UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE ACCESO SEGURO DE EMPRESAS EXTERNAS A REDES CORPORATIVAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MIGUEL ANTONIO VASQUEZ MENDOZA

PROMOCIÓN
1991 - I

LIMA – PERÚ
2010

IMPLEMENTACIÓN DE ACCESO SEGURO DE EMPRESAS EXTERNAS A REDES CORPORATIVAS

Dedico este trabajo a:

Mis padres, por su lucha y sacrificio en darme lo mejor;

A mi hijos, para que sirva de muestra para una superación continua;

A mi esposa, que me impulsó a cumplir un anhelo no cubierto.

SUMARIO

El presente informe describe la implementación de una plataforma estándar y segura para el acceso a diversos aplicativos de una empresa corporativa para con sus empresas colaboradoras.

El Capítulo I se refiere a los conceptos generales que se tendrán en cuenta en el presente informe. Una visión general sobre las tecnologías que se usan para la implementación de la plataforma segura.

El Capítulo II se refiere a la elaboración del proyecto que comprende la situación que existía en la empresa corporativa y las diversas definiciones que se dieron para la implementación de una solución única y segura.

El Capítulo III se refiere a la implementación del proyecto y las diversas etapas que comprende. Se incluyen definiciones y estándares que han involucrado diversas áreas de la empresa corporativa y exigencias que se dieron a las empresas colaboradoras.

En el Capítulo IV se muestran los temas presupuestales involucrados en el proyecto, tanto a nivel de inversiones como de gastos. Asimismo se presentan las etapas de la ejecución del proyecto.

Finalmente se presentan las conclusiones y las recomendaciones a seguir para con el presente proyecto.

ÍNDICE

INTRODUCCIÓN

El presente trabajo lo he desarrollado en una empresa corporativa que tenía la necesidad de mejorar la relación con sus clientes finales a través de las empresas colaboradoras. La solución que se planteó mejoró diversos aspectos de la empresa corporativa.

Los análisis realizados para poder decidir opciones de mercado para plantear una solución nos originó relevar el proceso que se seguía y se realizaron diversas tomas de muestras para poder analizar y tomar decisiones y obtener mejoras significativas.

CAPÍTULO I
MARCO TEÓRICO

1.1 Tecnología ADSL (Línea de Abonado Digital Asimétrica)

1.1.1 Introducción ADSL

Cuando hoy se habla de velocidades de acceso a Internet en entorno a Mbits/s parece mentira que en 1975 se creyera que 20Kbits/s sería la máxima velocidad de transmisión posible sobre líneas telefónicas. Las conexiones ADSL conocidas por la mayoría de nosotros prometen hacer realidad esos sueños de una navegación agradable y en condiciones que todos los usuarios de módems de 56Kbits/s no tenemos. La explosión de Internet no conoce límites, pero sin embargo los servicios no han mejorado de forma sustancial en los últimos años. Eso no es de extrañar porque hasta hace poco la existencia de ADSL era algo desconocido, el cable ha tardado en llegar a todo lo que no sea grandes urbes y en cuanto al RDSI, no merece la pena por lo que aporta.

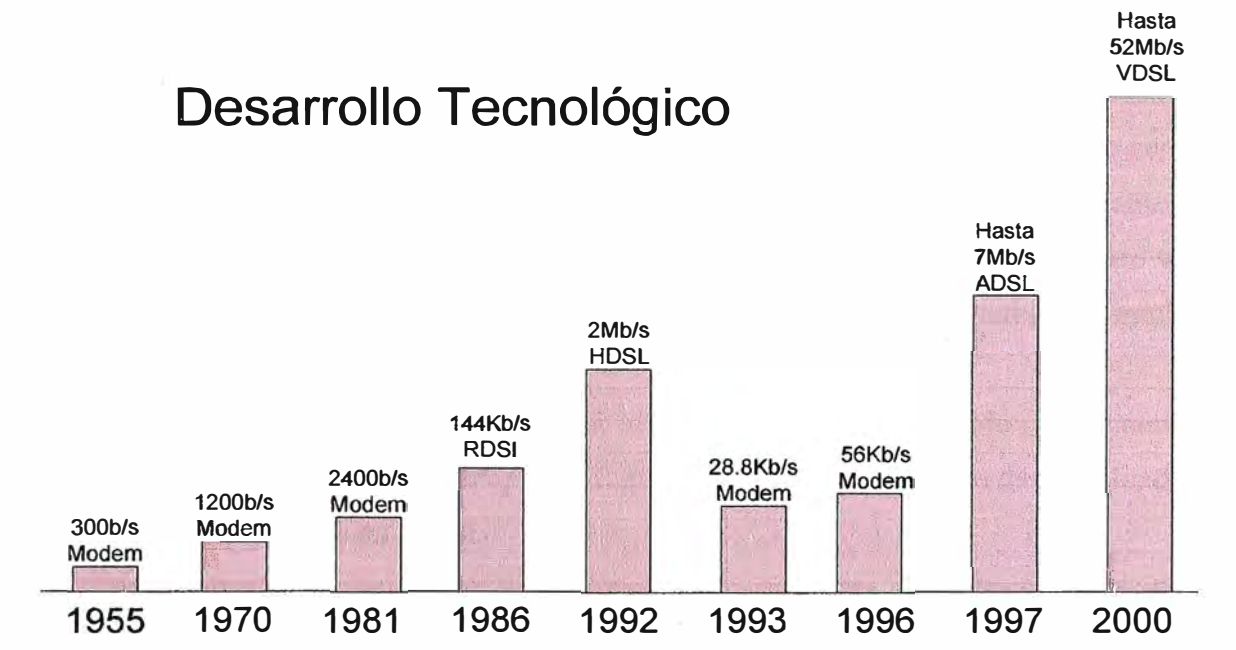


Figura 1.1 Evolución del uso de líneas telefónicas

Voy a detallar conceptos que están detrás de esa tecnología capaz de obtener ventaja a la línea convencional para luego revisar el ADSL práctico.

1.1.2 Funcionamiento ADSL

ADSL forma parte de una nueva familia de tecnologías, denominadas xDSL, diseñadas para ofrecer servicios de banda ancha y permitir, por sus características, una adopción muy rápida y con un coste muy inferior a otras soluciones con las que compiten.

El término ADSL significa "Línea de abonado digital asimétrica" (Asymetric Digital Suscriber Line) y es uno de los estándares que forman parte de la familia xDSL. Esta familia de tecnologías ofrece beneficios inmensos tanto para el usuario como para el operador de telefonía.

El por qué del ADSL se resume en:

- Permite velocidades teóricas de hasta 15Mbps (ADSL) en el canal descendente (download) que supera en más de 200 veces el ancho de banda que proporciona un módem de 56 Kbits/s.
- Ofrece integración de los servicios voz y datos y permite conversaciones telefónicas y transmisión de datos al mismo tiempo. Esto es posible porque se utilizan zonas distintas del espectro de frecuencia.
- Es una tecnología que aprovecha la infraestructura existente de cableado para telefonía básica por lo que su coste para el operador telefónico es mínimo. Por el contrario, utilizar cable con fibra óptica y crear una nueva red de telecomunicaciones implica un gasto elevado.
- El hardware necesario para implementar una línea ADSL es relativamente sencillo y de bajo coste. En cuanto al usuario, sólo hace falta un módem ADSL que suele ser una tarjeta PCI si es interno, mientras que si es externo se conecta al PC mediante una tarjeta de red. También se suele necesitar un separador (splitter) que separa entre voz y datos. Por parte del operador de telefonía las modificaciones tampoco implican cambios radicales.
- Las normas xDSL prometen evolucionar muy rápidamente de acuerdo con el aumento de tráfico y ya se está hablando de VDSL que ofrecería hasta 52Mbps de download.

1.1.3 Líneas Telefónicas en ADSL

Anteriormente se tenían las limitaciones de los módems que ofrecían velocidades hasta 56Kbps, insuficientes para otro uso que no sea exclusivamente el correo electrónico.

Una idea muy generalizada es que estas limitaciones estaban impuestas por la calidad de líneas telefónicas entre el usuario y el operador telefónico o el conocido bucle de abonado en términos de telecomunicaciones. El bucle de abonado consiste en un par de

cables que va entre el usuario y la central telefónica, y el cableado utilizado se conoce como par trenzado.

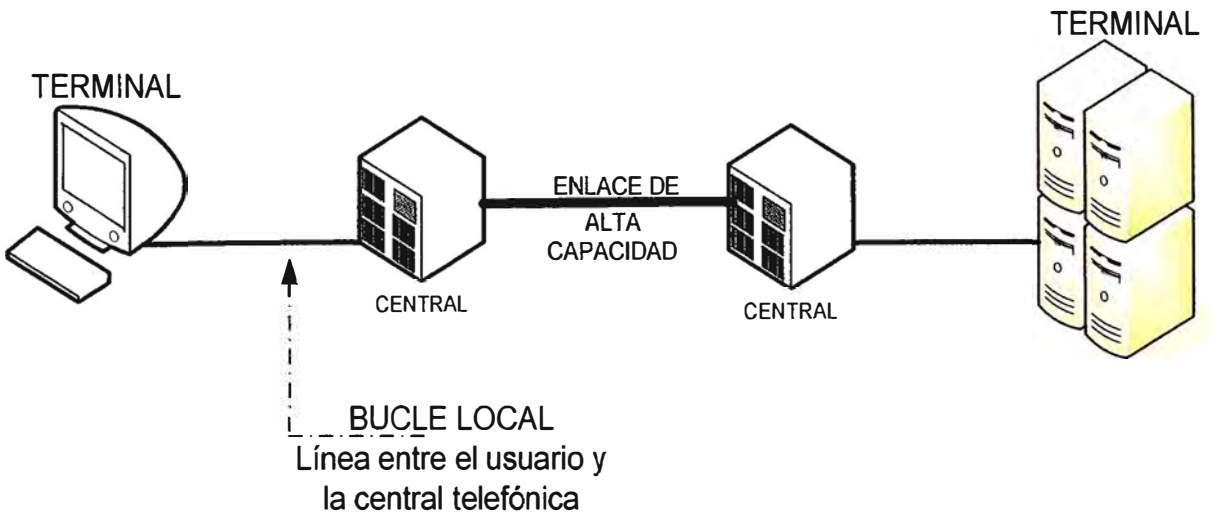


Figura 1.2 Bucle y líneas telefónicas

El par trenzado es el cableado más económico y el más utilizado en la actualidad. Se compone de dos conductores aislados independientemente y enrollados en forma de trenza. Este trenzado reduce de forma notable las interferencias y como suelen ir múltiples pares trenzados dentro del mismo encapsulado de plástico se utilizan longitudes de trenza distintas.

Como características del par trenzado aparte de su bajo coste se destaca:

- Permite transmitir señales eléctricas a distancias cortas hasta 1-5 Mhz.
- Coste muy bajo frente a cable coaxial y fibra óptica (utilizados en cable módems).
- Muy susceptible al ruido, que está siempre presente y a las interferencias de todo tipo.
- Se necesitan amplificadores en la transmisión cada 5 ó 6 Km.
- Con todo esto, el par trenzado no es un cableado para transmisiones a larga distancia ya que se necesitan repetidores cada 5 ó 6 Km frente a cada 40 Km en el caso de la fibra óptica. Las frecuencias a las que permite trabajar, en ADSL 1 - 5 MHz no son nada impresionantes tampoco si se comparan con las que posibilita la fibra óptica, del orden de THz, es decir, 1 millón de veces más. Lo que ocurre es que aparte de estar muy extendido, el par trenzado posee una clara ventaja económica frente a la fibra y al cable coaxial.

1.1.4 Alcance de Redes ADSL

El ADSL se ha desarrollado a principios de los 90 como un estándar de banda ancha pensado para ofrecer servicios de video bajo demanda bajo MPEG1, pero es ahora

cuando parece que se va a implantar de manera amplia.

Una de las principales ventajas de ADSL es que funciona sobre par trenzado que como ya se ha dicho es el "cableado" más utilizado. Se calcula que alrededor de un 85%-90% de las personas que tengan teléfono se podrán beneficiar de esta tecnología, esto supone que el operador de telefonía no tiene que hacer las inversiones elevadas en infraestructura que, por ejemplo, realizan los operadores de cable.

En Europa, la mayor parte de los abonados telefónicos se encuentran situados en un radio de 5 Km a la central telefónica; mientras que en Estados Unidos (USA), los abonados no están tan concentrados alrededor de la central.

La línea telefónica que se tiene en casa siguen esencialmente el mismo diseño de hace 100 años que se corresponde con "la época" de la invención del teléfono.

Para entender el concepto de ADSL es necesario explicar el fenómeno de atenuación. La información se transmite mediante señales eléctricas que al viajar por un medio, sea par trenzado o cualquier otro, sufren atenuación que básicamente consiste en un debilitamiento de la señal. Se puede pensar en la atenuación como en las pérdidas que sufre la señal eléctrica al transmitirse. Estas pérdidas dependen de la distancia y de la frecuencia de trabajo de una manera muy sencilla. Si aumenta la distancia o la frecuencia de trabajo, aumenta la atenuación.

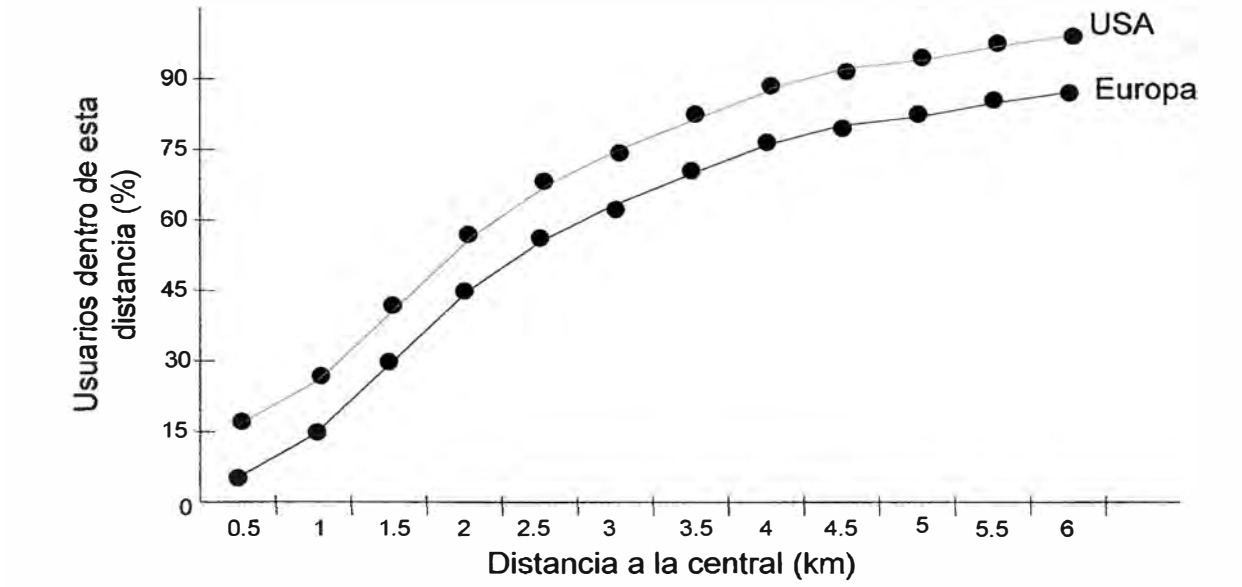


Figura 1.3 Estadísticas de usuarios sobre distancia hacia las centrales telefónicas

1.1.5 Redes ADSL

La filosofía que se encuentra detrás de ADSL consiste en optimizar y restringir estos dos parámetros. Si se reduce lo suficiente la distancia de transmisión y se emplean

técnicas de transmisión más elaboradas podremos disponer de una mayor velocidad de transmisión.

Uno de los requisitos para poder contratar una línea de ADSL es estar a menos de aproximadamente 5 Km de la central telefónica. Limitando la distancia reducimos de forma notable las pérdidas que sufrirá la información al transmitirse. Esto nos permite elevar de forma notable la frecuencia de trabajo que se traduce directamente en un aumento de la velocidad de transmisión.

En la figura 1.4 se tiene que reduciendo la distancia entre el usuario y la central telefónica se pueden conseguir mayores velocidades.

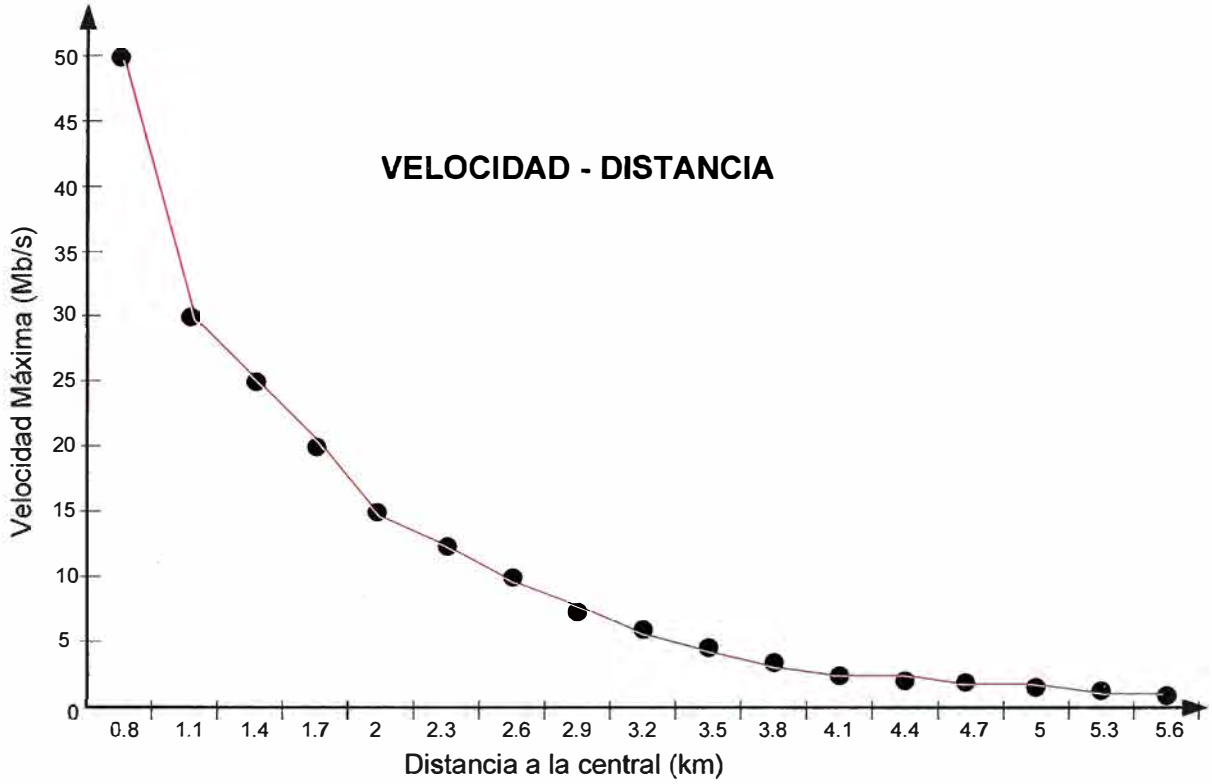


Figura 1.4 Relación distancia a la central con la velocidad que se puede alcanzar

Los modos de transmisión existentes:

- Simplex: sólo en una dirección.
- Half-duplex: es bidireccional pero sólo uno de los extremos puede enviar información en un instante dado.
- Full-duplex: bidireccional, ambos extremos pueden transmitir a la vez.

El término de transmisión asimétrica o simétrica se refiere al hecho de si se dispone de la misma velocidad en bajada y subida. Si estas dos velocidades son distintas el modo es asimétrico (ADSL), en caso contrario se habla de modo de transmisión simétrico (RDSI)

1.1.6 Funcionamiento Avanzado de Redes ADSL

La frecuencia representa las veces que algo se repite en un intervalo de tiempo y es la inversa del tiempo. Al conocer esta relación, esto nos permite convertir un gráfica en función del tiempo en una gráfica en función de la frecuencia. Esta representación en frecuencia recibe el nombre de espectro de frecuencia. Si el intervalo de tiempo considerado es el segundo, la frecuencia se mide en Hz. En comunicaciones, la norma habitual es hablar de frecuencias y no de tiempos. Por ejemplo, el teléfono de casa transmite entre 300Hz y 3400Hz. Esto es también el intervalo usado por los módems convencionales.

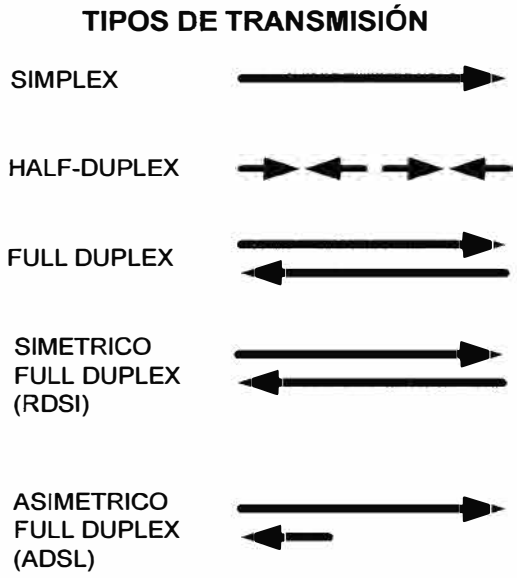


Figura 1.5 Tipos de Transmisión

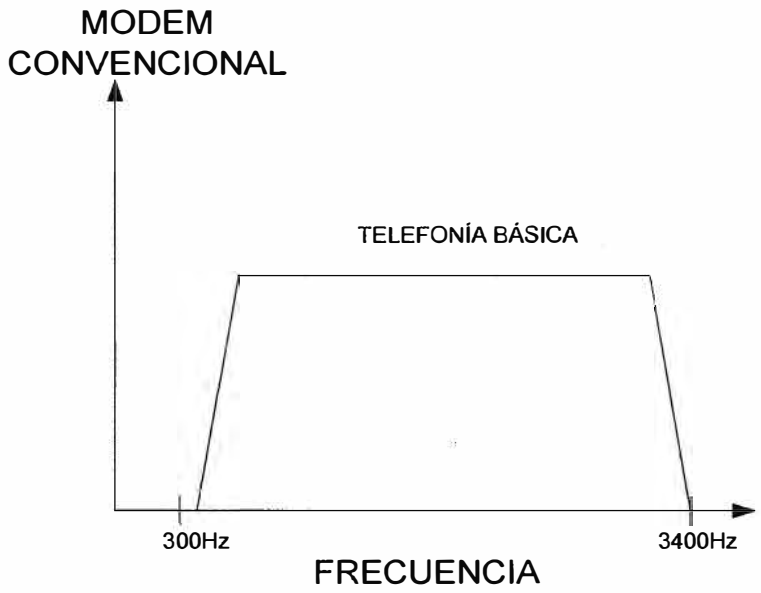


Figura 1.6 Uso del espectro en telefonía básica convencional

¿Pero qué ocurre en el caso de ADSL?, como se limita la distancia, en ADSL se utilizan frecuencias hasta 1 MHz e incluso superiores.

La velocidad de transmisión aumenta con un aumento de frecuencia, por lo que como aquí el aumento de frecuencia es de alrededor de 300 veces más, la mejora tiene que ser muy notable. La zona de más a la izquierda se reserva para telefonía básica y esto es lo que permite separar entre voz y datos, mientras que con un módem convencional se utiliza la misma zona. El splitter no es más que un filtro que separa estas dos regiones. Como se puede observar en la figura 1.7, se reservan frecuencias hasta los 25kHz y no hasta los 3.4Khz como medida de protección frente a interferencias.

Por tanto, se ha reducido la distancia y esto ha permitido aumentar la frecuencia de trabajo. El intercambio en este caso es muy rentable por que como se muestra, los usuarios se encuentran cerca de la central.

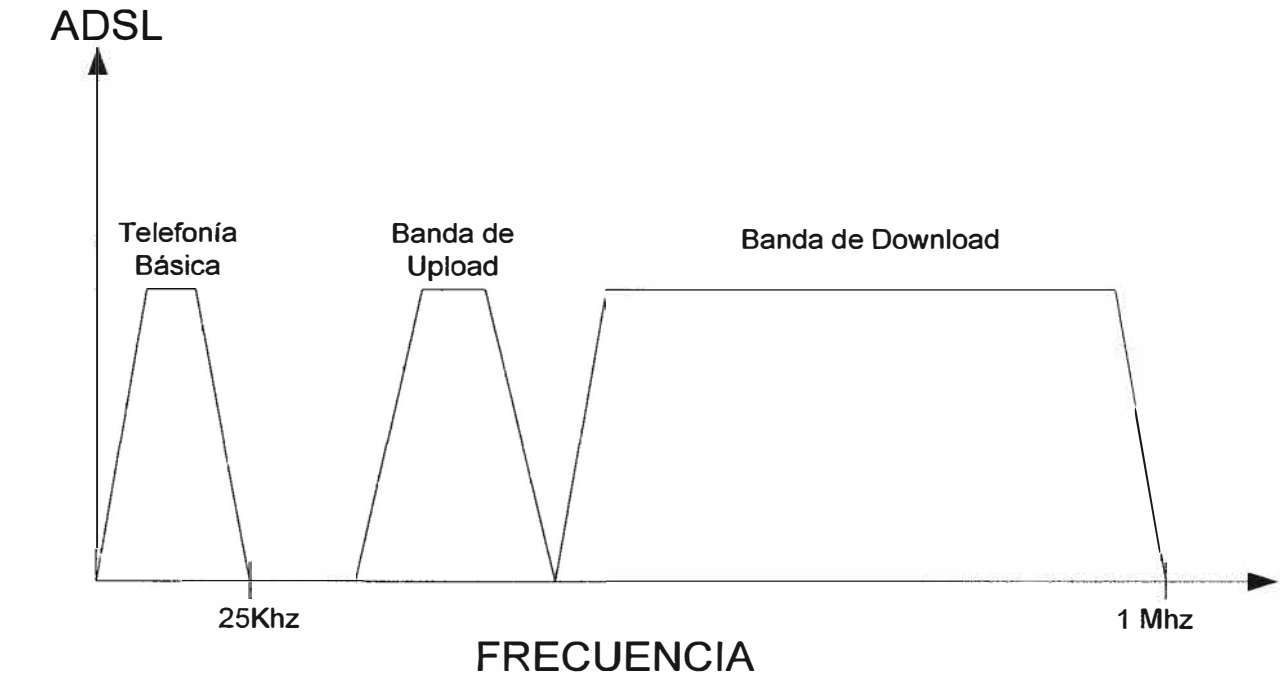


Figura 1.7 Uso del espectro para ADSL

Las mejoras que introduce ADSL no acaban aquí sino que se implementan técnicas inteligentes para poder optimizar al máximo la velocidad. Como ya se ha mencionado, las pérdidas aumentan con la frecuencia por lo que no es lo mismo transmitir a 250 Khz que a 1 Mhz. Por esta razón ADSL utiliza una técnica llamada DMT (Multi-tono discreto) que divide el ancho de banda utilizado en sub-canales. En ADSL se suelen utilizar 256 sub-canales que es el resultado de dividir el ancho de banda disponible, 1 Mhz, en sub-canales de 4 Khz. En el proceso de iniciación el Modem DMT testea cada sub-canal para

determinar la calidad de transmisión y posteriormente de acuerdo con los resultados enviará más o menos datos a través de él.

En teoría, cada canal puede transportar hasta 60 Kbits/s, por lo que multiplicando esta cifra por los 256 canales se obtiene 15.36 Mbits/s pero en la práctica esto se reduce a 1.5-9 Mbits/s por la existencia de ruido e interferencia en las líneas. La asignación variable de información según la calidad de transmisión que realiza DMT es algo muy necesario.

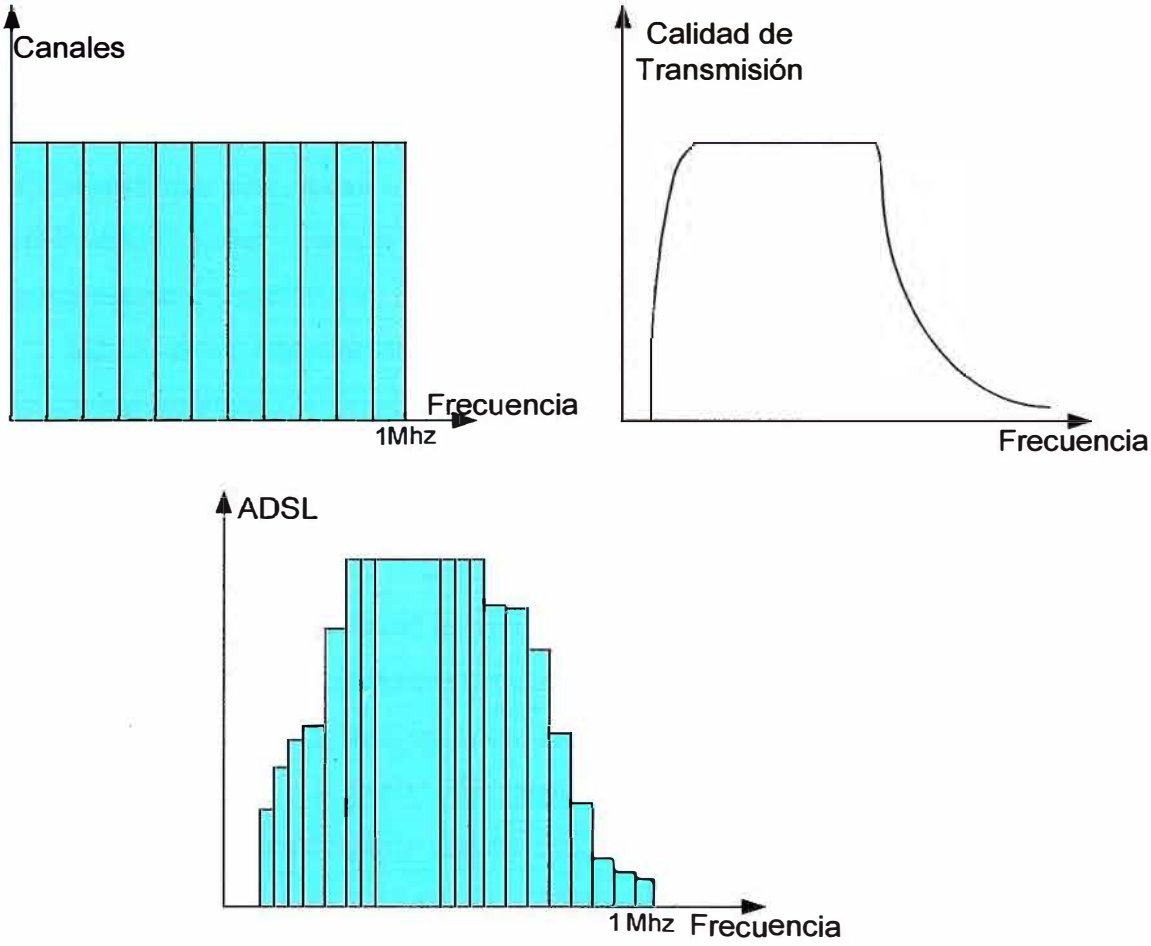


Figura 1.8 Combinación de canales con el espectro

1.2 Tecnología MPLS (Conmutación Multi-Protocolo mediante Etiquetas)

1.2.1 Introducción MPLS

Día a día, se hace más evidente el crecimiento de la red. El número de usuarios que se conecta a la red se incrementa de una manera asombrosa, ahora, este no es el mayor reto que tiene que enfrentar la Internet actual. Además de los usuarios que a ella se conectan, existen también las distintas aplicaciones que en ella se ejecutan, por ejemplo, las aplicaciones que se corren en entornos corporativos (videoconferencia, VoIP, etc.) que requieren de un tratamiento más especial que las aplicaciones que corre un usuario común

desde su casa.

Uno de los factores del éxito de nuestra Internet actual es el uso del protocolo TCP/IP como estándar para cualquier aplicación o servicio que en ella se ejecuta. Pero si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los nombrados anteriormente, entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas.

La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort". Esta situación se complementa con una nueva arquitectura de red de reciente aparición conocida como Multi-Protocol Label Switching (MPLS). MPLS se considera fundamental en la construcción de los nuevos cimientos para la Internet del siglo XXI.

MPLS es un estándar del IETF que surgió para agrupar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mediados de los 90. Como concepto, MPLS es un tanto difícil de explicar. Según el énfasis o interés que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como:

- Un sustituto de la conocida arquitectura IP sobre ATM.
- Como un protocolo para hacer túneles.
- Como una técnica para acelerar el encaminamiento de los paquetes.

En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (enlace) y 3 (red), combinando eficazmente las funciones del control de enrutamiento con la simplicidad y rapidez de la conmutación de nivel 2.

Pero ante todo esto, y sobre todo, debemos considerar MPLS como un avance más reciente en la evolución de las tecnologías de enrutamiento y forwading en redes IP, lo que implica una nueva manera de pensar a la hora de construir y gestionar estas redes.

1.2.2 Antecedentes

Para entender mejor las ventajas de la solución MPLS, se revisarán las tecnologías de integración de los niveles 2 y 3 que la precedieron.

a) IP sobre ATM

A mediados de los años 90, IP predominaba como protocolo de red ante otras arquitecturas que se encontraban en uso como: SNA, IPX, AppleTalk, OSI, etc. El gran auge de la Internet y su explosivo crecimiento generó un déficit de ancho de banda, ya que los "backbones" IP de los proveedores de servicio (NSP) estaban construidos con

enrutadores conectados por líneas dedicadas, lo que ocasionaba congestión y saturamiento de las redes. Había entonces que idear otras alternativas de ingeniería de tráfico.

La respuesta de los proveedores fue el incremento del número y de la capacidad de los enlaces. Del mismo modo, se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo.

Por lo tanto, los esfuerzos se centraron en aumentar el rendimiento de los enrutadores tradicionales, tratando de combinar, de diversas maneras, la eficacia y rentabilidad de los conmutadores ATM (capa 2 del modelo OSI) con las capacidades de control de IP (capa 3 del modelo OSI).

El funcionamiento IP/ATM supone la superposición de una topología virtual de enrutadores IP sobre una topología real de conmutadores ATM. Cada enrutador se comunica con el resto mediante los circuitos virtuales permanentes (PVC) que se establecen sobre la topología física de la red ATM, desconociendo la topología real de la infraestructura ATM que sustenta los PVC. (figuras 1.9 y 1.10).

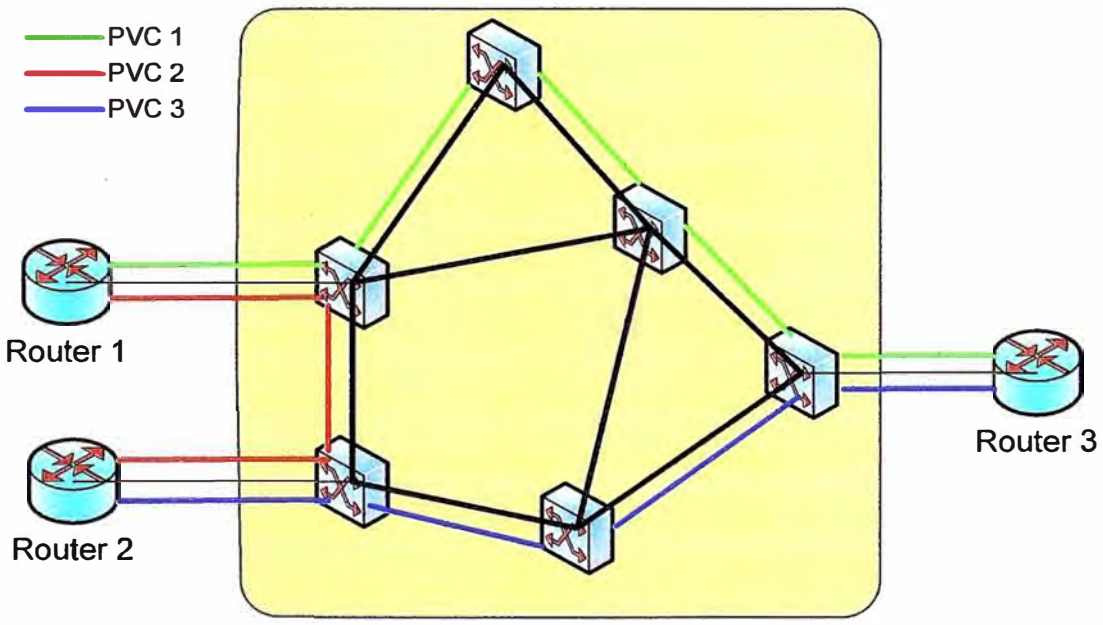


Figura 1.9 Topología Física Capa 2

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y enrutamiento) y el envío de las celdas por hardware (conmutación). En realidad los circuitos (PVCs) se establecen a base de intercambiar etiquetas en cada conmutador de la red, por lo tanto asociando etiquetas

entre todos los elementos ATM se determinan los PVCs.

El hecho de superponer IP sobre ATM permite aprovechar la infraestructura ATM ya existente, obteniendo de esta manera un ancho de banda a precios competitivos, y una rapidez de transporte de datos proporcionada por los conmutadores.

Sin embargo, el modelo IP/ATM también tiene sus inconvenientes. Se debe gestionar 2 redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio mayor costo en la gestión global de sus redes.

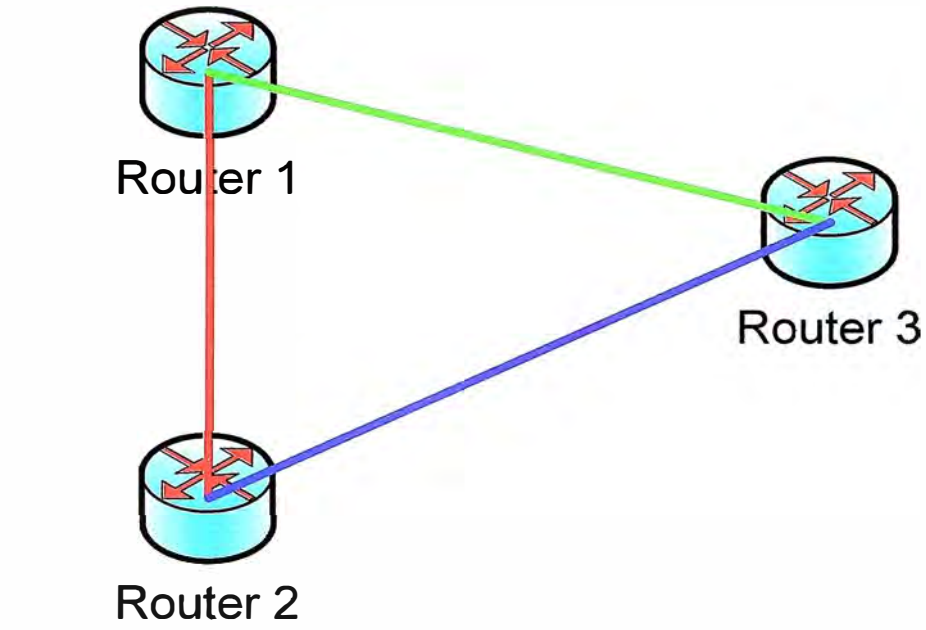


Figura 1.10 Topología Física Capa 3

b) Conmutación IP

Los problemas derivados del rendimiento de la solución IP/ATM, llevaron posteriormente al desarrollo de técnicas para la integración de los niveles de forma efectiva. Esas técnicas se conocieron como "conmutación IP" o "conmutación multinivel". El problema que presentaban estas soluciones o técnicas era la falta de inter-operatividad, ya que se usaban diferentes tecnologías privadas para combinar las capas 2 y 3 (OSI).

Todas las soluciones de conmutación multinivel (incluyendo MPLS) se basan en dos componentes básicos comunes:

b.1) La separación entre las funciones de control y envío.

b.2) El paradigma de intercambio de etiquetas para el envío de datos.

Al separar la componente de control de la componente de envío (b.1), cada una de ellas se puede implementar y modificar independientemente.

Para el envío de datos, se realiza un intercambio de etiquetas (b.2). Una etiqueta es

un campo de unos pocos bits y de longitud fija, que se añade a la cabecera del paquete y que identifica a una "clase equivalente de envío" (FEC, "Forwarding Equivalente Class"). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes.

El algoritmo de intercambio de etiquetas permite así la creación de caminos virtuales conocidos como LSP (Label-Switched Path), funcionalmente equivalente a los PVCs de ATM. La diferencia básica entre las técnicas de conmutación y el modelo IP/ATM es que en el fondo lo que se hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza (como son las redes IP), pero todo ello sin perder la visibilidad del nivel de red.

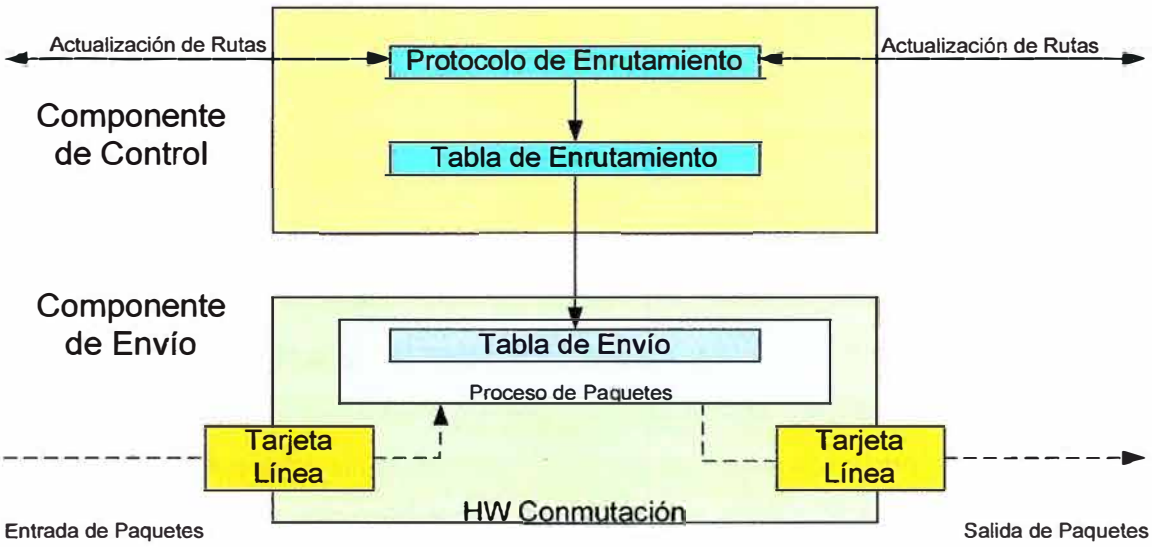


Figura 1.11 Conmutación IP

1.2.3 Conceptos MPLS

El problema fundamental que presentaban las diferentes soluciones de conmutación IP era la falta de inter-operatividad entre los productos de diferentes fabricantes. Además de esto, la mayoría de estas soluciones usaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas.

Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e inter-operativo.

Los objetivos establecidos por este grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.

- MPLS debía soportar el envío de paquetes tanto bajo demanda unidifusión (unicast) como multidifusión (multicast).
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP (Resource Reservation Protocol).
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

a) Componentes

- LSRs (Label Switching Router): Es un enrutador de alta velocidad especializado en el envío de paquetes etiquetados por MPLS. Participa en el establecimiento de las rutas (LSPs). Es capaz de enviar paquetes de capa 3 nativos. Los LSR, pueden ser internos o extremos, los primeros añaden o eliminan etiquetas, mientras que los segundos sustituyen unas etiquetas por otras.
- Etiqueta: es un identificador corto (de longitud fija) y con significado local, empleado para identificar un FEC. Un paquete puede tener una o más etiquetas apiladas (jerarquía). Cuando un paquete atraviesa dominios interiores a otros dominios, es cuando se produce el apilamiento de etiquetas. El LSR al recibir un paquete siempre consultará la etiqueta de nivel superior.
- FEC (Forwarding Equivalence Class): Agrupación de paquetes que comparten los mismos atributos (dirección destino, VPN) y/o requieren el mismo servicio (multicast, QoS). Se asigna en el momento en que el paquete entra a la red. Todos los paquetes que forman parte de la clase, siguen un mismo LSP.
- LSP (Label Switched Path): Es una ruta a través de uno o más LSRs en un nivel de jerarquía que sigue un paquete de un FEC en particular. Este camino puede establecerse tanto mediante protocolos de enrutamiento como manualmente.

b) Funcionamiento

El funcionamiento del protocolo MPLS debe seguir los siguientes pasos:

- Creación y distribución de etiquetas
- Creación de tablas en cada enrutador
- Creación de LSPs
- Agregar etiquetas a los paquetes con la información de la tabla.
- Envío del paquete

Se mostrará el funcionamiento de MPLS separándolo en dos componentes: envío

de paquetes y control de la información.

b.1) Envío de Paquetes

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son unidireccionales (simplex) por naturaleza; el tráfico bidireccional (dúplex) requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un conmutador de etiquetas (LSR) a otro, a través del dominio MPLS.

El envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de enrutamiento definidos por el ATM Forum; en lugar de ello, se utiliza el protocolo RSVP o bien un nuevo estándar de señalización LDP (Label Distribution Protocol).

Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Por ejemplo, si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. No es necesario administrar dos arquitecturas diferentes, lo que se haría transformando las direcciones y las tablas de enrutamiento IP en las direcciones y el enrutamiento ATM. Este problema lo resuelve el procedimiento de intercambio de etiquetas MPLS.

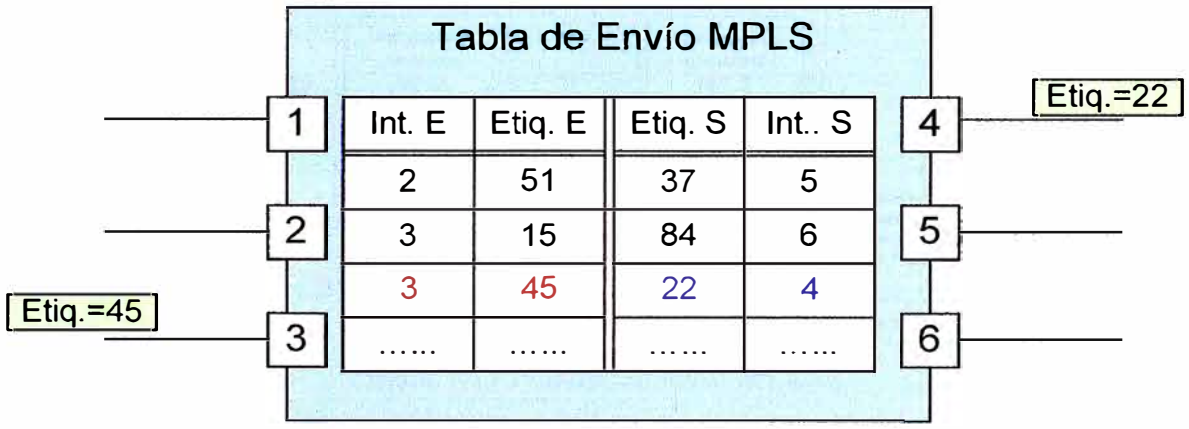


Figura 1.12 LSR Label Switching Router

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un enrutador que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de enrutamiento que

proporciona la componente de control.

Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada/salida correspondientemente, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola), en la figura 1.13 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS.

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 1.13 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Así mismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.

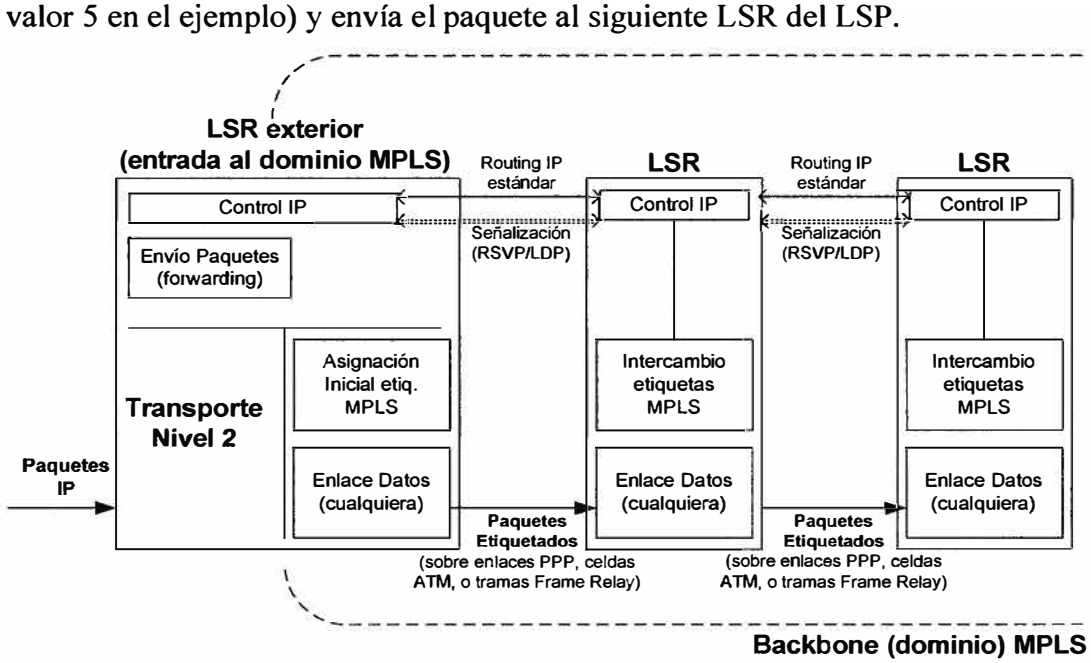


Figura 1.13 Funcionamiento del LSR

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar un paquete al LSR de cola (salida), este determina que el siguiente salto va fuera de la red MPLS, por lo que al consultar la tabla de conmutación de etiquetas, remueve la etiqueta y envía dicho paquete por enrutamiento convencional. Así, la identidad del paquete IP original queda enmascarada durante el transporte por la red MPLS.

Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las

especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (ATM, Frame Relay, etc.), se pueden utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (i.e. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del nivel 3.

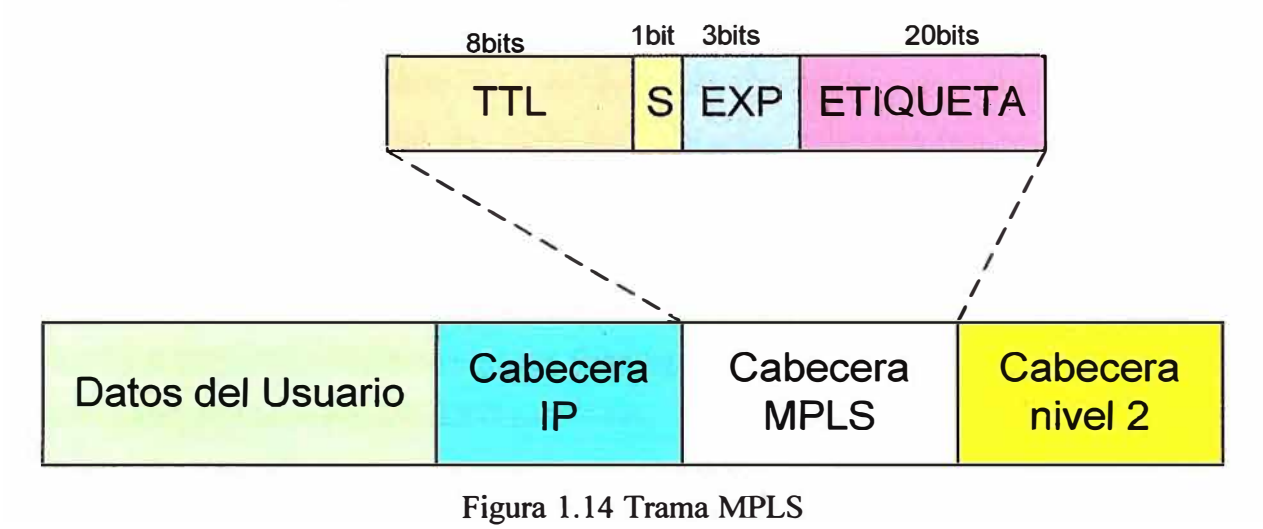


Figura 1.14 Trama MPLS

En la figura 1.14 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Los 32 bits de la cabecera MPLS se reparten en:

- 20 bits para la etiqueta MPLS.
- 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS).
- 1 bit de pila (stack) para poder apilar etiquetas de forma jerárquica.
- 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP.

b.2) Control de la Información

Se ha revisado el mecanismo básico de envío de paquetes en MPLS. Se revisarán dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs.
- Cómo se distribuye la información sobre las etiquetas a los LSRs.

Las tablas de envío se generan con la información que se tiene sobre la red, tales como topología, patrón de tráfico y características de los enlaces, entre otros. Esta

información es la que manejan los protocolos internos IGP (OSPF, IS-IS, RIP) para construir sus tablas de enrutamiento. MPLS utiliza esta información de estos protocolos para establecer los caminos virtuales o LSPs.

Para cada "ruta IP" en la red se crea un camino de etiquetas, concatenando las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización", necesaria siempre que se quiera establecer un circuito virtual. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas. De hecho, se están estandarizando diferentes protocolos para tal fin. Entre los protocolos existentes que se extienden para soportar MPLS, se encuentra el protocolo RSVP y BGP en las formas conocidas como MPLS-BGP, MPLS-RSVP-TUNNELS. También se están definiendo nuevos protocolos específicos para la distribución de etiquetas, como lo es el LDP (Label Distribution Prtocol) y CR_LPD (Constraint Based Routing Label Protocol). RSVP es preferido por IETF, LDP por Cisco y el CR_LPD por Nokia.

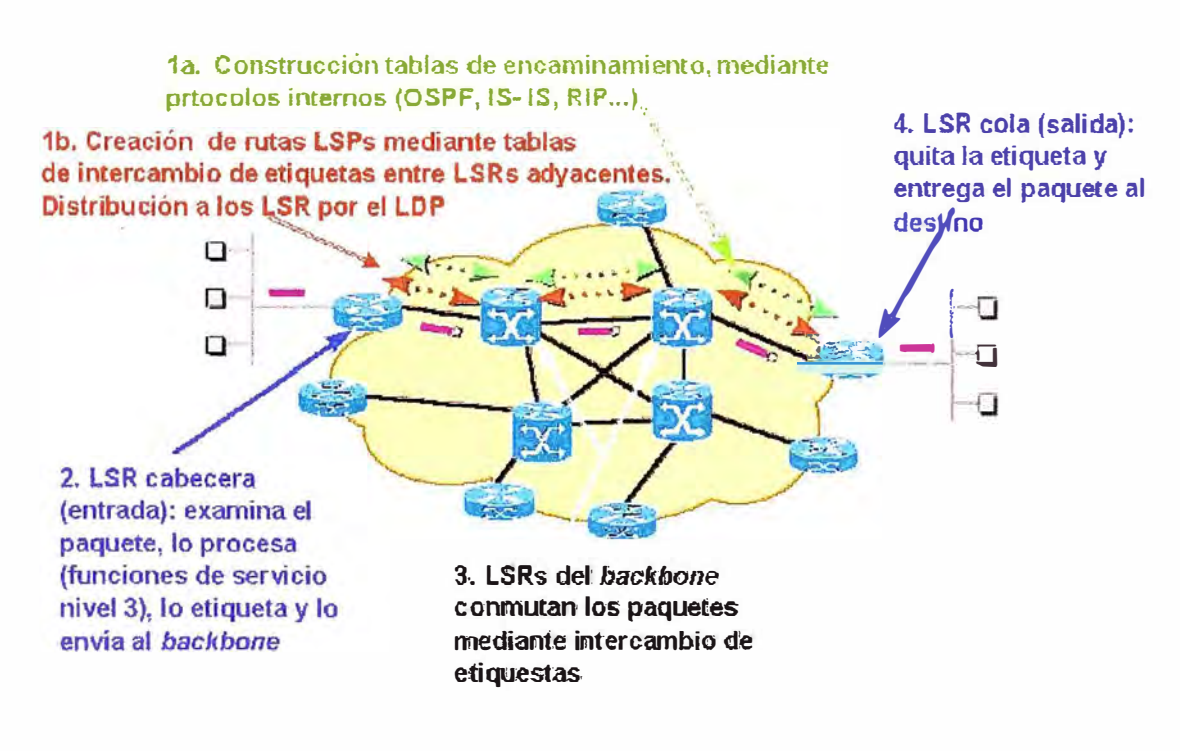


Figura 1.15 Funcionamiento MPLS

Las diferentes variaciones en el intercambio de etiquetas son:

- LDP: mapea los destinos IP (unicast) en etiquetas.
- RSVP, CR_LDP: es usado para ingeniería de tráfico y reserva de recursos.

- BGP: para etiquetas externas (VPN).

La figura 1.15 muestra el esquema global de funcionamiento de MPLS, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de enrutadores a una distancia de un sólo salto.

Esta unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de enrutadores). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y no se pierde la visibilidad sobre los paquetes IP. Esto abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

1.3 Acceso Seguro: Citrix

1.3.1 Servidor de Presentación (Citrix Presentation Server)

Citrix Presentation Server es un estándar del sector para la distribución de aplicaciones Windows al más bajo coste y a cualquier destino. Sus métodos de presentación virtual de aplicaciones y de distribución de aplicaciones mediante streaming facilitan el acceso de los usuarios desde cualquier dispositivo y a través de cualquier tipo de red. Con Presentation Server la distribución de aplicaciones representa un servicio que proporciona acceso a aplicaciones según lo piden los usuarios, al tiempo que permite una gran flexibilidad a la hora de utilizar arquitecturas de aplicación futuras.

Ya sea con equipos de sobremesa o portátiles con Windows, Macintosh, UNIX o Linux, dispositivos cliente de baja interactividad, terminales basados en Windows, dispositivos inalámbricos u otros aparatos en red, las soluciones de Citrix Presentation Server pueden utilizarse para:

- Ofrecer control de acceso seguro a medida en cualquier situación.
- Ofrecer acceso ininterrumpido a través de dispositivos, redes y ubicaciones.
- Ofrecer capacidad de ampliación y disponibilidad permanente en cualquier situación empresarial.
- Proteger la información a través de una arquitectura segura multidimensional.
- Controlar, supervisar y evaluar con mediciones los recursos de la infraestructura de acceso.

El Citrix Presentation Server permite que varios usuarios inicien sesión y ejecuten aplicaciones en sesiones independientes y protegidas del mismo servidor o de varios

servidores. Citrix Presentation Server se instala en equipos que ejecuten los Servicios de Windows Terminal Server, y las aplicaciones y demás recursos que se quieran distribuir se instalan y publican en servidores que ejecuten Citrix Presentation Server.

Por ejemplo, si quisiéramos instalar aplicaciones de productividad de oficina (procesadores de texto y hojas de cálculo), aplicaciones de planificación de recursos de empresa (SAP y PeopleSoft) u otras aplicaciones personalizadas, podríamos agrupar varios servidores para formar una comunidad de servidores. Cada comunidad de servidores está formada por un grupo de equipos administrados como una entidad. Las comunidades de servidores permiten distribuir aplicaciones y contenido a los usuarios de una forma flexible y eficaz.

1.3.2 Integración de la Interfaz Web de Citrix con el servidor web

Con la Interfaz Web se puede conceder a los usuarios acceso a los recursos publicados en Internet o en la Intranet. Los usuarios inician sesión en la Interfaz Web mediante un explorador Web normal y ven los enlaces a las aplicaciones que están autorizados para ejecutar.

La Interfaz Web crea dinámicamente una página HTML que muestra la comunidad de servidores para cada usuario. Después de iniciar sesión, cada usuario ve su página Web, personalizada con las aplicaciones y recursos que se hayan configurado. Con la Interfaz Web puede crear sitios Web independientes desde los que acceder a aplicaciones o sitios Web que puedan integrarse en el portal de la empresa.

La Interfaz Web puede utilizarse con Secure Gateway o Access Gateway para transferir datos con seguridad por Internet, ya que utiliza una tecnología de seguridad basada en estándares. Para controlar el acceso seguro a las aplicaciones en los equipos que ejecutan Presentation Server, puede usar las directivas y filtros de control de acceso de Access Gateway.

La edición Platinum permite la integración de la Interfaz Web con las funciones de autoservicio de Password Manager: autoservicio de desbloqueo de cuentas y restablecimiento de contraseñas. Puede configurar el servicio Password Manager y hacer que los usuarios registren una serie de preguntas de seguridad cuando inicien el agente de Password Manager. Cuando estas preguntas de seguridad están registradas, los usuarios pueden restablecer sus contraseñas de dominio o desbloquear sus cuentas de dominio desde la Interfaz Web, sin necesidad de que intervenga el equipo de asistencia técnica o un administrador del sistema.

1.3.3 Clientes de Citrix Presentation Server para un acceso remoto seguro

Citrix utiliza el protocolo ICA (Independent Computing Architecture) para intercambiar información entre el dispositivo cliente de un usuario y los recursos publicados en el equipo que ejecuta Citrix Presentation Server. El software de cliente de Citrix Presentation Server está disponible para varios dispositivos diferentes con el fin de que los usuarios puedan conectarse a aplicaciones publicadas desde distintas plataformas.

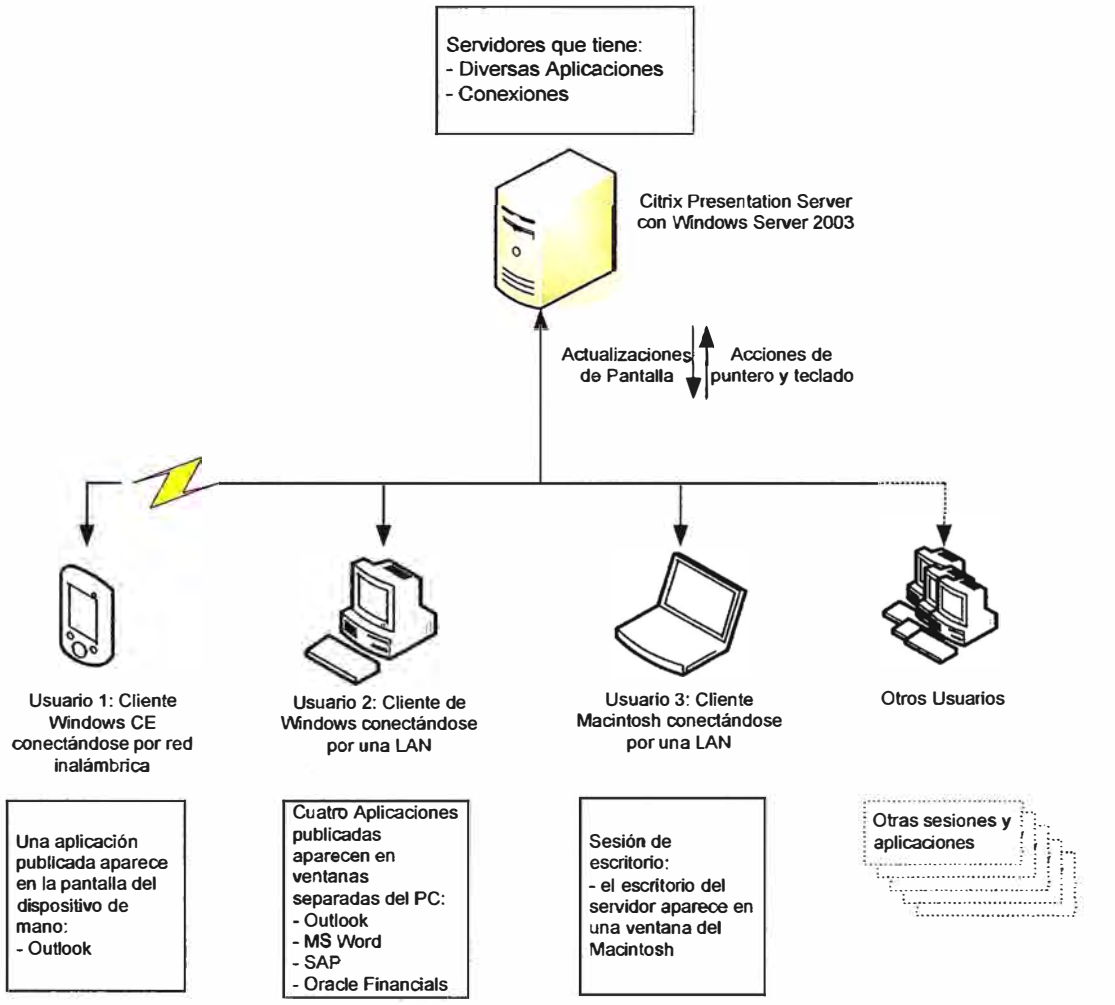


Figura 1.16 Conexiones con Citrix

La figura 1.16 muestra diversos clientes de Citrix Presentation Server conectándose a una comunidad de servidores y accediendo a aplicaciones y recursos publicados.

Los contenidos o las aplicaciones se publican una sola vez en el servidor, pero varios usuarios pueden acceder a ellos simultáneamente. El procesamiento de las aplicaciones en el cliente se mantiene en unos niveles mínimos, pues las aplicaciones se ejecutan totalmente en el servidor. El protocolo ICA envía las acciones del teclado y el puntero, así como las actualizaciones de pantalla entre el servidor y el cliente, por lo que el usuario del dispositivo cliente tiene la impresión de que el software se está ejecutando de

forma local.

Como las aplicaciones se ejecutan en el servidor y no en el dispositivo cliente, los usuarios pueden conectarse desde cualquier plataforma. Por ejemplo, Microsoft Outlook ejecutándose como aplicación publicada tiene el mismo aspecto y se utiliza igual tanto si el usuario se conecta desde un sistema de mano Windows CE como si lo hace desde un portátil Macintosh o una estación de trabajo Linux.

Además, para evitar que se consuman demasiadas licencias o recursos del servidor, es posible controlar las conexiones de los usuarios al servidor.

Con muchos clientes (incluidos los clientes para Windows, Java, Macintosh y Linux), se pueden proteger las comunicaciones ICA mediante los protocolos Secure Socket Layer (SSL) o Transport Layer Security (TLS). Estos protocolos ofrecen autenticación del servidor, cifrado del flujo de datos y comprobaciones de integridad de los mensajes, lo que garantiza la entrega segura de aplicaciones dentro de una LAN o en Internet.

1.3.4 Tráfico seguro en Internet (Secure Gateway)

Secure Gateway es una puerta de enlace con Internet para el envío y recepción de datos ICA en comunidades de servidores. Con Secure Gateway se puede proteger la seguridad de todo el tráfico de datos que pasa por Internet entre equipos en los que se ejecuta Citrix Presentation Server y estaciones de trabajo de clientes con SSL. El uso de Secure Gateway facilita el paso por los servidores de seguridad (o cortafuegos) y aporta mayor seguridad, ya que se establece un único punto de entrada y acceso seguro a las comunidades de servidores.

1.3.5 Consolas para la administración de la distribución

Citrix dispone de dos consolas para administrar los servidores y las comunidades de servidores, localmente y de forma remota.

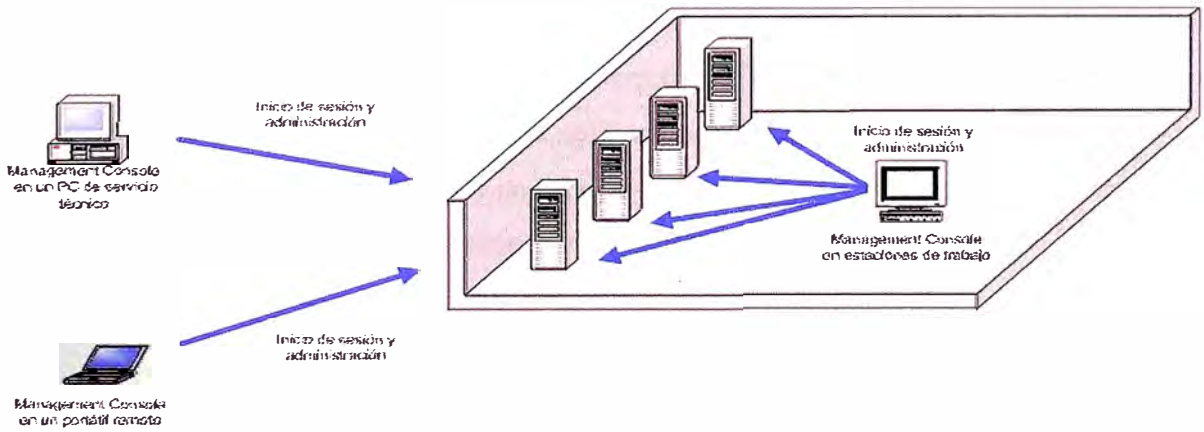


Figura 1.17 Supervisión de Plataforma

En la figura 1.17 se muestra la supervisión local y remota de una comunidad de servidores mediante las consolas de administración.

1.3.6 Consola de Accesos (Access Management Console de Citrix)

Se utiliza Access Management Console para administrar las propiedades de las aplicaciones, servidores y comunidades. Se puede crear diversos informes, configurar el acceso a las aplicaciones (a través de la Interfaz Web y del Agente de Program Neighborhood) y dar soporte a los inicios de sesión de participantes invitados de Conference Manager. Además, puede usar esta consola para configurar tareas de supervisión de estado, solucionar problemas notificados por alertas, diagnosticar problemas en la comunidad de servidores, ver información de hotfix para los productos Citrix y hacer un seguimiento de los cambios administrativos realizados con la consola.

Access Management Console ofrece ventajas adicionales para los clientes que adquirieron la edición Platinum: un punto centralizado para la administración y supervisión de la gestión de contraseñas, SmartAccess, y otras funciones de control de acceso de la edición Platinum.

1.3.7 Consola de Presentación (Presentation Server Console de Citrix)

Usar Presentation Server Console para conectar con cualquier comunidad de servidores del sistema, configurar directivas e impresoras, y para administrar zonas y entornos de aislamiento de aplicaciones de toda la comunidad. Use esta consola para acceder a los componentes de administración disponibles sólo en las ediciones Advanced y Enterprise de Citrix Presentation Server.

1.3.8 Soluciones ampliables para una integración de funciones perfecta

Aunque existen diversas soluciones en Citrix Presentation Server con muchas funciones adicionales, se puede instalar sólo las funciones necesarias en cada servidor y personalizar éste de acuerdo con las necesidades y la función del servidor en la organización. Entre estas funciones destacan: equilibrio de carga, análisis y supervisión de sistemas, empaquetado y distribución de aplicaciones, supervisión del rendimiento de los servidores, distribución de aplicaciones mediante despliegue sin necesidad de descarga (streaming), y servicios de presentación y organización de reuniones.

1.3.9 Servidor de Presetación Versión Platinum

Citrix Presentation Server Platinum Edition es la solución completa, específicamente diseñada para grandes organizaciones y empresas que necesitan un acceso integral y seguro a las aplicaciones, con capacidad de supervisión de rendimiento y gestión

de contraseñas. Está diseñado para grandes organizaciones y empresas multinacionales que proporcionan acceso continuado y que necesitan identificar rápidamente problemas de rendimiento de red y aplicaciones.

Platinum Edition incluye, además de todas las funciones de Enterprise Edition, lo siguiente:

a) Supervisión del rendimiento de aplicaciones mediante Citrix EdgeSight para Presentation Server. Es una solución de supervisión de rendimiento de extremo a extremo para equipos que ejecutan Citrix Presentation Server. Este componente supervisa las sesiones de usuario y rendimiento de servidores en tiempo real, lo que permite analizar, resolver y prevenir problemas. Se utiliza EdgeSight para asegurar que los usuarios de la organización tienen en todo momento los recursos necesarios para trabajar más productivamente.

b) Gestión de contraseñas mediante Citrix Password Manager para Presentation Server. Es una solución de inicio de sesión unificado (SSO o single sign-on) para grandes empresas y organizaciones, que ofrece un acceso seguro y controlado a aplicaciones de Windows, aplicaciones Web y aplicaciones basadas en host que se ejecutan en el entorno Citrix, así como a las aplicaciones locales del escritorio. Los usuarios sólo tienen que autenticarse una vez y Password Manager se encarga del resto, iniciando automáticamente la sesión en sistemas de información protegidos por contraseña, aplicando directivas de contraseñas, supervisando todos los sucesos relacionados con contraseñas, e incluso automatizando las tareas de los usuarios finales, cambios de contraseña inclusive.

c) Acceso remoto seguro mediante Citrix Access Gateway. Es un dispositivo universal VPN con SSL que ofrece un punto de acceso único, ininterrumpido y seguro para todas las aplicaciones y protocolos. Dispone de todas las ventajas de las VPN IPSec y SSL, pero sin su costosa y complicada implementación y administración. Los clientes que adquieren Access Gateway y la edición Platinum tienen derecho a la edición Advanced de Access Gateway que incluye Advanced Access Control. Advanced Access Control sirve para ajustar con precisión el control sobre los recursos a los que los usuarios tienen acceso y las acciones que dichos usuarios pueden realizar, facilitando así el cumplimiento del reglamento de la organización. Access Gateway ofrece el mejor acceso para todos: acceso seguro a la información para la empresa, acceso sencillo para los usuarios, y gestión sencilla para el departamento de IT.

d) Smart Access: el nivel de acceso adecuado se concede en función de las condiciones de

acceso, lo cual supone una garantía de seguridad. Estas condiciones de acceso son, por ejemplo, el tipo de usuarios y el lugar donde se encuentren, así como el dispositivo y la red que utilicen. En cada caso, se conceden distintos niveles de acceso, como la posibilidad de ver documentos sin modificarlos. Advanced Access Control proporciona SmartAccess en dos fases clave: detección y respuesta. En la fase de detección de SmartAccess, el sistema analiza el caso de acceso del usuario y luego responde con el nivel de acceso apropiado. Acceso permitido o acceso denegado ya no son las únicas respuestas que se pueden esperar de un intento de acceso, porque las organizaciones no sólo controlan a qué recursos tiene acceso cada usuario, sino cómo puede usar el usuario sus recursos una vez conseguido el acceso a ellos. Por ejemplo, un usuario que se encuentra en la cabina pública de Internet de un aeropuerto puede que sólo tenga permiso para ver o leer los archivos adjuntos al correo electrónico, pero no para descargar, modificar o imprimir esos archivos. No obstante, cuando ese mismo usuario trabaja desde su casa, sí dispondrá de todas las funciones para descargar, modificar e imprimir archivos. Además, Advanced Access Control se integra completamente con Citrix Presentation Server, con lo que aporta a las empresas el mismo nivel de control granular sobre las aplicaciones publicadas.

e) SmoothRoaming: Advanced Access Control es compatible con la tecnología SmoothRoaming, por lo que, cuando los usuarios se conectan desde varios dispositivos, redes y ubicaciones, el nivel de acceso adecuado para cada entorno de acceso se configura automáticamente.

f) Diseño Seguro: Advanced Access Control proporciona a los usuarios un acceso que es seguro por definición, capaz de proteger tanto la seguridad de la información de la empresa como la integridad de la red.Las tecnologías SmartAccess, SmoothRoaming y Diseño seguro (Secure by Design) colaboran mediante la combinación de las siguientes funciones:

- Seguridad integrada de punto final. Ofrece supervisión continuada en tiempo real para garantizar que los dispositivos pueden conectarse y permanecer conectados a la red con seguridad. El análisis de seguridad en el cliente evalúa la integridad de los dispositivos conectados y permite adaptar el nivel de acceso concedido, creando directivas, según los resultados del análisis.
- Conectividad VPN. Los recursos de red permiten conectividad de red privada virtual (VPN) directa con SSL a servidores, servicios y redes dentro de la red local (LAN) de la organización.
- Controles de acción. Permite a los administradores definir unas directivas para permitir

o denegar acceso de vista, modificación y guardado de documentos dependiendo de la identidad del usuario, el dispositivo y conexión que utilice y su ubicación.

- Compatibilidad con dispositivos móviles. Modifica las interfaces de correo electrónico y archivos para funcionar con PDA y otros dispositivos de pequeño tamaño.
- Acceso de sólo explorador. Permite el acceso a sitios Web, archivos y correo electrónico, con cualquier explorador Web en cualquier dispositivo. Se pueden representar automáticamente documentos de Microsoft Office para Presentación preliminar de HTML.
- Acceso seguro a archivos y correo electrónico basados en Web. Da acceso seguro al correo electrónico de la organización a través de Internet en una interfaz de usuario basada en Web. Permite que los usuarios accedan de forma segura a Microsoft Outlook y Lotus Notes en tiempo real y sincronicen la información para utilizarla sin conexión. Permite acceder de forma segura por Internet a los archivos compartidos de la red de la empresa mediante una interfaz Web.
- Integración avanzada con Presentation Server. Se puede utilizar el análisis de seguridad en el cliente y la ubicación del cliente para controlar las aplicaciones publicadas que están a disposición del usuario. Esta función amplía SmartAccess a Presentation Server, incluido el uso de filtros de Advanced Access Control para controlar la asignación de unidades del cliente local, operaciones de portapapeles y asignación de impresoras locales.
- Respaldo multilingüe. Proporciona respaldo completo de servidor y cliente para japonés, alemán, francés y español.
- Cifrado basado en estándares. Utiliza el cifrado SSL estándar para ofrecer acceso seguro a los recursos de la empresa.
- Plataforma de administración común. Proporciona una estructura unificada que incluye la configuración de cliente y servidor, el sistema de licencias, la supervisión y las herramientas de informes para brindar simplicidad administrativa, visibilidad empresarial y seguridad de la empresa.

CAPÍTULO II
PLANEAMIENTO DEL PROYECTO

2.1 Descripción

Hacia el año 2002, una empresa corporativa tenía diversos medios para que las empresas colaboradoras se conecten a la red interna, así como diversos tipos de seguridad para cada aplicativo que necesitara utilizar.

En ese año, el número de empresas colaboradoras se incrementó notablemente, y por ende el número de usuarios que necesitaban utilizar aplicativos de la empresa colaboradora se hizo inmanejable y no seguro para los fines que esperaba la empresa corporativa.

En dicho sentido, se planteó el proyecto de estandarizar todo lo referencia a la gestión de accesos y asegurarlos para poder brindar un mejor control y mejores servicios para los clientes finales de la empresa corporativa.

2.2 Antecedentes

2.2.1 Empresas Colaboradoras

La empresa corporativa clasificaba a sus empresas colaboradoras en los siguientes tipos:

a) Autorizadas: son aquellas empresas privadas que hacen convenios con la empresa corporativa para brindar los servicios de venta. La infraestructura (equipamiento de la oficina) es de la empresa privada.

b) Blindadas: son aquellas oficinas que la empresa corporativa implementa en su totalidad (local e infraestructura tecnológica) y que otorga en concesión a una empresa privada para que la administre y brinde los servicios de venta, post venta y cobros.

La empresa corporativa tenía un total de 177 empresas colaboradoras distribuidas en todo el Perú de acuerdo al TABLA N◦ 2.1.

2.2.2 Medios de Comunicación

Las empresas colaboradoras accedían a los diversos aplicativos de la empresa corporativa de acuerdo a los siguientes tipos de medios de comunicación:

a) Enlace Línea Dedicada: es aquel enlace Interlan de 64kbps que lo proveía una empresa de comunicaciones.

TABLA N° 2.1 Distribución de Agencias

Empresa Colaboradora	Lima	Provincias	Total
Autorizada	23	123	146
Blindada	20	11	31
Total	43	134	177

Figura 2.1 Distribución de Empresas Colaboradoras

b) Enlace Infovía: es aquel enlace que utiliza el acceso Internet con velocidad de 54 Kbps y utiliza el acceso telefónico. Lo proveía otra empresa de comunicaciones.

c) Enlace Infomóvil: es aquel enlace que utiliza un equipo celular para transmisión de datos con velocidad máxima de 14.4 Kbps de datos por la red inalámbrica. Lo proveía la empresa corporativa.

La distribución del total de empresas colaboradoras sobre el uso de los medios de comunicación indicadas se detallan en el TABLA N° 2.2.

2.2.3 Seguridad en Accesos

La seguridad que se utilizaba para el acceso a los diversos aplicativos de la empresa corporativa era:

a) Servicio VPN: se tenía un servidor con VPN Microsoft implementado en una DMZ definida para accesos de terceros a la red corporativa de la empresa corporativa. La seguridad pasaba por tener un cliente en la pc y se les brindaba un usuario y su clave para su acceso.

b) Aplicativo: las solicitudes de acceso a cada aplicativo de la empresa corporativa se hacía por diversos formatos existentes

c) Seguridad del Aplicativo: cada aplicativo tiene un usuario y clave definido para cada usuario, el mismo que se entregaba al representante legal de las empresas colaboradoras.

2.3 Problemática Encontrada

Para analizar la situación que se tenía, se recabó información para identificar los problemas. Los resultados obtenidos se muestran a continuación.

2.3.1 Medios de Comunicación

Se identificaron lo siguientes rubros:

- Caídas de los medios de comunicación
- Lentitud en los diversos aplicativos en las empresas colaboradoras
- Capacidad en Centro de Procesamiento de la Empresa Corporativa

a) Caídas de los medios de comunicación

La figura 2.3 muestra la estadística de incidencias registradas por problemas en las comunicaciones. El 77% de las empresas colaboradoras (136) tienen Infovía como medio de comunicación, el mismo que tuvo 55.64 caídas durante el período analizado (Enero 2001-Febrero 2002), lo que nos indica que el 41% de las mismas tuvo problemas.

b) Lentitud en los diversos aplicativos en las empresas colaboradoras

Se realizó una toma de muestras de tiempos de respuesta en algunos locales para el

Aplicativo Comercial (aplicativo principal) y el resultado se muestra en la TABLA N° 2.3. De igual forma se tomó tiempos de respuesta para el aplicativo comercial dentro de la red interna de la empresa corporativa y el resultado era de 5 segundos.

Esto evidenciaba que las operaciones en los aplicativos en las empresas colaboradoras no cumplen con las expectativas de la empresa corporativa para el servicio a sus clientes finales.

TABLA N° 2.2 Distribución de Agencias por Tipo de Enlace

Tipo: Autorizadas

Ubicación	Línea Dedicada	Infovía	Infomóvil	Total
Lima	21	2	0	23
Provincias	0	123	0	123
Total	**21**	**125**	**0**	**146**

Tipo Blindadas

Ubicación	Línea Dedicada	Infovía	Infomóvil	Total
Lima	7	0	13	20
Provincias	0	11	0	11
Total	**7**	**11**	**13**	**31**

Total de Agencias

Ubicación	Línea Dedicada	Infovía	Infomóvil	Total
Lima	34	2	7	43
Provincias	0	134	0	134
Total	34	136	7	177
Distribución	19%	77%	4%	100%

c) Capacidad en Centro de Procesamiento de la Empresa Corporativa

La línea dedicada utilizada por las empresas colaboradas era punto a punto, en dicho sentido, en el Centro de Procesamiento de Datos de la empresa corporativa se tenía tantos equipos de comunicaciones como enlaces se tenía. En dicho sentido, el espacio ocupado era de varios gabinetes. Esto originó que el crecimiento de este tipo de enlaces se

dejara suspendido por la no disponibilidad de espacio físico en el Centro de Procesamiento.

2.3.2 Aplicativos

Se identificaron lo siguientes rubros:

a) Fraudes

Se hizo un relevamiento de la cantidad de fraudes originados por las empresas colaboradoras y el resultado se muestra en la figura 2.4.

Figura 2.2 Distribución de Empresas Colaboradoras por Tipo Enlace

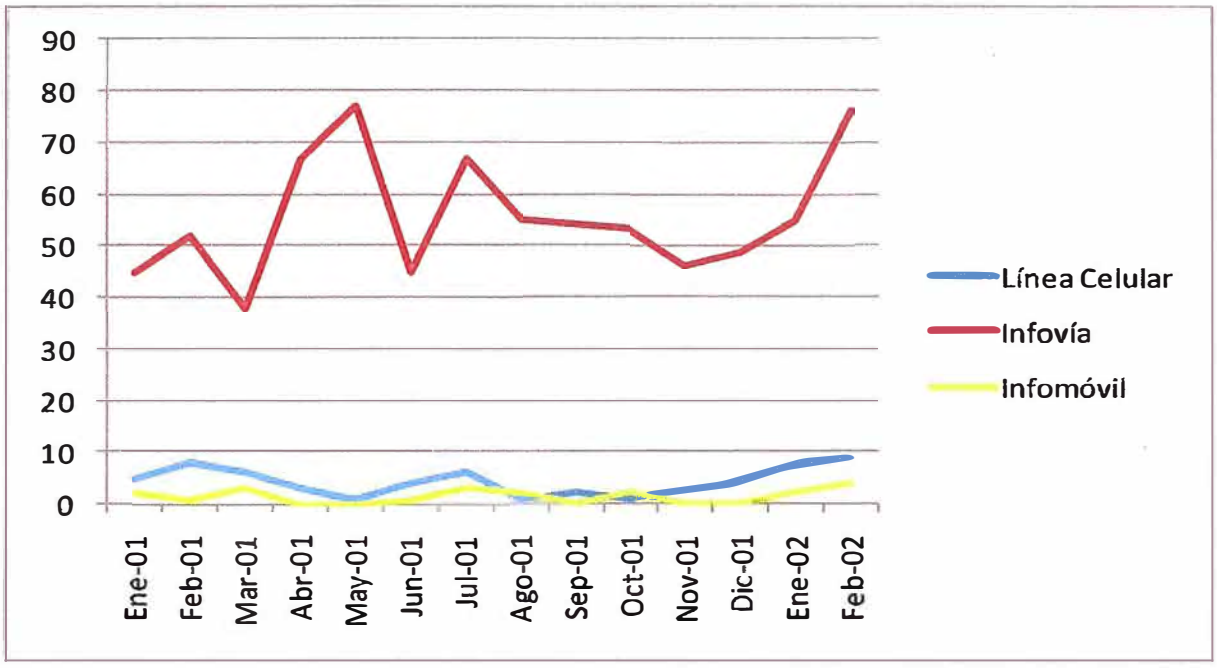


Figura 2.3 Histórico de caídas de los medios de comunicación

TABLA N° 2.3 Tiempos de respuesta por tipo de medio de comunicación

Tipo Medio	Empresa A	Empresa B	Empresa C	Promedio (seg)
Línea Dedicada	10	12	7	9.67
Infovía	43	54	48	48.33
Infomóvil	57	64	49	56.67

b) Atención de Requerimientos

Se hizo un relevamiento de los tiempos para los requerimientos de nuevos usuarios en los diversos aplicativos usados por la empresa colaboradora. Los resultados se muestran en el TABLA N° 2.4:

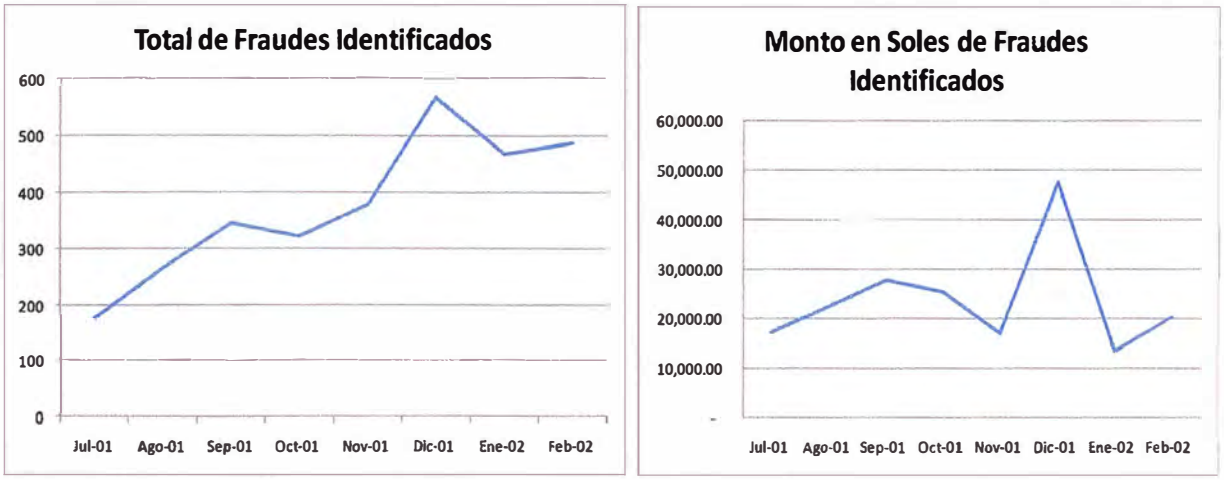


Figura 2.4 Histórico de Fraudes Identificados en Empresas Colaboradoras

TABLA N° 2.4 Tiempos de atención a requerimientos

Concepto		**Tiempo de Atención (Días)**
Medio de Comunicación	Enlace Dedicado	15
	Infovía	10
	Infomóvil	5
Equipos Comunicaciones	Configuraciones rutas, reglas	3
Aplicativos (*)	Aplicativo Corporativo	5
	Aplicativo Ventas	3
	Aplicativo Promociones	3

(*) Formato por cada aplicativo con un máximo de 5 requerimientos-usuarios (nuevos, cambios, eliminaciones)

CAPÍTULO III
INGENIERÍA DEL PROYECTO

3.1 Introducción

En el presente capítulo se detalla el desarrollo que se ha propuesto para solucionar los problemas detectados para la configuración existente y cuyo objetivo era el de normalizar los medios de comunicación y la seguridad inherente que debemos tener para el acceso a los aplicativos de la empresa colaboradora.

3.2 Premisas del Proyecto

3.2.1 Aplicativos

Para poder evaluar el consumo de ancho de banda, se han identificado los aplicativos que podría utilizar una empresa colaboradora:

- Comercial: aplicativo principal de la empresa corporativa donde se registran a los clientes y su historial.
- Ventas: aplicativo que se utiliza para registrar las ventas para su posterior liquidación en comisiones a las empresas colaboradoras.
- Promociones: aplicativo donde se publican las diversas campañas que se ofrecen a los clientes finales.

Se han realizado los análisis de consumos de ancho de banda de los diversos aplicativos en fechas y horas que se estimaron como de alta congestión. Los resultados son los indicados en las figuras 3.1 al 3.6.

Con el resultado de las pruebas, se definió el ancho de banda necesario por cada usuario cuando utiliza los tres (3) aplicativos, el mismo que se muestra en la TABLA N° 3.1.

De igual forma se tomaron tiempos de respuesta cuyo resultado se muestran en la TABLA N° 3.2.

3.2.2 Seguridad en el Acceso

Debido a las diversas evidencias de fraude que existía, se ha tomado la decisión que cada local de cada empresa colaboradora tenga un único identificador. En dicho sentido,

dentro la solución que se planteó que todo local de las empresas colaboradoras deberán contar con una única dirección (IP fija) que identifique cada dispositivo dentro la red que accederá a la red interna de la empresa corporativa.

Figura 3.1 Tiempos de Respuesta de Aplicativo Comercial del Día 1

Figura 3.2 Tiempos de Respuesta de Aplicativo Comercial del Día 2

3.2.3 Medios de Comunicación

Al revisar la cartera de los diversos tipos de medios de comunicación que ofrece una empresa de Telecomunicaciones y con la premisa definida del único identificativo por local se decidió que la empresa colaboradora utilice alguno de los medios indicados:

a) Accesos vía Enlace Internet: la solución fue utilizar la red ADSL y el producto elegido fue el Speedy Business, el cual nos asegura tener una única IP por local.

b) Accesos vía Enlace Dedicado: la solución fue utilizar la red MPLS y el producto es el IPVPN que cada empresa debe contratar con la empresa de Telecomunicaciones elegida.

Por el lado de la empresa corporativa se instaló cabeceras IPVPN en los CPD de la misma para tener alta disponibilidad en el acceso.

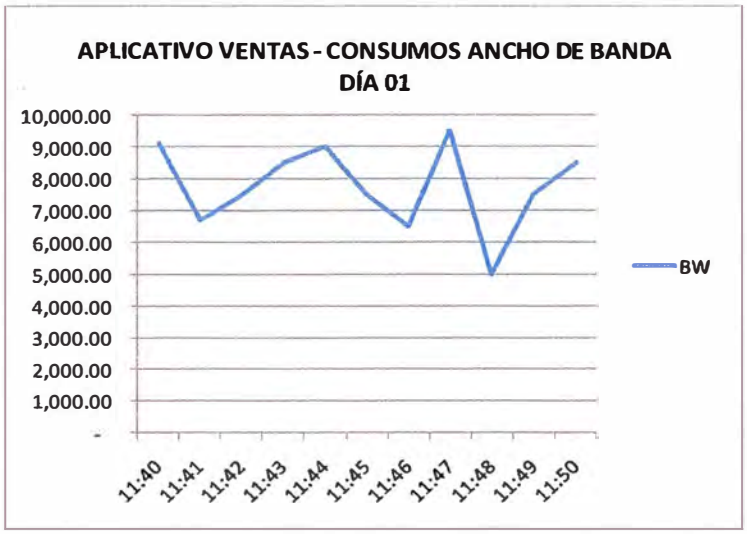


Figura 3.3 Tiempos de Respuesta de Aplicativo Ventas del Día 1

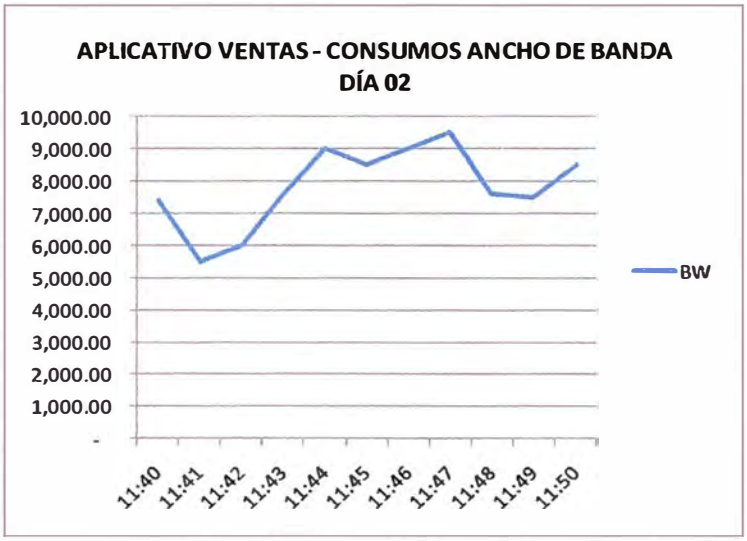


Figura 3.4 Tiempos de Respuesta de Aplicativo Ventas del Día 2

Las empresas colaboradoras tienen un máximo de 50 usuarios y para poder definir el ancho de banda a utilizar por cada empresa colaboradora se utilizó el cálculo de consumos de ancho de banda y cantidad de usuarios por cada local, en dicho sentido se han definido los tipos de enlace mostrados en la TABLA N° 3.3.

3.2.4 Aplicativos

Se revisaron los diversos formatos de solicitud de accesos y se definió un único formato de acceso, para lo cual se ha definido:

a) Perfiles por cada aplicativo.

b) Al personal de la empresa corporativa que podía autorizar el acceso de una empresa

colaboradora.

c) Datos mínimos que se deben solicitar a la empresa colaboradora.

Figura 3.5 Tiempos de Respuesta de Aplicativo Promociones del Día 1

Figura 3.6 Tiempos de Respuesta de Aplicativo Promociones del Día 2

TABLA N° 3.1 Consumos de BW por aplicativo

	APLICATIVO	BW (kpbs)
1	Comercial	15
2	Ventas	10
3	Promociones	06
	TOTAL	31

TABLA N° 3.2 Tiempos de Respuesta por Aplicativo

	APLICATIVO	Tiempo Respuesta (seg.)
1	Comercial	30
2	Ventas	22
3	Promociones	18

TABLA N° 3.3 Definición de Tipo de Enlace a usar

Cantidad de Usuarios	Tipo Enlace	Comentarios
Hasta 6	Speedy Business	El mínimo servicio es de 1Mbps con 10% asegurado
Entre 7 y 20	IPVPN 1Mbps	El uso de enlaces dedicados mejora el servicio a los usuarios de las empresas colaboradoras
Mayor a 20	IPVPN 2Mbps	

3.3 Diseño a Implementar

3.3.1 Arquitectura de Red

La arquitectura de red de accesos de las empresas colaboradoras se ha definido de acuerdo a la figura 3.7 y la figura 3.8

3.3.2 Estandarización de Accesos

Se ha definido un único formato de acceso cuyo diseño es el mostrado en la figura 3.9.

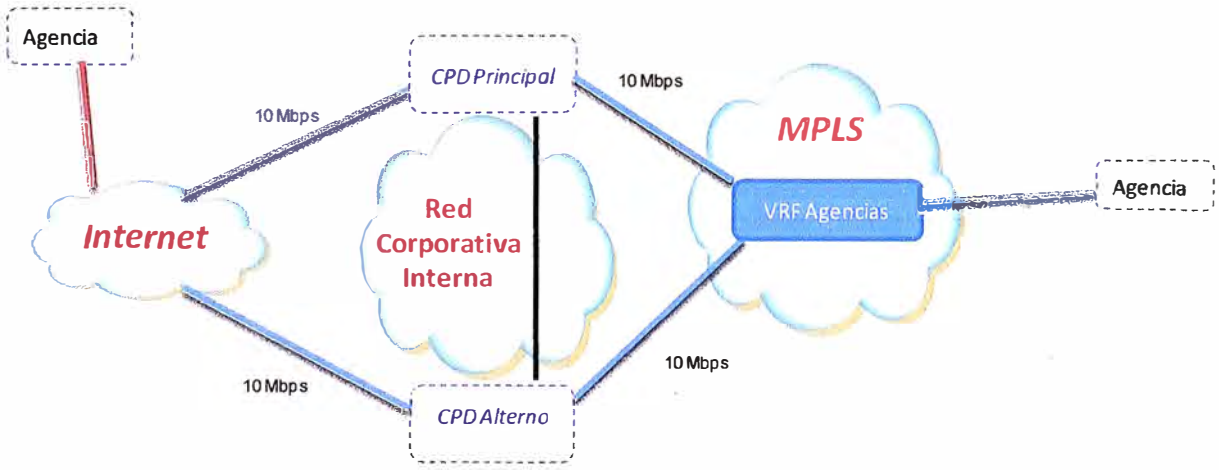


Figura 3.7 Arquitectura de Red Implementada

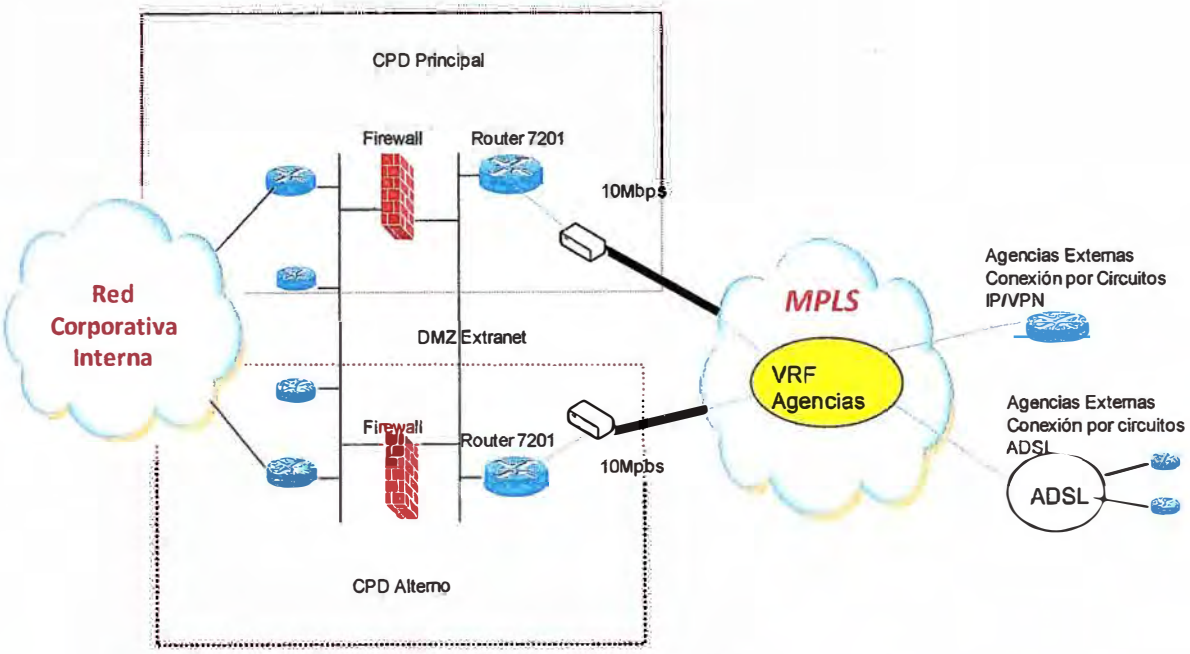
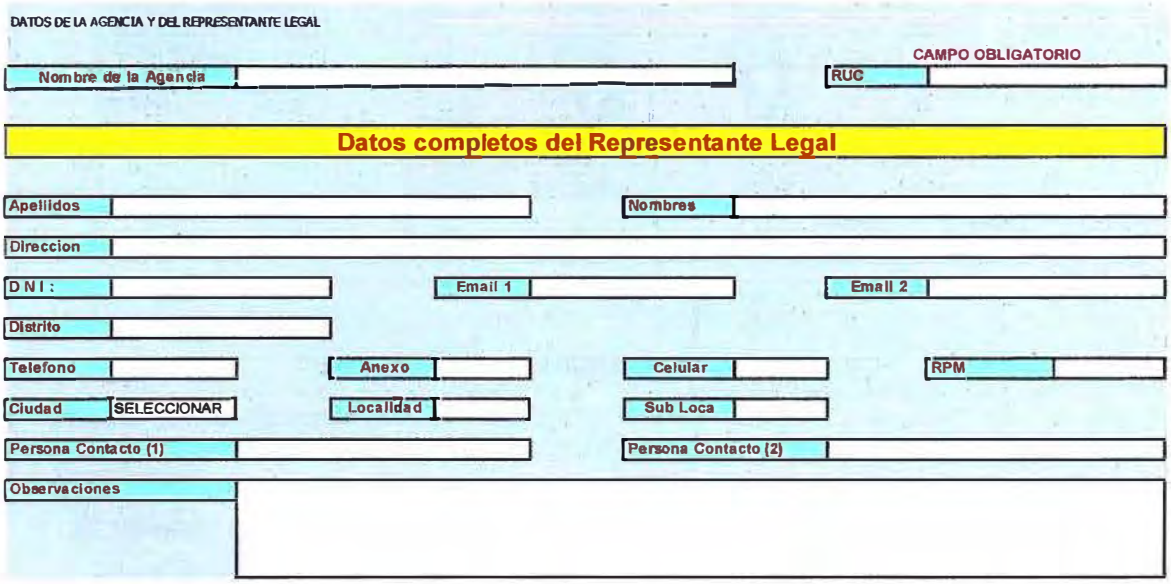


Figura 3.8 Arquitectura de Red Implementada

Datos del Autorizante

Datos de la Empresa Colaboradora



Datos de Aplicativos

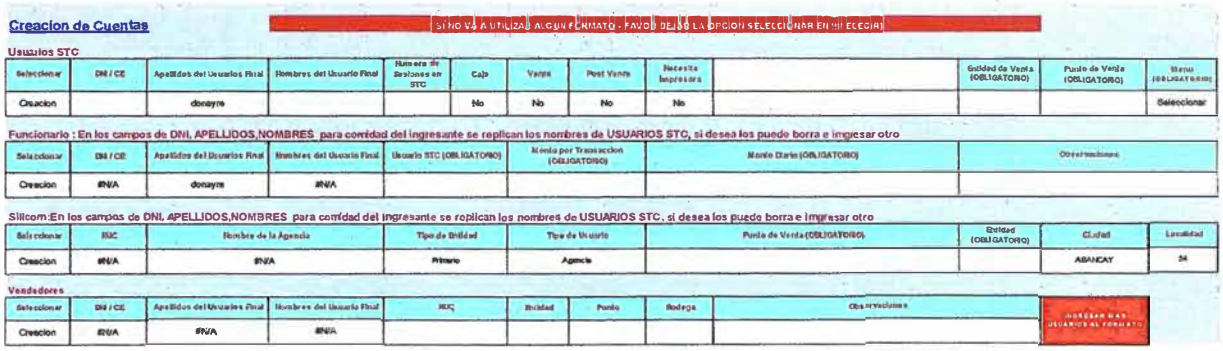


Figura 3.9 Detalle del formato único de accesos de empresas colaboradoras

3.3.3 Seguridad en Accesos

Se optó por la solución planteada por el proveedor Citrix cuya arquitectura de accesos se muestra en la figura 3.10.

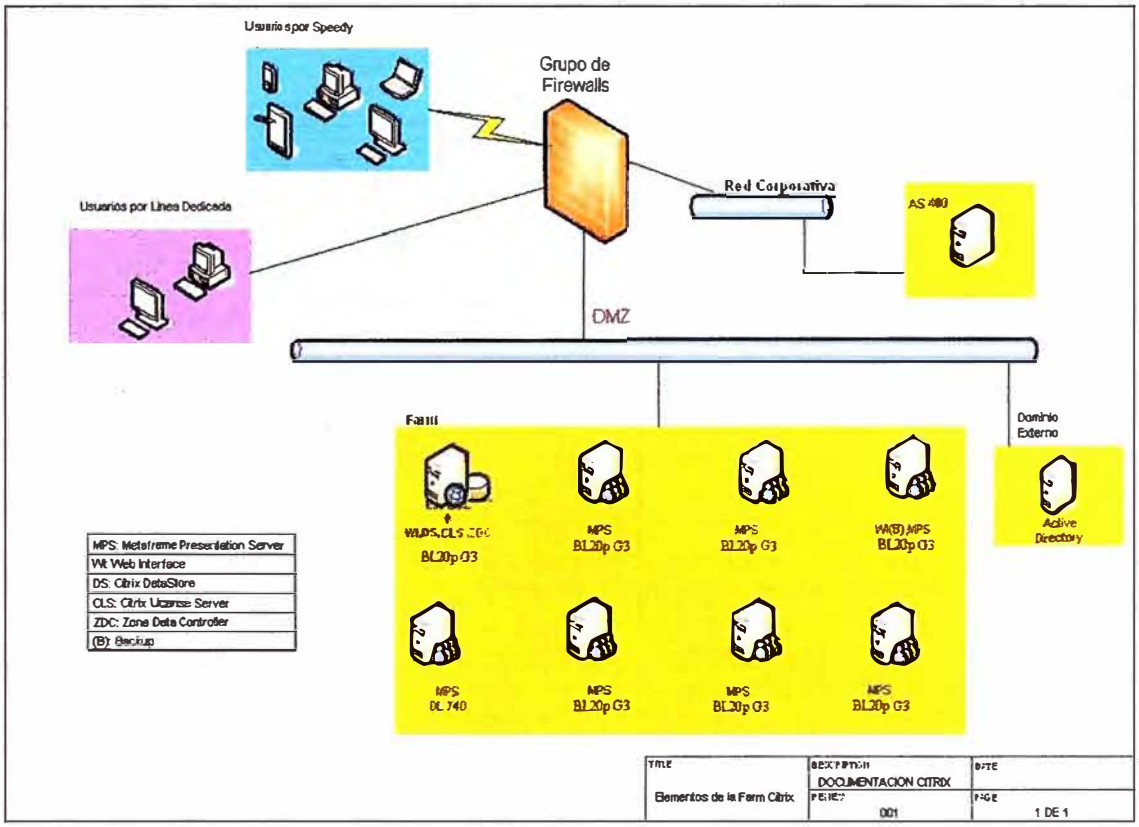


Figura 3.10 Arquitectura de Acceso Seguro

3.4 Puesta en Producción

3.4.1 Despliegue

El alcance del proyecto ha involucrado un total de 65 locales (37% del total) los mismos que se distribuyeron según la TABLA N◦ 3.4.

TABLA N° 3.4 Cantidad de Empresas involucradas en Proyecto

Tipo Acceso Empresa Colaboradora	Cantidad
Empresa con acceso Internet	40
Empresa con acceso IPVPN 1Mbps	20
Empresa con acceso IPVPN 2Mbps	5
TOTAL	**65**

La distribución de locales a nivel Perú se muestra en la figura 3.11.

Figura 3.11 Distribución de Agencias

Los anchos de banda definidos para el acceso central a ubicarse en los Centros de Procesamiento de Datos se indican en la TABLA N° 3.5.

TABLA N° 3.5 Ancho Banda a usar en Centro Procesamiento de Datos

Tipo de acceso en Centro de Procesamiento de Datos	BW (Mbps)
Acceso Internet	5Mbps
Acceso IPVPN	10Mbps

3.4.2 Resultados de la Implementación

Se realizó una revisión al término del despliegue de todos los locales y se tomaron muestras cuyos resultados se grafican en las figuras 3.12 y 3.13.

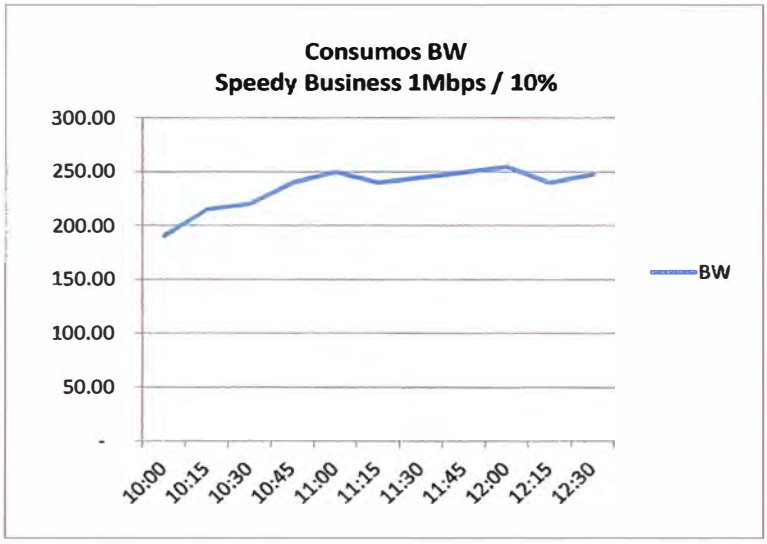


Figura 3.12 Ancho de Banda en Empresas Colaboradoras Enlace Speedy Business

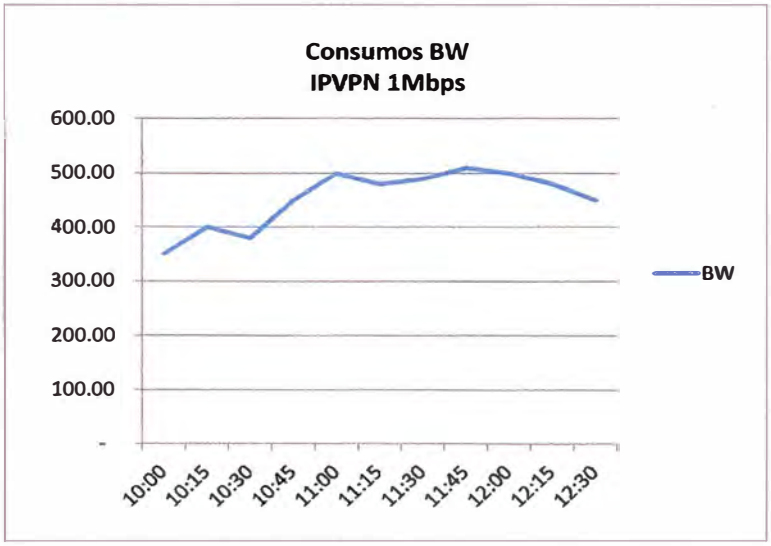


Figura 3.13 Ancho de Banda en Empresas Colaboradoras Enlace IPVPN

Se evaluó el consumo de ancho de banda de las cabeceras y el resultado se muestra en las figuras 3.14 y 3.15.

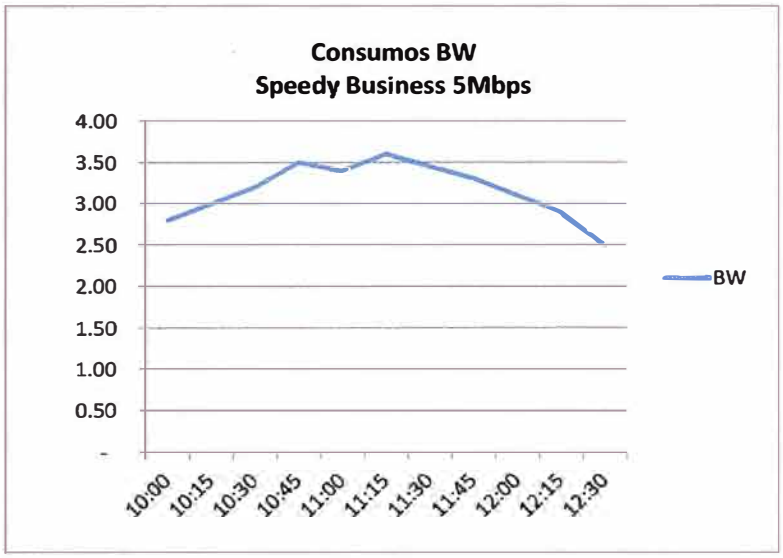


Figura 3.14 Ancho de Banda en Empresa Corporativa para Speedy Business

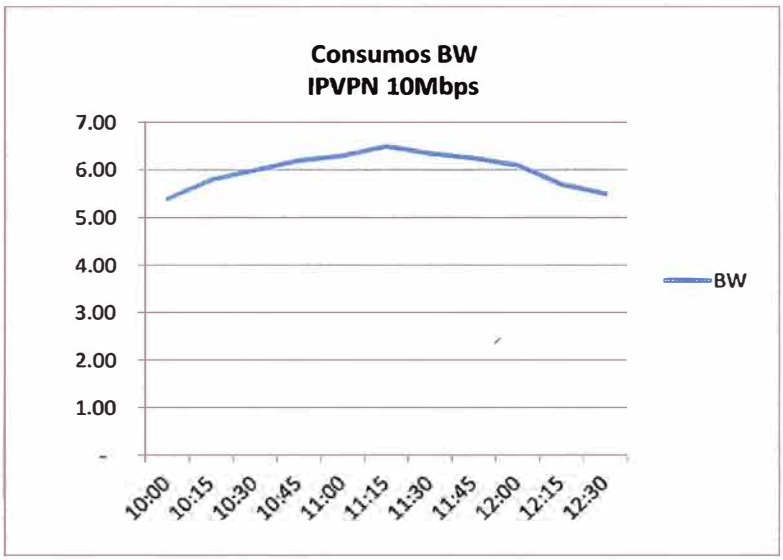


Figura 3.15 Ancho de Banda en Empresa Corporativa para enlace IPVPN

De igual forma se midieron tiempos de respuesta, cuyos resultados se muestran en la TABLA N◦ 3.6.

TABLA N◦ 3.6 Tiempos de Respuesta por Aplicativo

	APLICATIVO	Tiempo Respuesta (seg.)
1	Comercial	10
2	Ventas	7
3	Promociones	6

3.4.3 Equipamiento Utilizado

Los diversos equipos que se han utilizado en la implementación se muestran en las figuras 3.17 al 3.19.

Figura 3.17 Equipo utilizado en Enlaces Dedicados (IPVPN) en Empresas Colaboradoras CISCO ROUTER 2801

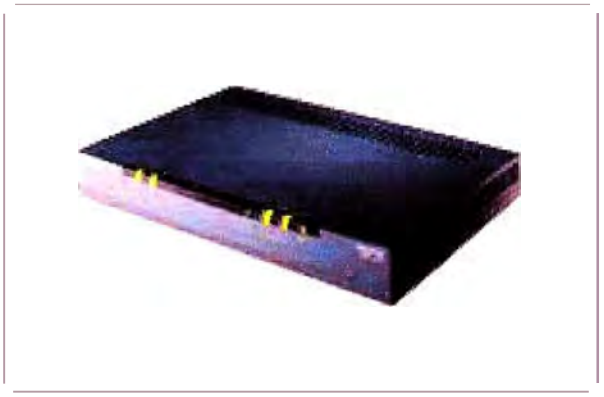


Figura 3.18 Equipo utilizado en Enlaces Interent (Speedy Business) en Empresas Colaboradoras (ZYXEL 643)

Figura 3.19 Equipo utilizado en Centro Procesamiento de Datos (Citrix Access Gateway)

3.4.4 Configuraciones Utilizadas

En las figuras 3.20 al 3.26 se muestran algunas de las configuraciones realizadas en los equipos de la plataforma implementada.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management]
"DisablePagingExecutive"=dword:00000001
"NonPagedPoolSize"=dword: 00000000
"PagedPoolSize"=dword: 20000000
"SystemPages"=dword:00003000
"PoolUsageMaximum"=dword:0000003c
"WriteWatch"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd]
"MemoryAllocationMode"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Parameters]
"MaxWorkItems"=dword:00002EE0
"MaxMpxCt"=dword:00000800
"MaxRawWorkItems"=dword:00000200
"MaxFreeConnections"=dword:00000064
"MinFreeConnections"=dword:00000020

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanworkstation\Parameters]
"MaxCmds"=dword:00000800
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters]
"MultiUserEnabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoRemoteRecursiveEvents"=dword:00000001
```

Figura 3.20 Configuración en el Registry de Servidores

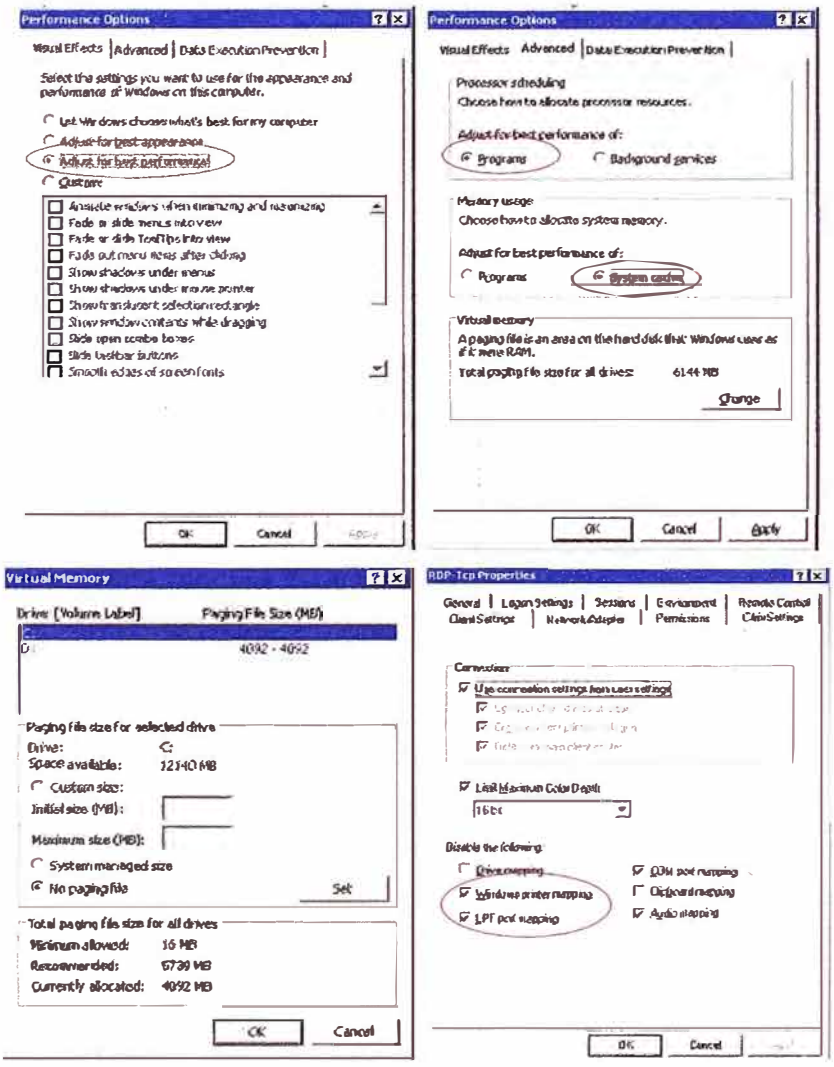


Figura 3.21 Configuraciones en parámetros de Servidores

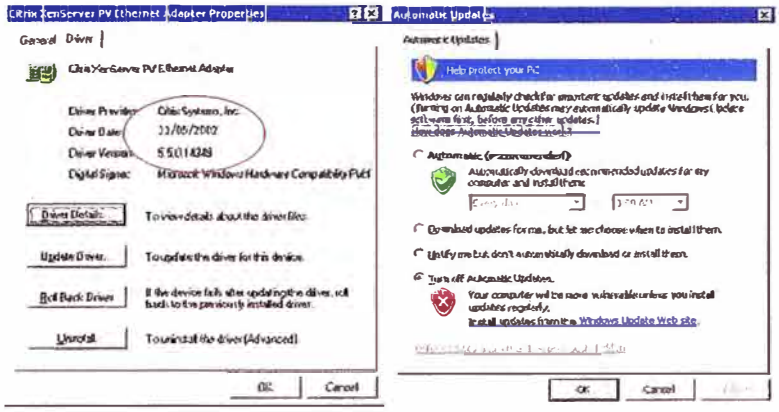


Figura 3.22 Configuraciones en Tarjeta y Antivirus en Servidores

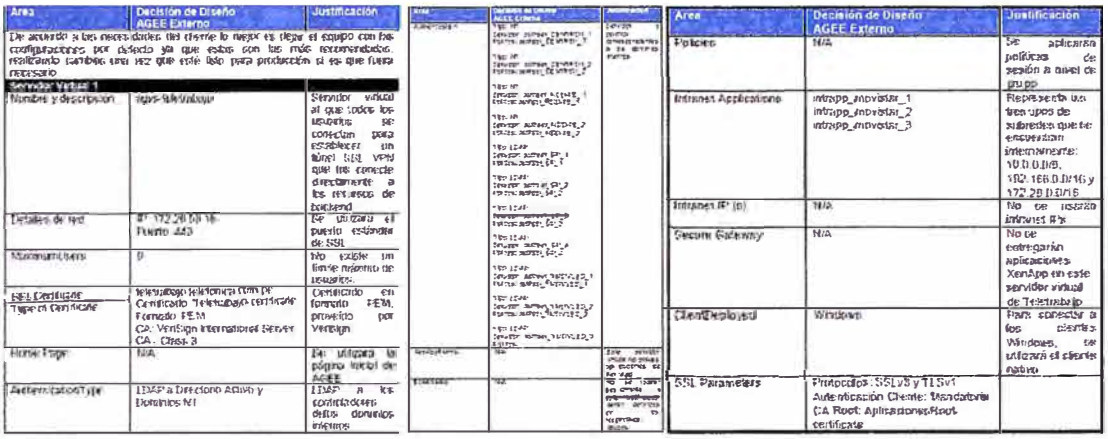


Figura 3.23 Configuraciones en Servidor Control de Accesos

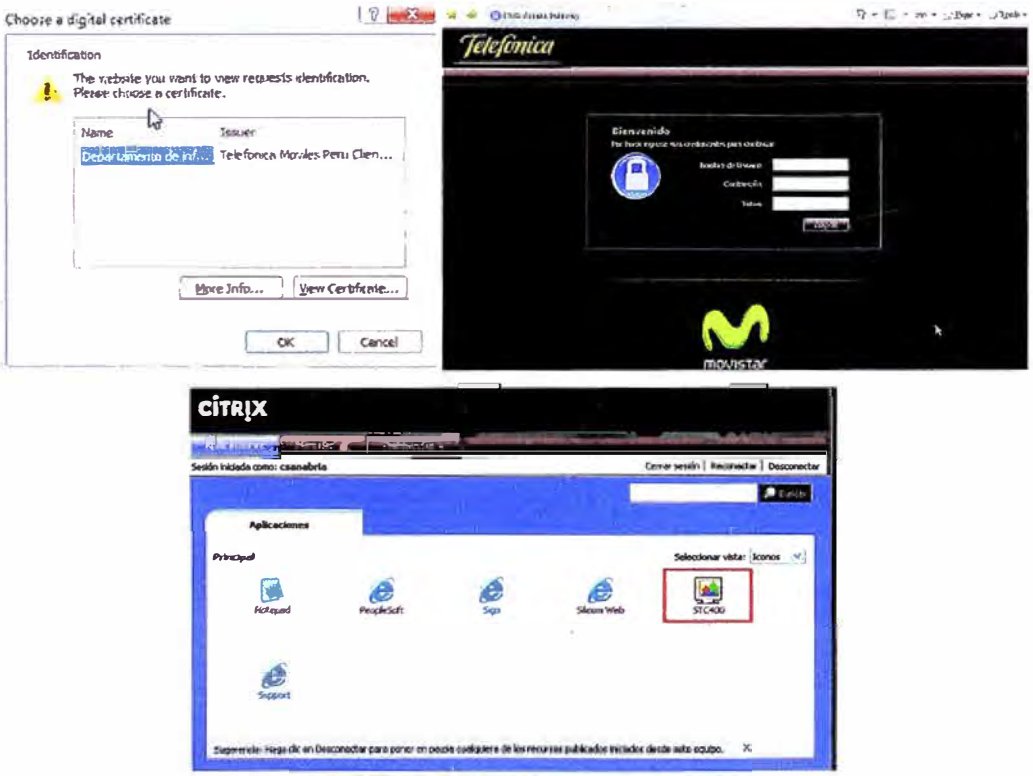


Figura 3.24 Configuración en estaciones clientes en Empresas Colaboradoras

Area	Decisión de Diseño Externos	Justificación
Política de Autenticación 1		
Nombre	authpol_Externo_1, authpol_Externo_2, authpol_Externo_3	Esta política permite la autenticación de usuarios en el dominio EXTERNOS
BindPoints	Servidores virtuales: vpnvs_movistar, vpnvs_testingtm, vpnvs_desarrollotom	Esta política se encuentra activada en los servidores virtuales que entregan aplicaciones XenApp
Expresión	ns_true	La política no requiere ningún filtro
Servidor de Autenticación 1		
Nombre	authser_Externo_1, authser_Externo_2, authser_Externo_3	Estos servidores de autenticación conectan el Directorio Activo del dominio EXTERNOS
Tipo	LDAP	La autenticación siempre se llevara a cabo contra el Directorio Activo del dominio EXTERNOS.
Detalles del Servidor	IP: 10.226.7.32, 172.28.5.67, 172.28.5.84 Port: 389 Timeout: 3 segs	Se definen tres controladores de dominio para brindar alta disponibilidad.
Base DN	DC=gp, DC=externo	Raíz del dominio

Figura 3.25 Configuraciones de Seguridad implementadas

Area	Decisión de Diseño AGEE Externos	Justificación
Política de Sesión 1		
Nombre	sesspol_<grupo>_1	Política de sesión correspondiente a las conexiones de los usuarios pertenecientes al grupo <grupo>
Bind Point	Servidor Virtual: vpnvs_movistar	Esta política solo debe ser usada por el servidor virtual para xenapp
Expresión	REQ.SSL_CLIENT_CERT_SUBJECT CONTAINS "O=<organizacion>"	Se verifica la existencia del certificado a nombre de "<organizacion>" que corresponde al grupo de AD, <grupo>
Perfil de Sesión 1		
Nombre	sessprof_legacy	Este perfil corresponde a los usuarios de la granja de Citrix XenApp actual
ICA Proxy	ON	Habilitado para recibir conexiones ICA y entregar aplicaciones virtualizadas
WI Home Page	http://10.226.7.135/Citrix/Legacy/auth/login.aspx	Este es la URL del Web Interface correspondiente de producción.
SingleSignOn NT Domain	EXTERNOS	Dominio de Directorio Activo donde se autentican los usuarios de Web Interface
Perfil de Sesión 2		
Nombre	sessprof_nuevaxa	Este perfil corresponde a los usuarios de la granja de Citrix XenApp nueva
ICA Proxy	ON	Habilitado para recibir conexiones ICA y entregar aplicaciones virtualizadas
WI Home Page	http://10.226.7.135/Citrix/nuevaxa/auth/login.aspx	Este es la URL del Web Interface correspondiente de producción.
SingleSignOn NT Domain	EXTERNOS	Dominio de Directorio Activo donde se autentican los usuarios de Web Interface
Política de Sesión 2		
Nombre	sesspol_<grupo>_2	Política de sesión correspondiente a las conexiones de los usuarios pertenecientes al grupo <grupo>. Esta política se requiere para que en caso de que un usuario pertenezca a más de un grupo, y de esta manera esté asignado a más de una aplicación, le sea otorgado el acceso.
Bind Point	Servidor Virtual: vpnvs_movistar	Esta política solo debe ser usada por el servidor virtual para xenapp
Expresión	REQ.SSL_CLIENT_CERT_SUBJECT NOT CONTAINS "O=<organizacion>"	Se verifica la no existencia del certificado a nombre de "<organizacion>" que corresponde al grupo de AD, <grupo>

Figura 3.26 Configuraciones de Sesiones implementadas

CAPÍTULO IV
EVALUACIÓN ECONÓMICA Y CRONOGRAMA

4.1 Costes de Inversión (CAPEX)

Los costes asociados a inversión se muestran en la TABLA N° 4.1.

TABLA N° 4.1 Costes de Inversión de la Solución

CATEGORIA	DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
HARDWARE	Servidores Tipo Blade (BL465c): 02 procesadores quad core 2.3GHz/ 02 discos de 146GB/16GB RAM	10	$9,000	$90,000
	Chasis	1	$35,000	$35,000
	Rack	1	$4,500	$4,500
	SUBTOTAL			**$129,500**
SOFTWARE	Windows Enterprise (EA)	10	$3,010	$30,100
	System Center Managment Suite	10	$1,275	$12,750
	Terminal CALs	200	$106	$21,200
	XenServer	10	$2,837	$28,370
	XenApp Nuevas	200	$341	$68,200
	RSA SW	200	$60	$12,000
	RSA Server	200	$90	$18,000
	SUBTOTAL			**$190,620**
SERVICIOS	RSA Servicio	1	$25,000	$25,000
	Servicios Implementación	1	$1,000	$1,000
	Acondicionamiento CPD	1	$1,500	$1,500
	SUBTOTAL			**$27,500**
ENLACES	**CENTRO DE PROCESAMIENTO DE DATOS (Enlace Internet 5Mbps)**			
	Equipo Router	1	$ 5,000.00	$ 5,000.00
	Instalación de router	1	$ 700.00	$ 700.00
	SUB-TOTAL			**$ 5,700.00**

CENTRO DE PROCESAMIENTO DE DATOS (Enlace IPVPN 10Mbps)			
Estudio Especial Conexión a Red	1	$ 1,000.00	$ 1,000.00
Equipo Router	1	$ 15,000.00	$ 15,000.00
Instalación de router	1	$ 700.00	$ 700.00
SUB-TOTAL			**$ 16,700.00**
EMPRESA COLABORADORA (Enlace Internet 1Mbps 10%)			
Conexión a Red Internet	40	$ 89.00	$ 3,560.00
Venta Router	40	$ 190.00	$ 7,600.00
SUB-TOTAL			**$ 11,160.00**
EMPRESA COLABORADORA (Enlace IPVPN 1Mbps)			
Estudio Especial Conexión a Red	20	$ 500.00	$ 10,000.00
Equipo Router	20	$ 700.00	$ 14,000.00
Instalación de router	20	$ 200.00	$ 4,000.00
SUB-TOTAL			**$ 28,000.00**
EMPRESA COLABORADORA (Enlace IPVPN 2Mbps)			
Estudio Especial Conexión a Red	5	$ 500.00	$ 2,500.00
Equipo Router	5	$ 1,000.00	$ 5,000.00
Instalación de router	5	$ 200.00	$ 1,000.00
SUB-TOTAL			**$ 8,500.00**
TOTAL CAPEX			**$417,680**

4.2 Costes de Operación (OPEX)

Los costes asociados a la operación se muestran en la TABLA N◦ 4.2.

TABLA N◦ 4.2 Costes de Operación de la Solución

CATEGORIA	DESCRIPCION	PAGO UNICO	PAGO MENSUAL
SERVICIOS	Despliegue (Pago único)	$2,000	
	Pago Mensual		$4,500
	SUBTOTAL	**$2,000**	**$4,500**
ENLACES	**CENTRO DE PROCESAMIENTO DE DATOS (Enlace Internet 4Mbps)**		
	Pago Mensual por Enlace		$1,800
	SUBTOTAL		**$1,800**
	CENTRO DE PROCESAMIENTO DE DATOS (Enlace IPVPN 10Mpbs)		
	Pago Mensual por Enlace		$3,000
	SUBTOTAL		**$3,000**
	EMPRESA COLABORADORA (Enlace Internet 1Mbps 10%)		

Pago Mensual por Enlace (40)		$8,000
SUBTOTAL		**$8,000**
EMPRESA COLABORADORA (Enlace IPVPN 1Mpbs)		
Pago Mensual por Enlace (20)		$6,000
SUBTOTAL		**$6,000**
EMPRESA COLABORADORA (Enlace IPVPN 2Mpbs)		
Pago Mensual por Enlace (05)		$2,500
SUBTOTAL		**$2,500**
TOTAL OPEX	$2,000	$25,800

4.3 Tiempos de Ejecución

El proyecto se realizó en 6 meses y el cronograma de tiempos se muestra en la figura 4.1.

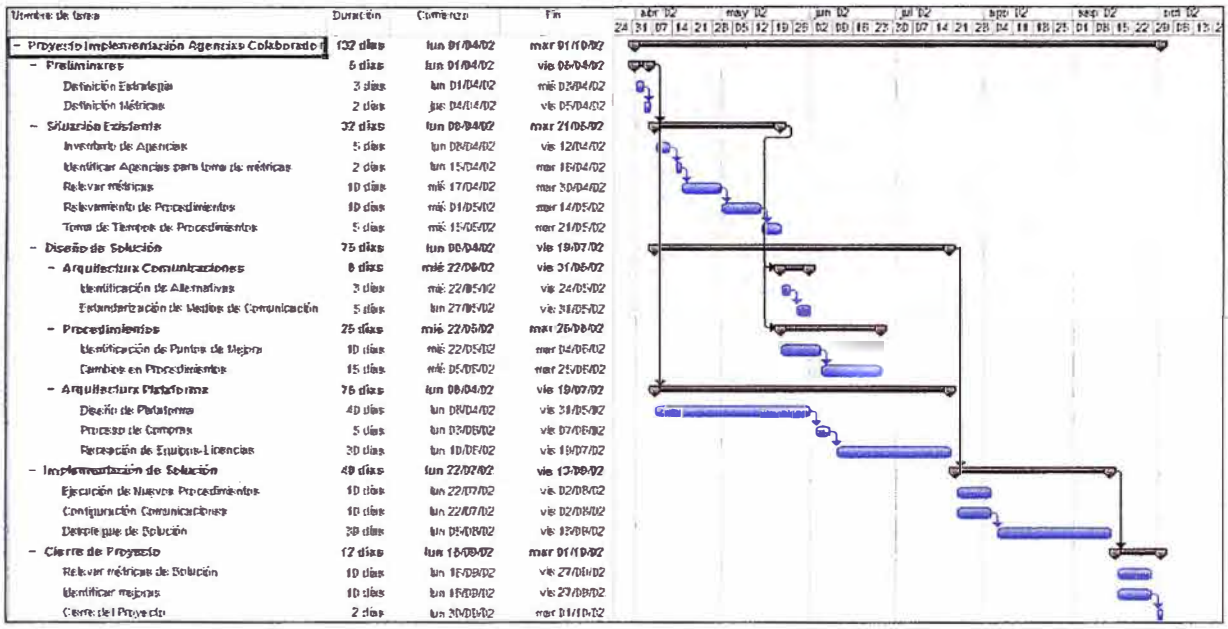


Figura 4.1 Cronograma de Actividades

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se evidencia que sin un monitoreo y seguimiento al servicio que se brinda en las empresas colaboradoras no se pueden identificar mejoras en el mismo.
2. El relevar la situación en empresas colaboradoras con métricas claramente identificables nos mostró que la situación de accesos tenía diversas deficiencias que originaban problemas en diversos aspectos como imagen, pérdidas económicas, falta de controles a la empresa corporativa.
3. Identificando soluciones de mercado para mejorar los accesos de las agencias colaboradoras originó mejoras en: tiempos de implementación, disminución en incidencias, mejorar los controles de seguridad, mayores ingresos.
4. La normalización de cada rubro de la solución origina mejores decisiones para la toma de las mejores alternativas a implementar.
5. El uso de tecnologías como la de Citrix, nos dan ventajas sobre el servicio que se requieren en las empresas colaboradoras y nos produce un mejor uso del ancho de banda a utilizar.

Recomendaciones

1. Continuar con la implementación de la solución para el total de las agencias colaboradoras.
2. Continuar con métricas para ir mejorando las normas iniciales que se realizaran para la implementación del proyecto.
3. Implementar mejora continua en los diversos procesos e ir analizando alternativas del mercado que puedan ser utilizadas para esta mejora.
4. Identificar dentro de las nuevas plataformas implementadas nuevas facilidades que mejoren los servicios que se brindan o se puedan implementar más servicios.

ANEXOS

ANEXO A
COMPARATIVOS

TABLA N° 1 Tiempos de Respuestas del Sistema Comercial Antes y Después de la Solución

MEDIO	ANTES (Seg.)	DESPUES (Seg.)
Línea Dedicada	9.67	3.20
Infovía	48.33	
Infomóvil	56.67	
Speedy Business		8.90

TABLA N° 2 Tiempos de Atención Antes y Después de la Solución

Concepto		Antes (Días)	Después (Días)
Medio de Comunicación	Enlace Dedicado	15	5
	Infovía	10	
	Infomóvil	5	
	Speedy Business		3
Equipos Comunicaciones	Configuraciones rutas, reglas	3	1
Aplicativos (*)	Aplicativo Corporativo	5	1
	Aplicativo Ventas	3	
	Aplicativo Promociones	3	

TABLA N° 3 Tiempos de Respuestas por Aplicativo Antes y Después de la Solución

APLICATIVO		Antes (Seg.)	Después (Seg.)
1	Comercial	30	10
2	Ventas	22	7
3	Promociones	18	6

ANEXO B
DETALLE DE ALCANCE

ITEM	EMPRESA COLABORADORA	LOCALIDAD	ENLACE	PC's
1	ANFERTEL SAC	Arequipa	IPVPN 1Mbps	19
2	ANFERTEL SAC	La Libertad	IPVPN 1Mbps	11
3	ARTELCO S.A.C.	Arequipa	IPVPN 1Mbps	18
4	ARTELCO S.A.C.	Cajamarca	IPVPN 1Mbps	18
5	CAVENTERPRISES S.A.	Apurimac	Speedy Business	2
6	CAVENTERPRISES S.A.	Arequipa	IPVPN 1Mbps	15
7	CAVENTERPRISES S.A.	Cajamarca	Speedy Business	6
8	CAVENTERPRISES S.A.	Cuzco	Speedy Business	6
9	CAVENTERPRISES S.A.	Huanuco	Speedy Business	4
10	CAVENTERPRISES S.A.	La Libertad	Speedy Business	5
11	CAVENTERPRISES S.A.	Lima	IPVPN 1Mbps	13
12	CELLSTAR	Ancash	Speedy Business	2
13	CELLSTAR	Arequipa	Speedy Business	6
14	CELLSTAR	Ayacucho	Speedy Business	5
15	CELLSTAR	Ica	Speedy Business	4
16	CELLSTAR	Junin	Speedy Business	6
17	CESAR'S CELL E.I.R.L.	Tumbes	Speedy Business	2
18	CESAR'S CELL E.I.R.L.	Ucayali	Speedy Business	3
19	DUALNET SA	Arequipa	Speedy Business	6
20	DUALNET SA	Cajamarca	Speedy Business	6
21	DUALNET SA	Cuzco	Speedy Business	6
22	DUALNET SA	Huancavelica	Speedy Business	5
23	FOCATEL SRL	Pasco	Speedy Business	6
24	IMPOPART & SERVICE SRL	Piura	Speedy Business	2
25	IMPOPART & SERVICE SRL	Tacna	Speedy Business	5
26	INFOTELECOM S.R.L.	La Libertad	Speedy Business	6
27	INFOTELECOM S.R.L.	Lambayeque	Speedy Business	4
28	J.L. NIEZEN S.A.	Arequipa	IPVPN 2Mbps	45
29	J.L. NIEZEN S.A.	La Libertad	IPVPN 1Mbps	20
30	J.L. NIEZEN S.A.	Lima	IPVPN 1Mbps	20
31	J.L. NIEZEN S.A.	Lima	IPVPN 2Mbps	40
32	J.L. NIEZEN S.A.	Piura	IPVPN 1Mbps	8
33	J.L. NIEZEN S.A.	Tacna	IPVPN 1Mbps	12
34	L & M BUSINESS	Lima	Speedy Business	2
35	LAMA LINE S.A.C	Lima	Speedy Business	3
36	LET'S TALK CELLULAR S.A.	Cajamarca	IPVPN 2Mbps	50
37	LET'S TALK CELLULAR S.A.	Lima	IPVPN 2Mbps	45
38	LET'S TALK CELLULAR S.A.	Lima	Speedy Business	2
39	LET'S TALK CELLULAR S.A.	Tacna	IPVPN 1Mbps	10
40	LIMA CELULAR	Lima	Speedy Business	5
41	MACRO TEX S.R.L.	Loreto	Speedy Business	4
42	ONE TELECOMUNICACIONES S.A.C.	La Libertad	Speedy Business	6
43	ONE TELECOMUNICACIONES S.A.C.	Lambayeque	Speedy Business	6
44	ONE TELECOMUNICACIONES S.A.C.	Madre de Dios	Speedy Business	6
45	ONE TELECOMUNICACIONES S.A.C.	Moquegua	Speedy Business	6

ITEM	EMPRESA COLABORADORA	LOCALIDAD	ENLACE	PC's
46	OVERLANDES SA	Arequipa	IPVPN 1Mbps	19
47	OVERLANDES SA	Cajamarca	IPVPN 1Mbps	14
48	OVERLANDES SA	Junin	IPVPN 1Mbps	13
49	OVERLANDES SA	Lima	IPVPN 1Mbps	16
50	OVERLANDES SA	Loreto	IPVPN 1Mbps	10
51	OVERLANDES SA	Piura	IPVPN 1Mbps	10
52	SERVICIO INTEGRAL DE COMUNICACIONES SAC	Amazonas	Speedy Business	2
53	SIMUCOM S.A.C.	Cajamarca	IPVPN 1Mbps	16
54	SIMUCOM S.A.C.	La Libertad	IPVPN 2Mbps	50
55	SIMUCOM S.A.C.	Lima	IPVPN 1Mbps	15
56	SPRYSSA S.A.	La Libertad	Speedy Business	5
57	SPRYSSA S.A.	Lima	Speedy Business	2
58	SPRYSSA S.A.	Madre de Dios	Speedy Business	2
59	STAR COM NET S.A.C.	Piura	Speedy Business	5
60	STAR COM NET S.A.C.	Puno	Speedy Business	4
61	STAR COM NET S.A.C.	San Martin	Speedy Business	4
62	WORD COMMUNICATIONS COMPANY EIRL	Tacna	Speedy Business	6
63	WORD COMMUNICATIONS COMPANY EIRL	Tumbes	Speedy Business	4
64	WORD COMMUNICATIONS COMPANY EIRL	Ucayali	Speedy Business	2
65	WORLD LINE SAC	Lima	IPVPN 1Mbps	15

ANEXO C
RESUMENES

DPTO	IPVPN 1MBPS	IPVPN 2MBPS	SPEEDY BUSINESS	TOTAL GENERAL
Amazonas			1	1
Ancash			1	1
Apurimac			1	1
Arequipa	4	1	2	7
Ayacucho			1	1
Cajamarca	3	1	2	6
Cuzco			2	2
Huancavelica			1	1
Huanuco			1	1
Ica			1	1
Junin	1		1	2
La Libertad	2	1	4	7
Lambayeque			2	2
Lima	5	2	5	12
Loreto	1		1	2
Madre de Dios			2	2
Moquegua			1	1
Pasco			1	1
Piura	2		2	4
Puno			1	1
San Martin			1	1
Tacna	2		2	4
Tumbes			2	2
Ucayali			2	2
TOTAL GENERAL	20	5	40	65

BIBLIOGRAFÍA

[1] Softdownload, "Tutorial de Tecnología ADSL", Argentina, 2001

[2] Aldo Valerio, "Conoce ADSL", Argentina, 2005

[3] James Reagan, MPLS Study Guide, Estados Unidos, 2002

[4] http://www.ldc.usb.ve/~poc/RedesII/Grupos/G5/index.html

[5] Citrix Systems, "Getting Started Citrix", Estados Unidos, 2002

[6] Citrix Systems, "Guía de Introducción a Citrix Presentation Server", Estados Unidos, 2001

[7] Citrix Consulting, "Implementación de Citrix Access Gateway Enterprise Edition", Perú, 2002

[8] Citrix Consulting, "Implementación de Citrix Essentials para XenServer", Perú, 2002

[9] Citrix Consulting, "Implementación de XenApp 5 Platinum Citrix® XenApp™ 5 Diseño de Arquitectura", Perú, 2002

[10] Citrix Consulting, "Implementación de Citrix Access Gateway Enterprise Edition Citrix® Access Gateway™ Enterprise Documento de Diseño Detallado", Perú, 2002

[11] Brian S. Madden, "Citrix MetaFrame XP: Advanced Technical Design Guide (Advanced Technical Design Guide series)", Estados Unidos, 2002

[12] Joseph M. Firestone, "Enterprise Information Portals and Knowledge Management", Estados Unidos, 2002

[13] Evento anual Citrix Solutions Summit, USA, 2002

[14] http://www.ctxdom.com/foros

[15] http://www.citrix.es/Productos_y_Soluciones/Productos/Citrix_Access_Gateway/