PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

MIGRACIÓN DE UNA RED DE CAJEROS AUTOMÁTICOS A TCP/IP

Tesis para optar el título de Ingeniero Electrónico

Presentado por:
CHRISTIAN EDDY VÁSQUEZ MONTES

Lima - PERÚ

2006

RESUMEN

Se plantea un problema de cambio de infraestructura y rediseño de red de comunicaciones en una empresa dedicada al servicio de transferencia electrónica de fondos interbancarios a través de una red de cajeros automáticos y al procesamiento y administración de tarjetas de débito y crédito.

Tanto en el frente de los cajeros automáticos o terminales transaccionales, como en el frente de los computadores que autorizan las transacciones, se han ido experimentando y exigiendo cambios, los cuales no solo han involucrado nuevas tecnologías y aplicaciones, sino también la apertura a protocolos de comunicación como el TCP/IP con nuevos servicios y posibilidades, en un servicio financiero, que por mantener altos niveles de seguridad, mantenía protocolos de comunicación "heredados" como el X.25 y el SNA.

En el presente documento se revisa la situación inicial de la red, los servicios y las necesidades del negocio, y la evolución de las redes de cajeros. Con el fin de conseguir los objetivos, se plantean propuestas de solución para dar soporte a las aplicaciones con protocolos "heredados" en una red IP, se revisan las alternativas técnico-económicas de enlaces de comunicación, las propuestas para la renovación de la infraestructura de comunicaciones y seguridad, y finalmente una serie de recomendaciones para la implantación y la migración a la red IP.

Con un adecuado planeamiento e implantación de políticas de seguridad adecuadas, en una red privada, publica o compartida con otra institución, es posible conseguir una red de cajeros automáticos TCP/IP eficiente, segura, con alta disponibilidad, y capaz de brindar mayores servicios.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

INDICE DE CUADROS

INTRODUCCIÓN

El presente documento trata de explicar cómo se ha enfrentado en los últimos años un plan de renovación de red en una empresa de servicios bancarios de transferencia electrónica de fondos (EFT – Electronic Funds Transfer), a la cual para referencia llamaremos SERBAN. Teniendo como socios a bancos e instituciones financieras, ha sido la encargada de ofrecerles entre otros, servicios tecnológicos como el de administración de una red de cajeros automáticos, y servicios de procesamiento de tarjetas de crédito y débito. SERBAN tiene como visión ser líder en el procesamiento y administración de medios de pagos electrónicos, con un servicio que se pueda distinguir por su seguridad confidencialidad y eficiencia.

Para establecer la red de cajeros automáticos (también conocidos por su acrónimo en ingles, ATM, Automatic Teller Machine) SERBAN crea una red privada, independiente a la de los bancos, pero con puntos terminales en muchas de sus agencias. En su creación adquieren lo último en equipos de comunicaciones, tales como PADs (ensamblador/desensamblador de paquetes) X.25, bastidores de módem analógicos, patches digitales, multiplexores de fibra óptica, entre otros. Adquiere cajeros automáticos NCR de segunda generación, Servidores NCR 34XX, equipos

criptográficos y equipos para grabación de tarjetas. Compran el software ESP-Link/FTS (Financial Transaction System) a la empresa canadiense SLM Soft, software desarrollado sobre la plataforma Unix (Open Soft), con herramientas de programación abiertas (Lenguaje C, Base de Datos Informix), con soporte a diferentes protocolos de comunicaciones: asíncrono, SNA/SDLC y X.25 utilizados en la conexión con los bancos y TCP/IP en las red interna. Utiliza estándares internacionales como: ISO8583 para el intercambio de mensajes entre bancos, DES para cifrar datos del mensaje, etc. Aplica un nuevo concepto: el Switch Financiero (al que denominaremos de aquí en adelante simplemente como SWITCH), o conmutador de transacciones desde cualquier tipo de terminal hacia cualquier ente autorizador.

Desde el punto de vista de negocio, la red maneja dos frentes de cambios tecnológicos, el de la red adquirente (formada por los cajeros automáticos, puntos de venta, etc. en la red propia y en otras redes, por donde se originan las transacciones de los clientes finales de las instituciones financieras) y el de la red emisora (formada por los enlaces y/o redes a las cuales se conectan los bancos e instituciones que autorizan las transacciones).

El proyecto tiene objetivo implantar la nueva infraestructura de comunicaciones sobre la base de la cuál se podía lograr:

- Renovación tecnológica y establecer nuevos esquemas de comunicación. El 60% de los equipos no deben tener más de 6 años de operación continua
- Reducción de costos. Los equipos y el software de soporte de protocolos heredados tienen altos costos de mantenimiento, y en algunos casos están discontinuados. Asimismo, se deben reducir los costos de los enlaces de comunicación tendiendo al uso de redes públicas o compartidas.

- Mayor flexibilidad, modularidad, escalabilidad e interoperabilidad. El equipamiento debe poder atender la mayor parte de las necesidades.
- Mantener altos niveles de seguridad, fiabilidad, y disponibilidad. La red debe mantener ratios mayores al 99.8 % de disponibilidad mensual.
- Reducir complejidad y establecer nuevos mecanismos de administración.
- Aumentar los servicios de comunicaciones ofrecidos (soporte seguro a clientes remotos, restablecimiento automático de enlaces averiados, transferencia de archivos, centro de procesamiento de datos alterno, etc.).

Este trabajo se presenta en tres capítulos. El primer capitulo plantea la situación inicial de la red, encontrándose una red netamente privada X25 y SNA.

En el segundo capitulo se reseña la evolución de los cajeros automáticos en las redes financieras de Perú, la evolución de las redes de comunicación de área extensa (WAN) de las entidades financieras, y una mirada a la seguridad en las redes.

En el tercer capítulo se revisan las alternativas técnicas y económicas para encontrar una solución al problema planteado de conectividad con cajeros y host usando el protocolo TCP/IP, orientando al esquema de una red IP con soporte a protocolos heredados. Seleccionadas las mejores propuestas técnicas y económicas, al final del capítulo, se resumen los costos generales del proyecto.

Finalmente se plantean recomendaciones para formar una nueva red, con capacidad de brindar nuevos servicios, y mantener la seguridad de la red.

CAPÍTULO I

1 SITUACIÓN INICIAL DE LA RED

Desde la concepción del negocio, la red de comunicaciones se segmentó en dos frentes: el de la red adquirente (formada por los cajeros automáticos) y el de las conexiones con instituciones: emisoras (formada por los enlaces a los bancos que autorizan las transacciones) y adquirentes (formada por los enlaces a las instituciones que forman otras redes de cajeros, POS, entre otros y reciben transacciones de los tarjeta-habientes de la Red).

La topología de la red formaba una gran estrella con los dos frentes descritos, ya que se consideró establecer líneas dedicadas desde el nodo de la empresa con cada una de las instituciones y con los cajeros automáticos en Lima, y los nodos en provincias. El nodo central de la aplicación SWITCH (conmutador transaccional) y de las comunicaciones eran un par de equipos Sun E3000. El equipo Sun contaba con software de comunicaciones Sun Solstice X.25 (para el manejo del protocolo X.25) y otro Sun Gateway SNA PU2.1 (para el manejo del protocolo SNA), con un arreglo externo de discos donde estaba montada la base de datos y la aplicación, las cuales podían ser desmontadas y montadas en un equipo Sun E3000 o en el otro idéntico, en los casos de contingencia.

1.1 La red de cajeros

Los cajeros automáticos únicamente trabajaban bajo el protocolo X25. Para el soporte de la red X.25 se tenía una red privada X25 en base a equipos PAD (Ensamblado/Desensamblado de Paquetes) marca Telematics modelo ACP-30, los cuales usaban puertos seriales sincrónicos para la conexión con enlaces dedicados por cada Cajero Automático en Lima y con los nodos de provincias. Los enlaces dedicados contratados, circuitos digitales de Digired del portador Telefónica del Perú, eran de baja velocidad, 9600 bps., ya que la aplicación transaccional utilizada no requería una mayor velocidad. Adicionalmente se contaba con un enlace dedicado, también por Digired, a la red pública de paquetes X25 de Telefónica Meganet. Desde esta red se podía lograr enlaces a ciertos cajeros en las ciudades de provincias con poca concentración de terminales. Se tenía entonces 10 nodos de comunicaciones en la sede central y 6 nodos de distribución en provincias, lo cual permitía conectar hasta 180 cajeros.

1.2 La red de instituciones

Cada una de las instituciones se comunicaba a través de una línea dedicada utilizando enlaces TDM de la red Digired de Telefónica, contratados a una velocidad de 9600bps. A nivel protocolo de comunicación, la mayoría usaban SNA y otras X.25. A nivel aplicación, el protocolo de intercambio de mensajes usado era el ISO8583, muy usado entre las entidades financieras.

1.2.1 Comunicación con host SNA de instituciones

Para la comunicación con los bancos, la red se soportaba en un ruteador marca Cisco modelo 2522, de mediana capacidad, sin funcionalidades de respaldo de enlace ni

contingencia de equipo. El ruteador conectado directamente a la red local ethernet recibía las tramas LLC2 del computador SWITCH convirtiendo estas tramas a SDLC en sus puertos seriales, conectados por líneas dedicadas a los computadores de los bancos. En el computador SWITCH se utilizaba software de emulación de terminal 3270 para que la aplicación pudiera utilizar SNA PU21.

1.2.2 Comunicación con host X.25 de instituciones

Para la comunicación con los bancos con soporte X.25, se utilizaban los mismos PADs usados para la comunicación X.25 con los cajeros automáticos, a los cuales se conectaban líneas dedicadas para el enlace con cada computador de banco.

A diferencia de la comunicación con los cajeros, en este caso, la única diferencia es el tamaño de los paquetes utilizados, configurados en el software de X.25 de computador SUN a 256 bytes (el tamaño de paquete utilizado para los cajeros es de 128 bytes).

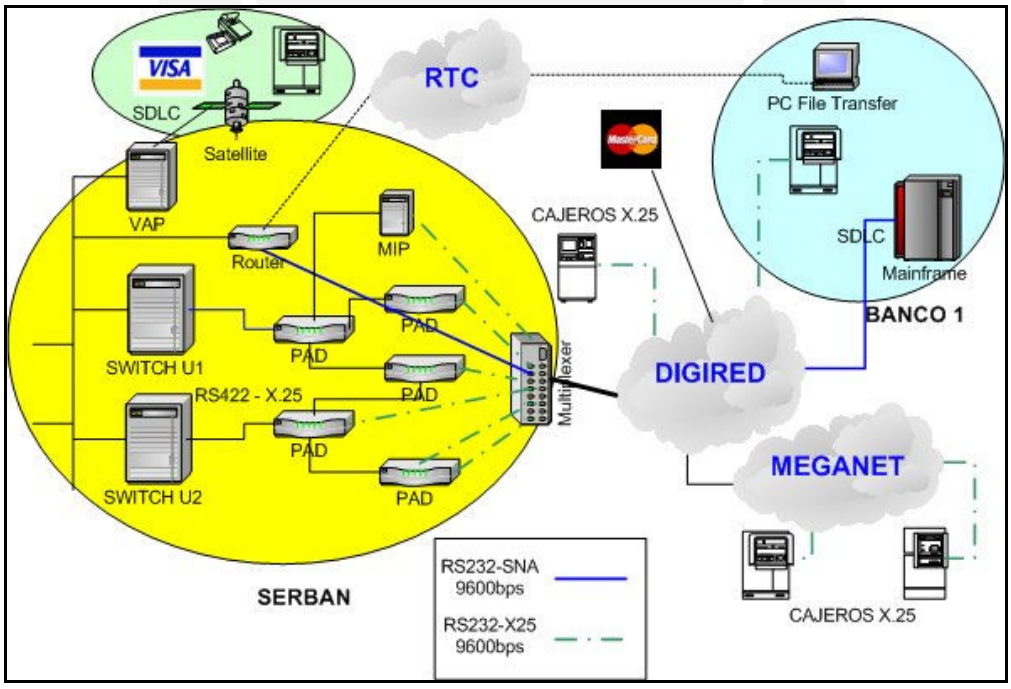

Fig.1.1 Esquema de comunicación inicial.

1.2.3 Comunicación con equipos de transferencia de archivos

Al fin de cada día se debía efectuar una serie de conciliaciones de las transacciones financieras y otros trabajos en lotes (creación, asociación, y generación de tarjetas, cuentas, etc.) para lo cual se utilizaban archivos de gran tamaño que enviaban y recibían las instituciones mediante un sistema de transferencia de archivos.

Para la transferencia desde los equipos remotos de las instituciones se usaban esquemas de conexión a redes remotas vía MODEM. Un ruteador con puertos asincrónicos PPP, y conexiones de MODEM analógico establecía los enlaces telefónicos conmutados y mantenía conexión TCP a un servidor de transferencia de archivos administrado por una aplicación con control de los archivos transmitidos y recibidos por institución. Esta aplicación, asimismo, contaba con mecanismos de compresión y encripción de los archivos con llaves diferentes por institución. Si bien se tenía conexiones seguras, la conexión conmutada resultaba muy lenta e inestable para los lotes de archivos a transmitir.

1.2.4 Comunicación con instituciones asociadas

Además de las instituciones miembros, se contaba con comunicación en línea con las redes de las marcas Visa y Mastercard. Cada una de estas redes impone su propio esquema de comunicación y sus políticas de seguridad. Cada una de ellas instala un computador de acceso a sus redes en SERBAN:

- VISA Intl. usa una conexión VSAT (una antena satelital de baja velocidad) bajo el protocolo SDLC desde su computador VAP (VISA Access Point), e internamente se comunica con los computadores de SERBAN por TCP/IP.

- Mastercard Intl. usa un circuito dedicado internacional a 64K usando TCP/IP desde su computador MIP (Mastercard Interface Processor), e internamente se comunica con los computadores de SERBAN con enlaces X25 y BSC.

Para la comunicación con Visanet Perú, operador adquirente de Puntos de Venta (POS), se utiliza una conexión a la red Interlan (red pública Frame Relay de Telefónica).

De lo expuesto se observa una problemática en cuanto a la infraestructura de red, compleja y costosa por el alto número de enlaces TDM punto a punto requeridos, y por la duplicidad de enlaces en las conexiones a los bancos, en donde se atiende cada servicio o tipo de datos por un circuito separado y de baja velocidad.

Adicionalmente se debía considerar que internamente el computador SWITCH, se comunicaba con los demás servidores de los procesos de producción usando la red local ethernet y el protocolo TCP/IP. En la misma red se podía ubicar a los computadores personales de la empresa, y algunos servidores de oficina, entre los cuales estaba un servidor de correo electrónico. Para la salida a Internet se utilizaba un firewall Check Point con licencia para 50 usuarios, ya que solo tenían autorización para comunicación con Internet el servidor de correo y no más de 10 usuarios.

No se contaba con posibilidad de conexiones de acceso remoto para soporte o para usuarios de otras instituciones.

CAPÍTULO II

2 DEFINICIONES Y CONCEPTOS GENERALES - LA EVOLUCIÓN DE LAS REDES DE CAJEROS

En el presente capítulo se explicarán algunas de las tecnologías que se explicarán en los capítulos siguientes, algunas de ellas de poca difusión.

2.1 La evolución de los Cajeros Automáticos.

A principios de la década de los 80´s aparecen los cajeros automáticos o ATMs en el Perú, siendo los primeros fabricantes en ofrecer sus equipos NCR, Interbold (representados por IBM), y Unisys. Ésta, la segunda generación de cajeros automáticos, fueron equipos controlados por procesadores tipo Intel 8086, NEC V2x, etc., usando sistemas operativos propietarios de aplicación específica.

Los dispositivos usados, eran una muestra de la tecnología de aquellos años: impresoras de recibos y de auditoría matriciales, dispensadores de dinero 60% mecánicos, con muy pocos sensores, monitores de vídeo monocromáticos. Los protocolos de comunicación que usaban (X.25, SNA LU2.0, Async) estaban limitados al uso de interfaces seriales RS232 de baja velocidad (hasta 19.2 Kbps.), ya que la aplicación en si era transaccional, es decir, se limitaba a enviar mensajes cortos del ATM al HOST y del HOST al ATM.

Cada fabricante desarrolló un protocolo de mensajería para su aplicación transaccional, los cuales deberían considerar los mensajes para enviar transacciones de retiro, consulta, etc. desde el cajero, ejecutar acciones sobre los dispositivos (impresora, pantalla, dispensador, lectora de tarjetas, etc.) e interpretar los mensajes de estados de los mismos, así como ejecutar remotamente comandos de administración y mantenimiento, como poner en servicio al cajero, recuperar los contadores de billetes del cajero, ejecutar un intercambio de llaves de terminal, cargar parámetros, cargar pantallas, etc.

Entre los lenguajes de mensajes transaccionales de cajero más conocidos está el NDC (NCR Direct Connect) desarrollado por NCR, y el 911/912 desarrollado por Diebold/Interbold.

En el siguiente cuadro se muestra un ejemplo de mensaje NDC, para una transacción de consulta de cuenta, entre un cajero NCR y el Computador SWITCH de SERBAN.

REQUERIMIENTO DE CAJERO

```
11{1c}006{1c}{1c}{1c}11{1c};4111020100000024=07111201846571900?{1c}{1c
} A    AA{1c}000000000000{1c}>4>893?16:;745<1{1c}{1c}
```

RESPUESTA DEL AUTORIZADOR

```
4{1c}{1c}{1c}{1c}00000000{1c}01044022{1c}20115-07-05
19:16{0e}7008104{0a}4924910200015548{0a}S/. 0.00 :BAL
{0a}{0e}?{0e}>{0a}{0a}------{0a}

4{1c}006{1c}{1c}111{1c}00000000{1c}03345{1c}302{1b}(>     RED
SERBAN{0a}{0a}{1b}(2{0e}9 CAJERO DE
PRUEBA{0a}**********************************{1b}(2{0a}{1b}(2{0e}
3DIA{0e}5HORA{0e}7SECUENCIA{0a}{1b}(2 15-07-05
21:01{0e}6006334{0a}{0a}{1b}(2TARJETA
:{0e}1**************0024{0a}{1b}(2TRANSACCION :{0e}1CONSULTA
{0a}{0a}{1b}(2CUENTA      : CUENTA CORRIENTE{0a}
0400016003 {0a}              BANK{0a}{0a}SALDO TOTAL :
S/.1,234,567,890.12{0a}SALDO DISP. :  S/.
9,876,543,210.98{0a}{0a}{1b}(>{0e}8GRACIAS{0a}{0c}{1d}115-07-05
21:01{0e}7006334{0a}4111020100000024{0a}BAL: S/. 0.00{0a}8102
0400016003{0e}2{0a}{0a}------{0a}
```

CONFORMIDAD DEL CAJERO

```
22{1c}006{1c}{1c}9
```

Fig. 2.1. Mensaje NDC entre cajero y SWITCH.

En el se pueden observar tres bloques claramente definidos. El primero es el requerimiento del cliente, en donde también se encuentran sus credenciales (numero de tarjeta, datos de la banda magnética, el PIN o clave secreta, el tipo de transacción y el monto requerido).En el segundo esta la respuesta del computador, en donde están los comandos de orden de dispensado para el ATM, junto con dos bloques de mensajes a imprimir en la impresora de auditoria, y en la impresora de recibos para el cliente. El tercer bloque es la confirmación del cajero que indica que la orden de dispensado fue ejecutada sin problemas.

La información contenida no sobrepasa los 20 Kbytes, para lo cual bajo un enlace de comunicación de 9.6kbps, se puede resolver una transacción en menos de 3 segundos.

La tercera generación de cajeros apareció antes de finalizar la década del 90. De la mano con los avances tecnológicos en las computadoras personales, se inició el uso de procesadores Intel Pentium II, así como el uso de sistemas operativos comerciales, como OS/2 y DOS. Empezaron a usar dispositivos más complejos, con mayor número de sensores para el control de las operaciones. En los dispositivos podemos resaltar impresoras térmicas, monitores VGA a color, y dispensadores con sensores ópticos para el control del paso de billetes por cada etapa del transporte (controlaban la opacidad – o nivel de luz que puede pasar a través del billete, el espesor y la longitud). Los protocolos de comunicación no tuvieron mayores cambios. En aquellos años en el Perú se comercializaban cajeros marca NCR, Olivetti e Interbold. La marca Olivetti fue agresiva en su comercialización, ya que ofrecía buenos precios, y software de cajeros con emulación NDC (para reemplazo de cajeros NCR) y 911/912 (para reemplazo de los cajeros Interbold).

En la cuarta generación de cajeros (desde el 2000 a la fecha) los cambios han ido implantándose sobre los dispositivos, buscando mejorar la seguridad. Se introdujo el Windows como sistema operativo, y el TCP/IP protocolo de comunicación por defecto.

Las lectoras de tarjetas fueron mejoradas en el transporte con el fin de evitar que se inserten dispositivos extraños, los dispensadores de dinero mejoraron su capacidad para identificar el dinero, con mejores metodologías y sensores, y corrigieron alguna vulnerabilidad, y a nivel de seguridad del PIN, se introdujo el cifrador con soporte a Triple DES en el teclado de usuario.

En la actualidad, la mayoría de marcas de cajero usan la versión Microsoft Windows XP de sistema operativo, con ciertas adaptaciones de cada fabricante de cajeros. Estos vienen por defecto con comunicación TCP/IP y alternativamente con protocolo X.25. Las instalaciones prescinden de la configuración de red Microsoft (el cajero queda como un dispositivo aislado del dominio de la empresa, ya que valida su propio inicio de sesión), solo tiene instalados los programas necesarios para la operación de la aplicación del cajero, y solo tiene abiertos los puertos de servicio TCP que se configuren para la aplicación.

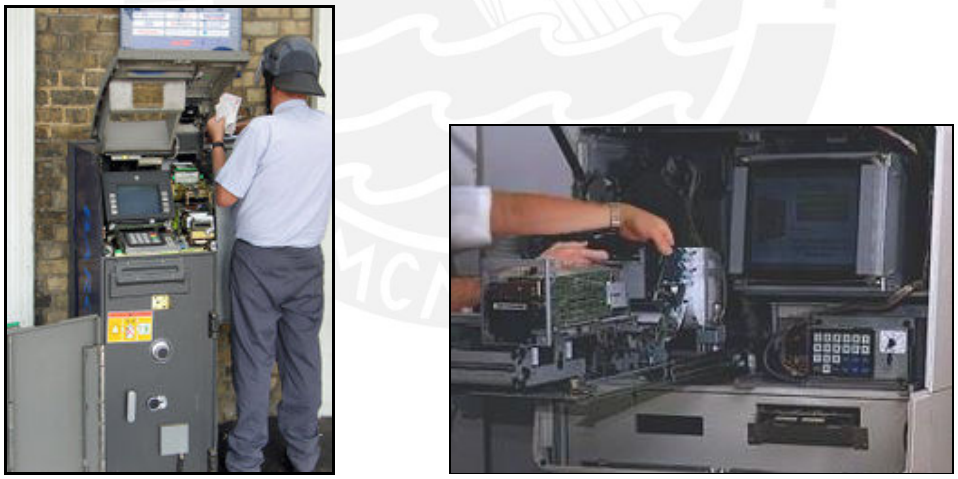

Fig. 2.2. Interior de cajeros NCR durante el servicio de reabastecimiento.

El incremento del uso de cajeros automáticos en el mundo ha hecho que los costos de los cajeros automáticos se reduzcan a menos de la mitad. Los primeros cajeros tenían un costo muy elevado, alrededor de US$ 40,000.00, mientras hoy en día los costos de

un cajero no superan los $17,000.00. Las marcas de cajeros que se comercializan en el Perú son NCR, Diebold y Wincor-Nixdorf (representado por IBM).

Las marcas de tarjetas Mastercard Intl. y VISA, como parte de sus políticas de seguridad de PIN en la región Latinoamérica, establecieron fecha limite para que los cajeros de las redes adquirentes soporten Triple DES. Este nuevo requerimiento de seguridad exigía que se hiciera un cambio radical en el cajero (significaba el cambio de todo el CPU del cajero y algunos dispositivos) o que se adquiriera nuevos cajeros, obligando a la mayoría de redes adquirentes a renovar las redes de cajeros en los últimos años.

2.2 La evolución de las Redes de Área Extendida (WAN)

Antes de la década del '90, las redes de comunicaciones bancarias se cimentaban en líneas dedicadas establecidas por circuitos analógicos (enlaces establecidos por módems V32 conectados por un circuito telefónico de par de cobre tendido de extremo a extremo entre dos instituciones), y en algunos casos enlaces de fibra óptica con el uso intensivo de multiplexores TDM, STDM o PCM. Cuando las distancias eran cortas (menos de una milla) entre una institución y uno de los nodos del carrier (la empresa de servicios), entonces se podían establecer circuitos digitales, utilizando módem con modulación de banda base (p.e. los Newbridge de Nortel). Con éstos se establecían las redes por conmutación de circuitos y también las redes de conmutación de paquetes, cuando se configuraba redes "full mesh", y se usaban equipos PAD.

2.2.1 Las redes X.25

Los circuitos analógicos estaban limitados a bajas velocidades (máximo 64 Kbps.), ya que eran muy propensos al ruido, y a las fallas. Por lo tanto los protocolos y equipos de comunicación debían ser capaces de vencer tales limitaciones.

Por esa razón, protocolos de conmutación de paquetes como el X.25 tuvieron tanto éxito y difusión en redes bancarias, redes de compañías aéreas, etc. Por ello, en Perú se creó la red pública de paquetes X.25 Perunet (de Entel Perú, con tecnología Telenet de Alcatel) interconectada con Megapac (la red de CPT en Lima), que luego se conoció como Meganet (con la llegada de Telefónica del Perú, y nuevo equipamiento Nortel).

Podemos señalar algunas características del protocolo X.25:

- Es básicamente una recomendación CCITT de cómo se debe realizar una transacción por conmutación de paquetes. Cómo un terminal modo paquete debe tener acceso a una red de datos modo paquete.

```
Frame: 1194 Captured at:   16:31:51
Length: 29    From: User    Status: Ok
X.25: Packet Type=Call Request     <0B>
X.25: LGN=0  LCN=2                 <02>
X.25: GFI=1
X.25:  M8=1  M128=0
X.25:  D=0  Q/A=0
X.25: Address Byte: 0xCC           <CC>
X.25:   Calling DTE address length=12
X.25:   Called DTE address length=12
X.25: Called DTE Address=716125045015  <716125045015>
X.25: Calling DTE Address=716014000280  <716014000280>
X.25: Facilities Length=8          <08>
X.25: Facility: Throughput Negotiation
X.25:  Throughput Class For Data Transmission From Called DTE=9600   <AA>
X.25:  Throughput Class For Data Transmission From Calling DTE=9600   <AA>
X.25: Facility: Packet Size Negotiation
X.25:  Called Packet Size=128
X.25:  Calling Packet Size=128
X.25: Facility: Window Size Negotiation
X.25:  Called Window Size=7        <07>
X.25:  Calling Window Size=7       <07>
-----------
Frame: 1195 Captured at:   16:31:52
Length: 27    From: Network    Status: Ok
X.25: Packet Type=Call Connected    <0F>
X.25: LGN=0  LCN=2                 <02>
X.25: GFI=1
X.25:  M8=1  M128=0
X.25:  D=0  Q/A=0
X.25: Address Byte: 0xCC           <CC>
X.25:   Calling DTE address length=12
X.25:   Called DTE address length=12
X.25: Called DTE Address=716125045015  <716125045015>
X.25: Calling DTE Address=716014000280  <716014000280>
X.25:
X.25: Facilities Length=6          <06>
X.25: Facility: Window Size Negotiation
X.25:  Called Window Size=2        <02>
X.25:  Calling Window Size=2       <02>
X.25: Facility: Packet Size Negotiation
X.25:  Called Packet Size=128
X.25:  Calling Packet Size=128
```

Fig. 2.3. Establecimiento de llamada X.25 con negociación de facilidades.

- Opera hasta el nivel de red. Se soporta en la capa de enlace (nivel 2 del modelo OSI), con LAP-B (Link Access Procedure - Balanced, que es una subfamilia del protocolo HDLC).
- Desarrolla procedimientos y mecanismos para la detección y corrección de errores, además de negociación de facilidades como: cobro revertido, negociación de parámetros, establecimiento de enlaces rápidos, grupos de usuarios, registro de problemas. En la Fig. 2.3 se puede observar el establecimiento de una llamada X.25 con negociación de facilidades.
- La velocidad de conmutación de los nodos es relativamente lenta. El control obliga a esperar la confirmación de la recepción de los paquetes, bajo un control de número de secuencia.
- Se generan conexiones virtuales mediante paquetes de requerimiento de llamada (SVC), o mediante PVC, lo cual permite un "multiplexado" de canales lógicos.
- Las redes X.25 han sido concebidas en su origen para trabajar con DTEs a velocidades desde 2400 hasta 64 Kbps. A mayores velocidades se requeriría una capacidad de proceso en los nodos excesiva y poco práctica.

2.2.2 Las redes SNA

En su mayoría los bancos usaban computadores marca IBM, que era la compañía que más soluciones de banca les podía brindar, y como tal, el protocolo de comunicación por defecto era el SNA. Es una arquitectura de comunicación propietaria de IBM, jerárquica y centralizada, que resolvía las comunicaciones cliente-servidor y par-a-par, con enrutamiento estático en cada uno de los servidores. SNA se diseñó en los días

en que un gran número de terminales no programables se conectaban a los Hosts de IBM. La jerarquía de la red SNA estaba formada por los Hosts, FEPs (procesador de comunicaciones), Clusters (o controladores remotos de terminal), y terminales.

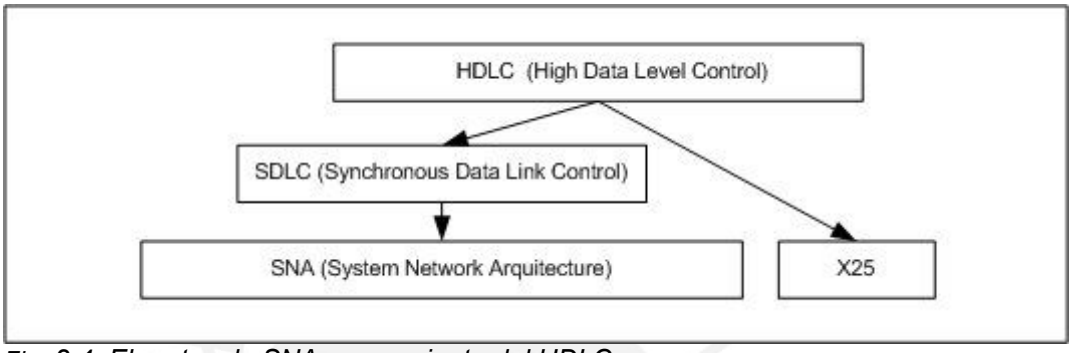

Fig. 2.4. El protocolo SNA, una variante del HDLC.

Al nivel de trama, el SNA se basa en el protocolo SDLC (Synchronous Data Link Control) el cual maneja la transferencia de información serial bit a bit, sincrónicamente *(ver fig. 2.4)*. Este protocolo a su vez, es una parte del protocolo HDLC (High Level Data Control) protocolo base para el X.25.

En cualquier enlace SDLC que conecta dos estaciones, una de ellas se designa como Primaria (Master, principal) la que controlará el enlace y la otra, como Secundaria (Slave, esclava). En un enlace puede designarse sólo una estación primaria pero puede tener múltiples estaciones secundarias en configuración multipunto o bucle. En el formato de la trama se identifica cuando la transmisión de la trama empieza y cuando termina (campos flag), se identifica a la estación secundaria (campo dirección: en X25=01 o 03, en SNA= C1,20, 25, si es “poll” = FF), qué acción ha de realizar el receptor con la información recibida (campo de control establece cuando la trama es de supervisión, no numerada o numerada para tramas de información), además de informar por la conformidad de tramas y mecanismos de recuperación de errores.

Las redes de las aplicaciones bancarias, llamadas de teleproceso, consistían en la conexión de terminales a un computador central, a través de redes LAN Token Ring y a través de controladores 3270, enlazados al computador central por circuitos conmutados y el protocolo SDLC/SNA. En resumen, se puede describir a las redes SNA como complejas y costosas de implantar, y solo utilizables para la transmisión de datos.

2.2.3 Las redes Frame Relay

A medida que las aplicaciones de oficina iban aumentando (las plataformas de back office como el correo electrónico, el uso de recursos de red compartidos, etc.), se hacia necesaria la interconexión de las redes LAN. Asimismo, los enlaces de comunicación habían iniciado la revolución digital, y se podía contar con mayores anchos de banda a menores costos. La calidad de los enlaces también aumentó enormemente: la tasa de error – BER – pasó de 10^{-5}-10^{-6} en los principios de los 80 a 10^{-12}-10^{-14} en la actualidad.

Entonces surgió el Frame Relay como alternativa a las redes de conmutación de paquetes X25, como transporte en enlaces con mayor ancho de banda, y para la interconexión de redes LAN que exigían mayor caudal de trafico, con comunicación tipo burst (rafagas) con velocidades altas pero espacios de tiempo libres. Se incorporaron nuevos equipos, los FRAD (esamblador / desensamblador Frame Relay), los ruteadores, entre otros, además de mantener la tecnología heredada como FEPs (Procesadores Frontales de SNA), los PADs (para SNA, X.25). En el Perú, la red publica de Frame Relay de Telefónica se llamó InterLan. La arquitectura del Frame Relay sólo comprende los dos primeros niveles del modelo OSI (físico y enlace), pero toma ventaja de la “inteligencia” de las capas superiores como el TCP en la capa de transporte (en donde se efectúan las labores de corrección de errores). Como realiza

un menor procesamiento, al llegar hasta la capa de enlace, con ello se eleva la performance de la transmisión de información. La conmutación es más simple y rápida que la convencional, además de ser transparente a los protocolos cursados.

Uno de los problemas de la definición en las redes publicas Frame Relay (como Interlan) era que la red privada debía ser centralizada, cada PVC debía establecerse con el nodo Central. Los enlaces entre puntos remotos sin pasar por el nodo central tenían costos extras.

A los pocos años, con el crecimiento de la Internet, el protocolo TCP/IP se difundió en las redes bancarias, iniciando su uso mayormente para las comunicaciones de Intranet, es decir para la comunicación entre sus agencias y oficina principal, teniendo como base a las redes Frame Relay. Las aplicaciones bancarias dejaron de basarse en la conexión al Host desde un terminal (aunque seguían usando emulaciones de terminal), y se inicio el uso de aplicaciones cliente-servidor, es decir aplicaciones que interactuaban directamente con las bases de datos.

2.2.4 Las redes ATM y MPLS

En las redes publicas (ofrecidas por las empresas portadoras), el frame relay fue siendo dejado de lado, como protocolo de capa de enlace o de conmutación de paquetes, por el ATM (Asynchronous Transfer Mode) formándose redes publicas ATM.

Una conexión ATM, consiste de "celdas" de información contenidas en un circuito virtual (VC). Estas celdas provienen de diferentes fuentes representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas variables tipo ráfagas (bursty traffic) como los datos.

Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para transporte de información y los restantes para uso de campos de control (cabecera) con información de origen y destino; es identificada por un "virtual circuit identifier" VCI

y un "virtual path identifier" VPI dentro de esos campos de control que incluyen tanto el enrutamiento de celdas como el tipo de conexión.

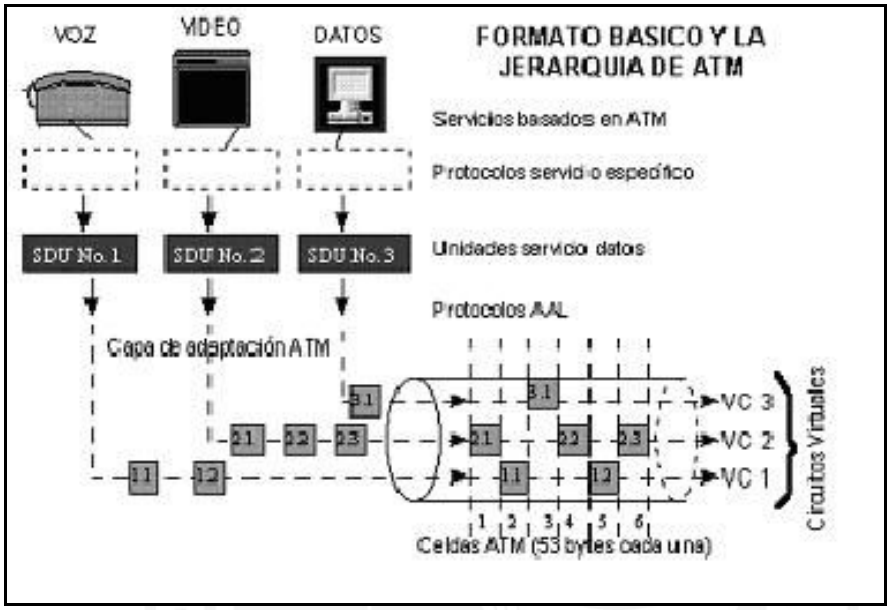

Fig. 2.5. Formato de Jerarquía ATM

La organización de la cabecera (header) variará levemente dependiendo de sí la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local - ya que pueden ser cambiados de interfaz a interfaz. La técnica ATM multiplexa muchas celdas de circuitos virtuales en una ruta (path) virtual colocándolas en particiones (slots), similar a la técnica TDM. Sin embargo, ATM llena cada slot con celdas de un circuito virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes. La figura siguiente describe los procesos de conmutación implícitos los VC switches y los VP switches.

Las redes ATM otorgaron ciertos niveles de seguridad a las redes de conmutación de paquetes, superiores a los logrados por Frame Relay, lográndose la creación de VLAN

entre los dominios de una empresa, con posibilidad de crear extranets limitadas con empresas satélites o proveedoras.

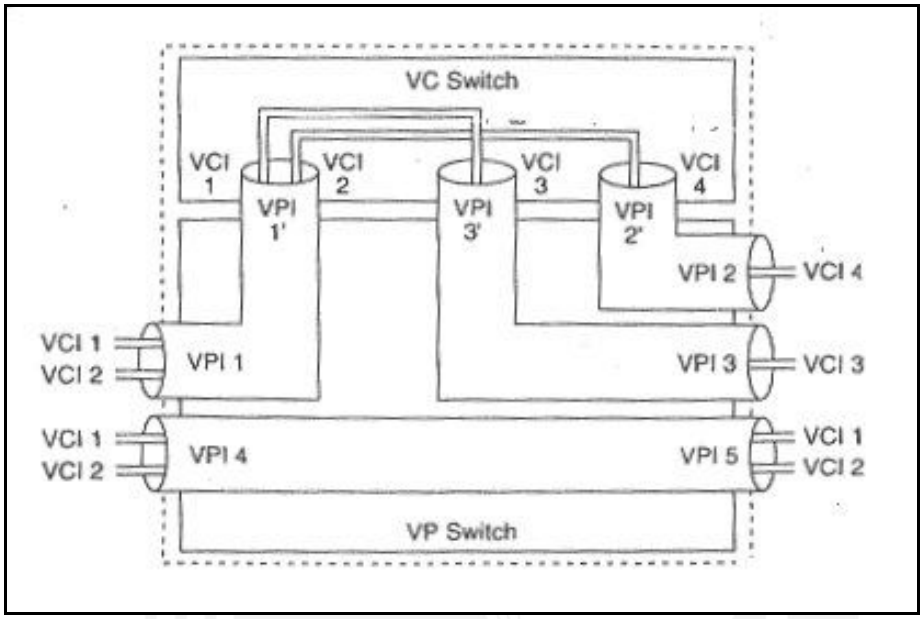

Fig. 2.6. Procesos de conmutación ATM implícito

A partir de la segunda mitad de los 90, con la llegada de FirstCom (luego AT&T y ahora Telmex), Millicom, Diveo, entre otras, iniciaron la competencia entre empresas portadoras, quitándole el monopolio a Telefónica.

Entonces se inició la competencia en la oferta de redes ATM de similares características, sobre las cuales se montan redes IP.

Un tiempo después, las redes ATM mejoran con la incorporación del MPLS. Una de las grandes ventajas de usar tecnología MPLS, ofrecida por empresas como Telefónica, es que se pueden formar redes “full mesh”, es decir una red privada en la que los nodos pueden comunicarse entre sí, sin pasar por el nodo central.

La gran tarea en las redes bancarias ha sido el integrar los servicios de comunicación, de tal forma que no existan redes separadas para los datos (la comunicación con las

aplicaciones de negocio, para los servicios de backoffice –correo electrónico, intranet, etc. - servicios de seguridad como alarmas, etc.), para voz (telefonía) y vídeo (tele conferencia, vigilancia, etc.). La convergencia de estas redes, buscaba principalmente una reducción de costos en equipamiento y enlaces, así como la mejora en los servicios.

RED o SERVICIO	Redes E1 (TDM)	Conmutación de Paquetes (X.25)	Frame Relay	ATM
Multiplicación	Deterministica	Estadística (canal lógico o circ. virtual)	Estadística (idem)	Estadística (canal virtual, con. Virtual)
Optimización del uso por los puertos	No	Si	Si	Si
Razón de transferencia (throughput) elevado	Si	No	Si	Si
Retardo	Muy bajo	Elevado	Bajo	Muy Bajo
Recuperación de errores por la red	No	Si	No	No
Longitud de Paquetes	No Aplica	Variable	Variable	Fija
Aplicación	Red de transporte	Servicio de interconexión de datos	Servicio de interconexión de datos	Red de transporte
Organismo de Estandarización		UIT, ISO	UIT, ANSI, IEEE	UIT
Velocidades Actuales		9.6 Kbps a 64 Kbps	56 a 2048 Kbps	45 a 155 Mbps
Longitud de paquete		Variable hasta 4096 octetos	Variable hasta 4096 octetos	Fija, 53 octetos
Multidireccionamiento		No	Si	Propuesto
Direccionamiento		X.121 de longitud variable	Fijo (DLCI de 10 bits) – PVC	Fijo (24 bits de VPI/VCI)
Servicio Connectionless		No	No	No
Circ. Virtual Permanente		Si	Si	Si
Circ. Virtual Conmutado		Si	Si	Si
Control de flujo explícito		Si	No	No
Corrección de errores a niveles de enlace		Si	No	No

Cuadro 2.1. Resumen de las características de protocolos de redes

En lo que respecta a los servicios de comunicaciones de datos, uno de los puntos de trabajo fue el mantener una red con los protocolos heredados (como el X25, usados en los Cajeros Automáticos, o como el SNA, usado en la comunicación con las aplicaciones de terminal). El reto al integrar estos servicios a las redes IP fue el de encapsular estos protocolos sobre TCP, lo cual veremos en el capitulo siguiente.

El cuadro 2.1 es un resumen de los protocolos de redes más usados en las redes de datos bancarios.

2.3 La gestión de red

La gestión de una red de cajeros siempre ha sido de suma importancia para poder administrar en forma integrada los elementos de la red, solucionar los posibles problemas sin demora, entre otros. El sistema de gestión regularmente estaba asociado al software de la aplicación y a las herramientas que podían entregar los fabricantes de los equipos de comunicaciones. En el caso de los concentradores Telematics se usaba un software SmartNet, que si bien cumplía con las funciones mínimas, era muy limitado sobre todo por su interfase en modo caracter.

Los sistemas de gestión podían entregar una visión sobre el estado de las interfaces de la red, las estadísticas de cada puerto en los nodos de la red, y en algunos casos notificaciones sobre alertas

La complejidad de las redes hace conveniente e incluso necesaria la adquisición de Sistemas Integrados de Gestión de Red que proporcionan las siguientes ventajas:

- Facilitan la localización y resolución de problemas en la red
- Permiten gestionar desde una consola los elementos activos de la red (ruteadores, switches, concentradores, etc.), siendo capaces de recibir información de sucesos procedente de los elementos gestionables, creando alarmas e incluso permitiendo crear acciones de respuesta ante esas alarmas.
- Permiten mantener un esquema general de toda la red, facilitando las labores de análisis con el fin de extender o modificar la estructura actual de la red. Estos sistemas suelen ofrecer una facilidad de exploración que permite descubrir los elementos de red y establecer la topología física y lógica.

- Disponen, en general, de gran número de aplicaciones integrables en el sistema de gestión, como herramientas de gestión/administración de sistemas operativos de red (Novell Netware, Windows NT, etc.), de gestión de nodos Unix, etc.

En entornos abiertos, como el TCP/IP, el protocolo de gestión definido es el SNMP (Simple Network Management Protocol) o protocolo simple de gestión de redes, es el protocolo de gestión de red más importante y usado en la actualidad. Forma parte del conjunto de protocolos TCP/IP y está definido en la capa de aplicación del mismo. SNMP busca la sencillez y es por ello que en la capa de transporte está soportado por el protocolo UDP (caracterizado por su rapidez y su falta de fiabilidad) a través del puerto 170.

La mayor parte de los elementos activos de red (ruteadores, concentradores, swiches, etc.) cuentan con agentes de gestión SNMP.

En esencia, la gestión de red se basa en el mantenimiento, en cada nodo gestionable de la red, de una base de datos de funcionamiento del nodo, denominada MIB. Esta base de datos, de estructura jerárquica, comprende los parámetros de configuración y funcionamiento del elemento gestionable. El mantenimiento de la MIB puede realizarse remotamente, desde una consola de gestión, gracias al agente de gestión. En el caso de SNMP la definición de la MIB está contemplada en el documento RFC 1213. Los agentes también pueden notificar algún evento detectado en el sistema a la consola de gestión mediante mensajes llamados traps.

La segunda versión de SNMP, denominada SNMPv2, ha introducido algunas de las ventajas de la gestión MIP, pero es en la nueva versión SNMPv3 en donde las ventajas de seguridad son enormes, ya que los agentes de SNMP deben buscar autenticación cada vez que responden a un comando, dejando de ser puntos vulnerables en la red.

Los cajeros como elementos TCP/IP son capaces de soportar SNMPv2 y ser gestionados desde una consola de administración preparada para tal fin. Así cada fabricante (NCR, Wincor-Nixdorf, y Diebold) ha desarrollado agentes SNMP residentes con potentes capacidades para el análisis de fallas en forma predictiva y el filtrado de eventos. El consola ofrece acceso remoto a un amplio conjunto de estadísticas del ATM y sus dispositivos residentes permitiendo la administración de sus estados de salud e información sobre el estado de los suministros.

2.4 La seguridad de redes

La interacción y colaboración entre dos entidades se desarrolla en base a la comunicación entre ellas y tiene como pre-requisito la confianza, que se construye y genera en base a políticas de seguridad.

En la comunicación entre dos entidades, independientemente del medio o protocolo usado, podemos aseverar que la comunicación es segura, si sabemos:

- Quien nos envía mensajes (autenticación)
- Que los mensajes no los va a “escuchar nadie mas” (confidencialidad)
- Que nadie los va a alterar en el camino (integridad)
- Que nadie negará la veracidad del mensaje (no repudiación).

En las antiguas redes teníamos la confianza de que todo esto se cumplía, por que teníamos redes formadas por enlaces dedicados (de cierta forma aseguraban privacidad) y por protocolos “seguros” (difícilmente adulterables).

Uno de los pilares en la difusión del Internet (la red pública más grande), es su protocolo de red y transporte, el cual se basa como otros en el modelo OSI: el IP (en la capa de red) y el TCP (en la capa de transporte). El protocolo IP, no es un protocolo fiable, ya que los datagramas pueden ser entregados con errores, fuera de secuencia, o no ser entregados por los nodos de red (si bien la red debe realizar su mejor

esfuerzo, es decir, todas las acciones posibles para que sean entregados correctamente). De tales funciones – garantizar la corrección de los datagramas, su llegada al DTE y de las fases de establecimiento y liberación de conexiones – se encarga un nivel superior, a través del protocolo TCP.

De allí es que parten algunos problemas de seguridad, que hacen del protocolo TCP/IP vulnerable a las suplantaciones (IP spoofing, intrusión de hackers), a la alteración de información (virus, troyanos), etc.

Eso ha generado el crecimiento en la industria de la seguridad de la información, creando técnicas de protección y defensa para minimizar las vulnerabilidades del protocolo. El llegar a un nivel de seguridad adecuado, con redes confiables hace que las instituciones financieras inicien operaciones con otras instituciones usando el protocolo TCP/IP.

Desde el punto de vista del modelo OSI, podríamos efectuar un análisis de la seguridad que se puede lograr por nivel:

- Seguridad en el nivel aplicación. Es la solución adecuada cuando el servicio de seguridad es específico de la aplicación o pasa a través de aplicaciones intermedias. Es el caso de los mensajes de correo, transacciones financieras vía Web, comercio electrónico (SET). Se puede considerar como ventaja que existen menos datos para procesar, que es una interfaz sencilla con la aplicación, pero se debe considerar como desventaja que se debe implantar por cada aplicación en cada sistema extremo.
- Seguridad en el nivel de transporte. Los datos procedentes de la aplicación se cifran en el terminal origen antes de ser transmitidos. Este es el caso de SSL (Secure Socket Layer) y WTLS (Wireless Transport Layer Security). La ventaja de ubicar la seguridad en este nivel es que sólo es necesario diseñar dos interfaces entre el nivel de seguridad y el de transporte, por otro lado tenemos

como desventaja que no permite ofrecer servicios a campos específicos de la aplicación.

- Seguridad en el nivel de red. Se aplica cuando se supone que los sistemas extremos son fiables y las redes subyacentes no lo son, un ejemplo de protocolo en este nivel es IPSEC. Cuando la seguridad esta ubicada en este nivel la desventaja es la no compatibilidad con sistemas conectados a otro tipo de redes, pero como ventajas tenemos que estos servicios de seguridad son transparentes a la aplicación, y además oculta detalles de la red.

En toda empresa se debe contemplar políticas de seguridad de red que contemplen por lo menos lo siguiente:

- Una política de acceso a los recursos que defina derechos y privilegios, para la conexión de redes externas, dispositivos o nuevo software en los sistemas.
- Una política de auditoria que defina responsabilidades de los usuarios, equipo de operaciones y administración. Debe permitir reportar problemas de seguridad.
- Una política de autenticación que establezca confianza a través de una efectiva política de contraseñas, y configure una guía para la autenticación desde puntos remotos.

Para aplicar las políticas de seguridad es necesario contar con los mecanismos necesarios, los cuales deben ser habilitados en la infraestructura de la red.

2.4.1 Protección perimétrica

En primer lugar la atención a los accesos en el perímetro de la red. Este primer “filtro” se basa en la comparación de cierto contenido de los paquetes (origen, destino, puertos de servicio, contraseñas, etc.) cuyo resultado conlleva a decisiones de

"apertura" o "cierre" de puertas, seguidas de otras posibles medidas de salvaguarda. Estos filtros pueden estar configurados en switches (a nivel de MAC address si es de capa 2 o a nivel de IP si es de capa 3), en ruteadores (a nivel de IPs, y puertos TCP) y en los Firewall.

El firewall

El firewall o cortafuego es un mecanismo de filtro avanzado que protege la confidencialidad e integridad de la información que lo atraviesa, protege una red de la otra en la que no se tiene confianza (Internet, o una extranet). Funcionalmente es un dispositivo lógico que tiene funciones de separación, limitación y análisis del flujo de la información que circula entre sus puertas. Como ejerce un control de acceso centralizado, su efectividad exige que lo atraviese todo usuario interno/externo/remoto para acceder desde/a las redes internas protegidas. Existen firewall que solo trabajan a nivel de red, también llamados de filtros de paquetes (que son básicamente ruteadores con filtros como lo explicamos unas líneas arriba), los firewall a nivel de aplicación o proxy (el dispositivo se convierte en el apoderado de las conexiones salientes por cada servicio) y los firewall activos (los cuales son una combinación de los dos anteriores). Este último es el usado en la actualidad y tiene la ventaja de agregarle inteligencia a la inspección de paquetes para evitar ser engañados con "ip spoofing", o ataques tipo DoS (denial of service). Algunas características funcionales de los firewall de última generación son las siguientes:

- Cifrado
- Soporte de redes virtuales privadas (VPN) usando IPSec y L2TP.
- Proxy de aplicación soportado (http, ftp, telnet, smtp,..)
- Soporte de detección de virus.
- Filtro de página web.

- Notificación de violación. Alarmas en correo, pop-up, snmp, etc.
- Autenticación de usuarios (propio o con servidores SecureID, Radius, etc.)
- Auditoria y registro de ingresos. Tanto de accesos permitidos como rechazados, así como eventos de configuración y autenticación.

Los Sistemas de Detección de Intrusos

Los sistemas de detección de intrusos (IDS, Intrusion Detection System) son dispositivos que instalados en la red, "escuchan" el trafico de la red, y detectan comportamientos anormales que podrían ser considerados como intrusiones o ataques a la red privada. Existen dos tipos de IDS, los de red (instalado en un dispositivo con puerto de monitoreo de red) y otro de Host (instalado en un servidor de aplicación critica). Al ser instalados como puntos de escucha su acción es solo de alertar pero difícilmente pueden evitar un posible ataque. La nueva generación de los IDS son los llamados Sistemas de Detección y Prevención de Intrusos (IDP), los cuales se instalan como un bridge en el punto de acceso a la red a proteger, escuchando todo el trafico entrante, y tomando acción sobre un comportamiento anómalo (puede efectuar desconexiones TCP y evitar una nueva conexión desde la dirección IP sospechosa).

2.4.2 Protección de contenido.

La protección de contenido implica que la data transmitida no sea conocida por un ente distinto al destino, así como que ésta no puede ser alterada o cambiada en el camino.

Si se quiere lograr esto en un enlace de comunicación TCP/IP, este debe pasar por un "túnel seguro", nombre con el cual se le conocen a los enlaces de Redes Privadas Virtuales (VPN). Estos túneles aseguran privacidad (es cifrado), autenticidad (usa

certificados digitales) e integridad (usan firma digital). Uno de los protocolos más usados es el IPSec, el cual tiene dos fases de negociación:

1. Fase 1, o negociación de llaves de cifrado IKE. Las llaves se generan bajo un método (usualmente Diffie-Hellman grupo2), se intercambian bajo un modo de autenticación (pre-shared o certificados digitales) cifradas bajo un algoritmo (p.e. 3DES), y se verifica su integridad por un algoritmo de hash (p.e. SHA-1 o MD5).
2. fase 2, o de cifrado de data. Se especifica el modo de encapsulación (ESP o AH), el algoritmo de cifrado (3DES), el tipo de autenticación (SHA-1 o MD5), entre otros.

Las conexiones IPSec pueden establecerse entre un cliente y una institución o "client to site" (conexiones remotas de Teletrabajo), y entre dos instituciones "site to site". A continuación se muestra las características de conexiones IPSec típicas.

Propiedades de Túnel		Alternativas en dispositivo VPN
Fase 1	Método de autenticación	Pre-Shared Secret o Certificado Digital
	Esquema de encripción	IKE
	Grupo Diffie-Hellman	Group 1, 2, 5 o 7
	Algoritmo de encripción	3DES, DES, AES128, AES912, o AES256
	Algoritmo Hashing	SHA-1
	Mode de negociación	MAIN, Agressive
	Tiempo de vida (para renegociar)	28,800 seg.
Fase 2	Método de encapsulación	ESP o AH
	Algoritmo de encripción	3DES, DES, AES128, AES912, o AES256
	Algoritmo de autenticación	SHA-1
	Perfect Forward Secrecy	Group 1, 2, 5 o 7
	Tiempo de vida (para renegociar)	3,600 seg.
	Lifesize en KB (para renegociación)	No

Cuadro 2.2. Parámetros de configuración de enlace VPN IP-Sec.

Si se quiere lograr la protección de la información antes de que salga al canal de comunicación, podemos evaluar el cifrado de la data (para ocultar la data) o el uso de

certificados digitales (para asegurarnos de la autenticidad del remitente y destinatario) o de valores de chequeo (para asegurar integridad). En este caso, a diferencia del IPSec, estamos dejando sin proteger las cabeceras de los datos, los cuales contienen información de red, como las direcciones IP origen y destino así como los puertos TCP usados.

En el caso de las aplicaciones transaccionales como el protocolo de mensajes de cajeros NDC y el protocolo de mensajes ISO8583 (para los mensajes a host), es posible usar el Message Autentication Code (MAC), el cual es un “valor de chequeo” generado mediante un cálculo matemático que usa como datos ciertos campos del mensaje intercambiado, que debe ser recalculado en el host destino, y comparado contra el valor de chequeo original para validar el mensaje. Esto requiere compatibilidad en el uso de una misma llave MAC y algoritmo de cifrado en los dos extremos de la aplicación.

CAPÍTULO III

3 PROPUESTA TÉCNICA

Para lograr los objetivos propuestos fue necesario plantear una reingeniería de toda la red, que se inicia seleccionando la solución de red que soporte a los protocolos heredados (SNA, X25,..), seleccionando productos y proveedores para la renovación de la infraestructura de comunicaciones y la re-distribución de enlaces por medios más ventajosos.

El rediseñar la red se ha definido desde varios frentes o niveles como los que se reseñan a continuación:

- al nivel de protocolo de comunicación (configurando la concentración de enlaces por interfaz, y protocolos encapsulados)
- al nivel de medios de comunicación (selección de empresa portadora y producto)
- al nivel de infraestructura: renovación de los equipos de comunicaciones
- al nivel de seguridad y
- al nivel de administración de red
- la migración de terminales bajo protocolo TCP/IP en la red WAN.

3.1 Alternativas de solución para las comunicaciones con protocolos heredados

Como se refirió en los capítulos anteriores, para la comunicación con los cajeros automáticos y con las instituciones, la red de SERBAN establecía enlaces dedicados controlados por un solo protocolo de comunicación: X.25 o SNA, a razón de que los equipos finales (cajeros automáticos y computadores centrales) soportaban solo aquellos protocolos. Como las aplicaciones finales (la de los hosts y la de algunos cajeros) no se podrían cambiar por sus altos costos, entonces el diseño de la nueva red debe considerar mantener los protocolos de comunicación en los que se basan.

Las redes ofrecidas por las empresas portadoras, muchas de ellas nuevas en el mercado peruano, solo ofrecían soluciones para protocolos IP. Se debía revisar la forma de integrar el X.25 y SNA sobre redes TCP/IP sin elevar los costos para instalaciones de cajeros que no requerían un ancho de banda alto (los 64 Kbps. ofrecidos como velocidad mínima por la mayoría de empresas portadoras para la instalación de cajeros era un exceso por la velocidad y por el costo).

La premisa era ahorrar costos y reducir la complejidad de la red, lo cual se podía lograr al concentrar varios enlaces en pocos circuitos dedicados (al reducir el número de circuitos contratados se ahorra en costos facturados por la empresa portadora y en el mantenimiento de puertos de ruteador). En el caso de la conexión con la sede principal de las instituciones, se podía lograr establecer un circuito único: para el enlace del Host, para los cajeros automáticos en la sede principal, para un servicio de transferencia de archivos y para comunicación por voz. En el caso del resto de cajeros, por su dispersión (en agencias de las instituciones y en puntos neutros) era más complicado establecer concentración de servicios.

3.1.1 Concentración de enlaces X.25

Una de las ventajas del X.25 es que puede concentrar un gran número de enlaces o circuitos virtuales por un solo canal físico. Teóricamente un circuito X.25 puede mantener hasta 255 circuitos virtuales, cada uno de ellos identificados por un LCN (Número de Canal Lógico).

Para las conexiones X.25 se plantea concentrar todos los enlaces X.25 en la red pública de paquetes X.25 llamada Meganet DPN de Telefónica del Perú, con un alto numero de canales LCN, en vez de tener varios enlaces costosos con un bajo numero de canales.

```
!
x25 routing   ← Activa ruteo X25
!
interface Serial1/2
 description LINK0-ULTRA3
 no ip address
 encapsulation x25 dce
 x25 htc 256          ← canal lógico + alto
 clockrate 9600       ← sincronismo que entrega el ruteador al otro equipo.
 lapb T1 9000
 lapb N2 10
!
interface Serial1/3
 description LINK-PADLAB
 no ip address
 encapsulation x25
 no ip mroute-cache
 x25 ltc 2            ← canal lógico + bajo para la conexión de cajeros
 x25 htc 128          ← canal lógico + alto que se puede establecer. 127 canales
 lapb T1 5000           contratados.
 lapb N2 10
!
x25 route ^7161.* interface Serial1/3  ← ruta principal
x25 route ^7161.* interface Serial1/0  ← ruta backup por dial-up
x25 route ^716014000280 interface Serial1/2
x25 hunt-group PadLAB vc-count interface Serial1/3← comando de
administración  para agrupar rutas y contabilizar SVCs por interfaces.
```

Interface de entrada que se conecta al Link X25 del Ultra
Parámetros X25 y LAPB según configuración de interface del Link X25 correspondiente.

Interface de salida que se conecta a Meganet.

Fig. 3.1. Modelo de configuración en ruteador Cisco de interfaces X25 para la comunicación de ATMs.

Dependiendo del tráfico de cada canal se debía efectuar un cálculo del ancho de banda necesario para soportar N enlaces (menor a 255). Si se tiene que una transacción promedio no sobrepasa los 2 Kbytes de datos (en el momento de

inicialización del cajero se llega al máximo de transferencia, al cargar 30 Kbytes de datos de parámetros) y se debe atender en promedio 3 transacciones por segundo de N cajeros, entonces 64 kbps era suficiente para atender a todos los cajeros.

En la Fig. 3.1 se muestra un ejemplo de la configuración de un ruteador Cisco (la marca de ruteadores de mayor comercialización), de una conexión a la red Meganet, sólo considerando una interfase de entrada y otra de salida:

3.1.2 Encapsulado de protocolos X25 sobre TCP/IP

Con la ayuda de los ruteadores se puede conseguir encapsular el protocolo X25 en un extremo de una red TCP/IP y des-encapsularlo en otro. Esto quiere decir que un ruteador en SERBAN o en la central del banco puede recibir paquetes X.25 por un puerto serial, y enrutarlos por un puerto ethernet u otro serial (con un camino IP), hasta una agencia en donde esté instalado otro ruteador que desencapsule los paquetes X.25 y los enrute a un puerto serial en donde esté conectado el cajero automático.

Esto se logra gracias a nuevas funcionalidades incluidas en ruteadores de las marcas Cisco (XOT: X25 over TCP) y Motorola (SOT: Serial over TCP). Ambas se basan en principios similares pero no son parte de un estándar y por lo tanto no son compatibles uno con el otro, ya que por ejemplo usan puertos TCP distintos. Solo la marca Cisco ha promovido al XOT para que llegue a ser un estándar en la industria (publicado por la IETF como el RFC 1613). Es por eso que para asegurar el funcionamiento de esta red, debe mantenerse uniformidad de marca de ruteadores.

La siguiente es una muestra de unas tramas de XOT registradas por un analizador de protocolos RADCOM durante el establecimiento de una conexión de cajero con X.25, entre dos ruteadores Cisco, uno con dirección IP 1.1.1.1 y otro con dirección IP 1.1.1.2 en la misma red. El puerto TCP asignado por Cisco es el 1998.

```
Frame: 1 Captured at:  -00:24.334
Length: 85    From: Port 2    Status: Ok
IP: Version = 4
IP: Total Length = 67
IP: Identification = 2
IP: Flags & Fragment Offset: 0x0000
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 255 [Seconds/Hops]
IP: Protocol: 6 TCP
IP: Header Checksum = 0xB7AE
IP: Source Address = 1.1.1.2
IP: Destination Address = 1.1.1.1
TCP: Source Port = 11014
TCP: Destination Port = X.25 Over TCP
TCP: Sequence Number = 1497322504
TCP: Acknowledgement Number = 1484356924
TCP: HLEN = 20 [Bytes]
TCP: Flags: 0x5018    ACK  PSH
TCP: Window = 8192
XOT: Version: 0
XOT: Length: 23
X.25: Packet Type=Call Request  LGN=0  LCN=2  D=0  Q/A=0
X.25: Called DTE Address=600013000013
X.25: Calling DTE Address=716014000280
X.25: Facility: Window Size Negotiation
X.25: Facility: Packet Size Negotiation

Frame: 2 Captured at:  -00:23.846
Length: 65    From: Port 1    Status: Ok
IP: Version = 4
IP: Total Length = 47
IP: Identification = 2
IP: Flags & Fragment Offset: 0x0000
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 255 [Seconds/Hops]
IP: Protocol: 6 TCP
IP: Header Checksum = 0xB7C2
IP: Source Address = 1.1.1.1
IP: Destination Address = 1.1.1.2
TCP: Source Port = X.25 Over TCP
TCP: Destination Port = 11014
TCP: Sequence Number = 1484356924
TCP: Acknowledgement Number = 1497322531
TCP: HLEN = 20 [Bytes]
TCP: Flags: 0x5018    ACK  PSH
TCP: Window = 8165
XOT: Version: 0
XOT: Length: 3
X.25: Packet Type=Call Connected  LGN=0  LCN=2  D=0  Q/A=0

Frame: 3 Captured at:  +00:00.000
Length: 179    From: Port 1    Status: Ok
IP: Version = 4
IP: Total Length = 161
IP: Identification = 3
IP: Flags & Fragment Offset: 0x0000
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 255 [Seconds/Hops]
IP: Protocol: 6 TCP
IP: Header Checksum = 0xB74F
IP: Source Address = 1.1.1.1
IP: Destination Address = 1.1.1.2
TCP: Source Port = X.25 Over TCP
TCP: Destination Port = 11014
TCP: Sequence Number = 1484356931
TCP: Acknowledgement Number = 1497322531
TCP: HLEN = 20 [Bytes]
TCP: Flags: 0x5018    ACK  PSH
TCP: Window = 8165
XOT: Version: 0
XOT: Length: 117
X.25: Packet Type=DATA  LGN=0  LCN=2  D=0  Q/A=0  P(S)=0  P(R)=0  M=0
User Data
OFFSET DATA                                          ASCII
003D: 31 31 1C 31 33 35 1C 1C 1C 31 3E 1C 3B 35 30 38  11.135...1>.;508
004D: 31 38 38 30 30 31 33 38 39 30 30 31 30 30 30 35  1880013890010005
(....)
```

Fig. 3.2. Captura de trafico XOT con un analizador de protocolo.

Como se observa en la fig. 3.2 los paquetes X.25 se montan intactos sobre el stack TCP, y no existe variación alguna en los parámetros de negociación de la conexión, ni

en los datos enviados por el cajero (en este caso la solicitud de una transacción).La configuración del XOT en los ruteadores Cisco es sencilla, y prácticamente solo implica enrutar el paquete de un cajero con una dirección X25 conocida a la dirección IP del ruteador destino en donde está conectado el cajero. El resto es manejo de tráfico TCP/IP.

```
ruteador  origen
x25 route ^600013000013 xot 1.1.1.2

ruteador destino
!
interface Ethernet0
ip address 1.1.1.2 255.255.255.0
!
interface Serial0
 description ATM REMOTO
 no ip address
 encapsulation x25 dce
 no ip mroute-cache
 x25 ltc 2          ← canal lógico + bajo para la conexión de cajeros
 x25 htc 3
!
x25 route ^600013000013 interface Serial0
```

Fig. 3.3. Configuración XOT de ruteadores Cisco para la conexión X25 de un ATM.

En la Fig. 3.4 vemos el caso de una conexión usando una red WAN IP, entre el SWITCH y el ATM X.25, la cual puede ser una red pública como Internet, o una red privada como la red de un banco.

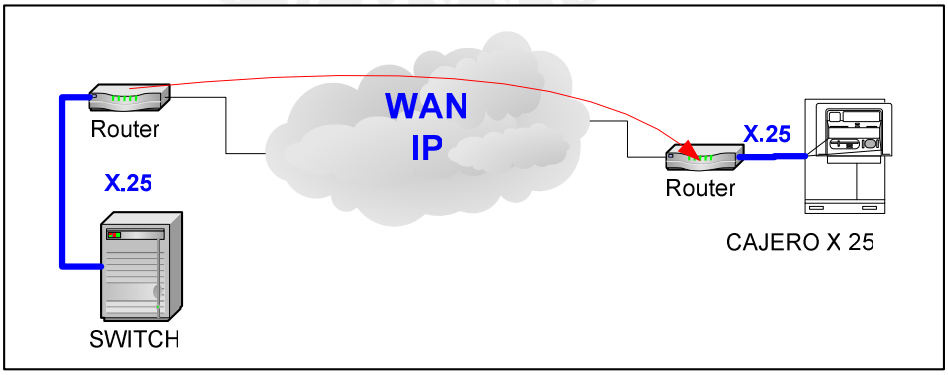

Fig. 3.4. Esquema de comunicación XOT entre dos ruteadores.

3.1.3 Encapsulado de protocolos SNA sobre TCP/IP

De forma similar que con el X25, los ruteadores pueden lograr que el protocolo SNA se puede encapsular sobre TCP en un extremo y sea transportado por una red IP hasta otro ruteador que lo haya des-encapsulado y entregue las tramas SNA al computador remoto, ya sea en SDLC (a un puerto serial) o en LLC2 (en la red ethernet).

Para lograr esto se puede hacer uso de un estándar como el Data Link Switch (DLSw), desarrollado por IBM en 1992 para lograr integrar sus computadores trabajando con SNA a una red IP, y que esta incluido en ruteadores como Cisco, Motorola, entre otros, como una funcionalidad especial (publicado por el IETF como el RFC 1795 en el año 1995).

La compañía Cisco incorporó en sus equipos las soluciones de comunicación de IBM, para las muchas variantes del SNA (APPN, APPC, etc.) que hasta en esos momentos era manejado por controladores de comunicaciones costosos. Entonces incorporaron alternativas como el SDLLC (conversión del LLC2 a SDLC), RSRB (Source Route Bridging), QLLC (transporte de SNA sobre X.25), STUN (túnel serial) entre otras.

En el caso de SERBAN, la solución propuesta se basa en que un ruteador Cisco (con el IBM feature set) reciba las tramas LLC2 enviadas por el computador SUN del SWITCH, las encapsule en TCP, y las transporte hasta el ruteador par, el cual tendrá una conexión serial para desencapsular SDLC y entregarlo directamente al computador AS/400 remoto.

De esta forma no se comprometía al banco o institución a modificar su aplicación y mantener un puerto serial como interfaz de comunicación.

Como se observa en la figura 3.5 el enlace DLSw (SNA sobre TCP/IP) requiere de lo siguiente:

- Un ruteador en SERBAN que esté en la red ethernet del computador SWITCH (con software SNA PU2.1

- un ruteador en el banco con puerto serial V24 para la conexión del Host del banco,
- un enlace TCP/IP entre ambos ruteadores.

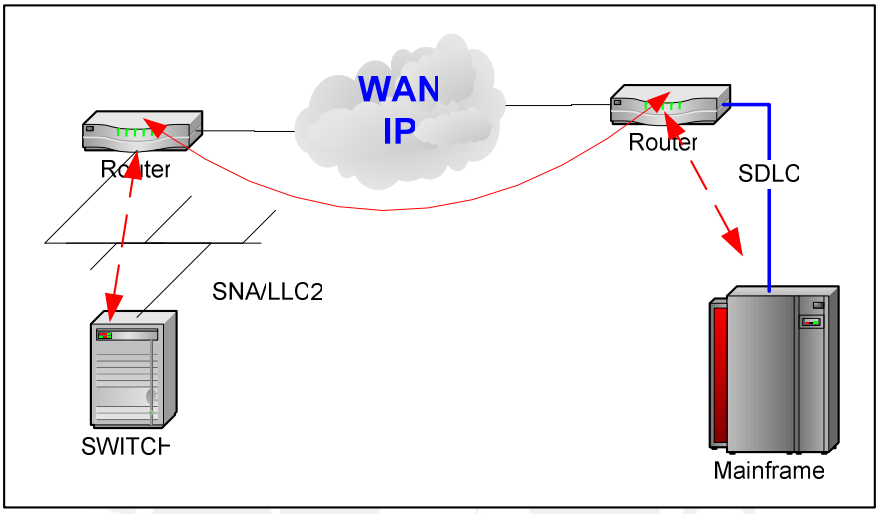

Fig. 3.5. Enlace DLSw entre dos ruteadores (SNA sobre TCP).

Se debe conseguir establecer un túnel DLSw (TCP/IP) para que luego se propaguen las direcciones MAC de las redes IBM Token Ring formadas en ambas redes (éstas se consideran como direcciones MAC ethernet invertidas). Una vez propagadas las direcciones MAC, podrán ser identificadas por las configuraciones SDLC (en el puerto serial del ruteador conectado al Host del Banco) y LLC (en el computador SWITCH con el software SNA) de cada equipo.

En las configuraciones de DLSw es necesario establecer y afinar ciertos parámetros de temporizadores, para conseguir la desconexión entre aplicaciones si es que una de ellas se cierra, o el mantenimiento del enlace a pesar de que no haya actividad (keepalive).

El comportamiento de la aplicación en el SWITCH y en el HOST no debería tener cambio alguno, toda vez que la interfase serial a usar sigue siendo la misma.

Una configuración de ruteadores mínima para estos enlaces es la siguiente en la Fig. 3.6:

Router1 (SERBAN)

```
!
dlsw local-peer peer-id 172.20.21.1
dlsw remote-peer 0 tcp 172.20.20.1 dest-mac 4000.0003.22c1
dlsw icanreach mac-exclusive            ← filtro de MACs en ruteador
dlsw icanreach mac-address 1000.0461.9e0e mask ffff.ffff.ffff
dlsw udp-disable
!
interface Loopback0
 ip address 172.20.21.1 255.255.255.0
 no keepalive
!
interface FastEthernet0/0
 duplex auto
 speed auto
 bridge-group 1
!
!
ip route 172.20.20.0 255.255.255.0 10.10.10.2 30
bridge 1 protocol ieee
```

Router2 (Banco)

```
!
dlsw local-peer peer-id 172.20.20.1
dlsw remote-peer 0 tcp 172.20.21.1
dlsw udp-disable
!
interface Loopback0
 ip address 172.20.20.1 255.255.255.0
 no keepalive
!
interface Serial1
 description SNA
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role secondary
 sdlc vmac 4000.0003.2200          ← MAC virtual del puerto SDLC
 sdlc address C1 xid-passthru
 sdlc partner 1000.0461.9e0e C1    ← MAC de equipo destino en SERBAN

 sdlc dlsw C1
!
ip route 172.20.21.0 255.255.255.0 10.10.10.1 30
```

Fig. 3.6. Configuración DLSw en ruteadores Cisco.

Para monitorear este enlace se debe ejecutar los siguientes comandos:

```
VERIFICA CONEXIÓN TCP/IP ENTRE DOS RUTEADORES

GMD361#sh dlsw peers
Peers:                state     pkts_rx   pkts_tx  type  drops ckts TCP   uptime
 TCP 172.20.20.1     CONNECT      22422     26084  conf      0    2   0     1w0d
Total number of connected peers: 1
Total number of connections:     1

VERIFICA EL APRENDIZAJE DE LOS MAC ADDRESS DE LAS REDES LOCAL Y REMOTA
(TRANSPORTADO POR EL CANAL DLSw)

GMD361#sh dlsw reachability
DLSw Local MAC address reachability cache list
Mac Addr         status     Loc.    port                 rif
1000.0461.9e0e   FOUND      LOCAL   FastEthernet0/0     --no rif--
4000.0003.21c1   SEARCHING  LOCAL
4000.0003.22c1   SEARCHING  LOCAL
4200.0000.0024   SEARCHING  LOCAL

DLSw Remote MAC address reachability cache list
Mac Addr         status     Loc.    peer
4000.0003.22c1   FOUND      REMOTE  172.20.20.1(2065) max-lf(17800)

DLSw Local NetBIOS Name reachability cache list
NetBIOS Name     status     Loc.    port                 rif

DLSw Remote NetBIOS Name reachability cache list
NetBIOS Name     status     Loc.    peer

GMD1720#sh dlsw reachability
DLSw Local MAC address reachability cache list
Mac Addr         status     Loc.    port                 rif

DLSw Remote MAC address reachability cache list
Mac Addr         status     Loc.    peer
1000.0459.1ab8   UNCONFIRM  REMOTE  172.20.21.1(2065)
                                    172.20.22.1(2065)
1000.0461.9e0e   FOUND      REMOTE  172.20.21.1(2065)
                                    172.20.22.1(2065)

DLSw Local NetBIOS Name reachability cache list
NetBIOS Name     status     Loc.    port                 rif

DLSw Remote NetBIOS Name reachability cache list
NetBIOS Name     status     Loc.    peer

VERIFICA QUE CONTROLADORES SNA HAYAN ESTABLECIDO CONTACTO

GMD361#sh dlsw circuits
Index           local addr(lsap)    remote addr(dsap)  state          uptime
2550137452      1000.0461.9e0e(04)  4000.0003.22c1(04) CONNECTED      00:41:55
Total number of circuits connected: 1
```

Fig. 3.7. Comandos de monitoreo de DLSw.

3.2 Alternativas de Enlaces.

Como parte de la llegada de nuevas empresas de servicios de telecomunicaciones, como Telmex (antes AT&T), Telefónica Empresas, Millicom, Diveo, entre otras, se han

renovado las tecnologías existentes hasta hace 5 años, para formar redes con backbone ATM, utilizando fibra óptica como medio de transmisión, digitalizando totalmente los medios de transmisión.

Detrás de estos backbone se puede mantener redes ATM/MPLS, redes IP, redes Frame Relay, enlaces dedicados clear channel (TDM), etc.

La tendencia de los portadores es la de ofrecer servicio de conexión a redes IP publicas, como Red IP-VPN de Telefónica, Red Data de Telmex, y no solo ofrecer líneas dedicadas (punto a punto), con múltiples medios de acceso (TDM, ADLS, MetroEthernet, RDSI, etc.) para que el cliente pueda crear sus redes privadas, sino también el servicio de administración de los equipos de comunicación en la sede del cliente y el alquiler de los mismos. Ofrecen redes IP multiservicio (transportan datos, voz (telefonía), video), con anchos de banda desde los 64Kbps hasta los 155 Mbps, calidad de servicio (priorización por servicio), y eficiencia del 99.95%, así como el servicio de alquiler, configuración y administración de los equipos de comunicación que entreguen el servicio de red.

En el caso de SERBAN, una empresa con el 80% de enlaces punto-punto, con una red privada X.25 y SNA controlados por una infraestructura que difícilmente podría ser multi-protocolo y multi-servicio como para poder iniciar una migración a TCP/IP y sostener proyectos de integración de servicios, era necesario renovar equipos de comunicaciones y cambiar la topología de la red, de tal forma de reducir los puertos de salida y por consiguiente la complejidad de red en SERBAN.

En el mercado local se consiguieron las siguientes alternativas:

3.2.1 Propuesta de Telefónica

Telefónica plantea como solución un proyecto de outsourcing (servicio integral) a tres años por alquiler de equipos de comunicación y circuitos para el acceso a redes

públicas IP-VPN (IP/MPLS) y Meganet (X.25), y el servicio de administración de la red con las siguientes características:

- Accesos de SERBAN y nodos a red IP-VPN, para formar una intranet.
    - Nodo central (2 Mbps), con 2 ruteadores Cisco 3640, configurados en redundancia y alta disponibilidad.
    - Nodo en bancos (64 Kbps), con ruteador Cisco 2610
- Red de Comunicaciones con Cajeros Automáticos X25, enlace a Meganet de 64K con ruteador Cisco 3640.
- Solución de Respaldo de última milla con RDSI libre de costo por llamada a dos BRI 0800 en SERBAN.

En el cuadro presentado a continuación se observa una referencia de los precios por enlace, y por el alquiler y venta de equipos de Telefónica.

COSTO DE SERVICIOS DE ACCESO A RED PUBLICA IP	Costo de Instalación	Costo de Mantenimiento Mensual
Acceso a IP-VPN (2 Mbps) en SERBAN	US$ 610.00	US$ 1,060.00
Acceso a IP-VPN (64 Kbps) en cada banco	US$ 610.00	US$ 134.00
Acceso a IP-VPN (256/128 Kbps) por ADSL para ATM´s TCP/IP	US$ 210.00	US$ 110.00

COSTO DE EQUIPOS DE ACCESO A RED PUBLICA IP	Costo de Alquiler	Costo de Venta
2 Ruteador Cisco 3640 (2 FEth, WAN: 2 V.35, 4 RS232, 2 BRI) en Nodo Central	US$ 3200.00	US$ 45,200.00
N Ruteadores Cisco 2610 (1 Eth., WAN: 1 V.35, 4 RS232, y 1 BRI) para cada Institución	US$ 107.00	US$ 4,100.00
N Ruteadores Cisco 827 (1 ADSL, 1 Eth.), por ATM TCP/IP.	US$ 26.00	US$ 950.00

COSTO DE SERVICIOS DE ACCESO A RED PUBLICA X25	Costo de Instalación	Costo de Mantenimiento Mensual
Acceso a Meganet a 64 Kbps en SERBAN para ATMs X.25	US$ 119.00	US$ 320.00
Acceso a Meganet a 9.6 Kbps por ATM X.25 Lima	US$ 500.00	US$ 192.20
Acceso a Meganet a 9.6 Kbps por ATM X.25 Provincia	US$ 500.00	US$ 192.20

Cuadro 3.1. Oferta económica de Telefónica

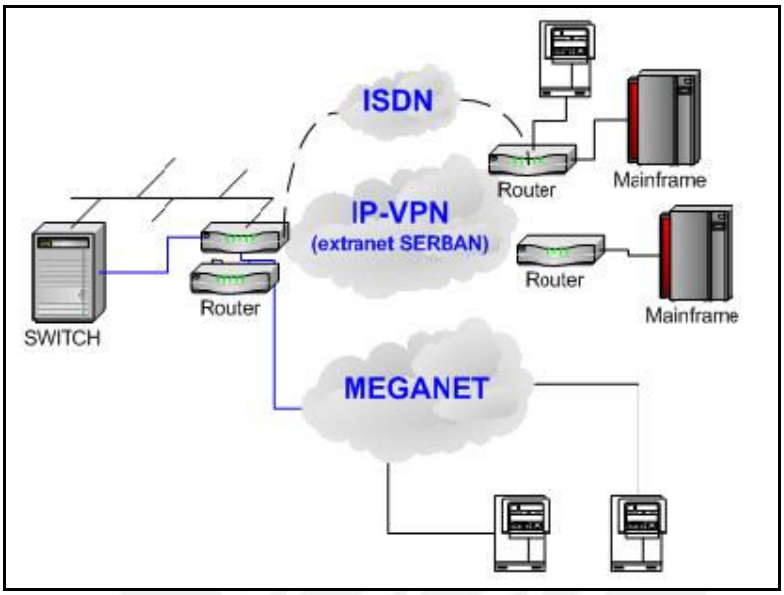

Fig. 3.8. Propuesta de Telefónica

Por esta propuesta se presentaron las siguientes observaciones:

- Costo muy elevado por outsourcing y poco flexible para los cambios posteriores en las configuraciones de la red.
- La opción de alquiler de equipos tiene un alto costo comparada con la de venta.
- El costo de la inversión y mantenimiento se eleva por el equipamiento a instalar en cada institución.

3.2.2 Propuesta de Telmex

Telmex propuso implementar una red privada multiservicio para SERBAN, sobre la cual se pueda operar una red IP, con accesos a SERBAN y a las instituciones miembros. Para garantizar la calidad del enlace usa fibra óptica como medio en la última milla.

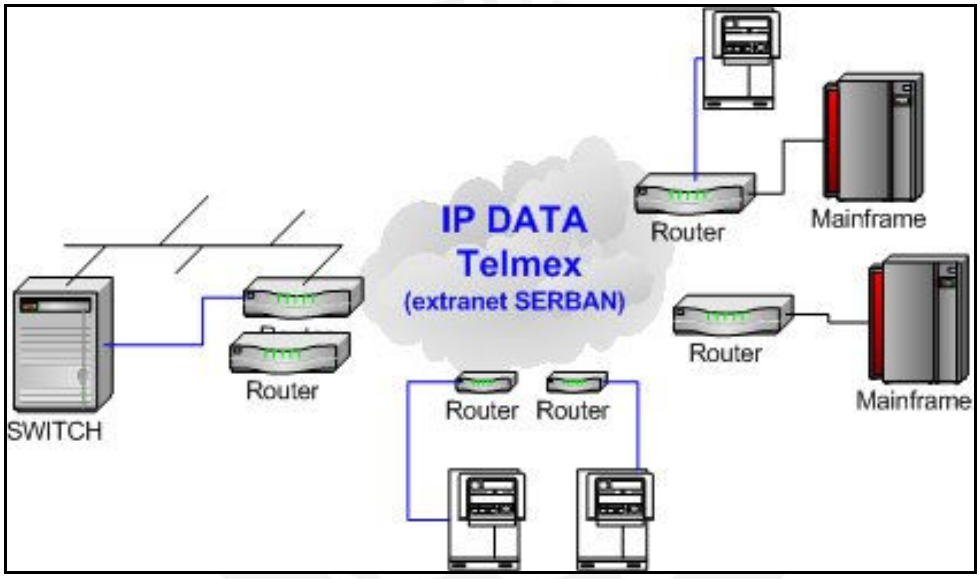

Fig. 3.9. Esquema de comunicación propuesto por Telmex.

La oferta de Telmex fue la de formar una red IP privada para SERBAN con puntos de accesos en el centro de computo de SERBAN (a 1 Mbps), en cada una de las instituciones (a 64 Kbps) y en cada cajero (a 64Kbps).

El costo de inversión y mantenimiento (Cuadro 3.2.) se elevan demasiado ya que contempla la instalación de un punto de fibra óptica y un ruteador Cisco en la ubicación de cada cajero automático. Adicionalmente, su solución no contempla la comunicación con los cajeros en provincia, ya que Telmex no tiene mucha infraestructura de red en provincia.

COSTO DE SERVICIOS	Costo de Instalación	Costo de Mantenimiento Mensual
Acceso 1 Mbps a red IP en SERBAN	US$ 910.00	US$ 910.00
Acceso 64 Kbps a red IP en cada banco y cajero.	US$ 612.00	US$ 200.00

COSTO DE EQUIPOS	Costo de Alquiler	Costo de Venta
2 Router Cisco 3662 en nodo central (2 FEth, WAN: 2 V.35, 4 RS232, 8 BRI).	US$ 615.24	US$ 36,985.00
N Router Cisco 2611 en bancos (1 Eth, WAN: 1 V.35, 3 RS232, y 1 BRI)	US$ 216.43	US$ 6,679.00
N Router Cisco 1605 en cajeros (1 Eth, WAN: 1 RS232)	US$ 90.50	US$ 1,450.00

Cuadro 3.2. Oferta económica de Telmex

3.2.3 Alternativa de acceso por red Celular

Dentro de la tecnología de redes celulares se revisó el CDPD (Cellular Digital Packet data). Este es un servicio de paquetes de datos para los sistemas AMPS/TDMA. CDPD es una red de datos que aprovecha los remanentes de los anchos de banda de la telefonía celular TDMA de Telefónica Móviles (ex red BellSouth). Se considera como una red IP con velocidades en los puntos de acceso hasta 19.2 Kbps. El punto de acceso al SWITCH sería a través de un circuito dedicado de 64Kbps a la red de datos de la empresa portadora y de ésta se tienen enlaces a módems inalámbricos de 19,2 kbps que se conectan a los cajeros con puertos seriales (si fuera X25) o ethernet (si fuera TCP/IP).

Los costos se pueden observar en el Cuadro 3.3.

Los precios son muy competitivos con los de Telefónica, para enfrentar el problema de comunicación de los cajeros automáticos en Lima.

	Instalación	Mensualidad
Enlace HDSL a BellSouth (64 Kbps)	US$ 600.00	US$ 220.00
Enlace CDPD (19.2 Kbps) por ATM	US$80.00	US$ 80.00
Alquiler de módem / ruteador por ATM	-	US$ 60.00

Cuadro 3.3. Costo de CDPD

En este caso los módem inalámbricos operan a la vez como ruteadores, y en algunos casos cuenta con interfases X.25 (si la conexión con el ATM así lo requiere), es decir, no necesitan equipos adicionales para la comunicación con el cajero.

El esquema en mención es aplicable para cualquier tipo de cajero, sin cambiar hardware ni software. Sólo se debe considerar que en lugares donde exista posible interferencia, o baja señal de radiofrecuencia se deberá usar antenas Yagui externas.

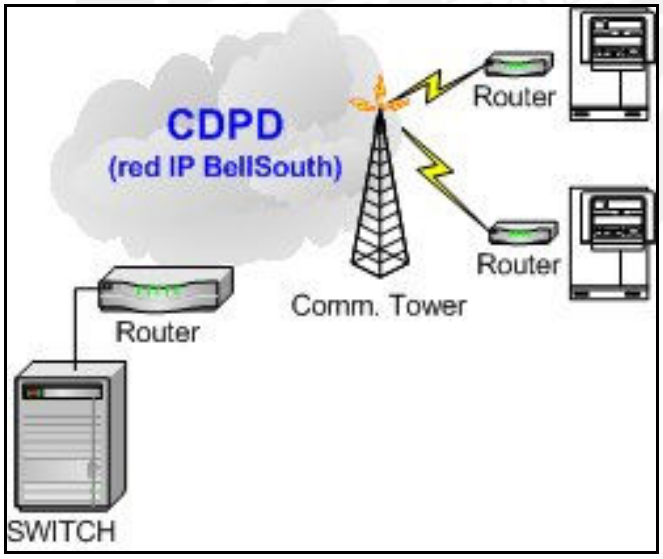

Fig. 3.10. Esquema de comunicación celular CDPD.

Soluciones similares a ésta, en cuanto a usar la red celular, se pueden plantear con otros proveedores de red celular GSM o CDMA, siempre teniendo en cuenta que:

- La red de cajeros es transaccional es decir no tiene mucho trafico. Las redes celulares al manejar en algunos casos criterios de cobro por tráfico y no por tiempo de conexión pueden ser de un costo conveniente.
- La red de transporte de datos de la red celular es IP, por lo cual si es necesario se debe buscar que el equipo Terminal efectúe la traslación al protocolo final (p.e. X.25).

3.2.4 Alternativa de Bancared de Asbanc

Bancared es la red formada por los bancos miembros de ASBANC (Asociación de Bancos del Perú), y que utiliza la red ATM de Telmex para brindar acceso a sus asociados (los bancos del Perú) a sus proveedores comunes, como entidades de servicios, de riesgos, de gobierno, etc. (por ejemplo Certicom, Sunat, Sunad, Edelnor, Luz del Sur, etc.). Bancared podía ofrecer a sus miembros (socios y proveedores) un servicio que consistía en:

- Acceso a Bancared a 1 Mbps
- Alquiler de un ruteador Cisco 2611, con dos interfaces ethernet, un NM con 4 puertos de anexo extendido (FXS), y un puerto BRI.
- Alquiler de una línea BRI ISDN contratada a Telefónica para la contingencia del enlace principal.
- Servicio de 4 líneas de anexos extendidos, para la comunicación de voz entre los miembros.
- Libre establecimiento de circuitos virtuales entre miembros.

Bajo este esquema se estaría pagando un monto por el concepto de instalación y otro por mantenimiento mensual.

	Instalación	Mensualidad
Servicios de Bancared	$ 1500.00	$ 600.00

Cuadro 3.4. Costos de Bancared de Asbanc.

Ya que Bancared cuenta con accesos establecidos a cada uno de los bancos miembros de SERBAN, se podría considerar esto como la alternativa de red privada ofrecida por Telmex a SERBAN, pero sin el costo por instalación y mantenimiento en cada uno de los bancos miembros.

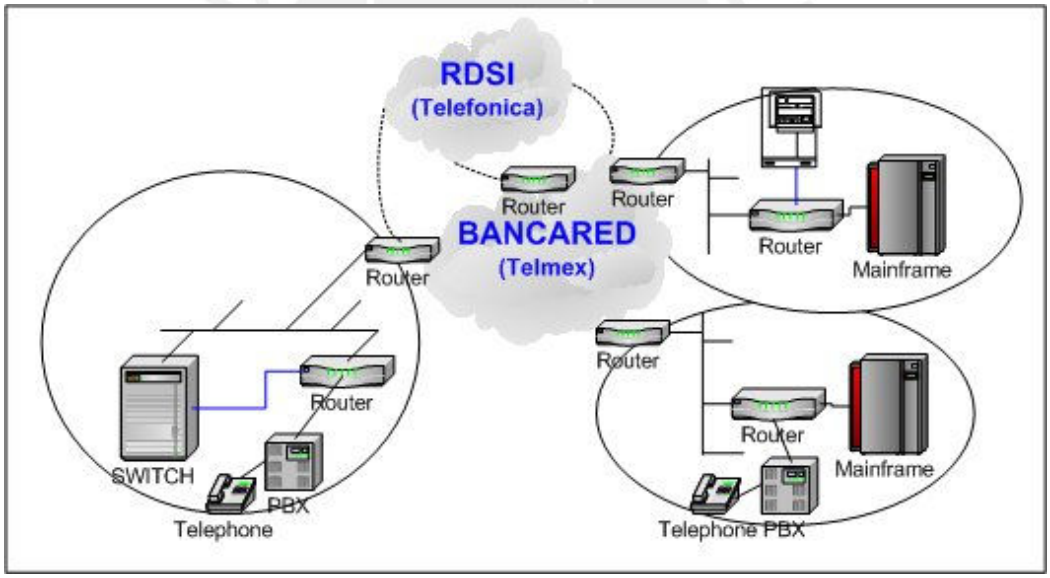

Fig. 3.11. Esquema de comunicación con Bancared.

La desventaja frente a la propuesta de Telmex, es que el ruteador de Bancared instalado en cada miembro no cuenta con puertos seriales para la conexión a equipos con protocolos X.25 y SDLC/SNA, por lo que se debe usar otros ruteadores de propiedad de los miembros. Para estos servicios es necesario utilizar equipos internos.

3.2.5 Integración con las redes privadas de las instituciones.

Como se explicó al inicio, la red de SERBAN planteaba mantener una red privada, lo cual significaba mantener una instalación de red en cada una de las agencias de las instituciones en donde se tenga un cajero automático y en cada centro de cómputo en donde esté el host emisor de la institución. Ese costo lo tenía que asumir el banco, si el cajero era de su propiedad, lo cual significaba un costo doble, ya que el banco tenía una red establecida en la misma agencia.

Se plantea esta alternativa para las instituciones que tienen cajeros automáticos en sus agencias, y deseen transportar en su red (desde su sede central hasta la agencia destino) el tráfico del cajero. No es una solución para los cajeros instalados en puntos neutros.

Para lograr esto se debe verificar lo siguiente en la red de las instituciones y SERBAN:

- Deben estar basadas en el protocolo TCP/IP.
- Deben poder establecer e implantar políticas de seguridad en sus redes.
- Deben poder configurarse puertos seriales con protocolos como el X.25 (en agencias) y SDLC (en la sede principal) en los equipos ruteadores de la institución.
- Debe existir un adecuado soporte de comunicaciones con cobertura 7x24 y herramientas de gestión que lo apoyen.
- Se debe establecer un enlace entre SERBAN y la institución, con soporte a TCP/IP y con el ancho de banda necesario para el tráfico de cajeros, host, y otros servicios.

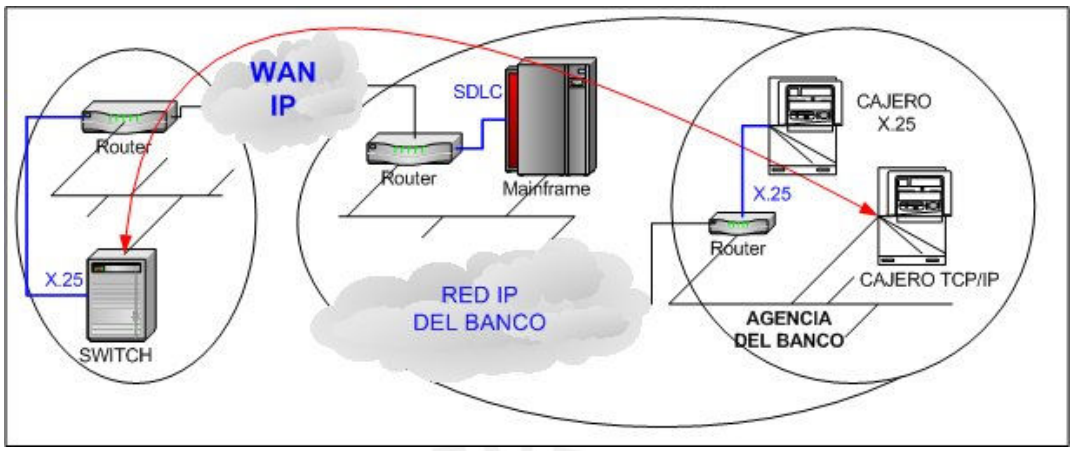

Fig. 3.12. Esquema de comunicación usando las redes privadas de los bancos.

Si bien con esta opción SERBAN prescinde de tener una red propia, los costos para la propia empresa y para sus miembros se reducen enormemente, quienes finalmente pueden tener mayores beneficios y aumentar su red de cajeros a menor costo.

	Marca / Modelo	Costo
Ruteador con puerto serial	Cisco 831, con 1 puerto ethernet y un puerto WIC (RS232)	US$ 1100.00
Modulo de puerto serial en el ruteador de la agencia	Módulo WIC (RS232) para ruteador Cisco	US$ 300.00
Par de short-modem banda base y corta distancia.	SRM-6S marca RAD	US$ 300.00

Cuadro 3.5. Costos asociados a la integración a otras redes, para el caso de un ATM X.25.

La comunicación con los cajeros automáticos puede llegar a ser la más compleja por el número de equipos, por su dispersión geográfica, con alcances nacionales, por los problemas de seguridad que habría que enfrentar y por las facilidades que el banco debe brindar a SERBAN.

Para lograr la integración de redes a nivel TCP/IP es necesario subir los protocolos como X25 y SNA a la capa TCP, de tal manera que se les pueda transportar. Sólo en esos casos se requiere de una inversión por parte del propietario del cajero, la Institución o SERBAN en uno o más de los siguientes equipos:

3.2.6 Recomendación para la contratación de enlaces

Las propuestas descritas tienen puntos que se complementan entre sí para dar solución a una nueva red que permita reducir costos a todos los miembros y lograr una mayor concentración de servicios que permita recuperar con pocos enlaces la mayor parte del servicio, si los enlaces principales sufren una contingencia.

La solución de acceso con las instituciones tiene dos variantes:

- El acceso por Bancared para las instituciones miembros de Asbanc.
- El acceso por IP-VPN de Telefónica para los demás miembros.

En las sedes principales se tendría instalado el ruteador de acceso, en donde estarían terminando los servicios de comunicación con el host (computador emisor bajo SNA o TCP/IP, el cajero de la sede principal entre otros.

Si las instituciones lo permiten, se usaría su red privada para establecer comunicación con los cajeros instalados en sus oficinas, ya sea con TCP/IP directamente o con XOT (X.25 sobre TCP).

Si no fuera posible, o si el cajero estuviera ubicado en puntos neutros (sin instalación de la institución), se usaría una de las siguientes alternativas:

- Si el cajero sólo tuviera soporte de X.25, se instalaría con acceso a Meganet a 9.6 Kbps. (en Lima y Provincias).

- Si el cajero tuviera soporte a TCP/IP, se instalaría con un punto de acceso a IP/VPN con ADSL (en Lima y provincias).

Una visión global de los enlaces es la que se presenta en el siguiente diagrama (Fig. 3.13), en donde se observa que las conexiones con las instituciones y cajeros prescinden de los circuitos dedicados punto a punto de Digired.

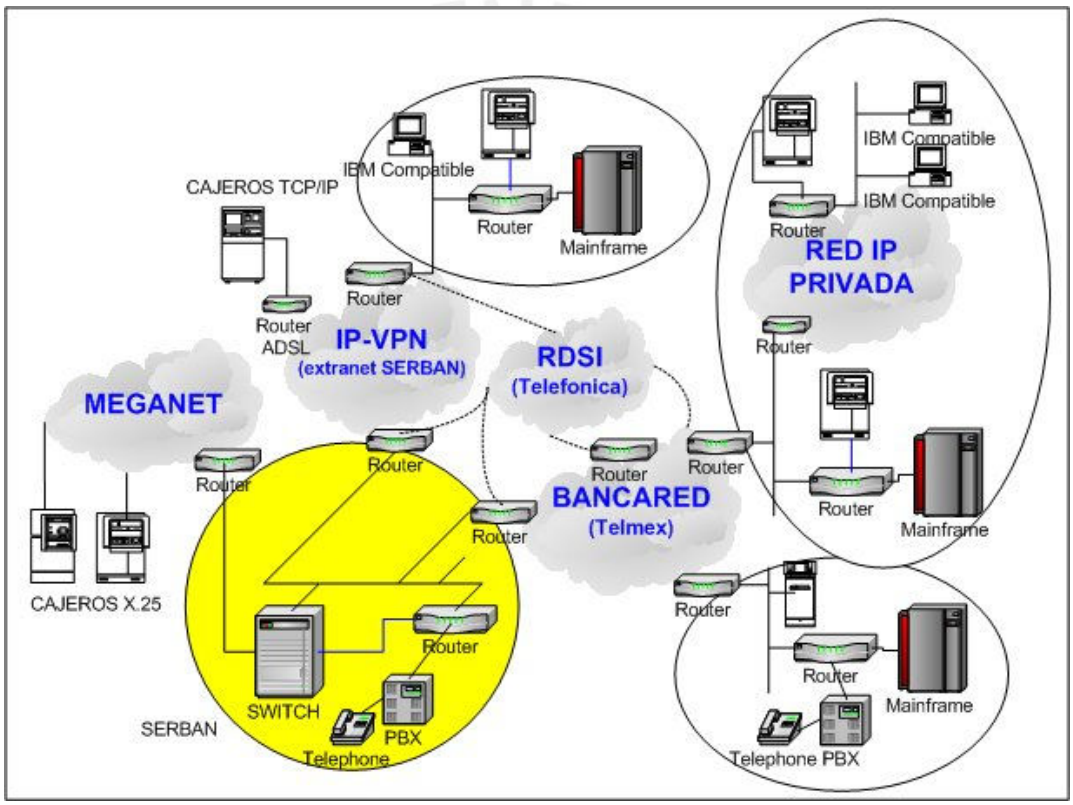

Fig. 3.13. Esquema de comunicación recomendado.

3.3 Renovación de la Infraestructura de Comunicaciones y Seguridad

Se tenía claro que con equipos concentradores PADs, con mas de 7 años de antigüedad, con solo interfases seriales, sin soporte a TCP/IP y sin mayor escalabilidad de software, no se podían obtener mayores logros. El nuevo sistema debía estar conformado por:

- Ruteadores multiprotocolo,
- Switches para la redes LAN,
- Una solución de administración de red,
- Un firewall que segmente la red a nivel capa 3 y proteja las red de servidores de producción de las redes externas.
- Una solución de detección de intrusos, exigida por los auditorias de seguridad bancarias,

que como sistema ofrezcan características de disponibilidad, confiabilidad, servicio y rendimiento acorde con los requerimientos de redes de misión crítica.

3.3.1 Ruteadores y Switches

Se recomendó la adquisición e instalación de dos ruteadores para soportar el tráfico de los host emisores bajo protocolo SNA (transacciones financieras, transferencia de archivos, entre otros) y el tráfico de los cajeros bajo protocolo X25, y su encapsulación a TCP/IP, con las siguientes características:

- Procesador de alta capacidad, características modulares y de alta disponibilidad (doble fuente de poder, hot swap de módulos, etc.)
- Interfaces Soportadas:

- Hasta 24 puertos Seriales, con soporte a RS232, V.35 y RS422.
- 02 puertos ethernet 10/100BASET
- 08 puertos BRI (para contingencia)

- Software de comunicaciones con soporte:
  - Multiprotocolo: TCP/IP, HDLC, SDLC, PPP, X25, XOT, Frame Relay, SNA y variantes - DLSw, SDLC, conversión SDLC a LLC2 (QLLC), etc.
  - Protocolos de ruteo (RIP, IGRP, etc.)
  - Seguridad (listas de acceso, VPN).
  - Alta Disponibilidad (VSRP, HSRP)
  - Administración (SNMP y RMON)

Se revisaron propuestas de equipos Cisco (Cisco 36xx), Nortel (Passport 54xx) y Motorola (MPR65xx). Si bien todos cumplían con los requisitos técnicos, los equipos Cisco contaban con mayores ventajas.

Desde hace algunos años, predomina en el mercado de equipos de comunicación la marca Cisco, fabricantes de equipos ruteadores, switches, soluciones de Voz sobre IP, concentradores VPN, firewalls, etc. No solo es la marca predominante en las ofertas de proveedores, es la que tiene mayor soporte de fabricante –con presencia local- y de los proveedores, también es la marca con mayor número de instalaciones en las instituciones financieras, lo cual asegura una compatibilidad cuando se trata de configurar funcionalidades especiales entre dos equipos como XOT y DLSw. Marcas de ruteadores como Motorola, Nortel, entre otras, siempre fueron ofrecidas como segunda opción en las propuestas solicitadas a los proveedores, y sin muchas ventajas de post-venta.

Se seleccionó y se recomendó la adquisición de dos ruteadores Cisco 3662, para configurarlos como redundantes entre sí y con características de alta disponibilidad.

Entre sus características técnicas, y razones por las que fue elegido, se pueden resaltar:

- Poseen un procesador RISC de 225 Mhz, 16Mb de flash, 64Mb DRAM, con una performance de 120 Kpps.
- Poseen dos fuentes de poder redundante,
- Poseen doble puerto fast ethernet,
- 6 slots para NM (network modules), entre los cuales se puede instalar diversos módulos o interfaces de red que lo hacen un equipo escalable y flexible:
    - Módulos NM con 8 puertos RDSI para la recuperación automática de enlaces.
    - Módulos NM-8AS con 8 puertos seriales, con cables con interfaces RS232, V.35 y RS422.
- Compatibilidad de módulos, y recuperación de los mismos en caliente (Hot Swapping).
- Capacidad de crecimiento (escalabilidad en hardware y software).

Fig. 3.14. Vista posterior de un ruteador Cisco3662.

Para mejorar la interacción de los ruteadores con la red de área local, se recomendó la compra de dos LAN Switch de borde de configuración fija de puertos, que tuvieran las siguientes características:

- Conmutación de capa 2 para zona de acceso, con puertos fast ethernet (24) y puertos gigabit ethernet (2) modulares (100BaseT de cobre o 100BaseSx de fibra).
- Equipo apilable, funcionamiento aislado y posibilidad de formación de cluster con otros equipos.
- Servicios avanzados:
    - Advanced QoS 802.1p, Enhaced security features, administración sofisticada de multicast.
    - Configuración de VLAN 802.1q, ISL.; listas de acceso, y VLAN trunking protocol (VTP).
    - Alta disponibilidad STP, IGMP
    - Alta seguridad: 802.1x, port security, MAC address notification, Radius, TACACs+.
    - Administración CLI, Web, SNMP y CMS (cluster management suite).
    - Puerto de monitoreo SPAN.

Por las mismas razones expresadas líneas arriba, se prefirió seleccionar un modelo entre los equipos marca Cisco. Se seleccionaron los equipos Cisco Catalyst 2950G, los cuales son equipos de borde de alto desempeño con todas las características requeridas.

3.3.2 Administración de la Red

Se necesita un sistema de administración de red global, tanto para los equipos de comunicación y servidores locales como para los equipos y servidores remotos en los bancos, bajo control de SERBAN.

La plataforma deben soportar las siguientes características básicas:

- Soporte SNMP, y reconocimiento de traps SNMP (filtros, generación alertas, etc.)
- Capacidad de descubrimiento de red.
- Capacidad de crecimiento y modularidad, para incorporar elementos y aplicaciones diversas relacionadas con la gestión.
- Configuración personalizada por cada dispositivo
- Recolección remota de estadísticas.
- Log de eventos y alarmas.
- Notificación por correo, sonido, etc. de alertas.
- Visualización remota del estado de los indicadores luminosos de los equipos Cisco.
- Control de seguridad (múltiples niveles de acceso, y perfiles de usuario)
- Apoyo en interfaz gráfica (GUI) e interfaz Web.

En el mercado existen soluciones disponibles que tienen una alta capacidad de crecimiento, pero a su vez son de alto costo. Es el caso de soluciones de HP Open View y Computer Associates. Cisco Systems por su parte tiene soluciones para redes pequeñas y medianas que permiten cubrir con los requerimientos y además poder visualizar y controlar al detalle los dispositivos de la misma marca.

La solución CiscoWorks 5.0 for Windows de Cisco, presenta dos módulos, el WhatsUpGold (WUG) que es el módulo de gestión de red y consola SNMP y el CiscoView que es el módulo de administración de los dispositivos Cisco. Este último permite una integración excelente con toda la gama de equipos Cisco, para un monitoreo y control muy intuitivo para operadores con poco conocimiento en programación de equipos Cisco. Ambos, de fácil configuración, se ajustan a los requerimientos descritos a un precio razonable.

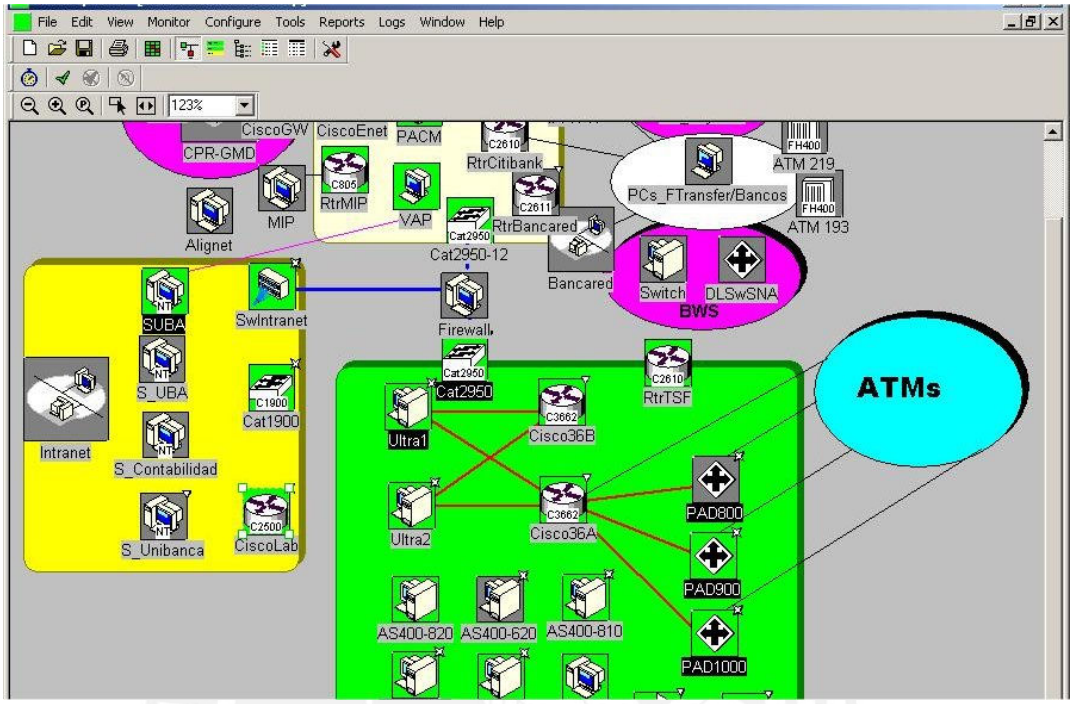

Fig. 3.15. Software CiscoWorks, módulo What´s Up Gold.

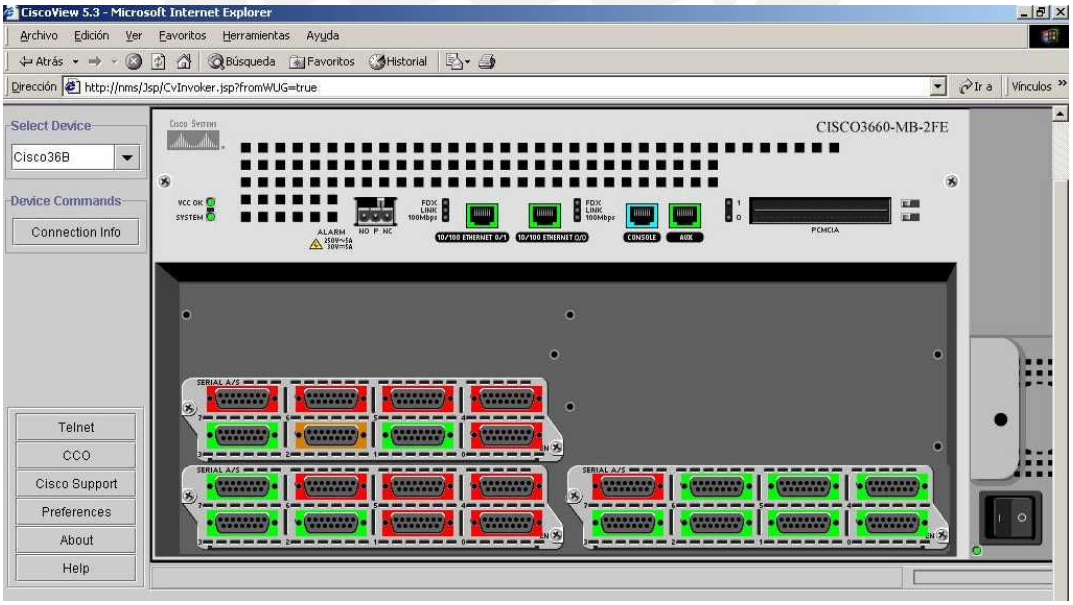

Fig. 3.16. Software CiscoWorks 5.0, módulo CiscoView con la vista posterior de un ruteador Cisco3662.

El módulo WhatsUpGold (WUG) permite descubrir la red, y registrar cada dispositivo de red como un objeto con diferentes niveles de administración según lo permita. Este programa, levanta un pequeño servidor Web que permite el monitoreo remoto usando sólo un navegador.

El servicio entregado a las instituciones financieras exige una disponibilidad del 99.8% mensual, es decir que la atención de la red debe ser de 24 horas al día, durante todo el año. Esta medición se efectúa con los reportes de disponibilidad que ejecuta la aplicación del Switch, pero también debe ser suministrada por los reportes estadísticos de la consola de gestión. En este caso el CiscoWorks puede generar un reporte para medir los niveles de disponibilidad.

Para la adquisición de la nueva infraestructura se solicitó cotizaciones a tres proveedores de equipos Cisco en el mercado local, a quienes se les solicito incluyeran en su oferta el mantenimiento preventivo y correctivo. Las ofertas económicas fueron las presentadas en la Cuadro 3.6.

	Telmex	Telefónica	GMD
Ruteador Cisco3662	US$ 42981.43	US$ 39,366.00	US$ 39,714.00
Switch Catalyst 2950	US$ 1701.35	US$ 1,615.95	US$ 1,662.35
CiscoWorks 5.0	US$ 1701.35	US$ 1,929.41	US$ 2,078.98
Inversión total	US$ 46,383.83	US$ 42,911.36	US$ 43,455.33
Mantenimiento Mensual	US$ 364.13	US$ 420.00	US$ 277.66

Cuadro 3.6. Resumen de ofertas para compra de equipos de red.

Para realizar la evaluación técnica-económica se tomaron los siguientes criterios de selección:

- Costos de inversión y mantenimiento.

- Tecnología (escalabilidad, flexibilidad, compatibilidad, presencia en el mercado)
- Alta disponibilidad (en equipos y configuración)
- Soporte a pruebas (participación en pruebas de laboratorio)
- Soporte y Mantenimiento (experiencia, y tamaño del staff)
- Proveedor (presencia local, capacidad de negociación).

De los cuadros revisados, y por puntajes otorgados a cada uno según los criterios de selección, se optó por la propuesta de la empresa GMD S.A.

Adicionalmente los proveedores de servicio, de las redes Bancared (Telmex) e IPVPN (Telefónica), entregan herramientas de monitoreo en sus portales web que permiten revisar el ancho de banda consumido por día, semana, y mes, lo cual permite efectuar controles y administrar adecuadamente el recurso disponible.

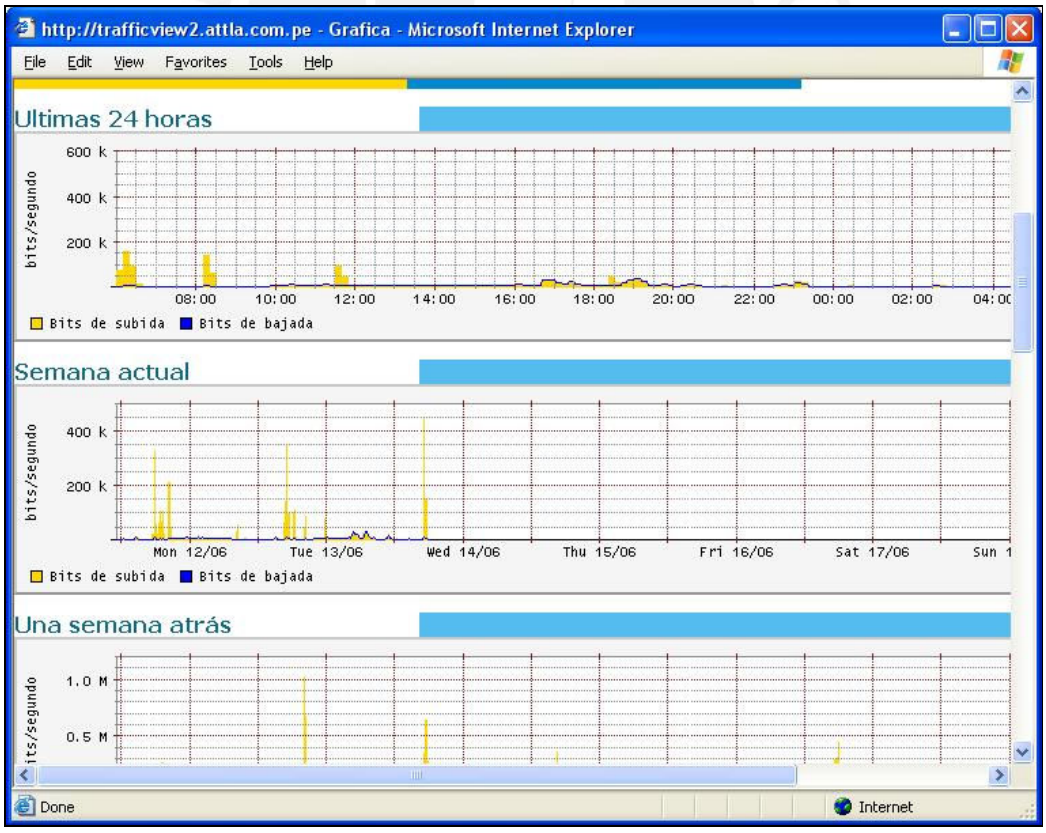

Fig. 3.17. Software TrafficView en portal de Telmex, para la medición del ancho de banda de Bancared.

3.3.3 Elementos de Seguridad

3.3.3.1 Firewalls

Si bien SERBAN contaba con un firewall para el acceso a Internet, este solo era para proteger una única zona de confianza (red de computadoras personales de usuarios y servidores de producción) de la zona de Internet. Solo algunas computadoras personales tenían definido una puerta de enlace por defecto (el equipo firewall).

Para iniciar los servicios TCP/IP con otras instituciones se debe separar la zona de red de confianza, en cuatro zonas o subredes, dos de ellas nuevas:

- Una nueva zona de red de Producción, en donde permanecerían los servidores de producción.
- Una nueva zona de red de Extranet, en donde se ubicarían a los ruteadores de acceso a Bancared, IP/VPN, y otras redes de socios de negocio o clientes como por ejemplo VISA y Mastercard, con los cuales se debe mantener un control de seguridad.
- La zona Intranet, en donde estarían las computadoras personales de SERBAN y los servidores de oficina, como el servidor de correo, servidores de archivos, y de contabilidad/logística. Esta es la única zona que podría tener acceso con Internet.
- La zona de Internet, o zona “no segura”.

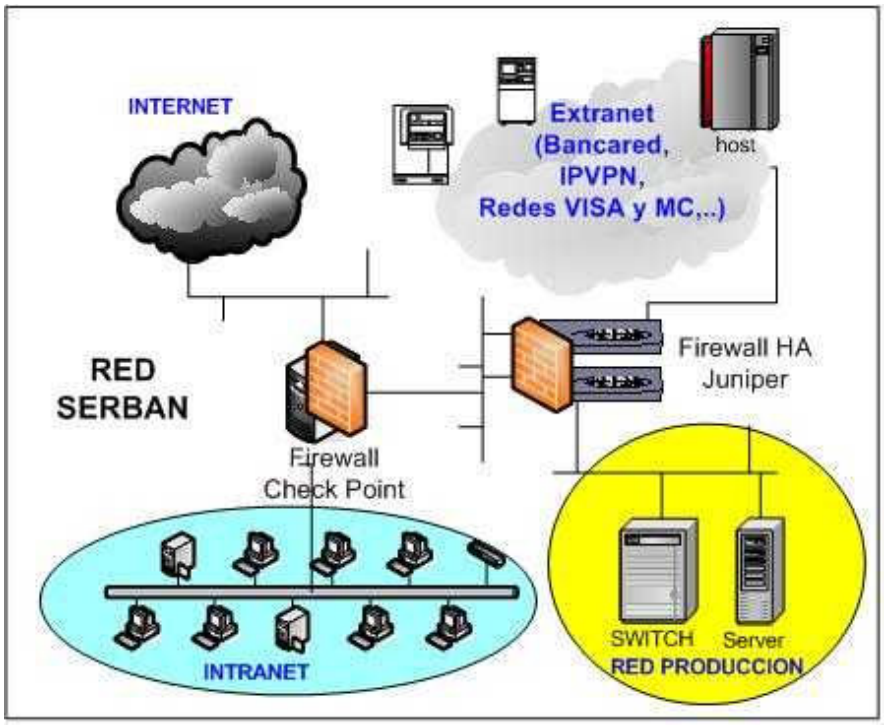

Fig. 3.18. Esquema de seguridad de SERBAN por zonas o subredes.

Para lograr esta división de zonas o subredes, con controles de accesos y enlaces entre una y otra zona, se debe instalar una solución de cluster (agrupamiento) de firewalls de alta disponibilidad entre las zonas extranet y producción, y para los accesos entre las zonas Internet e Intranet, potenciar el firewall CheckPoint en uso. Todos los equipos deben haber sido certificados por NCSA o ICSA. Los detalles de los cambios serían los siguientes:

- Firewall Internet/Intranet: el firewall en uso era un Check Point Firewall-1 v4.0 con licencia para 50 usuarios, instalado sobre un servidor IBM Netfinity con Windows NT 4.0, y con dos interfaces de red. Se renovaría la licencia de firewall a una nueva versión de firewall Check Point Express NG con soporte de VPN, y se cambiaría a un nuevo equipo con un sistema operativo confiable.
- Firewalls Extranet/Producción: el cluster de firewalls a instalar entre estas zonas asegura una alta disponibilidad y alta seguridad de equipos firewall en una

plataforma robusta con mínimo 4 interfaces de red, que diera soporte a un mayor número de usuarios y que tenga la funcionalidad de crear VPNs.

El producto a actualizar, el Check Point Express, es un firewall líder en el mercado con la tecnología "Stateful Inspection" (inspección de estado) el cual revisa los paquetes en varias capas de la comunicación (sobre la capa3: nivel de red). El producto Incluye varios módulos de software:

- Gateway VPN-1 Express: administrador de redes privadas virtuales (VPN) site-to-site (entre instituciones) o client-to-site (desde PC cliente usando software propietario). Adherido a la norma IPSec, negocia automáticamente el cifrado y algoritmos de autenticación de datos más complejos posibles entre los comunicantes. Esto incluye la norma de cifrado avanzado (AES) de 128-256 bits y los algoritmos de cifrado de datos Triple DES de 56-168 bits. Su facilidad de uso es su principal fortaleza.
- FireWall-1: módulo de firewall. brinda múltiples niveles de control de acceso, compatible con más de 150 aplicaciones, servicios y protocolos predefinidos, incluidas las aplicaciones Web, mensajería instantánea, aplicaciones de comunicación entre nodos de igual nivel, voz sobre IP, Oracle SQL, RealAudio y servicios multimedia. Permite la autenticación de usuarios localmente, o apoyado por servidores externos, tipo Radius, LDAP, RSA, etc.
- SmartCenter: consola centralizada de administración para múltiples módulos, con excelente presentación GUI, permite una administración eficiente de los logs, así como establecer múltiples filtros.

Este software sería instalado en un nuevo equipo con un sistema operativo Linux Red Hat "hardeneado" o asegurado por el mismo Check Point, de tal manera que sólo tenga los servicios y aplicaciones necesarias para su funcionamiento.

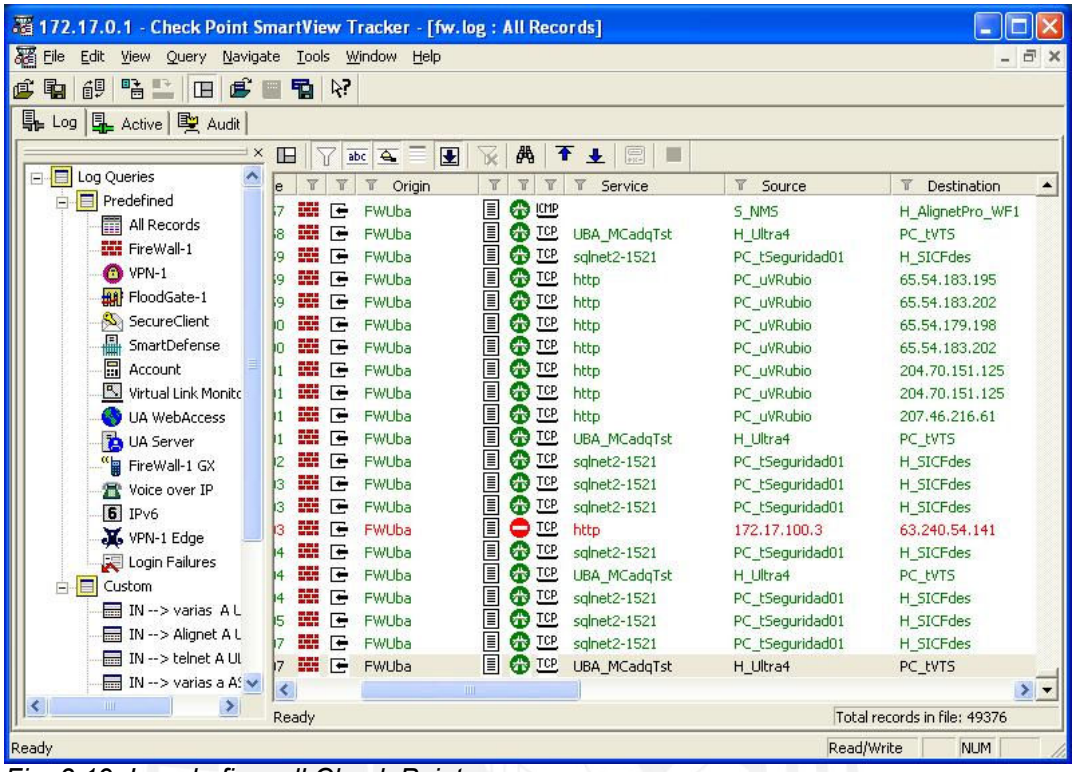

Fig. 3.19. Log de firewall Check Point.

El firewall Check Point debe asociarse con el directorio Active Directory (LDAP) del dominio Windows en la Intranet, de tal forma que se active la autenticación de usuarios por cada conexión establecida a los equipos servidores de producción, para la consulta o actualización en las aplicaciones. De esta forma también se tiene un control por acceso de cada usuario a los equipos de producción.

El equipo recomendado como plataforma de hardware para el firewall Check Point, es un eServer IBM x226 Intel Pentium Xeon 3Ghz / 512Mb RAM / HDD 80Gb / 4 ptos. ethernet 10/10/1000. La propuesta económica por el upgrade del firewall Check Point y por el nuevo servidor que lo soporta es la que sigue:

	Proveedor	Inversión	Mantenimiento Anual
Hardware: Server IBM x226	Cosapisoft	US$ 2,650.00	
Software: Check Point Express NG 50 IPs	CosapiSoft.	US$ 3,875.00	US$ 525.00
Total		US$ 6,525.00	US$ 525.00

Cuadro 3.7. Oferta por la actualización de hardware y software de firewall para Internet

Para el segmento Extranet/Producción se propuso un par de equipos firewall marca Juniper, modelo Netscreen 25 Baseline, configurados en alta disponibilidad (HA o High Availability). Estos se comercializan como equipos en appliance (equipo de red con el software aplicativo incluido), con las siguientes características:

- Capacidad de procesamiento de 100 Mbps.
- Capacidad de encripción en TripleDES de 20 Mbps.
- Soporte de 24,000 sesiones simultaneas, y usuarios ilimitados
- Soporte hasta 4 interfaces de red.
- Modos de funcionamiento: transparente (tipo Switch capa 2), y modo ruteador (para configuración FWW + VPN, permite enrutar tráfico entre túneles).
- Sistema operativo propietario RealTimeOS, permite creación de reglas de políticas de seguridad entre zonas de entrada y salida.
- Permite formación de diferentes tipos de redes VPN usando IPSec (P2P, Hub&Spoke, Full Mesh), o L2TP sobre IPSec.
- Permite autenticación de usuarios, registro de cambios efectuados por administrador, administración vía https y ssh (entre otros), notificación de eventos y registros de eventos en syslog o en el NMS, software de gestión propio, soporte de alta disponibilidad.

Para el funcionamiento de la alta disponibilidad utiliza el protocolo propietario NSRP, el cual permite trabajar a un equipo en modo activo y al otro en modo pasivo, con una sola dirección IP reconocida por la red. Cada uno tiene su dirección IP para administración, encargando el NSRP de sincronizar los cambios efectuados entre los equipos así como enviar información entre ellos sobre el estado de las interfaces.

Con este esquema de trabajo se puede apagar uno de los equipos para mantenimiento sin afectar a los usuarios, y sin perder conexiones.

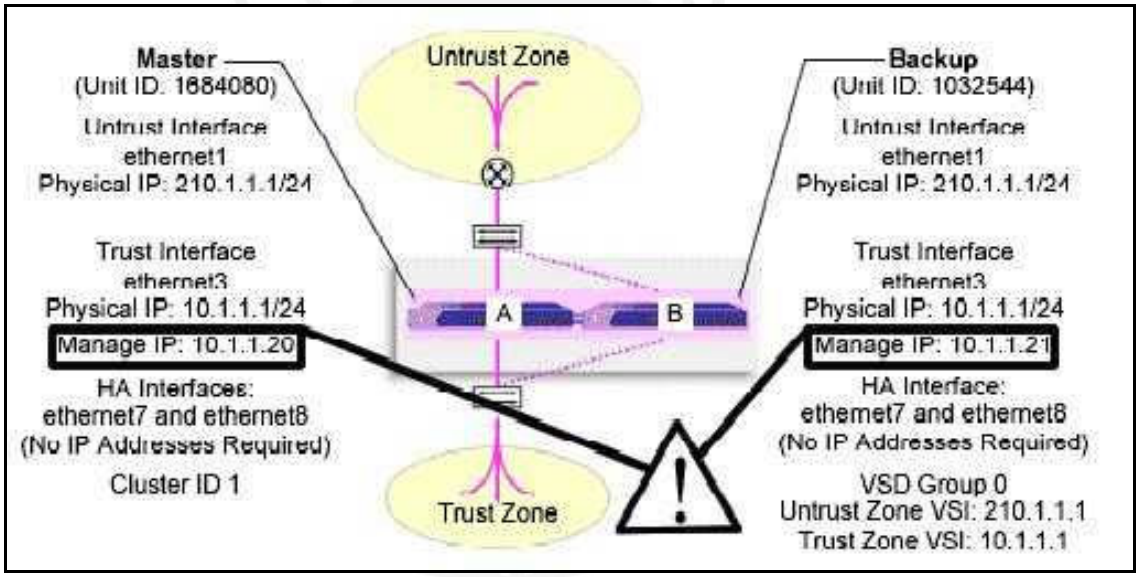

Fig. 3.20. Esquema de alta disponibilidad (HA) de firewalls Juniper.

Una de las grandes ventajas con estos equipos es su bajo precio comparado con equipos de la misma capacidad de la marca Check Point. En el cuadro 3.8 se puede apreciar que el costo por dos equipos Juniper en alta disponibilidad y para usuarios ilimitados es muy similar al de un solo equipo Check Point limitado para 50 usuarios (incluyendo servidor).

En resumen, para el equipamiento de equipos firewall, se consideró como mejor oferta para renovación de equipos Check Point a la de Cosapisoft y a la de Trendcorp, para la compra de equipos Juniper.

	Proveedor	Inversión	Mantenimiento Anual (SW)
Dos (2) equipos Juniper Netscreen-25 Baseline	Trendcorp	US$ 5,700.00	US$ 600.00
	Adexus	US$ 6,000.00	US$ 1000.00

Cuadro 3.8. Oferta de compra de dos equipos firewall en HA para el segmento Extranet/Producción.

3.3.3.2 Sistemas de Detección de Intrusiones.

Mientras los firewall efectúan los trabajos de control de acceso, autenticación, segmentación de red y algún nivel de protección DoS, los equipos de detección de intrusiones son la segunda capa de defensa, proveen monitoreo y prevención de ataques mediante detección de patrones conocidos (firmas de ataques) o anomalías de protocolo, y posterior rechazo de conexiones.

En el mercado los más reconocidos son los equipos de las marcas Juniper (equipos IDP-10, IDP100, según el nivel de tráfico) e ISS (con los equipos Proventia G-100).

Los equipos Juniper IDP-10 consisten en un módulo sensor instalado en modo bridge entre el ruteador de Internet y el firewall de control de acceso (que efectúa el trabajo de sensado de la red, y actúa sobre las conexiones TCP), y un servidor Linux Red Hat (disponible en la red) con el software de administración, el cual se encarga de administrar la configuración del sensor, cargarla al sensor cuando se encuentran listas, revisar y descargar las actualizaciones de firmas de ataques en Internet, y recibir de el sensor los registros de los eventos que pudo encontrar en el trafico de la red y las

acciones que tomó sobre ella. Asimismo, el software cliente de administración (GUI), se conecta a la consola de administración con el fin de efectuar los ajustes a la configuración de las reglas de la políticas de seguridad, de acuerdo al origen y destino de las conexiones, los puertos de servicio utilizado, y una calificación sobre los tipos de ataques que se podrían recibir, y las acciones a tomar por el sensor. El módulo de administración puede generar estadísticas y reportes básicos y personalizados.

El equipo de ISS, Proventía G100, trabaja de modo similar, sólo que en el mismo equipo sensor se incluye el módulo de administración para conexión vía html (bastante más limitada que la de Juniper), dejando a un tercer equipo para la recolección de los logs, y generación de estadísticas con un motor de base de datos externos.

Ambos equipos tienen las mismas capacidades de defensa basada en firmas y anomalías de tráfico (ataques de DNS, incumplimiento de protocolos, vulnerabilidades específicas de aplicaciones, troyanos, puerta trasera y administración remota, código móvil (JavaScript, Active-X), extensión de archivos oculta, gusanos de http: Code Red, Nimda), así como interceptación de diferentes ataques de red:

- Ataques de denegación de servicio DoS: SYN Flood, LANd.
- Ataques de IP: Disfraz de IP, Ataques mediante fragmentación de IP,

	Proveedor	Inversión	Mantenimiento Anual
Juniper IDP-10	Adexus	US$ 10,500.00	US$ 1600.00
ISS Proventia G100	CosapiSoft.	US$ 12,200.00	US$ 2800.00

Cuadro 3.9. Oferta por la compra de un sistema de detección de intrusiones.

Según lo observado en el cuadro 3.9, los costos de inversión y de mantenimiento del equipo de Adexus son menores. Asimismo, son mejores las facilidades de

administración, de generación de estadísticas y de reportes del equipo Juniper ofertado por Adexus S.A., por lo cual queda seleccionado.

En la Fig.20 se observa el esquema final de SERBAN luego de implantar todas las recomendaciones expresadas en el presente capitulo, como son la compra de infraestructura de comunicaciones, los equipos de seguridad y la segmentación de la red, y la nueva contratación de accesos a redes IP, así como la conexión de terminales a través de las redes privadas de los bancos.

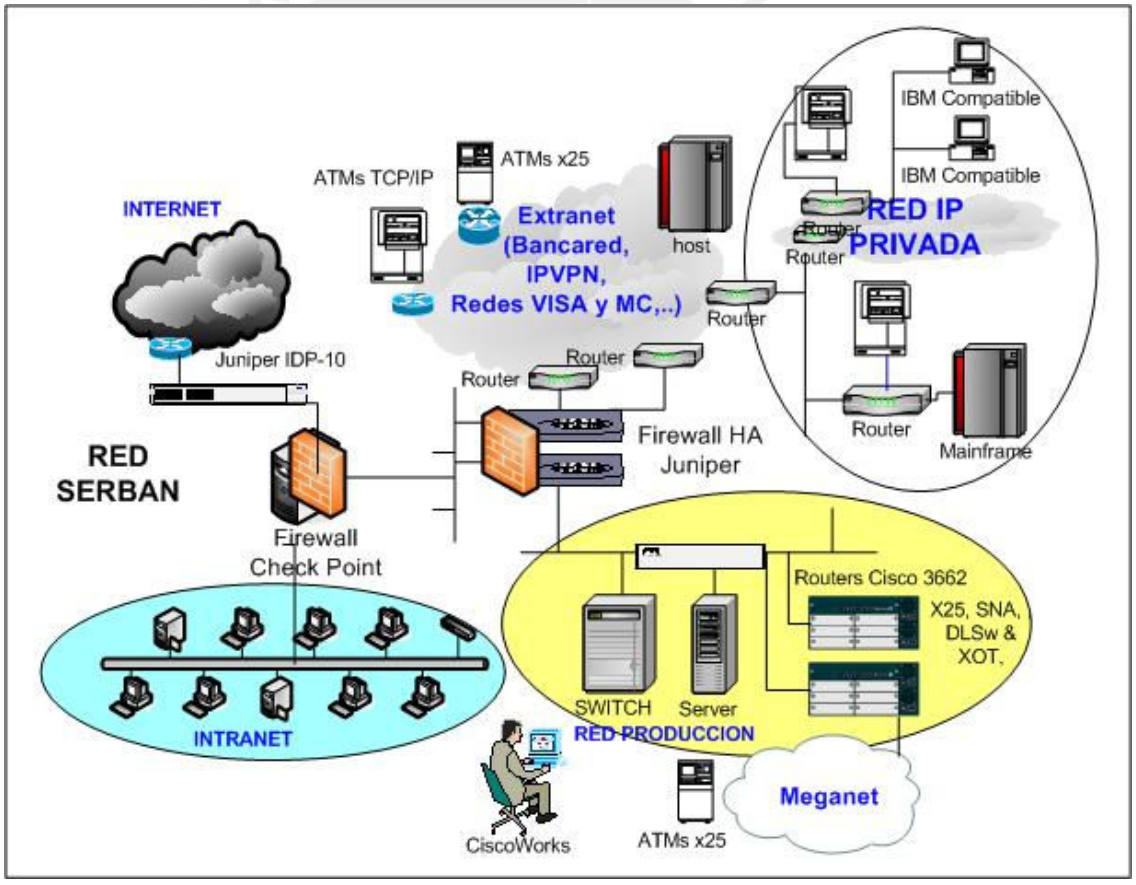

Fig. 3.21. Esquema final con nueva infraestructura en SERBAN.

3.4 Consideraciones por migración a protocolo TCP/IP.

El gran reto ha sido preparar las antiguas aplicaciones (lo cual implica una re-ingeniería de la programación de las interfaces de comunicaciones), la topología y la infraestructura de red, los terminales y los computadores remotos (y sus aplicaciones) que trabajan con protocolos heredados (SNA, X.25, BSC, etc.) para que soporten al TCP/IP con eficiencia y sobretodo, seguridad.

Esto se ha ido enfrentando paso a paso, en la medida que se han ido resolviendo temas de seguridad, de infraestructura, de desarrollo, venciendo tabúes existentes sobretodo en empresas financieras en donde la seguridad es lo que prima.

3.4.1 En las aplicaciones de Cajeros y Hosts

Las aplicaciones de cajeros y host son los principales puntos del negocio, y significan una gran inversión en el desarrollo por lo que su cambio es complicado y costoso. Es por ello que deben ser tratadas al detalle.

3.4.1.1 En los cajeros automáticos

Fabricantes de cajeros como NCR, Diebold y Wincor-Nixdorf (con presencia en el Perú), han ido innovando en tecnologías llegando a cambiar el sistema operativo (en la mayoría de casos usaban OS/2) a Windows 2000 y XP, usando en forma nativa el protocolo TCP/IP. El cajero podría ser instalado en una agencia bancaria como si fuera una computadora personal más (al bajo costo de un puerto de LAN Switch), integrándose a la comunicación de toda la agencia.

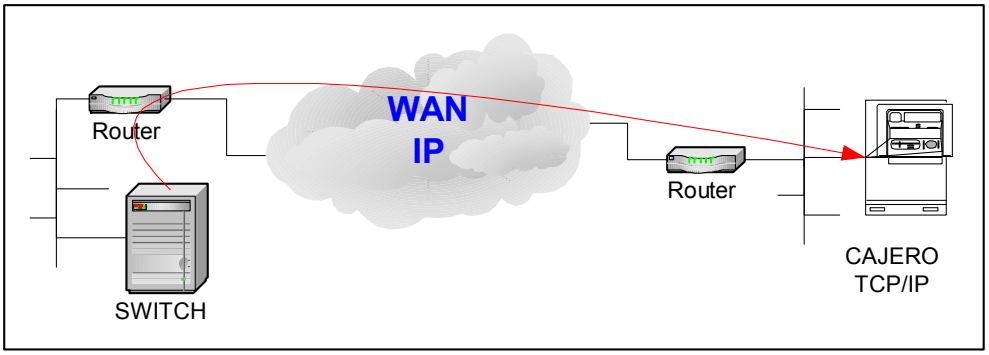

Fig. 3.22. Comunicación con cajero TCP/IP.

Si bien los fabricantes de cajeros tenían disponible la ultima generación de cajeros con Windows y TCP/IP desde el 2002, SERBAN recién inicio el proyecto de cambio de cajeros y adquisición de cajeros con TCP/IP desde que las marcas de tarjetas Mastercard Intl. y VISA establecieron fecha limite para que los cajeros de las redes adquirentes soporten Triple DES. Este nuevo requerimiento de seguridad exigía que se haga un cambio radical en el cajero o que se adquieran nuevos cajeros. En ambos casos, la configuración de comunicación con X.25 era un de alto costo extra (alrededor de $1000.00 por cajero).

Cada cajero automático con TCP/IP maneja los siguientes parámetros de comunicación básicos, únicos en la red:

- la dirección IP local,
- la dirección IP remota del SWITCH, y
- el puerto TCP (remoto si trabaja en modo cliente o el puerto local si trabaja en modo servidor).

Otros parámetros de configuración TCP son configurables en la aplicación pero son dejados en su valor por defecto:

- Cabecera con la longitud de la trama: 2 bytes.
- Activación/desactivación de “keepalives”, periodicidad: c/ 30 seg.
- Reintento de conexión luego de pérdida de enlace: c/30 seg.

En cuanto a la definición del modo de trabajo del cajero (servidor o cliente) se decidió que el cajero sea configurado en modo servidor, ya que de ese modo se tenía el control de la comunicación con el cajero desde el SWITCH. En lo que respecta a la dirección IP remota, ésta sería validada cada vez que levanta la conexión TCP, es decir, la aplicación del cajero no aceptaría ninguna conexión que no tenga como dirección origen la del SWITCH.

La asignación de puertos de servicio TCP en los cajeros se definió por una puerta TCP por institución: desde el puerto TCP 20020 al puerto TCP 20040 en forma consecutiva, de tal forma que mantenga un orden por cada institución.

La dirección IP del cajero la establece el dueño de la red local en donde está el cajero, de acuerdo a su plan de direccionamiento. En el caso de establecer un enlace usando una red pública o compartida, la dirección IP asignada al cajero debe ser trasladada a una dirección IP pública para que pueda ser visible desde el otro extremo de una red pública (esto se revisará más adelante).

En cuanto al sistema operativo, si bien usan uno comercial, como el Microsoft Windows XP o Windows 2000, éste ha sido preparado por el fabricante de modo que sólo tenga instalados los servicios y aplicaciones necesarios para el funcionamiento de la aplicación transaccional. A este proceso se le conoce como hardening o aseguramiento del sistema, lo cual lo protege de ataques que podrían ser efectivos en una instalación completa, y hace que la infección por virus sea poco probable.

La seguridad en los cajeros automáticos se basa en el principio básico de “proteger el dinero almacenado en su bóveda, y dispensarlo sólo a quien autorice el host NDC”.

Para esto el mecanismo de reconocimiento del host NDC o SWITCH debería ser el más adecuado, y se deberían manejar mecanismos para lograrlo:

1. La dirección IP del Switch (real o NAT) debe estar inscrita en la aplicación del ATM, y debe poder validarse para establecer la conexión.
2. Uso de llaves MAC diferentes por cada cajero para asegurar la integridad y la validez de los mensajes del ATM. Bajo este esquema se consigue un valor de chequeo calculado en base a ciertos campos de cada mensaje del ATM, con una llave distinta por ATM, el cual se inserta en el trailer del mensaje NDC, y el cual debe ser validado en el host NDC o Switch.
3. Protección del PIN del cliente con llaves de Triple DES de longitud doble, y políticas de seguridad para cargar llaves maestras diferentes por ATM, y el cambio dinámico de las llaves de trabajo o de cifrado de PIN cada vez que se cumpla uno de tres eventos:
    - ingreso de PIN errado tres veces consecutivas en el ATM
    - después de 24 horas del ultimo cambio de llave de trabajo
    - después de 1000 transacciones en el ATM.

Si bien la información que se envía al cajero puede quedar expuesta a la Red del Banco, esta será integra y confiable, y el PIN siempre estará protegido por las llaves de cifrado Triple DES. Un cifrado de línea para obtener mayor seguridad, sólo será posible estableciendo una VPN entre el cajero o un dispositivo de VPN colocado al costado del cajero y el concentrador VPN en la empresa de servicios.

Adicionalmente a la aplicación transaccional, se puede instalar al cajero agentes de control para efectuar las siguientes actividades:

- Monitoreo remoto mediante mensajes SNMP (independiente del monitoreo del Switch), en una consola gráfica ligada a una plataforma de Help-Desk. Esta

plataforma puede estar instalada en la institución y/o en SERBAN, y sólo requiere habilitar el puerto UDP 161 y 162 . Una plataforma de gestión de ATMs multimarca es Gasper, el cual trabaja sin problemas con agentes de administración en cajeros NCR y Wincor-Nixdorf, con una interfase amigable, efectúa seguimiento a la actividad de los cajeros, maneja eventos, mensajes de estado y efectúa estadísticas sobre las existencias de remesas de dinero para un ahorro en el almacenaje de dinero.

- Transferencia de archivos para el intercambio de archivos (imágenes y videos por campañas de marketing, el archivo de auditoria del ATM, etc.) con un servidor FTP en SERBAN o en la institución (según lo prefiera ésta). En ese caso el cajero levantaría automáticamente en modo cliente una conexión FTP, a una hora determinada del día (a una hora de bajo tráfico), enviaría el archivo de auditoria del día anterior y verificaría la existencia de un nuevo archivo (imagen o video) lo transferiría y lo aplicaría.
- Actualizaciones de antivirus. Según la decisión del banco, este puede optar por instalar software antivirus en el ATM, actualizable sólo desde un servidor en la propia red. Requiere habilitar el puerto TCP 81.Una solución de antivirus McAfee con una actualización usando el servidor Protection Pilot es totalmente compatible con la aplicación del cajero.

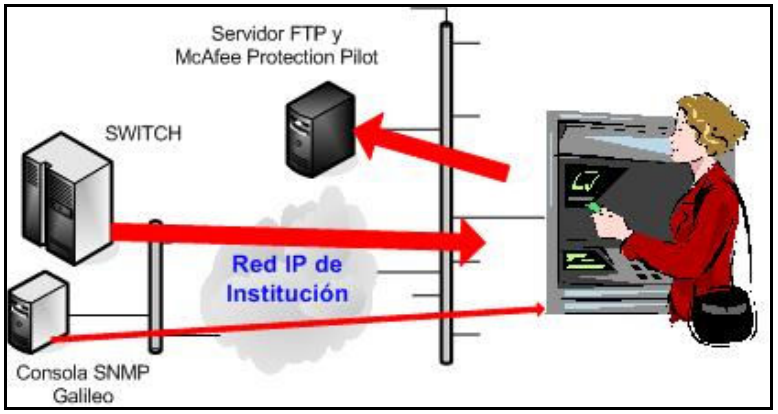

Fig. 3.23. Aplicaciones y conexiones en ATM.

Con la Fig. 3.22 se puede resumir que el ATM bajo protocolo TCP/IP es más versátil, logrando habilitar más servicios que cuando se usa otro protocolo:

- De la propia aplicación (como cliente o servidor)
- De administración (como cliente y como servidor de puertos UDP estándar)
- De transferencia de archivos (como cliente)
- De actualización de antivirus (como cliente)

3.4.1.2 En la comunicación con instituciones

El trabajo en este punto recae sobre las instituciones que tienen programada una interfaz de comunicaciones con SNA o X.25 y aceptan cambiarla a TCP/IP con los parámetros sugeridos por SERBAN:

- El establecimiento de dos conexiones, una conexión cliente (para transmitir los mensajes) y otra conexión servidor (para recibir los mensajes).
- Los puertos TCP servidor son asignados consecutivamente por pares por cada institución, desde el puerto 20300. Por ejemplo, la “institución 1” usaría el puerto TCP servidor local: 20300, y el puerto TCP servidor remoto: 20301.
- Cada mensaje debe contener una cabecera de 2 bytes con la longitud del mensaje.
- Se establece como tiempo de reconexión 20 segundos.

Aspectos de seguridad adicionales para proteger el contenido de la información de la comunicación Host-Switch podrían convenirse con la institución, de acuerdo a sus recursos disponibles: establecimiento de una VPN, o al nivel de aplicación el uso de llaves MAC.

Se debe tener en cuenta que la comunicación con la institución no sólo involucra el enlace Host-Switch, sino que en el nuevo esquema de concentración de enlaces

TCP/IP planteado, deberían estar los cajeros y los computadores para la transferencia de archivos.

La transferencia de archivos con la aplicación de control usada aplicaría sobre enlaces TCP con conexiones permanentes y ya no conmutadas (dial-up) de baja velocidad.

En lo que respecta a las instituciones asociadas, como VISA Intl. y Mastercard Intl., cada una de ellas ha dispuesto también un rediseño de sus redes, migrándolas a TCP/IP en su acceso LAN y WAN. Como se indicó en el primer capitulo, ambas tienen un computador de acceso instalado en SERBAN, y como parte de su migración a TCP/IP deberían ser cambiados a una zona “de protección”. Esto lo revisaremos más adelante.

3.4.2 Consideraciones de Seguridad en la red IP

Las consideraciones de seguridad se deben tomar básicamente por la conexión con redes públicas o redes no controladas.

Con protocolos heredados como el SNA y X25, en el caso de interconexión con redes públicas como Meganet (red publica X25 de Telefónica) con una difusión limitada tan sólo a empresas, era necesario filtrar las posibilidades de conexión sólo a las autorizadas por dirección X25 origen y destino, pero no era necesario más ya que las aplicaciones X25 limitaban cualquier acción no permitida.

Por el contrario el TCP/IP se ha convertido en el protocolo de facto y el gran propulsor del éxito de Internet. Su gran difusión ha permitido abaratar costos, sin embargo lo ha enfrentado con grandes problemas de seguridad: el robo de información, las suplantaciones, la alteración de la información, entre otros. Todos estos problemas se pueden superar implantando políticas de seguridad que logren:

- Desarrollar una red segura, con el control de accesos (listas de acceso y/o filtros en ruteadores, firewalls, Proxy,..) a nivel IP y TCP a computadoras críticas o de negocio.
- Mecanismos seguros de autenticación de usuarios, tales como contraseñas de una sola vez (OTP), dispositivos de token, y biométrica, y controles como por ejemplo la revocación de usuarios con exceso de intentos errados de autenticación.
- Mantener un programa de manejo de vulnerabilidades, que incluya actualización de antivirus y actualizaciones de seguridad del proveedor de los equipos, así como desarrollar y mantener sistemas de cómputo seguros, en donde no existan aplicaciones y servicios innecesarios o vulnerables a ataques.
- Monitorear y probar regularmente las redes, detectando cualquier comportamiento anómalo, o posibles ataques de zonas de red inseguras o de Internet.
- Establecer un programa de pruebas periódico, de vulnerabilidad de la red del tipo hacking ético.
- Proteger la información (cifrado, uso de firmas digitales, establecimiento de VPNs, etc.).

Para lograr estos alcances fue necesario implantar algunos equipos de seguridad además de establecer fuertes procedimientos de seguimiento y auditoria, los cuales incluyen instrucciones a los usuarios y administradores.

3.4.3 El plan de direccionamiento IP

La necesidad de ejecutar esta tarea se debe al continuo incremento de equipos con direccionamiento IP, y no sólo es cuestión de evitar encontrar un conflicto con otro equipo con una dirección idéntica, sino también el de cerrar la posibilidad de que en una red diseñada para un número limitado de equipos, puedan operar equipos capaces de intentar vulnerar la seguridad de los demás.

En los típicos entornos de red propietario como SNA, X25, es habitual adoptar esquemas de direccionamiento particulares que se han ido elaborando teniendo en cuenta únicamente las necesidades especificas de cada centro.

El acceso a Internet o a cualquier red publica por parte de una organización plantea dos problemas: de seguridad (toda maquina conectada esta a expensas de posibles accesos no controlados) y de escasez de direcciones (en una red como Internet con más de 35 millones de usuarios). Por ello la IANA (Autoridad de Asignación de Números de Internet) recomendó con el RFC 1597 a las redes de uso privado seleccionen su numeración dentro de los siguientes bloques (ver cuadro 3.10):

Rango	Clase	Número de bits para Hosts
10.0.0.0 – 10.255.255.255	A	24
172.16.0.0 – 172.31.255.255	B	20
192.168.0.0 – 192.168.255.255	C	16

Cuadro 3.10. Rango de direcciones permitidas para redes privadas.

Para el caso de SERBAN, en el cual se ha recomendado una segmentación de la red en zonas con el uso de equipos firewall, para un mejor control de la seguridad, se ha establecido el siguiente plan de numeración para sus redes internas:

Zona de Red	Dirección de red	Número de Hosts	Rango de IPs
Producción	172.16.1.0 255.255.255.224	30	172.16.1.1 a 172.16.1.30
Intranet	172.16.2.0 255.255.254.0	510	172.16.2.1 a 172.16.3.254
Extranet	172.16.4.0 255.255.255.0	254	172.16.4.0 172.16.4.254

Cuadro 3.11. Direcciones IP de SERBAN.

Dentro de la red extranet se definen los accesos a otras redes privadas, o públicas, algunas de las cuales definen sus propios planes de direccionamiento. Para poder participar en ellas es necesario efectuar la traslación de la IP privada de un equipo de SERBAN a la IP "publica" asignada o NAT (Network Address Translation).

Por ejemplo en el caso de Bancared, ASBANC ha definido la entrega a cada institución miembro de una subred de 254 direcciones IP para el uso de su red local, de la siguiente forma:

Banco 1 → 172.25.2.0 /24

Banco 2 → 172.25.3.0 /24

Banco 3 → 172.25.4.0 /24

……

Proveedor1 → 172.25.30.0 /24

SERBAN → 172.25.31.0 /24

Proveedor3 → 172.25.32.0/24

De ese modo, para la comunicación entre el Switch en SERBAN y un cajero automático en una de las agencias del Banco 3, es posible se hagan más de 2 NAT, lo cual asegura la protección de las redes privadas.

Switch	→ 172.16.1.3	NAT (172.16.4.103)	NAT 172.25.31.3
ATM	→ 10.1.2.3	NAT (192.168.1.103)	NAT 172.25.4.103

Es también posible enmascarar en una NAT (tipo hide) a todo un segmento de red en una sola IP, de tal forma que todos los equipos en esa red sean vistos como un solo equipo

Usuarios	→ 172.16.2.0	NAT (172.16.4.10)	NAT 172.25.31.10

Para la asignación de direcciones IP de cajeros en agencias, se recomienda utilizar una subred distinta a la de la agencia, tomando en consideración que se debe asignar una IP secundaria en la interfase ethernet del ruteador de la agencia para la salida al nodo central (ver Fig. 3.23).

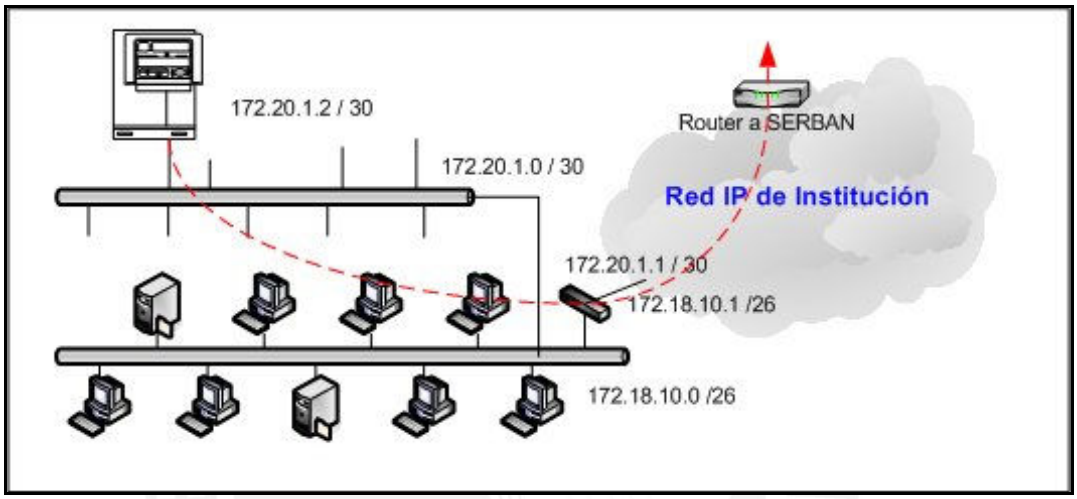

Fig. 3.24. Direccionamiento IP recomendado en agencia.

Esta subred debe ser dimensionada solo para el número de cajeros que se instalen en la agencia. Por ejemplo si se instala:

Un ATM → usar mascara de red 255.255.255.252
Hasta 5 ATMs → usar mascara de red 255.255.255.248

En el caso de IPVPN de Telefónica, la definición de red local la da el cliente, así como el plan de numeración en cada nodo remoto de su Intranet. Al igual que en Bancared, no interviene en el direccionamiento WAN, ni tampoco en la definición de las redes de apoyo: ISDN y loopback. En el nodo de acceso a IPVPN de SERBAN entonces se debía mantener el direccionamiento de la Extranet, pero para cada uno de los nodos

remotos había que efectuar una definición de red teniendo en cuenta que no debería haber más de 6 puntos en cada extremo, ya que 5 seria el límite de cajeros por nodo (ver Fig. 3.24)

En algunos casos, si la instalación quisiera asegurarse más se puede reducir el numero de equipos disponibles en la LAN a solo dos, el ruteador y el ATM. Por ejemplo en el nodo 5, se debería cambiar la mascara a 255.255.255.252.

Nodo 5 → 172.16.5.32 /30 → 172.16.5.33 a 172.16.5.34 Broadcast: 172.16.5.35

Nodo 1 → 172.16.5.0 255.255.255.248 → 172.16.5.1 a 172.16.5.6

Nodo 2 → 172.16.5.8 /29 → 172.16.5.9 a 172.16.5.14 Broadcast: 172.16.5.15

Nodo 3 → 172.16.5.16 /29 → 172.16.5.17 a 172.16.5.22 Broadcast: 172.16.5.23

Nodo 4 → 172.16.5.24 /29 → 172.16.5.25 a 172.16.5.30 Broadcast: 172.16.5.31

Nodo 5 → 172.16.5.32 /29 → 172.16.5.33 a 172.16.5.38 Broadcast: 172.16.5.39

Nodo 6 → 172.16.5.40 /29 → 172.16.5.41 a 172.16.5.46 Broadcast: 172.16.5.47

Nodo 7 → 172.16.5.48 /29 → 172.16.5.49 a 172.16.5.54 Broadcast: 172.16.5.55

……

Nodo 30 → 172.16.5.240 /29 → 172.16.5.241 a 172.16.5.246 Broadcast: 172.16.5.247

Nodo 31 → 172.16.5.248 /29 → 172.16.5.249 a 172.16.5.254 Broadcast: 172.16.5.255

Fig. 3.24. Direccionamiento IP de los nodos de la Intranet IP VPN de SERBAN.

Debería configurarse en una subred diferente al de la agencia, y con un rango de direcciones IP pequeña, como por ejemplo 255.255.255.252, la cual solo mantiene la IP del ruteador y la de un cajero.

El plan de direccionamiento IP de los cajeros se basaría en la red que se utilizaría como enlace.

3.4.4 El acceso remoto

Una solución de acceso remoto es necesaria cuando se tiene que dar soporte permanente a las aplicaciones a una red que espera un 99.8% de disponibilidad mensual, no sólo por parte del personal de la empresa sino por parte de sus proveedores, o también para la conexión de usuarios en instituciones asociadas.

La solución contempla el acceso desde cualquier punto de Internet a los equipos de desarrollo y/o a los equipos de producción dependiendo de las autoridades que pueda brindar la política de seguridad para el usuario, sin depender de conexiones dial-up o de una infraestructura de MODEM dial-up en SERBAN.

Disponiendo de equipos con características de concentrador VPN como el equipo firewall Check Point es posible establecer enlaces VPN desde clientes remotos usando el software SecuRemote de CheckPoint (software disponible libremente al adquirir la licencia de Check Point Express). La ventaja de la conexión usando SecuRemote es que la configuración reside en el concentrador VPN. En el concentrador se definen las comunidades VPN de acceso remoto que tienen los parámetros de conexión, y los usuarios que pertenecen a la comunidad, los cuales están asociados a las reglas de las políticas de acceso.

Una vez que el cliente ha entrado en contacto con el concentrador, identificando el usuario y reconociéndose entre los elementos en una fase I de IKE, recibe la configuración del concentrador incluyendo rutas permisibles, una dirección IP interna (de un pool de direcciones configuradas), y los parámetros de negociación de la fase II, típicamente llamado “proposals”

Propiedades de Túnel		Selección en dispositivo VPN
Fase 1	Método de autenticación	Certificados y usuarios locales
	Esquema de encripción	IKE
	Grupo Diffie-Hellman	Group 2
	Algoritmo de encripción	3DES
	Algoritmo Hashing	SHA-1
	Mode de negociación	Agressive
	Tiempo de vida (para renegociar)	No
Fase 2	Método de encapsulación	ESP
	Algoritmo de encripción	3DES
	Algoritmo de autenticación	SHA-1
	Perfect Forward Secrecy	Group 2
	Tiempo de vida (para renegociar)	No
	Lifesize en KB (para renegociación)	No

Cuadro 3.12. Parámetros de configuración de enlace VPN de Acceso Remoto.

3.4.5 El Centro de Contingencia

El mantener un Centro de Datos o Centro de Datos de Contingencia (CDC) en otra sede, implica tener una instalación con equipamiento similar o idéntico, dependiendo de la disponibilidad o tiempo para la recuperación de la red en el CDC. En el caso planteado, SERBAN define la recuperación en un tiempo máximo de 2 horas para efectuar la conmutación de las conexiones X25 y SNA, considerando que se puede establecer una sincronización permanente de las bases de datos del negocio (tarjetas, cuentas y transacciones) en un esquema de red Activo -Stand By mediante un enlace

TDM punto a punto. El 80% de las conexiones para la recuperación serian vía enlace conmutado (dial- up).

Ante una migración de los terminales de ATMs y Hosts a TCP/IP se debe considerar el equipamiento necesario para lograr el restablecimiento de los enlaces, los cuales se pueden resumir en:

- Implantar nodos de acceso a redes privadas de Bancared e IP-VPN, listos para asumir el mismo direccionamiento IP LAN del Centro de Datos principal, de tal forma que el cambio sea transparente para los nodos remotos. Esta operación debe ser efectuada por los Centros de Gestión respectivos.
- Punto de acceso a la red Meganet, para las conexiones X25 de algunos cajeros.
- Ruteadores Cisco con disponibilidad de memoria para efectuar el trabajo de emergencia de conversión SNA a DLSw y X25 a XOT y para la conexión de los cajeros por Meganet.
- Un firewall Juniper, para mantener la seguridad y la traslación de direcciones (NAT) necesarias.
- Ruteadores con conexiones a módems analógicos o puertos RDSI para recuperar por enlaces conmutados los enlaces faltantes a VISA y Mastercard entre otros.

El porcentaje de recuperación de red se elevaría al 95%, del total del numero de conexiones totales en servicio, en el caso de un desastre en el Centro de Datos principal que obligue a conmutar a la sede alterna, ya que los altos niveles de concentración de enlaces así lo permiten, contra el antiguo diseño de red con enlaces punto a punto TDM.

RECOMENDACIONES

1. Implantar la migración a TCP/IP de manera progresiva, consiguiendo las mejores alternativas de acceso al punto remoto, entregando soporte a las tecnologias antiguas, y con un adecuado plan de numeración IP e implantacion de politicas de de seguridad.
2. Los costos de inversión y de mantenimiento mensual aproximados de la nueva infraestructura de comunicaciones, para soporte de TCP/IP, sin considerar los costos de los cambios en algunas aplicaciones, son los que se muestran a continuación:

Costo de Accesos a redes IP	Costo de Instalación	Costo de Mantenimiento Mensual
IPVPN: acceso a 64 Kbps a red IP	US$ 612.00	US$ 200.00
Bancared: acceso a 1 Mbps	US$ 1500.00	US$ 600.00
Total	**US$ 2,112.00**	**US$ 800.00**

Equipos a Adquirir	Inversión	Mantenimiento
2 Ruteador Cisco3662 / 2 Switch Catalyst 2950 / 1 Cisco Works	US$ 43,455.33	US$ 277.66
1 Upgrade Firewall Check Point	US$ 6,525.00	US$ 525.00
2 Firewall Juniper Netscreen25 en HA	US$ 5,700.00	US$ 600.00
1 Juniper IDP-10	US$ 10,500.00	US$ 1,600.00
Total	**US$ 66,180.33**	**US$ 3,002.66**

Cuadro 3.13. Parámetros de configuración de enlace VPN de Acceso Remoto.

Estos costos pueden ser distribuidos en los meses que dure el proyecto, aproximadamente en 6 meses.

Tampoco se consideran los costos de implantacion del proyecto, ni los costos de los equipos remotos en la red IPVPN o en Bancared.

3. Escoger el router con las interfases adecuadas y la performance adecuada debe ser una tarea que se debe tomar con cuidado, así como el escoger la configuración adecuada. Estos deben llevarse primero a una maqueta de pruebas efectuando pruebas de saturacion y de los temporizadores de desconexion o timeout, o lo temporizadores de actividad (keepalive). El trabajo de encapsulamiento de SNA y X25 exige mucho afinamiento, sobre todo para aplicaciones transaccionales.

   Es altamente recomendable utilizar herramientas “analizadores de protocolo” con el fin de verificar el correcto funcionamiento de los equipos asi como las latencias que provocan.

4. Se debe considerar algunas pruebas piloto en el ambiente de produccion, en los cuales se debe incluir:
   - Probar la redundancia de la red
   - Identificar los cuellos de botella o puntos de posible problema de conectividad.
   - Verificar que el proveedor de servicio provee el servicio requerido.
   - Validar la tecnologia LAN, WAN y los dispositivos seleccionados.

5. Si bien el costo de los mantenimientos de software del equipamiento de seguridad es alto, se debe considerar que son equipos de seguridad que deben ser actualizados y deben tener soporte permanente.

CONCLUSIONES

1. La necesidad de migración a una red IP merece varias consideraciones que deben ser analizadas al detalle: nueva infraestructura de red, soporte a aplicaciones antiguas, politicas de seguridad, plan de direccionamiento IP, etc., que no significan un impedimento para iniciar un proceso de migración.
2. La inversión en la implantación de una red privada es muy costosa, por lo que es recomendable acceder a los servicios de una red de datos publica.
3. Una de las mejores prácticas para ahorrar costos en comunicaciones es la de compartir infraestructura de comunicaciones con otras instituciones, tal como lo propone Internet.
4. Las tecnologías de los equipos de comunicaciones permiten mantener antiguos protocolos de comunicación sin problemas, sin perder performance y sin desmedro de la seguridad de la red.
5. El nuevo esquema de red recomendado facilita la gestión, monitoreo, y la administracion de la red usando accesos rápidos y eficientes.
6. Un esquema de red basado en la concentración de enlaces en un menor número de puntos de accesos facilita la tarea de levantar un centro de contingencia con un mayor porcentaje de recuperación.

7. Probar el diseño de la red es un importante paso en el proceso de diseño que permite confirmar que el diseño alcanzó los objetivos técnicos y del negocio. Asimismo puede verificarse si se alcanza la performance que espera el cliente.
8. Es necesario documentar toda la informacion de configuraciones, esquemas de red, etc. y mantenerlo actualizado. Esto facilita la resolución de posibles problemas, la capacitación de nuevo personal, etc.
9. Usar las herramientas de gestión de red para lograr un análisis predictivo de la red, análisis de tráfico, verificar la caida de enlaces y el tiempo de no disponibilidad de los mismos.
10. Las posibilidades en redes IP son enormes, dependiendo del presupuesto que se pueda manejar. Algunos de los items que se pueden considerar para afinar el proyecto son:
    - Instalar “sensores IDS de host” en los servidores de producción, administrados por un software centralizado que puede tomar acción en varios puntos de la red, para una mayor seguridad.
    - Instalar un firewall - appliance pequeño en cada uno de los puntos de cajero automático para brindar una mayor protección al equipo y facilitar la creacion de una VPN con el concentrador VPN de SERBAN.
    - El configurar puntos de voz en el router de acceso a IP-VPN puede permitir la comunicación telefónica con los nodos remotos de las instituciones, asi estos estén en provincia.
    - Se puede configurar un segundo router de acceso a IPVPN por otro medio (como ADSL), configurado en alta disponibilidad (con HSRP) con el primer router, de tal forma que éste sea un nivel adicional de contingencia del router de acceso a la red IPVPN y no sólo como lo contempla RDSI que es enlace de contingencia al nodo remoto.

FUENTES

OPPENHEIMER, Priscilla
2003 Top-Down Network Design. 9na, ed.
Indianapolis: Cisco Press

Mc CABE, James D.
2003 Network Analysis, Architecture and Design
USA: Morgan Kaufmann Series in Networking

ALCÓCER GARCIA, Carlos
2000 Redes de Computadoras
Lima: Infolink

BLACK, Uyless
1995 Redes de Computadores, Protocolos, Norma e Interfaces
Madrid: Ra-Ma.

NCR CORP.
2003 NDC Referente Manual
Dayton (USA): NCR Corp. Press

CISCO SYSTEMS
2006 Cisco ® [En línea] San Jose, CA [Consultado 2006/05/10]
<http://www.cisco.com/>

SUN MICROSYSTEMS
2006 Sun ® [En línea] Santa Clara, CA [Consultado 2006/05/02]
<http://www.sun.com/documentation>

CHECK POINT
2006 Check Point ® [En línea] Red Wood, CA [Consultado 2006/05/04]
<http://www.checkpoint.com/ >

JUNIPER NETWORKS
2006 Juniper ® [En línea] Sunnyvale, CA [Consultado 2006/05/06]
<http://www.juniper.net/ >

WINCOR-NIXDORF
2006 Wincor-Nixdorf ® [En línea] Alemania [Consultado 2006/05/01]
<http://www.wincor-nixdorf.com/internet/es/Products/ >