Proxy Inverso”, el “Webseal” funge como “WebServer” del Cliente y a su vez se convierte en Cliente del “I-Planet” que es otro componente Web-Server que posteriormente se analizará, y que a su vez a través de un “Plug-in” se comunicará con el WAS o Web Application Server.

Este servidor contendrá dos productos, el “Network Dispatcher” y el “Webseal” con su manejador propio de Base de Datos denominado “LDAP”.

La “Alta Disponibilidad” se da entre el “LDAP” y el “Policy Director”, se tendrán dos servidores con los dos productos montados en cada uno de ellos, el “LDAP” permanecerá inhibido en el primer servidor dejando solamente operativo el “Policy”, en el segundo servidor se dejará inhibido el “Policy” dejando habilitado el “LDAP”, así si se cae un servidor, el otro componente inhibido automáticamente se habilitará vía un software denominado HACMP.

7. Portal:

Inicialmente no contábamos con esta facilidad, el Portal no es más que una página Web con la posibilidad de poder mostrar información estática a los clientes, no necesita ingresar a la aplicación propiamente dicha que reside mucho más atrás y que se encarga de la elaboración de las transacciones que se comunican con el Host, sin embargo el Portal cumple una función importantísima ya que provee de información fresca para el cliente interesado en saber por ejemplo sobre la bolsa, oficinas, productos, etc... que brinda la institución.

8. Firewalls Internos:

La institución posee dos conjuntos de “Firewalls”, un grupo que son los externos a los que ya hice referencia anteriormente y otros que son los internos, éstos no se diferencian en nada más que en las direcciones IP a usar y en el contenido de sus respectivas reglas que no podría ni mencionar por el carácter reservado y confidencial que atañen.

Este trabajo no pretende brindar información confidencial ya que se atentaría contra la ética y la confianza que puede sentir una institución hacia sus trabajadores por lo que me limitaré simplemente a mencionarlos como parte crucial en el esquema de la seguridad en un entorno de Internet.

Un HACKER haría mal uso de la información de las reglas y podría llevar a la bancarrota a una institución financiera si fuera el caso, no sólo por lo que podría hacer con las cuentas sino por el problema de imagen (altamente vulnerable) que dejaría en los clientes que optarían por retirar su dinero o dejar de hacer transacciones en una entidad financiera donde no existiera confidencialidad.

En principio, cualquier equipo puede hacer de “Firewall”, lo que lo diferencia es que soporte el software ““firewall”” propiamente dicho, para la solución planteada se escogió como Servidor un equipo “Sun” y como Sistema

Operativo “Solaris”, hasta ahí no sería un “Firewall” sin la presencia del “Firewall1” software proporcionado por la firma “Checkpoint” que permite la definición, manejo y control de las reglas. Este “Firewall1” corre por encima del “Solaris” que no es más que un UNÍX personalizado para este tipo de equipos “Sun” como también lo es el AIX para los equipos RS6000.

“La Alta disponibilidad” y el “Balanceo de Cargas” solo son posibles a través del producto “Stonebeat” que se monta sobre el “Solaris” y que permite justamente estas dos funciones que no serían posibles de ejecutar si no trabajaran en pareja.

El requerimiento que se destina a los “Firewalls” va a un IP Maestra que a su vez contiene la dirección de los dos “Ips” que trabajan bajo la modalidad de Cluster, es decir, en ese momento ambos “Firewalls” reciben el mismo requerimiento pero solo uno de ellos será el que finalmente atienda el requerimiento y esto es porque el “Stonebeat” decidirá por ellos.

Los 4 “Firewalls” están conectados a una consola gráfica que permite que pueda grabarse la información que pasa por ellos tanto de ida como de vuelta, se utiliza adicionalmente un software que permite la explotación de la información guardada conocido como “Wordtrends”.

9. Servidor Websphere Application Server:

Este servidor incluirá tres productos, el “I-Planet” que reemplazó anteriormente a un “Network Dispatcher” como publicador de páginas, el WAS o la aplicación propiamente dicha y el DB2 como base de Datos de la Aplicación. Inicialmente la Base de Datos trabajó en un mismo Servidor con el WAS, posteriormente se deshabilitó el DB2 del servidor y se le colocó en otro para que trabaje de manera independiente.

El esquema es como sigue:

Tenemos dos servidores, uno se denominará “Web Appplication Server (WAS1)” y el otro WAS2. En el Was1 se incluirá el “I-Planet”, el “WAS” propiamente dicho y el DB2 pero solo como “Cliente”, adicionalmente este servidor contendrá de manera natural los “Volumen Groups” y “File Systems” correspondientes a la data tanto de la aplicación como de la misma máquina. En el otro WAS también habrá un “I-Planet”, el “WAS” propiamente dicho y el “DB2” pero en este caso como Server, en este caso la máquina aparte de tener los volumen groups propiamente de la máquina contendrá los file systems correspondientes al DB2.

Si se cae el WAS1, los “filesystems” correspondientes a la aplicación en el WAS1 correrán automáticamente a formar parte de los “filesystems” del “WAS2”, con lo que el esquema de la alta disponibilidad quedaría garantizado. Si se cae el “WAS2” el “filesystem” correspondiente al DB2 que actuaba en el WAS2 pasa al WAS1 y el DB2 en el WAS1 que actuaba como Cliente pasa a actuar como Servidor.

Todo esto es posible gracias a un producto que se encarga de evaluar a ambos servidores y que permite la alta disponibilidad, su nombre es el “ACNP”.

La alta disponibilidad no se ha logrado totalmente ya que la “data” es única, solo la alta disponibilidad tiene efecto sobre los sistemas operativos, la data esta en un solo “Drower”, para que la alta disponibilidad sea total se necesitaría otro “Drower” y la configuración de discos de tal manera que permita la doble grabación, esto significaría una mayor inversión económica.

10. MQ-Series:

Elemento crucial para el manejo de los mensajes a ser transmitidos al Host. Existe un MQ a nivel de RS-6000 que contiene también el WAS y otro a nivel de Host que se encargarán de encapsular y desencapsular paquetes. El MQ trabaja bajo SNA que también tiene su contrapartida en el Host con un SNA de similares opciones.

11. SNA:

Elemento de comunicaciones que se conectará definitivamente con el Host para el envío y transmisión de información.

Se ha preferido usar SNA en vez de IP porque resulta ser más seguro y barato, se está pensando en una alternativa que consistiría en usar IP como medio de transmisión pero tener los paquetes encapsulados bajo SNA, así el "Hacker" aún conociendo la dirección IP del componente no podrá entender el mensaje por la protección natural que brinda el SNA.

El SNA es software y se montará sobre el enlace entre una tarjeta "Ethernet" del RS-6000 y la tarjeta "OSA" del "Host" a través de un SWITCH.

Una vez instalada la conexión SNA RS-6000 y Host el MQ estará listo para poder encapsular mensajes.

***Nota:** Debe entenderse que tanto el MQ como el SNA no son los mismos que se utilizan para los computadores grandes aunque su funcionalidad sea similar.*

12. Aplicación Host:

Esta aplicación debe estar preparada para reconocer el canal por donde llega el requerimiento y así activar los diferentes módulos necesarios que habrían de hacer que el Sistema pueda devolver el requerimiento solicitado. La aplicación en el Host es multicanal y está preparada como para poder reconocer de qué canal llega el requerimiento, es decir si se trata de una oficina, de un cajero o de un internauta.

Tuve participación en la implementación, desarrollo y mantenimiento de la parte de oficinas, del software que da cara al Host pero en cada una de las oficinas, se tuvo que cambiar en esa oportunidad un software bajo Visual Basic en los terminales de oficina con un "CICS/OS2" como servidor bajo la comunicación de "Named Pipes", el software de ventanilla se denominó "ALDO" (Automatización en Línea De Oficinas).

II.2 Networking.

- **Técnicas de acceso al LAN:**

El Ancho de Banda no es la única medida de performance en un LAN. Una estación debe ganar acceso al LAN para poder utilizar su ancho de banda. Todos los LANs tienen una forma de control de Acceso. Algunos LANs también proporcionan una forma de Prioridad de Acceso. Esta es la base para la Reserva del Ancho de Banda.

- **Access Token-Passing**

Transmite cuando recibe el Token libre, libera un token después de la transmisión, posee una estructura de ocho niveles de Reserva de Prioridad.

- **Seguridad de Datos**

La seguridad de datos puede ser el principal requerimiento en algunas aplicaciones. Medio Compartido: Los datos pasan a través de todas las estaciones en el segmento. Medio Dedicado: Los datos son dirigidos a la estación de destino sin pasar por otras estaciones.

- **Ethernet**

Ancho de Banda: 10 Mbps, Compartido, Half Duplex.

Acceso: CSMA/CD

Medio: Coax, STP, UTP & Fiber.

Excelente bajo costo en soluciones para grupos de trabajo: Ancho de banda adecuado para aplicaciones basadas en caracteres, el método de acceso se afecta bajo cargas fuertes, no es recomendable para aplicaciones en la que el tiempo de respuesta es crítico.

Puede crecer más allá de los grupos de trabajo: La segmentación para reducir los dominios de colisión es una solución probada. El empleo de la tecnología Ethernet Switching es muy recomendado, se puede añadir administración vía la tecnología de “hub” inteligente.

- **Token-Ring**

Ancho de Banda: 16/4 Mbps, Compartido, Half Duplex

Acceso: Token, 8 niveles de Prioridad de Acceso

Medio: STP, UTP & Fiber

Ventajas: Método de Acceso... Proporciona performance predecible aún bajo cargas fuertes, está basado en la calidad de servicio, posee 8 niveles de prioridad de servicio. Alto nivel de administración en la Capa Física: Recuperación

automática de fallas en cableado o tarjetas, aísla errores de software excesivos en un dominio que falla.

Desventajas: Componentes más caros que Ethernet.

- **Hub**

La selección de un Hub es un factor estratégico para el diseño de una red ya que el hub define la infraestructura de la red.

Fundamentalmente es un dispositivo de la capa física, puede venir de muchas formas, homogéneos o heterogéneos, inteligentes o no, administrables o no.

La capacidad del Hub estará determinada por la disponibilidad de la red, el nivel de control y la administración.

El diseño de los Hubs pueden hacer que el crecimiento y la migración sea sencilla o complicada.

- **Bridges:**

Conectan los Lan (locales o remotos)

Operan en la capa 2 del modelo OSI (sub-capa MAC)

Transparente a los protocolos de comunicación que se utilizan
(capa2,5)

Usa algoritmos sencillos para pasar los frames.

- **Router:**

Conectan LANs a LANs, LANs a WANs, WANs a WANs

Opera en la capa 3 del modelo OSI

Es independiente del protocolo, el router debe de soportar el protocolo de comunicación específico que se utiliza en la capa 3. Utiliza algoritmos complejos de enrutamiento.

- **Gateway:**

Conectan LANs con LANs, LANs con WANs y WANs con WANs

Opera de la capa 3 a la capa 7 del modelo OSI

Realiza conversión de protocolo

II.3 Modelo OSI de Comunicaciones

Modelo basado en capas. La International Organization for Standardization (ISO) es un organismo internacional que tiene a su cargo una amplia gama de estándares, incluyendo el modelo OSI de comunicaciones y de los protocolos OSI. También existe la American National Standards Institute (ANSI) que es el cuerpo coordinador para grupos voluntarios de estándares dentro de los Estados Unidos. ANSI es un miembro de ISO. Uno de los estándares más conocidos de ANSI es FDDI. El Electronic Industries Association (EIA) es un grupo que especifica estándares eléctricos para transmisión. El más conocido estándar de EIA es el RS-232. El Institute of Electrical and Electronic Engineers (IEEE) es una organización profesional que define estándares para redes. Los estándares más conocidos de la IEEE son los estándares de LAN IEEE 802.3 e IEEE 802.5 (ethernet y token-ring). Consultative Comité for International Telegraph and Telephone (CCITT) es una organización internacional que desarrolla estándares de comunicación. X25 es el estándar más conocido de CCITT.

Internet Activities Board (IAB) es un grupo de investigadores de internetwork que se reúnen regularmente para discutir temas pertinentes a Internet. Este grupo fija la mayoría de las políticas para Internet discutiendo y asignando temas a grupos de trabajo. Algunos de los Request form Comments (RFC) son

designados por la IAB como estándares para Internet, incluyendo Transmisión Control Protocol/Internet Protocol (TCP/IP) y el Simple Network Management Protocol (SNMP).



- **Física:**

Define las características eléctricas, mecánicas, los procedimientos para la activación. Mantenimiento y desactivación del enlace físico entre los sistemas.

- **Enlace Datos:**

Proporciona una transmisión de datos confiable a través de un medio físico. Tiene que ver con la dirección física, la topología de red, protocolos de línea, notificación de errores, entrega ordenada de datos y control de flujo.

- **Red:**

Proporciona conectividad y selección de rutas entre dos sistemas que pueden estar geográficamente separados y pertenecer a otras redes.

- **Transporte:**

Proporciona el servicio de transporte que aísla las capas superiores de los detalles de establecimiento, mantenimiento, finalización de los circuitos virtuales, detección y recuperación de fallas en el transporte, control de flujo, etc.

- **Sesión:**

Establece, administra y finaliza las sesiones entre las aplicaciones. Regula el diálogo entre las capas de presentación, mejora la eficiencia de la transmisión con clase de servicio, reporte de errores por excepción.

- **Presentación:**

Se asegura que la información enviada por capa superior podrá ser leída por la capa de aplicación del otro sistema. Tiene que ver con el formato, estructura de datos, conversión de códigos, etc.

- **Aplicación:**

Contiene una variedad de protocolos que se necesitan frecuentemente para: identificar, sincronizar, establecer procedimientos de recuperación, etc, entre dos sistemas que se van a comunicar.

II.4 Arquitectura TCP/IP

TCP/IP significa Transmisión Control Protocol/Internet Protocol

Protocolo Internet (IP)

La Arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos por la ISO, IICC, etc...

Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU), y con la expansión de la INETERNET se ha convertido en una de las arquitecturas de redes más difundidas.

El modelo OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por cuatro niveles: **el nivel subred (enlace y físico), el nivel interred (Red, IP), el protocolo proveedor de servicio (Transporte, TCP o UDP), y el nivel de aplicación.**

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP.

Las características de este protocolo son:

- No orientado a conexión
- Transmisión de unidades denominadas datagramas
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

La entrega del datagrama IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje.

Por otra parte, el IP no contiene suma de verificación para el contenido de datos del datagrama, solamente para la información del encabezado.

En cuanto al ruteo (encaminamiento) este puede ser:

- Paso a paso a todos los nodos
- Mediante tablas de rutas estáticas o dinámicas

El TCP/IP utiliza una dirección de 32 bites para identificar una máquina y la red a la cual está conectada. Únicamente el NIC(Centro de información de Red)

asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro) aparecen en la figura:



Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir.Local (hostid) en donde se identifica la red y el host dentro de la red. La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits (de orden más alto).

Las direcciones de Clase A corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 hosts en cada una.

Las direcciones de la Clase C tienen solo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Por último, las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.255.255.

Cabe decir que, las direcciones de Clase E (aunque su utilización es futura) comprenden el rango de 240.0.0.0 hasta 247.255.255.255.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits. Por comodidad estos bits se representan como si estuviesen separados por un punto, por lo que el formato de dirección IP puede ser red.local.local.local. para Clase A hasta red.red.red.local para Clase C.

A partir de una dirección IP, una red puede determinar si los datos se enviarán a través de una compuerta (GTW, ROUTER). Obviamente, si la dirección de la red es la misma que la dirección actual (enrutamiento a un dispositivo de red local, llamado *host directo*), se evitará la compuerta; pero todas las demás direcciones de red se enrutarán a una compuerta para que salgan de la red local. La compuerta que reciba los datos que se transmitirán a otra red, tendrá entonces que determinar el enrutamiento con base en la dirección IP de los datos y una tabla interna que contiene la información de enrutamiento.

Otra de las ventajas que ofrece el direccionamiento IP es el uso de **direcciones de difusión** (broadcast addresses), que hacen referencia a todos los hosts de la misma red. Según el estándar, cualquier dirección local (hostid) compuesta toda por 1s está reservada para difusión (broadcast). Por ejemplo, una dirección que contenga 32 1s se considera un mensaje difundido a todas las redes y a todos los dispositivos. Es posible difundir en todas las máquinas de una red alterando 1s a toda la dirección local o de anfitrión (hostid), de manera que la dirección 147.10.255.255 para una red de Clase B se recibiría en todos los dispositivos de dicha red; pero los datos no saldrían de dicha red.

Ejemplo 1:

Consideramos la siguiente dirección IP en binario:

11001100.00001000.00000000.10101010 (204.8.0.170)

La dirección de la máscara (MASK) es en binario:

11111111.11111111.11100000.00000000 (255.255.224.0)

Según lo visto anteriormente, para hallar la dirección de Subred (SubNet) tomamos la IP y considerando que todo lo que tenga 1s en la máscara se queda como esta en la IP, y todo lo que tenga 0s en la máscara se pone a 0 en la IP. Entonces, la dirección de Subred es:

11001100.00001000.00000000.00000000 (204.8.0.0)

Ejemplo 2:

Sea la dir IP 201.222.5.121, la dirección MASK 255.255.255.248, entonces haciendo los correspondientes cálculos binarios se tendrá la dirección resultante:

201.222.5.120	, donde....
201.222.5.121	=> Primera máquina de la subnet
201.222.5.122	=> Segunda máquina de la subnet
201.222.5.126	=> Ultima máquina de la subnet
201.222.5.127	=> Broadcast

La mayor ventaja de la codificación de la información de red en las direcciones de red en IP es hacer posible que exista un ruteo eficiente, otra ventaja es que las direcciones de red IP se pueden referir tanto a redes como a anfitriones (hosts). Por regla, nunca se asigna un campo "hostid" igual a 0 a un anfitrión individual, en vez de eso, una dirección IP con campo hostid a 0 se utiliza para referirse a la red en sí misma, en resumen:

Las direcciones IP se pueden utilizar para referirse a redes así como a anfitriones individuales. Por regla, una dirección que tiene todos los bits del campo hostid a 0, se reserva para referirse a la red en sí misma.

Protocolo de Control de Transmisión (TCP)

En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir debido a errores (falla el hardware, sobrecarga en la red,...) Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega de conexión y no confiable para transferencias de grandes volúmenes de información resulta ser la peor opción. Debido a esto, el TCP se ha vuelto un protocolo de propósito general para estos casos.

La interfaz entre los programas de aplicación y la entrega confiable (es decir las características del TCP) se definen en cinco funciones:

Servicio orientado a la conexión: El servicio de entrega de flujo en la máquina destino pasa al receptor exactamente la misma secuencia de bytes que le pasa el transmisor en la máquina de origen.

Conexión de Circuito Virtual: Durante la transferencia, el software de protocolo en las dos máquinas continúa comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo, ambas máquinas detectarán la falla y la reportarán a los programas apropiados de la aplicación. Se utiliza el término **circuito virtual** para describir dichas conexiones porque aunque los programas de aplicación visualizan la conexión como un circuito dedicado de hardware, la confiabilidad que se proporciona depende del servicio de entrega de flujo.

Transferencia de Memoria Intermedia: Los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente bytes de datos al software de protocolo. Cuando se transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado, que pueden ser tan pequeñas como un byte. En el extremo receptor, el software de protocolo entrega bytes del flujo de datos en el mismo orden en que se enviaron, poniéndolos a disposición del programa de aplicación receptor tan pronto como se reciben y verifican. El software de protocolo puede dividir el flujo en paquetes, independientemente de las piezas que transfiera el programa de aplicación. Para hacer eficiente la transferencia y minimizar el tráfico de red, las implantaciones por lo general recolectan datos suficientes de un flujo para llenar un datagrama razonablemente largo antes de enviarlo. Por lo tanto, inclusive ahí el programa de aplicación genera el flujo un byte a la vez, la transferencia a través de la red puede ser sumamente eficiente. De forma similar, si el programa de aplicación genera bloques de datos muy largos, el software de protocolo puede dividir cada bloque en partes más pequeñas para su transmisión. Para aplicaciones en las que los datos se deben entregar aunque no se llene una memoria intermedia, el servicio de flujo proporciona un mecanismo de “empuje o push” que las aplicaciones utilizan para forzar una transferencia. En el extremo transmisor, el “push” obliga al software de protocolo a transferir todos los datos generados sin tener que esperar a que se llene una memoria intermedia. Sin embargo, la función de “push” sólo garantiza que los datos se transferirán, por tanto, aún cuando la entrega es forzada, el software de protocolo puede dividir el flujo en formas inesperadas.

Flujo no estructurado: Posibilidad de enviar información de control junto a datos.

Conexión Full Duplex: Se permite la transferencia concurrente en ambas direcciones. Desde el punto de vista de un proceso de aplicación, una conexión full duplex permite la existencia de dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción aparente. Esto ofrece una ventaja: el software subyacente de protocolo puede enviar “datagramas” de

información de control de flujo al origen, llevando datos en la dirección opuesta. Este procedimiento de carga, transporte y descarga **REDUCE EL TRAFICO** en la red.

Existe una aparente contradicción muchas veces sometidas a debates, la pregunta que surge luego de las explicaciones es, **como puede el software subyacente de protocolo proporcionar una transferencia confiable si el sistema subyacente de comunicación sólo ofrece una entrega NO confiable de paquetes?**

La respuesta es complicada, pero la mayor parte de los protocolos confiables utilizan una técnica fundamental conocida como **acuse de recibo positivo con retransmisión**. La técnica requiere que un receptor se comunice con el origen y le envíe un mensaje de acuse de recibo (**ACK**) conforme recibe los datos. El transmisor guarda un registro de cada paquete que envía y espera un ACK antes de enviar el siguiente paquete. El transmisor también arranca un temporizador cuando envía un paquete y lo retransmite si dicho temporizador expira antes de que llegue un ACK.

El problema final de la confiabilidad surge cuando un sistema subyacente de entrega de paquetes lo duplica. Los duplicados también pueden surgir cuando las redes tienen grandes retrasos que provocan la retransmisión prematura. Para evitar la confusión causada por ACKs retrasados o duplicados, los protocolos de acuse de recibo positivos envían los números de secuencia dentro de los ACKs, para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes.

Pero, como casi todo en esta vida es un problema tras otro, el TCP no iba a ser menos; uno de los problemas que acarrea lo anterior es que un protocolo simple de acuses de recibo positivos ocupa una cantidad sustancial de ancho de banda de red debido a que debe retrasar el envío de un nuevo paquete hasta que reciba un ACK del paquete anterior.

La solución esta en otra técnica conocida como **ventana deslizante**, que es una forma más compleja de acuse de recibo positivo y retransmisión. Los protocolos de ventana deslizante utilizan el ancho de banda de red de mejor forma al permitir que el transmisor envíe varios paquetes sin esperar el ACK.

Al igual que el UDP, el TCP reside sobre el IP en el esquema de estratificación por capas de protocolos. El TCP permite que varios programas de aplicación en una máquina se comuniquen de manera concurrente y realiza el “demultiplexado” del tráfico TCP entrante entre los programas de aplicación. Así mismo, al igual que el UDP, el TCP utiliza números de **puerto de protocolo** para identificar el destino final dentro de una máquina. Cada puerto tiene asignado un número entero pequeño utilizado para identificarlo. Para comprender el significado de un puerto hay que pensar de cada puerto como en una cola de salida en la que el software de protocolo coloca los datagramas entrantes, aunque en realidad los puertos TCP son más complejos, ya que un número de puerto no corresponde a un solo objeto. El TCP utiliza la conexión, no el puerto de protocolo, como su abstracción fundamental; las conexiones se identifican por medio de un par de puntos extremos.

Un punto extremo es un par de números enteros (host, puerto), en donde **host** es la dirección IP de un anfitrión y **puerto** es un puerto TCP en dicho anfitrión.

Las conexiones vienen definidas por dos puntos extremos, y es más: la abstracción de la conexión para TCP permite que varias conexiones compartan un punto extremo (por ejemplo, varias conexiones en los mismos puertos). Esto es posible porque el TCP identifica una conexión por medio de un par de puntos extremos, y por eso varias conexiones en la misma máquina pueden compartir un número de puerto TCP.

La interfaz SOCKET

En primer lugar hemos de distinguir entre los protocolos de interfaz y el TCP/IP, debido a que los estándares no especifican exactamente cómo es que interactúan los programas de aplicación con el software de protocolo.

UNIX fue desarrollado y diseñado como un sistema operativo de tiempo compartido para computadoras uniprosesador. Se trata, como ya es sabido, de un S.O orientado a proceso, en el que cada programa de aplicación se ejecuta como un proceso de nivel usuario. Derivados de los MULTICS, los primitivos sistemas de E/S de UNIX siguen un paradigma conocido como "Open-Read-Write-Close": antes de que un proceso de usuario pueda ejecutar operaciones de E/S, llama a Open para especificar el archivo o dispositivo que se va a utilizar (recuerde la independencia de dispositivo de UNIX) y obtiene el permiso. La llamada a OPEN devuelve un pequeño entero (el descriptor de archivo) que el proceso utiliza al ejecutar las operaciones de E/S en el archivo abierto. Una vez abierto un objeto, se pueden hacer las llamadas Read y/o Write. Tanto read como Write toman tres argumentos (descriptor de archivo, dirección del buffer y nº de bytes a transferir). Una vez completadas estas operaciones el proceso llama a Close.

El "socket" es la generalización del mecanismo de acceso a archivos de Unix que proporciona un punto final para la comunicación. Al igual que con el acceso a archivos, los programas de aplicación requieren que el S.O (Sistema Operativo) cree un socket cuando se necesite. El S.O devuelve un entero que el programa de aplicación utiliza para hacer referencia al socket recientemente creado. La diferencia principal entre los descriptores de archivo y los descriptores de socket es que el sistema operativo enlaza un descriptor de archivo a un archivo o dispositivo del sistema cuando la aplicación llama al Open, pero puede crear sockets sin enlazarlos a direcciones de destino específicas.

Básicamente un socket es una API en la que el servidor espera en un puerto predefinido y el cliente puede utilizar sin embargo un puerto dinámico.

Ejemplo:

Creación de un socket:

Resultado = socket (pf, tipo, protocolo)

Pf especifica la familia de protocolo que se va a utilizar con el socket (PF_INET para TCP/IP)

El argumento “tipo” especifica el tipo de comunicación que se desea (SOCK_DGRAM para servicio de entrega de datagramas sin conexión, o SOCK_STREAM para servicio de entrega confiable de flujo).

Envío de datos:

Write (socket, buffer, length)

Especificación de una dirección local:

Bind (socket, localaddr, addrlen)

Sistema de Nombre de Dominio (DNS)

Los protocolos descritos anteriormente utilizan 32 bits, llamados direcciones de protocolos Internet para identificar máquinas. Aún cuando cada dirección proporciona una representación compacta y conveniente para identificar la fuente y el destino en paquetes enviados a través de la red, los usuarios prefieren asignar a las máquinas nombres fáciles de recordar.

El DNS tiene dos aspectos conceptualmente independientes. El primero es abstracto. Especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto a los nombres. El segundo es concreto: especifica la implantación de un sistema de computación distribuido que transforma eficientemente los nombres en direcciones.

Implantación de una Solución Internet en la Banca

Conceptualmente, la resolución de nombres de dominio procede de arriba hacia abajo, comenzando con el servidor de nombres raíz y siguiendo luego hacia los servidores localizados en las ramas del árbol de la red.

Hay dos formas de utilizar el sistema de nombres de dominio: contactar un servidor de nombres cada vez o solicitar al sistema de servidores de nombres que realice una traducción completa. En este caso, el software cliente forma una solicitud de nombres de dominio que contiene el nombre a resolver, una declaración sobre la clase del nombre, el tipo de respuesta deseada y un código que especifica si el servidor de nombres debe traducir el nombre completamente. Se envía la solicitud a un servidor de nombre para su resolución.

Cuando un servidor de nombres de dominio recibe una solicitud, verifica si el nombre señala un sub-dominio sobre el cual tenga autoridad. Si es así, traduce el nombre a una dirección de acuerdo con su base de datos y anexa una respuesta a la solicitud, antes de enviarla de regreso al cliente. Si el DNS no puede resolver el nombre completamente, verifica que tipo de interacción especificó el cliente. Si el cliente solicita una traducción completa (una resolución recursiva en la terminología DNS), el servidor se pone en contacto con un servidor de nombres de dominio que pueda resolver el problema del nombre y devuelve la respuesta al cliente. Si el cliente solicita una resolución no recursiva (resolución iterativa), el servidor de nombres no puede dar una respuesta. Se genera una réplica que especifica el nombre del servidor que el cliente deberá contactar la próxima vez para resolver el nombre.

Un cliente debe saber como contactar al último DNS para asegurarse de que el DNS puede alcanzar a otros, el sistema de dominio requiere que cada servidor conozca la dirección del último servidor en la raíz. Además, un servidor podría conocer la dirección de un servidor para el dominio de un nivel inmediatamente superior (llamado padre).

II.5 Protocolos

Los protocolos de comunicaciones usados en la solución se pueden dividir en:

- **Protocolos seguros:** tales como el SSL, Kerberos, usados en la protección de la data transportada.
- **Protocolo TCP:** Comunicación en “plano”, fácilmente entendible en cualquier sniffer.
- **Protocolo TCP/UDP:** User Defined Protocol, usada para la comunicación de monitores.
- **Protocolo SNA:** Protocolo de comunicación con el Mainframe S/390

II.6 Esquema General de la Solución

Ver Anexo “6”

El Esquema en Bloques:

1. Seguridad

- ◆ Firewalls Externos
- ◆ Webseal-Network Dispatcher
- ◆ Firewalls Internos
- ◆ LDAP/Policy Director
- ◆ WAS
- ◆ Acceso al Host

2. Zona de Acceso a Internet

- ◆ Routers
- ◆ Switches(2)
- ◆ Monitor de Intrusión
- ◆ Monitor Cisco-Works
- ◆ Simulador de Transacciones
- ◆ Firewalls Externos

3. Zona DMZ

- ◆ Firewalls Externos
- ◆ Switches(2)
- ◆ Monitor de Intrusión
- ◆ Webserver (Portal)
- ◆ Webseal-Networks Dispatcher (2)---Login
- ◆ Firewalls Internos

4. Zona Segura

- ◆ Firewalls Internos
- ◆ Switches(2)
- ◆ LDAP/Policy Director (2) (Autenticación)
- ◆ WAS (2)
- ◆ HOST

5. Zona de Operaciones y Gestión

- ◆ Switches(2)
- ◆ Consola de Real Secure
- ◆ Consola de Firewall-1
- ◆ Consola de Tivoli
- ◆ Consola de Operaciones
- ◆ Firewalls Internos
- ◆ Red DMZ
- ◆ Red Segura

6. Servidores de Desarrollo y Calidad

II.7 Evolución

Cambios de Versiones

Este punto está relacionado con dos situaciones, una es el cambio de versión de un producto como el WAS o el Policy Director y la otra es un cambio de versión en alguna “Clase” dentro de la aplicación Visual-Age.

Cuando se trata de un cambio de un Producto, éste es sometido a consenso por un “Comité de Cambios” que a su vez dictaminará la fecha en que debería de darse previo análisis del impacto que éste signifique. El Comité esta compuesto por personal de muchos grupos de Informática.

Implantación de una Solución Internet en la Banca

Se ha designado una ventana de mantenimiento que puede tomar 4 o 5 horas y que corresponde a las madrugadas, preferentemente durante los fines de semana. En este período se realizará el trabajo el cual, previamente discutido con el área de Soporte Técnico, contendrá “hitos” para volver a lo anterior si es que fallara algo en el camino. Los Cambios técnicos también se harán en los otros ambientes, aunque muchas veces el proceso ha sido en el sentido contrario, primero en Producción y luego en los ambientes de Pruebas.

Para el caso de la aplicación, se maneja de forma similar, con la única excepción de que en este caso sí se tiene que hacer rigurosamente pasando por los diferentes ambientes.

En ambos casos, al final de los trabajos, se comunicará al área de Organización quien con personal idóneo realizará el set de pruebas respectivo que dará conformidad al trabajo, dándolo por concluido.

Optimizaciones

Los cambios pueden tener como origen, corregir un problema, brindar una nueva facilidad o simplemente optimizar el sistema, por lo general el tema de optimización esta más relacionado con el trabajo de Soporte Técnico, se pueden reagrupar “Volumen-Groups”, mejorar tamaño de buffers, número de conexiones, etc, todo esto redundando en un mejor nivel de respuesta, nivel que obliga a una evaluación de los tiempos de respuesta, punto que se tocará de manera muy singular en el transcurso de la presentación de este trabajo.

III. Desarrollo de Informática:

III.1 Aplicación

Conceptos:

Todos estos usados por la solución.

- **Servlets:**

Programas en Java que realizan un trabajo y generan una salida pero que cumplen todas las siguientes características:

- ◆ **Portabilidad:** por estar escritos en Java aseguran su portabilidad entre diferentes plataformas que contengan la JVM.
- ◆ **Rendimiento:** Son instanciados por única vez pudiendo a partir de entonces atender muchas peticiones.
- ◆ **Concepto de sesión:** El servlet mantiene la información acerca de la sesión de un usuario, entre diferentes conexiones al mismo servlet o incluso a conexiones a BD.
- ◆ **Software distribuido:** Un servlet puede pasarle trabajo a otro servlet siempre y cuando esté muy recargado aún estando en diferentes máquinas.
- ◆ **Las ventajas de Java: Modularidad, reutilización u orientación a objetos.**
- ◆ **Multithread:** Dado que los servlets pueden manejar múltiples peticiones concurrentes, es posible implementar aplicaciones colaborativas como una videoconferencia.

- **JSP- Java Server Page**

Nueva tecnología que permite presentar páginas con contenido dinámico en base a "tags" especiales embebidos en el código HTML de la página.

Mediante estos tags podemos incrustar código JAVA para realizar tareas programáticas o bien acceder a un JavaBean para obtener un resultado.

La solución utiliza esta facilidad para mostrar las páginas por lo que no usa la interfase gráfica propia del Visual Age.

- **JavaBeans**

Son componentes hechos en Java reutilizables creados para encapsular una determinada lógica de negocio, un determinado servicio (un acceso a BD) o también pueden almacenar datos. Se utilizan en la construcción de aplicaciones como si fueran piezas de un mecano.

- **Enterprise Java Beans**

Debido a la similitud de nombres se confunden. Mientras que los JavaBeans son lógica de negocio encapsulada, los Enterprise JavaBeans (EJBs) constituyen una filosofía "Cliente/Servidor" y de programación en base a objetos distribuidos en si misma. Los EJBs pueden contactar clientes remotos a los que proporcionan un determinado proceso o función. Normalmente no funcionan por si solos sin ninguna interacción por parte de un cliente.

- **HTML**

HyperText Markup Language o Lenguaje marcador Estándar Generalizado permite desarrollar documentos para la www (World Wide Web).

Se considera un lenguaje fácil, bastante amigable y permite desarrollar aplicaciones rápidas para Internet.

La mayoría de documentos que vemos en la Internet han sido desarrollados usando esta herramienta.

- **XML**

Cuando HTML surgió, desencadenó un fenómeno editorial sin precedentes. Todo tipo de personas en el mundo entero empezaron a editar documentos en la Web. El diseño de páginas web empezó a convertirse en un tema de conversación no solo en la industria informática, sino también en cafeterías y bares. Parecía como si de la noche a la mañana todo el mundo tuviera una página web.

Actualmente, se observa el mismo fenómeno con XML. Los datos, que antes eran una especie de materia binaria no identificada, se han convertido en algo que el ciudadano de pie es capaz de leer y escribir porque es texto. Con XML, está al alcance de todos elaborar datos propios, moldeados y controlados con total libertad.

XML hace de este entorno un lugar más favorable para la interacción de las personas y los negocios entre empresas. XML permite realizar búsquedas más precisas, transferir componentes de software, describir cosas como series de páginas Web o transacciones de comercio electrónico, y mucho más.

XML está no sólo cambiando nuestra manera de pensar los datos, sino también nuestra visión global de la Web.

A diferencia del HTML con el XML podemos crear etiquetas propias que describan con precisión lo que deseamos saber. Por este motivo, las aplicaciones de

clientes pueden tener acceso a cualquier fuente de información de la Web, y en cualquier formato. Pero los datos XML no son solamente datos inteligentes, también son documentos inteligentes: al visualizar la información, el nombre de modelo puede aparecer con una fuente diferente a la del nombre de vendedor o con el precio más bajo resaltado en verde. A diferencia de HTML, el texto no tiene por qué ser presentado de forma uniforme, el texto inteligente XML puede controlar el contenido a transmitir. No es necesario elegir entre información de datos o de documentos; XML integra las dos cosas. Es posible procesar o datos o documentos o ambos simultáneamente.

Con este tipo de flexibilidad, estamos sin duda ante lo que podría denominarse la flamante nueva Web de información estructurada e inteligente.

- **UML:**
Metodología para desarrollo de Aplicaciones Orientadas a Objetos
- **JAVA:**

Java es un lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems, una empresa reconocida por sus estaciones de trabajo UNÍX de alta calidad. Moldeado en base a C++, el lenguaje Java se diseñó para ser pequeño, sencillo y portátil a través de plataformas y sistemas operativos, tanto a nivel de código fuente como en binario. Con frecuencia se dice que Java tiene el mismo origen que HotJava, un visualizador World Wide Web de Sun, como Netscape o Mosaic.

Además, Java proporciona una nueva forma de acceder a las aplicaciones. El software viaja transparentemente a través de la red. No hay necesidad de instalar las aplicaciones, ellas mismas vienen cuando se necesitan. Por ejemplo, la mayoría de los navegadores del Web pueden procesar un reducido número de formatos gráficos (típicamente GIF y JPG). Si se encuentran con otro tipo

de formato, el navegador estándar no tiene capacidad para procesarlo, tendría que ser actualizado para poder aprovechar las ventajas del nuevo formato. Sin embargo, un navegador con soporte Java puede enlazar con el servidor que contiene el algoritmo que procesa ese nuevo formato y mostrar la imagen. Por lo tanto, si alguien inventa un nuevo algoritmo de compresión para imágenes, el inventor sólo necesita estar seguro de que hay una copia en código Java de ese algoritmo instalada en el servidor que contiene las imágenes que quiere publicar. Es decir, los navegadores con soporte Java se actualizan a sí mismos sobre la marcha, cuando encuentran un nuevo tipo de archivo o algoritmo.

Sus orígenes:

Sun Microsystems, líder en servidores para Internet, uno de cuyos lemas desde hace mucho tiempo es “the network is the computer” (lo que quiere dar a entender que el verdadero ordenador es la red en su conjunto y no cada máquina individual), es quien ha desarrollado el lenguaje Java, en un intento de resolver simultáneamente todos los problemas que se le plantean a los desarrolladores de software por la proliferación de arquitecturas incompatibles, tanto entre las diferentes máquinas como entre los diversos sistemas operativos y sistemas de ventanas que funcionaban sobre una misma máquina, añadiendo la dificultad de crear aplicaciones distribuidas en una red como Internet.

Se puede leer más de cinco versiones distintas sobre el origen, concepción y desarrollo del Java, desde la que dice que este fue un proyecto que rebotó durante mucho tiempo por distintos departamentos de Sun sin que nadie le prestara atención, hasta que finalmente encontró su nicho de mercado en la aldea global que es Internet; hasta la más difundida, que justifica a Java como el lenguaje de pequeños electrodomésticos.

Hace algunos años, Sun Microsystems decidió intentar introducirse en el mercado de la electrónica de consumo y desarrollar programas para pequeños dispositivos electrónicos. Tras unos comienzos dudosos, Sun decidió crear una filial,

Implantación de una Solución Internet en la Banca

denominada FirstPerson Inc., para dar margen de maniobra al equipo responsable del proyecto.

El mercado inicialmente previsto para los programas de FirstPerson eran los equipos domésticos: microondas, tostadoras y, fundamentalmente, televisión interactiva.

Este mercado, dada la falta de pericia de los usuarios para el manejo de estos dispositivos, requería unos interfaces mucho más cómodos e intuitivos que los sistemas de ventanas que proliferaban en el momento.

Otros requisitos importantes a tener en cuenta eran la fiabilidad del código y la facilidad de desarrollo. James Gosling, el miembro del equipo con más experiencia en lenguajes de programación, decidió que las ventajas aportadas por la eficiencia de C++ no compensaban con el gran coste de pruebas y depuración. Gosling había estado trabajando en su tiempo libre en un lenguaje de programación que él había llamado "Oak", el cual, aún partiendo de la sintaxis de C++, intentaba remediar las deficiencias que iba observando.

Los lenguajes al uso, como C o C++, deben ser compilados para un chip, y si se cambia el chip, todo el software debe compilarse de nuevo. Esto encarece mucho los desarrollos y el problema es especialmente acusado en el campo de la electrónica de consumo. La aparición de un chip más barato y, generalmente, más eficiente, conduce inmediatamente a los fabricantes a incluirlo en las nuevas series de su cadena de producción, por pequeña que sea la diferencia en precio ya que, multiplicada por la tirada masiva de los aparatos, supone un ahorro considerable. Por tanto, Gosling decidió mejorar las características de "Oak" y utilizarlo.

El primer proyecto en que se aplicó este lenguaje recibió el nombre de proyecto Green y consistía en un sistema de control completo de los aparatos electrónicos y el entorno de un hogar. Para ello se construyó un ordenador experimental denominado *7 (Star Seven). El sistema presentaba una interfaz basada

en la representación de la casa de forma animada y el control se llevaba a cabo mediante una pantalla sensible al tacto. En el sistema aparecía Duke., la actual mascota de Java. Posteriormente se aplicó a otro proyecto denominado VOD (Video on Demand) en el que se empleaba como interfaz para la televisión interactiva. Ninguno de estos proyectos se convirtió nunca en un sistema comercial, pero fueron desarrollados enteramente en un Java primitivo y fueron como su bautismo de fuego.

Una vez más que en Sun se dieron cuenta de que a corto plazo la televisión interactiva no iba a ser un gran éxito, urgieron a FirstPerson a desarrollar con rapidez nuevas estrategias que produjeran beneficios. No lo consiguieron y FirstPerson cerró en la primavera de 1994. Pese a lo que parecía un olvido definitivo. Bill Joy, cofundador de Sun y uno de los desarrolladores principales de UNÍS de Berkeley, juzgó que Internet podría llegar a ser el campo de juego adecuado para disputar a Microsoft su primacía casi absoluta en el terreno del software, y vió en Oak el instrumento idóneo para llevar a cabo estos planes. Tras un cambio de nombre y modificaciones de diseño, el lenguaje Java fue presentado en sociedad en agosto de 1995. Lo mejor será hacer caso omiso de las historias que pretenden dar carta de naturaleza a la clarividencia industrial de sus protagonistas; porque la cuestión es si independientemente de su origen y entorno comercial, Java ofrece soluciones a nuestras expectativas. Porque tampoco vamos a desechar la penicilina aunque haya sido su origen fruto de la casualidad.

Por el momento, es muy probable que el motivo más trayente para aprender Java sea que los “applets” están escritos en este lenguaje. Si este no fuera el caso, el lenguaje Java en sí mismo tiene ventajas significativas sobre los demás lenguajes y otros ambientes de programación que lo hacen adecuado para realizar cualquier tarea de programación.

Java es independiente de la plataforma: Independencia de la plataforma es la capacidad del programa de trasladarse con facilidad de un sistema computacional a otro.

Java es simple: Ofrece toda la funcionalidad de un lenguaje potente, pero sin las características menos usadas y más confusas de éstos. C++ es un lenguaje que adolece de falta de seguridad, pero C y C++ son lenguajes más difundidos, por ello Java se diseñó para ser parecido a C++ y así facilitar un rápido y fácil aprendizaje.

Java elimina muchas de las características de otros lenguajes como C++, para mantener reducidas las especificaciones del lenguaje y añadir características muy útiles como el “garbage collector” (reciclador de memoria dinámica).

No es necesario preocuparse de liberar memoria, el reciclador se encarga de ello y como es un thread de baja prioridad, cuando entra en acción, permite liberar bloques de memoria muy grandes, lo que reduce la fragmentación de la memoria. Java reduce en un 50% los errores más comunes de programación con lenguajes C y C++ al eliminar muchas de las características de éstos, entre las que destacan:

- Aritmética de punteros
- No existen referencias
- Registros (struct)
- Definición de tipos (typedef)
- Macros (# define)
- Necesidad de liberar memoria (free)

Java está orientado a objetos: Para algunas personas, la técnica de programación orientada a objetos sólo es una manera de organizar programas, lo que puede conseguirse con cualquier lenguaje. Sin embargo, trabajar en un ambiente real de programación y lenguaje orientado a objetos, le permite utilizar en su totalidad las ventajas de la metodología orientada a objetos, además de sus capacidades para crear programas flexibles y modulares, así como reutilizar un código.

Java es fácil de aprender.

Java es distribuido: Java se ha construido con extensas capacidades de interconexión TCP/IP. Existen librerías de rutinas para acceder e interactuar con protocolos como “http y ftp”. Esto permite a los programadores acceder a la información a través de la red con tanta facilidad como a los archivos locales.

Java es robusto: Java realiza verificaciones en busca de problemas tanto en tiempo de compilación como en tiempo de ejecución. La comprobación de tipos en Java ayuda a detectar errores, lo antes posible, en el ciclo de desarrollo. Java obliga a la declaración explícita de métodos, reduciendo así las posibilidades de error. Maneja la memoria para eliminar las preocupaciones por parte del programador de la liberación o corrupción de memoria. Además para asegurar el funcionamiento de la aplicación, realiza una verificación de los “byte-codes”, que son el resultado de la compilación de un programa Java. Es un código de máquina virtual que es interpretado por el “interprete Java”. No es el código máquina directamente entendible por el hardware, pero ya ha pasado todas las fases del compilador: análisis de instrucciones, orden de operadores, etc., y ya tiene generada la pila de ejecución de órdenes.

Java proporciona, pues:

- Comprobación de punteros
- Comprobación de límites de arrays
- Excepciones
- Verificación de byte-codes.

Java es de arquitectura neutral: para establecer Java como parte integral de la red, el compilador Java compila su código a un archivo objeto de formato independiente de la arquitectura de la máquina que tenga el sistema de ejecución (Run-Time) puede ejecutar ese código objeto, sin importar en modo alguno la

máquina en que ha sido generado. Actualmente existen sistemas Run-Time para Solaris 2.x, SunOs 4.1.x, Windows 95, Windows Nt, Linux, Iris, Aix, Mac, Apple y probablemente haya grupos de desarrollo trabajando en el porting de otras plataformas.

Java es seguro: La seguridad en el Java tiene dos facetas. En el lenguaje, características como los punteros o el casting implícito que hacen los compiladores de C y C++ se eliminan para prevenir el acceso ilegal a la memoria. Cuando se usa Java para crear un navegador, se combinan las características del lenguaje con protecciones de sentido común al propio navegador.

El lenguaje C, por ejemplo, tiene lagunas de seguridad importantes, como son los errores de alineación. Los programadores C utilizan punteros en conjunción con operaciones aritméticas. Esto le permite al programador que un puntero referencie a un lugar conocido de la memoria y pueda sumar (restar) algún valor, para referirse a otro lugar de memoria. Si otros programadores conocen nuestras estructuras de datos pueden extraer información confidencial de nuestro sistema.

Java es portable: Más allá de la portabilidad básica por ser de arquitectura independiente, Java implementa otros estándares de portabilidad para facilitar el desarrollo. Los enteros son siempre enteros y además, enteros de 32 bits en complemento a 2.

Java es interpretado: Puede ejecutar directamente el código objeto.

Java es Multithread: Java permite muchas actividades simultáneas en un programa. Los threads son básicamente pequeños procesos o piezas independientes de un gran proceso. Al estar los threads construidos en el lenguaje, son más fáciles de usar y más robustos que sus homólogos en C y C++.

Java es dinámico: Java se beneficia todo lo posible de la tecnología orientada a objetos. Java no intenta conectar todos los módulos que comprenden una

aplicación hasta el tiempo de ejecución. Las librerías nuevas o actualizadas no paralizarían las aplicaciones actuales (siempre que mantengan el API anterior). Java también simplifica el uso de protocolos nuevos o actualizados. Si el sistema ejecuta una aplicación Java sobre la red y encuentra una pieza de la aplicación que no sabe manejar, tal como se ha explicado en párrafos anteriores, Java es capaz de traer automáticamente cualquiera de esas piezas que el sistema necesita para funcionar. Java, para facilitar que los módulos de “byte-codes” o los objetos o nuevas clases, haya que estar trayéndolos de la red cada vez que se necesiten, implementa las opciones de persistencia, para que no se eliminen cuando se limpie la caché de la máquina.

Visual-Age for Java:

Visual-Age for Java (para Java) es un entorno completo e integrado para la creación de aplicaciones y applets Java. Proporciona herramientas de programación visual y de gestión de código. Visual Age para Java, enterprise Edition, amplía aún más las posibilidades de este entorno:

- ◆ Permitiendo a los equipos de desarrolladores trabajar juntos de forma eficaz, aumentando así la productividad tanto del grupo como individual.
- ◆ Suministrando compiladores Java de alto rendimiento y herramientas personalizadas para sistemas operativos específicos.
- ◆ Proporcionando herramientas de generación de código para un acceso rápido a aplicaciones y datos empresariales.

Facilidades:

- ◆ Soporte de Programación en equipo.
- ◆ Enterprise Toolkits
- ◆ Enterprise Access

- ◆ Correlación automatizada de objetos con bases de datos relacionales.
- ◆ Aplicaciones CORBA en Java.
- ◆ Servlet Builder.
- Enterprise Access Builder.

Para mayor información:

<http://www.software.ibm.com/ad/vajava>

Recomendaciones para el Proyecto:

- ◆ Se recomienda definir varios proyectos Visual-Age agrupando cada uno en un área concreta de negocio o aplicación.
- ◆ Evitar que exista más de una edición abierta de un elemento (clase, paquete) durante el desarrollo, excepto en la situación de dos entornos diferenciados, como sería el caso de una edición abierta para realizar fixes sobre la versión de producción y otra edición asociada a un nuevo desarrollo.
- ◆ Evitar que existan diferentes grupos de usuarios para dos ediciones distintas de un mismo paquete, es decir tratar de que los grupos de desarrollo del paquete sean lo más inmutables posible entre ediciones.
- ◆ Tratar de que las clases reutilizables sólo tengan un único desarrollador que sea a su vez el propietario, para evitar que cambios en elementos críticos impacten negativamente en los elementos que lo utilicen o hereden de él. En general, evitar que el desarrollador de una clase no sea su propietario.
- ◆ Versionar periódicamente todos los elementos que componen el desarrollo, empezando por clases y paquetes y finalizando por

proyectos, para establecer “baselines” que permitan restablecer anteriores niveles cuando sea necesario.

- ◆ Mantener en el entorno de trabajo sólo aquellos proyectos y paquetes que son necesarios para cada desarrollador, con el fin de evitar que el tamaño de dicho entorno crezca innecesariamente.
- ◆ Cuando se tiene un Entorno de trabajo demasiado grande se pueden observar degradaciones en el rendimiento del proceso de desarrollo.
- ◆ Comprobar que se trabaja con las últimas versiones liberadas de los elementos de desarrollo.
- ◆ En cuanto a las tareas administrativas a realizar sobre el repositorio, es fundamental disponer de procedimientos automáticos diarios de backup de dicho archivo, que es el elemento más crítico del desarrollo.

Las Bases de Datos

El “Web Application Server” (WAS), posee su propia base de datos que es accesada desde la aplicación, esta base de datos contendrá información sobre los usuarios, similar información es grabada en el LDAP del Policy Director y luego cuando la transacción viajó al Host también se graba en una base de datos en el Host, luego se tienen tres puntos de concentración de información, cuando se de el “alta de usuario” o mejor dicho cuando se inscribe un usuario al sistema, la grabación de la inscripción se registra en las tres bases de datos, sin embargo muchas veces por razones de caídas del sistema, muchas veces no se llega a registrar en los tres niveles originándose que el usuario no pueda ingresar al sistema, para suplir esta situación incomoda se diseñó un sistema que permita nivelar las bases de datos, este sistema se conoce como de “Conciliación de Bases de Datos” y es útil porque una vez eliminadas las diferencias se puede volver a intentar la inscripción.

El criterio que prima es el de que “solo debe permanecer el usuario que esté inscrito en las tres bases de datos, de lo contrario debe ser eliminado en donde aparezca”.

Diseño de capas en la solución:

1. Adaptación de canal:

Se encarga de introducir en el servidor de aplicaciones (WebSphere Application Server) las peticiones de los distintos canales: Internet, Wap, GMS, TV, etc.

2. Servlets de Operaciones:

Es un servlet que se encarga de manejar la interface con la capa de presentación para las aplicaciones basadas en http.

3. Operaciones de Presentación

4. Operaciones Multicanal

5. Servicios:

Resuelven funcionalidades elementales reutilizables por las operaciones multicanal.

Adaptación de núcleo funcional:

Encargada de las comunicaciones con el núcleo funcional de negocio. Debe presentar una API lo mas independiente posible de la forma de comunicación con el núcleo funcional, de esta manera el servicio transaccional puede ser capaz de comunicarse indistintamente con varios núcleos funcionales.

Fase de Adaptación Técnica.

1. Metodología

Pasos a seguir:

- Ciclo Desarrollo – Adaptación Técnica
- Ciclo Desarrollo – Recepción e integración
- Análisis Funcional
- Arquitectura de la Aplicación
- CBTF (Conceptos básicos)
- Modelo Desarrollo
- Guía Desarrollo

2. Descripción de elementos y responsabilidades

- Analista Funcional
- Arquitecto Técnico
- Analista Programador

3. Resultados Previos a la Construcción de la Aplicación

Acerca de la Arquitectura General CBTF

CBTF es un framework de clases java para construir aplicaciones financieras que acceden a sistemas transaccionales



Esquema del Núcleo CBTF

- Framework de transacciones

- Operation y OperationStep (son secuencias atómicas de la lógica del negocio)
- Context: gestión de datos
- Constructores

Estos elementos del núcleo se integran y ejecutan dentro del servidor de aplicaciones.

Data Model (Contextos)

Es una estructura jerárquica que contiene el conjunto de datos que utiliza una operación.

No tiene una estructura predefinida. Se define externamente.

Los datos se acceden por su nombre. La operación no necesita saber su localización. La operación busca un dato en su jerarquía de contextos.

Las operaciones manejan un conjunto de datos que se comparten en la cadena de contextos. Un DataElement puede contener un dato simple o una colección

Operations

Una operación CBTF es la representación lógica de la lógica de negocio de una operación real.

Tiene asociado un contexto con los datos relevantes que han de manejar y los servicios para que una tarea determinada se ejecute.

Una operación puede ejecutar varias transacciones

Una `OperationStep` define una tarea común ejecutada por varias operaciones (Ej. Envío a Host).

Formats

Herramientas que formatean, desformatean cadenas de datos.

Normalmente los servicios (comunicaciones, impresoras financieras) requieren que los datos estén especialmente formateados. Los formatos permiten el intercambio de información entre los contextos de operación y los servicios. Desde las operaciones “`format()`” desde el servicio “`unformat()`”.

Se pueden definir externamente.

CBTF proporciona un conjunto de formatos que se pueden extender.

- `FieldFormats`
- `DateFormat`
- `FloatFormat`
- `IntegerFormat,....`
- `KeyCollectionFormat`
- `IndexedCollectionFormat`
- `ConstantFormat`
- `FormatDecorators`
- `CodeSetTranslator`
- `Delimiter`
- `Identifier`
- `Services`
- `Servicios de comunicaciones`
- `MQ Series`
- `SNA LU0/LU2`

- SNA APPC
- CICS
- Diario Electrónico
- Dispositivos financieros
- Impresión
- Contadores, etc...

Externalización de archivos mediante sgml (generales y de operación)

Los nombres de los sgmls se mantienen en reserva por razones de seguridad, pero tienen que ver con customización de path, datos, formatos. Definición de operaciones.

Definición de contextos. Definición de datos. Definición de servicios. Definición de formatos. Definición de formatos de transacciones. Definición de datos de transacciones.

La Arquitectura:

1. Descripción externa de la arquitectura y sus componentes, externa en cuanto a que no describe su funcionamiento interno sino su función de soporte para las aplicaciones.

La idea es desacoplar en capas y bloques independientes las funcionalidades como se ha descrito anteriormente:

Adaptación de canal

Presentación

Operaciones Multicanal

Servicios Elementales

Adaptación del núcleo funcional

Servicios no solicitados por el usuario

Modelos de encapsulación de la Base de Datos

Esquema general:



Las peticiones generadas por el usuario llegan al Sistema por diferente canales, siendo la capa de adaptación de canal la encargada de lanzar las peticiones al servidor de aplicaciones.

La capa de Presentación gestiona las particularidades de cada canal en cuanto a la interacción con el usuario, invocando a continuación las operaciones de negocio independiente del canal que sean necesarias.

Las operaciones multicanal utilizan los servicios elementales que la arquitectura pone a su disposición, uno de ellos el transaccional, que gestiona la invocación de transacciones del núcleo funcional 24horas. Este servicio se apoya en la capa de adaptación del núcleo funcional que gestiona la comunicación con éste.

Existen por otra parte servicios no solicitados por el usuario, que pueden activarse a petición del núcleo funcional.

Para todos los accesos a la Base de Datos se prevén modelos orientados a objetos que encapsulen, a la vez que aislen, a los servicios de la implementación física de la BD.

Para la implementación de este modelo de arquitectura se ha usado el “framework” de clases de IBM-CBTF.

Para una mayor facilidad en el desarrollo se ha optado por el uso de CBTF en el modo en que la externalización de cada operación se hace en un archivo independiente.

Estos archivos reciben el nombre de SGMLs

Adaptación de Canal:

Esta capa se encarga de introducir en el servidor de aplicaciones (WebSphere Application Server) las peticiones de los distintos canales- Internet, Wap, GSM, TV.....

Para los canales GSM y TV digital llegarán por medio del MQ-Series en tanto que para Internet y WAP las peticiones llegan a través de un servidor Web que invoca un único Servlet (Servlet de Operaciones) encargado de invocar a las operaciones de presentación.

Servlet de Operaciones:

Este es un Servlet que maneja el interfase con la capa de Presentación para las aplicaciones basadas en http. Se considera que un usuario solicita de la aplicación la ejecución de una acción determinada a la capa de presentación y proporciona los datos necesarios, el Servlet recoge esta información de la request de http y una vez ejecutados los procesos necesarios en la capa de presentación e inferiores, se encarga de invocar la JSP (Java Server Page) correspondiente y poner a su disposición los datos obtenidos.

Los datos de entrada al Servlet pueden llegar independientemente por método http Get o Post, ya que el Application Server se encarga de ponerlos a disposición del servlet mediante el objeto HttpServletRequest.

La identificación completa de la acción solicitada por el usuario se compone de tres parámetros que deben llegar al servlet: (proceso, operación, acción). Al haberse escogido el modelo JSP para la salida de páginas hacia el usuario, la función del Servlet termina cediendo el control a la JSP, habiendo colocado de nuevo los datos que necesita el objeto HttpServletRequest.

Logon:

Se recomienda el uso de un Servlet específico para la operación de Logon, dada sus especiales características, éste será el encargado además de validar al usuario, de generar en forma dinámica el menú de la aplicación con sus correspondientes frames e incluso invocar a la capa de presentación para generar la página inicial de la aplicación. La idea de que sea un Servlet específico y diferente al de operaciones, se debe a que la validación de usuarios puede darse a través de medios externos. (Policy Director)

Presentación:

La capa de Presentación se encarga del manejo de la interfase de usuario, en cuanto a:

- comprobación de datos introducidos por el usuario,
- control de navegación
- interacción con las funciones de negocio
- preparación de la información a enviar al usuario.

Esta capa está muy relacionada con las particularidades del protocolo http.

Operaciones de Presentación:

Una operación de presentación representa un conjunto de interacciones de usuario que realizan una funcionalidad específica, simple y reutilizable, es el elemento principal de la capa de presentación. La operación de presentación se apoya en una o varias funciones de negocio (operaciones multicanal) para resolver la funcionalidad de negocio independiente de presentación.

La Operación de Presentación se encarga de las siguientes funciones:

Control de la navegación dentro de su ámbito

Comprobación de los datos introducidos por el usuario

Interacción con las funciones de negocio

Preparación de los datos a enviar al usuario.

Procesos:

Un proceso es la secuencia de interacciones de usuario, con su lógica asociada, que desencadena cuando éste solicita una acción del primer nivel de la aplicación (ejemplo: una opción del menú principal) Existirá un proceso por cada funcionalidad genérica que se le ofrezca al usuario.

La función básica del proceso consiste en agrupar operaciones, permitiendo:

decidir la secuencia de las operaciones dentro del proceso, control de navegación

mantener un área de datos común a todas las operaciones del proceso

ejecutar las OP's y encadenarlas con o sin necesidad de intervención del usuario

JSP

La función de las JSPs es exclusivamente de presentación final.

Operaciones Multicanal:

Serán las responsables de invocar si es necesario, transacciones del núcleo funcional, acceso a base de datos, control de límites, auditabilidad, es decir implementarán el modelo del negocio. Para realizar las funciones se apoya en Servicios que pueden ser reutilizados por distintas operaciones.

Las funciones que debe resolver son:

Proporcionar una interfase consistente y limpia a la capa de presentación, aislándola de los detalles de implementación de las funciones internas de negocio.

Invocar funciones de negocios internas, que pueden ser:

- a) transacciones del núcleo funcional
- b) servicios de base de datos locales
- c) otros tipos de funciones de negocio

Implementar la lógica de negocio adicional a las funciones internas necesaria para las particularidades de los canales.

Resumen de Servicios y Funcionalidades:

1. Administración de Transacciones:

Se ha implementado una herramienta para generar SGMLs de datos y formatos de las transacciones a partir de un diccionario transaccional proporcionado por el núcleo de información. Los archivos son: de data y de formato.

2. **Arquitectura:**

◆ **Modelo de desarrollo:**

Basado en procesos, operaciones de presentación y multicanal.

◆ **Extensión BTF**

Nuevos decoradores y formatos, externalización de operaciones en sgmls por operación.

◆ **Excepciones:**

Se usa una clase genérica para la gestión de excepciones

◆ **Servicios:**

- a) Comunicaciones
- b) Diario
- c) Generación de identificadores
- d) Servicio de Caché
- e) Correo

3. **Modelo de acceso a base de datos**
4. **Servlets**
 - a) Inicialización del entorno BTF
 - b) Finalización del entorno BTF
 - c) Servlet de logon a las aplicaciones
 - d) Logout de la aplicación
 - e) El de Operación
5. **El SGML del sistema (XXX.ini)**
6. **SGMLs generales**
 - Todas las colecciones de datos de las transacciones
 - Formatos
 - Contextos
 - Operaciones

III.2 Evolución

Inicialmente cada uno trabajaba en su propia máquina que contenía el Visual-Age más el Websphere con la posibilidad de comunicarse contra un Host, que en este caso es el mismo que se tiene para el manejo de la plataforma de atención a oficinas que está ya bajo un esquema de Multicanal, las “clases” una vez modificadas habrían de ser llevada a una máquina receptora de la última versión y en la cual podría compilarse los paquetes, de allí se llevarían a Producción, posteriormente se crearía el ambiente de Calidad en el que otro grupo, Organización y Métodos daría su aprobación o desaprobación ante una implementación en Producción.

Se instalaría un producto denominado ENVI que tendría la particularidad de manejar un repositorio único, así nadie podría modificar lo que otros están modificando hasta que terminen de hacerlo.

Se programaron las funciones básicas, fueron muchas horas sin sueño y muchas dificultades las que se presentaron en el camino, un tema que fue crucial para Soporte fue el de los parámetros de las configuraciones, eso fue algo que costó mucho asimilar ya que en los demás países a pesar de tener configuraciones similares podían no necesariamente funcionar o comportarse de manera similar a pesar de tener los mismos parámetros.

Más tarde entenderíamos que la similitud es una palabra que denota mucha relatividad.

Optimizaciones (Páginas)

Fue una preocupación constante el reducir lo máximo posible, el peso de las páginas. Si bien es cierto, que constantemente se están pidiendo modificaciones que dan mayores funcionalidades, también es cierto que existe una gran preocupación de que este incremento de funcionalidades no afecten el tiempo de respuesta en el cliente.

Nuevos desarrollos

Las áreas comerciales son las llamadas a solicitar cambios en la Aplicación, éstas conocen los requerimientos de los clientes, se reúnen periódicamente con el equipo de Organización y Métodos y plantean sus requerimientos. En muchos casos, Sistemas participa de las reuniones, en otros, sólo se realiza la reunión con Métodos y Sistemas se encargará de hacer la evaluación

técnica y determinará el tiempo y la prioridad que este requerimiento tendrá con respecto a otras tareas que pueden estar pendientes también de atención, las áreas comerciales dependiendo de la importancia del cambio, presionarán a fin de que el requerimiento sea atendido o no con mayor rapidez.

Correcciones

Si bien es cierto que existe todo un flujo desde que el requerimiento es atendido hasta que es programado y resuelto por el área de Sistemas y luego de ser sometidos a pruebas en los ambientes de Desarrollo, Test y Calidad, el producto puede dar problemas en Producción con lo que se tienen dos caminos a seguir, o anular el cambio o investigar su solución “in situ”.

No ha sucedido solamente una vez, sino varias y estoy casi seguro que esto se da en muchas organizaciones, a pesar de someter los cambios a rigurosas pruebas, las condiciones en el ambiente de Producción suelen ser diferentes generando problemas muy difícilmente detectables en un ambiente de pruebas.

IV. Proveedores:

Tenemos dos importantes, uno de ellos es IBM encargada de la instalación, soporte del software base y monitoreo de la solución y el otro Telefónica del Perú, encargada de los aspectos de comunicaciones desde que el cliente solicita un requerimiento ya sea desde su casa o desde una cabina en el país o el extranjero y su llegada a los primeros juegos de dos Switches de la institución que permite la conectividad hacia el interior de la Organización.

IV.1 Herramientas de Monitoreo

Esta empresa tiene a su cargo como mencionara anteriormente, el monitoreo de la solución y ha incluido dentro de sus herramientas de monitoreo los siguientes productos:

- ♦ **Monitor CISCO Works**

Se utiliza una PC300GL. El monitor Cisco o monitor de eventos de los equipos de comunicaciones incluye el Wqindows como sistema operativo, el software de protección Norton Antivirus y el software especializado Cisco Works. Este equipo se encuentra monitoreando los routers, los circuitos digitales y los switches.

◆ **Simulador de Transacciones**

Se utiliza un PC300 GL. El simulador de Transacciones utiliza el Linux como sistema operativo base, y está compuesto por un conjunto de scripts en PERL desarrollados por IBM que permiten simular distintas transacciones del aplicativo y registrar sus tiempos de respuesta. De la misma manera está planificada la emisión de alarmas ante el evento de una caída de servicio. Esta es la herramienta oficial para la toma de tiempos de la solución.

◆ **Detectores de Intrusión**

Se utilizan dos PC300 GL. Los servidores Detectores incluyen el Windows NT como sistema operativo base, el software de protección Norton Antivirus y el software Real Secure Engine para la detección de intrusiones.

◆ **Consola de Detector de Intrusión**

Se utiliza un equipo Netfinity 5000. La consola incluye Windows como sistema operativo base, el software de protección Norton Antivirus y el Real Secure Console. Esta consola se conecta a los detectores de Intrusión para su monitoreo y generación de reportes.

◆ **Servidor Tívoli**

Se utiliza un servidor RS/6000 modelo 7046-B50. Incluye el software AIX como sistema operativo base, software Tivoli Netview y Tivoli Distributed Monitoring para monitoreo de estado de la red e información SNMP, software de la base de datos DB2 para almacenar la información.

◆ **Tívoli Distributed Monitoring**

Este producto monitorea aspectos como memoria disponible, disco, utilización de CPU, filesystems críticos, procesos críticos, etc. De acuerdo a lo definido en la etapa de instalación, alertando al operador cuando pasan ciertos umbrales previamente establecidos.

◆ **Tívoli Netview**

Permite al operador examinar en forma gráfica la topología de la red, incluyendo equipos de comunicación, impresoras, PC's y servidores, indicando eventos tales como la activación, caída, etc.

◆ **Webtrends Firewall Suite**

Este producto permite obtener información estadística y gráfica sobre el comportamiento de los firewalls: Tráfico IP, uso de puertos, eventos, etc.

Otras herramientas:

• **Sitescope**

Esta herramienta fue traída por especialistas de IBM USA para el Task Force, las funcionalidades implementadas son cubiertas e incluso excedidas por el Tivoli instalado en la solución, por lo que no es necesario su permanencia, sin embargo puede quedar si se desea.

- **Sniffer**

Esta herramienta fue traída también por los especialistas USA, su funcionalidad principal consiste en la captura de los datos transmitidos a través de la red de área local para su análisis. Por su naturaleza esta función es más propia de operativos de mejora de performance específicos ante la aparición de un problema, no teniendo sentido su uso diario pues adicionalmente, el análisis de la información capturada tiene que ser hecho por un experto en comunicaciones.

- **Page Dtailer**

Esta herramienta permite obtener los tiempos de respuesta con un nivel de detalle que permite el análisis para sugerir mejoras en las páginas, básicamente descompone los tiempos de respuesta en sus distintos componentes hasta el nivel de items. El Page Dtailer es un componente del IBM Websphere Studio.

- **Webtrends Log Analyzer**

Esta herramienta permite la obtención de datos estadísticos a partir de los logs de los servidores , brindando información acerca de comportamientos y tendencias de los usuarios respecto a la solución. El área usuaria que más provecho podría sacarle a la información es Marketing. El “Webtrends Log Analyzer” es un producto “Webtrends Corporations”.

V. Aspectos Críticos:

V.1 La Seguridad

La Seguridad es importante porque existe un continuo desarrollo y expansión de redes, el uso de equipamiento informático en tratamiento y transmisión de información crítica así como mayor facilidad para realizar con éxito un ataque.

Los ataques en la comunicación pueden ser:

- ⇒ Flujo normal: Fuente----destino
- ⇒ Eliminación: No llega al destino
- ⇒ Intercepción: Llega al destino pero también llega a otro destino no contemplado
- ⇒ Modificación: La información enviada desde la fuente no es la misma que llega al destino
- ⇒ Fabricación: Llega al destino información que no fue enviada por la fuente normal sino de una fuente no contemplada en el flujo normal.

Ver Anexo "11".

Un ataque pasivo es aquel en el que el enemigo se limita a la escucha, sin modificar el contenido, en tanto que un ataque activo puede emitir suplantando a alguno de los comunicantes, o capturar, modificar, eliminar, repetir, retrasar o reordenar los mensajes.

Implantación de una Solución Internet en la Banca

Los ataques activos pueden a su vez clasificarse en:

- Suplantación de identidad
- Reactuación
- Modificación
- Degradación fraudulenta del servicio
- Caballos de Troya
- Encaminamiento incorrecto

Prestaciones para el atacante:

⇒ Intercepción.....

Escucha Obtención de información privada
Análisis de Tráfico Información sobre relaciones entre clientes

⇒ Suplantación.....

Mejora de perfil
Fabricación de mensajes

⇒ Manipulación.....

Modificar, retrasar o eliminar mensajes

⇒ Intrusión.....

Acceso a recursos reservados

⇒ Degradación.....

Pérdida competitividad corporación

⇒ Seguridad.

Amenaza	+	Vulnerabilidad	=	Ataque =>	Impacto
II		II		II	II
V		V		V	V
Identificar		Minimizar		Reducir y Detectar	Acotar

Política de Seguridad:

Conjunto de reglas que delimitan o controlan las actividades relevantes en cuanto a seguridad de sujetos o entidades que se fundamentan en Estándares y reglas, contratos de usuarios y procedimientos.

La más segura: “Denegar todo aquello que no está expresamente permitido”.

Tipos de Firewall

- ◆ A nivel de red
- ◆ A nivel de aplicación

Filtrado de paquetes:

- ◆ Direcciones IP origen y destino
- ◆ Tipo de protocolo IP (UDP o TCP)

Implantación de una Solución Internet en la Banca

- ◆ Campo de opciones IP
- ◆ Eliminar paquetes con “source routing”
- ◆ Puerto TCP/UDP origen y destino
- ◆ Reglas diferentes para cada servicio
- ◆ Flags TCP (SYN, ACK)

Permiten distinguir conexiones entrantes y salientes

Protección centralizada

Independencia de los sistemas cliente

Dificultad herramientas filtrado de paquetes

Imposibilidad de filtrar por usuarios

Limitación del filtrado por servicios

No hay autenticación de dirección IP

Proxys:

Tiene acceso a los datos del nivel de aplicación.

Logging del sistema

Dependencia del servicio

Requiere modificación de clientes

Limitaciones Firewall:

- ◆ No proporcionan integridad de datos
- ◆ Son susceptibles a ataques de administración remota
- ◆ Implementación de VPN tiene un impacto negativo sobre rendimiento del FW
- ◆ No protegen contra ataques internos
- ◆ La mayoría corren sobre Sistemas Operativos no seguros.

Secure Sockets Layer (SSL)

Protocolo de seguridad creado por Netscape

Ofrece servicios de seguridad a protocolos de nivel de aplicación

Proporciona confidencialidad, integridad y autenticación

https: http sobre SSL

www.openssl.org

Está situado entre el protocolo TCP y el protocolo de aplicación.

Ver Anexo "12".

SSL Handshake Protocol

Ver Anexo "13"

V.2 Ambientes

Existen 4 ambientes perfectamente definidos, el primero de ellos es el de **Desarrollo**, este se encuentra controlado por el Producto ENVI que permite el manejo común de un repositorio para todos los clientes Visual-Age conectados al Producto, este primer nivel de Desarrollo también permite conectividad contra un Host de Desarrollo.

El segundo nivel es el de **Test**, en el que no hay desarrollo sino solamente ejecutables, este ambiente no goza de las bondades de un Firewall, etc.... ya que únicamente se comunica con un Host de desarrollo, sin embargo si tienen un MQ para su interconexión con el Host.

El tercer Nivel es el de **Calidad**, en el que se ha tratado al máximo posible, de emular el ambiente de Producción, si posee esquema de Seguridad y puede decirse que en la mayoría de los casos muchos pases a Producción han sido detenidos cuando en este ambiente se ha detectado alguna incongruencia. Este

ambiente es manejado por el área de Sistemas responsable de los cambios y que coincidentemente también se llama de Calidad.

El pase a este nivel también es controlado y el que lo hace tiene que llenar un formato que se guardará como constancia de cambio.

El último nivel es el de **Producción** y es el definitivo. Es de esperarse que las pruebas a las que fue sometido el cambio en los otros ambientes hayan sido suficientes como para garantizar que no existirán problemas una vez pasado el cambio.

V.3 Tiempos de Respuesta

Uno de los aspectos más importantes en el desarrollo de una aplicación en Internet, consiste en evaluar qué impacto producirá en el usuario de la aplicación el requerimiento de las páginas de la aplicación, específicamente nosotros tuvimos muchos problemas inicialmente en este aspecto por lo que tuvimos que incidir mucho en diseminar la solución de manera que nos permitiera poder determinar cuales eran los puntos cruciales sobre los que pendía el mayor consumo del tiempo de respuesta, para lograr el objetivos seguimos más o menos la siguiente metodología:

1. Identificar claramente los componentes de Software y Hardware componentes de la solución.
2. Identificar los posibles puntos de medición.
3. Determinar los posibles tiempos de LATENCIA de los paquetes de datos
4. Análisis desde los diferentes puntos de medición
5. Determinación del impacto del proveedor de acceso de Internet.

6. Determinación de los niveles de utilización de los servidores dentro de las estimaciones iniciales

- ◆ Firewalls
- ◆ Portal
- ◆ Ingreso a la Aplicación
- ◆ Autenticación
- ◆ Servidor de Aplicaciones

7. Conclusiones

Comunicaciones

Arquitectura

Aplicativo

V.4 Homogenización de Ambientes

Uno de los principales objetivos es lograr que no existan diferencias entre los ambientes de la solución, definitivamente sería muy caro pretender contar en los ambientes que no son de Producción con equipos caros y sofisticados perfectamente justificable sen un ambiente de Producción pero en esos casos se subrayará la diferencia y se mantendrá el control por lo que esta diferencia pueda ocasionar en los diferentes ambientes.

La homogenización puede verse desde dos aspectos, el físico y el lógico, desde el punto de vista físico lo importantes son los equipos con los que cuenta la solución, desde el punto de vista lógico es el software y las opciones de estos que pueden ser necesarios y no convenientes dependiendo del ambiente en donde se encuentren.

Es evidente que por ejemplo en un ambiente de desarrollo las opciones de un software están orientadas a hacer aplicaciones en tanto que en un ambiente de Producción o de Operación el software está orientado a la ejecución y no a la compilación ni el desarrollo del mismo.

V. 5 Conciliación de las Bases de Datos

La solución graba al momento de dar de “Alta” a un Cliente información de los tarjeta-habientes en varias bases de datos, inicialmente se graba en el LDAP que es parte del esquema de Seguridad, también se graba en el WAS y en el Host.

Muchas veces, la información solo queda grabado en algunas de las bases de datos por lo que un usuario queda bloqueado para el acceso.

El proceso de Conciliación creado por nosotros consiste en hacer que las bases de datos queden iguales eliminando las diferencias, el proceso se inicia en el ambiente local de Internet, los Scripts generarán reportes con las tarjetas existentes en cada uno de los ambientes (LDAP y WAS), estos reportes llegarán al Host que haciendo matching con la base de datos del Host generarán las diferencias que retornarán a los ambientes locales para su eliminación, el proceso finalizará en el Host quien eliminará sus diferencias, el proceso puede correrse eventualmente, sin embargo se ha decidido que sea diario.

V.6 Pases de Versiones

Como mencionara anteriormente el pase de versiones motivó una serie de polémicas ya que por un tiempo el pase de versiones sin control motivó que se tuvieran ambientes con diferentes versiones generando situaciones a veces incontrolables al momento de hacer las pruebas, se reglamentó el tema, creando una Comisión de Cambios, previa Homogenización de los ambientes, se estipuló que

cualquier cambio en el futuro debería ser identificado y controlado para asegurarse de que el mismo cambio se de en todos los niveles.

V.7 Backups

Involucran data y software base.

Diarios:

Tívoli

LDAP-PD

WAS1

Desarrollo – Repositorio ENVI

Para los LOGS

Tívoli

LDAP-PD

WAS1

Quincenales:

PD

LDAP

WAS1

Firewall

Webseal

V.8 Simuladores

El objetivo del Simulador es enviar transacciones a la solución bajo un intervalo de tiempo regular registrando los tiempos de respuesta y alertando si es que no hubo respuesta.

La prueba del Estrés consiste en enviar ráfagas de manera que se pueda saber si colapsa o no el sistema. Corren bajo Linux y se conectan a la solución en forma directa.

V.9 Herramientas de Gestión

La importancia de la gestión.

No siempre se le ha dado mucha importancia a este aspecto sin embargo se convierte en una de las piezas claves post instalación de un producto o de una solución, la institución esta tomando con mucha seriedad este punto y está orientándose a hacer inversiones que permitan visualizar el comportamiento de los diferentes comportamientos de la solución ya sea en forma de equipos como se software.

El Apoyo de Proveedores

Con personal y equipos

V.10 Controles Internos y Controles Externos

Auditoría

Las diferentes áreas comerciales así como las áreas orientadas a velar por la calidad en el servicio de atención al cliente, constantemente están demandando a informática modificaciones que mejorarán el nivel de calidad en el servicio, adicionalmente como se trata de un producto corporativo, la casa matriz constantemente está haciendo esfuerzos por compatibilizar versiones tanto de hardware o de software de manera que el software base que se desarrolla en le casa matriz pueda tener la misma implicancia no importando en que país posteriormente se lleve la solución.

La auditoría de la matriz hace llegar el pliego de sugerencias para que estas se cumplan, el seguimiento al cumplimiento de las mismas así como cualquier observación o enmendadura correrá a cargo de las reuniones de seguimiento que se cumplirán periódicamente en cada semana.

V.11 Distribución Física:

Gaveteros

La idea es que existan tantos como para poder almacenar los equipos, en la solución se ha contemplado la duplicidad de equipos en casi todos los componentes, así por ejemplo se tienen dos switches en cada nivel de acceso dentro de la estructura física de la solución, se tienen dos Policy Director, dos webseals, dos Ldap, cuatro firewalls, dos internos y dos externos, todos estos equipos se encuentran en diferentes gaveteros, la idea es que no estén en un mismo gavetero dos equipos similares, esto para que en caso de siniestro el otro gavetero respaldo pueda funcionar.

VI. Actividades de Apoyo

VI. 1 Comité de Cambios

Se creó este comité con el propósito de regular aún más los cambios y pases de Aplicaciones o modificaciones al entorno de Producción, la participación de los comités puede entenderse de la siguiente forma:

Cada unidad, que puede ser Desarrollo o Soporte Técnico anuncia que o un trabajo está listo para ponerse en Producción o que ya se han hecho las pruebas y la modificación al software de base ya se puede hacer en Producción, estos avisos sólo podrán ser reportados hasta el viernes de la semana anterior al cambio en un formato pre-establecido, si no son presentados tendrá que esperarse hasta el siguiente comité, si llega a tiempo, el comité en sus reuniones semanales de los lunes someterá a discusión los cambios con el área comercial quien tomará conocimiento de los cambios y hará la propaganda necesaria si es que el cambio lo amerita, al final de la reunión el comité enviará un documento con los trabajos aceptados para la semana.

VI.2 Reuniones de Seguimiento

Un día a la semana desde que se inició el Proyecto nos reunimos el equipo de trabajo encabezados por el Jefe de Informática y los representantes de Desarrollo, Soporte y Organización con el proveedor de los equipos.

Las reuniones tienen el propósito de hacer seguimiento a los pendientes a la fecha como evaluar las incidencias o situaciones inesperadas producidas a lo largo de la última semana que valga la pena ser comentada.

Asimismo, otro de los propósitos es dejar en claro todo aquello que hasta el momento no haya sido aclarado así como comprometer a los participantes a trabajos que logren resolver una situación nueva presentada.

VI.3 Reportes de Incidencias y Disponibilidad

Son dos reportes en uno solo, el objetivo que persigue este reporte es el de proporcionar a las diferentes jefaturas de informática y organización involucradas en el proyecto una idea de cómo se va dando el día a día del proyecto, el reporte tiene dentro de sus particularidades, la secuencia de incidencias presentadas en el día, así como el impacto que esta produjo en la continuidad del servicio que debe ser 7*24, así como la naturaleza del incidente y su porcentaje de indisponibilidad acumulada con respecto al mes, el total de inscripciones del día y el acumulado del mes así como las horas en que ha habido más accesos a la solución.

VI.4 Procedimiento de Crisis

Es importante entender que existe una gran preocupación por encontrar mecanismos inteligentes que permitan una adecuada reacción ante una incidencia en el ambiente de Producción, debe entenderse que este procedimiento es una extensión de aquellos que se vienen dando para enfrentar temas de crisis tanto para el ambiente On-Line como el Batch de la institución.

Crisis es la interrupción de un servicio que brinda la institución a sus clientes (internos o externos) que por su naturaleza o envergadura, importancia y/o

potencial demora en el tiempo de solución, debe de ser informado a los responsables de informática e incluso de la Organización en su conjunto.

Procedimiento:

- a) Una vez detectado el problema se deberá medir el impacto utilizando las herramientas disponibles. Esta actividad no deberá de tomar más de 10 minutos.
- b) Si estuviera personal especializado de producción se les deberá informar a fin de que puedan proporcionar datos adicionales.
- c) De haber más de un operador, deberá asumir el control aquel que tenga más experiencia.
- d) Se deberán repartir tareas a fin de no duplicar esfuerzos.
- e) El operador deberá activar la crisis en forma automática no pasando de los 15 minutos de haber sido detectado el incidente.
- f) Si existen dudas sobre la paralización del servicio se deberá consultar con el supervisor.
- g) Si el supervisor no puede ser ubicado se continuará con la cadena de mando hasta tener un jefe con quien coordinar.
- h) Una vez activada la crisis se deberá prestar atención a un anexo telefónico el cual ha sido destinado para las coordinaciones de informática
- i) Se deberá ubicar al coordinador de las incidencias que es un jefe específicamente designado para este propósito

Implantación de una Solución Internet en la Banca

- j) La alerta de crisis está diseñada para las jefaturas de informática, pero de igual forma se debe ubicar a los responsables técnicos directos e implicados en la solución de la incidencia.

- k) Si llamaran otras personas para indagar sobre la ocurrencia se les debe de indicar (de acuerdo a su nivel jerárquico) que no se les puede atender por estar abocados a la solución o se les dirá que se comuniquen con el coordinador general.

VII. Expectativas

VII.1 Tienda Virtual

Los clientes podrán hacer compras desde un portal que no es de la organización, el cliente por ejemplo entrará al Portal de Telefónica o de un Afp y seleccionará la opción de pago de nuestra corporación para lo cual la aplicación foránea se comunicará con la nuestra pasándole datos para que se pueda realizar los respectivos cargos y posteriormente retornará los status de éxito o fracaso de la transacción.

VII.2 Currículum Web

Esta opción es muy utilizada por las áreas de Selección de Personal, el usuario una vez ingresado en la página del portal de nuestra institución, podrá enviar su currículum indicando el puesto al que postula, se utiliza una opción de correo que dejará los curriculum en un “buzón” (e-mail) de personal para su inspección.

VII.3 Portal Inmobiliario

Esta opción permite la adquisición de inmuebles bajo nuestro portal, el usuario podrá ver fotos y detalles de los inmuebles a ofertar, se puede generalizar para cualquier otro tratamiento de venta.

VII.4 WAP

WAP son las iniciales de Wireless Application Protocol, o lo que es lo mismo Protocolo para aplicaciones sin hilos. Todo lo que se refiere a teléfonos móviles, Palmtops (Ordenadores de mano), portátiles y cualquier otro acceso a redes con dispositivos sin conexión física. WAP es una solución unificada para los servicios de valor añadido existentes y futuros. El protocolo incluye especificaciones para las capas de la torre OSI de sesión y transporte, así como funcionalidades de seguridad. WAP también define un entorno de aplicaciones, WAP es escalable, permitiendo así a las aplicaciones disponer de las capacidades de pantalla y recursos de red según su necesidad y en gran número de tipos de terminales. Los servicios podrán ser aplicables a pantallas de una sola línea o a terminales mucho más complejos. Como cualquier estándar, las ventajas son múltiples a la hora de desarrollar aplicaciones, fabricar terminales o estructurar la red.

Qué se puede hacer con el WAP?

- ◆ **Empresas:** Envío de faxes y e-mail al servidor de la intranet para una difusión de los mismos a menor coste o multienvío de e-mail a los móviles de la compañía. Recordatorio, agenda, trabajos en grupo, programación de viajes. Acceso a las bases de datos de la compañía (Stocks, clientes, proveedores, catálogos).

- ◆ **Personales:** Las últimas noticias de actualidad al alcance de tu mano, todas las noticias y novedades que se producen diariamente en el mundo del deporte, cartelera de todos los cines, resultado de premios de sorteos, información metereológica, anuncios clasificados para comprar, vender, buscar y cambiar todo lo que se te ocurra.

- ◆ **GMS:** Son las iniciales de Global System for Mobile communications (sistema global para comunicaciones globales) Es un sistema estándar para comunicación utilizando teléfonos móviles que incorporan tecnología digital. Permite utilizar el sistema SMS, iniciales de Short Message Service (servicio de mensajes cortos) para enviar y recibir mensajes de texto. Es la evolución tecnológica de los sistemas de comunicación móvil.

Al principio sólo existía telefonía móvil analógica mediante el sistema MovLine de Telefónica. Después aparecen los sistemas digitales que permiten transmisión de datos:

Bellsouth, Movistar, Nextel.

Los teléfonos móviles con tecnología digital GSM pueden utilizar los nuevos sistemas de comunicación:

Banca Electrónica, Mensajería, Teleavisos.

- ◆ **SMS:** Facilita a los teléfonos móviles GSM el envío y recepción de mensajes alfanuméricos. Los mensajes pueden tener hasta 160 caracteres. Como funciona?... Se prepara el mensaje en la pantalla de su teléfono móvil. Se realiza el envío de mensaje. A los pocos segundos una señal sonora avisa del mensaje de texto que ha recibido. El mensaje llega siempre, incluso cuando se está hablando por teléfono. Si está apagado, la red GSM almacena este mensaje para entregarlo en cuanto vuelva a ser operativo.
- ◆ **WML:** Wireless Markup Language, es el lenguaje en el que se definen las páginas. Se recomienda tener conocimientos de HTML, ya que WML es muy parecido a este último.

- ◆ **WML-Script:** Wireless Markup language Script, es el lenguaje en el que se definen los scripts.

Tiene el formato típico de un script. Parecido al JavaScript.

VII.5 Intranet

Uno de los proyectos más importantes luego de la estabilización del Internet es el Intranet, en este proyecto al idea es conectar a todos los empleados de la organización con funcionalidades propias de nuestro entorno de trabajo, se piensa generalizar el tema con todos los demás países de la corporación.

Se ha solicitado y se nos ha proporcionado equipos para el desarrollo inicial:

- a) Servidor Sun Enterprise E450-(ADEXUS)
- b) Servidor de Acceso Remoto CISCO, AS5300 (IBM)
- c) Netscape-Iplanet
- d) CA-XCOM
- e) ELA- DB2 Websphere

VII.6 Negocios Digitales y Comercio Electrónico

- ◆ Puede considerarse el Comercio Electrónico como el futuro de las riquezas de las Naciones.
- ◆ Las Modalidades del Comercio Electrónico son:
 1. B2B
 2. B2C
 3. C2C
 4. C2G
 5. G2G
 6. G2C

Implantación de una Solución Internet en la Banca

- ◆ El Internet puede tener debilidades en lo que significa la Seguridad Técnica y la Seguridad Legal.
- ◆ Legalmente hablando existen impedimentos legales al empleo de mensajes electrónicos así como una incertidumbre sobre la validez jurídica de esos mensajes.
- ◆ El objetivo de proyecto de Comercio Electrónico será el de dotar de valor probatorio a los mensajes de datos emitidos o contenidos en algún medio electrónico, así como permitir o facilitar el empleo del comercio electrónico concediendo igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que a los usuarios de la documentación consignada en papel.
- ◆ El proyecto de la Firma Digital dotará de seguridad jurídica a los mensajes de datos emitidos por algún medio electrónico, mediante la identificación veraz del remitente del mensaje y la integridad de los datos contenidos en éste.

VIII. OTROS

VIII.1 Capacitación

Este es un aspecto importantísimo, muchas veces por la misma presión de los “pendientes” se descuida este aspecto y terminamos capacitándonos “in situ”, debe entenderse que esto no es lo normal pero se debe a la escasez de especialistas en el campo así como a la cantidad de “pendientes” que constantemente llegan con etiqueta de “prioridad uno”.

Para el equipo de Desarrollo:

- ◆ Desarrollo de aplicaciones distribuidas usando Java
- ◆ Desarrollo de aplicaciones usando XML
- ◆ Fundamentos de Tecnología E-Business
- ◆ Seguridad para E-Business
- ◆ Application Framework para E-Business
- ◆ Desarrollando aplicaciones Server-Side usando Visual-Age for Java
- ◆ Taller de Programación Java
- ◆ Taller de WebSphere Application Server y Enterprise Java Beans
- ◆ Introducción a técnicas de MQ-Series
- ◆ Programación en MQ-Series
- ◆ Programación en Base de Datos como MS SQL Server 2000
- ◆ Diseño e Implementación Orientado a Objetos usando UML

Implantación de una Solución Internet en la Banca

Para el equipo de Soporte:

- ◆ AIX (Básico, Administración del Sistema, Determinación de Problemas, Manejo del Desempeño)
- ◆ AIX Configuración TCP/IP y acceso a Internet
- ◆ Seguridad en AIX
- ◆ RS/6000 Programación de Korn Shell
- ◆ Planeamiento de Seguridad en Internet y Firewall
- ◆ Fundamentos de la familia DB2
- ◆ DB2 SQL Workshop
- ◆ MQ-Series (Administración del Sistema)

Para el equipo de Dirección

- ◆ Liderazgo
- ◆ Dirección de Proyectos
- ◆ Toma de Decisiones Estratégicas
- ◆ Gerencia de Proyectos de Sistemas de Información

IX. Conclusiones y Recomendaciones

IX.1 Conclusiones

El trabajo ha sido muy arduo pero al fin la Solución se encuentra operativa, se han cometido muchos errores técnicos y administrativos, pero comparados con otros proyectos de menor envergadura los errores bien pueden pasar por desapercibidos, la experiencia bien ha valido la pena por el logro obtenido, muchas de las aplicaciones hechas en nuestro país han servido de modelo para el desarrollo en otros razón por la cual muchas veces se nos ha comentado que hemos “hecho productos para la exportación”, es de esperar que luego de esta etapa de implantación y adecuación haya una de consolidación en la que la solución alcance su mejor nivel, se está haciendo constantemente Pruebas de Esfuerzo a fin de dotar a la Solución de la Infraestructura necesaria que le permitirá soportar cualquier ataque masivo del exterior, se afinarán aún más los aspectos de Seguridad que permitan que la solución no sea violada por Hackers o expertos en seguridad que vean en nuestra Solución una posibilidad para cometer fechorías y de esa manera debilitar nuestro sistema.

Se está evaluando la posibilidad de reorganizar los departamentos de Informática de manera que puedan dar un mejor frente a la Solución Internet, en un futuro no muy lejano todas las actividades de la Institución funcionarán en torno a esta infraestructura que como mencionara en su momento será replicada en los diferentes ambientes según necesidades, el caso de Intranet es un ejemplo palpable,

Implantación de una Solución Internet en la Banca

Intranet tomará la infraestructura física y lógica de Internet con sus adecuaciones propias de sus necesidades.

Finalmente todo funcionará bajo el concepto “INTERNET”, las demás aplicaciones migrarán a este nuevo concepto que es el camino a seguir en el futuro, en algún momento no muy lejano nada se podrá hacer sin relacionarse con Internet, el futuro ya llegó y se llama “Internet”.

No siempre partir de una experiencia previa es una ventaja para la implementación de una nueva arquitectura, muchos países que tenían una gran experiencia en el tema de Internet han tenido que adaptarse a este esquema que no necesariamente es de última generación pero que sí responde a una solución Corporativa, esto es importante porque desde la óptica de la Corporación lo importante es que funcione no que sea último o que todo el mundo lo use, si hay una empresa que puede ser un cien por ciento confiable, la Corporación apuesta por ella aunque lo que le ofrezca solamente pueda usarse en la Corporación.

A pesar de poseer la misma Arquitectura el comportamiento de la Aplicación en los países americanos no resulta ser igual, el tema de dejar de lado lo que se piensa que está bien por algo que no se sabe si va a funcionar pero que debe funcionar es algo que motiva en los especialistas una reacción que a veces puede afectar el logro inmediato de las metas, la persona tiene que hacerse a la idea de que el norte ya está marcado y que tiene que lograr los objetivos sin desviarse del norte porque así fue dispuesto.

Tratar de igualar la “solución” en los diferentes países no es una labor fácil, ya que no todos parten igual, no todos tienen los mismos recursos y hasta sus Proveedores por las coyunturas a nivel país pueden otorgar facilidades que para otros resulta imposible de pensar, el tema de la “igualdad o homogenización de ambientes” es muy “caro”, los ambientes que no son Producción pueden no necesitar de algunas funcionalidades que si son vitales en Producción, esto hace pensar en racionalizar los recursos, nosotros hemos sido “cautos” y “conscientes” en lo que significa la inversión en equipos que pueden no ser necesariamente obligatorios en una

configuración por ejemplo de un ambiente de Pruebas, hemos partido del principio de “compartir” servidores con lo que los costos se minimizan.

Este trabajo pretende ser una GUIA para el iniciado en el desarrollo y soporte Internet, en este trabajo podrá tomar contacto aunque sea de una manera somera con algunos términos y conceptos que son claves en el desarrollo e implantación de una solución que bien puede ser nuestra o como es el caso de la Solución, una solución importada.

IX.2 Recomendaciones

◆ Alta disponibilidad:

Existen aún puntos en lo que la “alta disponibilidad” no se da en la medida que se deseara, por ejemplo en el caso de la Base de Datos del WAS, ésta si bien es cierto es respaldada se encuentra en un gabetero que es único, esto significaría inversión económica.

◆ Más Recursos-Hombre

Son muchos los requerimientos y poco los especialistas lo que origina que estas personas estén abocada mucho al tema descuidando otros aspectos importantes, se necesita una adecuación a la cultura informática reinante de manera que el resto de personal informático pueda introducirse en el tema y a la vez liberar a un grupo reducido de los mismos que tienen el control de toda la solución.

◆ Optimización en los niveles de Pruebas.

Aún faltan afinar muchos aspectos de las pruebas, un set de pruebas por cada tipo de modificación debería ser suficiente para reducir una prueba total por cada modificación elemental que se le de a la solución.

X. Bibliografía

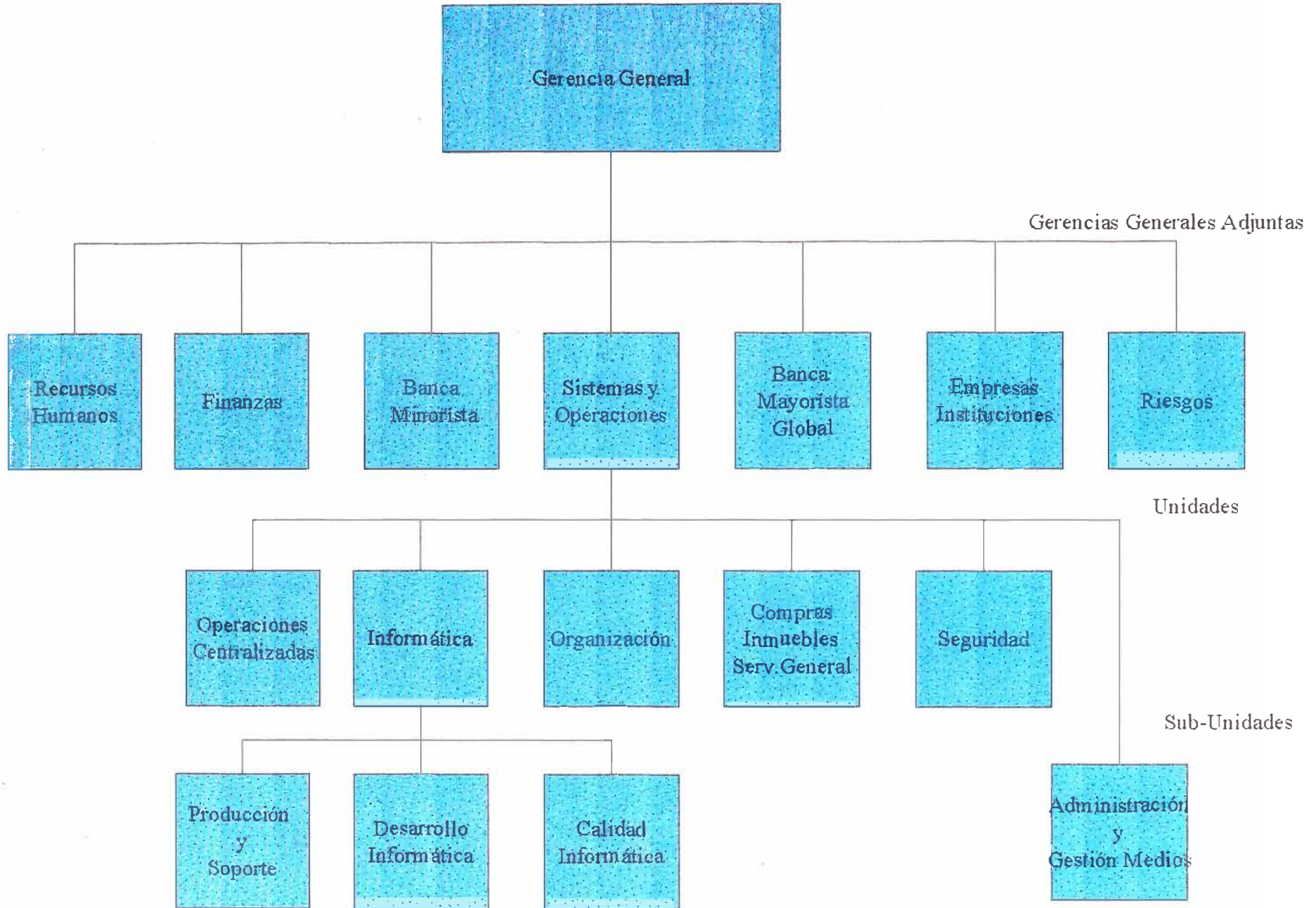
1. TCP/IP
TCP/IP --- Dr. Sidnie Fest Osborne McGraw-Hill
2. AIX
IBM AIX Ver 4. Basics – Student Notebook
IBM AIX Ver 4. Advanced System
3. JAVA
Descubre Java en 21 días , Milke Morgan, Prentice Hall
Java 2 , Agustín Fronte, RA-MA
Aprendiendo Java en 21 días, Laura Lemy, SAMS
Curso de Java, Centrinet-Madrid
4. Aplicación de tres capas
Intranet/Internet Developer - Cibertec
5. UML
El proceso Unificado de Desarrollo Software, Grady Beoch,
Addison Wesley
6. XML
XML, Charles Goldfarb y Paul Prescod, Prentice Hall
7. EJB
Enterprise Java Beans, Richard Monson, Haefel
8. HTML
HTML para Web, Laura Lemy, SAMS
9. Firewalls
Firewalls-Teoría y Práctica, Cosapi

10. SNA
IBM User's Guide Versión 3 Release 1.1
11. CBTF
Descripción CBTF, Centrisa-Madrid
12. Seguridad
IBM Security Policy Director
IBM Policy Director – Administration Guide-Up and Running
13. Comercio Electrónico
Estudio Muñiz, Forsyth, Ramírez, Pérez-Taimán & Luna-Victoria Abogados
14. LAN
Local Area Networks (LAN), James Fritz, Prentice Hall
15. Visual-Age for Java
Visual Age for Java 2.0, John Akerley, International Technical Support Organization
16. Core Servlets and Java Server Pages
Core Servlets and JSP, Marty Hall, Sun Microsystems
17. Windows NT
Windows NT Server 4, Allen Wyatt, QUE E & T
18. Bases de Datos
Sistemas de Bases de Datos, C.J. Date, Addison Wesley

X1. Anexos

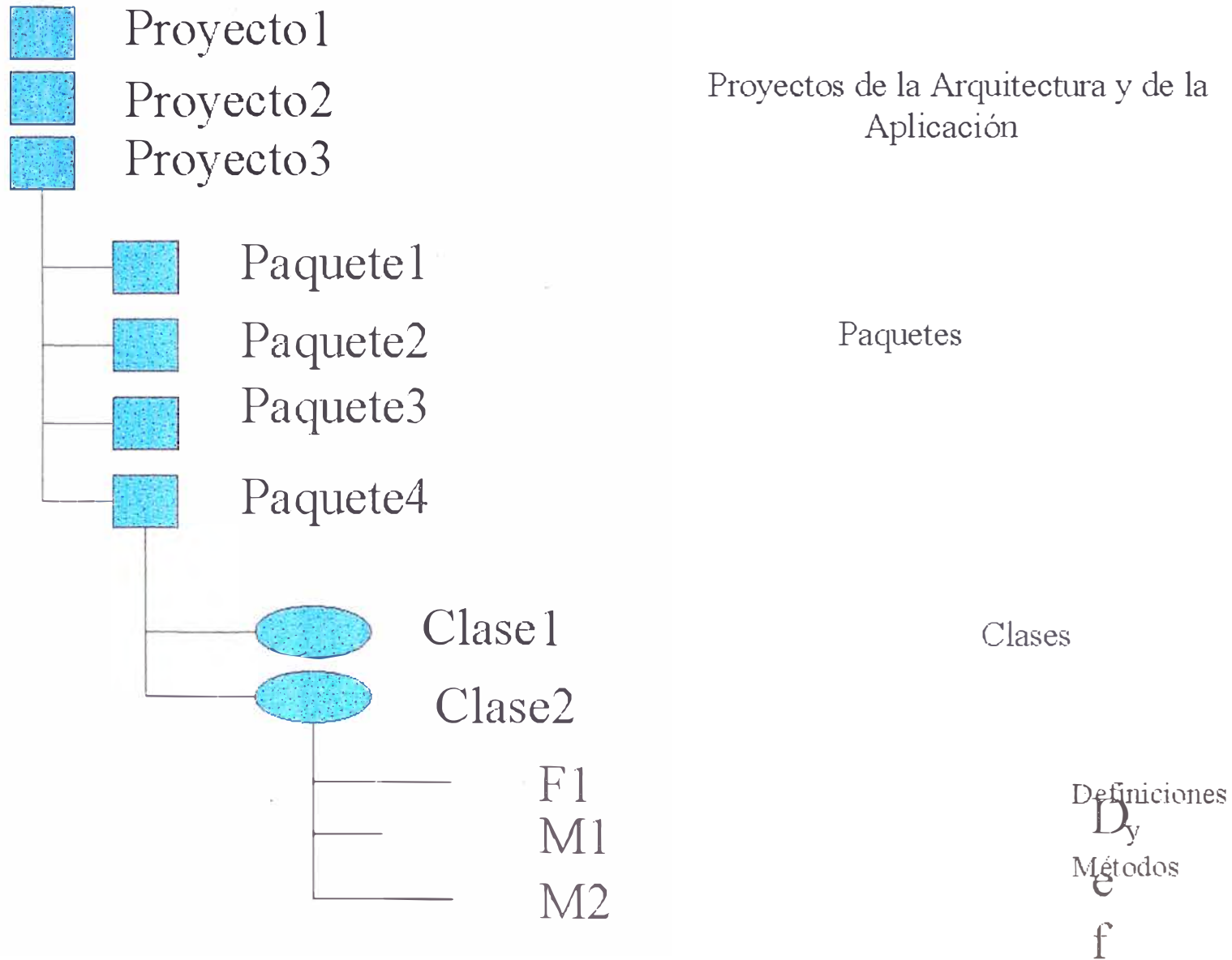
- Anexo 1 Organigrama de la Institución
- Anexo 2 Esquema de una Aplicación Visual-Age
- Anexo 3 Modelo OSI de Capas
- Anexo 4 Modelo OSI de Comunicaciones
- Anexo 5 Formatos para la Dirección “IP”
- Anexo 6 Esquema de la Solución
- Anexo 7 BTF
- Anexo 8 Arquitectura a tres niveles
- Anexo 9 Núcleo BTF
- Anexo 10 Arquitectura General Servidor de Clientes y Canales
- Anexo 11 Ataques a la Comunicación
- Anexo 12 SSL (Secure Socket Layer)
- Anexo 13 SSL Handshake Protocol
- Anexo 14 The Future of Wireless Banking
Implementation of Wireless Banking and Financial Systems
Lectura escogida de Rod Ghani especialista IBM
- Anexo 15 3G – 2B or not 2B!
Lectura escogida de Rod Ghani especialista IBM

Anexo "1"

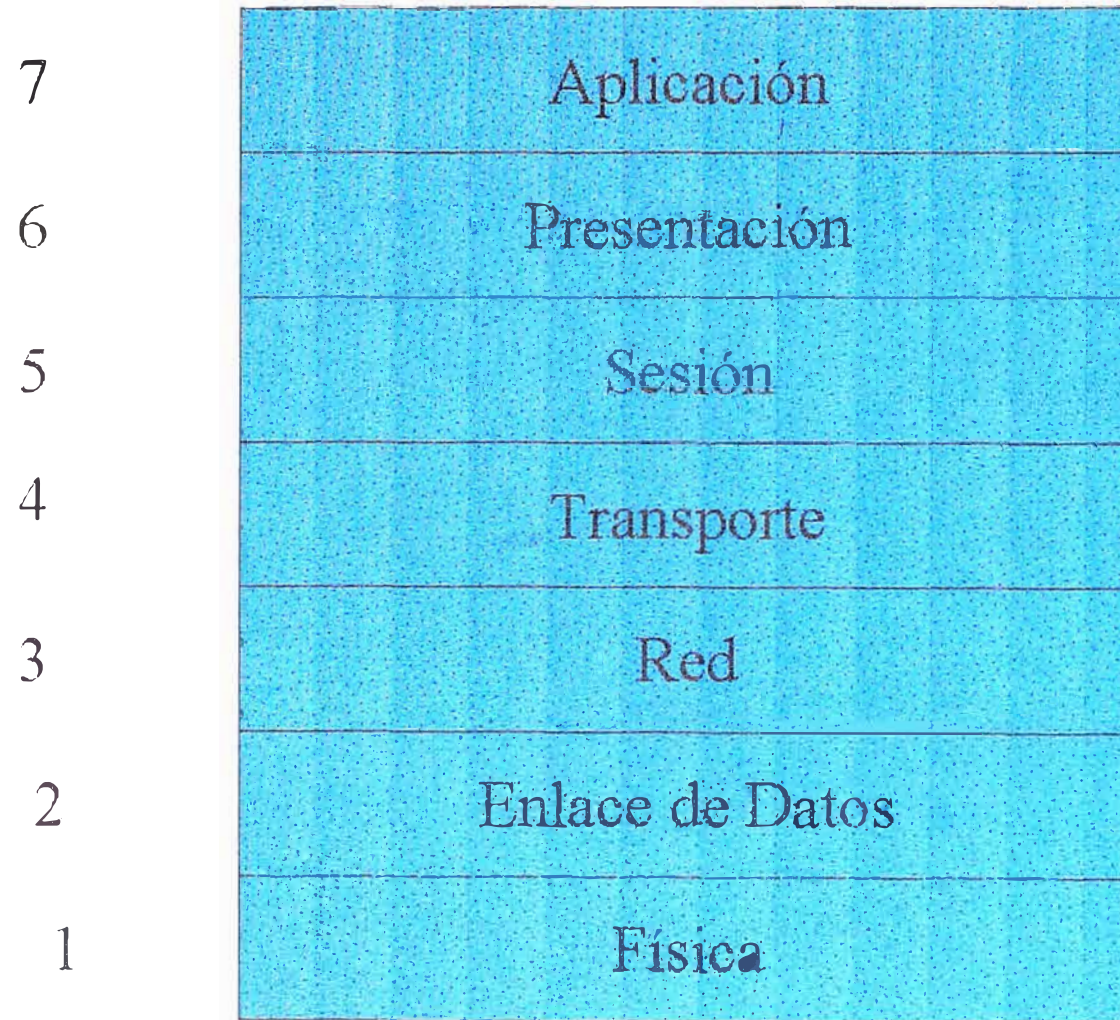


Anexo "2"

Esquema de una Aplicación Visual-Age



Modelo OSI de Capas

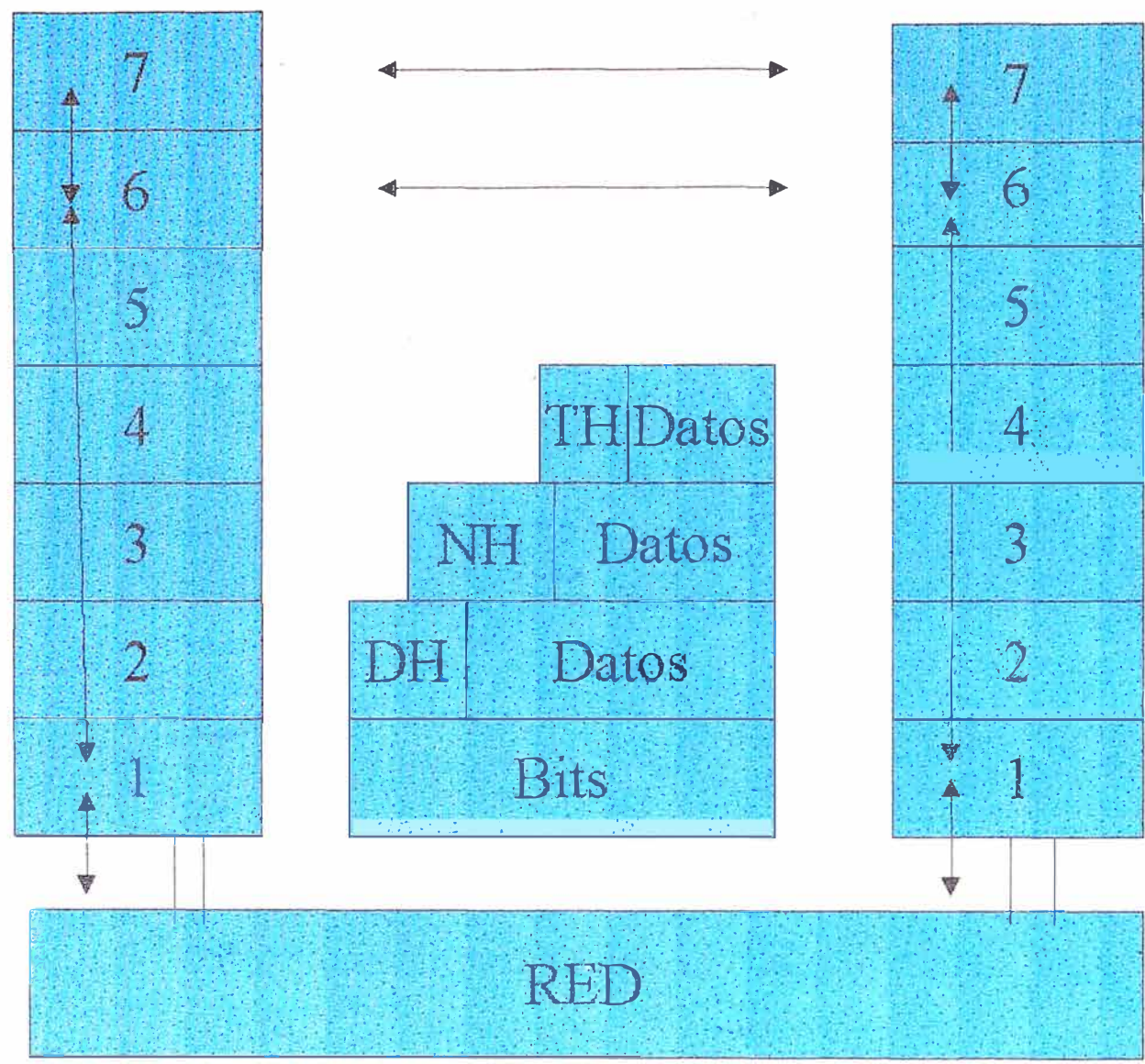


Anexo "4"

Modelo OSI de Comunicaciones

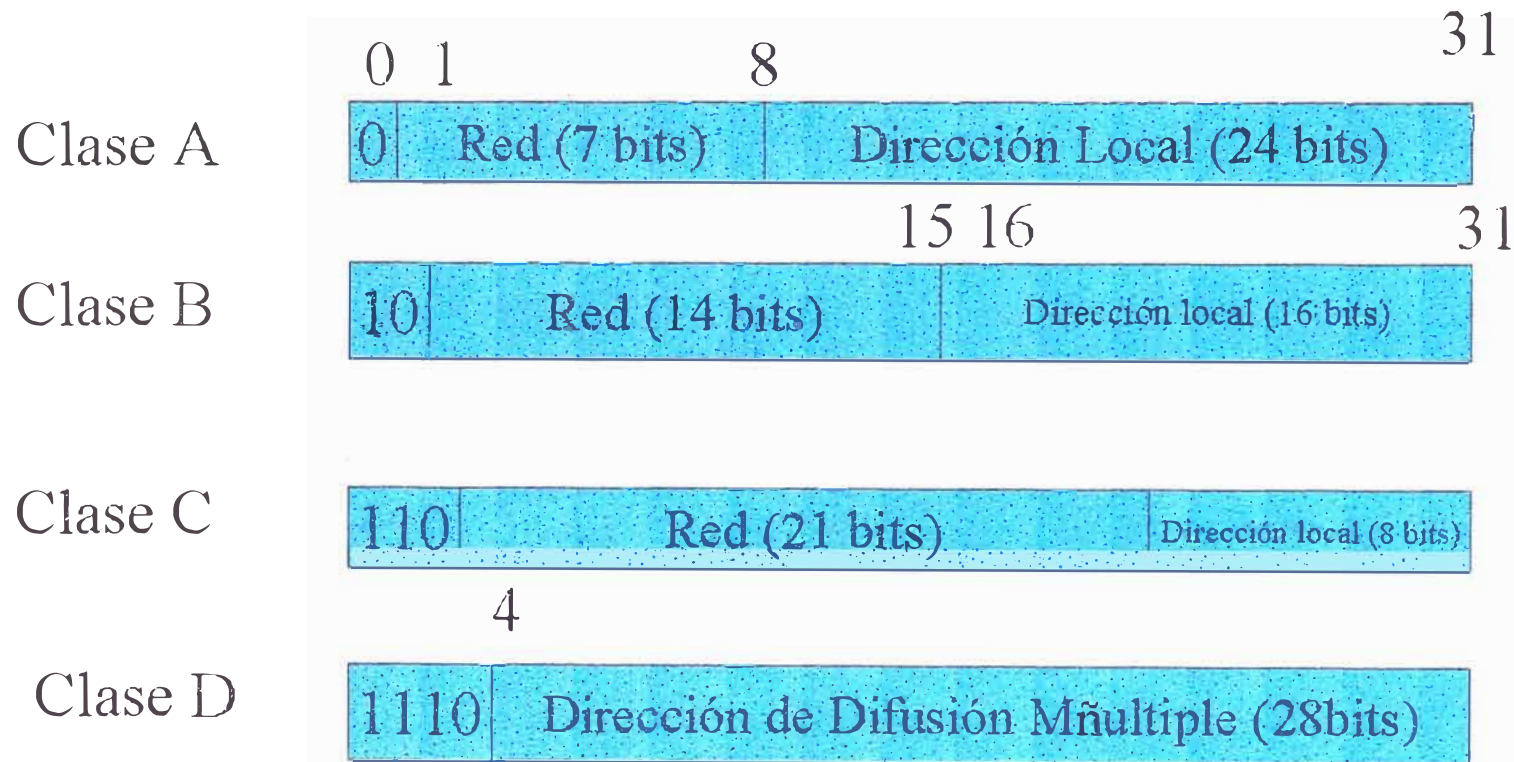
Sistema A

Sistema B



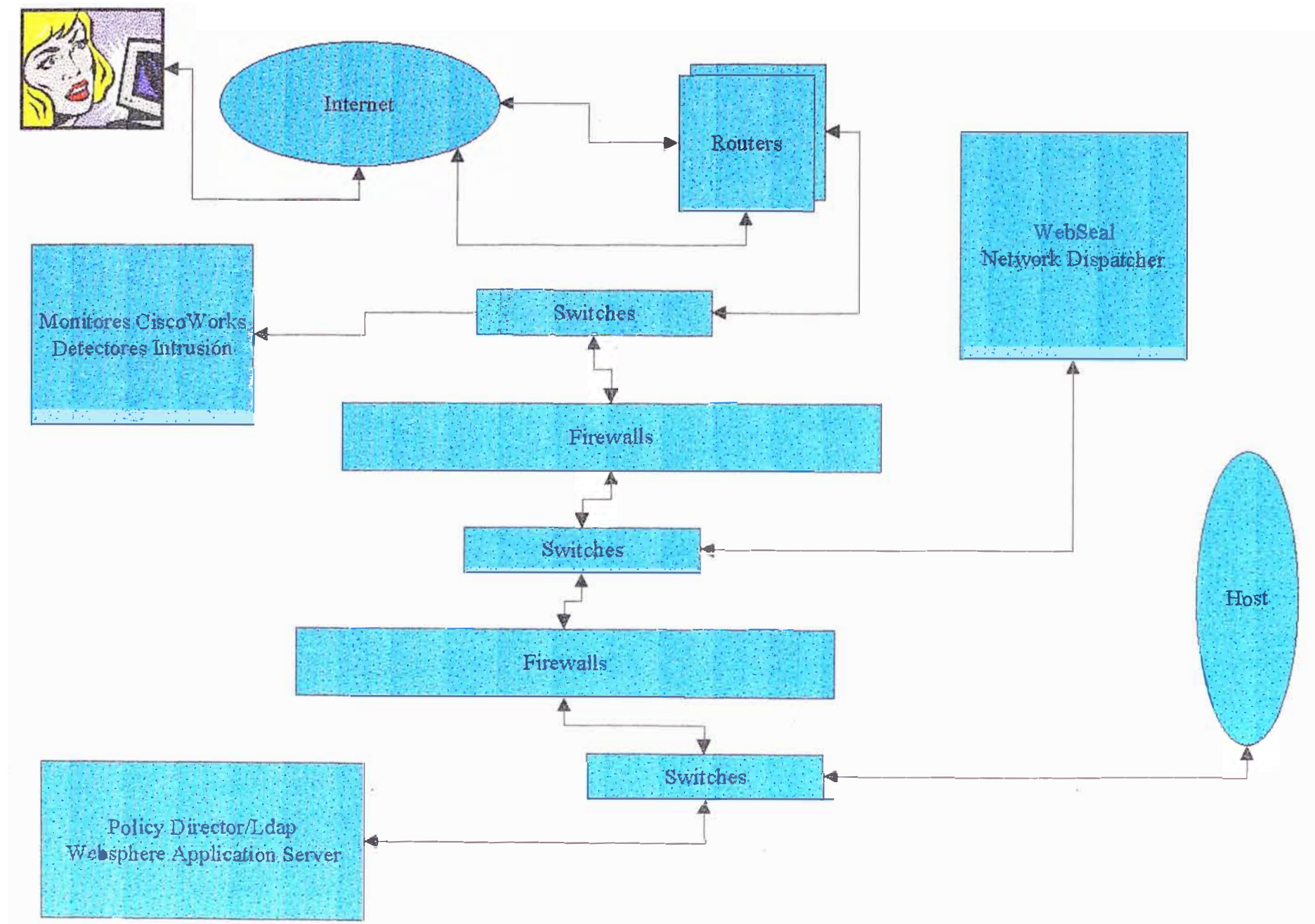
Anexo "5"

Formatos para la dirección IP



Anexo "6"

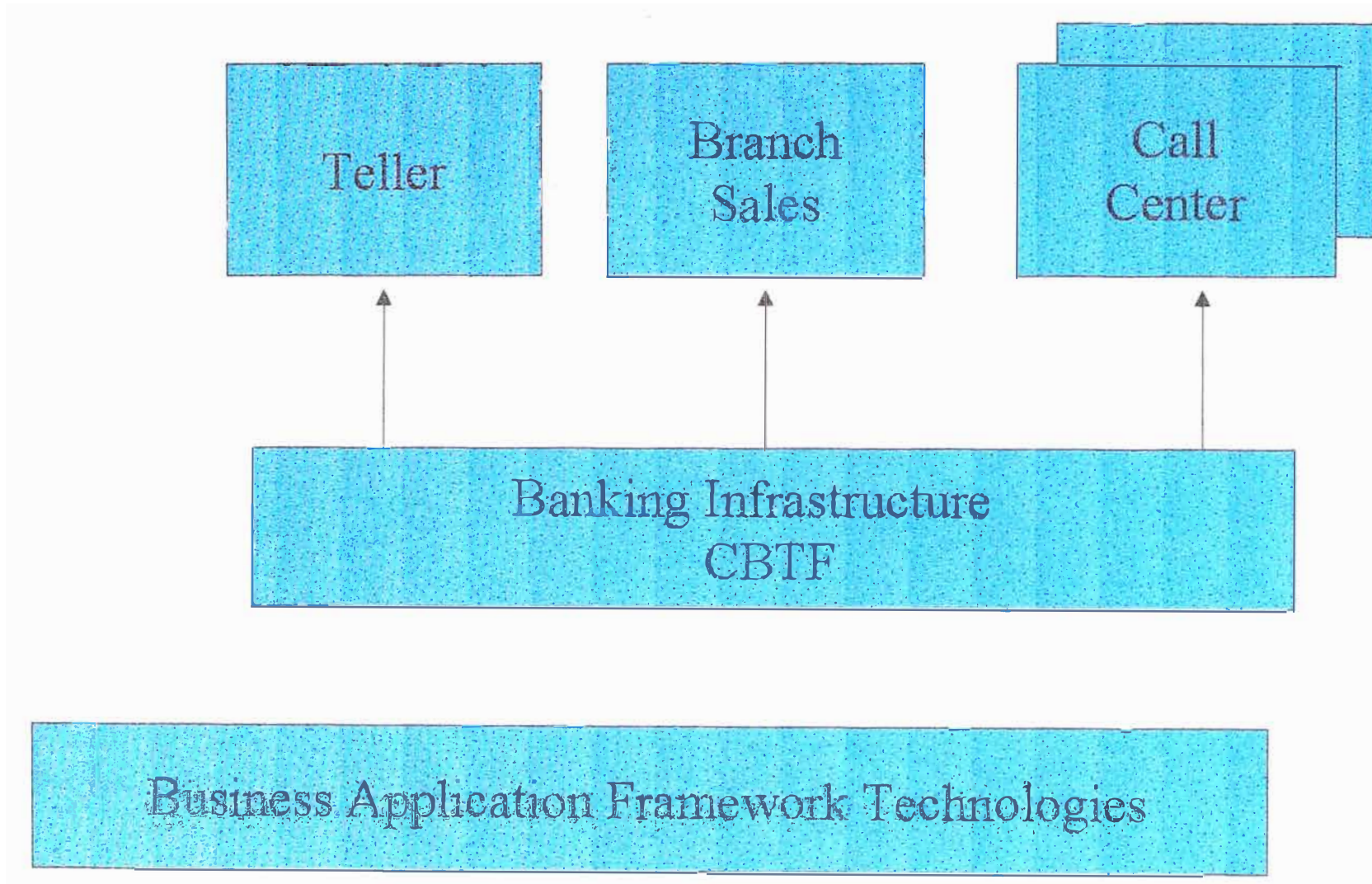
Esquema de la Solución



Anexo "7"

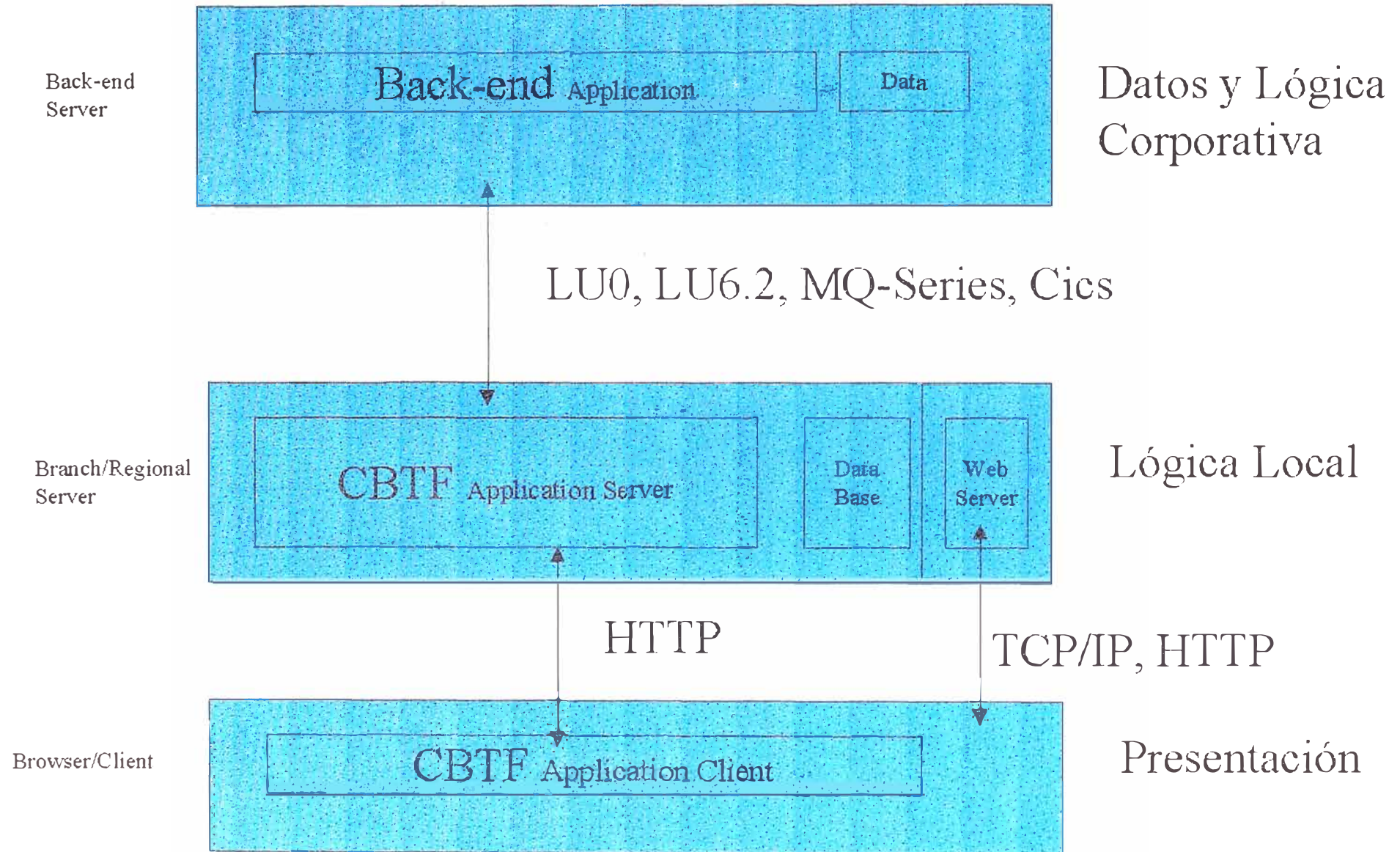
BTF

Framework de clases Java para construir aplicaciones financieras
Que acceden a Sistemas Transaccionales

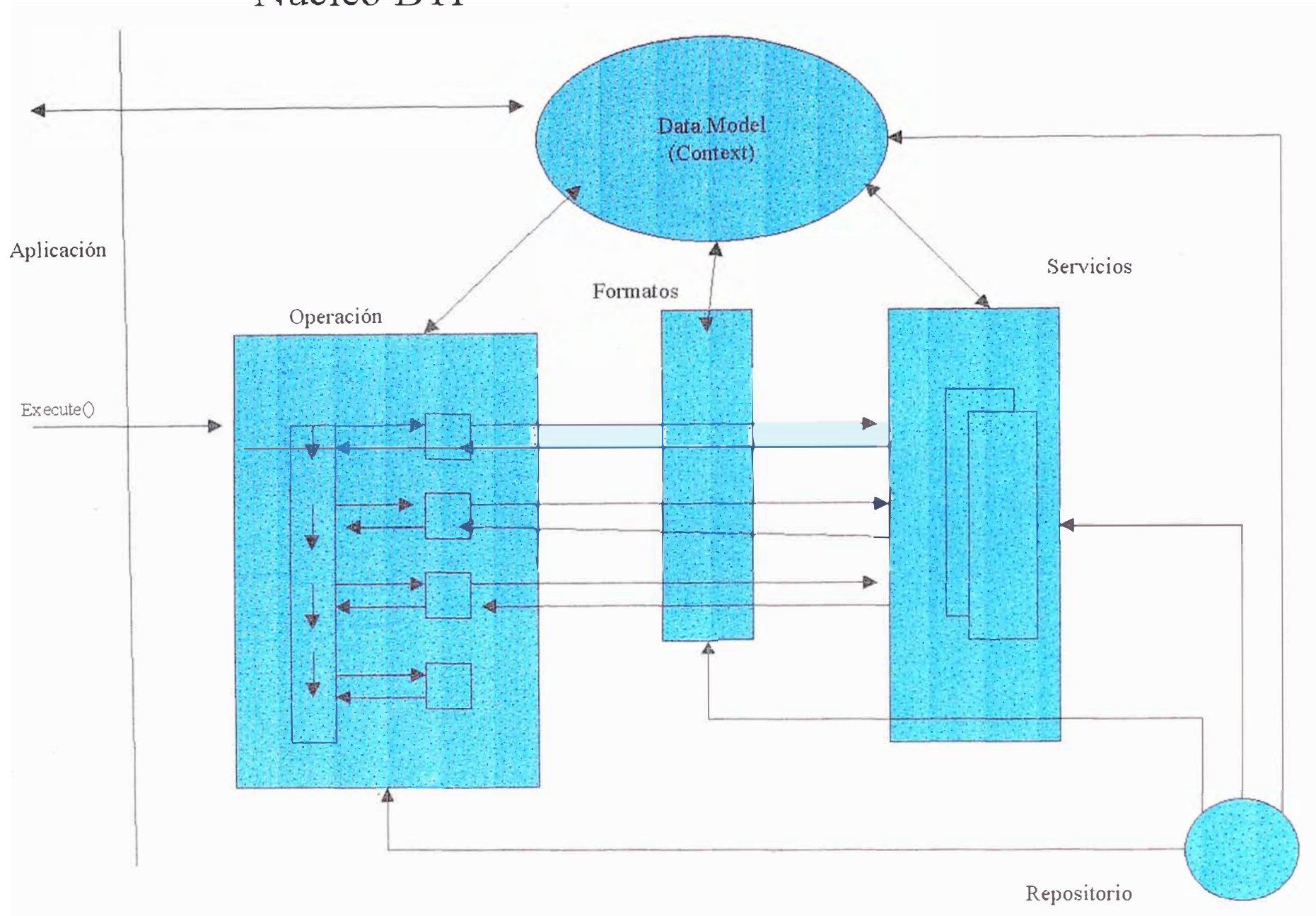


Anexo "8"

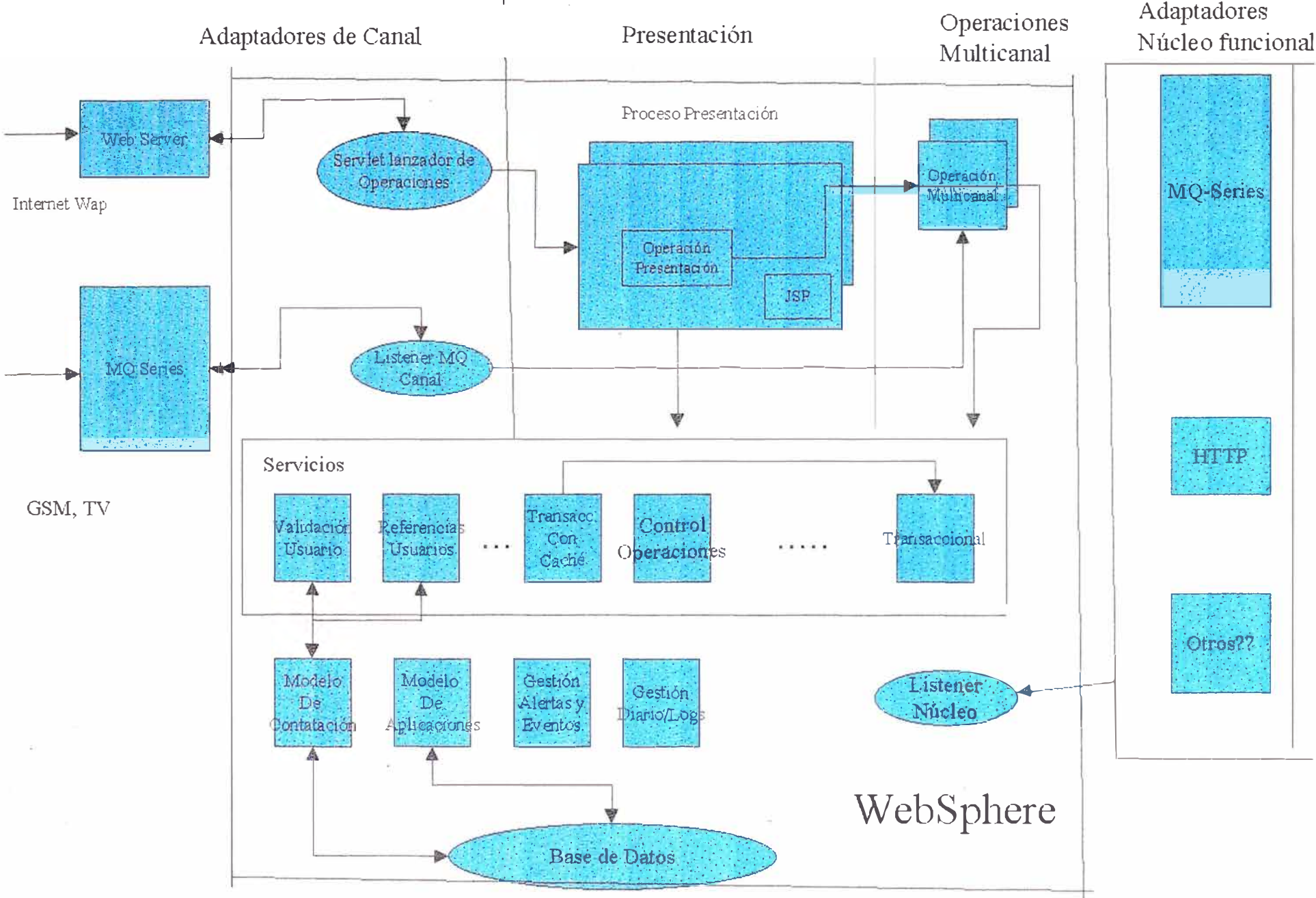
Arquitectura a tres niveles



Anexo "9" Núcleo BTF

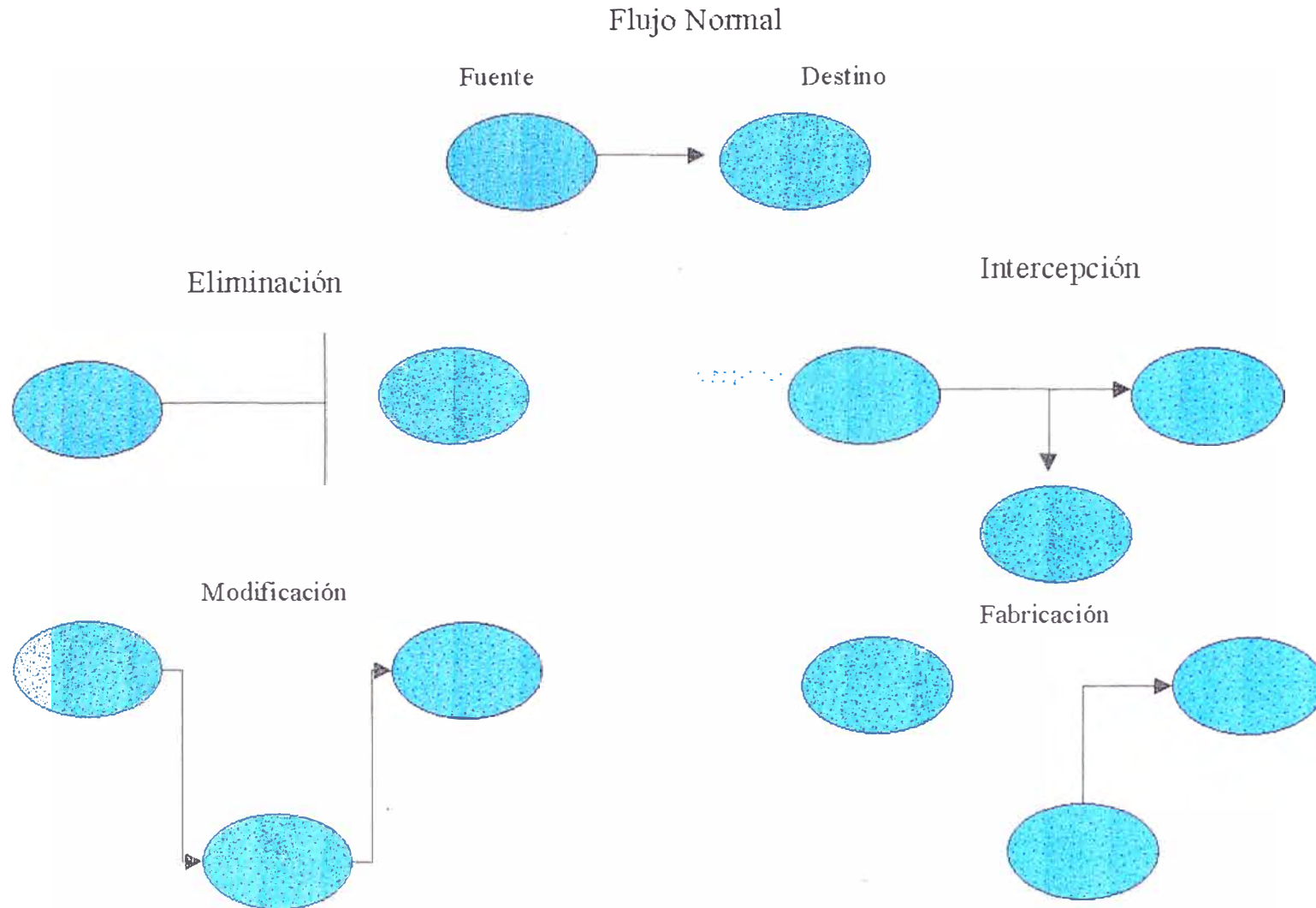


Arquitectura General Servidor de Clientes y Canales



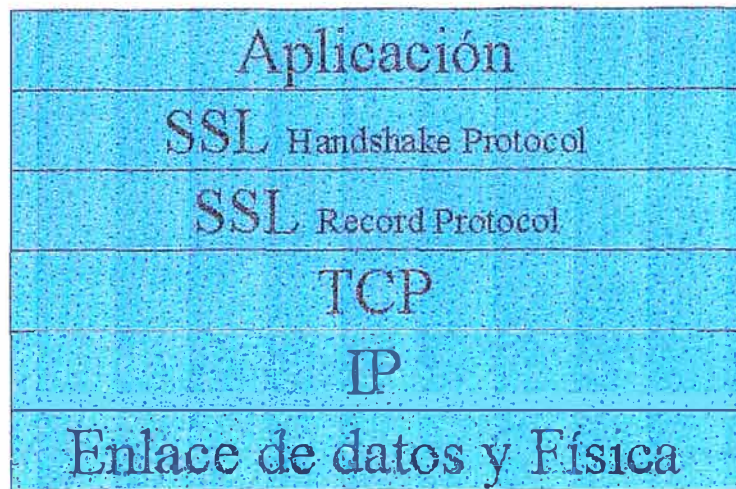
Anexo "11"

Ataques a la Comunicación



Anexo "12"

SSL (Secure Sockets Layer)

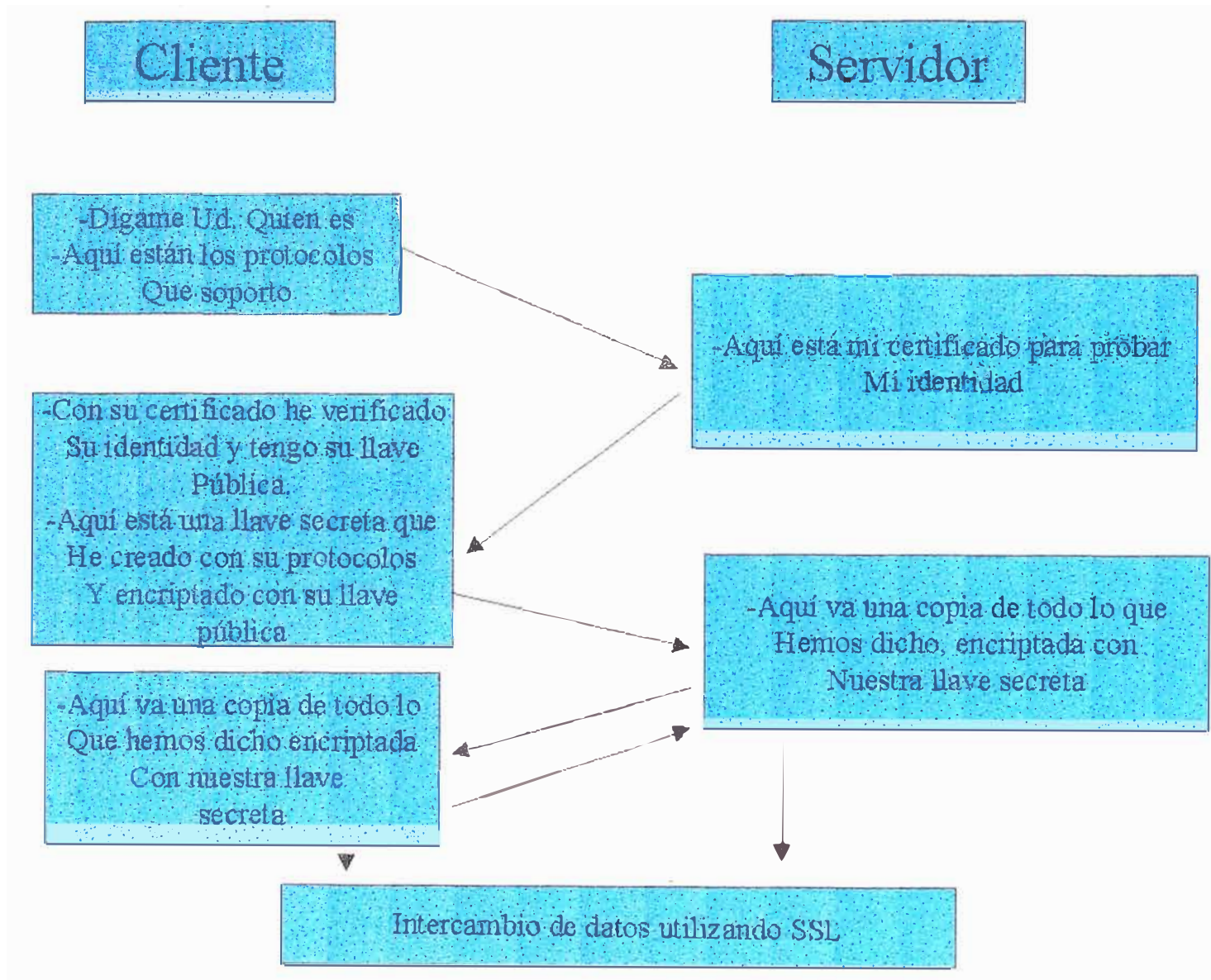


Permite a clientes y servidor
Autenticarse mutuamente y negocia
Un algoritmo de cifrado y claves
criptográficas

Encapsula los protocolos de
Nivel superior

Anexo "13"

SSL Handshake Protocol



The Future of Wireless Banking

Implementation of Wireless Banking and Financial Systems

Rod Ghani
Senior Consultant
IBM Global Services
03/15/2001

Introduction

Have you seen change yet?

Today's banking and trading institutions realize they must move and move quickly to capitalize on new business opportunities in wireless banking and trading. Resistance to the implementation of wireless banking can lead to major losses at the business and market share levels.

Wireless service soon will be a necessity for the end-user. Although many technological barriers need to be overcome, it is imperative to embrace the change.

Wireless banking and trading is only an extension of the product offerings for the financial institutions. It is not an extension of web technology, as often perceived.

Online banking and online trading works from standard TCP/IP connection to the Internet using a PC, while wireless applications present a much greater challenge.

Today, wireless banking lacks leadership in enforcing one standard. There are several network standards, PDA standards, browsing standards, protocol standards...etc.

In the wireless world, airwaves are the only vehicle to send and receive data. Depending on the physical location- inside or outside of a building, near or far from a tower, in a small town versus a metropolitan area- quality is highly variable.

Did my order go through?

Non-repudiation is one of the most contesting issues in wireless banking and trading. The user needs to have proof that the transaction has been executed and confirmed.

Wireless banking is revolutionizing the makeup of every financial and banking institution. It is radically transforming the services, needs, and expectations of societies across continents, regardless of culture. In the next twenty-four months and beyond, massive changes will occur in the way we interact with banks and trading institutions regarding our business and personal finances.

The revolution is driven by the client (end-user) demanding to have the information available conveniently anytime, anywhere. Immediate access is expected and required.

Change at the institutional level is not an easy task. Adaptability and flexibility are needed when dealing with a variety of legacy systems, connectivity issues, protocol challenges, and a constant explosion on the market of new devices. Large institutions are handicapped by their size and have to become aggressive to keep up with the rapid times.

Today, B2B, B2C, B2G and B2E are recognized to be vertical online markets. Wireless is going to subdivide these markets, and new services will emerge targeting new user groups.

Data managers and system developers are expected to offer more effective and efficient methods in data delivery, anytime, anywhere, using any device, regardless of platform, protocol, browser, service provider, financial institution, etc.

A snap shot of the future

- The Gomez Research estimates that the number of people accessing personal account information online will grow from approximately 8 million in 1998 to nearly 40 million people in 2003. Given the numbers, banks and other financial providers must realize the opportunity inherent within Internet and wireless capabilities.
- According to Jupiter Communications, approximately 100 million people in the U.S. will have wireless non-PC web access by the year 2003, versus 155 million landline access from PCs. This deduces that non-PC access will grow to 65% of the wireline PC access market within the next three to four years.
- According to Forrester research, almost 120 million Europeans already use mobile phones, exchanging more than two billion wireless text messages each month.
- By 2003, Forrester projects 219 million Europeans, or one-third of the population, will be on the wireless bandwagon. Of the 50 European e-commerce executives interviewed by Forrester, 90 percent plan to launch sites that will be accessible by mobile phones
- Financial products and services provide an ideal setting for Internet delivery. M-Bank is well positioned to serve this industry with companies such as Wells Fargo and Co. (NYSE:WFC), Bank of America Corp. (NYSE:BAC), Providian Financial Corp. (NYSE:PVN), MBNA Corp (NYSE:KRB), and Capital One Financial Corp. (NYSE:COF).
- A major bank reports that over 3 million online banking customers, representing more than 20% of its checking account customer base that it continues to sign up approximately 130,000 new online banking customers a month. Also, more than 750,000 online banking customers have signed up for the bank's electronic billing and payment service, says the institution, and the total dollar value of payments processed grew 36% last year. Over 3.1 million EBPP were made, totaling more than \$1 billion.
- "It took us over 10 years to reach two million online banking customers and only nine months to add one million more," says Jeanine Brown, Interactive Banking executive.
- GartnerGroup predicts that by 2004, 80 percent of new applications for consumer use will permit access from mobile device clients (Source: GartnerGroup conference 1999).
- GartnerGroup research estimates there are more than 60 million employees worldwide working outside the traditional office setting. The Gartner study also says that the number will grow to 108 million by 2002.

	Current Users	Potential Users
Developed Countries		
Developing Countries		
World		
Worldwide Potential		
Worldwide Potential (2002)		

Little G History

1G is the first generation in mobile technology. Started in the late 1970s until the late 1980s.

2G began in the 1990s and it is still being used today, such as CDPD, CDMA, and GSM.

3G is the third-generation of wireless. It is expected to reach maturity between the years 2003 and 2005.

3G is expected to deliver enhanced voice and data and even video. Its bandwidth can be as high as 2 Mbps and will operate at 2 GHz.

Will Wireless banking play a major role in new markets?

P2P (Person to Person), and P2A (Person to Anyone) will play a major role in the financial world. We will witness an abundance in money transfers. A user can make a payment, have it automatically deducted from the appropriate account, and deposited into the recipient account, with an email acknowledgement.

It's about time

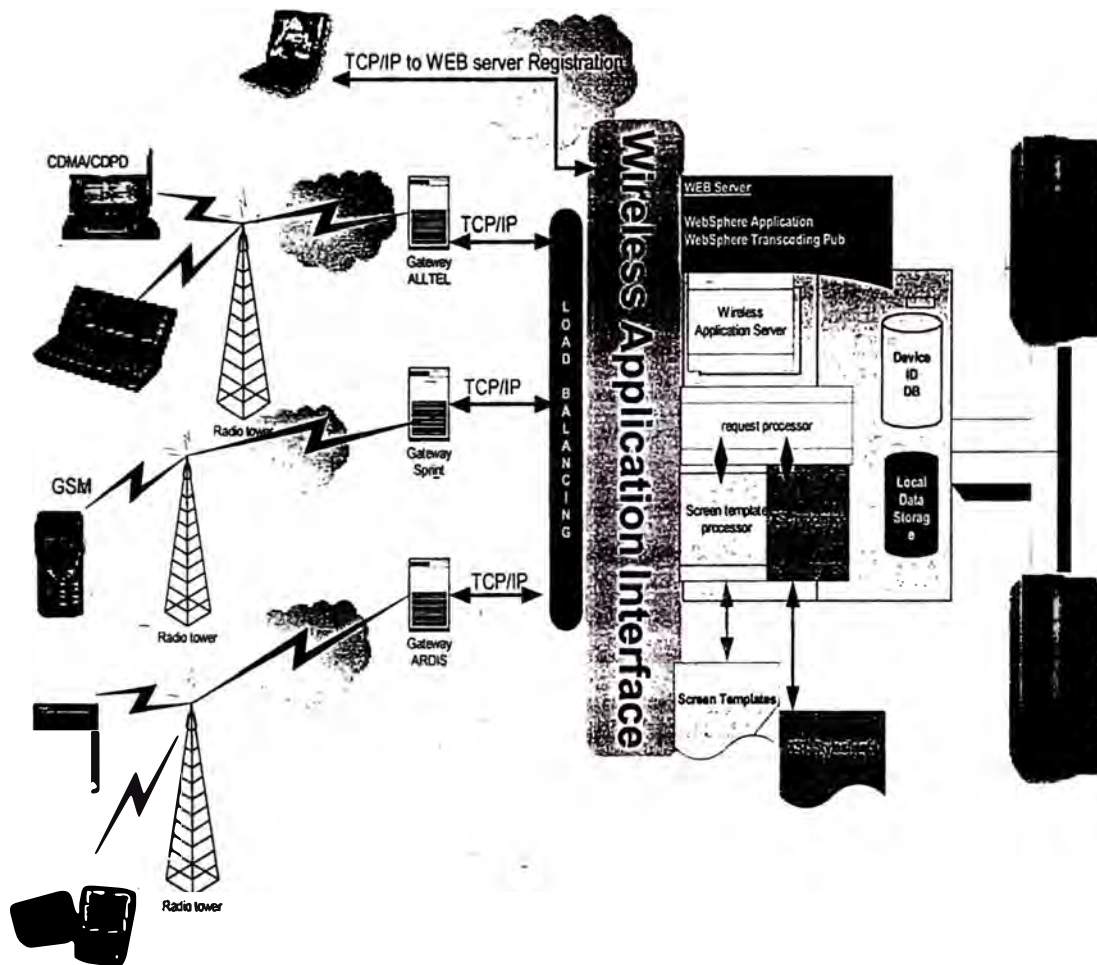
Time is the essence. Wireless banking and trading advantages are increasing by the day due to a rapid advancement in technology, rapid growth in wireless coverage, cost reduction in networking, and improvement in handheld devices, and bandwidth efficiency. Today, we can accomplish far more in wireless services, where it was not cost justifiable a year ago. With that in mind, WSP (Wireless Service Providers), corporations, and financial institutions can bank on the growth and take advantage of these opportunities.

The winners in today's wireless world are those who keep up with the change, cope with the challenges, and utilize the products and services offered.

Financial institutions must drive to enhance the systems delivery to create layers of an open system environment. Those who will use standard protocols will expand and thrive. Successful wireless implementation is delivered when the end-user can interact with the data easily, securely, and independent of a network operator or handheld device.

What are the components of a wireless system?

- Handheld devices
- Connectivity, Coverage, and Gateways
- Middleware processing engine
- Transcoding
- - API connection
- Data System Backend system



1- Handheld Devices

1. Thin Client devices, Palm, Workpad, Ipaq..
2. Two Way paging devices, like RIM
3. Smart-Phones, WAP phones
4. Others
5. Operating systems is a software program that manages the basic operations of a computer system.
 - a. Windows CE:
This is a light version of windows, developed by Microsoft. It is Installed on many of the PDA devices.
 - b. Palm OS:
It is developed by 3COM, proprietary platform. It is the most popular OS on the handheld due to the large market share that the Palm Pilot owns today. It supports some Java applications.
 - c. Linux: It is very promising for growth, open source base, Java friendly , very efficient, and it can be installed on many PDA devices and even on smart-phones
 - d. EPOC:
Symbian consortium drove the development of this operating system mostly for smart-phone devices used by Ericsson and Nokia. EPOC is one of the major operating systems in this market.

Each one of these handheld devices will require certain ways of communicating; they require their own Gateways to communicate to the application servers. Various sizes of screens create different data and screen layouts. Different keyboards generate different navigational options and different keys. The challenge is for the application server to sort out these devices, and send the data in the correct format to each handheld device.

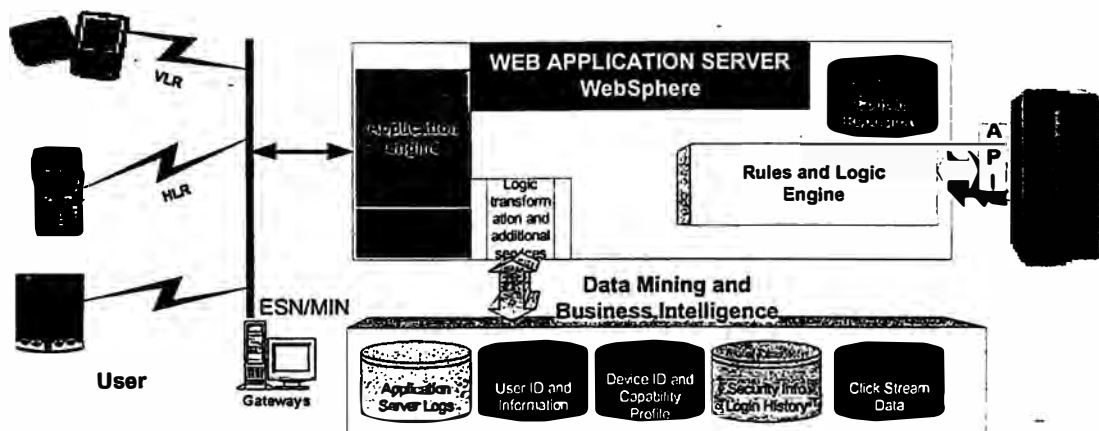
2- Connectivity, Coverage, and Gateways

In this section, we are going to explore the basic components of the wireless network architecture.

Starting from the end user, the handheld device can be any device that is used to access a local cell tower.

A cell tower is responsible for delivering local geographical coverage in a certain region. The coverage is divided into hexagonal boundaries.

The cell tower then sends the data to a Base Station. The data is then transferred to a switching center. The mobile switching center connects all Base Stations. The mobile network system will record, and identify all of the users information by Home Location Register (HLR), if the user is in the geographical network. If not, then the Visitor Location Register (VLR) will be tracking the call. This is when you pay



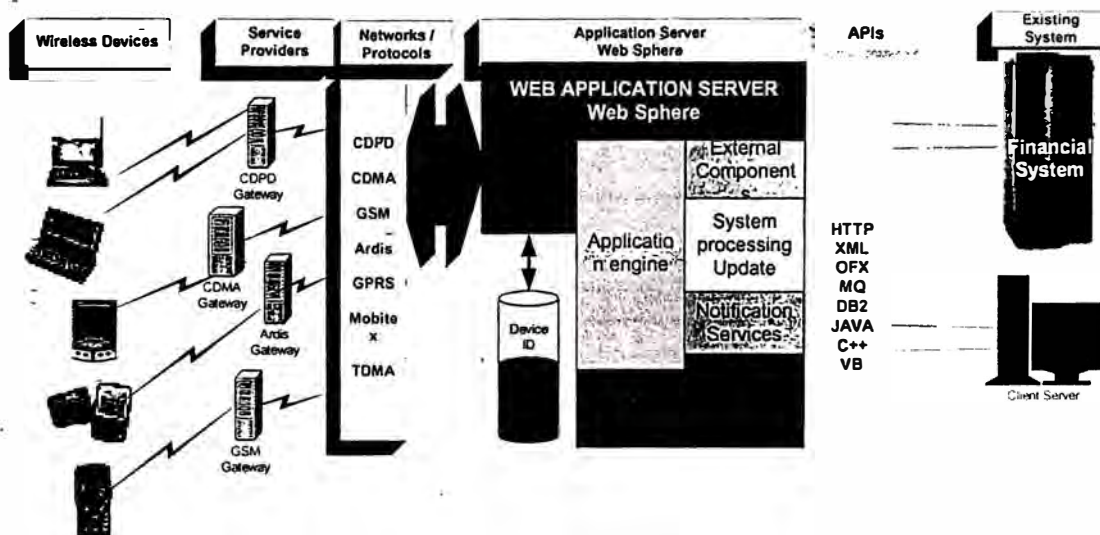
the big bucks for roaming. Once the call is initiated, the device will send its identity via its electronic Serial number (ESN) and Mobile Identity Number (MIN). This information is vital to have so the gateway can authenticate the user. This is where the application server can prepare the data to send back to the appropriate unit to be displayed.

A packet is a collection of data prepared in a specific way for transmission. There are two types of transmissions, circuit switched and packet switched. Circuit Switched is a dedicated circuit for communication between two dedicated devices. Its duration is for the entire call. Packet switching does not require a dedicated line between the sender and the recipient. This method enables the data to be divided into a number of packets and to be sent in different paths for its intended destination.

The connectivity will vary from one device to another, and from one service provider to another. The most challenging issue about the wireless systems is coverage.

As end users sign up with WSP (Wireless Service Providers), they quickly come to realize that the packages offered are not so perfect. Due to the limited coverage areas, it seems as if it's always the right plan at the wrong place.

Wireless service plans will vary in options as well as in cost. Some of the common protocols that the WSP support are GSM, (not so big in the US yet), CDPD, CDMA, Ardis...etc. All of which are trying to make it big. Wireless Service Providers are all jockeying for the position to be the global provider.



3- Wireless Middleware (Application server engine)

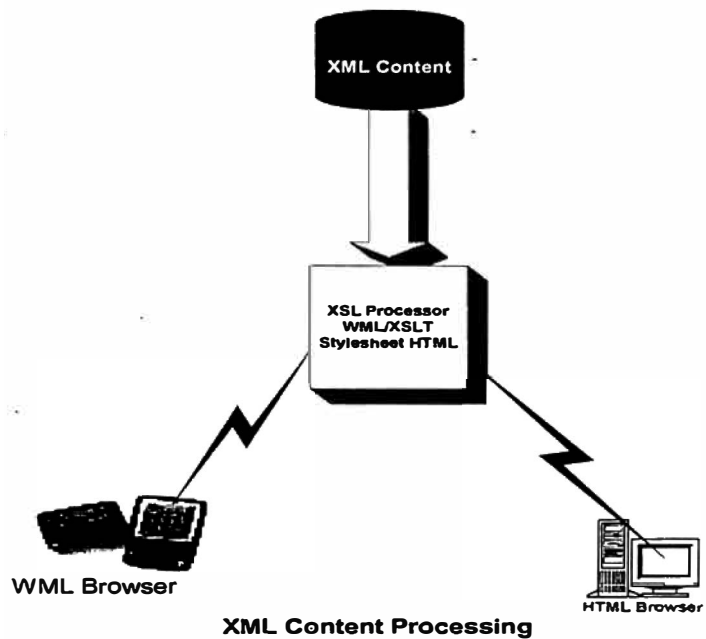
Wireless application is the focal point of the wireless system. This is where the flow of data is controlled, rules are set, and configuration files are executed. The application software should be an open system, easy to connect to and talk to other systems. One of the most common methods of communicating with backend systems is using XML API as the data delivery tool.

XML is used to extract and deliver data; XSL can perform the transformations, using the DTD files to execute the functions agreed on in the integration and design stage. Different handheld devices will have different screen templates. The Application server should be tracking the users sign-in by the device being used, in order for data to be presented correctly. The screen templates can be XML documents which conform to DTD files. The screen templates are used only to define the layouts of the screen. They are device specific.

4- Trans-coding, is it magic?

Transforming is the process of formatting the content (data) according to the handheld device request using XML, XSL style-sheets and DTD files. This method will enable the end-user to access data universally regardless of the device type.

Once a request from a handheld device is initiated, the application server will intercept the request to identify the device type and capture the content. Using several logical processes, the application server engine will process the data into an XML document, which can be communicated with the backend system via the API connection. The result of the requested data will be transformed-(processed) using XSL style-sheets and then reformatted for the handheld device that made the request initially. This process can become complex very quickly, depending on the number of the handheld devices supported and the type of services offered by the financial institute. Therefore, products like IBM's WebSphere can be valuable tools to build a robust financial system in a short time. The WebSphere application server will handle the data dynamically and adapt it to the handheld device. Also it can run multiple applications and requests, and can be easily integrated to the backend system.



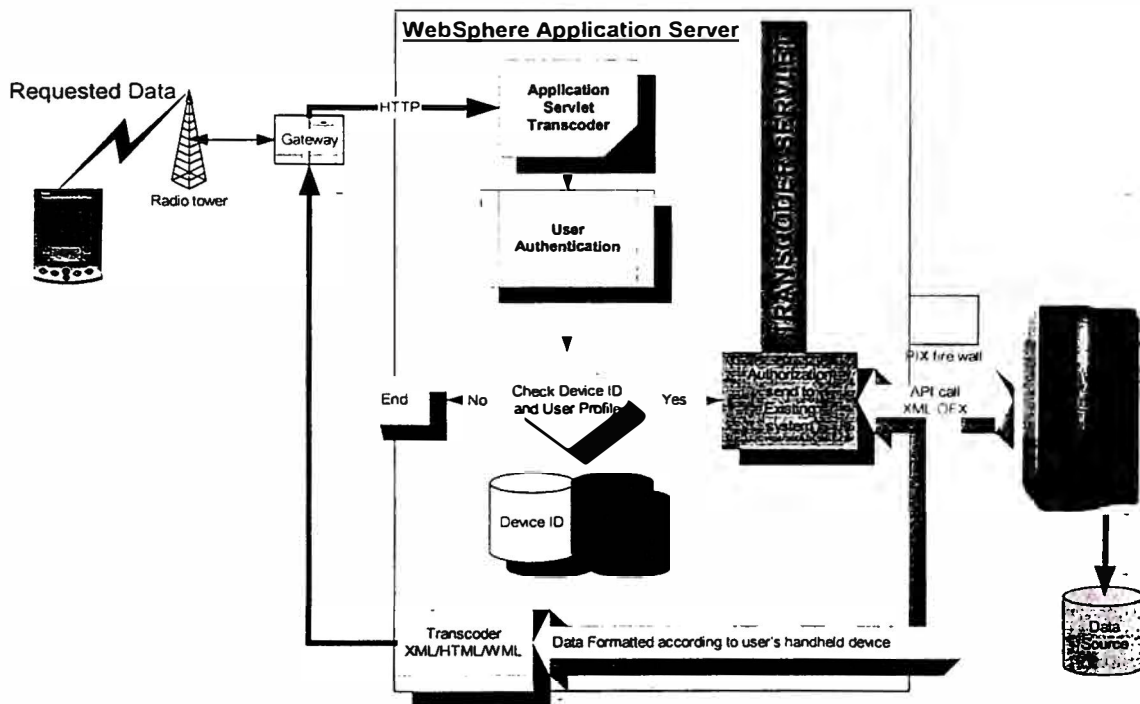
The WebSphere engine will select the correct screen template, format the data for the handheld device, and deliver the data requested. XSL is used for data transformation definitions, where the API will exchange the messages between the backend system and the application server. XSL and XSLT style sheets are mainly used to manage the presentation of the data, whereas the XML is handling the data.

Managing Data:

The application server can use common device characteristics to display the data. Using these standards can help in the development productivity.

User IDs and handheld device IDs are stored in the database at the application server level. The application server will access the database once a login request is received. The middleware database is used to prepare and format the data for the device requesting the login. The application server will also compare the registered device ID to the user ID for additional security verification. The application server communicates with the gateway server for the specific device that initiates the request. The gateway will push the information to the handheld device according to the connectivity platforms like CDPD, SMS, Mobitex, and CDMA.

The application server must accommodate for the different handheld platforms such as, thin client devices (IP based device), two-way paging, SMS messaging, and smart phones. It must then deliver the formatted data for that specific device data accordingly, end to end, in a reliable and secure manner.



Pushing or Pulling data?

Pull technology is when the handheld device initiates the communication using its gateway, requesting data. Then data is pulled from the application server down to the handheld device.

Push technology is when the application server is in more control over the handheld device. The application server will make decisions for the basic content and push data to the handheld device without waiting for the client's request.

In either, method authentication must take place first. The gateway transfers the handheld's request to the application server (middleware). The application server will then know the device type by its identifier. The information will be sent to the backend system of the financial institute, using the API between the application server and the backend system. The application server will receive the information from the backend system to report it to the handheld unit. At this time, the data will be formatted into appropriate screens for the device that requested the data. The data will be passed back to the wireless server provider gateway, and then back to the handheld device.

Wireless application Server must be device and network independent:

The wireless application server must be able to work with any of the networks offered by the Wireless Application Providers. The Application server should be:

- Easy to install, configure and add new services:
- The client application must be easy to install, customize, and add new handheld devices.
- Easy to Integrate with other servers and Back-End systems:
- Integration is one of the key steps for a successful implementation of the wireless project. The API of the existing financial institute's system must be reliable, and secure.

Open System:

The application server also must be an open system, using standard protocol to make it easier to add or change services, devices, and apply any customizations needed.

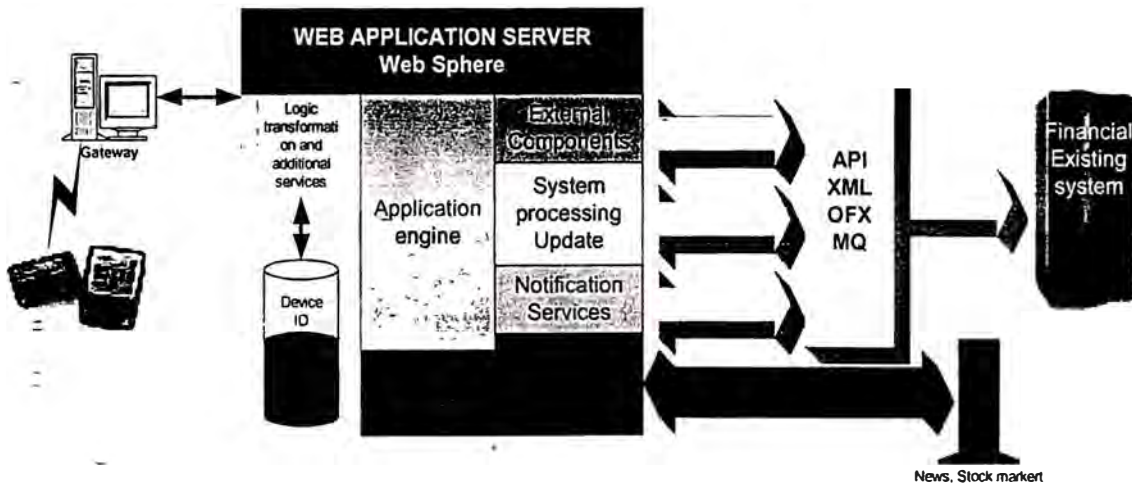
What about Screen Scrapping?

Screen scrapping is one method I would not recommend to use as a final solution. It's not a stable solution, due to maintenance required to keep updating the macro reader when fields are changed in the source document (Website). This method can leave more room for error. Screen scrapping is quick to implement, which can be a good tool for data presentation in the proof of concept stage.

The Wireless Application Server is not an Internet server nor an extension to the Internet:

The explosion of the wireless application industry in the last year or so has resulted in a common misconception. That is the wireless world is simply an extension to the Internet. While some wireless-enabling companies do use web-scraping (screen-scraping), a technique that captures screen content and transfers it to a wireless device. This technique tends to produce poor performance and unreliable wireless service. It's also more manual and maintenance intensive.

The most effective way to build a wireless application system is to connect into the back-end system, regardless of type. It could be a mainframe, client server, or a even Web-based system, using a direct connection via API.



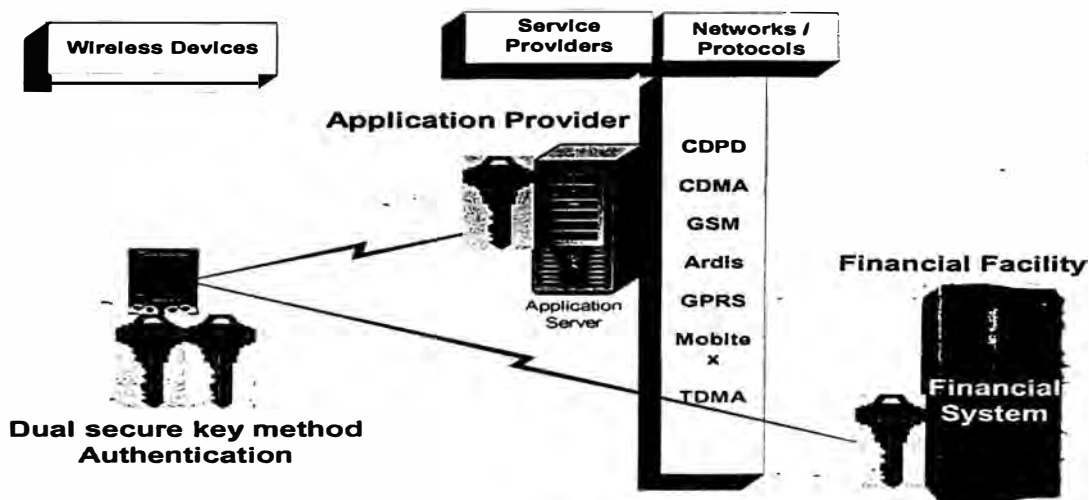
Security and Wireless Banking and Trading

Security is probably one of the most important issues in wireless banking, if not the most important.

A recent study on wireless banking security uncovered the main challenge facing both wireless banking innovators and online banking establishments; nearly 85 percent of respondents are worried about online security transactions, including credit card purchases. More than 90 percent expressed concern about revealing personal information online, such as social security numbers. Over 90 percent of proprietary cryptography has been broken. Cell phone systems have been hacked.

Wireless banking and trading is more vulnerable to attacks by hackers than many other wireless services. When data is flowing across a vulnerable environment, many of the available operating systems for phones and handheld devices offer little or no security. Most security violations occur within the institution or the service providers.

Customizing wireless security is extremely difficult, especially when computing power on the handheld devices is very limited.



Double key secure authentication is one of the protection methods used to verify access across different systems. Double key secure is where the user will authenticate two systems, the application server (at the Hosting service provider) and the financial institute. The transaction will be granted access, only when both locations agree.

Secure network architecture is achieved when all interaction points and data paths traveled, are implemented by using double secure keys.

It's proven this method of security can drastically reduce violations and system hacking internally and externally, because all three parties must agree. One of the more common securities used is PKI (Public Key Infrastructure), an encryption used for PDAs and Smart-phones security. PKI consists of two keys, a public key and a private key, used to authenticate the user and encrypt the data.

In addition, the financial institute should utilize the system to monitor access logs and flag questionable connections that can be done on the application server.

Encryption is a trade off between speed and security. A good rule of thumb is to encrypt on a 32-bit CPU at the rate of ten CPU clock cycles per byte. Look for the most compact software. It should run under 5,000 bytes of memory. Encryption can vary form one device to another, depending on the platform and the operating system. For additional protection, authentication can be implemented through user ID and password.

The Challenge

Wireless banking implementation is demanding. There are constantly changing standards for APIs, gateways, security methods, screens, operating systems, and browsers. There are also variable computing powers on the handheld devices and different bandwidth requirements.

Wireless banking can be risky, lengthy, and complicated to develop. APIs (interfaces) must be designed to connect to the existing backend system. The application server must be able to accommodate to all protocols and all devices. You never know which device the end user is going to use.

The application server must be able to communicate with all gateways, like WAP, GSM, two way paging, etc...

A product like Web Sphere can reduce development time drastically. Transcoding tested templates can make the developer's life much easier. The end result is a robust solution. Consulting companies promise a lot, but only few can deliver.

Since wireless banking is still at it's evolutionary stage, we must keep up with new technological advances, products, and development tools to help ease the transition.

The wireless network must be device and network independent. Most handheld devices have their own standards to deliver data across the data channels. The end user should be able to easily customize screens, alerts, notifications, and messaging request services. The system should be able to notify users regardless of the device type. Scalability is a major issue. Selecting the right platform to run the application server will dictate the available tools to work with. The wireless banking system must be an open system that can easily and reliably be integrated with new gateways to the backend system. This is a challenge not many banking institutions should undertake on their own.

The next best thing is out sourcing the development of the project, the implementation, and the hosting. Using a third party to administer and host the system is an option I would choose.

Selecting the right application vendor:

The vendor must have developed and installed a wireless financial system and must have a wide range of experience. Look for the following:

1. A trusted name and the longevity of the vendor is important
2. The vendor must have tested and used the product in a field specifically related to your field. For example, Wireless Trading is more demanding than Wireless banking. Wireless trading is time sensitive. Stocks, options, mutual funds, and bonds are all different services requiring different tools to process orders. The system must be able to deliver the data flawlessly and quickly to any handheld device. Wireless trading requires research capabilities. Wireless trading is much more active delivering user alerts, such as watch lists, quotes, charts, reports, notifications, summaries, and portfolio statuses. The wireless trading could be using external systems to gather data. The point is to be specific when dealing with application vendors; not all financial services are the same.
3. The testing and quality assurance stage must take place as early as possible to certify the systems. The application or applications must integrate fully to the backend system or systems, regardless of device type or platform. Management of all users definitions, events, requests, updates, changes, and requirements must be tested thoroughly.
4. Application servers must include monitoring tools and protocol management of all requests.
5. A turn key solution is an end-to-end solution. It goes from the backend system, where the data source resides, to the API connection, to the application server, to the WSP gateways, and then to the handheld units.

6. The vendor must have widely available resources and experienced programmers, systems architects and project managers. Additional manpower must be available immediately if needed.
7. References and physical site visits are key to comprehend the consulting, development, and hosting environment. The consulting company will be an extension of your business. This is the life link between you (your system) and your customers using the services.
8. Backup and catastrophe planning must be in place.
9. The wireless application system must be network and device independent. The application should be fully configurable with customizable screens, using standard API's. The wireless application server must be an open, modular architecture, to provide the user with the maximum flexibility and extensibility to make the development and deployment easier.
10. Development tools to enable you to make changes, add services, or deploy applications are crucial.
11. Products like IBM Web Sphere are End-to-End Solution for the wireless banking and trading enterprise. The IBM Web Sphere solution and Web Sphere Everyplace Suite are highly scalable server software, and have development tools for connecting millions of wireless devices to the Web. Java is capable to transcode, encapsulate the application logic, access XML documents, XSLT style sheets, and define the presentation. The Web Sphere architecture will help the programmer to focus on providing high quality. Web Sphere can handle the presentation and data management without getting involved in dynamic content generation. Views and screens can be developed for different devices easily and quickly using the same application logic.

The road to a successful implementation:

Remember, wireless users will not be able to multitask using the handheld devices; therefore, easier navigation will play a major role in the success of the project. It's crucial to test all users' functionality thoroughly, no matter how tight the schedule is for implementation. Depending on the type of network to be implemented, number of markup languages, and handheld devices to be supported. Testing can be cumbersome and complex. It is always a good idea to use multiple software development tools to test for the real world users. The financial institute should make use of the following steps for implementation and testing:

1. Documentation, Documentation, Documentation!! (in this order). Document all rules, procedures, and specifications.
2. Setup the application network environment as early as possible. Start with high-level conceptual and visual design.
3. Run traffic studies on bandwidth required to communicate between the backend system and the middleware system (application server), the gateways.
4. List all users functions and requirements.
5. Perform user analysis.
6. Perform technical assessment.
7. Hold users group meetings.
8. List business requirements.
9. Define functional requirements.
10. Definition of performance requirements hardware and software.
11. Use a standard API like MQ, or OFX (common in the banks industry), or develop XML API, which is becoming more popular.
12. Design business performance and process requirements.
13. Develop delivery plan.
14. Build a proof of concept to test all systems functions and requirements. Test APIs and architectural designs of the applications. Integrate with the data source (existing system) directly.
15. Start with a pilot (limited users).
16. Fix bugs, and fine tune systems performance.
17. Implement the full-scale rollout.

Conclusion

We must react to the new world economy quickly and offer what the clients are looking for!! The future of wireless banking is massive and aggressive in terms of requirements, demands, and support. The good news is, it's great for financial business, but we must be cautious in implementation and execution to deliver a reliable service.

Wireless media is challenging. Many variables are not under control yet. Coverage is a big hindrance. Legacy systems with different topologies and different platforms make things even tougher. There will be more streamline markets demanding new ways of conducting transactions.

The future of wireless banking and trading has promising magnitudes of growth. Jupiter Research expects 18 million more people in the United States will become wireless subscribers in 2001, increasing the total number to 128 million. Moreover, the percentage of subscribers with Internet-ready wireless handsets will quadruple during this year.

Despite millions of new users, the wireless market can expect some real challenges in the near future. "While penetration of wireless data services will gain momentum in 2001, a lack of substantial new technology deployments in the United States will stifle true innovation. Location-based services, high-speed networks, and highly sophisticated handsets will remain elusive in 2001."

Wireless banking is sensitive to security, and is essential to finding the right balance between speed and encryption. Accuracy, consistent availability, and reliability of the services are key to a successful implementation and survivability of the financial institute.

Geographical coverage is imperative to successful implementation. It must be clearly defined and understood. The confirmation of transactions is key to show the level of commitment and accuracy to your customers.

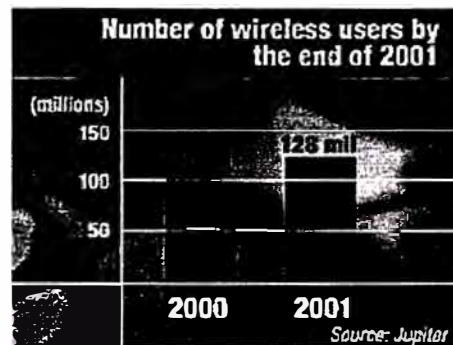
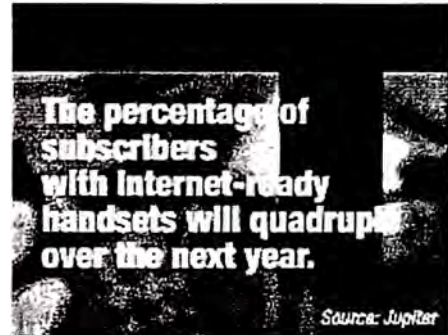
Wireless banking is greatly dependant on the efficiency of the bandwidth. The more efficient the bandwidth, the faster the content is downloaded. End-users requirements are driving a demand for faster transmission and higher bandwidth capacity.

In order to offer an enterprise wireless solution, major consortiums of the industry must break all political barriers and agree to a global format of communication. The consortiums must arrive at solution that can access all platforms across all networks regardless of device type, much like the Internet.

The financial institutions are between a rock and a hard place. They would like to extend their services to the wireless world, but they lack the resources and the expertise to implement and deliver to their customers in a timely manner.

Therefore, out-sourcing can be a vital option for the following reasons:

1. The financial institute can focus on their core business.
2. Extend the product offering in a timely manner, and get to the wireless market place sooner.
3. Outsourcing will help predict cost better, and forecast more accurate budgeting.
4. Use of the latest in technology.



Benefits of WebSphere middleware application server:

- The financial institute can extend the reach of its product to new markets in a much shorter time.
- Communicate with handheld devices seamlessly to access data and applications.
- Enhance data transfer using the load balancing function, which can detect bandwidth capability and optimized data streams.
- Reliable systems processing, and commanding encryption.
- Sophisticated monitoring tools.
- Reduces development time greatly.
- Scalable open architecture using XML and XSL standards.
- Integrates easily to backend systems, such as Mainframes and Client servers.
- Unmatched product support.
- End to end solution.

Wireless banking and trading must be a virtual and global solution. Competitive forces will shape the wireless banking industry and help deliver the offerings desired to the end users.

Wireless banking must reach a global standard before it can be unleashed to its greatest potential.

API	Application Programming Interface
CC/PP	Composite Capability/ Preferences Profiles
CDMA	Code Division Multiple Access
CGI	Common Gateway Interface
CPI	Capability and Preference Information
DCS	Digital Communications System
DTMF	Dual Tone Multi-Frequency
FDD	Frequency Division Duplex
GPRS	Global System for Mobile Communications
GSM	Global System for Mobile Communication
HTML	Hyper- Text Mark-up Language
HTTP	Hyper-Text Transport Protocol
JDBC	Java Database Connectivity
JSP	Java Server Pages
PCS	Personal Communications System
PDA	Personal Digital Assistant
PDC	Personal Digital Cellular
PeMS	Personalized e-Messaging Server
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
RDF	Resource Description Framework
SMS	Short Message Service
SSL	Secure Sockets Layer
TDD	Time Division Duplex
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WBXML	WAP Binary XML
WCMP	Wireless Control Message Protocol Wireless
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTA	Wireless Telephony Application
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformation
WTA	Wireless Telephony Application
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security

3G:

2B

or

Not

2B !

IBM Wireless

**By: Rod Ghani
August 2001**

Table of Contents

The Future	3
Background	4
1G	4
2G	4
3G	4
3G is based on packet switching technology	6
3G Standards and Specifications	6
3G is on a mission	8
Political challenge not technical	8
Building up from today's digital infrastructure network	9
3G is not home alone.....	9
Seamless IP: Is it meant to be?	10
Security	12
Conclusion.....	13
Appendix	15
References	15
Glossary.....	16

The Future

You are riding in a car with your colleague who is driving. Suddenly, your hand-held device comes on, asking you if you can take a video conference call from your team in Europe about a project you are working on. The call comes on and as you are watching them explaining the topic, you decide they need one of the spreadsheets you have in your laptop, which is in the trunk of your car. Using your Bluetooth technology you can transfer the file to your hand-held device and send it to your team in Europe while you are video conferencing with them. A few seconds later your team will receive and open your spreadsheet and start discussing options with them.

Now, you are thirsty from talking too much with your team, and search the net for the closest place to get a drink, and possibly an appetizer. Minutes later you arrive at the place and pick up your order. Using your hand-held unit, you transfer money from your account to the restaurant's cash register. You decide to have your drink and watch the local news in your hometown (which is about 1000 miles away) via your hand-held unit. The news recommends a new movie that just got the two thumbs up, so you switch over to your movies on demand and enjoy. While you're watching the movie a call from your excited daughter comes in. She wants to show you her A+ grade she got on her science report using her videophone.

Gas stations can also be automated. Once gas is pumped into the car, the charges are approved via a handheld unit or a device in the car using Bluetooth technology. Funds are transferred from the consumer's account into the gas station account using the 3G (3rd generation, global wireless connection) and short-range technology, the global wide area network. The same scenario can be applied to an intelligent vending machine. The service provider and the consumer both benefit a great deal from such technology by getting funds instantly and eliminating paper work and unnecessary delays. Also, price changes, re-ordering product, inventory control, service and warranty requests are easily done.

Don't leave home with out your PDA, in fact you should wear it.

Wearable communication devices are the up and coming fashion for the next few years. They come in the form of earrings, rings, and glasses. They are going to be hot commodities for retailers and service providers.

These devices are now called "wireless interactive devices" or (WIDs). WIDs are the next generation of the personal digital assistants or "PDAs". It is expected that these devices will be widely adopted by the consumer once speech recognition and wearable displays have been added.

Consumers may not have to carry cash ever again. With the major advancements being achieved with smart cards, now with a 100 Kbytes storage capacity, consumers can process transactions by selecting bank accounts or credit cards and transmitting the data to a merchant. This will be a dream come true. The PDA can also hold health records and personal information, etc.

Stowbridge Research (http://www.3gnewsroom.com/3g_article/article_0013.shtml) believes 3G phones will even have features we haven't considered yet. "People could buy smelly phones, which could attach a scent to an e-mail." This would be a benefit for e-commerce, as well as for personal communications. Do I need to go any further.. This is the reality of the future. Please join me in investigating how this will unfold.

Background

1G:

In the mid-1980s, two visionary telecommunication engineers came up with the idea for simple wireless voice services based on analog cellular technology. However, this technology offered low quality voice and coverage problems.

2G:

2G inherited many digital platform standards such as, TDMA (Time Division Multiple Access), circuit switched based technology developed in Europe, the IS95, based on CDMA (Code Division Multiple Access) technology systems, mainly GSM (Global System for Mobile).

2G provides better voice quality, higher capacity, global roaming capability, and lower power consumption.

2G systems also offer support for simple non-voice services like SMS (short messaging service). However, different 2G technologies are not compatible. There are also difficulties with roaming between GSM and IS95 countries. In addition, the low bit transfer rate of 2G systems (9.6 kbps for GSM) makes it unfeasible to transfer multimedia files, Internet browsers or large data files, which the consumer is now demanding.

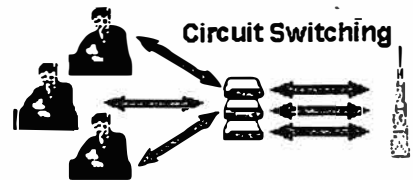


Figure 1 - Circuit Switching

3G:

UMTS ((Universal Mobile Telecommunications System) or 3G:

3G is a digitized voice, packet-based transmission of text, multimedia, (video conferencing, movies, etc.) at possible data rates higher than 2 megabits per second (Mbps). 3G services are being established by the International Telecommunications Union (ITU) and other regulatory bodies.

Major manufactures and operators around the world endorse UMTS. UMTS will roll out by 2002 for mobile users no matter where they are. The users will have access to a combination of satellite transmission and terrestrial wireless communication.

In order to achieve such throughput, we must think packet-switched connection because it is more efficient and effective in data transmission. Using the Internet protocol, a virtual connection is always available to any point in the network. Also the packet-switched connection is flexible enough to add other services, as well as easier billing methods such as flat rate, pay-per-session, asymmetric bandwidth.

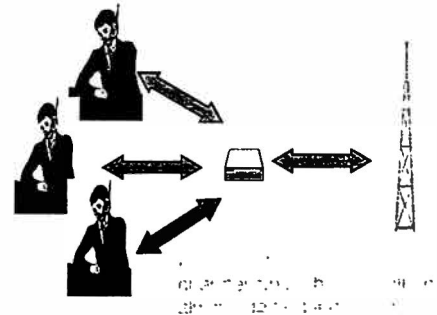
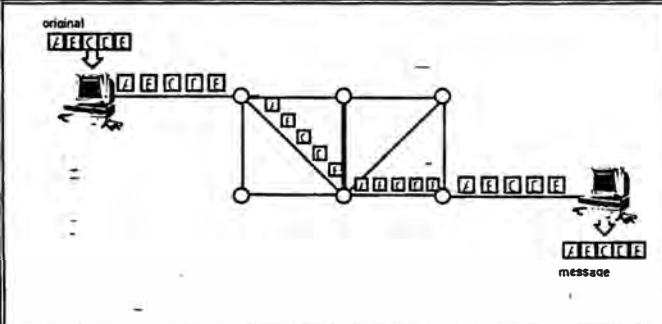
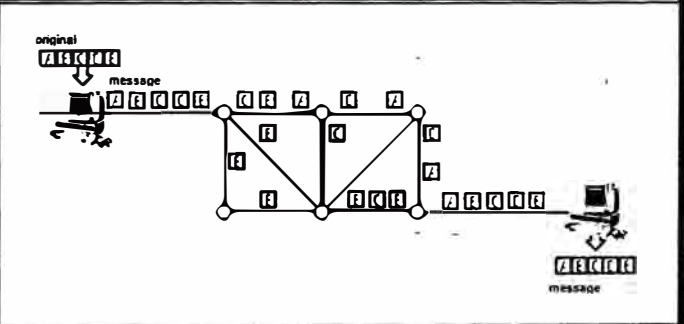


Figure 2 - Packet Switching

Table 1 - Technical Specifications & Features

	TECHNOLOGY		Speed	FEATURES
1G wireless	AMPS	Advanced Mobile Phone Service	4.8k-9.6k bit/sec.	<ol style="list-style-type: none"> 1. Analog voice service 2. No data service
2G wireless	CDMA	Code Division Multiple Access	9.6K bit/sec.	1. Digital voice
	TDMA	Time Division Multiple Access		2. Simple email
	GSM	Global System for Mobile		3. Data connection is limited
	PDC	Personal digital cellular		4. Download 3 min MP file 31-41 min
2.5 wireless	CDMA	Code Division Multiple Access	64-144K bit/sec.	1. Digital voice
	TDMA	Time Division Multiple Access		2. Send/Receive Large email
	GSM	Global System for Mobile		3. News Update, Web browsing
	PDC	Personal digital cellular		4. Download 3 min MP file 6-9 min
3G wireless	W-CDMA	Wide-band Code Division Multiple Access	UP to 2 M bit/sec.	1. Superior voice quality
	CDMA-2000	Based on the Interim Standard-95 CDMA standard		<ol style="list-style-type: none"> 2. Send/Receive Large email 3. News Update, Web browsing, always-on. 4. Multimedia, video conferencing 5. High Speed, Enhanced roaming 6. Download 3 min MP file 0.2-1 min

Table 2 - Circuit vs Packet Switched Technology

Circuit Switched	Packet Switched
	
<ol style="list-style-type: none"> 1. Basis of the public switched telephone network (PSTN). <p>Two devices initiate a dialog and establish a dedicated path through the network (a circuit).</p> <ol style="list-style-type: none"> 3. Information arrives in the same order it was sent. <p>Fixed, guaranteed amount for duration of connection.</p> <ol style="list-style-type: none"> 5. Inability to make use of less busy paths when network is congested. <p>Connection delay (physical connection must be established prior to data transmission)</p> <p>Little processing required at the nodes.</p>	<ol style="list-style-type: none"> 1. Basis of the Internet and most data communications services. 2. Messages broken into packets that are individually transmitted through the network. <p>Packets may take different routes and arrive in a different order.</p> <ol style="list-style-type: none"> 4. Variable (resources used only when packets being sent); but not necessarily guaranteed. 5. Packets can be routed around damaged or busy segments. <p>Queuing delay (shared ports on network devices).</p> <ol style="list-style-type: none"> 7. Requires more processing power at the nodes.

3G is based on packet switching technology

Network capacity is measured by the amount of data transferred over a period of time. In the case of 3G, the measurement is packet-based, and time based. This means the consumer is always connected, and a network resource is used only when actual data is transmitted. This is unlike circuit switched technology, where a dedicated circuit must be established between communication devices.

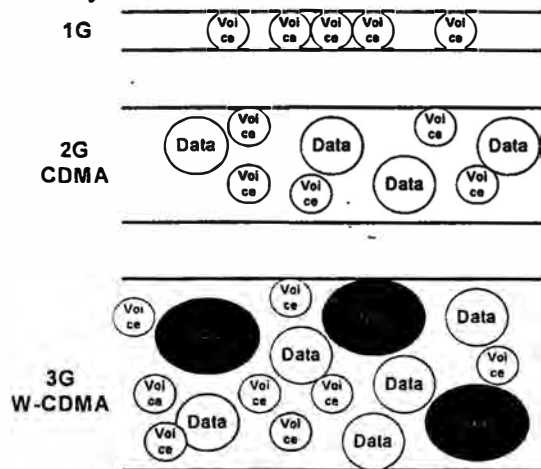


Figure 3 - 3G Services Compared

Most networks today using circuit switched technology, much like a telephone call, must be open to voice or data transfer until the call or the transmission is terminated. This architectural design is network demanding and circuit hungry.

3G will be based on more efficient communication technology called packet switching, where packets of data are transferred on different circuits using the shortest path to the intended receiver. This is made possible by using sophisticated data handling methods for voice and data transmissions that are bundled into digital packets. 3G will have a 2Mbps transfer rate with multimedia support. CDMA, IP base and EDGE (Enhanced Data Rates for Global Evolution) technology will be the new standard of the new global network.

3G Standards and Specifications

High-speed transmission multimedia support and video using digital packet switching is 3G technology. 3G will be standardized under 3GPP. Japan and Europe are taking the lead using WCDMA-DS. The United States will be using 3G *Harmonization of UTRA and CDMA2000*

There are three technologies under development for third generation systems:

- DS-CDMA (UTRA FDD)
- MC-CDMA (chip rate of 3.68Mchips)
- UTRA TDD (chip rate of 2.84Mchips)

The goal is to roll out 3G world wide, converting from 2G. Even though there will be three different 3G technologies, the primary 3G objectives will still be achieved. Which are:

Always on

- Global connection
- Fast Data transfer
- Multimedia support

The 3G consortia are committed to developing the technology around the W-CDMA and EDGE broadband air interfaces, which will determine how a signal is sent from the hand-held device to the base efficiently.

The International Telecommunication Union (ITU) is working with 3G operators to harmonize the different proposed standards. The ITU has decided on a single flexible standard with a choice of multiple access methods (CDMA, TDMA and a hybrid TDMA/CDMA). CDMA is perceived to be the predominant protocol.

CDMA2000 network synchronous, with two ways of downlink, the direct sequence (DS), which is a single carrier is activated with spreading bandwidth of 4.75 Mhz. This method will give you a better multi-path migration than the second option of CDMA2000, which is the Multi-carrier (MC). Either option chosen by the operator should be leveraged on existing digital network infrastructures.

3G systems will support several different bit rates. A 2-Mbps rate is suitable for stationary environments like an office building. A 384-Mbps rate can support a slow moving environment like walking. A bit rate of 144 Kbps supports a fast moving environment like driving.

Table 3 - Timeline of 3G Rollout Schedule

Since CDMA is already packet-based, it is an easier technology to upgrade to high-speed data

	CDMA	2000 IS95B	2001 1XRT	2002 HDR/	2003+ CDMA
Definition	• Code Division	• Interim Standard	• 1 X Radio Transmissio	• High Data Rate/3 X	• Phase 2 CDMA2000
Speed	• 9.6-14.4Kbps	• 64Kbps	• 144-614Kbps	• 2.4 Mbps	• 2-2.4 Mbps
Technology	• Code division	• Base station	• Base station	• Base station	• Software upgrade to
Frequency	• 800MHz, 1900MHz	• 1.25MHz spectrum	• 1.25MHZ spectrum	• 1.25MHZ spectrum	• 3X1.25MHz channels or
Other	• Better security through "spread	• ISDN compatible • Initial speeds of	• Doubles voice capacity • Initial	• HDR supports data transmissio	• Flexible IP structure • Support for simultaneou

□ Supports Circuit Switching Only Supports Packet Switching

Source: Qualcomm; CDMA Development Group; Mobile Office; Mainspring

3G is on a mission

Cellular phones allow users to talk on the move. The Internet proved to be successful in moving data, the combination of these two with high speed connection is known as the 3G (third generation). We are becoming more dependent on mobile devices by the day. Being mobile is no longer a luxury but is now a necessity.

The goal of the 3G consortia is to establish objectives for future global mobile telecommunications systems. These objectives include: operate under one common ground, develop handsets capable of universal communication coverage, provide seamless roaming between multiple networks, establish an open network architecture that can provide high-speed mobile access to internet-based services, and provide multimedia support.

The new hand-held devices must support video streaming, be capable of receiving large file downloads, and provide Internet access, in addition to the traditional voice communication. 3G will dramatically change the way people communicate, work and carry out their daily lives.

3G will define a new direction for mobile services that are already an integral part of modern business and personal life. Studies suggest that consumers are currently dedicating 18% of the communication spending to mobile services. This spending will increase to 24% by 2006 and 50% by 2015.

Once 3G is rolled out, we will be able to watch TV, conduct video conferencing, perform bank transactions, check on orders or inventory, and conduct business globally via our wireless hand-held device. This is ideal for the mobile worker and our personal daily tasks. 3G will empower B2B, B2C, B2G, B2E, and P2P communications; it will mean many things to many people.

Political challenge not technical

It's not about better technology, it's about the self-interest of each operator who is jockeying to be the preference of choice. The United States government lacks authority in enforcing the standards that are a major factor in implementing 3G in that country. Therefore, 3G's implementation has been delayed.

The GSM network has become a standard in Europe, and operators who adapted the GSM technology are trying to make it difficult for competitors with CDMAOne to switch to wideband for the next generation. The case is even stronger in the United States where the free market will provide more room for operators to pursue their own business plans. The government, Europe or US should play a stronger role in helping all operators to agree to one standard.

It's all up to the regulators (governments), and operators to work together to deliver the product to the consumer. 3G promises healthy business all cross the global networks. 3G revenue comes from monthly access sign up fees, and from

value added transactions. The ownership of the consumers is valuable to the operators. Demographics and surveys can be an additional revenue stream for the operator. Carriers owning a spectrum with projected consumer sign up will give them ideas on creating profitable paybacks.

The parties, financial investors, operators, and the wireless entities involved, must reach an agreement that will satisfy the regulators in building 3G infrastructure. Third Generation Mobile Telecommunications is scheduled for roll out in Japan and Europe in 2001-2002; so far Japan and Europe are running on time. The United States, on the other hand, is running behind schedule due to FCC spectrum licensing.

3G will be a major player in the market place. Investors and operators must work toward a common goal with the regulators. It's believed there will be over 600 million users in the year 2005 averaging \$23 billion spent every year on

Percentage of adults interested in new mobile services

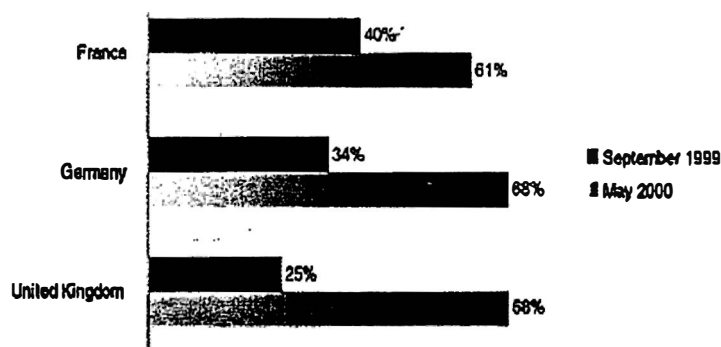


Figure 4 - Interest in New Mobile Devices

3G infrastructure. In the mean time hand-held purchases will increase to \$14 billion in 2001 and \$27 billion in 2006, according to ABI's Cellular IC report.

Building up from today's digital infrastructure network

Most of the foundation is in place already. By using the existing digital technology, the network can be expanded in the areas of bandwidth, the speed of data transfer, and multimedia support.

The main components of 3G is the core network, ATM based architecture, and packet switching. 2G a circuit switched digital architecture. By adding the R'00 component the current system will be able to support multimedia architecture.

Another advantage that can be built up on for 3G is the Terrestrial Radio Access Network (UTRAN).

This is the equivalent to the GSM BTS and Radio Network Controller (RNC). UTRAN uses a new modulation scheme, called Frequency Division Duplex (FDD), and W-CDMA.

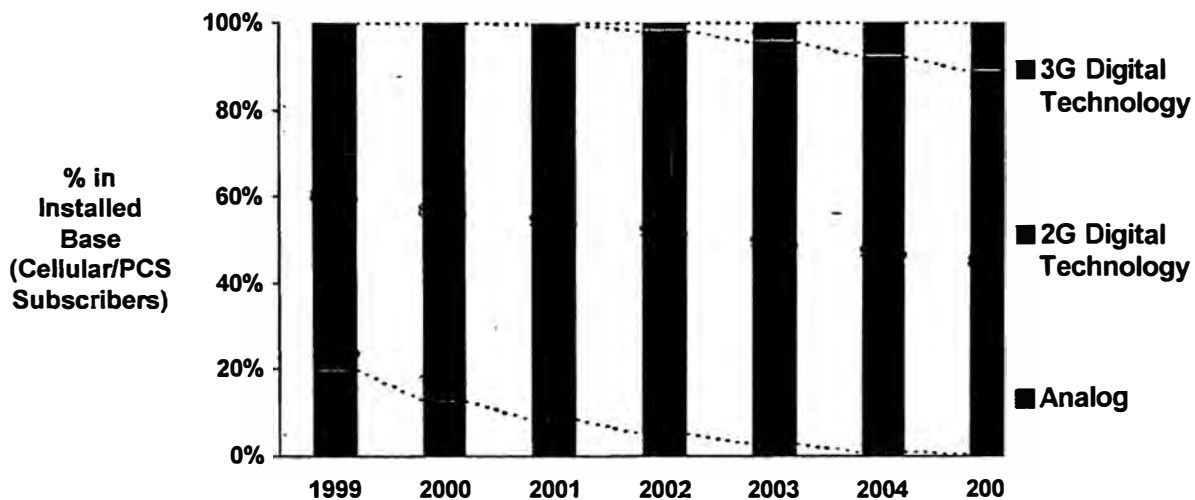
UTRAN mode is considered to be the most efficient within a single system regardless of the condition: wide area, urban, indoor or outdoor. It operates at 5 MHz and requires only one carrier

It's clear that 3G systems will step up the development of mobile applications and services. Mobile devices will become our virtual office, as well as our communication personal tool, much more than just a hand phone or a basic electronic organizer.

3G wireless running under a bandwidth up to 384 Kbps is scheduled to roll out next year, and will become common within the next 24 months. Conforming to the 3G standards will bring different carriers together to achieve a high-speed transfer rate globally.

Table 4 - Migration Schedule to Digital Wireless Technology

2G networks are expected begin to slowly give way to 2.5G and 3G in 2001 Migration to Digital Wireless Technology, 1999-2005



3G is not home alone

3G comes with heavy political overhead, and possible future threats from free spectrum networks, i.e. short-range wireless networks, Bluetooth and 802.11b. The short-range network is attractive to the consumer, because it can provide a 3G level of bandwidth, will not require licensing, no cost for the access time, these are one time device costs.

3G operators are hoping the adoption rate of 3G, and hosting advanced customized services, will outweigh the risk of the unlicensed short-range technologies. 3G operators and investors must keep their eye on the short-range technology, since it will be taking away market share. The question is how much?

Current forecasters think the consumers will find it cheaper to use Bluetooth or 802.11b instead of 3G, which will translate to about \$8 billion from 3G or 20% of the 3G market share by the year 2010. Bluetooth will play a major role in device short-range connectivity and communication in the medical industry, manufacturing industry, warehousing, distribution, corporate, and office.

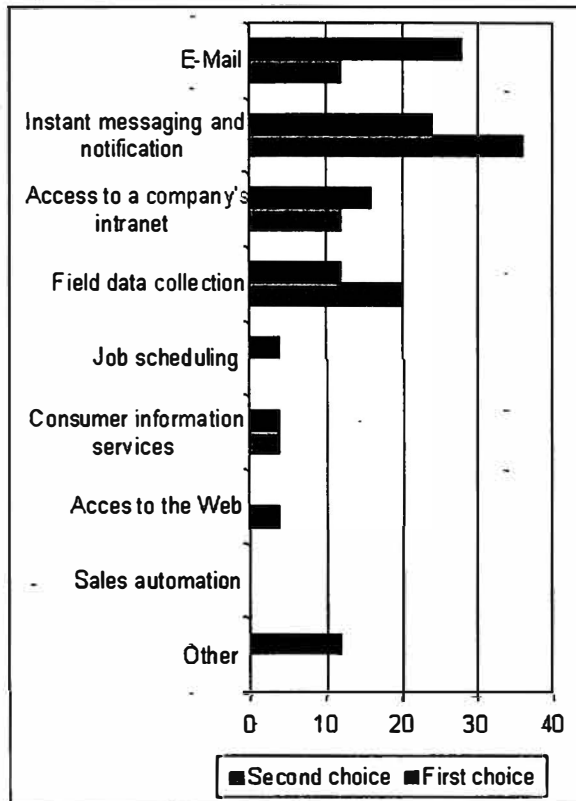


Figure 5 - Consumer Wireless Needs

According to Gartner Group, "By 2007, more than 60 percent of the European Union and U.S. population aged 15 to 50 will carry or wear a wireless computing and communications device at least six hours a day, and by 2010, more than 75 percent will do so."

Gartner Research believes that by 2007 over 30% of personal wireless computing devices will operate some form of personal peer-to-peer client application. Vendors and operators will be unable to exert any effective control over the distribution of information.

P2P architectures will present a new dimension of social challenges and computational gaps.

The short range network investors are marketing Bluetooth and 802.11b as the future of 3G, VoIP (Voice over IP), WLAN network with out the re-occurring monthly subscription cost to the consumer, ideal P2P (Peer-to-Peer) networking.

The short-range technology is simple to implement: Bluetooth requires a PC card for about \$250 per user to deliver speeds up to 11 Mbps of free bandwidth over a free spectrum at a range of up to 10 meters. 802.11b supports cell handover. Although Bluetooth and 802.11b are both peer-to-peer networks, they can extend their reach to WLAN access. Each activated device can act as a repeater to extend the transmission range, which can be viewed as a threat to 3G networks. In other words, users can move from WLAN applications to deliver wide area services. P2P (Peer-to-Peer) communication will become a reality, and when coupled with emerging technologies like Bluetooth, will enable innovative applications to emerge.

A recent report from Nomura Equity Research says, "Operators fear they will lose customers. Equipment makers fret that mobile handsets might be supplemented by personal digital assistants [PDAs]. The market for expensive network equipment might shrink as operators share infrastructure or use cheaper Internet-based technology like 802.11b to build urban wireless networks."

At this point no one knows what the outcome will be. It is believed that getting to the market sooner will secure more of the market share, with an early adoption rate making it harder to change for the consumer. So operators and vendors are betting on offering technology that can be easily adapted to any new standard. For instance, Telenor and Ericsson have joined forces with Birdstep, a software provider, to develop a platform working under new technologies as well as older ones, including Bluetooth, 3G, GSM, and GPRS.

Seamless IP: Is it meant to be?

Seamless IP is when 3G WLAN and short-range network technologies are enabled on the same handheld device.

The idea picked up steam when 802.11 was introduced and the big players got involved like IBM, 3Com, and Cisco. It's a question of economics now—how can the manufacturers capture the new revenue stream.

As indicated earlier, forecasters believe the Bluetooth and 802.11b pose a real threat to 3G's economics, so the idea of a seamless IP (3G and short range networking) looks appealing and may be the way to present the new services. But the reality of this option indicates that the technical challenge of implementing a seamless IP is underestimated by the operator as well as the consumers. The technical challenges are not with the communication protocol, but it's with the architectural management layer and the security issues between 3G and short range technologies; in addition to digital

voice, and multimedia capability all in one small terminal device, will require more power consumption and speed of connection. But once it is achieved the sooner these devices will arrive to the market.

Most likely Bluetooth will be a complement to 3G and will add revenue rather than take traffic away from 3G. It may never be a direct replacement for 3G mobile. Consumers don't care about which of the technologies are used, as long as they get fast reliable access service at a low cost, which makes the seamless IP theory an attractive option for the consumer.

Table 5 - Wireless Technology Performance and License Requirements

Technology	Max. Access Speed	Coverage/Range	Licensed	Timing
3G	2Mbps	National	YES	2002+
Bluetooth 2.0	2Mbps	100 meter	No	2002+
802.11b	11Mbps	2-8K meter	No	2002+
HiperLAN1	24Mbps	100 meter	Yes	2001
HiperLAN2	54Mbps	100 meter	Yes	2002

Source: PlanetWireless

The timing of the rollout of these technologies will be a key factor to the success and the adoption rate of the particular technology. Regulatory and business issues are making 3G implementation difficult and time is even more critical for 3G. If delayed, Bluetooth and 802.11b could capture more market share, resulting in 3G operators and investors losing substantial projected revenue.

Many of the wireless manufacturers are working fearlessly toward a seamless IP mobility, with hand-held devices that will automatically sense the best and most cost effective method to activate the best network. Many PDA and phone manufacturers are planning to have Bluetooth enabled devices in the near future.

UMTS and HiperLAN2 network operates at 5GHz and can deliver up to 54 Mbps to subscribers with high bandwidth. The objective is to be able to transfer data service seamlessly between short-range spectrum free networks and 3G WLAN networks. For instance, a project launched by Telenor and Ericsson, integrates B2E. Corporate users can capitalize on this technology and be profitable using e-mail and instant messaging throughout the corporate campus, warehouses, and manufacturing. PP2P (Personal Peer-to-Peer) will also be ideal for teenagers' communication, like games, video, music, which will effect the music and movie industry greatly.

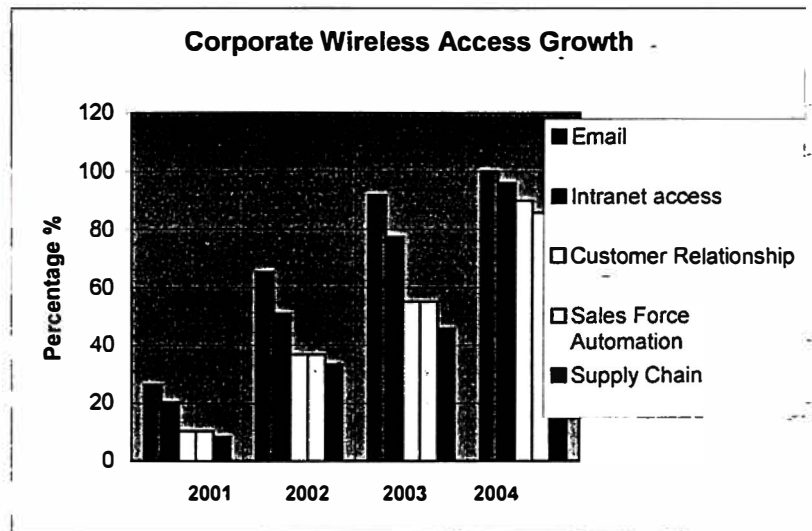


Figure 6 - Wireless Access Growth

3G investors and operators are still trying to figure out how to approach the short-range network dilemma, especially, when the short-range network is gaining momentum rapidly. It is powerful enough to deliver fast data transfer supporting virtually what 3G can support to an increasing number of users. Meanwhile the 3G operators and investors are still trying to agree on how to deal with the short-range issue. Do you ignore them and hope that short-range networks will always be a small player in the market or embrace them and capture the short-range wireless revenue.

The only logical next step is for the vendors, investors and operators to work together to combine short-range networks and 3G technologies. This could happen in the next three years.

Bluetooth devices are scheduled to hit the market in volume records. Many vendors now are selling add-on Bluetooth enabling kits to attach to current devices. Nokia is predicting to sell 250 million phones that are Bluetooth capable by the year 2003. This will account for 20-25% of the global market.

Security

The short-range networks present one classical problem, as the information becomes more readily available and thus so is hacking. Security could be an issue, especially when these networks operate on a commonly used frequency of 2.4 GHz, which is used by cordless phones, garage door openers, and microwaves.

Consumers can easily install and activate PP2P networks, which will allow consumers to communicate with adjacent devices using a third component for WLAN to access the Internet. Bluetooth enabled devices can also act as repeaters, which will increase the distance to communicate. Information such as personal and corporate records, music, and movies will become easier to be pirated. There is no single point to intercept or prevent such activity. Therefore, it becomes nearly impossible to trace consumers' requests and devices.

Conclusion

3G will dramatically change our lives by enabling us to be much more effective and efficient in our daily business and personal activities. The Internet will literally be with us no matter where we are, with multimedia support, video conferencing, file transfer, e-mail, and voice calls utilizing the promised bandwidth. The winners of 3G will certainly be the consumers.

Bluetooth and 802.11b will impact the 3G revenue mostly in hotspots such as airports, hotels, school or college campuses, shopping malls, restaurants and sports events, however it will not be a replacement for 3G. The short-range networks could even play a complementary role in certain countries.

The developers of 3G and short-range networks (Bluetooth and 802.11b) must work towards a complementary solution for the global communication and not be profit driven rivals. The wireless industry is competitive in nature and companies will be building their own standards for unregulated bands, which will lead to incompatible networks and products. The end result will affect the consumers greatly.

Bluetooth will play a major role in home appliance products (so called smart homes), from voice activated command, virtual assistance to remote control units, kitchen appliances, washing machines, air-conditioning, etc. Both 3G and Bluetooth can provide additional services, such as grocery shopping via smart refrigerators or other devices

B2E (Business-to-Employee) communication will be more effective and efficient by using the new technology, like instant messaging, which should improve customer service. Field and mobile employees will be able to communicate in ways that were not possible before and data availability will be a major contributor to fast and more accurate service.

Regulators such as governments must enforce the agreed-upon global standards of 3G. The operators and vendors must support and fund the global 3G project.

Consumer use will be the most significant factor to 3G's success. Unknown to us is which type of 3G services will be most desired by the consumer. i.e.; enhanced voice, larger email, videoconferencing, downloadable videos? We do know that whichever service the consumer chooses, it will have to be fast, reliable, and affordable.

Critical factors to 3G's lifeline:

- 1- Adoption rate of the consumers: This is one of the most important factors that will directly influence the success or the failure of 3G. Consumers will embrace 3G when the operators are offering not only a new value added service, but the service is reliable, delivers superior voice quality, global communication, always connected, with fast data transfer, and supports multimedia for video conferencing, and movies of demand. The sooner the consumers buy into these services the sooner 3G will become real.
- 2- 3G offerings must be flexible and easy to use.
- 3- Method of implementation of 3G will be critical. Business partners and operators must build effective and distinctive features rather than smarter technology. In addition to these features, the providers must target the consumers and utilize the best marketing channels to reach them.
- 4- Operators and investors must build the right business model the first time. Massive budgets are committed to 3G implementation. The challenge is to gain the revenue stream quickly by capturing the market share as early as possible to pay for the capital investments.
- 5- Governments must be unproblematic and help 3G operators by reducing the cost of 3G spectrum licensing.
- 6- Operators and investors must leverage and build up current digital technology, to reduce expense and to speed up roll out.
- 7- Handset manufacturers need to manufacture the product without proprietary standards, and to be independent regardless of the network used, or the geographical location.
- 8- Operators should place heavy emphasis on leveraging the early experiences of users and their needs.
- 9- It is yet not clear which business application the consumer will be interested in, however that must not delay the implementation of 3G.

- 10- Business partners need to provide the business model along with the right technology, to manage consumers, and suppliers, reliably, effectively, and affordably.
 - 11- Operators and manufacturers must keep a close eye on identifying any regulatory requirements as quickly as possible, especially if it leads to technical changes.
 - 12- Must focus on a specific market segment with priority of services offered.
 - 13- Operators need to build their own mobile portals for a new revenue stream, which should help consumers stay with the same provider.
 - 14- Providers should learn how to bill consumers for the new service, or the type of connection, in addition to volume and monthly subscriptions.
 - 15- Develop a flexible architecture, which is able to support new services quickly and reliably.
 - 16- Manufacturers must be ready to integrate with the short-range networks.
- 3G will happen, however, it may not be as fast as we wish it to happen.

Appendix

References

- **Generation Global Mobile Summit Japan**
- **Cerillion Technologies - Progress through evolution**
- **Lessons in Mobility From Asia/Pacific**
- **Lessons learned from Europe/JapanLucent technologies**
- **Gartner Dataquest Analysis**
- **Wireless Today/PBI Media**
- **NEC 3G Mobile Solution, Partners-What is the next step.**
- **Spectrum Strategy Consultant**
- **Universal Mobile Telecommunications System**
- **Mobile Wireless Internet Forum www.mwif.org**
- **Newsweek- What is 3G**
- **SK Telecom**
- **Caron Carlson, Wireless Week**
- **COM-13-6000 on www.gartner.com**
- **Sierra Wireless**
- **GSM forum**
- **Wireless Application Protocol Forum (WAP Forum)**
- **Cellmania.net - provides a community and news for wireless developers.**
- **Cellular News**
- **Unstrung.com**
- **Wireless Networks Online**
- **WirelessDevNet.com**
- **Wireless NOW**

Glossary

UMTS	Universal Mobile Telecommunications System
3G	Third-Generation
UTRAN	UMTS Terrestrial Radio Access Network
RNC	Radio Network Controller
Iu-PS	Packet Switched interface instead of Gb on the packet domain.
Iu-CS	Circuit Switched interface
EDGE	Enhanced Data rates for GSM Evolution
GPRS	General Packet Radio Service
FDD	Frequency Division Duplex
UTRA	Universal Terrestrial Radio Access
TDD	Time Division Duplex
3GPP	Third Generation Partnership Project
RTT	Radio Transmission Technologies
ITU	International Telecommunications Union
W-CDMA	Wide-band Code Division Multiple Access
GSM	Global System for Mobile
PDA	Personal Digital Assistants
WAP	Wireless Application Protocol
WIDs	Wireless Interactive Devices
TDMA	Time Division Multiple Access
CDMA	Code Division Multiple Access
SMS	Short Messaging Service
ITU	International Telecommunications Union
PDC	Personal digital cellular
AMPS	Advanced Mobile Phone Service
DS	Direct Sequence
MC	Multi-carrier
P2P	Person to Person
B2B	Business to Business
B2E	Business to Employee
B2G	Business to Government