

**UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**



**“DISEÑO PARA LA INTERCONEXIÓN DE REDES”
BANCARIAS COMPARTIENDO UNA ARQUITECTURA**

ETHERNET – ATM

INFORME DE INGENIERÍA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

MARCIAL ANDRÉS MILLA GARCÍA

PROMOCIÓN 1997 - 2

LIMA – PERÚ

2003

A mi Madre Martha por toda la ayuda y el apoyo que me ofrece.

A mis hermanos, y familiares por su apoyo de siempre.

A Mileni por su apoyo en la realización del informe.

SUMARIO

Describir una Solución ATM/Ethernet para la Interconexión de Redes Bancarias con los proveedores de Información que tengan en común, logrando generar una Red flexible, funcional y escalable. Adicionalmente, lograr compartir los costos en de dicha red desminuyendo la cantidad de enlaces y estandarizando la manera de entregarlos.

**“DISEÑO PARA LA INTERCONEXIÓN DE
REDES BANCARIAS COMPARTIENDO
UNA ARQUITECTURA ETHERNET – ATM”**

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO I	
INTRODUCCIÓN AL INTERNETWORKING	3
1.1. Historia sobre el TCP/IP	3
1.2. Dirección IP	4
1.3. Utilidad del TCP/IP	8
1.4. Tecnología de equipos utilizados en internetworking	9
1.4.1. Tecnología del switch	9
1.4.2. Tecnología de ruteador	10
1.5. Segmentando con switches y ruteadores	14
1.5.1. Segmentando LANS con switch	14
1.5.2. Segmentando subredes con ruteadores	15
1.6. Futuro de los switches	18
1.7. Futuro del ruteo	19
1.7.1. Interfaces LAN y WAN	19

CAPITULO II

INGENIERIA DEL PROYECTO:

DESCRIPCIÓN GENERAL DEL PROYECTO, OBJETIVO PRINCIPAL Y

TOPOLOGÍA DE LA RED	21
2.1. Antecedentes	21
2.2. Objetivo	29
2.3. Topología de la red	30
2.3.1. Descripción de la topología de los enlaces	30

CAPITULO III

CONMUTADORES Y ENRUTADORES DE INTERFACES

ETHERNET/ATM	34
3.1. Descripción de los equipos utilizados en la red ATM –Ethemet	34
3.2. Descripción de la red del proveedor de servicios ATM	34
3.3. Descripción de los equipos utilizados en la red sobre servicios ATM	41

CAPÍTULO IV

DISEÑO DE LA RED ATM/ETHERNET Y DEL BACKBONE IP PARA LA INTERCONEXIÓN DE LAS REDES BANCARIAS

4.1. Antecedentes para el diseño de la red ATM/Ethemet	51
4.2. Descripción de los enlaces y descripción lógica de la red	52
4.3. Distribución del plan de numeración	54
4.3.1. Dimensionamiento de las redes LAN de las sedes remotas	54
4.3.2. Diseño de la red WAN de interconexión de las sedes	57
4.3.3. Diseño de la red de loopbacks de administración de los equipos en las sedes remotas	57

4.4	Políticas de enrutamiento utilizadas para la seguridad y control de los paquetes	58
4.4.1	Definición del enrutamiento utilizado para la red principal	58
4.5	Descripción de las configuraciones en los equipos	78
4.5.1	Configuraciones de las sub-interfaces ATM	78
4.5.2	Configuraciones del enrutamiento de las redes permitidas	81
4.5.3	Configuraciones de la VoIP en cada sede remota	81
4.5.4	Configuraciones del nat dinámico / estático para los hosts permitidos	84
4.5.5	Configuraciones de redundancia (ISDN)	85
4.6	Descripción de las configuraciones en los equipos	87
4.6.1	Perdida de conexión con el equipo principal	87
4.6.2	Perdida de conexión con el equipo secundario	89
4.6.3	Perdida de conexión con la última milla	90
CAPÍTULO V		
CONSIDERACIONES FINALES Y EVALUACIÓN ECONÓMICA DEL		
PROYECTO		
5.1	Consideraciones de servicio	92
5.1.1	Coordinaciones para cambios y crecimientos	92
5.1.2	Niveles de aceptación de la red	93
5.2	Evaluación económica del proyecto	94
CONCLUSIONES		
ANEXOS		
BIBLIOGRAFÍA		
		101
		132

INTRODUCCIÓN

Actualmente se encuentra la necesidad de interconexión entre entidades bancarias, y proveedores de información. Esta necesidad, se ve reflejada en la gran cantidad de enlaces que maneja una entidad bancaria con sus diferentes proveedores de información. Dentro de sus proveedores de información tenemos entidades públicas y privadas con las cuales tienen algún tipo de intercambio de información electrónica. Tenemos como ejemplo entidades como la Superintendencia Nacional de Aduanas (SUNAD), RENIEC o Identidad, Centrales de Riesgo como Certicom o Infocorp, Centrales Centralizadas de Alarmas, Tiendas comerciales como Ripley, SAGA FALABELLA, etc. Siendo estas conexiones de diferentes maneras, sin seguir un *estándar de conexión al proveedor*. Esto debido a las variadas tecnologías que poseen estos proveedores de Información. Realmente el tipo de tecnología esta sujeta a características tales como la antigüedad de la entidad, también tenemos otro parámetro como son el tamaño y política de innovación de estas entidades, ya que permite esto innovaciones tecnológicas en sus Áreas de Tecnología de la Información. En algunos casos se puede observar tener un pool de módems de conexiones diversas en una sede de un Banco. Esto ocasiona tener grandes espacios ocupados por estos equipos, además no estamos teniendo en cuenta el costo en que se incurre en cada uno de estos enlaces por separados. A todo esto se suma la parte

de operación de estos enlaces ya que se complica con la diversidad de proveedores que emplean.

Este es un proyecto de conexión entre bancos y proveedores de información que necesitan entre ellos. Pero se debe de resaltar, que este proyecto tiene una tendencia a centralizar los servicios más comunes entre los bancos a un Nodo Central. Centralizando el tráfico generado a los requerimientos más comunes de los bancos. Dentro de las finalidades de este proyecto es la de generar una red TCP/ IP que sirva de interconexión de todos los bancos con los diferentes proveedores de información y servicios necesarios a las diferentes entidades bancarias. Además, podemos observar un gran impacto en el ahorro para estas Entidades, en el alquiler de circuitos dedicados de comunicación para con sus diferentes proveedores de información. Otro punto que contempla este proyecto es dar paso a la estandarización de los datos entregados por los proveedores de servicio. Es decir, servir de interlocutor entre los bancos y los proveedores de servicio, desarrollando aplicativos comunes y formatos estándares en los datos entregados. Al lograr estandarizar se consigue tener un ahorro de costos a todo nivel, desde la parte técnica hasta la parte operativa y del proceso en si mismo.

La Red de bancos es una red TCP/IP escalable, confiable y segura. Para lograr esa confiabilidad y seguridad por la cantidad y el tipo de tráfico importante que lleva , se tiene la consideración que esta red cuenta con un diseño con las opciones de redundancia en caso de caída del nodo Principal (falla física del equipo), como también en los casos de corte de fibra (En cualquier parte de la Red) y Problemas de intentos de violación de seguridad. Esta redundancia se llevará a cabo vía enlaces ISDN, que van por la red pública de telefonía.

CAPÍTULO I

INTRODUCCIÓN AL INTERNETWORKING

1.1. Historia sobre el TCP/IP

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPAnet) que conectaba redes de ordenadores de varias universidades y laboratorios en investigación en Estados Unidos. World Wide Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés). TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del

modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

1.2. Dirección IP

El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bit que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos. La dirección de Internet (IP Address) se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran

conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- a) Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A".
- b) Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de ordenadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".
- c) Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1

hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 ordenadores en cada red. Estas direcciones permiten un menor número de host que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1 .. 126	1 byte	3 byte	126	16.387.064
B	128 .. 191	2 byte	2 byte	16.256	64.516
C	192 .. 223	3 byte	1 byte	2.064.512	254

Tabla 1.1 - Tabla de direcciones IP de Internet.

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas,

resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al host. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El broadcast es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible.

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (subnets). Como ejemplo podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de dos bytes. En este caso sería posible utilizar el tercer byte para indicar en qué red Ethernet se encuentra un host en concreto. Esta división no tendrá ningún significado para cualquier otro ordenador que esté conectado a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho más cómodo el acceso que si se tratara de varias direcciones de clase C independientes.

Una entidad de transporte TCP acepta mensajes de longitud arbitrariamente grande procedentes de los procesos de usuario, los separa en pedazos que no excedan de 64K octetos y, transmite cada pedazo como si fuera un datagrama separado. La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que TCP deberá utilizar temporizadores y retransmitir los datagramas si es necesario. Los datagramas que consiguen llegar, pueden hacerlo en desorden; y dependerá de TCP el hecho de reensamblarlos en mensajes, con la secuencia correcta.

Cada octeto de datos transmitido por TCP tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecidos, desde hace tiempo, en el momento en que los números de secuencia den la vuelta. TCP, sin embargo, sí se ocupa en forma explícita del problema de los duplicados retardados cuando intenta establecer una conexión, utilizando el protocolo de ida-vuelta-ida para este propósito.

El control de flujo en TCP se trata mediante el uso de una ventana deslizante de tamaño variable. Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos que se pueden transmitir más allá del octeto asentido por el campo ventana y no cuántas TPDU.

1.3. Utilidad del TCP/IP

Muchas grandes redes han sido implementadas con estos protocolos, incluyendo DARPA Internet "Defense Advanced Research Projects Agency Internet", en español, Red de la Agencia de Investigación de Proyectos Avanzados de Defensa. De igual forma, una gran variedad de universidades, agencias

gubernamentales y empresas de ordenadores, están conectadas mediante los protocolos TCP/IP. Cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes en una red virtual llamada Internet. Las máquinas en Internet son denominadas "hosts" o nodos.

TCP/IP proporciona la base para muchos servicios útiles, incluyendo correo electrónico, transferencia de ficheros y login remoto.

El correo electrónico está diseñado para transmitir ficheros de texto pequeños. Las utilidades de transferencia sirven para transferir ficheros muy grandes que contengan programas o datos. También pueden proporcionar chequeos de seguridad controlando las transferencias.

El login remoto permite a los usuarios de un ordenador acceder a una máquina remota y llevar a cabo una sesión interactiva.

1.4. Tecnología de equipos utilizados en internetworking

1.4.1. Tecnología del switch

Un Switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El Switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC. El Switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo. Al segmentar la red en pequeños

dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

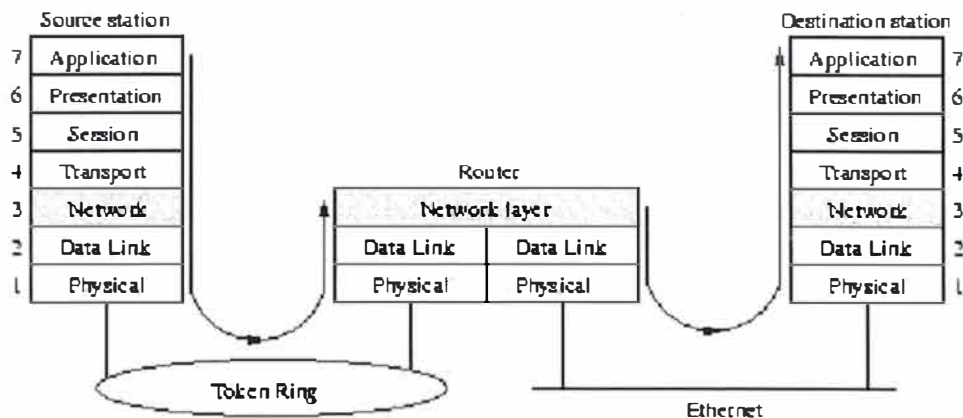


Figura 1.1 – Descripción de las capas OSI de operación para la comunicación de terminales

Lo más importante es saber donde utilizar un Switch. Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre cliente / servidor, Pues los usuarios juzgan la red por la rapidez de obtener un prompt y la confiabilidad del Servicio.

Hay diversos factores que involucran el incremento de ancho de banda en una LAN:

- ✓ El elevado incremento de nodos en la red.
- ✓ El continuo desarrollo de procesadores mas rápidos y poderosos en estaciones de trabajo y servidores.
- ✓ La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones intensivas cliente / servidor.

- ✓ Cultivar la tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.

La regla tradicional 80/20 del diseño de redes, donde el 80% del tráfico en una LAN Permanece local, se invierte con el uso del Switch. Los Switches resuelven los problemas de anchos de banda al segmentar un dominio de Colisiones de una LAN, en pequeños dominios de colisiones. En la figura la segmentación casi elimina el concurso por el medio y da a cada estación Final más ancho de banda en la LAN.

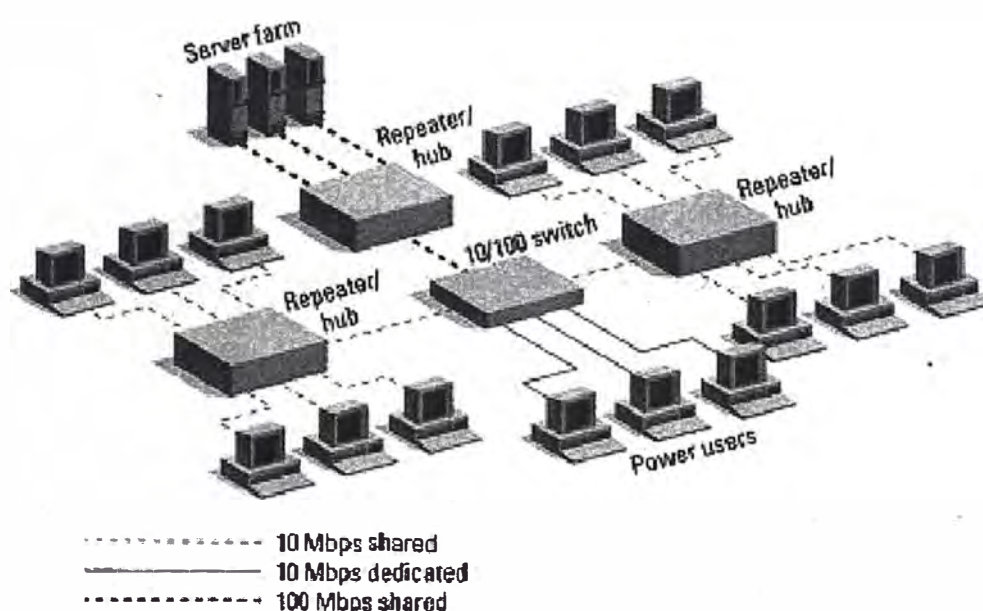


Figura 1.2 – Segmentación de dominios de colisión mediante Switches para resolver problemas de anchos de banda.

1.4.2. Tecnología de ruteador

Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de Firewall y un acceso económico a una WAN.

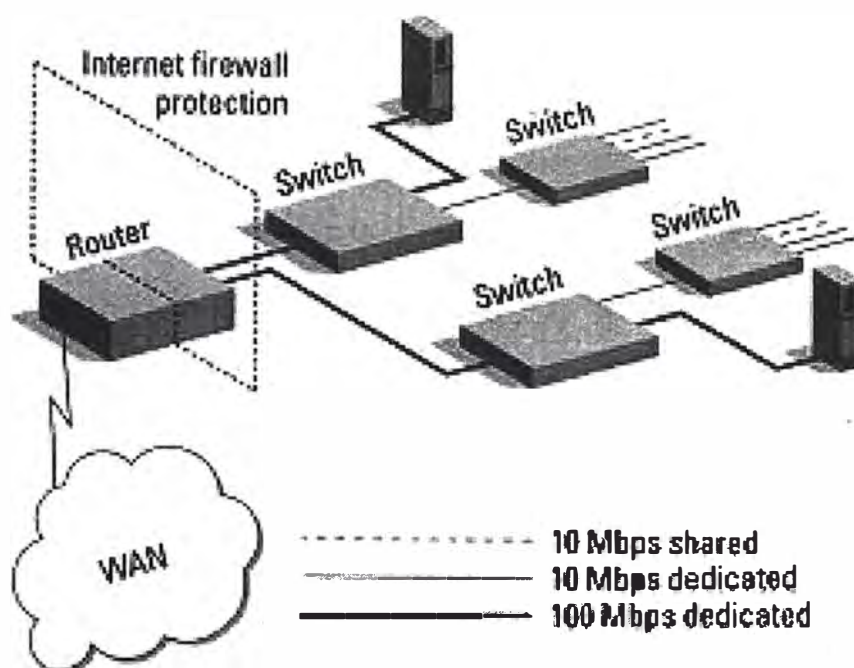


Figura 1.3 – Ubicación de ruteador dentro de una Red LAN.

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un Switch. Al funcionar en una capa mayor que la del Switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, APPLE TALK o DECNET. Esto le permite hacer una decisión más inteligente que al Switch, al momento de reenviar los paquetes.

El ruteador realiza dos funciones básicas:

- a) El ruteador es responsable de crear y mantener tablas de enrutamiento para cada capa de Protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de enrutamiento.

b) La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesamiento de tramas por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de Switch.

Al igual que el Switch, es importante en donde utilizar los ruteadores, y la respuesta viene de saber las funciones primarias de un ruteador. Las funciones primarias de un ruteador son:

- ✓ Segmentar la red dentro de dominios individuales de broadcast.
- ✓ Suministrar un envío inteligente de paquetes. Y
- ✓ Soportar rutas redundantes en la red.

Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del Ruteador es una subred separada, el tráfico de los broadcast no pasaran a través del ruteador.

Otros importantes beneficios del ruteador son:

- ✓ Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- ✓ Consolidar el legado de las redes de mainframe IBM, con redes basadas en PC's a través del uso de Data Link Switching (Dlsw).
- ✓ Permitir diseñar redes Jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.

- ✓ Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, FastEthernet, Token Ring, FDDI y ATM.

1.5. Segmentando con switches y ruteadores

Probablemente el área de mayor confusión sobre Switch y ruteador, es su habilidad para Segmentar la red y operar en diferentes capas del modelo OSI, permitiendo así, un tipo único de diseño de segmentación.

1.5.1. Segmentando LANS con switch

Podemos definir una LAN como un dominio de colisiones, donde el Switch esta diseñado para segmentar estos dominios en dominios más pequeños. Puede ser ventajoso, pues Reduce el número de estaciones a competir por el medio.

En la figura cada dominio de colisión representa un ancho de banda de 10 mbps, mismo que es compartido por todas las estaciones dentro de cada uno de ellos. Aquí el Switch Incrementa dramáticamente la eficiencia, agregando 60 mbps de ancho de banda.

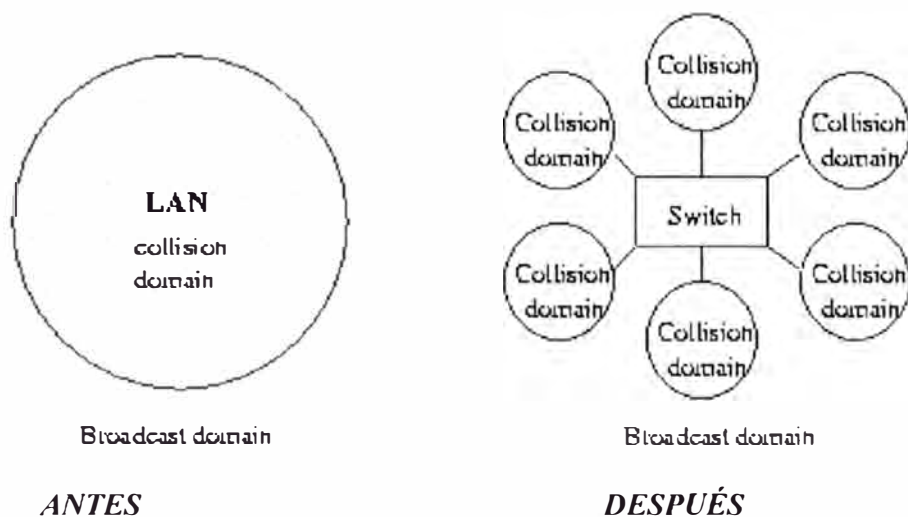


Figura 1.4 – Segmentación de un mismo dominio de colisión.

Es importante notar que el tráfico originado por el broadcast en un dominio de colisiones, Será reenviado a todos los demás dominios, asegurando que todas las estaciones en la red se puedan comunicar entre si.

1.5.2. Segmentando subredes con ruteadores

Una subred es un puente o un Switch compuesto de dominios de broadcast con dominios individuales de colisión. Un ruteador esta diseñado para interconectar y definir los limites de los dominios de broadcast.

La figura muestra que el tráfico de broadcast originado en un dominio es reenviado al otro dominio.

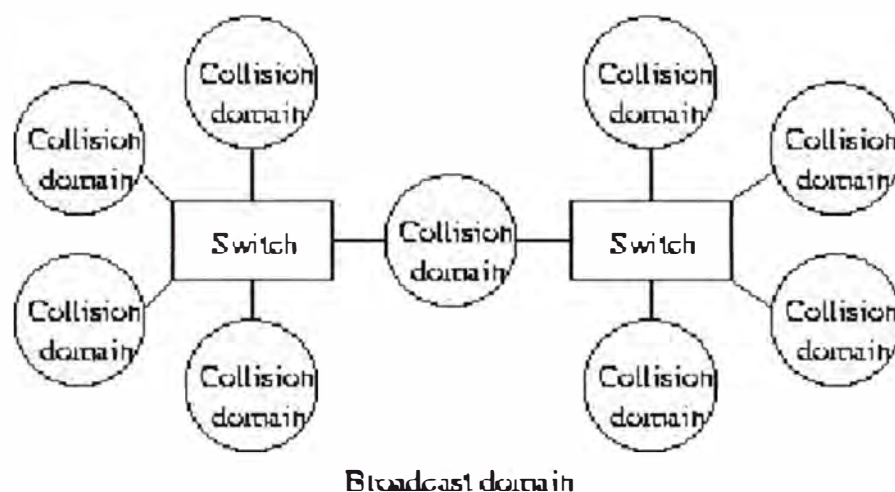


Figura 1.5 – Dominio de broadcast que se segmento en dos dominios de colisiones por un Switch

En la siguiente figura muestra que en este medio el tráfico generado de broadcast no fluye a través del ruteador al otro dominio.

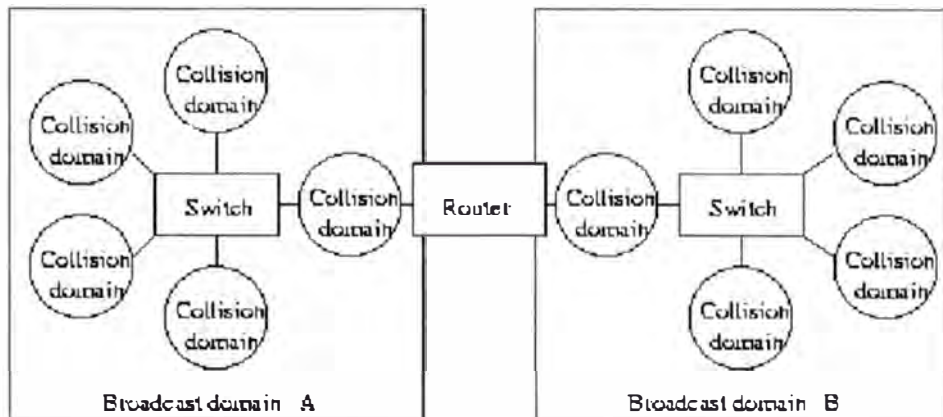


Figura 1.6 – Dominio de broadcast segmentado con un router. Con dos dominios de Broadcast.

Segmentación física

La figura ilustra como un router segmenta físicamente la red dentro de dominios de broadcast. En este ejemplo, el administrador de red instala un router como política de seguridad, además para evitar los efectos del broadcast, que alientan la red.

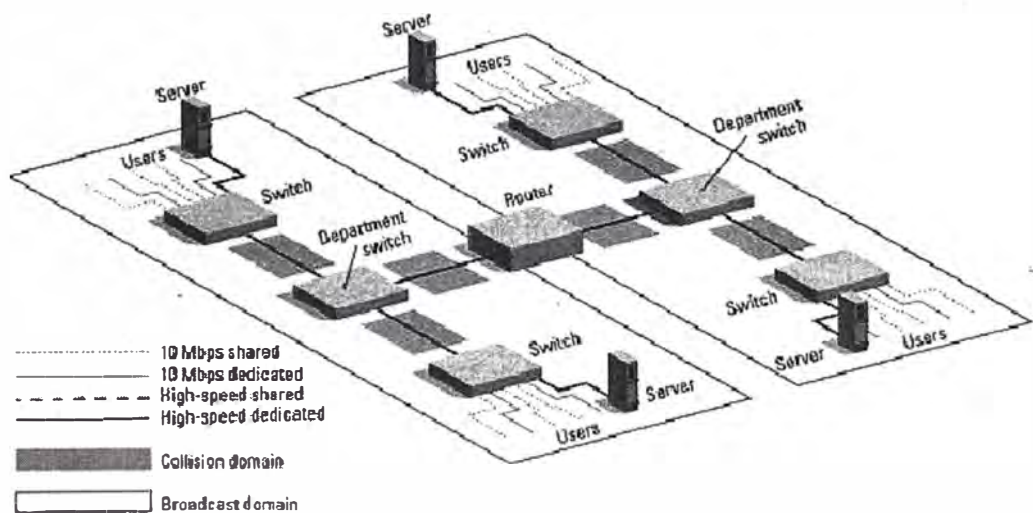


Figura 1.7 – Segmentación física de la Red dentro de dominios de Broadcast.

Se puede apreciar que el ruteador tiene una interface dedicada para cada departamento o Switch del grupo de trabajo. Esta disposición da al ruteador un dominio de colisión privado que aísla el tráfico de cada cliente / servidor dentro de cada grupo de trabajo. Si el patrón del tráfico está entendido y la red está propiamente diseñada, los Switches harán todo el reenvío entre clientes y servidores. Sólo el tráfico que alcance al ruteador necesitará ir entre dominios individuales de broadcast o a través de una WAN.

Segmentación lógica

Algunas metas pueden alcanzarse de una manera más flexible al usar ruteadores y Switches, para conectar LANs Virtuales separadas (VLANs). Una VLAN es una forma sencilla de crear dominios virtuales de broadcast dentro de un ambiente de Switches independiente de la estructura física y tiene la habilidad para definir grupos de trabajo basados en grupos lógicos y estaciones de trabajo individuales, más que por la infraestructura física de la red.

El tráfico dentro de una VLAN es conmutado por medios rápidos entre los miembros de la VLAN y el tráfico entre diferentes VLANs es reenviado por el ruteador.

En la figura los puertos de cada Switch son configurados como miembros ya sea de la VLAN A o la VLAN B. Si la estación final transmite tráfico de broadcast o multicast, el tráfico es reenviado a todos los puertos miembros. El tráfico que fluye entre las dos VLANs es reenviado por el ruteador, dando así seguridad y manejo del tráfico.

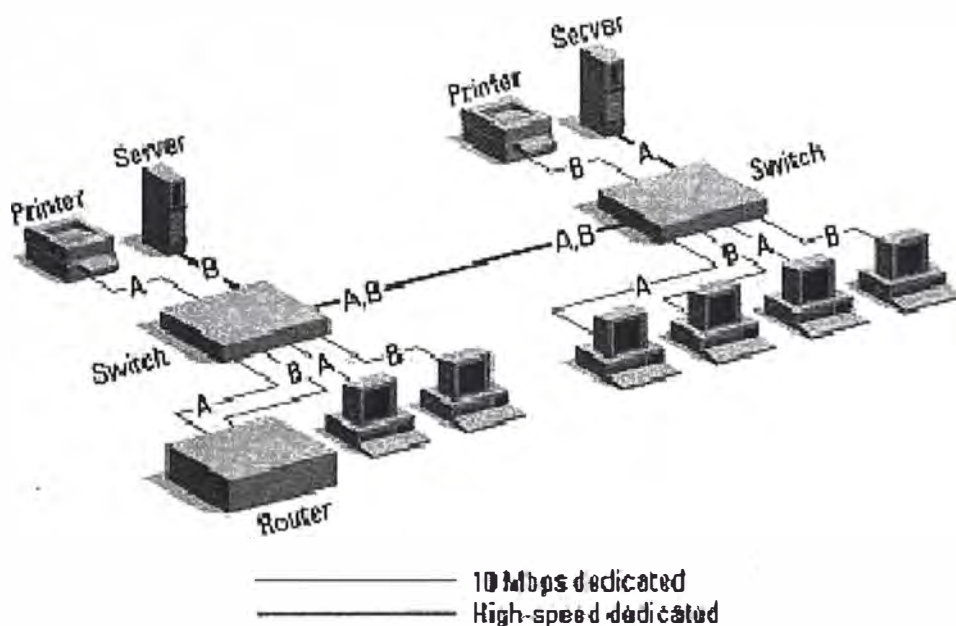


Figura 1.8 – Segmentación lógica entre Switches

1.6. Futuro de los switches

El precio de la tecnología del Switch continua descendiendo, como resultado del desarrollo unido con la eficiencia de la manufactura y técnicas de distribución. Como el costo por puerto del Switch se aproxima al de los HUBs, muchos usuarios eligen el Switch.

La extensa disponibilidad de la tecnología de Switch de bajo costo tiene implicaciones para las redes de los edificios y el Backbone de Campus. Habrá una demanda creciente para Switches de Backbone de alta densidad, con un número grande de puertos de alta velocidad, para enlazar grupos de trabajo individuales.

Eventualmente el equipo de escritorio será dedicado a enlaces de 10 Mbps, la mayoría de los servidores estarán conectados a los Switch de alta velocidad y ATM se usara en enlaces internos del edificios y al Backbone de Campus.

1.7. Futuro del ruteo

El enrutamiento es la llave para desarrollar redes internas. El desafío es integrar el Switch con enrutamiento para que el sistema aproveche el diseño de la red. Cada uno de los grandes vendedores de ruteadores tiene investigando más de 300 millones de dólares en hora / hombre, desarrollando líneas de código para sus productos. Cada liberación de software representa un tremendo esfuerzo de ingeniería, para asegurar que el ruteador soporte la última Tecnología y dirección de diseño en redes internas.

Inicialmente los Switches estarán en todas las organizaciones que requieran incrementar el ancho de banda y obtener la funcionalidad que necesitan. No obstante al incrementar la complejidad de la red, los administradores necesitarán controlar el ambiente de Switch, usando segmentación, redundancia, Firewall y seguridad. En este punto, la disponibilidad de Ruteo sofisticado esencialmente crecerá y la red se escalará en grandes redes de Switches.

El usuario demandará que los vendedores de ruteadores hagan sus productos fáciles de instalar y configurar.

1.7.1 Interfaces LAN y WAN

En general el enrutamiento dentro de los edificios se esta moviendo hacia un pequeño número de interfaces de alta funcionalidad para conectar Switches de alta densidad en los ruteadores. Este es el verdadero modelo costo-efectividad, especialmente cuando un gran número de interfaces LAN van de velocidades baja a media.

Como el número de interfaces LAN decremento, la venta para interfaces WAN sobre la Oficina central de ruteadores es movida a dos diferentes direcciones.

Algunos usuarios requerirán un incremento en el número de interfaces WAN de baja velocidad para conectar sus sitios remotos con arrendamiento de líneas y conexiones telefónicas. Otros usuarios requerirán unas cuantas interfaces físicas como Frame Relay e ISDN, proporcionando la funcionalidad de líneas dedicadas arrendadas por fracción de costo.

Antes de seleccionar entre Switch y ruteador, los diseñadores de red deben comprender como combinar estas tecnologías para construir eficientes redes escalables. Un Administrador de red será extremadamente escéptico de cualquier vendedor que sugiera una solución de alta funcionalidad que pueda ser construida usando sólo tecnología de Switch o de ruteador.

Los Switches y ruteadores son tecnologías complementarias que permiten a las redes escalar a tamaños mucho más allá de lo que se puede lograr usando sólo alguna de estas tecnologías. El ruteo proporciona un número de llaves de capacidad que no ofrece un Switch, tal como control de broadcast, redundancia, control de protocolos y acceso a WAN.

El Switch proporciona manejo de la red con un costo efectivo de migración que elimina anchos de banda pequeños. Los Switches pueden ser integrados fácilmente dentro de redes de ruteadores como reemplazo de la base instalada de repetidores, Hubs y puentes. Cuando ATM es eventualmente implementado en el Backbone, el ruteo será un requerimiento tecnológico para comunicarse entre VLANs.

CAPÍTULO II

INGENIERÍA DEL PROYECTO: DESCRIPCIÓN GENERAL DEL PROYECTO, OBJETIVO PRINCIPAL Y TOPOLOGÍA DE LA RED

2.1. Antecedentes

En la actualidad, la necesidad de interconexión entre entidades bancarias, y proveedores de información es una necesidad latente. Esta necesidad, se ve reflejada en la gran cantidad de enlaces que maneja una entidad bancaria con sus diferentes proveedores de información. Dentro de sus proveedores de información tenemos entidades públicas y privadas con las cuales tienen algún tipo de intercambio de información electrónica. Tenemos como ejemplo entidades como la Superintendencia Nacional de Aduanas (SUNAD), RENIEC o Identidad, Centrales de Riesgo como Certicom o Infocorp, Centrales Centralizadas de Alarmas, Tiendas comerciales como Ripley, SAGA FALABELLA, etc. Siendo estas conexiones de diferentes maneras, sin seguir un *estándar de conexión al proveedor*. Esto debido a las variadas tecnologías que poseen estos proveedores de Información. Realmente el tipo de tecnología esta sujeta a características tales como la antigüedad de la entidad, también tenemos otro parámetro como son el tamaño y política de innovación de estas entidades, ya que permite esto innovaciones tecnológicas en sus Áreas de Tecnología de la Información. En algunos casos se puede observar tener un pool de módems de conexiones diversas en una sede de un Banco. Esto ocasiona tener grandes espacios ocupados por estos equipos, además no estamos teniendo en cuenta

el costo en que se incurre en cada uno de estos enlaces por separados. A todo esto se suma la parte de operación de estos enlaces ya que se complica con la diversidad de proveedores que emplean. Este es un proyecto de conexión entre bancos y proveedores de información que necesiten entre ellos.

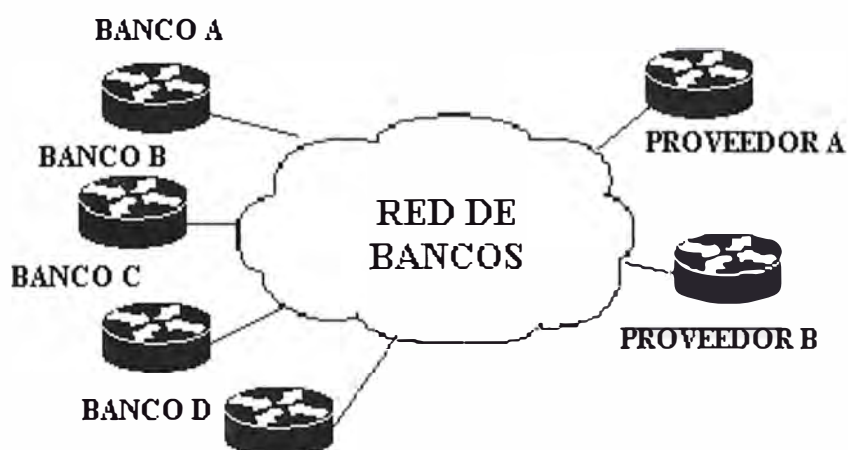


Figura. 2.1 – Proyecto de Interconexión de Bancos y Proveedores de Información.

Pero se debe de resaltar, que este proyecto tiene una tendencia a centralizar los servicios más comunes entre los bancos a un Nodo Central. Centralizando el tráfico generado a los requerimientos más comunes de los bancos.

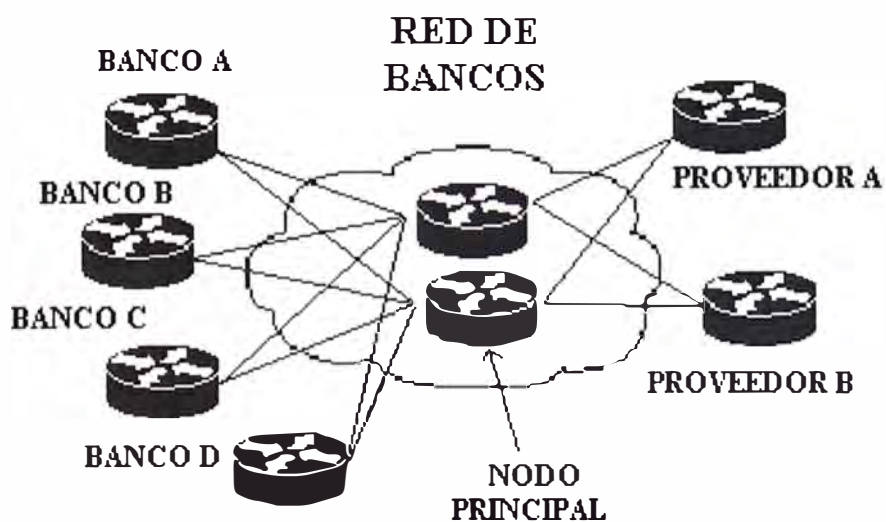


Figura. 2.2 – Conformación de la Red de Bancos por un Nodo Principal

Dentro de las finalidades de este proyecto es la de generar una red TCP/ IP que sirva de interconexión de todos los bancos con los diferentes proveedores de información y servicios necesarios a las diferentes entidades bancarias. Además, podemos observar un gran impacto en el ahorro para estas Entidades, en el alquiler de circuitos dedicados de comunicación para con sus diferentes proveedores de información. Otro punto que contempla este proyecto es dar paso a la estandarización de los datos entregados por los proveedores de servicio. Es decir, servir de interlocutor entre los bancos y los proveedores de servicio, desarrollando aplicativos comunes y formatos estándares en los datos entregados. Al lograr estandarizar se consigue tener un ahorro de costos a todo nivel, desde la parte técnica hasta la parte operativa y del proceso en si mismo.

La Red de bancos es una red TCP/IP escalable, confiable y segura. Para lograr esa confiabilidad y seguridad por la cantidad y el tipo de tráfico importante que lleva , se tiene la consideración que esta red cuenta con un diseño con las opciones de redundancia en caso de caída del nodo Principal (falla física del equipo), como también en los casos de corte de fibra (En cualquier parte de la Red) y Problemas de intentos de violación de seguridad. Esta redundancia se llevará a cabo vía enlaces ISDN, que van por la red pública de telefonía como se muestra en la gráfica adjunta (Fig. 3). En este gráfico se puede apreciar que los datos viajarían a través de otra plataforma (Plataforma ISDN) en caso de algún problema de los antes mencionados, logrando de esta manera no perder contacto ni mucho menos conexión con sus proveedores de información.

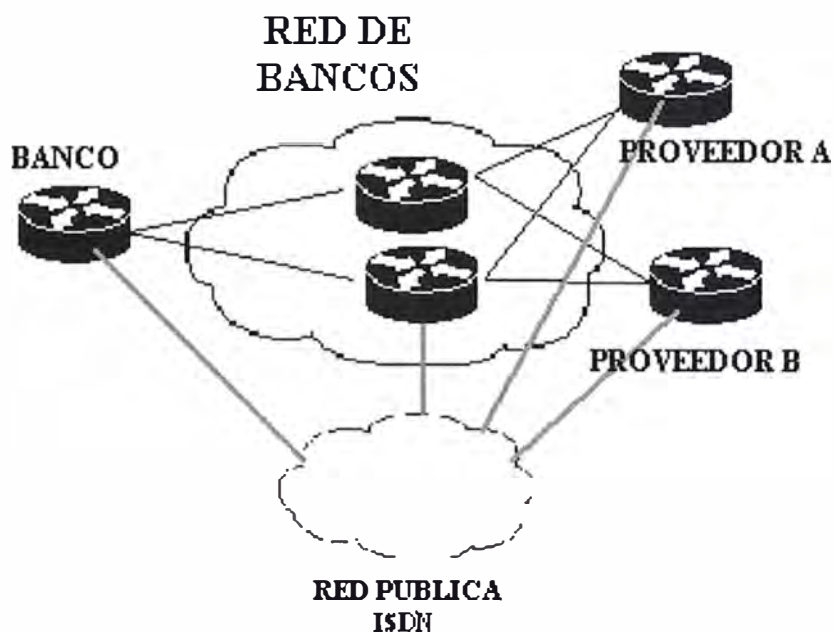


Figura. 2.3 – Redundancia de la Red por ISDN

Aprovechando la Red TCP/IP que se ha generado se pueden encapsular sobre IP otros servicios comunes e importantes como es la voz. Este servicio adicional se puede reflejar como un ahorro considerable en llamadas telefónicas utilizando la Red Pública para las coordinaciones necesarios entre las Entidades Bancarias y los proveedores de servicio. Utilizando la plataforma TCP/IP se podrá utilizar VoIP con las adecuaciones necesarias para tener un optimo servicio. Pero como todo beneficio tiene un costo, en este caso no fue ajeno a esto y se comporta de la siguiente manera. En cada caja llamado en este caso “*Equipo Multiservicio*” debe poseer el tipo de interface para interconexión con la sede. Para mantener un orden se generó estándares de conexión y un plan de numeración para las sedes.

A continuación se muestran los tipos de situaciones de conexiones telefónicas posibles para la utilizar la VoIP en cada una de las Sedes del Proyecto.

- a) Conexión directa entre anexos a los 4 puertos analógicos FXS.- Consiste en la conexión de aparatos telefónicos analógicos en forma directa al “Equipo

Multiservicio”. Esto normalmente aplicaba en sedes que no contaban con una PBX con puertos libres ó entidades con políticas muy estrictas con respecto a la conexión entre redes.



Figura.2.4 - Conexión directa entre anexos a los 4 puertos analógicos FXS

- b) Conexión directa entre anexos en los 4 puertos analógicos FXS y puertos E&M de una Central .- Consiste en la conexión de aparatos telefónicos analógicos en forma directa al “Equipo Multiservicio” en un lado y la conexión en otro lado con una Central Telefónica con puertos E&M. La utilización de puertos E&M dan mayor cantidad de beneficios como es la marcación transparente con los anexos telefónicos que maneja la central, esto, siempre que la central cuente con las características necesarias.



Figura.2.5 - Conexión directa entre anexos con puertos FXS y E&M en una PBX

- c) Conexión directa entre anexos en los 4 puertos analógicos FXS y troncales con FXS de una Central .- Consiste en la conexión de aparatos telefónicos analógicos en forma directa al “Equipo Multiservicio” en un lado y la conexión en otro lado con una Central Telefónica con puertos troncales utilizando en el router tarjetas con puertos FXS. La utilización de puertos FXS permiten conexión con los anexos telefónicos que maneja la central, esto, siempre que la central cuente con las características necesarias.



Figura 2.6 - Conexión directa entre anexos en los 4 puertos analógicos FXS y troncales con FXS de una Central

- d) Conexión directa entre 4 puertos E&M de una Central .- Consiste en la conexión en forma directa al “Equipo Multiservicio” en ambos lado con una Central Telefónica con puertos E&M. La utilización de puertos E&M dan mayor cantidad de beneficios como es la marcación transparente con los anexos telefónicos que maneja la central, esto, siempre que la central cuente con las características necesarias.



Figura.2.7 - Conexión directa entre 4 puertos E&M de una Central

- e) Conexión directa entre 4 puertos troncales de una Central vía tarjetas FXS .- Consiste en la conexión en forma directa al “Equipo Multiservicio” con puertos troncales de una Central Telefónica mediante puertos FXS. La utilización de puertos FXS dan mayor cantidad de cobertura ya que alcanza a todos los anexos telefónicos que maneja la central, esto, siempre que la central cuente con las características necesarias.



Figura 2.8 - Conexión directa entre 4 puertos troncales de una Central vía tarjetas FXS

El Proyecto para su realización se paso por 2 etapas, la cuales paso a mencionar:

- ✓ Etapa migratoria. En esta Etapa se necesitaba realizar las Encuestas de su topología de Red Interna y manera de interconexión a la Red de Bancos. Para tal efecto, se realizaron entrevistas y visitas en sitio para la colocación de los equipos a implementar. Durante esta Etapa se debía mantener al máximo el cuidado de las

conexiones y pruebas de servicio luego de la migración. Se debía mantener una gran flexibilidad para dar atención a los bancos debido a sus múltiples plataformas.

✓ Etapa Centralización de servicios comunes. Durante esta etapa se realizó la estandarización y centralización de los servicios más comunes entre Bancos tratando de normalizar las plataformas y Sistemas Operativos en la cual trabajaban los bancos.

Adicionalmente a estas Etapas, quedó la Red de Bancos con capacidad de crecimiento para la Implementación sobre esta plataforma de comunicación de otra Etapa que más adelante se implementará que es:

✓ Etapa Apertura a clientes de bancos (e-commerce). Colocación de Servidores en el Nodo Principal para el intercambio de información entre Bancos, tiendas y establecimientos que deseen tener este tipo de conexión.

Adicionalmente a los grandes accesos de conexión para datos, se tiene como valor agregado el transporte de canales de voz a través de la Red de Bancos y pasar anexos de Voz para la comunicación entre Bancos (Se debe tener en cuenta que el volumen de llamadas entre las Áreas de tesorería entre bancos es elevada, y adicionándose a estas llamadas se debe de considerar las que se realizan a los proveedores de información en caso de nuevas negociaciones o problemas en el servicio.

Se debe de considerar que existe redundancia a nivel de hardware como también a nivel de fibra. Para el primer caso se tiene un nodo secundario con una configuración imagen del nodo principal, con cierta salvedad en el parámetro de BW para variar la distancia administrativa de las rutas propagadas por este, y de esa manera poder darle una importancia de menor nivel.

2.2. Objetivo

Como principal objetivo se tiene la generación de una Red de interconexión bancaria sobre una *plataforma que sea rápida, flexible, redundante, escalable y que permita interoperabilidad con otras Redes*. Además, se debe conseguir que esta red permita bajar los grandes costos de mantenimiento y operación de sus enlaces dedicados con sus proveedores de información, dando facilidades de conexión con otras entidades.

La descripción de este objetivo fue claro ya que con los antecedentes mencionados en la primera parte se tiene claro el panorama de compartir los gastos de transporte y alquiler de equipos entre todas las entidades ya que esta es para uso de todos. Con este se lograba disminuir en gran cantidad los gastos que demandaban el tener demasiadas conexiones separadas con los proveedores de servicios.

El lograr tener una Empresa que le genere el Outsourcing de el mantenimiento y operación de sus enlaces de información generaba menor gastos a los bancos ya que tenía personal capacitado listo para actuar en caso de problemas sin ser de su empresa.

Para elegir el tipo de plataforma que cumpliera con esas características mencionadas se concluyó con ATM por las ventajas conocidas y por las grandes velocidades que ofrecía sobre las demás plataformas. Utilizando esta plataforma se cumpliría con que sea *rápida, flexible, redundante, escalable y que permita interoperabilidad con otras Redes*, ya que todo eso lo cumple.

Adicionalmente, tenemos que la tendencia de utilizar protocolos como TCP/IP nos permite dar la facilidad a la red de generar una interconexión no únicamente para datos si no también se tiene la de voz. Esta interconexión permitirá una

reducción considerable en los costes de llamadas telefónicas que se realizan entre las entidades bancarias y sus proveedores de información. El objetivo trazado para la propiedad de transporte de VoIP apunta a la interconexión de las todas las Centrales telefónicas de los bancos y de sus proveedores de información. Esto daría mayor opción de ahorro de costos y optimizaría al máximo el uso de esta Red.

2.3. Topología de la red

Con la descripción de la Topología de la Red podemos tener un mejor entendimiento del planteamiento e implementación del proyecto. La cual se resume en lograr interconexión entre las sedes hacia un Nodo Principal el cual actuaría como “Core” de la Red IP.

2.3.1. Descripción de la topología de los enlaces

Los enlaces de los Bancos y de los proveedores estaban dirigidos hacia un Nodo Principal un Nodo Redúndate. Ambos de la misma condición y parámetros de esta manera se tenía una redundancia de 1:1, es decir, se caía el enlace principal automáticamente se conmutaba al secundaria sin afectar el buen rendimiento del enlace. No se utilizaría este enlace redundante para compartir la carga si no, únicamente en caso de pérdida del enlace principal. Al mostrar la imagen se debe de tener en cuenta que únicamente se considera la Red Lógica hasta el equipo router en la Sede del Banco o proveedor. Es decir, las conexiones internas serán verificadas en otra sección a mas detalle. La Red esta compuesta por las conexiones lógicas de los puntos terminales y el Nodo Central que conformaría nuestro Core. En la gráfica que se muestra en la pagina a continuación nos indica las conexiones lógicas entre los equipos ha instalar. Estas conexiones lógicas son de las velocidades mostradas en el gráfico. Tenemos un enlace principal con una velocidad de 1 Mbps, luego un

enlace redundante hacia un Nodo secundario con la velocidad de 1 Mbps. Como consecuencia de tener una llegada hacia el local del banco o proveedor se colocó un tercer enlace redundante que es la conexión ISDN hacia el Nodo Secundario para evitar problemas de Ultima Milla y se perdieran Ambos enlaces lógicos hacia el Core Principal.

Adicionalmente, se puede observar que no se hace mención de los equipos del Nodo Principal ya que estos serán descritos más adelante; únicamente se observan los enlaces de conexión WAN entre el Core y las sedes remotas.

Se puede observar que se planteo la topología lógica en generar un doble enlace hacia los routers centrales para poder tener la capacidad de re-enrutar ciertos paquetes y si en algún caso se pudiera realizar compartimiento de carga o llamado también “Load-Balancing”. Esta configuración de permitía tener en el mismo dominio de Broadcast la conexión del router con ambos routers, dando facilidad en la redundancia y que esta fuera en forma dinámica. Se puede observar que todo esto se realiza mediante el uso de VLANs asignadas a cada una de las sedes y permite acabar en cada una de estas una conexión ATM . Permitiendo de esta manera la escalabilidad de la Red para permitir el crecimiento en cuanto la cantidad de PVCs de conexión como también de Nodos Principales de conexión.

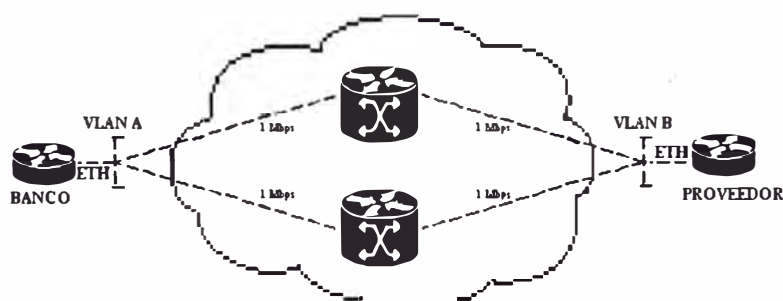


Figura 2.8 - Topología de Interconexión lógica para el intercambio de datos entre Bancos y Proveedores.

Toda la Red esta compuesta por **30 puntos** los cuales están repartidos entre Bancos y Proveedores de Información. Con esta capacidad inicial fue instalada, pero su diseño le dio la opción de crecimiento y flexibilidad para incorporar mas sedes y aumentar ese número inicial de sedes.

Para el intercambio de información entre los Bancos y los proveedores de información se tendría una conexión de la manera como muestra la gráfica a continuación.

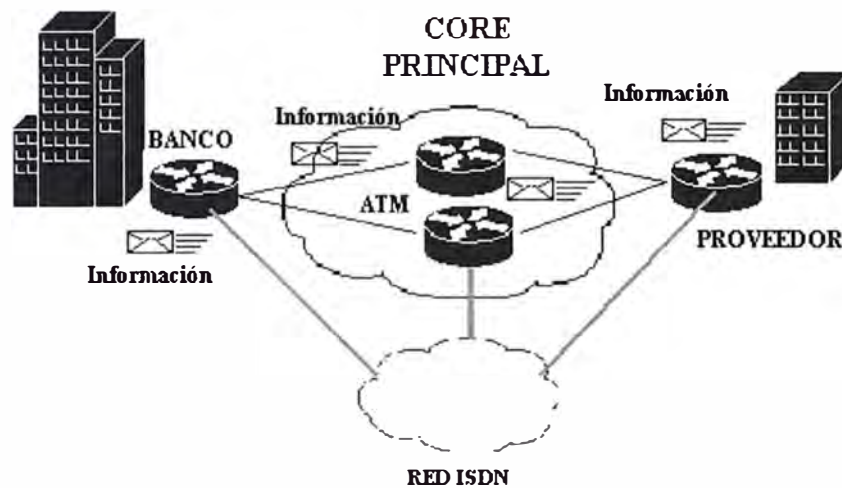


Figura 2.9 - Intercambio de información entre los Bancos y los proveedores.

En todo momento se lograría tener conexión con el proveedor de información para lograr acceder a la Base de Datos que necesite y realice las consultas del caso. Como observación principal que se puede tener es que son consultas transaccionales es decir, se le envía un requerimiento al proveedores de información y este le envía la respuesta al Banco. Pero la pregunta debe de ser ¿Como se logra esto?, la respuesta es utilizando simplemente los aplicativos generados por cada proveedor de Información los cuales son previamente aprobados por cada departamento de IT de cada Banco.

La Red de bancos generaría una Plataforma de conexión IP y los IT de cada Banco y proveedores generarían los Aplicativos sobre TCP/IP para que se generen tubos de conexión sobre sockets determinados e identificados para transportar la información. Esto es mostrado en el siguiente gráfico.

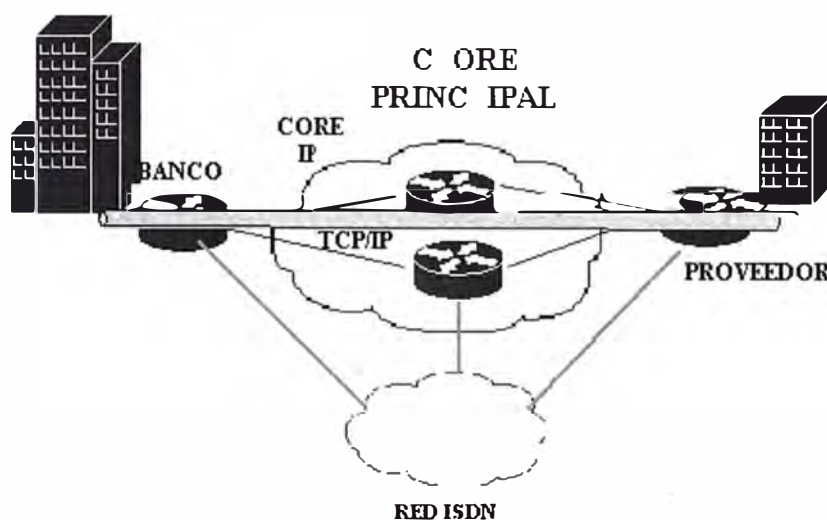


Figura 2.10 - Generación de tubos de conexión entre un Banco y un Proveedor mediante conexiones TCP/IP

Por ser una conexión con esas características no interesa por que parte de los enlaces pasará únicamente desean llegar hasta su punto final (End - Point).

Para terminar con la explicación de la Arquitectura lógica de los Enlaces de la Red de Bancos definimos que se cuenta con dos partes reconocidas en la arquitectura de la Red: Nodo central o *Core IP* y los equipos de Distribución y Acceso a la Red los cuales permitirán la flexibilidad comentada en el proyecto más adelante.

CAPÍTULO III CONMUTADORES Y ENRUTADORES DE INTERFACES ETHERNET/ATM

3.1. Descripción de los equipos utilizados en la red ATM -Ethernet

Para tener un mejor concepto sobre los equipos que se utilizaron y participaron en el proyecto se agrupará en equipos utilizados en la Red del Proveedor de Servicios y los equipos que serán utilizados en la Red de Multiservicios para Interconexión Bancaria. Es necesario la descripción de estos ya que implica el poder reconocer las funciones y formas de conexión entre ellos.

3.2 Descripción de la red del proveedor de servicios ATM

Equipo switch bpx 8620 (equipo atm)

El switch BPX 8620 es conmutador que trabaja en el protocolo ATM, el cual trabaja con conceptos experimentales tal como prevención de congestión en ATM de redes, servicio garantiza para clases múltiples de servicio, utilización justa y eficiente de los recursos de red, avanzada gestión de buffers, para ser utilizado en una red totalmente distribuida para el transporte de información.

La flexibilidad de la arquitectura del BPX permite la entrega de todos los beneficios del Protocolo ATM. Las características arquitectónicas básicas del BPX broadband constan de ranuras en el chasis (12 ranuras) que son disponibles a módulos de función de apoyo que implementan interfases de troncal / Línea a otro BPX/IGX/MGX o interfaces ATM UNI/NNI. Dos de ranuras se reservan para las tarjetas redundantes de control (BCCS), que combina ambos el conmutador y el

subsistema de control. Una de ranura se usa para la tarjeta de control de alarmas (ASM).

La función primaria del Conmutador es la de pasar tránsito entre las tarjetas de interfase. Una matriz crosspoint provee a los usuarios un mejor desempeño comparada al del autobús.

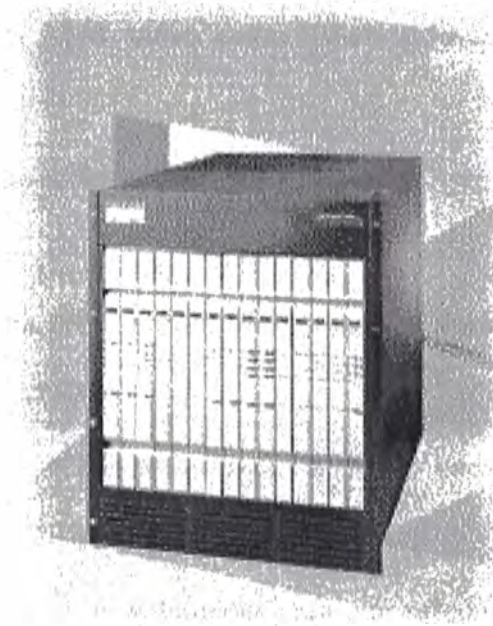


Figura 3.1- Vista frontal de un BPX 8620

Contiene una tarjeta BCC (broadband control card) que puede estar configurada como redundante y esta soporta las siguientes funciones:

- ✓ Conmutación de celdas ATM
- ✓ Comunicación interna Local y a Nodos Remotos
- ✓ Sincronización del Nodo
- ✓ Comunicación para la Administración de la Red
- ✓ Comunicación de Administración Local

Adicionalmente posee Tarjetas con interfaces de Alta densidad que proveen características avanzadas en ATM. Estas características avanzadas incluyen estándares basados en la administración del tráfico ATM, administración de cada circuito virtual (VC) y la administración de interfaces basadas en celdas hacia un equipo cliente (CPE) vía interface UNI o hacia interfaces ATM de otros equipos vía interfaces NNI estándares. Posee los siguientes tipos de interfaces:

- ✓ BXM-T3 — Soporta ATM nativo como troncal o línea y posee puertos con velocidad de un T3.
- ✓ BXM-E3 — Soporta ATM nativo como troncal o línea y posee puertos con velocidad de un E3.
- ✓ BXM-155 — Soporta ATM nativo como troncal o línea y posee puertos con velocidad de un OC-3 / STM-1.
- ✓ BXM-622 — Soporta ATM nativo como troncal o línea y posee puertos con velocidad de un OC-12 / STM-4.

Cada tarjeta del BPX están habilitadas para que se configure ambas tipos de conexiones PVCs o SVCs para los siguientes servicios ATM:

- ✓ Constant bit rate (CBR)
- ✓ Real-time variable bit rate (RT-VBR)
- ✓ Non-real time variable bit rate (NRT-VBR)
- ✓ Unspecified bit rate (UBR) with EPD
- ✓ Available bit rate (ABR)

Con esta variedad de tarjetas y capacidad de configuración de PVCs y SVCs podemos generar una Red con estos equipos los cuales nos permitan conectar a ellos equipos de clientes en forma directa o asimismo colocar equipos que permitan

cambiar el tipo de interface para la entrega del servicio según la velocidad que se desee utilizar. Esto se puede ver en la siguiente figura. Las características técnicas se pueden encontrar en los anexos correspondientes.

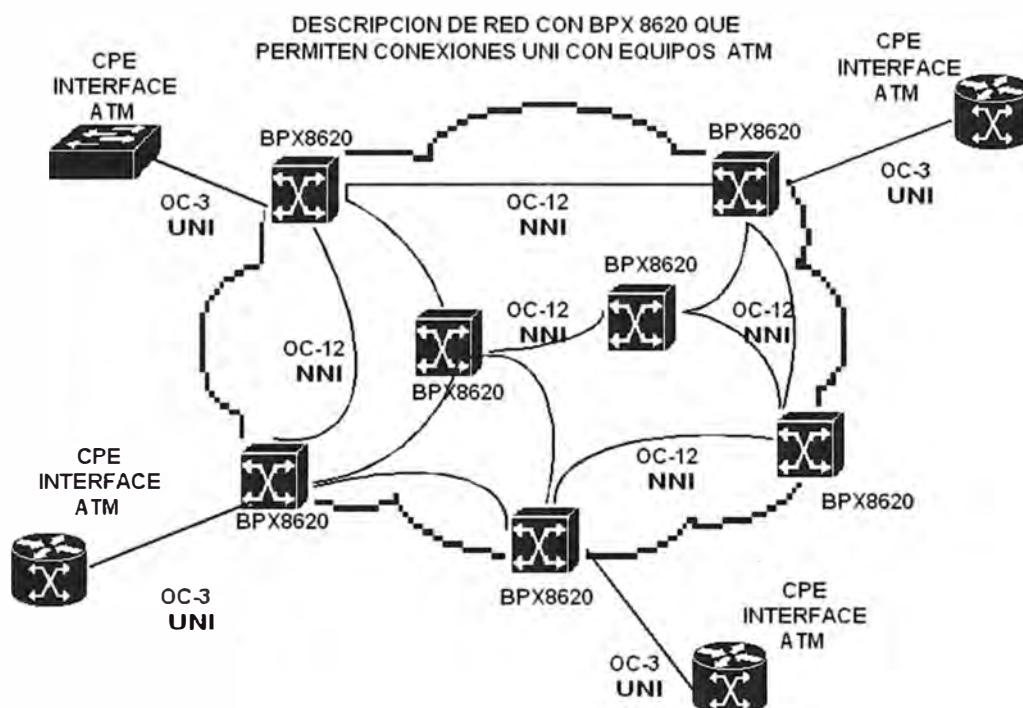


Figura 3.2- Red con BPX8620

Equipo switch catalyst 2820 (equipo ATM – Ethernet)

Los switches Ethernet de las series Cisco Catalyst 2820 son los complementos ideales para la línea de productos de conmutación y enrutamiento de alto rendimiento en ATM/Ethernet. Se distinguen por su facilidad de uso, configuración flexible y capacidad de actualización. Los switches de edición Standard están diseñados para trabajar rápidamente y conectar computadoras de sobremesa a servidores de alta velocidad o a una red backbone. El software edición Enterprise añade una capacidad de ampliación sin precedentes, así como una gran flexibilidad

en opciones de configuración de la red, incluyendo soporte para redes locales virtuales (VLAN), optimización del ancho de banda, seguridad mejorada y una óptima capacidad de gestión. Puede adquirir ahora el alto rendimiento y las capacidades de gestión del edición Enterprise o bien hacerlo en un futuro.

Los switches Ethernet de la edición Standard, Catalyst 2820, son una inversión adecuada para aumentar el ancho de banda de la red entre usuarios y servidores, con un costo comparable al de hubs gestionados. Una interfaz de navegador Web, y el soporte incorporado para Domain Name Service (DNS) y Dynamic Host Control Protocol (DHCP) consiguen que sea extraordinariamente sencillo de usar. El Catalyst 2820 ofrece una flexibilidad adicional gracias a sus dos ranuras y a un conjunto de módulos 100BASE-T, FDDI y ATM. Todos los switches de la edición Standard pueden actualizarse con la compra del kit de actualización a la edición Enterprise.

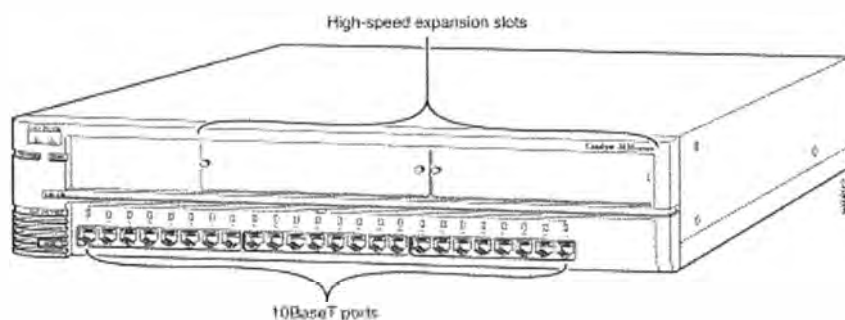


Figura 3.3 - Vista frontal del Catalyst 2820

Los switches Cisco de la edición Enterprise, Catalyst 2820, ofrecen enlaces de alta capacidad y capacidad de interconexión mediante la agregación de puertos Fast EtherChannel®. Fast EtherChanel puede proporcionar hasta 400 Mbps de ancho de banda por enlace en modo dúplex completo, dando un enlace ascendente óptimo a

backbones y servidores de alto rendimiento. Asimismo, los switches proporcionan una administración más sencilla, mejoras en la seguridad y control de distribución a través de enlace troncal ISL VLAN. Los switches de la serie Catalyst 1900 y 2820 mejoran la seguridad mediante la implementación de un control de acceso centralizado a través de TACACS+. Las contraseñas de consola multinivel permiten también la implementación de un sistema de acceso flexible y seguro para la consola de conmutación. Para facilitar su instalación en una red de gran tamaño, los switches de la edición Enterprise soportan la autoconfiguración de switches múltiples a través de un servidor de arranque y pueden gestionarse a través de la interfaz de líneas de instrucciones (CLI) Cisco IOS(r) Utilizados en combinación con los routers Cisco, switches de chasis y servidores de acceso, los switches de la edición Enterprise proporcionan mayor rendimiento, control de la gestión y mayor facilidad de uso en una red global Cisco.

Maneja los estándares siguientes:

- ✓ Dúplex completo IEEE 802.3x en puertos 10BaseT y 100 BaseT
- ✓ Control de flujo IEEE 802.3x en puertos 100BASE-T
- ✓ Protocolo de árbol de conmutación IEEE 802.1d
- ✓ Compatible con las especificaciones IEEE 802.3u 100BASE-TX y 100BASE-FX
- ✓ Especificación IEEE 802.3 10BASE-T
- ✓ Especificación AUI IEEE 802.3
- ✓ ATM Forum LANE 1.0; UNI 3.0/3.1; RFC 1483

Con la variedad de tarjetas que soporta en sus enlaces de Link podemos encontrar tarjetas de conexión OC-3 (Una velocidad de 155Mbps) nos permite

conectar estos equipos a la Red ATM generada por los BPX8620 mostrados anteriormente.

Estos equipos se conectan en forma directa y permiten cambiar el tipo de interface ATM a una interface Ethernet y por seguridad se utiliza la opción de generación de VLANs para la entrega del servicio según la velocidad que se desee utilizar. Esto se puede ver en la siguiente figura. Las características técnicas se pueden encontrar en los anexos correspondientes.

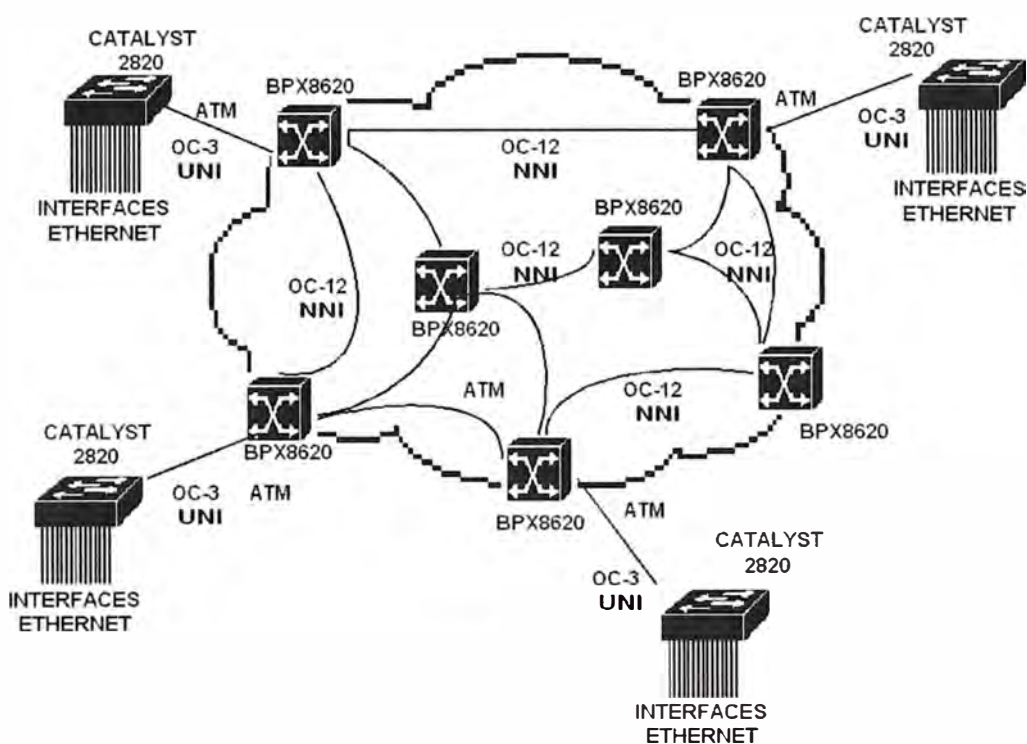


Figura 3.4 - Descripción de la conexión del Catalyst 2820 a la Red ATM para entregar interfaces Ethernet (10 Mbps)

3.3 Descripción de los equipos utilizados en la red sobre servicios ATM

Equipo Router 7206 (Equipo ATM – Ethernet - Fastethernet)

Las empresas y los proveedores de servicios siguen enfrentando la necesidad de optimización de los costos de gestión y funcionamiento, simplificando la gestión de redes y aumentando las oportunidades de beneficios. La serie Cisco 7200 satisface estos requisitos, ya que aún en una sola plataforma de bajo costo las funciones que antes llevaban a cabo varios dispositivos independientes. Mediante la integración de funciones, la plataforma multifunción de alto rendimiento Cisco 7200 ofrece una sola plataforma de bajo costo que admite:

- ✓ Interfaces LAN y WAN de alta densidad
- ✓ Conectividad ATM y Packet over SONET
- ✓ Conectividad directa Circuit Emulation Standard (CES) ATM para voz, datos y vídeo
- ✓ T3/E3 y T1/E1 multicanal de alta densidad con unidad de servicio de canal/unidad de servicio de datos (CSU/DSU) integrada
- ✓ Conectividad directa con el canal del procesador central de IBM
- ✓ Conmutación Ethernet Capa 2 de baja densidad
- ✓ Conectividad digital con el codificador-descodificador de voz y vídeo (CODEC) de centralitas telefónicas (PBX) T1/E1

Los routers de la serie Cisco 7200 pueden utilizarse con eficiencia, tanto en las redes de los proveedores de servicios como en las de las empresas para reducir los costos de aprovisionamiento WAN, dar soporte a servicios diferenciados y proporcionar aplicaciones de valor añadido como la gestión del tráfico, la

contabilidad y la calidad de servicio (QoS), y todo ello desde una sola plataforma. Las aplicaciones principales de los routers de la serie Cisco 7200 incluyen:

- ✓ Frontera WAN multifunción de alto nivel
- ✓ Backbone de empresa
- ✓ Equipamiento en la ubicación del cliente (CPE) del proveedor de servicios
- ✓ Puntos de presencia (POP) de proveedores de servicios
- ✓ Centros de datos de computadoras centrales y campus IBM

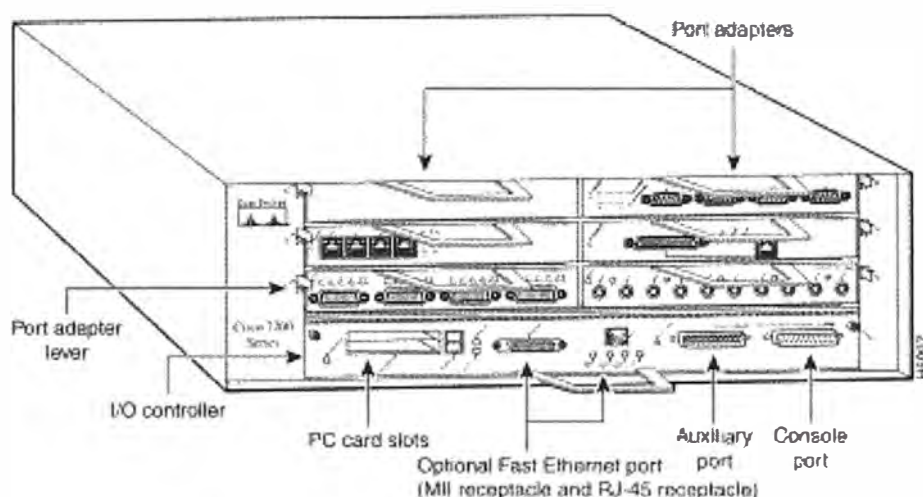


Figura 3.5: Vista Frontal del Router Multiservicio 7200

La serie Cisco 7200 cuenta con todos los servicios de software Cisco IOS® responsables de la gestión de la seguridad de la red, asignando QoS entre las aplicaciones o los usuarios, y ofreciendo servicios de valor añadido, tales como la contabilidad y cifrado NetFlow. Las aplicaciones QoS, como por ejemplo Committed Access Rate (CAR), Weighted Random Early Detection (WRED) y Weighted Fair Queuing (WFQ), pueden aplicarse de forma flexible para proporcionar precedencia entre direcciones IP, aplicaciones o usuarios específicos con un nivel alto de detalle.

La tecnología NetFlow forma parte del software Cisco IOS y permite que las empresas y los proveedores de servicios obtengan importantes ventajas del Cisco

7200, ya que proporciona de forma eficaz la información de contabilidad de tráfico necesaria para aumentar los ingresos y reducir los costos. NetFlow mejora las aplicaciones clave, incluyendo una contabilidad y facturación flexible y detallada para el uso de los recursos de la red y de las aplicaciones; monitorización proactiva de la red y resolución de problemas; e ingeniería de red táctica y planificación estratégica responsable.

La serie Cisco 7200 consta de un router Cisco 7206 de seis ranuras. La serie Cisco 7200 ofrece una densidad con capacidad de ampliación con una extensa gama de interfaces. Entre estas interfaces se incluyen:

- ✓ Ethernet, Fast Ethernet, 100VG-AnyLAN, Token Ring
- ✓ Fiber Distributed Data Interface (FDDI) (no disponible para VXR), serie
- ✓ ISDN (RDSI) de acceso primario (PRI)
- ✓ Interfaz de acceso básico (BRI), Interfaz serie de alta velocidad (HSSI), Packet over T3/E3, T1/E1/T3 multicanal y ATM

La serie Cisco 7200 ofrece unos niveles excepcionales de fiabilidad, disponibilidad y capacidad de reparación diseñados para hacer frente a aplicaciones vitales para la empresa. Con el fin de garantizar un alto nivel de disponibilidad, los sistemas Cisco 7200 admiten fuentes de alimentación duales con corriente compartida (corriente alterna o corriente continua) y la instalación y extracción en actividad de adaptadores de puerto de manera que puedan añadirse, extraerse o reemplazarse sin interrumpir el servicio. Una tarjeta de memoria Flash PC aumenta la fiabilidad ya que puede almacenar imágenes de software y archivos de configuración. Para aprovechar el tiempo de actividad al máximo, el Cisco 7200 es compatible con el protocolo Hot Standby Router Protocol (HSRP) del software Cisco IOS, que permite cambiar con

rapidez a un router de respaldo en caso de que fallen el sistema o el enlace. Los controladores ambientales ofrecen diversos niveles de ampliación de manera que el operador puede corregir problemas antes de que se cierre el sistema. Todos los componentes del sistema Cisco 7200 pueden sustituirse con facilidad.

El sistema Cisco 7200 también incluye una herramienta de gestión basada en HTML para simplificar la configuración y gestión de routers. Los clientes pueden usar un explorador Web para navegar a través de la interfaz de línea de instrucciones (CLI) con enlaces activos. A través de los enlaces activos los clientes también pueden resolver problemas básicos y verificar las versiones de software.

Con esta variedad de tarjetas y capacidad de configuración de PVCs y SVCs podemos considerarlo como un equipos para que sea CORE de la Red. Con esta capacidad no permitirá conectarnos a la Red ATM del Proveedor de transporte. Esto se puede ver en la siguiente figura. Las características técnicas se pueden encontrar en los anexos correspondientes.

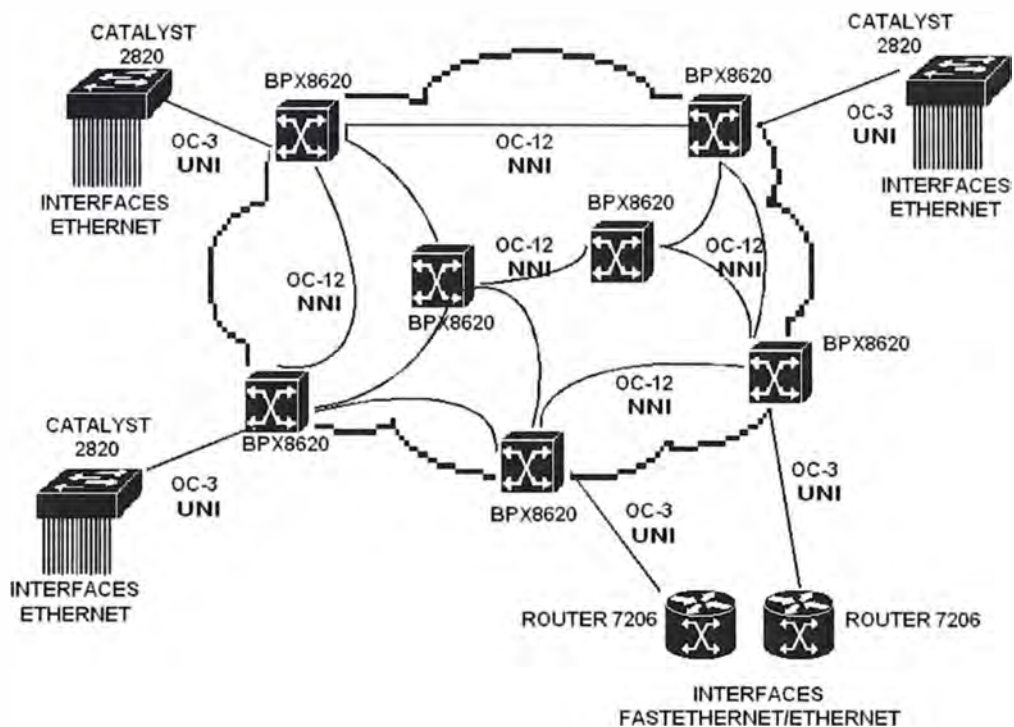


Figura 3.6- Descripción de la conexión del Router 7206 a la Red ATM

Equipo Router 2611 (Equipo Ethernet)

Cisco Systems proporciona una solución para las oficinas sucursales la integración, potencia y versatilidad de clase empresarial y proveedor con la familia de routers modulares multiservicio de la serie Cisco 2600.

La serie Cisco 2600, con una amplia base instalada, ofrece una solución rentable para satisfacer las necesidades actuales y futuras de las sucursales en lo referente a:

- ✓ Integración multiservicio de voz y datos
- ✓ Acceso a redes privadas virtuales (VPN) con opciones de firewall
- ✓ Servicios de acceso telefónico analógico y digital
- ✓ Enrutamiento con gestión de ancho de banda
- ✓ Enrutamiento entre VLAN

La arquitectura modular de la serie Cisco 2600 permite actualizar las interfaces para ajustarlas a la expansión de la red o a los cambios tecnológicos que se producen cuando se instalan nuevos servicios y aplicaciones. Al compartir las interfaces modulares con las series Cisco 1600, 1700 y 3600, la serie Cisco 2600 proporciona una protección de la inversión inigualable. Mediante la integración de las funciones de varios dispositivos independientes en una sola unidad compacta, la serie Cisco 2600 reduce la complejidad de gestionar la solución para redes remotas.

Con un potente procesador RISC y DSP de alto rendimiento y procesadores auxiliares en varias interfaces, la serie Cisco 2600 admite calidad de servicio (QoS) avanzada, seguridad y las características de integración en la red que actualmente demandan las sucursales.

La serie Cisco 2600 está disponible en tres niveles de rendimiento y seis configuraciones base:

- ✓ Cisco 2650 y Cisco 2651: hasta 37.000 de paquetes por segundo (pps), uno y dos puertos Ethernet 10/100 Mbps con autodetección
- ✓ Cisco 2620 y Cisco 2621: hasta 25.000 de pps, uno y dos puertos Ethernet 10/100 Mbps con autodetección
- ✓ Cisco 2610 a Cisco 2613: hasta 15.000 pps
- ✓ Cisco 2613: un puerto Token Ring
- ✓ Cisco 2612: un puerto Ethernet, un puerto Token Ring
- ✓ Cisco 2611: dos puertos Ethernet
- ✓ Cisco 2610: un puerto Ethernet

Todos los modelos también disponen de dos ranuras para tarjetas de interfaz WAN (WIC), una ranura para el módulo de red y una ranura para un módulo de

integración avanzada (AIM). Estas ranuras comparten más de cincuenta módulos distintos entre cuatro líneas de productos de Cisco.

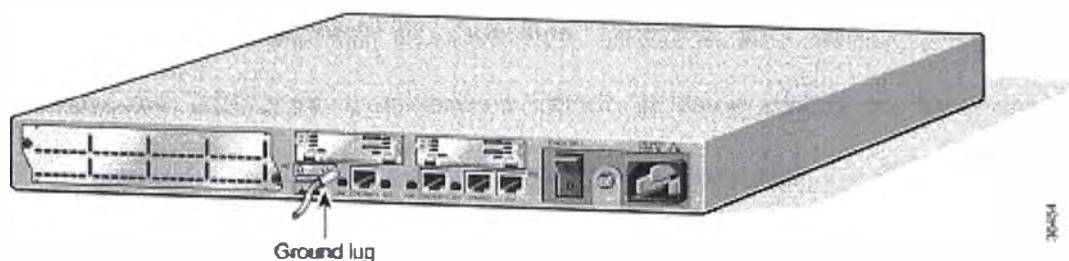


Figura 3.7: Vista posterior del router Multiservicio Cisco 2611

Las tarjetas de interfaz WAN disponibles para los routers Cisco 1600, 1700, 2600 y 3600 admiten una amplia gama de opciones seriales, RDSI de acceso básico y de unidad de servicio de canal y unidad de servicio de datos (CSU/DSU) para conexión WAN principal y de respaldo. Los módulos de red disponibles para las series Cisco 2600 y 3600 admiten una amplia gama de aplicaciones, incluyendo la integración multiservicio voz/datos, acceso telefónico analógico y RDSI, así como concentración de dispositivos serie. El módulo de integración avanzada de compresión de datos de la serie Cisco 2600 descarga a la CPU principal de las tareas de compresión de datos de alta velocidad, permitiendo que el tráfico de datos comprimidos alcance los 8 Mbps mientras libera las ranuras de interfaces externas para otras aplicaciones.

Al formar parte de las completas soluciones de red Cisco de extremo a extremo, la serie Cisco 2600 permite a las empresas ampliar la infraestructura de red de forma transparente y rentable a las pequeñas sucursales y les ofrece las siguientes ventajas:

- ✓ Protección de la inversión: ya que la serie Cisco 2600 admite componentes modulares actualizables en la instalación, los clientes pueden cambiar con

facilidad las interfaces de red sin tener que realizar una "actualización integral" de la solución implementada en la red de la oficina remota. Otra forma en que la ranura AIM de la plataforma Cisco 2600 protege la inversión económica es ofreciendo la capacidad de expansión necesaria para admitir servicios avanzados, tales como compresión y cifrado de datos asistida por hardware, aunque esta última función estará disponible próximamente.

- ✓ Costo de operación reducido: mediante la integración de las funciones de las CSU/DSU, dispositivos de terminación de red RDSI (NTI), modems firewalls, dispositivos de compresión o cifrado y demás equipamiento de los recintos de cableado de las sucursales en una sola unidad, la serie Cisco 2600 ofrece una solución que ahorra espacio y que puede gestionarse remotamente usando aplicaciones de administración de redes tales como CiscoWorks y CiscoView.
- ✓ Integración multiservicio voz/datos: Cisco ofrece la solución de integración multiservicio voz/datos más amplia y con mayores posibilidades de crecimiento. La serie Cisco 2600 permite a los administradores de redes reducir los costos de las llamadas de larga distancia entre oficinas y permite utilizar aplicaciones de nueva generación, como la mensajería integrada y centros de llamadas basados en Web. Utilizando los módulos de voz/fax, el router Cisco 2600 puede instalarse en redes de voz a través de IP (VoIP) y voz a través de Frame Relay (VoFR). Si se utilizan con el nuevo módulo de red troncal de voz por paquetes, un solo dispositivo de la serie Cisco 2600 puede admitir 60 llamadas de voz simultáneas, además de enrutamiento y otros servicios.
- ✓ Solución de clase empresarial y proveedor: cumple los requisitos que exigen las empresas de multiservicio y sus proveedores de servicios gestionados de

terminal de abonado con características de alta fiabilidad, conexiones WAN múltiples y la posibilidad de migrar de una infraestructura de sólo datos a una de TDM voz y datos.

Estos equipos serían los que se consideraran para los CPE; se instalarían en las Sedes para que sirvan de equipos multiservicio y poder interconectar la información y adicionalmente la parte de VoIP en cada Sede. Esto podría verse de la siguiente manera para un mejor entendimiento.

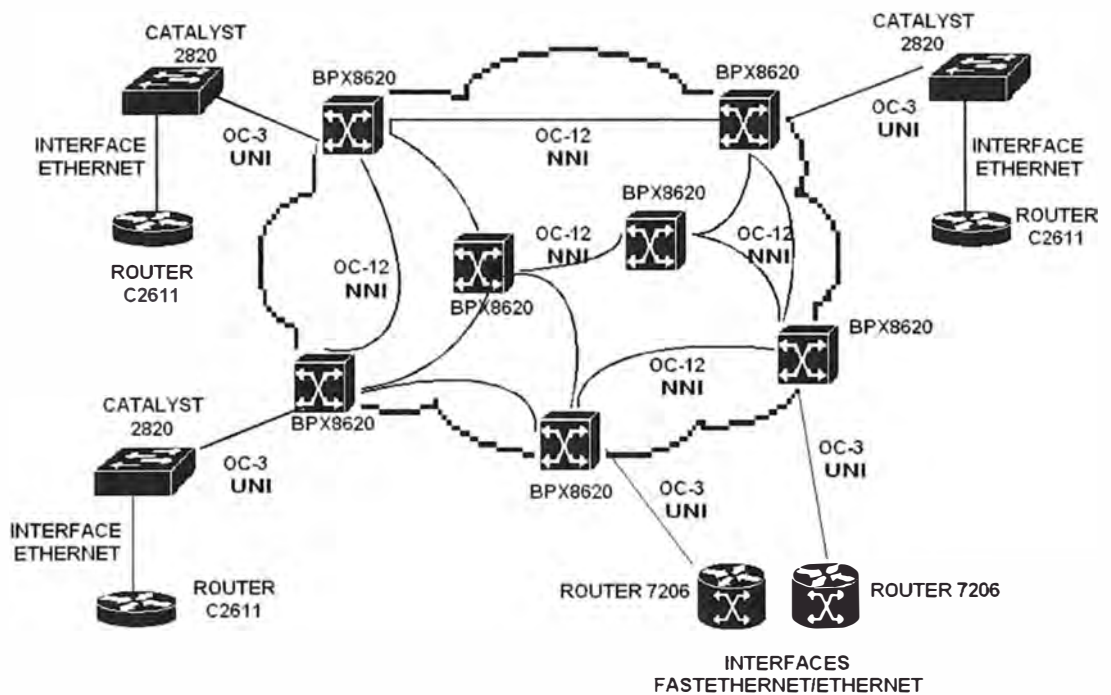


Figura 3.8: Distribución de los Router Cisco 2611

Con la figura anterior se puede uno dar cuenta las conexiones de los equipos y las formas de cómo estos han sido distribuidos para poder ofrecer una distribución y arquitectura de Red que se adapte al proveedor del transporte. Desde el punto de vista como cliente de la Red ATM este se ve de la siguiente manera:

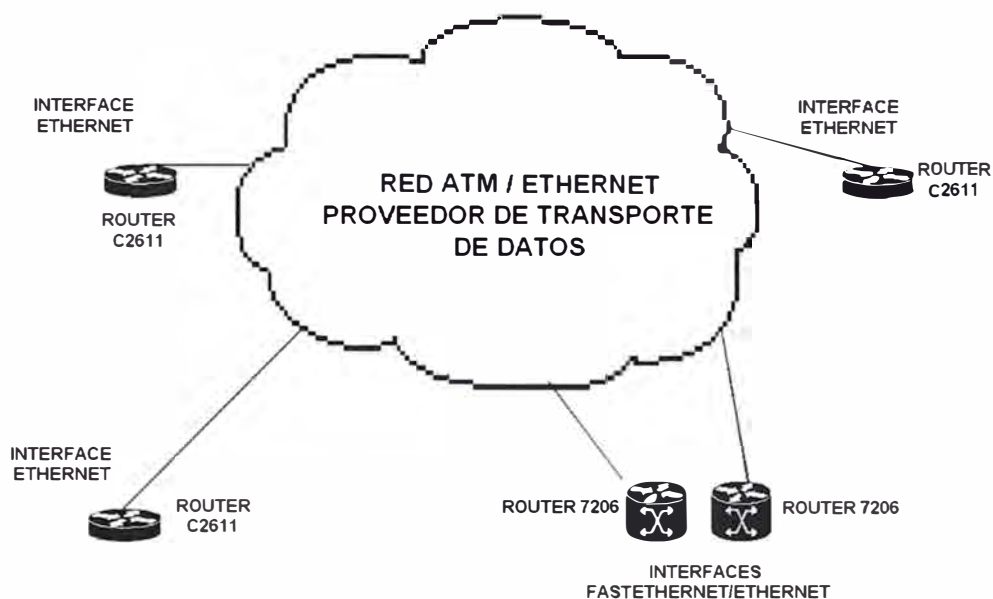


Figura 3.9: Red entregada al Cliente desde su punto de vista.

Se puede observar que se logró describir los equipos que se utilizarán en la Red de Transporte de Datos para la Interconexión Bancaria quedando claro la necesidad de encontrar este proveedor con transporte ATM/Ethernet descrito. Adicionalmente a las descripciones de los equipos utilizados se puede encontrar en los anexos mas detalle de las características y parámetros técnicos de cada uno de estos, como también la descripción de las tarjetas de VoIP que se utilizaron para la integración de la parte de Voz.

CAPÍTULO IV

DISEÑO DE LA RED ATM/ETHERNET Y DEL BACKBONE IP PARA LA INTERCONEXIÓN DE LAS REDES BANCARIAS

4.1. Antecedentes para el diseño de la red ATM/Ethernet

Esta Red de Interconexión es entre los Bancos y sus proveedores de Información. Entonces utilizando el capítulo anterior se tiene la distribución y los equipos a utilizar de acuerdo al protocolo que maneja la interface de conexión a la Red del Proveedor de transporte. Tenemos que se tiene una Red que puede proveer servicio de transporte de datos y puede ser conectada y atendida mediante interfaces Ethernet (Para velocidades Bajas) e interfaces OC-3 ATM (Para mayor velocidad de concentración).

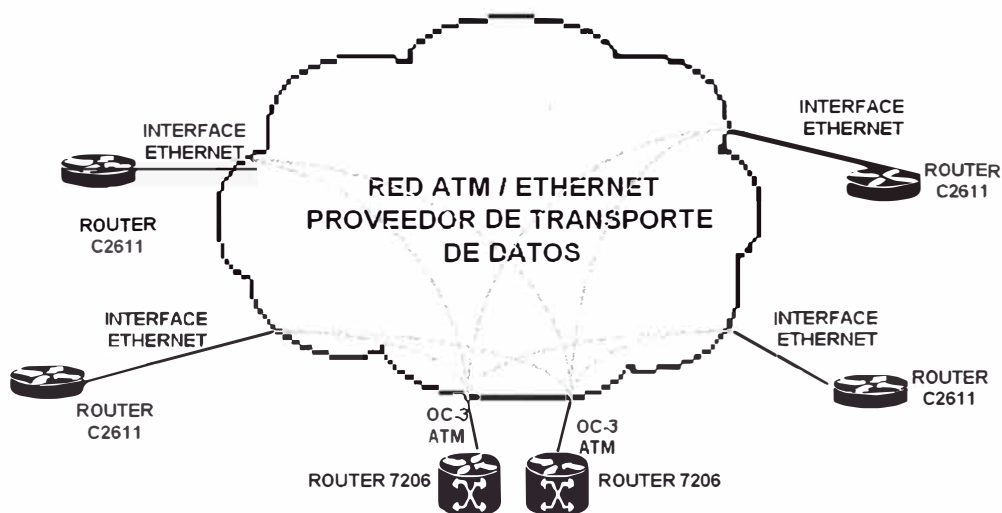


Figura 4.1 - Descripción de las Interfaces que se puede manejar en este proyecto para generar la Red ATM / ETHERNET

4.2 Descripción de los enlaces y descripción lógica de la red

Recordando el Capítulo 2 tenemos que los enlaces llegarían hacia un Equipo Ethernet/ATM el cual dividiría los dominios de Broadcast mediante la utilización de VLANs las cuales recibirían las conexiones de los 02 distintos Nodos principales ATM. Cada Enlace será de 1 Mbps hacia cada Nodo del Core IP el cual estará presentará una Topología en estrella para lograr la conectividad con todos

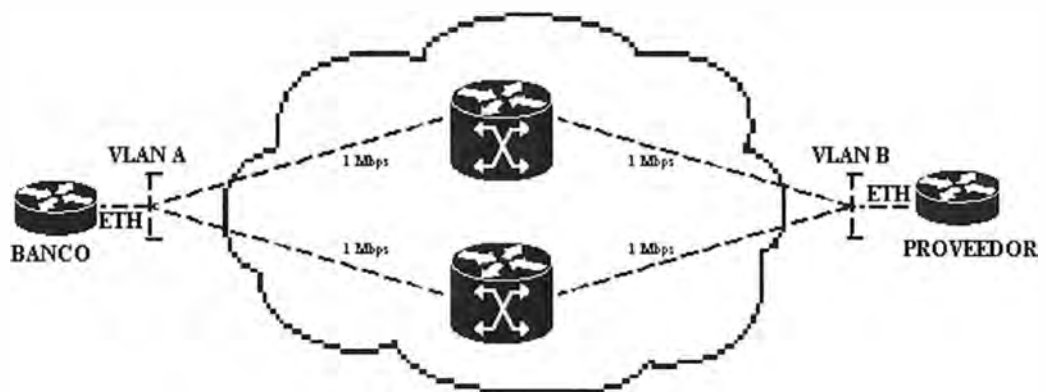


Figura 4.2 - Conexión con el Core IP mediante la utilización de VLANs.

La conectividad por cada VLAN es mediante sub-interfaces ATM las cuales manejan un dominio de Broadcast. Esto permite generar subnets para conectividad múltiple con más de 02 Nodos Principales o de Core. Esta particularidad permitirá más adelante incrementar nuevas Redes Sobre un mismo equipo o a su vez colocar equipos de redundancia prendidos en forma paralela sobre el mismo segmento WAN de las conexiones. A continuación mostramos el diagrama Lógico de la Red con los distintos nodos conectados y sus enlaces redundantes (Fig 4.3).

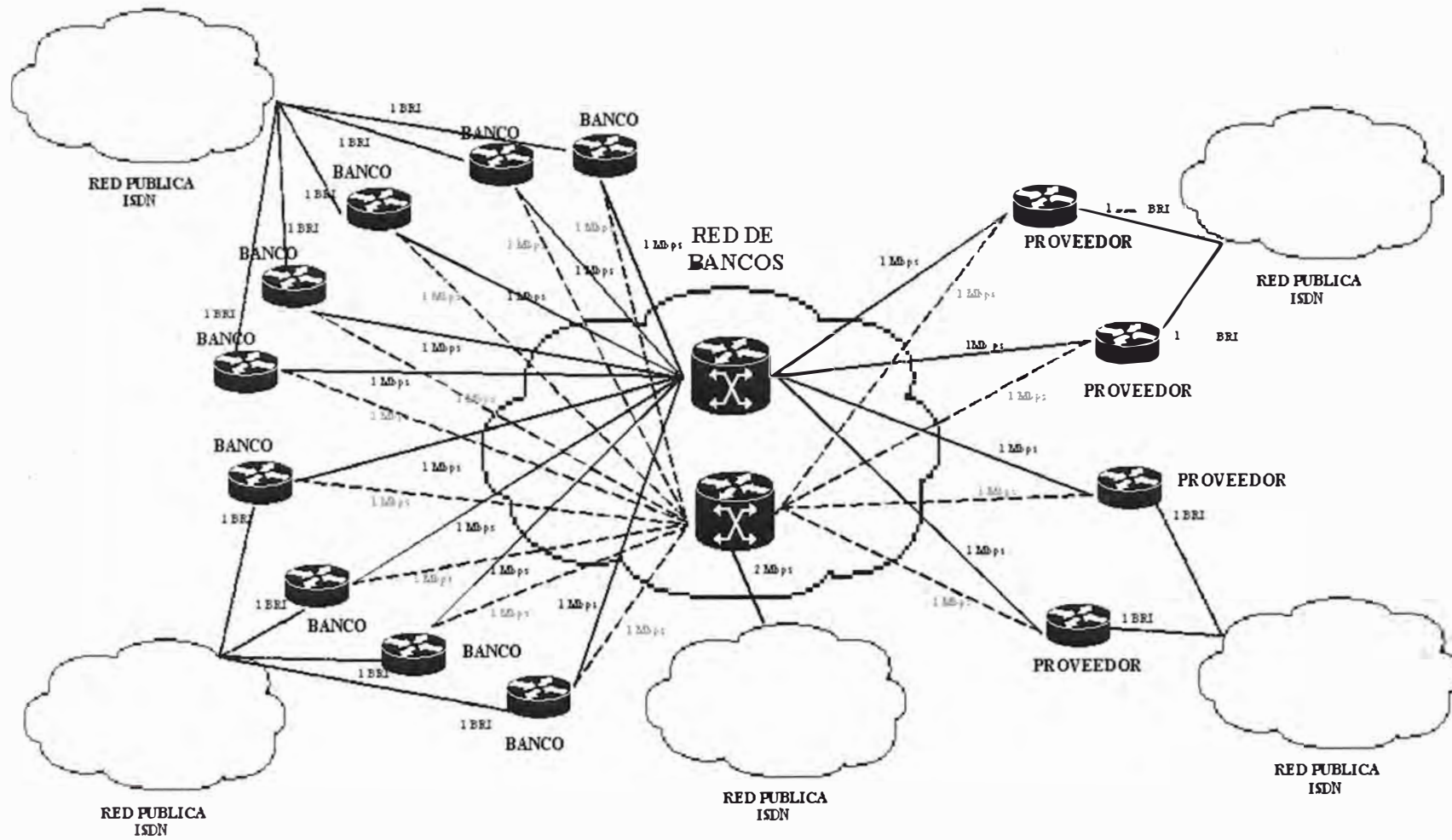


Fig. 4.3 - Diagrama Lógico de la Red de Bancos

4.3 Distribución del plan de numeración

4.3.1 Dimensionamiento de las redes LAN de las sedes remotas

El primer problema a encontrar en este proyecto fue la relación de números IP's de las Redes LAN que se encontrarían en los distintos bancos a interconectar. Estas redes podrían ser las mismas o traslaparse ya que pertenecen a distintos propietarios y ellos tomaban sus propias decisiones.

Por tal motivo se necesitaba encontrar una manera de cómo se iban a conocer las redes de cada Bancos para cualquier transacción y que puedan intercambiar información mediante paquetes IP's sin tener los problemas de traslapes de redes. La solución a este problema fue el conocer a cada red del banco con una Red Privada que nadie utilice en ninguna de sus Sedes y utilizar además una mascara suficiente para soportar todos los servicios que se montarían sobre esta plataforma. Teniendo siempre en cuenta el concepto de crecimiento de la Red a futuras implementaciones y la manera de cómo conectarse a los bancos.

Luego de un levantamiento de información se encontró un común denominador entre todos los puntos participantes, el cual siempre incurrían en utilizar las Redes Privadas mas comunes y conocidas las cuales eran 10.0.0.0/8, 172.16.0.0/16 y las clásicas 192.168.X.0/24. Dichas redes encontradas no se adjunta al presente trabajo por motivos de seguridad y confidencialidad con las redes involucradas. Como dato adicional, se podría decir que un 60% de los puntos incurrían en utilizar la Red Clase B 172.16.0.0/16 con su crecimiento interno hasta 172.21.0.0/16; lo cual dejaba un margen de utilización claro desde la Red 172.16.22.0/16 hasta 172.31.0.0/16. Con la conclusión obtenida de la investigación y recopilación de datos se concluyo en utilizar la Red 172.30.0.0/16 para motivos del proyecto. La cual sería distribuida a

cada punto una subred dentro de esta Red para su reconocimiento e intercambio de información. Esta distribución de IP's se apoyo en las hipótesis de crecimiento y cantidad de servicios sobre cada puntos de conexión.

ITM	SEDE	RED UTILIZADA	RED CRECIMIENTO	CANTIDAD DE USUARIOS
1	BANCO 001	10.0.0/8	SUFICIENTE	1144
2	BANCO 002	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1194
3	BANCO 003	10.0.0/8	SUFICIENTE	1111
4	BANCO 004	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1003
5	BANCO 005	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1102
6	BANCO 006	172.16.0.0/16	172.16.0.0 - 172.21.0.0/16	1087
7	BANCO 007	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1152
8	BANCO 008	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	993
9	BANCO 009	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1116
10	BANCO 010	172.16.0.0/16	172.16.0.0 - 172.19.0.0/16	1054
11	BANCO 011	10.0.0/8	SUFICIENTE	1162
12	BANCO 012	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1016
13	BANCO 013	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1133
14	BANCO 014	10.0.0/8	SUFICIENTE	1080
15	BANCO 015	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1113
16	BANCO 016	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1047
17	BANCO 017	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1111
18	BANCO 018	10.0.0/8	SUFICIENTE	1006
19	BANCO 019	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1081
20	BANCO 020	10.0.0/8	SUFICIENTE	1032
21	PROVEEDOR001	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1154
22	PROVEEDOR002	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1062
23	PROVEEDOR003	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1185
24	PROVEEDOR004	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	980
25	PROVEEDOR005	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1091
26	PROVEEDOR006	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1012
27	PROVEEDOR007	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1126
28	PROVEEDOR008	192.168.1.0/24	192.168.1.0 - 192.168.254.0/24	1172
29	PROVEEDOR009	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1176
30	PROVEEDOR010	172.16.0.0/16	172.16.0.0 - 172.20.0.0/16	1089

Tabla 4.1 – Dimensionamiento de las Redes LAN Sedes remotas

Esta hipótesis se basaron en una Plan de Soluciones posibles a integrar sobre esta Plataforma IP, que son beneficiosas a los Bancos para disminuir la cantidad de enlaces separados y concentrarlos en uno con mayor disponibilidad; Por tal se contó la cantidad de proveedores y la cantidad de nuevas opciones que se presentan en el mercado logrando llegar a un máximo de 100 posibles servicios sobre dicha red.

Esto generaría un crecimiento progresivo de hasta tener la necesidad de mantener 100 conexiones IP distintas entre dichas Redes y que a su vez esa conexión sea hacia 10 distintos puntos. Por tal motivo se tomo la siguiente premisa : “Se necesita asignar subredes de cómo mínimo 120 IP’s y que estas subredes sean como mínimo 120 distintas”. Partiendo de esto se generó el siguiente cuadro de distribución de Redes:

ITM	SEDE	RED ASIGNADA	CANTIDAD DE IP'S DISPONIBLES	OBSERVACION
1	PUNTO 001	172.31.1.0 / 24	254	No se traslapa ni repite
2	PUNTO 002	172.31.2.0 / 24	254	No se traslapa ni repite
3	PUNTO 003	172.31.3.0 / 24	254	No se traslapa ni repite
4	PUNTO 004	172.31.4.0 / 24	254	No se traslapa ni repite
5	PUNTO 005	172.31.5.0 / 24	254	No se traslapa ni repite
6	PUNTO 006	172.31.6.0 / 24	254	No se traslapa ni repite
7	PUNTO 007	172.31.7.0 / 24	254	No se traslapa ni repite
8	PUNTO 008	172.31.8.0 / 24	254	No se traslapa ni repite
9	PUNTO 009	172.31.9.0 / 24	254	No se traslapa ni repite
10	PUNTO 010	172.31.10.0 / 24	254	No se traslapa ni repite
11	PUNTO 011	172.31.11.0 / 24	254	No se traslapa ni repite
12	PUNTO 012	172.31.12.0 / 24	254	No se traslapa ni repite
13	PUNTO 013	172.31.13.0 / 24	254	No se traslapa ni repite
14	PUNTO 014	172.31.14.0 / 24	254	No se traslapa ni repite
15	PUNTO 015	172.31.15.0 / 24	254	No se traslapa ni repite
16	PUNTO 016	172.31.16.0 / 24	254	No se traslapa ni repite
17	PUNTO 017	172.31.17.0 / 24	254	No se traslapa ni repite
18	PUNTO 018	172.31.18.0 / 24	254	No se traslapa ni repite
19	PUNTO 019	172.31.19.0 / 24	254	No se traslapa ni repite
20	PUNTO 020	172.31.20.0 / 24	254	No se traslapa ni repite
21	PUNTO 021	172.31.21.0 / 24	254	No se traslapa ni repite
22	PUNTO 022	172.31.22.0 / 24	254	No se traslapa ni repite
23	PUNTO 023	172.31.23.0 / 24	254	No se traslapa ni repite
24	PUNTO 024	172.31.24.0 / 24	254	No se traslapa ni repite
25	PUNTO 025	172.31.25.0 / 24	254	No se traslapa ni repite
26	PUNTO 026	172.31.26.0 / 24	254	No se traslapa ni repite
27	PUNTO 027	172.31.27.0 / 24	254	No se traslapa ni repite
28	PUNTO 028	172.31.28.0 / 24	254	No se traslapa ni repite
29	PUNTO 029	172.31.29.0 / 24	254	No se traslapa ni repite
30	PUNTO 030	172.31.30.0 / 24	254	No se traslapa ni repite

Tabla 4.2 – Tabla de Ips de las Sedes Remotas

Este cuadro únicamente muestra una cantidad inicial la cual se tiene proyección hasta 255 puntos remotos que podría soportar esta Red IP. Para un mayor entendimiento del cuadro se muestra una regla de formación de dichas redes:

IP LAN : 172.31.(N+1).0

Mascara : 255.255.255.0

Para $N \in [0,253]$; Esto nos daría como resultado una cantidad máxima de 254 subredes que podría soportar en su crecimiento lo cual es suficiente para este caso. Con esta cantidad se podría considerar que hasta 254 puntos se podrían conectar en esta Red IP Privada de Bancos.

4.3.2 Diseño de la red WAN de interconexión de las sedes

Para el diseño de la Red WAN IP de interconexión de las Sedes se observa que la interoperabilidad de las Redes remotas esta solucionado con la distribución de un Plan de enmascaramiento de IP's internas de los clientes por otro planeado y controlado; no se encontraría problemas en elegir una Red IP WAN que no sea la misma de las IP's LAN asignadas a los bancos, pero siempre partiendo sobre una política de planeamiento, la cual se menciona a continuación: "La Red IP WAN elegida debe tener la capacidad de entregar subredes con capacidad mínima de 14 IP's para manejar esa cantidad de conexiones a nodos Principales y redundantes". En base a esta política se consideró manejar redes de mascara /28. Para cuestiones de ejemplo se tomo el siguiente cuadro:

Este cuadro únicamente muestra una cantidad inicial la cual tiene capacidad para crecimiento mínimo de 100 puntos remotas. Para un mayor entendimiento del cuadro se muestra una regla de formación de dichas redes:

ITM	SEDE	IP SUBRED	MASCARA	CANTIDAD IP DISPONIBLES
1	PUNTO 001	10.0.0.0	255.255.255.240	14
2	PUNTO 002	10.0.0.16	255.255.255.240	14
3	PUNTO 003	10.0.0.32	255.255.255.240	14
4	PUNTO 004	10.0.0.48	255.255.255.240	14
5	PUNTO 005	10.0.0.64	255.255.255.240	14
6	PUNTO 006	10.0.0.80	255.255.255.240	14
7	PUNTO 007	10.0.0.96	255.255.255.240	14
8	PUNTO 008	10.0.0.112	255.255.255.240	14
9	PUNTO 009	10.0.0.128	255.255.255.240	14
10	PUNTO 010	10.0.0.144	255.255.255.240	14
11	PUNTO 011	10.0.0.160	255.255.255.240	14
12	PUNTO 012	10.0.0.176	255.255.255.240	14
13	PUNTO 013	10.0.0.192	255.255.255.240	14
14	PUNTO 014	10.0.0.208	255.255.255.240	14
15	PUNTO 015	10.0.0.224	255.255.255.240	14
16	PUNTO 016	10.0.0.240	255.255.255.240	14
17	PUNTO 017	10.0.1.0	255.255.255.240	14
18	PUNTO 018	10.0.1.16	255.255.255.240	14
19	PUNTO 019	10.0.1.32	255.255.255.240	14
20	PUNTO 020	10.0.1.48	255.255.255.240	14
21	PUNTO 021	10.0.1.64	255.255.255.240	14
22	PUNTO 022	10.0.1.80	255.255.255.240	14
23	PUNTO 023	10.0.1.96	255.255.255.240	14
24	PUNTO 024	10.0.1.112	255.255.255.240	14
25	PUNTO 025	10.0.1.128	255.255.255.240	14
26	PUNTO 026	10.0.1.144	255.255.255.240	14
27	PUNTO 027	10.0.1.160	255.255.255.240	14
28	PUNTO 028	10.0.1.176	255.255.255.240	14
29	PUNTO 029	10.0.1.192	255.255.255.240	14
30	PUNTO 030	10.0.1.208	255.255.255.240	14

Tabla 4.3 – Distribución de Redes WAN para Interconexión.

IP WAN : 10.0.M. 16N

Mascara : 255.255.255.240

Para $N \in [0,15]$ y $M \in [0,9]$; Esto nos daría como resultado una cantidad máxima de 160 subredes que podría soportar en su crecimiento los cual es suficiente

para este caso. Siempre se debe de tener en cuenta que se debe de llevar una asignación correlativa para una mejor administración de los recursos.

4.3.3 Diseño de la red de loopbacks de administración de los equipos en las sedes remotas

Para el diseño de la Red WAN IP de interconexión de las Sedes se observa que la interoperabilidad de las Redes remotas esta solucionado con la distribución de un Plan de enmascaramiento de IP's internas de los clientes por otro planeado y

ITM	SEDE	IP SUBRED	MASCARA	CANTIDAD IP DISPONIBL
1	PUNTO 001	10.0.10.0	255.255.255.252	2
2	PUNTO 002	10.0.10.4	255.255.255.252	2
3	PUNTO 003	10.0.10.8	255.255.255.252	2
4	PUNTO 004	10.0.10.12	255.255.255.252	2
5	PUNTO 005	10.0.10.16	255.255.255.252	2
6	PUNTO 006	10.0.10.20	255.255.255.252	2
7	PUNTO 007	10.0.10.24	255.255.255.252	2
8	PUNTO 008	10.0.10.28	255.255.255.252	2
9	PUNTO 009	10.0.10.32	255.255.255.252	2
10	PUNTO 010	10.0.10.36	255.255.255.252	2
11	PUNTO 011	10.0.10.40	255.255.255.252	2
12	PUNTO 012	10.0.10.44	255.255.255.252	2
13	PUNTO 013	10.0.10.48	255.255.255.252	2
14	PUNTO 014	10.0.10.52	255.255.255.252	2
15	PUNTO 015	10.0.10.56	255.255.255.252	2
16	PUNTO 016	10.0.10.60	255.255.255.252	2
17	PUNTO 017	10.0.10.64	255.255.255.252	2
18	PUNTO 018	10.0.10.68	255.255.255.252	2
19	PUNTO 019	10.0.10.72	255.255.255.252	2
20	PUNTO 020	10.0.10.76	255.255.255.252	2
21	PUNTO 021	10.0.10.80	255.255.255.252	2
22	PUNTO 022	10.0.10.84	255.255.255.252	2
23	PUNTO 023	10.0.10.88	255.255.255.252	2
24	PUNTO 024	10.0.10.92	255.255.255.252	2
25	PUNTO 025	10.0.10.96	255.255.255.252	2
26	PUNTO 026	10.0.10.100	255.255.255.252	2
27	PUNTO 027	10.0.10.104	255.255.255.252	2
28	PUNTO 028	10.0.10.108	255.255.255.252	2
29	PUNTO 029	10.0.10.112	255.255.255.252	2
30	PUNTO 030	10.0.10.116	255.255.255.252	2

Tabla 4.4 – Distribución de Redes Loopback

controlado; no se encontraría problemas en elegir una Red IP WAN que no sea la misma de las IP's LAN asignadas a los bancos, pero siempre partiendo sobre una política de planeamiento, la Red IP WAN elegida debe tener la capacidad de entregar subredes con capacidad mínima de 14 IP's para manejar esa cantidad de conexiones a nodos Principales y redundantes". En base a esta política se consideró manejar redes de mascara /28.

4.4 Políticas de enrutamiento utilizadas para la seguridad y control de los paquetes

Como se pueden dar cuenta esta sería una Red IP la cual toda la flexibilidad y funcionalidad se ve comprometida con el enrutamiento de las Redes. Por tal motivo detallamos las características utilizadas en la Red.

4.4.1 Definición del enrutamiento utilizado para la red principal

El enrutamiento es un proceso de *relay* en el que los elementos son reenviados de una ubicación a otra. En las redes informáticas, el tráfico generado por el usuario, como el correo electrónico o los documentos gráficos o de texto, es reenviado de un origen lógico a un destino lógico. Cada dispositivo de la red posee una dirección lógica, de forma que se es posible contactar con él individualmente; en algunos casos, también se puede conectar con los dispositivos como parte de un grupo más grande de dispositivos. Para que un router actúe como dispositivo de *relay* efectivo, debe conocer la topología lógica de la red y ser capaz de comunicarse con sus dispositivos vecinos. Un router puede configurarse para reconocer varios esquemas distintos de direccionamiento lógico e intercambiar regularmente información sobre la topología con otros dispositivos de la red. El mecanismo de aprender y mantener el conocimiento de la topología de red se considera que es la función de enrutamiento. El movimiento real del tráfico por el router, desde una interfaz interna

a una externa, constituye una función separada y se la considera la función de Switching. Un dispositivo de enrutamiento debe llevar a cabo tanto las funciones de enrutamiento como las de Switching para que sea un dispositivo de *relay* efectivo.

Requisitos del enrutamiento

Un *router* debe conocer tres elementos para poder enrutar:

- ✓ El *router* debe determinar si tiene activo el paquete de protocolos.
- ✓ El *router* debe conocer la red de destino.
- ✓ El *router* debe saber qué interfaz externa constituye la mejor ruta para el destino.

Para que un dispositivo de enrutamiento tome la mejor decisión de enrutamiento, primero debe entender la dirección de destino lógica. Para que esto ocurra, el paquete de protocolos que utiliza el esquema de direccionamiento lógico debe estar habilitado y activado en el *router* en ese momento. Algunos ejemplos de paquetes de protocolos comunes son el *Transmission Control Protocol / Internet Protocol*, Protocolo para el control de la transmisión / Protocolo Internet (TCP /IP), el *Internetwork Packet Exchange*, Intercambio de paquetes entre redes (IPX) y DECnet, de *Digital Equipment Corporation*.

Una vez que el *router* entiende el esquema de direccionamiento, la segunda decisión consiste en determinar si la red de destino lógica es un destino válido en la tabla de enrutamiento actual. Si la red lógica de destino no existe en la tabla de enrutamiento, los dispositivos de enrutamiento podrían estar programados para descartar el paquete y generar un mensaje de error (por ejemplo, un mensaje IP *Internet Control Message Protocol*, Protocolo ICMP), para notificar el hecho al remitente del evento. Algunos administradores de redes han logrado reducir el tamaño de las tablas de enrutamiento de sus redes incluyendo únicamente unas

cuantas redes de destino y especificando luego una entrada de ruta predeterminada. Si se especifica, se seguirá una ruta predeterminada si la red de destino lógica no se incluye como parte de la tabla de enrutamiento del dispositivo.

La decisión final que debe tomar el dispositivo de enrutamiento si la red de destino está en la tabla de enrutamiento, consiste en determinar a través de qué interfaz externa va a ser reenviado el paquete. La tabla de enrutamiento sólo contendrá la mejor ruta (o rutas) a cualquier red lógica de destino. La mejor ruta a la red de destino estará asociada con una determinada interfaz externa por el proceso del protocolo de enrutamiento. Los protocolos de enrutamiento utilizan una métrica para determinar la mejor ruta a un destino. Una métrica más baja indica una ruta más adecuada; si dos o más rutas tienen una métrica igual de baja, todas esas rutas serán compartidas. A la opción de compartir tráfico de paquetes por múltiples rutas se denomina equilibrado de la carga al destino. Cuando se conoce la interfaz externa, el router también deberá poder usar un método de encapsulación (en otras palabras, un tipo de trama Capa 2) al reenviar el paquete al dispositivo lógico de próximo salto de la ruta *relay*.

Información sobre enrutamiento

La información necesaria para llevar a cabo la operación de enrutamiento se incluye en la tabla de enrutamiento del router, y es generada por uno o más procesos del protocolo de enrutamiento. La tabla de enrutamiento se compone de múltiples entradas, y cada una de ellas indica lo siguiente:

- ✓ El mecanismo en virtud del cual se conoció la ruta. Los métodos de aprendizaje pueden ser dinámicos o manuales.

- ✓ El destino lógico, bien una red principal o una subred de una red principal. En casos aislados, puede haber direcciones de host en la tabla de enrutamiento.
- ✓ La distancia administrativa, que es una medida de la fiabilidad que supone el mecanismo de aprendizaje. La distancia administrativa se discute en la próxima sección, "*Distancia administrativa*".
- ✓ La métrica, que es una medida del "*coste añadido*" de la ruta, en virtud de lo que define el protocolo de enrutamiento. La métrica de enrutamiento se trata más adelante en la sección "*Métrica del enrutamiento*".
- ✓ La dirección del dispositivo de *relay* de próximo salto (*router*) en la ruta hacia el destino.
- ✓ Lo actualizada que está la información sobre la ruta. Este campo indica el tiempo que ha estado la información en la tabla de enrutamiento desde la última actualización. Dependiendo del protocolo de enrutamiento que se esté utilizando, la información de introducción de ruta puede ser actualizada de forma periódica para garantizar que está actualizada.
- ✓ La interfaz encargada de alcanzar la red de destino. Es el puerto a través del cual el paquete abandona al router y se reenvía al siguiente dispositivo de *relay* de próximo salto.

Ejemplo de una tabla de enrutamiento IP sobre un router.

```
rCISCO# sh ip route  
  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

<pre> i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default U - per-user static route, o - ODR Gateway of last resort is 10.8.4.34 to network 0.0.0.0 I 172.16.0.0/16 [100/118654] vía 172.16.7.9, 00:00:23, Ethernet0/1 C 10.8.4.32/29 is directly connected, Ethernet0/0 </pre>

Tabla 4.5

Distancia administrativa

El proceso de enrutamiento es el responsable de seleccionar la mejor ruta a cualquier red de destino. Dado que puede haber más de un mecanismo de aprendizaje en un *router* en un momento dado, es necesario que haya un método para elegir entre distintas rutas cuando se conoce la misma ruta desde múltiples orígenes. En el caso de IP en un *router CISCO*, el concepto de distancia administrativa se utiliza como método de selección para los protocolos de enrutamiento IP.

La distancia administrativa se utiliza como medida de la fiabilidad del origen de la información de enrutamiento IP. Sólo es importante cuando un *router* conoce una ruta a un destino desde más de un origen.

Es mejor que haya valores bajos en la distancia administrativa que valores altos. Por regla general, las distancias administrativas predeterminadas han sido asignadas con una preferencia por las entradas manuales sobre las entradas conocidas dinámicamente, y los protocolos de enrutamiento con una métrica más sofisticada sobre los que tienen una métrica más sencilla. En la Tabla 3.2 se presenta un esquema comparativo de las distancias administrativas predeterminadas.

Componente de entrada en la tabla de enrutamiento	Descripción
I	<p>Cómo se conoció la ruta (en este caso, por el <i>Interior Gateway Routing Protocol</i>, Protocolo IGRP.</p> <p>Los otros códigos posibles para este componente se muestran en la leyenda "Codes" del Ejemplo.</p>
172.16.0.0/16	Red/subred lógica de destino
[100	Distancia administrativa (factor de fiabilidad) de IGRP.
/118654]	Valor métrico (alcance); por defecto para IGRP, es una combinación del ancho de banda y del retraso.
via 172.16.7.9	Dirección lógica de próximo salto (el próximo router).
00:00:23	Momento de la entrada (en horas:minutos:segundos) desde la última actualización.
Ethernet 0/0	Interfaz a través de la cual se conoció la ruta y a través de la que se irán los paquetes buscando el destino.

Tabla 4.6- Interpretación de los componentes de la tabla de enrutamiento del Ejemplo anterior.

Origen de la ruta	Distancia administrativa predeterminada
Interfaz conectada	0
Ruta estática fuera de una interfaz	0
Ruta estática de un próximo salto	1
Ruta de resumen EIGRP	5
BGP externa	20
EIGRP interna	90
IGRP	100
OSPF	110
IS-IS	115
RIP (v1 y v2)	120
EGP	140
EIGRPexterna	170
BGP interna	200
Desconocido	255

Tabla 4.7. Distancias administrativas predeterminadas de orígenes de rutas.

Métrica de enrutamiento

En una red enrutada, el proceso de enrutamiento se apoya en el protocolo de enrutamiento para mantener una topología libre de bucles y para localizar la mejor ruta a cada red de destino.

La definición de cuál es la mejor ruta a cualquier destino es una característica que diferencia a los distintos protocolos de enrutamiento. Cada protocolo de

enrutamiento utiliza una medida diferente. Los *routers* publican la ruta a una red en términos de valor métrico.

Algunos ejemplos habituales de métricas son la cuenta de salto (el número de *routers* que hay que atravesar), el coste (en base al ancho de banda), y un valor compuesto (utilizando varios parámetros en el cálculo). Si la red de destino no es local a un *router*, la ruta se representará por la suma de los valores métricos que definen en todos los enlaces que deben ser atravesados desde el *router* para alcanzar esa red.

Cuando el proceso de enrutamiento conoce los valores métricos asociados con las distintas rutas (presuponiendo que existen múltiples rutas), entonces se puede tomar la decisión de enrutamiento. El proceso de enrutamiento selecciona la ruta que tenga el valor métrico más bajo. En *routers* CISCO, si hay múltiples rutas bajo métricas iguales en un entorno IP, existirá la opción de compartir la carga (también conocido como equilibrado de la carga) entre las distintas rutas. Para IP, CISCO soporta por defecto cuatro rutas con métricas iguales a una red de destino común. Es posible configurar un máximo de seis rutas con métricas iguales en el CISCO IOS utilizando el comando de configuración de *router maximum-paths*.

Las dos secciones siguientes revisan las métricas de enrutamiento de *Routing Information Protocol*, Protocolo de la información de enrutamiento (RIP) y de IGRP.

Métrica del enrutamiento IGRP

El protocolo IGRP de CISCO es un protocolo de enrutamiento muy utilizado en redes TCP/IP medianas y grandes. IGRP utiliza una métrica compuesta, basada en el ancho de banda, retraso, fiabilidad, carga y unidad de transmisión máxima (MTU). En el cálculo de algoritmos estándar IGRP, sólo están activados por defecto el ancho

de banda y los valores de retraso (remítase a la barra lateral "Cálculo de la métrica IGRP", más adelante en esta sección, para obtener una descripción del cálculo de la métrica IGRP).

La métrica compuesta IGRP puede distinguir diferencias sutiles en las características de los enlaces, por lo que selecciona la ruta a la red de destino con ancho de banda más alto (más rápido). En la Figura siguiente, el router A sólo selecciona una ruta a la red 192.168.10.0; se trata de la ruta *Fiber Distributed Data Interface*, Interfaz de datos distribuida por fibra (FDI), ya que el ancho de banda de 100 Megabits por segundo (Mbps) es más alto que el de las otras rutas disponibles. Si hay una ruta de métrica equivalente (al menos, en un uno por ciento), estará activado el equilibrado de la carga.

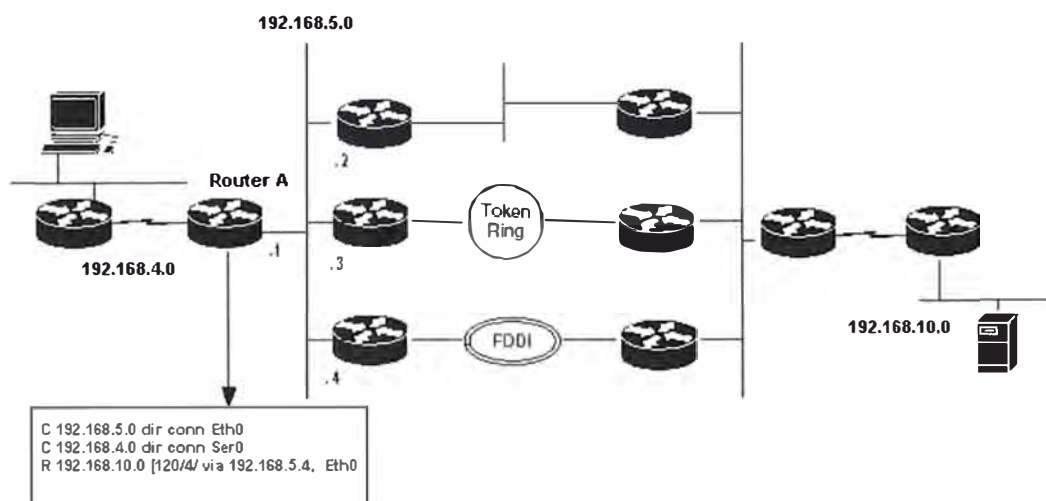


Figura 4.4 – Cálculo de la métrica para el enrutamiento de una subred.

IGRP también es capaz de hacer un equilibrado de la carga por rutas de coste desigual, dentro de una varianza especificada.

Cálculo de la métrica IGRP

IGRP calcula la métrica sumando valores de diferentes características del enlace a una red de destino. la fórmula Que se emplea es la siguiente:

$$Metric_1 = (K1 \times bandwidth) + (K2 \times bandwidth) / (256 - Load) + (K3 \times delay)$$

Si K5 no es igual a 0, se hace un cálculo adicional:

$$Metric_2 = Metric_1 \times (K5 / [reliability + K4])$$

los valores K de estas fórmulas son constantes que se pueden definir utilizando el comando de configuración *metric weights*. Los valores de constante predeterminados por defecto son K1 = K3 = 1 y K2 = K4 = K5 = 0, por lo que, la fórmula es:

$$Métrica = Ancho de Banda + Retraso.$$

Para determinar el ancho de banda que se usa en este cálculo, busque el más pequeño de los anchos de banda desde las interfaces salientes a lo largo de la ruta hasta el destino, en kilobits por segundo (Kbps), y divida 10'000,000 entre ese número. Observe que el ancho de banda que se da en el comando *show interfaces* de CISCO IOS está en kilobits por segundo.

Para determinar el retraso que se usa en este cálculo. sume todos los retrasos desde las interfaces salientes a lo largo de la ruta hasta el destino, en microsegundos, y divida este número entre 10.

Observe que el retraso que se da en el comando *show interfaces* de CISCO IOS está en microsegundos.

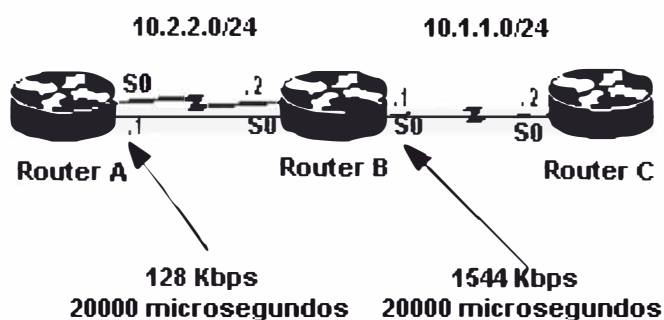


Figura 4.5 - La Figura presenta una red de ejemplo que ilustra el cálculo de la métrica IGRP.

En la Figura el *router* B publica la red 10.1.1.0 al *router* A. la métrica que el *router* B publica para 10.1.1.0 se calcula así:

$$\text{Ancho de banda} = 10000000 / 1544 = 6476$$

$$\text{Retraso} = 20000 / 10 = 2000$$

$$\text{Métrica} = \text{Ancho de Banda} + \text{Retraso} = 8476$$

El *router* A calcula la métrica que coloca en su tabla de enrutamiento para 10.1.1.0 de esta forma:

$$\text{Ancho de banda} = 10000000 / 128 = 78125$$

Utilizando el ancho de banda mínimo de la ruta, que, en este caso, es de 128 Kbps.

$$\text{Retraso} = (20000 + 20000) / 10 = 4000$$

$$\text{Métrica} = \text{Ancho de Banda} + \text{Retraso} = 82125$$

Protocolos de enrutamiento

Existen muchas formas de clasificar los protocolos de enrutamiento. Las secciones siguientes tratan dos de estas categorías (los que tienen clases frente a los que no las tienen, y el vector de distancia frente al estado de enlace). Se define cada

uno de estos términos, y se facilitan ejemplos. Observe que algunos protocolos de enrutamiento poseen características que traspasan los límites de las categorías.

Funcionamiento del vector de distancia

Las actualizaciones periódicas y rutinarias del enrutamiento que generan la mayoría de protocolos de enrutamiento por vector de distancia solo se dirigen a los dispositivos de enrutamiento que estén conectados directamente. El directorio que suelen usar los dispositivos que envían las actualizaciones es una difusión lógica, aunque, en algunos casos, se pueden especificar actualizaciones unidifusión.

En un entorno de vector de distancia puro, la actualización del enrutamiento incluye una tabla de enrutamiento completa, como se ve en la figura siguiente. Cuando un router recibe una tabla completa de un vecino, puede verificar todas las rutas conocidas y luego realizar cambios en la tabla local en base a la información actualizada recibida este proceso es fácil de entender. La comprensión por parte de un router de la red se basa en la perspectiva que tiene el vecino sobre la topología de red por tanto, el planteamiento del vector de distancia suele denominarse “enrutamiento por rumor”.

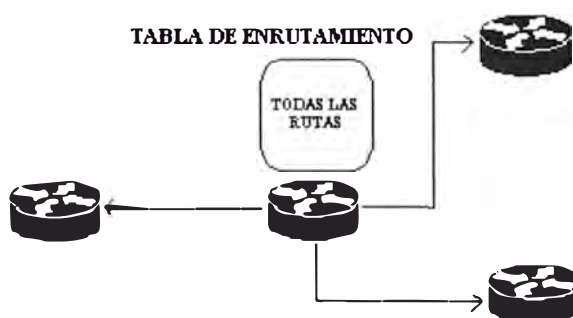


Figura 4.6 – Envío de las tablas de enrutamiento a los equipos vecinos del mismo Sistema Autónomo.

Los Protocolos de enrutamiento por vector de distancia puros envían toda su tabla de enrutamiento. CISCO IOS soporta varios protocolos de vector de distancia, entre los que se incluyen RIPv1, RIPv2 e IGRP. Los routers CISCO también soportan EIGRP, un protocolo avanzado de vector de distancia.

Tradicionalmente, los protocolos de vector de distancia también eran protocolos con clase. RIPv2 y EIGRP constituyen ejemplos de protocolos de vector de distancia más avanzados que exhiben un comportamiento sin clase.

EIGRP también exhibe algunas características de estado. Los protocolos de enrutamiento suelen estar asociados con la capa de red de un conjunto de protocolos.

Sin embargo los protocolos de enrutamiento utilizan el mecanismo de envío de capa de red para intercambiar información de enrutamiento, pero el proceso de protocolo de enrutamiento, en sí mismo, no existen en la capa de red.

La figura a continuación muestra la ubicación de los protocolos de enrutamiento por vector de distancia IP que hay en el modelo de referencia OSI.

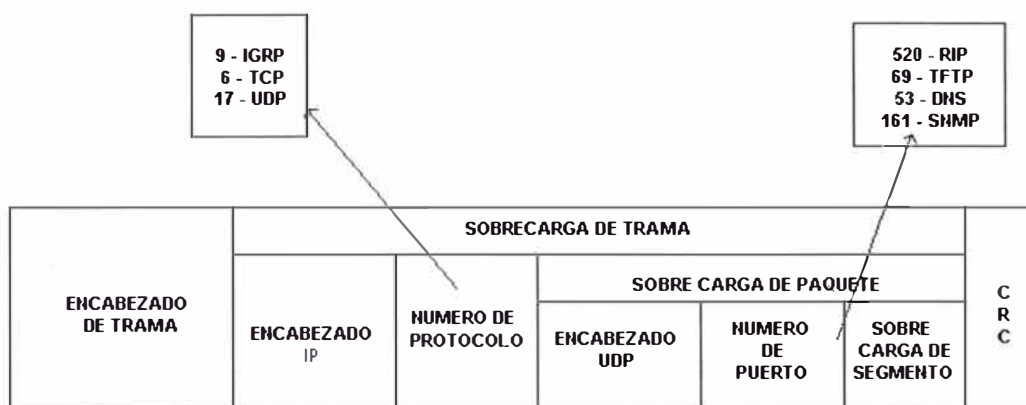


Figura 4.7 - Ubicación de los protocolos de enrutamiento por vector de distancia IP.

Como se ve en la figura anterior reside en la capa de transporte, como protocolo

Otros números de protocolo reconocibles son el 6 y el 17, respectivamente, para TCP y *User Datagram Protocol* (UDP), Protocolo de datagrama de usuario. RIP reside en la capa de aplicación y posee un número de puerto UDP de 520.

Otros números de puerto UDP conocidos son el puerto 53 para el *Domain Name Server*, Servidor de denominación de dominio (DNS), el puerto 69 para el *Trivial File Transfer Protocol*, Protocolo TFTP, y el puerto 161 para el *Simple Network Management Protocol*, Protocolo simple de administración de redes (SNMP).

La tabla mostrada a continuación compara las características de los distintos protocolos de enrutamiento por vector de distancia soportados en los routers CISCO.

Características	RIPv1	RIPv2	IGRP	EIGRP
Cuenta a infinito	X	X	X	
Horizonte dividido	X	X	X	X
Temporizador de espera	X	X	X	
Actualizaciones con ruta poisoning	X	X	X	X
Equilibrado de la carga – rutas iguales	X	X	X	X
Equilibrado de la carga – rutas desiguales		X	X	
Soporte VLSM		X		X
Algoritmo de enrutamiento	BELL	BELL	BELL	DUAL
Métrica	Saltos	Saltos	Comp.	Comp.
Límite de la cuenta de salto	15	15	100	100
Escalabilidad	Pequeña	Pequeña	Mediana	Grande

Tabla 4.8 - Tabla de características de acuerdo al protocolo de enrutamiento.

La mayoría de protocolos de enrutamiento por vector de distancia utilizan el algoritmo de Bellman-Ford para el cálculo de ruta, EIGRP es un protocolo avanzado de vector de distancia y utiliza Diffusing Update Algorithm (DUAL).

Funcionamiento del estado de enlace

Los protocolos de enrutamiento por estado de enlace solo generan actualizaciones cuando hay un cambio en la topología. Cuando un enlace cambia de estado, el dispositivo que detecta el cambio creará una publicación del estado de enlace (*Link State Advertisement LSA*) que concierna a ese enlace (ruta); luego, la LSA se propaga a todos los dispositivos vecinos que utilicen una dirección de multidifusión especial. Cada dispositivo de enrutamiento toma una copia de la LSA, la reenvía a todos los dispositivos vecinos (este proceso se denomina *flooding, o técnica de inundación*), y luego actualiza la base de datos de topología (una tabla que contiene toda la información sobre el estado de enlace de la red). Esta inundación de la LSA es necesaria para garantizar que todos los dispositivos de enrutamiento conozcan el cambio con el fin de poder así actualizar sus bases de datos y crear una tabla de enrutamiento que refleje la nueva topología.

La mayoría de los protocolos de estado de enlace requieren un diseño jerárquico. El planteamiento jerárquico, como la creación de múltiples áreas lógicas en OSPF, reduce la necesidad de inundar una LSA en todos los dispositivos del dominio de enrutamiento, ya que el uso de las áreas restringe la inundación al límite lógico del área en vez de a todos los dispositivos de dominio OSPF. En otras palabras, un cambio en área debe ocasionar el recalcular de la tabla de enrutamiento para solo esa área, no para todo el dominio.

CARACTERÍSTICA	OSPF	IS-IS	EIGRP
Topología jerárquica - necesaria	X	X	
Retiene el conocimiento de todas las rutas posibles	X	X	X
Resumen de ruta – manual	X	X	X
Resumen de ruta – automática			X
Publicaciones de activación de eventos	X	X	X
Equilibrado de la carga – rutas iguales	X	X	X
Equilibrado de la carga – rutas desiguales			X
Soporte VLSM	X	X	X
Algoritmo de enrutamiento	Dijkstra	IS-IS	DUAL
Métrica	Coste	Coste	Compuesta
Limite de la cuenta de salto	Ilimitada	1024	100
Escalabilidad	Grande	Muy Grande	Grande

Tabla 4.9 – Comparación de las características que presentan los protocolos de enrutamiento por estado de enlace.

Observe que EIGRP es técnicamente un protocolo avanzado de vector de distancia pero presenta algunas características de estado de enlace. Además, IS-IS aparece por motivos de comparación y no se utiliza mucho.

IS-IS es el algoritmo de enrutamiento que utiliza el conjunto de protocolos de la International Organization for Standardization, Organización internacional de normalización (ISO), que incluye el Connectionless Network Service, Servicio de red no orientado a conexión (CLNS).

Convergencia eigrp

A continuación presentamos algunos de los términos que se usan en esta sección, lo cual ayudará a entender como converge EIGRP.

- ✓ **Tabla de topología.** EIGRP mantiene una copia de las tablas de enrutamiento de sus vecinos en su tabla de topología.

- ✓ **Sucesor.** Es la mejor ruta a un destino , seleccionada a partir de la tabla de topología y colocada en la tabla de topología.
- ✓ **Sucesor factible.** Es otra ruta a un destino (no la mejor ruta, pero una que se podría usar si la mejor ruta no se encuentra disponible). Se mantiene en la tabla de topología.
- ✓ **Distancia publicada.** Es la métrica EIGRP publicada por un vecino para un destino.
- ✓ **Distancia factible.** Es la métrica EIGRP para una red de destino.

Un router que ejecuta EIGRP utiliza mensajes de multidifusión fiables cuando envía consulta y actualizaciones a otros routers.

La secuencia de eventos para la convergencia EIGRP cuando el router C de la figura a continuación detecta el fallo en la red 1.1.0.0 es como sigue en la figura siguiente.

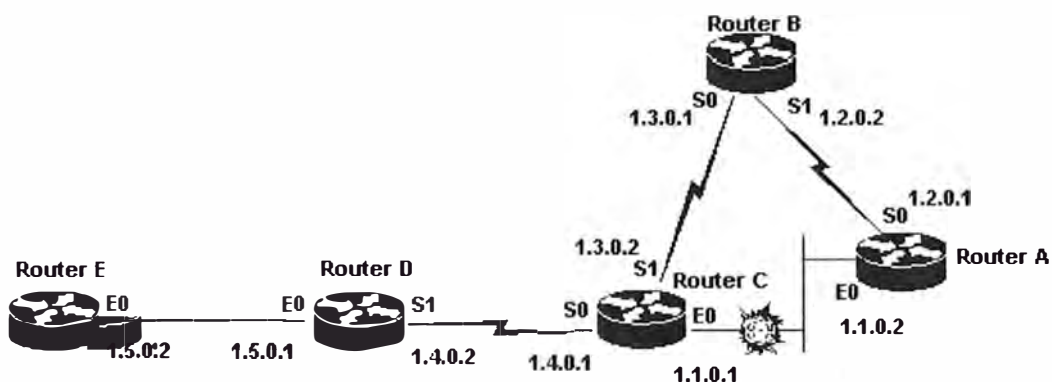


Figura 4.8 – Detección de falla y convergencia EIGRP.

- a) El router C detecta el fallo de enlace en la Ethernet entre los routers A y C, comprueba la tabla de topología para buscar un sucesor factible, no encuentra una ruta alternativa calificada e introduce el estado de activo (indicando que debe de buscar activamente una nueva ruta).

- b) El router C envía una consulta a todas las interfaces buscando nuevas alternativas al enlace fallido (la dirección de multidifusión EIGRP 224.0.0.10 se usa para las consultas). Los routers vecinos reconocen la consulta.
- c) La respuesta del router D indica que no hay otra ruta a la red 1.1.0.0.
- d) La respuesta del router B contiene una ruta al enlace fallido, aunque tiene una distancia factible más alta.
- e) El router C acepta la nueva ruta y la información de la métrica, las coloca en la tabla de topología y crea una nueva entrada en su tabla de enrutamiento.
- f) El router C envía una actualización sobre la nueva ruta a todas las interfaces. Todos los vecinos confirman la actualización y envían actualizaciones propias (que se confirman) al remitente. Estas actualizaciones bidireccionales son necesarias para asegurarse de que las tablas de enrutamiento se sincronizan y para validar el reconocimiento de la nueva topología por parte del vecino.

Desde el punto de vista del router E, el tiempo de convergencia es el total del tiempo de detección, más los tiempos de consulta y respuesta, más los tiempos de actualización. El tiempo real para que el router E converja es muy rápido, aproximadamente de 2 segundos.

4.5 Descripción de las configuraciones en los equipos

A continuación describiremos las configuraciones realizadas tanto en los equipos de Nodo como en cada una de los equipos CPE de cada banco o sede remota. Dichas configuraciones será distribuida de acuerdo a la función que desarrollaban, las cuales han sido distribuidas de la siguiente manera:

- ✓ Configuraciones de las Sub-Interfaces ATM,
- ✓ Configuraciones del Enrutamiento de las Redes permitidas,

- ✓ Configuraciones de la VoIP en cada Sede Remota,
- ✓ Configuraciones del NAT Dinámico / Estático para los Host Permitidos,
- ✓ Configuraciones de Redundancia (ISDN).

4.5.1 Configuraciones de las sub-interfaces ATM

En esta parte mostraremos los comandos de línea utilizados en los routers para poder recibir las sub-interfaces ATM las cuales sirvieron para recepcionar las conexiones PVC desde los equipos 2820 hasta el router 7206. Estas interfaces se configuraron en cada uno de los router 7206 del Nodo Principal. A continuación mostramos un ejemplo de configuración de las sub-interfaces.

ROUTER ATM (PRINCIPAL ó SECUNDARIO)

```
i
bridge irb
!
interface ATM6/0
description Conexion de Tarjeta OC-3 ATM
no ip address
no ip directed-broadcast
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
description PVC de conexión a Sede Remota
atm pvc 101 0 101 aal5snap 13208 13208
bridge-group 1
```

```

interface BV11

description Interface virtual VBI

mac-address 1000.2000.1001

mtu 1500

ip address 10.13.4.249 255.255.255.248

no ip directed-broadcast

ntp broadcast client

!

bridge 1 protocol ieee

bridge 1 route ip

```

De estos comandos verificamos la generación de las Sub-interfaces ATM como también de las interfaces BVI para colocar el número IP. Con esta configuración se logra obtener las conexiones que se muestran a continuación en el gráfico, donde las conexiones son en una misma Red de máscara 29.

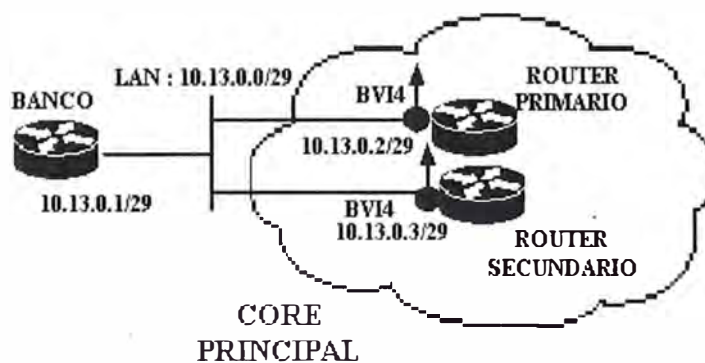


Figura 4.9 – Interfaces BVI de interconexión con los equipos en Ethernet.

Durante la configuración se puede especificar que clase de protocolo se puede rutear. Se puede colocar IP como es el caso o IPX de acuerdo al protocolo que se esta manejando.

ITM	SEDE	VPI	VCI	VC	DIALER	ANEXO
1	PUNTO 001	0	101	101	1	2100
2	PUNTO 002	0	102	102	2	2200
3	PUNTO 003	0	103	103	3	2300
4	PUNTO 004	0	104	104	4	2400
5	PUNTO 005	0	105	105	5	2500
6	PUNTO 006	0	106	106	6	2600
7	PUNTO 007	0	107	107	7	2700
8	PUNTO 008	0	108	108	8	2800
9	PUNTO 009	0	109	109	9	2900
10	PUNTO 010	0	110	110	10	3000
11	PUNTO 011	0	111	111	11	3100
12	PUNTO 012	0	112	112	12	3200
13	PUNTO 013	0	113	113	13	3300
14	PUNTO 014	0	114	114	14	3400
15	PUNTO 015	0	115	115	15	3500
16	PUNTO 016	0	116	116	16	3600
17	PUNTO 017	0	117	117	17	3700
18	PUNTO 018	0	118	118	18	3800
19	PUNTO 019	0	119	119	19	3900
20	PUNTO 020	0	120	120	20	4000
21	PUNTO 021	0	121	121	21	4100
22	PUNTO 022	0	122	122	22	4200
23	PUNTO 023	0	123	123	23	4300
24	PUNTO 024	0	124	124	24	4400
25	PUNTO 025	0	125	125	25	4500
26	PUNTO 026	0	126	126	26	4600
27	PUNTO 027	0	127	127	27	4700
28	PUNTO 028	0	128	128	28	4800
29	PUNTO 029	0	129	129	29	4900
30	PUNTO 030	0	130	130	30	5000

Tabla 4.10 - Distribución de VCI VPI para la asignación de VCs.

4.5.2 Configuraciones del enrutamiento de las redes permitidas

A continuación mostramos los comandos necesarios para realizar el enrutamiento entre los equipos del Nodo Principal. En la cual se debe asignar un AS (Autónomo System) para caso del ejemplo se ha escogido el 523. Luego publicamos las redes de la WAN que los une a los puntos remotos y la Red LAN que

interconecta ambos equipos. Luego debemos de redistribuir las redes aprendidas por rutas estáticas para colocar dentro de la tabla de EIGRP y que esta pueda ser propagada.

Luego se debe de elegir la lista de las redes que se desea proagar (Es decir, nos e va ha propagar todas las redes por seguridad y adicionalmente se debe configurar las Redes que se van a permitir recibir por medio del EIGRP de acuerdo a la interface deseada. Todo esto se puede observar en las líneas siguientes de los comandos de línea.

ROUTER ATM (PRINCIPAL ó SECUNDARIO):

```
!  
router eigrp 523  
  redistribute static metric 100000 10 255 10 1500  
  network 10.0.0.0  
  network 172.25.0.0  
  distribute-list 11 out BVI2  
  distribute-list 52 in BVI2  
  no auto-summary  
  eigrp log-neighbor-changes  
ip route 0.0.0.0 0.0.0.0 Null0  
access-list 11 permit 0.0.0.0  
access-list 52 permit 10.8.7.8 0.0.0.3  
access-list 52 permit 172.25.2.0 0.0.0.255
```


ROUTER REMOTO:

!

router eigrp 523

redistribute static metric 100000 10 255 10 1500

passive-interface Ethernet0/1

network 10.0.0.0

network 172.25.0.0

no auto-summary

eigrp log-neighbor-changes

ip route 172.25.20.0 255.255.255.0 Loopback0

De la misma manera en el punto remoto se debe de colocar el mismo AS (Autónimo System) que el punto central para que reciba la tabla que ha sido condidera para enviar hasta que converja las redes. Y como la parte principal es la de redistribuir las rutas estaticas en donde se publicará la Red LAN asignada a esta sede remota como una “LAN Aparente”.

4.5.3 Configuraciones de la VoIP en cada sede remota

Esta configuración únicamente se realiza en los CPEs remotos ya que la VoIP sería entre sedes. Lo que pasaría en los Nodos únicamente sería IP. A continuación se muestra las configuraciones de la parte de VoIP de las Sedes remotas para lograr una interconexión de acuerdo al tipo de interface de conexión a su PBX o anexo directo. Muy aparte de la interface física se debe de realizar la siguiente conexiones.

En esta configuración se podrá observar que se debe de configurar el tipo de puerto como también el número de “POT” asignado. Luego se debe de generar todos los “dial-peer” que sean necesarios para apuntar a todas las sedes existentes. Cada uno de estas conexiones apunta al router ó CPE terminal a donde debe de llegar la conexión TCP/IP de VoIP. Entonces podemos afirmar que esta debe de ser similar en cada uno de los CPE excepto que no contendrá el “Dial-peer” del mismo router.

ROUTER REMOTO:

```
!  
voice-port 1/0/0  
  echo-cancel coverage 24  
!  
dial-peer voice 1 pots  
  destination-pattern 21  
  port 1/0/0  
!  
dial-peer voice 13 voip  
  destination-pattern 25  
  session target ipv4:10.8.7.21  
  ip precedence 5  
  no vad
```

Para un mejor entendimiento se debe de generar un Plan de numeración de anexos de 4 cifras de las cuales las 2 primeras darán la dirección y las últimas

permitirá dar mayor flexibilidad en el crecimiento de las interfaces de conexión.

Esta distribución se puede observar en la tabla 1.

4.5.4 Configuraciones del nat dinámico / estático para los host permitidos

Como se solucionó el problema de los traslapes de Redes mediante la asignación de Redes “LAN Aparentes”; era necesario realizar traslaciones de los números IP de los Host con números IP que los llamaremos “IP Permitidos”; los cuales pueden atravesar el Backbone IP sin ningún problema de ir a la interface NULL. De esta manera era importante la implementación de NAT dinámico y Estático de acuerdo a la necesidad de las conexiones en los Host. A continuación mostramos la configuración estándar para los equipos CPE remotos.

ROUTER REMOTO:

```
interface Ethernet0/0
```

```
ip nat outside
```

```
!
```

```
interface Ethernet0/1
```

```
ip nat inside
```

```
!
```

CONFIGURACION ESTATICA

```
ip nat translation timeout 90
```

```
ip nat inside source static 172.16.1.100 172.25.11.80
```

```
!
```

CONFIGURACION DINAMICA

```
ip nat pool pcerticom 172.25.11.24 172.25.11.24 prefix-length 24
```

```
ip nat inside source route-map serv02 pool pcerticom overload

ip access-list extended certicom

  permit ip host 172.16.1.200 host 172.25.34.5

  permit ip host 172.16.1.200 host 172.25.34.10

  permit ip host 172.16.1.100 host 172.25.34.5

  permit ip host 172.16.1.100 host 172.25.34.10
```

Para este ejemplo podemos observar una Sede con ambos casos ya que puede tener conexiones con Host que necesitan levantar circuitos TCP/IP en ambas direcciones (Para ese caso se necesita una traslación Estática) o en una dirección (Para este caso se necesita un conexión dinámica).

4.5.5 Configuraciones de redundancia (isdn)

De acuerdo a la distribución lógica mostrada en secciones anteriores debemos de ver que se necesita configuración únicamente en el router secundario y en todos los CPE remotos para servir de redundancia en caso de perdida de última milla en la conexión al proveedor del transporte de datos.

A continuación mostramos los comandos para realizar las configuraciones de las interfaces para redundancia con ISDN.

ROUTER ATM (SECUNDARIO):

```
!  
username rRemoto password 7 072B38212B213036  
isdn switch-type primary-net5
```

```
controller E1 4/0

framing NO-CRC4

pri-group timeslots 1-31

!

interface Dialer11

ip address 10.8.6.45 255.255.255.252

encapsulation ppp

dialer remote-name rRemoto

dialer pool 1

dialer-group 1

ppp authentication chap

!

map-class dialer bancared

dialer idle-timeout 60

dialer fast-idle 5

dialer wait-for-carrier-time 3

ROUTER REMOTO:

!

username Rbackup password 7 040417081E013E

isdn switch-type basic-net3

call rsvp-sync

!

interface BRI0/0
```

```
encapsulation ppp

dialer pool-member 1 priority 200 max-link 1

dialer pool-member 2 priority 200 max-link 1

isdn switch-type basic-net3

ppp authentication chap

!

interface Dialer1

bandwidth 64

ip address 10.8.6.46 255.255.255.252

ip nat outside

encapsulation ppp

dialer pool 1

dialer remote-name Rsecundario

dialer string 6105555 class bancos

dialer-group 1

ppp authentication chap

!

!

map-class dialer bancos

dialer idle-timeout 60

dialer fast-idle 5

dialer wait-for-carrier-time 1
```

Se observa la generación de interfaces Dialer para permitir mayor flexibilidad en la cantidad de conexiones dando la opción de colocar una nueva Red paralela y compartir el mismo CPE remoto. Esto se concretaría años después luego de verificar la robustez del diseño.

4.6 Descripción de las configuraciones en los equipos

La parte más importante del diseño se centra en la capacidad de redundancia que pueda tener para mantener el SLA contratado. Este SLA será visto y desarrollado en el capítulo siguiente. Para desarrollar la parte de la redundancia lo dividiremos en 3 casos los cuales encierran las posibles caídas de enlaces que pueda sufrir la Red de Interconexión Bancaria. Estas situaciones serían las siguientes:

- ✓ Pérdida de conexión con el Equipo Principal
- ✓ Pérdida de conexión con el Equipo Secundario
- ✓ Pérdida de conexión con la Última Milla

A continuación desarrollaremos cada uno de estos casos. Los cuales muestran la dirección a tomar de las conexiones TCP/IP como de los paquetes UDP.

4.6.1. Pérdida de conexión con el equipo principal

En este caso se observa la pérdida de conexión con el router principal a causa de desconfiguración, problemas en el PVC, mal funcionamiento del router Principal, problemas en el jumper de conexión de la interface OC-3 del ATM del router 7206. La dirección que tomaría cada una de las conexiones de datos TCP/IP o los paquetes UDP seguirían por la conexión del router 7206 secundario en forma automática sin demora en tiempo ni pérdida de paquetes durante la conmutación de la ruta.

Esta ruta seguida por el paquete o de la conexión se muestra en la gráfica siguiente.

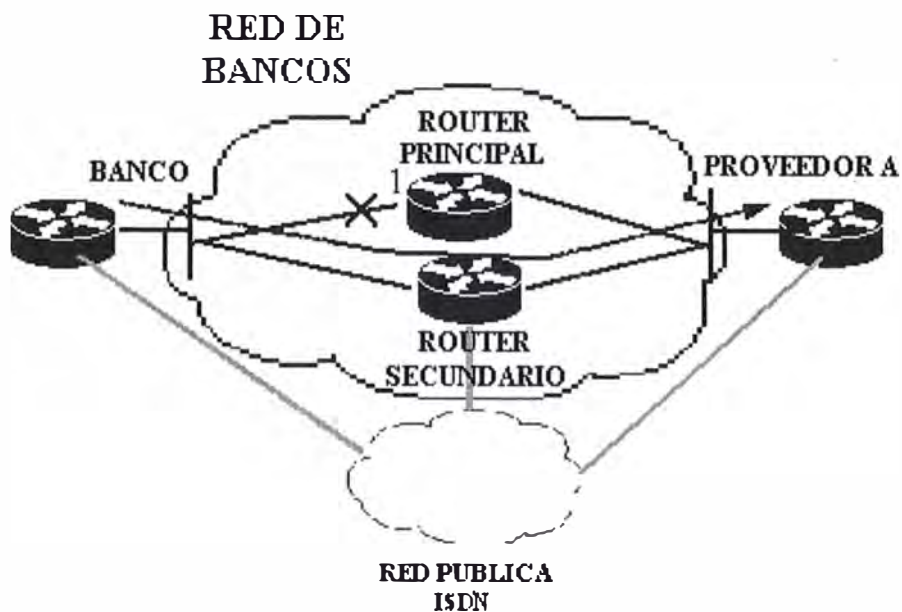


Figura 4.10– Caída de conexión con el router Principal.

4.6. 2. Pérdida de conexión con el equipo secundario

En este caso se observa la pérdida de conexión con el secundario a causa de desconfiguración, problemas en el PVC, mal funcionamiento del router Principal, problemas en el jumper de conexión de la interface OC-3 del ATM del router 7206. Esto no afectaría la dirección que tomaría cada una de las conexiones de datos TCP/IP o los paquetes UDP y seguirían por la conexión del router 7206 primario sin demora en tiempo ni pérdida de paquetes ya que no habría conmutación de la ruta.

Esta ruta seguida por el paquete o de la conexión se muestra en la gráfica siguiente.

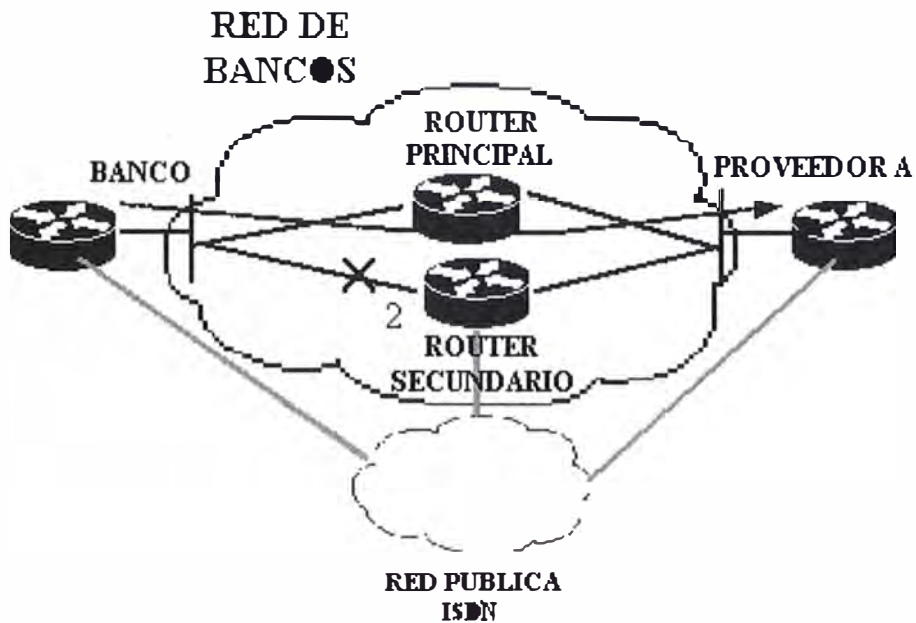


Figura 4.11 – Caída de conexión con el router Secundario.

4.6. 3. Pérdida de conexión con la última milla

En este caso se observa la pérdida de conexión en la última Milla; esto genera pérdida de conexión con el router principal y secundario al mismo momento problemas en la fibra, mal funcionamiento del Catalyst 2820, problemas en el jumper ó en la Fibra Optica. La dirección que tomaría cada una de las conexiones de datos TCP/IP o los paquetes UDP seguiría a través de la conexión ISDN hacia el router 7206 secundario en forma automática con una demora mínima de 5 segundos, Esto genera una pérdida mínima de paquetes durante la conmutación de la ruta.

Esta ruta seguida por el paquete o de la conexión se muestra en le gráfica siguiente.

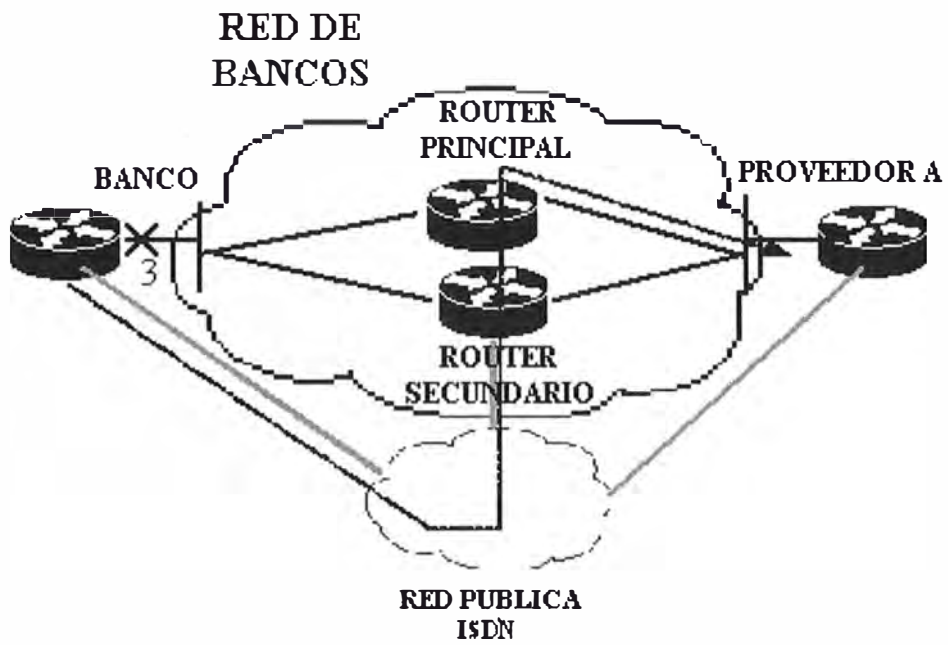


Figura 4.12 – Caída de conexión en la última Milla o conexión al Proveedor de Servicio.

CAPÍTULO V

CONSIDERACIONES FINALES Y EVALUACIÓN ECONÓMICA DEL PROYECTO

5.1 Consideraciones de servicio

Como se pudo verificar en todo el proyecto se necesitaba tener una Alianza directa con el Proveedor del Transporte para que este pudiera entregar un Nivel de Servicio de Aceptación (SLA) elevado ya que la importancia de estos enlaces radica directamente al emplazar a los demás enlaces dedicados antiguos que pudieran tener las Entidades bancarias con sus proveedores de servicio hacia uno solo con velocidad de acceso muy por encima de los manejados actualmente.

5.1.1 Coordinaciones para cambios y crecimientos

Para que este tipo de Red sea manejada en forma apropiada y no tenga complicaciones de coordinación, se deben de tener en cuenta ciertas consideraciones las cuales paso a mencionar:

- ✓ La Red debe de ser Administrada por un Ente (*Administrador de la Red de Bancos*) representante de todos los participantes. Ya que esta Red se encuentra en cada uno de los locales de estos y posee una conexión autorizada debe ser coordinado cualquier tipo de trabajo con una única persona que sirva de nexo a las demás entidades participantes y poder de esa manera mantener un control de accesos y modificaciones. Esta persona se encargaría adicionalmente el informar sobre el crecimiento de la Red como también el ingreso de nuevos proveedores de Información como Bancos Nuevos.

- ✓ La Red debe de poseer un Supervisor Técnico (*Administrador Técnico de la Red de Bancos*) como representante de las Entidades participantes, que tenga como responsabilidad principal el auditar las configuraciones realizadas cada cierto periodo, como también debe de cerciorase que las redundancias siempre estén listas para casos de contingencia. Adicionalmente esta persona se encargaría de mantener y solucionar en línea los problemas y/o nuevos requerimientos de los puntos instalados.
- ✓ La Red únicamente debe ser manipulada y configurada por la Empresa (*SopORTE Técnico de la Red de Bancos*) que entregaría el Outsourcing de transporte , monitoreo y configuración. Este responsable será supervisado en todo momento por la Entidad Supervisora Técnica.

Debido a lo indicado anteriormente se tomó para la implementación de este proyecto la asignación de estas personas y se consideró dentro del contrato para que este totalmente claro en las negociaciones.

5.1.2 Niveles de aceptación de la red

Cuando se comentó sobre el Nivel de Aceptación de la Red (SLA) este es calculado de acuerdo a la cantidad de Minutos disponibles de la Red. Es decir, se tiene un promedio en minutos mensuales que debería de estar activa la Red y en caso de averías el tiempo de falla, corte o degradación de servicio se contabiliza y se lleva a minutos para poder saber que porcentaje de minutos estuvo disponible la red. Este SLA puede ser medido de diferentes maneras, es decir, puede ser medido como métrica mensual o como métrica Anual acumulada. En algunos casos se mide en forma Anual y al siguiente año se llevan los contadores a cero y nuevamente se calcula para el siguiente año.

A continuación colocamos la fórmula del cálculo del SLA para una situación que se considera en el proyecto tratado.

$$SLA_{proyecto} = ((CMAp - CMDp) / CMAp) \times 100\%$$

Donde:

CMAp : Cantidad de Minutos Disponibles durante el periodo de medición.

CMDp : Cantidad de Minutos de Falla durante el periodo de medición.

Para este caso se medía en forma mensual lo que significaba que el *CMAp* es de 43200 minutos de disponibilidad Total al Mes. Por lo tanto, uno debe de indicar en el contrato cual es el grado de disponibilidad que aceptará dicha Empresa de Outsourcing. Para dar tal dato, se debe de tener en cuenta la disponibilidad de las Redes sobre las cuales se monta dicha Red.

Pongamos un ejemplo que se desee un SLA del 99.5% de disponibilidad, esto quiere decir, que únicamente puede tener 216 minutos de falla al mes en toda la Red. Con este valor nos damos cuenta de la importancia que se tiene al pedir estos grados de aceptación, ya que afecta directamente al Precio de venta del Producto final.

Para poder llegar a estos Niveles de Aceptación tan exigentes se toman ciertas medidas técnicas para lograr cumplirlo, por ejemplo una de estas es la de tener el Nodo Principal dentro de un *Collocation* (Ubicar dentro de un Local del Proveedor los equipos Principales) para de esta manera lograr tener mayor seguridad y cumplir con los parámetros necesarios tanto en el ambiente como en la energía eléctrica. De esta manera se puede dar mejor uso eficiente de los equipos Principales.

5.2 Evaluación económica del proyecto

Dentro de la evaluación económica se considera la compra de equipos Cisco 2611 y Cisco 7206 con distintas configuraciones de acuerdo a las conexiones que se

encontraban en cada local y de las configuraciones necesarias en el Nodo Principal y Secundario.

a) Tenemos al Equipo Router Cisco 2611 con la configuración de 2 interfaces Ethernet, 1 interface BRI ISDN S/T y 04 puertos FXS.

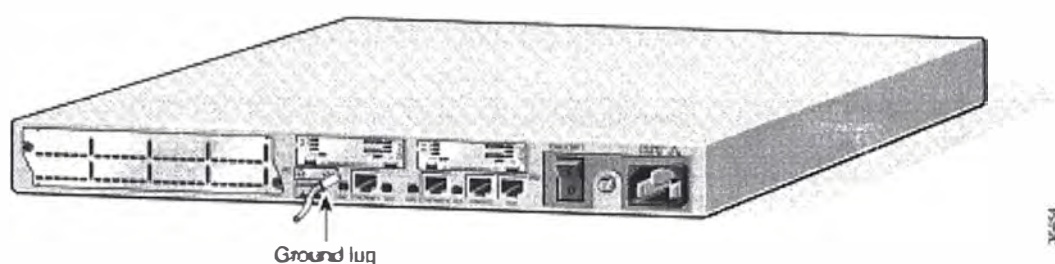


Figura 5.1- Vista posterior del router Multiservicio Cisco 2611

EQUIPO CISCO ROUTER 2611 W/2E/1B-S/T/2FXS

Product	Description	Price (\$)	Discount	Price F.O.B. (\$)	Price Lima (\$)
CISCO2611	Dual Ethernet Modular Router w/ Cisco IOS IP Software	2,495.00	49%	1,272.45	1,463.32
CAB-AC	Power Cord, 110V	0.00	49%	0.00	0.00
S26AP-12103T	ENTERPRISE PI.US	1,300.00	49%	663.00	762.45
MEM2600-32U48D	32 to 48MB DRAM Factory Upgrade for the Cisco 2600	1,000.00	49%	510.00	586.50
MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600	700.00	49%	357.00	410.55
NM-2V	Two-Slot Voice/fax Network Module	1,700.00	49%	867.00	997.05
VIC-2FXS	Two-port Voice Interface Card – FXS	400.00	49%	204.00	234.60
WIC-1B-S/T	1-Port ISDN WAN Interface Card(dial and leased line)	500.00	49%	255.00	293.25
TOTALES (\$)		8,095.00	49%	4,128.45	4,747.72

b) Tenemos al Equipo Router Cisco 2611 con la configuración de 2 interfaces Ethernet, 1 interface BRI ISDN S/T y 04 puertos E&M.

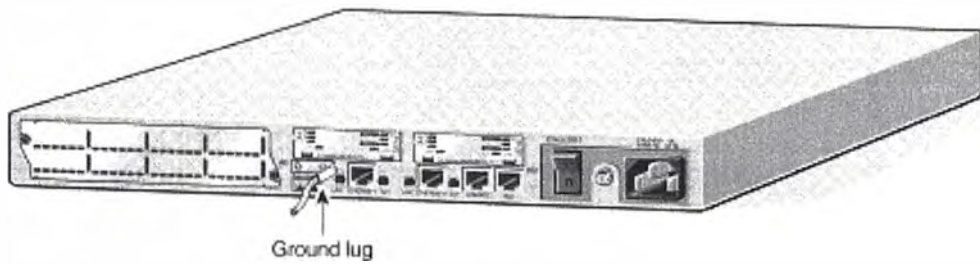


Figura 5.2: Vista posterior del router Multiservicio Cisco 2611

EQUIPO CISCO ROUTER 2611 W/2E/1B-S/T/2E&M

Product	Description	Price (\$)	Discount	Price F.O.B. (\$)	Price Lima (\$)
CISCO2611	Dual Ethernet Modular Router w/ Cisco IOS IP Software	2,495.00	49%	1,272.45	1,463.32
CAB-AC	Power Cord.110V	0.00	49%	0.00	0.00
S26AP-12103T	ENTERPRISE PLUS	1,300.00	49%	663.00	762.45
MEM2600-32U48D	32 to 48MB DRAM Factory Upgrade for the Cisco 2600	1,000.00	49%	510.00	586.50
MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600	700.00	49%	357.00	410.55
NM-2V	Two-Slot Voice/fax Network Module	1,700.00	49%	867.00	997.05
VIC-2E/M	Two-port Voice Interface Card - E&M	400.00	49%	204.00	234.60
WIC-1B-S/T	1-Port ISDN WAN Interface Card(dial and leased line)	500.00	49%	255.00	293.25
TOTALES (\$)		8,095.00	49%	4,128.45	4,747.72

c) Tenemos al Equipo Router Cisco 7206 Principal con la configuración de 2 interfaces FastEthernet, 1 interface PRI ISDN S/T, 4 puertos CBR y 01 puerto OC-3 ATM.

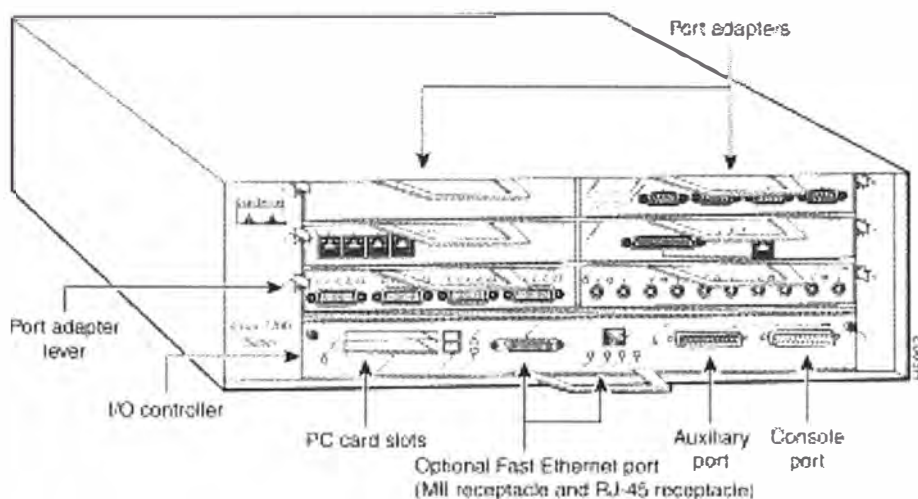


Figura 5.3: Vista Frontal del Router Multiservicio 7206

EQUIPO PRINCIPAL CISCO ROUTER 7206 W/2FE/1OC-3/4CBR

Product	Description	Price (\$)	Discount	Price F.O.B. (\$)	Price Lima (\$)
CISCO7206	Cisco 7206. 6-slot chassis. 1 AC Supply w/IP Software	7.000.00	49%	3.570.00	4.105.50
NPE-225	Network Processing Engine NPE-225 (128MB default memory)	4.500.00	49%	2.295.00	2.639.25
C7200-I/O	Cisco 7200 Input/Output Controller	1.000.00	49%	510.00	586.50
MEM-I/O-FLC20M	Cisco 7200 I/O PCMCIA Flash Memory. 20 MB Option	400.00	49%	204.00	234.60
PWR-7200	Cisco 7200 AC Power Supply Option	0.00	49%	0.00	0.00
CAB-AC	Power Cord, 110V	0.00	49%	0.00	0.00
S72A-12103T	Cisco 7200 Series IOS Enterprise	3.000.00	49%	1.530.00	1.759.50
PA-A2-4E1XC-OC3SM	CES OC3 Port Adapter 4E1 Ports 120ohms	10.000.00	49%	5.100.00	5.865.00
PA-2FEISL-TX	2 port Fast Ethernet/ISL 100BaseTx Port Adapter	3.800.00	49%	1.938.00	2.228.70

TOTALES (\$) **29,700.00** **49%** **15,147.00** **17,419.05**

d) Tenemos al Equipo Router Cisco 7206 Secundario con la configuración de 2 interfaces FastEthernet, 1 interface PRI ISDN S/T, 4 puertos CBR y 01 puerto OC-3 ATM.

EQUIPO SECUNDARIO ROUTER 7206 W/2FE/1OC3/4CBR/1 E1-PRI

Product	Description	Price (\$)	Discount	Price F.O.B. (\$)	Price Lima (\$)
CISCO7206	Cisco 7206, 6-slot chassis, 1 AC Supply w/IP Software	7,000.00	49%	3,570.00	4,105.50
NPE-225	Network Processing Engine NPE-225 (128MB default memory)	4,500.00	49%	2,295.00	2,639.25
C7200-I/O	Cisco 7200 Input/Output Controller	1,000.00	49%	510.00	586.50
MEM-I/O-FLC20M	Cisco 7200 I/O PCMCIA Flash Memory, 20 MB Option	400.00	49%	204.00	234.60
PWR-7200	Cisco 7200 AC Power Supply Option	0.00	49%	0.00	0.00
CAB-AC	Power Cord, 110V	0.00	49%	0.00	0.00
S72A-12103T	Cisco 7200 Series IOS Enterprise	3,000.00	49%	1,530.00	1,759.50
PA-A2-4E1XC-OC3SM	CES OC3 Port Adapter 4E1 Ports 120ohms	10,000.00	49%	5,100.00	5,865.00
PA-2FEISL-TX	2 port Fast Ethernet/ISL 100BaseTx Port Adapter	3,800.00	49%	1,938.00	2,228.70
PA-MC-2E1/120	2 port multichannel E1 port adapter with G.703 120ohm	4,500.00	49%	2,295.00 0	2,639.25
TOTALES (\$)		34,200.00	49%	17,442.00	20,058.30

Considerando que se cuenta con un Nodo principal y uno secundario para conformar el Core o núcleo de la Red. Adicionalmente las 18 Sedes Bancarias y las 12 Sede proveedoras de información se puede tener el siguiente monto de inversión.

COSTOS RESUMEN DE INVERSIÓN

Product	Description	Total F.O.B. (\$)	Total Lima (\$)	Cantidad	Sub-Total (\$)
Nodo Principal	Equipo Cisco Router 7206 w/2FE/1OC-3/4CBR	15,147.00	17,419.05	1	17,419.05
Nodo Secundario	Equipo Cisco Router 7206 w/2FE/1OC-3/4CBR/1 E1-PRI	17,442.00	20,058.30	1	20,058.30
Equipo CPE (FXS)	Equipo Cisco Router 2611 w/2E/1B-S/T/2FXS	4,128.45	4,747.72	10	47,477.20
Equipo CPE (E&M)	Equipo Cisco Router 2611 w/2E/1B-S/T/2E&M	4,128.45	4,747.72	20	54,954.40
TOTALES (\$)		40,845.90	46,972.79	-	179,908.88

CONCLUSIONES

1. Esta Red de Interconexión bancaria logró estandarizar las conexiones de los Bancos hacia sus proveedores de Información. Estas conexiones anteriormente eran de forma indistinta y utilizaban protocolos propietarios; los cuales significaban en cuestión económica realizar compras de equipos adicionales y a su vez implicaba tener un soporte por la misma empresa que entregaba dicho servicio.
2. Con esta Red de Interconexión bancaria se logró disminuir la cantidad de Enlaces por cada Banco hacia sus proveedores de información. Esta disminución de los enlaces también disminuye el riesgo operativo en el mantenimiento, operación y gestión de estos Circuitos. Todo esto ya que no era necesario almacenar una Base de datos enorme para saber a que proveedor pertenece cada uno de estos enlaces, en vez se tendría únicamente un número que llamar para reportar un caso de problema o avería.
3. Con esta Red de Interconexión bancaria se logró una disminución en los costos de mantenimiento, operación y gestión de las conexiones a los proveedores de información.
4. Con esta Red de Interconexión bancaria se logró manejar mayores capacidades para el transporte de los datos. Ya que estaríamos utilizando una plataforma que puede obtener mayores velocidades de conexión por cada puerta hasta de 4 Mbps (Es lo recomendable por puerta Ethernet antes de encontrar colisiones en

la interface física) y en la puerta principal hasta 155Mbps con el mismo equipamiento.

5. Con esta Red de Interconexión bancaria se logró una Red escalable, flexible y soporta cualquier tipo de servicio dentro de dicha plataforma. Con este tipo de Red se ha logrado solucionar problemas de integración de tecnologías pasadas con el equipo llamado multiservicio en cada uno de los extremos de la Red.

ANEXOS

ANEXO A GLOSARIO

ABR	Available Bit Rate
AIM	AOL Instant Messenger
ARPA	Agencia de Programas Avanzados de Investigación
ARPAnet	Red informática de ARPA
ASM	Tarjeta de Control de Alarmas
ATM	Asynchronous Transfer Mode
BACKBONE	Red Central
BCC	Broadband Control Card
BCCS	Tarjeta Redundante de Control del BPX
BPX	Broadband Packet Exchange
BRI	Basic Rate Interface
CAR	Committed Access Rate
CBR	Constant Bit Rate
CERN	Consejo Europeo de Investigación Nuclear
CES	Circuit Emulation Standard
CLI	Command Line Interface
CLNS	Connectionless Network Service
CPE	Customer Premises Equipment
CSMA/CD	Carrier Sense Multiple Access/with Collision Detection
DARPA	Defense Advanced Research Projects Agency
DECNET	Digital Equipment Corporation
DLSW	Data Link Switch
DNS	Domain Name Server
DSP	Digital Signal Processing/Processor
DUAL	Diffusing Update Algorithm
E&M	Interface de Voz con señalización E y M
E-COMMERCE	Comercio Electrónico
FDDI	Fiber Digital Device Interface
FRAME RELAY	Conmutación de Frames
FTP	File Transfer Protocol
FXO	Foreign exchange office
FXS	Foreign exchange station
HSRP	Hot Standby Router Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol

ICMP	Internet Control Message Protocol
IP	Internet Protocol
IP ADDRESS	Dirección Internet
IPX	Internetwork Packet Exchange
ISDN	Integrated Service Digital Network
ISL	Inter Switch Link
IT	Information Technology
LAN	Local Area Network
LANE	LAN Emulation
LSA	Link State Advertisement
LOAD BALANCING	Balanceo de carga
MAC	Media/Medium Access Control
MBPS	Mega Bit per Second
NNI	Network Interface
NRT-VBR	No Real Time - Variable Bit Rate
OSI	Internacional Organization for Standardization
PBX	Private Branch Exchange
POP	Point of Presence
PPS	Paquetes por Segundo
PRI	Primary-Rate Interface
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RISC	Reduced Instruction Set Computing
RT-VBR	Real Time - Variable Bit Rate
SLA	Service Level Agreement
SMTP	Service Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SUBNET	Sub Red
SUNAD	Superintendencia Nacional de Adunas
SVC	Switched Virtual Circuit
SWICTH	Conmutador
TACACS	Total Access Communication System Access Control
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TPDU	Transport Protocol Data Unit
UDP	User Datagram Protocol
UNI	User Network Interface
VBR	Variable Bit Rate
VC	Virtual Circuit
VLAN	Virtual LAN
VoFR	Voice over Frame Relay
VoIP	Voice over IP

VPN	Virtual Private Network
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WIC	Wan Interface Card
WIRED	Weighted Random Early Detection
WWW	World Wide Web

ANEXO B
ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS
FAMILIA CISCO BPX 8600

<p>CISCO BPX 8620</p> <p>Dimensions</p>	<p>H x W x D: 22.75 x 17.72 x 27 in (57.8 x 45 x 68.6 cm)</p> <p>Rack mountable in industry-standard EIA/RETMA racks (17.75-in. [45.1 cm] minimum between rails); rack-mount adapters are available for mounting in 23-in. (58.42 cm) telco racks</p>
<p>BPX 8600 Weight (Approximation)</p>	<p>73 lb (33.2 kg) empty BPX shelf with fans, but without power supplies</p> <p>6 lb (2.7 kg) each BPX card</p> <p>2 lb (0.9 kg) each DC power entry module</p> <p>18 lb (8.2 kg) empty AC power supply tray</p> <p>16 lb (7.3 kg) each AC power supply</p>
<p>CISCO BPX 8620</p> <p>Power Requirements</p>	<p>1400W dissipation (max)</p> <p>-48 VDC or 208/240 VAC input</p>
<p>Crosspoint Switch Fabric</p>	<p>Peak switching capacity of 19.2 Gbps</p> <p>Twelve 800/1600-Mbps switch ports that support up to</p>

	<p>OC-12/STM-4 cell rate</p> <p>Arbiter establishes up to 20 million cell connections per second</p>
<p>Network Interfaces</p>	<p>T3/DS3 (44.736 Mbps) with physical layer convergence procedure (PLCP) per TA-TY-000773</p> <p>E3 (34.368 Mbps) per ITU-T Rec. G.804</p> <p>OC-3/STM-1 (155.520 Mbps), complies with SONET standards Bellcore TR-253-CORE, ANSI T1.105; complies with SDH standards ITU-T G.707, G.708, G.709, G.957, G.958</p> <p>OC-12/STM-4 (622.08 Mbps), complies with SONET standards Bellcore TR-253-CORE, ANSI T1.105; complies with SDH standards ITU-T G.707, G.708, G.709, G.957, G.958</p> <p>Automatic protection switching per ITU-T Rec. G.783</p>
<p>Common Network Interface Features</p>	<p>Up to 16 independent queues for class-based queuing</p> <p>Queues programmable for maximum queue depth, minimum service bandwidth, maximum service bandwidth, cell loss priority (CLP) thresholds, Explicit Forward Congestion Indication (EFCI) thresholds</p> <p>Fully compliant ABR VS/VD implementation</p>

	<p>Explicit rate marking</p> <p>EFCI Marking</p> <p>ForeSight closed-loop, rate-based congestion management</p>
<p>Broadband Service Interfaces</p>	<p>T3/DS3 UNI (44.736 Mbps) with PLCP per TA-TY-000773</p> <p>E3 UNI (34.368 Mbps) per ITU-T Rec. G.804</p> <p>OC-3/STM-1 UNI (155.520 Mbps), complies with SONET standards Bellcore TR-253-CORE, ANSI T1.105; complies with SDH standards ITU-T G.707, G.708, G.709, G.957, G.958</p> <p>OC-12/STM-4 UNI (622.08 Mbps), complies with SONET standards Bellcore TR-253-CORE, ANSI T1.105; complies with SDH standards ITU-T G.707, G.708, G.709, G.957, G.958</p>
<p>Optional Redundancy</p>	<p>All components are optionally redundant to 100-percent system redundancy, including the control processor, cross point switch, network interfaces, service interfaces, critical backplane signals, power supplies, power modules, and cooling fans.</p>
<p>Network Management</p>	<p>Interfacing-to-network management is provided via:</p>

Interfaces	<p>One 802.3 attachment unit interface (AUI) for local connectivity to network management systems</p> <p>Two asynchronous control/printer ports</p>
Alarms, Indicators, and Controls	<p>Major node alarm, minor node alarm, alarm cut-off, and history indicators</p> <p>Visual and audible (major and minor) relay closures provided for connection to Central Office (CO) alarm system, including power supply status indicators and activity indicator.</p> <p>Each interface module has a minimum of three visual indicators:</p> <p>Active (green) / Standby (yellow) / Fail (red)</p>
Clock Sources	<p>Internal, free-running oscillator, Stratum 3</p> <p>Can be phase-locked to any trunk or line</p> <p>May be phase-locked to either of two T1/E1 external clock inputs</p>
Node Synchronization	<p>Stratum 3 clock per ATT PUB 62411</p> <p>Software-programmable source: internal clock, transmission line, auxiliary port to an external clock source</p>

Acoustical Measured 2 ft from the frame on all sides	Front 61.0 dB Back 65.2 dB Left Side 57.0 dB Right Side 57.5 dB
Shock	Withstands 10G, 10 ms. at 1/2 sine wave
Vibration	Withstands 1/4G, 20 to 500 Hz
Heat Transfer to Room	Up to 7200 BTUs depending on node configuration
Certification	EMI FCC Part 15, EN55022 (CISPR-A Certification), IEC 801-2 (VCCI Class 2) Saftey UL 1950, CSA 950, EN60950 ESD/Immunity EN55082-1, -2, -3, -4, -5

FAMILIA CISCO ROUTER 7200

Especificaciones del NPE Característica	Ventaja
Alto rendimiento	
Alto rendimiento	<ul style="list-style-type: none"> • Un rendimiento de conmutación de CEF de hasta 400 Kpps

	<ul style="list-style-type: none"> • Un rendimiento del plano de conmutación de hasta 1 Gbps • Compatible con configuraciones de alta densidad • Compatibilidad con los actuales medios de alta velocidad • Permite servicios Capa 3 avanzados tales como compresión, cifrado y gestión del tráfico (QoS, recuento del tráfico y seguridad) • Completo soporte para el software Cisco IOS
Soporte multifunción	
Soporte multifunción	<ul style="list-style-type: none"> • Simplifica la arquitectura de red • Reduce los costos de aprovisionamiento y de funcionamiento/gestión • Ahorra espacio en el bastidor • Proporciona mayores oportunidades de ingresos a los servicios CPE y de gestión de red
Aplicaciones	<ul style="list-style-type: none"> • El alto rendimiento y la versatilidad de los routers de la serie Cisco 7200 hacen que sean la mejor elección para una amplia gama de aplicaciones tales como: <ul style="list-style-type: none"> ○ Gateways VPN de empresas ○ Puntos de presencia (POP) de proveedores de servicios ○ Centros de datos con procesadores centrales y campus IBM
Interfaces	<ul style="list-style-type: none"> • La más amplia gama de adaptadores de puertos para LAN, WAN y soporte de medios • La alta densidad de routers adaptadores de puertos ofrece una solución ampliable con muchas opciones de medios a un bajo precio por puerto.
Gigabit Ethernet o 2 puertos Fast Ethernet en el controlador de E/S	<ul style="list-style-type: none"> • Conserva las ranuras de adaptador de puerto • Reduce el precio por puerto Gigabit Ethernet y Fast Ethernet

<p>Adaptadores de puerto estándar con Cisco 7500/VIP</p>	<ul style="list-style-type: none"> • Simplifica la gestión de repuestos • Protege las inversiones del cliente en interfaces
<p>Soporte multiservicio</p>	
<p>Intercambio multiservicio (MIX)</p>	<ul style="list-style-type: none"> • Los sistemas Cisco 7204 VXR y Cisco 7206 VXR son compatibles con la función de conmutación DS0 de las aplicaciones con tasa de bits constante, como la telefonía, con la ayuda del MIX integrado. • Compatible con los futuros adaptadores de puertos de voz digital que tienen MIX activado
<p>Adaptadores de puertos</p>	<ul style="list-style-type: none"> • La emulación de circuitos ATM posibilita la existencia de servicios de integración de datos, voz y vídeo • Admite los futuros adaptadores de puertos multicanal activados con MIX
<p>Tiempo máximo de actividad de la red</p>	
<p>Instalación y extracción en actividad de los adaptadores de puerto</p>	<ul style="list-style-type: none"> • Permite actualizar fácilmente a una mayor densidad y a nuevos adaptadores de puerto sin necesidad de reiniciar o desconectar el sistema • Reduce la intervención en la operación debido a que los adaptadores de puerto se reconfiguran automáticamente
<p>Fuentes de alimentación dobles con corriente compartida</p>	<ul style="list-style-type: none"> • Mayor fiabilidad con sistema redundante (corriente alterna o corriente continua) • El reparto de carga amplía la vida útil de la fuente de alimentación • Permite que el usuario instale fuentes de alimentación dobles para el suministro principal; cada fuente de alimentación cuenta con su propio cable, con lo que se eliminan los riesgos asociados con el fallo de las fuentes de alimentación ininterrumpida (UPS) • Las fuentes de alimentación comparten la

	realiza el cambio automáticamente
Inicio rápido	<ul style="list-style-type: none"> • Permite reparar en cuestión de segundos, reduciendo el tiempo de inactividad y el impacto en la fiabilidad de la red
Monitorización ambiental	<ul style="list-style-type: none"> • Avisa al operador en caso de fluctuaciones antes de que se genere un error grave, con lo que permite resolver el problema proactivamente con el sistema en línea
Capacidad de gestión y de servicio	
CiscoWorks y CiscoView	<ul style="list-style-type: none"> • Permite la gestión simplificada de los routers de la serie Cisco 7200
Interfaz de gestión del explorador de Web de Cisco	<ul style="list-style-type: none"> • Ofrece una herramienta de navegación a través de la interfaz de línea de instrucciones y permite que el usuario verifique el estado o modifique la configuración simplemente apuntando y haciendo clic.
Memoria Flash del sistema	<ul style="list-style-type: none"> • Permite realizar actualizaciones rápidas y fiables del software y del microcódigo • Administración centralizada; no es necesario visitar cada emplazamiento de los routers para actualizar el software o el microcódigo
Componentes reemplazables en las instalaciones	<ul style="list-style-type: none"> • Permite reparar componentes sin tener que enviar el sistema a la fábrica
CSU/DSU integradas en los adaptadores de puerto	<ul style="list-style-type: none"> • Simplifica la gestión remota de todos los elementos del equipamiento de cliente (Customer Premise Equipment, CPE), con lo que se

	una reducción de los costos de funcionamiento
Diseño ergonómico	
Indicadores LED de estado	<ul style="list-style-type: none"> • Permiten determinar el estado operativo con rapidez
Facilidad de acceso a todos los componentes	<ul style="list-style-type: none"> • Permite reparar en cuestión de segundos, reduciendo el tiempo de inactividad y el impacto a la red
Instalación flexible en bastidor	<ul style="list-style-type: none"> • Permite optimizar las instalaciones a través de instalación frontal o posterior
Gestión de los cables	<ul style="list-style-type: none"> • Sistemas de alivio de presión y puntos de anclaje, con lo que se simplifica la instalación y se impiden desconexiones accidentales o daños a los cables

FAMILIA CISCO ROUTER 7200

Rangos de densidad de la serie Cisco 7200 Característica	Cisco 7206	Cisco 7204 VXR	Cisco 7206 VXR
Ranuras configurables	6	4	6
Puertos Ethernet (10BaseT)	48	32	48
Puertos Ethernet (10BaseFL)	30	20	30
Puertos Fast Ethernet (TX)	3	4	Hasta 6 ¹
Puertos Fast Ethernet (FX)	3	4	Hasta 6 ¹

Adaptadores de puertos EtherSwitch	2	2	2
Puertos 100VG-AnyLAN	3	4	Hasta 6 ¹
Puertos FDDI (FDX, HDX)	3	0	0
Puertos ATM	3	4	Hasta 6 ¹
Packet over SONET	2	2	2
Adaptadores de puertos ATM-CES (voz, vídeo y datos), doble ancho	1	1	1
Puertos Token Ring (FDX, HDX)	24	16	24
Puertos serie síncronos	48	32	48
Puertos ISDN BRI (U y S/T)	48	32	48
Puertos ISDN PRI, T1/E1 multicanal	48	32	48
Puertos T3 multicanal	2	Hasta 4 ¹	Hasta 6 ¹
Puertos HSSI	6	Hasta 8 ¹	Hasta 12 ¹
Puertos Packet over T3/E3 (DSU integrada)	6	Hasta 8 ¹	Hasta 12 ¹
Puertos de interfaz del canal IBM (ESCON y paralelo)	3	6	6

FAMILIA CISCO ROUTER 7200

Especificaciones de dimensiones y peso de la serie Cisco 7200 Características	Cisco 7204 VXR	Cisco 7206 y Cisco 7206 VXR
Altura	5,25 pulgadas (13,34 cm)	5,25 pulgadas (13,34 cm)
Anchura	16,8 pulgadas (42,67 cm)	16,8 pulgadas (42,67 cm)
Profundidad	17 pulgadas (43,18 cm)	17 pulgadas (43,18 cm)
Peso (máx.)	50 libras (22,7 kg)	50 libras (22,7 kg)
Peso (instalación/mín.)	36,60 libras (16,64 kg)	36,60 libras (16,64 kg)

REQUISITOS DE ALIMENTACIÓN

Requisitos de alimentación de la serie Cisco 7200 Características	Cisco 7204 VXR	Cisco 7206/ Cisco 7206 VXR
Entrada, salida AV, vatios	370 vatios máx. 280 vatios máx.	370 vatios máx. 2 80 vatios máx.
Voltaje de entrada de corriente alterna (CA)	de 100 a 240 VCA	de 100 a 240 VCA
Frecuencia	de 50 a 60 Hz	de 50 a 60 Hz
Corriente de entrada CA	5 A máx. a 110 VCA 2,5 A máx. a 240VCA	5 A máx. a 110 VCA 2,5 A máx. a 240VCA

Corriente de entrada CC	5,8 amperios máx. a -48 VDC	5,8 amperios máx. a -48 VDC
Disipación de calor	560 W (1262 Btu/hr)	560 W (1262 Btu/hr)
Voltaje de entrada CC	-38 VCC mín. -48 VCC nominal -72 VCC máx.	-38 VCC mín. -48 VCC nominal -72 VCC máx.

CONDICIONES AMBIENTALES

Especificaciones ambientales de la familia Cisco 7200 Función	Cisco 7204 /Cisco 7204 VXR	Cisco 7206/ Cisco 7206 VXR
Temperatura de actividad	de 32 a 104 ° F (de 0 a 40 ° C)	de 32 a 104 ° F (de 0 a 40 ° C)
Humedad relativa	de 10 a 90% sin condensación	de 10 a 90% sin condensación
Temperatura de inactividad	de -4 a 149° F (de -20 a 65° C)	de -4 a 149° F (de -20 a 65° C)

FAMILIA CISCO ROUTER 2600

La serie Cisco 2600 proporciona una flexibilidad sin paralelo y opciones de densidad de puertos para las sucursales. La siguiente tabla resalta algunas de las posibles configuraciones de la serie Cisco 2600:

Aplicación	Nº máx. admitido
Llamadas de voz simultáneas (digitales/analógicas)	60/4
Conexiones T1/E1 (incluyendo ATM)	8
Modems integrados	16
RDSI PRI (canales B)	64

RDSI BRI	10
Serial asíncrona	37
Serial síncrona	12

- Procesador principal: 80 MHz RISC (Cisco 265x); 50 MHz RISC (Cisco 262x); 40 MHz RISC (Cisco 261x)
- Memoria Flash: de 8 a 16 MB (Cisco 261x y Cisco 262x); de 8 a 32 MB (Cisco 265x sólo)
- Memoria de sistema (DRAM): de 32 a 64 MB (Cisco 261x y Cisco 262x); de 32 a 128 MB (Cisco 265x sólo, usa SDRAM)
- Ranuras para tarjetas de interfaz WAN: 2
- Ranuras para módulos de red: 1
- Ranura AIM: 1
- Consola/velocidad auxiliar: 115,2 Kbps (máxima)
- Ancho: 17,5 pulgadas (44,5 cm)
- Altura: 1,69 pulgadas (4,3 cm)
- Profundidad: 11,8 pulgadas (30 cm)
- Peso (mín.): 8,85 libras (4,02 kg.)
- Peso (máx.): 10,25 libras (4,66 kg)
- Disipación de potencia: 72 W (máximo)
- Voltaje de corriente alterna (CA) de entrada: de 100 a 240 VCA
- Frecuencia: de 47 a 64 Hz
- Tensión de entrada CA: 1,5 amperios
- Voltaje de corriente continua (CC) de entrada: de -38 V a -60 V (etiqueta UL)
- Tensión CC de entrada: 2 amperios
- Temperatura de actividad: de 32 a 104° F (de 0 a 40° C)
- Temperatura de inactividad: de -13 a 158° F (de -25 a 70° C)
- Humedad relativa: de 5 a 95% sin condensación
- Nivel de ruido (mín.): 38 dbA
- Nivel de ruido (máx.): 42 dbA

TABLA DE MODULOS UTILIZADOS

Módulo	Descripción
VIC-2BRI-S/T-TE¹	Tarjeta de interfaz de voz/fax del equipo terminal BRI S/T de dos puertos para el módulo de red de voz/fax
VIC-2FXS	Tarjeta de interfaz de voz/fax del equipo terminal BRI S/T de dos puertos para el módulo de red de voz/fax

	voz/fax
VIC-2FXO-M1²	Dos tarjetas de interfaz de puerto FXO voz/fax para módulos de red voz/fax con identificación de llamada y desconexión por supervisión (versión norteamericana y otros países)
VIC-2FXO	Dos tarjetas de interfaz de puerto FXO voz/fax para módulos de red de voz/fax (versión norteamericana y otros países)
VIC-2FXO-M2²	Dos tarjetas de interfaz con puerto FXO voz/fax con identificación de llamada y desconexión de supervisión (versión europea)
VIC-2FXO-EU	Tarjeta de interfaz de voz/fax FXO de dos puertos (versión europea)
VIC-2FXO-M3	Tarjeta de interfaz de voz/fax de dos puertos FXO para Australia
VIC-2E/M	Tarjeta de interfaz de voz/fax con dos puertos E&M para el módulo de red de voz/fax

NM-1V	Un módulo de red con ranura para la tarjeta de interfaz de voz/fax
Requisitos de Cisco IOS	11.3(1)T o posterior para la serie Cisco 3600
	11.3(4)T o posterior para la serie Cisco 2600
Número de producto Cisco	800-02489-01
Especificaciones FCC	Dispositivo FCC clase B
Repuesto	NM-1V=
Tiempo medio entre fallos (MTBF)	946.423 horas
Requiere una VIC	VIC-2FXS 800-02493-01
	VIC-2E/M 800-02497-01

	VIC-2FXO-M1 800-05298-01
	VIC-2FXO-M2 800-05920-01
	VIC-2FXO 800-02495-01
	VIC-2FXO 800-4581-01
	VIC-2FXO-EU 800-03639-01
	VIC-2BRI-S/T-TE 800-03803-1
	VIC-2BRI-NT/TE

NM-2V	Un módulo de red con dos ranuras para la tarjeta de interfaz de voz/fax
Requisitos de Cisco IOS	11.3(1)T o posterior para la serie Cisco 3600
	11.3(4)T o posterior para la serie Cisco 2600
Número de producto Cisco	800-02491-01
Especificaciones FCC	Dispositivo FCC clase B
Repuesto	NM-2V=
MTBF	755.717 horas
Requiere como mínimo una VIC (dos como máximo)	VIC-2FXS 800-02493-01
	VIC-2E/M 800-02497-01
	VIC-2FXO-M1 800-05298-01

	VIC-2FXO-M2 800-05920-01
	VIC-2FXO 800-02495-01
	VIC-2FXO 800-4581-01
	VIC-2FXO-EU 800-03639-01
	VIC-2BRI-S/T-TE 800-03803-1
	VIC-2BRI-NT/TE

VIC-2E/M	Tarjeta de interfaz de voz/fax E&M de dos puertos
Tipo de interfaz	Para entroncamiento con PBX
Requisitos de Cisco IOS	11.3(1)T o posterior para la serie Cisco 3600
	11.3(4)T o posterior para la serie Cisco 2600
Número de producto Cisco	800-02497-01
Conformidad	Dispositivo FCC clase B, CE
Normas de seguridad	UL 1950
Repuesto	VIC-2E/M=
Formatos de señalización de dirección	DTMF en banda
	Impulsos fuera de banda (10/20 pps)
Formatos de señalización	Inmediato, acceso telefónico retardado, inicio rápido
Tipos de señalización	I, II, III y V
Límite actual E-Lead	100 mA

Sensibilidad M-Lead	> 3 mA
Distorsión de impulsos	< 2%
Conector físico	4 hilos/2 hilos
Número de conectores/puertos	Dos
MTBF	1.943.521 horas

VIC-2FXS	Tarjeta de interfaz de voz/fax FXS de dos puertos
Tipo de interfaz	Tarjeta de interfaz Foreign Exchange Station
Requisitos de Cisco IOS	11.3(1)T o posterior para la serie Cisco 3600
	11.3(4)T o posterior para la serie Cisco 2600
Número de producto Cisco	800-02493-01
Conformidad	Dispositivo FCC clase B, CE
Normas de seguridad	UL1950
Repuesto	VIC-2FXS=
Formatos de señalización de dirección	DTMF en banda
	Impulsos fuera de banda (10/20 pps)
Formatos de señalización	Inicio en bucle, inicio en tierra
Tono de timbre	Configurable para los requisitos de distintos países
Voltaje del timbre	<45 Vrms a 5 REN a 25 Hz (frecuencia configurable)

Frecuencias del timbre	20 Hz, 50 Hz
Conector físico	RJ-11
Número de conectores/puertos	Dos
MTBF	2.248.909 horas

VIC-2FXO	Tarjeta de interfaz de voz/fax FXO de dos puertos
Tipo de interfaz	Foreign Exchange Office
Requisitos de Cisco IOS	11.3(1)T o posterior para la serie Cisco 3600
	11.3(4)T o posterior para la serie Cisco 2600
Número de producto Cisco	800-02497-01
Conformidad	Dispositivo FCC clase B, CE
Normas de seguridad	UL1950
Repuesto	VIC-2FXO=
Formatos de señalización	Inicio en bucle, inicio en tierra
Formatos de señalización de dirección	DTMF en banda
	Impulsos fuera de banda (10/20 pps)
Supervisión de desconexión de tono	Desconexión de llamadas en tonos de proceso inferiores a 600 Hz
Desconexión por interrupción de la alimentación	Desconexión de la llamada en caso de interrupción de la alimentación durante > 600 mseg

Conector físico	RJ-11
Número de conectores/puertos	Dos
MTBF	2.302.609 horas

VIC-2BRI-ST-TE	Tarjeta de interfaz de voz/fax BRI de dos puertos (en el terminal)
Tipo de interfaz	ISDN (RDSI) de acceso básico
Requisitos de Cisco IOS	12.0(3)T o superior para las series Cisco 3600 y 2600
Número de producto Cisco	800-03803-01
Conformidad	FCC parte 68 CS03 CTR3 TS -031 JATE Green Book
Normas de seguridad	UL1950, CAN/CSA-C22.2, IEC 950, EN60950
Repuesto	VIC-2BRI-ST-TE=
Normativas ITU	ITU-T Q.920, Q.921, Q.930, Q.931
Interfaz	S/T de usuario de cuatro hilos
ISDN (RDSI) de acceso digital	Acceso básico (BRI) 4B+2D
Conector físico	RJ-45

Número de conectores/puertos	Dos
MTBF	2.951.544 horas

FAMILIA CISCO FIREWALL SECURE PIX 515

	PIX Firewall 515-R	PIX Firewall 515-UR
Hardware		
Carcasa	Instalable en bastidor de 19 pulgadas (viene con hardware para instalar en bastidor); una unidad de bastidor	Instalable en bastidor de 19 pulgadas (viene con hardware para instalar en bastidor); una unidad de bastidor
Memoria de acceso aleatorio	32 MB	64 MB
Memoria Flash	16 MB	16 MB
Puerto de consola	RJ-45	RJ-45
Dispositivo de inicio/actualización	Sólo TFTP	Sólo TFTP
Puerto de recuperación de errores*	Desactivado	DB-25 EIA/TIA-232
Dimensiones físicas		
Altura	1,72 pulgadas (4,37 cm)	1,72 pulgadas (4,37 cm)
Ancho	16,82 pulgadas (42,72 cm)	16,82 pulgadas (42,72 cm)
Profundidad	11,8 pulgadas (29,97 cm)	11,8 pulgadas (29,97 cm)

Peso	11 libras (4,99 kg)	11 libras (4,99 kg)
Requisitos de alimentación		
Autoconmutación	100-240 VCA	100-240 VCA
Frecuencia	50-60 Hz	50-60 Hz
Corriente	1,5-0,75 amperios	1,5-0,75 amperios
Entorno de actividad		
Temperatura de actividad	de -5 a +45° C (de -25 a 113° F)	de -5 a +45° C (de -25 a 113° F)
Temperatura de inactividad	de -25 a 70° C	de -25 a 70° C
Humedad de actividad	95% de humedad relativa (RH)	95% de humedad relativa (RH)
Altitud de actividad	9.843 pies (3.000 m), 25° C (77° F)	9.843 pies (3.000 m), 25° C (77° F)
Altitud de inactividad	15.000 pies (4.570 m), 77° F (25° C)	15.000 pies (4.570 m), 77° F (25° C)
Choque en actividad	74 pda/seg (1,88 m/seg) 1/2 entrada de seno	74 pda/seg (1,88 m/seg) 1/2 entrada de seno
Choque en inactividad	60G 11 ms. 1/2 entrada de seno	60G 11 ms. 1/2 entrada de seno
Vibración en actividad	Entrada aleatoria de 0,41 Grms ² (de 5 a 500 Hz)	Entrada aleatoria de 0,41 Grms ² (de 5 a 500 Hz)
Vibración en inactividad	Entrada aleatoria de 0,41 Grms ² (de 5 a 500 Hz)	Entrada aleatoria de 0,41 Grms ² (de 5 a 500 Hz)

Disipación de calor (en el peor de los casos y con el máximo consumo)	160,37 BTU/hr	160,37 BTU/hr
EMI	CE, VCCI clase II, FCC, BCIQ, Austel	CE, VCCI clase II, FCC, BCIQ, Austel
Agencias de seguridad	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950
Estándar UL-1950	3ª edición	3ª edición
TUV EN 60950	2ª edición, Am. 1-4	2ª edición, Am. 1-4
Estándar IEC-950/VDE-0805 EN-60-950	Sí	Sí
Bellcore	No	No

ANEXO C
ENTREVISTA TÉCNICA REALIZADA A LOS BANCOS PARA
OBTENER INFORMACIÓN EN EL DISEÑO

ENTREVISTA TECNICA POR BANCO

Información del Cliente

Dirección del lugar:

Especificar el nombre(s), título(s) y número(s) de teléfono de la persona(s) de contacto para el ingreso durante horas regulares, después de horas y feriados/fines de semana.

Horas Regulares Horas No Regulares Feriados/Fin semana

Nombre _____

Cargo _____

Teléfono _____

Fax _____

E-mail _____

Horario de Trabajo

Especificar procedimiento de acceso al Edificio/Oficina en caso de averías

Especificar el nombre y número de teléfono del coordinador del local, responsable en asegurar que el ambiente este preparado en forma adecuada para la instalación y soporte de los equipos.

Especificar el número de teléfono más cercano a los equipos instalados.

Ambiente

En que piso serán ubicados los equipos ha instalar

Si no esta en el primer piso, hay elevador : ___Si ___No

Que otro tipo de equipos contiene este ambiente?

Con que tipo de equipo de aire acondicionado está provisto el ambiente?

_____ Ninguno

_____ Aire acondicionado normal de oficina

_____ Aire acondicionado piso inferior

Sistema Eléctrico

Indicar a continuación el nombre y número de teléfono de la persona encargada del servicio eléctrico del local.

Al equipo ha instalar se le ha proveído energía estabilizada AC ó DC?

_____ 120 VAC

_____ 208 VAC

_____ 240 VAC

_____ 48 VDC

Nota.- El esquema actual de energía variará dependiendo de la específica configuración del sistema.

El sistema eléctrico que posee es normalizado con punto a cero (neutro a tierra)

Cuenta con UPS para evitar cortes de energía eléctrica? ___Si ___No

En caso afirmativo, especificar si está preparado para soportar

Para 2611 240 VAC con 0.8 A Max. _____

Para 7206 240 VAC con 2.5A Max. _____

Cableado

Existe alguna restricción de cuantos cables puedan ser tendidos sobre canaletas y rack ? Si No

Si es afirmativo, especificar.

Existe alguna bandeja para el direccionamiento de cables?

Si No

En sus instalaciones cuenta con bandejas para cable UTP, Coaxial, Otros?

Si No

Existe algún plan de señalización , usado para cables en este Local?

Si No

Si la respuesta es afirmativa, describirla

Aplicaciones de Datos

Especificar las aplicaciones de Datos soportadas en las conexiones a implementar.

Host to host

Host to terminal

LAN / WAN

Video Conferencia

Otros, especificar

Hay alguna aplicación sensible al retardo (multidrop, etc)? Si No

Si la respuesta es afirmativa, describirla

Alguna aplicación asíncrona será soportada ? Si No

Si la respuesta es afirmativa, describirla

Red del Cliente

Que tipo de red usará para conectarse a la Red a Implementar ?

Ethernet

FastEthernet

TokenRing

Otros (Especificar)

Indicar a que tipo de equipo se conectará :

Cuantos usuarios va ha soportar este servicio ?

Cuantos servidores desea integrar a su Enlace ?

Por favor describa en términos generales su red actual. Si es posible proveer un diagrama topológico de esta.

Que tipo de red es, bridged o routed?

Que protocolos usará para conectarse a sus proveedores de Información IP, IPX, SNA, Appletalk?

Si Ud. usa protocolo IP, Que tipo de direcciones IP utiliza en su red ?

Si es pública, proveer la red y la máscara del segmento a conectar.

Si es privada, proveer la red y la máscara del segmento a conectar a su WAN.

Que protocolos de enrutamiento son usados dentro de su red RIP, EIGRP, OSPF?

Su compañía tiene alguna política de seguridad? Si es afirmativa, proveer el nombre del oficial de seguridad.

Que tipo de seguridad ha previsto para la interconexión ?

Firewall (Software) _____

Firewall (Hardware) _____

Conexión Directa a LAN _____

BIBLIOGRAFIA

1. ATM Internetworking
Anthony Alles. Cisco Systems Inc, Marzo 1995.
2. Redes de comunicación
Enciclopedia Microsoft(R) Encarta(R) 98. (c) 1993-1997 Microsoft Corporation.
3. REDES LOCALES Y TCP/IP
RAYA, José Luis
4. REDES DE BANDA ANCHA
CABALLERO, José Manuel
5. COMERCIO ELECTRÓNICO Y ESTRATEGIA EMPRESARIAL
Hacia la Economía Digital, 2ª Ed. Actualizada y Revisada - Del ÁGUILA, Ana Rosa
6. REDES ATM
Principios de Interconexión y su Aplicación - GUIJARRO, Luis
7. SISTEMAS DE AUTENTIFICACIÓN PARA SEGURIDAD EN REDES
OPPLIGER, Rolf
8. REDES DE ALTA VELOCIDAD
GARCÍA, Jesús; FERRANDO, Santiago y PIATTINI, Mario