

UNIVERSIDAD NACIONAL DE INGENIERIA
Facultad de Ingeniería Eléctrica y Electrónica



DISEÑO DE LA RED DE COMUNICACIONES BASADO EN FRAME RELAY, X.25
E ISDN CON ENRUTADORES Y
CONMUTADORES DEL BANCO DE CREDITO DEL PERU

INFORME DE INGENIERIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRONICO

César Augusto Nieto Astete

Promoción 1991 – 2

Lima – Perú - 1997

A mis padres y hermanos,

A Susana,

A Fernando Caller, Oscar Granados,

A mi Alma Mater,

A mi ciudad natal Huancayo.

SUMARIO

El número de aplicaciones que se implementa en el Banco y el número de transacciones que diariamente se realiza, exige un sistema de comunicaciones de alta confiabilidad y disponibilidad que garantice una atención rápida y continua.

El presente trabajo constituye un resumen de todos los aspectos técnicos teóricos y prácticos en el análisis y diseño de una red de envergadura. Esta fué basada en tecnologías disponibles en el mercado tal como: frame relay, X.25 e ISDN. El uso de estas tecnologías permitió la interconexión de las agencias con los nodos centrales con capacidad de redundancia.

Este trabajo está basado en la experiencia de una implementación real, por lo cuál se constituye en un aporte importante, pues detalla los diferentes criterios prácticos utilizados y limitaciones técnicas encontradas. Como resultado del diseño, esta red actualmente viene operando satisfactoriamente y se encuentra en proceso de crecimiento.

**DISEÑO DE LA RED DE COMUNICACIONES BASADO EN
FRAME RELAY, X.25 E ISDN CON ENRUTADORES Y
CONMUTADORES DEL BANCO DE CREDITO DEL PERU**

TITULO DEL TEMA: DISEÑO DE LA RED DE COMUNICACIONES BASADO EN FRAME RELAY, X.25 E ISDN CON ENRUTADORES Y CONMUTADORES DEL BANCO DE CREDITO DEL PERU

AUTOR: César Augusto Nieto Astete

PARA OPTAR : El Título Profesional de INGENIERO ELECTRONICO

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

UNIVERSIDAD NACIONAL DE INGENIERIA

LIMA, 1997

EXTRACTO

El presente trabajo consta de 4 capítulos que en forma práctica nos permiten mostrar el proceso de análisis y diseño de una red de amplio alcance basado en protocolos de comunicaciones tales como relevo de tramas (frame relay), X.25, e ISDN (Integrated Services Digital Network).

El primer capítulo presenta un estudio sobre la teoría del transporte del protocolo SNA (System Network Architecture) sobre una tecnología basado en enrutadores que operan principalmente con direcciones IP. Se explica la evolución, la técnica y ventajas frente a otras soluciones

El capítulo dos describe una serie de conceptos con relación a las redes y reglas de diseño de los mismos. Este capítulo incluye una breve explicación de los conceptos más importantes en diseño de redes, una explicación sobre las topologías de redes, alternativas de los diseño basado en frame relay, X.25 e ISDN. Asimismo, se describe el sistema de direccionamiento y las opciones de los protocolos de enrutamiento, mostrándonos una serie de alternativas que pueden ser aplicados de acuerdo a los requerimientos de la red que se desea implementar.

El capítulo tres detalla el diseño realizado y las alternativas escogidas. Este capítulo también presenta una descripción de la topología implementada, los equipos requeridos y las configuraciones y optimizaciones realizadas.

El capítulo cuatro nos muestra los gastos de inversión para la implementación de esta red de gran escala, materia del presente trabajo.

Asimismo se presenta algunas conclusiones derivadas del diseño e implementación de la red, así como también las recomendaciones que pueden ser importantes cuando se diseña e implementa una red de gran magnitud.

Finalmente, se adjuntan apéndices que nos muestran las particularidades de la red así como ciertos detalles y características de los equipos adquiridos.

INDICE

	Pag
INTRODUCCION	1
CAPITULO I	
DATA LINK SWITCHING (DLSW)	
1.1 Introducción	3
1.2 Fundamentos	4
1.3 Conexión de transporte	7
1.4 Formatos de los mensajes SSP	7
1.5 Parámetros de direccionamiento	9
CAPITULO II	
CONSIDERACIONES DE DISEÑO DE REDES	
2.1 Topología	13
2.1.1 Uso del modelo NBMA para acceso	13
2.1.2 Uso del modelo jerárquico para escalar	13
2.1.3 Escalamiento limitado con malla completa NBMA	13
2.1.4 Paquetes IPX SAP en una configuración malla completa NBMA	14
2.1.5 Configuración estrella de una malla parcial NBMA	15
2.1.6 Configuración de malla jerárquica	16
2.1.7 Configuración de malla híbrida	16
2.1.8 Escalamiento apropiado en una topología de malla híbrida	17
2.2 Consideraciones de diseño de una red frame relay	17

VIII

2.2.1	Dispositivos de acceso frame relay	18
2.2.2	Obtención del direccionamiento global	19
2.2.3	Control de flujo por descarte proporcional de paquetes	20
2.2.4	Uso de la notificación de congestión explícita	21
2.2.5	Enrutamiento dinámico en frame relay	21
2.2.6	Uso de protocolos de enrutamiento dinámico	22
2.2.7	Priorización del frame relay	22
2.2.8	Compatibilidad de señalización del enrutador y la red	23
2.2.9	Enlace punto a punto que provee compatibilidad completa	23
2.2.10	Broadcast inherente en redes LAN	24
2.2.11	Multiacceso de tipo No Broadcasting	24
2.2.12	Métricas de enrutamiento que no se basan en el CIR	24
2.2.13	Subinterfaces frame relay	25
2.2.14	Conmutación frame relay	26
2.3	Consideraciones de diseño de la red X.25	27
2.3.1	Uso de circuitos X.25 como enlaces de datos WAN	28
2.3.2	Uso del modelo NBMA para acceso de bajo costo	28
2.3.3	Uso de subinterfaces	28
2.4	Consideraciones de diseño de ISDN	29
2.4.1	Interfaces BRI y PRI de ISDN	30
2.4.2	Flexibilidad del ISDN con agregación de canal B	31
2.4.3	Nodos remotos con interface BRI a nodo central PRI	32
2.5	Consideraciones del direccionamiento IP	33
2.5.1	Direccionamiento jerárquico	33
2.5.2	Enrutamiento sin clases	35
2.5.3	Resumen de rutas	36

2.5.4	Direcciones para redes privadas	37
2.6	Protocolos de enrutamiento	38
2.6.1	Categorías de los protocolos de enrutamiento	38
2.6.2	La determinación de las rutas depende de las métricas	38
2.6.3	Uso de vectores de distancia	39
2.6.4	Uso de rutas estáticas	40
2.6.5	Protocolo de enrutamiento EIGRP	40
2.6.6	Distribución de direcciones para una red clase B	44
2.6.7	Asignación de direcciones de subredes y hosts	44
2.6.8	Enrutamiento sin clases de direcciones IP	45
2.6.9	Máscaras de subredes de longitud variable	46
2.6.10	Enrutamiento de protocolos basados en vectores de distancia y estado de enlace	47

CAPITULO III

DISEÑO DE LA RED DE COMUNICACIONES

3.1	Diseño de interconexión de principales sucursales	59
3.1.1	Topología de interconexión de sucursales	59
3.1.2	Diseño de los dispositivos de comunicaciones de sucursales	60
3.2	Diseño de la red de agencias	70
3.2.1	Topología de interconexión de agencias	70
3.2.2	Diseño de los dispositivos de comunicaciones de agencias	71
3.2.2.1	Agencias vía frame relay	71
3.2.2.2	Agencias vía X.25	71
3.3	Diseño de la red frame relay	72
3.3.1	Suscripción de la red frame relay	72
3.3.2	Capacidad del número de DLCI en los enrutadores	75

3.3.2.1 Limitaciones técnicas	76
3.3.2.2 Limitaciones prácticas	76
3.3.3 Análisis de tráfico	78
3.3.4 Actualización de rutas	79
3.4 Diseño de la red X.25	80
3.4.1 Direccionamiento X.25	80
3.4.2 Uso del modelo NBMA para acceso de agencias vía X.25	84
3.4.3 Servicios adicionales que se usan vía X.25	86
3.5 Diseño del sistema de direcciones IP	87
3.6 Diseño del protocolo de enrutamiento	91
3.6.1 Enrutamiento usando EIGRP	91
3.6.2 Control del ancho de banda	92
3.6.3 Configuración punto a punto	93
3.6.4 Diseño del protocolo de enrutamiento EIGRP	93
CAPITULO IV	
ASPECTOS ECONOMICOS	
4.1 Costo de equipos de comunicaciones	95
4.1.1 Costo de inversión en equipos de comunicaciones en La Molina	95
4.1.2 Costo de inversión en equipos de comunicaciones en la Oficina Principal	96
4.1.3 Costo de inversión en equipos de comunicaciones en sucursal San Isidro	96
4.1.4 Costo de inversión en equipos de comunicaciones en sucursal Miraflores	96
4.1.5 Costo de inversión en equipos de comunicaciones en sucursal Callao	97

4.1.6	Costo de inversión en equipos de comunicaciones en agencias	
	Gran Lima	97
4.2	Costo de facilidades de comunicaciones	97
4.2.1	Pago de 3 enlaces E1 2,048 Kbps servicio frame relay	97
4.2.2	Pago de 100 enlaces 64 Kbps servicio frame relay	98
4.2.3	Pago de 4 enlaces a 512 Kbps	98
	CONCLUSIONES Y RECOMENDACIONES	99
	APENDICE A Modelo de Configuración de Enrutadores	103
	APENDICE B Catálogos	117
	BIBLIOGRAFIA	153

INTRODUCCION

Los últimos años se han caracterizado por un crecimiento vertiginoso de las redes de área local. Muchas instituciones y empresas las han acogido como estrategia tecnológica para competir en el mercado. Uno de los sectores en donde se ha manifestado este crecimiento vertiginoso ha sido el sector financiero, de lo cual he sido testigo en mis años de labor profesional.

Con el crecimiento de las redes de área local, también crece la necesidad de interconectarlas para formar redes WAN (Wide Area Network). Sin embargo, uno de los principales obstáculos que se presentan es la no existencia de facilidades de comunicación para la implementación de tales redes.

En este último año el proveedor local Telefónica del Perú ha dado un paso importante al lanzar al mercado las facilidades frame relay e ISDN. Uno de los bancos más grande del Perú ha decidido ser uno de los primeros en usar estas tecnologías, para lo cual ha emprendido en una cambio importante en su sistema de comunicación con la finalidad de soportar las nuevas soluciones de sistemas de teleproceso debido a la reingeniería desarrollada.

Este cambio ha significado la modernización mediante el empleo de tecnologías de punta de su red de comunicaciones a nivel nacional usando enrutadores y conmutadores para unir sus principales sucursales y agencias formando la nueva estructura de comunicación basado en plataformas frame relay, X.25 e ISDN con el fin de soportar los protocolos TCP/IP (Transmission Control Protocol/Internet

Protocol), IPX y SNA, constituyéndose de esta manera en la primera red de comunicaciones de este tipo en el país.

El presente trabajo manifiesta mi experiencia lograda en estos años, debido a mi total participación en el equipo que realizó esta importante tarea, comenzando desde las pruebas de fuerza, la convocatoria a concurso de precios, el diseño y la implementación de la red WAN. Cabe destacar que el Señor Andrés Morita tuvo relevante participación en el equipo trabajo.

Espero que los detalles vertidos en este trabajo contribuyan como una referencia importante en proyectos de redes de comunicaciones basados en frame relay, X.25 e ISDN.

CAPITULO I DATA LINK SWITCHING (DLSW)

1.1 Introducción

Data link switching (DLSW) es un mecanismo que facilita el transporte de los protocolos IBM SNA (System Network Architecture) y el IBM NETBIOS (Network Basic Input Output Services), siendo esta técnica la usada entre los conmutadores de enlace de datos. Este protocolo no posee un completo enrutamiento, mientras que sí provee conmutación en el nivel de enlace de datos del SNA y el encapsulamiento en el transporte TCP/IP sobre la Internet. Este protocolo está regido por un RFC (Request For Comments) que determina los formatos de tramas y protocolos para el multiplexaje de datos entre los conmutadores de enlace de datos. La implementación inicial usa el TCP como transporte con integridad entre conmutadores de enlace de datos (data link switches). Sin embargo, otros protocolos de transporte como el OSI TP4 (Open System Interconnection Transport Protocol 4) podrían ser usados en el futuro.

DLSW puede soportar sistemas SNA(Physical Unit PU 2, PU 2.1 and PU 4) y opcionalmente sistemas NETBIOS conectados a una red de área local que sea compatible con IEEE802.2, así como sistemas SNA (PU 2-primario o secundario- y PU 2.1) conectado a enlaces IBM SDLC (IBM Synchronous Data Link Control). Los sistemas SDLC son provistos con una apariencia de LAN (Local Area Network) dentro del DLSW, es decir cada SDLC PU es presentado al protocolo SSP (Switch to Switch Protocol) como un único par de direcciones MAC/SAP (Media

Access Control/Source Access Point). Para los sistemas conectados a una red Token Ring, DLSW aparece como un puente de enrutamiento de origen (Source-Routing Bridge). Los sistemas Token Ring que son accedidos a través del DLSW aparecen como un sistema conectado a un anillo adyacente. Este es un anillo virtual que es manifestado dentro de cada DLSW.

1.2 Fundamentos

El mecanismo DLSW fue desarrollado para proveer soporte para SNA y NetBIOS en enrutadores multiprotocolares, ya que tanto SNA como NetBIOS son básicamente protocolos orientados a la conexión. El procedimiento llamado Data Link Control (DLC) que ellos usan en la LAN es el 802.2 Logical Link Control (LLC) tipo 2. DLSW también acomoda los protocolos SNA sobre los enlaces de la red WAN (Wide Area Network) vía el protocolo SDLC.

El estándar IEEE802.2 Tipo 2 fue diseñado asumiendo que el retardo de tránsito en la red podría no ser predecible. Por tanto los elementos del procedimiento LLC tipo 2 usan un temporizador fijo para detectar las tramas perdidas. Cuando un puente (bridge) remoto es usado sobre los enlaces de una red de área amplia (WAN), especialmente a bajas velocidades, los retardos en la red son altos y pueden variar exageradamente en casos de congestión. Cuando los retardos exceden el valor del temporizador denominado time-out, el nivel de LLC tipo 2 intenta retransmitir. Si las tramas no fueron realmente perdidas y sólo estuvieron retardados, es posible que ellas puedan convertirse en algo confuso para el procedimiento LLC tipo 2. Consecuentemente el enlace puede eventualmente salir de operación si el retardo excede el temporizador T1 varias veces el contador de reintento N2.

Teniendo en cuenta el uso de los servicios LLC tipo 2, el mecanismo DLSW maneja los problemas siguientes:

- Time-outs (tiempos expirados) de DLC.
- Acknowledges (reconocimiento) de DLC sobre la red WAN.
- Control de Flujo y Congestión.
- Control de Broadcast (transmisión) en la búsqueda de paquetes.
- Límites de Source-Route Bridging Hop Count (Conteo de los puntos de puente entre la fuente y las rutas).

NETBIOS también hace un uso extensivo de los servicios de datagramas que usan los servicios LLC tipo 1 no orientados a la conexión. En este caso, el DLC se encarga de los problemas mencionados en la lista de arriba.

La principal diferencia entre el DLC y el Bridging, es que para los datos orientados a la conexión el DLSW termina el Data Link Control donde el Bridging no lo puede realizar.

En un bridge tradicional, el Data Link Control es de extremo a extremo. El DLSW termina la conexión LLC tipo 2 en el conmutador. Significando que las conexiones LLC tipo 2 no cruzan la red de área amplia. El DLSW multiplexa las conexiones LLC dentro de una conexión TCP con el otro DLSW. Por lo tanto, las conexiones LLC en cada uno de los extremos son totalmente independientes. Es de completa responsabilidad del DLSW distribuir las tramas que ha recibido de una conexión LLC del otro extremo. El protocolo TCP es usado entre los extremos DLSW para garantizar una distribución de tramas.

Como resultado de este diseño, los tiempos expirados (time-outs) de LLC son limitados a la red de área local. También, el reconocimiento (acknowledge) LLC tipo 2 no viaja a través de la red WAN, por lo tanto reducen el tráfico a través de

los enlaces de la red amplia. Para enlaces SDLC, el polling y los poll-response ocurren localmente, no sobre la red amplia. Los Broadcast de tramas de búsqueda están controlados por el Data Link Switch una vez que la ubicación de un sistema destino es descubierto. Finalmente, el conmutador puede proveer control de flujo y congestión.

Sólo una copia de una unidad denominada LPDU (Link Protocol Data Unit) es enviada entre los conmutadores de DLC en mensajes SSP (XIDFRAME y INFOFRAME). Reintentos del LPDU son absorbidos por el Data Link Switch que lo recibe. El Data Link Switch que transmite el LPDU recibido en un mensaje SSP a un control local de datos DLC, realizará un reintento en la manera apropiada para el DLC local. Esto puede involucrar un temporizador de reintento y mantener un contador de reintento. La longitud del temporizador y el número de reintento es una implementación escogida basado en los parámetros de la configuración de usuarios y el tipo de DLC.

El DLSW usa un direccionamiento para establecer las conexiones entre los sistemas SNA. Los dispositivos conectados a un SDLC son definidos con las direcciones SAP (Source Access Point) y MAC (Media Access Control) para habilitarles la comunicación con los dispositivos conectados a una LAN.

Desde que el conmutador Data Link puede ser implementado en enrutadores multiprotocolares, pueden haber situaciones donde el puente y el conmutador son habilitados. Las tramas SNA pueden ser identificadas por sus enlaces SAP. Valores típicos del SAP para SNA son 0x04, 0x08 y 0x0C. Para NETBIOS siempre se usa un valor de enlace de SAP de 0xF0.

1.3 Conexión de transporte

El conmutador de Enlace de Datos puede ser usado en pares o por ellos mismos. Un simple DLSW internamente realiza una conmutación de enlace de datos a otro sin usar TCP (ver Fig 1.3). Los DLSW apareados multiplexa los enlaces de datos sobre un nivel de transporte usando un protocolo denominado Switch-to-Switch Protocol (SSP).

Antes de que el Data Link Switch ocurra entre dos enrutadores, ellos deben establecer dos conexiones TCP entre ellos. Cada Conmutador de Enlace de Datos mantendrá una lista de enrutadores con capacidad de DLSW y sus estados de activo/inactivo. Después de que la conexión TCP es establecida, los mensajes SSP son intercambiados para establecer las capacidades de los dos conmutadores Data Link. Una vez que el intercambio se ha completado, el DLSW empleará mensajes de control SSP para establecer circuitos extremo a extremo sobre la conexión a nivel de transporte. Dentro de la conexión de transporte, los mensajes SSP son intercambiados. Los formatos y tipos de los mensajes SSP son documentados posteriormente.

Los parámetros por defecto asociados con las conexiones TCP entre los Data Link Switch son los siguientes:

- Familia de Sockets AF_INET.
- Tipo de Socket SOCK_STREAM.
- Número de puerto de lectura 2065.
- Número de puerto de escritura 2067.

1.4 Formatos de los mensajes SSP

Los siguientes diagramas muestran los dos formatos de las cabeceras de los mensajes intercambiados entre los Data Link Switch, Control e Información (ver

Fig. 1.1 y Fig 1.2). La cabecera de los mensajes de control es usado para todos los mensajes excepto en las tramas de información (INFOFRAME) y los mensajes de control de flujo independientes (IFCM), los cuales son enviados en formatos de las cabeceras de información. Los encabezados de los mensajes INFOFRAME, KEEPALIVE y IFCM son 16 bytes de longitud, y los encabezados de los mensajes de control son 72 bytes de longitud. Los campos en los primeros 16 bytes en todos los encabezados de los mensajes son los mismos.

Los primeros 16 bytes de los encabezados de los mensajes de control e información contienen campos idénticos. Una breve descripción de los campos es el siguiente:

- El campo del número de versión indica un valor decimal de 49. Esto es usado para indicar el DLSW v1.

La longitud del encabezado es 0x48 hexadecimal para mensajes de control, indicando un valor decimal de 72 bytes, ó 0x10 hexadecimal para información y mensajes independientes de control de flujo, indicando un valor de 16 bytes.

- El campo de Longitud de Mensajes define el número de bytes dentro de un campo de datos.
- El campo del byte de control de flujo.
- El campo del Número de Encabezado es 0x01 hexadecimal indicando el valor de 1.
- El campo de Prioridad de Circuito.
- El campo de Dirección de Trama es 0x01 hexadecimal para las tramas enviadas desde el DLSW origen al DLSW destino, y es 0x02 hexadecimal para las tramas enviadas desde el DLSW destino al origen DLSW.

1.5 Parámetros de direccionamiento

Un enlace de datos está definido como una asociación lógica entre dos estaciones finales usando el Data Link Switch. Esto está identificado por un identificador Data Link Switch ID (14bytes) consistiendo en un par de direcciones de conexión asociados con cada uno de los sistemas finales. Cada dirección de la conexión está representado por la concatenación de la dirección MAC (6 bytes) y la dirección LLC (1 byte). Cada dirección de conexión está clasificado como "destino" en el contexto de direcciones MAC/SAP de una trama exploradora enviadas en la primera trama usado para establecer un circuito o el "origen" en el contexto de las direcciones MAC/SAP origen .

Un circuito extremo a extremo está identificado por un par de identificadores ID del circuito. Un identificador ID del circuito es un número de 64 bits que identifica el circuito DLC dentro de un simple DLSW.

(00) Número de Versión	(01) Longitud de Cabecera=72
(02) Longitud de Mensaje	
(04) Correlación con el Enlace de Datos remoto	
(08) ID de Puerto de DLC remoto	
(12) Campo reservado	
(14) Tipo de Mensaje	(15) Byte de Control de Flujo
(16) ID de Protocolo	(17) Número de Cabecera
(18) Reservado	
(20) Trama más larga	(21) Banderas SSP
(22) Prioridad del Circuito	(23) Tipo de Mensaje
(24) Dirección MAC destino (Formato No-Canónico)	
(30) Dirección MAC origen (Formato No-Canónico)	
(36) SAP origen	(37) SAP destino
(38) Dirección de Trama	(39) Reservado
(40) Reservado	
(42) Longitud de Cabecera de DLC	
(44) ID de Puerto DLC origen	
(48) Correlación con Enlace de Datos origen	
(52) ID de Transporte origen	
(56) ID de Puerto DLC destino	
(60) Correlación con Enlace de Datos destino	
(64) ID de Transporte destino	
(68) Campo reservado	
(64) Campo Reservado	

Mensaje de Control

Fig. 1.1 Formato de Mensajes de Control

(00) Número de Versión	(01) Longitud de Cabecera=72
(02) Longitud de Mensaje	
(04) Correlación con el Enlace de Datos remoto	
(08) ID de Puerto de DLC remoto	
(12) Campo reservado	
(14) Tipo de Mensaje	(15) Byte de Control de Flujo

Mensajes de Información

Fig 1.2 Formato de Mensajes de Información

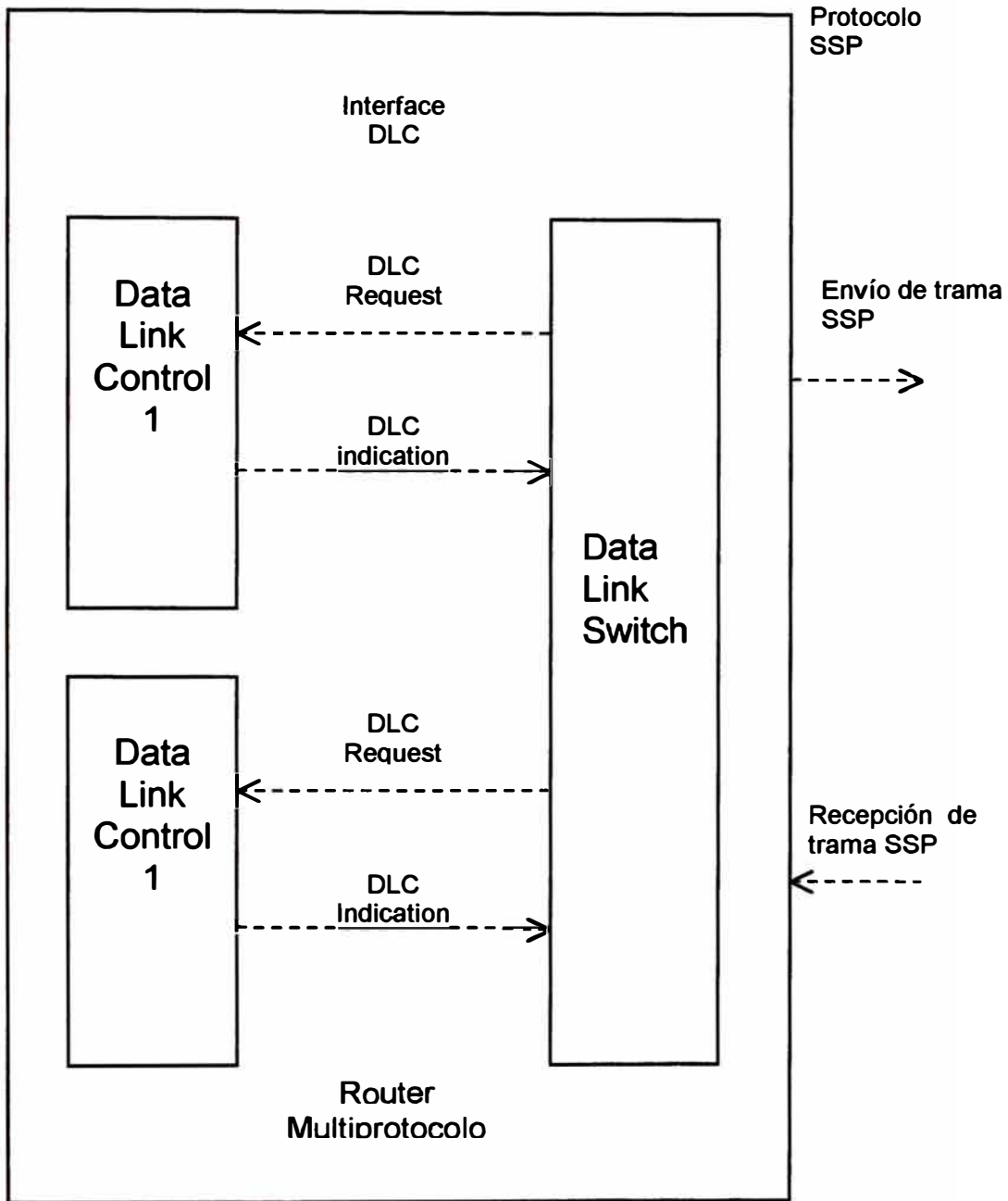


Fig 1.3 Diagrama del Sistema DLSW

CAPITULO II CONSIDERACIONES DE DISEÑO DE REDES

2.1 Topología

2.1.1 Uso del modelo NBMA para acceso

La conectividad en el corazón de la red amplia es crítica. En tratados acerca de topologías, el modelo NBMA (Non Broadcast Multiaccess) en frame relay es una topología que se ajusta mejor al nivel de acceso ofreciendo mejor costo-beneficio, no sucede lo mismo cuando se aplica en el corazón de la red amplia. Es decir que es más conveniente usarlo en el área de acceso que usarlo en el corazón de la red amplia.

2.1.2 Uso del modelo jerárquico para escalar

Muchos modelos con capacidad de escalamiento en una red frame relay fueron examinados (ver Fig. 2.1). El objetivo es proveer una conectividad de bajo costo y alto beneficio para un gran número de nodos. Los modelos que se tienen son:

- Malla completa.
- Malla Parcial.
- Malla Jerárquica (ver Fig. 2.2).
- Malla Híbrida.

2.1.3 Escalamiento limitado con malla completa NBMA

La conectividad que provee una malla completa en el modelo NBMA, presenta las siguientes ventajas:

- Conectividad completa con todos los protocolos.

- Retardo de salto simple entre ambos nodos.

Regla de Diseño: Usar el diseño de una malla completa NBMA para conectividad independiente del protocolo en pequeña escala.

El número de circuitos virtuales requeridos en una malla completa se incrementa como el valor al cuadrado del número de nodos de enrutamiento. Debido a que los proveedores de servicios cobran por cada circuito virtual, el costo se incrementa de acuerdo a la ecuación $N*(N-1)/2$. Cualquier flujo de transmisión denominado Broadcast copiando sobre-encabezados tiene la misma ecuación. Si el número de nodos se incrementa, la ruta de acceso rápidamente se congestiona debido al Broadcast.

Reglas de diseño: Restringir el número de nodos de enrutamiento en una configuración de malla completa frame relay. Se debe determinar la cantidad de tráfico debido a los protocolos de enrutamiento y otros paquetes de Broadcast.

2.1.4 Paquetes IPX SAP en una configuración malla completa NBMA

Los enrutadores con capacidad de manejar el protocolo IPX generan Broadcast de paquetes denominados SAP (Service Advertisement Protocol) cada 60 segundos. Siete paquetes SAP se concentran en un sólo paquete Broadcast denominado Broadcast SAP. Al calcular el número de paquetes SAP y multiplicarlos por el número de enrutadores nodales, se determina que los paquetes SAP usarán una cantidad sustancial de ancho de banda en el enlace de acceso.

Para lograr controlar los SAPs se tiene las siguientes reglas:

- Reducir el número de enrutadores peer de una topología NBMA.
- Filtrar los paquetes SAP con listas de acceso.
- Usar información SAP estáticos.

- Usar el protocolo Network Link State (NLSP).
- Usar protocolos de enrutamiento adecuados para IPX.

2.1.5 Configuración estrella de una malla parcial NBMA

Se debe usar una configuración en estrella si todos los nodos están conectados a un punto central. Con esta configuración el número de circuitos virtuales es minimizado. Las copias de Broadcast sólo están reducidos al enrutador central, convirtiéndose además el nodo central en un sólo punto de falla.

Una conectividad completa puede ser lograda en esta configuración sólo si el Split Horizont puede ser deshabilitado, otra alternativa puede ser usar rutas estáticas.

La replicación de broadcast en el nodo central es un factor limitante para la topología en estrella de malla parcial.

Para una conectividad completa, el nodo central viene a ser un punto principal de falla. Cabe mencionar que todo el tráfico entre los nodos debe ser decidido por el enrutador central mientras que todas las tramas son transmitidas dos veces a través de la red frame relay.

Reglas de diseño: No se debe usar un diseño en estrella de malla parcial con NBMA, a menos que la mayor parte del tráfico se dirija al nodo central o viceversa.

Existe otra opción de diseño: la estrella dual para una topología NBMA. En esta configuración todos los nodos tienen conectividad a dos nodos centrales, o a dos de los enrutadores en el nodo central. En este tipo de diseño no existe un único punto de falla, por lo tanto es una configuración que se encuentra entre una topología de malla completa y una topología en estrella (ver Fig. 2.3).

2.1.6 Configuración de malla jerárquica

La red NBMA frame relay puede ser escalada para un gran número de nodos usando una jerarquía de grupos NBMA. Cada grupo NBMA es mantenido con un número pequeño de peers. Cada grupo NBMA tiene una topología de malla completa permitiendo que todos los nodos tengan una conectividad total.

Algunas características del diseño de una topología de malla jerárquica son:

- Todos los protocolos tienen una conectividad completa.
- Los grupos de Broadcast NBMA son mantenidos pequeños.
- Los circuitos virtuales son requeridos en pequeña cantidad.
- El tráfico está localizado en el nivel de acceso.
- Las listas de acceso y filtros son implementados en el nivel central.

Regla de diseño: El uso de una malla jerárquica permite escalar en una red frame relay NBMA (ver Fig. 2.4).

Las desventajas a considerar en esta topología son:

- Las tramas pueden cruzar la red frame relay 3 veces.
- La configuración de una malla jerárquica es complicada.
- El mantenimiento de una red jerárquica es también complicada.

2.1.7 Configuración de malla híbrida

Los accesos frame relay son de bajo costo y gran rendimiento, el objetivo de un diseño de malla híbrida es usar pequeños grupos NBMA en el nivel de acceso y circuitos en malla punto a punto en el núcleo de la red WAN. Las ventajas de esta topología son:

- Conectividad completa con una malla parcial en el núcleo de la red WAN.
- Enrutamiento robusto en el núcleo de la red WAN.

- Uso del frame relay para acceso de bajo costo y alto beneficio a los nodos remotos.
- Escalabilidad mientras los grupos NBMA se mantienen pequeños.
- Uso de diseño jerárquico para controlar el tráfico en el nivel de acceso.
- Minimiza el número de circuitos virtuales requeridos.

Regla de diseño: El uso de una malla híbrida con un frame relay NBMA provee un acceso frame relay de bajo costo y gran beneficio y un núcleo robusto de la red.

2.1.8 Escalamiento apropiado en una topología de malla híbrida

Puede resultar muy costoso construir una adecuada malla parcial de circuitos dedicados punto a punto para el núcleo de la red WAN. Para obtener un escalamiento de bajo costo y alto beneficio se debe minimizar el alcance del núcleo.

2.2 Consideraciones de diseño de una red frame relay

La motivación para usar una red de conmutación de paquetes (frame relay) en una red WAN es el ahorro de dinero y reducción de retardos. En un escenario punto a punto donde se desea tener una topología de malla y se desea tener enlaces de redundancia, cada enrutador debe tener varios puertos físicos. Además, para llegar a un enrutador remoto se tienen que efectuar varios saltos (Hops) los cuales introducen retardos. Si se quiere reducir tales retardos, la topología adecuada es la malla completa (Full Mesh). Lamentablemente, empleando malla completa, el costo de los equipos de comunicaciones también se van a incrementar.

Concepto de Diseño: En el establecimiento de redundancia con un enlace punto a punto, se tiene que considerar un costo adicional para las interfaces

seriales y otros circuitos. El deseo de ahorrar dinero eliminando enlaces punto a punto puede causar elevados retardos y muchos saltos entre enrutadores ubicados en diferentes nodos.

El frame relay fue conceptualizado como una alternativa de bajo costo y alto beneficio para los enlaces punto a punto, donde cada nodo podía ser conectado a otro con un circuito virtual. En la actualidad cada enrutador requiere sólo una interface serial física conectada al proveedor de servicios. Los retardos en la red frame relay consiste de un sólo salto entre nodos. El retardo real en la nube frame relay depende de la tecnología a nivel físico. Algunos servicios de frame relay operan sobre Cell Switching (conmutación de celdas) ó ATM (Asynchronous Transfer Mode), los cuales producen bajo retardo. Frame relay es mayormente implementado por un proveedor como servicio de transporte, pero también puede ser usado en redes privadas (ver Fig. 2.8).

2.2.1 Dispositivos de acceso frame relay

Frame Relay es una red de datos de conmutación de paquetes, que fué diseñado para ser un enlace de datos más rápido que el X.25. El éxito de frame relay fue debido a la gran mejora en los medios de transmisión de fibra óptica. Al igual que el X.25, frame relay define la conexión entre un dispositivo cliente DTE (Data Terminal Equipment) y un dispositivo de red DCE, el DTE es típicamente un enrutador y el DCE (Data Circuit-Terminating Equipment) es un conmutador frame relay, el DTE y el DCE se refieren al nivel de enlace de datos, no al nivel físico. Las velocidades de acceso es a 56Kbps, 64Kbps ó 1.544 Mbps.

La unidad del servicio frame relay es el Circuito Virtual Permanente (PVC). El circuito PVC está identificado por un identificador de conexión (DLCI), siendo el número DLCI un identificador local entre el DTE y el DCE, el contrato del DLCI

(Data Link Connection Identifier) especifica el CIR (Committed Information Rate) proveído por el proveedor.

Concepto de diseño: el número DLCI se refiere a un circuito PVC, y es una configuración local.

2.2.2 Obtención del direccionamiento global

Los proveedores del servicio de frame relay deben ofrecer un sistema de direccionamiento local, el sistema de direccionamiento global es simplemente una conveniencia, no tiene efecto en la funcionalidad del enrutador, cada nodo usa el mismo número de circuito PVC para comunicarse a un nodo señalado con un direccionamiento global, el límite del direccionamiento global que limita la red de frame relay es de 972 DLCI, representando 972 nodos ó conexiones físicas.

La configuración de los enrutadores puede ser realizada de manera fácil con el direccionamiento global. Un simple archivo de configuración puede ser usado para lograr un mapa de los números DLCI a las direcciones destinatarias.

El contrato por el servicio de frame relay especifica una serie de parámetros. Cada proveedor de servicios implementa los contratos de diferentes maneras, los elementos típicos incluyen:

Access Rate (Ar)

- Típicamente 64 Kbps ó 1.544 Mbps.

Committed Information rate (CIR)

- Ancho de banda garantizado del circuito PVC.

Committed Burst Limit (Bc)

- Datos aceptados por el conmutador a la velocidad de acceso (access rate).
- Determinados por el espacio de buffer usados para el circuito PVC.

Excess burst limit (Be)

- Datos en exceso aceptados por el conmutador a la velocidad de acceso.
- Determinados por el exceso de espacio de buffers usados para el circuito PVC.

Maximum data rate (MaxR)

- Obedece a la fórmula $(Bc+Be)/Bc \times CIR$.

Concepto de diseño: El conmutador del proveedor de frame relay debe colocar el bit de discard eligibility DE en las tramas que han excedido el CIR.

2.2.3 Control de flujo por descarte proporcional de paquetes

Normalmente el control de flujo del frame relay consiste en el descarte de paquetes en el conmutador o en el enrutador. Esto es similar al control de flujo sobre otros medios LAN ó WAN. Este control es responsable de comunicar a los servidores centrales para que retarden la transmisión ó reduzcan el tamaño de ventana de transmisión. Muchos servidores realizan una contención en el enlace de frame relay mientras que los enrutadores ponen en cola todo el tráfico. Cuando la capacidad de acceso en el enlace es excedida, el enrutador simplemente descarta los paquetes una vez que la cola de salida (Output Queue) está completamente llena. El descarte de paquetes está en proporción a la velocidad con la cual los servidores se encuentran enviando información. El enrutador no usa el CIR para determinar el descarte de paquetes.

Este tipo de control de flujo trabaja bien con protocolos inteligentes tales como el TCP/IP que se ajustan al CIR. El estándar para el control de flujo del frame relay aún no ha sido decidido, muchos vendedores han implementado esquemas propietarios por lo que diferentes circuitos virtuales PVC tienen diferentes niveles de prioridad.

2.2.4 Uso de la notificación de congestión explícita

Las redes frame relay pueden indicar congestión en un circuito virtual con el bit denominado Forward Explicit Congestion Notification (FECN) y el bit Backward Explicit Congestion Notification (BECN), esto es una indicación que el CIR ha sido excedido ó que las facilidades han sido compartidas y los conmutadores están sobrecargados. En los casos de ocurrencias de congestión se ha observado que no es de tiempo prolongado y que rápidamente es resuelto, por lo que muchas veces los servidores no han tenido tiempo de reaccionar.

Como se ha mencionado en el caso del enrutador, el protocolo TCP realiza un control independiente y no responde a los bits de notificación de control de congestión.

2.2.5 Enrutamiento dinámico en frame relay

El número de enrutadores peer intercambiando las actualizaciones de rutas en una red local es típicamente pequeño, existe un límite práctico para escalar los grupos de enrutadores que envían intercambios de actualización de rutas o intercambio de paquetes denominados Hellos, de tal manera que si el número de enrutadores peers incrementa, el ancho de banda y el uso de recursos del CPU destinados al procesamiento de rutas se incrementa.

Para el enrutamiento dinámico sobre el Frame Relay, el procedimiento es el siguiente se copia cada paquete de enrutamiento sobre cada enrutador peer usando un número elevado de ancho de banda, se debe mantener un tráfico de Broadcast menor que el 20% del ancho de banda del enlace. Esto limita el número de enrutadores peers que pueden intercambiar tablas de rutas.

El DLCI es un campo de 10 bits. Algunos de los número DLCI son reservados para señalización y direccionamiento de grupos. Se debe tener en cuenta que los

conmutadores de los proveedores no tengan limitaciones de DLCI. Los límites de configuración de DLCI en los enrutadores dependen de la capacidad del enrutador. El enrutador debe copiar los broadcast en cada circuito PVC, es decir si el número de circuitos PVC se incrementa, la sobrecarga de broadcast ocupa mayor ancho de banda del acceso.

Concepto de diseño: Mantener el número de enrutadores peer en un número pequeño cuando se está realizando enrutamiento dinámico sobre frame relay, y las actualizaciones de rutas deben consumir menos que el 20% del ancho de banda del enlace.

2.2.6 Uso de protocolos de enrutamiento dinámico

El uso de protocolos de enrutamiento que sólo advierten cambios para reducir la cantidad de tráfico de Broadcast en una red con gran número de enrutadores conectados en configuración multipunto es necesario. Se debe además considerar los efectos del enrutamiento de paquetes Hellos, Keepalives y todos los demás tipos de Broadcast, considerando que siempre se deben encontrar ocupando menos del 20% del ancho de banda del enlace.

2.2.7 Priorización del frame relay

La priorización sobre el frame relay no ha sido estandarizado. El enrutador puede priorizar sobre el acceso del ancho de banda. Para ser óptimo, la prioridad tendría que extenderse a lo largo de todo el recorrido del circuito PVC, una posibilidad es usar el bit DE para señalar las tramas de menor prioridad, los equipos de diferentes proveedores han implementado esquemas de priorización propietarios.

2.2.8 Compatibilidad de señalización del enrutador y la red

La especificación original de señalización de frame relay es llamado Link Management Interface (LMI). LMI fue propuesto por el Frame Relay Forum. Consecuentemente, el ANSI y el CCITT han estandarizado el LMI con algunas variantes. El dispositivo enrutador ha escoger debe soportar las tres versiones por lo tanto se puede usar cualquiera de las especificadas por el proveedor :

Frame Relay Forum	Link Management Interface (LMI).
CCITT	Y.122 Arquitectura de las Tramas. Q.922 Transferencia de Datos. Q.933 Annex A Señalización.
ANSI	T1.606 Arquitectura de las Tramas. T1.618 Transferencia de Datos. T1.617 Annex D Señalización.

2.2.9 Enlace punto a punto que provee compatibilidad completa

Los enrutadores pueden ser configurados en punto a punto virtual en la red WAN. Cada enlace tiene un mapa a una red ó una subred. Cuando un enlace falla, los protocolos de enrutamiento se ajustarán. Una conectividad completa de protocolo es mantenido para todos los protocolos en una malla parcial.

Conceptos de Diseño: Los protocolos tienen conectividad completa en una malla parcial. Se debe mantener una configuración punto a punto virtual en la red WAN

2.2.10 Broadcast inherente en redes LAN

Los protocolos de red entienden el Broadcast de la red local. Los Broadcast a nivel de direcciones MAC y Multicast son inherentemente soportados por todas las redes locales.

Conceptos de diseño: Los enrutadores y protocolos de red usan los mecanismos de Broadcasting de redes LAN.

2.2.11 Multiacceso de tipo No Broadcasting

Los enrutadores conectados a una malla de circuitos de Frame Relay pueden ser modelados como una red o una subred. Sin embargo, la red frame relay misma no soporta Broadcasting. Para simulación de una red LAN, la red frame relay está configurado como una malla completa de circuitos virtuales PVC entre los enrutadores peers. Cada Broadcast es copiado a cada peer. Esto es conocido como el modelo multiacceso de tipo no broadcast NBMA.

El copiado de Broadcast tiene dos mayores impactos:

- El procesador del enrutador tiene que copiar cada Broadcast.
- Cada copia es transmitida sobre el mismo enlace de acceso.

Regla de diseño: El modelo mencionado limita la escalabilidad del grupo de enrutadores conectados.

2.2.12 Métricas de enrutamiento que no se basan en el CIR

Los protocolos de enrutamiento inteligentes realizan decisiones de enrutamiento basados en el ancho de banda, saltos o alguna otra métrica. En el modelo NBMA, los enrutadores no pueden asignar diferentes métricas a cada circuito PVC. Un ancho de banda por defecto de 56 Kbps es asignada a cada circuito PVC frame relay. Otras medidas de enrutamiento son derivados de este ancho de banda.

Concepto de diseño: El ancho de banda de cada PVC es 56 Kbps sin importar el CIR que se ha escogido.

2.2.13 Subinterfaces frame relay

Las subinterfaces son una característica del sistema operativo de los enrutadores Cisco (usados en la presente solución) que facilitan una configuración frame relay y escalamiento mucho mas fácil, denominándose enrutamiento de circuito virtual.

Con la configuración de las subinterfaces, cada circuito virtual PVC genera un mapa a una diferente red o subred. El resultado es que el frame relay trabaja al igual que enlaces punto a punto, las subinterfaces frame relay son mapas a líneas dedicadas.

La configuración de subinterfaces elimina mucho de los problemas y complejidad de la red NBMA permitiendo una completa conectividad con configuraciones de malla parcial con los siguientes protocolos:

- IPX RIP y SAP.
- AppleTalk.
- DECnet.
- CLNS.

Los protocolos de red y protocolos de puente realizan un mapa directamente a circuitos permanentes virtuales. Lográndose:

- El Split Horizon no es más un problema.
- Los problemas con OSPF son eliminados.

Los protocolos de enrutamiento son generalmente mas efectivos con circuitos punto a punto virtuales. Los siguientes son algunos de los beneficios que podemos mostrar:

- Las métricas de rutas son determinados basados en los circuitos virtuales PVC.
- Las estadísticas son coleccionados en base a los circuitos virtuales.
- Las listas de acceso se aplican en base a cada uno de los circuitos virtuales.
- Múltiples protocolos son soportados en un circuito virtual.

Regla de diseño: El uso de subinterfaces facilita un mejor control y enrutamiento a nivel de red.

2.2.14 Conmutación frame relay

Un enrutador Cisco puede ser configurado como un conmutador frame relay. el enrutador puede ser configurado como un DCE, DTE o NNI.

Las configuraciones del conmutador frame relay puede ser local o remoto. Como un conmutador frame relay local, el enrutador conecta directamente circuitos PVC en dos interfaces seriales. Los circuitos virtuales PVC son estáticamente direccionados, el enrutador es normalmente configurado como un DCE para un conmutador local.

Las interfaces seriales son dedicadas al tráfico frame relay. Siendo imposible tener otros tipos de encapsulamiento al mismo tiempo.

El enrutador puede funcionar como un conmutador frame relay remoto. En esta configuración, un túnel con encapsulamiento genérico de ruta se conecta al enrutador. Las tramas frame relay son encapsuladas en datagramas IP y son enrutadas a través de la red IP.

El conmutador frame relay remoto puede ser usado para construir una red frame relay privada. Esta conmutación también es usual cuando el proveedor sólo soporta IP y puede tener el servicio frame relay disponible a sus clientes por encapsulamiento de datos en IP.

Las características de un frame relay remoto:

- Los circuitos virtuales PVC son normalmente enrutados en el conmutador frame relay. La performance del backbone IP esta determinado por la velocidad del conmutador IP. Si el backbone es *silicon switched*, el encapsulamiento de tramas frame relay son conmutados a través de un núcleo IP.
- Un conmutador frame relay local puede ser combinado con un conmutador frame relay remoto para realizar una red frame relay privada flexible.

2.3 Consideraciones de diseño de la red X.25

X.25 es una red de datos de paquetes, las redes X.25 pueden ser públicas o privadas. Las redes públicas son conocidas como redes públicas de datos (PDN). En sus inicios estas redes fueron construidas sobre circuitos análogos no muy eficientes. La eficacia fue incorporada en el nivel de enlace de datos y nivel de red .

El X.25 usa el protocolo de enlace de datos denominado Link Access Procedure Balanced (LAPB). El protocolo de nivel de paquete también provee circuitos virtuales que mantienen la integridad de datos en el nivel de red. Debido a que usa un protocolo complejo de ventana corrediza en sus dos niveles, las redes X.25 tienen bajo throughput y alta latencia comparado con frame relay. Cada circuito virtual tiene su propio control de flujo de ventana corrediza en el nivel de X.25. La ventana es local entre el PAD (Packet assembler/diassembler) y el conmutador X.25.

Los servicios de X.25 son disponibles en muchos países, para una conexión internacional de conectividad X.25 se proveen dispositivos bajo normas X.75.

2.3.1 Uso de circuitos X.25 como enlaces de datos WAN

Un PAD X.25 ó un enrutador es un DTE lógico, el DCE lógico es un concentrador ó un conmutador localizado en el proveedor. En internetworking, el circuito virtual X.25 es usado igual que un enlace de datos. La red X.25 es utilizado con este propósito porque el protocolo de transporte de datos, al igual que el TCP provee transferencia integral de datos. Los enrutadores usualmente realizan una llamada X.25 para formar un circuito SVC (Switched Virtual Circuit) con otros enrutadores. Cada uno de los enrutadores son identificados por una dirección X.121, existe un mapa de direcciones que relacionan X.121 con la dirección del protocolo (ver Fig. 2.9).

Conceptos de Diseño : Los enrutadores usan los circuitos virtuales X.25 como enlaces de datos para transportar tráfico de múltiples protocolos.

2.3.2 Uso del modelo NBMA para acceso de bajo costo

Es una posibilidad de configuración al igual que las redes frame relay, permite el establecimiento de enlaces X.25 a cada uno de los enrutadores remotos, a diferencia de las redes LAN, las actualizaciones de rutas se realizan mediante copias a cada una de las interfaces virtuales.

Reglas de diseño : Usar NBMA X.25 para un acceso de bajo costo y gran eficiencia ó para transmisión de datos que mantienen integridad de información.

2.3.3 Uso de subinterfaces

Otra de la opciones que se puede escoger es el uso de subinterfaces que mejoran la configuración X.25. Cada subinterface es configurado como una subred ó red diferente. El circuito virtual X.25 actúa al igual que un enlace punto a punto. La principal ventaja de subinterfaces punto a punto es la capacidad robusta de enrutamiento. Las configuraciones de subinterfaces elimina los temas

del modelo NBMA relacionados a la conectividad de una malla parcial y Split Horizon.

Reglas de diseño: Cuando toda la plataforma se basa en enrutamientos basados en circuitos virtuales X.25 se debe usar el sistema de enrutamiento robusto que provee las subinterfaces.

2.4 Consideraciones de diseño de ISDN

La Red Digital de Servicios Integrados (ISDN) fué desarrollado por las compañías telefónicas con la intención de crear una red digital total. Los servicios ISDN incluyen lo siguiente:

- Equipo Terminal 1 (TE1) - Designa un dispositivo que es compatible con una red ISDN. Un TE1 conecta a una Terminación de Red tipo 1 ó tipo 2.
- Equipo terminal 2 (TE2) - Designa un dispositivo que no es compatible con ISDN y requiere de un adaptador de terminal.
- Adaptador de Terminal (TA) - Convierte señales eléctricas estandares en el formato usado por ISDN de tal manera que dispositivos que no son ISDN pueden ser conectados a una red ISDN.
- Adaptador de Red tipo 1 (NT1) - Conecta el cableado de 4 hilos ISDN del usuario a la facilidad convencional del loop local.
- Adaptador de Red tipo 2 (NT2) - El tráfico directo desde y hacia los diferentes dispositivos del usuario y el NT1. El NT2 es un dispositivo inteligente que realiza conmutación y concentración.

Los puntos de referencia de interface ISDN incluyen lo siguiente:

- La interface S/T define la interface entre el TE1 y el NT. La interface S/T es también usado para definir la interface entre el NT y el TA.
- La interface R define la interface entre el TE2 y el TA.

- La interface U define la interface de dos hilos entre el NT y la nube ISDN.

2.4.1 Interfaces BRI y PRI de ISDN

La interface BRI (Basic Rate Interface) es muchas veces escrito como $BRI=2B+D$. La interface provee dos canales B (Bearer) de 64 kbps y uno adicional de 16 kbps denominado canal de señalización (canal D). Los canales B transportan datos de usuario. El canal de señalización transporta información de control, así como establecimiento de llamada y señales de terminación de llamada.

La interface PRI (Primary Rate Interface) ofrece 23 canales de 64 kbps de datos y un canal de señalización en los Estados Unidos (23B+D). Para Europa y muchos países del resto del mundo, la interface PRI ofrece 30 canales de datos y uno de señalización. El primero es debido a las facilidades T1 y el segundo a facilidades E1 (ver Fig. 2.10).

Después de que la llamada ISDN ha sido establecida, el enrutador puede usar ISDN para transportar cualquier protocolo de nivel superior a múltiples destinos.

Los siguientes son soportados:

- IP.
- IPX.
- AppleTalk.
- Banyan Vines.
- DECnet Phase IV.
- OSI.

Un administrador puede seleccionar protocolos tales como HDLC, PPP. La opción PPP habilita el protocolo CHAP (Challenge Handshake Authentication Protocol), un método estándar y popular para control de llamadas.

Adicionalmente pueden ser soportados encapsulaciones X.25, LAPB y Frame Relay (ver Apendice A.2).

Una de las características para mantener una conectividad intermitente es el conocido Dial on Demand Routing (DDR). El DDR abre un canal B ISDN en respuesta a un paquete interesante. Un filtro de lista de acceso puede ser usado para determinar que paquetes son interesantes.

Si un paquete que no es interesante arriba después de un tiempo configurado, el enlace DDR será interrumpido. Cuando múltiples nodos remotos están tratando de establecer una comunicación, se debe usar encapsulación PPP con CHAP de tal manera que el nodo remoto pueda ser identificado cuando la llamada se realice.

Reglas de Diseño: Se debe usar PPP con CHAP de tal manera que el nodo remoto pueda ser identificado, adicionalmente se debe usar el ancho de banda de ISDN de acuerdo a la demanda para proveer un canal de acuerdo a necesidad.

2.4.2 Flexibilidad del ISDN con agregación de canal B

Algunos enrutadores, en especial Cisco Systems soportan ancho de banda en demanda (BOD). Cuando el primer canal B alcanza el límite de tráfico configurado, el segundo canal es establecido. Los dos canales forman un grupo de canales obteniendo 128 kbps. El denominado MPP es un nuevo estándar del Internet Engineering Task Force (IETF). Este detalle está especificado en el RFC 1717. El MPP no especifica como un enrutador debería cumplir el proceso de usar un canal B ISDN extra, en este caso se busca asegurar que los paquetes arriben en la secuencia necesaria al enrutador de recepción. Para cumplir, los datos encapsulados en PPP y el datagrama poseen un número de secuencia. Adicionalmente, MPP provee la habilidad de segmentar paquetes de datos antes

de la encapsulación para mejorar la performance del resecuenciamiento y reensambleje en el nodo final.

Las principales metas de un diseño de ISDN son las siguientes:

- Conservar el Ancho de Banda.
- Manejo de Tarifa/Enlace.

Desde que ISDN es un servicio que se basa en el consumo, el diseño debe ser implementado para limitar el uso del enlace ISDN.

2.4.3 Nodos remotos con interface BRI a nodo central PRI

En este diseño, una LAN del nodo remoto Ethernet o Token Ring accesa a un recurso central vía sesiones BRI a PRI. Cada enrutador en el nodo remoto está equipado con un servicio BRI que ofrece dos canales de 64 kbps para datos. Uno ó ambos canales B pueden ser usados para conectar a un enrutador en el nodo central.

En el nodo central, las llamadas que llegan terminan en un enrutador central equipado con enlace T1 ó E1.

El diseño es similar a los precedentes diseños, aunque el enfoque en este caso es una simple conectividad. Existen tipos de enrutadores que ofrecen a bajo costo interfaces Ethernet e ISDN, que soportan enrutamiento IPX, IP, AppleTalk y Bridging para otros protocolos. De acuerdo a las dimensiones y requerimientos de tráfico se encuentran disponibles diferentes opciones de enrutadores.

Una interface BRI puede ser usado para proveer un enlace alternativo vía línea conmutada para un enlace dedicado. El ISDN es una manera de obtener un enlace de bajo costo y gran beneficio que provee 64 kbps o más ancho de banda. El enlace de respaldo es disparado cuando una línea dedicada presenta una falla o alcance los límites de una carga de transmisión configurada (ver Fig. 2.11).

El enlace primario y el de respaldo permanecen en diferentes direcciones de subredes. La interface ISDN es configurada en modo pasivo con respecto al protocolo dinámico de enrutamiento. Una alternativa al ISDN es una línea telefónica análoga. Un módem dispara una conexión cuando el enrutador pone en activo la señal DTR (Data Terminal Ready).

Una simple interface PRI provee enlaces de respaldo hasta 23 (T1) y 30 (E1) nodos remotos, cada nodo remoto puede contar con un enlace BRI, esta configuración provee una estrategia densa y respaldo costo-beneficio.

Reglas de Diseño: Usar la interface primaria ISDN para proveer respaldo para muchos nodos remotos.

2.5 Consideraciones del direccionamiento IP

2.5.1 Direccionamiento jerárquico

Daremos un rápido panorama acerca de un sistema de direccionamiento jerárquico, prefijo de enrutamiento, direccionamiento sin clases y máscaras de subredes de longitud variable. Estos no son conceptos nuevos, la arquitectura telefónica ha manejado prefijos de enrutamiento por muchos años. Un conmutador telefónico en Arequipa no necesita conocer como llegar a una línea específica en Huancayo. Sólo requiere reconocer que la llamada no es local. El proveedor de larga distancia sólo requiere reconocer que el código 064 es para Huancayo y no requiere conocer los detalles de la línea en mención en Huancayo.

Bajo este panorama un enrutador sólo necesita saber cuál es el próximo salto (Hop), no es necesario saber los detalles de cómo alcanzar el nodo final que no es local.

De manera similar al ejemplo de telefonía. Los enrutadores IP también realizan decisiones jerárquicas. Una dirección IP consiste de una parte denominada prefijo

y una parte denominado hosts (dirección de los puntos de servidores y estaciones en la red LAN). Los enrutadores usan el prefijo para determinar el camino para una dirección destino que no es local. La parte de host es usado para alcanzar las estaciones y servidores locales (ver Fig. 2.5).

Un prefijo identifica un bloque de número de host y es usado para enrutamiento de este bloque. De acuerdo al RFC 1518, un prefijo es “una dirección IP y alguna indicación del bit significativo más izquierdo dentro de esta dirección”. La indicación del bit significativo más a la izquierda ha sido tradicionalmente usado como una indicación de la clase de dirección y una máscara de subred.

La especificación original IP, en el RFC 760, no usa clases. El número de red fué definido como el primer octeto, el primer octeto fué un prefijo.

Las tres direcciones IP de clientes definen un prefijo de cierta longitud.

- Una dirección clase A tiene una longitud de prefijo de 8.
- Una dirección clase B tiene una longitud de prefijo de 16.
- Una dirección clase C tiene una longitud de prefijo de 24.

La longitud del prefijo fué variada aún antes de que los conceptos de subredes fueran introducidos. La longitud del prefijo puede ser determinado por los primeros bits en una dirección, el cual identifica la clase de dirección.

- Una dirección clase A siempre comienza con 0.
- Una dirección clase B siempre empieza con 10.
- Una dirección clase C siempre empieza con 110.

Un prefijo es una dirección IP y una indicación del bit significativo de la izquierda dentro de la dirección, el prefijo fue convencionalmente realizado con una máscara de subred. Ultimamente, la indicación de longitud se ha realizado del número de red y un slash, por ejemplo 192.10.168.0/21. Tradicionalmente los números IP

hosts conocieron sólo tres longitudes de prefijos: 8, 16 y 24. Para entender que la longitud del prefijo local es extendido, se debe usar un valor denominado máscara de subred.

Los hosts tienen una habilidad limitada para entender las longitudes del prefijo. Ellos conocen la longitud para la configuración local pero no de las configuraciones remotas. Tradicionalmente enrutamiento de clase completa no transmiten ninguna información acerca de la longitud del prefijo.

2.5.2 Enrutamiento sin clases

Esta técnica es conocida como VLSM (Variable-Length Subnet Masking) y provee información de la longitud del prefijo explícitamente con cada uso de una dirección. El prefijo es evaluado independientemente en cada lugar que es usado. Esto no difiere del enrutamiento tradicional, donde la máscara de la subred dentro de una red es ocultado para las redes externas dentro de una interred (ver Fig. 2.6).

La habilidad de tener diferentes prefijos de dirección en diferentes puntos soporta un uso más eficiente de los espacios de direcciones IP y reduce el tráfico de enrutamiento.

El uso de VLSM permite un uso más eficiente de los espacios de direcciones permitiendo un gran número de subredes con pequeños bloques de direcciones. La mejor manera de usar VLSM es primero realizar una subred del espacio de dirección completamente usando una máscara fija de subred. Por ejemplo, tomar un bloque clase B con una subred de 8 bits de máscara. Después, tomar una de las subredes y proceder a separar una subred con una máscara extendida. Si una pequeña subred es agrupada, la información de rutas puede ser consolidada. La consolidación óptima ocurre con bloques contiguos de direcciones en

potencias de dos. Por ejemplo, direcciones de 4, 16, ó 512 pueden ser representados por una simple entrada de rutas.

El uso de VLSM es típicamente para numerar líneas seriales, cada línea serial requiere de un número de subred, necesitando sólo dos direcciones de host, si se escoge una subred de clase completa entonces el gasto de direcciones tratando de numerar sólo dos puntos es demasiado.

2.5.3 Resumen de rutas

El resumen de rutas es denominado Aggregation y Supernetting. El resumen de rutas se refiere a ubicar múltiples direcciones IP de manera que permita el resumen a un número pequeño de entradas en la tabla de rutas. Reduciendo el uso de memoria en enrutadores y el tráfico de enrutamiento de protocolo. Para que un resumen de rutas opere correctamente se debe reunir (ver Fig. 2.7):

- Múltiples direcciones IP deben compartir el mismo orden de los bits de mayor significado.
- Las tablas de rutas y los protocolos deben basar sus decisiones de enrutamiento en direcciones IP de 32 bits y una longitud de prefijo que puede ser hasta de 32 bits.
- Los protocolos de enrutamiento deben soportar la longitud de prefijos con las direcciones IP de 32 bits.

Los protocolos RIP e IGRP siempre realizan un resumen de información de rutas por un número mayor de red. Ellos son denominados protocolos de enrutamiento de clase completa porque siempre consideran la clase de la dirección IP. Sin embargo, no es el camino más eficiente y flexible para agregar información de rutas. BGP4, OSPF y EIGRP pueden soportar prefijos de

enrutamiento reduciendo el número de rutas advertidas con las siguientes características:

- Una entrada de rutas debe coincidir con un bloque de dirección de host, subred ó red.
- Las tablas de rutas deben ser más pequeñas.
- La performance del conmutador debe ser más rápida.
- El tráfico del enrutamiento de protocolo es reducido.

Concepto de diseño: Los protocolos de enrutamiento con prefijo y sin clases permiten que bloques contiguos de hosts, subredes, y redes sean representados por una simple ruta.

2.5.4 Direcciones para redes privadas

La autoridad en asignación de direcciones IP Internet Assigned Numbers Authority (IANA) a reservado tres bloques de direcciones para redes privadas. Una empresa que decide usar direcciones IP de este espacio de direcciones, definido en el RFC 1597, puede ser realizado sin la autorización del IANA ó un Registro de Internet. Las direcciones pueden ser usadas por muchas redes particulares.

Una ventaja de usar direcciones privadas es que el espacio direcciones globalmente únicas son conservados para el resto de internet. El uso de direcciones privadas facilitan la flexibilidad en el diseño de una red, teniendo mayor cantidad de direcciones disponibles para asignar.

Rangos que se pueden usar:

10.0.0.0 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

2.6 Protocolos de enrutamiento

2.6.1 Categorías de los protocolos de enrutamiento

Existen muchos protocolos de enrutamiento especializados para IP, estos pueden ser caracterizados por la manera de uso.

- Efecto directo de enrutamiento de hosts.

Los hosts descubren el enrutador por defecto usando proxy ARP.

Configuración estática del enrutador puente.

Gateway Discovery Protocol (GDP) o ICMP Router Discovery Protocol (IRDP).

- Hot Standby Router Protocol (HSRP) característica de enrutadores Cisco.

- Protocolos de enrutamiento interno dentro de un sistema autónomo.

Routing Information Protocol (RIP).

Interior Gateway Routing Protocol (IGRP) y Enhanced IGRP.

IS-IS integrado.

Open Shortest Path First (OSPF).

- Protocolos de enrutamiento exterior entre sistemas autónomos.

Border Gateway Protocol (BGP).

2.6.2 La determinación de las rutas depende de las métricas

Los protocolos de enrutamiento determinan la mejor ruta a una red destino por intercambio de métricas de ruta. Aquí algunos ejemplos de las métricas de rutas:

- Conteo de saltos (Hop Count) RIP.
- Costo OSPF.
- Ancho de Banda y Retardo IGRP.
- Carga y Versatilidad, opciones de IGRP.

2.6.3 Uso de vectores de distancia

Los enrutadores usan un valor denominado **distancias administrativas** para diferenciar las fuentes de la información de rutas. Muchos protocolos de enrutamiento pueden proveer información de rutas para una red en particular al mismo tiempo usando métricas incompatibles. La determinación de rutas a una red remota, siempre usa las fuentes de información con el menor valor de las distancias administrativas. La distancia administrativa es igual a la medida de la **confidencia** en la fuente de la información. Una distancia administrativa es un valor entero hasta 255.

Los siguientes son ejemplos de valores de distancias administrativas:

Redes conectadas directamente	0
Rutas estáticas a una red	1
Rutas derivadas de BGP	20
Rutas derivadas de IGRP	100
Rutas derivadas de OSPF	110
Rutas derivadas de RIP	120

La distancia administrativa puede ser cambiada para favorecer a un protocolo de enrutamiento en especial o la fuente de información de rutas. Mientras que los enrutadores construyen sus tablas de rutas IP basados en las siguientes fuentes de información:

- Ingreso de rutas estáticas.
- Configuración de la interface local.
- Estado de la interface local.
- Estado de la señal CD (Carrier Detect).
- Contadores y temporizadores denominados Keepalives.

- Protocolos de enrutamiento dinámico y métricas de rutas.
- Address Resolution Protocol (ARP) y ARP Inverso.
- Redistribución entre protocolos de enrutamiento.
- Decisiones políticas implementados con listas accesos.

2.6.4 Uso de rutas estáticas

Una ruta estática es manualmente configurada como una entrada de rutas. Una ruta por defecto es un ejemplo de una ruta estática. Las rutas estáticas son preferidas a las aprendidas dinámicamente, porque ellos poseen un valor administrativo menor.

Las rutas estáticas pueden ser usadas para reducir el consumo de ancho de banda en enlaces WAN. El uso de rutas estáticas son recomendadas en el nivel de red si los enrutadores están conectados por un servicio tolerante a fallas tal como el X.25, este uso con X.25 permitirá ahorrar la carga de paquetes debido a la constante actualización de información de rutas.

2.6.5 Protocolo de enrutamiento EIGRP

El protocolo de enrutamiento Enhanced IGRP tiene muchas características favorable para construir inter-redes escalables:

- Soporte sofisticado basado en métricas de 32 bits.
- Fácil de instalar.
- Escala sin necesidad de sintonizar interredes de gran magnitud.
- Usa un protocolo de transporte eficiente.
- Convergencia dentro del lapso de un segundo de detección de la falla del enlace.

El protocolo Enhanced IGRP tiene módulos dependientes de protocolo que soportan el enrutamiento para IP, IPX y AppleTalk. El módulo IPX también soporta

el actual paquete Novell Service Advertisement Protocol (SAP). Cada protocolo cliente tiene sus parámetros separados tales como: Hellos, Timers y Métricas.

Un motor común de protocolo incluye el algoritmo Diffusing Update Algorithm (DUAL), descubrimiento de dispositivos vecinos y un protocolo eficiente de actualización de tablas, EIGRP mantiene tablas de enrutamiento separados y usa paquetes Hellos separados para descubrir enrutadores vecinos por cada protocolo DDP, IP e IPX.

Enhanced IGRP tiene propiedades de escalamiento y soporta redes de gran escala. Una alternativa para tener un sistema autónomo simple y extenso es usar un proceso separado para cada campus. Luego puede usarse el protocolo BGP (Border Gateway Protocol) ó un proceso diferente EIGRP para conectar los diferentes campus y formar así una red nacional ó internacional de gran escala.

El algoritmo que usa Diffusing Update Algorithm posee las siguientes características:

- Convergencia dentro del lapso de un segundo de detección de falla.
- Filtro de enrutamiento en cualquier nodo.
- Protocolo Hello previene los denominados agujeros negros.
- La actualización secuencial y confirmada (acknowledge) garantizan la convergencia.
- Propagación de información de rutas de nodos afectados.

Los denominados Hellos se transmiten cada 5 segundos y evitan los agujeros negros que originarían pérdida de información.

EIGRP soporta tres protocolos clientes:

- Interactúa con IGRP - soporta IP.
- Interactúa con IPX-RIP y IPX-SAP - Soporta IPX.

- Interactúa con RTMP - Soporta DDP.

EIGRP es individualmente habilitado por cada protocolo cliente, automáticamente redistribuye tablas de enrutamiento y SAPs a cada uno de los clientes. Por defecto, advierte actualizaciones completas de RIP, SAP y RTMP en interfaces de red LAN y realiza una eficiente actualización sólo en interfaces WAN.

En adición a una tabla de enrutamiento, EIGRP mantiene una tabla de rutas activa por cada enrutador adyacente, proporcionando al enrutador EIGRP un camino rápido para predecir cómo el enrutamiento cambiará cuando el estado de un enlace de red varíe.

Cuando el estado de un enlace cambia, el enrutador puede inmediatamente cambiar la tabla activa de enrutamiento basado en la información de una copia local de la tabla de rutas de vecinos, esto es denominado Computación Local, porque no afecta a otros enrutadores.

Cuando una tabla de enrutamiento de vecinos no posee un sucesor más adecuado, la computación denominada diffusing se lleva a cabo. El enrutador se pone en un estado de activo y procede a enviar requerimientos (queries). Este requerimiento se propaga hasta que la nueva ruta sea encontrada.

Otra de las características interesantes de EIGRP es la capacidad de realizar un resumen de rutas, esto va de la mano con un adecuado sistema de direccionamiento. De acuerdo a una topología jerárquica el resumen de rutas se lleva a cabo en el enrutador de frontera de la jerarquía. Esta capacidad permite disminuir el número de rutas en las tablas de enrutamiento, esto se debe a que se realiza un resumen de bloques de direcciones con un prefijo de enrutamiento que puede ser manualmente configurado. La técnica VLSM que es descrita en este

capítulo es soportado porque la información de máscaras de subredes es transmitido con la información de enrutamiento.

El mejor lugar para configurar un resumen manual de bloques contiguos es en el nivel de distribución ó nivel central. Para usar esta característica , bloques de direcciones son ubicados en el nivel de edificio ó campus.

La capacidad de usar un resumen de rutas e incluir información de prefijos en la información que se envía permite advertir entre subredes a través de una red mayor de diferente numeración, este es un caso de discontinuidad de red que no es resuelta por RIP ó IGRP.

La convergencia de la que hemos venido mencionando se produce de esta manera, el algoritmo DUAL permite que EIGRP pueda converger rápidamente, aquí la descripción de cómo sucede la convergencia:

1. La interface local es declarada con problemas (esto se realiza por detección de falla de portadora, una red Token Ring con Beaconing, tres veces los paquetes Hellos de 5 segundos sin respuesta para otros enlaces).
2. El enrutador se fija en las rutas locales y de adyacencias buscando una ruta alterna.
3. El enrutador cambia a la ruta alterna inmediatamente si ésta es encontrada localmente.
4. El enrutador envía requerimientos (queries) a los adyacentes, si ninguna ruta alterna es encontrada localmente.
5. El requerimiento se propaga hasta que una nueva ruta es encontrada.
6. Los enrutadores afectados actualizan sus rutas.

La convergencia de Enhanced EIGRP es rápida porque los cambios de información de rutas se propaga inmediatamente a los nodos afectados.

Una característica bastante usada de EIGRP, es el balance de tráfico, es decir soporta balance de tráfico de hasta cuatro rutas diferentes. Esto se puede realizar desarrollando las varianzas que es una característica de los protocolos de enrutamiento.

2.6.6 Distribución de direcciones para una red clase B

Las direcciones IP de internet se encuentran disponibles sólo para redes pequeñas debido a la baja disponibilidad de números de red, en la actualidad sólo se obtienen rangos de direcciones Clase C. Para optimizar el uso de bloques de direcciones se debe realizar una distribución adecuada de las direcciones, en este caso se puede seguir la siguiente metodología:

- Se debe estimar el número de subredes requeridas y duplicarlas.
- Estimar el número máximo de hosts en una subred.
- Asignar bits suficientes en cada terminación de los bits asignados localmente para hosts y subredes.
- Distribuir las diferencias para determinar la máscara.

Una variación de esta idea es determinar el promedio del número de hosts requeridos en una subred y usar este valor para determinar el número de bits de requeridos. Se debe usar una configuración de subinterfaces ó subredes secundarias para otorgar subredes adicionales cuando el número de hosts haya excedido el límite determinado.

2.6.7 Asignación de direcciones de subredes y hosts

La asignación de los números de subred se realiza desde la izquierda y las direcciones de hosts desde la derecha. Si existe poca disponibilidad de subredes se puede añadir un bit a la máscara. Si no existe disponibilidad de hosts, se puede substraer un bit de la máscara.

Cuando se ubica la cantidad de hosts, simplemente se realiza una cuenta binaria de los números de hosts comenzando desde el bit que se encuentra más a la derecha. Cuando se asigna números de subred, se realiza una cuenta binaria empezando desde el bit que se encuentra más a la izquierda. Este procedimiento es denominado *mirroring*.

De esta manera, no se obliga a usar máscaras discontinuas de subredes. Las máscaras discontinuas de subredes no son permitidas porque son incompatibles con los prefijos ó enrutamiento sin clases.

2.6.8 Enrutamiento sin clases de direcciones IP

Los protocolos RIP e IGRP siempre realizan un resumen de la información de enrutamiento de acuerdo a números de redes mayores. Son llamados protocolos de enrutamiento de clase completa porque siempre ponen atención a la clase de red IP. Esta no siempre es la manera más eficiente y flexible de agregar información de enrutamiento.

BGP4 usa Classless Inter-Domain Routing CIDR para agregar bloques de redes Clase C como una simple ruta. Esto reduce el número de rutas advertidas a través de la internet.

Similarmente, EIGRP y OSPF tienen la habilidad de soportar prefijos de enrutamiento. Si se encuentran correctamente configurados, bloques contiguos de subredes pueden ser consolidados como una simple ruta. Esta característica también se permite para rutas específicas de hosts. Si más de una entrada en la tabla de enrutamiento cumple con un destino particular, la mayor coincidencia de prefijos en la tabla de enrutamiento es usada.

Las características pueden ser:

- Las tablas de rutas pueden ser más cortas.

- La performance de conmutación puede ser más rápida.
- Una entrada de enrutamiento debe coincidir con un bloque direcciones de hosts, subredes o redes.
- Muchas rutas pueden coincidir con un destino, pero la mayor coincidencia es aplicada.

2.6.9 Máscaras de subredes de longitud variable

Las máscaras de subredes de longitud variable (VLSM) son típicamente usadas para numerar líneas seriales, cada línea serial necesita un número de subred. El VLSM hace más eficiente el uso de espacio de direcciones permitiendo grandes subredes y pequeñas subredes.

Se debe ser cuidadoso al asignar VLSM, porque es muy posible que se puedan originar conflicto de direcciones. Una manera segura de usar VLSM es primero lograr subdividir el espacio de direcciones usando un número fijo de máscara. Por ejemplo, subdividir una red mayor de clase B con una máscara de 8 bits. Siguiendo, tomar una red resultante y volver a subdividirlo con una máscara extendida. Si las pequeñas subredes son agrupadas, la información de enrutamiento puede ser consolidada.

Una consolidación óptima ocurre con bloques contiguos de direcciones en potencias de 2. Por ejemplo, pueden ser direcciones 4, 16 ó 512 representados por una simple entrada de ruta.

El uso de VLSM ahorra el uso de direcciones de subredes en una red WAN, esto es debido a que la conexión entre enrutadores sólo requiere de dos direcciones de hosts.

2.6.10 Enrutamiento de protocolos basados en vectores de distancia y estado de enlace

Una manera de caracterizar un protocolo de enrutamiento es por la información que es intercambiada entre dos entes.

Protocolos de enrutamiento basados en vectores de distancia:

- También conocidos como enrutamiento por rumores.
- Los enrutadores intercambian información conseguida de sus vecinos.

Protocolos de enrutamiento basados en Estado de Enlace:

- También conocidos como enrutamiento por propaganda.
- Los enrutadores sólo informan de las tablas conocidas acerca de los enrutadores conectados directamente.

Los protocolos de distancia pueden enviar una tabla entera por cada interface que posea. Cuando la información es recibida desde un vecino, la métrica local es añadida y las rutas son añadidas a la tabla local de enrutamiento. Todas las rutas de una tabla son transmitidas en actualizaciones periódicas ó en instantes de tiempo establecidos.

Los protocolos de estado de enlace transmiten el estado del enlace local a los vecinos. El denominado Link State Advertisement (LSA), propaga la información a cada vecino que pertenece a la misma área. Un enrutador puede recibir muchas copias de un LSA. La ruta tomada por los paquetes LSA es determinada por la adyacencia entre enrutadores.

Cada enrutador debe mantener una copia idéntica de la base de datos de los estados de los enlaces. La base de datos de los enrutadores de un área deben ser los mismos y no existe posibilidad de filtrado dentro de la misma área.

COSTOS Y RIESGOS

•Están los costos dentro del presupuesto?

•Son los riesgos manejables?

•Pensar en costos bajos

- Hardware
- Software
- Tiempo de asesoría

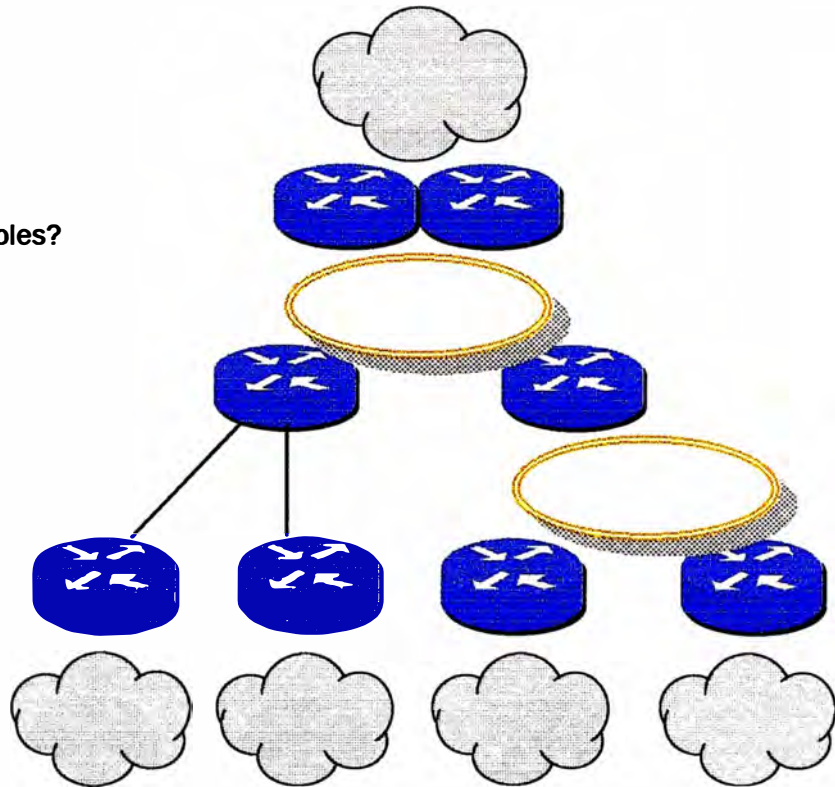


Fig. 2.1 Red de Topología Jerárquica

EL MODELO DESCRIBE LA TOPOLOGIA FISICA

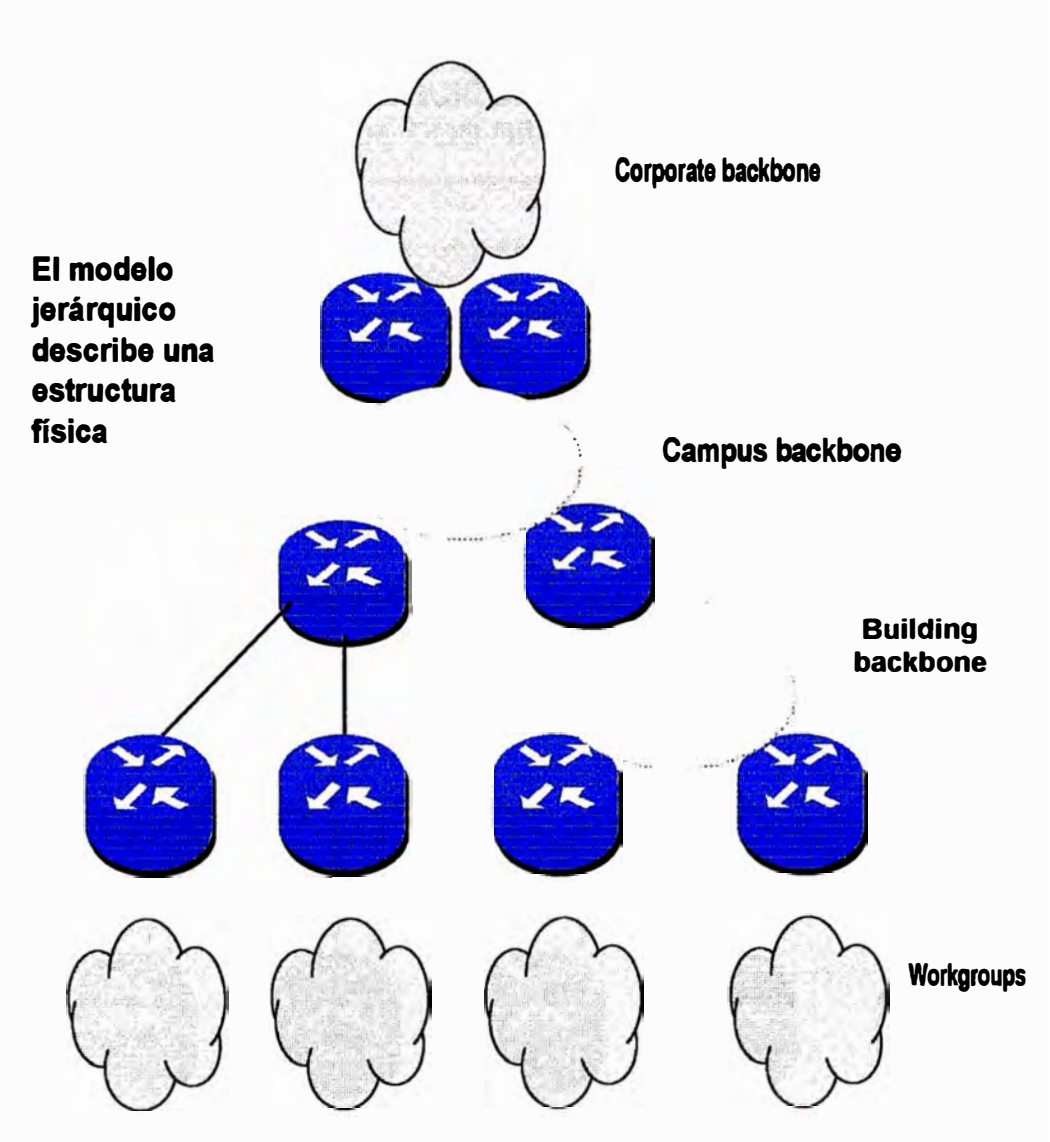
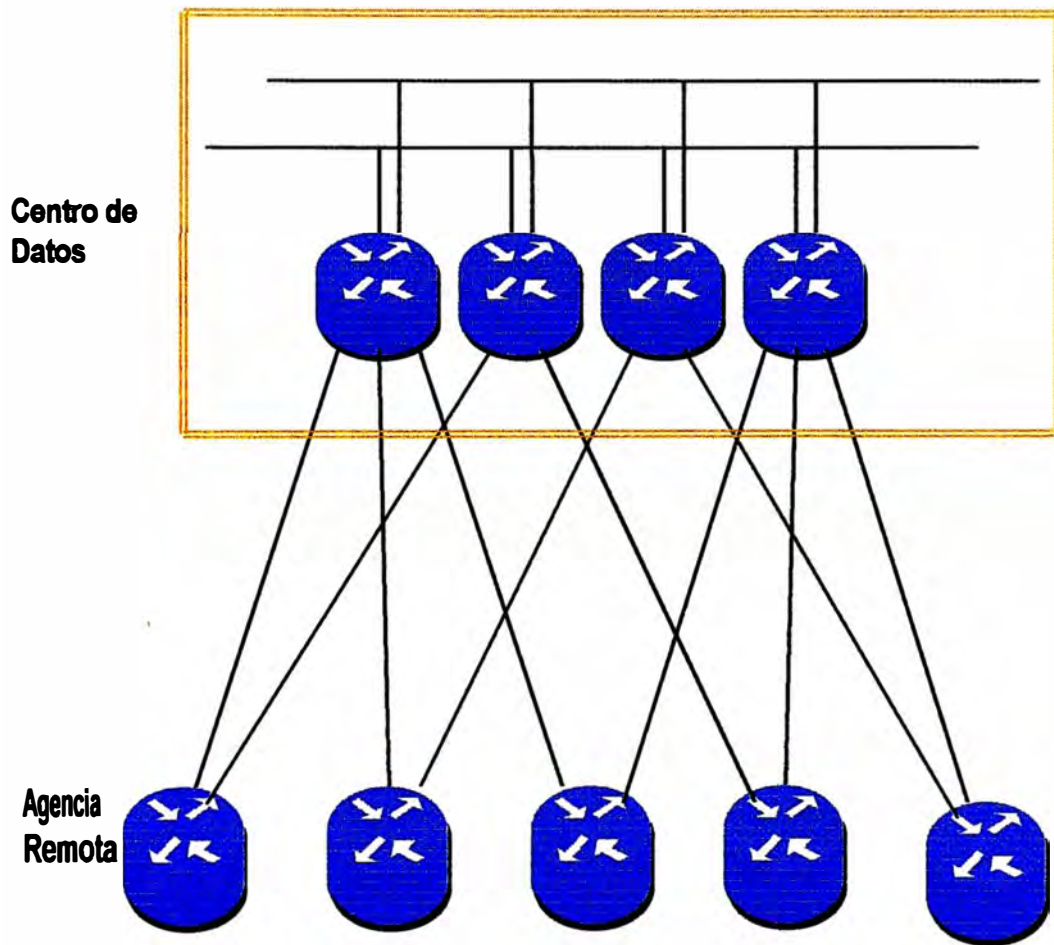


Fig. 2.2 Componentes del Modelo

MODELO JERARQUICO CON REDUNDANCIA DE DOS NIVELES



- **Uso de Redundancia**

Fig 2.3 Modelo Jerárquico con redundancia de dos niveles

IMPLEMENTACION DE ENRUTADORES

•Enrutadores en cada Nivel cumplen su función

•Características de enrutadores deben ser consistentes en cada nivel

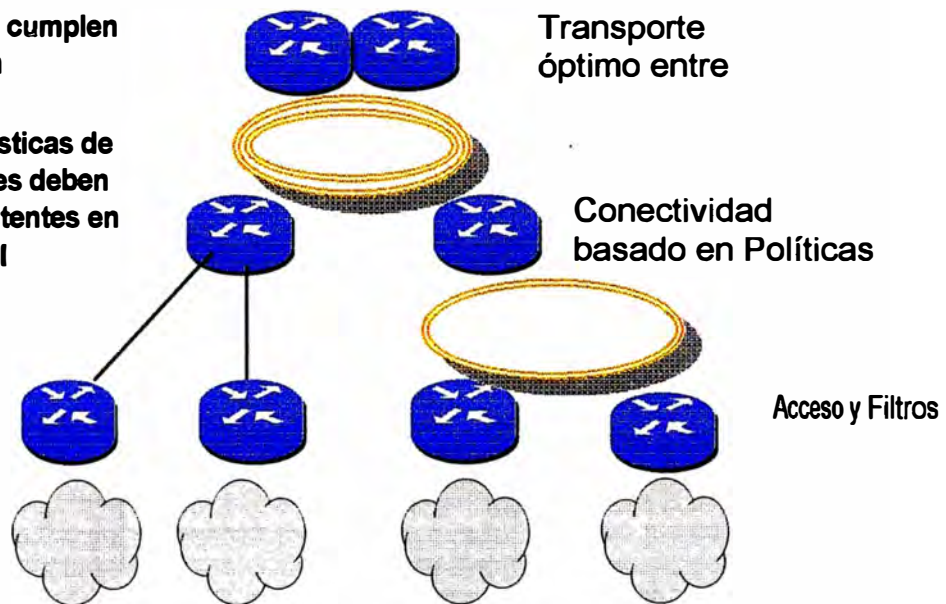
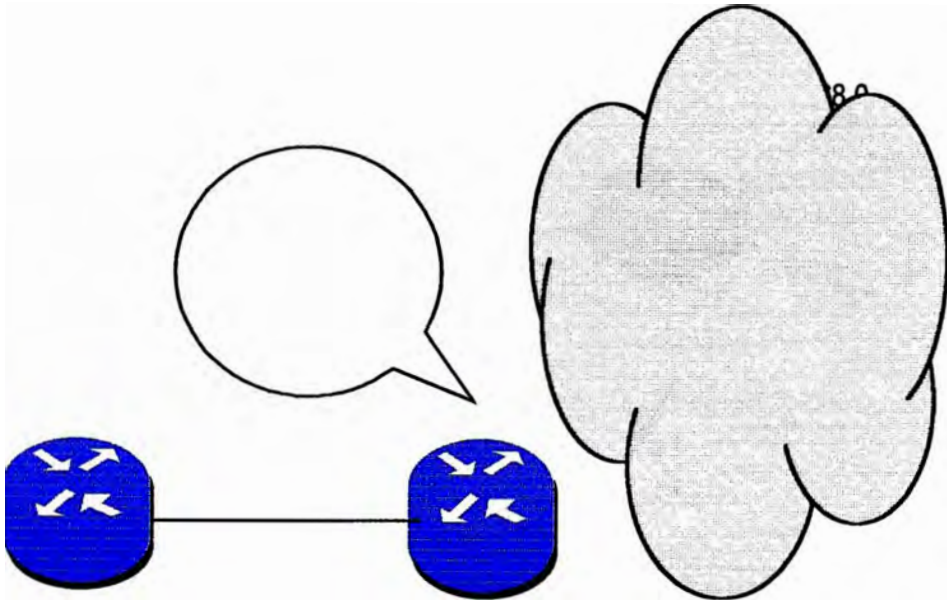


Fig. 2.4 Niveles de acceso,distribución y núcleo

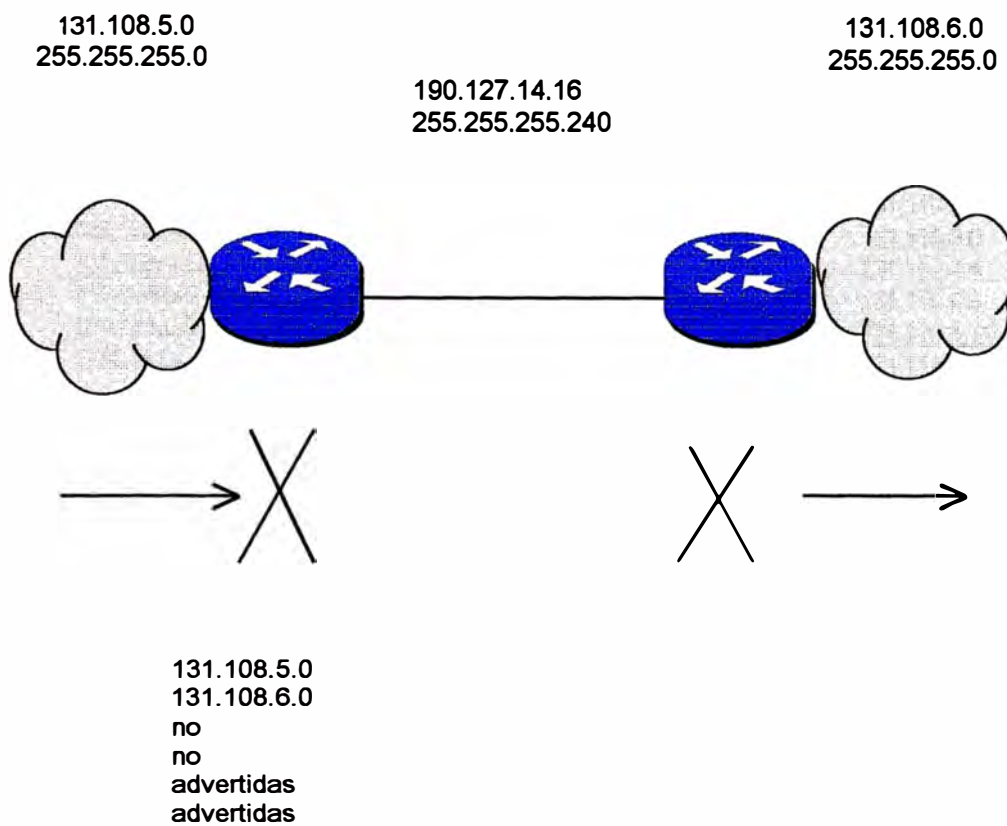
ENRUTAMIENTO DE DIRECCIONES SIN CLASE Y PREFIJOS



- CIDR usado por BGP4
- Prefijo de enrutamiento para EIGRP y OSPF

Fig. 2.5 Enrutamiento de Direcciones sin Clase

SUBREDES DISCONTINUAS Y ENRUTAMIENTO DE CLASES



Subredes remotas no alcanzables
Sólo red mayor es advertida

Fig. 2.6 Problema de Subredes discontinuas que son resueltas por EIGRP y

OSPF

RESUMEN DE ENRUTAMIENTO DE DIRECCIONES SIN CLASE

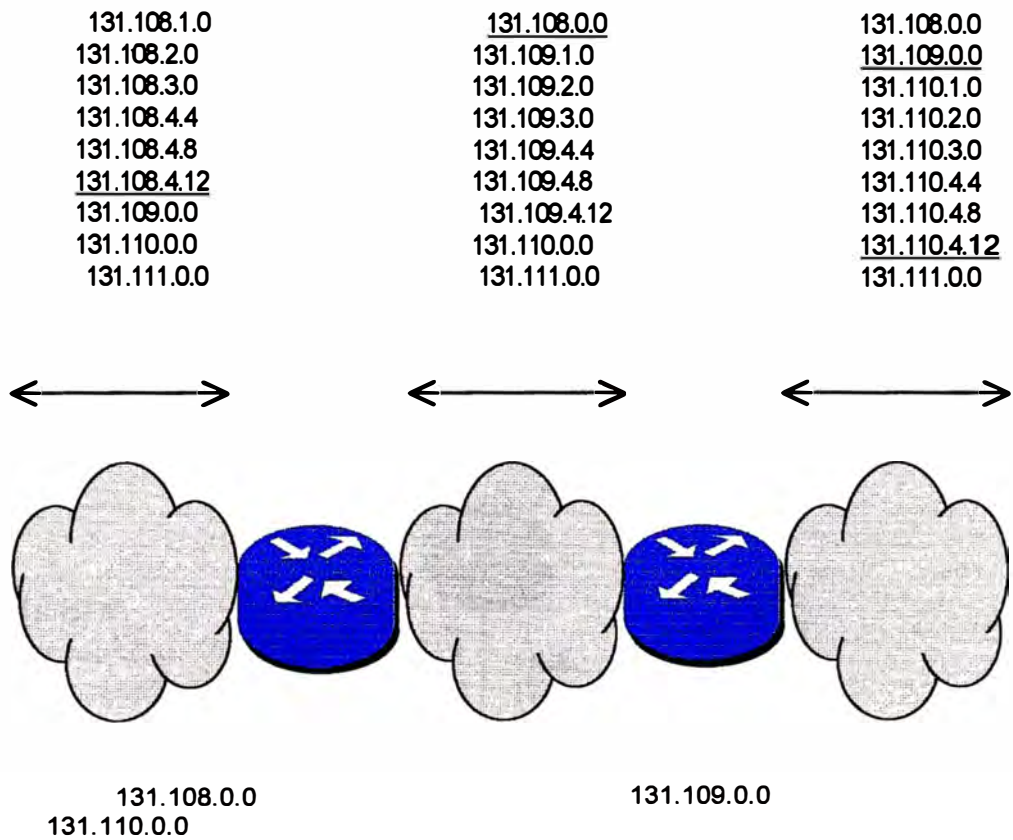


Fig. 2.7 Resumen de Bloques de Rutas

CONMUTACION REMOTA DE FRAME RELAY INTEGRADA

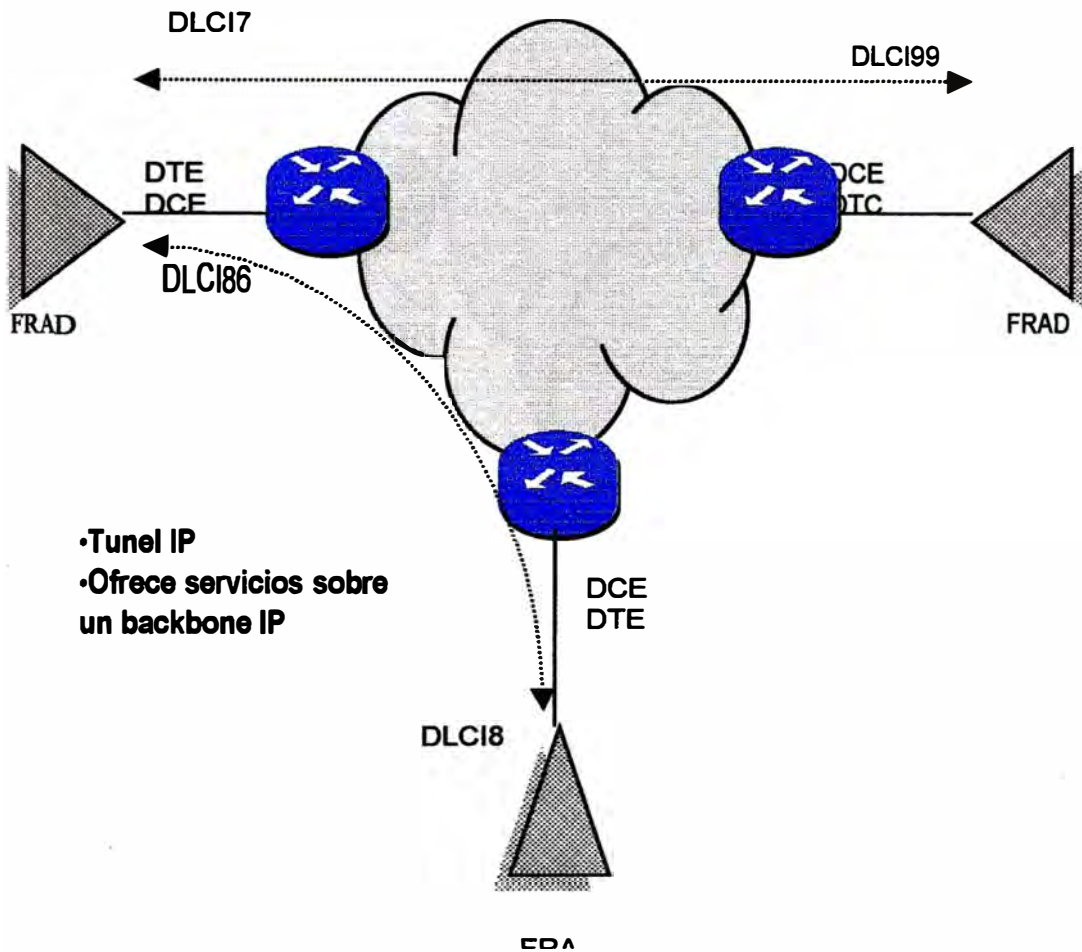
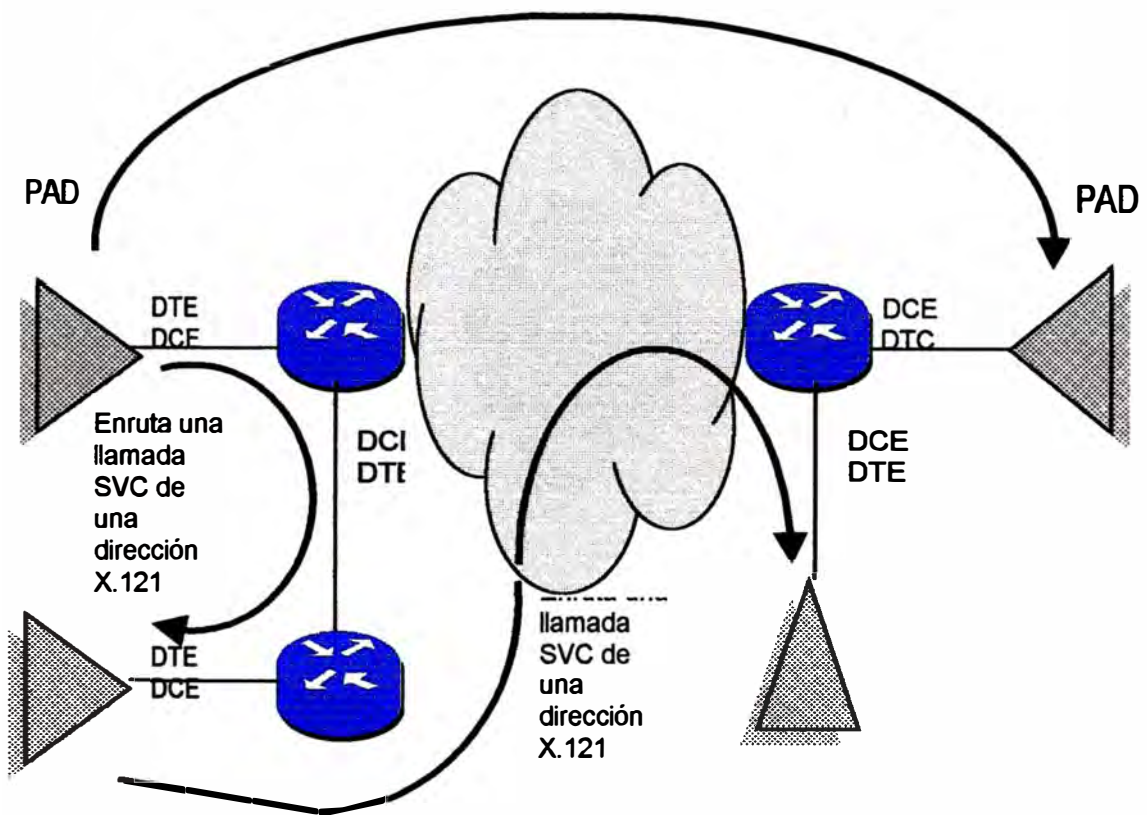


Fig. 2.8 Conmutación de Servicios Frame Relay en una Red IP

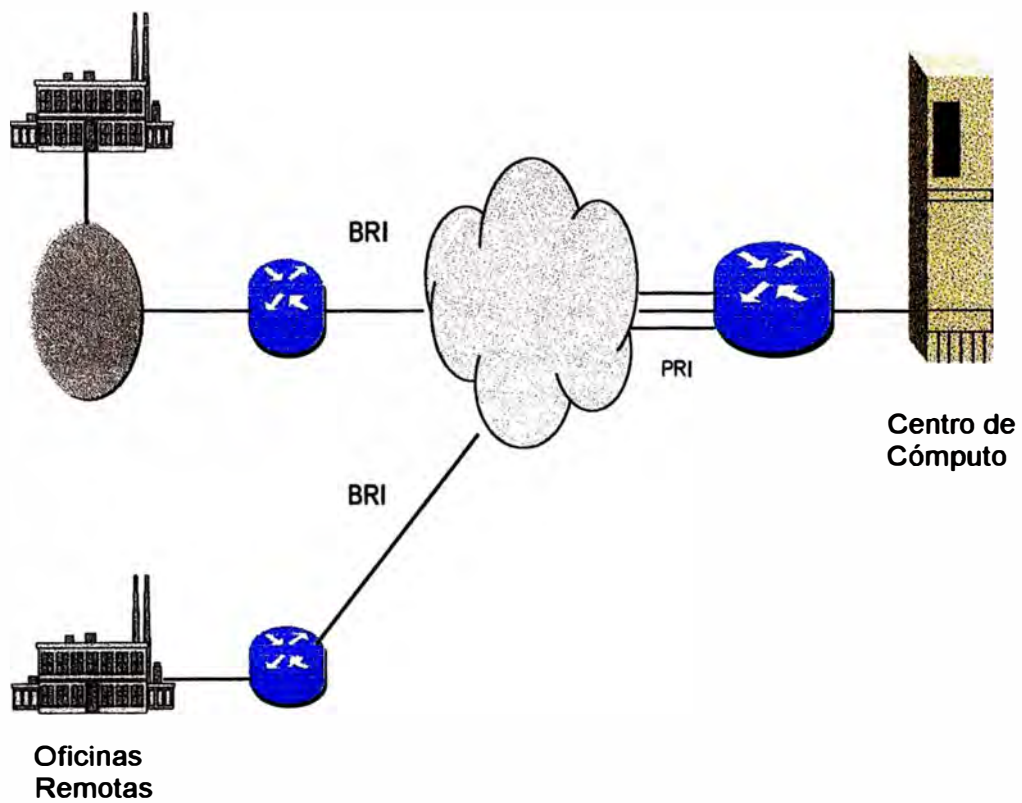
CONMUTACION LOCAL Y REMOTA X.25



- Uso de servicios integrados sobre backbone IP
- Conmutación IP de alta performance en backbone

Fig. 2.9 Conmutación de una red X.25

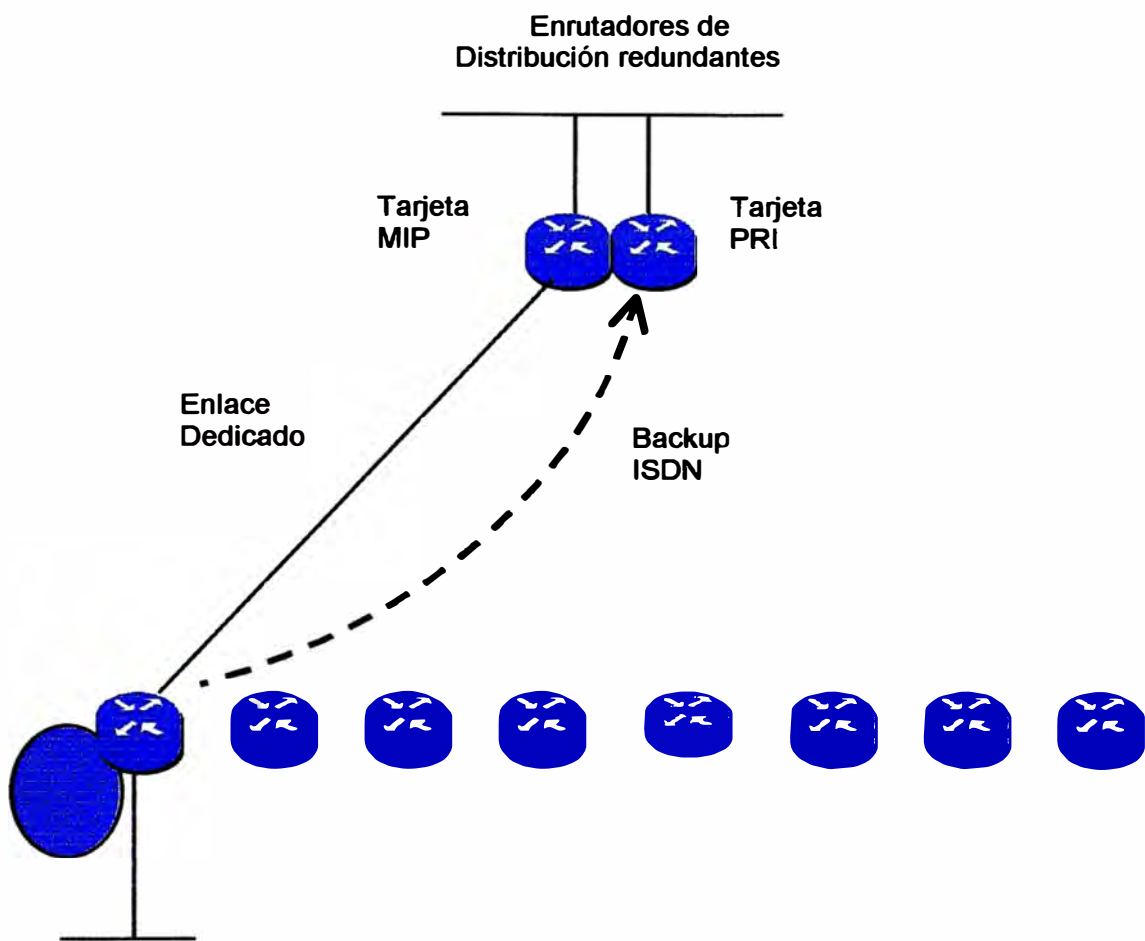
ENLACES BRI REMOTOS A PRI CENTRAL



- Las oficinas remotas ingresan a red central vía cisco 7000 o 4500

Fig. 2.10 Esquema de Contingencia basado en ISDN

RESPALDO MASIVO VIA ISDN



•Con un sólo PRI se pueden atender 23 agencias remotas concurrentemente

Fig. 2.11 Esquema de respaldo para las agencias

CAPITULO III DISEÑO DE LA RED DE COMUNICACIONES.

Este capítulo se caracteriza por detallar el diseño implementado de acuerdo a las recomendaciones y criterios del capítulo anterior. La descripción se divide en dos bloques, el primer bloque se refiere a la interconexión de cinco principales sucursales y en el siguiente bloque se describe la interconexión de las agencias con los centros principales.

Debido a que se tiene instalado dos centros de cómputo, uno principal y otro de respaldo, las consideraciones tomadas para la implementación siempre han sido mantener una disponibilidad de red WAN con capacidad de enrutamiento a estos dos principales centros.

3.1 Diseño de interconexión de principales sucursales

Estas cinco sucursales predominan por el volumen de tráfico que generan y por poseer un sistema interconectado de microondas, en el diseño se ha considerado formar un Backbone manteniendo una estructura de topología jerárquica para la interconexión de las agencias.

3.1.1 Topología de interconexión de sucursales

La topología escogida para lograr la interconexión de los mismos, es Malla Parcial con redundancia a dos centros. Esta topología permite mantener un sistema redundante de comunicaciones de Sucursales de San Isidro, Callao y Miraflores hacia OP Lima y La Molina.

El enrutador primario de La Molina tiene enlaces E1 a cada enrutador primario de las otras sucursales, estos enlaces son parte del sistema de microondas de tipo punto a punto con protocolo HDLC, propietario de Cisco Systems.

El enrutador secundario de la Sucursal de OP Lima tiene enlaces de 512 kbps a cada enrutador secundario ubicado en las Sucursales de San Isidro, Miraflores y Callao mientras que el enlace al enrutador secundario de La Molina es a 155 Mbps con fibra óptica monomodo con protocolo ATM (Asynchronous Transfer Mode) para mantener un enlace de alta velocidad entre el centro de cómputo principal y el de respaldo. Los enlaces a 512 Kbps punto a punto HDLC son proporcionados por Telefónica.

Con esta topología se pretende mantener una máxima redundancia: de medios de transmisión y de equipo de comunicaciones. Para lo cual se ha dispuesto instalar en cada uno de los centros dos dispositivos de comunicaciones: un enrutador primario y otro secundario.

Los enlaces realizados vía el sistema de microondas son tipo No Framed G.703, que permite un máximo de disponibilidad de 2.048 Mbps. Los enlaces a 512 Kbps vía sistema Digired requieren de un módem óptico con interface V.35.

Los enrutadores primarios que requieren conexión G.703 deben usar un conversor V.35/G.703 para lograr la compatibilidad de interfaces. Los enrutadores secundarios usan interfaces V.35.

3.1.2 Diseño de los dispositivos de comunicaciones de sucursales

Se realizaron pruebas de performance y facilidades de configuración con los diferentes dispositivos presentes en el mercado, de acuerdo a los resultados se eligió como dispositivo de comunicación: enrutadores Cisco Systems. Considerando que, los nodos La Molina y OP Lima tienen un requerimiento de

tráfico mayor y una disponibilidad de puertos para cubrir los requerimientos de conexiones punto a punto, se eligieron los enrutadores Cisco 7000 y para los otros nodos se eligieron enrutadores de la serie 4500 de Cisco Systems.

Para mayor conocimiento de estos dispositivos vamos a detallar mayores características técnicas de los mismos.

Cisco 7000

Bastante usado como enrutador central por la cantidad de puertos y la capacidad de procesamiento, denominado Cisco System series 7000 (Para mayor información técnica ver Apéndice B Catálogos), este enrutador se caracteriza tener un chasis modular, siendo sus principales características las siguiente:

- Posee Procesadores de Interface de Red de inserción y retiro en línea.
- Posee una arquitectura TRI-bus que incluyen buses Cxbus, Sxbus y dBus de 533Mbps.
- Las interfaces permiten crecimiento, asimismo escalamiento en memoria, potencia y software.
- Monitoreo de condiciones de ambiente de temperatura y potencia.
- Sistema de Refrigeración total.

Las interfaces que se pueden acondicionar son:

- Route Processor. Sistema de procesador principal.
- Switch Processor. Procesador de conmutación de paquetes dedicado.
- Silicon Switch Processor. Una opción para el Switch Processor, para mejorar la capacidad de conmutación.
- Interface Processor. Ocupa las ranuras 0 a 4, cinco ranuras son disponibles.

El enrutador Cisco 7000 tiene un sistema redundante de fuente, que pueden operar simultáneamente, los principales tipos de interfaces que permiten son los siguientes:

- FDDI.
- Ethernet AUI.
- Token Ring.
- HSSI.
- ATM.
- Serial.
- Conexión a canal de Host IBM.

La arquitectura TRI-Bus es un diseño compuesto de tres distintos buses que realizan diferentes tareas:

El **bus de diagnóstico** (dBus), realiza funciones de manejo de sistema, así como provee funcionalidades de descubrimiento, control y diagnóstico de fallas de:

- Los accesos de lectura a los tipos de módulos del CxBus, números de revisión del hardware, números seriales de los módulos, números de puertos y ranuras físicas y números de puertos lógicos.
- Los accesos de escritura para los números lógicos de ranuras, control de almacenamiento del microcódigo y prueba de los procesadores de interface.
- Detección del Route Processor, de la inserción y retiro de módulos, el cual permite funciones Hot Swap (cambio de dispositivos en línea).
- Propagación del reloj del CxBus.

El **bus extendido** de cisco (CxBus) es un bus de 533 Mbps de conmutación síncrona, diseñada para llevar datos entre los procesadores de interfaces y el Switch Processor o Silicon Switch Processor. Los procesadores de interface

transfieren paquetes hacia el buffer de memoria del SP (Switch Processor), el cual determina el puerto de salida cuando el paquete es enviado de vuelta al Cxbus directo al procesador de interface de salida.

El SxBus es un **bus de comunicación** entre procesadores a 153 Mbps está diseñado para llevar información entre el Route Processor y el Switch Processor.

Cada uno de estos buses operan autónomamente con sus propias tareas y con una pequeña dependencia de los otros procesadores del sistema.

Route processor

El Route Processor es el procesador principal del sistema en el enrutador. Contiene el CPU, el software del sistema y muchos componentes de la memoria del sistema. Mantiene y ejecuta las funciones de manejo que controlan el sistema, tiene los siguientes componentes:

- CPU Motorola MC68040 de 25 Mhz.
- 64 MB de memoria principal.
- 16 MB de memoria flash.
- 128 KB de NVRAM.
- PCMCIA Flash.
- Banco de direcciones MAC para los puertos de las interfaces.

La memoria NVRAM almacena la configuración del sistema y los reportes de monitoreo de ambiente, está protegido con baterías de litio que retienen la configuración. Mientras tanto, las memorias dinámicas DRAM almacenan las tablas de rutas, protocolos y aplicaciones de actividad de red. Estas residen en memorias SIMM.

Switch processor

La función del Switch Processor (SP), es decidir el destino de un paquete y conmutarlo basado en esta decisión. El SP usa un procesador de 16 millones-de-instrucciones-por-segundo (mips) que provee alta velocidad y una conmutación autónoma. El microcódigo SP contiene instrucciones de software específicos.

Interfaces WAN

Las interfaces WAN del enrutador que fueron usados para la solución de la topología fueron:

CX-AIP interface ATM

Con las siguientes características:

- Re-ensamblamiento de hasta 512 buffers simultáneamente, cada buffer es un paquete.
- Soporte de hasta 4096 circuitos virtuales.
- Soporte de AAL 5 y AAL3/4.
- Aunque el número de interfaces está físicamente limitado en cada enrutador, se debe configurar un diseño de limitación práctica determinado por el ancho de banda del bus del sistema.

El tipo de interface es el SONET de conexión monomodo con conector tipo ST2 a 155 Mbps.

CX-FSIP interface fast serial

La interface FSIP provee de 8 puertos independientes, puertos síncronos que soportan full-duplex a enlaces E1 (2.048 Mbps). Cada puerto soporta interfaces disponibles como V.35 y G.703/G.704, cada uno puede soportar señales de reloj interno o externo.

Cada módulo puede soportar un ancho de banda agregado de 16 Mbps. En el caso de los enrutadores del diseño, se han considerado 4 interfaces seriales V.35 y 4 G.703/G.704 de 75 ohms no balanceado que requiere de un cable de transición con un conector BNC al final de la red.

Interfaces LAN

Las interfaces LAN considerados para la solución de la topología son:

CX-EIP interface ethernet

La interface ethernet EIP provee 4 puertos de 10 Mbps, cada puerto soporta Ethernet versión 1 y Ethernet 802.3/Ethernet Version 2.

CX-FIP interface FDDI

La interface Fiber Distributed Data Interface FDDI contiene un procesador de 16 mips para una velocidad de 100 Mbps. El puerto que se usa es de tipo Dual Attachment Station DAS, con el cual el enrutador se conecta al anillo primario y secundario. Posibilitando a la estación de cambiar del anillo primario a secundario para mantener la integridad de la red en caso de evento de falla.

El conector que es usado es PHY-A y PHY-B multimodo con conectores MIC. La topología a implementar considera dos edificios principales, cada uno de los cuales posee enrutadores de la serie Cisco 7000.

Enrutador primario La Molina

Este enrutador posee las siguientes características:

- Cuatro puertos G.703 E1 y cuatro seriales.
- Un puerto FDDI DAS.
- Dos puertos ethernet (01 para el enlace TCP/IP y 01 para Translational Bridging).
- Un Route Processor, Un switch Processor.

- Un puerto de Canal ESCON para conexión a Host.

Enrutador secundario La Molina

Este enrutador posee las siguientes características :

- Cuatro puertos G.703 E1 cuatro seriales.
- Un puerto FDDI DAS
- Dos puertos ethernet (01 para el enlace TCP/IP y 01 para Translational Bridging).
- Un Route Processor, Un switch Processor.
- Un puerto ATM 155 Mbps.
- Un puerto de Canal ESCON para conexión a Host.

Enrutador primario oficina principal

Este enrutador posee las siguientes características:

- Cuatro puertos G.703 E1 y cuatro seriales.
- Cuatro puertos ethernet (01 enlace DLSw, 01 Translational Bridging y 01 conexión a la red).
- Un Route Processor, Un switch Processor.
- Un puerto ATM 155 Mbps.
- Un puerto de Canal ESCON para conexión a Host.

Enrutador secundario oficina principal

Este enrutador posee las siguientes características:

- Cuatro puertos G.703 E1 cuatro seriales.
- Cuatro puertos ethernet (01 para el enlace TCP/IP y 01 Translational Bridging, 01 conexión a red).
- Un Route Processor, Un switch Processor.
- Un puerto de Canal ESCON para conexión a Host.

Cisco 4500

Los enrutadores de las demás sucursales: Miraflores, Callao, San Isidro y los enrutadores especializados en DLSw son de la Serie Cisco 4500 (Para mayor información técnica ver Apéndice B Catálogos), estos enrutadores poseen un microprocesador RISC Orion de 100 Mhz con capacidad de memoria de 32 Mbps y 32 Mb de Memoria Flash.

Este enrutador tiene una característica en su plataforma que soporta hasta 3 módulos procesadores, los cuales pueden ser:

- Seriales, que pueden ser: Standard, ISDN BRI, ATM, CE1 (ISDN PRI), CT1 (ISDN PRI) y G.703.
- Ethernet que puede ser AUI y 10BaseT.
- Token Ring.
- FDDI.

En su arquitectura el enrutador posee un bus interno, los módulos procesadores ingresan en el bus y forman parte del diseño del sistema.

Interfaces ethernet

Se tienen dos versiones: un puerto simple y puerto dual para una densidad máxima de 6 puertos ethernet por chasis. Ambas unidades proveen conexiones AUI y 10BaseT.

Interfaces token ring

Los módulos son disponibles con uno o dos puertos hasta un máximo de 6 interfaces token ring.

Interfaces FDDI

Cada módulo soporta una interface de red FDDI. Las versiones disponibles soportan fibra multimodo dual o single-attached hasta un máximo de dos módulos FDDI.

Interfaces seriales

Son módulos disponibles con dos o cuatro puertos seriales, hasta un máximo de 12 puertos síncronos. Puede ser X.25 con señalización física RS232 y V.35, DTE ó DCE dependiendo del tipo de cable que se requiera.

Interfaces ISDN

Los módulos son disponibles con 4 ó 8 puertos BRI. Cada puerto tiene un conector RJ45 para interface con un elemento NT1.

Uno de los módulos usados en el diseño, es el tipo ISDN PRI denominado CE1/PRI. La interface CE1 provee un E1 canalizado, vía un cable coaxial conectado a un dispositivo CSU (Channel Service Unit). El controlador provee hasta 30 canales virtuales; cada canal virtual es presentado al sistema como una interface serial que puede ser individualmente configurado. Este controlador CE1 realiza una transmisión bidireccional a la velocidad E1 de 2.048 Mbps, funcionando como un enlace que soporta ISDN PRI.

En el nodo La Molina, se ha considerado enrutadores Cisco Systems series 4500 para soporte especializado, los cuales se dimensionaron de esta manera:

Enrutadores Cisco especializados en DLSW

Este enrutador posee las siguientes características

- Dos interfaces ethernet..
- 32 MB de memoria DRAM.
- 16 MB de memoria flash

- 128 KB NVRAM.

Enrutadores Cisco de acceso

Este enrutador tiene la función de acceso, que permite enlaces X.25 a nodos remotos que no cuentan con frame relay; adicionalmente puede soportar enlaces ISDN PRI de respaldo por enlace ISDN. Las interfaces que posee:

- Cuatro interfaces seriales.
- Dos interfaces ethernet.
- Una interface CE1/PRI.
- 32 MB de memoria DRAM.
- 16 MB de memoria flash.
- 128 KB NVRAM.

Enrutadores Cisco de acceso a sucursales

Estos se encuentran desplegados en las sucursales de San Isidro, Miraflores y Callao, los cuales permiten la interconexión de las redes locales. En el caso de San Isidro, se cuenta con un enlace de respaldo ISDN PRI que colecta un grupo de agencias en caso de fallas. Las interfaces que poseen son:

- Cuatro interfaces seriales.
- Dos interfaces ethernet.
- Una interface CE1/PRI.
- 32 MB de memoria DRAM.
- 16 MB de memoria flash.
- 128 KB NVRAM.

3.2 Diseño de la red de agencias

Una vez configuradas e interconectadas los cinco nodos, se procedió a la configuración de cada una de las agencias de Lima Metropolitana. para los cuales se diseño la siguiente arquitectura:

3.2.1 Topología de interconexión de agencias

El número de agencias del Banco en Lima Metropolitana es 100. Para la interconexión de las mismas se determinó el uso del modelo jerárquico, la concentración de los enlaces de agencias se realizaron a tres nodos principales que forman parte del Backbone. Esta concentración se realizó usando una configuración de tres circuitos virtuales de frame relay, servicio rentado a la red Interlan de Telefónica del Perú.

Los tres nodos de concentración: La Molina, San Isidro y Oficina Principal fueron escogidos por poseer las facilidades de comunicación.

El uso de frame relay permitió generar los tres circuitos virtuales mencionados a cada uno de los nodos desde los enrutadores remotos. Es decir, cada punto de concentración soporta una configuración de 100 circuitos virtuales. En los párrafos siguientes explicaremos las capacidades de enlace escogidas.

Algunas de las agencias fueron interconectadas usando X.25 debido a que aún no existía disponibilidad del servicio frame relay, la topología adecuada para esta configuración es la jerárquica. Se aprovechó circuitos especiales disponibles en estas agencias para realizar la interconexión vía X.25 al enrutador de acceso instalado en el nodo La Molina.

3.2.2 Diseño de los dispositivos de comunicaciones de agencias

De acuerdo a la topología a implementar descrita anteriormente, el diseño de los dispositivos de comunicaciones, puede ser subdividida en dos bloques: agencias vía frame relay y agencias vía X.25.

3.2.2.1 Agencias vía frame relay

Para realizar la implementación de esta topología, fué instalado en cada una de las agencias un dispositivo DTU conectado al servicio frame relay a través de un circuito digital de cobre.

El dispositivo de comunicación usado en la agencia fué:

Enrutador Cisco 2500

El enrutador es de la serie Cisco 2500 (Para mayor información técnica ver Apéndice B Catálogos). Dos modelos de esta serie fueron usados: el cisco 2503, que posee una interface ethernet, dos puertos seriales y una interface ISDN BRI; el modelo Cisco 2520, que posee una interface ethernet, 4 seriales y una interface ISDN BRI.

3.2.2.2 Agencias vía X.25

En cada una de estas agencias fueron reutilizados los circuitos especiales instalados anteriormente, estos circuitos especiales se concentran en uno de los tres nodos sucursales: La Molina, San Isidro y Oficina Principal. Por necesidad de configuración de la red X.25 se usó un equipo conmutador X.25 (switch).

Una conexión X.25 es una relación DCE/DTE con capacidad de configurar circuitos virtuales, es necesario usar conmutadores X.25 para evitar que el enrutador central posea un número de interfaces correspondientes a cada nodo remoto, se usa conmutadores X.25 para permitir ocupar una interface en el

enrutador central, mientras el conmutador concentra todos los circuitos especiales que provienen de cada enrutador remoto.

Los dispositivos de comunicaciones usados en esta etapa:

- Enrutadores Cisco 2500.
- Conmutadores X.25 Codex Motorola.
- Modems V.34 Penril.

Enrutadores Cisco 2500

(Para mayor información técnica ver Apéndice B Catálogos).

Conmutadores X.25

Este conmutador es marca Codex Motorola de la serie MPR 6520 (Para mayor información técnica ver Apéndice B Catálogos) cuyas características son las siguientes:

- 19 puertos configurables X.25 RS232/V.35 DTE/DCE
- 1 puerto de consola.
- La tarjeta principal del 6520 viene con 8 Mbps de DRAM con capacidad de crecimiento a 16 kbps.

3.3 Diseño de la red frame relay

Basado en las consideraciones descritas en el capítulo anterior se procedió a llevar a cabo las siguientes consideraciones de planeamiento para la red de frame relay.

3.3.1 Suscripción de la red frame relay

La mayoría de las redes implementadas son basados en topologías estrellas. En el caso de la red a instalar se tiene que los principales servidores de aplicaciones y el host IBM se encuentran localizados en una región centralizada. Para el desarrollo de esta topología se puso bastante cuidado al proveer el adecuado

ancho de banda y recursos necesarios en el manejo del tráfico total requerido por nuestra organización, se tuvo en cuenta la cantidad de bytes adicionales suministradas por el sobreencabezado (overhead) de paquetes.

En muchos casos, la sub-suscripción en este tipo de ambientes es común y no son cuidadosamente planeados, esto puede originar una performance adversa en la red incluyendo postrísimos tiempos de respuesta. Un problema de bajo nivel asociado con esta pobre performance es muchas veces atribuible a una sub-estima del volumen real de tráfico y patrones de tráfico que existe en la red.

La cantidad de nodos remotos con que se cuenta en la actualidad es de 100 agencias que se requirieron conectar a la nube frame relay, para esto se solicitaron tres principales accesos con velocidades de E1 (2.0 Mbps), se considerará lo siguiente:

1.- Suscripción a una velocidad física de acceso.

Es la velocidad de acceso que se proveen a las agencias. Se requirieron de tres enlace a los nodos centrales a velocidades de 2.0 Mbps con capacidad de proveer acceso a 100 agencias conectados a velocidades físicas de 64 Kbps.

En caso de que cada una de las agencias genera un tráfico de 100% de burst, la capacidad del enlace central es suficiente para soportar el tráfico total:

$$100 * 64 \text{ kbps} = 6.4 \text{ Mbps},$$

mientras que,

$$3 * 2.048 \text{ Mps} = 6.1 \text{ Mbps}.$$

Con el conocimiento de todo el tráfico y del ancho de banda requerido, se asignaron las cantidades necesarias de memoria requeridas a los enrutadores, aún con la cantidad de protocolos que debería soportar (IP, IPX y SNA) y tomando en cuenta el crecimiento de nuevas aplicaciones se decidió por esta

consideración por ser la elección más segura. Como se está usando toda la disponibilidad del ancho de banda el CIR solicitado fue igual a la velocidad de acceso es decir 64 Kbps.

La otra alternativa que se consideró fue la siguiente:

2.- Suscripción con un valor moderado del CIR.

Considerando los enlaces remotos a velocidades físicas de 64 kbps, se asumió un valor de CIR de 32 kbps.

Bajo el mismo cálculo anterior se determina la necesidad de 2 enlaces E1 (2 Mbps) a la zona central. En este caso, 100 agencias remotas cada una con 64 kbps y con un CIR de 32 Kbps. Si todas las agencias remotas envían un tráfico al 100% del burst al mismo tiempo ocurrirá una congestión al ingreso de los dos enlaces E1 de la red frame relay, en este caso el conmutador en el lado del proveedor empezará a eliminar paquetes. Lo mismo ocurrirá al ingreso de la red, si el tráfico va más allá de los límites establecidos, los casos de congestión ocurrirá por la multiplexación de los 100 circuitos virtuales.

Este caso fué necesario analizar con mayor cuidado y se requería tener un mayor conocimiento del ancho de banda necesitado y el crecimiento con el transcurso del tiempo. Escogiendo un CIR de 32 Kbps significa que el requerimiento es tener un ancho de banda garantizado disponible para enviar al menos 32 kbps de datos, con la flexibilidad de envía de tráfico burst encima de esta velocidad, pero no por un tiempo sostenido, esto hace que las redes frame relay puedan manejar un tráfico burst. No es recomendable en estos escenarios que todos los accesos remotos puedan tener accesos burst al mismo tiempo, aunque basados en algunos patrones estos pueden originarse, tal como los broadcast.

Para escoger el escenario mas adecuado se realizó un análisis del tráfico, generalmente en el ambiente de Banco, donde cada agencia soporta un enrutador que está conectado vía frame relay a la zona central. Cada agencia soporta un segmento de LAN que conecta las estaciones de trabajo de la agencia y líneas seriales conectados a cajeros automáticos (ATM Automated Teller Machines). Las aplicaciones en las estaciones de trabajo son primariamente interactivas (solicitud/respuesta) pero también son usados para Transferencias de Archivos, generalmente al iniciar procesos batch o tareas de impresiones. Como esto es realizado fuera de hora de atención a público, el proceso de respuestas interactivas durante el horario normal reunen o superan los requerimientos. Las transferencias de información son bastante largas , especialmente en los días de mayor actividad, a esto se suma las tareas de actualización de versiones de software conocido como distribución de software. Existe también un pico de uso de los ATM en estos días y las sobrecargas de líneas pueden ser largas. Si las transferencias de archivos ocurren en este período pico de tiempo. Los tiempos de respuesta de los ATM serán adversamente afectados.

De acuerdo a las pruebas que se realizaron, el consumo de ancho de banda originado por las aplicaciones en agencias no supera los 32 kbps, en períodos de tráfico sostenido por lo cual las alternativas 1 y 2 fueron factibles. Se decidió usar los tres enlaces E1 para casos de contingencia y crecimiento futuro.

3.3.2 Capacidad del número de DLCI en los enrutadores

Una de las estimaciones que se tuvieron que realizar es el número de DLCI que se puede configurar en un enrutador Cisco y específicamente el número de DLCI por interface serial, generalmente se convierten en dos interrogantes: Cuántos DLCI por interface y cuántos DLCI por enrutador. Sencillamente el número

depende de varios factores, uno de los principales factores es la limitación técnicas los cuales muchas veces van más allá de los máximos prácticos.

3.3.2.1 Limitaciones técnicas

1.- Número de DLCI, de acuerdo a la estructura de la trama de frame relay aproximadamente 1000 DLCI pueden ser configurados en un sólo enlace por los diez bits reservados para el número de DLCI, esto es considerando los DLCI reservados que depende de la implementación de los fabricantes, el número máximo de DLCI es aproximadamente 1000.

2.- Actualización del LMI Status, de acuerdo a las configuraciones realizadas con el proveedor se viene usando el protocolo LMI (ANSI Annex D, y estándar ITU-T). Este protocolo, requiere que todos los estados de los circuitos virtuales PVC que vienen siendo reportados por la red, puedan ocupar un simple paquete y generalmente, esta es una limitación que reduce el número de DLCI a menos de 800, como veremos esto también depende del tamaño del MTU.

La fórmula es la siguiente:

$(MTU-20)/5 = \text{Max DLCIs (aproximadamente)}$.

$(1500-20)/5 = 296$.

Donde el valor 20 es la cantidad de bytes de la cabecera de LMI y Frame Relay.

NOTA: Los números calculados varían levemente dependiendo del tipo de LMI.

3.3.2.2 Limitaciones prácticas

1.- **Datos del Usuario.**- Se tiene que aproximar la cantidad y tipo de los datos de usuarios que se espera pueda viajar a través del circuito virtual, para nuestro caso fué muy difícil de tener un valor estimado del tráfico por ser de tipo burst, teniendo

referencias de que las transferencias de archivos rápidamente consumen el CIR y los límites del burst de exceso. De acuerdo a nuestros requerimientos, se requieren varios DLCI en una sola interface física, por lo cual el tráfico en el enlace físico se empezó a eliminar o reducir el broadcast y evitar multiples protocolos limitandolos a IP, IPX y SNA.

2.- Tráfico Broadcast. Se tienen dos implicancias:

2.1 El consumo de ancho de banda por el tráfico broadcast y,

2.2 Replicación de broadcast en los enrutadores de núcleo en la zona central.

Para evitar el tráfico de broadcast se usó el siguiente criterio:

- Filtros de ruta y SAPs.

3.- Consumo de Memoria.- Depende de los factores :

- El número de aplicaciones ejecutándose en el enrutador.
- Protocolos que usa el enrutador.
- Dimensiones de las tablas de rutas.

Para los cuales existe un requerimiento de la cantidad de memoria, para soportar adicionalmente la cantidad de DLCI que se requiera configurar.

4.- Consumo de Procesador.- Los enrutadores Cisco proveen facilidades tales como compresión, priorización y protocolos de procesos compartidos (process switched). Estas facilidades incrementan el uso del procesador, lo cual es una limitante para incrementar el número de circuitos virtuales. Actualmente, en las versiones posteriores a la 11.0, varias de estas características han sido movidos a un proceso de conmutación rápido (fast switching).

Se tomaron las siguientes guías:

- Se desarrolló un sistema de configuración de enrutadores para eliminar lo más posible el Broadcast en el enlace frame relay. En el uso de TCP/IP se

procedió a minimizar las tablas de rutas usando resumen de rutas IP y minimizando el tamaño de la tabla para las actualizaciones.

- El número máximo de DLCI por plataforma de enrutador se tomó en base a la siguiente referencia:

2500: 1 x enlace T1/E1 @ 60 DLCI por interface = 60 total.

4000: 1 x enlace T1/E1 @ 120 DLCI por interface = 120 total.

4500: 3 x enlace T1/E1 @ 120 DLCI por interface = 360 total.

4700: 4 x enlace T1/E1 @ 120 DLCI por interface = 480 total.

7000: 4 x enlace T1/E1/T3/E3 @ 120 DLCI por interface = 480 total.

7200: 5 x enlace T1/E1/T3/E3 @ 120 DLCI por interface = 600 total.

2500: 1 x enlace T1/E1/T3/E3 @ 120 DLCI por interface = 720 total.

3.3.3 Análisis de tráfico

Uno de los principales temas en redes basadas en frame relay, es el consumo de ancho de banda de tráfico Broadcast. La razón es la replicación de paquetes en una simple interface física, esto es más común en el nodo central donde la concentración de circuitos virtuales en el enlace físico es mucho mayor que en los nodos de acceso ó distribución. Se realizaron análisis de tráfico con enrutadores configurados con múltiples protocolos y como resultado de estos análisis se observaron una sobrecarga de cabeceras de información. Se obtuvo como resultado el siguiente patrón de Broadcast originado por:

- Protocolos de enrutamiento.
- Protocolos de rutas.
- Transparent Bridging.
- DLSW.

3.3.4 Actualización de rutas

El efecto de actualización de rutas en una red frame relay, tiene un significativo impacto en la performance. Se observaron que las razones de este comportamiento es la actualización de rutas en la salida de la interface por cada circuito virtual PVC (DLCI). Así cuando se configura DLCI múltiples en una simple interface frame relay, las actualizaciones de rutas serán replicados por cada DLCI. Mientras que los protocolos de enrutamiento conocidos como vectores de distancia (Distance Vector) como RIP e IGRP, son fácilmente predecibles porque las actualizaciones se producen en intervalos regulares de tiempo, no sucede lo mismo con protocolos basados en estados de enlace (Link State) como OSPF o IS-IS. El protocolo que venimos usando es el EIGRP el cual a pesar de ser un protocolo de vectores de distancia avanzado, también posee el mismo comportamiento de categoría que el OSPF. Aunque EIGRP no es un protocolo de estado de enlace, las actualizaciones de rutas son propagadas de una manera similar a un protocolo de estado de enlace, es decir una actualización sucede cuando una adyacencia es perdida.

Aquí una descripción de los protocolos de ruta que nuestros equipos tienen configurados: IP, IPX y SNA.

IPX RIP

La actualización de paquetes (Routing Information Protocol) IPX RIP, ocurre cada 60 segundos. Cada paquete puede contener hasta 50 entradas de rutas con un total de 536 bytes, 38 bytes de cabecera de información y cada entrada de ruta ocupa 8 bytes. Si se advierte 500 rutas IPX sobre enlaces frame relay configurados con 100 DLCI, se podría finalizar con 536 bytes de actualizaciones de IPX cada 60 segundos ó un 58.4 kbps de ancho de banda consumido. Para

permanecer en los niveles permisibles de sobrecarga (15% o menos) una velocidad de 512 kbps debería ser requerido.

$500/50 = 10$ paquetes * 38 bytes = 380 bytes de cabecera.

$500 * 8 = 4000$ bytes de entradas de rutas.

Total = $4380 * 100 = 438,000$ bytes de actualizaciones de IPX cada 60 segundos.

$438,000/60 \text{ seg} * 8 \text{ bits} = 58.4 \text{ Kbps}$

Configuración frame relay en una agencia típica es mostrada en el Apéndice A.1.

3.4 Diseño de la red X.25

En el diseño implementado se ha considerado las siguientes características:

3.4.1 Direccionamiento X.25

Un sistema de direcciones X.25 consiste de una combinación de números decimales de 14 dígitos. Cabe destacar que la red X.25 que se está formando es una red privada, por lo cual se dispone de un sistema de numeración que permite con facilidad reconocer cada uno de los nodos a los cuales la dirección representa.

Por ejemplo, un valor usado es el siguiente 716630017, cada grupo de dígitos representa lo siguiente:

71 : Código País.

66 : Código BCP.

300 : Código Sucursal.

01 : Número de agencia que depende de la sucursal .

7 : Dispositivo de comunicación

Por lo tanto 71 (Perú), 66 (BCP), 300 (La Molina), 01 Agencia (Agencia Nueva Sede), y 7 enrutador.

Otros parámetros que se deben considerar son los siguientes:

Tamaño de Paquete: El tamaño de paquete es 1024. Para evitar la fragmentación de los datagramas IP, lograr evitar un consumo de CPU y medios de comunicación.

Tamaño de ventana: Parámetros K y W: Se usó el valor de $K=7$ $W=7$ para optimizar la calidad y eficiencia de transmisión en el medio de comunicación. El incremento del tamaño de ventana permite el envío de mayor número de paquetes con un sólo requerimiento de certificación de llegada (acknowledge). Es óptimo incrementar este valor cuando los enlaces son de buena calidad, si el enlace se encuentra con ruido entonces el proceso de retransmisión se complica, debido a que es mayor el número de paquetes que se envían.

De acuerdo a pruebas en Laboratorio que se realizaron, se concluyó que las líneas o circuitos especiales pueden permitir eficientemente una configuración $k=7$, $w=7$ y $n=1024$.

Los circuitos especiales analógicos que son provistos por Telefónica son circuitos punto a punto que se concentran en nuestras principales sucursales.

Para soportar la concentración de agencias en tres centros principales se ha implementado una red X.25 con la instalación de un conmutador X.25 en cada centro. Los conmutadores que se encuentran en San Isidro y Oficina Principal, se conectan al conmutador de La Molina con enlaces a 128 Kbps. Estos enlaces de alta velocidad ocupan puertos V.35 en los conmutadores. Las direcciones adoptadas son las siguientes:

Conmutador La Molina	7166300007
Conmutador Oficina Principal	7166200007
Conmutador San Isidro	7166100007

Las características de cada puerto de enlace entre conmutadores:

Velocidad: 64 kbps.

Tipo de puerto: DCE ó DTE dependiendo al puerto que es conectado.

Dirección de Enlace: DTE ó DCE lógico, depende del puerto remoto a conectar.

Número de canales SVC: 128.

Secuencia de Cuenta de Frames: NORMAL.

Ventana de Tramas K: 7.

Secuencia de Cuenta de Paquetes: EXTENDIDO.

Ventana de Paquetes: 15.

Tamaño del Paquete: 1024.

Las características de los puertos de enlace del conmutador con los enrutadores son:

Velocidad: Depende de la velocidad del módem.

Tipo de puerto: DCE se usa cable cruzado (cross-over) para conectar a puerto DCE de módem.

Dirección de Enlace: DCE lógico.

Número de canales: 4.

Secuencia de Cuenta de Frames: NORMAL.

Ventana de Tramas K : 7.

Secuencia de Cuenta de Paquetes: NORMAL.

Ventana de Paquetes: 7.

Tamaño del Paquete: 512.

Se tiene una configuración en las tablas de rutas de los conmutadores X25, de tal manera que las llamadas X.25 de los enrutadores remotos puedan encontrar

una ruta al enrutador central. De acuerdo a las configuraciones realizadas, sólo es permitido que los remotos realicen llamadas X.25 a los centrales.

Los puertos seriales s0 de los enrutadores Cisco 2503 tienen la siguiente configuración (Ver Apéndice A.1) :

```
encapsulation x25
x25 address 7166300457
x25 htc 4
x25 win 7
x25 wout 7
x25 ips 512
x25 ops 512
```

El enrutador central ubicado en La Molina tiene el puerto conectado al conmutador X.25 con la siguiente configuración:

```
encapsulation x25
x25 address 7166300007
x25 htc 134
x25 win 7
x25 wout 7
x25 ips 512
x25 ops 512
```

Los valores usados fueron determinados de acuerdo a los resultados obtenidos en las pruebas que se realizaron. Adicionalmente es necesario entender que ancho de banda y el throughput son conceptos diferentes. Una congestión en el ancho de banda afecta negativamente el throughput, mientras que el ancho de banda permanece inalterado.

El throughput puede ser mejorado de la siguiente manera:

- Reduciendo la congestión del ancho de banda disponible.
- Incremento de tamaño de ventana W.
- Incremento del Tamaño de paquete.
- Incrementado el número de circuitos virtuales.

3.4.2 Uso del modelo NBMA para acceso de agencias vía X.25

La plataforma X.25 descrita anteriormente sirve adicionalmente para implementar el sistema de respaldo vía enlace conmutado de una agencia cuando se produce una avería en el enlace frame relay. Por esta razón, no se usa subinterfaces en la configuración para definir cada uno de los enlaces X.25, en este caso se ha adoptado el modelo NBMA. Este modelo permite poseer una configuración para cada uno de los enrutadores remotos de tal manera se tiene disponible cuando se realicen los procedimientos de recuperación a fallas (enlace de respaldo X.25). Se deben usar comandos tales como:

```
x25 map protocol address x.121-address nvc count
```

Se usa este comando para establecer una relación estática entre las direcciones de protocolos de mayor nivel y las direcciones usadas en la red X.25. En este caso un máximo de nueve protocolos pueden ser configurados para alcanzar un simple enrutador central.

La opción protocolo se encarga de seleccionar el tipo disponible que puede ser uno de los siguientes: IP, DECNET, XNS, IPX, APPLETALK, VINES, APOLLO, BRIDGE, CLNS y COMPRESSEDTCP. Mientras que la opción de direcciones x.121 especifica la dirección X.25 en el enrutador remoto al cual se va a conectar.

Por ejemplo, en el enrutador central se tiene la siguiente configuración:

```
x25 map ip 172.30.137.2 7166200017 broadcast no-outgoing compress.
```

```
x25 map ip 172.30.137.3 7166200027 broadcast no-outgoing compress.
```

```
x25 map ip 172.30.137.4 7166200037 broadcast no-outgoing compress.
```

```
x25 map ip 172.30.137.5 7166200047 broadcast no-outgoing compress.
```

```
x25 map ip 172.30.137.6 7166200057 broadcast no-outgoing compress.
```

En el enrutador remoto se tiene la siguiente configuración:

```
x25 map ip 172.30.137.1 7166300007 broadcast compress.
```

Con estas configuraciones podemos apreciar que se va a establecer un circuito SVC que transportará tramas IP, la opción no-outgoing en el enrutador central evita que se inicie llamadas X.25 hacia el remoto. Debido a que una parte de esta configuración está destinado a los enlaces de respaldo no es necesario que el enrutador central se encuentre continuamente iniciando una comunicación remota.

Los módems usados son tecnología V.32 del fabricante Penril Communications, por la calidad de línea los enrutadores remotos tienen enlaces desde 9.6 kbps hasta 14.4 kbps. Considerando la cantidad de tráfico y de acuerdo a los resultados de las pruebas que se realizaron, el comando compress que se incluye en la configuración, provee la capacidad de compresión de carga con una eficiencia de 2 a 1(payload compression). El uso de esta compresión aumenta en 5% el uso del CPU del enrutador remoto y permite un throughput casi al doble de la velocidad, aproximadamente a 19.2 kbps. Con esta característica, el tiempo de respuesta que se obtiene en las agencias se encuentra dentro de los límites de tolerancia deseados.

En la actualidad, no es aún requerido configuraciones del protocolo IPX por lo cual sólo se ha considerado incluir las configuraciones con soporte a protocolo IP.

3.4.3 Servicios adicionales que se usan vía X.25

Lo descrito anteriormente es usado para interconectar los enrutadores vía una red X.25 y los parámetros usados permiten una configuración para transportar IP vía X.25, permitiendo la interconexión de las redes remotas LAN a las redes centrales.

Los cajeros automáticos se constituyen en uno de los servicios estratégicos del Banco, estos cajeros tienen conexiones X.25 a un computador TANDEM ubicado en la Sede Central La Molina.

Por consideraciones de costo se ha determinado usar el mismo circuito usado para interconexión de los enrutadores, para lo cual se hace uso de puertos adicionales en los enrutadores (cisco 2520) con configuración x.25. El tráfico X.25 puede ser enrutado localmente entre los puertos seriales del enrutador. En este caso, sentencias estáticas mapean direcciones x.121 a puertos seriales. El enrutador permite interfaces X.25 conectados a diferentes puertos para realizar conexiones SVC o PVC, característica conocida como comutación X.25 local .

Por consideraciones de redundancia, se usa otra característica que proveen los enrutadores Cisco, la capacidad de transportar X.25 sobre TCP/IP conocido como XOT o conmutación X.25 remota, permitiendo a las interfaces conectados a diferentes enrutadores establecer conexiones SVC ó PVC. Este mecanismo es desarrollado por un túnel de todas las llamadas X.25 y tráfico de datos entre los enrutadores en una conexión TCP, no interesa si en el medio puede existir otra red X.25 ó frame relay.

El comando usado para establecer el túnel es:

```
x25 route 71663000071* ip add 134.1.1.1
```

Con este comando el enrutador direcciona todas las llamadas que contiene la dirección x.121 descrita a la dirección remota ubicada en el enrutador central. Los enlaces de los puertos seriales a los cajeros tienen una velocidad de 9.6 kbps, algunos conectados directamente y otros por distancia conectados con módems denominados módems de cola.

Mientras que, el enrutador central X.25 tiene dos interfaces conectados vía X.25 al computador TANDEM. Estos enlaces son a 64 kbps y cada enlace soporta 30 cajeros. La configuración en el enrutador central varía debido a que recibe la llamada x.25 del cajero, en este punto ya no es necesario realizar un túnel puesto que se trata sólo de una conmutación local.

```
x25 route 71663000071* interface serial 4.
```

3.5 Diseño del sistema de direcciones IP

De acuerdo a las sugerencias vertidas en el capítulo anterior, el objetivo es establecer un sistema de direccionamiento que posea las siguientes características:

- Rango de direcciones establecidas para redes privadas.
- Sistema de máscara variable VLSM para ahorro de direcciones.
- Asignación de bloque de direcciones para resumen de rutas.
- Rango de hosts que permita crecimiento.

En el caso de la red en mención, se requiere cubrir los siguientes requerimientos:

Número de Redes Remotas en Agencias vía frame relay : 90.

Número de Redes Remotas en Agencias vía X.25 : 10.

Número de Estaciones de Trabajo en las redes remotas: 40.

Número de Redes en las Sucursales de Lima : 5.

Número de Estaciones de Trabajo en las redes de Sucursales:

La Molina : 850.

Oficina Principal : 600.

San Isidro : 450.

Miraflores : 200.

Callao : 200.

Número de subredes en la red Frame Relay : 270.

Número de subredes en la red X.25 : 11.

Número de subredes en el Backbone de Sucursales : 8.

De acuerdo a las cantidad requerida de hosts y redes, considerando además un crecimiento futuro en el número de agencias y estaciones de trabajo de los mismos, se realizó un sistema de distribución de direcciones IP. En este caso se trata de una red de gran escala con una topología compleja, por la cual se determinó el uso de una dirección privada.

La dirección escogida es clase B 172.30.0.0. Basado en esta dirección y con el uso de máscara variable se obtiene lo siguiente :

Bloques de direcciones a asignar:

172.30.0.0 / 18

172.30.64.0 /18

172.30.128.0 /18

172.30.192.0 /18

Considerando el uso del primer bloque de direcciones se obtiene las direcciones para las agencias, cada subred tiene una capacidad de un crecimiento hasta 62 estaciones (ver tabla 1).

Agencia 1	172.30.1.0 /25
Agencia 2	172.30.1.128 / 25
Agencia 3	172.30.2.0 /25
Agencia 4	172.30.2.128 /25
Agencia 5	172.30.3.0 /25
Agencia 126	172.30.63.0 /25

Tabla 1

Las direcciones para las Sucursales fueron obtenidas haciendo uso del segundo bloque disponible, cada dirección tiene capacidad de soportar hasta 16 subredes con capacidad 1022 estaciones de trabajo, de este grupo sólo se requiere 5 subredes (ver tabla 2).

La Molina	172.30.64.0 / 14
Oficina Principal	172.30.68.0 /14
San Isidro	172.30.72.0 /14
Miraflores	172.30.76.0 /14
Callao	172.30.80.0 /14

Tabla 2

El bloque de direcciones asignado a los enlaces punto a punto con configuración de subinterfaces en la red frame relay se describe en la siguiente tabla, con esta distribución se tiene hasta 512 subredes con dos números de hosts (ver tabla 3).

Agencia 1	Dirección
Serial 0.1	172.30.128.4 / 30
Serial 0.2	172.30.128.8 / 30
Serial 0.3	172.30.128.12 /30
Agencia 2	Dirección
Serial 0.1	172.30.128.16 / 30
Serial 0.2	172.30.128.20 / 30
Serial 0.3	172.30.128.24 /30

Tabla 3

La red X.25 se caracteriza por mantener una sólo subred, el uso del modelo NBMA permite la formación de una especie de red LAN, usando una sola dirección de red. El sistema de direcciones debe cubrir la cantidad de direcciones de red y el número de puntos de estaciones requeridos, para lo cuál se ha obtenido la siguiente tabla, con capacidad de 256 estaciones ó puntos de enrutadores remotos (ver tabla 4).

Enrutador Central	172.30.137.1 / 24
Agencia 1	172.30.137.2 /24
Agencia 2	172.30.137.3 /24
Agencia 3	172.30.137.4 /24

Tabla 4

En la actualidad, en cada una de las agencias se tiene instalado un módem con una línea telefónica conectado al puerto serial 1 del enrutador, como una medida de respaldo ante la falla del enlace principal. Para este caso, adicionalmente se tiene configurado una red X.25 con las mismas características que la anterior y que se concentra al enrutador central X.25. El bloque de direcciones asignado para este caso es el siguiente (ver tabla 5).

Enrutador Central	172.30.138.1 /24
Agencia 1	172.30.138.2 /24
Agencia 2	172.30.138.3 /24
Agencia 3	172.30.138.4 /24
Agencia 4	172.30.138.5 /24

Tabla 5

3.6 Diseño del protocolo de enrutamiento

3.6.1 Enrutamiento usando EIGRP

EIGRP es el protocolo que se viene usando para que los enrutadores puedan intercambiar sus tablas de información, fué necesario contar con un control de uso de ancho de banda en la red frame relay, para que no se consuma la mayor parte de ella con el procesamiento de EIGRP. El EIGRP fue significativamente mejorado en las versiones del software IOS releases 10.3, 11.0, 11.1. La implementación fue cambiada para mejorar la performance en redes de baja velocidad (incluyendo frame relay) y en configuraciones con muchos enrutadores vecinos. Es importante usar mejoras para el caso de la red frame relay y en puntos con bajas velocidades (9.6 kbps).

3.6.2 Control del ancho de banda

Por defecto EIGRP limita el uso del ancho de banda a no más del 50% del ancho de banda disponible. El principal beneficio de controlar el uso del ancho de banda que realiza EIGRP es la pérdida de paquetes EIGRP, esto fué observado cuando el proceso del enrutador central empezó a generar datos con mayor rapidez que la línea podía absorber. La segunda opción es poseer un determinado ancho de banda disponible para paquetes de datos aún cuando el flujo esté completamente operando.

Los comandos que se usaron fueron los siguientes:

```
Bandwidth 64
```

Y adicionalmente,

```
ip bandwidth-percent eigrp 172 40
```

El comando menciona que EIGRP debe usar el 40% de 64. Desde que este valor es usado para cálculos de las métricas, este valor puede ser modificado por razones de control de porcentajes usados por EIGRP.

Si el ancho de banda es configurado para ser un valor relativamente menor que la velocidad real del enlace, una configuración mejorada puede desmejorar el tiempo de convergencia del protocolo que una configuración original. Si el valor es pequeño y existe muchas rutas en el sistema, la convergencia puede ser muy baja por lo cuál se presentan procesos de detección tales como "Stuck in Active". el cual puede prevenir a la red de una convergencia en todo momento. Este estado fue evidenciado por repetidos mensajes tal como:

```
%DUAL-3-SIA : Route XXX stuck-in-active state in IP-EIGRP YY. Cleaning up.
```

Para solucionar el problema fue necesario configurar :

```
router eigrp
```

timers active-time

Este comando eleva al valor active del timer de EIGRP. Si el valor del ancho de banda es configurado para ser mayor, las pérdidas de paquetes de EIGRP ocurren. Los paquetes serán retransmitidos, degradando la convergencia.

3.6.3 Configuración punto a punto

Debido a que esta configuración permite un mayor control, se viene usando cada DLCI unido a cada configuración de subinterfaces, el cual permite poseer un ancho de banda configurado separadamente en cada subinterface. Esta es la mejor configuración si los circuitos virtuales tienen diferentes capacidades. Cada subinterface es configurado con un valor que no es mayor que el ancho de banda asociado al circuito virtual, el total ancho de banda para todas las subinterfaces no excede el ancho de banda de la línea de acceso.

3.6.4 Diseño del protocolo de enrutamiento EIGRP

Los enrutadores Cisco implementan protocolos tales como RIP, OSPF, IGRP y EIGRP. Generalmente los administradores de redes escogen entre estos protocolos. De acuerdo a la topología implementada los enrutadores de las agencias, poseen 3 circuitos virtuales PVC definidos a tres diferentes nodos, considerando dos de ellos como circuitos alternativos ante fallas de alguno de los enlaces primarios. Y adicionalmente se consideran enlaces alternativos vía ISDN o enlaces por conmutada vía X.25. Entonces se requiere de un protocolo de rápida convergencia, inicialmente se decidió usar el protocolo IGRP con las siguientes desventajas:

Convergencia de Protocolo : Retardo de 3 a 6 minutos en la actualización de una ruta nueva, esto es debido a su deficiencia en la detección de loops por el cual se tiene que imponer pérdidas temporales de rutas, los cuales fueron

originados por los HoldDowns o técnicas de Route-Poisoning que previenen los loops, los cuales en efecto tienen un tiempo de retardo. Adicionalmente los protocolos tales como RIP e IGRP no soportan sistemas de direccionamiento IP de máscara variable. Adicionalmente, se tiene que observar las actualizaciones periódicas de las tablas de rutas cada 90 segundos con los cuales se presentan problemas de sincronización que posee RIP.

Por estas limitaciones se tuvieron dos alternativas, el uso de OSPF y EIGRP. Los análisis que se hicieron nos permitieron observar que los protocolos de vectores de distancia es en efecto superior a los protocolos de estados de enlace por la flexibilidad en casos de redes con complejidad como es en el caso de nuestra red. El actual contendor de EIGRP es OSPF, desde que EIGRP incluye correcciones para las limitaciones conocidas de los protocolos de vectores de distancia, manteniendo su simplicidad.

CAPITULO IV ASPECTOS ECONOMICOS

Se considera conveniente presentar el costo de inversión realizado en equipos de comunicación que fueron necesarios en la implementación de la red. Asimismo se incluye los gastos que se realizan al año en el alquiler de las facilidades de comunicación.

4.1 Costo de equipos de comunicaciones

4.1.1 Costo de inversión en equipos de comunicaciones en La Molina.

En la Molina :

02 Enrutadores Cisco 7000

Costo Unitario: US\$ 177,100.00 Costo Total : US\$ 354,200.00

02 Enrutadores Cisco 4500

Costo Unitario: US\$ 14,780.00 Costo Total : US\$ 29,560.00

02 Enrutadores Cisco 4500

Costo Unitario: US\$ 22,530.00 Costo Total : US\$ 45,060.00

02 Conmutadores Ethernet Lanplex 2500 3COM

Costo Unitario: US\$ 8,350.00 Costo Total : US\$ 16,700.00

01 Conmutador ATM LightStream 100 Cisco

Costo Unitario: US\$ 21,900.00 Costo Total : US\$ 21,900.00

4.1.2 Costo de inversión en equipos de comunicaciones en la Oficina Principal.

En la Oficina Principal:

02 Enrutadores Cisco 7000

Costo Unitario: US\$ 177,100.00 Costo Total : US\$ 354,200.00

02 Enrutadores Cisco 4500

Costo Unitario: US\$ 14,780.00 Costo Total : US\$ 29,560.00

01 Enrutador Cisco 4500

Costo Unitario: US\$ 22,530.00 Costo Total : US\$ 22,530.00

02 Conmutadores Ethernet Lanplex 2500 3COM

Costo Unitario: US\$ 8,350.00 Costo Total : US\$ 16,700.00

4.1.3 Costo de inversión en equipos de comunicaciones en sucursal San Isidro.

En la sucursal San Isidro:

02 Enrutadores Cisco 4500

Costo Unitario: US\$ 22,530.00 Costo Total : US\$ 45,060.00

02 Conversores E1 de G.703 a V.35

Costo Unitario: US\$ 4,200.00 Costo Total : US\$ 8,400.00

4.1.4 Costo de inversión en equipos de comunicaciones en sucursal Miraflores.

En la sucursal Miraflores :

- 02 Enrutadores Cisco 4500

Costo Unitario: US\$ 22,530.00 Costo Total : US\$ 45,060.00

02 Conversores E1 de G.703 a V.35 RAD

Costo Unitario: US\$ 4,200.00 Costo Total : US\$ 8,400.00

4.1.5 Costo de inversión en equipos de comunicaciones en sucursal Callao.

En la sucursal Callao:

02 Enrutadores Cisco 4500

Costo Unitario: US\$ 22,530.00 Costo Total : US\$ 45,060.00

02 Conversores E1 de G.703 a V.35 RAD

Costo Unitario: US\$ 4,200.00 Costo Total : US\$ 8,400.00

4.1.6 Costo de inversión en equipos de comunicaciones en agencias Gran Lima.

En las agencias Gran Lima:

100 Enrutadores Cisco 2503

Costo Unitario: US\$ 4,445.00 Costo Total : US\$ 444,500.00

- 14 Vanguard 100 Motorola Codex

Costo Unitario: US\$ 950.00 Costo Total : US\$ 13,300.00

- 128 Modems v.32 Penril Datability

Costo Unitario: US\$ 980.00 Costo Total : US\$ 125,440.00

4.2 Costo de facilidades de comunicaciones

El proveedor del servicio Interlan en la actualidad es Telefónica del Perú.

4.2.1 Pago de 3 enlaces E1 2,048 Kbps servicio frame relay.

(01 La Molina, 01 OP Lima, 01 San Isidro).

Pago única vez

Acceso Costo Unitario US\$ 2,720.00 Costo Total US\$ 8,160.00

Pago mensual

Acceso Costo Unitario US\$ 1,923.50 Costo Total US\$ 5,770.50

4.2.2 Pago de 100 enlaces 64 Kbps servicio frame relay.

(100 agencias de Gran Lima)

Pago Unica Vez

Acceso	Costo Unitario	US\$ 1,360.00	Costo Total	US\$ 136,000.00
--------	----------------	---------------	-------------	-----------------

Pago Mensual

Acceso	Costo Unitario	US\$ 430.00	Costo Total	US\$ 43,000.00
--------	----------------	-------------	-------------	----------------

4.2.3 Pago de 4 enlaces a 512 Kbps

(Servicio Digired desde OPLima a La Molina, San Isidro, Miraflores y Callao).

Pago Unica Vez

Acceso	Costo Unitario	US\$ 3,900.00	Costo Total	US\$ 15,600.00
--------	----------------	---------------	-------------	----------------

Pago Mensual

Acceso	Costo Unitario	US\$ 890.00	Costo Total	US\$ 3,560.00
--------	----------------	-------------	-------------	---------------

CONCLUSIONES Y RECOMENDACIONES

Para el proceso inicial que se realizó paralelamente al diseño de las redes, fué muy importante la implementación de un plan de pruebas. Estas pruebas fueron realizados con enrutadores de marca 3Com, Cisco y con el conmutador multiprotocolo Motorola. Se incluyeron pruebas de facilidad de configuración de X.25 y frame relay con protocolos IP e IPX. Se midió el tiempo de respuesta y el comportamiento de red usando priorización de protocolos, realizando operaciones simultáneas de transferencia de datos y transacciones bancarias.

En el proceso también se detectó problemas en el desarrollo de las aplicaciones, estas generalmente fueron desarrollados como aplicaciones de redes LAN, al aplicarlos en un ambiente WAN tuvieron un deterioro en el tiempo de respuesta, por lo cuál fue necesario la optimización de las aplicaciones. Es recomendable, cuando se diseña una red implementar un plan de pruebas que facilite el conocimiento del funcionamiento de las redes y aplicaciones.

Uno de los principales problemas encontrados durante la implementación de la red frame relay, fué la falta de experiencia y conocimiento inicial en configuración y mantenimiento de una red frame relay, razón que motivó continuas pérdidas de los enlaces, gran número de mensajes FECN y BECN que fueron originados por un CIR configurado a 0 y la falta de disponibilidad de ancho de banda en los enlaces troncales de Telefónica. A esto se suma la falta de una adecuada calibración y medición de la calidad del enlace del tramo final, desde el nodo

frame relay al enrutador de la agencia, originando problemas de CRC o pérdidas de enlace. Razón por lo cuál fué necesario realizar un trabajo preventivo en la verificación de la calidad de línea con anticipación a la puesta en producción de una agencia.

El protocolo de enrutamiento inicial usado en producción fue IGRP, no se usó EIGRP porque la versión 10.3.6 de los enrutadores Cisco incluían varias deficiencias que en su mayoría fueron resueltas en la versión 10.3.13. El uso de IGRP mostró serias deficiencias como protocolo de enrutamiento en redes complejas, debido a su característica de un tiempo de 280 segundos de HoldDown Time que impide una rápida convergencia a rutas alternativas disponibles. La pérdida temporal de rutas en los enrutadores originaron que se pierdan sesiones SNA (DLSW), estas sesiones están consideradas como críticas. El IGRP fue una barrera en el proceso de implementación de redes con VLSM para el sistema de direccionamiento diseñado. Una vez realizado el cambio a EIGRP se solucionaron los problemas de convergencia y facilidades de uso de VLSM.

El cambio de un sistema de punto a punto y basado en protocolos SDLC a sistema de protocolos Frame Relay, X.25, TCP/IP e IPX fué un cambio a gran escala, uno de los principales problemas que se resolvió fue la falta de preparación de técnicos y profesionales de áreas de mantenimiento, operación e instalaciones. Se emprendió una agenda de charlas técnicas en temas de X.25, frame relay, IP e internetworking, lográndose transmitir la experiencia necesaria en el control y monitoreo de redes. Asimismo, se logró implementar un sistema de administración y manejo basado en SNMP. La plataforma actualmente usada es HP Openview de NCR denominada ONE VISION.

Una de las principales herramientas que facilitó la implementación y solución de los diferentes problemas presentados tanto a nivel de comunicaciones como a nivel de sistemas operativos fue el uso de un analizador de protocolos SNIFFER de Network General, esta herramienta analiza protocolos como IP, IPX, SNA, NETBIOS en redes Ethernet y Token Ring; PPP, SNA, frame relay y X.25 en enlaces seriales. Actualmente, se ha modernizado la herramienta con la adición de capacidad de análisis de ISDN, protocolos como HTTP y DLSW. Existe en el mercado diferentes tipos de analizadores, con diferentes capacidades de análisis y a diferentes precios que facilitan su adquisición.

El uso del protocolo DLSW fué criticado por especialistas de IBM del Perú, quienes argumentaron que este protocolo usaba una exagerada cabecera compuesto por 89 bytes por cada frame que se enviaba. Los 89 bytes están constituidos por una cabecera IP, una cabecera TCP, una cabecera de DLSW. El uso de las cabeceras de TCP e IP facilitan la capacidad de redundancia del circuito DLSW establecido, por lo cuál si una ruta al enrutador DLSW remoto es perdida, se usa las rutas alternativas sin necesidad de reconfiguración del enrutador de la agencia. Los argumentos en contra fueron resueltos por los siguientes criterios: Primero, el uso de DLSW sobre TCP/IP permite la capacidad de redundancia ante fallas de enrutadores intermedios y la facilidad de tener el protocolo SNA con una certificación local (local acknowledge) evitando un tráfico innecesario de tramas de control y supervisión a través de la red, manteniendose el tráfico de estas tramas en forma local. Segundo, el enrutador de la agencia con el enrutador local establecen un circuito DLSW, los datos de varias sesiones se pueden agrupar en una sólo trama DLSW, por lo cual se disminuye la cantidad de intercambio de tramas entre ambos. Con estas dos características la performance

del mecanismo DLSW se incrementa y se disminuye el efecto de retardo por 89 bytes de cabecera que incluye el protocolo, lo cuál ha sido demostrado con el transcurso del tiempo en las instalaciones realizadas cuyas agencias poseen tiempos de respuesta hasta de 2.5 segundos para sesiones 3270 con el host IBM.

Generalmente, cuando se presenta tiempos de respuesta fuera de los valores esperados, se tiene un diagnóstico inicial como problema de comunicaciones, en muchos casos son correctos cuando estos problemas son originados por ruido y pérdida de comunicaciones o la falta de ancho de banda disponible para la cantidad de tráfico que se transmite. En otras ocasiones se deben considerar que los retardos no solamente son causados por los medios de comunicación, también son producidos por la capacidad de procesamiento de los servidores y la cantidad de información transferida por estos. En muchas ocasiones se tuvieron que optimizar las aplicaciones porque no estaban diseñados para trabajar en redes WAN, por el excesivo tráfico innecesario que transmite. Por ejemplo, tablas y descripción de campos cuando estos ya se encuentran disponibles localmente ó la solicitud de búsqueda de una base de datos en forma secuencial, originando un aparente retardo causado por la saturación de los medios y los dispositivos de comunicaciones.

APENDICE A

MODELO DE CONFIGURACION DE ENRUTADORES

A.1 Configuración de una agencia típica

```

version 10.3
service timestamps log datetime msec
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname AGENCIA1
!
enable use-tacacs
enable last-resort password
enable password 7 020E054F1E0807344D5D00
!
frame-relay switching
x25 routing
dlsw local-peer peer-id 172.30.1.1
dlsw remote-peer 0 tcp 192.168.1.1 cost 2 lsap-output-list 201
dlsw remote-peer 0 tcp 192.168.1.2 cost 5 lsap-output-list 201
dlsw remote-peer 0 tcp 192.168.1.3 cost 2 lsap-output-list 201 backup-peer
192.168.1.1
dlsw remote-peer 0 tcp 192.168.1.4 cost 5 lsap-output-list 201 backup-peer
192.168.1.2
dlsw bridge-group 1
!
interface Ethernet0
description Interfaz Ethernet - LAN
ip address 172.30.1.1 255.255.255.128
bridge-group 1
!
interface Serial0
description Interfaz Serial Frame Relay a Interlan - 64k
no ip address
encapsulation frame-relay
no ip route-cache
!
interface Serial0.1 point-to-point
description DLCI a La Molina
ip address 172.30.128.6 255.255.255.252
bandwidth 56
no cdp enable
frame-relay interface-dlci 16 broadcast
frame-relay ip tcp header-compression passive
!
interface Serial0.2 point-to-point
description DLCI a OPLima
ip address 172.30.128.10 255.255.255.252
bandwidth 48
no cdp enable

```

```
frame-relay interface-dlci 17 broadcast
frame-relay ip tcp header-compression passive
!
interface Serial0.3 point-to-point
description DLCI a San isidro
ip address 172.30.128.14 255.255.255.252
bandwidth 64
no cdp enable
frame-relay interface-dlci 18 broadcast
frame-relay ip tcp header-compression passive
!
interface Serial1
description Interfaz Serial X.25 Backup
ip address 172.30.138.2 255.255.255.0
encapsulation x25
bandwidth 10
no keepalive
x25 address 71663000017
x25 ltc 2
x25 htc 4
x25 win 7
x25 wout 7
x25 ips 512
x25 ops 512
x25 map ip 172.30.138.1 71663000007 broadcast compress
!
interface BRI0
no ip address
shutdown
!
interface Async1
no ip address
!
router eigrp 172
passive-interface Ethernet0
network 172.30.0.0
  distribute-list 2 out Serial0.1
  distribute-list 2 out Serial0.2
  distribute-list 2 out Serial0.3
!
ip host man 172.30.64.10
ip domain-name bcp.com.pe
ip name-server 172.30.64.15
logging buffered 30000
access-list 2 permit 172.30.1.0 0.0.0.127
access-list 201 permit 0x0000 0x0D0D
access-list 201 deny 0x0000 0xFFFF
tacacs-server host 172.30.64.12
tacacs-server attempts 1
tacacs-server last-resort password
```

```
tacacs-server timeout 3
tacacs-server extended
tacacs-server authenticate connections
tacacs-server authenticate enable
tacacs-server notify connections
tacacs-server notify enable
tacacs-server notify logout
tacacs-server notify slip
snmp-server community public RO
snmp-server community sistemas RW
snmp-server trap-source Ethernet0
snmp-server trap-authentication snmpv1
snmp-server location Agencia1
snmp-server contact Servicio de Telecomunicaciones
snmp-server enable traps frame-relay
snmp-server host 172.30.64.16 bcpsnet tty framerelay x25 snmp
bridge 1 protocol ieee
!
line con 0
  exec-timeout 1 30
  login tacacs
line aux 0
  exec-timeout 1 30
  login tacacs
  transport input all
line vty 0 4
  exec-timeout 1 30
  login tacacs
!
end
```

A.2 Configuración ISDN de una agencia típica

Ejemplo de configuración 2503

C2503#wr t

Current configuration:

```

!
version 10.2
!
hostname C2503
!
enable password test
!
username C4000 password cisco
isdn switch-type basic-dms100
!
interface Ethernet0
ip address 172.16.10.1 255.255.255.0
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
ip address 172.16.20.1 255.255.255.0
encapsulation ppp
bandwidth 56
dialer idle-timeout 300
dialer map ip 172.16.20.2 name C4000 speed 56 broadcast 14155551234
dialer map ip 172.16.20.2 name C4000 speed 56 broadcast 14155556789
dialer hold-queue 5
dialer load-threshold 100
dialer-group 1
isdn spid1 408555432101 5554321
isdn spid2 408555987601 5559876
ppp authentication chap
!
router igrp 1
network 172.16.0.0
!
ip route 192.168.24.0 255.255.255.0 172.16.20.2
access-list 100 deny ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!

```

```

!
dialer-list 1 list 100
!
line con 0
line aux 0
line vty 0 4
password test
login
!
end

```

Explicación de Configuración

```

C2503#wr t
#####
Current configuration:
!
version 10.2
!
hostname C2503
!
enable password test
!
username C4000 password cisco

```

The username "C4000" is the hostname of the remote router and is used by the dialer map command below. The username is case sensitive and must match the remote router's hostname exactly.

The password, which is used by the CHAP authentication process, is case sensitive and must match the remote router's password exactly.

Note: To avoid confusion, the unencrypted form of the password cisco is shown in this sample configuration. In the actual configuration, the password would appear in its encrypted form: 7 13061E010803, where 7 denotes the encryption type and 13061E010803 is the encrypted form of the password cisco. When entering or making changes to the username command, always type the password in its unencrypted form and do not enter the encryption type (7). It is set automatically.

```
isdn switch-type basic-dms100
```

The ISDN switch type must match your carrier's equipment. If you change the switch-type, you must reload the router for the new switch type to take effect.

```
interface Ethernet0
ip address 172.16.10.1 255.255.255.0
```

```
interface Serial0
no ip address
```

```

shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
ip address 172.16.20.1 255.255.255.0

encapsulation ppp

```

PPP encapsulation is recommended over HDLC in order to allow the use of CHAP authentication.

```
bandwidth 56
```

The default bandwidth setting for a BRI interface is 64k. If you configured your dialer map statements with the speed 56 option, you should include the bandwidth statement.

Note: This command does not control the speed of your ISDN line. It sets the correct reference point for the BRI port's show interface statistics, for the dialer load-threshold command, and for IGRP/EIGRP routing metrics.

```
dialer idle-timeout 300
```

This command sets the number of seconds the ISDN connection will remain open if no interesting traffic is being routed. The timer is reset each time an interesting packet is forwarded.

```

dialer map ip 172.16.20.2 name C4000 speed 56 broadcast 14155551234
dialer map ip 172.16.20.2 name C4000 speed 56 broadcast 14155556789

```

The dialer map command is used with CHAP authentication to place the initial call to the remote router when interesting traffic is forwarded to the BRI interface. Once the connection is active, the dialer idle-timeout command determines how long it will remain active. A dialer map statement is required for each ISDN phone number that will be called. Be aware though, that two dialer map statements pointing to the same location might activate both B channels when you may only want to use one channel.

Note: The command parameters for this example are:

172.16.20.2 = the IP address of the remote router's BRI interface. To determine this address, type show interface bri 0 at the remote router's console prompt.

name C4000 = the hostname of the remote router. The name is case sensitive and should match the name configured for the username command above.

speed 56 = sets the dialer speed to 56k for ISDN circuits that are not 64k end-to-end, and should be included in both routers' dialer map statements. Most installations in North America must be configured for 56K.

broadcast = allows the forwarding of broadcast packets. Unless broadcast packets are specified as interesting packets by the dialer-list command, they will only be forwarded when the ISDN link is active.

```
14155551234
```

14155556789 = the remote router's ISDN telephone numbers.

```
dialer hold-queue 5
```

This command allows interesting packets to be queued until the ISDN connection is established. In this example, five interesting packets will be queued.

```
dialer load-threshold 100
```

This command is used to configure bandwidth on demand by setting the maximum load before the dialer places another call through the second B channel. The load is the calculated weighted average load value for the interface, where 1 is unloaded and 255 is fully loaded. The actual load value you should configure depends on the characteristics of your particular network. In this example, the second B channel will be activated when the load reaches 39% of maximum utilization, which is 100 divided by 255.

```
dialer-group 1
```

The dialer-group 1 command enables the dialer-list 1 on the BRI interface, which determines which packets will be interesting and activate the ISDN connection.

```
isdn spid1 408555432101 5554321
```

```
isdn spid2 408555987601 5559876
```

The isdn spid commands are used if your carrier assigns spids to your ISDN lines.

```
ppp authentication chap
```

This command enables CHAP authentication.

```
router igrp 1
```

```
network 172.16.0.0
```

```
ip route 192.168.24.0 255.255.255.0 172.16.20.2
```

This IP route command creates a static route to the remote router's network via the remote router's BRI interface. This is required because dynamic routes are lost when the ISDN link is down.

Note: The command parameters for this example are:

192.168.24.0 = the target network.

255.255.255.0 = the target network mask. A 255 in an octet's position specifies an exact match for that octet is required, and a 0 in an octet's position specifies any value will match.

172.16.20.2 = the address of the next hop that can be used to reach the target network.

```
access-list 100 deny ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

This access list determines which IP packets will be interesting and activate the ISDN link. The access-list you should create depends on your particular network design.

Note: The command parameters for this example are:

```
access-list 100 deny ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
```

defines all broadcast packets as uninteresting.

```
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

defines all other IP packets as interesting.

```
dialer-list 1 list 100
```

This command points to access-list 100, which determines which IP packets will be interesting.

```
line con 0
line aux 0
line vty 0 4
password test
login
!
end
```

Ejemplo de configuración de ISDN en enrutador C4500

```
C4000#wr t
#####
Current configuration:
!
version 10.2
!
hostname C4000
```

```
enable password test
!
username C2503 password cisco
isdn switch-type basic-dms100
!
interface Ethernet0
ip address 192.168.24.65 255.255.255.0
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
ip address 172.16.20.2 255.255.255.0
encapsulation ppp
bandwidth 56
dialer idle-timeout 300
dialer map ip 172.16.20.1 name C2503 speed 56 broadcast 14085554321
dialer map ip 172.16.20.1 name C2503 speed 56 broadcast 14085559876
dialer hold-queue 5
dialer load-threshold 100
dialer-group 1
isdn spid1 415555123401 5551234
isdn spid2 415555678901 5556789
ppp authentication chap
!
router igrp 1
network 172.16.0.0
network 192.168.24.0
!
ip route 172.16.10.0 255.255.255.0 172.16.20.1
access-list 100 deny ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
dialer-list 1 list 100

line con 0
line aux 0
line vty 0 4
password test
login
!
end
```

Explicación de configuración

```

C4000#wr t
#####
Current configuration:
!
version 10.2
!
hostname C4000
!
enable password test
!
username C2503 password cisco

```

The username "C2503" is the hostname of the remote router and is used by the dialer map command below. The username is case sensitive and must match the remote router's hostname exactly.

The password, which is used by the CHAP authentication process, is case sensitive and must match the remote router's password exactly.

Note: To avoid confusion, the unencrypted form of the password cisco is shown in this sample configuration. In the actual configuration, the password would appear in its encrypted form: 7 13061E010803, where 7 denotes the encryption type and 13061E010803 is the encrypted form of the password cisco. When entering or making changes to the username command, always type the password in its unencrypted form and do not enter the encryption type (7). It is set automatically.

```

isdn switch-type basic-dms100

```

The ISDN switch type must match your carrier's equipment. If you change the switch-type you must reload the router for the new switch type to take effect.

```

interface Ethernet0
ip address 192.168.24.65 255.255.255.0

```

```

interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
ip address 172.16.20.2 255.255.255.0

```

```

encapsulation ppp

```

PPP encapsulation is recommended over HDLC in order to allow the use of CHAP authentication.

bandwidth 56

The default bandwidth setting for a BRI interface is 64k. If you configured your dialer map statements with the speed 56 option, you should include the bandwidth statement.

Note: This command does not control the speed of your ISDN line. It sets the correct reference point for the BRI port's show interface statistics, for the dialer load-threshold command, and for IGRP/EIGRP routing metrics.

dialer idle-timeout 300

This command sets the number of seconds the ISDN connection will remain open if no interesting traffic is being routed. The timer is reset each time an interesting packet is forwarded.

```
dialer map ip 172.16.20.1 name C2503 speed 56 broadcast 14085554321
dialer map ip 172.16.20.1 name C2503 speed 56 broadcast 14085559876
```

The dialer map command is used with CHAP authentication to place the initial call to the remote router when interesting traffic is forwarded to the BRI interface. After the connection is active, the dialer idle-timeout command determines how long it will remain active. A dialer map statement is required for each ISDN phone number that will be called. Be aware though, that two dialer map statements pointing to the same location might activate both B channels when you may only want to use one channel.

Note: The command parameters for this example are:

172.16.20.1 = the IP address of the remote router's BRI interface. To determine this address, type show interface bri 0 at the remote router's console prompt.

name C2503 = the hostname of the remote router. The name is case sensitive and should match the name configured for the username command above.

speed 56 = sets the dialer speed to 56k for ISDN circuits that are not 64k end-to-end, and should be included in both routers' dialer map statements. Most installations in North America must be configured for 56K.

broadcast = allows the forwarding of broadcast packets. Unless broadcast packets are specified as interesting packets by the dialer-list command, they will only be forwarded when the ISDN link is active.

14085554321

14085559876 = the remote router's ISDN telephone numbers.

dialer hold-queue 5

This command allows interesting packets to be queued until the ISDN connection is established. In this example, five interesting packets will be queued.

dialer load-threshold 100

This command is used to configure bandwidth on demand by setting the maximum load before the dialer places another call through the second B channel. The load is the calculated weighted average load value for the interface, where 1 is unloaded and 255 is fully loaded. The actual load value you should configure depends on the characteristics of your particular network. In this example, the second B channel will be activated when the load reaches 39% of maximum utilization, which is 100 divided by 255.

dialer-group 1

The dialer-group 1 command enables the dialer-list 1 on the BRI interface, which determines which packets will be interesting and activate the ISDN connection.

```
isdn spid1 415555123401 5551234
isdn spid2 415555678901 5556789
```

The isdn spid commands are used if your carrier assigns spids to your ISDN lines.

ppp authentication chap

This command enables CHAP authentication.

```
router igrp 1
network 172.16.0.0
network 192.168.24.0
ip route 172.16.10.0 255.255.255.0 172.16.20.1
```

This ip route command creates a static route to the remote router's network via the remote router's BRI interface. This is required because dynamic routes are lost when the ISDN link is down.

Note: The command parameters for this example are:

172.16.0.0 = the target network.

255.255.0.0 = the target network mask. A 255 in an octet's position specifies an exact match for that octet is required, and a 0 in an octet's position specifies any value will match.

172.16.20.1 = the address of the next hop that can be used to reach the target network.

```
access-list 100 deny ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

This access list determines which IP packets will be interesting and activate the ISDN link. The access-list you should create depends on your particular network design.

Note: The command parameters for this example are:

```
access-list 100 deny ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.
```

defines all broadcast packets as uninteresting.

```
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

defines all other IP packets as interesting.

```
dialer-list 1 list 100
```

This command points to access-list 100, which determines which IP packets will be interesting.

```
line con 0  
line aux 0  
line vty 0 4  
password test  
login  
!  
end
```

APENDICE B

CATALOGOS

Cisco 2500 Series

Note Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

Product Overview

The Cisco 2500 series routers provide a variety of models designed for small office and remote site environments. Each model supports at least two of the following interfaces:

- Ethernet
- Token Ring
- Synchronous serial
- Asynchronous serial
- ISDN BRI
- Hub

Cisco 2500 routers come with Flash EPROM technology for simplified software maintenance. These systems support a variety of Cisco IOS software feature sets, so you can choose a feature set that supports your specific protocol environment. The software feature sets range from an IP and bridging-only to the full array of Cisco's software functionality, including APPN and RMON.

Mission-specific models contain less memory and less hardware functionality in order to support a subset of protocols. Each mission-specific model can be upgraded to full router capability by downloading a new Cisco IOS software feature set and, if necessary, adding memory.

Cisco 2500 series model numbers ending with -CH are available either through the Cisco authorized reseller channel, or through your local Cisco sales office. Hardware options can also be ordered through the Cisco authorized reseller channel.

Cisco 2500 series models can be divided into the following categories:

- Single LAN routers---Models 2501, 2501-CH, 2502, 2502-CH, 2503, 2503-CH, 2504, 2504-CH, 2520, 2520-CH, 2521, 2521-CH, 2522, 2522-CH, 2523, and 2523-CH.
- Mission-specific, entry-level routers---Models 2501CF, 2502CF, 2503I, 2504I, 2520CF, 2520LF, 2521CF, 2521LF, 2522CF, 2522LF, 2523CF, and 2523LF
- Router/hub combinations---Models 2505, 2505-CH, 2507, 2507-CH, 2516, 2516-CH, 2517, 2518, and 2519
- Access servers---Models 2509 to 2512 (refer to the section "Cisco 2500 Series Access Servers" in the chapter "Access Servers," later in the catalog)
- Dual LAN routers---Models 2513, 2513-CH, 2514, 2514-CH, 2515, and 2515-CH
- Modular routers---Models 2524, 2514-CH, 2525, and 2525-CH

Standard Features

All the Cisco 2500 series models support the features listed in Table 140.

Table 140 : Cisco 2500 Series Summary of Features

Characteristic	Description																												
Flash memory	Minimum of 8 MB of Flash memory; however, depending on the Cisco IOS release that shipped with the system, it might require more memory. Refer to <u>Table 152</u> and <u>Table 153</u> , later in this chapter, for the minimum Flash memory required for each feature set. ¹																												
DRAM memory expandability	Minimum DRAM required by the Cisco IOS release that shipped with the system. Refer to <u>Table 152</u> and <u>Table 153</u> , later in this chapter, for the minimum DRAM required for each feature set.																												
Processor type	20-MHz 68030																												
Software options---Cisco IOS Release 11.2	<table style="width: 100%; border: none;"> <tr> <td style="width: 20%;">IP</td> <td style="width: 40%;"></td> <td style="width: 20%; text-align: right;">Routing</td> <td style="width: 20%;"></td> </tr> <tr> <td>IP/IPX</td> <td>with IBM base functionality and</td> <td>Plus</td> <td></td> </tr> <tr> <td>Desktop</td> <td>(IP/IPX/AppleTalk/DEC)</td> <td>APPN</td> <td></td> </tr> <tr> <td>Desktop</td> <td>(IP/IPX/AppleTalk/DEC)</td> <td>Plus</td> <td></td> </tr> <tr> <td>Enterprise</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enterprise</td> <td></td> <td></td> <td>Plus</td> </tr> <tr> <td>Enterprise/APPN/Plus</td> <td></td> <td></td> <td></td> </tr> </table>	IP		Routing		IP/IPX	with IBM base functionality and	Plus		Desktop	(IP/IPX/AppleTalk/DEC)	APPN		Desktop	(IP/IPX/AppleTalk/DEC)	Plus		Enterprise				Enterprise			Plus	Enterprise/APPN/Plus			
IP		Routing																											
IP/IPX	with IBM base functionality and	Plus																											
Desktop	(IP/IPX/AppleTalk/DEC)	APPN																											
Desktop	(IP/IPX/AppleTalk/DEC)	Plus																											
Enterprise																													
Enterprise			Plus																										
Enterprise/APPN/Plus																													

	Mission-specific Cisco 2500 series: application-specific software
Software options---Cisco IOS Release 11.1 and 11.0	IP Routing with IBM base functionality IP/IPX Routing with IBM base functionality and APPN ² Desktop with IBM base functionality Enterprise/APPN ² RMON
	Mission-specific Cisco 2500 series: application-specific software
Dimensions (H x W x D)	Models 2501 to 2516 and 2520 to 2525: 1.75 x 17.5 x 10.56 in. (4.44 x 44.45 x 26.82 cm) Models 2517 to 2519: 3.0 x 19.0 in. (7.62 x 48.26 cm)
Weight (average shipping)	Models 2501 to 2516 and 2520 to 2525: 10 lb (4.5 kg) Models 2517 to 2519: 12.5 lb (5.7 kg)
Standard components	Power supply and cord kit ³ Console cable adapter RJ-45-to-DB-9 19 in. rack-mount/wall-mount kit

¹ If your system requires more than 8MB of Flash memory, the additional memory must be ordered separately.

² This feature set is available with Cisco IOS Release 11.0 and later releases.

³ The console cable kit includes an RJ-45-to-RJ-45 roll-over console cable, an RJ-45-to-DB-25 male DCE adapter, an RJ-45-to-DB-25 female DTE adapter, and an RJ-45-to-DB-9 female DTE adapter.

The environmental specifications for the Cisco 2500 series are listed in Table 141.

Table 141 : Cisco 2500 Series Environmental Specifications

Description	Specification
Consumption	For models 2501 to 2525: 40W
Input	For models 2501 to 2516 and 2520 to 2525: 110 to 220 VAC ¹ , 50 to 60 Hz --48 VDC ² For models 2517 to 2519: 90 to 260 VAC, 47 to 63 Hz
Current rating	For models 2501 to 2516 and 2520 to 2525: 1.0A at 60 Hz, 0.5A at 50 Hz For models 2517 to 2519: 5.0A at 60 Hz, 3.5 A at 50 Hz
Operating	For models 2501 to 2516 and 2520 to 2525: 32 to 104°F (0

temperature range	to 40°C) For models 2517 to 2519: 50 to 95°F (10 to 35°C)
Nonoperating temperature range	For models 2501 to 2516 and 2520 to 2525: --40 to 185°F (to 85°C) For models 2517 to 2519: --4 to 185°F (--20 to 85°C)
Humidity (noncondensing)	For models 2501 to 2525: 5 to 95%

¹ VAC = volts alternating current.

² VDC = volts direct current.

Hardware

The Cisco 2500 series routers are discussed in the following sections:

Memory Options

All Cisco 2500 models include a minimum of 8 MB of Flash memory; however, depending on the Cisco IOS software release shipped with the system, it might require more memory. Additional Flash memory can be purchased to allow for dual banking or potential future code growth.

There are two types of DRAM memory in the Cisco 2500 series routers: primary and shared (packet). Primary memory is used to store the operating configuration, routing tables, caches, queues, and packets. Shared memory is used to store incoming and outgoing packets. In [Table 142](#), the physical configuration column lists the amount of DRAM SIMM memory supported. The system usage column lists how the system allocates the total DRAM memory installed.

Table 142 : Shared and Primary DRAM Memory—Cisco 2500 Series

Total DRAM Memory	Physical Configuration	System Usage	
	DRAM SIMM	Shared DRAM Memory	Primary DRAM Memory
4 MB	4 MB	2 MB	2 MB
8 MB	8 MB	2 MB	6 MB
16 MB	16 MB	2 MB	14 MB

Table 143 : Cisco 2500 Series Hardware Options

Description	Product Number
Rack-Mount Kits	
19-in. rack-mount kit ¹	ACS-2500RM-19=
24-in. rack-mount kit	A25-2500RM-24=
Memory Options	
Boot ROM upgrade	BOOT-2500=
4-MB DRAM	MEM-1X4D
4-MB DRAM (spare)	MEM-1X4D=
8-MB DRAM	MEM-1X8D
8-MB DRAM (spare)	MEM-1X8D=
16-MB DRAM	MEM-1X16D
16-MB DRAM (spare)	MEM-1X16D=
4-MB Flash SIMM	MEM-1X4F
4-MB Flash SIMM (spare)	MEM-1X4F=
8-MB Flash SIMM	MEM-1X8F
8-MB Flash SIMM (spare)	MEM-1X8F=
4- to 8-MB Flash SIMM upgrade ²	MEM-1X8F-U
4- to 8-MB Flash SIMM upgrade ³ (Cisco 2517, Cisco 2518, and Cisco 2519 only)	MEM-1X8F-DFB-U
8-MB dual-bank Flash SIMM ⁴ (Cisco 2517, Cisco 2518, and Cisco 2519 only) (spare)	MEM-1X8F-DFB=
16-MB dual-bank Flash SIMM ⁵ (Cisco 2517, Cisco 2518, and Cisco 2519 only)	MEM-1X16F-DFB
16-MB dual-bank Flash SIMM ⁵ (Cisco 2517, Cisco 2518, and Cisco 2519 only) (spare)	MEM-1X16F-DFB=
Modules	
2-wire switched 56-kbps CSU/DSU module (for Cisco 2524 and Cisco 2525 routers only)	SM25-56K2

4-wire 56/64-kbps DSU/CSU module (for Cisco 2524 and Cisco 2525 routers only)	SM25-56K4
Fractional T1/T1 DSU/CSU module (for Cisco 2524 and Cisco 2525 routers only)	SM25-T1
Five-in-one synchronous serial module (for Cisco 2524 and Cisco 2525 routers only)	SM25-5IN1
ISDN BRI module (for Cisco 2524 and Cisco 2525 routers only)	SM25-BRI-S/T
ISDN with integrated NT1 device module (for Cisco 2524 and Cisco 2525 routers only)	SM25-BRI-U
Blank slot cover (for Cisco 2524 and Cisco 2525 routers only)	SM25-BLANK
Redundant Power Systems	
600W redundant AC power system for the Cisco 2500 series routers	PWR-600-AC-RPS
Redundant power supply 22/18 OIR Y-load cable	CAB-RPSY-2208
Redundant power supply 22/18 load cable	CAB-RPS-2218=
Redundant power supply 22/08 load cable	CAB-RPS-2208=
Redundant power supply field upgrade for Cisco 2500 series routers	ACS-2500RPS=
Cables	
EIA/TIA-232 male DTE interface, 10 ft (3 m)	CAB-232MT
EIA/TIA-232 female DCE interface, 10 ft (3 m)	CAB-232FC
EIA/TIA-449 male DTE interface, 10 ft (3 m)	CAB-449MT
EIA/TIA-449 female DCE interface, 10 ft (3 m)	CAB-449FC
EIA-530 male DTE interface, 10 ft (3 m)	CAB-530MT
V.35 male DTE interface, 10 ft (3 m)	CAB-V35MT
V.35 female DCE interface, 10 ft (3 m)	CAB-V35FC
X.21 male DTE interface, 10 ft (3 m)	CAB-X21MT
X.21 female DCE interface, 10 ft (3 m)	CAB-X21FC

Ethernet AUI adapter cable	CAB-3CE18=
Auxiliary/console cable kit ⁶	ACS-2500ASYN
RJ-45-to-DB-25 management card console cable ⁷	CAB-MGMT-RH
Shielded power cable, United States ⁷	CABS-AC
Shielded power cable, Australia ⁷	CABS-ACA
Shielded power cable, Italy ⁷	CABS-ACI
Shielded power cable, Europe ⁷	CABS-ACE
Shielded power cable, United Kingdom ⁷	CABS-ACU

¹ The 19-inch rack-mount kit can only be ordered as a spare; a 19-inch rack-mount kit is included with all Cisco2500 series routers. An optional 24-inch rack-mount kit can be ordered from Cisco Systems.

² Applies to Cisco IOS Release 11.x feature sets that require more than 4-MB Flash memory. Not available as a spare. Supported on the Cisco 2517, 2518, 2519, and AccessPro PC cards.

³ Applies to Cisco IOS Release 11.x feature sets that require more than 4-MB Flash memory. Not available as a spare. Supported on the Cisco 2517, 2518, 2519, AccessPro PC cards, and AS5100 access servers.

⁴ Dual-bank Flash memory is required for Cisco 2517, 2518, 2519, AccessPro PC cards, and AS5100 access servers because these models contain only one slot for Flash memory. It can operate as either two banks of 4 MB for dual-Flash bank operation or as 8 MB contiguous. Supported on the Cisco 2517, 2518, 2519, AccessPro PC cards, and AS5100 access servers.

⁵ Dual-bank Flash memory is required for Cisco 2517, 2518, 2519, AccessPro PC cards and AS5100 access servers because these models contain only one slot for Flash memory. It can operate as either two banks of 8 MB for dual-Flash bank operation or as 16 MB contiguous. Supported on the Cisco 2517, 2518, 2519, AccessPro PC cards, and AS5100 access servers.

⁶ The auxiliary/console cable kit includes an RJ-45-to-RJ-45 roll-over console cable, an RJ-45-to-DB-25 male DCE adapter, an RJ-45-to-DB-25 female DTE adapter, and an RJ-45-to-DB-9 adapter.

⁷ Applies to the Cisco2517, Cisco2518, and Cisco2519 router/hubs only.

Access Servers

Models 2509, 2509-CH, 2510, 2511, 2511-CH, and 2512 are designed to function as access servers for remote node and asynchronous/synchronous routing. For complete information, refer to the chapter "[Access Servers](#)" later in the catalog.

Dual LAN Routers

Models 2513, 2513-CH, 2514, 2514-CH, 2515, and 2515-CH (see [Figure 141](#) through [Figure 143](#)) provide higher density LAN support and include all the common features listed in [Table 140](#). In addition, these models support the interfaces listed in

Table 147.

Table 147 : Dual LAN Router Interface Options

Model	Ethernet	Token Ring	Serial	ISDN BRI
2513 2513-CH (reseller channel)	1	1	2	0
2514 2514-CH (reseller channel)				
2515 2515-CH (reseller channel)	0	2	2	0

Modular Routers

Models 2524, 2524-CH, 2525, and 2525-CH provide LAN and WAN access in a low-cost modular router platform that can grow with your internetworking needs. The Cisco 2524 offers an Ethernet (AUI or 10BaseT) LAN connection, and the Cisco 2525 offers a Token Ring (STP or UTP) LAN connection. Both routers can accommodate up to three WAN modules—two synchronous serial and one ISDN.

The choice of synchronous serial WAN modules is as follows:

- 2-wire, switched, 56-kbps DSU/CSU
- 4-wire, 56/64-kbps DSU/CSU
- Fractional T1/T1 DSU/CSU
- Five-in-one synchronous serial

The choice of ISDN WAN modules is as follows:

- ISDN BRI
- ISDN with integrated NT1 device

The ISDN WAN modules are keyed so that you cannot insert them into the synchronous serial WAN slots. A blank slot cover is installed over unused slots.

Software

The Cisco 2500 series offers the following types of feature sets:

- Basic. The basic feature set for the hardware platform.
- Plus. The basic feature set plus additional features.

- Plus 40. The basic feature set, plus features, and 40-bit data encryption.
- Plus 56. The basic feature set, plus features, and 56-bit data encryption.

Note Cisco IOS images with 40-bit Data Encryption Standard (DES) support may legally be distributed to any party eligible to receive Cisco IOS software. 40-bit DES is not a cryptographically strong solution so its use should be carefully evaluated.

Cisco IOS images with 56-bit DES are possibly subject to export and/or import controls and may have a limited distribution. For more information, contact your sales representative or distributor, or visit CCO at <http://www.cisco.com/www/export/encrypt.html>, or send e-mail to export@cisco.com.

The Cisco IOS feature set tables use the following conventions to identify features:

- X : the feature is offered in the basic feature set
- -- : the feature is not offered in the feature set
- Plus: the feature is offered in the Plus feature sets
- Encrypt: the feature is offered in the Encryption (Plus 40 and Plus 56) feature sets

Cisco 4000 Series

Note Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

Product Overview

The Cisco 4000 series consists of the Cisco 4000, Cisco 4000-M, Cisco 4500, Cisco 4500-M, Cisco 4700, and Cisco 4700-M routers. Although the Cisco 4000, Cisco 4500, and Cisco 4700 routers are no longer orderable, they are still supported. The Cisco 4000, Cisco 4500, and Cisco 4700 routers have been replaced by the Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M routers.

The Cisco 4000 series routers run Cisco IOS software, Cisco's industry-leading networking software that provides a variety of feature sets. You can choose a feature set that supports your specific protocol environment. Cisco IOS software assures robust, reliable internetworks by supporting both LAN and WAN protocols, optimizing WAN services, and controlling internetwork access. In addition, Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks.

The Cisco 4000 series routers offer Flash EPROM technology as a standard feature. Flash EPROMs enable you to distribute new software releases from a central location. After the software is distributed, the routers can reboot from programs stored in local Flash memory.

All models provide a configurable modular router platform by using network processor modules (NPMs)---individual removable cards used for external network connections. Because the router's modules support many variations of protocols, line speeds, and transmission media, the Cisco 4000 series can accommodate all types of network computing environments. As Cisco introduces new modules, the Cisco 4000 series can be upgraded to keep pace with technological advances.

The Cisco 4000 series routers can support combinations of up to three of the following NPMs:

- 1-, 2-, or 6-port Ethernet
- 1-port Fast Ethernet
- 1- or 2-port Token Ring

- 1-port multimode FDDI (both single [SAS] and dual attachment station [DAS])
- 1-port single-mode FDDI (DAS)
- 2- or 4-port synchronous serial
- 2-port high-speed serial and 16-port low-speed serial
- 4- or 8-port ISDN BRI
- 1-port channelized T1/ISDN PRI
- 1-port channelized E1/ISDN PRI (balanced or unbalanced)
- 4-port serial G.703 and G.704 (balanced or unbalanced)
- 1-port HSSI
- 1-port ATM (single-mode or multimode) OC-3c
- 1-port ATM DS-3
- 1-port ATM E3

Table 116 : Cisco 4000 Series Summary of Features

Characteristic	Cisco 4000-M	Cisco 4500-M	Cisco 4700-M ¹
Supported network interfaces	Ethernet Token Ring FDDI Serial ISDN BRI Channelized E1/T1 ISDN PRI	Ethernet Token Ring FDDI HSSI High-density serial ISDN BRI Channelized E1/T1 ISDN PRI ATM OC-3c DS-3 ATM E3	Ethernet Token Ring FDDI HSSI High-density serial ISDN BRI Channelized E1/T1 ISDN PRI ATM OC-3c DS-3 ATM E3
Slots available for modules	3	3	3
Software options--- Cisco IOS Release 11.2	IP IP Plus 40 IP Plus 56 Desktop (IP/IPX/AppleTalk)	IP IP Plus 40 IP Plus 56 Desktop (IP/IPX/AppleTalk/DEC)	IP IP Plus 40 IP Plus 56 Desktop (IP/IPX/AppleTalk/DE

	k/DEC) Desktop (IP/IPX/AppleTalk/DEC) Plus k/DEC) Plus Desktop (IP/IPX/AppleTalk/DEC) Plus 40 k/DEC) Plus 40 Desktop (IP/IPX/AppleTalk/DEC) Plus 56 k/DEC) Plus 56 IP/IPX/APPN with IBM base functionality with IBM base Enterprise functionality Enterprise Plus 40 Enterprise Plus 56 Enterprise Plus 40 Enterprise Plus 56 Enterprise Plus 40 Enterprise Plus 56 Enterprise/APPN Plus 40 Enterprise/APPN Plus 56 Plus Enterprise/APPN Plus 40 Enterprise/APPN Plus 56	Desktop (IP/IPX/AppleTalk/DEC) Plus Desktop (IP/IPX/AppleTalk/DEC) Plus 40 Desktop (IP/IPX/AppleTalk/DEC) Plus 56 IP/IPX/APPN with IBM base functionality Enterprise Plus 40 Enterprise Plus 56 Enterprise/APPN Plus 40 Enterprise/APPN Plus 56	C) Desktop (IP/IPX/AppleTalk/DEC) Plus C) Desktop (IP/IPX/AppleTalk/DEC) Plus 40 C) Desktop (IP/IPX/AppleTalk/DEC) Plus 56 C) IP/IPX/APPN with IBM base functionality Enterprise Plus 40 Enterprise Plus 56 Enterprise Plus 40 Enterprise Plus 56 Enterprise/APPN Plus 40 Enterprise/APPN Plus 56
Software options--- Cisco IOS Release 11.0 and 11.1	IP Routing IP Routing with IBM base functionality IP/IPX Routing with IBM base functionality IP/IPX/APPN with IBM base functionality Desktop Desktop with IBM base functionality Enterprise Enterprise/APPN	IP Routing IP Routing with IBM base functionality IP/IPX Routing with IBM base functionality IP/IPX/APPN with IBM base functionality Desktop Desktop with IBM base functionality Enterprise Enterprise/APPN	IP Routing IP Routing with IBM base functionality IP/IPX Routing with IBM base functionality IP/IPX/APPN with IBM base functionality Desktop Desktop with IBM base functionality Enterprise Enterprise/APPN
Processor type	40-MHz 68030	100-MHz IDT Orion RISC	133-MHz IDT Orion RISC
Flash memory	4 MB standard, expandable to 8 or 16 MB	4 MB standard, expandable to 8 or 16 MB	4 MB standard, expandable to 8 or 16 MB

Main memory	8 MB standard, expandable to 16 or 32 MB	16 MB standard, expandable to 32 MB	16 MB standard, expandable to 32 or 64 MB
Shared memory	4 MB ² standard, expandable to 16 MB	4 MB standard, expandable to 8 or 16 MB	4 MB standard, expandable to 8 or 16 MB
Nonvolatile random-access memory (NVRAM)	128 KB	128 KB	128 KB
Dimensions (H x W x D)	3.4 x 17.6 x 17.7 in. (8.6 x 44.7 x 43.4 cm)	3.4 x 17.6 x 17.7 in. (8.6 x 44.7 x 43.4 cm)	3.4 x 17.6 x 17.7 in. (8.6 x 44.7 x 43.4 cm)
Weight (average shipping)	24 lb (10.9 kg)	24 lb (10.9 kg)	24 lb (10.9 kg)
Agency approvals	UL 1950, CSA 22.2, TÜV-GS mark, EN 60950, FCC Class A, Canadian DOC Class A, VDEA, VDE Class B, EN 55022 Class B, VCCI Class 2	UL 1950, CSA 22.2, TÜV-GS mark, EN 60950, FCC Class A, Canadian DOC Class A, VDEA, VDE Class B, EN 55022 Class B, VCCI Class 2	UL 1950, CSA 22.2, TÜV-GS mark, EN 60950, FCC Class A, Canadian DOC Class A, VDEA, VDE Class B, EN 55022 Class B, VCCI Class 2

¹ The Cisco 4700-M includes an additional 64-MB main memory option, which was not available for the Cisco 4700. The 64-MB option significantly increases the routing table sizes that can be supported in the router.

² Cisco4000 routers and early versions of Cisco4000-M routers shipped with 1MB of standard shared memory. Those systems must be upgraded to 4MB of shared memory when you install an FDDI interface or have more than five physical or virtual interfaces.

Table 117 : Cisco 4000 Series Environmental Specifications

Description	Specification
Consumption	200W (682 Btu ¹ /hour)
Input	100 to 240 VAC ²
Frequency	47 to 63 Hz

Current rating	3.0A @ 100V; 1.5A @ 240V
Operating temperature range	32 to 104°F (0 to 40°C)
Nonoperating temperature range	--40 to 185°F (--40 to 85°C)
Humidity (noncondensing)	5 to 95%

¹ Btu = British thermal units.

² VAC = volts alternating current.

Standard Features

Cisco 4000 series routers have the following standard features:

- Three slots for NPMs, which can be Ethernet, Token Ring, FDDI, HSSI, ISDN BRI, ISDN PRI, ATM, or serial network interfaces. See the section "Hardware" in this chapter for configuration information.
- 40-MHz 68030 processor (Cisco 4000-M), 100-MHz IDT Orion RISC (Cisco 4500-M), or 133-MHz IDT Orion RISC (Cisco 4700).
- 8 MB (Cisco 4000-M) or 16 MB (Cisco 4500-M and Cisco 4700-M) of expandable RAM.
- 128 KB of NVRAM.
- 4 MB of expandable Flash memory.
- 4 MB of expandable shared memory.
- AC or DC power supply. (The Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M offer both AC and DC power supplies.)
- Power cord.

Hardware

Network Processor Modules

Cisco 4000 series routers support combinations of up to three network processor modules (NPMs). Table 118 describes the maximum number of each module supported by a specific system and the minimum Cisco IOS software release required for each module. Table 118 also lists product numbers for the NPMs.

Table 118 : NPM Configurations--Cisco 4000 Series

NPM Type	Cisco 4000	Cisco 4500, Cisco 4500-	Minimum Cisco IOS	Product Number	Hardware Restrictions
----------	------------	----------------------------	----------------------	-------------------	-----------------------

	and Cisco 4000-M	M, Cisco 4700-M ¹	Software Release Required	s	with Other NPMs
1-port 10BaseT Ethernet	3	--	9.14(1)	NP-1E	No restrictions
1-port 100BaseT X Fast Ethernet	--	2	11.1(5) ²	NP-1FE	If one NP-1FE is installed, only one ATM or one FDDI module can be installed in the same router. If two NP-1FEs are installed, you cannot install any ATM or FDDI modules in the same router. Full-duplex mode is supported only when the Fast Ethernet module is the sole high-speed module configured.
2-port 10BaseT Ethernet	3	3	9.14(1)	NP-2E	No restrictions
6-port 10BaseT Ethernet	--	3	10.3(6)	NP-6E	No restrictions
1-port Token Ring	3	3	9.14(5)	NP-1RV2	No restrictions
2-port Token Ring	3	3	9.14(5)	NP-2R	No restrictions
1-port single attachment multimode FDDI	1	2	9.14(1)	NP-1F-S-M	Maximum of two high-speed modules can be installed per router.
1-port dual attachment multimode FDDI	1	2	9.14(1)	NP-1F-D-MM	Maximum of two high-speed modules can be installed per router.

1-port dual attachment single-mode FDDI	1	2	9.14(3)	NP-1F-D-SS	Maximum of two high-speed modules can be installed per router.
2-port serial	3	3	9.14(6)	NP-2T ³	No restrictions
4-port serial	3	3	10.1	NP-4T	4 Mbps maximum speed per interface.
2-port high-speed synchronous and 16-port low-speed synchronous	--	2	11.2(3)P	NP-2T16S-V.35 NP-2T16S-RS232 NP-2T16S-X21	Maximum of two 2-port high-speed synchronous and 16-port low-speed synchronous modules can be installed per router. No restrictions with other modules.
1-port HSSI	--	2	11.2(5)P	NP-1HSSI	Maximum of two HSSI modules when both are run at high speeds. Maximum of 12 Mbps per HSSI when two HSSI modules are configured and another high-speed module is also installed.
4-port ISDN BRI	2	2	10.2	NP-4B ⁴	Not compatible with the three PRI modules, unless the PRI modules are configured for channelized service.
8-port ISDN BRI	1	2	10.2	NP-8B ⁴	Not compatible with the three PRI modules, unless the PRI modules are configured for channelized service.
1-port channelized T1/ISDN PRI	1	2	10.3(4)	NP-CT1	When configured for PRI, the NP-CT1 is not compatible with the 4- and 8-port ISDN BRI modules. Is compatible with these modules when

					configured for channelized service.
1-port channelized E1/ISDN PRI, unbalanced	1	2	10.3(4)	NP-CE1U	When configured for PRI, the NP-CE1U is not compatible with the 4- and 8-port ISDN BRI modules. Is compatible with these modules when configured for channelized service.
1-port channelized E1/ISDN PRI, balanced	1	2	10.3(4)	NP-CE1B	When configured for PRI, the NP-CE1B is not compatible with the 4- and 8-port ISDN BRI modules. Is compatible with these modules when configured for channelized service.
4-port serial E1/G.703 and E1/G.704, unbalanced	3	3	10.2(4)	NP-4GU	No restrictions
4-port serial E1/G.703 and E1/G.704, balanced	3	3	10.2(4)	NP-4GB	No restrictions
1-port single-mode ATM OC-3c	1	1	10.3(4)	NP-1A-SM	Maximum of two high-speed modules can be installed per router.
1-port multimode ATM OC-3c	1	1	10.3(4)	NP-1A-MM	Maximum of two high-speed modules can be installed per router.
1-port ATM DS-3	1	2	11.0(5)	NP-1A-DS3	Maximum of two high-speed modules can be installed per router.

1-port ATM E3	1	11.0(5)	NP-1A- E3	No restrictions
------------------	---	---------	--------------	-----------------

¹ A maximum of two high-speed interfaces is supported on the Cisco4500 and Cisco4700 routers. This includes Fast Ethernet, FDDI, and ATM OC-3 or DS-3. The only exception to this rule is that you cannot configure more than one ATM OC-3 on a single router.

² For Cisco IOS Release 11.2, the NPE-1FE NPM is not supported until Cisco IOS Release 11.2(2)P.

³ The NP-2T does not support half-duplex, but the NP-4T does.

⁴ A maximum of either two NP-4B NPMs or one NP-8B NPM is supported on the Cisco4000 or Cisco4000-M routers.

Memory Options

All Cisco 4000 series routers share the same physical design. Each router offers three slots for LAN or WAN connectivity and uses the same optional NPMs and software features for compatibility and investment protection. Three different types of memory are available for the Cisco 4000 series---main memory, shared memory, and system Flash memory. Each type of memory serves a different purpose in routing packets from one interface to another. The benefit of this architecture is that the system can read program instructions or routing table data from main memory at the same time as it is moving packets between interfaces (using shared memory), thus increasing overall system performance and lowering network latency.

Factors That Affect Memory Requirements

You can change memory configurations in the Cisco 4000 series to accommodate internetworking demands. The memory requirements are driven by the following three factors:

- Main DRAM memory---can be upgraded to allow for network expansion, the use of additional protocols or Cisco IOS services, or newer Cisco IOS software releases.
- Shared DRAM memory---can be upgraded to improve I/O performance or to use higher densities or more physical or virtual interfaces.
- Flash memory---can be upgraded to hold several Cisco IOS software images for easy management.

Main DRAM Memory

The Cisco 4000 series runs from an image stored in main DRAM. This memory is also used by the system for tables and stacks. The amount of main memory required is determined by the size of the image and by the configuration of the

internetwork. Cisco regularly publishes product bulletins that detail what memory is required for any particular Cisco IOS feature subset, and also releases documentation that specifies what memory is needed.

Shared DRAM Memory

The Cisco 4000 series routers use shared DRAM (also known as packet memory) for handling user data. The recommended amount of shared memory is determined by the type and number of physical or virtual interfaces supported by the router. Other factors that impact the amount of required shared memory are the type of routing selected and the degree of throughput to the various interfaces.

The standard configuration for shared DRAM is 4 MB for the Cisco 4000 series. This is sufficient for most configurations with fewer than 24 physical or virtual interfaces. For routers with 24 or more interfaces or B channels (for example, NP-9B, CT1, and CE1), upgrading to a minimum of 8 MB of shared memory is required.

Software Feature Sets

The Cisco 4000 series routers support the following software releases:

- Cisco IOS Release 11.2, 11.1, and 11.0 feature sets

Note For all Cisco 4000 series routers, software must be ordered separately from the chassis. Traditional software packaging is no longer included in the base price of the system.

The Cisco 4000, Cisco 4500, and Cisco 4700 routers are no longer orderable, but Cisco IOS Releases 11.2, 11.1, and 11.0 are supported on these routers. The Cisco 4000, Cisco 4500, and Cisco 4700 routers have been replaced by the Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M routers.

The Cisco 4000 series offers the following types of feature sets:

- **Basic.** The basic feature set.
- **Plus.** The basic feature set plus additional features.
- **Plus 40.** The basic feature set, plus features, and 40-bit data encryption.
- **Plus 56.** The basic feature set, plus features, and 56-bit data encryption.

Note Cisco IOS images with 40-bit Data Encryption Standard (DES) support may legally be distributed to any party eligible to receive Cisco IOS software. 40-bit DES is not a cryptographically strong solution so its use should be carefully evaluated.

Cisco IOS images with 56-bit DES are possibly subject to export and/or import

controls and may have a limited distribution. For more information, contact your sales representative or distributor, or visit CCO at <http://www.cisco.com/www/export/encrypt.html>, or send e-mail to export@cisco.com.

The Cisco IOS feature set tables use the following conventions to identify features:

- X : the feature is offered in the basic feature set
- -- : the feature is not offered in the feature set
- Plus: the feature is offered in the Plus feature sets
- Encrypt: the feature is offered in the Encryption feature sets

Cisco IOS Feature Set Upgrades

Cisco IOS feature set upgrades are easy to order for the Cisco 4000 series. The following is an example:

You have a Cisco 4500-M router running the Cisco IOS Release 11.2 IP Routing (basic) feature set. You want to upgrade to the Cisco IOS Release 11.2 Enterprise/APPN Plus 56 feature set. You are crossing three feature sets: one to get from IP to Enterprise, one to add APPN, and one to add Plus 56 (basic to plus). To complete the upgrade, use the following guidelines:

- Order FL45-CA= (IP to Enterprise upgrade license, charged item)
- Order FL45-APPN= (APPN upgrade license, charged item)
- Order FL45-Y= (Plus 56 upgrade license, charged item)
- Order additional DRAM and Flash card memory (if you do not have the minimum required DRAM and Flash card memory for the new feature set)
- Order SW45ANY-11.2.1= (Cisco IOS 4500/4700 Enterprise/APPN Plus 56 software on diskette, charged item)

Cisco 7000 Series

Product Overview

The Cisco 7000 series of multiprotocol routers includes the Cisco 7000 and the Cisco 7010. These routers combine Cisco Systems' proven software technology with exceptional reliability, availability, serviceability, and performance features to meet the requirements of today's most mission-critical internetworks. The Cisco 7000 series provides information system professionals with the flexibility they need to meet the constantly changing requirements at the core and distribution points of the internetwork. The Cisco 7000 series also provides a clear migration path to tomorrow's technologies.

Network interfaces reside on modular interface processors, which provide a direct connection between the CxBus and the external network, and support any combination of ATM, channelized T3, Ethernet, Fast Ethernet, FDDI, IBM channel attachment, multichannel E1 and T1, HSSI, synchronous serial, Token Ring, and Packet OC-3 interfaces. The Cisco 7000 router provides five slots for interface processors; the Cisco 7010 router provides three slots for interface processors.

In a standard Cisco 7000 series router, route processing and switching are accomplished by a Route Processor (RP), Switch Processor (SP), and Silicon Switch Processor (SSP). In a Cisco 7000 series router upgraded to Cisco 7500 functionality, route processing and switching are accomplished by the 7000 Series Route Switch Processor (RSP7000).

The Cisco 7000 series runs Cisco IOS software, Cisco's industry-leading networking software. Cisco IOS software assures robust, reliable internetworks by supporting both LAN and WAN protocols, optimizing WAN services, and controlling internetwork access. In addition, Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks.

The reliability, availability, and serviceability features of the Cisco 7000 series include the following:

- Online software reconfiguration---Enables software configuration changes to occur without rebooting or interrupting network applications and services.
- Online insertion and removal---Allows seamless upgrades to higher density and new interface processors without rebooting or taking the system offline. Reduces operator intervention because like interface processors are automatically reconfigured.
- Fast boot---Enables the system to come online quickly (35 seconds is typical) after software upgrades, minimizing impact on the network.
- Environmental monitoring---Alerts you to fluctuations before critical conditions occur, allowing proactive resolution while the system stays online.
- Self-diagnostics and tools---Ensures that modules are operational before

going online, eliminating potential network problems.

- Optional dual power supply systems (Cisco 7000 only)---Extends individual power supplies by load sharing.
- Flash memory and EPROM---Enables fast, reliable, software and microcode upgrades. Allows a single, centralized point of administration, obviating the need to visit each router site when upgrading software or microcode.

Table 86 : Cisco 7000 Series Summary of Features

Characteristic	Cisco 7000	Cisco 7010
Supported network interfaces	Ethernet 10BaseT, AUI ¹ , and 10BaseFL Fast Ethernet (100BaseT and MII) Token Ring FDDI (half and full duplex) HSSI Synchronous serial ATM Multichannel on T1 or E1 lines, ISDN Channelized T3 Packet OC-3 IBM channel	Ethernet 10BaseT, AUI ¹ , and 10BaseFL Fast Ethernet (100BaseT and MII) Token Ring FDDI (half and full duplex) HSSI Synchronous serial ATM Multichannel on T1 or E1 lines, ISDN PRI Channelized T3 Packet OC-3 IBM channel
Power supplies	2	1
Interface processor slots	5	3
System processor slots ²	2	2
Software options---Cisco IOS Release 11.2 ³	IP and basic Routing and VIP Desktop and IBM Desktop/IBM and APPN Desktop/IBM, APPN, and VIP Enterprise and VIP Enterprise and APPN Enterprise, APPN, and VIP	IP and VIP Routing and Desktop and IBM Desktop/IBM and VIP Desktop/IBM and APPN Desktop/IBM, APPN, and VIP Enterprise and VIP Enterprise and APPN Enterprise and APPN Enterprise, APPN,

		and VIP
Additional software options--- Cisco IOS Release 11.2 on Cisco 7000 series systems with an RSP7000 and RSP7000CI	IP and Encryption ⁴⁰ IP and Encryption 56 Desktop/IBM and Encryption 40 Desktop/IBM and Encryption 56 Desktop/IBM/APPN and Encryption 40 Desktop/IBM/APPN and Encryption 56 Enterprise and Encryption 40 Enterprise and Encryption 56 Enterprise/APPN and Encryption 40 Enterprise/APPN and Encryption 56	IP and Encryption 40 IP and Encryption 56 Desktop/IBM and Encryption 40 Desktop/IBM and Encryption 56 Desktop/IBM/APPN and Encryption 40 Desktop/IBM/APPN and Encryption 56 Enterprise and Encryption 40 Enterprise and Encryption 56 Enterprise/APPN and Encryption 40 Enterprise/APPN and Encryption 56
Software options--- Cisco Release 11.1 and 11.0 ³	IP Routing IP/IPX Routing and IBM IP/IPX Routing, IBM, and APPN Desktop and IBM Enterprise and IBM Enterprise, IBM, and APPN	IP Routing IP/IPX Routing and IBM IP/IPX Routing, IBM, and APPN Desktop and IBM Enterprise and IBM Enterprise, IBM, and APPN
Onboard memory	Flash RP: 4 MB standard	Flash RP: 4 MB standard
PCMCIA memory card	Flash RP: Optional 8 or 16 MB RSP7000: 8 MB, expandable to 40 MB (8, 16, or 20 MBs per card), 2 slots available	Flash RP: Optional 8 or 16 MB RSP7000: 8 MB, expandable to 40 MB (8, 16, or 20 MBs per card), 2 slots available
Processor type	RP: 25-MHz 68040 CPU, 16-MB RAM, 64-MB option available RSP7000: MIPS RISC, 32-MB RAM expandable to 128-MB	RP: 25-MHz 68040 CPU, 16-MB RAM, 64-MB option available RSP7000: MIPS RISC, 32-MB RAM expandable to 128-MB

Dimensions (H x W x D)	19.25 x 17.5 x 24.1 in. (48.9 x 44.45 x 61.34 cm)	10.5 x 17.5 x 17 in. (26.67 x 44.45 x 43.18 cm)
Weight (average shipping)	~149 lbs (~67.6 kg) with 5 interface processors and 2 power supplies	~83 lbs (~37.65 kg) with 3 interface processors and 1 power supply

¹ AUI = attachment unit interface.

² System processors include a combination of the Route Processor (RP) and Switch Processor (SP) (or Silicon Switch Processor [SSP]), or the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

³ Feature sets can be enhanced with VIP2 support, CIP2 support, and/or four feature licenses (WAN packet protocols, interdomain routing, Network Address Translation, and Netflow switching on the RSP7000).

⁴ All Encryption images include the NetFlow switching license.

Table 87 : Cisco 7000 Series Environmental Specifications

Description	Cisco 7000	Cisco 7010
AC-input power supplies	700W (2380 Btu ¹ /hour)	600W (2040 Btu/hour)
DC-input power supplies	1000W input requirement 700W power output 300W (1024 Btu/hr) heat dissipation 20A (-48 VDC)	800W input requirement 600W power output 300W (1024 Btu/hr) heat dissipation 18A (-40 VDC)
Input	100 to 240 VAC ² autoranging	100 to 240 VAC autoranging
Frequency	50 to 60 Hz autoranging	50 to 60 Hz autoranging
AC current rating	12A @ 100V; 6A @ 240V	9A @ 100V; 4A @ 240V
Airflow	140 cfm ³ through the system blower	Side-to-side through chassis by variable-speed, 6-fan array
Radiated acoustic noise	62 dB ⁴	47 dB
Operating temperature	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)

Nonoperating temperature range	-40 to 185°F (-40 to 85°C)	-4 to 149°F (-20 to 65°C)
--------------------------------	----------------------------	---------------------------

¹ Btu = British thermal units.
² VAC = volts alternating current.
³ cfm = cubic feet per minute.
⁴ dB = decibels

Standard Features

The Cisco 7000 series base system includes the following standard features:

- System chassis, which includes a single power supply
- Three slots for interface processors for the Cisco 7010; five slots for interface processors for the Cisco 7000
- AC-input and DC-input power supplies
- Dual AC-input and DC-input power supplies (Cisco 7000 only)
- Power cord (AC only)
- Rack-mounting hardware
- Cable-management brackets (Cisco 7010 only)
- Standard system:
 - Route Processor:
 - 25-MHz 68040 CPU
 - Console port (female EIA/TIA-232---DCE mode)
 - Auxiliary port (EIA/TIA-232 DTE)
 - 16-MB DRAM, upgradeable to 64 MB
 - 8-MB ROM
 - 4-MB Flash EPROM for downloadable microcode and software updates
 - 128-KB NVRAM
 - Slot for optional 8- or 16-MB Flash memory card
 - Real-time calendar clock with battery backup
 - Switch Processor:

Controls communication between the CxBus interface processors and the system processor

Three models available:
 SP---Switch Processor (default model)
 SSP---Silicon Switch Processor with 512-KB spare
 SSP-2MB---Silicon Switch Processor with 2-MB spare

- Upgraded RSP7000 system:
 - MIPS RISC CPU, external clock speed of 50 MHz and an internal clock speed of 100 MHz
 - Console port (male EIA/TIA-232---default DCE mode)
 - Auxiliary port (EIA/TIA-232 DTE)
 - 32-MB DRAM default, upgradeable to 128 MB (user configurable)
 - 128-KB NVRAM
 - 8-MB Flash memory via PCMCIA Flash memory cards, upgradeable to 40 MB (user configurable)
 - Battery backup
 - Real-time calendar clock

Hardware

Hardware for the Cisco 7000 series includes processors, interface processors, serial cables, memory, a second power supply (Cisco 7000 only), and accessories. [Table 91](#) lists hardware option product numbers for the Cisco 7000 series.

Processors

The standard system requires one Route Processor and one Switch Processor (or Silicon Switch Processor). An upgraded RSP7000 system requires one 7000 series Route Switch Processor (RSP7000) and one 7000 series Chassis Interface (RSP7000CI). Most processors can be ordered in three ways: as part of an initial system, as spares, or as upgrades.

RSP7000 Flash Memory Cards

In an RSP7000 system, Flash memory cards can be used to store and boot Cisco IOS images and/or system configurations. A Cisco 7000 series router with the RSP7000 option can also be used as a TFTP server, with the Flash memory used to store other files such as software and microcode images for other systems. Cisco recommends using one card for image storage and another for configurations. The

number of system images that can be stored on the card depends both on the Flash memory card size and the file size.

The RSP7000 Flash memory card is available in 8-, 16-, or 20-MB densities. The card is an Intel Series 2+ Flash memory card, which conforms with PCMCIA format. The Flash memory card that is shipped with the RSP7000 contains a software image; the same Flash memory card ordered as a spare is shipped blank and must be formatted before use.

RSP7000 Memory Options

By default, the RSP7000 is shipped with 32 MB of DRAM. Refer to [Table 88](#) for DRAM size recommendations based on the size of your network. Then, consult with your Cisco system engineer to determine the recommended DRAM configuration for your unique network.

DRAM Guidelines

Use the following guidelines when ordering DRAM for the Cisco 7000 series:

- For the RSP7000, DRAM is contained in four SIMM slots (two banks of two SIMMs each).
- For the RSP7000, bank 0 must be greater than or equal to bank 1.
- Do not mix DRAM sizes within a bank.

Software

Software Feature Sets

This section describes Cisco IOS software feature sets for the Cisco 7000 series. With feature sets, you can order software combinations that support your particular application. Optional licenses expand the feature sets by providing WAN packet protocol, interdomain routing, Network Address Translation, Netflow switching (with the RSP7000 only), and CIP2 support. To order, select one feature set (there is no default) and one or all of the optional feature licenses.

The Cisco 7000 series offers the following type of feature sets:

- **Basic.** The basic feature set for the Cisco 7000 series.

The Cisco IOS feature set tables use the following conventions to identify features:

- **X** : the feature is offered in the basic feature set
- **--** : the feature is not offered in the feature set

You can still order earlier Cisco IOS software releases, which are available as software feature sets. Unless you specify otherwise, you will receive the default software version.

Table 94 : Cisco IOS Software Feature Licenses—Cisco 7000 Series

Category	Features	Product Number
RP		
WAN packet protocols	X.25, X.25 switching, Switched 56, Frame Relay, Frame Relay switching, SMDS, ATM DXI, SMDS over ATM In Cisco IOS Release 11.2 only: all of the above plus Frame Relay SVC support (DTE) and Frame Relay traffic shaping	FR-WPP7, FR-WPP7=
Interdomain routing ¹	BGP, EGP for Internet scale routing In Cisco IOS Release 11.2 only: all of the above plus BGP4 ²	FR-IR7, FR-IR7=
VIP/VIP2 support	Included automatically with VIP order	--
CIP2 support ³	TCP/IP offload feature for CIP (or CIP2)	FR-CIP-TCPOFF, FR-CIP-TCPOFF=
	SNA support feature for CIP2 SNA	FR-CIP-CSNA, FR-CIP-CSNA=
RSP7000		
WAN packet protocols	X.25, X.25 switching, Frame Relay, SMDS, Frame Relay switching, Switched 56, ATM DXI, SMDS over ATM In Cisco IOS Release 11.2 only: all of the above plus Frame Relay SVC support (DTE) and Frame Relay traffic shaping	FR-WPP75, FR-WPP75=
Interdomain routing ¹	BGP, EGP for Internet scale routing In Cisco IOS Release 11.2 only: all of the above plus BGP4 ²	FR-IR75, FR-IR75=
Network Address Translation (NAT) ⁴	NAT support	FR-NAT75, FR-NAT75=
Netflow switching	Netflow switching	FR-NF75, FR-NF75=

VIP/VIP2 support	Included automatically with VIP order	--
CIP2 support ³	TCP/IP offload feature for CIP2	FR-CIP-TCPOFF, FR-CIP-TCPOFF=
	SNA support feature for CIP2 SNA	FR-CIP-CSNA, FR-CIP-CSNA=

¹ Interdomain routing is automatically included with all Cisco7000 series RPs with 16-MB RAM. However, this option is appropriate for all other Cisco7000 and 7500 series system processors.

² BGP4 includes soft configuration, multipath support, and prefix filtering with inbound route maps.

³ To calculate CIP memory requirements, see the section "CIP2 Memory Guidelines" in the chapter "Interface Processors for the Cisco 7000 Family."

⁴ Requires CiscoIOS Release 11.2.

6520 MPRouter PRO Spec Sheet

Software

Wide Area Protocols

- Frame Relay DTE
- Frame Relay switching (DCE)
- Frame Relay Annex A (ANSI T.617)
- Frame Relay Annex D (ANSI T.617)
- Frame Relay Annex G (ANSI T.617)
- Local Management Interface (LMI)
- X.25 DTE
- X.25 switching
- RFC 877
- ISDN (Q.921/Q.931)
- X.25 on "D" channel support
- Transparent HDLC support (TBOP)
- MX.25 multidrop X.25 protocol
- XDLC
- Novell IPX WAN
- Voice Relay

LAN Protocols

- AppleTalk routing
- OSPF
- TCP/Telnet
- UDP
- PPP
- IP routing
- IPX routing

- RIP
- Source Route Bridging (SRB)
- Transparent bridging (spanning tree IEEE 802.1d)
- SLIP support
- RFC 1294/1490 compliant Frame Relay encapsulation of supported LAN protocols

Management and Utilities

SNMP management Billing support TFTP to host and intemode software download
Kermit configuration upload/download

Bandwidth Management

- Data compression
- Bandwidth on Demand (BOD)
- Dial on Demand (DOD)
- Data Connection Protection (DCP) (X.25, Async, SDLC)
- Link backup (V.25bis and ISDN)
- Traffic prioritization
- Frame Relay DLCI muxing

Legacy Protocols

- Async
- Transparent Polled Async (TPA)
- NCR BISYNC
- IBM BSC 3270
- IBM BSC 2780/3780
- Burroughs Poll Select
- IBM 2260
- TCOP
- TBOP
- SIEMENS HDLC

- SNA/SDLC support
- Physical Unit (PU) re-mapping and spoofing
- QLLC transport (IBM NPSI) point-to-point multidrop (up to 64 PUs)
- Conversion SDLC to RFC 1490
- Conversion SDLC to LLC2
- Conversion LLC2 to RFC 1490

Hardware

6520 Platform

- PC Tower, 7 ISA- compatible expansion slots
- 1 EIA232D Control Terminal Port with easy to use menu
- 3 RS232 ports (300 bps to 80Kbps)
- High MTBF power supply
- Auxiliary cooling fan
- Motorola 68030 processor powered motherboard
- 2 high speed serial ports (500 bps -1.544Mbps)
- V.35, V.36, V.24 and V.11 DB25 cable interfaces
- 3 Megabytes of Non-Volatile FLASH
- 4 MB DRAM
- 4 MB Local DRAM

Platform Options

- Ethernet LAN Interface board (ELAN) with integral DSP address filtering, AUI and 10BaseT support
- Token Ring LAN Interface board (TLAN) with integral DSP address filtering and 4/16 Mbps UTP/STP support
- SNMP managed 6 port 10 BaseT Ethernet Hub card (6520 supports up to 24 ports/4 cards)
- Integral 56 Kbps DSU
- Integral ISDN Basic Rate Interface (2B+D)
- Integral V.22bis modem

- Backup FLASH memory SIMM
- DRAM expansion for up to 8 Mbytes of local 68030 DRAM
- DRAM expansion for up to 8 Mbytes of Global buffer DRAM
- Dual port Serial Data Board expansion (V.24, V.36, V.35, V.11, X.21)
- High performance dual port Serial Data Board expansion (V.36, V.35, V.11, X.21)
- Frame Data Compressor
- Dual port T1 interface board
- Dual port E1 interface board
- Dual port E&M analog voice Digital Signal Processing Module (DSPM/EM)
- Dual port FXS analog voice Digital Signal Processing Module (DSPM/FXS)
- Quad port digital voice server Digital Signal Processing Module (DSPM/SM)
- Voice Ringer and -48V supply
- 19 inch rack mount hardware kit
- Physical

Environment

- Operating temperature: 32 to 122 degrees F (0 to 50 degrees C)
- Storage temperature: -40 to 158 degrees F (-40 to 70 degrees C)
- Relative humidity: 5% to 90% (non-condensing)

Power Requirements

- 90-132 VAC/180-264VAC
- 48 to 63 Hz

Dimensions

- Height: 17.8 in. (45.3 cm)
- Width: 10.0 in. (25.5 cm)
- Depth: 16.8 in. (42.8 cm)

Certification

- FCC, UL, CSA, TUV, AUSTEL, EMC/Telecom/LVD CE Marking

- 6520 MPRouter Features and Benefits

High Performing Dual Core Routing and Bridging

- Low response times
- Bandwidth efficiency
- Quality voice transmission
- Multimedia transport capability

Voice Support

- Integration of voice with data traffic
- 8/16 Kbps compression minimizes network bandwidth requirement
- Support for analog and digital voice port connections

Widest Range of Protocol Support

- Consolidate WAN networks
- Minimize data communications equipment costs
- Capitalize on lowest available WAN tariffs

WAN Optimization Features

- Minimize required bandwidth
- Improved application performance
- Integral payload data compression

Value Add Features

- Design for average rather than peak throughput requirements
- Link restoral via ISDN or other switched services
- Minimize carrier costs using most appropriate switched services

Dual Ethernet Connectivity

- Supports multi-LAN environments
- Dual Ethernet configurations provides network resiliency

Network Management

- SNMP management

- Ease of use
- Reduced configuration time
- High visibility into WAN performance and utilization

Best IBM Support in the Industry

- Ease of migration from host based Legacy Systems to Client-server applications
- Boundary Network Node compatible (NCP 7.X)

Software Download

- Low upgrade costs
- No on site services necessary
- Keep technology current without major reinvestment

BIBLIOGRAFIA

1.- Analyzing Broadband Networks: Frame Relay, SMDS y ATM.

Mark A. Miller, M&T Books, 1995.

2.- TCP/IP Illustrated Volume I : The Protocols.

W. Richard Stevens, Addison Wesley, 1995.

3.- ATM Solutions for Enterprise Networking.

David Ginsburg, Addison Wesley, 1996.

4.- Routing in the Internet.

Christian Huitema, Prentice Hall, 1997.

5.- Installation and Maintenance of Cisco Routers.

Cisco Systems, 1995.

6.- Advanced Cisco Routers Configuration.

Cisco Systems, 1995.

7.- Internetwork Design Fundamentals

Cisco Systems, 1996.