ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERIA ELECTRICA

TEMA: DISEÑO DE UNA RED TCP/IP SOBRE X.25 PARA UNA INSTITUCION BANCARIA

TESIS PREVIA A LA OBTENCION DEL TITULO DE INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

ANGEL HOMERO CHINCHERO VILLACIS

QUITO, JULIO DE 1997

CERTIFICACION

Certifico que la presente Tesis ha sido desarrollada en su totalidad por Angel Homero Chinchero Villacís.

Ing. Pablo Hidalgo

DIRECTOR DE TESIS

Quito, Julio de 1997

PROLOGO

La presente Tesis tiene por objeto realizar el diseño de una red de datos a nivel nacional para una Institución Bancaria, en donde se requiere integrar todos los sistemas, en base a la arquitectura **Cliente / Servidor**, empleando protocolos de comunicaciones estándares y seguros, seleccionado **TCP/IP** como el protocolo más idóneo para la implementación de las redes locales y **X.25** para las comunicaciones entre las agencias.

Es un proyecto teórico - práctico que sirve como ayuda a la implementación de redes en general, basados en el protocolo TCP/IP, en el cual se describe los fundamentos de redes, puentes, ruteadores, protocolos de enrutamiento y las principales redes utilizadas en la transmisión de los datos.

Se realiza un análisis de los dispositivos que se utilizan en la red de datos, el software que utilizan para su funcionamiento, y la forma de interconexión de dichos dispositivos para obtener una red confiable y con adecuada velocidad de transmisión de la información.

Mediante el presente trabajo se establecen los métodos para el diseño de redes tanto locales como extendidas, en donde se indican los principales aspectos que se deben tomar en cuenta para tales objetivos.

Se describe un caso práctico de implementación de Red TCP/IP sobre **X.25** en una Institución Bancaria, y finalmente se realizan las pruebas y análisis de la red, empleando herramientas de monitoreo avanzadas.

CONTENIDO

CAPITULO I FUNDAMENTOS DE REDES Y PROTOCOLOS

1.1 INTRODUCCION A LAS REDES DE DATOS

Las redes de datos son esenciales, pues permiten enviar programas e información hacia super computadoras remotas para su procesamiento, recuperar los resultados e intercambiar la información con el resto de usuarios.

Cuando se implementa una red de área local, la transmisión de datos se realiza a altas velocidades, en tanto que en redes de área extendida debido a las bajas velocidades que se manejan se pueden alcanzar grandes distancias.

En la actualidad se proporciona un conjunto de normas de comunicación, para que redes heterogéneas se comuniquen entre sí, en forma independiente de sus conexiones físicas y tecnológicas y de los sistemas operativos de red.

1.1.1 CIRCUITOS CONMUTADOS Y CONMUTACION DE PAQUETES

La comunicación entre redes se divide en dos tipos básicos: **conmutación de circuitos** que es orientada a conexión y **conmutación de paquetes** llamada también sin conexión.

Los circuitos conmutados operan formando una conexión dedicada y segura, pero el costo del circuito es alto independientemente del tráfico.

En una red de conmutación de paquetes, la información se transfiere en unidades llamadas **paquetes** , que por lo general tienen sólo unos cientos de octetos[1] de datos y transportan adicionalmente información de identificación que permite al *hardware* de la red saber cómo enviar el paquete hacia el destino.

La ventaja de la conmutación de paquetes, radica en que se puede hacer múltiples conexiones compartidas por pares de computadoras que se están comunicando. La desventaja es que

[1] Octeto = 1 Byte

cuando se incrementa la actividad se reduce la capacidad de transmisión, produciendo retardos en la red .

1.1.2 REDES DE AREA EXTENDIDA Y LOCAL [2]

Las redes de Conmutación de Paquetes se dividen en dos grandes categorías : ***Wide Area Network*** o ***WAN*** y ***Local Area Network*** o ***LAN***.

La comunicación en redes *WAN* cubre grandes distancias, pero opera a velocidades lentas en el rango de 9600 bps a 155 Mbps, con retardos que pueden variar de unos cuantos milisegundos a varias decenas de segundos, dependiendo de la tecnología de los medios de transmisión (líneas telefónicas, radio, satélite) , distancia y de la congestión en la red .

Las tecnologías *LAN* operan a velocidades muy altas, pero sacrifican la capacidad de recorrer grandes distancias. Se limitan a recorrer áreas pequeñas como edificios operando desde 10 Mbps a 2 Gbps. Ofrecen tiempos de retardo mucho menores que la red *WAN,* llegando hasta 10 milisegundos.

1.1.3 ARQUITECTURA DE CAPAS DE RED

Las capas son funciones y servicios agrupados de manera lógica dentro de un *set* específico.
Una capa en un sistema, realiza tareas específicas para comunicarse con la capa correspondiente en otro sistema similar, manteniendo el movimiento de los datos desde la fuente hasta el destino a través del camino correcto y realizando el control del volumen de tráfico a fin de minimizar las congestiones.

Las tareas básicas de cada capa son :

- Realizar funciones primitivas[3] basándose en la capa inmediatamente inferior.
- Provee servicios para la capa superior.

---

[2] Redes Globales de Información con *Internet* y *TCP/IP* Douglas Comer
[3] Las funciones primitivas deciden si el mensaje es correcto y seleccionan una acción apropiada en base al tipo de mensaje o la dirección destino

Son diseñadas en forma estándar, de modo que cualquier cambio en una de ellas no requiera cambios en las demás.

Las capas **inferiores** proveen el enlace físico de los componentes de red, en tanto que las capas **superiores** dan los servicios orientados a las aplicaciones .

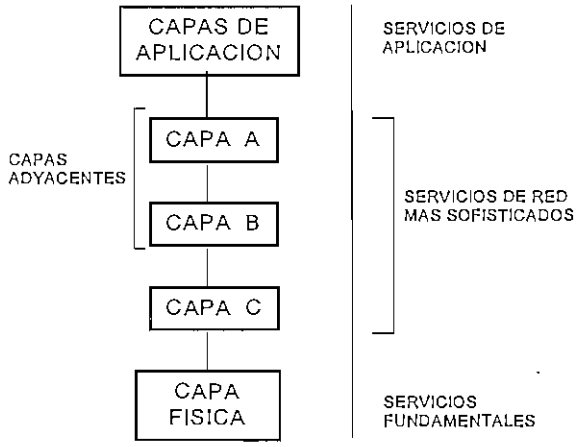


Figura 1.1 Estructura de una Red

Cada capa adiciona valores a la información que está siendo procesada, con el fin de que los niveles superiores se beneficien de un conjunto de servicios de red.

Las funciones de comunicación entre capas ubicadas al mismo nivel son equivalentes

1.1.4 ENCAPSULAMIENTO

La arquitectura de capas proporciona reglas para que dos capas ubicadas al mismo nivel, pero en sistemas distintos, interactúen entre sí, permitiendo el intercambio de datos entre la capa del sistema origen y la capa del sistema destino.

Para transmitir los mensajes al otro sistema, se trasladan éstos hacia abajo capa por capa, de modo que en cada una de ellas se añade información de control en forma de cabecera. Mediante la información adicionada el mensaje es rastreado en la posición donde se encuentre.

Esta adición de información de control se conoce como **ENCAPSULAMIENTO**, el cual trasforma el mensaje a un formato distinto en cada una de las capas por las que atraviesa.

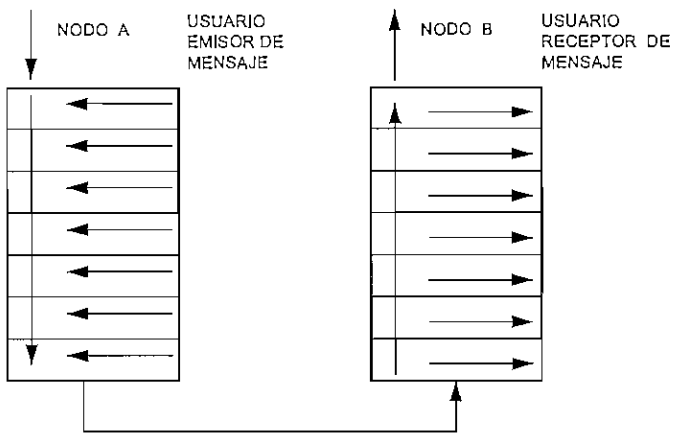


Figura 1.2 Flujo del mensaje entre emisor y receptor

La información de control es un conjunto de reglas con procedimientos, criterios de selección de encaminamiento, o chequeo de los datos, siendo entendida sólo por la capa ubicada al mismo nivel en el otro sistema similar.

En el destino receptor, el mensaje ingresa hacia arriba , capa por capa, cada una de las cuales interpreta y actúa sobre la información de control adicionada por la capa equivalente en el sistema origen.

1.1.4.1 FLUJO DE DATOS DESDE EL EMISOR HASTA EL RECEPTOR

A los datos emitidos por un sistema, la capa receptora sólo le quita la información de control añadida en la capa del mismo nivel en el sistema emisor, sin influir sobre las demás cabeceras añadidas por las demás capas.

Una vez eliminada la cabecera correspondiente al nivel donde se halla el dato, se pasa la parte restante a la capa superior siguiente.

Este proceso se realiza hasta obtener el dato depurado.

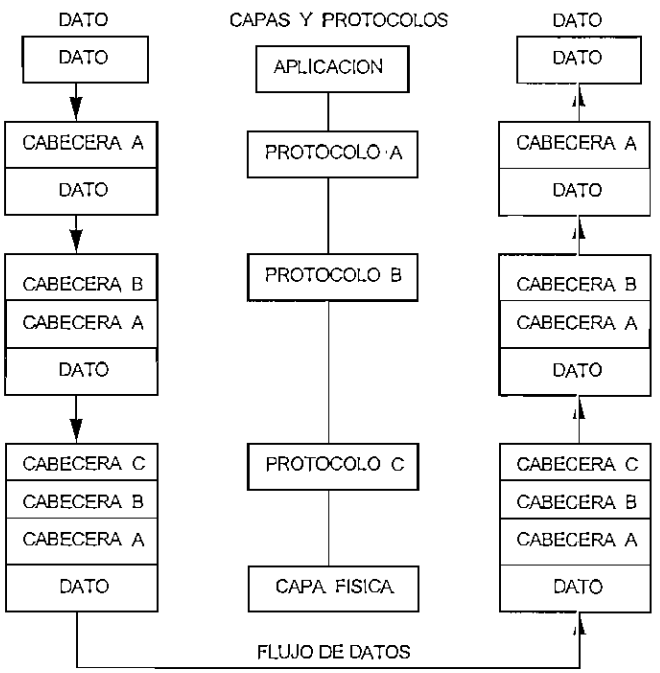


Figura 1.3 Encapsulamiento en cada capa

1.1.5 EL MODELO *OSI (OPEN SYSTEM INTERCONECTION)* [4]

El modelo OSI (*Open System Interconection*) , es un sistema compuesto por siete capas. Las tres inferiores definen la manera como la computadora interactúa con la red física , y representan la subred de comunicaciones para los datos.

Las tres capas superiores constituyen los servicios y aplicaciones para los usuarios, como son las transferencias de archivos, correo electrónico, transmisión de documentos , etc.

La capa intermedia es la capa de transporte y provee el intercambio de datos entre los sistemas finales.

[4] *Internetworking Technology Overview , Cisco Systems* Capítulo 1

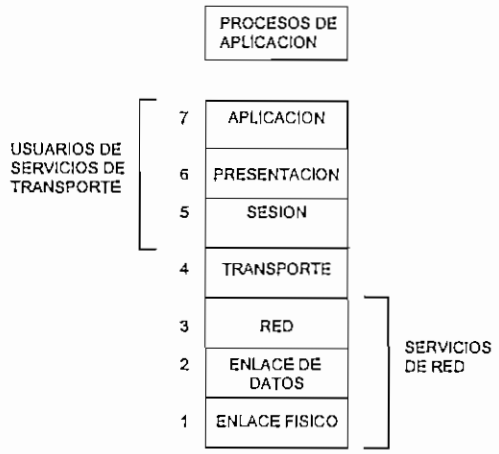


Figura 1.4 Modelo *OSI* de capas de red

- **Capa 7 - Aplicación:** Provee el interfaz hacia los procesos de aplicación y establece conexiones con otras aplicaciones.

- **Capa 6 - Presentación:** Esta capa transforma los datos a los diferentes formatos (*ASCII, EBCDIC*) , de modo que puedan ser usados y entendidos por los procesos de aplicación. Esto es debido a que el sistema emisor puede haber enviado los mensajes en un formato diferente.

- **Capa 5 - Sesión:** Establece las sesiones, que son conexiones lógicas entre dos procesos de aplicación. Maneja el intercambio de datos entre procesos de aplicación y realiza el control empleando comandos de sesión.

- **Capa 4 - Transporte:** Asegura que los mensajes liberados por el proceso de aplicación transmisor lleguen al proceso de aplicación receptor. Si un mensaje se recibe con error en el nodo destino, la capa 4 envía un comando a la capa 4 en el nodo origen, pidiendo que el mensaje sea retransmitido.

- **Capa 3 - Red:** Provee el encaminamiento a través de la red, desde el origen hasta el destino. Cada nodo usa la dirección destino en la cabecera de red para enrutar el mensaje hasta el nodo destino apropiado.

- **Capa 2 - Enlace**: Establece una conexión de enlace, transfiere el dato y mantiene la conexión con el nodo adyacente empleando el protocolo de enlace apropiado.

- **Capa 1 - Física:** Provee la conexión física, eléctrica y mecánica, al canal de comunicaciones.

1.2 PRINCIPALES PROTOCOLOS DE RED

Un **PROTOCOLO** es un conjunto de reglas para el intercambio de información. Parte de la información que viaja en la trama de datos son requerimientos de un servicio, o respuestas al requerimiento previo.

Para que se produzca la comunicación, el intercambio de información se puede producir entre:

- Capas correspondientes ubicadas en diferentes nodos.
- En la misma capa dentro de un nodo, como se muestra en la figura 1.5 en donde los protocolos B y C operan e intercambian información en la capa 6 del *host* A.
- Entre capas adyacentes en el mismo nodo. En este caso los protocolos F y G pueden interactuar entre sí dentro del *host* A.
- Entre capas no adyacentes en el mismo nodo. En este caso los protocolos D y F dentro del *host* A pueden interactuar entre sí, sin la intervención del protocolo E.

Los protocolos que operan entre capas adyacentes dentro de un mismo nodo son conocidos como protocolos de capas adyacentes, y los que funcionan entre capas correspondientes, pero en diferentes nodos se llaman protocolos par a par (*Peer To Peer*) como se muestra en la figura 1.5.

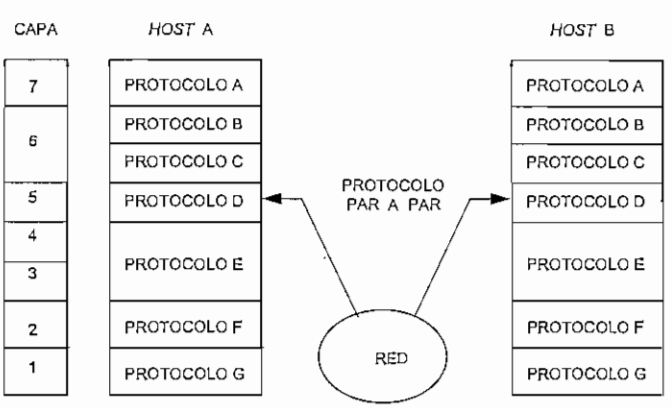


Figura 1.5 Protocolos en el modelo *OSI*

Los protocolos añaden o quitan cabeceras en cada una de las capas , dependiendo si está enviando o recibiendo el paquete de datos. Para el modelo *OSI* el encapsulamiento de la información es de la siguiente manera:

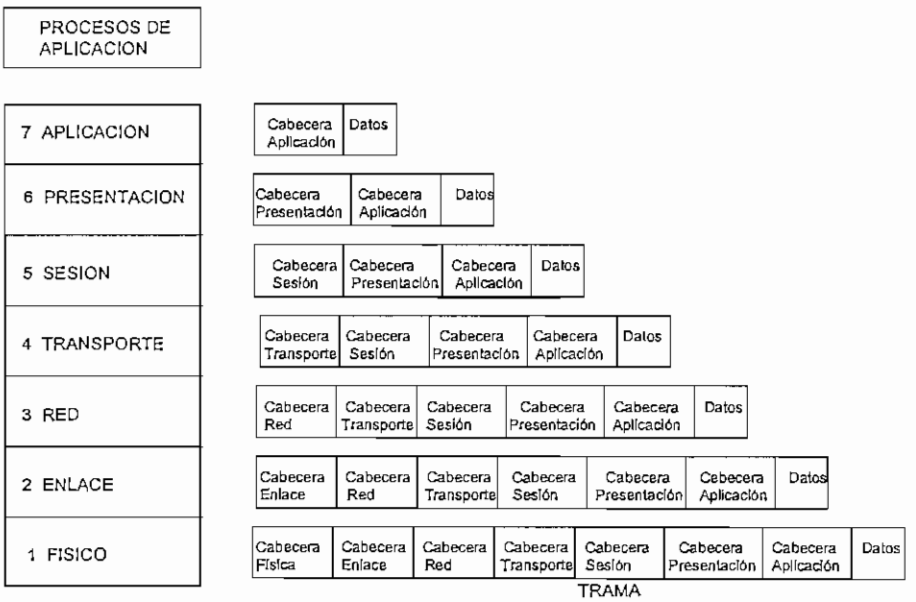


Figura 1.6 Colocación de Cabeceras en cada capa del modelo *OSI*

A continuación se exponen las principales características de algunos protocolos utilizados en redes de computadoras.

1.2.1 PROTOCOLOS DE RED X.25 [5]

X.25 define la interacción serial punto a punto, entre un *DTE* y un *DCE* a través de dispositivos de traslación llamados ensambladores/desensambladores de paquetes *PADs*, empleando las tres primeras capas del modelo de referencia *OSI* como indica la figura 1.7.

Los tres niveles definidos por X.25 son:

. Capa 1 - Nivel Físico

. Capa 2 - Nivel de Enlace

. Capa 3 - Nivel de Paquete

[5] *X.25 Technical Concepts Open Strategies,Inc and NCR*

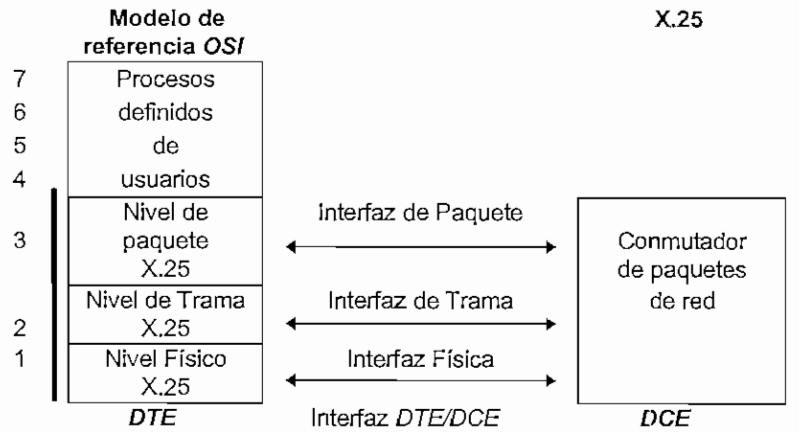
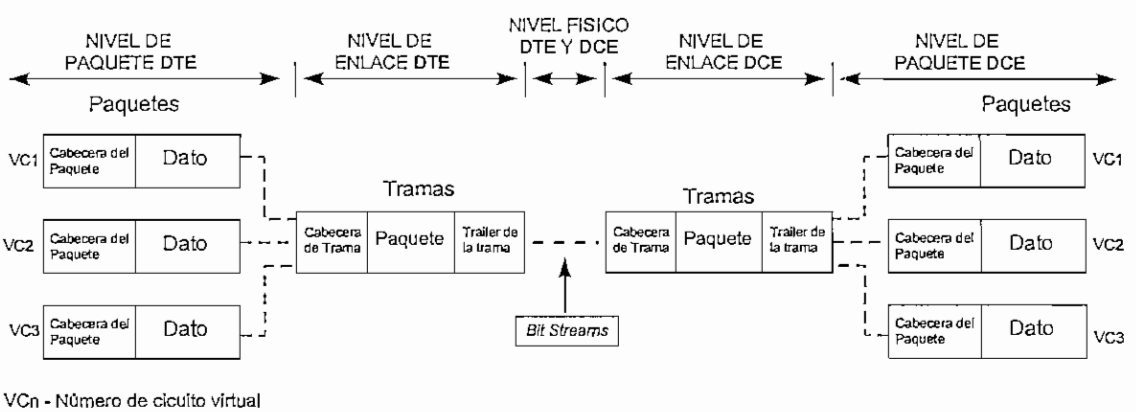


Figura 1.7 Modelo X.25 tomando como referencia el modelo *OSI*

El flujo de datos a través de los niveles X.25 se realiza de la siguiente manera:

1. El Nivel de Paquete en el equipo *DTE* toma los datos de los procesos de usuario y los transmite lógicamente al nivel de paquete del equipo *DCE*.
2. El Nivel de Enlace del *DTE* transmite lógicamente hacia el nivel de enlace del *DCE* una trama que contiene el paquete generado en el Nivel de Paquete.
3. El Nivel Físico del *DTE* convierte la trama en una cadena de bits y los transmite hacia el Nivel Físico del *DCE*.
4. El Nivel Físico del *DCE* recibe la cadena de bits y los ensambla en una trama para ser enviada al Nivel de Enlace del *DCE*.
5. El Nivel de Enlace chequea la existencia de errores en la información y la pasa hacia el nivel de paquete del *DCE*.

Los procesos anteriores se muestran en la figura 1.8



VCn - Número de circuito virtual

Figura 1.8 Flujo de datos a través de los niveles X.25

La comunicación entre procesos de usuario no está definido en X.25, por tanto, para el flujo de datos *end to end* entre equipos *DTEs* es necesario utilizar la capa de transporte, como indica la figura 1.9.

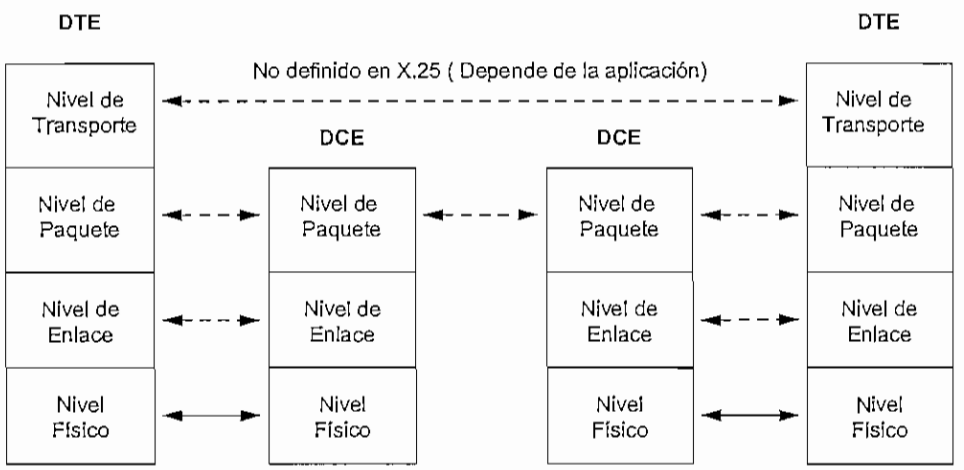


Figura 1.9 Flujo de datos entre *DTEs*

El formato de la información varía en cada nivel X.25, como se indica en la figura 1.10.

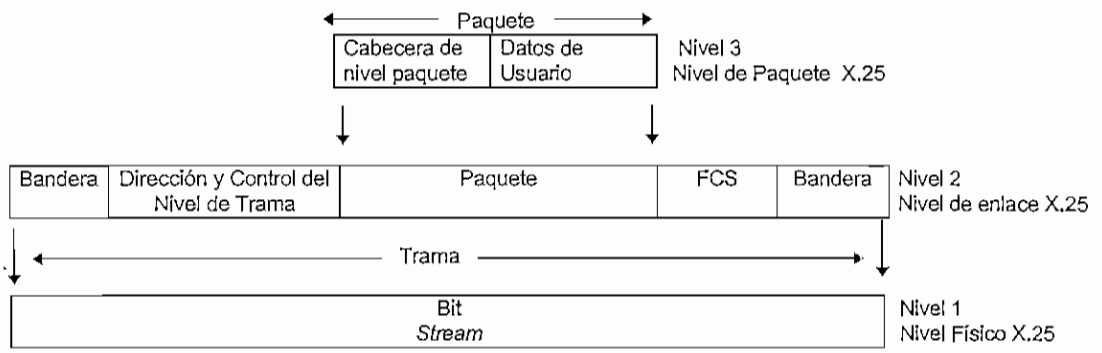


Figura 1.10 Formato del mensaje en cada nivel X.25

1.2.1.1 NIVEL FISICO

El Nivel Físico define la manera en que los niveles físicos entre un *DTE* y un *DCE* son activados, mantenidos o desactivados y se identifican por sus características mecánicas, eléctricas y funcionales, definidas en las recomendaciones X.21 y X.21 *bis* para soportar conexiones sincrónicas punto a punto *full duplex*.

Como se observa en el cuadro 1.1, la recomendación X.21 *bis* emplea el interfaz V.24 para conectar *DTEs* sincrónicos. Además es posible la utilización de servicios digitales de datos empleando interfaces V.35 que permiten obtener velocidades superiores a 48 Kbps.

VELOCIDAD	MODEM ESTANDARD	INTERFAZ ESTANDARD	ESTANDARD ELECTRICO	ESTANDARD MECANICO	# DE PINES
< 20 Kbps	series - V	V.24	V.28	ISO 2110	25
< 20 Kbps	series - V	V.24	X.26	ISO 4902	37
48 Kbps	V.35	V.24	V.35	ISO 2593	34
48 Kbps	V.36	V.24	X.26/X.27	ISO 4902	37

Cuadro 1.1 Características eléctricas y mecánicas escogidas por la recomendación X.21 bis

La recomendación X.21 identifica los circuitos del interfaz X.24 para el intercambio de datos entre *DTEs* a través de los circuitos T y R, que se produce cuando el interfaz está en estado de transferencia de datos.

1.2.1.2 NIVEL DE ENLACE

El Nivel de Enlace controla el flujo de paquetes entre el *DTE* y el *DCE*, incorporando procedimientos de detección y corrección de errores. Funciona como una línea de transmisión libre de errores, empleando una trama como vehículo para transportar cada paquete, tratando a cada paquete como un dato a ser transmitido o recibido.

Los circuitos virtuales definidos en el nivel de paquete pueden ser multiplexados a través de un mismo circuito físico.

El número de secuencia asignado al paquete en el Nivel de Paquete es independiente y no guarda relación con el número de secuencia de la trama que lo transporta.

El establecimiento/desconexión del enlace se realizan empleando los siguientes protocolos:

- *Link Acces Protocol Balanced LAPB*
- *Link Access Protocol LAP*

Ambos son conocidos como *Single Link Procedures SLPs* y su funcionamiento se describe en la figura 1.11.

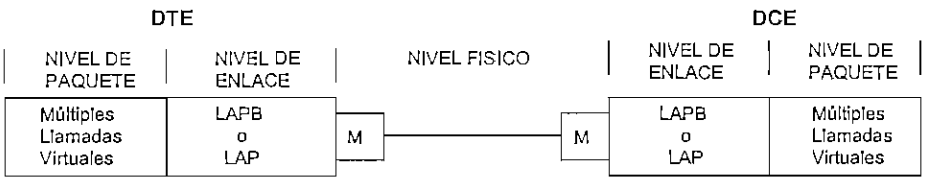


Figura 1.11 Niveles de Interfaz DTE/DCE para procesos de enlace simple

El formato, secuencia, y mecanismos de reconocimiento de la trama se especifican en el protocolo *HDLC*.

El formato de la trama X.25 en el nivel de enlace se indica en la figura 1.12.

FLAG	ADDRESS	CONTROL	INFORMATION	FCS	FLAG
F 01111110	A 8 bits	C 8 bits	I N bits	FCS 16 bits	F 01111110

Figura 1.12 Formato de la Trama X.25

- *FLAG*

  Es un octeto (01111110) que delimita las tramas.

- *ADDRESS*

  Es un octeto que asigna direcciones secundarias únicas al *DTE* y al *DCE*, para identificar las tramas recibidas, así como una trama comando o una trama respuesta a un comando, como indica la figura 1.13, en donde los equipos operan simultáneamente en dos vías.

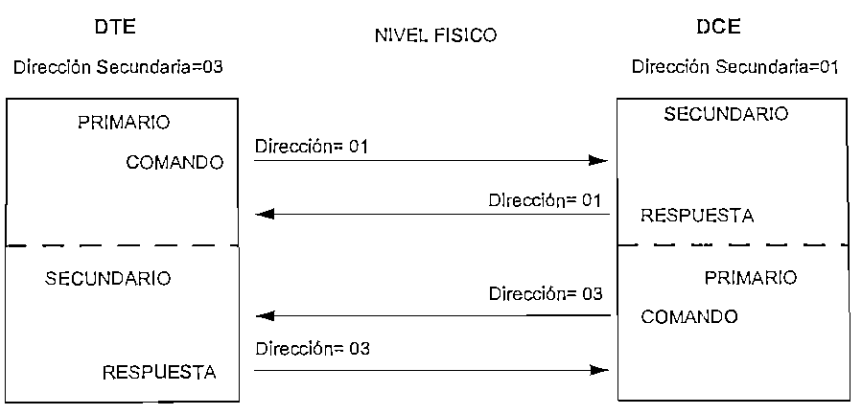


Figura 1.13 Direcciones secundarias DTE/DCE

La asignación de las direcciones secundarias se realiza de la siguiente manera:

- Dirección secundaria *DTE* = 03

- Dirección secundaria *DCE* = 01

- ***CONTROL***

Es un octeto que contiene: el número de secuencia de la trama, la información de control, y la identificación del tipo de trama mediante los dos bits menos significativos.

Se tiene tres tipos de tramas:

1. Trama de Información (I) (XXXXXXX0), que contiene un paquete en el campo de Información.
2. Trama de Supervisión (S) (XXXXXX01), que se emplea para funciones de supervisión del enlace como :
   - Reconocimiento de trama de información
   - Petición de retransmisión de trama de información
   - Petición de suspensión temporal de trama de información
3. Trama No Numerada (U) (XXXXXX11), usada para operaciones de control del enlace como:
   - Inicio del enlace, colocando al *DCE* y *DTE* en modo de transferencia de información.
   - Desconexión del enlace, colocando al *DTE* y *DCE* fuera del modo de transferencia de información.
   - Rechazo del enlace, reportando errores no recuperados.

El formato del campo de control para el Protocolo de Acceso al Enlace Balanceado (*LAPB*) se indica en la figura 1.14, en donde los campos tienen el siguiente significado:

- **N(S)** - Número de secuencia transmitida, que es un número rotativo generado en el emisor, que identifica la trama de información que es transmitida.
- **N(R)** - Número de secuencia recibida, generado en el receptor, que es un número rotativo que identifica la siguiente trama que espera ser recibida.

- **P/F** - Es un bit de *Poll* en comandos o un bit Final en respuestas.

  En un comando indica que se requiere una respuesta, en tanto que en una respuesta indica que es una respuesta a un comando con el bit *P* en *on*.

- **SS** - Identifica un tipo particular de la trama de supervisión.
- **MMMMM** - Especifica un tipo particular de trama No Numerada.

Bits del campo de CONTROL	8	7	6	5	4	3	2	1
Formato en la Trama Información	N(R)			P	N(S)			0
Formato en la Trama Supervisión	N(R)			P/F	S	S	0	1
Formato en la Trama No Numerada	M	M	M	P/F	M	M	1	1

Figura 1.14 Formato del campo *CONTROL* del protocolo *LAPB*

Los comandos y respuestas del Protocolo de Acceso al Enlace Balanceado (*LAPB*) se indican en el cuadro 1.2.

FORMATO	COMANDO	RESPUESTA
Transferencia de Información	*I* (información)	
Supervisión	*RR* (receptor listo)	*RR* (receptor listo)
	RNR (receptor no listo)	*RNR* (receptor no listo)
	REJ (*reject* o rechazo)	*REJ* (*reject* o rechazo)
No Numerada	*SABM* (*Set asynchronous balanced mode*)	
	DISC (desconexión)	
		DM (modo desconectado)
		UA (reconocimiento de trama No Numerada)
		FRMR (trama rechazada)

Cuadro 1.2 Comandos y respuestas del protocolo *LAPB*

INFORMATION

Es un campo opcional de longitud variable que generalmente contiene el paquete a ser transmitido.

- *FRAME CHECK SEQUENCE (FCS)*

  Es un código de redundancia cíclica de 16 bits para detección de tramas erróneas.

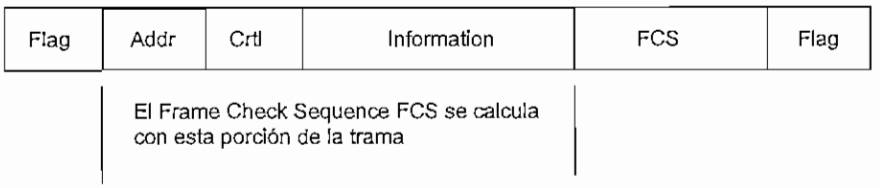


Figura 1.15 Campos de la trama incluidos en el cálculo de FCS

Como indica la figura 1.15, el *FCS* está determinado por los campos de dirección, control e información de la trama, el cual es calculado antes de la transmisión e insertado en el campo *FCS* de la trama.

En el receptor se vuelve a calcular el *FCS* y se compara con el valor transmitido. Si los dos valores no coinciden, la trama se descarta.

1.2.1.2.1 FASES DE COMUNICACION EN EL NIVEL DE ENLACE

Hay tres fases para la comunicación de tramas entre el *DCE* y el *DTE*:

a) **Fase de Establecimiento del Enlace.-** Establece la comunicación del Nivel de Enlace entre el *DTE* y el *DCE*, en donde el *DCE* indica que está en capacidad de establecer el enlace enviando banderas continuas.

   Las tramas que se intercambian entre *DTE* y *DCE* en esta fase son:

   - ***Set Asynchronous Balanced Mode (SABM)***, es una trama comando que coloca a la estación direccionada en el modo asincrónico balanceado para la fase de transferencia de información.

   - ***Disconnect Command (DISC)***, se usa para informar a la estación receptora que la estación transmisora ha suspendido las operaciones.

El receptor acepta la desconexión y el emisor entra en la fase de desconexión.

- ***Disconnected Mode (DM)***, se emplea para reportar que el emisor está lógicamente desconectado del enlace y es una respuesta al comando *DISC.*

- ***Unnumbered Acknowledgment (UA)***, es una trama de respuesta, usada para reconocer la recepción y aceptación de las tramas *SABM* o *DISC.*

b) **Fase de Transferencia de Información.** Es el modo normal, en donde las tramas de Información que contienen datos son transmitidas y reconocidas entre el *DTE* y el *DCE.*

Proceso de Reconocimiento

Cada trama de Información enviada entre el *DTE* y el *DCE* debe ser reconocida antes que el transmisor pueda considerarla como recibida.

El ciclo envío/reconocimiento se realiza empleando las secuencias de *bits* N(S) y N(R) del campo de control.

El receptor reconoce la recepción de una trama, insertando el número de la siguiente trama que éste espera recibir en los *bits* N(R) de una trama que retorna.

Si la trama de Información recibida tiene el *bit* P=0, puede ser reconocida con una trama de información o con una de supervisión y si la trama de Información recibida tiene el *bit* P=1, ésta es reconocida con una trama de supervisión con el *bit* F=1.

Parámetro K

Especifica el tamaño de la ventana de transmisión (1-7), que permite enviar más de una trama de información a la vez, antes de recibir un reconocimiento.

En el ejemplo de la figura 1.16 el valor de la ventana es K=2, donde después de transmitir las tramas 0 y 1, el *DTE* se bloquea hasta recibir el reconocimiento *ACK1* que confirma que la trama *INFO* 0 se recibió (N(R)=1).

El *DTE* se bloquea nuevamente luego de transmitir el *INFO* 2, por cuanto no ha recibido todavía el *ACK2* del *INFO* 1.

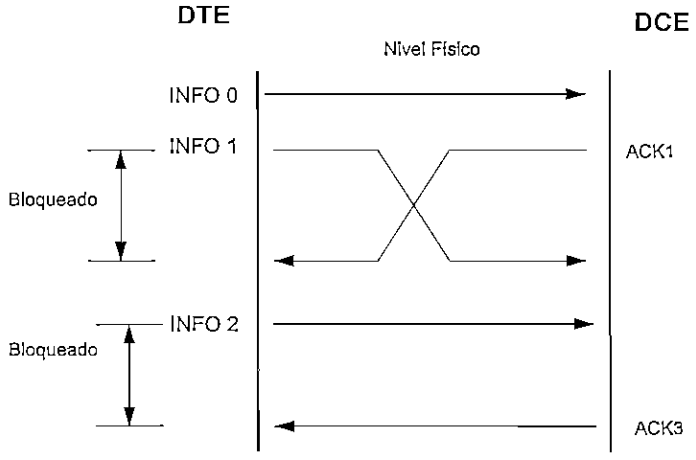


Figura 1.16 Ejemplo de reconocimiento de tramas con tamaño de ventana K=2

Parámetro N1

Indica el máximo número de bits en una trama de Información (excluyendo las banderas y los ceros insertados) que una estación acepta de otra estación. El *DCE* y *DTE* pueden tener valores diferentes de N1, de la siguiente forma:

- El *DTE* debe tener mínimo 1080 bit (135 octetos)
- El *DCE* mayor o igual a 2072 bits (259 octetos)

Uso de Tramas de Supervisión

Se utilizan para indicar el inicio y la finalización de la transmisión de las tramas de Información. Estas son :

- ***Receiver Ready (RR)***. Esta trama indica que la estación está lista para recibir tramas de Información y se utiliza para borrar una condición anterior de ocupado (*BUSY*).

- ***Receiver not Ready (RNR).*** Es una trama que indica una condición de ocupado (*BUSY*), inhabilitando temporalmente a la estación para recibir tramas.

- ***Reject (REJ).*** Es una trama que el receptor utiliza para pedir una retransmisión de la trama de Información, cuando se detecta en la recepción un error de secuencia de la trama.

  El campo N(R) de la trama *REJ*, contiene el número de la trama que la estación espera recibir. El receptor descarta cualquier trama recibida luego de enviar el *REJ*.

  El transmisor luego de recibir el *REJ*, retransmite la trama como indica la figura 1.17.

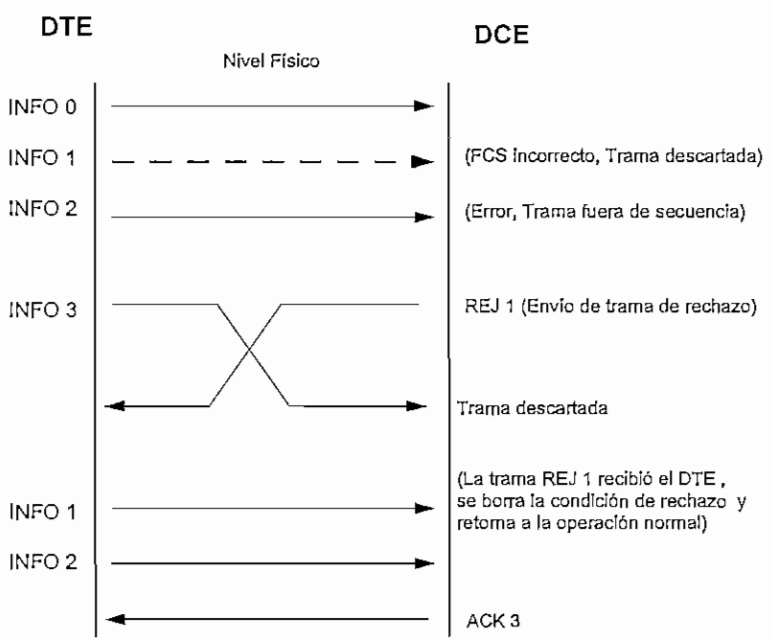


Figura 1.17 Proceso de rechazo de tramas

c) **Fase de desconexión del Enlace.** Se desconecta la comunicación entre el *DTE* y el *DCE*, empleando el comando *DISC*.

1.2.1.3 NIVEL DE PAQUETE

El Nivel de Paquete provee múltiples conexiones lógicas bidireccionales a través de un simple enlace físico, mediante la utilización de circuitos virtuales. A los datos de usuario se les añade

una cabecera para transformarlos en paquetes, los cuales son enviados a través de cada uno de los circuitos virtuales generados.

Los paquetes transferidos a través de los interfaces *DTE/DCE* son contenidos en el campo de Información de la trama del nivel de enlace, un paquete por trama.

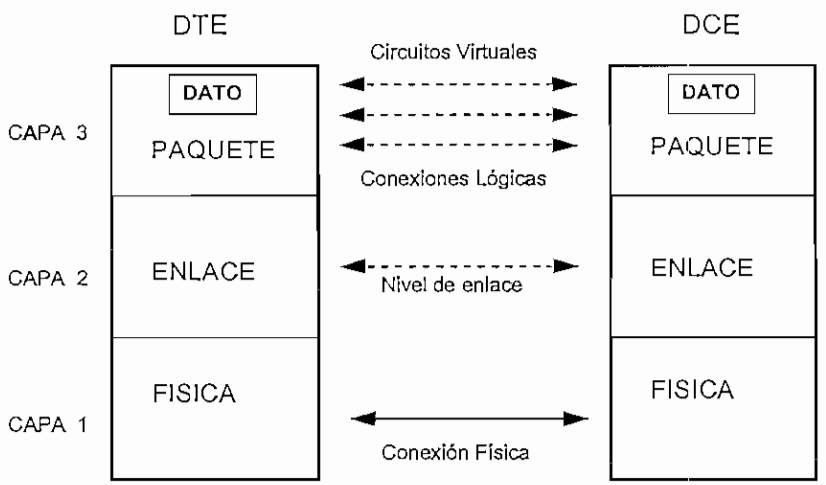


Figura 1.18 Capas definidas por X.25

El nivel de paquete define el formato del paquete, procesos de recuperación de error, facilidades de usuario, y procesos para conmutación de circuitos virtuales.

El protocolo de Nivel de Paquete provee los siguientes servicios:

- Multiplexación de múltiples canales lógicos a través de un enlace simple.
- Circuitos virtuales conmutables y permanentes
- Control de flujo para prevenir congestión de la red.
- Un esquema de secuencia de paquete que garantiza que el paquete llegue al destino en la secuencia correcta.
- Un esquema de reconocimiento local o *end to end* para detectar paquetes perdidos.
- Procesos de recuperación de errores cuando se produce errores de dirección.
- Un esquema que permite la conversión del tamaño del paquete entre *DTEs*.

Cada paquete tiene una cabecera que identifica al canal lógico a donde se transmite, como se indica en la figura 1.19. El receptor examina la cabecera y determina el canal lógico al cual se dirige el paquete.

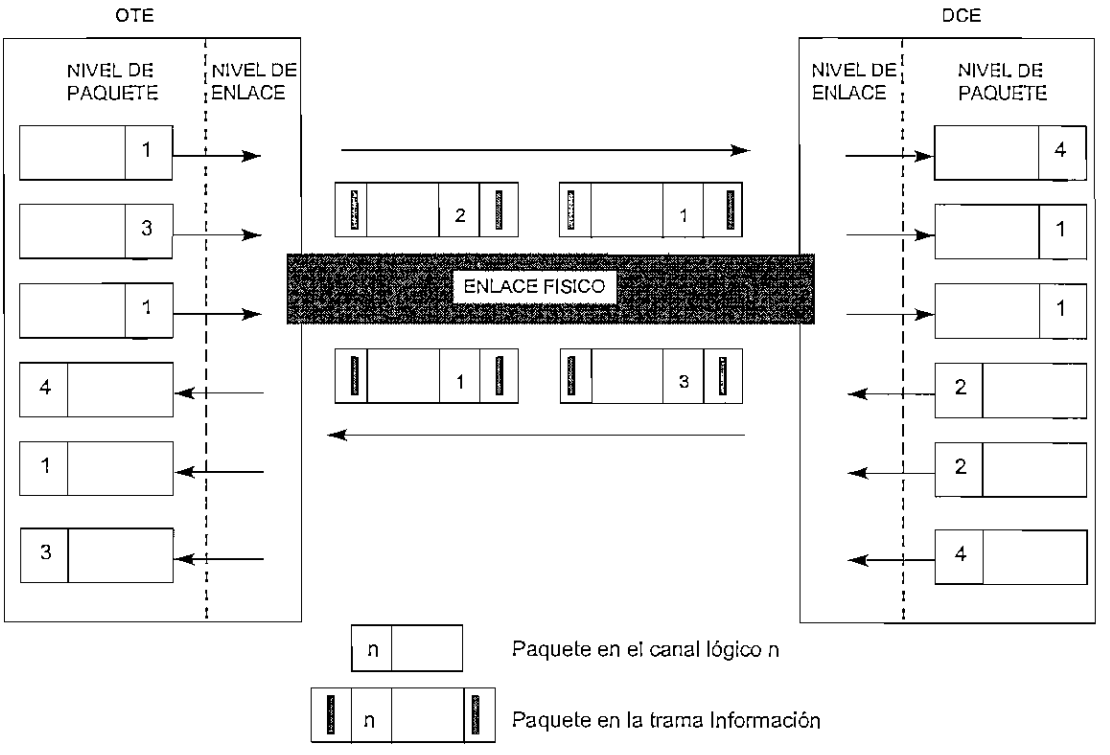


Figura 1.19 Multiplexación de paquetes

1.2.1.3.1 CIRCUITOS VIRTUALES

El Nivel de Paquete soporta múltiples circuitos virtuales a través de un enlace simple. Un circuito virtual es una asociación *end to end* entre dos *DTEs*. Esto se realiza estableciendo un camino permanente o temporal desde uno de los canales lógicos de un *DTE* hacia uno de los canales lógicos de otro *DTE*.

La figura 1.20 muestra los circuitos virtuales formados en cuatro *DTEs*, en donde el número del canal lógico (*LCN*) en un lado del circuito virtual no necesariamente es el mismo *LCN* en el otro lado.

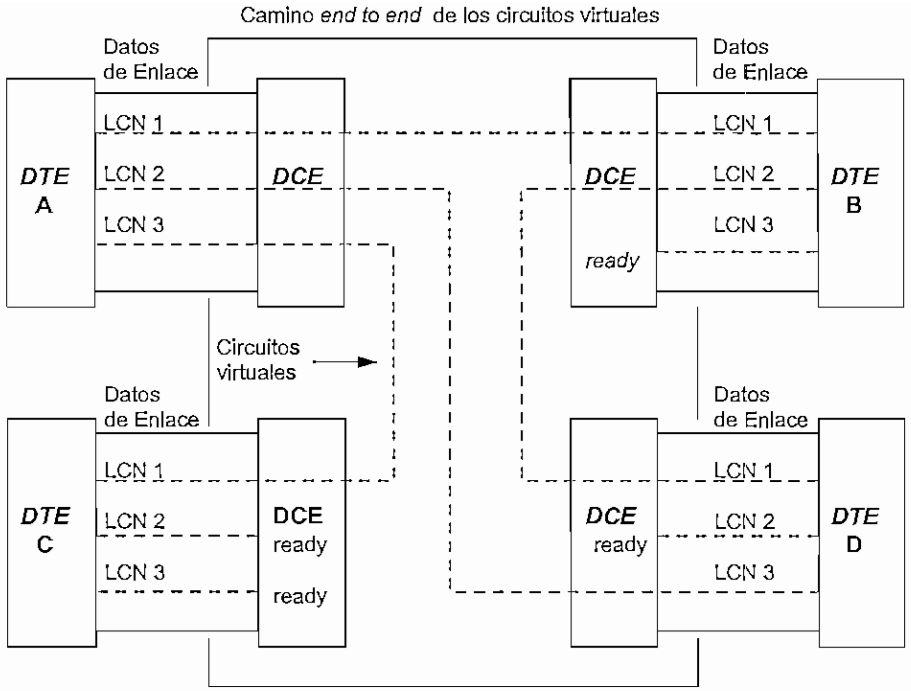


Figura 1.20 Formación de circuitos virtuales entre *DTEs*

a) CIRCUITOS VIRTUALES CONMUTABLES *SVCs*

Es una asociación entre dos *DTEs,* que puede ser disuelta por petición de cualquiera de las dos estaciones. Los canales lógicos son asociados con una llamada virtual solo durante el tiempo en que la llamada permanece.

Los estados y fases de los circuitos virtuales conmutables son:

- ***Ready State.-*** Un canal lógico está en estado ready cuando éste no está asignado a una llamada virtual.

- ***Call Establishment Phase.-*** Es iniciada por un *DTE,* en donde se intercambian varios mensajes entre la fuente y el destino con el propósito de identificar a los *DTEs*, el número de canal lógico *LCN* que utilizará cada uno, y las facilidades.

  Si la llamada es aceptada, los canales lógicos ingresan en el estado de *Flow Control Ready.*

- ***Flow Control Ready State.-*** Este estado de un canal lógico se produce cuando la fase de Transferencia de Datos e Interrupción es reinicializada por un reset o cuando es encendido el equipo.

- ***Data and Interrupt Transfer Phase*** En esta fase los paquetes de datos y los paquetes de interrupción pueden ser intercambiados entre los *DTEs*. Un paquete de interrupción es un paquete que salta los procesos de control de flujo.

Los circuitos virtuales conmutables pueden ser:

1. *One way Incoming SVCs*, que pueden ser usados solo para llamadas entrantes.
2. *Two way SVCs* , empleados por llamadas entrantes y salientes.
3. *One way Outgoing SVCs*, se utilizan solo para llamadas salientes.

b) CIRCUITO VIRTUAL PERMANENTE *PVCs*

En un circuito virtual permanente el *LCN* en cada lado de la conexión es asignada permanentemente y el *PVC* está siempre en la fase de transferencia de datos e interrupción. Los procesos de reinicialización borran y reinicializan todos los circuitos virtuales asociados con el interfaz *DTE/DCE* donde es iniciado este proceso.

c) CANALES LOGICOS

Un circuito virtual entre dos *DTEs* tiene asignado independientemente un número de canal lógico en cada interfaz *DTE/DCE*. Los *LCNs* usados por los *SVCs* son asignados a una llamada establecida, en tanto que en los PVCs son asignados en forma permanente. Cada paquete transferido a través del interfaz *DTE/DCE* contiene un *LCN*.

El *LCN* del interfaz *DTE/DCE* local de un circuito virtual no necesita ser igual al *LCN* asignado al interfaz *DTE/DCE* remoto del mismo circuito virtual. La red es responsable de mantener el rastro de los *LCNs* asociados a las estaciones locales y remotas, como indica la figura 1.21.

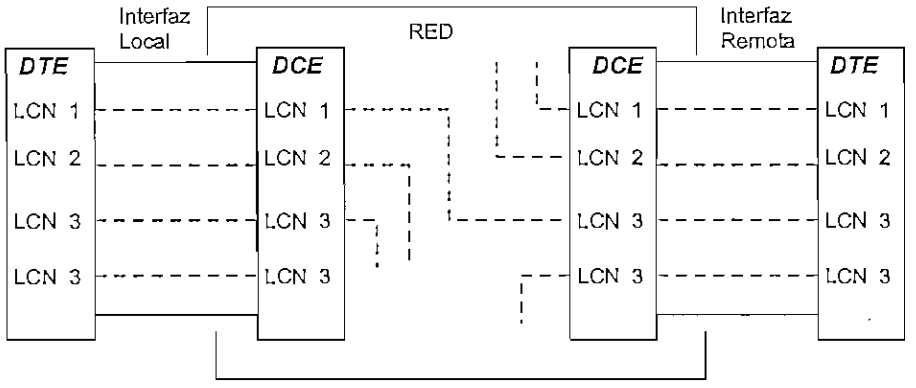


Figura 1.21 Ejemplo de *LCNs* en los terminales local y remoto de un circuito virtual

El nivel de paquete soporta varios tipos de paquetes, como muestra el cuadro 1.3, en donde se indica la dirección de la transmisión, la clasificación y el tipo de circuito virtual que se genera para cada paquete:

TIPO DE PAQUETE		SERVICIO	
Desde el *DCE* hasta el *DTE*	**Desde el *DTE* hasta el *DCE***	***SVC***	***PVC***
	Llamada de inicio y borrado		
Incoming call	*Call request*	X	
Call Connected	*Call accepted*	X	
Clear indication	*Clear request*	X	
DCE clear confirmation	*DTE clear confirmation*	X	
	Datos e Interrupciones		
DCE data	*DTE data*	X	X
DCE Interrupt	*DTE Interrupt*	X	X
DCE interrupt confirmation	*DTE interrupt confirmation*	X	X
	Control de flujo y *reset*		
DCE RR	*DTE RR*	X	X
DCE RNR	*DTE RNR*	X	X
	DTE REJ	X	X
Reset Indication	*Reset request*	X	X
DCE reset confirmation	*DTE reset confirmation*	X	X
	Restart		
Restart indication	*Restart request*	X	X
DCE restart confirmation	*DTE restart confirmation*	X	X
	Diagnóstico		
Diagnostic		X	X
	Registro		
Registration confirmation		X	X
	Registration request	X	X

Cuadro 1.3 Tipos de paquetes X.25

1.2.1.3.2 FORMATO DEL PAQUETE

Cada paquete consiste de tres primeros octetos que contienen campos comunes al resto de paquetes, como se indica en la figura 1.22.

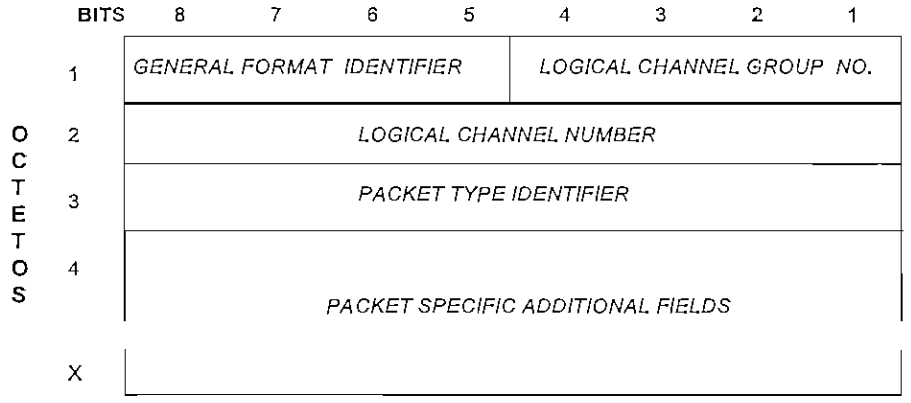


Figura 1.22 Formato del Paquete

- ***General Format Identifier (GFI)***

  Es usado para identificar el esquema de numeración de secuencia en los paquetes.

  En los paquetes de datos se usa para confirmación de liberación del paquete (bit D) y para diferenciar los paquetes que contienen diferente tipo de información (bit Q).

- ***Logical Channel Group Number (LCGN) y Logical Channel Number (LCN)***

  Ambos campos identifican a los *LCNs*, en donde los 4096 canales lógicos pueden ser divididos en 16 (0-15) grupos de 256 (0-255) canales lógicos.

  Los equipos *DTEs* examinan los dos campos para identificar la conexión virtual asociada con cada paquete, con el fin de liberarlos hacia los procesos de alto nivel apropiados.

  Permite realizar la multiplexación de paquetes.

- ***Packet Type Identifier***

  Examinando este campo, el *DTE* o *DCE* pueden determinar el tipo de paquete.

- ***Packet Specific Additional Fields***

  Es un campo opcional que depende del tipo de paquete, como son: los datos y algunos paquetes de control.

- **ESTABLECIMIENTO DE LA LLAMADA**

El establecimiento de llamada se aplica solo para circuitos virtuales conmutables *SVCs*, establecidos entre un *DTE* llamador y un *DTE* llamado. Los *LCNs* usados para manejar un *SVC* en el *DTE* que llama y en el *DTE* llamado, son asignados en el proceso de establecimiento de la llamada.

Los elementos que intervienen en el establecimiento de la llamada se indican en la figura 1.23, en donde se identifican las siguientes estaciones:

- El *DTE* llamador que inicia la llamada se denomina *calling DTE*
- El *DCE* conectado al *DTE* que inicia la llamada se denomina *local DCE*
- El *DCE* conectado al *DTE* que recibe la llamada se denomina *remote DCE*
- El *DTE* que recibe la llamada se denomina *called DTE*

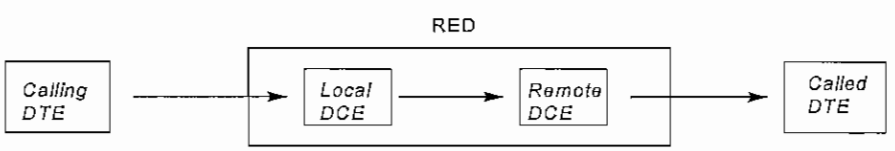


Figura 1.23 Fase de establecimiento de llamada

- ***CALL REQUEST / CALL ACCEPT***

Como indica la figura 1.24, el *calling DTE* inicia la llamada virtual enviando un paquete *Call Request* al *local DCE*, asignando un *LCN* dentro del paquete para identificar esta llamada. Este paquete contiene la dirección de la red del *called DTE* y opcionalmente la dirección de red del *calling DTE.*

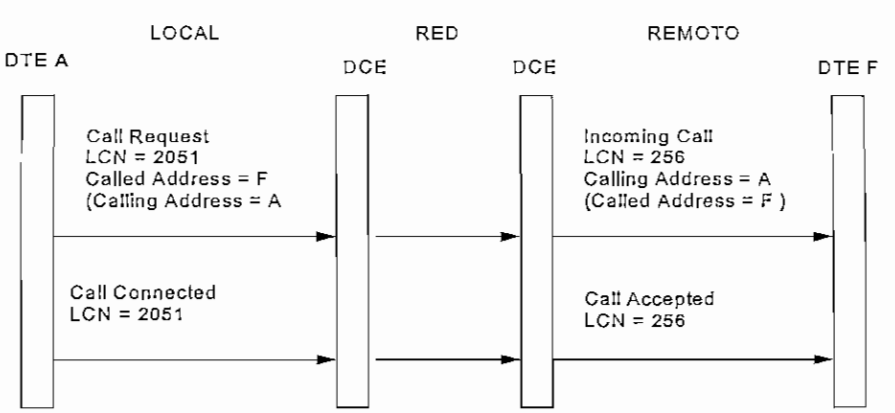


Figura 1.24 Fase de establecimiento de llamada

El *local DCE* transmite el *Call Request* a través de la red hasta el *remote DCE.*

El *remote DCE* recibe el paquete y asigna un *LCN* para identificar la llamada en este lado, luego transfiere un paquete *Incoming Call* hasta el *Called DTE*. Este paquete es el mismo paquete recibido pero cambiado la cabecera, el cual contiene la dirección de red del *Calling DTE* y opcionalmente la dirección de red del *Called DTE.*

El paquete *Incoming Call* notifica al *Called DTE* que el *DTE* identificado por la dirección de red incluida, está llamando.

Para aceptar la llamada el *Called DTE* envía un paquete *Call Accepted* que contiene el mismo *LCN* del paquete *Incoming Call* hacia el *remote DCE*, confirmando el establecimiento del circuito virtual especificado en el *LCN* incluido.

El *remote DCE* entonces transmite el *Call Accepted* a través de la red hasta el *Local DCE*.

Cuando el *Local DCE* recibe el paquete, éste modifica el campo *LCN,* ingresando el número de conexión lógica (*LCN*) que estaba en el paquete *Call Request.* Luego este paquete es enviado hacia el *Calling DTE* como un paquete *Call Connected*, notificando que el circuito virtual identificado por el *LCN* incluido en el paquete, ha sido confirmado por el *Called DTE*.

El *Calling DTE* recibe el paquete *Call Connected*, quedando establecida la llamada y empezando la fase de transferencia de datos e interrupciones.

El formato de los paquetes *Call Request/Incoming Call* se muestran el la figura 1.25.
El formato de los paquetes *Call Accepted/Call Connected* se muestran el la figura 1.26.

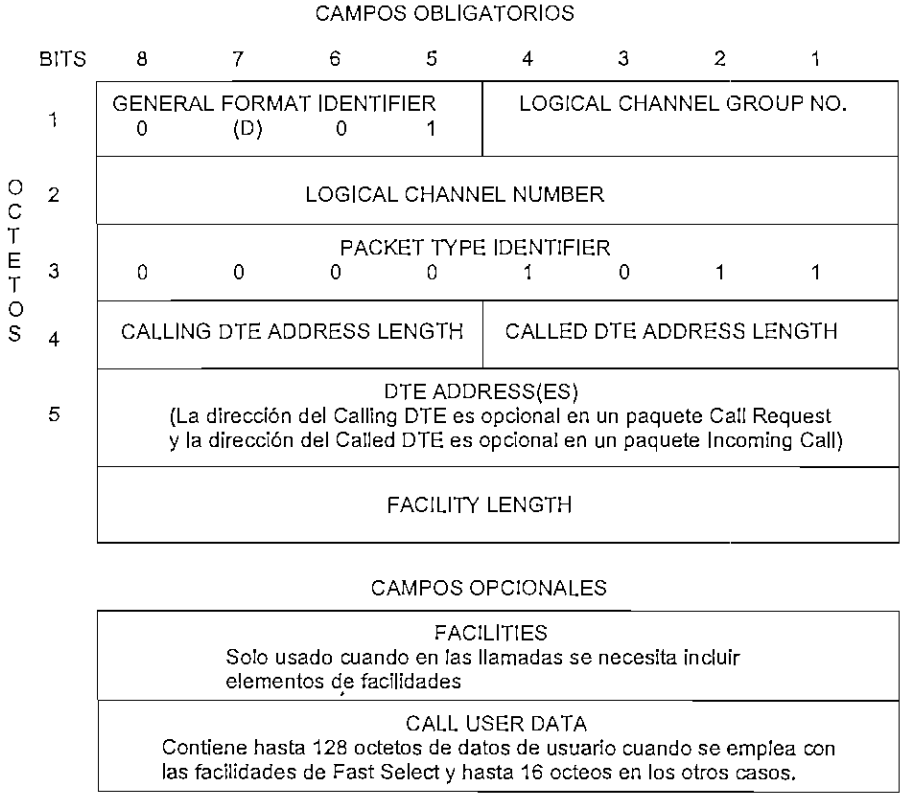


Figura 1.25 Formatos de los paquetes *Call Request* e *Incoming Call*

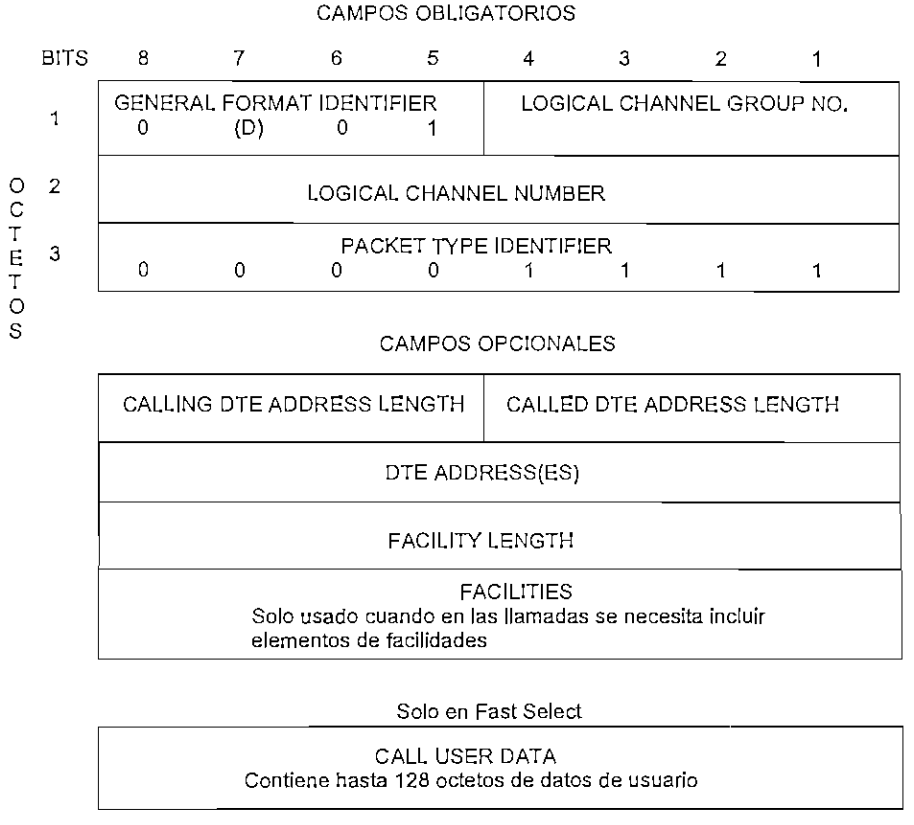
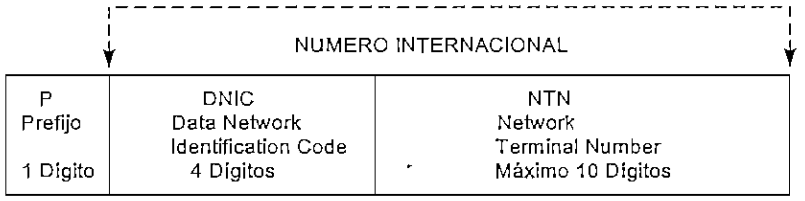


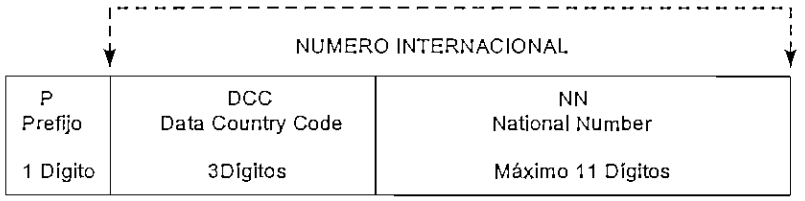
Figura 1.26 Formato de los paquetes *Call Accepted* y *Call Connected*

1.2.1.3.3 FORMATO DE DIRECCION DTE

La dirección *DTE* puede ser la dirección de red del *DTE* o cualquier otra identificación agregada entre el *DTE* y el *DCE* , especificadas por la recomendación X.121 cuyos formatos se indican en la figura 1.27.



a) Formato de dirección X.121 para DTEs en países con más de una red



b) Formato de dirección X.121 para DTEs en países con una red integrada

Figura 1.27 Formatos de dirección X.121 para *DTEs*

En ambos casos la dirección *DTE* tiene máximo 14 dígitos (el prefijo no es parte de la dirección *DTE*). La identificación de los dígitos es la siguiente:

- **Prefijo P** Es usado para llamadas internacionales salientes e indica que la llamada se hace para otro país.

- ***Data Network Identification Code (DNIC).*** Sirve para identificar cualquier red en el mundo. El primer dígito representa una de las 6 zonas del mundo (2-7), los dos dígitos siguientes representan al país en la zona, y el último dígito representa una red dentro del país.

- ***Network Terminal Number (NTN)*** Se utiliza para especificar la dirección de un DTE dentro de la red con una longitud máxima de 10 dígitos, como se indica en la figura 1.28, donde los 8 primeros dígitos se emplean para identificar un *DTE* específico y los dos últimos identifican uno de los puertos del *DTE*, con lo que la llamada se puede enviar a un proceso de alto nivel específico, como por ejemplo a un programa de aplicación.

A A A Código de área 3 Dígitos	S S S S S Número de servidor 5 Dígitos	P P Subproceso o dirección de puerto 2 Dígitos

a)

N N Localización geográfica 2 Dígitos	N N N N N N Dirección DTE 6 Dígitos	C C Usuario definido 2 Dígitos

b)

X X Identificador DCE 2 Dígitos	Y Area DCE 1 Dígito	Z Z Z Z Z Identificador DTE 5 Dígitos	U U Subdirección de identificador 2 Dígitos

c)

Figura 1.28 Formatos del *Network Terminal Number (NTN)*

- ***Data Country Code (DCC)*** Es equivalente a los tres primeros dígitos del *DNIC* empleado por países que tienen una sola red.

- ***National Number (NN)*** Equivale al último dígito del *DNIC* combinado con un *NTN* y es usado por países con una sola red.

1.2.1.3.4 TRANSFERENCIA DE DATOS

Los datos son divididos en paquetes para transmitirlos a través de la red. Los paquetes asociados con un circuito virtual específico contienen el *LCN* asignado a este circuito virtual. Esto permite al *DTE* identificar el circuito virtual al cual cada paquete recibido pertenece. Como resultado los paquetes son enrutados hacia los procesos de alto nivel.

En cambio cuando un proceso de alto nivel tiene un dato para enviar, el *DTE* pone en el campo *LCN* del paquete resultante el *LCN* asociado con el proceso de alto nivel. Esto permite al *DCE* identificar el circuito virtual que debe usar cada paquete que se envía.

El *DCE* destino cambia la cabecera del paquete colocando en el campo *LCN*, el *LCN* asociado con el circuito virtual de este lado. Esto le permite al *DTE* enrutar el paquete hacia los procesos de alto nivel

1.2.2 *FTP (FILE TRANSFER PROTOCOL)* [6]

Es un protocolo de *Internet*[7] que tiene el propósito de transferir archivos entre computadoras.

- Es un protocolo interactivo

- Se puede manipular archivos en el sistema remoto

- Se puede transferir datos desde un archivo fuente hasta un archivo destino

El usuario debe conocer el *"login"* y el *"password"* del sistema remoto.

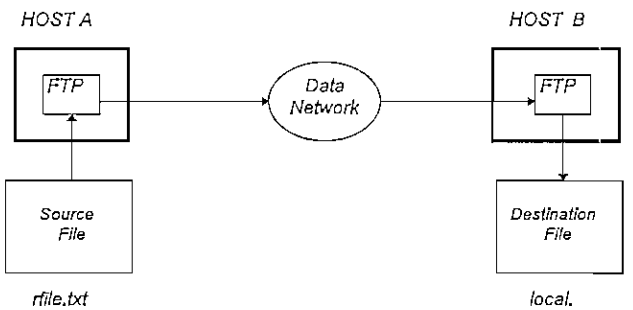


Figura 1.29 Proceso *FTP*

1.2.3 *SMTP (SIMPLE MAIL TRANSFER PROTOCOL)*

Es un protocolo que provee procesos de emisión y recuperación de correo electrónico y seguridades a un determinado grupo de usuarios.

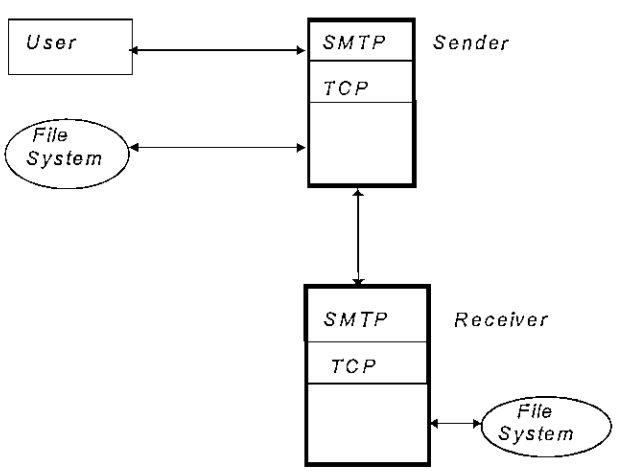


Figura 1.30 Proceso *SMTP*

Para el transporte, *SMTP* utiliza *TCP* por ser un servicio confiable.

---

[6] *TCP/IP Technical Concepts , Open Strategies, Inc and NCR* Capítulo 4

[7] Conjunto de redes y ruteadores que abarca la mayoría de países y utiliza los protocolos *TCP/IP* para formar una sola red virtual cooperativa.

1.2.4 *TCP (TRANSPORT CONTROL PROTOCOL)*

Es un protocolo de transporte orientado a conexión, que garantiza la entrega de los datos generados en la capa de Aplicación, sin errores, duplicaciones, pérdida del orden de las unidades de datos.

Esta capacidad de detección y corrección de errores hace que TCP opere totalmente en sistemas de liberación de paquetes y pueda ser aplicado en una amplia variedad de redes , tanto en *LANs* de alta velocidad como también en *WANs.*

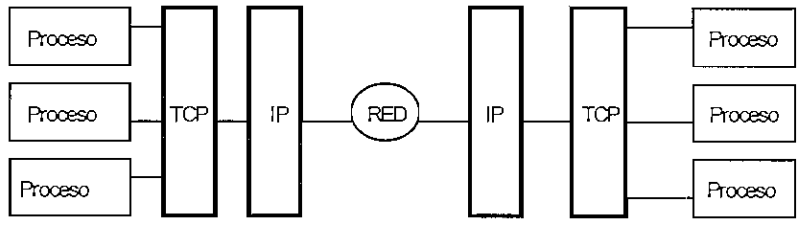


Figura 1.31 Multiplexación TCP/IP

TCP permite la conexión Múltiplex entre más de una pareja de usuarios, para el intercambio de información. Su unidad de intercambio de datos es el SEGMENTO.

1.2.5 *IP (INTERNET PROTOCOL)*

IP ofrece un servicio de conexión no confiable entre *hosts*, o hacia las capas superiores en el mismo nodo. Su unidad de intercambio es el **datagrama**, el mismo que pueden ser fragmentado para la transmisión y reensamblado en el nodo destino.

En sistemas con *gateways*[8], *IP* enruta cada datagrama independientemente, entre redes diferentes, para lo cual emplea tablas de rutas ubicadas tanto en el *host* como en el *gateway*.

Los datagramas *IP* pueden tomar caminos diferentes hacia el destino, dependiendo de las condiciones y facilidades del medio, por lo que pueden llegar al destino en desorden, lo cual **no** garantiza la confiabilidad de los mismos, aun cuando sea sólo parte del mensaje.

[8] Gateway es una computadora dedicada al enrutamiento de paquetes entre redes

Algunos datagramas pueden ser eliminados dependiendo de condiciones, como la expiración del tiempo de vida (*Time To Live TTL*), congestión en la red o errores de bits.

1.2.6 *ICMP (INTERNET CONTROL MESSAGE PROTOCOL)*

Este protocolo permite que los ruteadores o *hosts* envíen mensajes de error o de control hacia otros ruteadores o *hosts* .

Cuando un datagrama causa un error, el *ICMP* reporta la condición de error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

Todos estos mensajes se describen en detalle en el Anexo 1.

1.3 TECNOLOGIAS DE ACCESO AL MEDIO

1.3.1 *ETHERNET / IEEE* 802.3 [9]

Ethernet e *IEEE 802.3* son tecnologías basadas en *CSMA/CD* (*Carrier Sense Multiple Access / Collision Detection*), en donde una estación detecta si la red está libre para enviar información , caso contrario espera un tiempo para volver a intentar la transmisión.

Si dos estaciones escuchan que la red está disponible, y envían datos simultáneamente, se produce una colisión que daña los dos mensajes, y por lo tanto deben ser retransmitidos.

Los mensajes llegan a todas las estaciones , las cuales deben determinar si los datos son o no destinadas a éstas.

Ethernet provee servicios a las capas 1 y 2 del modelo *OSI*, mientras que *IEEE 802.3* trabaja en la capa 1 y parte de la capa 2 , pero no define un enlace lógico.

El cuadro 1.4 muestra una relación de *Ethernet* y *IEEE 802.3* con sus diferentes configuraciones.

---

[9] *Internetworking Technology Overview , Cisco System* Capítulo 5

Características Físicas

Características	*Ethernet*	IEEE 802.3			
		10 Base 5	10 Base 2	1 Base 5	10 Base T
Transferencia de Datos Mbps	10	10	10	1	10
Métodos de Señalamiento	Banda base	Banda base	Banda base	Banda base	Banda base
Longitud máxima del segmento (m)	500	500	185	250	100
Medio	Cable coax. 50	Cab. coax. 50	Cab. Coax. 50	UTP	UTP
Topología	Bus	Bus	Bus	Estrella	Estrella

Cuadro 1.4 Características físicas de los medios *Ethernet* e *IEEE* 802.3

Los formatos de las tramas *Ethernet* y 802.3 son :

Ethernet

Bytes	7	1	6	6	2	46 - 1500	4
	Preámbulo	SOF	Dirección destino	Dirección fuente	Tipo	Datos	FCS

IEEE 802.3

Bytes	7	1	6	6	2	46 - 1500	4
	Preámbulo	SOF	Dirección destino	Dirección fuente	Longi tud	Datos	FCS

SOF = *Start of frame delimiter*
FCS = *Frame check sequence*

Figura 1.32 Formato de las tramas *Ethernet* e *IEEE* 802.3

- El tipo indica el formato que está siendo usado para el campo de datos.
- La longitud indica el tamaño del dato que precede a *FCS*.
- Cuando el área de datos no completa la longitud especificada, se rellena con ceros.

1.3.2 *TOKEN RING / IEEE 802.5* [10]

Token Ring e *IEEE 802.5* son dos tecnologías compatibles. Tienen una topología en estrella, con las estaciones conectadas a una *multistation access unit* (*MSAU*).

	Token Ring	IEEE 802.5
Transferencia de datos	4/16 Mbps	4/16 Mbps
Estaciones/ Segmentos	260 (STP) 72 (UTP)	250
Topología	Estrella	No especificado
Medio	Par Trenzado	No especificado
Señalamiento	Banda base	Banda base
Método de acceso	Token Passing	Token Passing
Encodificación	Manchester Diferencial	Manchester Diferencial

Cuadro 1.5 Características físicas de *Token Ring* e *IEEE* 802.5

TOKEN PASSING mueve una pequeña trama llamada ***Token*** por toda la red . La posesión del *token* de una estación, le otorga el derecho a transmitir, pero si no tiene información para enviar, lo pasa a la siguiente estación. Cuando se envía información, se cambia el estado del *Token* y se pasa a la siguiente estación. Mientras la información esté circulando en el anillo, no hay *token* en la red, de modo que la otra estación, debe esperar a que el *token* sea liberado, lo cual se produce cuando la transmisión anterior alcanza su destino. Con este método se evita colisiones en la red.

Se puede calcular el tiempo en que una estación está apta para transmitir, por lo que es ideal en redes que manejan retardos, como en automatización de fábricas.

Permite dar **prioridades** a las estaciones , mediante un campo de prioridad en la trama.

---

[10] *Internetworking Technology Overview , Cisco System* Capítulo 6

Sólo las estaciones con prioridad igual o mayor que la prioridad contenida en el *Token* pueden apoderarse del *Token*. Cuando se envía información , sólo las estaciones con prioridad más alta que la prioridad de la estación emisora tienen derecho a utilizar la trama del *Token*. Cuando se completa la transmisión, la estación final debe reasignar el *token* con la prioridad de la estación emisora anterior. Si una estación emisora falla , la trama generada puede bloquear el anillo, por lo que un monitor activo debe detectar esta anomalía, remover la trama, y generar un nuevo *token*.

Si la estación se daña , el *MSAU* puede removerla del anillo si es necesario.

Un ejemplo de conexión se muestra en la figura 1.33:

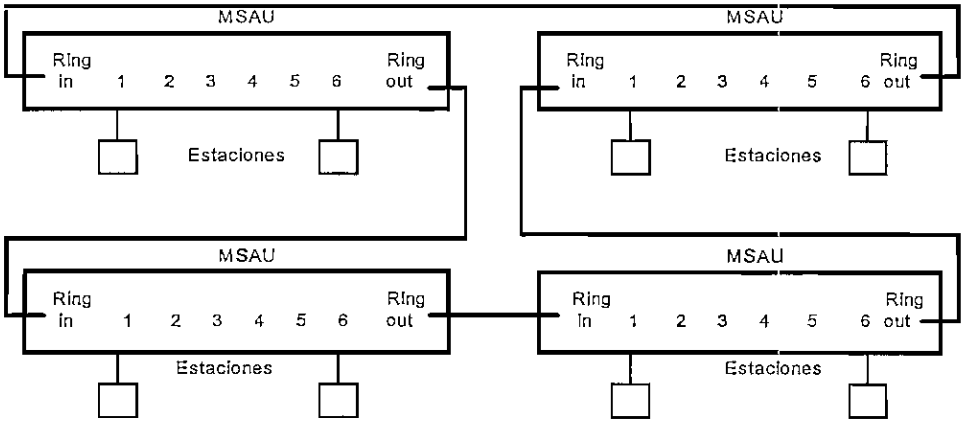


Figura 1.33 Conexión Token Ring de *multistation access unit MSAU*

En estas redes se tiene dos tipos de tramas: Trama de *Token* y Trama de Datos / Comandos como se muestra en la figura 1.34.

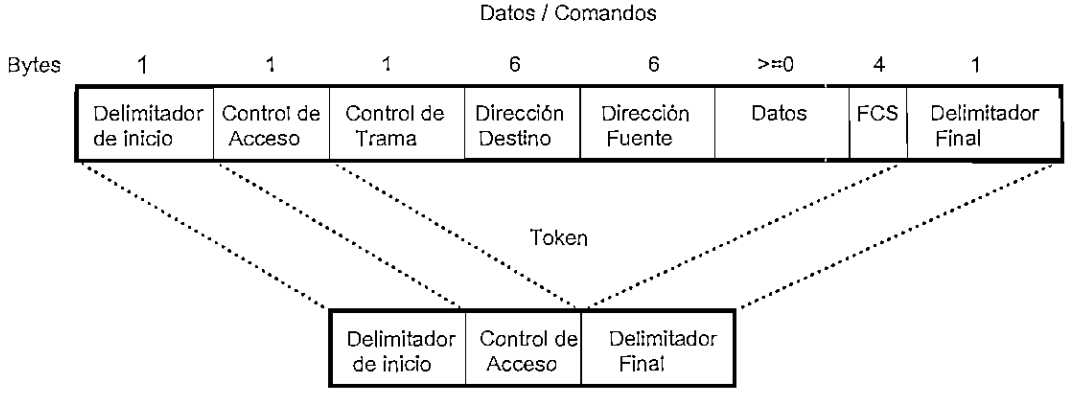


Figura 1.34 Formato de la trama *Token Ring*

Los diferentes campos en la trama tienen las siguientes funciones:

- El delimitador de inicio sirve para alertar a la estación el arribo del *Token* (o de la trama Datos /Comandos).
- El delimitador final indica si la trama está dañada y si tiene la debida secuencia.
- El *byte* de control de acceso contiene los bits de prioridad, el bit que diferencia las tramas de datos/comandos de la trama *Token*, un bit de monitoreo para determinar si la trama está circulando indefinidamente en el anillo.
- El campo de datos lleva información para los protocolos de las capas superiores.
- El *byte* de control de trama indica si la trama contiene datos o información de control.
- *FCS* sirve para determinar si la información se dañó en el transcurso de la transmisión, en cuyo caso es eliminada.

1.3.3 *FDDI (FIBER DISTRIBUTED DATA INTERFACE)* [11]

Es un método muy veloz de transmisión *Token Passing* por fibra óptica, con anillo dual a 100 Mbps. Es más confiable porque usa anillos redundantes, los cuales operan en sentidos opuestos.

Con fibras *single mode*[12] se tiene un mayor ancho de banda y se puede transmitir a distancias más largas que las fibras multimodo.

FDDI está formado por cuatro módulos :

- Control de acceso al medio (*MAC*) . Define como el medio es accesado, incluyendo el formato de trama, manejo de token , direcciones , *CRC* [13], recuperación de errores.
- Protocolo de Capa Física (*PHY*) . Son los procesos de encodificación de datos, requerimientos de reloj, tramas.

---

[11] *Internetworking Technology Overview, Cisco System* Capítulo 7

[12] La fibra *Single Mode* propaga un sola frecuencia de luz a través de la fibra

[13] *CRC* (Código de Redundancia Cíclica) es un número entero calculado a partir de una secuencia de octetos utilizados para detectar errores que aparecen cuando una secuencia de octetos se transmite de una máquina a otra.

- Capa del Medio Físico (*PMD*). Determina las características del medio de transmisión, incluyendo el enlace de fibra óptica, niveles de potencia, *BER*, componentes ópticos y conectores.
- Manejador de la Estación (*SMT*) . Realiza la configuración de la estación *FDDI* y del anillo, controla la remoción/inserción de estaciones, inicialización, aislamiento y recuperación de fallas.

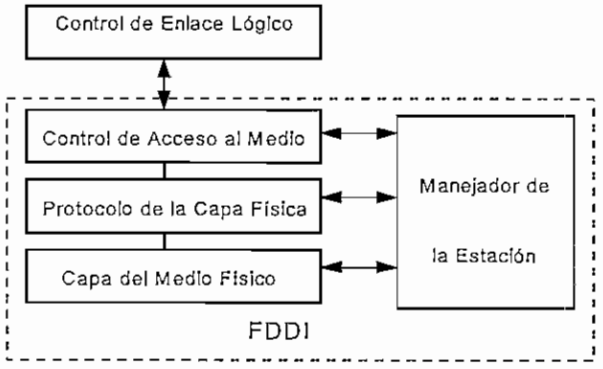


Figura 1.35 Estructura de *FDDI*

El formato de la trama *FDDI* es similar al de *Token Ring*.

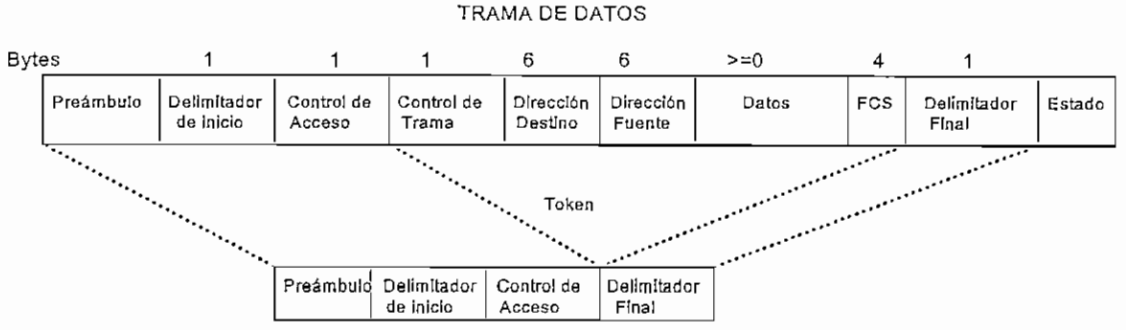


Figura 1.36 Formato de la trama de datos *FDDI*

El preámbulo prepara a cada estación para recibir la trama. El estado permite a la estación fuente determinar si un error ha ocurrido y si la trama fue reconocida y copiada por la estación receptora.

FDDI tiene dos anillos en sentidos opuestos, donde el primario es usado para transmitir datos y el secundario es para respaldo, con lo cual se consigue tolerancia a fallas. Los anillos constan de dos o más conexiones punto a punto entre estaciones adyacentes.

Las estaciones simples (*Single attachment station SAS*) se conectan al anillo primario a través de concentradores que aseguran que las fallas de las estaciones no interrumpan el anillo, mientras que las duales (*Dual attachment station DAS*) se conectan a los dos anillos por cuanto posee 2 puertos A y B.

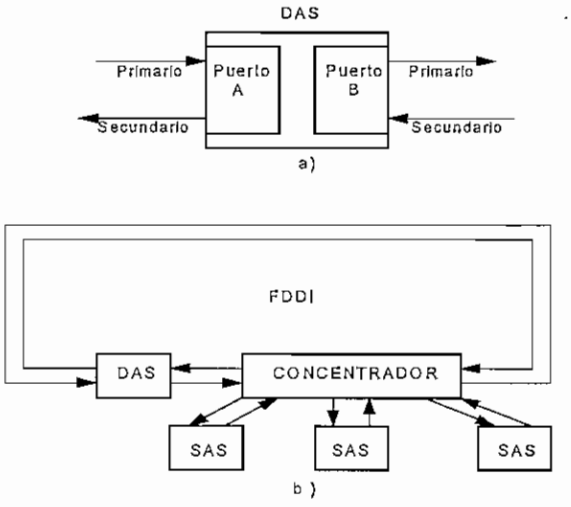


Figura 1.37 a) Estación *FDDI* Dual b) Anillo *FDDI* con estaciones Duales y Simples

Soporta tráfico sincrónico y asincrónico, en donde el sincrónico puede ocupar parte de los 100 Mbps de ancho de banda , asignándose a estaciones que requieren transmisiones continuas como es el caso de información de voz y vídeo, en tanto que el asincrónico toma el resto del ancho de banda.

Cuando un anillo falla, el dual de respaldo entra a funcionar inmediatamente. Si una estación dual se daña, las dos adyacentes unen los dos anillos, con lo cual se forma nuevamente el camino para que el *token* siga circulando, como se muestra en la figura 1.38.

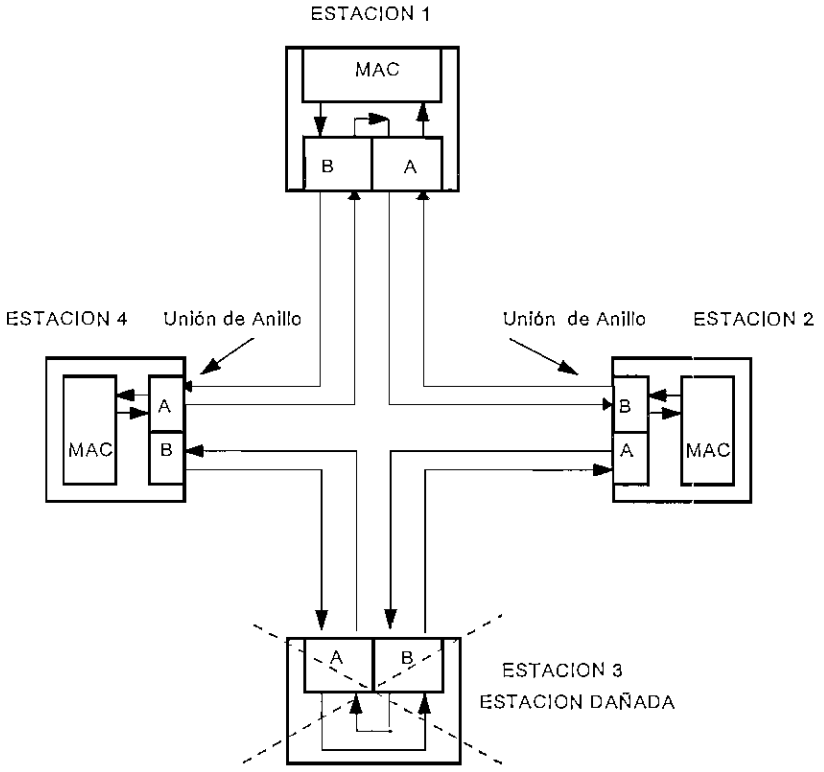


Figura 1.38 Conexión *FDDI* redundante , con estaciones Duales (Falla estación 3)

Cuando un cable falla, las estaciones 3 y 4 cierran el anillo, como se muestra en la figura 1.39.

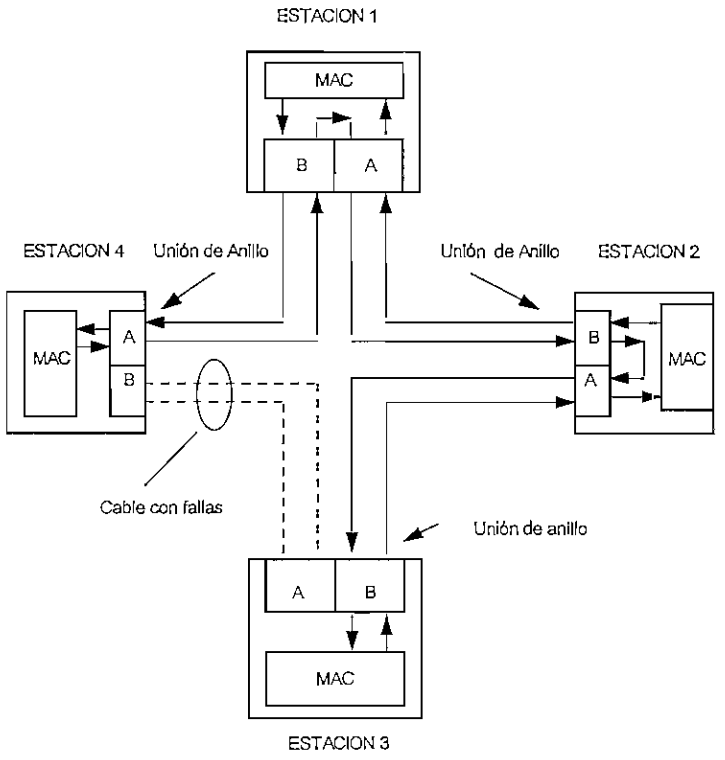


Figura 1.39 Conexión *FDDI* redundante (falla el cable de fibra óptica)

1.3.4 *ATM (ASYNCHRONOUS TRANSFER MODE)* [14]

Es una tecnología de red orientada a la conexión de alta velocidad, utilizado tanto en redes *LAN* como en *WAN*. Operan en velocidades superiores a 100 *Mbps* , para lo cual utiliza **conmutadores** de datos de alta velocidad, conectados a cada una de las estaciones anfitrionas. Es independiente del protocolo ya que soporta *Ethernet , Token Ring, FDDI.*

Las conexiones son realizadas con fibra óptica para operar en el rango de 100 a 155 Mbps. Las capas más bajas utilizan tramas de tamaño fijo llamados **celdas** , de 53 octetos de largo, de los cuales 5 son el encabezado, y los otros 48 son de datos.

Para enviar celdas es necesario, primero establecer la conexión entre el emisor y el receptor, para lo cual los conmutadores *ATM* establecen la ruta requerida entre las dos estaciones . Cuando se termina la transmisión de celdas, el conmutador desconecta las dos computadoras.

El funcionamiento de este tipo de redes se describe en el capítulo 5 y en el Anexo 2.

1.4 ELEMENTOS DE RED

1.4.1 NODO

Un nodo es cualquier procesador o terminal que contiene el *hardware* y el *software* necesario para soportar la arquitectura de red, con el fin de permitir que los procesos de aplicación hagan uso de la red, tal como se ilustra en la siguiente figura:

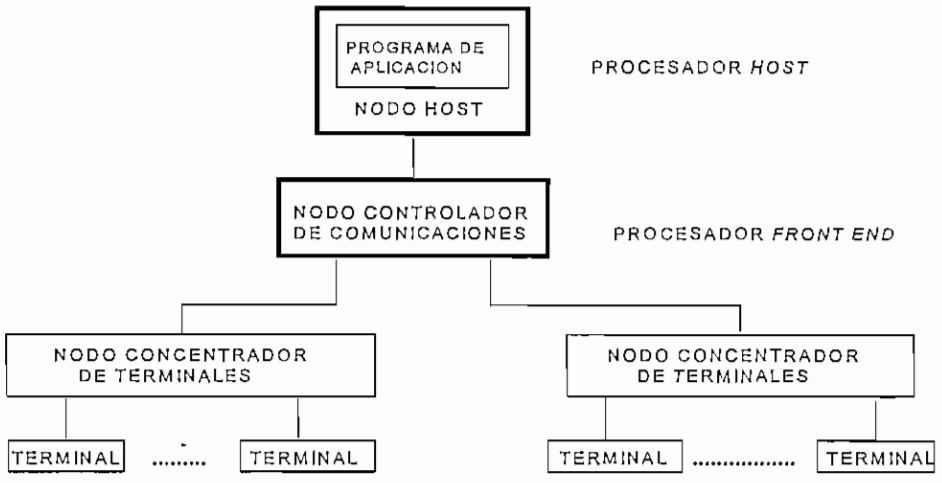


Figura 1.40 Disposición de nodos en una red

[14] Redes Globales de Información con *Internet* y *TCP/IP*, Douglas Comer

1.4.2 *HUBS* O CONCENTRADORES [15]

Son dispositivos que concentran los medios de conexión. Pueden ser **homogéneos** cuando soportan un simple protocolo de *LAN* (Sólo *Ethernet, o* sólo *Token Ring*) , en tanto que los **heterogéneos** soportan múltiples protocolos de *LAN.*

Cuando los *Hubs* son inteligentes, permiten la configuración, manejo, estadísticas , de cada uno de los puertos, con el fin de aislar daños, cuando éstos se producen. Además tienen el protocolo *SNMP*[16], para que pueda ser controlado por un software de monitoreo de red.

El ancho de banda disminuye cuando aumenta el número de usuarios en el *hub,* lo cual puede ocasionar un cuello de botella en las comunicaciones.

Se divide el ancho de banda del siguiente modo:

Ancho de banda total = MBits por usuario x Número de usuarios

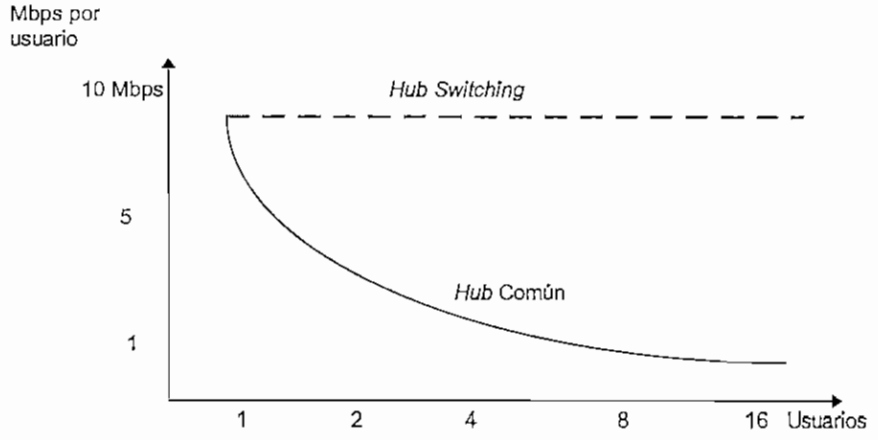


Figura 1.41 Variación del ancho de banda con el número de usuarios conectados en un *Hub*

Para interconectar medios diferentes, se utiliza **transceptores,** con el fin de integrar redes que utilizan diferentes tipos de cableados. Existen transceptores de AUI/BNC, AUI/RJ45 BNC/RJ45 y otras combinaciones posibles.

---

[15] *IBM Server Technical Training, IBM PC Institute* Capítulo 5
[16] *SNMP (Simple Network Monitoring Protocol)*, protocolo empleado para monitorear *hosts*, ruteadores y redes.

1.4.3 *HUB SWITCHING* DEDICADOS [17]

Mantiene el ancho de banda, independientemente del número de usuarios.

A los servidores se les coloca en una línea dedicada.

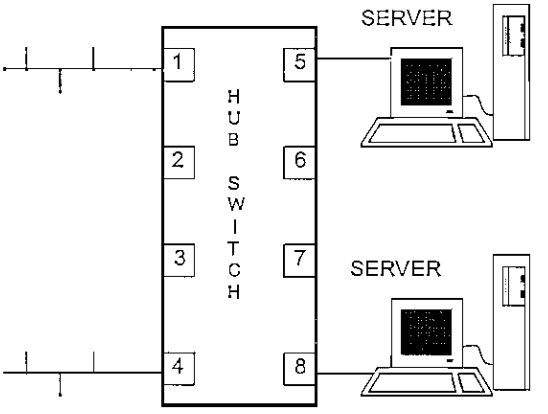


Figura 1.42 Conexión Servidores al *Hub Switching*

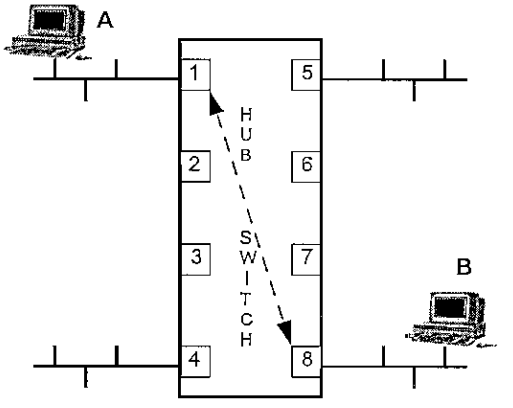


Figura 1.43 A envía paquetes a B a través del *switch*

Los *Hubs Switching* mantienen una tabla de rutas con las direcciones físicas de los equipos, lo que permite enviar los paquetes directamente al puerto que contiene la dirección destino, con lo cual se reducen las colisiones. Por ser una tecnología veloz, acepta paquetes de todos los puertos simultáneamente.

[17] *IBM Server Technical Training , IBM PC Institute* Capítulo 5

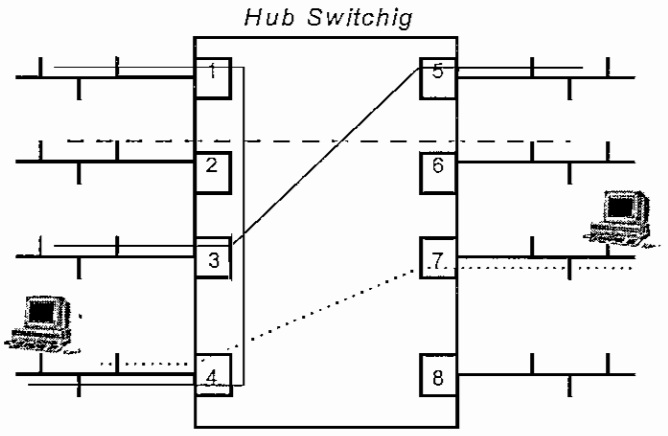


Figura 1.44 Operación de los puertos del *Hub Switching*

1.4.4 PUENTES Y RUTEADORES

Un ruteador es un equipo de propósito especial, que se conecta a dos o más redes y envía paquetes de una red a otra. Analiza las direcciones de destino en un paquete y compara con una tabla de rutas para decidir hacia donde debe enviar dicho paquete. Trabajan hasta la capa de red.

Un puente en cambio se conecta a dos o más redes y envía paquetes completos entre ellas. Operan en la capa física y se valen de las direcciones físicas de las estaciones para dirigir los paquetes hasta los destinos respectivos.

Estos dos elementos serán estudiados en detalle en el capitulo 2 y 5.

Otros elementos de red como conmutadores, servidores, arreglos de discos serán analizados en capítulos posteriores.

CAPITULO II PRINCIPIOS DE ENRUTAMIENTO

En un sistema de conmutación de paquetes , el **enrutamiento** es el proceso de selección de un camino por el que se envía paquetes de datos desde la fuente hasta el destino a través de la subred de comunicaciones.

Este capítulo describe los principios de los puentes y de los ruteadores, en donde se analiza la estructura interna y los protocolos que utilizan para su funcionamiento. Se analiza los principales protocolos ruteables como el TCP/IP y también los protocolos de enrutamiento.

2.1 FUNDAMENTOS DE PUENTES (*BRIDGES)*

Un puente es un dispositivo que conecta dos o más redes *LAN* utilizando las capas física y de enlace, empleando protocolos no "ruteables", con la finalidad de formar una sola red local de mayor extensión.

Algunos puentes emplean la capa física y la de enlace para unir redes de diferente tecnología como es el caso de *Ethernet* y *Token Ring.* La transformación de los paquetes del formato *Ethernet* al *Token Ring* se realiza en la capa de enlace a nivel de la subcapa de Control de Acceso al Medio *MAC*, como se muestra en la figura 2.1 .

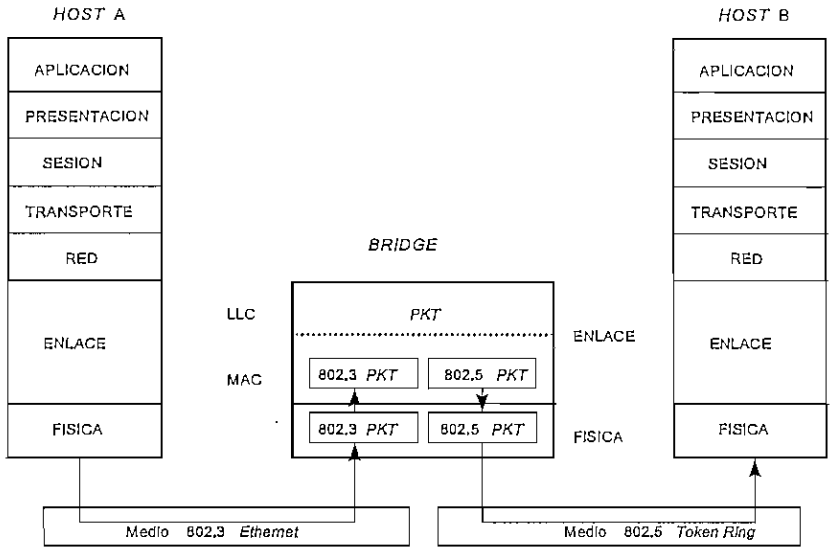


Figura 2.1 Unión de red *Ethernet* y *Token Ring* mediante *bridge* [1]

[1] *Internetworking Technology Overview, Cisco* Capítulo 3

Los puentes transforman los paquetes de las redes locales como *Token Ring* o *Ethernet* a paquetes manejables por dispositivos seriales, a través de los cuales se realiza los enlaces remotos entre los puentes, empleando protocolos de bajo nivel como X.25 o *Frame Relay*.

El tráfico fluye entre redes *LANs* a través de una red *WAN* sobre circuitos virtuales conmutables o permanentes (*SVC* o *PVC*), formados entre los puentes remotos como se muestra en la figura 2.2 b.

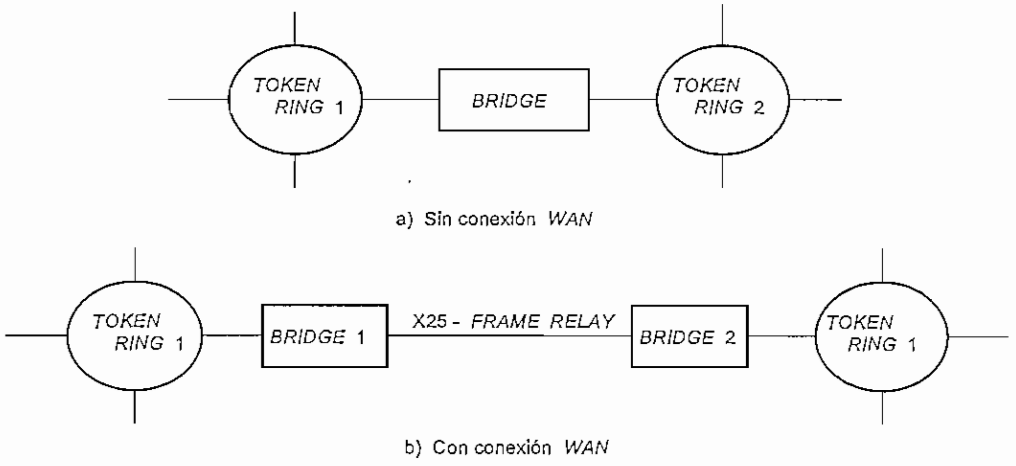


Figura 2.2 Conexión de redes locales mediante *Bridge* [2]

Los puentes empleados para unir redes remotas están formados por dos módulos:

- módulo de *LAN*
- módulo de *WAN*

El interfaz *WAN* de los puentes local y remoto se conectan mediante *SVCs* en X.25 o *PVCs* en *Frame Relay,* como se indica en la figura 2.3. En este caso, el ***BRIDGE*** **LOCAL** (NODO 1) pasa los datos de la red *LAN* 1, a través del módulo de enlace *bridge* de *LAN* hasta el módulo de enlace *bridge* de *WAN*. En el ***BRIDGE*** **REMOTO** (NODO 2) los datos ingresan por el módulo de enlace *bridge* de *WAN* y son enviados hasta la red *LAN* 2 a través del módulo de enlace *bridge* de *LAN*.

[2] *6500 Series Bridging, Motorola*

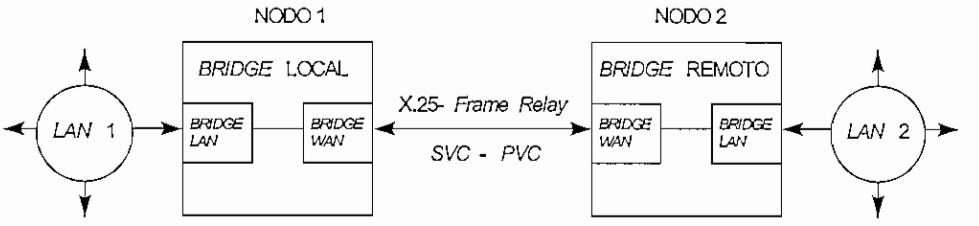


Figura 2.3 Conexión de nodos Bridge, en el módulo *LAN* y *WAN*

Cuando se tienen varias redes *LAN*, éstas se enlazan mediante pares de módulos de *bridge*, empleando los diferentes interfaces y puertos de los nodos, como se muestra en la figura 2.4. En este ejemplo se ilustra la conexión de tres redes *LAN*, en donde el *Bridge* 1 en los nodos 1 y 2 conectan las redes *LAN* 1 y *LAN* 2 , el *Bridge* 2 de los nodos 1 y 3 enlazan las redes *LAN* 1 y *LAN* 3 , y el *Bridge* 3 de los nodos 2 y 3 conectan las redes *LAN* 2 y *LAN* 3. Se forma un circuito virtual independiente por cada enlace físico entre puentes.

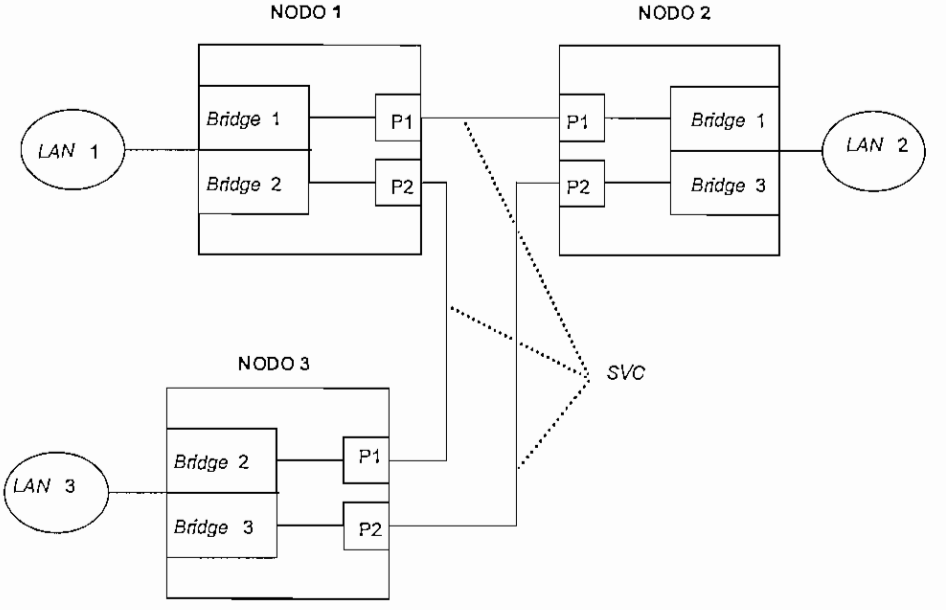


Figura 2.4 Conexión de 3 redes locales a través de *bridges* empleando circuitos virtuales independientes por enlace

Otra forma de conexión se muestra en la figura 2.5, en donde cada uno de los puertos físicos de *WAN* de los nodos tienen dos circuitos virtuales *SVC* para los enlaces. El tráfico entre las redes *LAN* 1 y *LAN* 3, se realiza por el circuito virtual generado a través del *bridge* del Nodo 2. En el

Nodo 2 se produce un puente entre los puertos P1 y P2, con el fin de enlazar los *Bridge* 2 de los Nodos 1 y 3, a través de un circuito virtual, sin pasar hacia la red LAN 2.

La transferencia de datos entre las redes *LAN* 1 y *LAN* 2 se realiza por el circuito virtual generado por el enlace entre los *Bridge* 1 de los Nodos 1 y 2 a través de los puertos P1.

Las redes *LAN* 2 y *LAN* 3 se unen a través de los *Bridge* 3 de los Nodos 2 y 3, conectando los puertos P2 y P1 respectivamente.

Con este tipo de conexión se ahorra un puerto en los Nodos 1 y 3 .

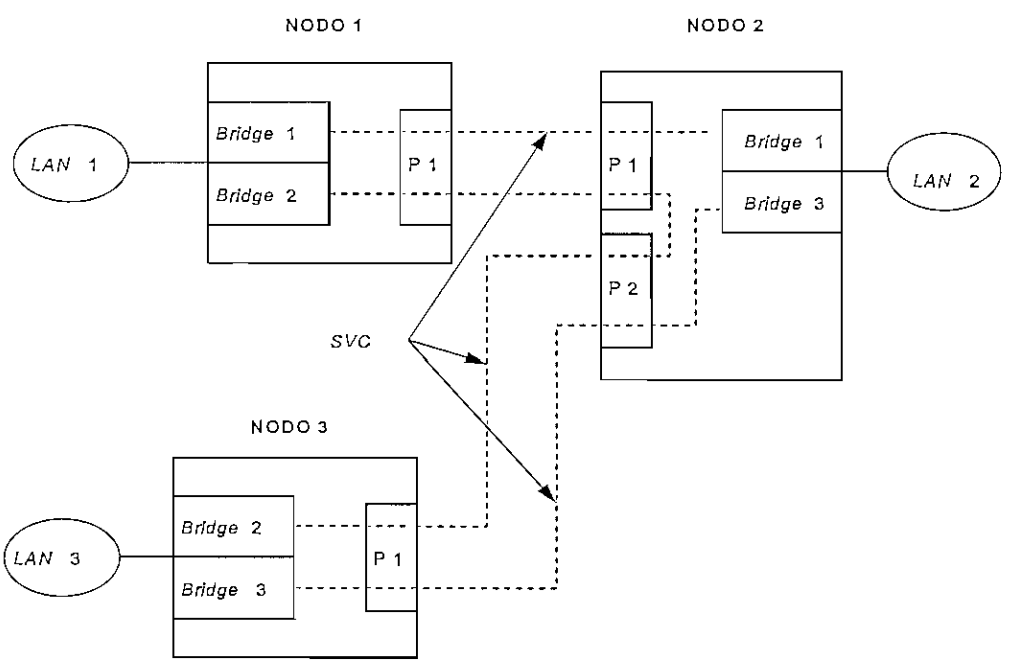


Figura 2.5 Conexión de 3 redes locales a través de *bridges* empleando circuitos virtuales dobles por cada enlace [3]

2.1.1 ESTRUCTURA DE UN PUENTE

Los puentes están formados por dos módulos como se muestra en la figura 2.6 :

- Módulo del puerto *LAN*
- Módulo del adaptador de *WAN*

[3] *6500 Series Bridging, Motorola*

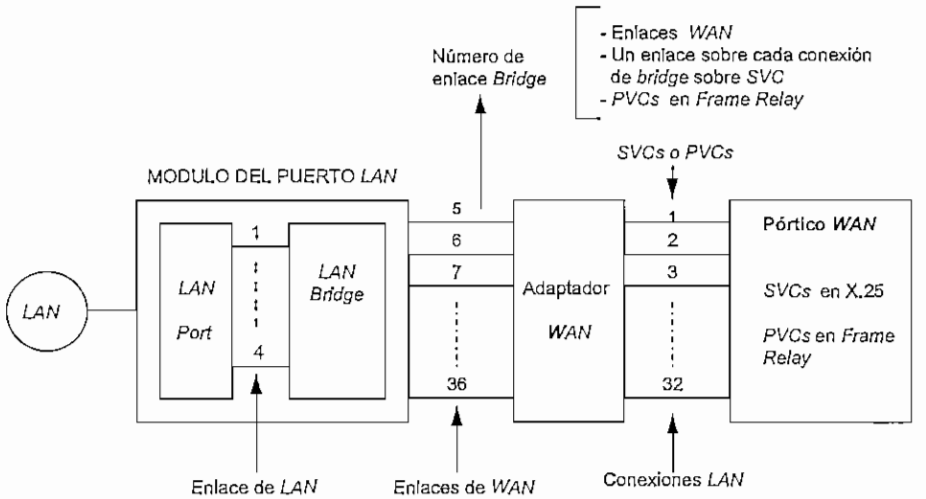


Figura 2.6 Estructura lógica interna de un puente [4]

En los dos módulos se generan enlaces, identificados como enlaces *bridge* de *LAN* y enlaces *bridge* de *WAN*. El enlace de *LAN* permite pasar el tráfico de datos desde el puerto *LAN* hasta el submódulo *LAN Bridge*, y los enlaces de *WAN* pasan los datos desde el submódulo *LAN Bridge* hasta el Adaptador de *WAN*.

El Adaptador de *WAN* local, establece y mantiene conexiones lógicas con el módulo Adaptador de *WAN* remoto a través de circuitos virtuales a los cuales se les denomina Conexiones *LAN*.
El nodo *bridge* considera a la *LAN* y a la *WAN* como redes conectadas por enlaces. Los enlaces pueden ser establecidos con circuitos virtuales conmutables en X.25 o circuitos virtuales permanentes en *Frame Relay*.

Los datos son transmitidos entre los adaptadores de *WAN*, dependiendo del tamaño, uno por uno o en ráfaga encapsulados en X.25.

En el ejemplo de la figura 2.7, el Nodo 100 tiene 3 Conexiones de *LAN* en el mismo puerto de *WAN* numeradas de 1 a 3, las cuales sirven para enlazarse con los puentes remotos 200, 300 y 400. Cada Conexión de *LAN* se relaciona con un enlace de *Bridge* los cuales están identificados del número 5 al 7.

[4] *6500 Series Bridging, Motorola*

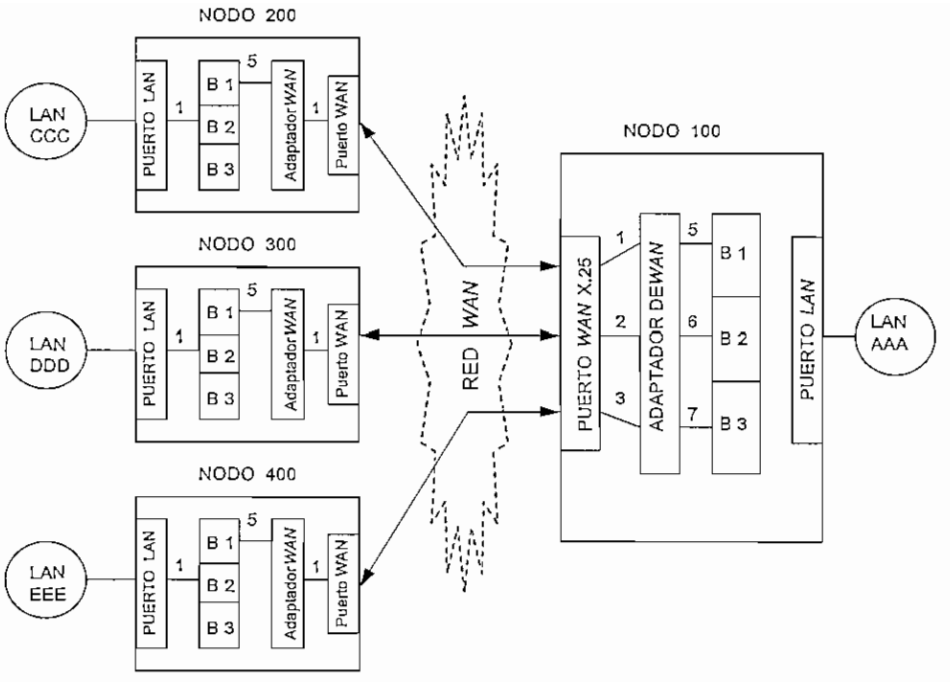


Figura 2.7 Descripción de los módulos de *bridge* en el enlace entre nodos remotos en una red *WAN* [5]

El cuadro 2.1 muestra la tabla de Conexiones *LAN* y Enlaces *bridge* formados en el Nodo 100 al comunicarse con los Nodos 200, 300 y 400 de la figura 2.7.

Número de Conexión de *LAN* local	Número de Enlace *Bridge*	Nodos remotos llamados	Identificación de Conexiones *LAN* y Enlaces *Bridge* de los Nodos remotos
1	5	Nodo 200	1 - enlace *bridge* 5
2	6	Nodo 300	1 - enlace *bridge* 5
3	7	Nodo 400	1 - enlace *bridge* 5

Cuadro 2.1 Tabla de Conexiones *LAN* y Enlaces de *Bridge* del Nodo 100

Para abrir un circuito X.25, el puente local hace una llamada a una dirección de un puente destino, en la que se incluye la subdirección del Adaptador de *WAN* del puente destino que para el caso de los puentes *Codex* tiene la subdirección 94. El formato de la dirección llamada se muestra en la figura 2.8.

Dirección del nodo destino	Subdirección del Adaptador *WAN*

Figura 2.8 Formato de llamada de un *bridge* local a un remoto

[5] *6500 Series Bridging, Motorola*

Para el caso de la red de la figura 2.7, el Nodo 100 hace las llamadas a los otros nodos mediante las direcciones indicadas en el cuadro 2.2, generando un circuito virtual por cada llamada hasta los nodos destinos.

Nodo llamado	Parámetros de llamada
Nodo 200	20094
Nodo 300	30094
Nodo 400	40094

Cuadro 2.2 Parámetros de llamada a los nodos destinos desde el Nodo 100

2.1.2 PUENTE TRANSPARENTE

Se llaman **Puentes Transparentes** aquellos cuya presencia y operación son transparentes a los *hosts* de la red. Este puente tiene la capacidad de decidir donde enviar los datos, para lo cual analiza las direcciones de la red y host destinos de las tramas que arriban al puente. Compara con las direcciones de las redes almacenadas en su base de datos, y envían las tramas hacia el puerto por donde puede alcanzar la red y *host* destino.

La base de datos con las direcciones en un puente transparente, se actualizan cada vez que existe un cambio en la red, para lo que realiza una búsqueda de redes, hosts y puentes existentes. De este modo se mantiene una base de datos consistente, con las direcciones y conexiones *bridges* activas, y elimina de la lista a las inactivas.

2.1.3 FILTROS *BRIDGE*

En un *bridge* se puede filtrar los datos de la fuente y/o del destino, tanto de entrada como de salida mediante herramientas que filtran las diferentes direcciones y protocolos que viajan en la red. Por ejemplo, si llega un paquete con una dirección fuente dada, y coincide con la lista de direcciones de ingreso filtradas, este paquete se descartará.

Se puede filtrar paquetes que salen del *bridge* a un destino, con lo cual se evita el tráfico innecesario hacia ese destino a través de la *WAN*.

Básicamente las funciones que tienen los filtros de *Bridge* son:

- Reducir el tráfico innecesario que afecta a la *performance* de la red *LAN.*
- Restringir el acceso a ciertos segmentos de *LAN* por razones de seguridad.
- Reducir el tráfico en la *WAN*, en donde el ancho de banda es limitado, disminuyendo la congestión y minimizando los retardos a través de la *WAN.*

En el ejemplo de la figura 2.9, el puente filtra los protocolos *IPX, SPX, NetBEUI*, y permite el paso de las tramas con datos ***IP***, hasta la red destino.

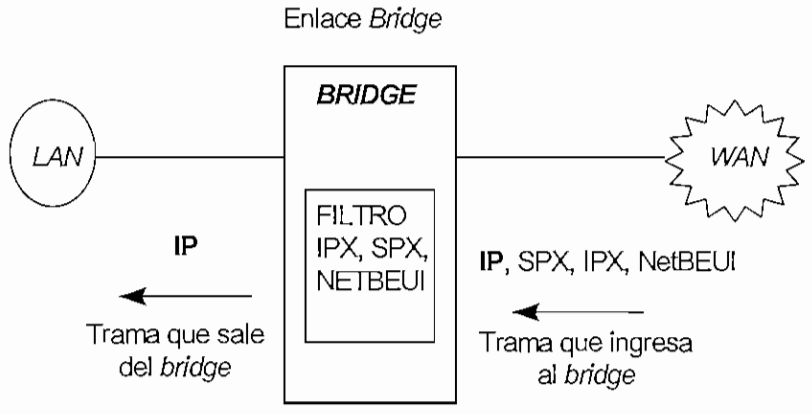


Figura 2.9 Filtración de tramas en un *bridge*

2.1.4 *SPANNING TREE PROTOCOL ENTITY (STPE)*

Es un protocolo que reduce los múltiples caminos entre redes *LAN*, a un sólo camino activo simple, con el fin de evitar lazos o rutas permanentes. El tráfico para las demás vías se bloquea.

En el ejemplo de la figura 2.10, se considera a los enlaces *bridge*, como enlaces conectados a través de puertos diferentes, en donde, para ir de la red *LAN* 1 a la *LAN* 4, se puede utilizar 3 caminos paralelos que son (5-7), (6-8), (6-9-10), e incluso se puede producir un lazo infinito.

El protocolo *STPE* identifica el camino más óptimo, que en este caso es (5-7) pasando por el *bridge* 2 , y bloquea el resto de caminos.

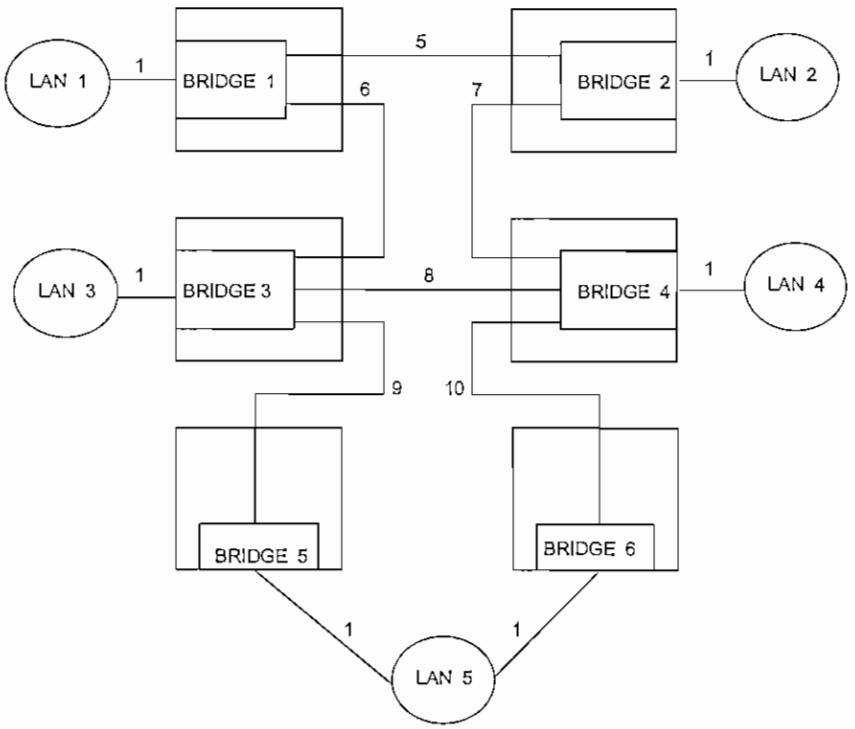


Figura 2.10 Conexión de nodos *bridge* con enlaces independientes, para que *STPE* identifique el camino más óptimo entre nodos [6]

Para determinar el camino óptimo hasta un destino a través de *bridges*, se hace una exploración de rutas. En el *Bridge* fuente, la ruta se especifica en la trama que es enviada por éste. El número de *bridge* es usado para especificar la ruta.

Por ejemplo en la figura 2.10, los *Bridges* B1 y B2 están unidos por un sólo enlace identificado como 5. Cuando hay más de dos bridges en paralelo, pueden generarse más de un enlace.

Para configurar el *Spanning Tree*, los *bridges* intercambian con sus respectivos vecinos, mensajes de saludos y reconocimientos a través de los enlaces.

Hay tres tipos de enlaces:

- Enlace *bridge* raíz que es el camino más óptimo hasta el *bridge* raíz.
- Enlaces *bridge* designados, que son los demás enlaces en el *Spanning Tree*.
- Enlaces *bridge Standby*, que son los enlaces que no están en el *Spanning Tree*.

[6] *6500 Series Bridging, Motorola*

Los enlaces raíz y designado, están en estado de disponibilidad, mientras que el *standby* es bloqueado para que no se produzcan lazos y caminos largos.

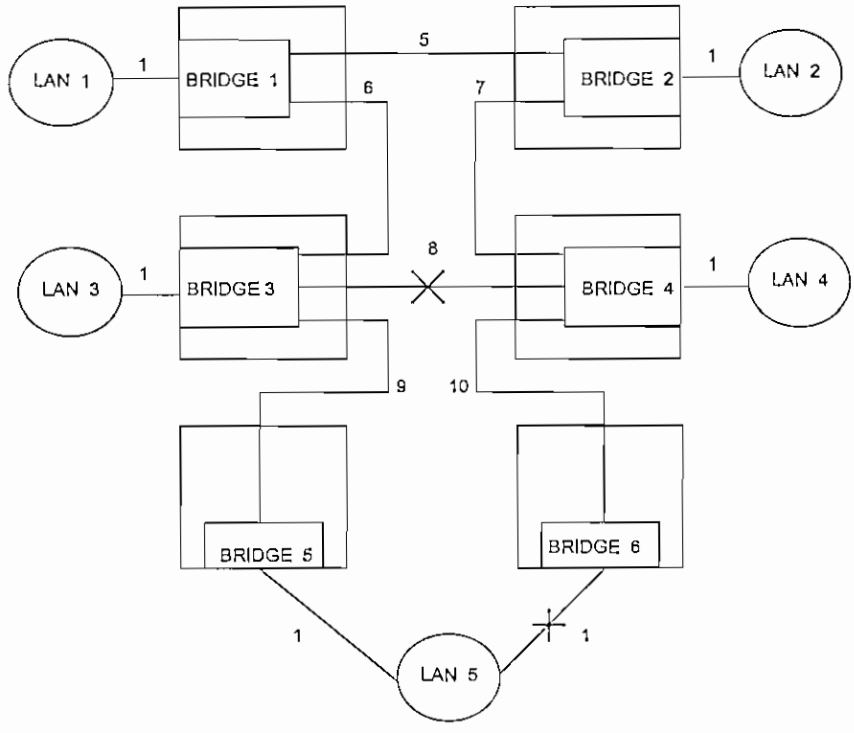


Figura 2.11 Bloqueo de enlaces no óptimos entre nodos *bridge* [7]

En el ejemplo de la figura 2.11, se considera como *bridge* raíz al *Bridge* 1.

El enlace raíz que determina el camino más óptimo desde los *Bridges* 2, 3, 4, 5 y 6, para alcanzar el *Bridge* raíz **B1**, son los enlaces 5, 6, 7, 9, 10 respectivamente, los cuales son configurados independientemente en cada uno de los nodos, como se indica en el cuadro 2.3.

Los restantes enlaces (1, 5, 6), (1, 7), (1, 9), (1,10), (1), son configurados en los *Bridges* 1, 2, 3, 4, 5 respectivamente como enlaces designados, los cuales completan el *Spanning Tree* en cada uno de los nodos. El enlace 1 se utiliza para comunicación con la red *LAN* conectada directamente a cada nodo *Bridge*.

En el *Bridge* 3 y 4 el enlace 8 se configura como enlace bloqueado, porque no se lo utiliza para alcanzar los otros nodos, con el fin de evitar lazos.

[7] *6500 Series Bridging, Motorola*

Para enlazarse al resto de nodos, el *Bridge 3* emplea los enlaces 6 y 9. Por el enlace 6 puede comunicarse con los *Bridges* 1, 2, 4 , 6. En tanto que por el enlace 9 se comunica con el *Bridge* 5. El *Bridge* 4 emplea los enlaces 7 y 10 para comunicarse con los otros nodos.

El *Bridge* 6 bloquea el enlace 1 por ser considerado como redundante, y se comunica con el resto de *Bridges* a través del enlace 10.

De esta forma se elimina lazos y caminos redundantes en la red de la figura 2.11, cuya representación final se muestra en el cuadro 2.3 .

	Bridge 1	***Bridge 2***	***Bridge 3***	***Bridge 4***	***Bridge 5***	***Bridge 6***
Bridge Raíz	**B1**					
Enlace Raíz		5	6	7	9	10
Enlace Designado	1,5,6	1,7	1,9	1,10	1	
Enlace Standby Bloqueo de datos			8	8		1

Cuadro 2.3 Tipos de enlace formados en los nodos *bridge* [6]

Para determinar los enlaces más óptimos, los puentes intercambian entre sí mensajes de saludo denominados ***HELLO.***

El mensaje *Hello* que un puente envía hacia los demás, contiene el número de identificación del puente, conformado por la dirección *MAC* del pórtico *LAN* y la prioridad del puente:

Identificación del puente *ID* = Prioridad del puente + dirección *MAC*

El puente con el número de identificación más bajo se considera como Puente Raíz (Prioridad del puente = 1), desde el cual salen los enlaces designados, hacia los demás puentes y redes. El formato del mensaje *Hello* se describe en el capítulo 3.

Se puede tener varios enlaces a través de un mismo puerto, cada uno con diferente prioridad, tal como se indica en la figura 2.12, escogiéndose para la comunicación, el enlace que tiene la

[6] *6500 Series Bridging, Motorola*

prioridad más baja, tanto hacia el lado de la red *LAN*, como al lado de la red *WAN*. Esto significa que un enlace con prioridad **1** tiene mayor valor que un enlace con prioridad **2**.

Para escoger el enlace raíz, primero se toma al de menor costo; si es que existen dos con el mismo costo entonces se escoge el de prioridad menor.

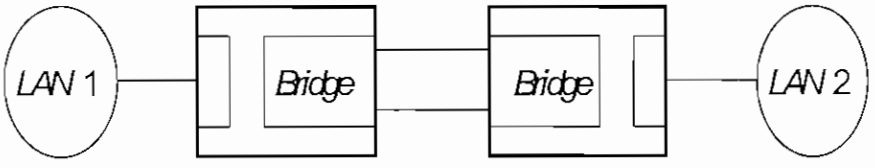


Figura 2.12 Conexión de *bridges* con doble enlace

2.2 FUNDAMENTOS DE RUTEADORES [9]

Los **Ruteadores** son dispositivos que transfieren los paquetes entre redes diferentes, a través de un camino óptimo, empleando las direcciones del equipo origen y destino contenidas dentro del paquete a transferir. La ruta hacia otras redes se escoge de una **tabla de rutas**, las cuales están almacenadas en una base de datos dentro del ruteador.

Un ruteador opera en las tres primeras capas del modelo *OSI*, como se muestra en la figura 2.13, en donde la parte de enrutamiento se realiza en la capa de red, empleando la tabla de rutas.

La forma de operación del ruteador es la siguiente :

1.- Accesa a la capa red, en donde toma las direcciones fuente y destino del paquete.

2.- Forma una lista de direcciones y caminos entre y hacia los nodos de la red.

3.- En la capa red, toma la dirección del *header* y compara con las direcciones de la tabla de rutas, para determinar el mejor camino.

[9] *6500 Series Routing , Motorola*

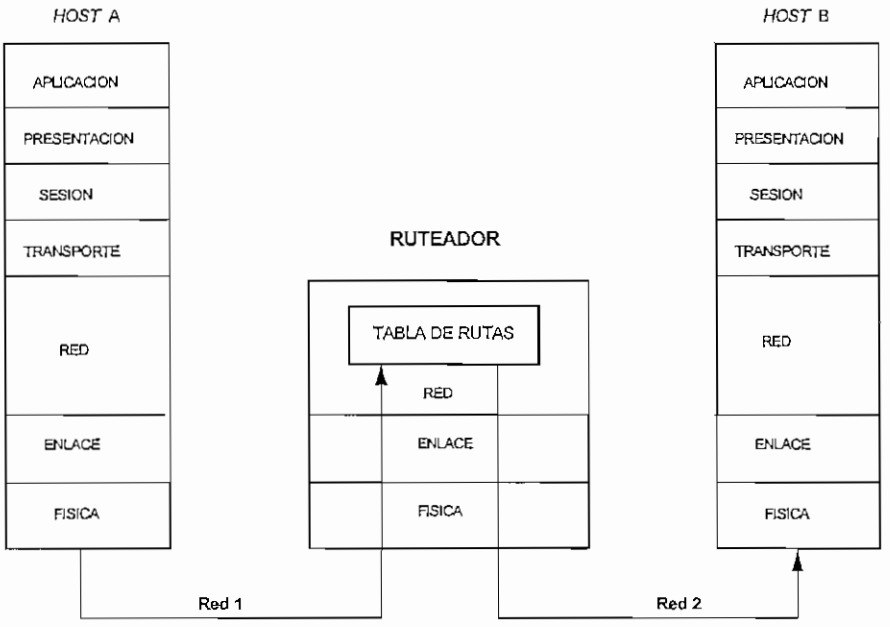


Figura 2.13 Enlace de redes a través de un ruteador

2.2.1 ESTRUCTURA DE UN RUTEADOR

La estructura de un ruteador se muestra en la figura 2.14, la cual consta de los siguientes módulos:

- Módulo de red local *LAN*
- Módulo de Enrutamiento
- Módulo Adaptador de red extendida *WAN*

El adaptador de *WAN* conecta el puerto de *LAN* a los puertos de *WAN*, enlazando cada interfaz de Enrutamiento *WAN* con circuitos virtuales conmutables de los puertos X.25 o con circuitos virtuales permanentes en los puertos *Frame Relay*. Estos circuitos virtuales se denominan **Conexiones *LAN*.**

. El interfaz de enrutamiento de red local se identifica como interfaz **1** .

. Hay 32 interfaces de enrutamiento *WAN*, numeradas del **5-36** , por lo que se tiene hasta **32** conexiones lógicas.

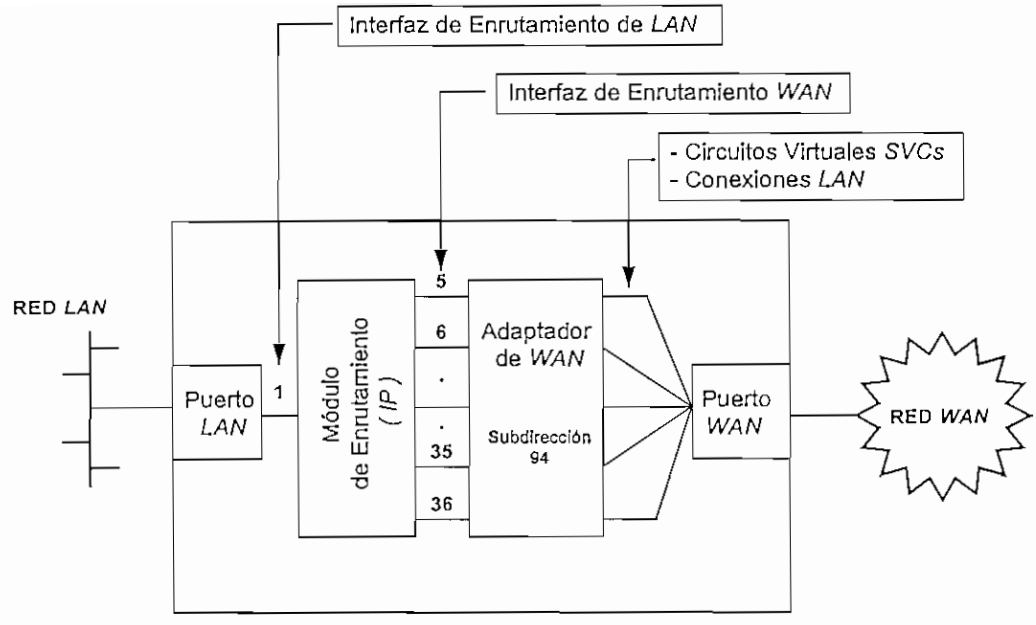


Figura 2.14 Estructura de un Ruteador

En la figura 2.15 se muestra la estructura de un Puente - Ruteador, en el cual el módulo de *WAN* conecta los módulos *Bridge* y *Router* de *LAN* con los puertos de *WAN*. Este dispositivo funciona como puente para transferir protocolos no ruteables y como ruteador para transferir los protocolos ruteables.

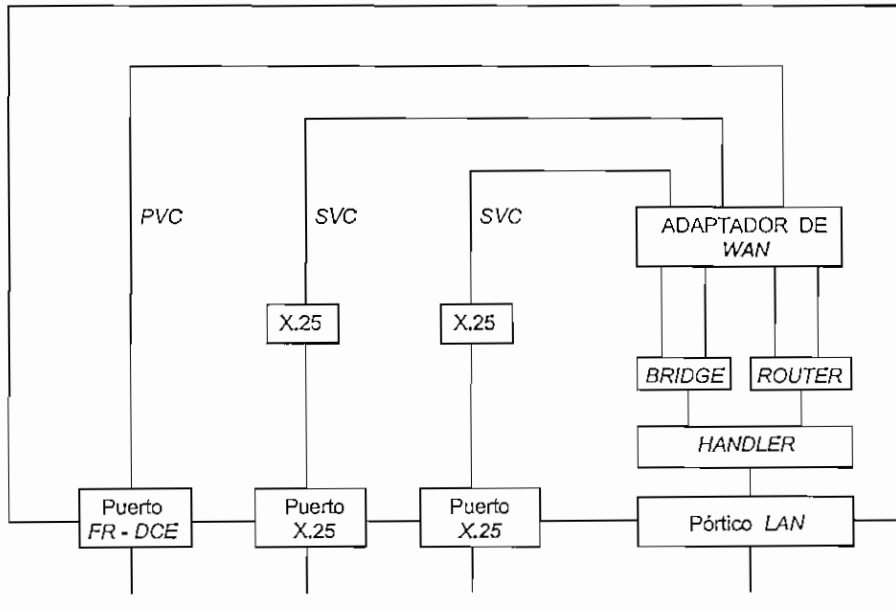


Figura 2.15 Direccionamiento y conexión entre los diferentes puertos del ruteador [10]

[10] *6500 Series Routing , Motorola*

En los ruteadores se debe configurar la tabla de interfaces de enrutamiento de *LAN* y de *WAN* para que los paquetes puedan ser enrutados hacia sus destinos.

El adaptador de *WAN* encapsula los datos usando los siguientes métodos:

- Encapsulamiento Multiprotocolo *RFC* 1294
- Encapsulamiento *IP RFC* 877

El **encapsulamiento Multiprotocolo *RFC* 1294**, especifica el transporte de datos sobre *Frame Relay*, el cual soporta los protocolos *IP* y *RIP*, manejando además *SNA*. El formato de la trama en *Frame Relay* se muestra en la figura 2.16.

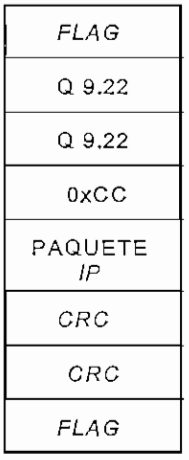


Figura 2.16 Encapsulamiento Multiprotocolo *RFC* 1294 para *Frame Relay*

El **Encapsulamiento *IP RFC* 877**, especifica el transporte de *IP* sobre X.25 usando *NLPID (Network Layer Protocol Identification)*, cuyo valor es 0xCC.

El datagrama *IP* es enviado como parte de los datos de la trama X.25, sin adicionar otros *Headers*, cuyo formato se muestra en la figura 2.17.

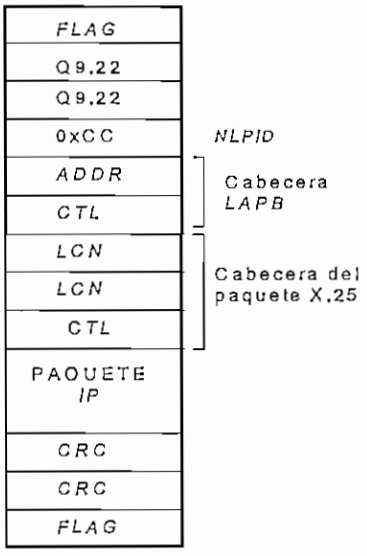


Figura 2.17 Encapsulamiento *IP RFC* 877 sobre X.25

Los circuitos virtuales conmutables *SVCs* pueden ser Permanentes, si están operables hasta que el usuario los desactive, o pueden ser *SVCs* en Demanda, soportando tráfico IP sobre X.25, si se activan cuando hay datos para ser enviados y se desactivan cuando todos los datos han sido enviados.

2.2.1.1 EJEMPLO DE ENRUTAMIENTO *FRAME RELAY*

El ejemplo de la figura 2.18 muestra la operación de un ruteador *IP* en *Frame Relay* .

El módulo de enrutamiento del Nodo D tiene configurado los interfaces 1, 5, 6, 7 con direcciones *IP* diferentes que pertenecen a los segmentos de red *LAN Ethernet* y de red *WAN* dirigidos a los Nodos A, B, C.

El adaptador de *WAN*, genera conexiones lógicas *LCONs* hacia cada uno de los ruteadores *IP* remotos a través del Interfaz *Frame Relay FRI* del módulo de red *WAN* del Nodo D.

El Interfaz *Frame Relay FRI* genera una estación *Sn* por cada conexión lógica hacia los nodos remotos a través de los puertos de red *WAN*.

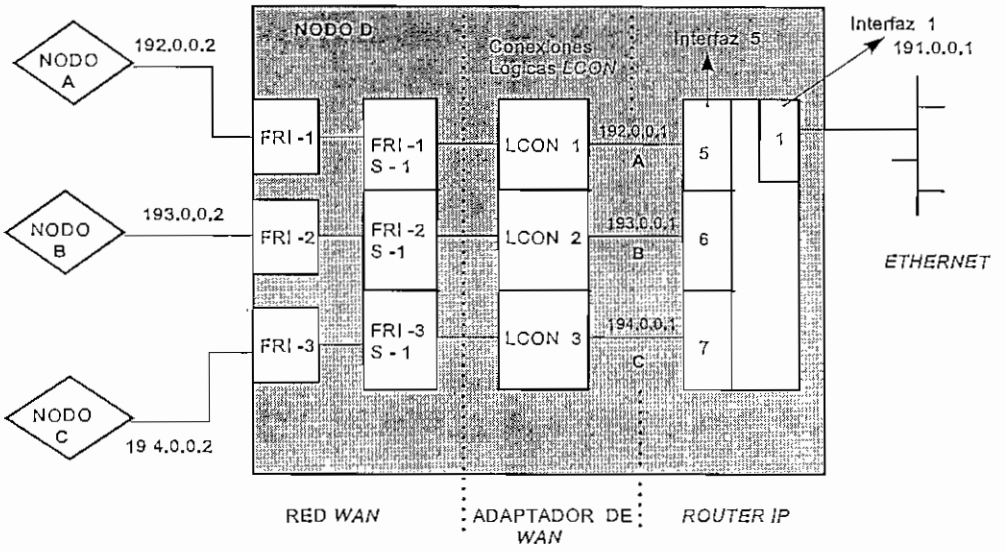


Figura 2.18 Estructura interna lógica de un ruteador en *Frame Relay* [11]

Lo expuesto anteriormente se resume en el cuadro 2.4.

Módulo de *Router IP*		Adaptador de *WAN*	Módulo de Red *WAN*		Nodo
Interfaz	Dirección IP	Conexión Lógica *LCON*	Interfaz *Frame Relay*	Estación *S*	Destino
1 Ethernet	191.0.0.1	red local 191			
5	192.0.0.1	1 - red 192	FRI - 1 puerto 1	S - 1	Nodo A 192.0.0.2
6	193.0.0.1	2 - red 193	FRI - 2 puerto 2	S - 1	Nodo B 193.0.0.2
7	194.0.0.1	3 - red 194	FRI - 3 puerto 3	S - 1	Nodo C 194.0.0.2

Cuadro 2.4 Configuración de los interfaces de Router y estaciones Frame Relay del Nodo D

2.2.1.2 EJEMPLO DE ENRUTAMIENTO *IP* SOBRE X.25

La conexión entre dos ruteadores *IP* en X.25 se muestra en la figura 2.19.

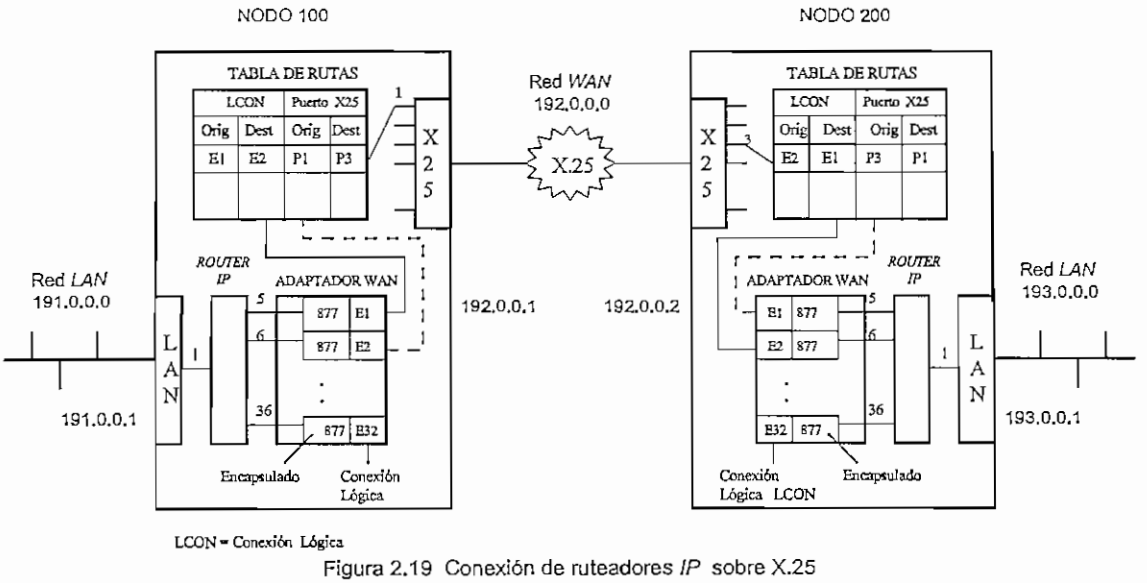


Figura 2.19 Conexión de ruteadores *IP* sobre X.25

[11] *6500 Series Routing , Motorola*

En los registros de las tablas de rutas X.25 se configura: la dirección X.25 de los nodos destinos, el puerto *WAN* del nodo local a través del cual nos conectamos al ruteador destino y la prioridad de cada conexión. Además se direcciona la información desde el adaptador de *WAN* local hacia el puerto *Ethernet* mediante una conexión lógica *LAN* a través del interfaz 1.

En el ejemplo de la figura 2.19, el NODO 100 se conecta al puerto 3 (X25-3) del NODO 200 remoto a través del puerto local 1 (X.25-1). Para llegar hasta la red *Ethernet*, se direcciona el adaptador de *WAN* del NODO 100 local que tiene la dirección 10094 hacia una Conexión *LAN*, como se muestra en el cuadro 2.6.

TABLA DE RUTAS X.25 DEL NODO 100			
Registro	**Dirección X.25**	**Destino local**	**Prioridad**
1	10094	Conexión LAN al puerto Ethernet	1
2	200	X25-1	1
.			
.			

Cuadro 2.6 Tabla de rutas X.25 de nodo 100 en el ejemplo de la figura 2.19

Los **Interfaces de Enrutamiento *IP*** de *LAN* y *WAN* son configurados con direcciones *IP* individuales y la configuración se guarda en un registro ***En*** por cada interfaz.

Los interfaces de *WAN* son direccionados hacia los puertos X.25 mediante conexiones lógicas *LCONs* que en este caso corresponde a circuitos virtuales conmutables *SVCs*.

La configuración de los interfaces de enrutamiento *IP* para el NODO 100, del ejemplo de la figura 2.19, se muestra en el cuadro 2.5.

El interfaz 1 tiene la dirección IP 191.0.0.1 que pertenece a la red local 191.0.0.0 *Ethernet*. El interfaz 5 se configura con la dirección 192.0.0.1 que pertenece a la red *WAN* 192.0.0.0 , y se conecta al interfaz 5 del NODO 200 remoto que tiene la dirección 192.0.0.2.

Módulo de *Router IP*			**Adaptador de *WAN***
Registro	**Interfaz**	**Dirección IP**	**Conexión Lógica *LCON***
1	1	191.0.0.1 interfaz de *LAN*	
2	5	192.0.0.1 interfaz de *WAN*	1 - Dirigida al puerto X25-1
.	.	.	.

Cuadro 2.5 Configuración de los interfaces de Enrutamiento del Nodo 100 del ejemplo 2.19

En la figura 2.20 siguiente se describe un ejemplo de conexión de *routers*:

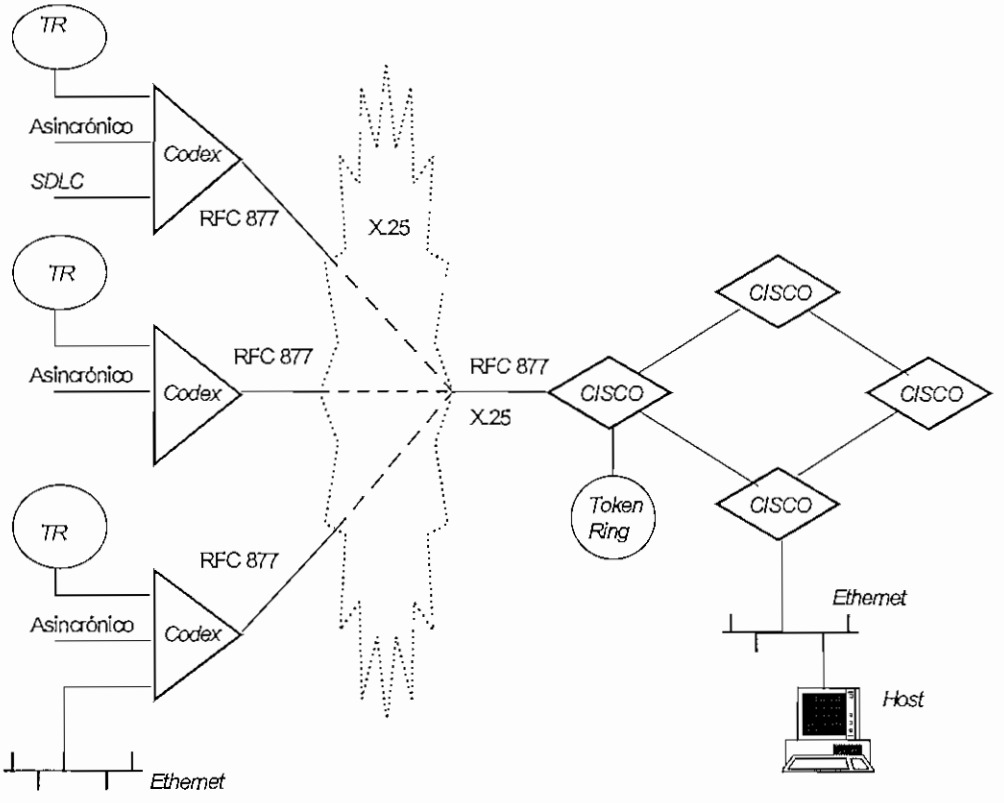


Figura 2.20 Conexión de Ruteadores *CISCO* y *CODEX* en red *WAN* X.25 [12]

2.2.2 ALGORITMOS DE ENRUTAMIENTO

Los algoritmos de enrutamiento son diseñados con las siguientes características:

Optimos.- Es la capacidad del algoritmo de enrutamiento para seleccionar la mejor ruta, que está determinada por los *metrics* como el número de saltos, retardos, ancho de banda del canal.

Simplicidad.- Deben ofrecer grandes utilidades, con el mínimo *software* y con la menor adición de cabeceras en los paquetes.

Eficiencia.- Facilita los cálculos complejos, usando grandes cantidades de datos de las tablas de rutas.

Robustez.- Debe funcionar correctamente cuando hay fallas de *hardware*, sobrecarga etc.

[12] *Series Routing , Motorola*

Flexibilidad.- Se adapta a los cambios producidos en la red, como la variación en el ancho de banda, encolamiento en el *router*, retardos y otras variables.

Rápida Convergencia.- Es el acuerdo al que llegan los *routers* para designar cuál es la mejor ruta, en donde los algoritmos se encargan de tomar esta decisión.

Cuando una red cae, y luego se pone disponible, los protocolos de enrutamiento envían mensajes de actualización de rutas. Estos mensajes ingresan en las redes, estimulando a los *routers* para que recalculen las nuevas rutas óptimas.

Si la convergencia se vuelve lenta, se puede producir un lazo.

Escalabilidad.- Es la facilidad de operar tanto en redes pequeñas como en ambientes grandes

2.2.2.1 TIPOS DE ALGORITMOS DE ENRUTAMIENTO [13]

Los algoritmos de enrutamiento se clasifican en :

- **Algoritmos Estáticos** .- Son algoritmos rígidos, en donde las tablas de rutas son establecidas por un administrador de red. No pueden reaccionar ante cambios producidos en la red y son empleados en redes relativamente simples cuyo tráfico de datos es bajo.

- **Algoritmos Dinámicos** .- Son algoritmos flexibles que reaccionan ante cambios producidos en la red. Recalculan y actualizan las tablas de rutas luego de recibir un mensaje de algún cambio producido en la red. Las tablas cambiadas se liberan a la red para que el resto de ruteadores actualicen sus tablas.

- **Algoritmos de Camino Simple** .- Permiten un solo camino hasta el destino a través de una línea simple.

- **Algoritmos de Camino Múltiple** .- Soportan múltiples caminos hasta el destino a través varias líneas con el fin de mejorar la confiabilidad del tráfico.

- **Algoritmos Planos** .- Son algoritmos que operan en un espacio plano, donde todos los ruteadores operan en el mismo nivel y con características similares.

---

[13] *Internetworking Technology Overview, Cisco* Capítulo 2

- **Algoritmos Jerárquicos** .- Son algoritmos en los cuales los datos deben atravesar por ruteadores agrupados por niveles jerárquicos hasta alcanzar su destino. Los ruteadores se ubican en grupos lógicos llamados dominios, sistemas autónomos o áreas, donde el grupo de ruteadores con el más alto nivel de jerarquía forman la columna vertebral de la red.

- **Algoritmos de *Host* Inteligente** .- Son algoritmos en los que los *hosts* tienen la capacidad de escoger el camino más óptimo para transferir los datos hasta un destino determinado, empleando una cantidad significativa de tiempo.

- **Algoritmos de Ruteador Inteligente** .- Asumen que los *hosts* no conocen las rutas por lo que asignan a los ruteadores inteligentes para que calculen las rutas óptimas hasta un destino.

- **Algoritmos Intradominio** .- Son algoritmos que operan dentro de un mismo dominio.

- **Algoritmos Interdominio** .- Trabajan tanto dentro de un dominio como con otros dominios .

- **Algoritmos Estado de Enlace** .- Con estos algoritmos un ruteador prueba el estado de actividad de todos los ruteadores vecinos que comparten un enlace con éste y difunde periódicamente la información del estado del enlace hacia los otros ruteadores.

- **Algoritmos Vector Distancia** .- Los ruteadores emplean estos algoritmos para difundir una lista de todas las redes que pueden alcanzar y la distancia hasta cada red.

Los algoritmos de enrutamiento utilizan parámetros denominados **métricas** para determinar la mejor ruta. Las métricas empleadas son las siguientes :

- Longitud del camino
- Alcanzabilidad
- Retardos
- Ancho de banda
- Carga
- Costo de la comunicación.

2.3 PROTOCOLOS RUTEABLES

2.3.1 PROTOCOLO *TCP / IP* [14]

Las redes *IP* son un grupo de segmentos de red que son interconectadas por ruteadores, como se indica en la figura 2.21.

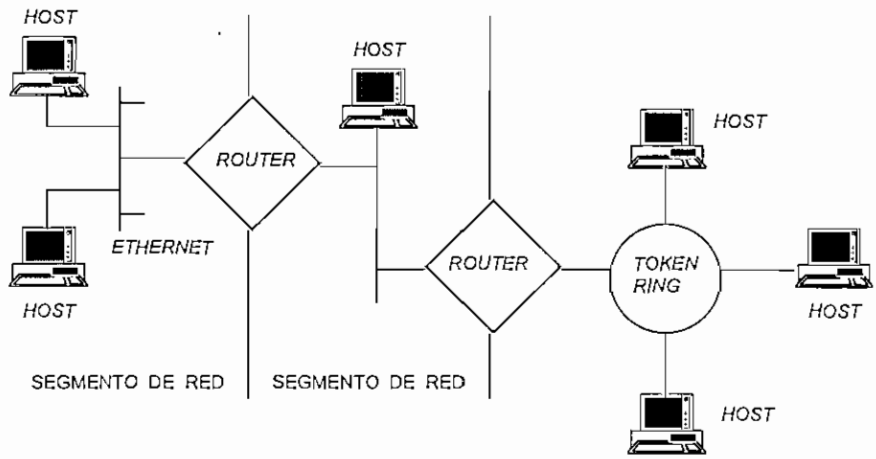


Figura 2.21 Conexión de segmentos de redes *IP*, mediante ruteadores

En los servicios sin conexión, los paquetes entre el destino y la fuente son enrutados independientemente y por tanto pueden tomar caminos diferentes.

En una red ***TCP/IP***, una estación puede conectarse a una o más redes, a través de ruteadores.

IP enruta los paquetes de la siguiente manera:

- Recibe el paquete y lee en el *header* la dirección destino.
- Si el paquete está destinado al ruteador, *IP* lleva el paquete hasta el módulo interno apropiado.
- Si el paquete está destinado a un host en una red conectada directamente al ruteador, *IP* ajusta y relaciona la dirección destino con la dirección física apropiada que se encuentra en la tabla *ARP (Address Resolution Protocol)*.
- Si el paquete está destinado a un host en una red remota, *IP* usa la tabla de rutas para determinar cual interfaz del ruteador se requiere para alcanzar la red destino. La tabla

[14] *Internetworking Technology Overview, Cisco* Capítulo 18

contiene las direcciones de red destino y la dirección *IP* del siguiente ruteador al cual se debe saltar, para encontrar el destino.

- Si la dirección *IP* del paquete no consta en la tabla de rutas, éste es enrutado hasta el *router default*. Los *routers default* son usados para enrutar paquetes cuyas direcciones destinos no están en la tabla de rutas. De este modo un ruteador siempre conoce la ubicación en donde se encuentra un paquete.

Un ruteador puede filtrar direcciones para bloquear y controlar el acceso de paquetes, previniendo así que paquetes con formato o destinos incorrectos estén viajando en la red.

2.3.1.1 *ROUTER O GATEWAY DEFAULT*

Un *router* o *gateway default*, enruta paquetes hacia redes destinos desconocidas, como se muestra a continuación en el ejemplo de la figura 2.22 .

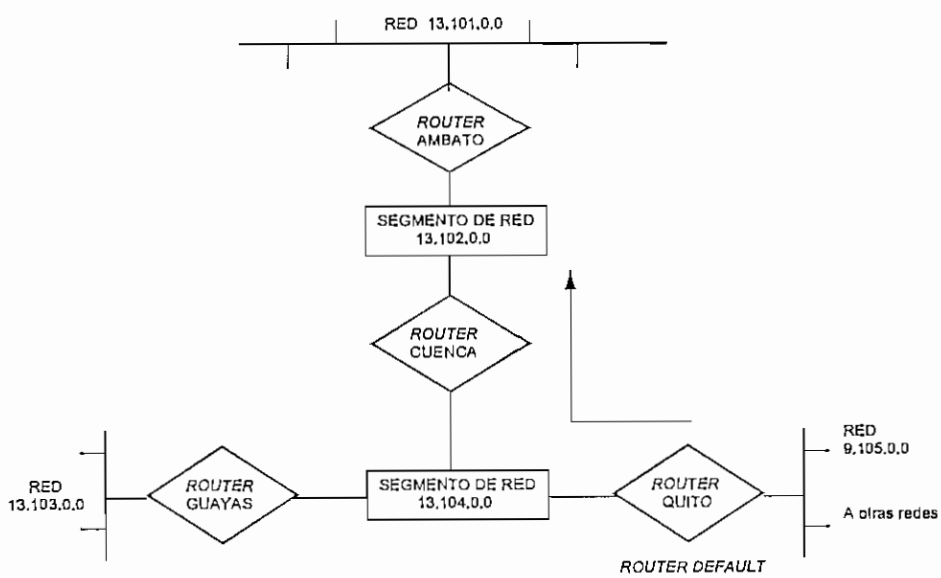


Figura 2.22 Conexión de segmentos de red *IP* independientes a través de ruteadores y *gateways default*

En este caso el *gateway default* es Quito, por cuanto éste conoce a la red 13 y a cualquier otra red desconocida. Los demás *routers* y *hosts* , para accesar a una red diferente de la 13 deben tener como *gateway default* al *router* de Quito.

2.3.2 PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES *(A.R.P.)* [15]

Address Resolution Protocol A.R.P. es un protocolo de bajo nivel, que mapea dinámicamente la dirección *IP* a la dirección física *MAC (Medium Access Control).*

El ejemplo de la figura 2.23 muestra el proceso *ARP* siguiente:

1.- Un paquete *IP*, llega al ruteador con una dirección destino 219.1.82.07

2.- El ruteador determina que el paquete debe ser liberado en el interfaz *Ethernet* local .

Consulta en la tabla de rutas, para determinar la *MAC address* de la estación que tiene la dirección *IP* 219.1.82.07.

Si el cache *ARP* no tiene mapeado la dirección 219.1.82.07, realiza el siguiente proceso:

3.- El *router* elimina el paquete, e inicia el protocolo *ARP* para determinar el *MAC address* de la estación destino.

4.- Un requerimiento *ARP* es lanzado a la red, con un *broadcast* de la dirección del *host* destino.

5.- La estación que detecta su dirección *IP* en el paquete *ARP*, responde con su *MAC address.*

6.- El cache *ARP* del ruteador se actualiza con la información *MAC* enviada por la estación, de modo que no se repita el procedimiento para otros paquetes que arriban.

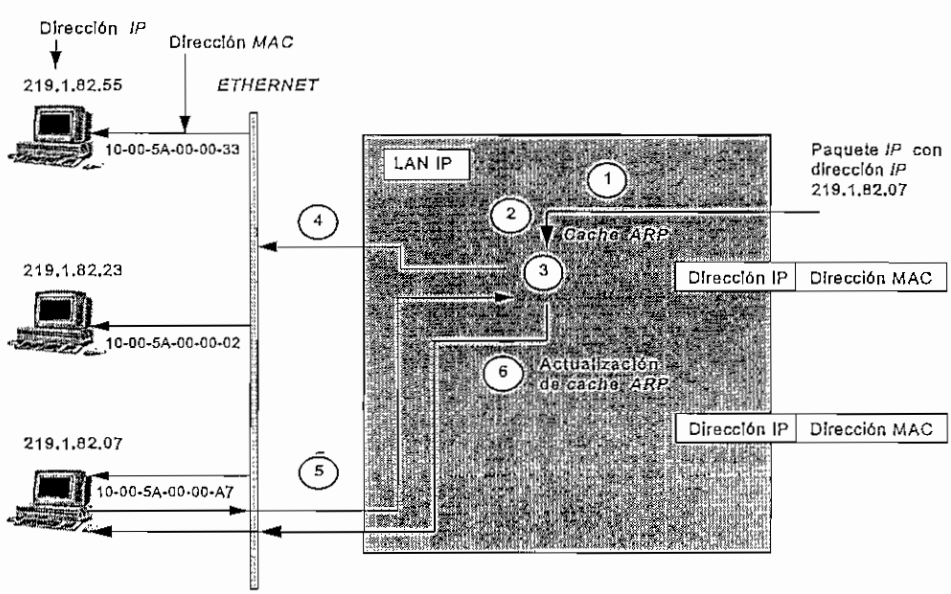


Figura 2.23 Proceso *ARP* en un ruteador *IP*

[15] *6500 Series Routing , Motorola*

2.3.2.1 PAQUETES *BROADCAST*

Es un mensaje destinado para todos los *hosts* en la red . Por lo general estos mensajes son usados para actualizar las tablas de rutas *IP* en otros ruteadores.

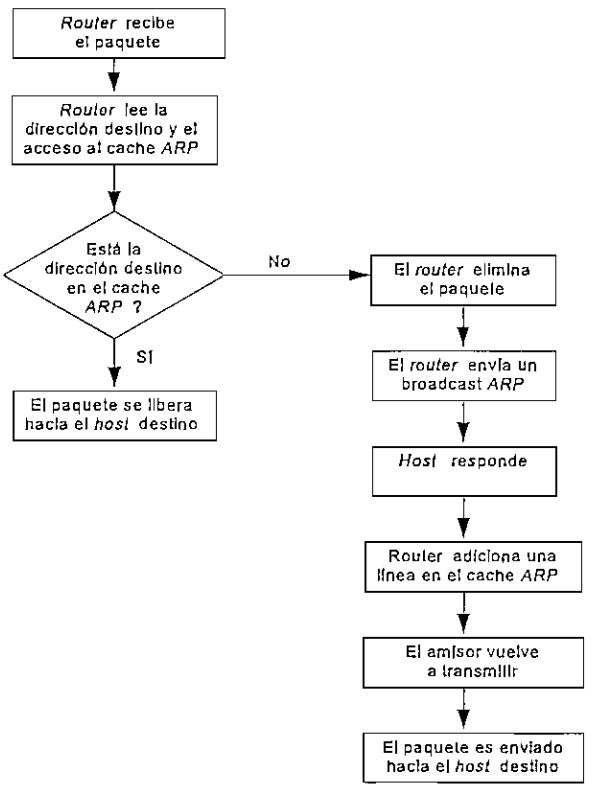


Figura 2.24 Diagrama de flujo del funcionamiento del protocolo *ARP*

2.3.3 *ROUTING INFORMATION PROTOCOL (RIP)* [16]

Es un *Interior Gateway Protocol* (*IGP*) que detecta dinámicamente las redes alcanzables y la información de rutas en sistemas autónomos.

RIP es un protocolo Vector-Distancia que permite intercambiar información de destinos a través de la red, trabajando del siguiente modo:

1.- Cada ruteador envía periódicamente un mensaje de *broadcast* con sus rutas, hacia sus vecinos, en el cual se incluye una lista de redes y el costo (basado en el número de saltos) para llegar a cada una de las redes.

2.- El ruteador usa las tablas de rutas, para decidir cual ruteador cercano (vecino) debe utilizar para enrutar un determinado paquete.

[16] *6500 Series Routing , Motorola*

Este proceso se ilustra en el ejemplo de la figura 2.25 donde se tienen las siguientes redes:

13.101.0.0

13.102.0.0

13.103.0.0

13.104.0.0

El ruteador D se configura como *router default* con un costo de 10 *Hops*.

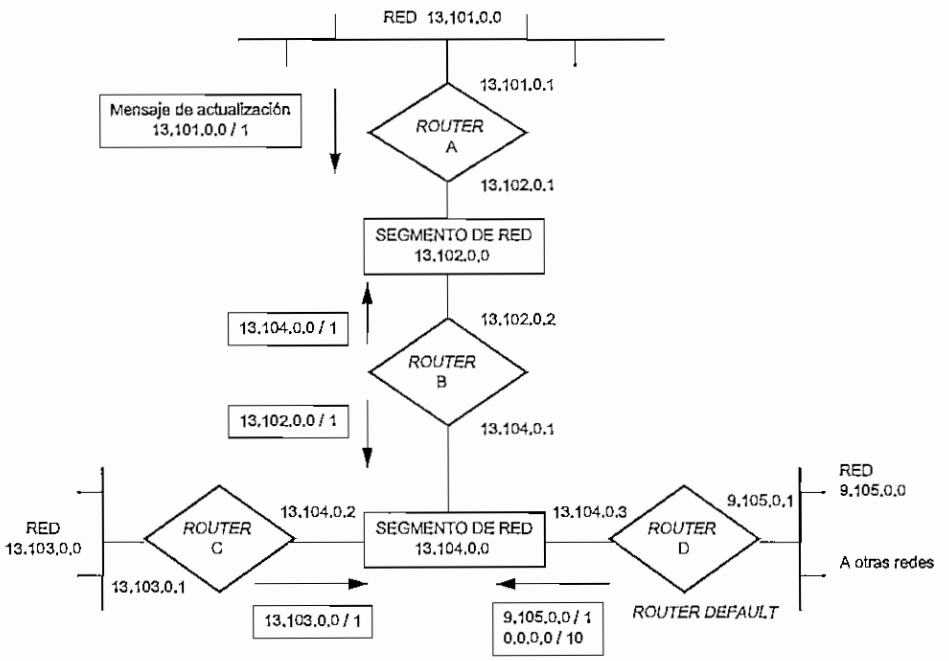


Figura 2.25 Proceso del protocolo *RIP* en los ruteadores de una red *IP*

El cuadro 2.6 muestra la información de las redes adyacentes que cada ruteador envía mediante mensajes de *broadcast* hacia el resto de nodos vecinos para actualizar la tabla de rutas en cada uno de ellos.

Ruteador	Envía *broadcast* a la red	Con la siguiente información
A	13.102.0.0	13.101.0.0 *hop* = 1
	13.10 1.0.0	13.102.0.0 *hop* = 1
B	13.104.0.0	13.102.0.0 *hop* = 1
	13.102.0.0	13.104.0.0 *hop* = 1
C	13.104.0.0	13.103.0.0 *hop* = 1
	13.103.0.0	13.104.0.0 *hop* = 1
D	9.105.0.0	13.104.0.0 *hop* = 1
	13.104.0.0	9.105.0.0 *hop* = 1 0.0.0.0 *hop* = 10

Cuadro 2.6 Mensajes de *broadcast* de los ruteadores de la red de la figura 2.25

Por ejemplo los mensajes de actualización para la ruta hacia la red **13.101.0.0** de la figura 2.25 tiene el siguiente proceso:

1.- El Ruteador A envía un mensaje de *broadcast* a la red adyacente 13.102.0.0 indicando que para alcanzar la otra red adyacente **13.101.0.0** se requiere de un salto. Hacia la otra red adyacente 13.101.0.0 envía otro mensaje de *broadcast* indicando que para alcanzar la red adyacente 13.102.0.0 se requiere un salto.

El ruteador A está uniendo las redes 13.101.0.0 y 13.102.0.0.

2.- El Ruteador B lee el mensaje enviado por A y genera una ruta hacia la red **13.101.0.0**, indicando que se necesita dar un salto para llegar a la red destino, atravesando primero el ruteador A que tiene la dirección 13.102.0.1.

3.- Luego el ruteador B envía un mensaje *broadcast* hacia la red 13.104.0.0 indicando que para alcanzar la misma red **13.101.0.0** se requiere dar dos saltos, es decir, adiciona un salto más al mensaje anterior.

4.- Los ruteadores C y D leen el mensaje *broadcast* enviado por el ruteador B y generan una ruta hacia la red 13.101.0.0 indicando que se requiere dar dos saltos para llegar a la red destino, atravesando primero por el ruteador B que tiene la dirección 13.104.0.1 y luego por el ruteador A.

Los ruteadores analizan los mensajes de *broadcast* que reciben y van generando una tabla de rutas en la que se incluye la dirección *IP* de la red destino, el número de saltos requeridos para alcanzar la red y la dirección del siguiente ruteador por el cual se puede llegar a la red destino.

Después del proceso de *broadcast*, en cada ruteador se genera una base de datos con las tablas de rutas como se muestra en el cuadro 2.7 para los ruteadores A y B de la figura 2.25.

La tabla del ruteador A indica que para alcanzar la red no adyacente 13.103.0.0 se requiere dos saltos, ésto es, debe atravesar dos ruteadores, pasando primero por el ruteador B que tiene la dirección 13.102.0.2 y luego por el ruteador C; para alcanzar la red 13.104.0.0 se requiere de un salto y debemos pasar por el ruteador B que tiene la dirección 13.102.0.2.

Para alcanzar las redes 13.101.0.0 y 13.102.0.0 adyacentes al ruteador A no se requieren saltos.

Ruteador	Red	Saltos	Siguiente salto
A	13.101.0.0	0	
	13.102.0.0	0	
	13.103.0.0	2	13.102.0.2 ruteador B
	13.104.0.0	1	13.102.0.2 ruteador B
	9.105.0.0	2	13.102.0.2 ruteador B
	0.0.0.0	11	13.102.0.2 ruteador B
B	13.101.0.0	1	13.102.0.1 ruteador A
	13.102.0.0	0	
	13.103.0.0	1	13.104.0.2 ruteador C
	13.104.0.0	0	
	9.105.0.0	1	13.104.0.3 ruteador D
	0.0.0.0	10	13.104.0.3 ruteador D

Cuadro 2.7 Tabla de rutas estructurada en los ruteadores A y B de la red *IP* de la figura 2.25

La tabla de rutas del Ruteador B de la figura 2.25, indica que para alcanzar la red 103.101.0.0 se requiere de un salto a través del ruteador A que tiene la dirección 13.102.0.1 ; para llegar a la red 13.103.0.0 se necesita dar un salto a través del ruteador C que tiene la dirección 13.104.0.2; para alcanzar la red 9.105.0.0 se requiere de un salto a través del ruteador D que tiene la dirección 13.104.0.3; para llegar hasta otras redes se requiere dar 10 saltos a través del *router default* D que tiene la dirección 13.104.0.3

El número límite de saltos es 15, en tanto que 16 se considera como infinito número de saltos. *RIP* no evalúa la velocidad del enlace de un camino particular, y es lento para encontrar nuevas rutas cuando la red cambia en su topología, lo cual ocasiona que se consuma considerablemente el ancho de banda.

Otros protocolos ruteables como *Apple Talk*, *DECNet*, y *Netware* se describen en el Anexo 1.

2.4 PROTOCOLOS DE ENRUTAMIENTO

2.4.1 ENRUTAMIENTO INDIRECTO [17]

El enrutamiento indirecto consiste en determinar el camino a través de la red. Para ello se usa algoritmos de enrutamiento y se emplea tablas de rutas. La información de enrutamiento varía dependiendo del algoritmo usado para generar las tablas.

Los algoritmos generan valores numéricos llamados ***metrics*** o métricas. Algunos algoritmos completan sus tablas con el destino de red y con el siguiente salto, [*Destination NetID/Next Hop*].

El cuadro 2.8 muestra una tabla de rutas, la cual indica que para alcanzar una red destino, el paquete es enviando al sistema o *gateway* identificado como *Next Hop.*

Destination NetID	***Next Hop***
18.	G - 1
36.5	G - 2
164.32.	G - 2
122.	G - 3
Default	G - 1

Cuadro 2.8 Tabla de rutas de redes destino con el siguiente *gateway* G a donde debe dirigirse el paquete

Otros algoritmos asocian ***destination/metric*** para determinar la mejor ruta. Esta asociación da al *router* algunas opciones para alcanzar el destino por varias rutas dependiendo de cual *metric* es la más conveniente.

El *metric* es referido más bien como una distancia, por lo que se debe incluir también la distancia física. Si se asocia la **distancia/camino**, se indica el camino exacto para el paquete, lo cual no es efectivo si se trabaja en redes grandes.

[17] *TCP/IP Technical Concepts, Open Strategies,Inc and NCR* Capítulo 6

2.4.2 PROTOCOLOS DE *GATEWAY*[18]

Los ***Gateways*** son sistemas intermedios que conmutan paquetes entre diferentes redes usando un grupo de protocolos. Estos se conectan físicamente a dos o más redes, y mantienen tablas de rutas con información actualizada de las redes locales y remotas a las que puede accesar, escogiendo el mejor camino.

Operan en la capa de Acceso a la Red *(Network Access Protocol NAP)* y en la capa *IP*, como se indica en la figura 2.26, que corresponden a las capas física, enlace y red del modelo *OSI*. Por tanto las tramas solamente son desencapsuladas y encapsuladas.

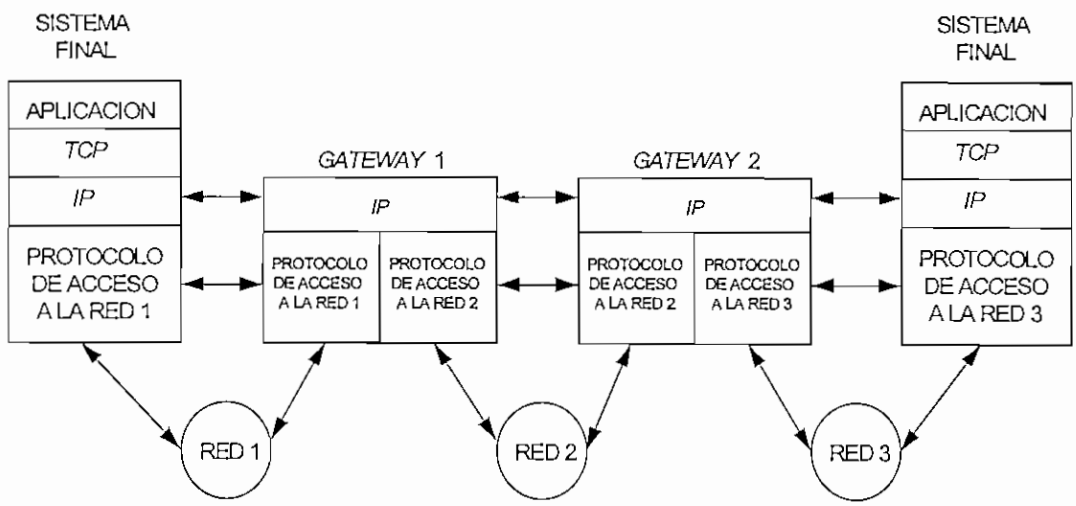


Figura 2.26 Disposición de los *Gateways* en una red de datos

Las tablas de rutas se actualizan mediante el intercambio y comparación de tablas de rutas entre *gateways*, usando el protocolo *Gateway to Gateway (GGP)*

Un ***Gateway* Núcleo** es un *gateway* central que contiene información de todas las rutas posibles de *internet*. Estos asignan las tareas de enrutamiento a gateways secundarios, que son los encargados de encontrar la ruta adecuada hacia un destino.

Los protocolos de gateway se describen en mayor detalle en el Capítulo 3 en el numeral que corresponde a Enrutamiento en Sistemas Autónomos.

[18] *TCP/IP Technical Concepts, Open Strategies,Inc and NCR* Capítulo 6

2.4.3 TABLA DE MANEJO DE RUTAS [19]

Cuando *IP* recibe un datagrama, ejecuta un algoritmo para escoger la ruta basándose en la tabla de rutas que tiene la máquina y contesta a las siguientes preguntas:

1.- Es este datagrama para mi ?.

2.- Es este datagrama para un *host* en una red conectada directamente al ruteador ?. (Un *host* que no requiere rutear a través de *gateways*)

3.- Conozco a un *gateway* en la red conectada directamente, el cual es un camino hacia la red destino ?.

4.- Conozco a un *gateway default* en cualquiera de las redes conectadas directamente ?.

Las preguntas 3 y 4 requieren la comparación de las direcciones destino de los datagramas con la tabla de rutas. *IP* realiza este proceso tanto en los *hosts* destino como en los *gateways*.

Las tablas de rutas contiene la dirección *IP* de una red destino y la dirección del siguiente *gateway* G a partir del *gateway* de referencia en el camino hacia esta red. Este se conoce como *Next Hop* o siguiente salto.

Ejemplo

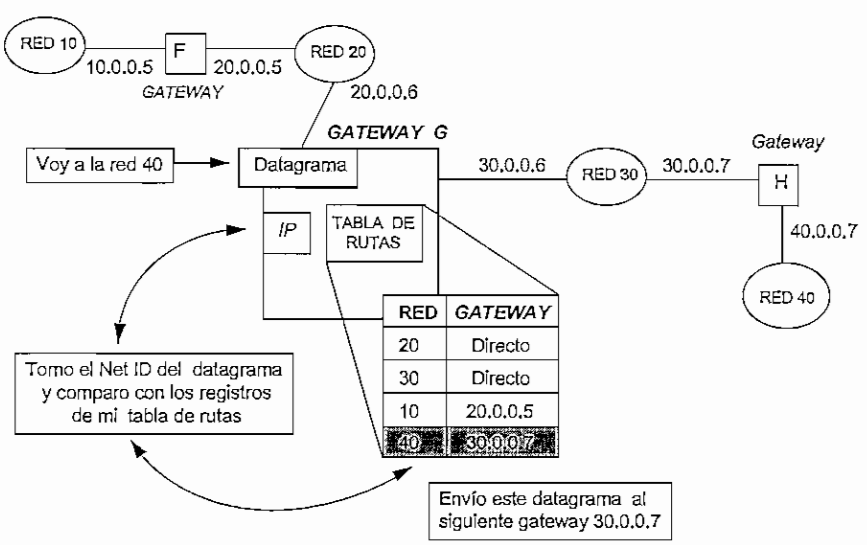


Figura 2.27 Descripción del funcionamiento del *Gateway* G

[19] *TCP/IP Technical Concepts, Open Strategies,Inc and NCR* Capítulo 6

En el ejemplo de la figura 2.27 se muestra el funcionamiento de un *Gateway* **G**, en el cual se realizan los siguientes procesos:

1.- El datagrama llega al *gateway* **G** para ser enviado a la red **40**.0.0.0.

2.- El software *IP* del *gateway* acepta el datagrama para ser procesado.

3.- *IP* ejecuta el algoritmo:

. Extrae el *NetID* (**40**) de la dirección *IP* destino del datagrama.

. Consulta la tabla de rutas y compara con el *NetID.*

. Hace las cuatro preguntas para determinar la responsabilidad de enrutamiento.

4.- Para llegar a la red **40** se tiene un *next hop* de 30.0.0.7 que es la dirección del *gateway* **H** en el lado que está directamente conectado a **G**, es decir **G** y **H** pertenecen a la red 30 al mismo tiempo. **H** permite el paso del datagrama hacia la red 40.

2.4.4 COMPARACION DE LAS RUTAS ESTATICAS Y RUTAS DINAMICAS

Las tablas de rutas varían de acuerdo al algoritmo de enrutamiento utilizado. Por ejemplo si éstas se generan por un algoritmo de rutas estáticas, las tablas resultantes deben ser mapeadas por el administrador antes de que el enrutamiento se inicie. Las rutas pueden ser cambiadas sólo por el administrador.

No se permite cambios severos en la topología, porque la red se torna inconsistente y además las tablas requieren un constante mantenimiento debido a estas variaciones.

Los algoritmos de enrutamiento Dinámico ajustan automáticamente los cambios en la red. Las tablas de rutas dinámicas son constantemente actualizadas, mediante el intercambio de mensajes que recalculan las rutas y envían mensajes de actualización a otros *routers*, los cuales ajustan sus rutas en forma adecuada.

2.4.5 METRICAS (*METRICS*)

Los *metrics* son valores numéricos utilizados por los algoritmos de enrutamiento para determinar la mejor ruta hacia una red destino.

El algoritmo de enrutamiento calcula los *metrics*, que son valores que se obtienen en función de variables como retardos , ancho de banda, calidad del medio de transmisión, etc.

Los *metrics* son valores que establecen la confiabilidad de cada enlace de red, los retardos requeridos para mover el paquete de la fuente al destino, el ancho de banda, la carga, la máxima unidad de transferencia (*MTU*), el costo de comunicación, etc .

Los metrics más empleados son:

- **Longitud del Camino** .- Algunos protocolos de enrutamiento definen a la longitud del camino como la suma de los costos asociados con cada uno de los enlaces a través de los que pasa el dato. Otros protocolos de enrutamiento lo definen como la cantidad de saltos a través de los ruteadores que el paquete debe dar para llegar al destino.

- **Alcanzabilidad** .- Es un parámetro determinado por la velocidad de recuperación de un enlace cuando éste se ha caído.

- **Retardo** .- Es el tiempo requerido para mover un paquete de la fuente hasta el destino a través de la red. Depende de varios factores como el ancho de banda de los enlaces de red intermedios, calidad de los puertos, congestionamiento en los enlaces intermedios y la distancia física que debe atravesar.

- **Ancho de Banda** .- Se refiere a la capacidad de tráfico que tiene un enlace. Para enlaces *Ethernet* el ancho de banda es 10 Mbps.

- **Carga** .- Es el grado de ocupación que tienen los equipos de la red, como por ejemplo el grado de utilización del *CPU*, procesamiento de paquetes por segundo, transmisión de paquetes por segundo, etc.

- **Costo de la Comunicación** .- Se refiere al costo monetario de los medios de transmisión.

2.4.6 COMPARACION DE LOS ALGORITMOS VECTOR DISTANCIA Y ESTADO DE ENLACE

El vector distancia y estado de enlace son dos algoritmos de enrutamiento.

Los algoritmos **Vector Distancia**, son utilizados por los *gateways* para generar información de enrutamiento mediante un *metric* llamado cantidad de saltos (*hop count*). Un *Hop Count* es la suma de los *gateways* a través de los cuales el mensaje debe pasar, para alcanzar el destino final en un sistema autónomo.

Cada *gateway* tiene un *set* de rutas para todas las redes conectadas, donde se identifica el destino y el número de saltos que se requieren para alcanzar el destino.

Los *gateways* vecinos periódicamente intercambian información de sus tablas de rutas. Cuando hay un cambio en la topología de la red, el *router* genera un nuevo *set* de rutas, denominándose este proceso Convergencia.

Cuando un *router* A envía su tabla de rutas a su vecino B, el router B une esta tabla con la suya y transmite esta tabla resultante a su *router* vecino C.

Vector(Destino)	Distancia (En saltos)
Red 2	1
Red 5	3
Red 21	5
Red 36	7
Red 43	3

Cuadro 2.9 Ejemplo de Vector destino vs Distancia en saltos

Si bien este algoritmo es fácil de implementar, tiene sus desventajas:

. Si los cambios de rutas son muy rápidos, su cálculo no se alcanza a realizar.

. No trabaja bien en *Internets* grandes, puesto que las tablas de rutas grandes transmitidas adicionan congestión a la red.

El algoritmo **Estado de Enlace**, es conocido como *Short Path First* (*SPF*), en donde se requiere que cada *gateway* tenga información completa de la topología, esto es, debe tener un mapeo a los demás *gateways*.

En lugar de enviar las tablas de rutas completas, un esquema Estado de Enlace realiza dos tareas:

1.- Hace un chequeo activo del estado de sus vecinos , preguntándoles:

¿ Hola, está usted vivo y alcanzable ? .

2.- Envía la información de los Estados de Enlaces a todos los *gateways* en forma de mensajes de *broadcastings* periódicos.

Este mensaje no especifica rutas. Lo único que da a conocer es, si es posible la comunicación entre dos *gateways*.

Cuando el mensaje del Estado llega al *gateway*, éste usa esta información para actualizar el mapa de *internet*, subiendo o bajando los enlaces.

Cada *router* envía la información del estado de los enlaces a cada uno de sus vecinos, los cuales a su vez se encargan de transmitir hacia sus respectivos vecinos, produciéndose una especie de transmisión en cascada.

Cuando un *router* recibe la información de los enlaces, éste construye un árbol invertido, poniendo en la raíz su propia información y en las ramas coloca la información de sus vecinos. El árbol se reduce de modo que el camino más corto a cada red destino siempre se encuentra en el árbol y la tabla de rutas es construida en base al árbol resultante.

Cada enlace tiene asociado un *routing metric*, que influye en el tipo de servicio (*Type of Service TOS*) como retardos, confiabilidad, velocidad, y es colocado en cabecera *IP*.

Las ventajas de los protocolos que utilizan el algoritmo Estado de Enlace son :

- Cada *gateway* calcula las rutas independientemente.
- Como los *gateways* hacen el cálculo localmente, la convergencia se garantiza.
- Los mensajes de estados de enlace llevan sólo información de una conexión directa a un *gateway*.
- El enrutamiento Estado de Enlace es más confiable que el Vector Distancia.

CAPITULO III PROTOCOLOS TCP/IP

Este capítulo describe el funcionamiento de los principales Protocolos *Internet*: Protocolo *IP*, Protocolo *Internet* de Mensajes de Control *ICMP*, Protocolo de Control de Transmisión *TCP*, Protocolo de Datagrama de Usuario *UDP*, Protocolos de enrutamiento *IP*, los servicios de aplicación como *Telnet* y Protocolo de Transferencia de Archivos *FTP*; y el modelo Cliente - Servidor.

Se estudia el encapsulamiento IP en X.25 y *Frame Relay*.

3.1 PROTOCOLOS *INTERNET*

TCP/IP (*Transmisión Control Protocol / Internet Protocol*), son un conjunto de protocolos que sirven para interconectar redes *LAN* similares o diferentes a través de redes *WAN*.

El modelo *Internet*, referido al modelo *OSI*, tiene la siguiente configuración:

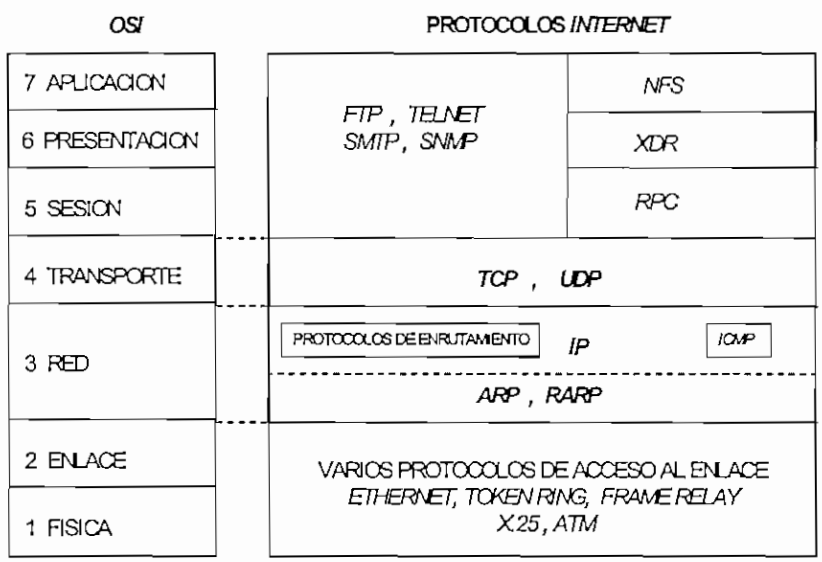


Figura 3.1 Modelo *Internet* referido al modelo *OSI* [1]

La capa física de acceso a la red, permite el intercambio de datos entre una estación y la red física a la cual está conectada. El protocolo depende del tipo de red implementado, tales como *Ethernet, Token Ring, FDDI, X.25, ATM, Frame Relay.*

[1] *Internetworking Technology Overview, Cisco Systems*, Capítulo 18

La capa Red (*internet)*, permite que los datos lleguen a múltiples redes. Los protocolos principales que se ubican en esta capa son: *IP* e *ICMP (Internet Control Message Protocol)*[2].

La capa Transporte es la encargada de transportar y entregar los datos generados en la capa de aplicación, sin errores, duplicaciones, pérdida de orden, etc. Los protocolos representativos de esta capa son: *TCP* orientado a conexión, y *UDP* sin conexión.

3.1.1 PROTOCOLO *INTERNET IP*

Es un protocolo que opera en la capa red ofreciendo un servicio de conexión no confiable entre estaciones, o para las capas superiores en el mismo nodo.

La unidad de intercambio entre estaciones es el **datagrama**, el cual puede tomar caminos diferentes hasta el destino, por lo que el arribo del mensaje se realiza en desorden, dependiendo de las condiciones y facilidades del medio, lo cual no garantiza la confiabilidad del mensaje.

El datagrama IP consta de una cabecera y datos. La cabecera IP tiene información de direcciones y parámetros de control.

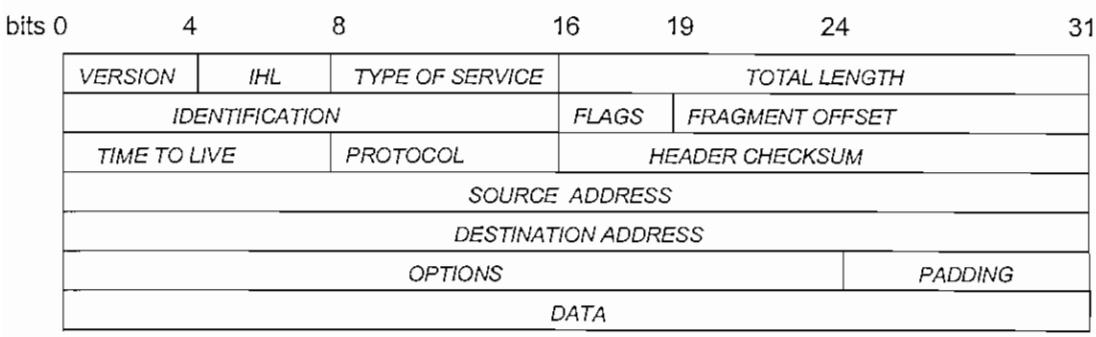


Figura 3.2 Formato del datagrama *IP*

Version: Indican el número de versión y permite la evolución del protocolo.

IHL:*Internet Header Lenght*.- Longitud de la cabecera *internet*.

Type of Service: Especifica la confiabilidad, prioridad, retardos, y parámetros de envío.

---

[2] *ICMP* = Protocolo de Mensajes de Control *Internet* que resuelve errores y controla mensajes

Total Length: Indican la longitud total en octetos del datagrama, incluido el header.

Identification: Es la identificación única del datagrama.

Flags: Ocupa 3 bits, los dos primeros se usan para control de fragmentación y reensamblado, el tercero no es usado.

Fragment Offset: Indica donde fue fragmentado el datagrama, medido en unidades de 64 bits.

Time to Live (TTL): Es el tiempo de vida del datagrama, el cual sirve para evitar que el datagrama viaje indefinidamente por la red.

Protocol: Indica el protocolo del siguiente nivel que recibe el campo de datos en el sistema destino.

Header Checksum: Chequea la integridad sólo del header.

Source Address: Especifica la red y la estación origen.

Destination Address: Especifica la red y la estación destinos.

Options (variable): Son opciones requeridas o solicitadas por el emisor.

Padding (variable): Asegura que la parte final del header tenga 32 bits. Es decir, los campos *Options* más *Padding* deben completar 32 bits.

Data (variable): Debe ser múltiplo de 8 bits .

La longitud total del campo de datos más la cabecera debe tener máximo 65.535 octetos.

En sistemas con *gateways*, cada datagrama es enrutado en forma independiente hacia las diferentes redes, mediante las tablas de rutas contenidas tanto en las estaciones, como en el *gateway*.

Las características principales del protocolo *IP* se resumen a continuación:

- *IP* enruta los datagramas en áreas congestionadas y actúa rápidamente mediante decisiones de enrutamiento de datagramas.
- No garantiza la integridad del dato.
- La desconfiabilidad se produce cuando la estación se satura, o si la red falla.

3.1.1.1 ENCAPSULAMIENTO *IP*

El encapsulamiento consiste en colocar una cabecera al datagrama *IP*, luego de lo cual pasa a la capa de acceso a la red, para ponerlo en una trama. En la trama de igual modo se coloca una cabecera.

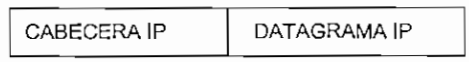


Figura 3.3 Encapsulamiento del datagrama *IP*

Cuando el datagrama llega a su destino, la cabecera de la trama se quita y el datagrama pasa a la capa *internet* donde la cabecera *IP* es leída.

3.1.1.2 FRAGMENTACIÓN Y REENSAMBLADO

La **fragmentación** es el proceso por el cual *IP* divide al datagrama en fragmentos manejables por las redes que tienen un determinado *MTU* (*Máxima Unidad de Transferencia*), reduciéndolos a un tamaño menor o igual al *MTU*. El tamaño del fragmento es determinado por el tipo de red.

El proceso de juntar nuevamente al datagrama fragmentado se denomina **reensamblado.**

3.1.1.3 DIRECCIONAMIENTO *IP*[3]

Cada máquina en la red está identificada por su dirección *IP*, que consta de 32 bits divididos en 4 octetos que identifican tanto a la red (*Net ID*) como al *Host* (*Host ID*).

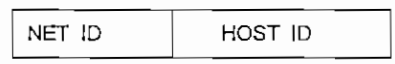


Figura 3.4 Formato de dirección *IP*

Las redes de *Internet* se clasifican por el tamaño y las direcciones asignadas. Las tres principales redes son:

Clase A - Se tiene hasta 128 redes (2^7), y sobre los 16 millones de *hosts* por cada red.

El primer bit de la dirección es 0. El primer octeto se emplea para identificar la red y los tres restantes para identificar la estación.

red.*host.host.host*

[3] *TCP/IP Technical Concepts, Open Strategies, Inc. and NCR*, Capítulo 4

El rango de NetID es: 1 - 126 , donde las identificaciones 0 y 127 son reservadas.

La máscara[4] de red es 255.0.0.0

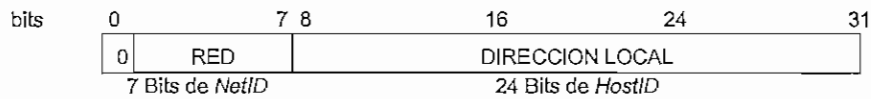


Figura 3.5 Formato de dirección *IP* para redes clase A

Clase B - Son redes medianas, en donde se tienen 2^{14} redes con 2^{16} usuarios cada una.

Los primeros dos bits de la dirección son 10. Los dos primeros octetos se emplea para identificar la red, y los dos restantes para identificar la estación.

red.red.*host.host*

El rango de NetID es: 128.1 - 191.254.

La máscara de red es 255.255.0.0

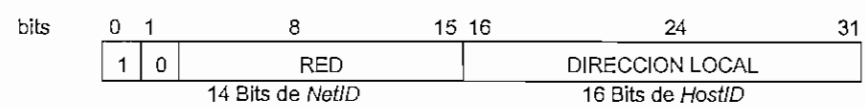


Figura 3.6 Formato de dirección *IP* para redes clase B

Clase C - Son redes pequeñas, en donde se tienen 2^{21} redes con 254 usuarios por red.

Los primeros tres bits de la dirección son 110. Los tres primeros octetos se emplea para identificar la red, y el último para identificar la estación.

red.red.red.*host*

El rango de NetID es: 192.1 - 223.254.254

La máscara de red es 255.255.255.0

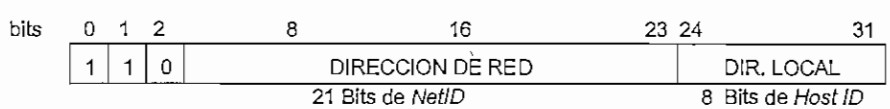


Figura 3.7 Formato de dirección *IP* para redes clase C

La dirección 255 se utiliza para *broadcasting* , es decir para enviar mensaje a toda la red.

Los otros protocolos que se ubican en la capa *internet* como *ICMP, ARP* y *RARP* se describen en detalle en el Anexo 1.

[4] La máscara de red son cuatro octetos que sirven para determinar el número de la red y de la estación, en donde el valor 255 indica que todos los bits del octeto son unos (255=11111111)

3.1.2 PROTOCOLO DE CONTROL DE TRANSMISION *TCP* [5]

Es un servicio de transporte de flujo confiable, que adapta y robustece al protocolo *IP*. Se caracteriza por las siguientes funciones:

- Orientación de flujo.
- Conexión de circuito virtual, establecido entre las estaciones transmisoras y receptoras.
- Flujo no estructurado, es decir, las estaciones negocian el formato de los mensajes antes de iniciar una conexión, lo cual depende de las aplicaciones que se ejecutan en las estaciones.
- Conexión *Full Dúplex*, que permite la transferencia en ambas direcciones, con un canal de datos y un canal de control de comunicaciones.

TCP permite que varios programas de aplicación, se comuniquen entre ellos mediante la asignación de puertos de identificación para cada aplicación.

Las conexiones de circuito virtual son identificadas por medio de un par de puntos extremos. Un punto extremo está formado por la dirección *IP* de una estación y un puerto *TCP* en dicha estación. Varias conexiones en una misma máquina pueden compartir un número de puerto, por cuanto *TCP* asocia los mensajes entrantes con una conexión.

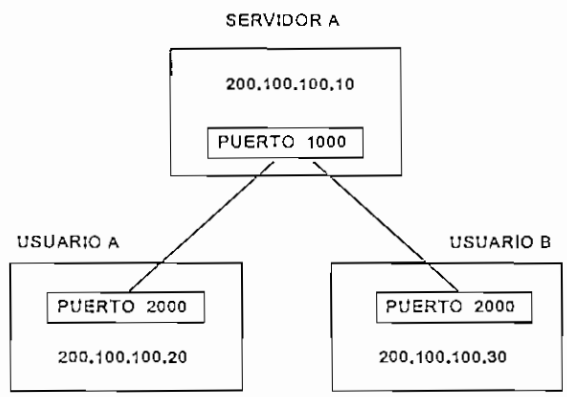


Figura 3.8 Conexiones de puertos de usuarios con puerto de servidor

Para el ejemplo de la figura 3.8, los usuarios B y C cuyas direcciones *IP* son 200.100.100.20 y 200.100.100.30 respectivamente tienen un servicio identificado con el puerto 2000. El servicio 2000 de los usuarios se comunica con un servicio identificado con el puerto 1000 en el Servidor A

[5] Redes Globales de Información con Internet y TCP/IP, Douglas Comer, Capítulo 9

que tiene dirección IP 200.100.100.10. Se forman conexiones virtuales desde los usuarios hasta el servidor A de la siguiente forma:

(200.100.100.20, 2000) y (200.100.100.10, 1000)
(200.100.100.30, 2000) y (200.100.100.10, 1000)

TCP divide y segmenta los datos de las aplicación, para que sean manejables por *IP*.

3.1.2.1 ESTABLECIMIENTO DE UNA CONEXION *TCP*

Para establecer el canal de comunicación entre estaciones, *TCP* utiliza un saludo de tres etapas (*Three Way Handshake*), el cual sincroniza a las dos estaciones, estableciéndose una comunicación orientada a conexión.

Este proceso se realiza de la siguiente manera:

- La estación 1 envía el número de secuencia de sincronización inicial aleatoria ***SYN = x***
- La estación 2 recibe la señal de sincronismo *SYN=x* , y responde con un mensaje de reconocimiento ***ACK = x+1*** (la señal *SYN* aumentada en 1) y envía además su propia secuencia de sincronismo ***SYN = y.***
- La estación 1 recibe los dos mensajes (*ACK*=x+1 y *SYN=y*) y envía un mensaje de reconocimiento ***ACK =y+1*** (*SYN=y* aumentado en 1), hacia la estación 2.
- La estación 2 recibe el *ACK=y+1*, quedando establecida la conexión, a través de la cual los datos pueden fluir en ambas direcciones.

El proceso anterior se muestra en la figura 3.9:

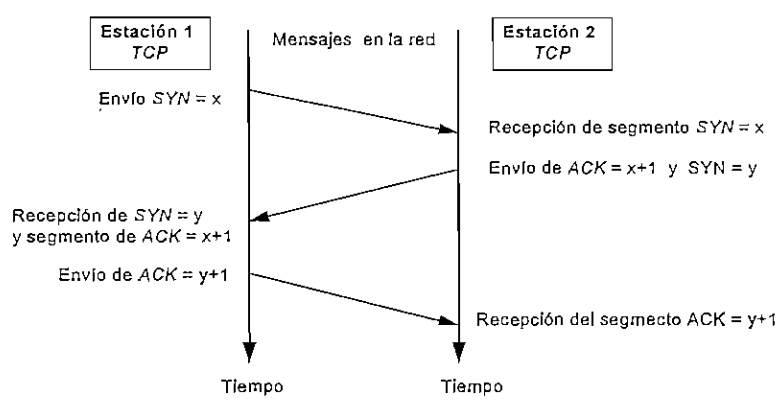


Figura 3.9 Proceso de establecimiento de una conexión *TCP* entre estaciones

3.1.2.2 CIERRE DE UNA CONEXIÓN *TCP*

El cierre de la conexión es necesario para evitar pérdidas de datos en ambas estaciones, para lo cual, se emplea el mismo método de tres etapas, en donde, en lugar de enviar secuencias *SYN* , se envían secuencias de finalización ***FIN*** entre las estaciones , como se indica en la figura 3.10.

La Estación 1 genera un mensaje ***FIN=x*** inicial para cerrar la conexión. La Estación 2 en lugar de generar un mensaje FIN inmediatamente, envía un reconocimiento de recibo ***ACK=x+1*** a la Estación 1 y luego informa a la aplicación, la solicitud de cierre. Informar a la aplicación de la solicitud de cierre y obtener una respuesta, puede tomar un tiempo considerable. El reconocimiento de recibo ***ACK=x+1*** evita la retransmisión del mensaje inicial ***FIN=x*** desde la Estación 1 durante la espera. Cuando la aplicación autoriza el cierre de la conexión, la Estación 2 envía el segundo mensaje ***FIN=y*** junto con el mismo reconocimiento de recibo ***ACK=x+1*** en respuesta al mensaje inicial ***FIN=x*** para no perder la secuencia de mensajes. La Estación 1 responde con el tercer mensaje que es un reconocimiento de recibo ***ACK=y+1*** en repuesta a los mensajes ***FIN=y*** y ***ACK=x+1***. La Estación 2 recibe el mensaje ***ACK=y+1*** y la conexión se cierra.

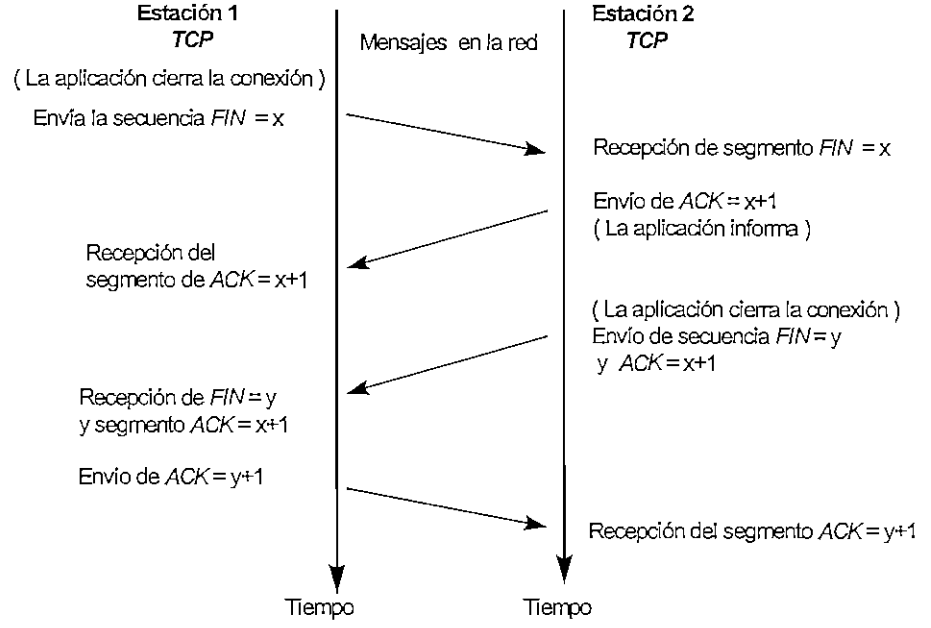


Figura 3.10 Proceso de cierre de una conexión *TCP*

3.1.2.3 RECONOCIMIENTO POSITIVO CON RETRANSMISIÓN

Cada paquete tiene un número de secuencia provisto por el *TCP* inicial; mediante este número los paquetes son contados por el receptor, y reensamblados en el propio orden.

El reconocimiento positivo es enviado por el receptor del paquete hasta el emisor. Esto se hace añadiendo un 1 al número de secuencia del paquete que fue recibido.

Si se recibe el reconocimiento en el emisor, éste continua transmitiendo. Si el tiempo expira sin que el emisor reciba el reconocimiento, éste retransmitirá el paquete .

Si el receptor detecta la pérdida de un paquete, solicita una retransmisión del paquete perdido, refiriéndose al número de secuencia.

En la figura 3.11 se observa un ejemplo de reconocimiento positivo y retransmisión. Después que la conexión se estableció, TCP_A envía 20 octetos a TCP_B con un número de secuencia de *DATA:201*

B recibe el paquete y adiciona 20 (número de octetos recibidos) al último número de secuencia que ha llegado (201). Entonces envía un *ACK:221* hacia A.

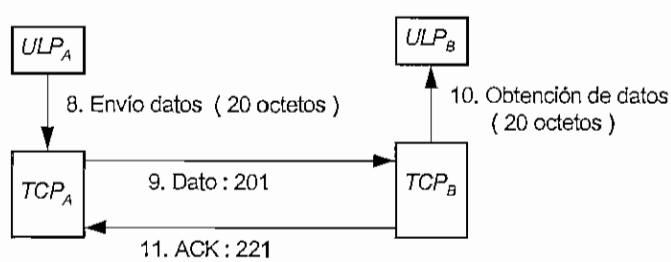


Figura 3.11 Transmisión de datos a través de una conexión *TCP*

En el ejemplo de la figura 3.12, si B envía 125 octetos hacia A con un número de secuencia de *DATA:551*, A adiciona 125 al último número de secuencia recibido y envía un *ACK:676* hacia B. Pero si el *ACK* nunca llega a B, el TCP_B espera por el *ACK* hasta que ocurre un *time out*. En este caso retransmite los 125 octetos a la estación A. A recibe la retransmisión y envía un reconocimiento hacia B.

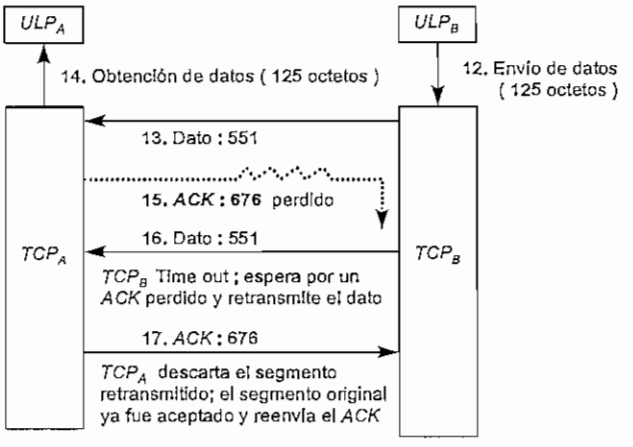


Figura 3.12 Retransmisión de datos en una conexión *TCP*

3.1.2.4 VENTANA DESLIZANTE

Es un mecanismo que controla el flujo de mensajes a nivel de octeto, evitando la sobrecarga y pérdida, por el envío de datos y la espera de sus reconocimientos. Esto significa que un segundo paquete puede ser enviado antes de que el reconocimiento del primer paquete sea recibido.

Tiene tres apuntadores. El primer apuntador separa los octetos que ya se enviaron y que fueron reconocidos mediante un *ACK*. El segundo apuntador define el octeto más alto en la secuencia que se puede enviar, antes de recibir más reconocimientos de recibo. El tercero separa los octetos que ya se enviaron de los que aun no se envían. Con este método se mejora el uso del ancho de banda disponible.

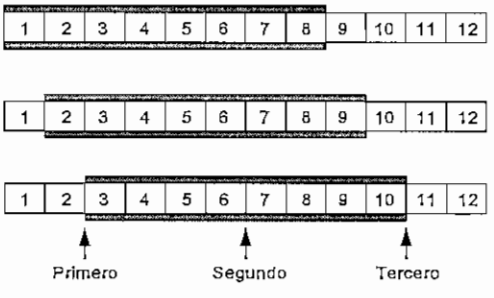


Figura 3.13 Ventana deslizante de 8 paquetes

Si se tiene una ventana que abarca 8 paquetes, el emisor conoce que puede enviar hasta 8 paquetes antes de recibir un reconocimiento *ACK*. Luego de recibir el *ACK* del primer paquete, el

emisor envía el paquete 9. Luego de recibir el segundo *ACK*, éste envía el paquete 10, y así sucesivamente, manteniendo una ventana deslizante de 8 paquetes para la transmisión.

Como *TCP* es *full duplex* , en cada extremo de una conexión se mantiene dos ventanas (una para recepción y otra para transmisión).

TCP permite que varios programas de aplicación, se comuniquen entre ellos mediante la asignación de puertos de identificación para cada aplicación. Las ventanas de tamaño variables disminuyen o aumentan, dependiendo del estado de flujo de octetos y del tamaño de las ventanas ubicadas en el otro extremo de la conexión.

3.1.2.5 CONTROL DE FLUJO

El receptor puede hacer que el emisor aumente o disminuya la velocidad de emisión mediante el control de flujo.

El receptor puede pedir bloques grandes de datagramas, si éste puede manejarlos, y solicitar que disminuya la emisión si se encuentra saturado. De esta forma las estaciones con diferente *"performance"* pueden operar entre si.

Para controlar el tamaño del datagrama, *TCP* usa el campo de *OPCIONES* de la cabecera *IP* para realizar las negociaciones entre los dos sistemas. El receptor especifica el máximo tamaño del segmento que puede manejar, y el emisor se ajusta a estos requerimientos.

3.1.2.6 TIEMPOS DE RETRANSMISION *TCP*

TCP usa un algoritmo de Tiempo de Adaptación que determina el tiempo de viaje de los paquetes enviados. Si se excede en este tiempo se produce un *Time Out* y se retransmite el segmento. Si la red está lenta o rápida, el tiempo se ajusta después de que cada segmento es enviado y recibido en el receptor.

3.1.2.7 FORMATO DEL SEGMENTO *TCP*[6]

La unidad de transferencia entre estaciones es el segmento, el cual permite establecer y cerrar conexiones, transferir datos, enviar reconocimientos de recibos, indicar tamaño de ventanas, etc .

Su formato es el siguiente :

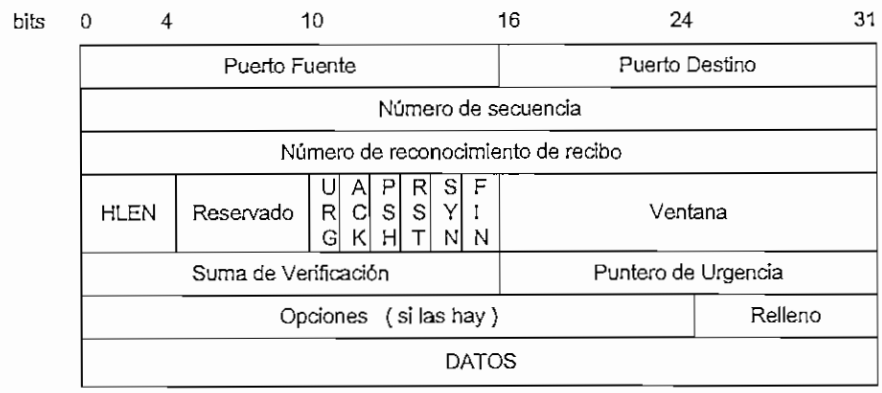


Figura 3.14 Formato del mensaje *TCP*

Puertos . Se usa para indicar la dirección de varios programas de aplicación.

TCP debe conocer que aplicación está enviando y recibiendo cada datagrama.

Número de Secuencia . Los números de secuencia son requeridos por el sistema destino para ordenar la posición de cada segmento y asegurar que todos sean recibidos.

Número de Reconocimiento . Es un número que indica que el datagrama se ha recibido.

Este número se genera añadiendo 1 al número de secuencia del paquete recibido.

El número de secuencia está en la misma dirección del flujo del segmento, en tanto que el número de reconocimiento está en la dirección opuesta.

Header Length. Especifica la longitud del encabezado del segmento, medida en múltiplos de 32 bits y depende de los campos de OPCIONES y RELLENO.

Banderas . Son 6 bits que determinan el propósito y contenido del segmento *TCP*. Estos bits son:

URG, ACK, PSH, RST, SYN, FIN.

URGent. Indica que el campo *URG* es válido, con lo cual se da prioridad a un segmento sobre otro.

ACK. Indica que el campo acknowledgment es válido.

---

[6] Redes Globales de Información con *Internet* y *TCP/IP*, Douglas Comer, Capítulo 13

PuSH. Los datos se preparan para el flujo rápido en la recepción del dato.

ReSeT. Se usa cuando la línea sale fuera de sincronismo, en cuyo caso cualquiera de los dos lados puede hacer un *reset* y reconfigurar sus parámetros.

SYN. Número de secuencia de sincronización. Se usa como una " petición de conexión" y como " petición de conexión aceptada" y es usado como parte del *Three-Way - Handshake.*

FINish. Es enviado cuando la transmisión es cerrada.

Ventana . *TCP* indica la cantidad o tamaño del dato que acepta, enviando un segmento para especificar el tamaño del *buffer* en el campo ventana.

Suma de verificación . *IP* hace un chequeo solo en este Header .

TCP realiza un chequeo en el *header* interno más el dato.

Opciones . Se usa para negociar *el software TCP* del otro terminal y determinar el máximo tamaño del segmento. Este campo maneja el control de flujo.

3.1.2.8 SUMA DE VERIFICACIÓN / PSEUDOCABECERA *TCP*

El Pseudoencabezado hace el chequeo íntegro del segmento. Esta cabecera no es transmitida pero se la emplea para generar el número de suma de verificación, independientemente en el emisor y en el receptor.

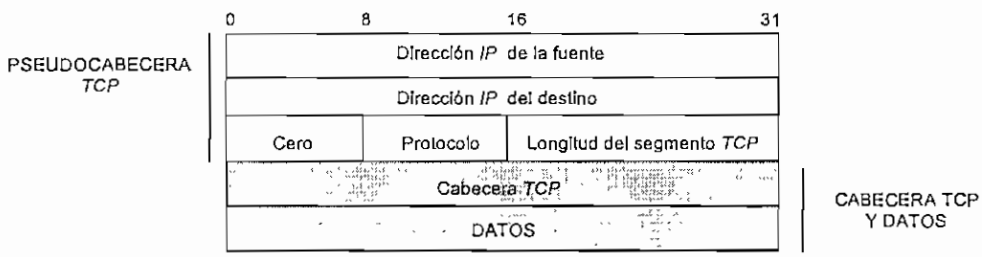


Figura 3.15 Pseudocabecera *TCP*

Como se indica en la figura 3.15, en la parte superior la Pseudocabecera contiene la dirección *internet* fuente y destino. Se incluye el número de protocolo , la longitud del segmento, y un bloque de ceros de relleno para completar la longitud total a un múltiplo de 16 bits. *TCP* totaliza estos valores e inserta esta cantidad en el campo de la Suma de Verificación de la cabecera *TCP*. En el

destino se verifica estos valores, haciendo un cálculo similar e independientemente del proceso realizado en el emisor.

Esta verificación asegura que el dato no se corrompa y que el paquete alcance el destino correcto.

3.1.2.9 CONGESTION [7]

Es una condición de retardos severos, causado por una sobrecarga de datagramas en uno o más puntos de conmutación o en *gateways*.

Cuando se produce la congestión, el *gateway* "encola" los datagramas hasta que puedan ser enrutados.

Los retardos se incrementan, por lo que los paquetes son retransmitidos con más frecuencia agravando la congestión a tal punto, en que la red se torna inservible produciéndose una Congestión de Colapso.

Para evitar los **Colapsos**, *TCP* reduce la velocidad de transferencia cuando se presenta congestión.

TCP utiliza dos técnicas para la reducción de la congestión:

- Arranque lento
- Disminución multiplicativa

El **arranque lento** previene de condiciones en que los *gateways* no tengan tráfico o que tengan una elevada congestión.

Para cada conexión, *TCP* debe conocer el tamaño de la ventana receptora.

Para controlar la congestión se tiene un segundo límite que es la Ventana de congestión, la misma que se reduce en un 50% cuando hay pérdida de un datagrama, en un proceso de **disminución multiplicativa**. Los segmentos que permanecen en dicha ventana reducen sus

---

[7] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capítulo 5

tiempos de transmisión en forma exponencial, de modo que se reduce el tráfico y los *gateways* pueden limpiar sus *buffers.*

3.1.3 PROTOCOLO DE DATAGRAMA DE USUARIO *UDP*[8]

Es un protocolo de transporte con un servicio de entrega de datos, **sin conexión** y no confiable, empleado por *IP* para transportar mensajes entre estaciones, por lo que éstos pueden perderse, duplicarse o llegar en desorden.

Proporciona puertos de protocolo, para distinguir entre muchos programas que se ejecutan en una máquina. Esto es, además de los datos *UDP* contiene los números de puertos origen y destino, para la entrega de mensajes.

Los mensajes *UDP* se denominan datagramas de usuario, los cuales son encapsulados como mensajes *IP* como indica la figura 3.16:

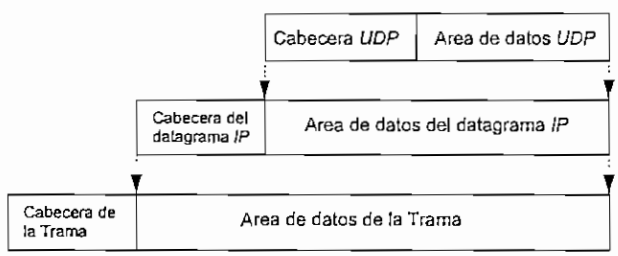


Figura 3.16 Encapsulado *UDP*

El formato del datagrama *UDP* es el siguiente:

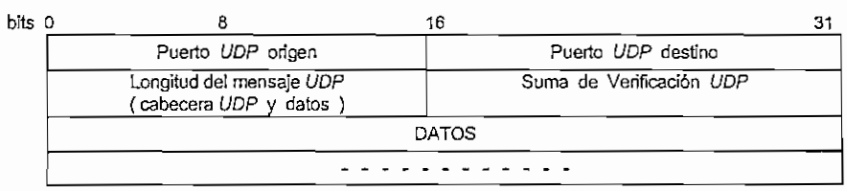


Figura 3.17 Formato del datagrama *UDP*

Se identifican los puertos origen y destino para distinguir a cada una de las aplicaciones que se ejecutan. La longitud del mensaje es medida incluyendo datos y cabecera *UDP*.

[8] Redes Globales con *Internet* y *TCP/IP*, Douglas Comer, Capítulo 12

3.1.3.1 PSEUDO ENCABEZADO *UDP*

Para calcular la suma de verificación, *UDP* añade el Pseudo Encabezado al datagrama, como se indica en la figura 3.18, en el que se incluyen las direcciones *IP* de las estaciones origen y destino, con lo cual se asegura que el mensaje sea entregado al destinatario. En el receptor, si la suma de verificación es correcta, el datagrama es aceptado, caso contrario se descarta.

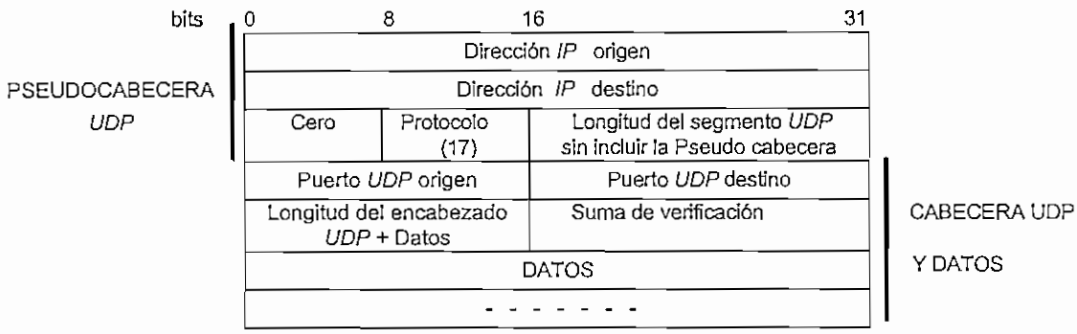


Figura 3.18 Pseudo cabecera *UDP*

El número de protocolo es 17 para *IP*. La capa *IP* transfiere los datos entre un par de estaciones, mientras que *UDP* sólo es responsable de diferenciar entre varios puertos fuentes o destinos dentro de una estación.

En la capa *IP*, las direcciones *IP* se vuelven a calcular, y la Pseudo cabecera se elimina.

3.1.3.2 MULTIPLEXADO / DEMULTIPLEXADO *UDP*

El multiplexado y demultiplexado, se realiza a través de los puertos de protocolos asociados con las aplicaciones. Una vez negociados los puertos de envío-recepción se puede transmitir mensajes. El encargado de realizar este proceso es *UDP*.

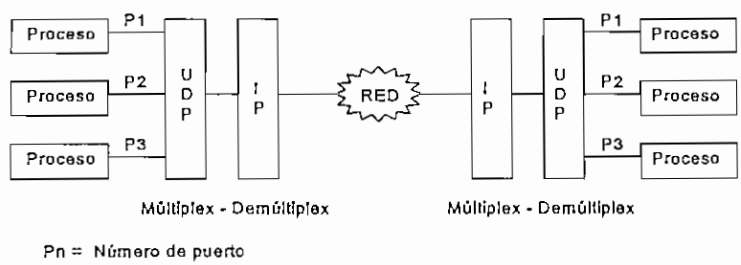


Figura 3.19 Multiplexación *UDP*

Cuando hay muchos datos para un puerto determinado, se producen colas de espera.

3.2 PROTOCOLOS DE ENRUTAMIENTO *IP* [9]

3.2.1 PROTOCOLO DE *GATEWAY* EXTERIOR *EGP*

Es un protocolo dinámico para comunicación entre *gateways* exteriores, en donde las tablas de rutas se actualizan automáticamente usando un simple algoritmo, sin el empleo de *metrics*, por lo que no se puede hacer la selección de la ruta más conveniente.

EGP no es un protocolo Vector Distancia ni Estado de Enlace, y hace las decisiones de enrutamiento basándose en la alcanzabilidad de una red, manteniendo información de las redes que pueden ser alcanzadas a través de ciertas rutas. Envía actualizaciones a sus vecinos a intervalos regulares de 30 o 60 segundos, en donde se indica las redes que están directamente conectadas .

Las computadoras que usan este protocolo se llaman Vecinos *EGP* y los mensajes que se intercambian se denominan **adquirir un vecino**.

Cuando un vecino es reconocido, el sistema pide información de sus rutas. A su vez el vecino envía un paquete con información de accesibilidad de las redes mediante un proceso de actualización. Luego de recibir la actualización, el *gateway* emisor, envía esta información a sus otros vecinos. *EGP* se vuelve frágil cuando *internet* crece.

- No tiene control sobre los lazos que ocurren en redes de múltiples rutas.
- Las actualizaciones grandes entorpecen el funcionamiento de la red .
- Como no usa *metrics*, no puede hacer decisiones inteligentes, por tanto no puede distinguir cual es el camino más corto y adecuado.

3.2.2 PROTOCOLO DE *GATEWAY* DE BORDE O LIMITE *BGP*

Es un protocolo Inter-Dominio que reemplaza al *EGP* y sirve para comunicarse con los *core gateways* y/o entre *gateways* exteriores.

Trabajan sobre una capa de transporte confiable. Además de la alcanzabilidad, *BGP* usa también un *metric* para hacer decisiones inteligentes y detecta lazos de rutas.

---

[9] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capítulo 6 y 16

Inicialmente los *routers BGP* se intercambian las tablas de rutas completas, y las actualizaciones se hace cuando hay un incremento de información en la tabla.

BGP mantiene las tablas de rutas con todos los caminos posibles a una red particular, pero escoge la más óptima de todas para enviar actualizaciones, las cuales tienen solo el número de sistemas autónomos que están en el camino a la dirección *IP* destino.

En este caso el *metric* es un número arbitrario que especifica el grado de preferencia de un camino dado, y son asignados por el administrador de red mediante archivos de configuración, en el que se incluye factores como, contador de dominios, tipo de enlace, costos.

BGP tiene tolerancia ante fallas por cuanto es un protocolo redundante, es decir si una conexión o un *gateway* falla, los otros pueden detectar la falla y asumir el control sobre esta comunicación.

3.2.3 PROTOCOLOS DE *GATEWAYS* INTERIORES *IGP*

Es un grupo de protocolos que completan las comunicaciones "intra-domain", siendo los más representativos *RIP* y *OSPF*.

3.2.3.1 PROTOCOLO DE INFORMACIÓN DE RUTEO *RIP*

Es un protocolo de enrutamiento Vector-Distancia y *gateway* interior. Inicialmente *RIP* se comunica con sus vecinos inmediatos, enviando toda la tabla de rutas.

Cada *gateway* en el dominio envía la misma tabla de rutas a todos los *gateways*, en la cual sólo varía el número de saltos a cada punto destino. Las tablas varían sólo cuando se produce un cambio físico en la red.

El formato de mensaje *RIP* se muestra en la figura 3.20:

Comando (1 - 5)	Versión (1)	Debe estar puesto a cero
Familia de red 1		Debe estar puesto a cero
Dirección *IP* de la red 1		
Debe estar puesto a cero		
Debe estar puesto a cero		
Distancia hacia la red 1		
Familia de red 2		Debe estar puesto a cero
Dirección *IP* de la red 2		
Debe estar puesto a cero		
Debe estar puesto a cero		
Distancia hacia la red 2		

Figura 3.20 Formato del mensaje *RIP*

El **Comando** especifica una operación de acuerdo al cuadro 3.1:

Comando	Significado
1	Solicitud para información parcial o completa de enrutamiento
2	Respuesta con distancias de red de pares desde la tabla de enrutamiento del emisor
3	Activar el modo de trazado (obsoleto)
4	Desactivar el modo de trazado (obsoleto)
5	Reservado para uso interno de *Sun Microsystems*

Cuadro 3.1 Tipos de comandos en el mensaje *RIP*

Versión.- Es la versión del protocolo usado por el receptor para verificar y asegurar la interpretación del mensaje de ingreso.

Familia de red n.- Indica el protocolo usado para interpretar la dirección de red, es decir *RIP* no es específico para *TCP/IP.*

Tiene 4 octetos para direccionar la red, que es más de los 4 octetos que *IP* requiere.

Distancia hasta la red n.- Es el número de saltos a la dirección especificada y va de 1 a 15. El valor de 16 equivale a infinito es decir que no existe ruta.

Las limitaciones de *RIP* son:

- El máximo número de saltos es 15, por eso es preferible usarlo en dominios pequeños.
- No detecta lazos de rutas, por tanto si se producen 15 saltos en lazo, el datagrama será descartado.
- Presenta una baja convergencia. Si tiene una gran cantidad de información de rutas para enviar a su vecino inmediato, y este vecino procesa la información con su tabla y el resultado envía a otro vecino, el proceso se torna tedioso.

- Usa sólo el *metric* contador de saltos, pero no puede diferenciar entre enlaces lentos o rápidos, terrestres o satelitales, y no considera factores como costos o congestión.

3.2.3.2 PROTOCOLO DE SALUDO *HELLO*

Es un protocolo que utiliza un algoritmo Vector-Distancia y una métrica basada en retardos en la red. Sincroniza los relojes entre un conjunto de estaciones y permite que cada máquina calcule las rutas con los retardos más cortos hacia los destinos. Cada mensaje transporta una entrada de datos para la fecha y la hora, para estimar los retardos a las diferentes redes.

Figura 3.21 Formato del mensaje de saludo *HELLO*

3.2.3.3 PROTOCOLO *OPEN SHORTEST PATH FIRST OSPF*

Es un protocolo de rutas dinámicas, en el cual se emite sólo los cambios que se producen en el estado de enlace (conectividad).

OSPF hace lo siguiente:

- Usa múltiples *metrics*, es decir, puede determinar el costo, rutas múltiples basadas en el retardo, rapidez, etc. Además emplea un reconocimiento ***ACK*** para asegurar la entrega.
- Es sensible para los servicios de las capas superiores (*TOS Type of Service*). Esto significa que el emisor puede escoger el tipo de servicio de entrega, por ejemplo el emisor puede seleccionar una línea dedicada de costo elevado para entrega inmediata de mensajes, y líneas telefónicas o conexiones seriales de bajo costo para comunicaciones comunes.
- Provee balance de carga, es decir, si se tiene múltiples rutas para un destino dado y con el mismo costo, entonces *OSPF* distribuye el tráfico por igual en todas las rutas.

- Permite dividir una red en áreas de topología distinta, en donde cada una de ellas puede usar el *OSPF* independientemente.
- Permite esquemas de autenticación, garantizando que sólo los gateways autorizados propaguen información de enrutamiento.

El formato del encabezado del mensaje *OSFP* es el siguiente:

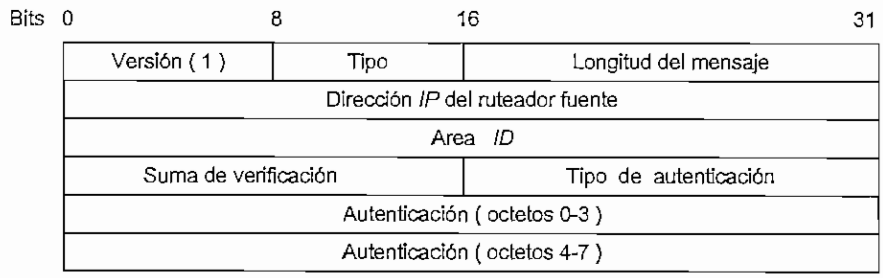


Figura 3.22 Encabezado del mensaje *Open Short Test First*

OSPF utiliza cuatro mensajes:

1.- Envía un mensaje de saludo *HELLO* en cada enlace periódicamente para establecer y probar la accesibilidad a sus vecinos alcanzables, en el cual se incluyen:

. La máscara de la red a la que pertenece el ruteador designado al cual se envía el mensaje.

. *Dead Timer*, que es el tiempo que transcurre para considerar que un vecino se ha caído.

. *Hello Interrupt*, es el tiempo entre mensajes de saludo.

. *Gateway Priority*, es un entero que designa un *gateway backup*.

. Direcciones *IP* de los ruteadores vecinos del ruteador fuente.

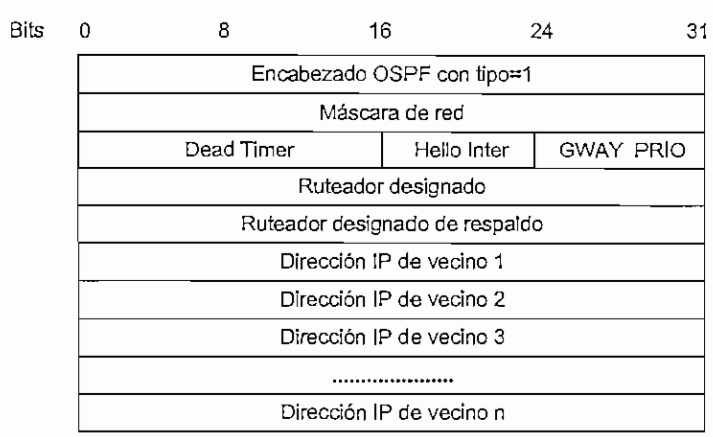


Figura 3.23 Mensaje de saludo *Hello* OSPF de un *gateway* a sus vecinos

2.- *OSPF* usa mensajes de Descripción de Base de Datos para inicializar su base de datos de la topología de red. En este caso un *gateway* sirve como *master* y los otros como esclavos, los cuales responden a cada mensaje enviado por el *master*.

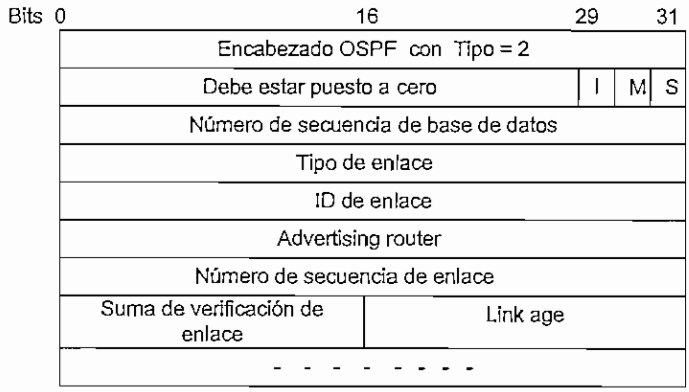


Figura 3.24 Formato del mensaje Descripción de la Base de Datos *OSPF*

3.- Los *gateways* envían mensajes de Solicitud de Estado de Enlace hacia los vecinos pidiendo información actualizada de una lista de enlaces específicos. Los vecinos responden con la información más actualizada. Si la lista es muy grande se requerirá más de un mensaje.

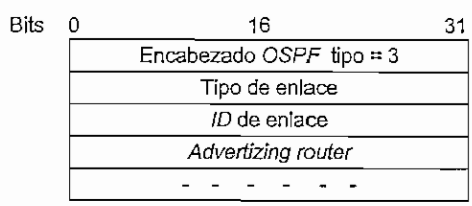


Figura 3.25 Mensaje de Solicitud de Estado de Enlace de *OSPF*

4.- Los *gateways* emiten mensajes de Actualización de Estado de Enlace hacia los vecinos con información actualizada de los enlaces conectados directamente al *gateway*. Los vecinos reciben estos mensajes y actualizan sus tablas de rutas.

El formato del mensaje de actualización del estado de enlace es :

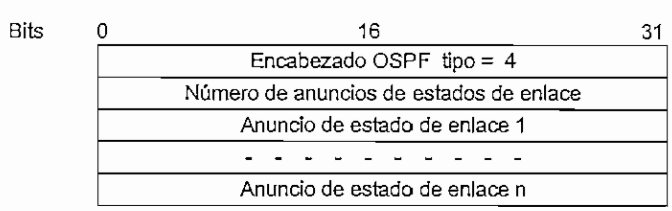


Figura 3.26 Actualización del Estado de Enlace de *OSPF*

3.3 ENRUTAMIENTO Y SISTEMAS AUTONOMOS

Los sistemas autónomos se conocen como dominios autónomos, dominios administrativos y rutas dominios. Un sistema autónomo es un grupo de redes y *gateways* que están bajo un control administrativo simple.

Como se observa en la figura 3.27 los *gateways* núcleo en los sistemas facilitan el enrutamiento en una red compleja, la cual es observada por el *gateway* como una red simple.

Para accesar a las redes ocultas de un sistema autónomo, los *gateways* no-núcleo del sistema deben enviar información de éstas al *gateway* núcleo.

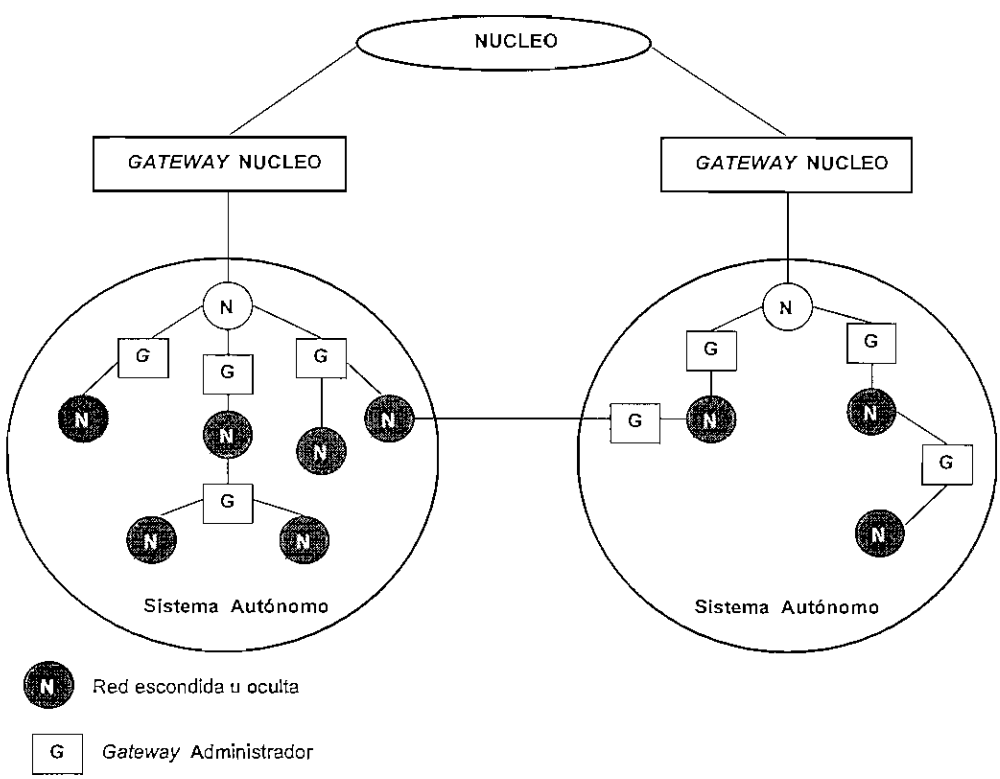


Figura 3.27 *Gateways* Administradores , redes y redes ocultas en sistemas autónomos [10]

Los *gateways* administradores guardan información de todas las redes ocultas y de la operabilidad entre dominios, y garantizan que las rutas de las redes y *gateways* bajo su control sean consistentes y confiables.

[10] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capítulo 6

Las rutas distribuidas permiten la determinación local de las rutas dentro del sistema autónomo y permiten a *internet* expandirse.

Si el intercambio de información de rutas se hace entre *gateways* que están en sistemas autónomos separados, éstos son considerados como *Gateways* Exteriores y el enrutamiento se denomina Inter-Domain.

Cuando el intercambio se realiza entre *gateways* del mismo dominio , son considerados como *Gateways* Interiores y el enrutamiento es Intra-Domain . Estos se denominan vecinos y tienen un enlace directo.

Los gateways encuentran a sus vecinos empleando el protocolo *HELLO.*

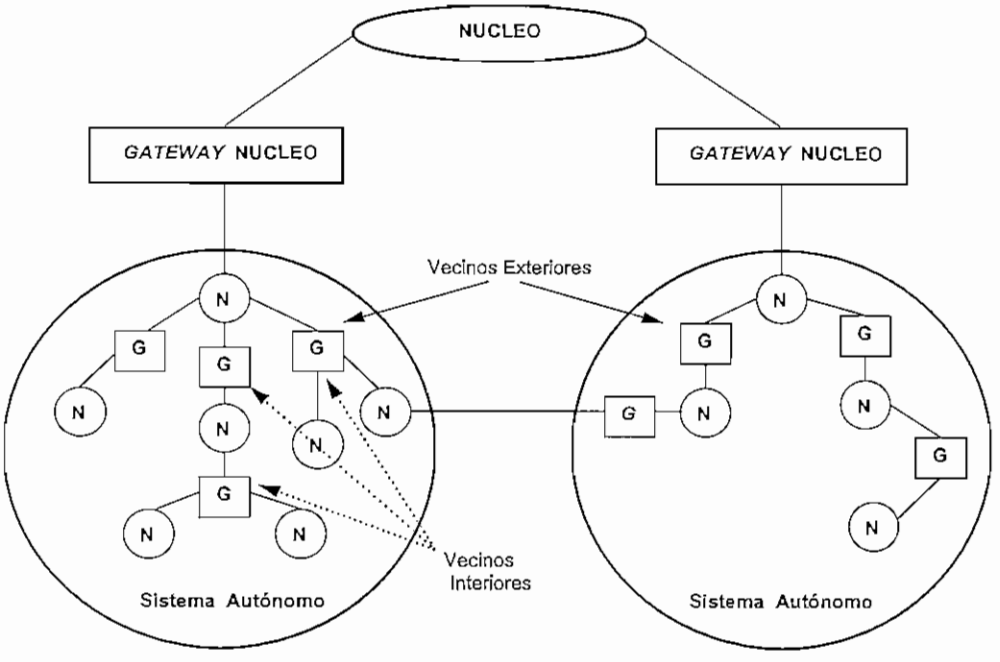


Figura 3.28 *Gateways* Vecinos Interiores y Exteriores en Sistemas Autónomos

Los sistemas autónomos utilizan *gateways* interiores y exteriores para establecer el enrutamiento dentro y fuera del sistema autónomo, de modo que el tráfico hacia los gateways núcleo se reduce.

3.4 DOMINIOS

3.4.1 DOMINIOS DE NOMBRES [11]

Un **dominio** es un grupo de *hosts* que tienen un propósito común y son administrados por una central.

Los Nombres de Dominios son generados en forma jerárquica separados por un punto, en donde el nombre de la izquierda tiene la menor jerarquía.

xyz.com

El *Network Information Center NIC* controla todos los grandes grupos de dominios, los cuales se clasifican en forma jerárquica como se indica en la figura 3.29.

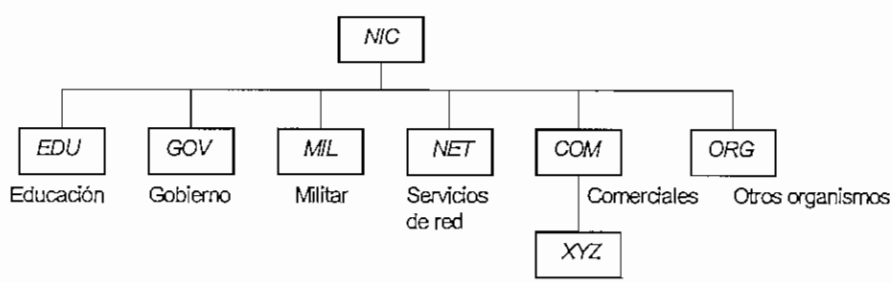


Figura 3.29 Jerarquía de Nombres de Dominios de *Internet*

En cada dominio se puede asignar subdominios.

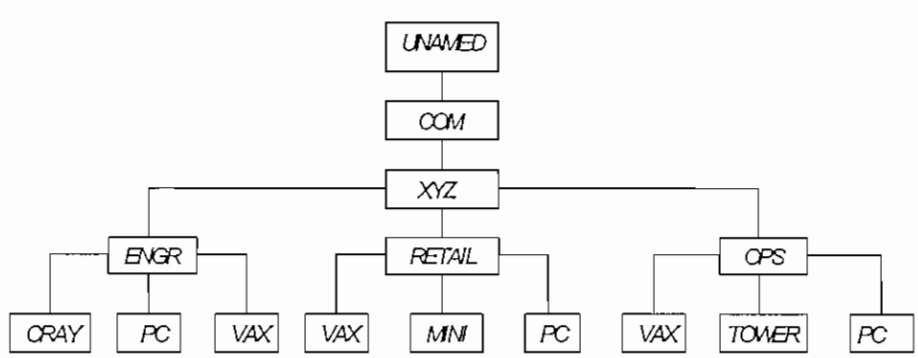


Figura 3.30 Subdominios

[11] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capítulo 8

vax.engr.xyz.com y **vax.ops.xyz.com** son máquinas diferentes por cuanto operan bajo distintos brazos del árbol y deben tener direcciones *IP* únicas.

Un Servidor de Nombres *DNS* permite el "mapeo" de nombres de dominios para determinar mediante ellos la dirección *IP* de los hosts.

Los subdominios se registran con los subdominios jerárquicamente superiores. Por ejemplo el subdominio **ops.xyz.com** se registra con el subdominio **xyz.com** donde ops.xyz.com es un subdominio de xyz.com.

Un servidor de nombres puede delegar responsabilidades a una máquina que está dentro de su dominio para que conteste todas las peticiones hechas al servidor.

3.4.2 TIPOS DE SERVIDORES DE NOMBRES

Se tienen los siguientes tipos de servidores de nombres:

Primario.- Es la primera máquina a la que se pide información.

Secundario.- Son las máquinas que responden a los requerimientos cuando el servidor primario delegó las funciones al secundario.

Cache.- Son los que pasan los requerimientos o pedidos a otros servidores de nombres.

Forwarding **(remoto).-** Es un servidor que pasa las peticiones a otro servidor de nombres y regresa la contestación al peticionario, pero no almacena una copia de la información.

Resolvers.- Es el interfaz del sistema operativo al *DNS*. Busca las respuestas a los requerimientos pasando las peticiones hacia los servidores remotos o locales.

3.5 SERVICIOS DE APLICACION

3.5.1 *TELNET* [12]

Terminal de acceso remoto que provee una conexión orientada al octeto bidireccional con el servidor remoto, con el propósito de usar una serie de servicios y aplicaciones que están presentes en el Servidor.

Para que un *host* funcione como terminal, se requiere de un proceso de Terminal Virtual de Red *NVT* el cual genera los parámetros de un terminal. Varios usuarios y procesos pueden interactuar con el módulo *NVT*.

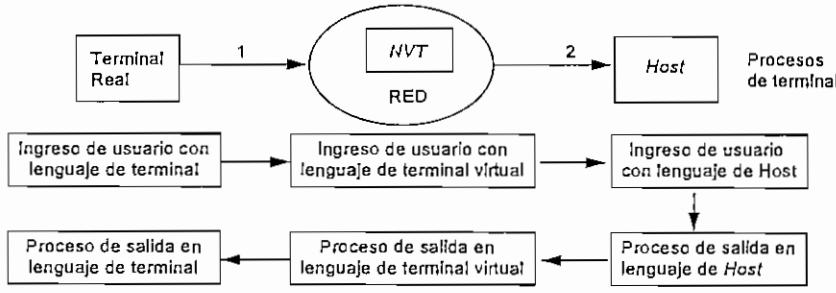


Figura 3.31 Proceso *Telnet* con terminal virtual

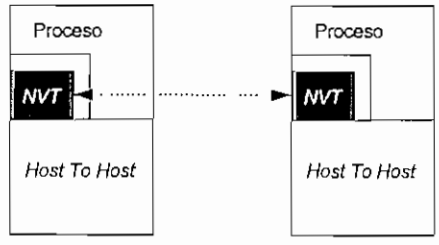


Figura 3.32 Conexión entre *hosts* mediante Terminal Virtual de Red

Telnet provee una conexión *TCP* a cualquier *host*. Ambos lados de la comunicación asumen que su enlace es mediante *NVT*.

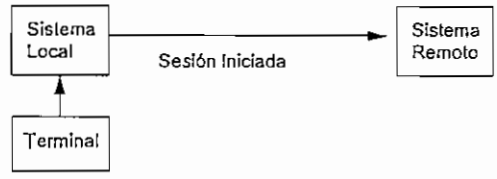


Figura 3.33 Negociación *Telnet*

Los interfaces del proceso *Telnet* se describen en el Anexo 1.

[12] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capitulo 9

3.5.2 PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS *FTP* [13]

Mueve archivos de una computadora a otra. El comando ***ftp > get rfile.txt local.txt*** trae un archivo remoto **rfile.txt** y lo copia en el **local.txt** del sistema, en el cual el comando fue realizado, en este caso el *host* B.

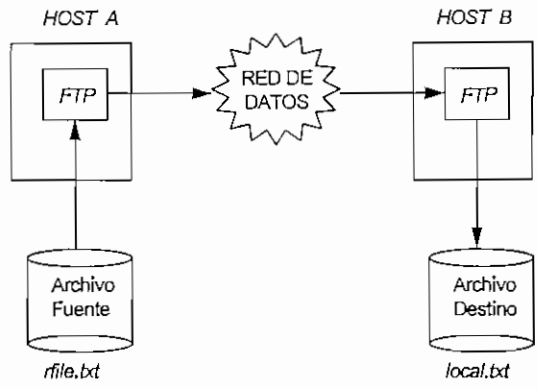


Figura 3.34 Proceso *FTP*

FTP provee controles de autenticación, por lo cual el usuario debe enviar el *login* y el *password* a la máquina remota.

FTP establece una conexión dual entre el cliente y el servidor como se indica en la figura 3.35:

. Una conexión realiza la transferencia de datos.

. La otra conexión controla la transferencia, mediante comandos y respuestas.

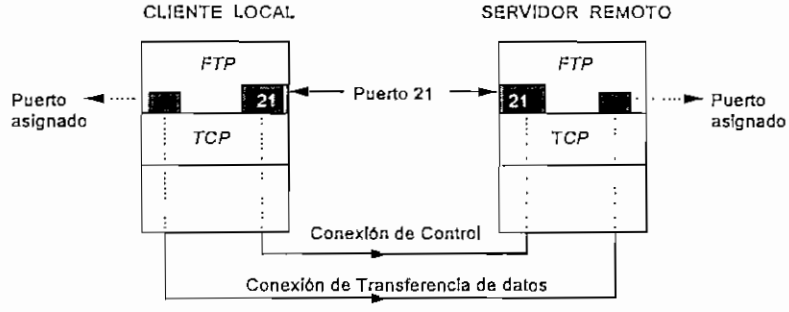


Figura 3.35 Conexión Dual *FTP*

FTP utiliza *TCP* para tener una conexión confiable y *Telnet* para su control, mediante el siguiente procedimiento:

1.- El Cliente se conecta al Servidor desde un número de puerto de protocolo asignado.

---

[13] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capitulo 9

2.- En el servidor, un proceso escucha en el puerto 21, el requerimiento *FTP* del cliente.

3.- El servidor genera un proceso esclavo que acepta y realiza el control de la conexión.

4.- Un proceso separado maneja la conexión para transferencia de datos.

5.- El servidor asigna al usuario un puerto sin uso, en su máquina para la transferencia de datos.

En la figura 3.36 el cliente C establece conexiones de control en forma independiente al servidor A y B, controlando desde C la transferencia de archivos de A hacia B.

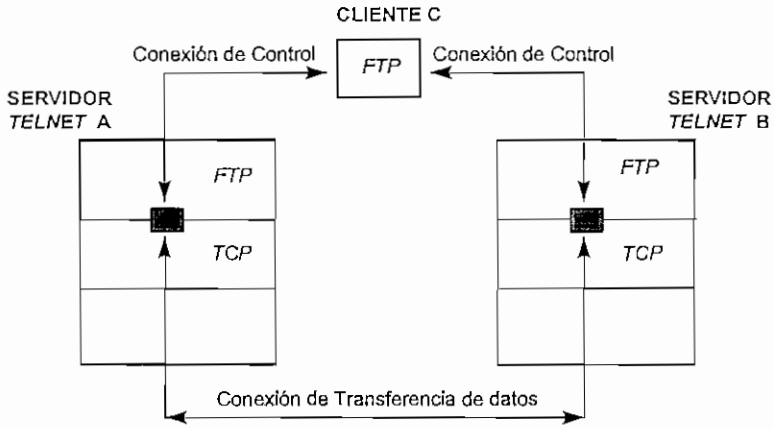


Figura 3.36 Enlace Doble con Conexiones de control *FTP* independientes

3.6 MODELO CLIENTE / SERVIDOR [14]

Este modelo representa la interacción entre aplicaciones. Un cliente que está ejecutando un programa envía una petición de servicio a un servidor. El servidor procesa el pedido y devuelve el resultado al cliente.

En *UNIX* los programas remotos del servidor se denominan procesos. *Network File System* (*NFS*) permite compartir en línea archivos, en forma transparente para el usuario .

NFS consta de tres partes:

- *NFS* - que es el protocolo propiamente dicho.
- *RPC* - Llamada a Procedimientos Remotos
- *XDR* - Representación de datos externos

[14] *TCP/IP Technical Concepts, Open Strategies,Inc. and NCR*, Capitulo 7

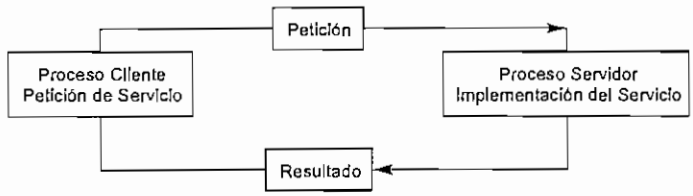


Figura 3.37 Proceso Cliente / Servidor

3.6.1 *REMOTE PROCEDURE CALL (RPC)*

RPC es una herramienta para crear programas Cliente - Servidor , el cual es independiente del protocolo de transporte por cuanto se encuentra en la capa Sesión.

Da las bases para el intercambio de mensajes en todas las aplicaciones *NFS*.

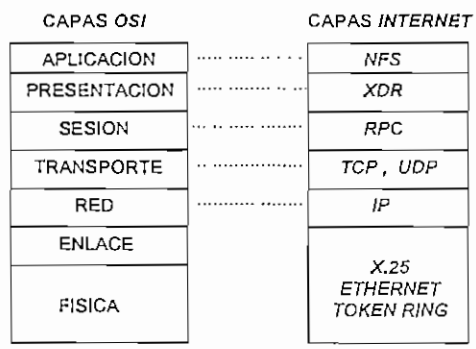


Figura 3.38 Ubicación de *RPC* en el modelo *OSI* e *Internet*

Si *RPC* se ejecuta con *UDP* como protocolo de transporte, el programa *RPC* se identifica con un número de puerto. *UDP* no hace reconocimientos de recibo, no ordena los mensajes, ni controla la velocidad de transmisión, y los datos generados en *RPC* pueden ser perdidos o llegar fuera de orden.

Si *RPC* se usa con un protocolo confiable como *TCP*, la aplicación deduce del mensaje de *"reply"* que el proceso se ejecutó exactamente una vez. Pero si recibe un *"no reply"*, éste no puede asumir que el proceso remoto fue ejecutado. Por tanto con protocolos orientados a conexión, la aplicación necesita manejo de *"time outs"* y reconexión cuando el servidor falla.

3.6.2 *LOCAL PROCEDURE CALL*

El modelo de Llamada a Procesos Locales *LPC* es similar al modelo *RPC*. En *LPC*, el programa que llama, coloca argumentos para un procedimiento en alguna localidad específica. Los resultados del proceso son extraídos de la localidad y el programa puede continuar.

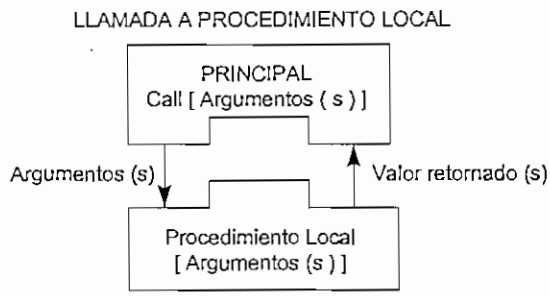


Figura 3.39 Llamada a un Procedimiento Local, *LPC*

3.6.3 PROCESO CLIENTE

El proceso Cliente envía un mensaje de llamada *RPC* al proceso Servidor y espera por una contestación o *reply*. Los procesos servidores emiten los resultados en mensajes *RPC* de respuesta.

Una vez que el cliente recibe el mensaje de respuesta , los resultados del procedimiento son extraídos y el programa que llama reanuda su operación.

3.6.4 PROCESO SERVIDOR

El proceso Servidor está inactivo pero permanece latente, esperando el arribo de un mensaje de llamado *RPC*. Cuando éste llega, los procesos servidores extraen los parámetros del procedimiento, calculan los resultados, envían los mensajes de respuesta, y esperan por el siguiente mensaje de llamado.

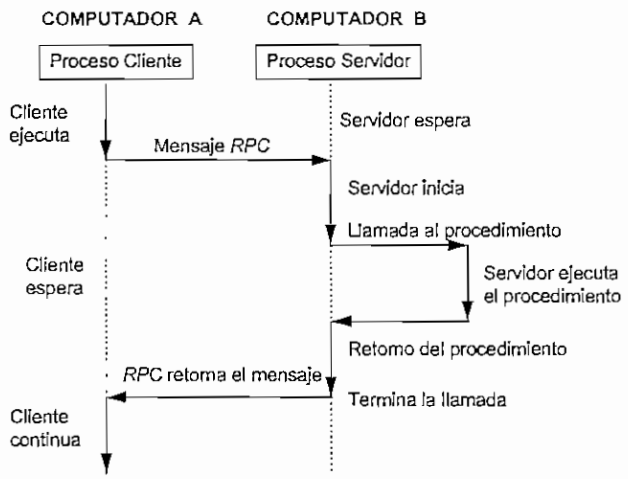


Figura 3.40 Ejecución de un *RPC*

3.7 ENCAPSULAMIENTO *IP* EN X.25 Y *FRAME RELAY*

3.7.1 ENCAPSULAMIENTO IP SOBRE X.25 [15]

Los datos *IP* son encapsulados mediante el **Encapsulamiento** ***IP RFC877*** , o ***RFC1356*** que es la versión actualizada, para que los datos puedan ser transmitidos a través de redes *X.25*. La utilización de *IP* se establece en la capa de red X.25 mediante el campo de Identificación de Protocolo. El datagrama *IP* es enviado como una Unidad de Dato de Protocolo *PDU*.

El campo *Call User Data (CUD)* del paquete, contiene un octeto llamado *Network Layer Protocol Identifier (NLPID)* que identifica el protocolo de red encapsulado sobre el circuito virtual X.25, el cual para el caso de *IP* tiene el valor (11001100) o **CC** en hexadecimal. *IP* es encapsulado en un circuito virtual, abierto con el valor **CC** del *CUD* .

El ancho de banda se mejora al utilizar el menor número de protocolos encapsulados en la red X.25 .

Si el paquete *IP* es más grande que el *MTU (Maximum Transfer Unit)* configurado en el *PDU* X.25, el datagrama se fragmenta. Para que no haya fragmentación, la longitud del datagrama debe ser de 1500 octetos y la longitud del *PDU* de 1501.

[15] *Multiprotocol Interconnect on X.25, Malis, Robinson, & Ullmann*

Los protocolos de las capas superiores a la red *IP*, como *TCP* o *UDP* no son afectados en la transmisión de los paquetes.

El formato del encapsulamiento *IP* se muestra a continuación en la figura 3.41.

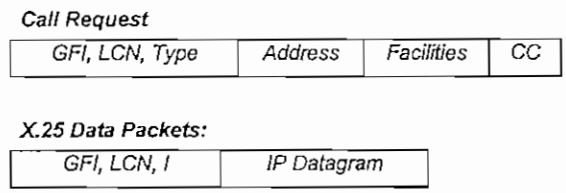


Figura 3.41 Encapsulamiento *IP* sobre X.25

Como se observa en la figura 3.42, el adaptador de *WAN* en los ruteadores X.25 encapsula los datos con el encapsulamiento *RFC 877* definido para X.25.

El datagrama IP va en el área de datos del paquete X.25.

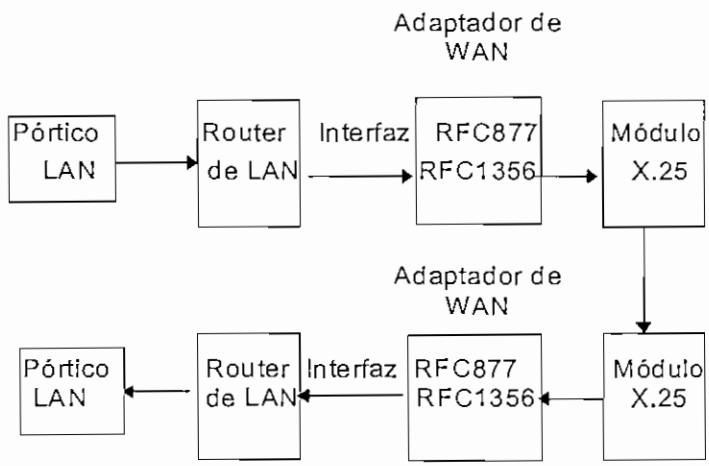


Figura 3.42 Encapsulado / Desencapsulado IP en X.25

3.7.2 ENCAPSULAMIENTO *IP* EN *FRAME RELAY*

Para el caso de *Frame Relay* el encapsulamiento empleado es el ***RFC1294*** o el ***RFC1490*** que es una versión mejorada. El Adaptador de *WAN* del ruteador añade una cabecera al paquete al frente del dato, usando la Identificación del Protocolo de Nivel de Red (*NLPID*) que para el caso de *TCP/IP* es 0xCC.

Dirección Q.922	Control 0x03	*NLPID* 0xCC	Paquete o fragmento de paquete *IP*	*FCS*

Figura 3.43 Formato de Encapsulamiento *IP* en RFC1294 [16]

Luego de esto, el paquete pasa al módulo *Frame Relay* para ser enviado al ruteador remoto donde se desencapsula el dato y pasa al módulo de LAN, como se indica en la figura 3.44.

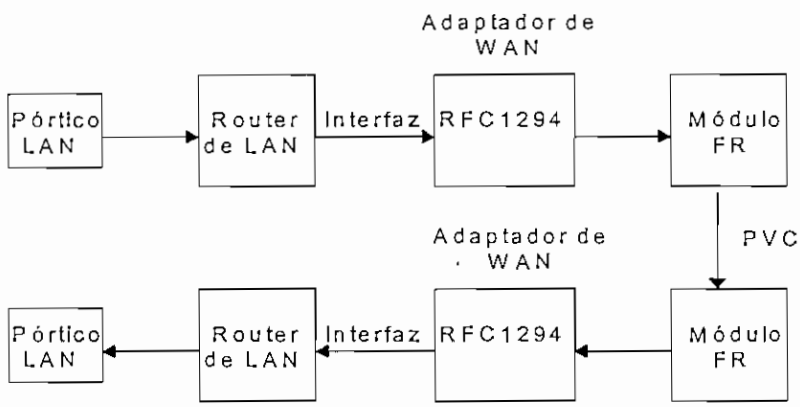


Figura 3.44 Encapsulamiento *IP* en *Frame Relay*

El datagrama IP viaja en la parte de datos de la trama *frame relay* a través de los circuitos permanentes creados en el enlace entre ruteadores.

Frame Relay ofrece servicios de transmisión de datos más rápidos que X.25, razón por la cual las redes X.25 migran hacia *Frame Relay* a través de Intercambiadores de paquetes de X.25 a *Frame Relay* como se describe en el capítulo 5.

[16] 6500 Series Routing, Motorola

CAPITULO IV SERVIDORES DE RED [1]

Este capítulo describe la arquitectura de los Servidores de red y realiza un estudio de los principales elementos que influyen en su funcionamiento como: buses internos, memoria, procesador, tarjetas controladoras de red, arreglo de discos.

4.1 FUNDAMENTOS TECNICOS DE UN SERVIDOR DE RED

El Servidor es el elemento más importante en el funcionamiento de una red; realiza las siguientes tareas:

- Comparte recursos como discos, impresoras, *plotters*, etc.
- Ejecuta aplicaciones con bases de datos corporativas, correo electrónico.
- Permite establecer enlaces de comunicaciones.

4.1.1 TIPOS DE SERVIDORES

. Servidor de Impresión

Comparte una o más impresoras con muchos usuarios, para lo cual emplea el DMA[2] del puerto de impresión y un gran espacio en disco para imprimir los archivos que se van ubicando en una cola . El beneficio es que reduce el costo de impresión

. Servidor De Archivos

Comparte datos, aplicaciones, dispositivos de almacenamiento como discos, *CDs*, etc.

Utiliza en forma intensiva los discos y los interfaces de comunicaciones.

Centraliza el almacenamiento de datos y respaldos; realiza un control de virus y da seguridad e integridad a los datos.

. Servidor de Comunicaciones

Permite la conexión entre usuarios dentro de una red local *LAN* y entre sistemas remotos externos a través de enlaces de Acceso Remoto.

---

[1] *IBM Server Technical Training, IBM PC Institute*
[2] *DMA= Direct Memory Access*

. Servidor de Aplicaciones

Es un servidor que realiza grandes cantidades de cálculos, con el uso intensivo de los componentes *I/O* como *CPU*, *RAM*, interfaces *I/O* de disco. Esta clase de servidor debe garantizar la seguridad e integridad de los datos.

4.1.2 CARACTERÍSTICAS DE UN SERVIDOR

Un servidor debe tener los siguientes atributos:

- Integridad de los datos
- Seguridad del sistema
- Disponibilidad del sistema
- Prestaciones
- Expandibilidad / Actualizaciones
- Facilidad de configuración y uso
- Estética.

En cuanto a su arquitectura las características son:

- Bus I/O avanzado
- Controlador de memoria
- Sistema de Procesador
- Subsistema de discos
- Adaptador de red

a) BUS I/O DE UN SERVIDOR

El bus es la columna vertebral de un servidor, el mismo que provee el camino para la transferencia de los datos del procesador a los otros subsistemas, debiendo por lo tanto estar protegidos contra bombardeos de partículas alfa y emisiones electrónicas de otros dispositivos.

La flexibilidad de los buses debe permitir la implementación de diferentes productos e incrementar las prestaciones y funcionalidad de otros subsistemas.

• **Bus Maestro**

Son subsistemas inteligentes que realizan el control del bus, liberando al procesador de operaciones de control y transferencia de datos.

- Permite el trabajo en paralelo e independiente de subsistemas inteligentes (disco y *LAN*) y *CPU*, por cuanto los adaptadores tienen su propio *DMA* y procesador.
- Incrementa funciones y capacidades en un servidor.
- Eficiente comunicación entre sistemas.

Operación del Bus Maestro

1.- El *CPU* almacena un comando en un área de instrucción de memoria

2.- El *CPU* indica al bus maestro que hay una serie de comandos en memoria en una dirección particular y continua ejecutando otros comandos.

3.- El adaptador de bus maestro accesa a memoria, toma el comando y lo empieza a ejecutar. (La instrucción puede ser : Extraer un dato de un disco y enviarlo a memoria).

4.- El bus maestro realiza las operaciones necesarias para localizar el dato en disco.

5.- El dato es transferido a memoria a través del *DMA* (bus maestro) sin usar el controlador *DMA* del sistema.

6.- El bus maestro indica al *CPU* que el dato está en memoria y la transferencia se completa.

7.- El *CPU* procesa el dato.

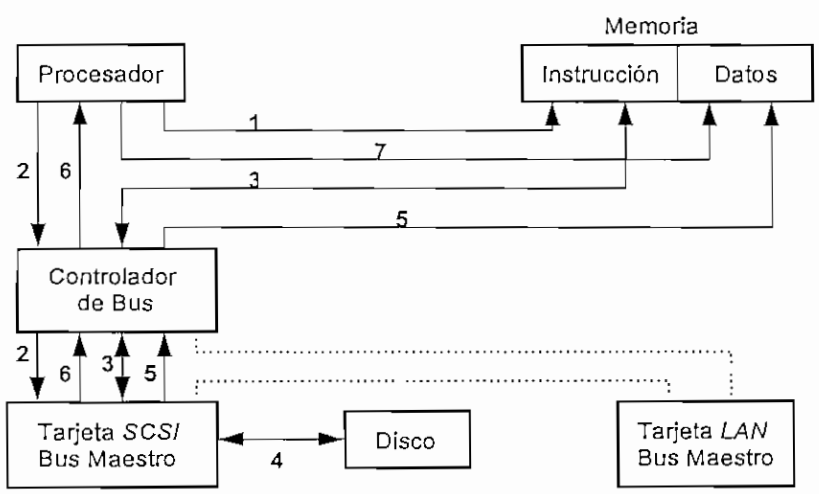


Figura 4.1 Forma de operación del Bus Maestro

El uso de múltiples *DMA* en dispositivos *I/O* permite dar más tiempo al procesador para realizar otras tareas.

• **Buses Locales**

Son usados para conectar componentes planares y dispositivos de alta velocidad, en donde se realizan operaciones *I/O* de almacenamiento y comunicaciones intensivas.

Este tipo de bus se denomina *PCI (Peripheral Component Interconect)* y utiliza todos los recursos que no están ocupados por otros buses y dispositivos.

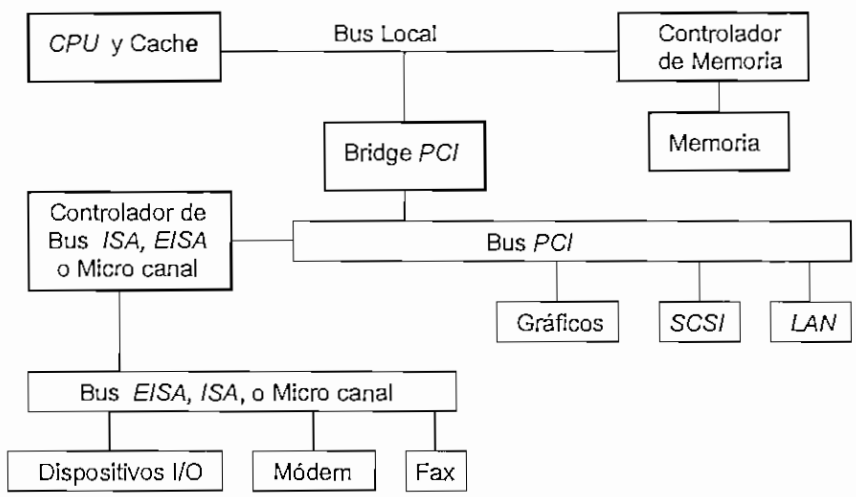


Figura 4.2 Disposición de los buses locales

- Provee alta velocidad de transferencia de datos entre los dispositivos del board (memoria y *CPU*) y algunos módulos de expansión.
- La velocidad del bus es de 33 MHz
- La velocidad de transferencia es 132 MB/s en buses de 32 bits y 264 MB/s en buses de 64 bits.
- Es independiente del procesador
- Soporte total de bus maestro
- Permite de 2 a 3 slots de expansión.
- Hay integridad del dato con chequeo de la paridad del bus.
- Los adaptadores se configuran automáticamente.
- Requieren de un *bridge* para manejar más dispositivos.

- **Buses Micro Canal**

Los buses microcanal son empleados en la mayor parte de servidores de red y tienen las siguientes características:

- Arquitectura de 16, 32 o 64 bits.
- Transferencia hasta 160 MB/s
- Soporta bus maestro
- Es independiente del tipo de procesador, por ser un bus asincrónico.
- Gran número de canales *DMA*
- Niveles de interrupción compartidos.
- Usa software para configurar los adaptadores.
- Integridad y confiabilidad de los datos, mediante el chequeo de paridad del bus.

El chequeo de sincronismo del canal provee detección y corrección de errores con dispositivos que manejan bus maestro. Cuando el dato es incorrecto, el dispositivo receptor pide que sea enviado nuevamente, con lo cual se reduce los errores y corrupción de datos.

Para calcular la velocidad de transferencia del bus de datos se emplea la siguiente fórmula:

Máxima capacidad del bus de datos en Mbps=Frecuencia(MHz)xAncho de banda (bits)

Para microcanal en el que tanto el bus como el sistema operativo es de 32 bits se tiene:

10 MHz x 32 bits= 320 Mbits/s

320/8 = 40 MB/s

Como se observa en la figura 4.3, para el caso del bus **microcanal *streaming*** de 64 bits, cada 100 ns se transmiten 8 bytes de datos, para lo cual se colocan datos también en el bus de direcciones, de manera que se incrementa la velocidad de transferencia a 80 MB/s.

Si se duplica la velocidad del reloj a 20 MHz, la transferencia de datos llega a 160 MB/s

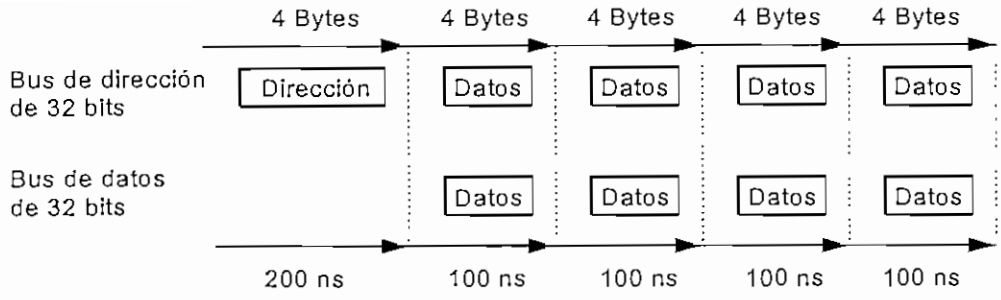


Figura 4.3 Transmisión de datos en bus micro canal *streaming*

b) MEMORIA DEL SERVIDOR

Se debe dimensionar y distribuir la memoria en función del sistema operativo, aplicaciones y procesos que se ejecutan en un servidor.

Las memorias más utilizadas en los servidores son:

- Memorias *ECC (Error Correction Code)*, que proveen chequeo y corrección de errores de un bit simple, producidos por el bombardeo de partículas alfa, beta y gama, deterioro del *SIM* (oxidación y calor). Detecta todos los errores de 2 bits pero corrige solo algunos.
- Memoria *ECC* con Paridad, son memorias que controlan de mejor manera la detección y corrección de los datos.

• Bus Dual de Memoria

Se accesa a memoria en forma independiente, como se indica en la figura 4.4:

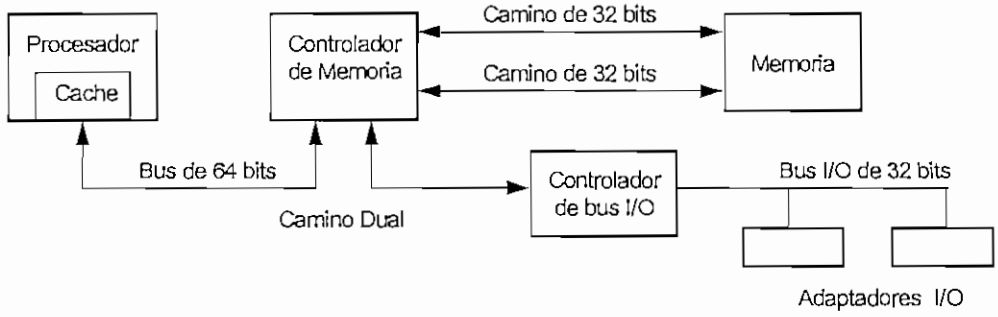


Figura 4.4 Bus dual de memoria

La memoria puede entrelazarse en dos vías, en donde se tiene accesos independientes a los bancos, pero en forma secuencial cuando se transmite en forma de ráfaga. Con este método el *CPU* y los dispositivos *I/O* tienen accesos más rápidos a memoria.

El *CPU* no espera a que salga el dato de un banco, sino que puede accesar al otro banco para procesar otro dato.

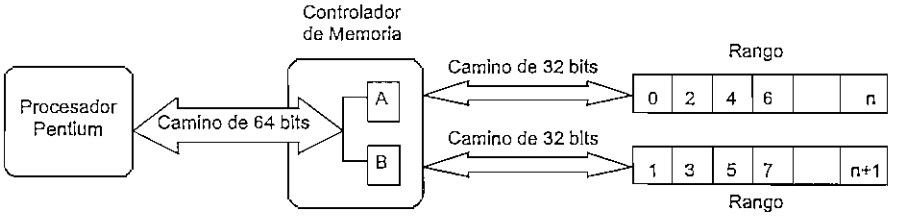


Figura 4.5 Memoria entrelazada de dos vías

c) ARQUITECTURA *SINCHRO STREAM*

Es un método que sincroniza la operación de dispositivos lentos y veloces y controla el flujo de datos a los mismos, asegurando que trabajen en sus niveles óptimos.

Envía los datos a diferentes destinos al mismo tiempo.

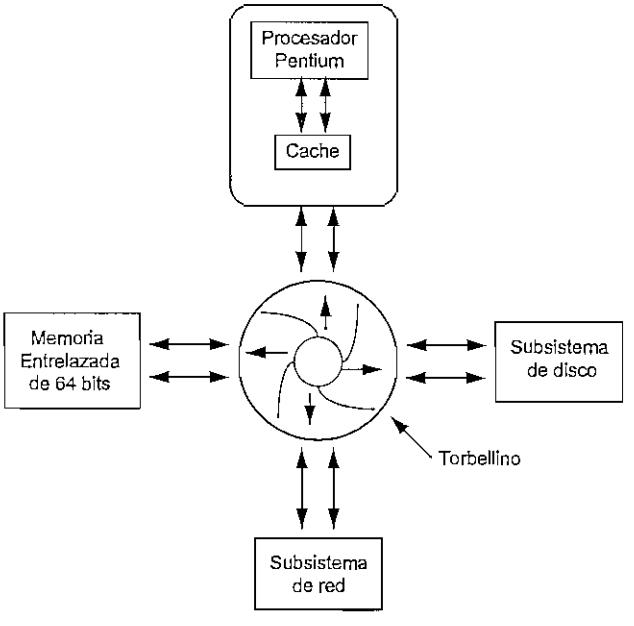


Figura 4.6 Arquitectura *Synchro Stream*

Mientras un Subsistema realiza una operación, los otros subsistemas pueden realizar otras tareas en forma independiente, todas las cuales serán completadas en un ciclo de sincronismo. Con este método se elimina la competencia entre las tarjetas con bus maestro y el *CPU* por el bus de datos, evitándose un cuello de botella por la sobrecarga del mismo.

Predice los datos que necesita un dispositivo y los toma de memoria antes de que sean requeridos. Una vez requerido el dato, éste es presentado al dispositivo, con lo que los tiempos de espera se reducen al mínimo.

d) PROCESADOR

El procesador es el subsistema que realiza las tareas más complejas en un servidor. Los procesadores empleados en la actualidad son los *Pentium* que sobrepasan los 100 MHz de velocidad y cuentan con memoria *RAM* cache para que dispositivos veloces almacenen datos y/o instrucciones traidas de dispositivos lentos.

Se tienen los siguiente niveles de cache:

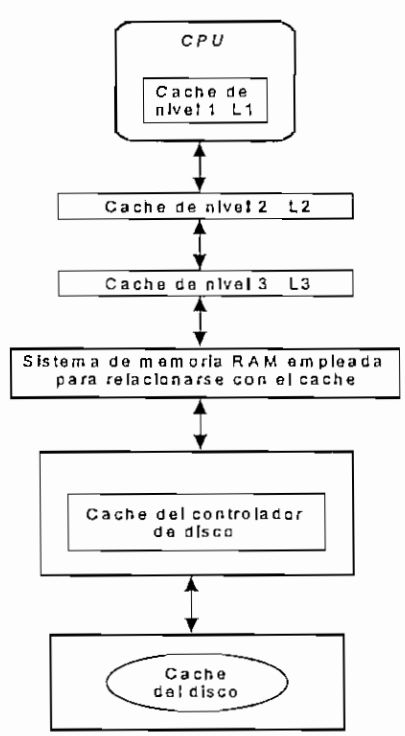


Figura 4.7 Disposición de la memoria *cache* en los diferentes niveles de procesamiento

La memoria cache es 10 veces más rápida que la memoria convencional, por lo que basta utilizar pequeñas cantidades de ésta para incrementar las prestaciones del *CPU*.

El nivel óptimo del cache externo de nivel 2 es 128 KB. Si se añade más cache no se mejora mucho en el performance del *CPU* como se muestra en la figura.

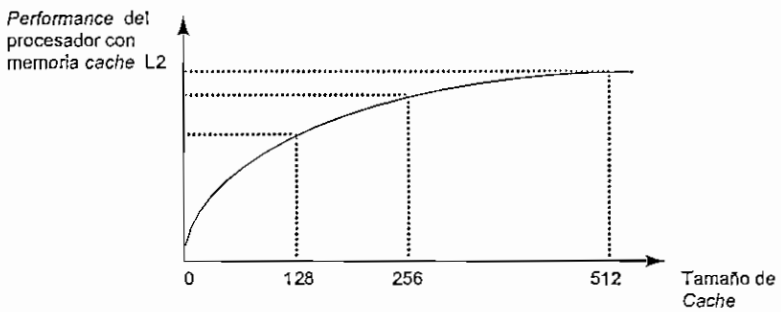


Figura 4.8 *Performance* del procesador con la memoria *cache*

4.1.3 MULTIPROCESAMIENTO

El multiprocesamiento se refiere a cuando el servidor opera con dos o más *CPUs* para mejorar el manejo de bases de datos y aplicaciones cliente / servidor con gran número de usuarios. Los sistemas operativos deben manejar multiprocesadores como es el caso de *UNIX, NT, OS2.*

a) MULTIPROCESAMIENTO SIMÉTRICO

Es un sistema en el cual los procesadores tiene las mismas velocidades y pueden accesar a la memoria disponible para ejecutar por separado una parte de cada aplicación.

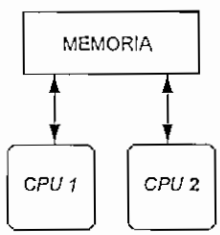


Figura 4.9 Multiprocesadores Simétricos fuertemente acoplados

Al añadir un procesador simétrico, se incrementa la velocidad del proceso en un 50% por cuanto los cuellos de botella se producen en la memoria compartida.

b) MULTIPROCESAMIENTO ASIMÉTRICO

En este caso los procesadores pueden tener velocidades diferentes y no requieren estar acoplados, por cuanto cada *CPU* tiene memoria independiente para realizar tareas y operaciones por separado.

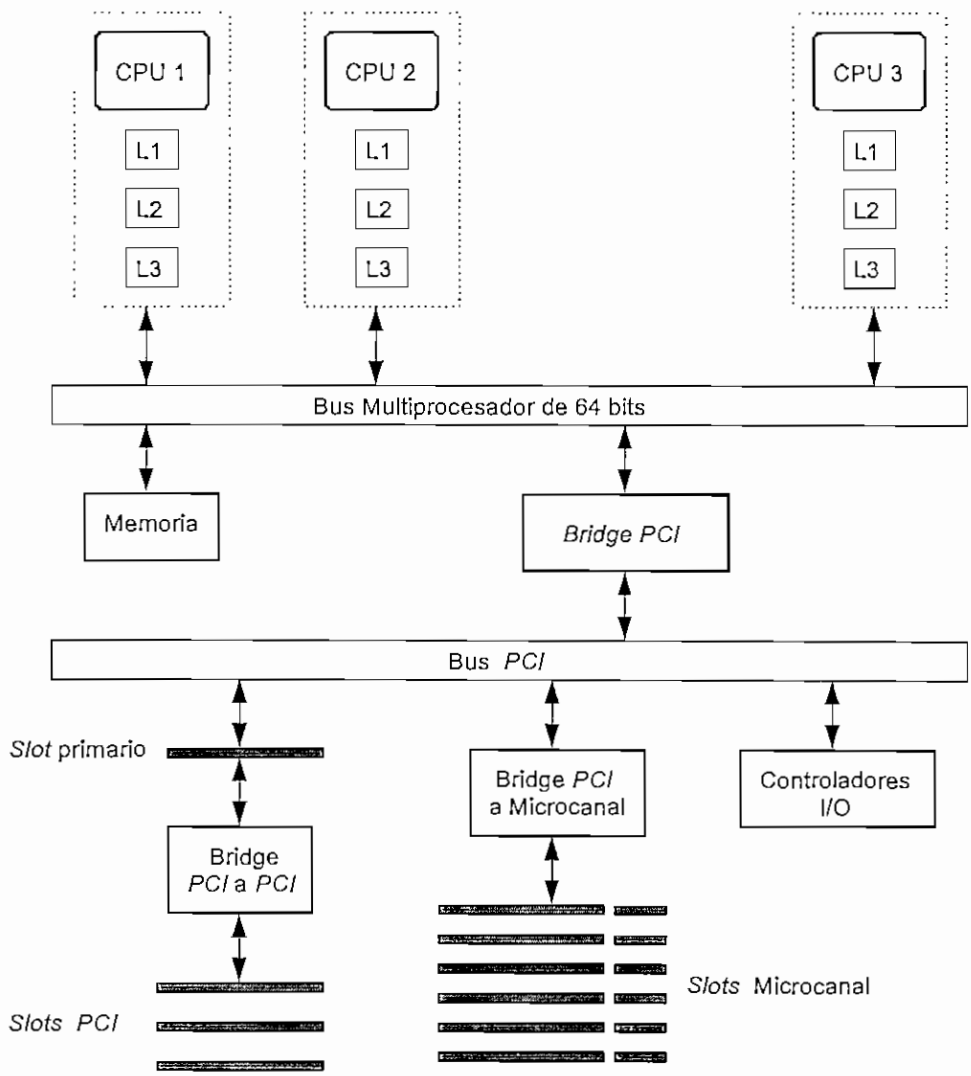


Figura 4.10 Multiprocesadores asimétricos Conexión de Procesadores de diferentes velocidades

Las caches siempre deben actualizarse para que los datos empleados sean coherentes, ya que se puede tomar los datos del *cache* de una *CPU* para realizar un proceso en otra *CPU*.

4.2 DISPONIBILIDAD Y TOLERANCIA A FALLAS DE UN SERVIDOR

La tolerancia a fallas es la habilidad de un sistema computacional para resistir a condiciones que podrían ocasionar daños, como por ejemplo pérdida de energía o fallas mecánicas en los discos duros.

Una alta tolerancia a fallas va asociada con una elevación de costos en el equipo.

Para evitar los daños se debe contar con sistemas de protección de la información tales como:

- Fuentes de Poder Ininterrumpibles *UPSs,* que permiten al servidor seguir trabajando por un tiempo suficiente (10 a 20 minutos), para que guarde sus datos y realice el cierre adecuado del sistema, cuando el sistema de energía principal falla. Además protege de voltajes altos, bajos y ruido en la línea de alimentación.
- Servidores redundantes
- Arreglos de discos *RAIDs*
- Respaldos de información

4.2.1 SERVIDORES REDUNDANTES

Es un servidor en el que se puede instalar algunos componentes y mantenerlos como respaldo de otros que pueden fallar, como por ejemplo:

- Fuentes de poder
- Controladores y unidades de disco
- Procesadores
- Canales y adaptadores de entrada / salida
- Adaptadores de red *LAN*
- Memoria y controladores de memoria

Sin embargo por ser muy caros, se lo debe realizar sólo en máquinas estratégicas.

4.2.2 SERVIDORES DUALES

Esta solución tiene dos servidores con el mismo subsistema de discos de modo que si uno de ellos falla, el otro puede arrancar con el arreglo de discos de la máquina que falló.

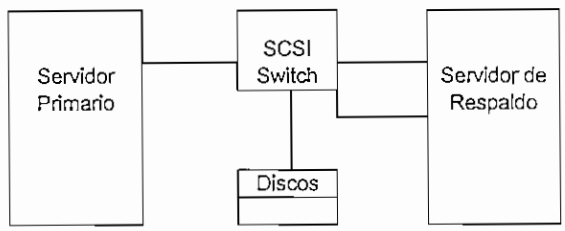


Figura 4.11 Servidores Duales

La conmutación de un equipo a otro se realiza empleando un software de detección de fallas, el cual puede operar a través de interfaces *SCSI* , seriales y de red como *Ethernet* .

4.2.3 SERVIDORES ESPEJO

Son servidores que tienen *hardware* y *software* idénticos y se comunican mediante un nexo de alta velocidad a través del cual el equipo primario envía mensajes al secundario sobre su estado de actividad.

El servidor secundario mantiene una imagen espejo de memoria y de disco del primario, por lo que la información se graba tanto en el uno como en el otro servidor. Cuando el primario falla , el equipo de respaldo entra a funcionar inmediatamente sin que se detengan los procesos.

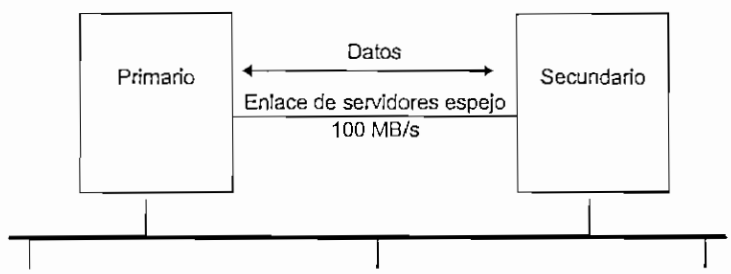


Figura 4.12 Conexión de servidores espejo a través de red *Ethernet*

Cuando el primario entra a funcionar nuevamente, se realiza una resincronización de los dos servidores.

4.2.4 ARREGLO REDUNDANTE DE DISCOS INDEPENDIENTES *RAIDs* [3]

Es un método que permite utilizar múltiples discos en forma de matriz para incrementar la disponibilidad, performance (prestaciones, utilidad) y capacidad de un servidor. Los arreglos son vistos como unidades lógicas.

Los arreglos más importantes son:

- RAID -0
- RAID -1
- RAID -4
- RAID -5

a) *RAID* - 0

Es un método rápido y de menor costo en el cual los datos son distribuidos en franjas a través de todos los discos, por lo que no tiene tolerancia a fallas y tampoco integridad de los datos debido a que no realiza corrección de errores.

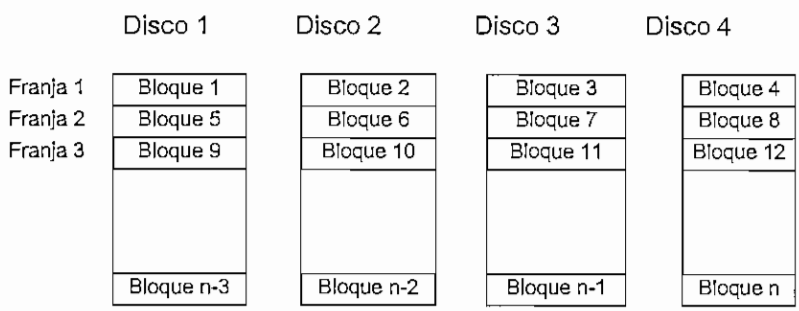


Figura 4.13 Arreglo de discos *RAID* - 0

b) *RAID* -1 ESPEJO TRANSPARENTE

Los datos se escriben simultáneamente en los dos discos, de modo que si el disco falla , entra a funcionar el disco espejo.

Una parte de un dato se puede leer en un disco y la otra parte en el disco espejo, por lo que es método rápido y confiable. Sin embargo los costos se duplican.

[3] *IBM Server Technical Training, IBM PC Institute*, Capítulo 3

Figura 4.14 Disco espejo *RAID* - 1

c) *RAID* - 4

Este método graba en un disco información de paridad del bloque de datos. Cuando un disco falla, los datos de éste se obtienen de los datos de los otros discos y del disco de paridad.

El chequeo de paridad puede causar cuello de botella. Si bien es más seguro, es lento para procesos de escritura.

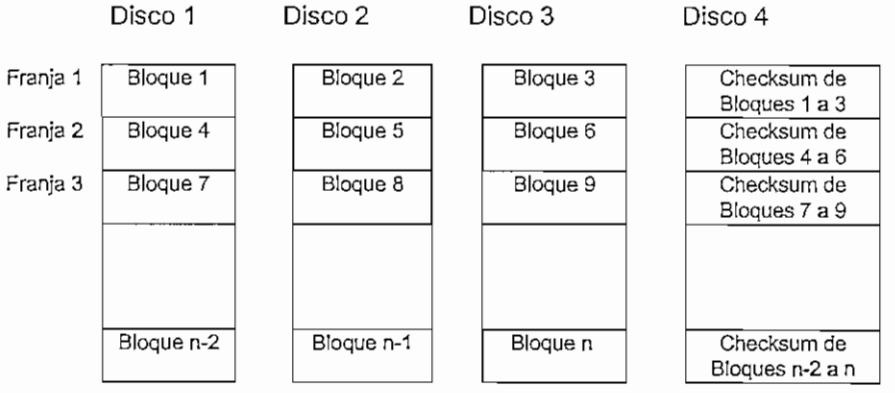


Figura 4.15 Arreglo de discos *RAID* - 4

d) *RAID* -5

Distribuye los datos y el chequeo de paridad en todos los discos, para asegurar la máxima prestación de lectura cuando se accesa a una gran cantidad de archivos en ambientes de procesos transaccionales.

Debido a los bloques de chequeo de paridad distribuidos en todos los discos, se pierde un disco pero se elimina el cuello de botella y se tiene una gran tolerancia a fallas e integridad de los datos.

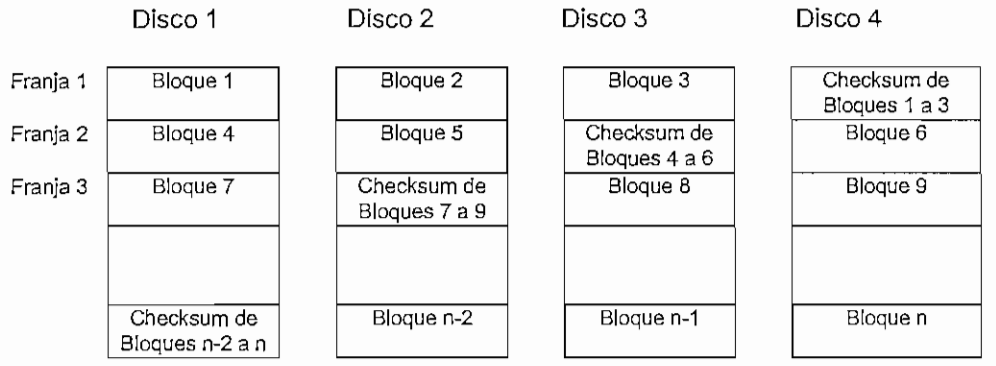


Figura 4.16 Arreglo de discos *RAID* - 5

Cuando se instala un disco en el arreglo en reemplazo de uno dañado, los datos se regeneran en función de los datos que se encuentran en los demás discos.

4.2.5 RESPALDOS

Los respaldos de datos, bases de datos y sistemas operativos en unidades de cinta son la parte más importante de la tolerancia a fallas. Si se produce un desastre total, se debería estar en capacidad de instalar un nuevo hardware y restaurar los datos desde la cinta.

El método para realizar un respaldo es **Abuelo-Padre-Hijo** en donde se realiza las siguientes tareas:

- Respaldo diario total o incremental, donde las cintas generadas son rotadas cada semana.
- Respaldo semanal total, donde las cintas se rotan cada cuatro semanas.
- Respaldo mensual total, las cintas se rotan cada año.
- Respaldo anual total, donde las cintas generadas son guardadas por cada año.
- Una vez realizado los respaldos se los verifica y prueba.

Para un servidor pequeño se tiene el siguiente listado de cintas:

- 5 cintas para respaldo diario
- 4 cintas de respaldo semanal
- 12 cintas de respaldo mensual

La cinta de diciembre se conserva por lo que las otras 20 cintas se las vuelve a utilizar.

4.3 PRESTACIONES Y AFINAMIENTO DE UN SERVIDOR

En un servidor elementos que afectan a las prestaciones (*performance*) como el procesador, la memoria, los discos, las comunicaciones, las aplicaciones pueden ser observados en tiempo real con el fin de identificar potenciales cuellos de botella en el sistema. Los resultados de la observación pueden ser almacenados para un análisis comparativo posterior.

Si se produce una pérdida en las prestaciones se puede generar alertas para que los administradores realicen las operaciones adecuadas para mejorar el estado del sistema, como por ejemplo falta de memoria, o el *CPU* está trabajando al 100% , disco falla en sectores dañados, etc. Para esto se debe especificar límites de actividad y escalas de tiempo específicos.

Se debe conocer el *hardware* que se dispone para mejorar las prestaciones, como por ejemplo memoria *RAM*, memoria cache y cómo influye cada uno de ellas en las prestaciones, y una vez instalados realizar un afinamiento con el nuevo hardware, con el fin de que el sistema utilice todos los elementos en forma equilibrada.

4.3.1 PROCESO DE AFINAMIENTO

Existen muchos factores que pueden afectar a las prestaciones del servidor como son :

- Procesador y arquitectura del bus
- Sistema de memoria
- Discos
- Topología de red y ancho de banda
- Número de servidores y usuarios
- Tipo de aplicaciones

Se debe identificar donde se producen los problemas y hacer los cambios respectivos, luego de lo cual se realizará el afinamiento del servidor.

El proceso de afinamiento se muestra en la figura 4.17

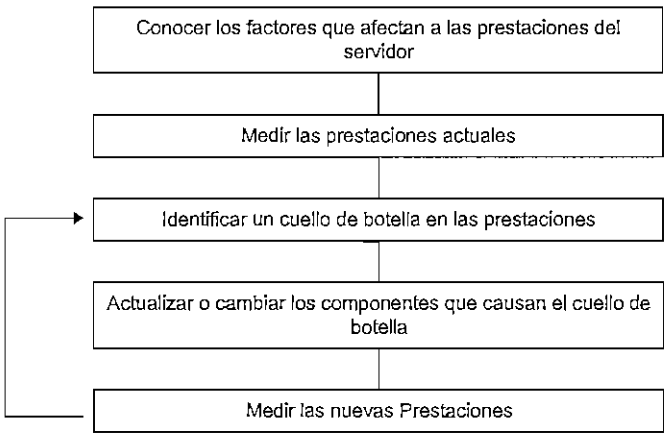


Figura 4.17 Proceso de afinamiento

En los cambios se debe considerar los beneficios en función de los costos, con el fin de justificar la inversión en los elementos adicionales.

Por ejemplo se puede observar en las siguientes figuras como influye el cambio de discos, tarjetas de red más rápidos y memoria en el desempeño de un servidor de archivos, en función del número de usuarios.

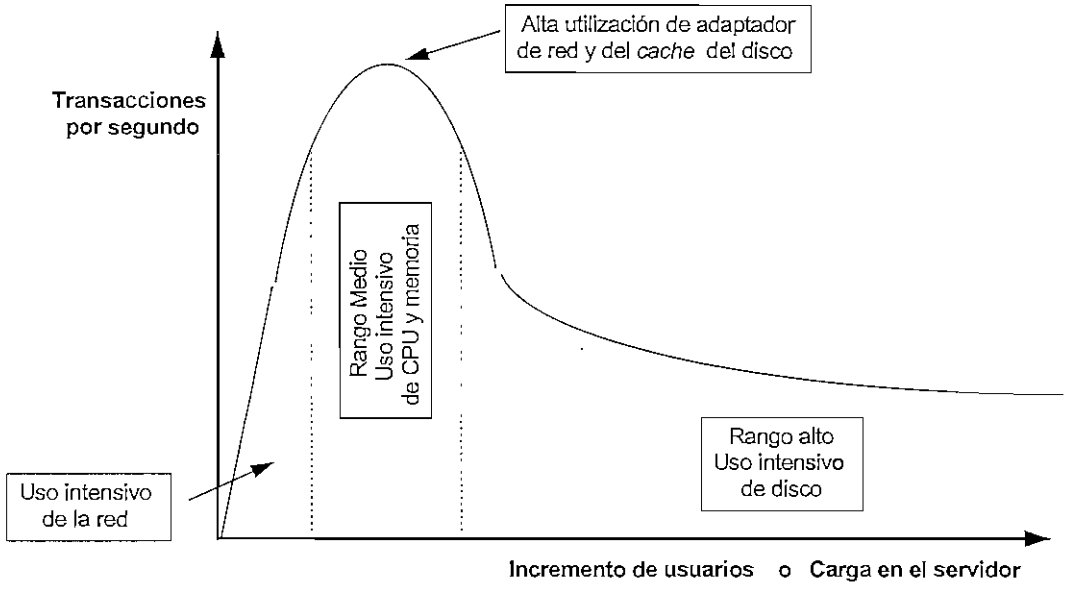


Figura 4.18 Características de *Performance* en un Servidor

Usando una tarjeta de red más rápida se puede mejorar las prestaciones, pero la carga de usuarios debe ser baja.

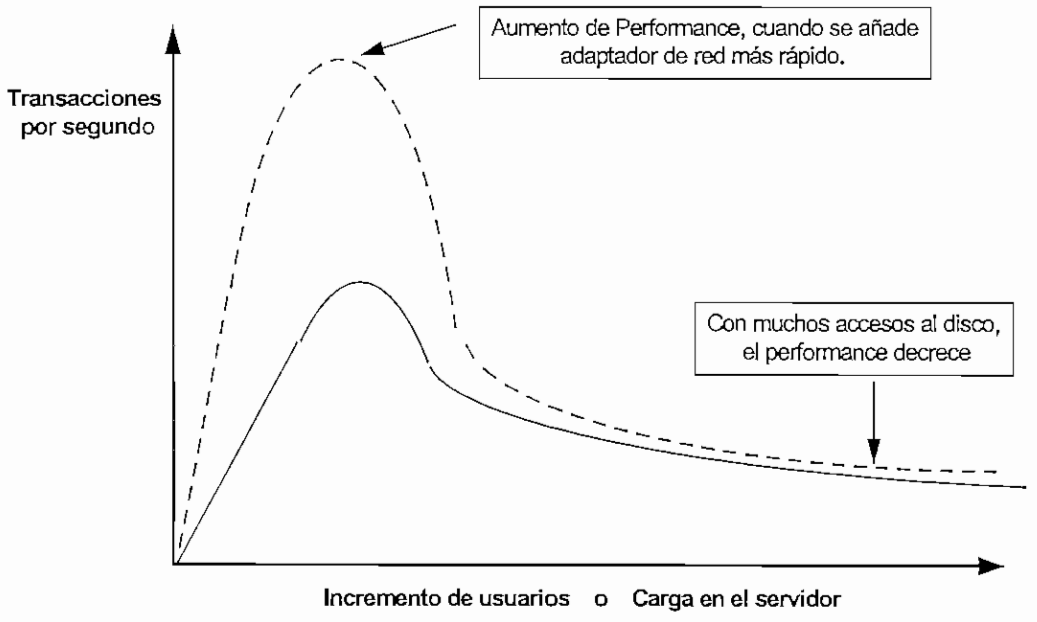


Figura 4.19 Efectos en el Servidor al añadir tarjetas de red más rápidas

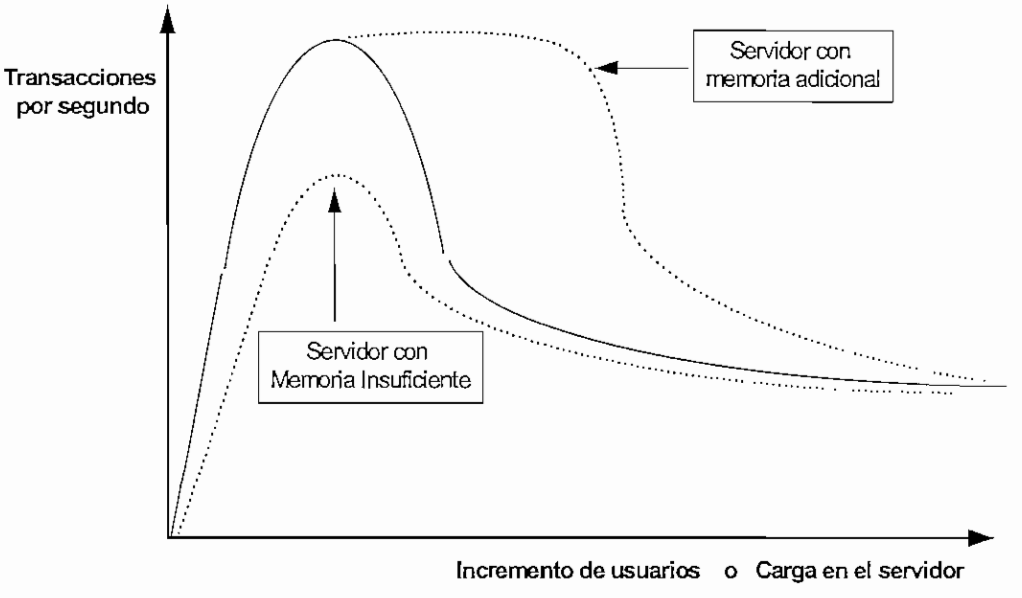


Figura 4.20 Efectos en el Servidor al remover o añadir memoria

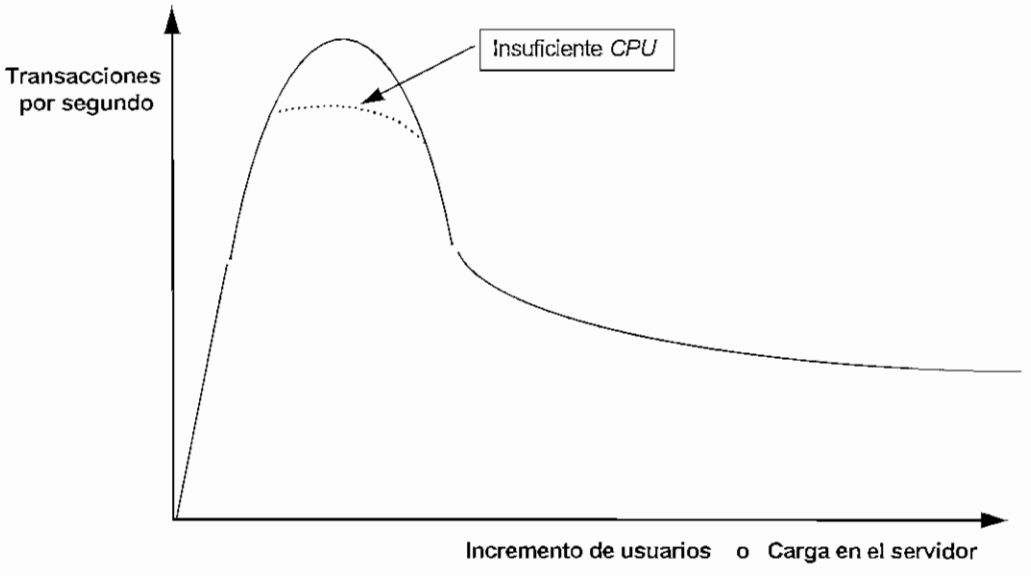


Figura 4.21 Efectos en el Servidor cuando el *CPU* es insuficiente

Cuando se pone un disco más veloz, las prestaciones se mantienen cuando se incrementa el número de usuarios.

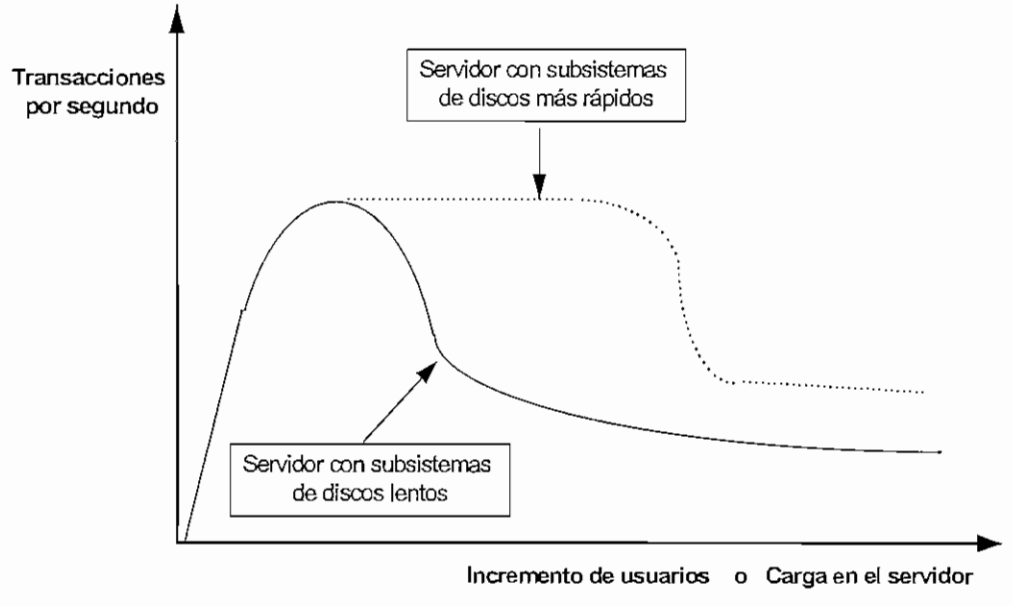


Figura 4.22 Efectos en el Servidor con subsistemas de discos rápidos

El servidor trabaja en forma óptima con pocos usuarios, por cuanto tienen poco acceso al disco, pero si se incrementa el número de usuarios , el número de transacciones por segundo que se pueden realizar se reduce, lo cual disminuye las prestaciones del servidor.

Como se observa en la figura 4.23, lo ideal es cambiar la tarjeta de red y los discos por unos más veloces, para tener un mayor número de usuarios ejecutando tareas a mayor velocidad.

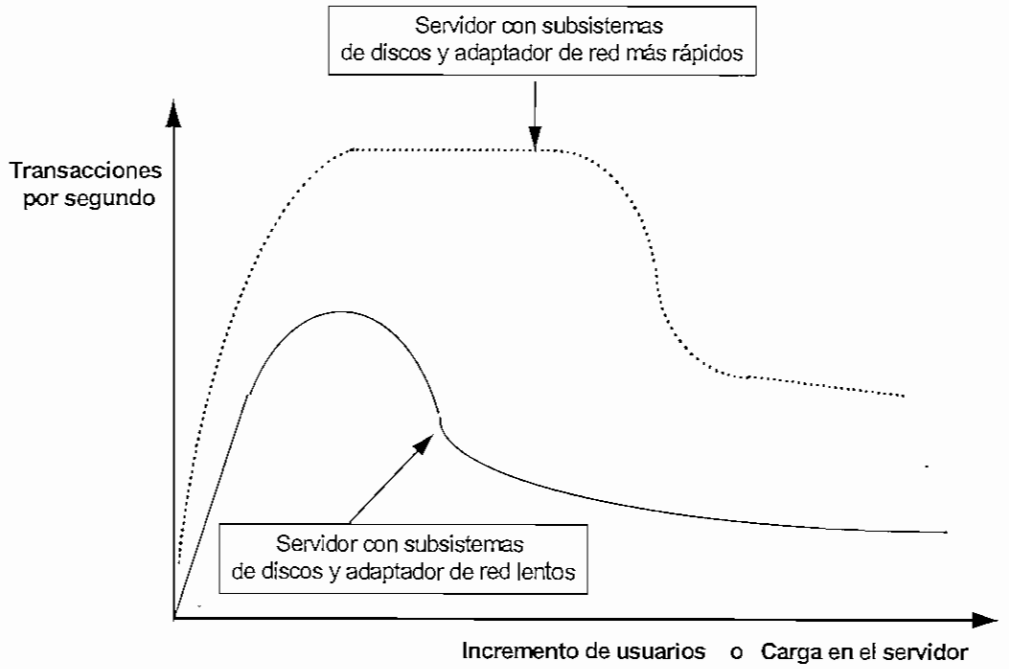


Figura 4.23 Efectos en el Servidor al añadir subsistemas de red y de discos rápidos

La figura 4.24 muestra un resumen de los principales factores que afectan a las prestaciones en un servidor

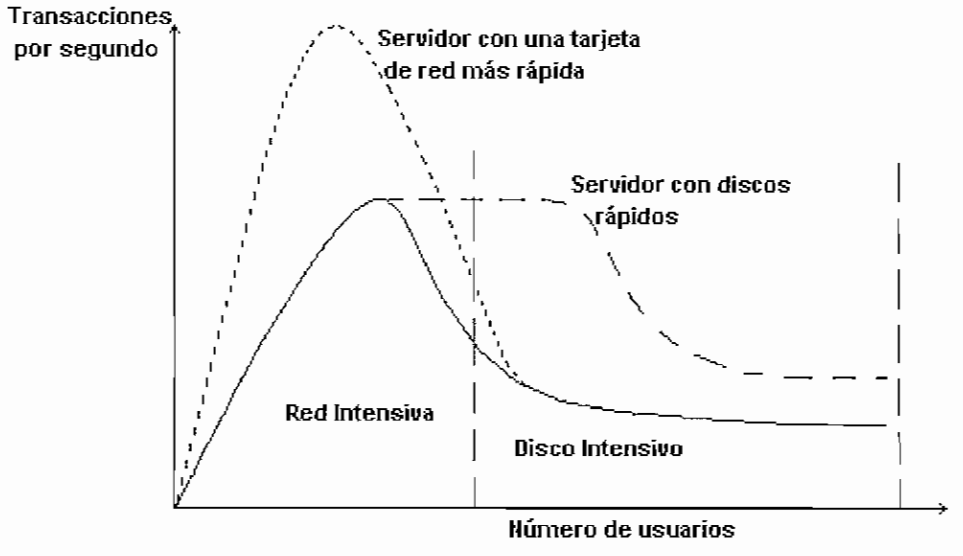


Figura 4.24 Resumen de efectos en el Servidor con los diferentes dispositivos

CAPITULO V DISEÑO DE LA RED *TCP / IP* SOBRE *X.25*

Este capítulo abarca el diseño de una red TCP/IP sobre X.25 para una institución bancaria, para lo que se realiza primero el análisis de la infraestructura existente tanto en la matriz como en las agencias para dar una solución tanto en *software* como en *hardware*. Analizados los requerimientos del sistema, se presenta una solución para una nueva red de datos que en este caso se escoge TCP/IP como protocolos de alto nivel y X.25 para la implementación de la red extendida. Se recomienda varios equipos para el funcionamiento de la red. Se realiza el diseño de la red extendida y de las redes locales tanto en la matriz como en las agencias. Finalmente se describe un caso particular para una Institución Bancaria.

5.1 ANALISIS DE REQUERIMIENTOS

En esta fase se toma en cuenta los siguientes aspectos:

a) Entidades y funciones de la institución que van a ser automatizadas

. Departamentos como: Sistemas, Soporte Técnico, Contabilidad, Financiero, Administrativo, Cámara y Tránsito, Seguridad

. Gerencias

. Cajas

. Cajeros automáticos

. Agencias

. Comunicaciones

b) Aplicaciones que se requieren y que van a correr para realizar la automatización

. Sistemas de Control para los diferentes Sistemas Operativos y Aplicaciones

. Sistemas de Control de red local y red extendida

. Aplicaciones bancarias como: Contabilidad, Cuentas Corrientes, Firmas, Ahorros, Cartera, Remesas, Custodia y garantía, Plazo fijo, Mesa de dinero, Administración de personal.

. Automatización de equipos redundantes como servidores, arreglos de discos, respaldos.

. Sistemas de monitoreo, audio y vídeo.

c) Seguridades del sistema

. Todos los sistemas y la red en general, deben ser en lo posible inaccesibles para personas externas al banco, con la finalidad de evitar daños graves en el funcionamiento de la red de datos, tanto en *software* como en *hardware*.

. Para mayor seguridad, los usuarios tienen privilegios reducidos e ingresan al sistema con Identificación y Autentificación. Los administradores en los diferentes sistemas operativos deben monitorear a los usuarios.

. Los enlaces de comunicación deben ser privados y de uso exclusivo del banco. En lo posible se establece caminos redundantes entre la agencia y la matriz para asegurar una operación permanente.

d) Confiabilidad y Disponibilidad

Se refiere a los datos que los servidores y usuarios manejan son válidos y actualizados y pueden ser utilizados en el momento en que sean requeridos.

e) Tolerancia a fallas en misiones críticas

Se debe contar con los medios necesarios para mantener el sistema siempre operativo a pesar de que cualquier elemento en la red falle. Entre los elementos requeridos se tienen:

. Servidores redundantes

. Subsistemas de discos externos

. Alimentación (*UPSs*)

. Cintas de respaldos (Unidades y *software* de manejo)

. Memoria

. Adaptadores de red *LAN* redundantes

f) Prestaciones

Se toma en cuenta las características de los equipos para su mejor desempeño en la red de datos, entre las que se encuentran:

. *CPU* (*Pentium*, multiprocesadores)

. Subsistemas de discos (arreglos internos y externos)

. Memoria (Cantidad, paridad, con corrección de errores)

. Adaptadores de *LAN* (Velocidad, tecnología)

g) Capacidad

Se refiere a la capacidad de almacenamiento que tienen los equipos tanto en disco como en memoria, para lo que se tiene las siguientes consideraciones:

. Subsistemas de discos (Tamaño, con arreglos o sin arreglos)

. Capacidad de discos

. Memoria (Tipo , cantidad)

. Número de usuarios

. Capacidad del adaptador de discos (Velocidad, canales, etc.)

h) Gestión y manejo tanto del sistema como de la red

Es necesario contar con software para monitorear y analizar los sistemas operativos, las aplicaciones y las comunicaciones.

i) Costos

Una red con tolerancia a fallas si bien es segura, incrementa los costos de equipos.

5.1.1 ANALISIS DEL ENTORNO EXISTENTE

En esta etapa los puntos más importantes son :

- **El cableado existente** en la anterior instalación, en donde se determinará el tipo de cable y las conexiones, para mediante eso ver si se puede realizar un cambio del mismo , tomando en cuenta el tiempo y el costo que implica su realización.
- **El *hardware* y software existente**
  - Tipo de Servidores y estaciones existentes, con sus respectivos adaptadores de red.
  - Los Sistemas Operativos y Aplicaciones con los que la entidad está trabajando

El Banco opera originalmente como una Institución Financiera, en base a un modelo Multiusuario que se muestra en la figura 5.1, cuyas características son:

- Dos servidores *SANYO* 3380 en la matriz Quito, cuya configuración es:

  . *CPU RISC* con un procesador central *Motorola* XC88100 que opera a 20 Mhz.

  . 128 MB de memoria *RAM*

. 2 discos *SCSI* de 1GB

. Cinta de 525 MB para respaldos

. Controladora Multipuerto, con sus respectivas regletas de 8 puertos cada una, donde van conectadas las terminales no inteligentes mediante cables seriales.

. El sistema operativo que maneja es *UNIX* multiusuario propietario.

. Adicionalmente se tiene software para red *TCP/IP*

. La base de datos se denomina *PIC*.

. Las aplicaciones instaladas en el servidor, son empleadas para realizar procesos contables y administrativos de una institución financiera, y son de uso exclusivo de los equipos *Sanyo*, es decir no es un sistema abierto y amigable.

- En Guayaquil y Cuenca existen servidores *SANYO* de similares características al anterior, pero la velocidad del procesador es de 16 Mhz.
- Terminales tontas en Quito, Guayaquil, Cuenca que van conectadas a las regletas multipuerto. Ambato tiene una terminal no inteligente enlazada con *modems* hacia Quito.
- Computadoras emulando terminales no inteligentes.

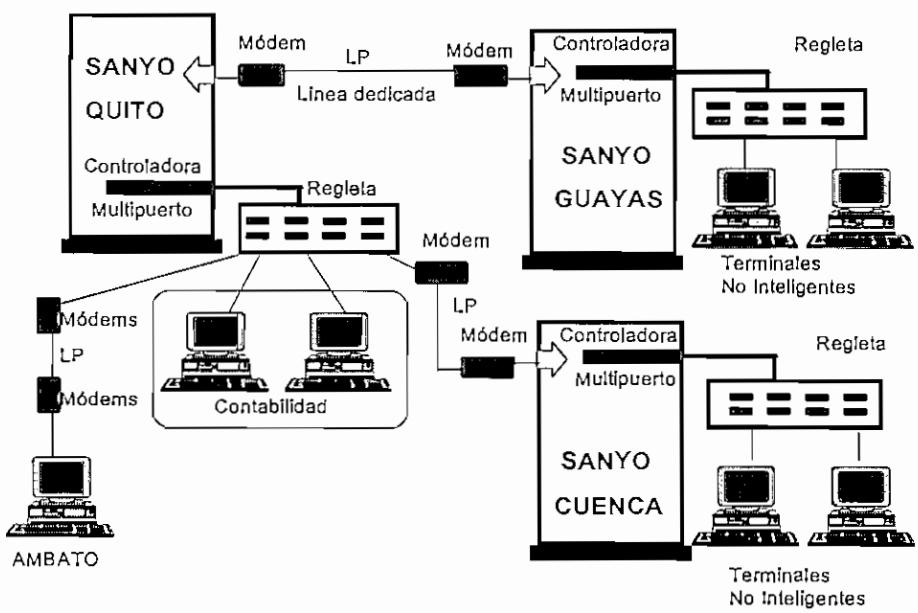


Figura 5.1 Red de datos Original de la Institución Financiera

- La comunicación entre las terminales y el servidor es tipo serial asincrónica, trabajando a 9600 bps *Full* dúplex.

- El cable empleado para la instalación es multipar telefónico sin blindaje, el cual funciona bien por operar a velocidades bajas y en distancias relativamente cortas dentro del edificio.
- Para el enlace con las agencias en Guayaquil, Cuenca y Ambato se utilizan *modems* con comunicación asincrónica de 9600 bps a través de líneas dedicadas LP.
- Cada regleta multipuerto atiende a un área o departamento determinado.
- Cuentan con dos *UPS* de las siguientes características:
  . 2 KVA cada uno, que alimentaban por separado a los servidores *UNIX Sanyo.*
  . 10 minutos de tiempo de permanencia de energía

Por lo descrito anteriormente , no existe en la Financiera una red propiamente dicha. La instalación es demasiada rígida y no permite el crecimiento de la misma. Los servidores *SANYO* resultan demasiado lentos y sin capacidad para las aplicaciones que se requieren implementar, para que la Institución pueda operar como un Banco.

Como una solución para la Red de Datos se sugiere una red tipo *Ethernet* para las redes locales en la matriz y agencias, por las siguientes condiciones:

- Conectividad para un amplio rango de dispositivos.
- Gran cantidad de tarjetas adaptadoras de red disponibles para las estaciones de trabajo, cuyo costo es mucho menor que las tarjetas *Token Ring.*
- Buena *performance* en redes locales pequeñas.
- Control de tráfico y colisiones mediante *Hubs* inteligentes que son más baratos que los *MAUs* de *Token Ring.*
- Facilidad de conexión de las estaciones de trabajo.
  . Cable coaxial *BNC*, para realizar una topología en bus.
  . Cable trenzado *UTP* categoría 5 con conectores RJ45, para una topología de red en estrella.
  . Conectores *AUI*
- La red no se torna inconsistente cuando una estación o un *Hub* falla, lo cual no ocurre en *Token Ring* , por cuanto si una estación falla el token se pierde y la red controlada por el *MAU* no funciona.

- Las controladoras de red funcionan a :

. 10 Mbps (Transmisión *Half* Dúplex) en bus *ISA*

. 20 Mbps (Transmisión *Full* Dúplex) en bus *PCI* con tecnología *Streamer.*

- Se puede transportar múltiples protocolos por la red como: *TCP/IP, IPX/SPX, PPP, NetBEUI, NetBIOS,* etc.
- En el servidor *Sanyo* se instala una tarjeta de red para conectarse a la red *Ethernet* nueva mediante un Transceiver .

  El protocolo *TCP/IP* soportado por el *UNIX Sanyo* , permitiría la migración de los datos hacia los nuevos sistemas .

5.1.2 ANALISIS DEL ENTORNO NATURAL

Aquí se toma en cuenta los factores que afectan la tolerancia a fallas, como son:

. Desastres naturales, como terremotos, inundaciones, etc.

. Fallas de energía, voltajes inestables, accidentes.

Ante estos problemas es necesario contar con respaldos de la información, arreglos de discos, servidores redundantes, *UPS*, todos los cuales disminuyen el riesgo de pérdida de información.

5.1.3 CONSIDERACIONES DE APLICACION

Se analiza el tipo de aplicaciones que van a "funcionar" en un determinado sistema operativo, de modo que facilita escoger el tipo de máquina, *CPU*, discos, memoria, adaptadores de red que debe tener un servidor.

5.1.3.1 CUELLOS DE BOTELLA

Para escoger cada uno de los servidores se toma en cuenta los sitios y dispositivos en los que se producen los "cuellos de botella" que retardan a la red:

- En los **servidores de archivos**, los cuellos de botella se producen en los dispositivos de almacenamiento, adaptadores de red y memoria.

- En los **servidores de comunicaciones** se producen en el *CPU*, el bus *I/O* y la velocidad de las líneas de comunicaciones.
- En los **servidores de correo electrónico** se produce en el *CPU*, memoria, y los dispositivos de almacenamiento.
- En un **servidor de aplicaciones y base de datos** se produce por la velocidad del *CPU*, dispositivos de almacenamiento (discos y arreglos), memoria.
- En el **servidor de impresión** se produce en el puerto paralelo, en la velocidad de la impresora y en el ancho de banda de los buses *I/O.*

Para disminuir los "cuellos de botella" es necesario mejorar cada elemento en cada uno de los servidores y estaciones de trabajo. Los principales elementos que se toman en cuenta son CPU, memoria, disco y tarjetas de red como se describe en el cuadro 5.1.

Discos	CPU	Memoria	Tarjeta de red *LAN* I/O
- Con cache - Acceso rápido - Arreglos de discos - Controladores de bus maestro -Controladores *SCSI* - Discos *SCSI* veloces	- Pentiums - Velocidades altas - Cache de segundo nivel - Múltiples CPUs	- Cantidad - Velocidad - Memorias entrelazadas - Diseño del bus - Controladores de memoria.	- Tarjetas que manejan bus maestro - *Software* de *LAN* - Manejo de 32 bits

Cuadro 5.1 Mejoramiento de dispositivos para eliminar cuellos de botella

5.1.3.2 REQUERIMIENTOS DE *HARDWARE* PARA LOS SERVIDORES CENTRALES

En los Servidores Centrales se van a ejecutar aplicaciones que realizan gran cantidad de operaciones matemáticas y transacciones que consumen gran cantidad de tiempo de procesador y de memoria.

Los sistemas de aplicaciones a instalarse en los Servidores Centrales son :

- Contabilidad
- Cuentas Corrientes
- Cuentas de Ahorros
- Firmas
- Cartera

- Remesas

- Custodia y garantía

- Plazo fijo

- Mesa de dinero

- Administración

- Bases de datos

5.1.3.3 PROCEDIMIENTO PARA DETERMINAR NÚMERO DE PROCESADORES, ESPACIO EN DISCO Y MEMORIA

a) Número De Procesadores

Para determinar el número de procesadores, se deben realizar los siguientes pasos:

1. Calcular la carga equivalente del sistema.
2. Estimar la intensidad del *CPU* con las aplicaciones que se están ejecutando en el sistema.
3. Determinar el número óptimo de procesadores basados en los resultados de los pasos 1 y 2.

b) Cantidad De Memoria

Para determinar la cantidad de memoria requerida, se deben realizar los siguientes pasos:

1. Estimar el número de usuarios a tiempo completo en el sistema (carga equivalente).
2. Estimar el uso de memoria para aplicaciones y para el sistema.
3. Identificar el tipo de aplicaciones que corren en el sistema.
4. Determinar la cantidad óptima de memoria, basados en el resultado de los pasos 1, 2 y 3.

c) Requerimientos de Disco

Para determinar los requerimientos de disco duro, se deben realizar los siguientes pasos:

1. Estimar los requerimientos de espacio en disco para usuarios
2. Estimar los requerimientos de espacio en disco para el sistema
3. Estimar los requerimientos de espacio en disco para aplicaciones.
4. Determinar el total de espacio de disco basados en los resultados de los pasos 1, 2 y 3.

Los detalles del cálculo de CPU, memoria y disco se describen en el Anexo 3.

Del análisis anterior se determina que los requerimientos de *CPU*, memoria y discos que el Servidor Central debe tener para la correcta operación del Banco son:

Nombre	Valor
Disco	10 GB *SCSI*
Memoria	256 MB con detección y corrección de errores
Procesador	2 *Pentium* de 166 Mhz (1) - Multiprocesamiento Simétrico
Red	Tarjeta de red *Ethernet* 10 BaseT
Dispositivo de *Backup*	*Tape* Helicoidal de 5 GB

Cuadro 5.2 Resumen de Requerimientos del Servidor

Por tal motivo el Servidor debe tener las siguientes características:

- Arquitectura microcanal.
- Multiprocesadores *Pentiums* de 166 Mhz, mínimo dos procesadores, con el fin de acelerar las transacciones y realizar tareas independientes.
- 256 MB de memoria *RAM*. Expandible en módulos.
- 10 GB de disco interno
- Debe soportar arreglos de discos externos para las bases de datos.
- Arreglos de cintas para realizar los respaldos en forma rápida y segura.
- Controladores *SCSI*
- Controladores Multipuerto.
- Controladores de red X.25 y *Ethernet*.
- Sistema operativo multiusuario *UNIX*.
- Sistema operativo de red *X.25* y *TCP/IP*.
- Sistemas de bases de datos.
- Sistema Bancario Integrado.

Para evitar cualquier contratiempo, se debe contar con un equipo de respaldo, en lo posible configurado con las mismas características del equipo que está en producción. El servidor secundario opera en forma paralela, con el fin de que si el primario falla, éste entra en funcionamiento. Los servidores pueden estar conectados a través de un bus *SCSI* compartiendo un arreglo de discos o pueden comunicarse a través de red X.25 o *Ethernet* empleando el comando *Telnet* de *TCP/IP*, como se muestra en la figura 5.2.

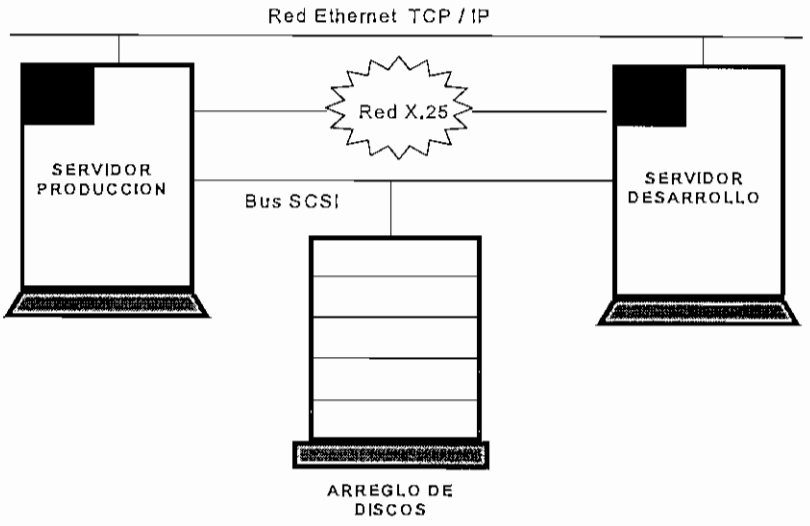


Figura 5.2 Servidores Redundantes conectados

5.1.3.4 REQUERIMIENTOS PARA LOS SERVIDORES *WINDOWS NT* Y USUARIOS

El cuadro 5.3 muestra las características de los equipos que se utilizarán para Servidores de Agencia, Servidores de Imagen, Computadora de Clasificadora de Cheques, Terminales Administrativas, Terminales Financieras y Usuarios de red.

Características	Servidores de Agencia	Servidor de Imágenes	Computador de Clasificadora	Computador de Scanner	Terminales Administrativas y Financieras	Usuarios
Arquitectura	*ISA/PCI*	*ISA/PCI*	*ISA/PCI*	*ISA/PCI*	*ISA/PCI*	*ISA/PCI*
Procesador	Pentium de 133 Mhz	Pentium de 133 Mhz	486 DX4 de 75 Mhz	486 DX4 de 75 Mhz	486 DX4 de 75 Mhz	486 DX4 de 75 Mhz
Memoria	64 MB	64 MB	64 MB	64 MB	32 MB	16 MB
Controlador *SCSI*	*SCSI-2 PCI*	*SCSI-2 PCI*	*SCSI 7731* propietario	*SCSI* para *Scanner*	no	no
Disco	*SCSI* 2 GB	*SCSI* 2 GB	*IDE* 850 MB	*SCSI* de 1 GB	*IDE* 540 MB	IDE 540 MB
Cinta *SCSI*	2 GB	2 GB	no	no	no	no
Controlador de red *WAN*	X.25 *Eicon*	no	no	no	no	no
Controlador de red *LAN*	*Ethernet Intel*	*Ethernet Intel*	*Ethernet Intel*	*Ethernet Intel*	*Ethernet SMC*	*Ethernet SMC*
Sistema Operativo	*Windows NT Server*	*Windows NT Server*	Windows para Trabajo en Grupos	Windows para Trabajo en Grupos	Windows para Trabajo en Grupos	Windows para Trabajo en Grupos
Software de red	*TCP/IP NetBEUI Netbios*	*TCP/IP NetBEUI Netbios*	*TCP/IP NetBEUI Netbios*	*TCP/IP NetBEUI Netbios*	*TCP/IP NetBEUI Netbios*	*TCP/IP NetBEUI Netbios*
SQL server	si	si	no	no	no	no
Software especial	no	Captura de imágenes	Clasificación de Cheques y captura de imágenes	Para *Scanner*	no	no
Aplicaciones Bancarias	si	si	si	si	si	si

Cuadro 5.3 Descripción de Servidores y Usuarios de red

Los requerimientos de *Software* para los **Servidores de Agencia** son:

- *Windows NT server*, que permite realizar procesos Cliente / Servidor.
- *SQL* server, que opera bajo *Windows NT* para el manejo de las bases de datos.
- Aplicaciones bancarias básicas para la operación entre los usuarios locales de la agencia y el Servidor Central *UNIX*, como: Contabilidad, Cuentas corrientes, Cuentas de Ahorros, Firmas.
- Software de red, tanto para red local como para red extendida entre los que están :
  . X.25 para red extendida empleada sólo en el servidor de agencia.
  . *TCP/IP* para red local y extendida
  . *PPP* para acceso remoto mediante puertos seriales asincrónicos.
  . *NetBEUI* para red local
  . *Netbios* para manejo de *sockets* en *SQL Server*
- Software de administración y monitoreo de red local

En la figura 5.3 se muestra la manera como los usuarios se comunican con las aplicaciones instaladas en el servidor *UNIX* a través del servidor de la agencia *NT*.

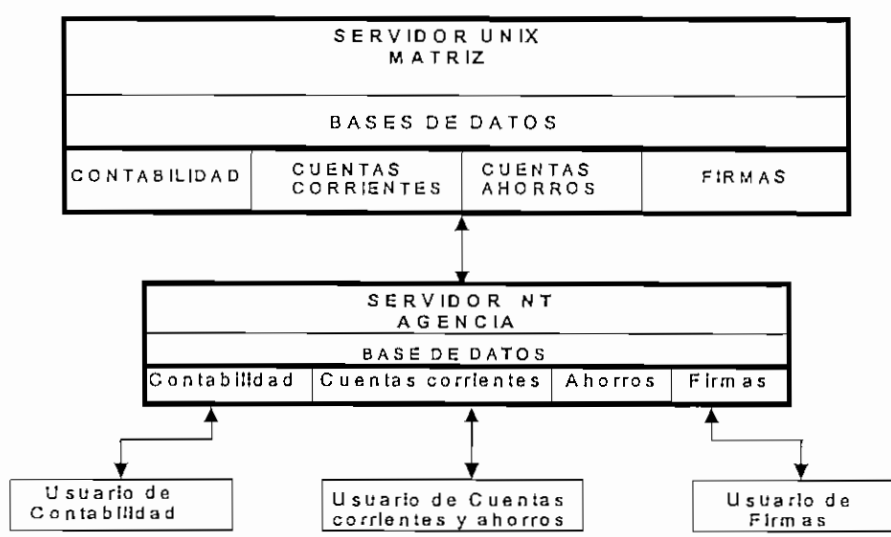


Figura 5.3 Acceso de Usuarios a las aplicaciones instaladas en el Servidor *UNIX*.

El **servidor de imágenes** tiene aplicación para el procesamiento gráfico de documentos, tales como las imágenes de los cheques capturados por las cámaras fotográficas de una clasificadora de cheques en la matriz y las imágenes capturadas por un *Scanner* en la matriz y

agencias. Las imágenes son procesadas diariamente y guardadas en un arreglo de discos ópticos externos de lectura - escritura *JUKE BOX*, eliminando la utilización de microfilmadoras.

El **computador de clasificadora de cheques** tiene *Software* para el control de la clasificadora de cheques, con el cual se realiza los procesos de Cámara del Banco que son: Clasificación y Captura de imágenes de los cheques.

Las **terminales Administrativas**, **Financieras** y **Usuarios** realizan procesos contables, transacciones bancarias, procesos administrativos y operan bajo Windows para Trabajo en Grupo y tienen instaladas aplicaciones bancarias primarias para accesar a los módulos principales del Servidor *NT* de la agencia y del Servidor Central *UNIX* de la matriz.

La figura 5.4 muestra la forma en que se distribuyen los servidores, terminales financieras, terminales administrativas y usuarios en las agencias. El servidor *NT* de agencia se comunica con el Servidor *UNIX* a través de enlaces X.25 .

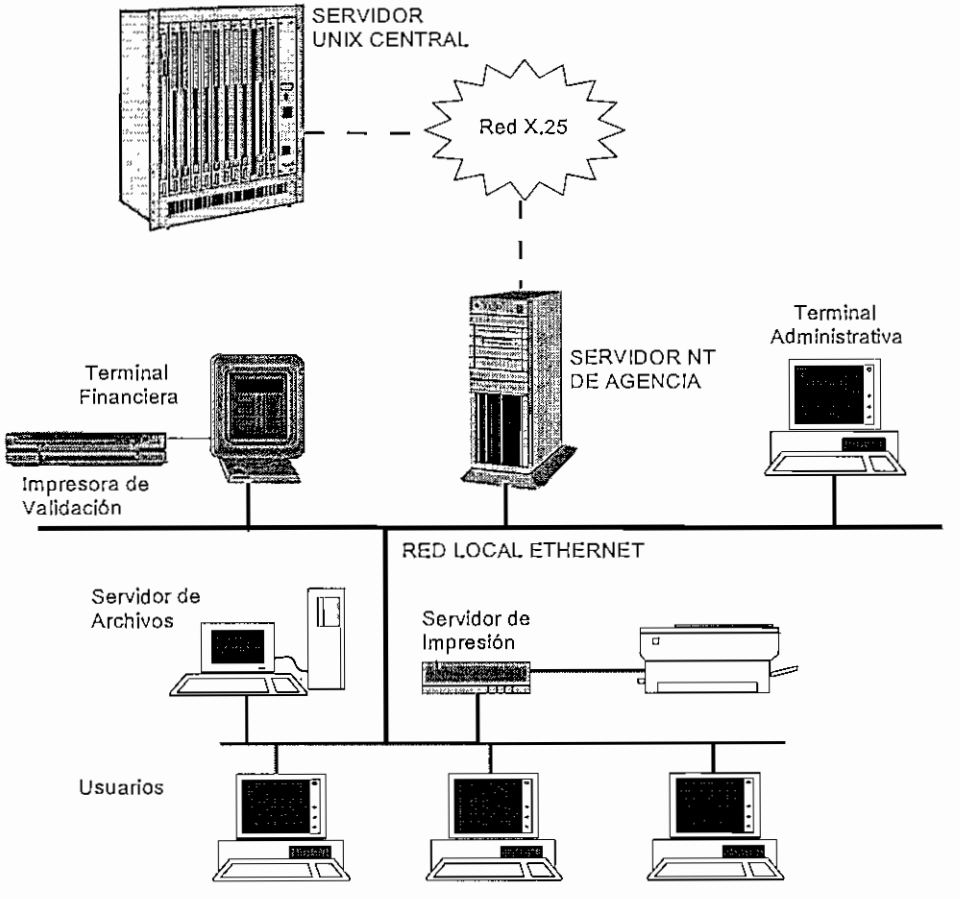


Figura 5.4 Distribución de servidor de agencia y usuarios en la red

5.2 CARACTERISTICAS TECNICAS DE LOS EQUIPOS Y MATERIALES

5.2.1 SERVIDORES CENTRALES *UNIX*

Entre las opciones de Servidores Centrales del Banco se tiene a los equipos marca ***AT&T*** correspondiente a los modelos 3430, 352X y 352X-XP, 357X y 357X-XP, 355X y 355X-XP y 5100C cuyas características se muestran a continuación en el cuadro comparativo 5.4.

CARACTERISTICAS	AT&T 3430	AT&T 352X	AT&T 352X-XP	AT&T 355X	AT&T 355X-XP	AT&T 357X	AT&T 357X-XP	AT&T 5100C
Arquitectura Microcanal	sí	sí	sí	sí	sí	sí	sí	sí
Multiprocesamiento	sí	sí	sí	sí	sí	sí	sí	sí
Número de Procesadores Pentium de 166 Mhz	2	1 a 8	4 a 16	2 a 8	4 a 16	2 a 8	4 a 16	4 a 32
Procesadores Cuadráticos [1]	no	no	sí	no	sí	no	sí	sí
Nivel de cache	1,2	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3
Cantidad máxima de memoria *RAM*	1 GB	2 GB	2 GB	2 GB	2 GB	4 GB	4 GB	4 GB
Arreglo Interno de discos	no	no	no	no	no	no	sí	sí
Arreglo de discos externo	sí	sí	sí	sí	sí	sí	sí	sí
Controladoras *SCSI* Duales	sí	sí	sí	sí	sí	sí	sí	sí
Controladoras *SCSI Quadratics*	no	sí	sí	sí	sí	sí	sí	sí
Controladora *MPCA*[2] para red *WAN*	sí	sí	sí	sí	sí	sí	sí	sí
Fuentes Redundantes	no	5	5	5	5	5	5	5
UPS interno	no	sí	sí	sí	sí	sí	sí	sí
Sistema Operativo *UNIX AT&T*	sí	sí	sí	sí	sí	sí	sí	sí
Sistema Operativo *Windows NT*	sí	sí	sí	sí	sí	sí	sí	sí
Cintas Helicoidales de 5 GB	sí	sí	sí	sí	sí	sí	sí	sí
Soporta discos SCSI de 4GB	sí	sí	sí	sí	sí	sí	sí	sí

Cuadro 5.4 Comparación entre Servidores marca AT&T

Los modelos *XP* se utilizan en modelos cliente-servidor de gran escala y manejan módulos cuadráticos de procesadores que tienen 4 procesadores con memoria cache de niveles 1, 2 .

Las controladoras *SCSI* microcanal pueden ser:

. Duales para dispositivos internos y externos

. *Quad*, que tienen 4 canales independientes para manejo de dispositivos externos, donde se requieren buses redundantes como es el caso de arreglo de discos, cintas.

Las controladoras microcanal de red *LAN* pueden ser :

. *Ethernet 10 Base T, 10 Base 5/2*

. *Token Ring*

. *FDDI*

[1] Los procesadores Cuadráticos son 4 procesadores Pentium de 166 Mhz instalados en un solo módulo.
[2] *MPCA= Multi Protocol Card Adapter* es un controlador de red extendida que soporta *HDLC* y X.25

Una forma de conexión de todos estos equipos se muestra en la figura 5.5, en donde los servidores redundantes A, B, C comparten arreglos de discos externos a través de buses SCSI y pueden comunicarse entre si a través de una red *Ethernet* mediante TCP/IP.

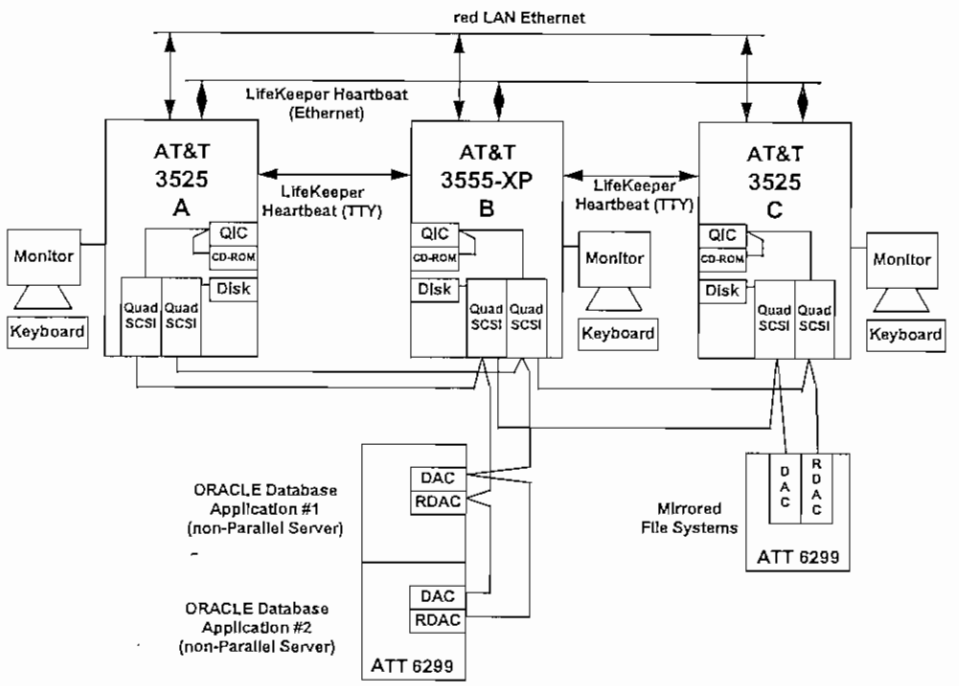


Figura 5.5 Conexión entre Servidores AT&T con arreglos de discos externos compartidos

5.2.2 ARREGLO DE DISCOS REDUNDANTES 6299

Tiene las siguientes características:

- Dos controladoras de arreglo de discos *SCSI* redundantes: *DAC* y *RDAC*.

  . *DAC* (*Disk Array Controller*) , es el controlador **activo** que maneja los discos del arreglo.

  . *RDAC* (*Redundant Disk Array Controller*), es el controlador **pasivo**, que se activa cuando el *DAC* o los controladores *SCSI* de la cadena instalados en los servidores fallan. Se tiene por lo tanto un bus *SCSI* redundante.

- Soporta 20 discos de 1 a 4 GB trabajando con *UNIX ATT*.
- Tiene 4 fuentes redundantes
- Puede ser conectado a un servidor redundante, para darle al sistema una tolerancia a fallas como se indica en la figura 5.6, en donde el arreglo se conecta a los Sistemas A y B mediante buses *SCSI* redundantes.

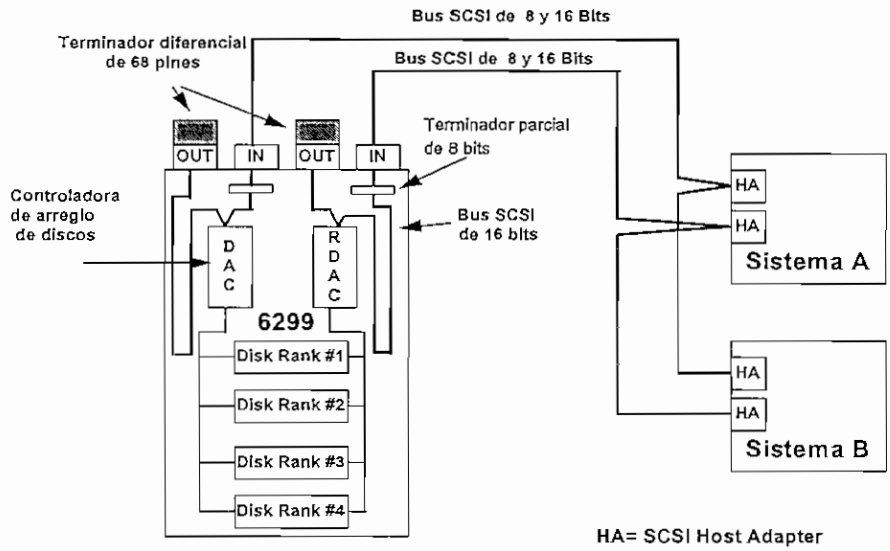


Figura 5.6 Conexión del Arreglo de discos AT&T 6299 a los Sistemas A y B

5.2.2.1 CONMUTACIÓN DE SERVIDORES REDUNDANTES CON PROTOCOLO *TCP/IP*

La conmutación (*Switchover*) de los servidores redundantes se realiza mediante un *Software* especial basado en el protocolo *TCP/IP*, para lo cual los sistemas redundantes se conectan en una red *LAN* exclusiva, por donde se realiza el monitoreo del estado de las operaciones que están realizando los equipos.

Para la conmutación con *TCP/IP* se debe instalar tarjetas de red (*Ethernet, Token Ring, o FDDI*) en cada sistema. Una dirección *IP* conmutable debe estar activa en un sistema. Cada sistema emplea una dirección *IP* para las aplicaciones en la red *TCP/IP* .

El sistema activo requiere 2 tarjetas de red:

- Una primaria para la dirección *TCP/IP* usada por las aplicaciones en situaciones normales.
- Una para monitorear el estado de funcionamiento de los servidores, cuya información permite realizar la conmutación de los servidores en forma automática cuando uno de ellos falla.

En el sistema *standby*, se requieren dos tarjetas de red :

- Una para la dirección *TCP/IP* reservada, la cual cambia a la dirección del sistema activo estándar cuando el servidor principal falla.
- Una para el monitoreo del estado operacional de los servidores.

El cuadro 5.5 muestra 3 aplicaciones X, Y y Z ubicadas en los arreglos y que se ejecutan en los servidores A, B y C de la figura 5. 7.

Aplicación	Primario	Secundario
X	Sistema A	Sistema B
Y	Sistema B	Sistema A
Z	Sistema C	Sistema B

Cuadro 5. 5 Ejecución de las aplicaciones en los sistemas primarios y secundarios

En condiciones normales cada servidor ejecuta una sola aplicación.

La aplicación X que normalmente corre en el sistema A puede ejecutarse en el B (**no** en ambos) en caso de que A falle. La aplicación Y del sistema B tiene como equipo de respaldo el sistema A, cuando B falle.

El sistema B puede ejecutar las tres aplicaciones cuando, los equipos A y C fallen. Esto se puede realizar por cuanto los buses SCSI entre el sistema A, B y el primer arreglo de discos están compartidos entre los tres y los otros buses SCSI entre los sistemas A, C y el segundo arreglo también están compartidos. Además los servidores pueden comunicarse entre si mediante el comando *Telnet* de *TCP/IP* a través de la red *Ethernet* a la que están conectados.

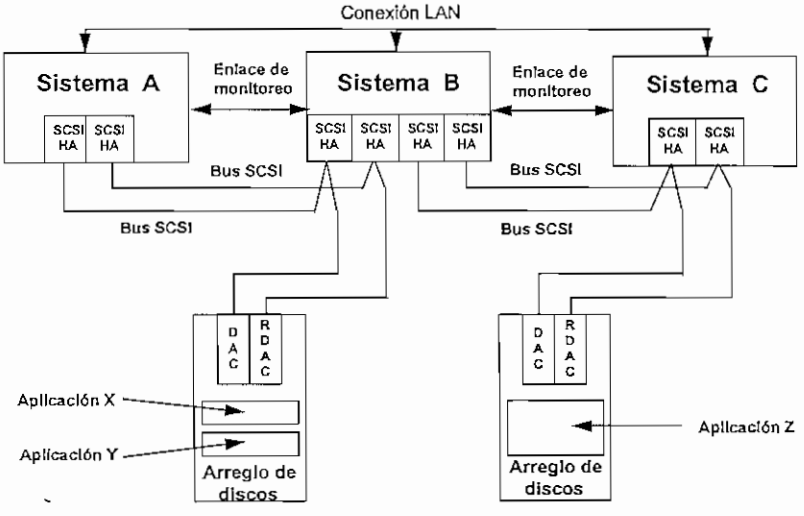


Figura 5. 7 Conexión de Sistemas Redundantes a través de buses *SCSI* compartidos y mediante conexión de red local.

5.2.3 RUTEADORES

Entre los principales ruteadores que se pueden emplear para la implementación de la red extendida se tienen el *CISCO* 500-CS y el *CODEX* 6520 de *Motorola*. Las características de estos ruteadores se muestra en el cuadro 5.6.

Los dos ruteadores tienen un puerto de consola para configurar los puertos, estableciendo los protocolos de comunicaciones de red local y de red extendida, las tablas de rutas y monitorear las estadísticas de cada uno de los interfaces de red (puertos).

En los dos ruteadores el interfaz de red local puede tener una sola de las siguientes opciones:

. *Ethernet* con velocidad de transmisión de 10 *Mbps* por puerto.

. *Token Ring* de 4 a 16 *Mbps* de velocidad, seleccionado por software.

. *FDDI* que alcanza una velocidad de 100 *Mbps* empleando fibras multimodo y monomodo.

- Los protocolos de comunicaciones soportados son:

. *SDLC* (*Synchronous Data Link Control*)

. X.25

. *Frame Relay*

. *TCP/IP*

. *SLIP*

. Punto a Punto

CARACTERISTICAS	CISCO 500-CS	CODEX 6520
Puertos de red Extendida	6 fijos	Mínimo 5 con posibilidad de crecimiento hasta 19 puertos
Tipo de puerto de red extendida	RS232, V.35, X.21, RS499 por pedido	V.35 el puerto1, RS232 de los puertos 2 al 6, RS232D los puertos adicionales.
Puertos de red Local	1	1
Tipo de puerto de red local direccionable	*Ethernet AUI, Token Ring, FDDI*	*Ethernet RJ45, Token Ring*
Protocolos de puente	*-Source Route Bridge SRB* *-Ethernet Transparent Bridging ETB*	*-Source Route Bridge SRB* *-Ethernet Transparent Bridging ETB*
Protocolos ruteables	*IP, IPX, ARP, RARP*	*IP, IPX, ARP, RARP*
Encapsulamiento de datos	*-RFC* 877 para X.25 *-RFC* 1294 para *Frame Relay*	*-Codex* propietario *-RFC* 877 y 1356 para X.25 *-RFC* 1294 para *Frame Relay*
Puertos de red extendida opcionales	no	14 puertos adicionales
Puertos de *modem*	no	1 puerto mediante tarjeta opcional en el segundo zócalo
Actualización de *BIOS*	sí	si en forma local o remota
Soporte remoto	sí	sí
Monitoreo de puertos y enlaces	mediante consola local	mediante consola local y remota

Cuadro 5.6 Características de los ruteadores Cisco 500-CS y *Codex* 6520

Los puertos de red extendida son configurables para que los ruteadores actúen como *DTE* o *DCE*, y tienen las siguiente interfaces:

. V.24 para transmisión estándar de 2400 hasta 19.200 bps

. V.35 para transmisiones de alta velocidad desde 2400 a T1 (1,544 Mbps)

La figura 5.8 muestra la disposición de los puertos del ruteador *Cisco 500-CS*, el cual tiene un puerto de red local con interfaz AUI, por lo que se necesita un *Transceiver* AUI/RJ45 o AUI/BNC para conectarlo a la red *Ethernet*.

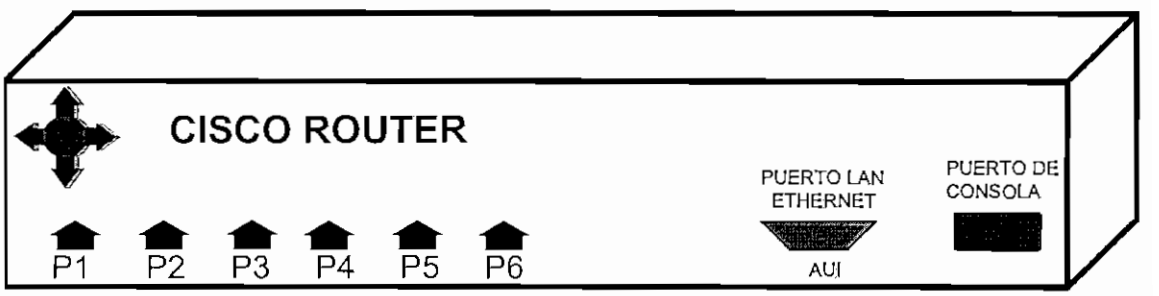


Figura 5.8 Distribución de puertos en el ruteador *Cisco 500-CS*

La figura 5.9 muestra la distribución de los puertos del ruteador *Codex* 6520.

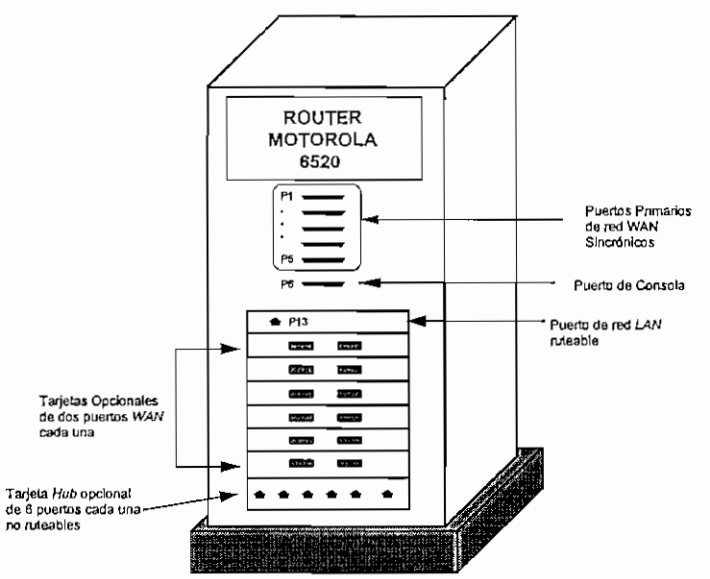


Figura 5.9 Distribución de puertos en el ruteador Codex 6520

El puerto de red local direccionable puede ser *Ethernet* o *Token Ring* .

La mínima configuración del ruteador *Codex* 6520 tiene 6 puertos, de los cuales 5 son para red *WAN* y un puerto de consola. El puerto 1 es un puerto V.35 que puede ser configurado para que el ruteador opere como *DTE* o *DCE* y del puerto 2 al 5 son RS232.

En los *slots* de expansión se puede adicionar 7 tarjetas de red *WAN* de dos puertos cada una.

Opcionalmente se puede añadir una tarjeta *Hub* de 6 puertos no direccionables, a los cuales se conectan el puerto de red local P13 direccionable y los *hubs* maestros de la red de datos.

La figura 5.10 muestra la forma de conexión de ruteadores *Codex* en una red extendida y en una red local.

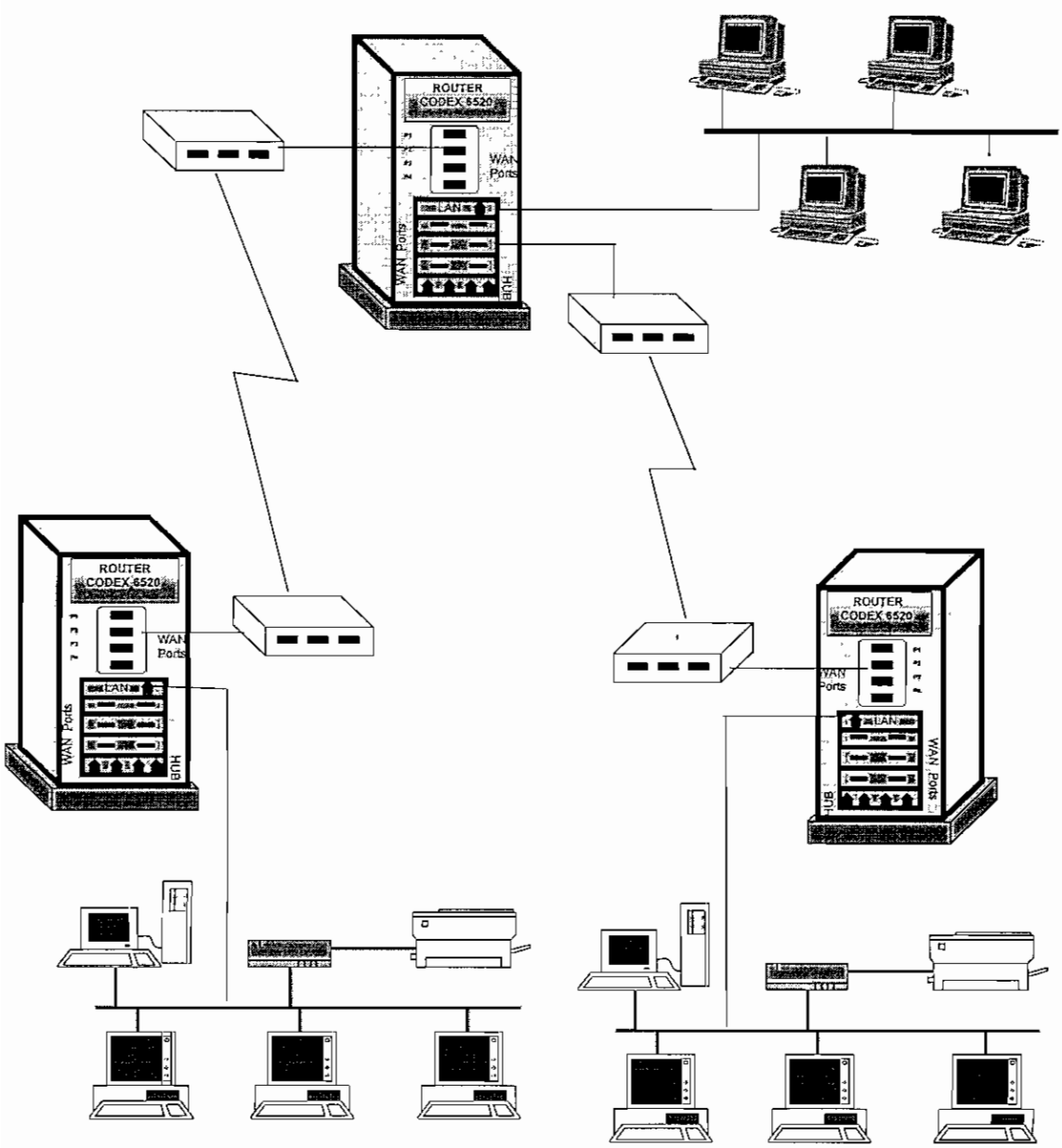


Figura 5.10 Interconexión de ruteadores *Codex* 6520

La estructura interna de un ruteador se estudió en el capitulo 2 y la forma de encapsular los datos *IP* en X.25 y *Frame Relay* se describió en el capítulo 3.

Tanto el ruteador *Codex* 6520 y *Cisco 500-CS* deben estar configurados con las mismas opciones para que puedan operar tanto en *Frame Relay* como en X.25. Una de las conexiones válidas se muestra en la figura 5.11.

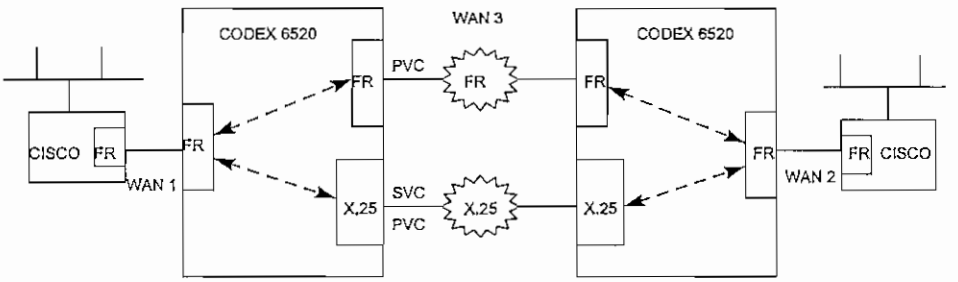


Figura 5.11 Interconexión de ruteadores *Cisco* y *Codex* a través de *Frame Relay* y *X.25*

5.2.4 *DTU Data Termination Unit*

Es un equipo que permite enviar dos canales de datos sobre una sola línea **digital**. Cada canal tiene un ancho de banda de 64 Kbps, pudiendo ser configurable como *DTE* o *DCE*, y pueden operar sincrónica o asincrónicamente. En transmisiones sincrónicas las velocidades van de 0.15 a 64 Kbps. Cuando se emplea un sólo canal se alcanza los 128 Kbps.

Permite conexión a puertos V.35, X.21/RS449, V.24/RS232.

Este equipo utiliza Multiplexación por División de Tiempo de los dos canales de datos.

La línea digital llega a una central, en donde se distribuye los canales a sus respectivos destinos remotos como se indica en la figura 5.12.

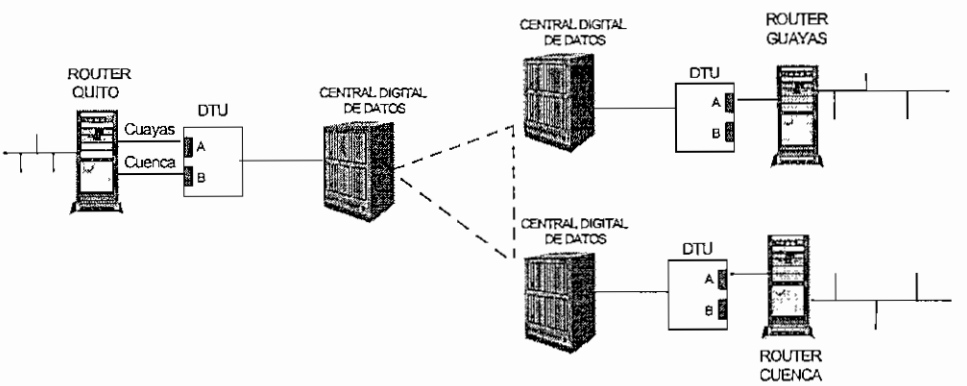


Figura 5.12 Utilización de *DTUs* para unir redes locales remotas a través de centrales digitales

5.2.5 *VTU Video Termination Unit*

Esta unidad comprime los datos de vídeo capturados por una cámara para transmitirlos sobre la red *WAN*, utilizando un ancho de banda bajo de vídeo. La compresión llega hasta cadenas de 128 Kbps.

Los datos pueden ser enviados por la *WAN* en enlaces T1(1.544 Mbps) o E1(2,048 Mbps), hasta el Sistema Manejador de Vídeo remoto y permite el monitoreo en tiempo real de lugares que necesitan estar vigilados como bóvedas, cajas, cajeros en un banco.

Las señales de Vídeo, Voz y Datos son multiplexados con Multiplexers que manejan T1, E1 como se observa en la figura 5.13.

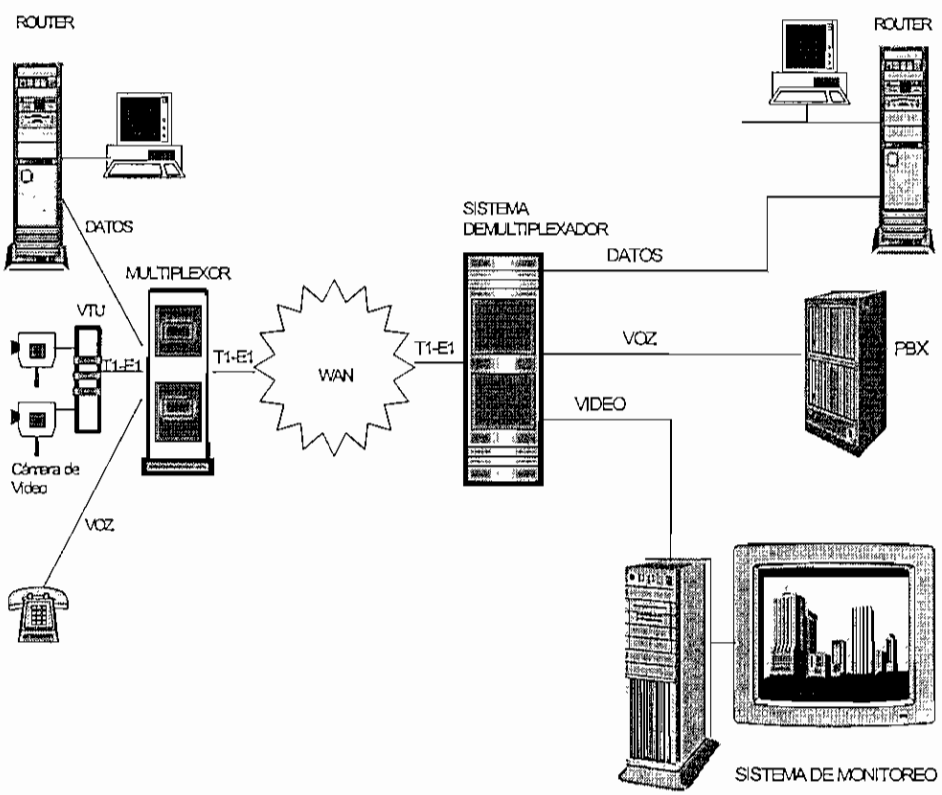


Figura 5.13 Multiplexación de señales de voz, vídeo y datos en redes digitales

5.3 ALTERNATIVAS DE DISEÑO

En el diseño de la red de datos los objetivos a alcanzar son :

- Mejorar las comunicaciones tanto en la red local como en la red extendida, tomando en cuenta las tecnologías existentes para la transmisión de datos.
- Reducir el tiempo e incrementar la distancia de transmisión
- Facilitar el acceso a la información
- Reducir los costos operacionales de la red
- Estandarizar la red total
- Crecimiento

Para el diseño de la red extendida *WAN* se tienen las siguientes alternativas:

- *X.25*
- *Frame Relay*
- *ATM*

Para la red local se tienen las siguientes opciones:

- *Ethernet*
- *Token Ring*
- *FDDI*
- *ATM* para red local

Las comunicaciones de datos a través de facilidades de transmisión analógicas se las realiza a bajas velocidades vía *modems*.

En la actualidad se han implementado redes digitales que permiten disminuir las barreras de tiempo y distancia en la transmisión de datos, voz, imagen y vídeo, empleando controladores de comunicaciones, multiplexores, conmutadores que permiten el manejo de la información sobre las líneas digitales.

La figura 5.14 muestra la forma de interconexión de redes a través de redes analógicas y digitales.

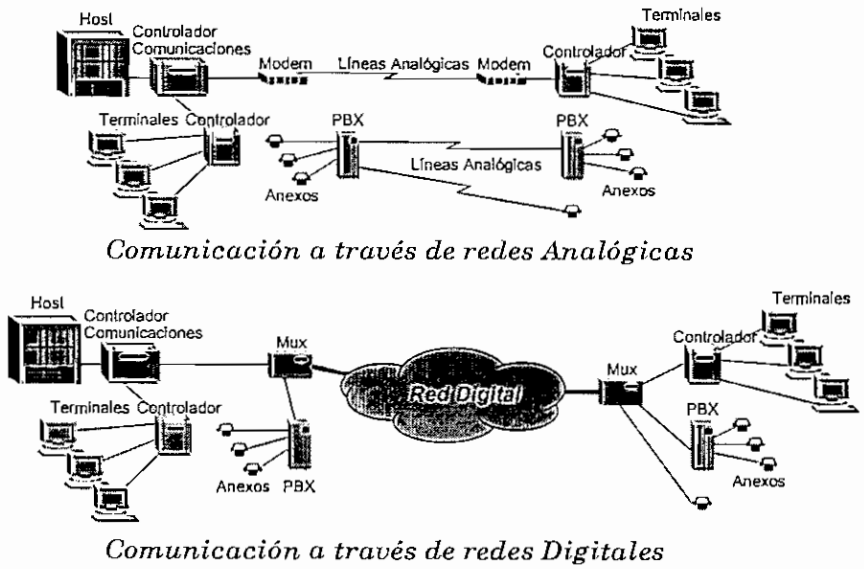


Figura 5.14 Redes Analógicas y Digitales

A continuación en la figura 5.15 se muestra la velocidad de transferencia de paquetes/celdas en circuitos conmutados y en líneas privadas en los diferentes tipos de redes *WAN*.

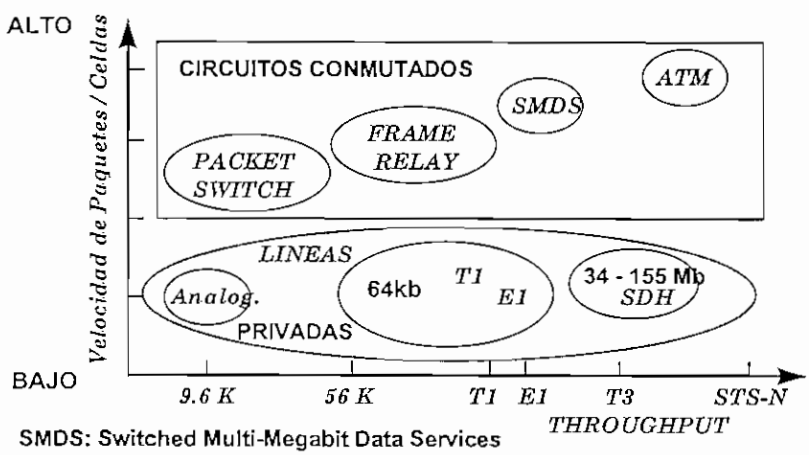


Figura 5.15 Comparación de las líneas analógicas con las líneas digitales

Con circuitos conmutados se obtiene mayores velocidades de transmisión de paquetes en *Frame Relay* y de celdas empleando *ATM*.

En la actualidad un 70 % de redes *WAN* forman parte de las redes digitales. *Frame Relay* ha ido evolucionando hasta un 40 % de instalaciones, en tanto que *ATM* está cogiendo fuerza por su mayor velocidad de transmisión de datos, como se muestra en la figura 5.16.

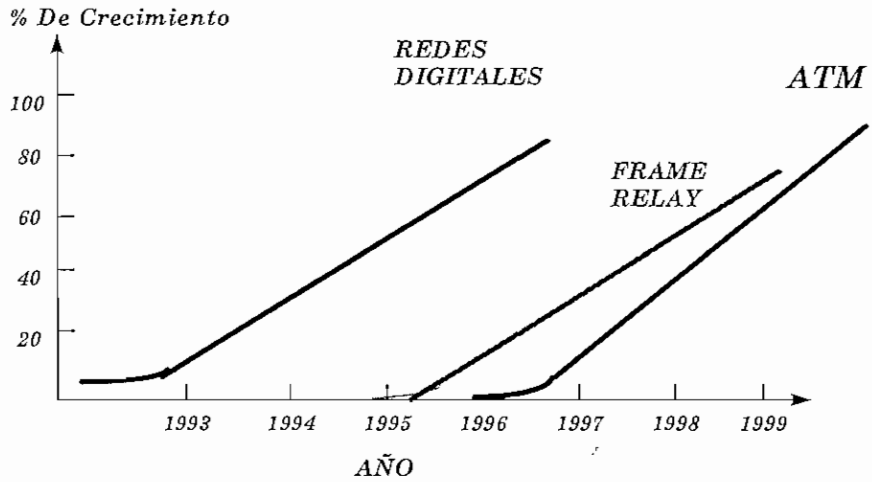


Figura 5.16 Evolución de las redes

Las redes locales *LAN* modernas manejan procesamientos de vídeo, voz , imágenes y datos, para lo cual emplea conmutación de paquetes a velocidades altas dentro de la misma *LAN*.

5.3.1 RED X.25 [3]

Como ya se describió en el capítulo 1, en el numeral 1.2.1, esta red está formada por tres niveles que son:

1- Nivel Físico

2- Nivel de Trama

3- Nivel de Paquete

Es una red de conmutación de paquetes de datos confiable y económica, que opera en líneas analógicas y digitales, enlaces de radio, enlaces vía satélite.

X.25 define la interacción punto a punto entre equipos *Data Terminal Equipment DTEs* a través de circuitos virtuales bidireccionales conmutables *SVCs* o permanentes *PVCs*. Los circuitos *SVCs* se emplean cuando las transmisiones de los datos son esporádicos y los *PVCs* cuando el flujo de datos entre equipos *DTEs* es permanente.

El nivel 3 de paquete del modelo X.25 genera los circuitos virtuales para la comunicación *end - to - end* entre *DTEs*. Cuando se establece un circuito virtual entre *DTEs*, el *DTE* origen envía el

[3] Internetworkig Technology Overview, Cisco Systems, Capítulo 12

paquete primero hacia un *DCE*, el cual observa el número del circuito virtual para determinar como debe enrutar el paquete a través de la red X.25. El nivel 3 X.25 permite escoger la ruta del *DCE* que se conecta directamente al *DTE* destino, como se muestra en la figura 5.17.

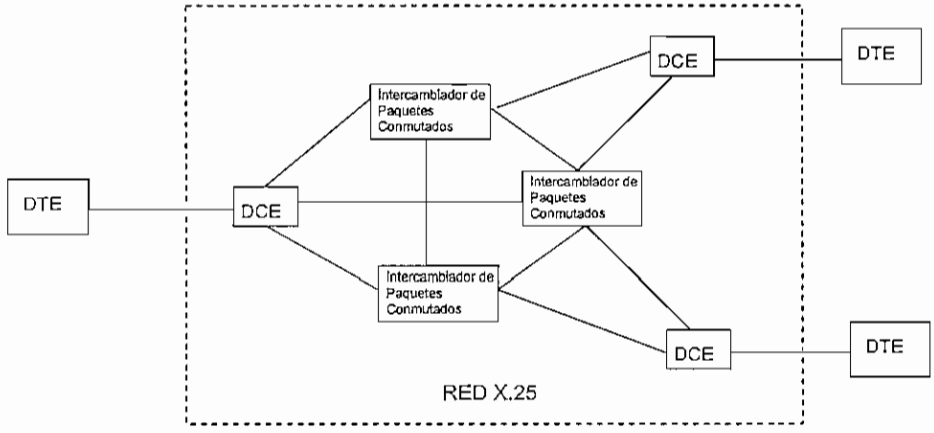


Figura 5.17 Modelo X.25

El nivel 2 de trama permite iniciar la comunicación entre el DTE origen y el DCE destino y durante la transferencia de la información chequea que las tramas arriben en el receptor en la secuencia correcta y libre de errores.

El nivel 1 físico define las características mecánicas y eléctricas del medio de conexión entre los equipos que intervienen en la red X.25. El nivel 1 usa el protocolo de capa física X.21 el cual soporta conexiones punto a punto con velocidades de hasta 19.2 *bps* y transmisiones sincrónicas *full duplex* .

Se logra transmisiones aceptables a velocidades que van de 2.4 Kbps a 28.8 *Kbps* dependiendo de la calidad del enlace. No puede integrar voz, vídeo y datos.

En el Ecuador la calidad de los enlaces de transmisión dependen en su mayoría de EMETEL y su estado tecnológico.

Para mejorar las comunicaciones de X.25 se debe migrar hacia las plataformas *Frame Relay* y *ATM* mediante equipos de Transferencia e Intercambio de Paquetes (*PTX*) desde la red X.25 hacia las redes *Frame Relay* y *ATM.*

Las velocidades que maneja los equipos *PTX* son :

- V.24/V.28/RS232/RS422 hasta los 64 Kbps
- V.35/X.21 hasta 1.544Mbps
- T1(1.544 Mbps)
- E1(2.048 Mbps)
- T3(45 Mbps)
- E3(34 Mbps)

Los paquetes X.25 se encapsulan en la trama *Frame Relay*.

Para migrar desde la red *Frame Relay* hacia la red *ATM*, se emplea el Intercambiador de Paquetes de *Frame Relay* a *ATM* (*FRATM*), los cuales se conectan con la red *ATM* mediante enlaces DS-3, o E3 y a la red *Frame Relay* con enlaces T1.

Los *Frame Relay Engine (FRE)* y los *Packet Engine (PE)* permiten incrementar el número de puertos en cada una de las redes. La Migración de la red X.25 se describe en la figura 5.18 en donde la red dorsal constituye la red *ATM* que trabaja a altas velocidades.

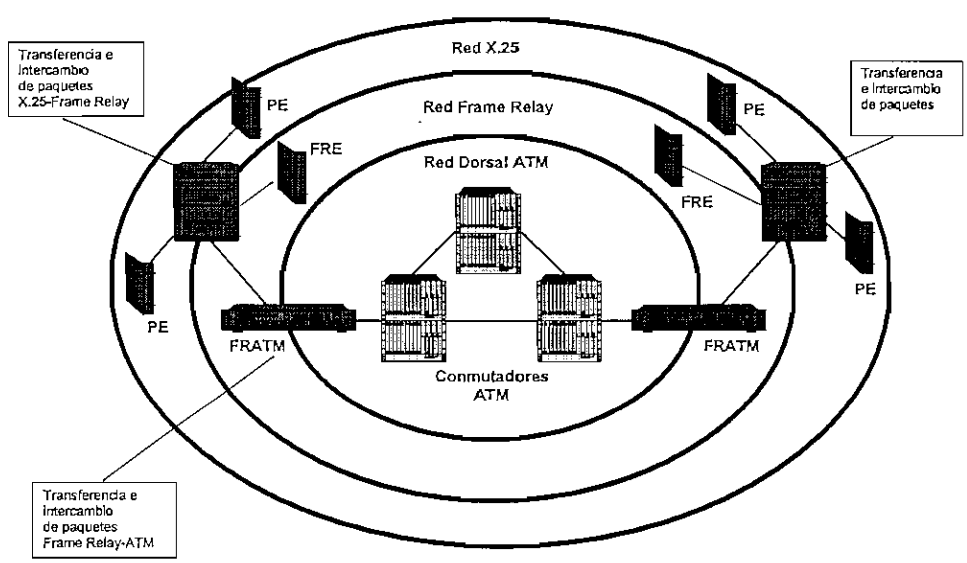


Figura 5.18 Migración de la red X.25 hacia *Frame Relay* y *ATM*

5.3.2 RED *FRAME RELAY* [4]

Es una red moderna de mayor velocidad que emplea la técnica de conmutación de tramas, orientado a la conexión de redes *LANs* remotas. La velocidad de transmisión va de 0 - 2 Mbps, es decir operan con velocidades T1(1.544 Mbps) y E1(2.048 Mbps) .

Para alcanzar estas velocidades se emplean enlaces digitales de circuitos conmutados, o enlaces de fibra óptica .

Frame Relay permite transmitir Voz, Imágenes, Vídeo y Datos, entre redes *LAN* remotas, por una sola línea; para ésto se emplean *MUX* digitales operando a velocidades T1/E1. Realiza una multiplexación estadística de los circuitos virtuales para el uso eficiente del ancho de banda disponible.

Frame Relay detecta errores de bits pero no los corrige, además no tiene control del flujo de datos por los circuitos virtuales, dejando estas tareas a los protocolos de las capas de red superiores.

La red dorsal está formada por conmutadores *Frame Relay* como se muestra en la figura 5.19.

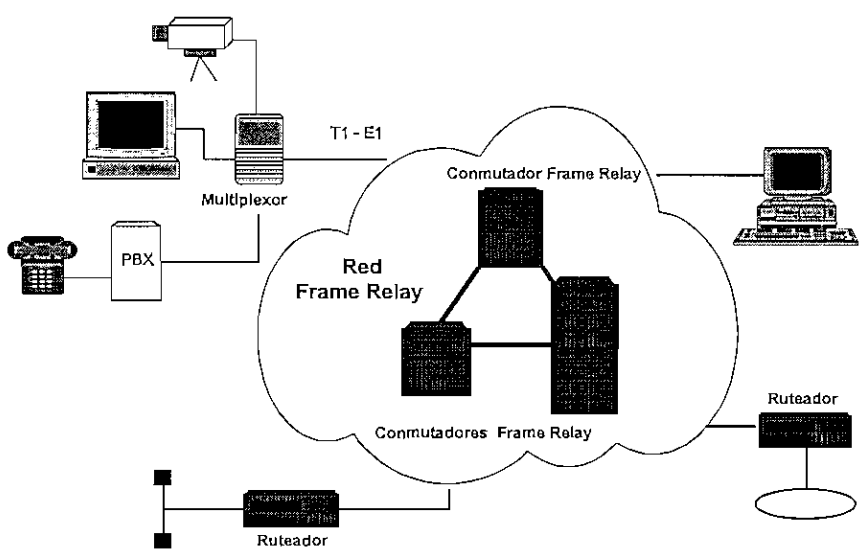


Figura 5.19 Red *Frame Relay*

[4] Internetworkig Technology Overview, Cisco Systems, Capítulo 12

La trama *Frame Relay* está delimitada por banderas de inicio y fin de 1 byte cada una como se indica en la figura 5.20.

La dirección tiene 2 bytes, dentro de la cual está la Identificación de Conexión del Enlace de Datos *DLCI,* la misma que identifica a la conexión lógica (circuito virtual por el que se envía los datos) que es multiplexada en el canal físico. Los ruteadores extremos pueden tener diferente *DLCI* para referirse a la misma conexión.

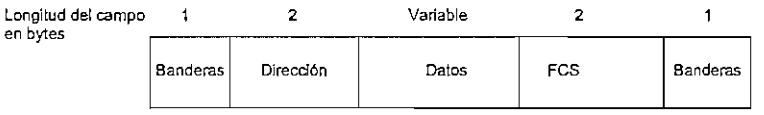


Figura 5.20 Trama *Frame Relay*

En el ejemplo de la figura 5.21 el ruteador 1 tiene un *DLCI*=12 y el ruteador 2 un *DLCI*=82 para identificar el circuito virtual formado para el enlace de los dos equipos.

Si el Ruteador 1 va a enviar una trama al ruteador 2, entonces el ruteador 1 coloca el valor de 82 en su campo *DLCI* y envía el dato a la red *WAN*. El ruteador 2 toma el dato y cambia el campo *DLCI* a 12 y responde al ruteador 1, con lo cual queda establecido el enlace.

Dentro del campo *DLCI* se incluye también bits de control de congestión, los cuales alertan a los ruteadores origen y destino para que puedan tomar una decisión.

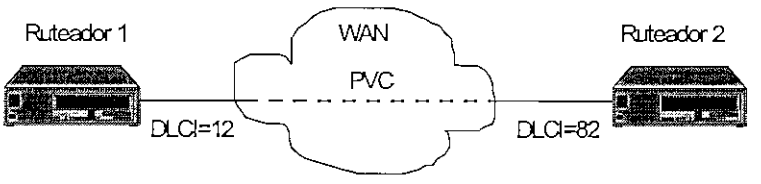


Figura 5.21 Ejemplo de conexión entre ruteadores a través de *Frame Relay*

5.3.3 RED *ATM ASYNCHRONOUS TRANSFER MODE*

Es una red de **banda ancha** orientada a conexión para la transferencia de Voz, Vídeo, y Datos, a través de enlaces de alta velocidad que alcanza hasta 155 Mbps, que opera tanto en redes locales como también en redes extendidas.

Son redes de alto nivel de desempeño, flexibilidad y crecimiento.

Puede conectarse con los servicios existentes *Frame Relay* y X.25 a través de conmutadores de transición de red.

Se emplea en educación a distancia, imágenes médicas, vídeo/conferencia, etc.
La red dorsal *ATM* está compuesta de conmutadores enlazados por lo general mediante **fibra óptica.**

La unión de las redes *LAN Ethernet* a la red *ATM* se lo hace con *Hubs* Conmutables *ATM*, los cuales tienen puertos 10 *BaseT Ethernet* conmutables para conectarse a la red *LAN*, y un puerto que opera a OC-3 (155 Mbps) o STM-1(155 Mbps) para unirse a la red *ATM* a través de fibra óptica. La disposición de estos equipos se muestra en la figura 5.22.

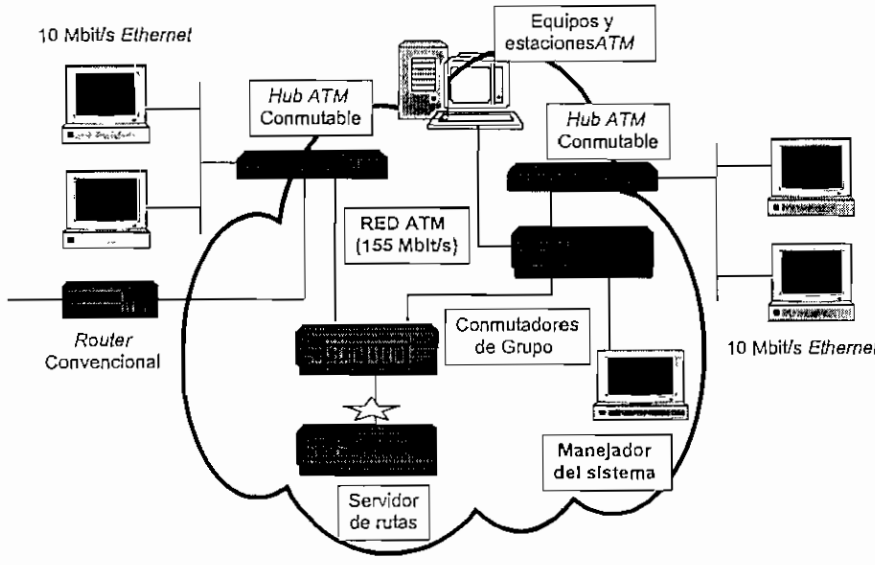


Figura 5.22 Red *ATM*

Los paquetes *Ethernet* son segmentados en **celdas** *ATM* de 53 *bytes* para su transmisión a través de circuitos virtuales. En el *Hub* remoto se reensambla el paquete para enviarlo al destino.

Estos *Hubs* conmutables manejan resolución de direcciones físicas *MAC*, y mantiene una memoria con las direcciones físicas de equipos conectados a sus puertos *Ethernet* y *ATM* , con lo cual puede conmutar los paquetes en forma directa dentro de la red local *Ethernet*, como también hasta los destinos remotos sin requerir mayormente del Servidor de rutas *ATM.*

Los Conmutadores de Grupo *ATM* constituyen el núcleo de la red, y conmutan las **celdas** *ATM* hasta sus destinos a través de circuitos virtuales conmutables o permanentes. Sus interfaces son OC-3, que operan a 155 Mbps sobre fibras ópticas multimodo o monomodo.

El Servidor de Rutas contiene el mapa entre las direcciones *MAC Ethernet* y direcciones *ATM*, las cuales son usadas por los *Hubs* Conmutables y las estaciones *ATM* (conectadas directamente a los conmutadores de grupo) , para establecer la comunicación de las estaciones *Ethernet* con los equipos y estaciones *ATM* conectados a través de una red *ATM.*

La estructuración de la red, el formato de las celdas, el modelo de referencia y la conmutación de celdas *ATM*, se describen en detalle en el Anexo 2.

Finalmente se puede indicar que todas las redes mencionadas anteriormente se relacionan entre sí para integrarse en una sola red global de manejo de datos, voz, vídeo/conferencia, imágenes como se indica en la figura 5.23, donde la transferencia de información entre estaciones remotas es transparente al tipo de red por la que atraviesa.

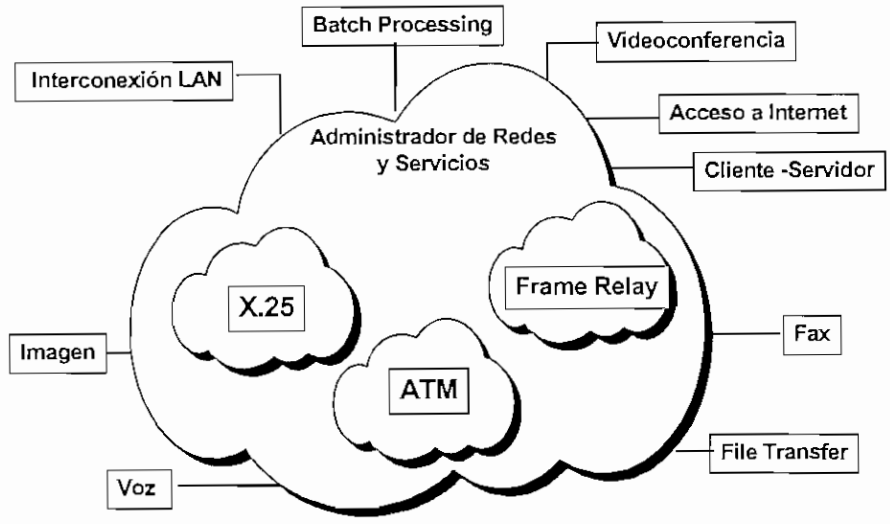


Figura 5.23 Integración de las redes X.25, *Frame Relay* y *ATM*

5.4 DISEÑO DE LA RED *LAN* EN MATRIZ Y AGENCIAS

5.4.1 DISEÑO DE LA RED *LAN* EN LA MATRIZ

Como una solución para la Red de Datos en la matriz se sugiere una red tipo *Ethernet* , por las condiciones anotadas en el *item* 5.1.1.

La columna vertebral ***Backbone*** de la red se forma por ***Hubs Switching*** unidos por fibra óptica, para que las transmisiones entre éstos sea a altas velocidades, y a distancias más grandes, en el orden de 1 Km con fibras multimodo y monomodo. Estos equipos conmutan los datos a sus respectivos destinos, con lo cual el ancho de banda para los puertos *Ethernet* no se divide como ocurre en los *hubs* comunes.

Todos los puertos del *Hub* trabajan a 10 Mhz de transmisión de datos, con lo cual la red se torna más veloz y debido a la conmutación de los paquetes se evita los congestionamientos.
Los puertos del *hub switching* son 10 *BaseT* a los cuales se conectan los ruteadores, todos los Servidores *UNIX,* Servidores *NT* y equipos que requieran ser accesados a altas velocidades como son: servidores de imágenes, servidores de departamentos, servidores de archivos etc.

El resto de puertos sirven para poner *Hubs* **comunes** en cascada mediante cable *UTP*.

Cada 5 pisos se coloca una caja de distribución donde se instala un *Hub Switching*, el cual maneja a los *hubs* comunes del respectivo piso, de los dos pisos superiores y de los dos inferiores, con el objetivo de tener una mejor distribución del cableado, como se muestra en la figura 5.24.

Los ***hubs* comunes** tienen 12 puertos 10 *Base T* los cuales sirven al resto de usuarios de la red. Si se requiere un mayor número de puertos, se puede poner *hubs* en cascada uniéndolos mediante cable *UTP*. La desventaja de estas conexiones es que el ancho de banda total se divide por el número de puertos, con lo cual la velocidad de transmisión disminuye y las colisiones aumentan.

Las conexiones de los *Hubs* comunes y los usuarios se los hace mediante cable trenzado *UTP* categoría 5 a una distancia máxima de 100 metros entre dos puntos.

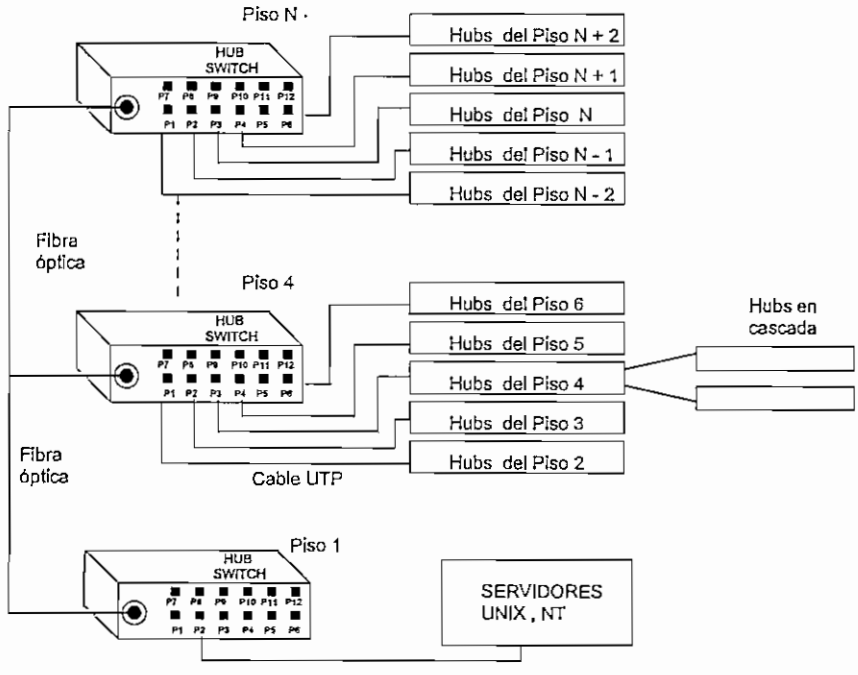


Figura 5.24 Distribución de *Hubs Switching* y *Hubs* comunes

La configuración física de la red en la matriz se muestra en la figura 5.25.

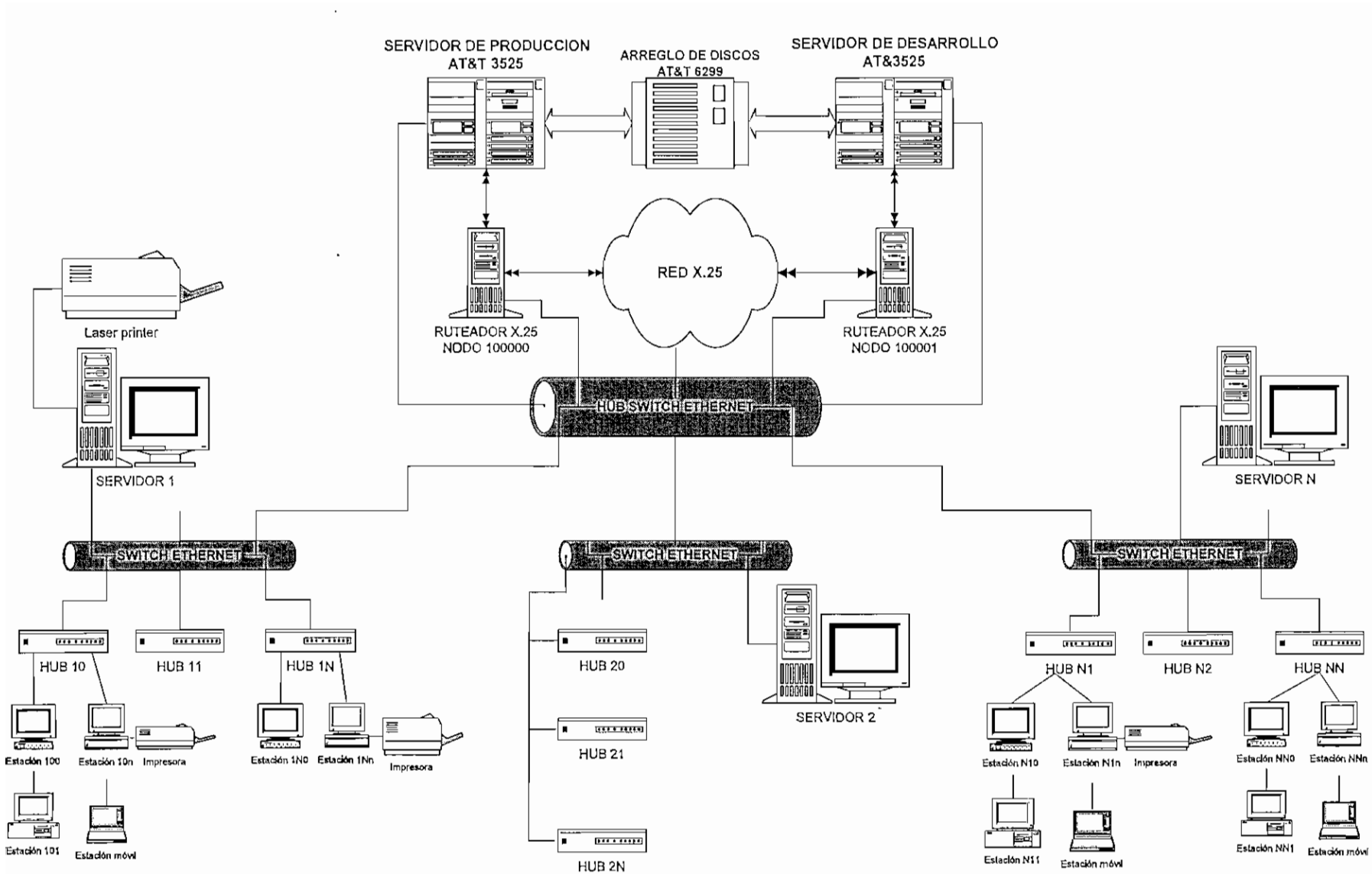


Figura 5.25 Configuración física de la red en la matriz

La dirección de red local *IP* de la matriz es **130.000**.000.000 cuya máscara de red es 255.255.000.000.

Para asignar las direcciones *IP*, se clasifica a los equipos en grupos, de acuerdo a las funciones que realizan, y a las áreas donde están operando, entre los que se tienen:

- Ruteadores y *Gateways*
- Servidores
- Usuarios

Los servidores más importantes se instalan en el centro de cómputo. Los usuarios están distribuidos en diferentes áreas, en cada una de la cuales también pueden ser instalados servidores departamentales.

Para asignar nombres a los equipos se emplean las siglas de los departamentos donde están ubicados, seguidas de un número que especifica al usuario. Una posible distribución de los equipos en el Banco se muestra en el Anexo 4.

Los ***gateways*** permiten el paso de una red a otra como se muestra en la figura 5.26.

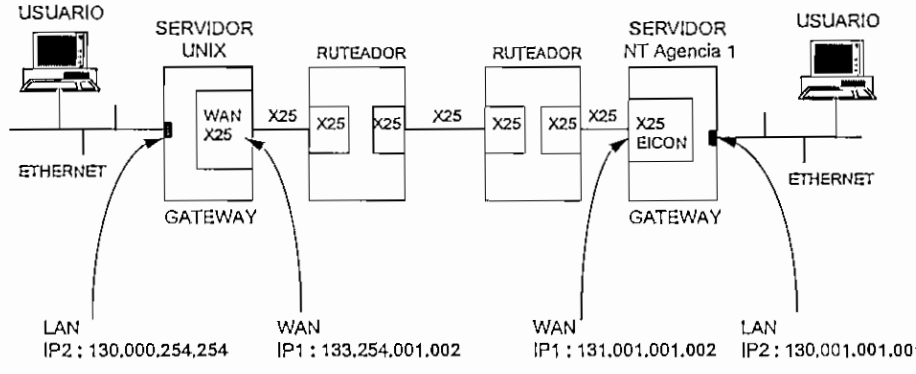


Figura 5.26 Servidores *UNIX* y *NT* actuando como *gateways* de red *Ethernet* a *X.25*

Cuando los servidores *UNIX* y *NT* tienen instalados una tarjeta de red *WAN* X.25 y una de red *LAN Ethernet* como se indica en la figura 5.26, éstos se constituyen en *gateways* de la red. Cada interfaz de red tiene su propia dirección *IP*, lo cual permite unir las redes *Ethernet* remotas a través de la red X.25, como se muestra en la figura 5.26.

En este caso la dirección *IP* del puerto *Ethernet* del servidor es la dirección del *gateway* para los usuarios. Las direcciones *IP* de red *LAN* y de red *WAN* se toman del cuadro 4.1 del Anexo 4.

Cuando se emplea el puerto *Ethernet* del ruteador como se indica en la figura 5.27, no se requiere de tarjetas de red *WAN* X.25 en los servidores. En este caso el ruteador se constituye en el *gateway* de la red.

Los servidores y usuarios se conectan a las demás redes, empleando como dirección de *gateway* , a la dirección *IP* del puerto *Ethernet* del ruteador, como se indica en la figura 5.27.

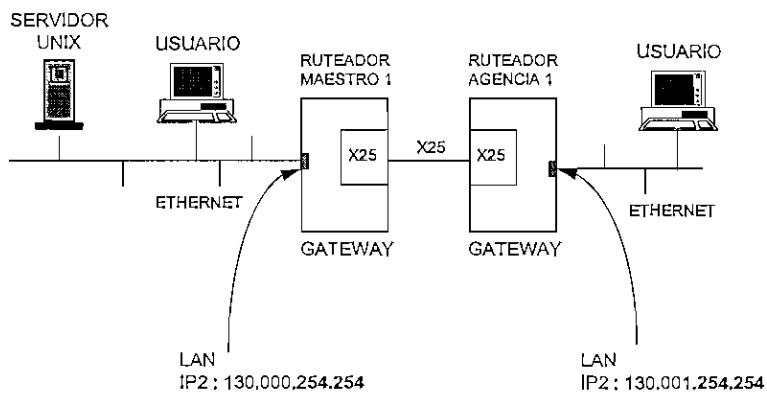


Figura 5.27 Ruteador actuando como gateway de red *Ethernet* a *X.25*

El detalle de la asignación de direcciones *IP* a los servidores y usuarios en la red de la matriz se describe en el Anexo 4.

5.4.2 DISEÑO DE LA RED *LAN* EN AGENCIAS

Para el diseño de la Agencia se sigue los mismos pasos que en la matriz. La red local será tipo *Ethernet* con el ***backbone*** formado por *hubs switching* a los cuales se conectan los servidores de la agencia y los *hubs* comunes que manejan usuarios.

En la agencia los equipos a los que se les asigna direcciones IP son los ruteadores, servidor de agencia y usuarios.

El esquema general de la agencia se muestra en la figura 5.28 y el detalle de las asignaciones *IP* se describen en el Anexo 4.

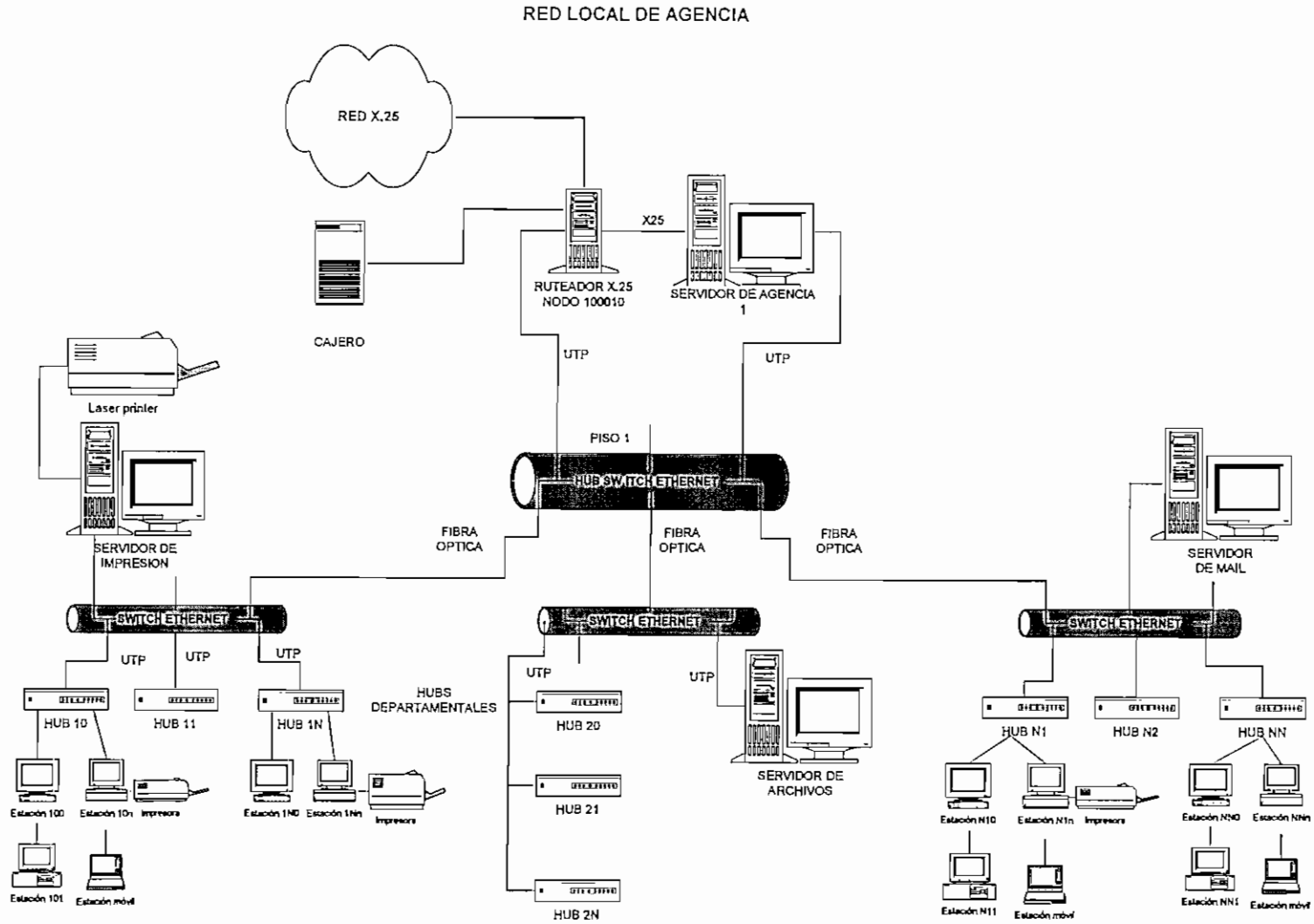


Figura 5.28 Distribución física de red local de Agencia

5.5 DISEÑO DE LA RED *WAN*

5.5.1 DISEÑO DE LA RED WAN X.25

Para la red *WAN* se empleará el protocolo X.25, por cuanto éste realiza un mejor control de los errores de los datos en la red extendida.

- La nube X.25 estará formada por los ruteadores *Codex* 6520, instalados en la matriz y en las agencias como muestra la figura 5.29.

- **En la Matriz**

- En la matriz se colocan dos ruteadores Maestros para tener redundancia en las comunicaciones hacia las agencias, y la disponibilidad de puertos conforme el Banco vaya creciendo .
- Los dos ruteadores maestros van unidos mediante puertos X.25 .
- El número de puertos X.25 requeridos para los ruteadores Maestros viene dado por la fórmula A+1, donde A es el número de agencias incluida la matriz y se añade un puerto porque se requiere uno adicional para enlazar el ruteador maestro redundante.
- A los puertos X.25 de los ruteadores también se puede conectar equipos que tienen tarjetas de red X.25, como son los Servidores *AT&T* que tienen instalados las controladoras Multiprotocolo que manejan X.25 dentro del sistema operativo *UNIX AT&T*.

  Se pueden conectar equipos con tarjeta de red X.25 - *EICON* que operan con Servicios de *WAN* instalados adicionalmente en el *Windows NT* .
- Mediante Servicios de Acceso Remoto de los servidores *NT* que tienen tarjetas de red X.25, se puede accesar a la red *WAN* (ruteadores maestros) en forma directa sin la necesidad de emplear ruteadores adicionales.
- Los equipos que tengan *PCTCP*[5] pueden accesar también en forma remota, mediante el empleo de *SLIP*, hacia el puerto del ruteador maestro, el cual debe ser configurado también con *SLIP*. El ruteador se encarga de encaminar los paquetes hasta el puerto destino. Esto es útil por cuanto, no se requiere de tarjetas de red *WAN* adicionales en las computadoras ni un ruteador para enlazarse hasta la matriz.

---

[5] *PCTCP = Personal Computer Transport Control Protocol* es un paquete que maneja *TCP/IP* , desarrollado por *FTP Software Inc.*

- **En las Agencias**

- En cada una de las agencias se coloca un ruteador al cual se conecta el Servidor de Agencia
- Una de las razones por la que se coloca un ruteador en cada agencia es por que se puede conectar más dispositivos que manejan comunicaciones X.25 a la red *WAN*, como es el caso de los cajeros automáticos, los cuales por regla se han colocado en los sitios donde se instalan las agencias.
- En las agencias pequeñas, donde no exista cajeros automáticos u otros dispositivos X.25 no es necesario colocar el ruteador, ya que los equipos se conectan directamente a la nube mediante el Servicio de Acceso Remoto que funciona tanto en *Windows NT* como también en *Windows* común.

El ***backbone*** de la red está formado por dos ruteadores instalados en el centro de cómputo de la matriz como se muestra en la figura 5.29.

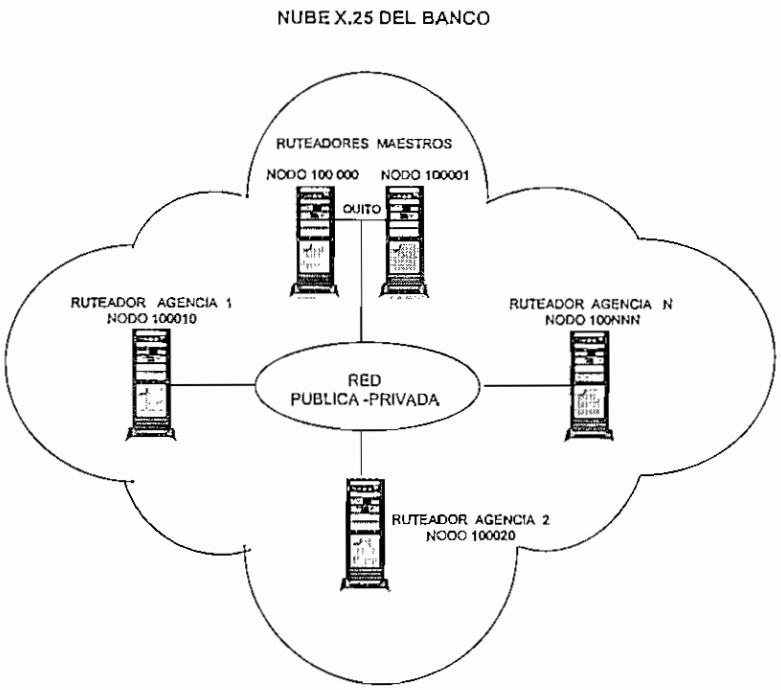


Figura 5.29 Red X.25 del Banco

- El **Ruteador Maestro 1** sirve a las agencias que están ubicadas dentro de la ciudad o en áreas circundantes.

- Del **Ruteador Maestro 2** en adelante sirven a las agencias ubicadas en otras ciudades y provincias.

Las direcciones X.25 en los diferentes equipos tendrán los siguientes formatos:

XXX	YYY

A la dirección XXX se asigna el valor **100** para los ruteadores Maestros y de Agencias. Para los Servidores, *Gateways* y cajeros con puertos de red *WAN* X.25 se asigna la dirección **101** por cuanto son nodos adicionales en la nube X.25.

Equipo	Dirección X25
Ruteadores	100YYY
Servidores	101YYY
Gateways	101YYY
Cajeros	101YYY

Cuadro 5.7 Direcciones X.25 de equipos principales de la red

Las agencias se identificarán con tres dígitos numerados en su inicio de 10 en 10, empezando desde 100**010**.

Los ruteadores que forman el ***backbone*** X.25 tendrán las direcciones más bajas empezando en 100**000** hasta 100**009** , lo que permite tener 10 ruteadores maestros en cascada para una mayor disposición de puertos X.25 en la Matriz.

Por ejemplo los ruteadores maestros tendrán las siguientes direcciones X.25:

Nombre del Ruteador	Dirección X.25
Maestro 1	100**000**
Maestro 2	100**001**
.	.
Maestro 9	100**008**
Maestro 10	100**009**

Cuadro 5.8 Direcciones X.25 de los ruteadores maestros

Los ruteadores de Agencias son numerados en orden de importancia. Las agencias que se ubican dentro de la ciudad donde está la Matriz, tendrán las primeras direcciones, a partir de

100010 y se incrementará de 10 en 10, de acuerdo al número de agencia, como se muestra en el cuadro 5.9.

Nombre del Ruteador	Dirección X.25
Agencia 1	100010
Agencia 2	100020
.	.
Agencia 10	100100
.	.
Agencia 20	100200
.	.
Agencia 99	100990
.	.
Agencia Adicional	100011
Agencia Adicional	100012

Cuadro 5.9 Direcciones X.25 de los ruteadores de Agencia

Note que los números de las agencias coinciden con los dígitos remarcados de la dirección X.25 de los ruteadores. Este procedimiento permite adicionar agencias cuando sea necesario, por cuanto se tiene un margen adicional de 9 direcciones de agencia por cada nodo configurado originalmente.

Además permite asignar direcciones más coherentes a los equipos que manejan X.25 y que están conectados al ruteador.

- La subdirección X.25 está dado por el número de puerto en los nodos y tendrá el formato que se indica en la figura 5. 30.

DIRECCION						SUBDIRECCION
X	X	X	Y	Y	Y	Número de puerto
1	0	0	0	0	0	0 1

Figura 5.30 Formato de dirección y subdirección *X.25*

El número de puerto tiene 2 dígitos conforme al número de puertos instalables en el ruteador. Por ejemplo la asignación de las direcciones X.25 de los puertos en los ruteadores Maestros 1, Maestro 2 y de Agencia 1 se muestra en el cuadro 5.10.

	RUTEADOR MAESTRO 1 Dirección X.25 del Nodo : 100000	RUTEADOR MAESTRO 2 Dirección X.25 del Nodo : 100001	RUTEADOR DE AGENCIA 1 Dirección X.25 del Nodo : 100010
Número de Puerto	Dirección X.25 del Puerto	Dirección X.25 del Puerto	Dirección X.25 del Puerto
1	10000001	10000101	10001001
2	10000002	10000102	10001002
3	10000003	10000103	10001003
.	.	.	.
19	10000019	10000119	10001019

Cuadro 5.10 Direcciones X.25 de los puertos de ruteadores Maestros 1, 2 y de Agencia 1

Los ruteadores Maestros como se observa en el cuadro 5.10, deben tener el mayor número de puertos X.25. Por lo que una configuración posible sería:

- 19 puertos X.25

- 1 puerto *Ethernet.*

A los equipos X.25 adicionales que se conectan a los ruteadores Maestros y de Agencias, como servidores, cajeros, se les asignan las direcciones con el formato **101**YYY, donde la subdirección YYY tiene el siguiente significado:

Dirección 101YYY	
YYY	Equipos Adicionales
101000 a 101009	- Servidores de la Matriz - *Gateways* - Cajeros Automáticos
101010 a 101990	- Servidores de las Agencias - Cajeros

Cuadro 5.11 Significado de la subdirección YYY en adicionales X.25

En la Matriz los servidores X.25 se los numera en orden de importancia desde 101000 hasta 101009. Las direcciones más bajas se asignan a los equipos de mayor jerarquía, que en este caso son los servidores *UNIX* (101000 , 101001), como puede observarse en el cuadro 5.12.

EQUIPOS X.25 ADICIONALES CONECTADOS AL NODO MAESTRO 1	Dirección X.25 del Equipo
Servidor *UNIX* PRODUCCION con X.25	101000
Servidor *UNIX* de DESARROLLO con X.25	101001
Servidor *NT* con tarjeta *EICON* X.25 y Servicios de *WAN*	101002
Servidor *NT* de Agencia sin ruteador enlazándose mediante Acceso Remoto (RAS)	101003
Cajero automático con tarjeta X.25	101004
.	
Equipos adicionales X.25	101009

Cuadro 5.12 Direcciones X.25 de equipos adicionales conectados al ruteador Maestro 1

En las agencias, las direcciones de los Servidores van de **101**010 hasta **101**990 en incrementos de 10 en 10, de modo que los ruteadores y servidores coinciden en el segundo factor de la dirección para tener una mejor identificación como se indica en el cuadro 5.13.

Para los cajeros y equipos X.25 adicionales en las agencias se cambia el último dígito de la dirección en cada agencia como se muestra en el cuadro 5.13.

Número de Agencia	Dirección del Ruteador de Agencia	Dirección del Servidor de Agencia	Dirección del Cajero
1	100010	101010	101011
2	100020	101020	101021
3	100030	101030	101031
.	.	.	.
N	100NNN	101NNN	101NN1

Cuadro 5.13 Dirección X.25 de los servidores y de los cajeros automáticos en las agencias

Las direcciones X.25 de los puertos del nodo MAESTRO 1 y los equipos que se conectan a ellos se muestran en el siguiente cuadro:

ASIGNACION DE PUERTOS DEL RUTEADOR MAESTRO 1			
Dirección X.25 del Nodo: 100000		EQUIPOS X.25 ADICIONALES CONECTADOS AL RUTEADOR	
Número de Puerto	Dirección X.25 del Puerto del Nodo	Equipo Conectado al puerto del ruteador	Dirección X.25 del puerto del Equipo
1	10000001	Ruteador Maestro 2 100001 Puerto1	10000101
2	10000002	Libre para conexión de ruteadores en cascada	
3	10000003	Servidor *UNIX* PRODUCCION con Controlador de *WAN X.25*	101000
4	10000004	Servidor *UNIX* de DESARROLLO con Controlador de *WAN X.25*	101001
5	10000005	Servidor *NT* con tarjeta *EICON* X.25 y Servicios de *WAN*	101002
6	10000006	Servidor *NT* de Agencia sin ruteador enlazándose mediante Acceso Remoto (*RAS*)	101003
7	10000007	Cajero automático con tarjeta X.25	101004
8	10000008	Ruteador de Agencia 1 100010 Puerto 1	10001001
.	.	.	.
19	10000019	Ruteador de Agencia 12 100120 Puerto 1	10012001

Cuadro 5.14 Asignación de direcciones X.25 a los puertos del nodo Maestro 1

Los ruteadores Maestros secundarios utilizan los dos primeros puertos para conectarse en cascada con los otros ruteadores maestros , y el resto son para conectarse al puerto 1 de los ruteadores de Agencias o a los Servidores de agencias mediante Servicio de Acceso Remoto.

Un procedimiento similar se realiza para las Agencias, donde no se tiene más de dos dispositivos X.25 conectados al ruteador, como se indica en el cuadro 5.15 para la Agencia 1.

ASIGNACION DE PUERTOS DEL RUTEADOR DE AGENCIA 1			
Dirección X.25 del Nodo: 100010		EQUIPOS X.25 ADICIONALES EN LA MATRIZ	
Número de Puerto	Dirección X.25 del Puerto del Nodo	Equipo Conectado al puerto del ruteador	Dirección X.25 del puerto del Equipo
1	10001001	Ruteador Maestro 1 100000 Puerto 03	10000003
2	10001002	Servidor *NT* con tarjeta *EICON* X.25 y Servicios de *WAN*	101010
3	10001003	Cajero automático con tarjeta X.25	101011
4		libre	
5		libre	

Cuadro 5.15 Asignación de direcciones X.25 a los puertos del nodo Agencia 1

Por lo tanto en las agencias solo se requiere ruteadores con la mínima configuración:

- 5 puertos X.25
- 1 puerto *Ethernet*

Los servidores de Agencia también se configuran como un nodo más conectado a la nube X.25, asignando una dirección X.25 a la tarjeta de red *WAN EICON* la cual trabaja con software adicional denominado Servicios de *WAN* dentro de *Windows NT*. Se realiza un cuadro de los servidores con sus respectivas direcciones como se indica a continuación:

AGENCIA	NOMBRE DEL SERVIDOR	DIRECCION X25 DE LA TARJETA DE RED *WAN* EICON
Matriz	SERVER01	101000
Matriz	SERVER02	101001
Matriz	MATRIZ	101002
Matriz	.	.
Matriz	NNNNNN	101009
Agencia 1	SERAG001	101010
Agencia 2	SERAG002	101020
Agencia 3	SERAG003	101030
.	.	.
Agencia **N**	SERAG**0NN**	101**NN0**
Agencia sin ruteador	SERAG**NNN** enlazado al nodo maestro 2 con *RAS*	101**NNN**

Cuadro 5.16 Asignación de direcciones X.25 para los servidores de matriz y agencias

La configuración X.25 de los ruteadores maestros y de agencias es la siguiente:

PARAMETROS	MAESTRO 1	MAESTRO 2	AGENCIA 1	AGENCIA 2	AGENCIA N
Node Name	MAESTRO 01	MAESTRO 02	AGENCIA 01	AGENCIA 02	AGENCIA N
Node Address	100001	100002	100010	100020	100nnn
Node Number	001	002	010	020	nnn
Maximum Routing Hops	15	15	15	15	15
Maximum Simultaneous Call	100	100	100	100	100
LAN Connection Subaddres	94	94	94	94	94
Traffic Priority	MED	MED	MED	MED	MED
Traffic Priority Step	8	8	8	8	8
Max Frame Size	2200	2200	2200	2200	2200
Route Selection Table Size	16	16	16	16	16
Mnemonic Table Size	16	16	16	16	16
Number of Network Services channels	1024	1024	1024	1024	1024
PVC Setup Table Size	32	32	32	32	32

Cuadro 5.17 Configuración X.25 de los nodos Maestros y de Agencias

Para establecer los enlaces, los puertos de los ruteadores Maestros y de Agencias deben estar configurados con los mismos parámetros, sólo se diferencian en las direcciones X.25 propias de cada puerto en los respectivos ruteadores. Por ejemplo los puertos del ruteador Maestro 1 tendrá la siguiente configuración:

CONFIGURACION DE LOS PUERTOS X.25 EN NODO MAESTRO 1					
PARAMETROS	PUERTO 1	PUERTO 2	PUERTO 3	PUERTO 4	PUERTO 5
Port Type	X.25	X.25	X.25	X.25	X.25
Connectión Type	Simple	Simple	Simple	Simple	Simple
Clock Source	Externo	Externo	Externo	Externo	Externo
Clock Speed	19200	19200	19200	19200	19200
Link Address	DTE	DCE	DCE	DCE	DCE
Number of PVC Channels	0	0	0	0	0
Number of SVC Channels	32	32	32	32	32
K Frame Window	7	7	7	7	7
W Packet Window	2	2	2	2	2
P Packet Size	256	256	256	256	256
Port Address	10000001	10000002	10000003	10000004	10000005
Reconnection Time out	2	2	2	2	2

Cuadro 5.18 Configuración de los puertos X.25 en el nodo Maestro 1

Los puertos de los servidores *UNIX* que tiene Controladora Multiprotocolos con X.25, servidores de agencia con *Windows NT* con Controladora *EICON X.25* y de los cajeros que tienen puertos *X.25*, deben tener configuraciones similares a los parámetros de los puertos a los cuales van conectados, para que funcionen apropiadamente.

La red *WAN* descrita anteriormente es una red totalmente X.25 donde los servidores de agencia están unidos a la red mediante X.25, como se muestra en la figura 5.31.

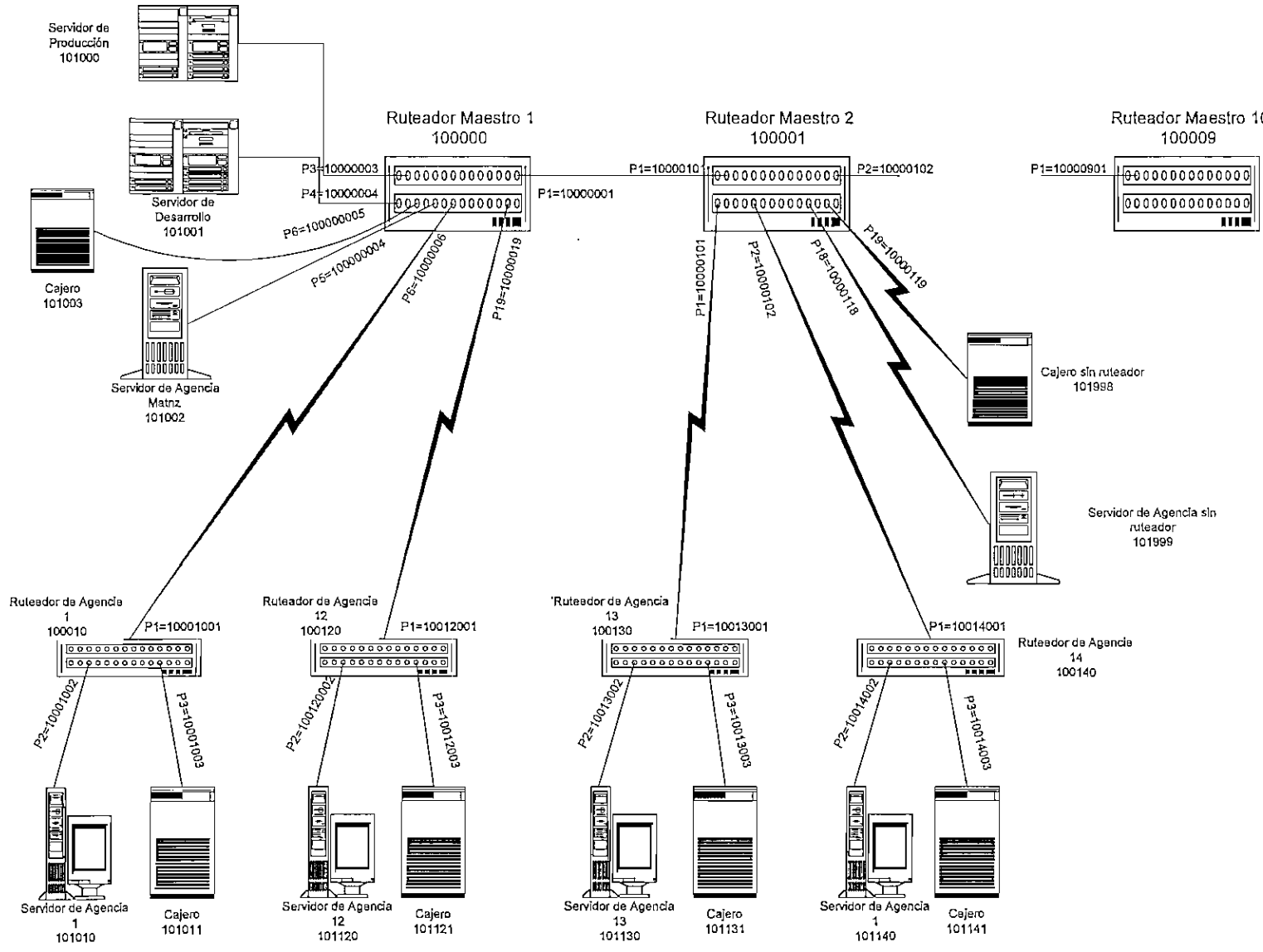


Figura 5.31 Direcciones X.25 de Servidores, ruteadores, cajeros automáticos en la matriz y agencias

5.5.1.1 TABLAS DE RUTAS X.25 DE LOS NODOS

- Las tablas de rutas X.25 en un ruteador tienen el siguiente formato:

TABLA DE RUTAS DEL NODO 100						
Registro	Dirección X.25	Destino	Prioridad	....	Destino	Prioridad
1	200	X25-1	1		X25-2	2
2	300	X25-2	1	....	X25-5	4
3						

Cuadro 5.19 Tabla de rutas del Nodo 100 del ejemplo de la figura 5.32

Para análisis se ha escogido una red formada por los tres ruteadores de la figura 5.32.

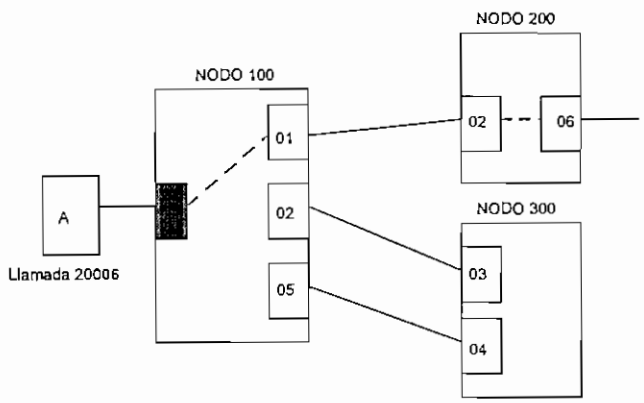


Figura 5.32 Ejemplo de conexión de ruteadores a través de X.25

Cada registro está compuesto por dirección, destino y prioridad:

- La **Dirección X25** , es la dirección X25 del equipo remoto al cual se llama para entregar un paquete.
- El **Destino** , es el número de un puerto del nodo local a donde se debe enviar la llamada para alcanzar el destino.
- La **Prioridad** , permite escoger el camino más óptimo.

La forma de operar es la siguiente:

- Si el equipo **A** quiere enlazarse al puerto **06** del nodo 200, hace una llamada con la dirección **20006** .
- El nodo 100 examina sus tablas y determina que el camino óptimo para alcanzar el nodo 200 es a través de su puerto local **01** y encamina la llamada hacia este puerto.
- El paquete abandona el nodo 100 por el puerto 01 y llega al puerto 02 del nodo 200.
- El nodo 200 examina la subdirección **06** y envía la llamada hacia su puerto **06** .

- La subdirección X.25 del *WAN Adapter* es **94** , la cual se direcciona también en la tabla de rutas, para unir los puertos X.25 con el puerto de red local *Ethernet*, mediante conexiones lógicas de *lan* ***LCONs*** cuando se emplea **enrutamiento *IP***. Tiene prioridad secundaria, es decir se lo utilizará cuando los nodos estén muy congestionados para accesar a la red *Ethernet* local .

Basándose en los criterios anteriores se configura las tablas de rutas X.25 para los Nodos. Por ejemplo para los ruteadores **MAESTRO 1** y **MAESTRO 2** las tablas de rutas X.25 son :

TABLA DE RUTAS DEL RUTEADOR MAESTRO 1 100000			
Registro	Dirección X.25	Destino	Prioridad
1	100001*	X.25 - 01	1
2	100002*	X.25 - 01	1
.	.	.	.
9	100009*	X.25 - 01	1
	Ruteadores Agencias		
10	100010*	X.25 - 08	1
11	100020*	X.25 - 09	1
12	100030*	X.25 - 10	1
.	.	.	.
19	100100*	X.25 - 17	1
20	100110*	X.25 - 18	1
21	100120*	X.25 - 19	1
22	100130*	X.25 - 01	1
23	100140*	X.25 - 01	1
24	100150*	X.25 - 01	1
.	.	.	.
.	100nnn*	X.25 - 01	1
	Servidores de Matriz		
x	101000*	X.25 - 03	1
x+1	101001*	X.25 - 04	1
x+2	101002*	X.25 - 05	1
.	101003*	X.25 - 06	1
.	101004*	x25 - 07	1
	Servidores de Agencias		
y	101010*	X25 - 08	1
y+1	101020*	X.25 - 09	1
y+2	101030*	X.25 - 10	1
.	101040*	X.25 - 11	1
.	.	.	.
.	101012*	X.25 - 19	1
.	101013*	X.25 - 01	1
.	101014*	X.25 - 01	1
.	.	.	.
.	.	.	.
.	101nnn*	X.25 - 01	1
z	10000094	LCON	2

TABLA DE RUTAS DEL RUTEADOR MAESTRO 2 100001			
Registro	Dirección X.25	Destino	Prioridad
1	100000*	X.25 - 01	1
2	100002*	X.25 - 02	1
3	100003*	X.25 - 02	1
.	.	.	.
9	100009*	X.25 - 02	1
	Ruteadores de Agencia		
10	100010*	X.25 - 01	1
.	.	"	"
20	100110*	X.25 - 01	1
21	100120*	X.25 - 01	1
22	100130*	X.25 - 03	1
23	100140*	X.25 - 04	1
24	100150*	X.25 - 05	1
25	100160*	X.25 - 06	1
.		.	.
36	100290*	X.25 - 19	1
37	100280*	X.25 - 02	1
38	100290*	X.25 - 02	1
39	100300*	X.25 - 02	1
.	.	"	.
.	.	"	.
	100nn0*	X.25 - 02	1
	Servidores de Agencia		
x	101000*	X.25 -01	1
. .	. .	. .	. .
.	101120*	X.25 - 01	1
.	101130*	X.25 - 03	1
.	101140*	X.25 - 04	1
.	101150*	X.25 - 05	1
.	101160*	X.25 - 06	1
.	.	.	.
.	101290*	X.25 - 19	1
.	101300*	X.25 - 02	1
.	101310*	X.25 - 02	1
.	.	.	.
.	101990*	X25 - 02	1
y	10000194	LCON	2

Cuadro 5.20 Tabla de rutas X.25 en los ruteadores Maestro 1 y Maestro2

* Considera como válidas a todas las direcciones que empiezan con la secuencia que está anterior al asterisco.

Por el puerto 01 del ruteador MAESTRO 1 se accesa a los ruteadores maestros restantes, a los ruteadores de Agencias conectados a éstos y a los servidores que van conectados a los ruteadores de Agencia a partir de la AGENCIA 13.

- Para el nodo AGENCIA 1 la configuración de las tablas de rutas es la siguiente:

TABLA DE RUTAS DEL NODO AGENCIA 1 100010			
Registro	Dirección X.25	Destino	Prioridad
1	100000*	X.25 - 01	1
2	100001*	X.25 - 01	1
.	.	"	.
11	100020*	X.25 - 01	1
12	100030*	X.25 - 01	1
.	.	"	.
.	100nn0*	X.25 - 01	1
	Servidores		
.	101000*	X.25 - 01	1
.	101001*	X.25 - 01	1
.	.	"	.
.	101009*	X.25 - 01	1
.	101010* servidor de agencia local	X.25 - **02**	1
.	101011* cajero automático	X.25 -03	1
.	101020*	X.25 - **01**	1
.	101030*	X.25 - 01	1
.	.	"	.
.	101nn0*	X.25 - 01	1
y	10001094	LCON	2

Cuadro 5.21 Tabla de rutas X.25 en el nodo de Agencia 1

- Desde una agencia se alcanza el resto de nodos a través del puerto **01** del nodo local.
- Cuando el servidor tiene solo puerto *Ethernet*, se cambia la prioridad de *LCON* a **1**, con lo cual el ruteador entrega los paquetes directamente a la red *Ethernet* de la agencia.

5.5. 2 DISEÑO DE LA RED *WAN TCP/IP* EN X.25

Para la red *TCP/IP* se escoge una red **Clase B** que tiene hasta 2^{16} usuarios por cada red escogida, lo que permite un crecimiento a futuro de la red global *TCP/IP*.

El formato del direccionamiento *IP* es ***red.red.host.host***

Para razones de diseño se parte de una dirección de red base que corresponde a la dirección de red de la **matriz**.

RED 130.000.000.000 MASCARA 255.255.000.000

- A partir de estos valores se va generando el resto de redes y subredes, tanto para las *LAN* como para las *WAN*, en donde se involucra el direccionamiento *IP* sobre X.25 en los ruteadores.
- Para la red *WAN* se crean redes *IP* exclusivas por cada enlace físico entre nodos desde las agencias hasta los ruteadores maestros de la matriz. Esto permite tratar a la red en tramos independientes para un mejor enrutamiento de paquetes, monitoreo y administración de los enlaces a través de X.25. Además aisla la interferencia entre redes *IP*, mediante una correcta tabla de rutas.
- Cada puerto del ruteador tendrá su propia dirección *IP* para enrutar los paquetes que vienen desde las diferentes redes.

  Por conveniencia las direcciones *IP* para los puertos de *WAN* se las asigna con las direcciones menos significativas de cada red. Por ejemplo para el enlace entre los Ruteadores Maestros 1 y 2 se tiene el siguiente direccionamiento:

MAESTRO 1	MAESTRO 2
Dirección *IP* del Puerto 1	Dirección *IP* del Puerto 1
133.001.001.001	133.001.001.002

Cuadro 5.22 Direcciones IP del puerto 1 en los ruteadores Maestro 1 y Maestro 2

Note que las dos direcciones *IP* corresponden a una misma red.

- La asignación de redes *IP* se realiza mediante **13Y.XXX.000.000**, donde XXX es el número de agencia y la Y corresponde al orden jerárquico de la red. El *backbone* de la red determina la jerarquía ya que es la columna de la red *IP*.

- Las redes *IP* que se necesitan para una mejor identificación de la red son:

  . **130.XXX**.000.000

  . **131.XXX**.000.000

  . **132.XXX**.000.000

  . **133.XXX**.000.000

- La red **130.XXX** corresponde a la dirección de las redes locales de la matriz y las agencias.

La matriz tiene la dirección de red **130.000**.000.000, en tanto que para la dirección de red de las agencias el segundo término de red va incrementándose de acuerdo al número de agencia correspondiente, como se muestra en el cuadro 5.23.

AGENCIA	DIRECCION DE RED IP
MATRIZ	**130.000**.000.000
AGENCIA 1	**130.001**.000.000
AGENCIA 2	**130.002**.000.000
AGENCIA 3	**130.003**.000.000
. .	. .
AGENCIA N	**130.NNN**.000.000

Cuadro 5.23 Dirección *IP* de redes locales de la Matriz y de las Agencias

- Las redes **131.XXX** corresponden a las redes independientes entre los Ruteadores de Agencia con los respectivos Servidores, los cuales están enlazados mediante X.25, donde XXX corresponde al número de agencia o al número de servidor de agencia.

En cada una de estas redes, se tiene solo dos direcciones *IP*, la primera identifica al puerto del ruteador y la segunda al puerto *WAN EICON* del servidor. La dirección *IP* asignada al ruteador es menor que la del puerto *EICON* del servidor. Por ejemplo en la **Agencia 1** se tiene las siguientes direcciones *IP*:

. Puerto de ruteador 131.001.**001.001**

. Servidor (puerto *WAN*) 131.001.**001.002**

El cuadro 5.24 indica las direcciones *IP* del puerto de los servidores de agencia y de los respectivos ruteadores a los que están conectados.

AGENCIA	Dirección IP del puerto del Ruteador de Agencia	Dirección IP del puerto del Servidor de Agencia
AGENCIA 1	**131.001**.001.001	**131.001**.001.002
AGENCIA 2	**131.002**.001.001	**131.002**.001.002
AGENCIA 3	**131.003**.001.001	**131.003**.001.002
. .	. .	. .
AGENCIA N	**131.NNN**.001.001	**131.NNN**.001.002

Cuadro 5.24 Direcciones IP entre los ruteadores de agencia y los respectivos servidores de agencia

- Las direcciones **132.XXX** pertenecen a las redes *IP* formadas por los enlaces X.25 entre los ruteadores Maestros y los ruteadores de cada agencia. El valor XXX corresponde al número de agencia. Del mismo modo, los puertos de los ruteadores maestros tienen la dirección *IP* inferior a la de los ruteadores de cada agencia remota, como se indica en el cuadro 5.25.

AGENCIA	Dirección IP del puerto del Ruteador Maestro	Dirección IP del puerto del Ruteador de Agencia
AGENCIA 1	**132.001**.001.001	**132.001**.001.002
AGENCIA 2	**132.002**.001.001	**132.002**.001.002
AGENCIA 3	**132.003**.001.001	**132.003**.001.002
.	.	.
AGENCIA N	**132.NNN**.001.001	**132.NNN**.001.002

Cuadro 5.25 Direcciones *IP* entre el ruteador Maestro y los ruteadores de agencia

- Las redes **133.XXX**.000 se utilizan para direccionar el *Backbone* X.25 formado por los ruteadores Maestros colocados en cascada, donde XXX corresponde a la red formada por el enlace entre ruteadores maestros. La dirección asignada para estos enlaces son de valor bajo, de modo que la dirección menor tiene el ruteador maestro precedente.

Dentro de estas redes se colocan las redes *IP* formadas por los enlaces X.25 entre los Servidores *UNIX*, *NT*, Agencia Matriz, Cajeros con el ruteador MAESTRO 1. Las direcciones de red *IP* de estos enlaces tienen valores altos, empezando con **133.254**.001.002 para el Servidor *UNIX* de PRODUCCION y **133.254**.001.001 para el ruteador MAESTRO 1, los cuales forman la red **133.254.0.0**, y se va disminuyendo el segundo factor de red para los otros enlaces como indica el cuadro 5.26.

Servidor	Dirección IP del Servidor	Dirección IP del Ruteador MAESTRO 1
UNIX PRODUCCION	*WAN*: **133.254**.001.002 *LAN*: **130.000**.001.001	**133.254**.001.001
UNIX DESARROLLO	*WAN*: **133.253**.001.002 *LAN*: **130.000**.001.002	**133.253**.001.001
SERVIDOR NT	*WAN*: **133.252**.001.002 *LAN*: **130.000**.001.003	**133.252**.001.001
SERVIDOR DE CAJEROS	*WAN*: **133.251**.001.002 *LAN*: **130.000**.001.004	**133.251**.001.001
SERVIDOR DE AGENCIA MATRIZ	*WAN*: **133.250**.001.002 *LAN*: **130.000**.001.005	**133.250**.001.001
SERVIDOR DE ACCESO REMOTO	*WAN*: **133.249**.001.002 *LAN*: **130.000**.001.006	**133.249**.001.001

Cuadro 5.26 Direcciones *IP* de red local y extendida de los servidores de la Matriz y dirección *IP* de red extendida del ruteador Maestro 1 al cual se conectan los servidores

Las tarjetas de red *WAN* y de red *LAN* de los Servidores *UNIX* y de los servidores de las agencias también tendrán su propia dirección de red. Por lo tanto estas computadoras se constituyen en *gateways* que permiten el paso de red *Ethernet* a X.25.

- La estructura de las redes mencionadas anteriormente se muestran en la figura 5.33.

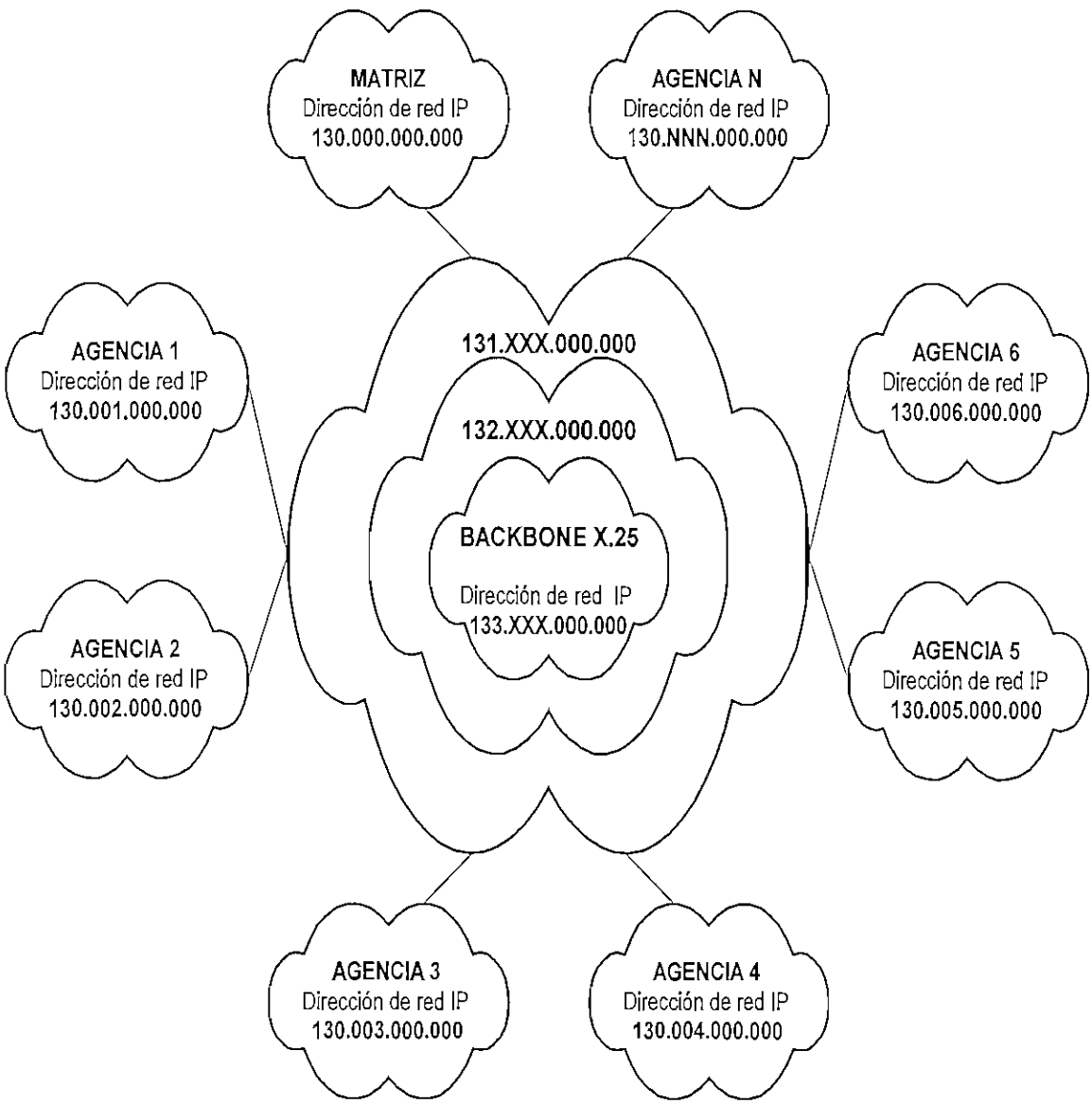


Figura 5.33 Estructura general de la red *TCP/IP* en el Banco

Se establece una tabla de correspondencia de direcciones X.25 con sus respectivas direcciones *IP* en cada uno de los puertos de los ruteadores. Además se debe especificar las dirección *IP* y X.25 de los destinos.

El cuadro 5.27 muestra la correspondencia X.25 con *IP* de los puertos del ruteador Maestro 1 y sus respectivos destinos.

CONFIGURACION *IP* DE LOS PUERTOS DEL RUTEADOR MAESTRO 1						
ORIGEN			DESTINO			
Número Puerto	Dirección X.25 del puerto	Dirección *IP* del Puerto	Dispositivo Destino	Número Puerto	Dirección X.25 del puerto	Dirección *IP* del Puerto
P1	10000001	133.001.001.001	Ruteador MAESTRO 2	P1	100001	133.001.001.002
P2	10000002	133.001.xxx.xxx	Libre para cascada			
P3	10000003	133.254.001.001	*UNIX* PRODUCCION	P1	101000	133.254.001.002
P4	10000004	133.253.001.001	*UNIX* DESARROLLO	P1	101001	133.253.001.002
P5	10000005	133.252.001.001	*WINDOWS NT*	EICON	101003	133.252.001.002
P6	10000006	133.251.001.001	CAJERO	P1	101004	133.251.001.002
P7	10000007	133.250.001.001	Libre			
P8	10000008	132.001.001.001	Ruteador AGENCIA 1	P1	100010	132.001.001.002
P9	10000009	132.002.001.001	Ruteador AGENCIA 2	P1	100020	132.002.001.002
P10	10000010	132.003.001.001	Ruteador AGENCIA 3	P1	100030	132.003.001.002
P11	10000011	132.004.001.001	Ruteador AGENCIA 4	P1	100040	132.004.001.002
P12	10000012	132.005.001.001	Ruteador AGENCIA 5	P1	100050	132.005.001.002
P13	10000013	132.006.001.001	Ruteador AGENCIA 6	P1	100060	132.006.001.002
P14	10000014	132.007.001.001	Ruteador AGENCIA 7	P1	100070	132.007.001.002
P15	10000015	132.008.001.001	Ruteador AGENCIA 8	P1	100080	132.008.001.002
P16	10000016	132.009.001.001	Ruteador AGENCIA 9	P1	100090	132.009.001.002
P17	10000017	132.010.001.001	Ruteador AGENCIA 10	P1	100100	132.010.001.002
P18	10000018	132.011.001.001	Ruteador AGENCIA 11	P1	100110	132.011.001.002
P19	10000019	132.012.001.001	Ruteador AGENCIA 12	P1	100120	132.012.001.002
ETHERNET		130.000.254.254	***LCON*** (Conexión *LAN*)			

Cuadro 5.27 Configuración *IP* de los puertos del ruteador Maestro 1

En el ruteador Maestro 1 el puerto *Ethernet* se configura con la dirección *IP* 130.000.**254.254**, formando parte de la red local de la matriz; para el resto de ruteadores maestros se va disminuyendo el último término de la dirección de red. Este puerto se lo emplea cuando los servidores no tienen puerto de *WAN*, pero tienen un puerto *Ethernet*; por tal motivo tanto el ruteador como los servidores se conectan directamente a la red *Ethernet*. En estos casos el ruteador es la pasarela (*gateway*) entre la red *Ethernet* de la matriz y la red X.25 sincrónica.

El cuadro 5.28 indica la correspondencia X.25 con *IP* en el ruteador MAESTRO 2:

CONFIGURACION IP DE LOS PUERTOS DEL RUTEADOR MAESTRO 2						
ORIGEN			DESTINO			
Número Puerto	Dirección X.25 del Puerto	Dirección IP del Puerto	Dispositivo Destino	Número Puerto	Dirección X.25 del puerto	Dirección IP del Puerto
P1	10000101	133.001.001.002	Ruteador MAESTRO 1	P1	100000	133.001.001.001
P2	10000102	133.002.001.001	Ruteador MAESTRO 3	P1	100002	133.002.001.002
P3	10000103	132.013.001.001	Ruteador AGENCIA 13	P1	100130	132.013.001.002
P4	10000104	132.014.001.001	Ruteador AGENCIA 14	P1	100140	132.014.001.002
P5	10000105	132.015.001.001	Ruteador AGENCIA 15	P1	100150	132.015.001.002
P6	10000106	132.016.001.001	Ruteador AGENCIA 16	P1	100160	132.016.001.002
P7	10000107	132.017.001.001	Ruteador AGENCIA 17	P1	100170	132.017.001.002
P8	10000108	132.018.001.001	Ruteador AGENCIA 18	P1	100180	132.018.001.002
P9	10000109	132.019.001.001	Ruteador AGENCIA 19	P1	100190	132.019.001.002
P10	10000110	132.020.001.001	Ruteador AGENCIA 20	P1	100200	132.020.001.002
P11	10000111	132.021.001.001	Ruteador AGENCIA 21	P1	100210	132.021.001.002
P12	10000112	132.022.001.001	Ruteador AGENCIA 22	P1	100220	132.022.001.002
P13	10000113	132.023.001.001	Ruteador AGENCIA 23	P1	100230	132.023.001.002
P14	10000114	132.024.001.001	Ruteador AGENCIA 24	P1	100240	132.024.001.002
P15	10000115	132.025.001.001	Ruteador AGENCIA 25	P1	100250	132.025.001.002
P16	10000116	132.026.001.001	Ruteador AGENCIA 26	P1	100260	132.026.001.002
P17	10000117	132.027.001.001	Ruteador AGENCIA 27	P1	100270	132.027.001.002
P18	10000118	132.028.001.001	Ruteador AGENCIA 28	P1	100280	132.028.001.002
P19	10000119	132.029.001.001	Ruteador AGENCIA 29	P1	100290	132.029.001.002
ETHERNET		130.000.254.253	***LCON*** (Conexión *LAN*)			

Cuadro 5.28 Configuración *IP* de los puertos del nodo Maestro 2

Para el resto de ruteadores MAESTROS se sigue un procedimiento similar.

- En las agencias se configuran los puertos del ruteador de agencia y el puerto *WAN EICON* de los Servidores *NT*. El enlace ruteador - servidor de agencia tiene la red **131.XXX** y el enlace ruteador de agencia hacia el ruteador maestro tiene la red **132.XXX** donde XXX es el número de agencia.

En este caso la asignación de direcciones *IP* se realiza mediante el siguiente esquema:

- red **132.xxx** - 132.xxx.001.001 ruteador maestro
  - 132.xxx.001.002 ruteador de agencia
- red 131.xxx - 131.xxx.001.001 ruteador de agencia
  - 131.xxx.001.002 puerto *EICON* del servidor de agencia

Para el caso de la AGENCIA 1 la red *IP* es 131.**001**, y la correspondencia X.25 - IP de los puertos del ruteador de Agencia **1** con sus respectivos destinos se indica en el cuadro 5.29.

CONFIGURACION IP DE LOS PUERTOS DEL RUTEADOR AGENCIA 1 X.25 : 100010						
ORIGEN			**DESTINO**			
Número Puerto	**Dirección X.25 del puerto**	**Dirección *IP* del Puerto**	**Dispositivo Destino**	**Número Puerto**	**Dirección X.25**	**Dirección *IP* del Puerto**
P1	10001001	132.001.001.002	Ruteador MAESTRO 1	P8	100000	132.001.001.001
P2	10001002	**131.001**.001.001	Servidor de Agencia	EICON	101010	131.001.001.002
P3	10001003					
P4	10001004					
P5	10001005					
ETHERNET		130.001.254.254	***LCON*** (Conexión *LAN*)			

Cuadro 5.29 Configuración *IP* de los puertos del ruteador de la Agencia 1

En los ruteadores de las agencias se configura también el puerto *Ethernet* con la dirección *IP* 130.**XXX**.254.254 donde XXX es el número de agencia. Este puerto se emplea cuando los servidores de agencia no tienen puerto de *WAN* , pero tienen un puerto *Ethernet.*

Si el servidor de agencia tiene solo puerto *Ethernet* la dirección *IP* es 130.**XXX**.001.0001, donde XXX es el número de la agencia.

- En los servidores de agencia se asignan direcciones *IP* al puerto de red *LAN* y red *WAN* .

Al puerto X.25 (*EICON*) del servidor de agencia se le asigna una dirección *IP* baja dentro de la red, pero superior a la dirección del puerto del ruteador, para diferenciar del resto de direcciones *IP* ordinarias.

Al puerto *Ethernet* para diferenciarlo se le asigna la dirección **130.XXX.001.001**, donde XXX es el número de la agencia.

Por lo tanto estos servidores se constituyen en *gateways* que permiten el paso de *Ethernet* a X.25.

La disposición general de la red *WAN IP* establecida se muestra en la figura 5.34.

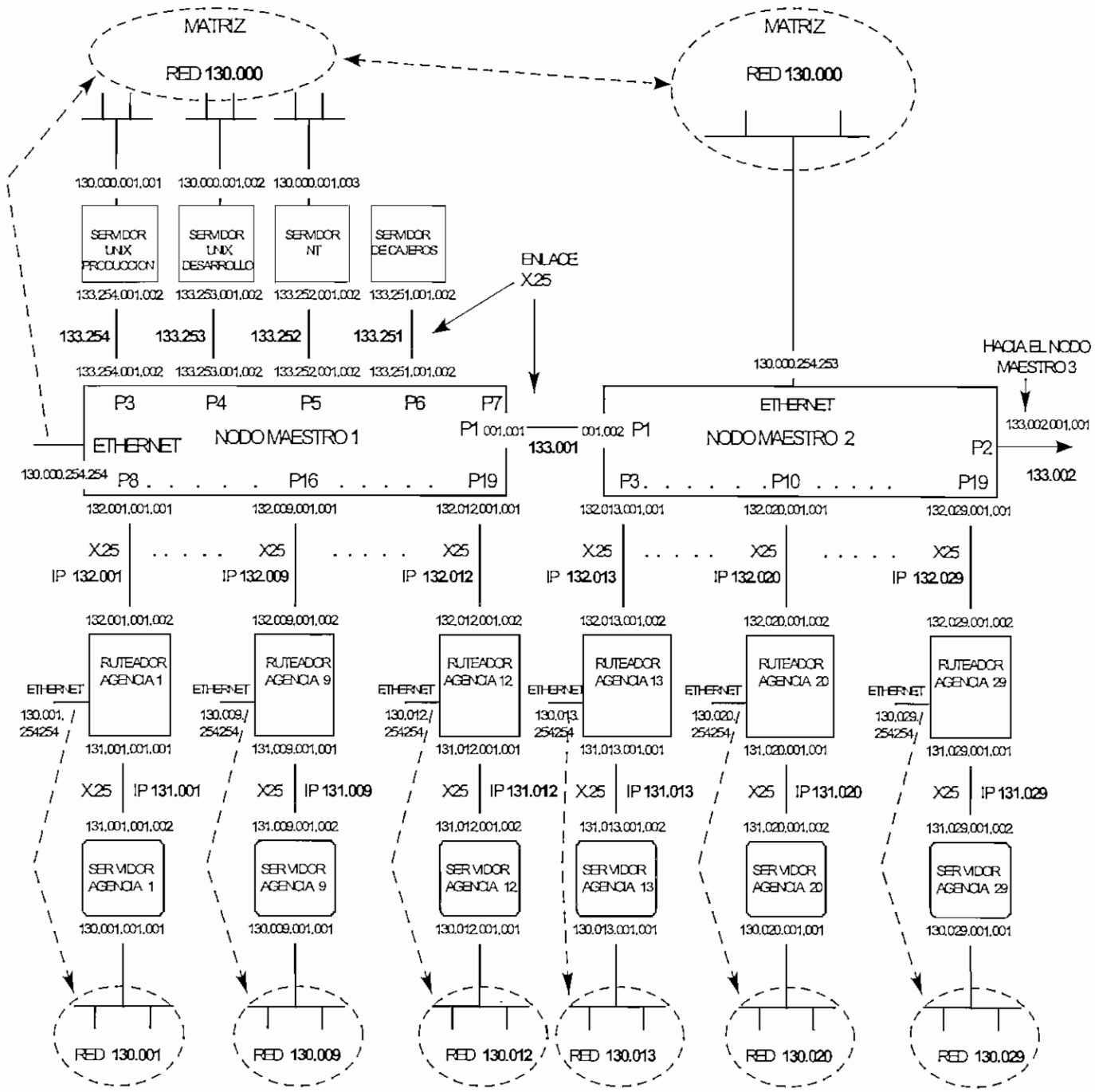


Figura 5.34 Disposición general de la red TCP/IP del Banco
Redes *IP* extendidas y locales en agencias

La correspondencia de *IP* con X.25 en cada uno de los dispositivos de la red , se muestra en la figura 5.35.

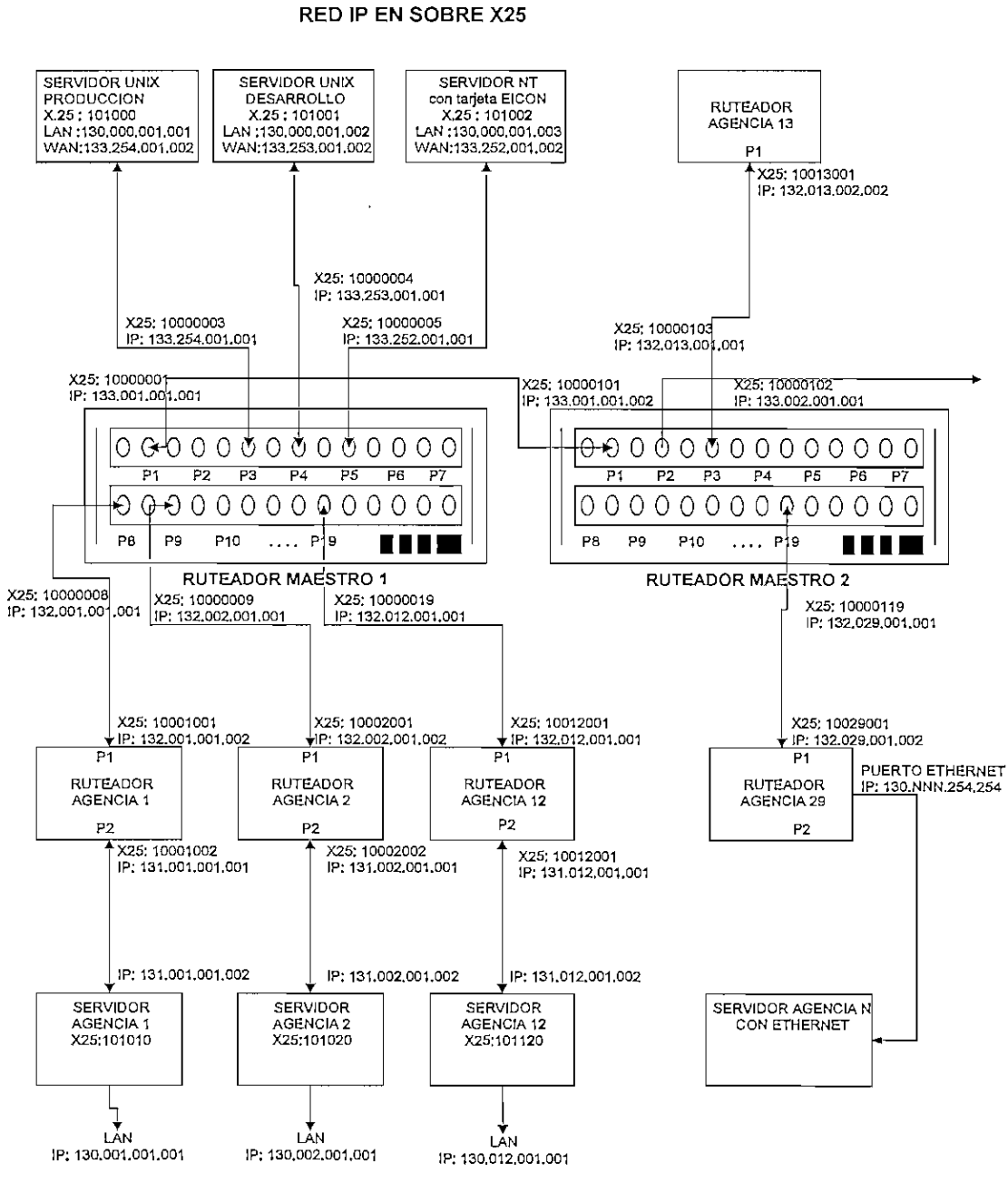


Figura 5.35 Correspondencia de direcciones IP con direcciones X.25 en cada dispositivo de la red

Los paquetes *IP* son encapsulados en X.25 usando la norma *RFC877*, en donde el paquete *IP* corresponde a la parte de datos de la trama X.25 como se describió en el capítulo 3.

- En los ruteadores se debe configurar la tabla de interfaces de enrutamiento de *LAN* y de *WAN*, para que los paquetes *IP* puedan ser enrutados hacia sus destinos. La disposición de los módulos mencionados se muestra en la figura 5.36.

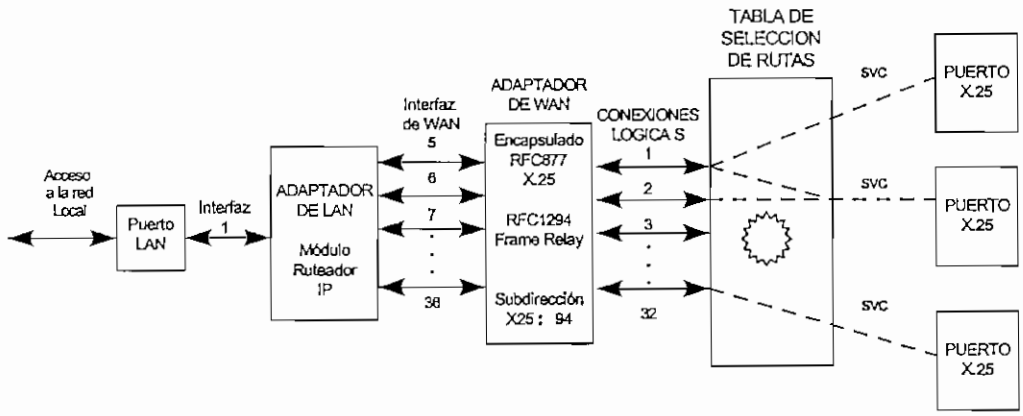


Figura 5.36 Diagrama de bloques de un ruteador

- El adaptador de *WAN* enlaza el puerto de *LAN* con los puertos de *WAN*, conectando los interfaces de enrutamiento *WAN* a circuitos virtuales conmutables de los puertos X.25.

  . El interfaz de red local se identifica como interfaz **1**.

  . Hay 32 interfaces de enrutamiento *WAN*, numeradas de **5-36** , por lo que se tiene hasta **32 Conexiones Lógicas** por ruteador hacia 32 agencias remotas como máximo.

- La conexión entre dos ruteadores X.25 se muestra en la figura 5.37.

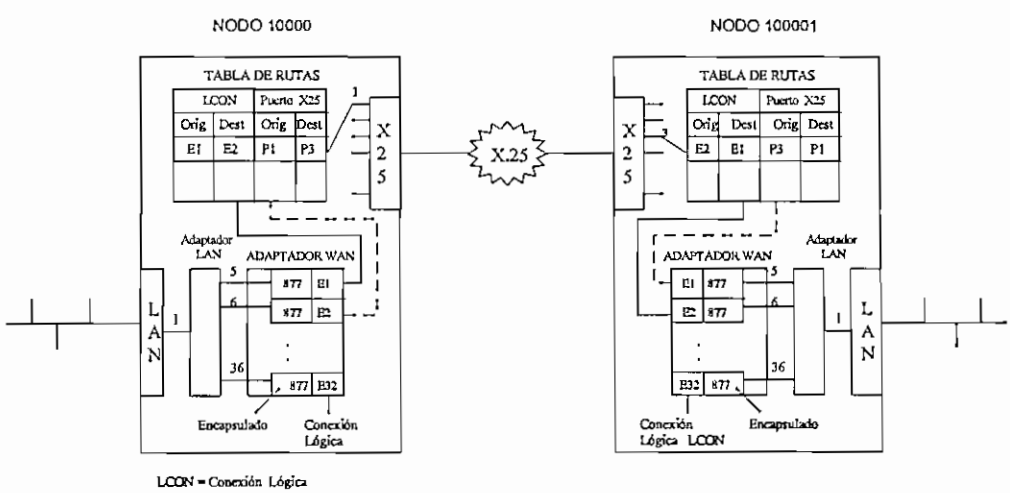


Figura 5.37 Enlace con enrutamiento *IP* sobre X.25

- Cada **Interfaz de Enrutamiento** de *LAN* y *WAN* se configura con una dirección *IP* única.

El interfaz de *LAN* debe tener una dirección *IP* que pertenezca a la red local.

A cada interfaz de enrutamiento *WAN* le corresponde una sola conexión lógica con un puerto X.25 determinado, como se indica en el cuadro 5.30 para el ruteador Maestro 1.

CONFIGURACION DE INTERFACES DE ENRUTAMIENTO DEL RUTEADOR MAESTRO 1			
NUMERO DE INTERFAZ	DIRECCION IP DEL INTERFAZ	NUMERO DE CONEXION LÓGICA	PUERTO CORRESPONDIENTE
1	130.000.254.254	1	*ETHERNET*
2	no usado	no usado	no usado
3	no usado	no usado	no usado
4	no usado	no usado	no usado
5	133.001.001.001	2	Puerto 1 X25
6	133.249.001.001	3	Puerto 2 X25
7	133.254.001.001	4	Puerto 3 X25
8	133.253.001.001	5	Puerto 4 X25
9	133.252.001.001	6	Puerto 5 X25
10	133.251.001.001	7	Puerto 6 X25
11	133.250.001.001	8	Puerto 7 X25
12	132.001.001.001	9	Puerto 8 X25
13	132.002.001.001	10	Puerto 9 X25
14	132.003.001.001	11	Puerto 10 X25
15	132.004.001.001	12	Puerto 11 X25
16	132.005.001.001	13	Puerto 12 X25
17	132.006.001.001	14	Puerto 13 X25
18	132.007.001.001	15	Puerto 14 X25
19	132.008.001.001	16	Puerto 15 X25
20	132.009.001.001	17	Puerto 16 X25
21	132.010.001.001	18	Puerto 17 X25
22	132.011.001.001	19	Puerto 18 X25
23	132.012.001.001	20	Puerto 19 X25
24	Libre	21	
25	Libre	22	Puerto x X25
26	Libre	23	
27	Libre	24	Puerto x X25
.	Libre	.	
.	Libre	.	
36	Libre	32	Puerto x X25

Cuadro 5.30 Direcciones *IP* de los interfaces de enrutamiento del nodo Maestro 1

- Los interfaces libres se los puede asignar a un puerto ya configurado o a cualquier otro puerto que se adicione.

- El ruteador de la AGENCIA 1, ocupa sólo 5 interfaces para los 5 puertos, el resto de interfaces y conexiones lógicas están disponibles para utilizarlos cuando se añadan puertos al ruteador. Este ruteador tendrá la siguiente configuración de sus interfaces:

CONFIGURACION DE INTERFACES DE ENRUTAMIENTO DEL RUTEADOR AGENCIA 1			
NUMERO DE INTERFAZ	DIRECCION *IP* DEL INTERFAZ	NUMERO DE CONEXION LÓGICA	PUERTO CORRESPONDIENTE
1	130.001.254.254	1	ETHERNET
2	no usado	no usado	no usado
3	no usado	no usado	no usado
4	no usado	no usado	no usado
5	132.001.001.002	2	Puerto 1 X25
6	131.001.001.001	3	Puerto 2 X25
7	131.001.002.001	4	Puerto 3 X25
8	131.001.003.001	5	Puerto 4 X25
9	131.001.004.001	6	Puerto 5 X25
10	Libre	7	Libre
11	Libre	8	Libre
.	Libre	.	Libre
.	Libre	.	Libre
.	Libre	.	Libre
.	Libre	.	Libre
36	Libre	32	Libre

Cuadro 5.31 Direcciones *IP* de los interfaces de enrutamiento del nodo de Agencia 1

5.5.2.1 TABLAS DE RUTAS *IP* DE LOS RUTEADORES

Las tablas de rutas *IP* están formados por registros, cada uno de los cuales contiene la dirección de red destino , la dirección *IP* del siguiente ruteador por el cual se puede pasar para alcanzar la red, y el número de saltos que se necesita para llegar a la red destino.

El número de saltos, es el número de ruteadores (incluido el ruteador local) que el datagrama debe atravesar para llegar a la red destino.

El ejemplo de la figura 5.38 permite ilustrar el funcionamiento de las tablas de enrutamiento *IP* en los ruteadores enlazados a través de X.25.

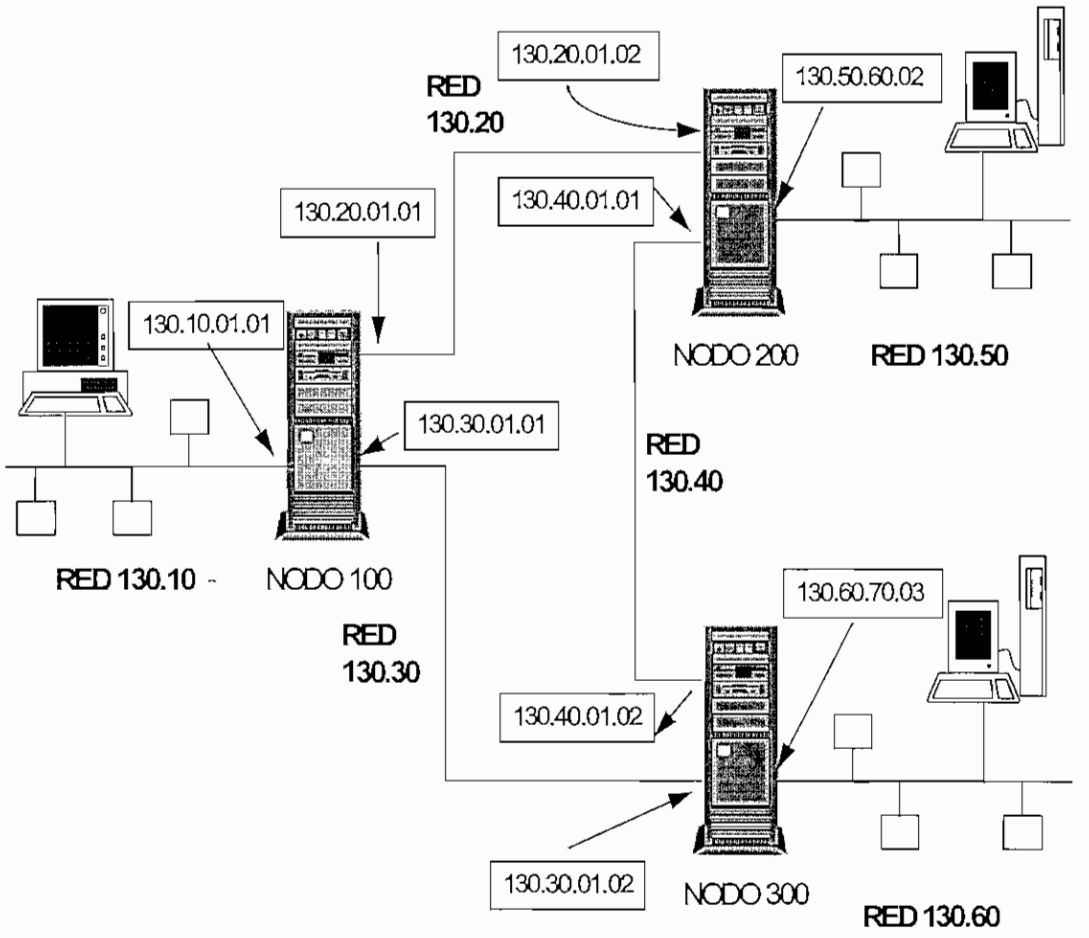


Figura 5.38 Ejemplo de asignación de direcciones IP en las redes locales y extendidas

La tabla de enrutamiento *IP* del NODO 100 del ejemplo de la figura 5.38 se describe en el cuadro 5.32.

TABLA DE RUTAS IP DEL NODO 100		
RED DESTINO	SIGUIENTE SALTO	NÚMERO DE SALTOS
130.50	130.20.01.02	2
130.50	130.30.01.02	3
130.60	130.30.01.02	2
130.60	130.20.01.02	3

Cuadro 5.32 Tabla de rutas IP en el Nodo 100 del ejemplo de la figura 5.38

De acuerdo con las consideraciones anteriores la tabla de rutas *IP* para los ruteadores MAESTRO1 y AGENCIA 1 de la red del Banco se indica en el cuadro 5.33.

TABLA DE RUTAS IP DEL RUTEADOR MAESTRO 1 100000		
RED IP DESTINO	DIRECCION IP DEL SIGUIENTE SALTO	NÚMERO DE SALTOS HASTA EL DESTINO
130.000	133.254.001.002	2
	133.253.001.002	2
	133.252.001.002	2
	133.250.001.002	2
	133.001.001.002	2
130.001	132.001.001.002	3
130.002	132.002.001.002	3
130.003	132.003.001.002	3
.	.	
130.012	132.012.001.002	3
130.013	133.001.001.002	4
130.014	133.001.001.002	4
.	.	.
130.029	133.001.001.002	4
130.030	133.001.001.002	5
130.032	133.001.001.002	5
.	"	"
131.001	132.001.001.002	2
131.002	132.002.001.002	2
131.003	132.003.001.002	2
.	"	"
131.012	132.012.001.002	2
131.013	133.001.001.002	3
131.014	133.001.001.002	3
.	"	"
131.029	133.001.001.002	3
131.030	133.001.001.002	4
.	"	"
132.001	132.001.001.002	1
132.002	132.002.001.002	1
132.003	132.003.001.002	1
.	"	"
132.012	132.012.001.002	1
132.013	133.001.001.002	2
132.014	133.001.001.002	2
.	"	"
132.029	133.001.001.002	2
132.030	133.001.001.002	3
.	"	"
133.001	131.001.001.002	1
133.002	133.001.001.002	2
133.003	133.001.001.002	3
.	"	.
133.009	133.001.001.002	9
Para los servidores		
133.249	133.249.001.002	1
133.250	133.250.001.002	1
133.251	133.251.001.002	1
133.252	133.252.001.002	1
133.253	133.253.001.002	1
133.254	133.254.001.002	1

TABLA DE RUTAS IP DEL RUTEADOR AGENCIA 1 100010		
RED IP DESTINO	DIRECCION IP DEL SIGUIENTE SALTO	NÚMERO DE SALTOS HASTA EL DESTINO
130.000	132.001.001.001	3
130.001	131.001.001.002	2
130.002	132.001.001.001	4
130.003	132.001.001.001	4
.	.	.
.	.	.
130.012	132.001.001.001	4
130.013	132.001.001.001	5
130.014	132.001.001.001	5
.	.	.
.	.	.
130.029	132.001.001.001	5
130.030	132.001.001.001	6
130.032	132.001.001.001	6
.	"	"
.	"	"
131.001	131.001.001.002	1
131.002	132.001.001.001	3
131.003	132.001.001.001	3
.	"	"
.	"	"
131.012	132.001.001.001	3
131.013	132.001.001.001	4
131.014	132.001.001.001	4
.	"	"
131.029	132.001.001.001	4
131.030	132.001.001.001	5
.	"	"
132.001	132.001.001.001	1
132.002	132.001.001.001	2
132.003	132.001.001.001	2
.	"	"
132.012	132.001.001.001	2
132.013	132.001.001.001	3
132.014	132.001.001.001	3
.	"	"
132.029	132.001.001.001	3
132.030	132.001.001.001	4
.	"	"
133.001	132.001.001.001	2
133.002	132.001.001.001	3
133.003	132.001.001.001	4
.	"	.
133.009	132.001.001.001	10
Para los servidores		
133.249	132.001.001.001	2
133.250	132.001.001.001	2
133.251	132.001.001.001	2
133.252	132.001.001.001	2
133.253	132.001.001.001	2
133.254	132.001.001.001	2

Cuadro 5.33 Tabla de rutas IP en los ruteadores Maestro 1 y Agencia 1

- Los ruteadores de las agencias como se indica en la figura 5.39 se pueden conectar al *backbone* X.25 mediante los siguientes enlaces:

. **Telefónicos** para las áreas urbanas, que tienen un buen servicio de líneas telefónicas *Dial* y Dedicadas. En las principales ciudades del Ecuador se pueden emplear este tipo de comunicaciones .

. **Vía satélite** para los sitios donde no existan líneas telefónicas o sean éstas de mala calidad, como es el caso de las regiones orientales e insular.

. **Radio** para los sitios cercanos, donde no existen líneas o son de mala calidad las líneas telefónicas, como por ejemplo Lasso, Machachi, Cayambe.

. **Celular** en lugares donde no existe líneas telefónicas y se requiere de usos esporádicos, como son los cajeros automáticos, los cuales ocupan la línea solo cuando el usuario lo requiere. La ventaja de éste enlace es que se pueden instalar cajeros en cualquier sitio del país.

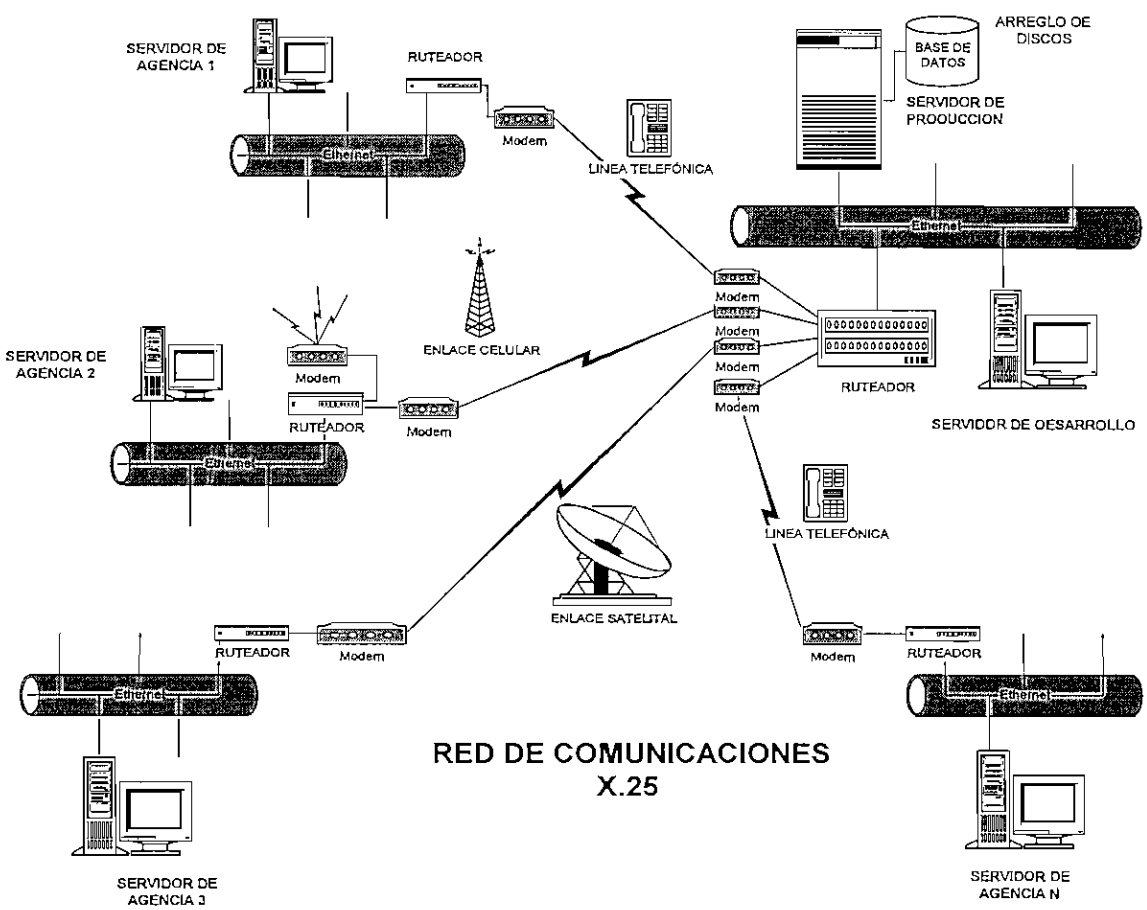


Figura 5.39 Tipos de enlaces de red extendida

5.6 INTERCONECTIVIDAD

Para describir la interconexión de equipos se toma como caso práctico la red de datos diseñada para el BANCO INVESPLAN, que trabaja con X.25 para los enlaces de red *WAN* y *TCP/IP* para la conexión entre las redes *LAN* de las diferentes agencias.

5.6.1 RED *TCP/IP* SOBRE X.25 PARA EL BANCO INVESPLAN

Para este caso particular la nube X.25 está formada por 4 ruteadores *Codex* 6520 distribuidos de la siguiente manera:

- **Quito** el ruteador Maestro denominado QUITO 100
- **Guayaquil** el ruteador de Agencia 1 denominado GUAYAS 200
- **Cuenca** el ruteador de Agencia 2 denominado CUENCA 300
- **Ambato** el ruteador de Agencia 3 denominado AMBATO 400

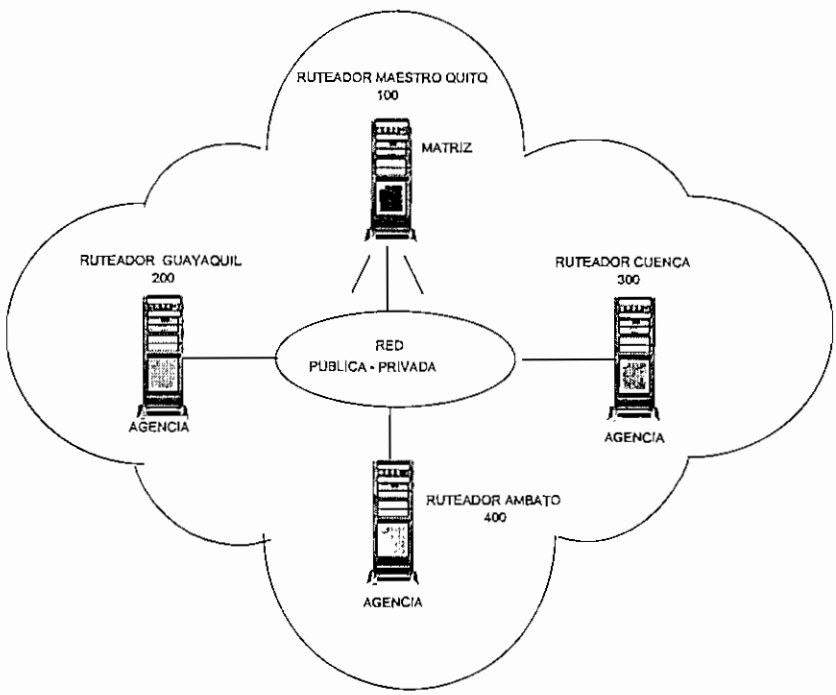


Figura 5.40 Nube X.25 del Banco INVESPLAN

Cada ruteador tiene la siguiente configuración en *hardware*:

- 5 puertos X.25 por cuanto las agencias que tiene el banco son pocas.
- 1 puerto *Ethernet* que se conecta directamente a la red *Ethernet* en la matriz y las agencias.

Los ruteadores se constituyen en los ***Gateways*** que permiten la transmisión de los paquetes *TCP/IP* entre redes *Ethernet* de las agencias a través de la red *WAN* X.25.

5.6.1.1 RED *WAN* X.25 DEL BANCO INVESPLAN

La red *WAN* X.25 está formada por los cuatro ruteadores cuyas direcciones son 100, 200, 300 y 400 numerados en orden de importancia.

El ruteador maestro está en Quito, al cual se enlazan mediante X.25 los ruteadores de las agencias de Guayaquil, Cuenca y Ambato.

La configuración de estos ruteadores se indica en el cuadro 5.34.

PARAMETROS DE LOS NODOS	QUITO	GUAYAQUIL	CUENCA	AMBATO
Node Name	QUITO	GUAYAS	CUENCA	AMBATO
Node Address	100	200	300	400
Node Number	100	200	300	400
Maximum Routing Hops	15	15	15	15
Maximum Simultaneous Call	100	100	100	100
LAN Connection Subaddres	**94**	**94**	**94**	**94**
Traffic Priority	MED	MED	MED	MED
Traffic Priority Step	8	8	8	8
Max Frame Size	2200	2200	2200	2200
Route Selection Table Size	16	16	16	16
Mnemonic Table Size	16	16	16	16
Number of Network Services Channels	1024	1024	1024	1024
PVC Setup Table Size	32	32	32	32

Cuadro 5.34 Configuración de los ruteadores de la matriz y agencias

En el ruteador maestro QUITO 100 se configura los parámetros X.25 de los puertos, cuyas direcciones tienen el formato 100XX , donde XX es el número de puerto del ruteador, de los cuales solo se emplean los puertos P1, P2 y P3 para conectarse con las tres agencias.

El puerto 1 se configura para que el ruteador funcione como *DTE* y el resto para *DCE*.

CONFIGURACION DE LOS PUERTOS X.25 DEL RUTEADOR QUITO 100					
PARAMETROS	PUERTO 1	PUERTO 2	PUERTO 3	PUERTO 4	PUERTO 5
Port Type	X.25	X.25	X.25	X.25	X.25
Connection Type	Simple	Simple	Simple	Simple	Simple
Clock Source	Externo	Externo	Externo	Externo	Externo
Clock Speed	**64000**	**64000**	**19200**	**19200**	**19200**
Link Address	***DTE***	*DCE*	*DCE*	*DCE*	*DCE*
Number of PVC Channels	0	0	0	0	0
Number of SVC Channels	32	32	32	32	32
K Frame Window	7	7	7	7	7
W Packet Window	2	2	2	2	2
P Packet Size	256	256	256	256	256
Port Address	10001	10002	10003	10004	10005
Reconnection Time out	2	2	2	2	2

Cuadro 5.35 Configuración de los puertos X.25 del ruteador QUITO 100 del Banco

En las agencias solo se requiere de un puerto P1 configurado con parámetros X.25 similares a los puertos del ruteador QUITO 100 para el enlace con la matriz.

CONFIGURACION DEL PUERTO 1 X.25 EN LAS AGENCIAS			
PARAMETROS	PUERTO-1 NODO GUAYAS 200	PUERTO-1 NODO CUENCA 300	PUERTO-1 NODO AMBATO 400
Port Type	X.25	X.25	X.25
Connection Type	Simple	Simple	Simple
Clock Source	Externo	Externo	Externo
Clock Speed	64000	64000	19200
Link Address	*DTE*	*DTE*	*DTE*
Number of PVC Channels	0	0	0
Number of SVC Channels	32	32	32
K Frame Window	7	7	7
W Packet Window	2	2	2
P Packet Size	256	256	256
Port Address	20001	30001	40001
Reconnection Time out	2	2	2

Cuadro 5.36 Configuración de los puertos X.25 en los ruteadores de las agencias

La tabla de rutas de los ruteadores tienen pocos registros por el tamaño de la red.

El ruteador maestro QUITO 100 tiene la siguiente tabla de rutas X.25:

TABLA DE RUTAS DEL RUTEADOR QUITO 100			
Registro	Dirección X.25 remota	Puerto local X25 destino	Prioridad
1	200*	X.25 - 01 Puerto 1	1
2	300*	X.25 - 02 Puerto 2	1
3	400*	X.25 - 03 Puerto 3	1
4	10094	*LCON*	1

Cuadro 5.37 Tabla de rutas X.25 del nodo QUITO 100

En todos los ruteadores es necesario enrutar el Adaptador de *WAN* cuya dirección X.25 es YYY**94**, hacia el módulo de Conexión *LAN* (***LCON***), con lo cual se forma un circuito virtual usado para el tráfico entre las redes *LAN* a través de X.25. El valor YYY es la dirección X.25 de los ruteadores. Para el ruteador QUITO 100 la dirección X.25 del adaptador de *WAN* es 10094 y se enruta a *LCON* con prioridad 1.

Para el resto de agencias se sigue los mismos pasos para configurar las tablas de rutas X25.

En los cuadros 5.38, 5.39, 5.40 se observa que para accesar al resto de redes X.25, se lo hace a través del puerto local P1 de los ruteadores de agencia.

TABLA DE RUTAS DEL RUTEADOR GUAYAS 200			
Registro	Dirección X.25 remota	Puerto local X.25 destino	Prioridad
1	100*	X.25 - 01 Puerto 1	1
2	300*	X.25 - 01 Puerto 1	1
3	400*	X.25 - 01 Puerto 1	1
4	20094	*LCON*	1

Cuadro 5.38 Tabla de rutas X.25 del ruteador GUAYAS 200

TABLA DE RUTAS DEL RUTEADOR CUENCA 300			
Registro	Dirección X.25 remota	Puerto local X.25 destino	Prioridad
1	100*	X.25 - 01 Puerto 1	1
2	200*	X.25 - 01 Puerto 1	1
3	400*	X.25 - 01 Puerto 1	1
4	30094	*LCON*	1

Cuadro 5.39 Tabla de rutas X.25 del ruteador CUENCA 300

TABLA DE RUTAS DEL RUTEADOR AMBATO 400			
Registro	Dirección X.25 remota	Puerto local X.25 destino	Prioridad
1	100*	X.25 - 01 Puerto 1	1
2	200*	X.25 - 01 Puerto 1	1
3	300*	X.25 - 01 Puerto 1	1
4	40094	*LCON*	1

Cuadro 5.40 Tabla de rutas X.25 del nodo AMBATO 400

Los dos puertos P1 y P2 del ruteador QUITO 100 se multiplexan mediante un *DTU* (*Data Termination Unit*) hasta la central digital de datos de TELEHOLDIN, en donde se demultiplexa hacia las agencias de Guayaquil y Cuenca, con el fin de usar una sola línea de datos hacia las dos agencias a velocidades altas. Cada canal del *DTU* trabaja a 64 Kbps con lo cual se incrementa la velocidad de transmisión con las agencias más importantes. El enlace con Ambato se lo hace con línea dedicada a 19200 bps mediante *modems*.

La disposición de ruteadores y equipos en las agencias se muestra en la figura 5.41.

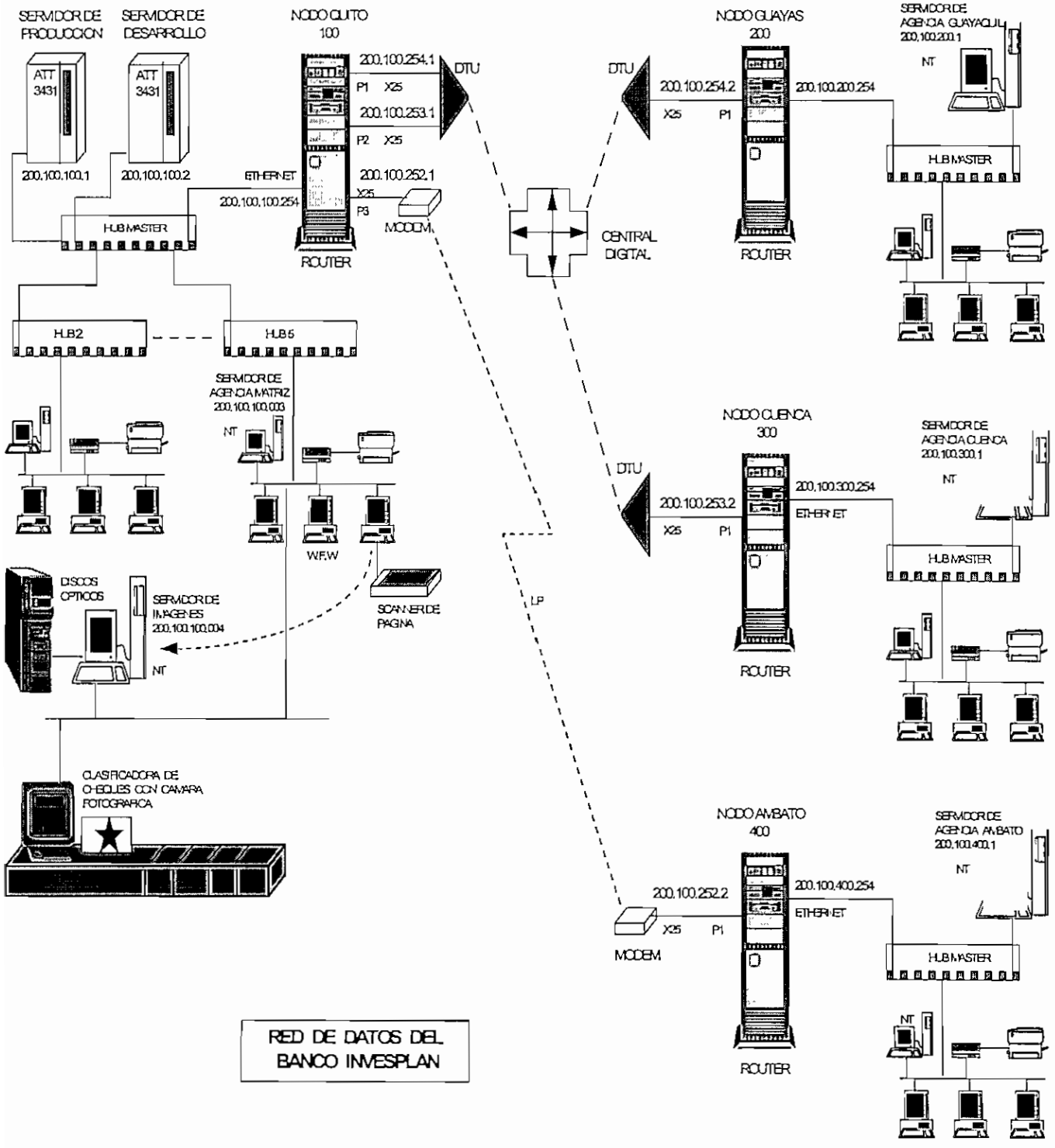


Figura 5.41 Disposición de ruteadores y equipos en la red de datos del Banco

5.6.1.2 RED *IP* DEL BANCO INVESPLAN

Para la implementación de la red *IP* se escoge una red tipo C, por cuanto la cantidad de servidores y usuarios en el banco es mediana.

Las redes locales *IP* en cada Agencia son:

- 200.100.**100** red local de la Matriz Quito
- 200.100.**200** red local de la Agencia Guayaquil
- 200.100.**300** red local de la Agencia Cuenca
- 200.100.**400** red local de la Agencia Ambato

La red *WAN IP* tiene tres redes independientes, formadas por los enlaces del ruteador de la matriz con los ruteadores de las otras agencias. Estas son:

- 200.100.**254** red formada por el enlace entre los ruteadores QUITO 100 y GUAYAS 200
- 200.100.**253** red formada por el enlace entre los ruteadores QUITO 100 y CUENCA 300
- 200.100.**252** red formada por el enlace entre los ruteadores QUITO 100 y AMBATO 400

Cada red *WAN IP* tiene dos *hosts* que en este caso son los ruteadores que forman el enlace; las direcciones de *host* más bajas tiene el ruteador maestro como se indica en la figura 5.42.

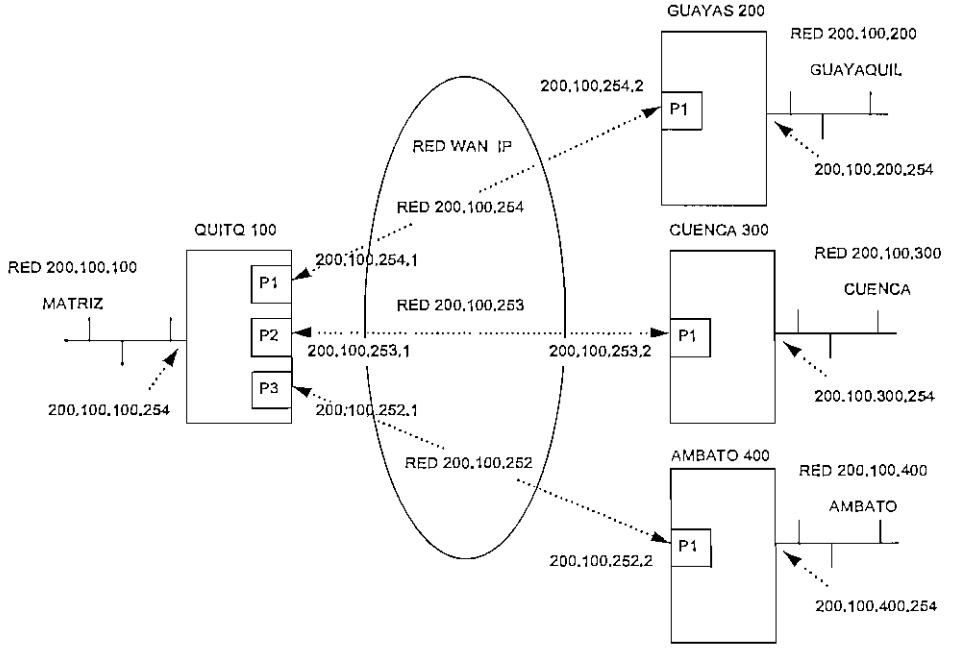


Figura 5.42 Redes IP extendidas y redes IP locales de la matriz y de las agencias

En cada ruteador se debe configurar el puerto *Ethernet* para la red local, el cual ocupa la dirección *IP* más alta, en tanto que los servidores tienen asignados las direcciones más bajas.

Las direcciones *IP* en los ruteadores de la matriz y agencias de la red de la figura 5.42 se indican en los cuadros 5.41, 5.42, 5.43 y 5.44.

DIRECCIONES *IP* EN EL RUTEADOR QUITO 100			
PUERTO	RED *IP*	DIRECCION *IP* DEL PUERTO	DIRECCION *IP* DESTINO
P1	200.100.254	200.100.254.1	200.100.254.2 Puerto 1 del ruteador GUAYAS 200
P2	200.100.253	200.100.253.1	200.100.253.2 Puerto 1 del ruteador CUENCA 300
P3	200.100.252	200.100.252.1	200.100.252.2 Puerto 1 del ruteador AMBATO 400
ETHERNET	200.100.100	200.100.100.254	RED LOCAL

Cuadro 5.41 Direcciones IP de los puertos en el ruteador QUITO 100

DIRECCIONES *IP* EN EL RUTEADOR GUAYAS 200			
PUERTO	RED *IP*	DIRECCION *IP* DEL PUERTO	DIRECCION *IP* DESTINO
P1	200.100.254	200.100.254.2	200.100.254.1 Puerto 1 del ruteador QUITO 100
ETHERNET	200.100.200	200.100.200.254	RED LOCAL

Cuadro 5.42 Direcciones IP de los puertos en el ruteador de Agencia GUAYAS 200

DIRECCIONES *IP* EN EL RUTEADOR CUENCA 300			
PUERTO	RED *IP*	DIRECCION *IP* DEL PUERTO	DIRECCION *IP* DESTINO
P1	200.100.253	200.100.253.2	200.100.253.1 Puerto 2 del ruteador QUITO 100
ETHERNET	200.100.300	200.100.300.254	RED LOCAL

Cuadro 5.43 Direcciones IP de los puertos en el ruteador de Agencia CUENCA 300

DIRECCIONES *IP* EN EL RUTEADOR AMBATO 400			
PUERTO	RED *IP*	DIRECCION *IP* DEL PUERTO	DIRECCION *IP* DESTINO
P1	200.100.252	200.100.252.2	200.100.252.1 Puerto 3 del ruteador QUITO 100
ETHERNET	200.100.400	200.100.400.254	RED LOCAL

Cuadro 5.44 Direcciones IP de los puertos en el ruteador de Agencia AMBATO 400

Para que las redes *Ethernet* remotas se conecten entre si, se deben configurar los interfaces de enrutamiento de los ruteadores.

En el ruteador QUITO 100 se configuran un interfaz para *LAN* y tres para *WAN*:

- Interfaz 1 para el puerto *Ethernet* local
- Interfaz 5 para el enlace de red *WAN* con el ruteador GUAYAS 200
- Interfaz 6 para el enlace de red *WAN* con el ruteador CUENCA 300
- Interfaz 7 para el enlace de red *WAN* con el ruteador AMBATO 400

En el ruteador GUAYAS 200 se configuran dos interfaces, uno para *LAN* y otro para *WAN*:

- Interfaz 1 para el puerto *Ethernet* local

- Interfaz 5 para el enlace de red *WAN* con el ruteador QUITO 100

En el ruteador CUENCA 300 se tiene un interfaz para *LAN* y otro para *WAN*:

- Interfaz 1 para el puerto *Ethernet* local

- Interfaz 5 para el enlace de red *WAN* con el ruteador QUITO 100

El ruteador AMBATO 400 se configura con un interfaz para *LAN* y otro para *WAN*:

- Interfaz 1 para el puerto *Ethernet* local

- Interfaz 5 para el enlace de red *WAN* con el ruteador QUITO 100

La conexión de estos interfaces de enrutamiento se muestran en la figura 5.43.

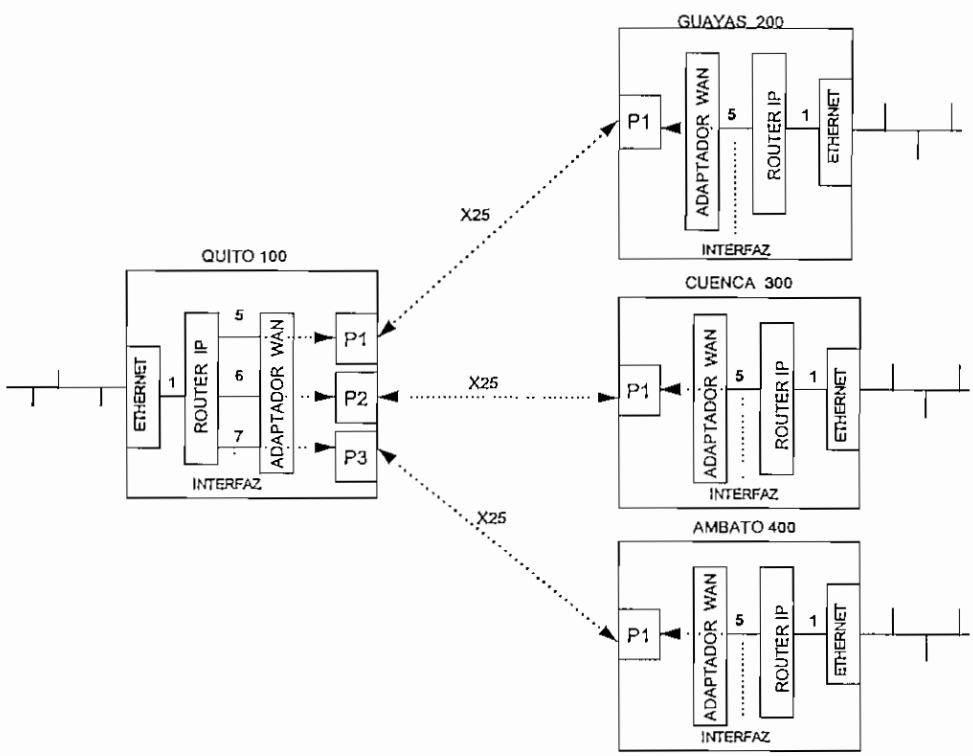


Figura 5.43 Configuración de Interfaces de enrutamiento en los ruteadores de la red

De acuerdo con la figura 5.43, cada interfaz establece una conexión hacia un puerto destino.

En los ruteadores se generan las tablas de registros con la configuración de cada uno de los interfaces de enrutamiento, donde debe constar la dirección *IP*, máscara, la identificación de la conexión *WAN* local , y los protocolos de enrutamiento que manejan los interfaces, como se indica en los cuadros 5.45, 5.46, 5.47, 5.48.

INTERFACES *IP* DEL RUTEADOR QUITO 100				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* local	Dirección *IP*	Máscara
1	1		200.100.100.254	255.255.255.000
2	5	1	200.100.254.001	255.255.255.000
3	6	2	200.100.253.001	255.255.255.000
4	7	3	200.100.252.001	255.255.255.000
.	.		.	.

Cuadro 5.45 Direccionamiento IP de las interfaces de enrutamiento en el ruteador QUITO 100

INTERFACES *IP* DEL RUTEADOR GUAYAS 200				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* local	Dirección *IP*	Máscara
1	1		200.100.200.254	255.255.255.000
2	5	1	200.100.254.002	255.255.255.000
.	.		.	.

Cuadro 5.46 Direccionamiento IP de las interfaces de enrutamiento en el ruteador GUAYAS 200

INTERFACES *IP* DEL RUTEADOR CUENCA 300				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* local	Dirección *IP*	Máscara
1	1		200.100.300.254	255.255.255.000
2	5	1	200.100.253.002	255.255.255.000
.	.		.	.

Cuadro 5.47 Direccionamiento IP de las interfaces de enrutamiento en el ruteador CUENCA 300

INTERFACES *IP* DEL RUTEADOR AMBATO 400				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* local	Dirección *IP*	Máscara
1	1		200.100.400.254	255.255.255.000
2	5	1	200.100.252.002	255.255.255.000
.	.		.	.

Cuadro 5.48 Direccionamiento IP de las interfaces de enrutamiento en el ruteador AMBATO 400

Las conexiones *LAN LCONS* son circuitos virtuales que se forman por el enlace entre ruteadores para permitir el flujo de datos *IP* entre redes *Ethernet* remotas.

Para conectarse al interfaz *WAN* de enrutamiento *IP* de un ruteador remoto, el ruteador local debe indicar el número de Identificación de la conexión *WAN* remota. Una vez que se enlazan los módulos de Adaptador de *WAN* del ruteador local y remoto, el circuito virtual queda establecido y los paquetes *IP* son enrutados hacia los puertos *Ethernet* de los ruteadores o hacia otros ruteadores remotos de la red. Con este proceso se establece la conexión entre redes *Ethernet* remotas a través de un circuito virtual X.25.

La **Identificación de Conexión *WAN* remota** permite seleccionar el interfaz de *WAN* correcto en el ruteador remoto, para establecer la conexión entre los Adaptadores de *WAN* local y remota. Para que se realice este proceso, en los ruteadores se configura la Tabla de Conexiones *LAN*, para cada interfaz de enrutamiento *IP* del **adaptador de *WAN***, especificando el número de interfaz *WAN*, el tipo de enlace entre los ruteadores, la Identificación de Conexión de *WAN* remota, y el tipo de encapsulamiento, como se indica en el cuadro 5.49.

TABLA DE CONEXIONES *LAN* DEL RUTEADOR QUITO 100				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* remota	Tipo de conexión *LAN*	Tipo de Encapsulamiento
1	5	1 Interfaz 5 del ruteador GUAYAS 200 - puerto 1	Punto a Punto	Codex RFC 877
2	6	1 Interfaz 5 del ruteador CUENCA 300 - puerto 1	Punto a Punto	Codex RFC 877
3	7	1 Interfaz 5 del ruteador AMBATO 400 - puerto 1	Punto a Punto	Codex RFC 877
.	.			.

Cuadro 5.49 Tabla de Conexiones lógicas de LAN en el ruteador QUITO 100

Por cada Conexión *LAN* enlazada a los interfaces destinos, se forma un circuito virtual X.25 independiente. Se puede generar varios circuitos virtuales o *LCONs* hacia un mismo destino a través del mismo puerto X.25, para lo cual se enrutan varios interfaces locales hacia varios interfaces remotas a través del mismo puerto.

El ruteador QUITO 100 forma tres circuitos virtuales *LCONs* con los ruteadores destinos.

El tipo de encapsulamiento escogido para los paquetes *IP* es *Codex*, porque todos los ruteadores son del mismo tipo y el encapsulado y desencapsulado se realiza sin problemas.

Si los ruteadores fueran de diferente marca, el encapsulamiento debe ser *RFC877* para que los paquetes *IP* puedan ser transmitidos en X.25.

Para los ruteadores de las agencias, la tabla de conexiones *LAN* varía en la identificación de conexión remota como se indica en los cuadros 5.50, 5.51, 5.52.

TABLA DE CONEXIONES *LAN* DEL RUTEADOR GUAYAS 200				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* remota	Tipo de conexión *LAN*	Tipo de Encapsulamiento
1	5	1 Interfaz 5 del ruteador QUITO 100 - puerto 1	Punto a Punto	Codex RFC 877

Cuadro 5.50 Tabla de Conexiones lógicas de LAN en el ruteador GUAYAS 200

TABLA DE CONEXIONES *LAN* DEL RUTEADOR CUENCA 300				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* remota	Tipo de conexión *LAN*	Tipo de Encapsulamiento
1	5	2 Interfaz 6 del ruteador QUITO 100 - puerto 2	Punto a Punto	Codex RFC 877

Cuadro 5.51 Tabla de Conexiones lógicas de LAN en el ruteador CUENCA 300

TABLA DE CONEXIONES *LAN* DEL RUTEADOR AMBATO 400				
Número de registro	Número de Interfaz	Identificación de conexión *WAN* remota	Tipo de conexión *LAN*	Tipo de Encapsulamiento
1	5	3 Interfaz 7 del ruteador QUITO 100 - puerto 3	Punto a Punto	Codex RFC 877

Cuadro 5.52 Tabla de Conexiones lógicas de LAN en el ruteador AMBATO 400

En el ruteador GUAYAS, la identificación de conexión remota es **1**, lo cual significa que se enlazará al interfaz **5** del adaptador de *WAN* del ruteador QUITO por el puerto **1**.

En el ruteador CUENCA, la identificación de conexión remota es **2**, lo cual significa que se enlazará al interfaz **6** del adaptador de *WAN* del ruteador QUITO por el puerto **2**.

En el ruteador AMBATO la identificación de conexión remota es **3**, por lo que se enlazará al interfaz 7 del adaptador de *WAN* en el nodo QUITO por el puerto **3**.

Para la transmisión de los paquetes, el tamaño del *MTU* (*Maximum Transmission Unit*) es 1500 octetos.

Las tablas rutas *IP* que se generan en los ruteadores se indican en los cuadros 5.53 a 5.56.

Por ejemplo, para que un paquete *IP* vaya del ruteador GUAYAS a la red *LAN* **200.100.300** de CUENCA, el paquete debe ir primero al ruteador QUITO e ingresar a éste por el interfaz de *WAN* configurado con la dirección 200.100.254.001. La tabla además indica que para llegar a la red 200.100.300 se necesita pasar por dos ruteadores adicionales, que en este caso son el ruteador QUITO 100 y el ruteador CUENCA 300.

TABLA DE RUTAS *IP* DEL RUTEADOR QUITO 100		
RED DESTINO	SIGUIENTE SALTO	NÚMERO DE SALTOS
200.100.100	——	0
200.100.200	200.100.254.002	1
200.100.300	200.100.253.002	1
200.100.400	200.100.252.002	1
200.100.254	——	0
200.100.253	--------	0
200.100.252	——	0

Cuadro 5.53 Tabla de enrutamiento IP del ruteador QUITO 100

TABLA DE RUTAS *IP* DEL RUTEADOR GUAYAS 200		
RED DESTINO	SIGUIENTE SALTO	NÚMERO DE SALTOS
200.100.100	200.100.254.001	1
200.100.200	——	0
200.100.300	200.100.254.001	2
200.100.400	200.100.254.001	2
200.100.254	--------	0
200.100.253	200.100.254.001	1
200.100.252	200.100.254.001	1

Cuadro 5.54 Tabla de enrutamiento IP del ruteador GUAYAS 200

TABLA DE RUTAS *IP* DEL RUTEADOR CUENCA 300		
RED DESTINO	SIGUIENTE SALTO	NÚMERO DE SALTOS
200.100.100	200.100.253.001	1
200.100.200	200.100.253.001	2
200.100.300	——	0
200.100.400	200.100.253.001	2
200.100.254	200.100.253.001	1
200.100.253	——	0
200.100.252	200.100.253.001	1

Cuadro 5.55 Tabla de enrutamiento IP del ruteador CUENCA 300

TABLA DE RUTAS *IP* DEL RUTEADOR AMBATO 400		
RED DESTINO	SIGUIENTE SALTO	NÚMERO DE SALTOS
200.100.100	200.100.252.001	1
200.100.200	200.100.252.001	2
200.100.300	200.100.252.001	2
200.100.400	-------	0
200.100.254	200.100.252.001	1
200.100.253	200.100.252.001	1
200.100.252	-------	0

Cuadro 5.56 Tabla de enrutamiento IP del ruteador AMBATO 400

5.6.2 RED *IP* EN MATRIZ Y AGENCIAS

La red local en la matriz y agencias es tipo *Ethernet*, en donde el ***backbone*** está formado por *HUBs* inteligentes apilables *SEHI*, lo que permite tener un mayor número de puertos sobre los cuales se puede hacer el control de colisiones, o aislamiento de algún puerto cuando éste falla. En los *Hubs* apilados no se divide el ancho de banda, por cuanto son *Hubs* independientes conectados a través de un bus ancho de datos.

La disposición general de los *hubs* en la matriz se muestra en la figura 5.44.

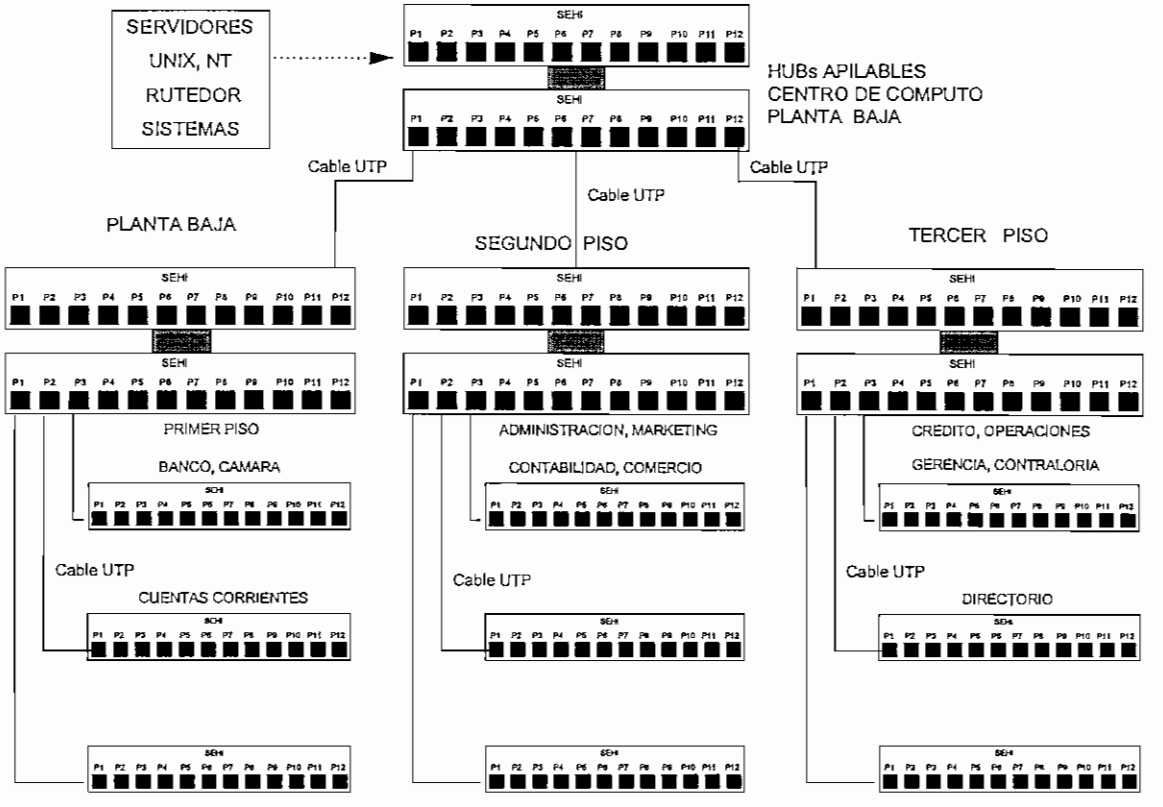


Figura 5.44 Distribución general de los *Hubs* en la Matriz del Banco

Los *hubs* que forman el *backbone* se ubican en el centro de cómputo. El resto de *hubs* ubicados en los diferentes pisos se conectan al *backbone* mediante cable *UTP* categoría 5 cruzado. Las estaciones se conectan a los *hubs* mediante cable *UTP* categoría 5.

Los servidores y usuarios tienen puertos *Ethernet* para conectarse a la red local.

Al *Hub Backbone* de la figura 5.44 deben conectarse directamente los siguientes equipos:

- Servidor *UNIX* Producción
- Servidor *UNIX* Desarrollo
- Servidor de Agencia Matriz
- Servidor *NT* de Imágenes
- Servidor de Sistemas
- Servidor de Impresión
- Servidor de *Mail*
- Servidor de Archivos
- Ruteador QUITO 100

Los Servidores de la matriz tienen las direcciones de red *IP* local más bajas, empezando desde 200.100.100.001 para el *UNIX* PRODUCCION, y se incrementa el factor de *host* de acuerdo a la importancia del servidor como se indica en el cuadro 5.57.

El ruteador tiene la dirección 200.100.100.254 que es la más alta en la red local.

SERVIDOR	NOMBRE	DIRECCION	*GATEWAY*
UNIX PRODUCCION	SERVER01	200.100.100.001	200.100.100.254
UNIX DESARROLLO	SERVER02	200.100.100.002	200.100.100.254
AGENCIA MATRIZ	MATRIZ001	200.100.100.003	200.100.100.254
IMAGENES	IMAG001	200.100.100.004	200.100.100.254
SISTEMAS	SISTEM001	200.100.100.005	200.100.100.254
ARCHIVOS	ARCH001	200.100.100.006	200.100.100.254
IMPRESION	IMPR001	200.100.100.007	200.100.100.254
OTROS SERVIDORES		200.100.100.008 200.100.100.009	200.100.100.254

Cuadro 5.57 Dirección IP de los servidores de la Matriz del Banco

Para asignar direcciones *IP* e identificar a los usuarios se han establecido grupos de trabajo divididos por áreas.

Los nombres de los usuarios van de acuerdo al grupo en el que están operando, como se indica en el cuadro 5.58.

DIRECCIONAMIENTO *IP* EN LA MATRIZ QUITO RED 200.100.100				
AREA	**GRUPO**	**NOMBRES**	**DIRECCION *IP***	***GATEWAY***
Sistemas	Sistemas	SISTEMXX	200.100.100.01X 200.100.100.02X	200.100.100.254
Banco	- Cuentas Corrientes - Cajas - Cámara	- CTCTE0X - CAJAS0X - CAMAR0X	200.100.100.03X 200.100.100.04X 200.100.100.05X	200.100.100.254
Crédito personal Crédito Corporativo	Crédito	CREDIT0X	200.100.100.06X	200.100.100.254
Contabilidad	Contabilidad	CONTA0X	200.100.100.07X	200.100.100.254
Comercio Exterior	Comercio	COMER0X	200.100.100.08X	200.100.100.254
Administración Recursos Humanos	Administración	ADMIN0X	200.100.100.09X	200.100.100.254
Marketing	Marketing	MARKT0X	200.100.100.10X	200.100.100.254
Organización y Métodos	Métodos	METOD0X	200.100.100.11X	200.100.100.254
Operaciones	Operaciones	OPER0X	200.100.100.12X	200.100.100.254
Contraloría	Contraloría	CNTLRA0X	200.100.100.13X	200.100.100.254
Gerencia	Gerencia	GEREN0X	200.100.100.14X	200.100.100.254
Directorio	Directorio	DIREC0X	200.100.100.15X	200.100.100.254

Cuadro 5.58 Asignación de nombres y direcciones IP de los usuarios en la Matriz

El valor X corresponde al número del usuario.

En cada usuario se debe configurar la dirección *IP* del *gateway* a través del cual se accesa al resto de redes remotas de las agencias, que en este caso es el ruteador QUITO 100.

El protocolo de red predeterminado en la configuración de red de los usuarios es *TCP/IP*, a través del cual se realiza todas las operaciones de red, como son :

- Compartir archivos
- Compartir directorios
- Accesos a informaciones remotas
- Acceso a servidores *UNIX* y sus datos, etc.

Para las agencias de Guayaquil, Cuenca y Ambato el proceso de direccionamiento *IP* es similar al de la matriz, pero cambia el prefijo del número de usuario X, la dirección de la red y la del *gateway*, como se indica a continuación en los cuadros 5.59 a 5.64.

DIRECCIONAMIENTO *IP* EN LA AGENCIA GUAYAQUIL			RED 200.100.200	
AREA	GRUPO	NOMBRES	DIRECCION *IP*	*GATEWAY*
Banco	- Cuentas Corrientes - Cajas - Cámara	- CTCTE1X - CAJAS1X - CAMAR1X	200.100.200.03X 200.100.200.04X 200.100.200.05X	200.100.200.254
Crédito personal Crédito Corporativo	Crédito	CREDIT1X	200.100.200.06X	200.100.200.254
Contabilidad	Contabilidad	CONTA1X	200.100.200.07X	200.100.200.254
Comercio Exterior	Comercio	COMER1X	200.100.200.08X	200.100.200.254
Administración Recursos Humanos	Administración	ADMIN1X	200.100.200.09X	200.100.200.254
Marketing	Marketing	MARKT1X	200.100.200.10X	200.100.200.254
Organización y Métodos	Métodos	METOD1X	200.100.200.11X	200.100.200.254
Operaciones	Operaciones	OPER1X	200.100.200.12X	200.100.200.254
Contraloría	Contraloría	CNTLRA1X	200.100.200.13X	200.100.200.254
Gerencia	Gerencia	GEREN1X	200.100.200.14X	200.100.200.254
Directorio	Directorio	DIREC1X	200.100.200.15X	200.100.200.254

Cuadro 5.59 Asignación de nombres y direcciones IP de los usuarios en la Agencia Guayaquil

SERVIDORES DE LA AGENCIA GUAYAQUIL			
SERVIDOR	NOMBRE	DIRECCION	*GATEWAY*
AGENCIA	GUAYAS01	200.100.200.001	200.100.200.254
ARCHIVOS	ARCH101	200.100.200.002	200.100.200.254
IMPRESION	IMPR101	200.100.200.003	200.100.200.254
OTROS SERVIDORES		200.100.200.004 200.100.200.005	200.100.200.254

Cuadro 5.60 Asignación de nombres y direcciones IP de los servidores en la agencia Guayaquil

DIRECCIONAMIENTO *IP* EN LA AGENCIA CUENCA			RED 200.100.300	
AREA	GRUPO	NOMBRES	DIRECCION *IP*	*GATEWAY*
Banco	- Cuentas Corrientes - Cajas - Cámara	- CTCTE2X - CAJAS2X - CAMAR2X	200.100.300.03X 200.100.300.04X 200.100.300.05X	200.100.300.254
Crédito personal Crédito Corporativo	Crédito	CREDIT2X	200.100.300.06X	200.100.300.254
Contabilidad	Contabilidad	CONTA2X	200.100.300.07X	200.100.300.254
Comercio Exterior	Comercio	COMER2X	200.100.300.08X	200.100.300.254
Administración Recursos Humanos	Administración	ADMIN2X	200.100.300.09X	200.100.300.254
Marketing	Marketing	MARKT2X	200.100.300.10X	200.100.300.254
Organización y Métodos	Métodos	METOD2X	200.100.300.11X	200.100.300.254
Operaciones	Operaciones	OPER2X	200.100.300.12X	200.100.300.254
Contraloría	Contraloría	CNTLRA2X	200.100.300.13X	200.100.300.254
Gerencia	Gerencia	GEREN2X	200.100.300.14X	200.100.300.254
Directorio	Directorio	DIREC2X	200.100.300.15X	200.100.300.254

Cuadro 5.61 Asignación de nombres y direcciones IP de los usuarios en la Agencia Cuenca

SERVIDORES DE LA AGENCIA CUENCA			
SERVIDOR	NOMBRE	DIRECCION	*GATEWAY*
AGENCIA	CUENCA01	200.100.300.001	200.100.300.254
ARCHIVOS	ARCH201	200.100.300.002	200.100.300.254
IMPRESION	IMPR201	200.100.300.003	200.100.300.254
OTROS SERVIDORES		200.100.300.004 200.100.300.005	200.100.300.254

Cuadro 5.62 Asignación de nombres y direcciones IP de los servidores en la Agencia Cuenca

DIRECCIONAMIENTO *IP* EN LA AGENCIA AMBATO			RED 200.100.400	
AREA	GRUPO	NOMBRES	DIRECCION *IP*	*GATEWAY*
Banco	- Cuentas Corrientes - Cajas - Cámara	- CTCTE3X - CAJAS3X - CAMAR3X	200.100.400.03X 200.100.400.04X 200.100.400.05X	200.100.400.254
Crédito personal Crédito Corporativo	Crédito	CREDIT3X	200.100.400.06X	200.100.400.254
Contabilidad	Contabilidad	CONTA3X	200.100.400.07X	200.100.400.254
Comercio Exterior	Comercio	COMER3X	200.100.400.08X	200.100.400.254
Administración Recursos Humanos	Administración	ADMIN3X	200.100.400.09X	200.100.400.254
Marketing	Marketing	MARKT3X	200.100.400.10X	200.100.400.254
Organización y Métodos	Métodos	METOD3X	200.100.400.11X	200.100.400.254
Operaciones	Operaciones	OPER3X	200.100.400.12X	200.100.400.254
Contraloría	Contraloría	CNTLRA3X	200.100.400.13X	200.100.400.254
Gerencia	Gerencia	GEREN3X	200.100.400.14X	200.100.400.254
Directorio	Directorio	DIREC3X	200.100.400.15X	200.100.400.254
.	.	.	.	.

Cuadro 5.63 Asignación de nombres y direcciones IP de los usuarios en la Agencia Ambato

SERVIDORES DE LA AGENCIA AMBATO			
SERVIDOR	NOMBRE	DIRECCION	*GATEWAY*
AGENCIA	AMBATO01	200.100.400.001	200.100.400.254
ARCHIVOS	ARCH301	200.100.400.002	200.100.400.254
IMPRESION	IMPR301	200.100.400.003	200.100.400.254
OTROS SERVIDORES		200.100.400.004 200.100.400.005	200.100.400.254

Cuadro 5.64 Asignación de nombres y direcciones IP de los servidor en la Agencia Ambato

En los *Hubs* Inteligentes también se puede asignar una dirección *IP* y una dirección de *gateway*. La ventaja de ésto es que los paquetes que van a otras redes, son enviados directamente al puerto donde está conectado el ruteador. Las direcciones *IP* para estos *Hubs* son configuradas con direcciones menores que las direcciones de los ruteadores o *gateways* en las respectivas agencias como indica el cuadro 5.65:

DIRECCION *IP* DE *HUBS* INTELIGENTES		
AGENCIA	DIRECCION *IP*	*GATEWAY*
QUITO	200.100.100.253	200.100.100.254
GUAYAQUIL	200.100.200.253	200.100.200.254
CUENCA	200.100.300.253	200.100.300.254
AMBATO	200.100.400.253	200.100.400.254

Cuadro 5.65 Asignación direcciones IP de los *Hubs* en matriz y agencias

La configuración *TCP/IP* de servidores y usuarios dentro del software de red se describe en detalle en el Anexo 5.

5.7 APLICACION CON CAJEROS AUTOMATICOS

Una de las aplicaciones adicionales de *TCP/IP* es la implementación de Cajeros Automáticos *ATM (Automatic Teller Machine)* en redes *Ethernet*, conectados a un *Hub* común, con lo cual se obtiene transacciones más rápidas, por cuanto antes trabajaban con enlaces a 9600 bps conectados al puerto serial del Servidor de cajeros.

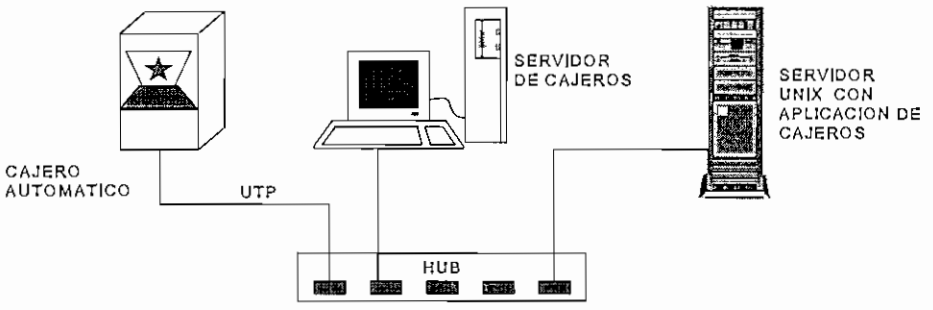


Figura 5.45 Conexión de Cajero Automático a la red *Ethernet*

La tarjeta de red *Ethernet* empleada en el cajero es una *3COM*, y para conectarlo al *Hub* se utiliza cable trenzado *UTP* categoría 5.

En el **Servidor de cajeros** corre una aplicación que constituye el interfaz transaccional entre el Servidor *UNIX* y el cajero automático.

El sistema operativo del cajero es *OS/2*, sobre el cual se instala el *software* de red, que en este caso es *PCTCP*, que maneja todos los protocolos *TCP/IP*, incluido *SLIP* y *PPP*

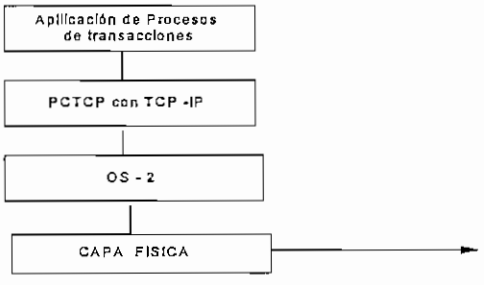


Figura 5.46 Módulos instalados en el Cajero

Para que funcione dentro de la red, se debe instalar los *drivers* de la tarjeta *Ethernet 3COM*.

Una vez que la tarjeta es reconocida, se añade el *TCP/IP* para el transporte y enrutamiento de los datos.

La disposición jerárquica de estos módulos se muestra en la siguiente figura:

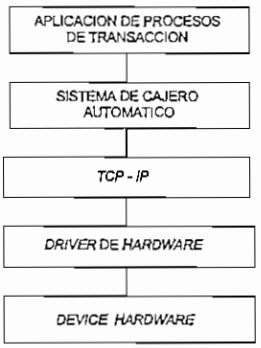


Figura 5.47 Disposición jerárquica de los módulos instalados en el cajero

Cuando se instala el *TCP/IP* en *OS/2* , se debe configurar la dirección *IP* del cajero, que corresponde a la dirección *IP* de su tarjeta *Ethernet* (*ND0*) con su respectiva máscara de red. Adicionalmente se indica la dirección del *router* o *gateway* por donde se puede accesar al resto de redes *IP*. El nombre del *host* es *ATM*.

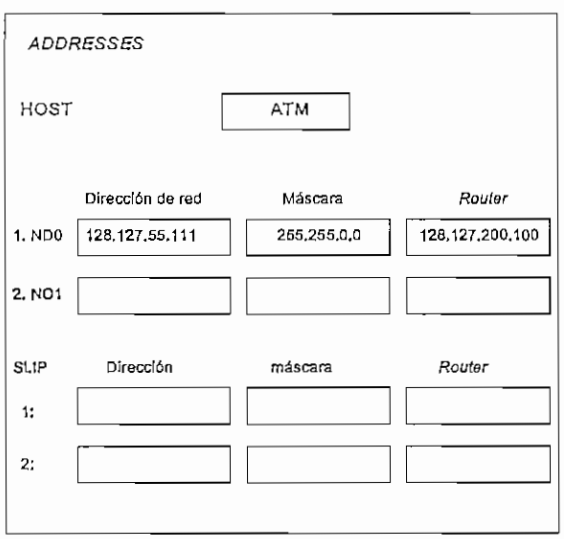


Figura 5.48 Configuración IP del PCTCP en el Cajero Automático

Los archivos que se deben tomar en cuenta para que funcione el *TCP/IP* son:

- *CONFIG.SYS*
- *PROTOCOL.INI*
- *PCTCP.INI*
- *STARTUP.CMD*
- PCTCP.CMD

En el *CONFIG:SYS* se instala los *drivers* de la tarjeta *Ethernet*, y el manejador de *sockets* para *OS/2:*

DEVICE = DRIVER NDIS.OS2 que para el cajero es *NDIS3COM.OS2*

DEVICE = SOCKET.OS2

En el *PROTOCOL.INI* se configuran la tarjeta *Ethernet* y sus *drivers* y se establece un enlace con los *sockets.*

[Nombre del Adaptador] [3COM]

Driver name = *NDIS3COM$* para reconocer cualquier *driver* de la *3COM*

Configuración de *hardware* *interrupt* = 5

I/O address = 300

[*SOCKET*]

Driver name = NDIS3COM$

Bindings = 3COM enlaza el *socket* con el [Nombre del adaptador]

En el *STARTUP.CMD* que es semejante al *AUTOEXEC.BAT* se pone el comando que enlaza el *driver* de la tarjeta *Ethernet* con el *software* de red que en este caso es el *TCP/IP.*

netbind

En el *PCTCP.CMD* que es otro bloque ejecutable se configuran las interfaces y rutas del cajero automático, donde se debe incluir la ruta al Servidor *NT* que es el que contiene el programa interfaz hacia el Servidor *UNIX.* Los comandos son:

ifconfig interface Dirección IP máscara

ifconfig ND0 128.130.50.40 255.255.0.0 **red 128.130**

Para añadir la ruta hacia el servidor se tiene el siguiente comando:

route add Dirección IP Dirección de Gateway

route add 130.100.01.02 128.130.50.254 **red 130.100**

El Servidor ***NT*** tiene la dirección 130.100.01.02, es decir está en una red diferente a la del cajero, por lo tanto se debe especificar la dirección del *gateway* que en este caso es el 128.130.50.254. Esto se muestra en el siguiente gráfico:

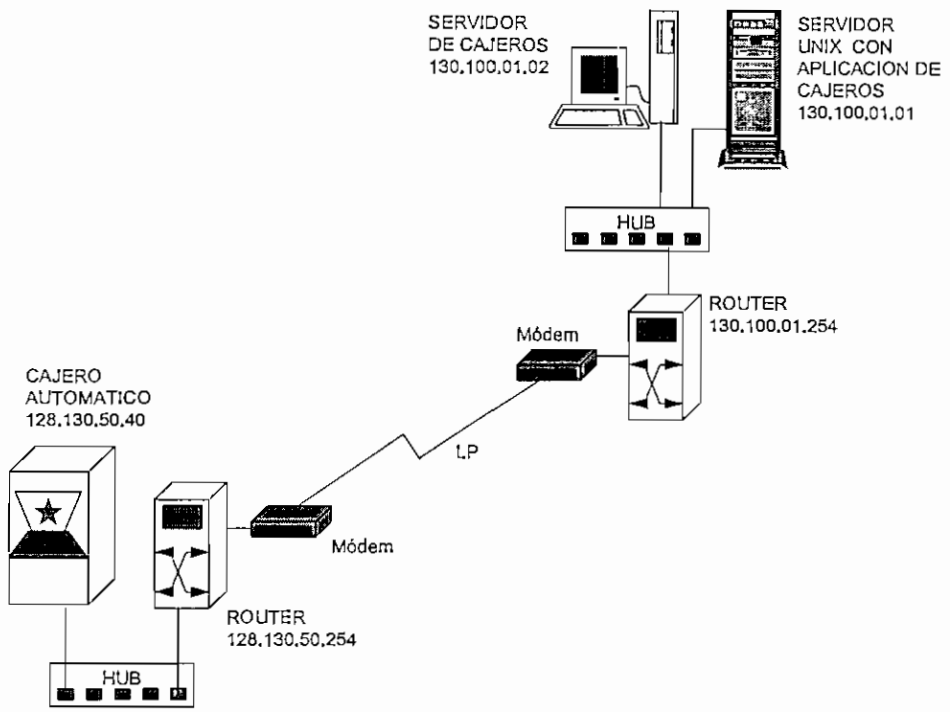


Figura 5.49 Configuración IP de un cajero remoto

-Cuando se introduce la **tarjeta** en el cajero, éste detecta la validez de la misma y envía al servidor un mensaje con la dirección del cajero, solicitando una conexión lógica.

- El servidor le responde al cajero con un mensaje de aceptación de la conexión.
- El cajero envía su dirección de *socket* disponible y el servidor responde con el número del *socket* del programa de Transacciones residente en el *NT*.
- Se establece de este modo un **circuito virtual**, para el envío-recepción de datos en el cajero.
- Una vez terminada la transacción, el cajero cierra el *socket* y el enlace se termina. Por lo tanto se forma un circuito virtual *on demand*, es decir se abre sólo cuando el cajero lo solicita. Esto se puede emplear para instalar cajeros en lugares donde no hay líneas telefónicas, para lo cual se utiliza enlaces celulares que se activan sólo cuando el proceso a realizarse en el cajero es válido.

CAPITULO VI IMPLEMENTACION

La implementación de la red de datos comprende el análisis de los recursos con los que cuenta el BANCO tanto en *software* como *hardware*, para luego determinar una solución óptima para la red de datos a nivel nacional.

Una vez que el Banco ha comprado la solución, se establece un cronograma de instalación, asignando recursos humanos y económicos para la ejecución del proyecto en lapsos de tiempo adecuados, utilizando herramientas técnicas que determinan el estado óptimo de la red.

En este capítulo además se realiza una estimación del costo total de la instalación, para finalmente mencionar las proyecciones de la red.

6.1 ANTECEDENTES

La implementación de la red *TCP/IP* se realiza en INVESPLAN, que anteriormente era una Institución Financiera. Al convertirse en banco solicita asesoramiento tanto en *Software* como en *Hardware* para alcanzar este objetivo.

Se asigna el personal técnico para que realice las primeras inspecciones a la institución, con el fin de realizar el análisis de la red antigua, para luego determinar la solución del sistema a implementar.

La red original, es un modelo multiusuario instalado en la casa matriz Quito y en las agencias de Guayaquil, Cuenca y Ambato, en cada una de las cuales había un servidor que atendía a varias terminales no inteligentes conectadas a través de puertos seriales asincrónicos.

Los dos servidores principales *SANYO* 3380 estaban localizados en la matriz Quito. Las características de estos equipos son:

. *CPU RISC* con procesador central *Motorola* XC88100 que opera a 20 *Mhz* de velocidad y dos procesadores *Motorola* XC88200 para el manejo del bus *SCSI* y otros dispositivos periféricos como regletas.

. 128 MB de memoria *RAM*

. Controladora *SCSI* que soporta 7 dispositivos

. 2 discos *SCSI* de 1GB

. Cinta *SCSI* de 525 MB para respaldos

. Controladora Multipuerto, con sus respectivas regletas de 8 puertos cada una, donde van conectadas las terminales no inteligentes mediante cables seriales y una comunicación serial asincrónica.

. Los servidores de las agencias tienen similares características a los equipos principales.

Las agencias se comunican con la matriz empleando los puertos seriales asincrónicos mediante *modems* a través de líneas dedicadas.

. El sistema operativo que manejaban es *UNIX* multiusuario propietario.

. Las aplicaciones instaladas en el servidor, eran empleadas para realizar procesos contables y administrativos de una institución financiera, y era de uso exclusivo de los equipos *Sanyo*, es decir no era un sistema abierto y amigable.

En la figura 6.1 se muestra la configuración original de la red INVESPLAN.

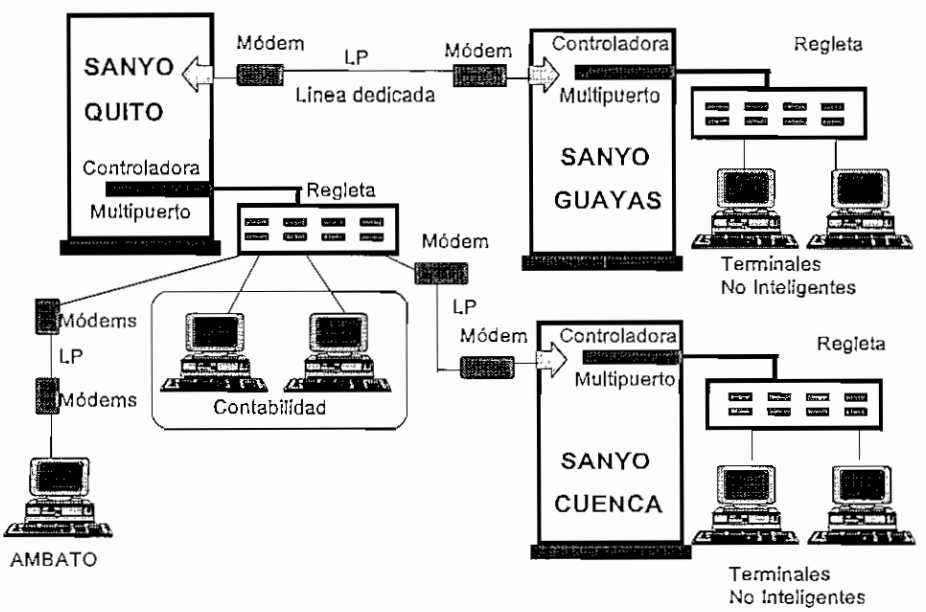


Figura 6.1 Configuración original de la Red INVESPLAN

. Cada regleta multipuerto atendía a una área o un departamento determinado.

. El cable empleado para la instalación era multipar telefónico sin blindaje , el cual funcionaba bien por operar a velocidades bajas y en distancias relativamente cortas dentro del edificio.

Los servidores *SANYO* resultaban demasiado lentos y sin capacidad para las aplicaciones que se requerían implementar para que la Institución pueda operar como un Banco.

Por lo descrito, la instalación era demasiada rígida y no permitía el crecimiento de la red.
Luego del análisis anterior se sugiere un cambio total en la configuración para la red de datos para la operación del Banco, siendo una buena alternativa la implementación de redes locales *Ethernet* en la matriz y en las agencias, operando a 10 *Mbps*, con lo que se obtiene una mayor velocidad de transmisión de los datos.

La comunicación en las redes locales se la realizaría a través de *Hubs* Inteligentes *Cabletron*, empleando para la conexión con cada uno de los usuarios cable *UTP* nivel 5, siendo necesario un cambio total del cableado anterior.

Para la red extendida se recomienda una red X.25 por la confiabilidad e integridad de los datos, empleando ruteadores *Codex* 6520 enlazados en un inicio mediante *modems Motorola* 3266 a través de líneas dedicadas

Se recomienda el cambio de los servidores *Sanyo* por equipos más rápidos como son los Servidores *ATT* 3430 para que la velocidad de proceso y el funcionamiento del Software Bancario adquirido por el Banco sea aceptable.

- En los servidores *SANYO* se instala una tarjeta de red *Ethernet* propia del equipo, para conectarse a la red nueva, empleando como protocolo de comunicación el *TCP/IP* soportado por el *UNIX Sanyo,* con la finalidad de que puedan operar en forma paralela con los nuevos equipos y sistemas, hasta que la nueva implementación funcione en su totalidad.

Para esto fue necesario añadir un *Transceiver* a cada tarjeta de red *Sanyo* como se muestra en la figura 6.2

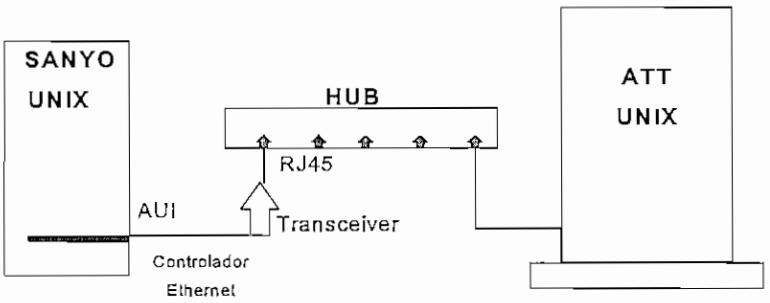


Figura 6.2 Conexión del servidor *Sanyo* a la nueva red

6.2 CRONOGRAMA DE INSTALACION

Para la realización del cronograma de instalación se ha empleado el ***Microsoft Project***, que permite realizar el calendario de tareas.

Se elabora una lista de personal técnico que se emplea en la instalación, a cada uno de los cuales se les asigna las diferentes tareas, de modo que no resulten sobrecargados de trabajo. Para el cronograma se elaboró una lista de 20 técnicos de diferentes especialidades ubicados en Quito y Guayaquil como se muestra en el cuadro 6.1, en el que se especifica el costo por hora de trabajo normal de un técnico.

ID	TECNICOS	UNIDADES	COSTO/H	COSTO TOTAL	TRABAJO
1	Ing. Elec Q1	1	S 20,00/h	S 6.400,00	320h
2	Ing. Elec Q2	1	S 20,00/h	S 9.120,00	456h
3	Ing. Elec Q3	1	S 20,00/h	S 6.080,00	304h
4	Ing. Elec Q4	1	S 20,00/h	S 5.920,00	296h
5	Ing. Elec G1	1	S 20,00/h	S 6.400,00	320h
6	Ing. Elec G2	1	S 20,00/h	S 2.880,00	144h
7	Ing. Sist Q1	1	S 20,00/h	S 5.760,00	288h
8	Ing. Sist Q2	1	S 20,00/h	S 7.520,00	376h
9	Ing. Sist Q3	1	S 20,00/h	S 4.960,00	248h
10	Ing. Sist Q4	1	S 20,00/h	S 4.160,00	208h
11	Ing. Sist G1	1	S 20,00/h	S 4.160,00	208h
12	Ing. Sist G2	1	S 20,00/h	S 2.560,00	128h
13	Ing. Sist G3	1	S 20,00/h	S 4.800,00	240h
14	Téc. Elec. Q1	1	S 15,00/h	S 3.720,00	248h
15	Téc. Elec. Q2	1	S 15,00/h	S 3.240,00	216h
16	Téc. Elec. Q3	1	S 15,00/h	S 1.920,00	128h
17	Téc. Elec. Q4	1	S 15,00/h	S 1.200,00	80h
18	Téc. Elec. G1	1	S 15,00/h	S 2.160,00	144h
19	Téc. Elec. G2	1	S 15,00/h	S 2.160,00	144h
20	Téc. Elec. G3	1	S 15,00/h	S 720,00	48h

Cuadro 6.1 Personal Técnico asignado al Proyecto

El programa *MS-Project* calcula automáticamente las horas que cadà técnico emplea en la realización del proyecto y obtiene un costo total en cada uno de ellos. En este caso no se emplea sobre tiempos.

El proyecto tiene una duración de 120 días laborables. Los días tomados para los cálculos son sólo los laborables, cada uno con una duración de 8 horas.

Para cada una de las tareas y subtareas se asigna la fecha de inicio, la fecha de finalización, el tiempo de duración, el personal técnico empleado, las tareas predecesoras o anteriores de las que depende, y el porcentaje cumplido de la tarea, como se muestra en los listados de Cronograma 1-1 a 1-4 en el Anexo 7.

El programa calcula el número de horas empleado en cada tarea y subtarea y el costo en dólares, el cual depende del precio de la hora de trabajo de los técnicos utilizados en una tarea o subtarea determinada. Estos cálculos se muestran en los listados identificados como Cronograma 2-1 a 2-4 en el Anexo 7.

La asignación de los técnicos se la realiza de modo que cada uno trabaje máximo 8 horas diarias, evitando la sobrecarga de trabajo y sobre tiempos.

La disposición de las tareas y subtareas se las puede observar en forma gráfica como se indica en los cuadros identificados como Cronograma 3-1 a 3-8 en el Anexo 7, donde se muestra el porcentaje de la tarea que se ha cumplido hasta una determinada fecha.

Las subtareas tienen la mezcla de las barras de ***Task*** y ***Progress*** y se ubican dentro de la barra de ***Summary*** que es totalmente negra. Algunas tareas para su realización dependen del cumplimiento de tareas anteriores. Si no se cumplen las tareas anteriores, el proyecto se detiene.

La topología y disposición general de la red que se instala se muestra en la figura 6.3

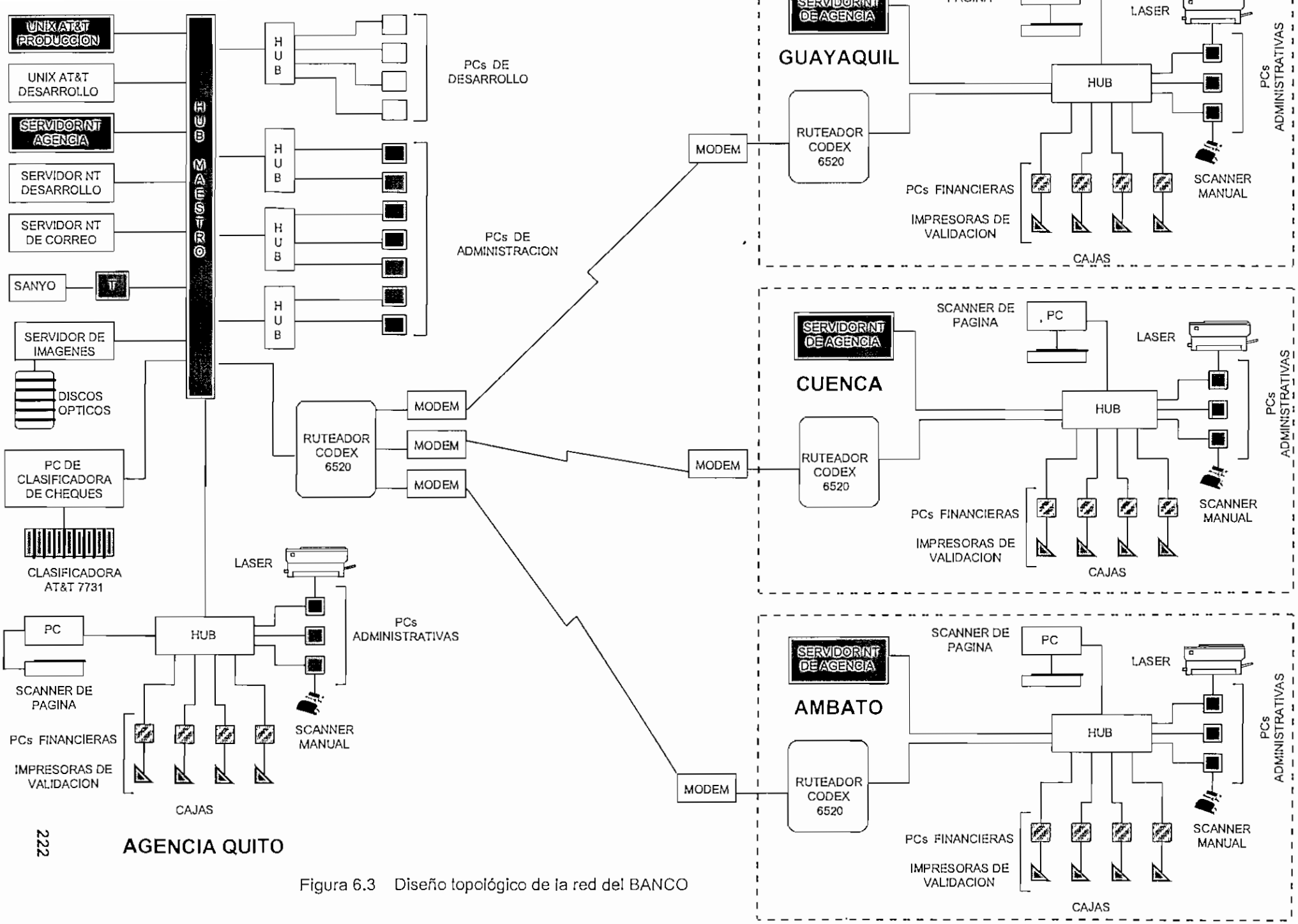


Figura 6.3 Diseño topológico de la red del BANCO

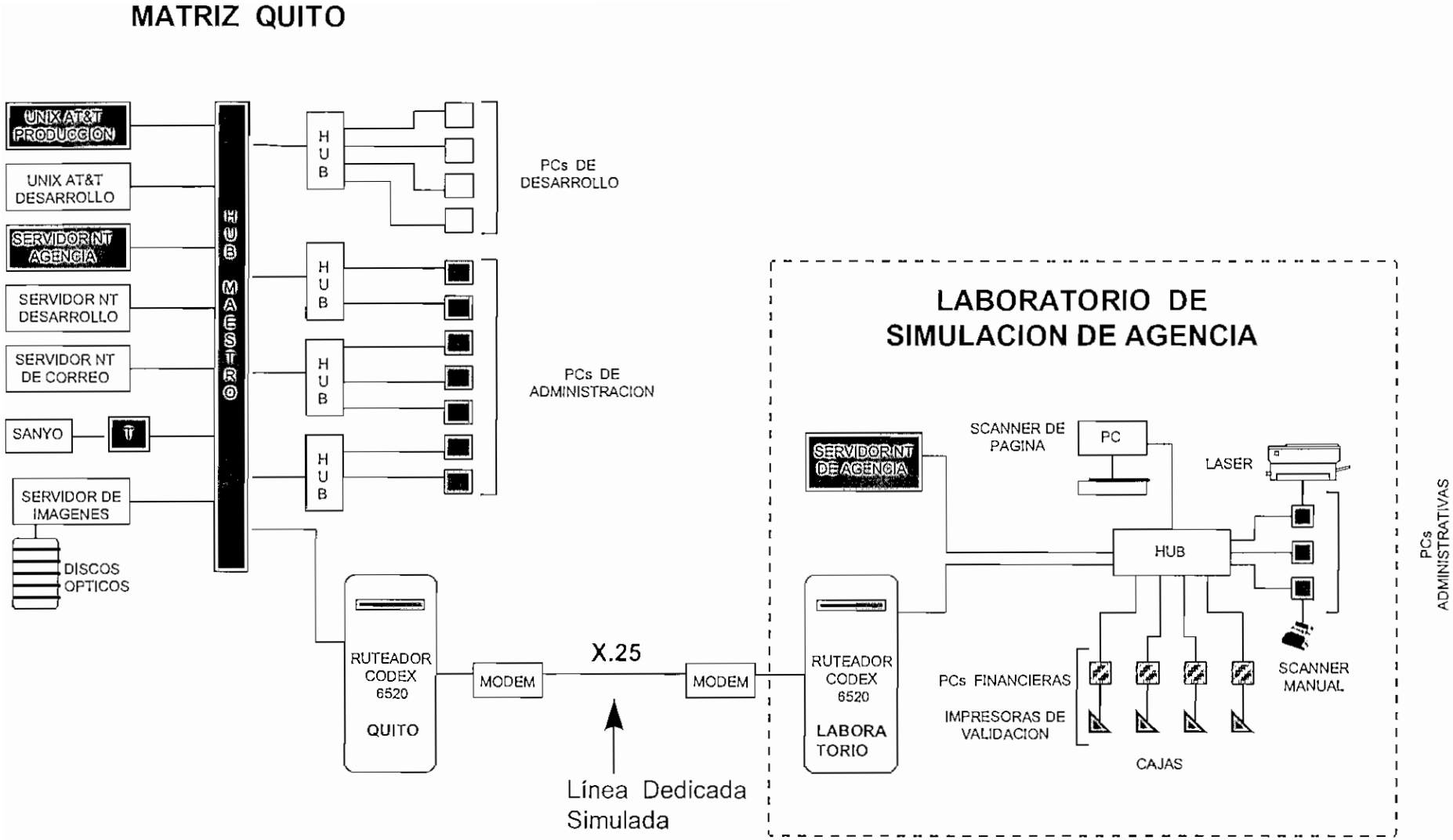


Figura 6.4 Implementación del Laboratorio en el BANCO

La implementación del "Laboratorio de Simulación de Agencia", en la Matriz del Banco se muestra en la figura 6.4, en donde la línea dedicada entre *modems* se puede simular empleando un cable de 2 o 4 hilos cruzado.

De igual forma si no se tienen *modems* se utilizan cables *RS232 pin* a *pin* o cruzado, dependiendo si los puertos de los ruteadores están configurados como *DTE* o *DCE*.

6.3 PROCEDIMIENTOS DE PRUEBAS

6.3.1 IMPLEMENTACION DE LABORATORIO

Para la implementación de la red es necesario un Laboratorio para realizar todas las pruebas necesarias tanto en la red Local como en la red Extendida, como se muestra en la figura 6.5

El laboratorio de Soporte y Pruebas sirve para simular la Matriz y una Agencia como se muestra en la figura 6.3; éste consta de dos ruteadores, dos *modems*, dos *Hubs*, un servidor *UNIX*, dos servidores *NT* y usuarios para realizar las respectivas pruebas de conexión.

Los *modems* se pueden remplazar por cables *RS232 pin* a *pin* cuando un ruteador es *DTE* y el otro es *DCE*, o por un cable *RS232* cruzado cuando los dos ruteadores trabajan como *DTE*.

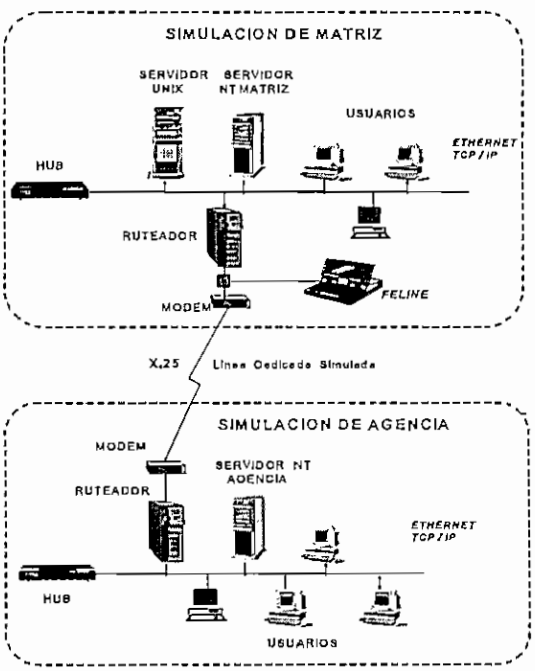


Figura 6.5 Laboratorio de Pruebas y Soporte

Se configuran y realizan los diagnósticos de los ruteadores para formar la red extendida *IP* empleando las utilidades de éstos.

En los Servidores y Usuarios se cargan los Sistemas Operativos y luego el Software de red que en este caso es *TCP/IP*, configurando los equipos con direcciones *IP* únicas.

Se configuran discos fijos **maestros** de Servidores *Windows NT* y de Usuarios de *Windows* para Trabajo en Grupo, luego se realiza copias de los discos para el resto de Servidores y Usuarios. Se configuran los parámetros individuales en cada disco y se instala en los respectivos equipos. Con este procedimiento se agilita el proceso de configuración de Servidores y Usuarios de la red.

6.3.2 MONITOREO DE RED EXTENDIDA Y LOCAL

Una herramienta para el análisis de datos es el *FELINE* que permite observar y analizar el flujo de datos entre equipos que se comunican a través de una red *WAN* X.25, para lo cual el analizador se conecta en la línea de datos X.25. Los datos del enlace X.25 son capturados y guardados para su análisis posterior en los diferentes niveles del modelo X.25.

A continuación se muestra capturas de datos obtenidas en el laboratorio implementado con ruteadores *Motorola Vangard* 3000 enlazados a través de puertos X.25.

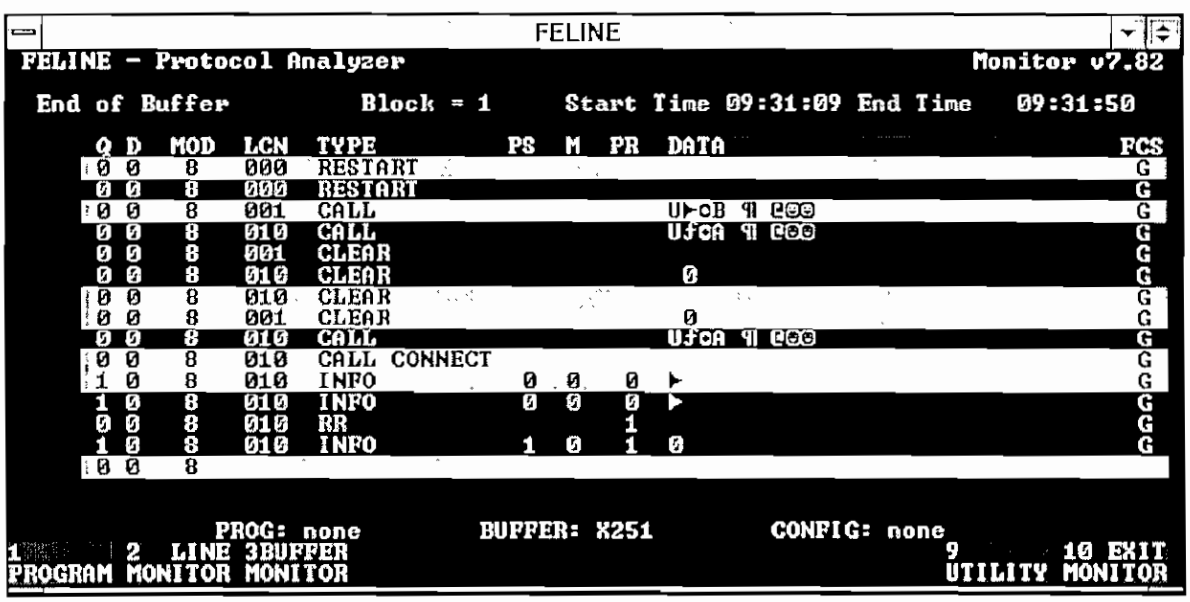


Figura 6.6 Enlace inicial de dos ruteadores sobre X.25

La figura 6.6 muestra la forma en que los dos ruteadores inician el enlace X.25 entre sí cuando éstos son inicializados o activados. En este caso, el ruteador configurado como *DTE* inicia una llamada *CALL* al ruteador configurado como *DCE* y espera una respuesta. El ruteador configurado como *DCE* realiza también una llamada *CALL* al ruteador *DTE*, el cual responde al requerimiento mediante *CALL CONNECT*, quedando establecida la conexión entre los dos.

Parte de los datos obtenidos en la captura de la figura 6.6 se muestran en detalle en el cuadro 6.2.

```
       Block Number: 1              FELINE DATA BUFFER                    Page 1

  Start Date:   [ 02/23/97 ]  Start Time: [ 09:31:09 ]  End Time:   [ 09:31:50 ]
  Protocol:     [   X.25   ]  Code:       [  ASCII 8 ]  Parity:     [  NONE    ]
  Baud Rate:    [   9600   ]  Clk Source: [ EXTERNAL ]  Buffer:     [CONTINUOUS]
  Mode:         [ SYNC NRZ ]  Select Addr:[    ALL   ]  Time Stamp:[    OFF   ]
  Ext Address:  [    OFF   ]  Ext Control:[    OFF   ]  Control:    [ MONITOR  ]
  Select LCN:   [    ALL   ]
  Select LGN:   [    ALL   ]
                                                        Disk:       [CONTINUOUS]
                 Input Leads              Output Leads
                -------------            -------------
                IN 1 =   CTS             OUT 1 =
                IN 2 =   DSR             OUT 2 =
                IN 3 =   DCD             OUT 3 =  DTR
                IN 4 =                   OUT 4 =  RTS
*******************************************************************************
CELL LINE Q D  MOD  LCN  TYPE          PS  M  PR  DATA                        FCS
*******************************************************************************
25   DTE= 0 0   8   000  RESTART                   NU NU                       G
36   DCE= 0 0   8   000  RESTART                   NU NU                       G
83   DTE= 0 0   8   001  CALL                       U DL HT  B NU D4 NU  @ SH  G
96   DCE= 0 0   8   010  CALL                       U SP HT  A NU D4 NU  @ SH  G
123  DCE= 0 0   8   001  CLEAR                     NU NU                       G
134  DCE= 0 0   8   010  CLEAR                     NU  0                       G
137  DTE= 0 0   8   010  CLEAR                     NU NU                       G
156  DTE= 0 0   8   001  CLEAR                     NU  0                       G
179  DCE= 0 0   8   010  CALL                       U SP HT  A NU D4 NU  @ SH  G
199  DTE= 0 0   8   010  CALL CONNECT                                          G
208  DTE= 1 0   8   010  INFO           0  0   0   DL                          G
218  DCE= 1 0   8   010  INFO           0  0   0   DL                          G
228  DCE= 0 0   8   010  RR                     1                             G
237  DCE= 1 0   8   010  INFO           1  0   1    0                         G
247  DTE= 0 0   8   010  RR                     1                             G
256  DTE= 1 0   8   010  INFO           1  0   1    0                         G
266  DTE= 0 0   8   010  RR                     2                             G
275  DTE= 0 0   8   010  INFO           2  0   2    E NU NU  4 NU SX NU NU  <  G
281  DCE= 0 0   8   010  RR                     2                             G
299  DCE= 0 0   8   010  INFO           2  0   2    E NU NU  4 NU SX NU NU  0  G
398  DTE= 0 0   8   010  INFO           3  0   2    E NU NU  4 NU ET NU NU  0  G
425  DCE= 0 0   8   010  INFO           3  0   2    E NU NU  4 NU ET NU NU  0  G
524  DTE= 0 0   8   010  RR                     3                             G
545  DCE= 0 0   8   010  RR                     3                             G
554  DCE= 0 0   8   010  RR                     4                             G
557  DTE= 0 0   8   010  RR                     4                             G
572  DCE= 0 0   8   010  INFO           4  0   4    E NU NU  4 NU EQ NU NU  ;  G
575  DTE= 0 0   8   010  INFO           4  0   4    E NU NU  4 NU EQ NU NU  ;  G
698  DCE= 0 0   8   010  RR                     5                             G
701  DTE= 0 0   8   010  RR                     5                             G
```

Cuadro 6.2 Enlace inicial X.25 entre dos ruteadores Vangard 3000

La figura 6.7 muestra el flujo de datos en X.25 cuando se realiza una conexión *Telnet* desde un usuario de red local *Ethernet* hasta un servidor *UNIX* remoto que también está conectado en una red *Ethernet* remota.

Con ésto se puede analizar el flujo y tipo de información *IP* que se transmite por las conexiones X.25.

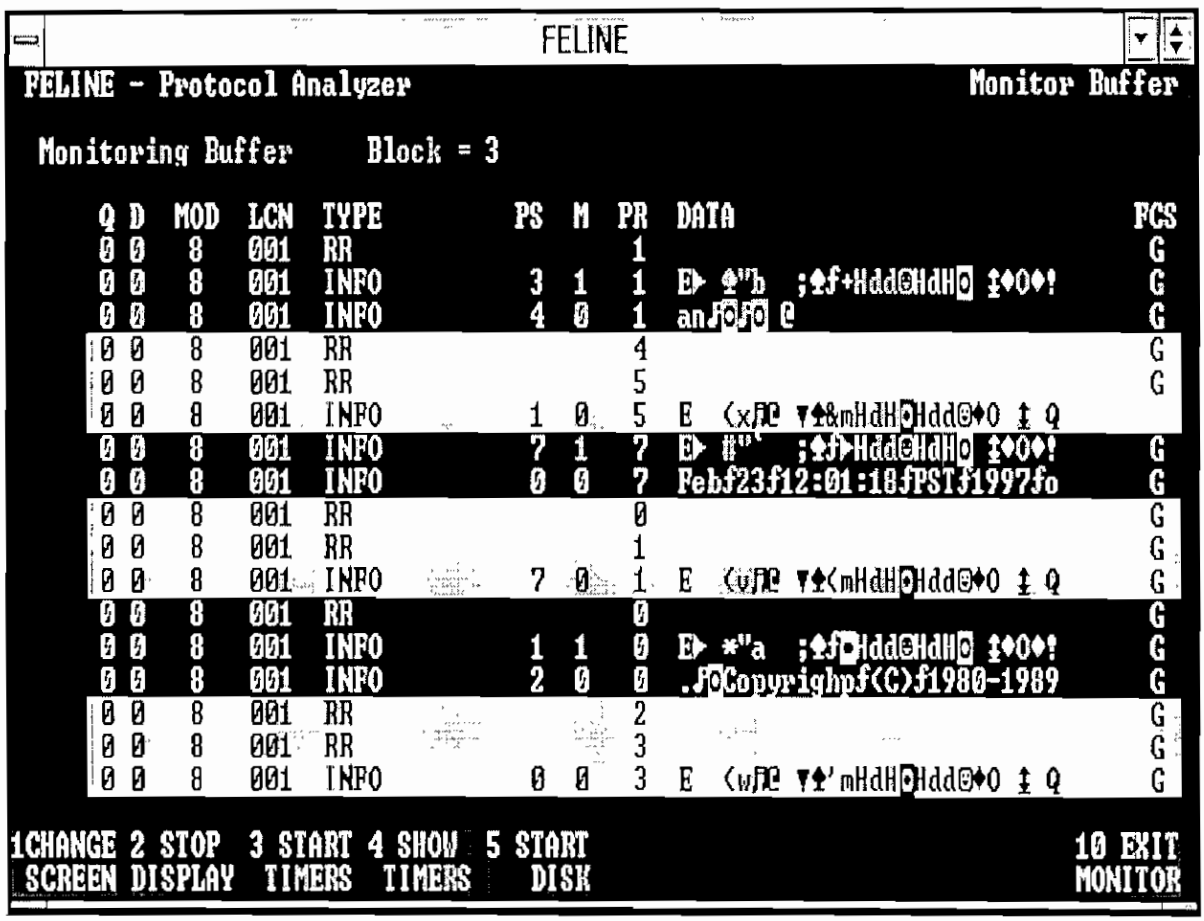


Figura 6.7 Proceso *Telnet* a través de X.25

El cuadro 6.3 muestra parte de los datos capturados en el proceso de la figura 6.7, donde se observa que el servidor responde enviando la fecha **Feb 23**, la hora **12:01:18** y el año **1997** y ***Copyright*** **1980-1989**, hacia el usuario remoto; todos estos datos se envían en el campo *INFO*.

```
  Block Number: 1                FELINE DATA BUFFER                          Page 1
  Start Date:  [ 02/23/97 ]  Start Time: [ 10:05:14 ]  End Time:  [ 10:05:47 ]
  Protocol:    [   X.25   ]  Code:       [ ASCII 8 ]  Parity:    [  NONE    ]
  Baud Rate:   [   9600   ]  Clk Source: [ EXTERNAL ]  Buffer:    [CONTINUOUS]
  Mode:        [ SYNC NRZ ]  Select Addr:[    ALL   ]  Time Stamp:[    OFF   ]
  Ext Address: [    OFF   ]  Ext Control:[    OFF   ]  Control:   [ MONITOR  ]
  Select LCN:  [    ALL   ]
  Select LGN:  [    ALL   ]
                 Input Leads            Output Leads
                 -----------            ------------
                 IN 1 =   CTS           OUT 1 =
                 IN 2 =   DSR           OUT 2 =
                 IN 3 =   DCD           OUT 3 =  DTR
                 IN 4 =                 OUT 4 =  RTS
*******************************************************************************
Block = 1     Cell =1

DCE=  HT   c   H   d   d  SH   H   d   H  LF  NU  EB  ET   "   2   /  SY   #
DTE=

DCE=  NU   c  RS   J   P  CN  DL  NU  BL   X  NU  NU  DE   ~  SH  DE   {  SH
DTE=

DCE=  CR  LF  CR  LF   U   N   I   X  SP   S   y   s   t   e   m  SP   V  SP
DTE=

DCE=   R   e   l   e   a   s   e  SP   3   .   2  SP   (   r   c   h   a   n
DTE=

DCE=   .   1   a   h   o   r   .   c   o   m   )  SP   (   p   p   y   p   0
DTE=

DCE=   )  CR  LF  CR  NU  CR  LF  CR  NU  NU   @   Q  D4  F2
DTE=                                                        F1  EX   B  DL

DCE=  DL  NU  D4   \  NU  NU   l   o   g   i   n   :  SP  NU   @  BL   b  F2
DTE=

DCE=
DTE=  F1  EX  AK  DL  SH  SH  VT   9  F2  F1  EX  BS  DL  SH  ET   E  NU  NU

DCE=   c  RS   U   P  CN  DL  NU  SI   0  NU  NU   P   a   s   s   w   o   r
DTE=

DCE=   d   :  NU   @  DL   R  F2                                      F1  EX
DTE=                                  F1  EX   (  DL  SH  SH  SB  CN  F2

DCE=  CN  DL  NU  NK   "  NU  NU   L   a   s   t  SP  SP  SP   s   u   c   c
DTE=

DCE=   e   s   s   f   u   l  SP   l   o   g   i   n  NU   @  SP  NK  F2
DTE=                                                                    F1

DCE=                                                F1  SH  AK  DL  SH   a  CR
DTE=  SP   k   e   y  NU  NU  NU   @   &   W  F2

DCE=  NU   c  RS   ^   P  CN  DL  NU   ]  D1  NU  NU  SP  SP   f   o   r  SP
DTE=

DCE=   r   o   o   t   :  SP   S   u   n  SP   F   e   b  SP   2   3  SP   0
DTE=

DCE=   8   :   4   2   :   2   9  SP   P   S   T  SP   1   9   9   7  SP   o
DTE=

DCE=   n  SP   p   p   y   0   1  CR  LF  SP  SP  SP   2  SP   u   n   s   u
DTE=

DCE=   c   c   e   s   s   f   u   l  SP   l   o   g   i   n   s  SP   f   o
DTE=

DCE=   r  SP   r   o   o   t   :  SP   S   u   !   5  F2  F1  SH  LF  DL  SH
DTE=

DCE=   h       n      SP      F           e   b  SP          2       3
DTE=      F1  SH      SH      RS      EX  F2              F1  EX      (

DCE=      SP      1      0       :           0   8   :   4   7  SP   P   S
DTE=  DL      SH      SH      D2      FS  F2
```

DCE=	T	SP	1	9	9	7	SP	o	n	SP	t	t	y	p	0	CR	LF	NU
DTE=																		
DCE=	NU	-	r	NU	NU	S	C	O	SP	U	N	I	X	SP	S	y	s	t
DTE=																		
DCE=	e	m	SP	V	/	3	8	6	SP	R	e	l	e	a	s	e	SP	3
DTE=																		
DCE=	.	2	CR	LF	C	o	p	y	r	i	g	h	t	SP	(	C	)	SP
DTE=																		
DCE=	1	9	7	6	-	1	9	8	9	SP	U	N	I	X	SP	S	y	s
DTE=																		
DCE=	t	e	m	SP	L	a	b	o	r	a	t	o	r	i	e	s	,	SP
DTE=																		
DCE=	I	n	c	C	c	F2	F1	SH	`	DL	SH	FF	.	CR	LF	C	o	p
DTE=																		
DCE=	y	r			i		g		h		t		SP		(			C
DTE=			F1	EX		SO		DL		SH		A		1		7	F2	
DCE=	)	SP	1	9	8	0	-	1	9	8	9	SP	M	i	c	r	o	s
DTE=																		
DCE=	o	f	t	SP	C	o	r	p	t	NU	@	n	HT	F2				
DTE=															F1	EX	SP	DL
DCE=	o	p	y	r	i	g	h	t	SP	(	C	)	SP	1	9	8	3	-
DTE=																		
DCE=	1	9	9	2	SP	T	h	e	SP	S	a	n	t	a	SP	C	r	u
DTE=																		
DCE=	z	SP	O	p	e	r	a	p	i	o	n	,	SP	I	n	c	.	CR
DTE=																		
DCE=	LF	A	1	1	SP	R	i	g	h	t	s	SP	R	e	s	e	r	v
DTE=																		
DCE=	e	d	CR	LF	r	c	h	9	SO	F2	F1	SH	F	DL	SH	SP	a	n
DTE=																		
DCE=	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	W	e	l	c	o	m	e	SP
DTE=																		
DCE=	t	o	SP	S	C	O	SP	U	N	I	X	SP	S	y	s	t	e	m
DTE=																		
DCE=	SP	V	/	3	8	6	SP	R	e	l	e	a	s	e	SP	3	.	2
DTE=																		
DCE=	9	F2	F1	SH	,	DL	SH	D	SP	SP	SP	SP	SP	SP	SP	F	r	o
DTE=																		
DCE=			m		CR		LF		CR		LF		SP			SP	SP	SP
DTE=	F1	EX		J		DL		SH		A		FF		z	F2			
DCE=	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	T	h
DTE=																		
DCE=	e	SP	S	a	n	t	a	SP	C	r	u	z	SP	O	p	e	r	a
DTE=																		
DCE=	t	i	o	n	,	SP	I	n	c	.	CR	LF	CR	LF	CR	LF	y	o
DTE=																		
DCE=	u	SP	h	a	v	e	SP	m	a	i	l	CR	LF	NU	@	B	p	F2
DTE=																		
DCE=	"	NU	c	RS	^	P	CN	DL	NU	SI	.	NU	NU	T	E	R	M	SP
DTE=																		
DCE=	=	SP	(	a	n	s	i	)	SP	NU	@	%	U	F2				
DTE=															F1	EX	SP	DL

Cuadro 6.3 Captura de datos de un proceso *Telnet* sobre un Enlace X.25

En la figura 6.8 se muestra un proceso *FTP* desde una máquina con *Windows* para Grupos hasta una máquina con *Windows NT* a través de X.25.

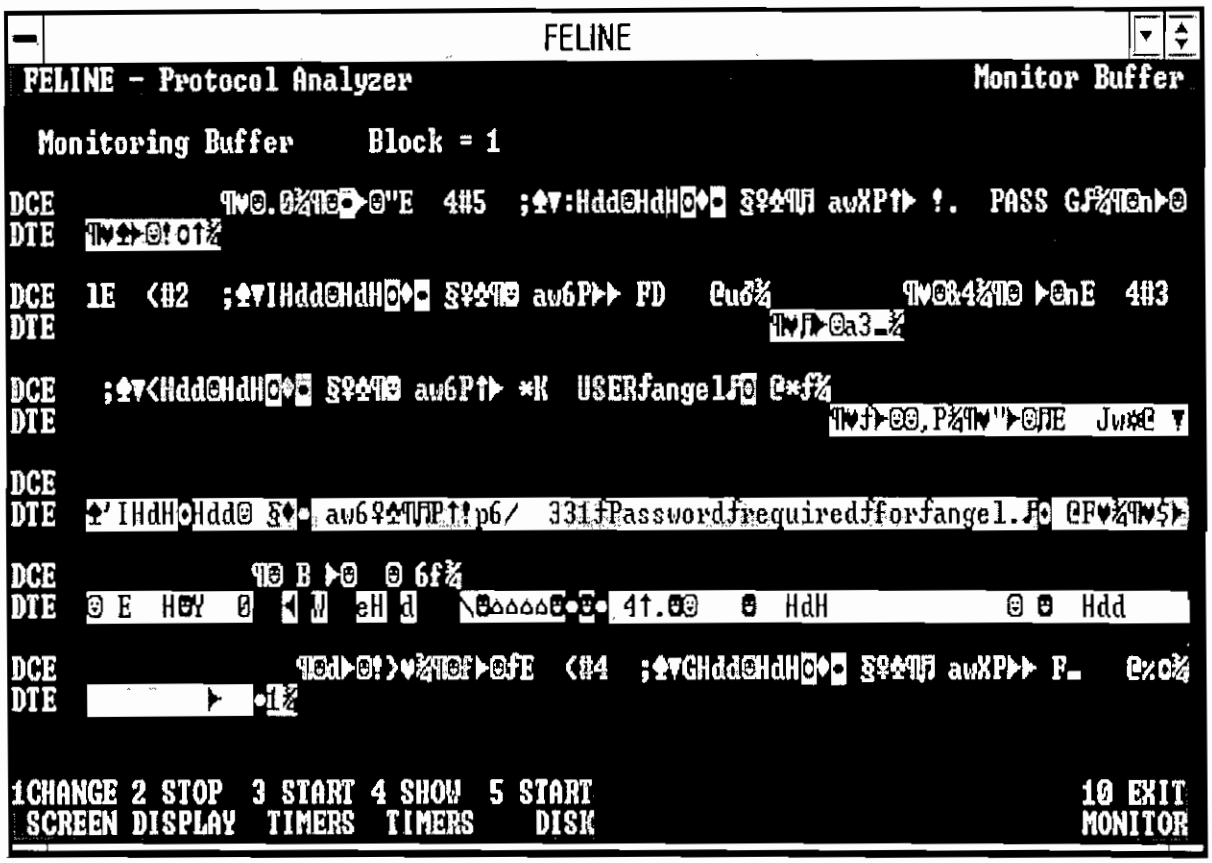


Figura 6.8 Proceso *FTP* a través de X.25

Parte de los datos capturados en el proceso *FTP* de la figura 6.8 se indican en el cuadro 6.4, donde se observa que el equipo con *Windows NT* le responde al usuario **angel** pidiendo que ingrese un ***password*** para tener acceso a los archivos. El usuario ingresa el *password* que en este caso es ***angel*** que se ingresa a continuación de **PASS** en el cuadro 6.4. Se observa luego que el usuario ingresa en el Servidor *Windows NT* 3.5 cuya dirección *IP* es 200.100.100.1.

Cada vez que se ejecuta un comando en el equipo remoto *NT* como por ejemplo un ***DIR*** aparece al final de la operación el mensaje ***Transfer Complete.***

```
 Block Number: 1              FELINE DATA BUFFER                        Page 1

 Start Date:  [ 02/23/97 ]  Start Time: [ 12:22:57 ]  End Time:  [ 12:24:00 ]
 Protocol:    [   X.25   ]  Code:       [  ASCII 8 ]  Parity:    [  NONE    ]
 Baud Rate:   [   9600   ]  Clk Source: [ EXTERNAL ]  Buffer:    [CONTINUOUS]
 Mode:        [ SYNC NRZ ]  Select Addr:[    ALL   ]  Time Stamp:[    OFF   ]
 Ext Address: [    ON    ]  Ext Control:[    OFF   ]  Control:   [ MONITOR ]
 Select LCN:  [    ALL   ]
 Select LGN:  [    ALL   ]
                                                      Disk:      [CONTINUOUS]
                 Input Leads              Output Leads
                 -----------              ------------
                 IN 1 =   CTS             OUT 1 =
                 IN 2 =   DSR             OUT 2 =
                 IN 3 =   DCD             OUT 3 =  DTR
                 IN 4 =                   OUT 4 =  RTS
********************************************************************************
Block = 1     Cell =1

DCE=
DTE=  D4  SX   P  CN   !  NU  SY   h  NU  NU   2   2   0  SP   s   e   r   v

DCE=
DTE=   i   d   o   r  SP   W   i   n   d   o   w   s  SP   N   T  SP   F   T

DCE=
DTE=   P  SP   S   e   r   v   e   r  SP   (   V   e   r   s   i   o   n  SP

DCE=                                                  F1  EX   A   *   r  F2
DTE=   3   .   5   )   .  CR  LF  NU   @  BS   E  F2

DCE=  SX  NU   a   w   6   P  CN  DL  NU   *   K  NU  NU   U   S   E   R  SP
DTE=

DCE=   a   n   g   e   l  CR  LF  NU   @   *  SP  F2
DTE=                                                  F1  EX  SP  DL  SH  SH

DCE=
DTE=   6  FF  EQ  D4  SO   P  CN   !   p   6   /  NU  NU   3   3   1  SP   P

DCE=
DTE=   a   s   s   w   o   r   d  SP   r   e   q   u   i   r   e   d  SP   f

DCE=
DTE=   o   r  SP   a   n   g   e   l   .  CR  LF  NU   @   F  EX  F2  F1  EX

DCE=  SO  NU   a   w   X   P  CN  DL  NU   !   .  NU  NU   P   A   S   S  SP
DTE=

DCE=   a   n   g   e   l  CR  LF  NU   @  BL   #  F2
DTE=                                                  F1  EX   (  DL  SH   A

DCE=
DTE=   X  FF  EQ  D4  SB   P  CN   !   h   &   0  NU  NU   2   3   0  SP   U

DCE=
DTE=   s   e   r  SP   a   n   g   e   l  SP   l   o   g   g   e   d  SP   i

DCE=                                          F1  SH   l  DL  SH   a   O  HT  F2
DTE=   n   .  CR  LF  NU   @   c  SH  F2

DCE=   w   s   P  CN  DL  NU  D2   }  NU  NU   S   Y   S   T  CR  LF  NU   @
DTE=

DCE=
DTE=   d   a  NU  NU   2   1   5  SP   W   i   n   d   o   w   s   _   N   T

DCE=
DTE=  SP   v   e   r   s   i   o   n  SP   3   .   5   0  CR  LF  NU   @   ^

DCE=   ;  NU  NU   P   O   R   T  SP   2   0   0   ,   1   0   0   ,   1   0
```

```
DTE=

DCE=   0   ,   1   ,   4   ,   9  CR  LF  NU   @   w  AK  F2
DTE=                                                      F1  EX   d  DL

DCE=
DTE=   a   w  DL  FF  EQ  D4   8   P  CN   !   J   w   \  NU  NU   2   0   0

DCE=
DTE=  SP   P   O   R   T  SP   c   o   m   m   a   n   d  SP   s   u   c   c

DCE=                                                      F1  SH  AK  DL
DTE=   e   s   s   f   u   l   .  CR  LF  NU   @   N  GS  F2

DCE=   `  NU  NU   L   I   S   T  CR  LF  NU   @  SI   I  F2
DTE=                                                      F1  EX   J  DL

DCE=
DTE=   a   w   .  FF  EQ  D4   >   P  CN   !   D  LF  BL  NU  NU   1   5   0

DCE=
DTE=  SP   O   p   e   n   i   n   g  SP   A   S   C   I   I  SP   m   o   d

DCE=
DTE=   e  SP   d   a   t   a  SP   c   o   n   n   e   c   t   i   o   n  SP

DCE=
DTE=   f   o   r  SP   /   b   i   n   /   l   s   .  CR  LF  NU   @  CR  D3

DCE=   0      NU      NU      ;      AK      US          ?   H          d
DTE=      SP      SP      SP      SP      SP      0   D          I   R

DCE=   d      SH      H       d      H       LF      ET      BS      NU
DTE=      >       SP      SP      SP      SP      SP      SP      SP      SP

DCE=
DTE=   1   :   5   2   A   M  SP  SP  SP  SP  SP  SP  SP   0   D   I   R   >

DCE=
DTE=  SP  SP  SP  SP  SP  SP  SP  SP  SP  SP   c   i   n   c   o  CR   ,   -

DCE=
DTE=  F2  F1  EX   ,  DL  SH   T  LF   0   8   -   0   6   -   9   7  SP  SP

DCE=      F1  SH      J       DL      SH      A       ET  1   F2
DTE=   1          1       :       5       1       A               M   SP  SP

DCE=
DTE=  SP  SP  SP  SP  SP   0   D   I   R   >  SP  SP  SP  SP  SP  SP  SP  SP

DCE=
DTE=  SP  SP   c   u   a   t   r   o  CR  LF   0   8   -   0   6   -   9   7

DCE=
DTE=  SP  SP   1   1   :   5   9   A   M  SP  SP  SP  SP  SP  SP  SP   <   D

DCE=                                                                  F1  SH
DTE=   !   D   e  SH  NU  NU   2   2   6  SP   T   r   a   n   s   f

DCE=      NU      DL      SH      *       E       NU      NU      (       #
DTE=   e      r       SP      c       o       m       p       1       e

DCE=      A       NU  NU              ;       AK      US      :       H
DTE=   t      e               .  CR      LF      NU      @       EX      c   F2
```

Cuadro 6.4 Captura de datos de un proceso *FTP* sobre un Enlace X.25

Para el monitoreo de la red *Ethernet* se emplea el ***SMS NETMONITOR*** que opera en *Windows NT* y permite el análisis de múltiples protocolos que viajan en la red *Ethernet* como los protocolos *TCP/IP, IPX/SPX.*

Se puede analizar las tramas y paquetes de datos que se intercambian entre pares de equipos.

La figura 6.9 muestra la captura de datos de un proceso TELNET entre los equipos TERMINAL 1 y SERVIDOR , el programa identifica el origen y destino de los datos que viajan en la red *Ethernet* y los va almacenando. Se puede observar que los equipos son fuente o destino en forma alternada para el envío y la recepción de mensajes.

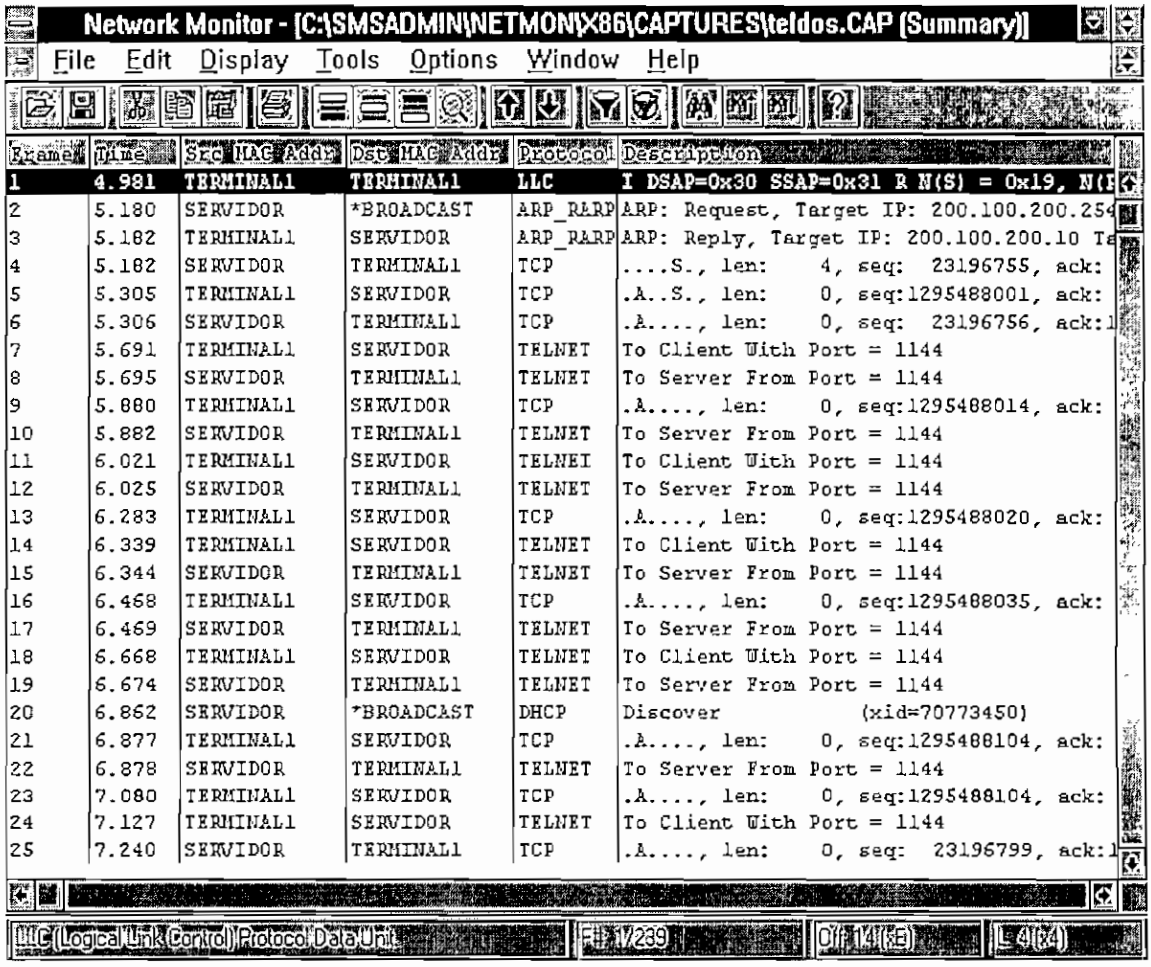


Figura 6.9 Captura de datos *Ethernet* en un proceso *Telnet* desde TERMINAL1 a SERVIDOR con *NETMONITOR SMS*

Mediante *NETMONITOR* se puede analizar los protocolos y datos de cada una de las capas.

La figura 6.10 describe el proceso *Telnet* del TERMINAL1, en donde los datos del protocolo *TELNET* que llegan al usuario TERMINAL 1 son ***login:***, los cuales viajan sobre *TCP* que es el protocolo de transporte.

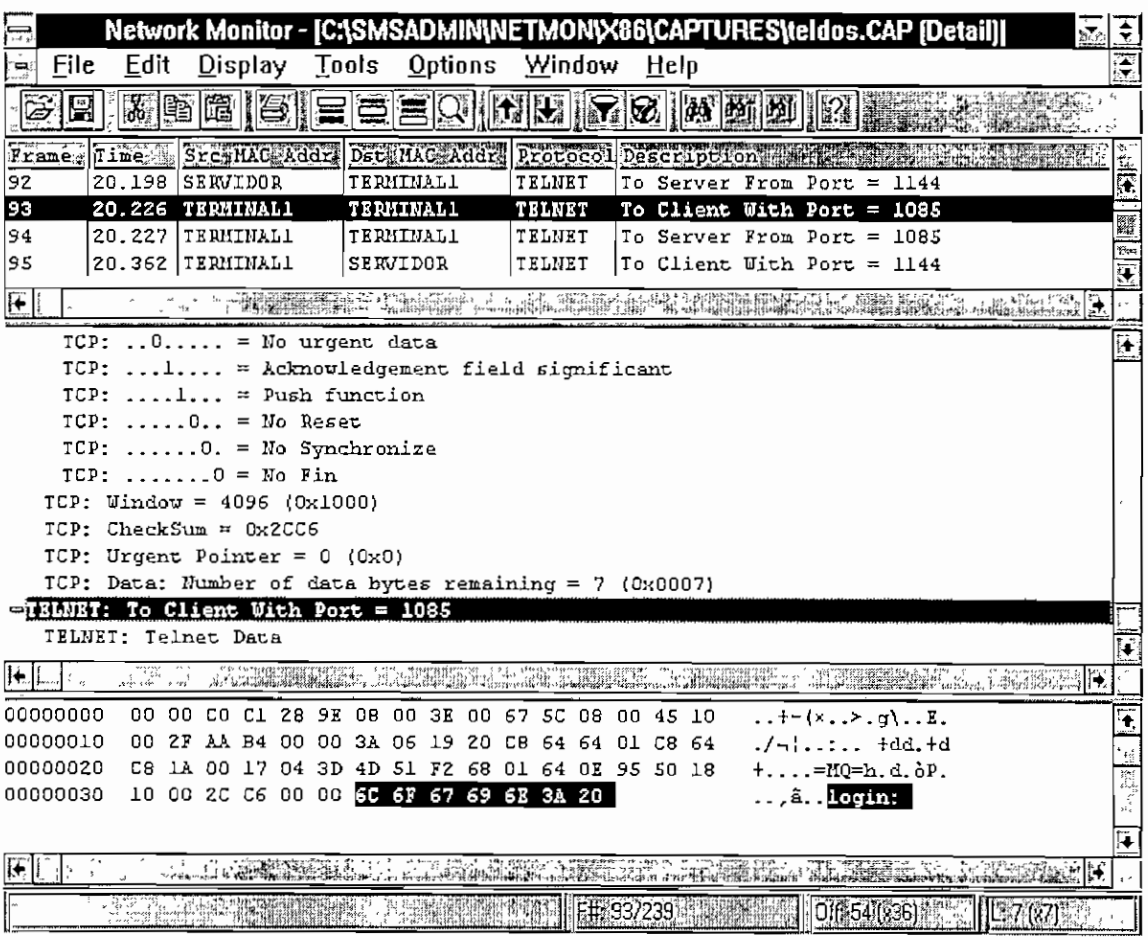


Figura 6.10 Análisis de protocolos en proceso *Telnet* entre TERMINAL 1 y SERVIDOR mediante *SMS NETMONITOR*

Parte de los datos capturados en la pantalla de la figura 6.10 se muestran en el cuadro 6.5, en donde se puede analizar los datos de la trama *Ethernet*, los datagramas *IP* que identifican las direcciones fuente y destino, el protocolo de transporte *TCP* que identifica los puertos y *sockets* origen y destino y el protocolo *Telnet* cuyos datos en este caso son ***login***: que son enviados del TERMINAL 1 al SERVIDOR.

```
*******************************************************************************
Frame    Time     Src MAC Addr   Dst MAC Addr   Protocol  Description
24       7.127    TERMINAL1      SERVIDOR       TELNET    To Client With Port = 1144
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   SERVIDOR        IP

  FRAME: Base frame properties
      FRAME: Time of capture = Feb 23, 1997 10:6:21.303
      FRAME: Time delta from previous physical frame: 47 milliseconds
      FRAME: Frame number: 24
      FRAME: Total frame length: 61 bytes
      FRAME: Capture frame length: 61 bytes
      FRAME: Frame data: Number of data bytes remaining = 61 (0x003D)
      ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
      ETHERNET: Destination address : 00AA00B56B50
      ETHERNET: Source address : 08003E00675C
      ETHERNET: ......0. = Universally administered address
      ETHERNET: Frame Length : 61 (0x003D)
      ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
      ETHERNET: Ethernet Data: Number of data bytes remaining = 47 (0x002F)

  IP: ID = 0xAA8C; Proto = TCP; Len: 47
      IP: Version = 4 (0x4)
      IP: Header Length = 20 (0x14)
      IP: Service Type = 16 (0x10)
      IP: Total Length = 47 (0x2F)
      IP: Identification = 43660 (0xAA8C)
      IP: Flags Summary = 0 (0x0)
      IP: Fragment Offset = 0 (0x0) bytes
      IP: Time to Live = 58 (0x3A)
      IP: Protocol = TCP - Transmission Control
      IP: CheckSum = 0x1958
      IP: Source Address = 200.100.100.1
      IP: Destination Address = 200.100.200.10
      IP: Data: Number of data bytes remaining = 27 (0x001B)

  TCP: .AP..., len:    7, seq:1295488104, ack:  23196799, win: 4096, src:   23 (TELNET)
   dst: 1144
      TCP: Source Port = Telnet
      TCP: Destination Port = 0x0478
      TCP: Sequence Number = 1295488104 (0x4D379468)
      TCP: Acknowledgement Number = 23196799 (0x161F47F)
      TCP: Data Offset = 20 (0x14)
      TCP: Reserved = 0 (0x0000)
      TCP: Flags = 0x18 : .AP...
          TCP: ..0..... = No urgent data
          TCP: ...1.... = Acknowledgement field significant
          TCP: ....1... = Push function
          TCP: .....0.. = No Reset
          TCP: ......0. = No Synchronize
          TCP: .......0 = No Fin
      TCP: Window = 4096 (0x1000)
      TCP: CheckSum = 0xA4CD
      TCP: Urgent Pointer = 0 (0x0)
      TCP: Data: Number of data bytes remaining = 7 (0x0007)

  TELNET: To Client With Port = 1144
      TELNET: Telnet Data

00000:  00 AA 00 B5 6B 50 08 00 3E 00 67 5C 08 00 45 10   ....kP..>.g\..E.
00010:  00 2F AA 8C 00 00 3A 06 19 58 C8 64 64 01 C8 64   ./....:..X.dd..d
00020:  C8 0A 00 17 04 78 4D 37 94 68 01 61 F4 7F 50 18   .....xM7.h.a..P.
00030:  10 00 A4 CD 00 00 6C 6F 67 69 6E 3A 20           ......login:
```

Cuadro 6.5 Captura de datos de un proceso *Telnet* con *NETMONITOR*

En la figura 6.11 se observa que la dirección *IP* del TERMINAL 1 es 200.100.200.10 y del SERVIDOR es 200.100.100.1, es decir que están ubicados en redes diferentes enlazados mediante ruteadores a través de X.25 .

En el Anexo 6 se muestra en detalle los datos de la captura del proceso *Telnet*, en donde se observa que incluso se obtiene datos confidenciales como son el ***login*** y el ***password*** del ***root*** en el Servidor *Unix*, lo cual constituye un peligro si el *NETMONITOR* es operado por personal no autorizado, los cuales podrían ingresar desde otro equipo para modificar alguna de las bases de datos o algún parámetro del *UNIX* con el propósito por ejemplo de hacer sabotaje.

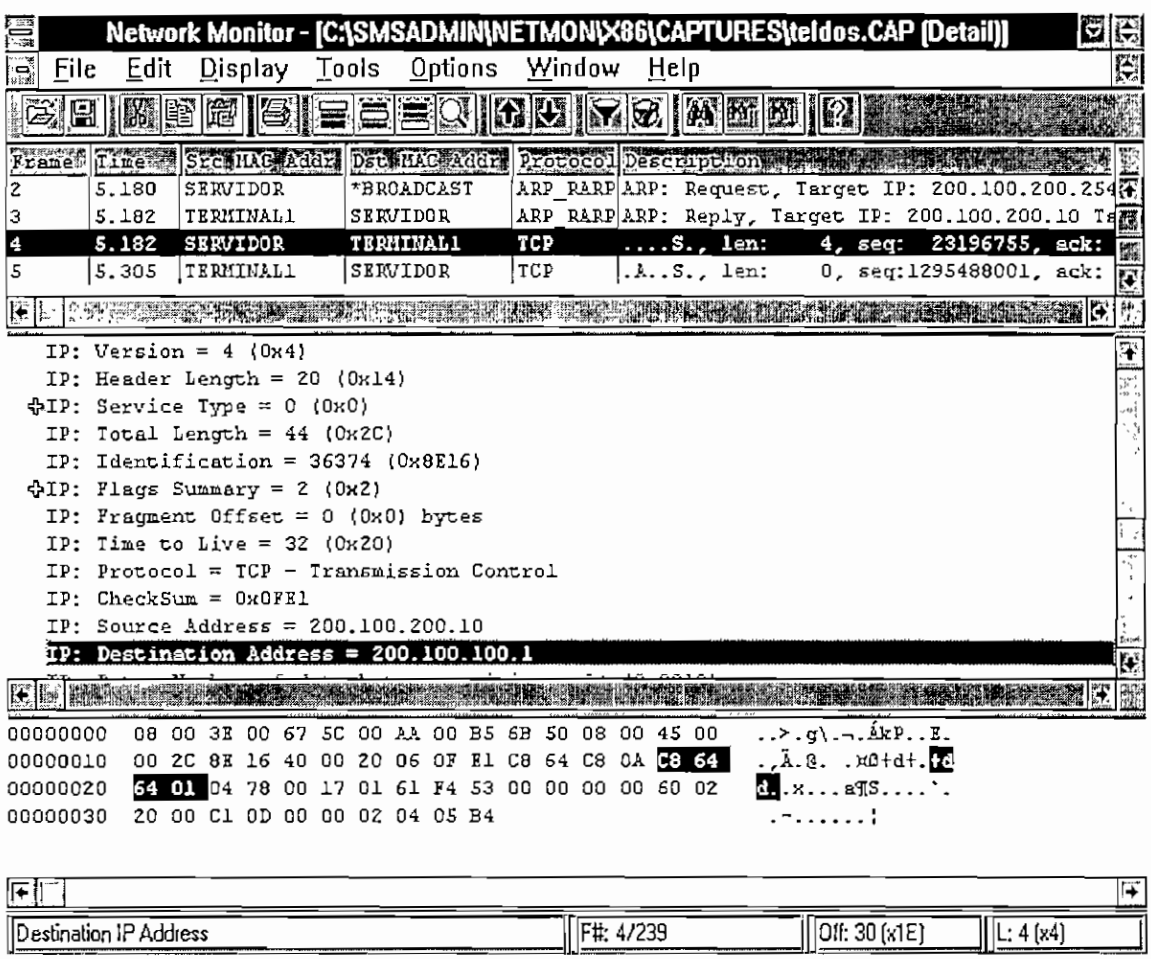


Figura 6.11 Análisis de protocolos *TCP/IP* entre TERMINAL 1 y SERVIDOR

La figura 6.12 muestra las bases de datos que se generan con los nombres, direcciones de red de las máquinas que están enviando mensajes en la red *Ethernet*.

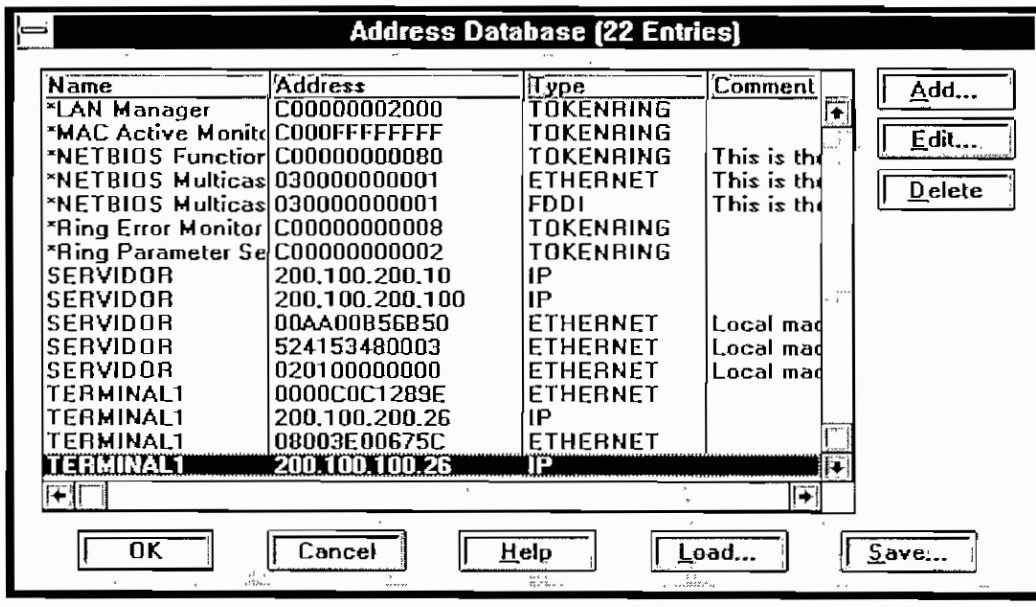


Figura 6.12 Base de datos con Nombres de Máquinas , Direcciones y tipo de red

También se puede realizar un monitoreo gráfico del uso de los diferentes recursos en los servidores, como son : procesador , memoria , tarjeta de red, *TCP*, *IP*, etc.

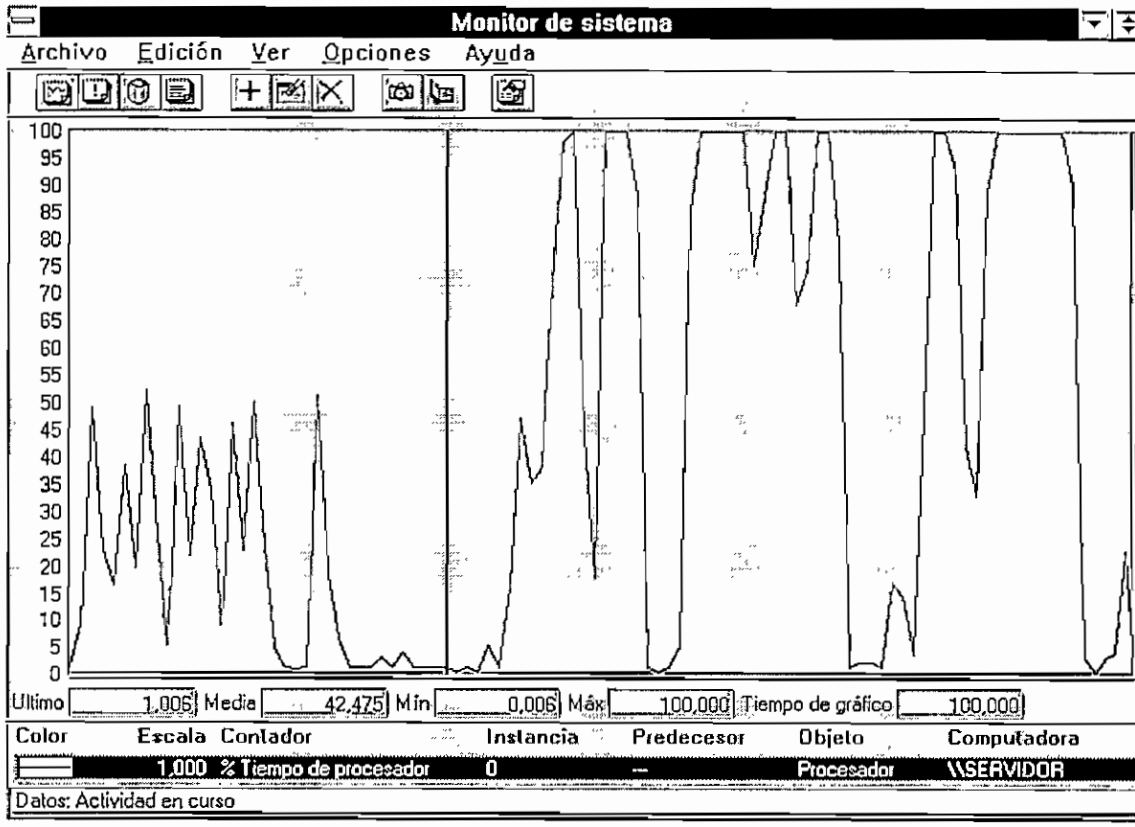


Figura 6.13 Monitoreo de Procesador en Servidor NT mediante *NETMONITOR*

La figura 6.13 muestra el porcentaje de utilización del Procesador, el mismo que se satura cuando se ejecutan varias aplicaciones a la vez. Esto ayuda a tomar decisiones, como puede ser el incremento de memoria en las máquinas para reducir la carga en el procesador.

También se puede hacer un análisis del segmento de red al cual está conectado el equipo, para chequear la carga en la red.

6.3.3 MONITOREO DEL FLUJO DE DATOS EN LA RED *ETHERNET* LOCAL

Para el monitoreo de la carga de datos en la red local de la Matriz y de las Agencias se coloca el *NETMONITOR* en un puerto del *Hub* Maestro (***Backbone*** de la red de la figura 6.3) de la red diseñada. De este modo se mide el flujo de datos entre los usuarios de la red y los Servidores *UNIX* y *NT* que están conectados con el *Hub* Maestro.

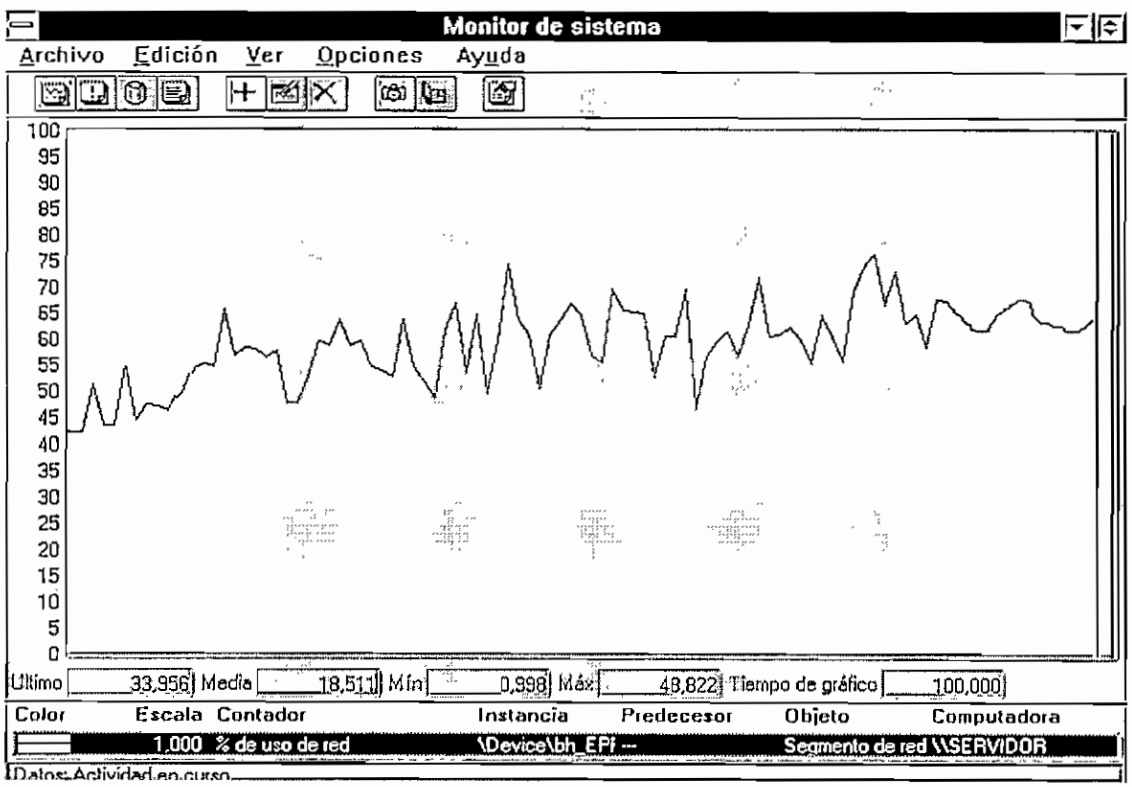


Figura 6.14 Monitoreo de Flujo de Datos en horas pico

La figura 6.14 muestra gráficamente el flujo de datos en el *Hub* Maestro en las **horas pico** que son por lo general de **10-12 a.m.** y de **15-17 p.m.**, en cuyos espacios se transfiere gran cantidad de información mediante procesos *FTP* desde las agencias hacia los Servidores de la

Matriz para realizar actualizaciones de los datos. Se observa que el porcentaje de utilización de la red en las horas críticas oscila alrededor del 60 %, el cual está dentro de los requerimientos de velocidad y rendimiento de la red.

El flujo de datos en las horas pico se puede observar en forma estadística en la figura 6.15.

Con este análisis se miden los siguiente parámetros:

- El porcentaje de utilización de la red en las horas pico es del 65 % en promedio.
- Se transmiten 220 tramas por segundo promedio a través del *Hub* Maestro.
- Son enviados 174.555 *bytes* por segundo
- Hay 5 mensajes de *Broadcast* por segundo
- Hay 4 mensajes *Multicast* por segundo

En general se puede decir que el estado de la red es normal.

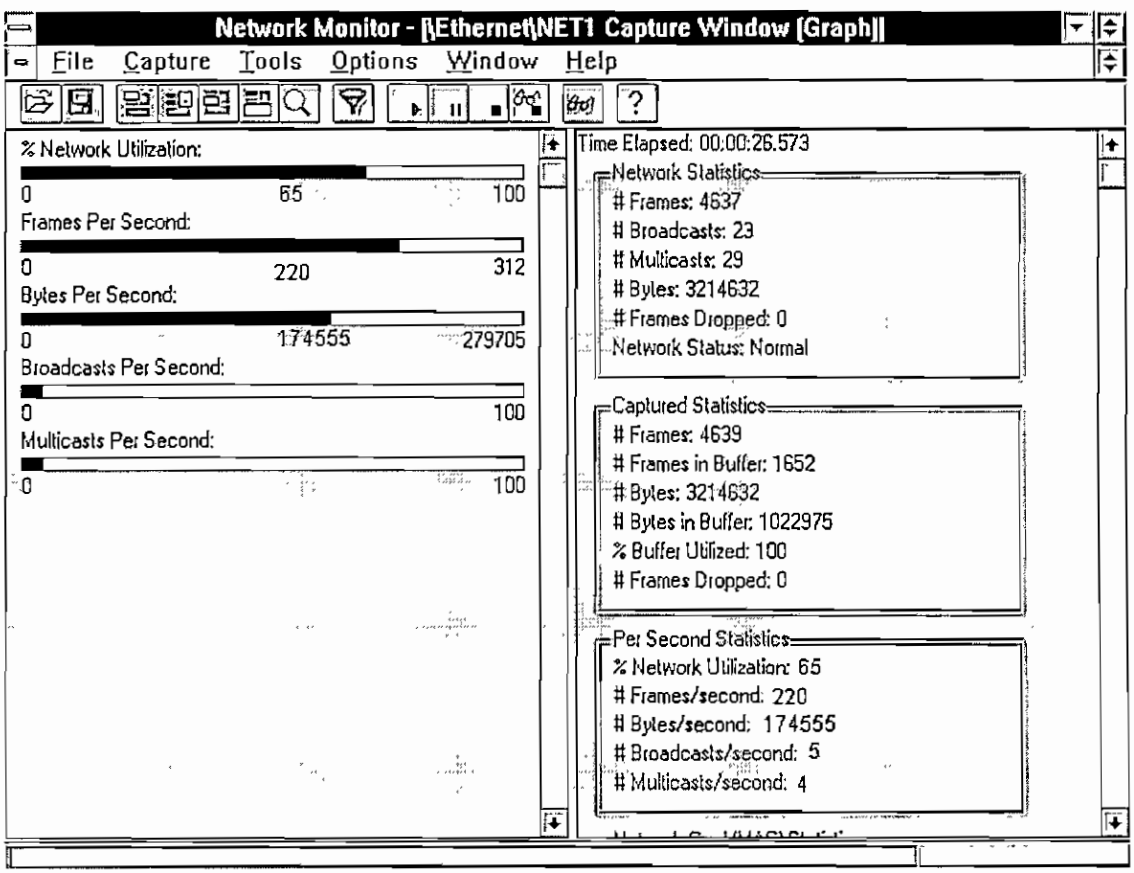


Figura 6.15 Estadísticas del flujo de datos en las horas pico

6.4 ANÁLISIS DE COSTOS

Mediante los cálculos realizados por ***Microsoft Project*** en el cronograma de instalación descrito en la sección 6.2 se obtiene los resultados de duración, tiempo en horas de trabajo y el costo total del soporte técnico requerido para la realización del proyecto.

Los resultados son los siguientes:

Fecha de Inicio : Lunes 26 de Febrero de 1996

Fecha de Finalización : Viernes 9 de Agosto de 1996

Duración : 120 días laborables

Tiempo de Trabajo : 4544 horas

Costo del Soporte Técnico : $ 85.840

Total de Técnicos : 20

El costo del Soporte Técnico se calcula en base al costo de la hora de trabajo de cada uno de los técnicos descritos en el cuadro 6.1 de la sección 6.2 .

El valor de los equipos de comunicación es aproximadamente de $ 54.200 en el que se incluye los costos de ruteadores, *modems*, *DTU*, y *Hubs* como se indica en el cuadro 6.6.

COSTOS DE EQUIPOS DE COMUNICACION DEL BANCO			
DESCRIPCION DE GASTOS	CANTIDAD	COSTO UNITARIO Dólares	COSTO TOTAL Dólares
Ruteadores *Motorola Codex* 6520 - 5 Puertos X.25, *Frame Relay*, *PAD* - 1 puerto de consola - 1 puerto Ethernet UTP de 10 Mbps	4	4.000,00	16.000,00
Modems Motorola Codex 3266	6	1.200,00	7.200,00
Unidades DTU digitales	5	1.200,00	6.000,00
Hubs Inteligentes Cabletron - 12 puertos *UTP* de 10 Mbps - 1 puerto *AUI* - 1 expansión para Stack	5	2.000,00	10.000,00
Hubs No Inteligentes *Cabletron* - 12 puertos *UTP* de 10 Mbps - 1 puerto *AUI* - 1 conexión al Hub maestro	10	1.500,00	15.000,00
Costo total de equipos de comunicación			**54.200,00**

Cuadro 6.6 Costos de equipos de comunicación de red *LAN* y *WAN*

Como se observa en el cuadro 6.7 el costo de la instalación del cable comprende solo el valor de los materiales por cuanto el costo de la mano de obra se incluye en el costo del soporte técnico.

COSTOS DE INSTALACION DE CABLE DE RED *UTP* DEL BANCO			
DESCRIPCION DE GASTOS	CANTIDAD	COSTO UNITARIO Dólares	COSTO TOTAL Dólares
Cable de red *UTP* nivel 5 (300 m)	10	180,00	1.800,00
Canaletas de 2x1" 2,4 m	300	14,00	4.200,00
Patch panels de 24 Puntos	15	180,00	2.700,00
Conectores RJ45 nivel 5	500	0,42	210,00
Roseta para RJ45	250	1,00	250,00
Costo total de instalación de cables			**9.160,00**

Cuadro 6.7 Costo de instalación del cable de red

El costo de las líneas dedicadas (Emetel) y de las líneas digitales empleadas para la comunicación entre agencias se calculó con referencia a un año de utilización de cada una de ellas, como se indica en el cuadro 6.8.

COSTOS ANUALES DE LAS LINEAS DE COMUNICACION			
DESCRIPCION DE GASTOS	CANTIDAD	COSTO UNITARIO Dólares	COSTO ANUAL TOTAL Dólares
Líneas Dedicadas	3	130/mes	4.680,00
Líneas Digitales			
Quito-Guayaquil	1	1750/mes	21.000,00
Quito-Cuenca	1	2250/mes	27.000,00
Quito-Ambato	1	1250/mes	15.000,00
Costo total de líneas de comunicación calculado al año de servicio			**67.680,00**

Cuadro 6.8 Costos de líneas de comunicación de red extendida

El cuadro 6.9 describe los costos de Servidores Centrales *UNIX*, Servidores *NT*, y usuarios con Windows para Trabajo en Grupo.

Se asume para el cálculo de computadoras que el Banco va ha cambiar la plataforma anterior, por cuanto resultaba obsoleta para el funcionamiento en redes *Ethernet*.

El valor de los elementos empleados para actualizar el *Hardware* se incluye dentro del costo total de los equipos, por cuanto sólo se realizó un incremento en la cantidad de memoria de los mismos.

COSTOS DE SERVIDORES Y USUARIOS DE LA RED DE DATOS DEL BANCO			
DESCRIPCION DE GASTOS	CANTIDAD	COSTO UNITARIO Dólares	COSTO TOTAL Dólares
Servidor *ATT* 3430 *UNIX* - 2 Procesadores *Pentium* de 90 Mhz - 4 Discos SCSI de 2 GB - 128 MB de memoria *RAM* - Doble canal *SCSI* - Tarjeta *Ethernet* de 10 Mbps - Unidad de Cinta de 2 GB - Unidad de *diskett* de 1.44 MB	2	20.000,00	40.000,00
Servidor *NT* - *Globalyst ATT* 3238 - Procesador *Pentium* de 90 Mhz - 64 MB de memoria *RAM* - Controladora *SCSI* - Disco SCSI de 1 GB - Tarjeta *Ethernet* de 10 Mbps - Unidad CD ROM	20	2.500,00	50.000,00
Usuarios - *Globalyst ATT* 3238 - Procesador 486DX2 de 66 Mhz - 16 MB de memoria RAM - Disco de 540 MB - Tarjeta *Ethernet* de 10 Mbps	100	1.500,00	150.000,00
Costo total de servidores y usuarios			240.000,00

Cuadro 6.9 Costos de Servidores y Usuarios de red

El cuadro 6.10 describe el costo de impresoras, *Scanners*, arreglo de discos ópticos de lectura - escritura para almacenamiento de imágenes de cheques y documentos.

COSTOS DE EQUIPOS ADICIONALES DE LA RED DE DATOS DEL BANCO			
DESCRIPCION DE GASTOS	CANTIDAD	COSTO UNITARIO Dólares	COSTO TOTAL Dólares
Scanner de Página *Epson*	4	450,00	1.800,00
Scanner Manual	8	120,00	960,00
Impresora *Laser*	8	470,00	3.760,00
Impresora de Cajas *NCR* 5021	16	600,00	9.600,00
Impresora matricial *Epson* LX 300	15	180,00	2.700,00
Impresora matricial *Epson* 1770	10	420,00	4.200,00
Arreglo de Discos Opticos	1	6.000,00	6.000,00
Clasificadora de Cheques *NCR* 7731	1	15.000,00	15.000,00
Costo total de equipos adicionales			44.020,00

Cuadro 6.10 Costos de equipos adicionales

En el cuadro 6.11 se describe el costo del *software* donde el ítem más alto es las Aplicaciones Bancarias con un valor aproximado de $ 200.000.

El valor de los "parches" de actualización se incluye en el valor del *Software* adquirido, en tanto que el *software* de monitoreo de red al ser opcional no se toma en cuenta para los cálculos.

COSTOS DE SOFTWARE			
DESCRIPCION DE GASTOS	CANTIDAD	COSTO UNITARIO Dólares	COSTO TOTAL Dólares
Software			
- *UNIX ATT release* 3.2	1	8.000,00	8.000,00
- *Sybase* 10	1	15.000,00	15.000,00
- *SQL Server*	1	4.400,00	4.400,00
- Aplicaciones Bancarias	1	200.000,00	200.000,00
- *Windows NT* 3.51	1	2.200,00	2.200,00
- *Windows* para Trabajo en Grupo	1	130,00	130,00
- *Software* de Clasificadora de Cheques	1	2.000,00	2.000,00
- *Software* de Captura de Imágenes	1	4.000,00	4.000,00
- *Software* de Monitoreo de Red			
. SMS (opcional)	1	2.000,00	2.000,00
. *Observer* (opcional)	1	1.000,00	1.000,00
.*Sniffer* (opcional)	1	14.000,00	14.000,00
Costo total de Software			235.730,00

Cuadro 6.11 Costo del Software

El cuadro 6.12 muestra un resumen de los costos de instalación de la Red de Datos del Banco en el que se incluye el costo de Soporte Técnico, materiales, *Hardware* y *Software*.

ANALISIS DE COSTOS DE LA IMPLEMENTACION DE LA RED DE DATOS DEL BANCO		
DESCRIPCION DE GASTOS	CANTIDAD	COSTO TOTAL Dólares
Costo Total de Soporte Técnico	20	85.840,00
Costo total de equipos de comunicación		54.200,00
Costo total de instalación de cables		9.160,00
Costo total de líneas de comunicación calculado al año de servicio		67.680,00
Costo total de servidores y usuarios		240.000,00
Costo total de equipos adicionales		44.020,00
Costo total de Software		235.730,00
TOTAL		736.630,00

Cuadro 6.12 Costos de Mano de Obra, Materiales, Equipos y *Software*

El valor total de la instalación es aproximadamente $ 733.510 el cual se justifica debido a que se realiza un cambio total de la red de datos tanto en *hardware* como en *software*.

6.5 PROYECCIONES

- Aumentar los usuarios por red local, para lo cual, el primer paso es añadir hasta 5 *Hubs* no Inteligentes de 12 puertos unidos a un *Hub* Inteligente a través de un bus ancho, para incrementar los puertos manteniendo el mismo ancho de banda de 10 *Mbps* para todos los *hubs* apilados.

- La red local puede migrar de 10 *BaseT* a 100 *BaseT* empleando el mismo cable UTP nivel 5, para lo que se debe cambiar las tarjetas de red de los equipos por tarjetas *Fast Ethernet* que pueden negociar las velocidades de operación de 10 o 100 *Mbps*, dependiendo del *Hub* al cual estén conectados. Se puede añadir otras tarjetas de red que operen a 20 *Mbps Full Duplex*.

  Para operar a mayor velocidad se debe cambiar los *Hubs* 10 *BaseT* por unos de 100 *BaseT* o por *Hub Switchs* de 100 *Mbps*. Los servidores *UNIX* , *NT* y usuarios especiales pueden estar conectados al *Switch* para lo cual se debe cambiar las tarjetas de red por unas que también operen a 100 *Mbps*.

- La red *WAN* se puede cambiar de X.25 a *Frame Relay* empleando los mismos ruteadores *Codex*, por cuanto los puertos de estos equipos soportan este tipo de comunicación. Las líneas empleadas pueden ser las líneas dedicadas de Emetel o las líneas digitales manejadas por Teleholdin, las cuales tienen un costo mayor como se muestra en el análisis de costos del cuadro 6.8. Para operar con las líneas digitales se requiere de equipos adicionales como son los *Data Termination Unit* de dos canales descritos en la sección 5.2, en los que se utiliza un canal para datos y un canal para voz, cada uno operando a 64 *Kbps* y haciendo el uso eficiente del ancho de banda.

  Otra forma de migrar las redes X.25 a una red *Frame Relay* se describe en la sección 5.3, en donde la red X.25 se conecta a la red dorsal *Frame Relay* a través de equipos de Transferencia e Intercambio de Paquetes y permite la migración a una red más veloz que puede llegar a una velocidad de transmisión de 2,048 *Mbps*.

Para migrar de la red *Frame Relay* a una red *ATM* se requiere de Intercambiadores de Paquetes de *Frame Relay* a *ATM* como se describió en las secciones 5.3.

- *ATM* es la red dorsal de banda ancha del futuro que permite la transferencia de voz, vídeo y datos a través de enlaces orientados a la conexión mediante fibra óptica por la que se alcanza una velocidades de 155 *Mbps*, 622 *Mbps* dependiendo del tipo de enlace.

En la sección 5.3.3 se describe la forma en que se puede migrar las redes *Ethernet* locales 10 *BaseT* hacia una red *ATM* empleando *Hubs* conmutables *ATM*, los cuales se conectan a la red dorsal *ATM* mediante enlaces por fibra óptica.

Se puede tener usuarios especiales conectados directamente a la red *ATM*, para lo cual se necesita de un interfaz de red *ATM* instalado en el computador, que por lo general deberían ser los Servidores *UNIX* y *NT*, con lo cual la velocidad de acceso a los recursos de cada computador se mejora notablemente.

- Otra forma de incrementar la velocidad de proceso es añadiendo memoria en los equipos, siendo recomendado subir hasta 32 MB en los usuarios, para que puedan trabajar más rápido si se cambia el Windows para Grupos con *Windows* 95.

- A los servidores *UNIX* se les puede poner un procesador adicional de 90 *Mhz* e incrementar la memoria de 256 hasta 1 *GB* con lo cual se incrementaría la velocidad de las transacciones en un 75 por ciento.

Se puede añadir discos internos de 4 *GB* con la finalidad de manejar las aplicaciones y bases de datos en forma más flexible.

Para añadir un arreglo de discos externos es necesario poner una tarjeta *SCSI* diferencial que maneja dispositivos externos.

- Para el incremento de agencias nuevas se requiere realizar las mismas tareas descritas en el cronograma de instalación, esto es, acondicionar el local con las instalaciones eléctricas y de datos respectivas. Se debe contratar el medio de enlace hasta la agencia, el que puede ser vía radio, satélite, línea telefónica dedicada Emetel, línea digital.

Para los enlaces vía satélite es necesario contratar canales de comunicación, lo cual incluye el alquiler de las antenas y los respectivos equipos de transmisión / recepción.

Los enlaces vía radio requieren del análisis geográfico de la zona donde se van ha ubicar las agencias. Se realiza el cálculo y dimensionamiento de equipos de radio que en ocasiones requieren de estaciones de repetición ubicadas en sitios estratégicos.

Se puede multiplexar canales de datos a través de una sola línea de comunicación empleando Multiplexores. Cada canal transmite datos de diferente tipo. En las agencias se coloca Demultiplexores que separan a los canales de datos y los envían a los respectivos destinos.

Se puede enlazar una **Agencia Nueva** mediante Servicio de Acceso Remoto, para lo cual se necesita que el Servidor *NT* de Agencia y el Servidor de *RAS* de la Matriz se comuniquen entre sí utilizando sus puertos seriales conectados a través de *modems*. A los puertos seriales de los servidores se les asigna una dirección *IP* y sirve para que el resto de usuarios de la agencia que tienen instalado *TCP/IP* puedan accesar a la Matriz a través de los servidores de *RAS* que se constituyen en *gateways* para este tipo de comunicación. Con este método nos ahorramos un ruteador costoso. La velocidad que se puede alcanzar en este tipo de enlaces es 19.200 *bps* como máximo.

Para el acceso a la red de usuarios especiales remotos a través de *modems*, se puede emplear del mismo modo el *RAS* instalado tanto en el servidor *NT* y en el Windows para Trabajo en Grupos pero no tiene la opción de utilizar el protocolo *TCP/IP*.

CAPITULO VI CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

- El presente trabajo de tesis, permitió familiarizarse con los avances tecnológicos en *hardware* y *software*, con la finalidad de dar una solución a la red de datos a nivel nacional en una Institución Bancaria, empleando los protocolos de alto nivel *TCP/IP* que son transportados a través de una red extendida confiable como es X.25, que ayuda a que la información que maneja el banco viaje en forma segura y libre de errores, lo cual es muy importante en este tipo de instituciones, donde se requiere un alto grado de integridad de los datos, por cuanto realizan procesos transaccionales, en donde la fallas en las comunicaciones pueden ocasionar pérdidas económicas incalculables.

- Se ha logrado mejorar las comunicaciones del Banco tanto en la red local como en la red extendida, reduciendo el tiempo e incrementando la distancia de transmisión, con lo que se facilita el acceso a la información y por lo tanto se reduce los costos de operación de la red, para lo cual fue necesario utilizar equipos de comunicación especiales como ruteadores, *hubs*, tarjetas controladoras de red.

- El método empleado para el direccionamiento X.25 de la red de datos, resulta adecuado por cuanto se ha tomado en cuenta las posibilidades de crecimiento que puede tener el Banco, a nivel de red extendida. Es decir la red es flexible a cambios que se produzcan en la red, como es el caso de incremento en el número de agencias o la instalación de equipos adicionales X.25.

- El direccionamiento *IP* realizado en la presente tesis permite tener una red estructurada, con el fin de facilitar las tareas de control y administración de la misma y permite el crecimiento tanto a nivel de red extendida como también a nivel de redes locales en cada una de las agencias, en donde se pueden generar usuarios de red en forma fácil, empleando similares métodos a los utilizados en el diseño de la red.

- Las tablas de rutas generadas tanto a nivel de X.25 como también a nivel de *IP*, permiten el correcto funcionamiento de la red de datos del banco por cuanto se estableció las correctas correspondencias entre las direcciones *IP* y las direcciones X.25, de forma que la información que viaja en la red llega hasta su destino y no se producen pérdidas por enlaces equivocados.

- Cuando se emplea *TCP/IP* sobre *X.25* se deben ajustar los parámetros de *X.25*, tales como el tamaño y la ventana de transmisión de los paquetes, así como los parámetros *TCP* como por ejemplo la ventana deslizante *TCP*, para lograr un rendimiento adecuado en la transferencia de archivos entre las redes de las agencias y la red de la matriz.

  Cuando se incrementa el tamaño del paquete X.25 o el tamaño de ventana de transmisión, se deben realizar los cambios tanto en el equipo transmisor como en el receptor, que para nuestro caso son los ruteadores X.25.
  Los parámetros de *default* de los ruteadores X.25 funcionan correctamente en el Banco.

- Cuando se interconectan las redes *LAN* de las agencias y la matriz a través de conexiones X.25, los protocolos de las capas superiores también influyen en el rendimiento de la transmisión de datos, produciendose retardos en la transferencia de datos, ocasionados por la adición de cabeceras.

- Tanto X.25 como *TCP/IP* realizan la detección y corrección de errores, por tal motivo la red se torna más lenta pero segura.
  Frame Relay en cambio deja que las capas superiores realicen la detección y corrección de los errores, siendo una de las razones por la que estas redes son más rápidas siendo una buena opción en redes *TCP/IP* en donde la integridad de los datos no es un punto fundamental.

- La evolución de los sistemas de información ha sido desde los sistemas jerárquicos hacia los sistemas en donde la información fluye en forma lateral entre los grupos de trabajo.

- Para la instalación de una red de datos de un Banco, es necesario contar con el personal técnico adecuado, entrenado y con los conocimientos suficientes para solucionar los problemas que se presenten en el transcurso de la implementación de la red de datos. Los ingenieros de *hardware* deben tener conocimientos de *software* básico para ser un verdadero soporte para la Institución Bancaria.

7.2 RECOMENDACIONES

- Para diseñar la red *IP* de una Institución Bancaria de tamaño grande es recomendable escoger una red tipo B que permite el crecimiento a futuro de la red de datos, por cuanto se puede generar hasta 2^{14} redes con 2^{16} usuarios cada una. Además se pueden generar subredes formando grupos de usuarios para tener mayor control sobre los mismos.

- Se puede enlazar una **Agencia Nueva** mediante Servicio de Acceso Remoto entre el Servidor *NT* de Agencia y el Servidor de *RAS* de la Matriz, los cuales se comunican entre sí utilizando sus puertos seriales conectados a través de *modems* con una velocidad de 19200 bps. A los puertos seriales de los servidores se les asigna una dirección *IP* y sirve para que el resto de usuarios de la agencia que tienen instalado *TCP/IP* puedan accesar a la Matriz a través de los servidores de *RAS* que se constituyen en *gateways* para este tipo de comunicación. Con este método nos ahorramos un ruteador.

- Para incrementar la velocidad de proceso en las transacciones es necesario realizar mejoras en los servidores y usuarios, pero principalmente en los Servidores *UNIX,* donde se adicionan procesadores, memoria, discos, tarjetas de red, arreglo de discos, de forma que el rendimiento del sistema en general mejore en un 75 %.

  En un futuro la red X.25 del Banco puede migrar hacia *Frame Relay*, para lo cual a los puertos de los ruteadores se los configura como *Frame Relay* y para el enlace entre redes se utilizan los multiplexores digitales de dos canales *DTU*, permitiendo la transmisión de voz y datos a través de líneas digitales de 64 *kbps*. Actualmente se emplean varios de los

puertos de los ruteadores para realizar tales operaciones entre las agencias. Sin embargo vale indicar que el costo de las líneas es bastante alto, pero se justifica por cuanto la transferencia de datos entre agencias se torna más rápido.

- Las redes X.25 y *Frame Relay* deben ser diseñadas con la posibilidad de poder migrar en el futuro hacia redes *ATM* para la transmisión de voz , vídeo y datos. Para este propósito se debe dimensionar y seleccionar los equipos y materiales con el fin de que no se requiera cambiar la infraestructura de red implementada anteriormente. *ATM* se convierte en la red dorsal de alta velocidad tanto a nivel de red local como a nivel de red extendida y se emplea intercambiadores de paquetes para transferir los datos de la red anterior hacia la red *ATM* , disminuyendo el costo en equipos y materiales.

  Cuando se interconectan dos redes *Frame Relay* a través de una red dorsal *ATM,* los circuitos virtuales *PVC* de *Frame Relay* son multiplexados a través de un sólo circuito virtual *PVC ATM.* Además los datos encapsulados en *FR* son transportados en forma transparente por *ATM.*

- Cuando se utiliza *Frame Relay* en redes privadas, se multiplexa el tráfico proveniente de varios lugares a través de la red dorsal extendida *Frame Relay*. Esto permite reducir el número de circuitos y el costo del ancho de banda. Una ventaja de la multiplexación de las conexiones lógicas a través de una conexión física simple es que disminuye el número de puertos físicos permitiendo así reducir el costo de acceso a las redes.

- *Frame Relay* se la utiliza cuando la transferencia de información es imprevisible, como en redes de tamaño medio que por lo general usan aplicaciones tales como correo electrónico, aplicaciones cliente-servidor, aplicaciones de manufacturas. No es recomendable en aplicaciones donde el tráfico de información es continuo como es el caso de desarrollo de software, transferencia de imágenes.

- Es recomendable que los ruteadores no funcionen al mismo tiempo como puentes, ya que los protocolos no enrutables como *NETBEUI* sobrecargan a la comunicación X.25 y las transmisiones se tornan lentas y con colisiones. La forma de evitar este congestionamiento, es establecer al *TCP/IP* como protocolo único de transporte y red, para lo que se debe eliminar en los usuarios y servidores el protocolo *NETBEUI.*

  Se debe configurar a los ruteadores para que operen solo con protocolos enrutables.

- También cabe mencionar que una red *Ethernet* funciona mucho más rápido cuando tiene un solo protocolo predeterminado para el intercambio de la información entre estaciones, evitando la existencia de paquetes con diferentes formatos que pueden ocasionar congestiones dentro de la red *Ethernet.*

- Actualmente se tiene redes *Ethernet* mucho más rápidas utilizando la misma infraestructura de cable *UTP* categoría 5, donde se utiliza *Hubs* 100 *BaseT* que operan a 100 MHz, con lo cual se incrementa la velocidad de transferencia entre estaciones.

  Sin embargo para migrar a este tipo de red se requiere un cambio de las tarjetas controladoras de red en las computadoras, de 10 *BaseT* a 100 *BaseT*, lo cual se justifica solo si la red es demasiado lenta.

- Es recomendable que los *Hubs* principales estén enlazados entre si a través de dos cables con el fin de mantener las comunicaciones cuando uno de los enlaces falla.

- Para el análisis de mensajes y datos que fluyen en una red se debe contar con sistemas de monitoreo de red, como es el caso de *Netmonitor*, que permite observar a los mensajes en cada una de las capas y determinar la forma de funcionamiento de las aplicaciones.

- Los criterios y métodos utilizados para el diseño de la red *TCP/IP* sobre X.25 para una Institución Bancaria pueden ser aplicados para diseñar e implementar redes en otro tipo de Instituciones que requieren una alta integridad en la transferencia de su información.

BIBLIOGRAFIA

[1] Comer, Douglas, Redes Globales de Información con Internet y TCP/IP, México, Prentice Hall, 1996

[2] Open Strategies Inc. and NCR, TCP/IP Technical Concepts, Usa, 1996

[3] Open Strategies Inc. and NCR, OSI/WAN Concepts, Usa, 1996

[4] Open Strategies Inc. and NCR, X.25 Concepts, Usa, 1996

[5] IBM PC Institute, IBM Server Technical Training, Usa, 1996

[6] FTP Software, Inc., PC/TCP Network Software V2.3 User Guide, Usa, 1986-1993

[7] NCR. Corporation, WIN-TCP User's Guide, Usa, 1991

[8] Motorola, Inc., 6500 Series Options and Protocols, Usa, 1995

[9] Sigmond and Agder Researh Foundation, TCP/IP over X.25, TeleKtronikk, Usa, 1992

[10] Malis, A. and Ullmann, R, Request For Comments 1356, Usa, 1992

[11] Bradley, T., Brown, C., and Malis, A., Request For Comments 1490, Usa, 1993

[12] Cisco Systems, Inc., ATM Internetworking, Usa, 1996

[13] Cisco Systems, Inc., Internetworking Technology Overview, Usa, 1995

[14] Uyless, Black, Redes de Computadoras, Protocolos, Normas e Interfaces, México, Macrobit, 1990

ANEXO 1 PROTOCOLOS ADICIONALES

1.1 PROTOCOLOS ENRUTABLES ADICIONALES

1.1.1 PROTOCOLOS *APPLE TALK*[1]

Son protocolos que trabajan en redes de equipos *Macintosh* que operan en base al modelo Cliente - Servidor.

La relación de los protocolos *Apple Talk* con el modelo de referencia *OSI* se muestra en la figura 1.1.

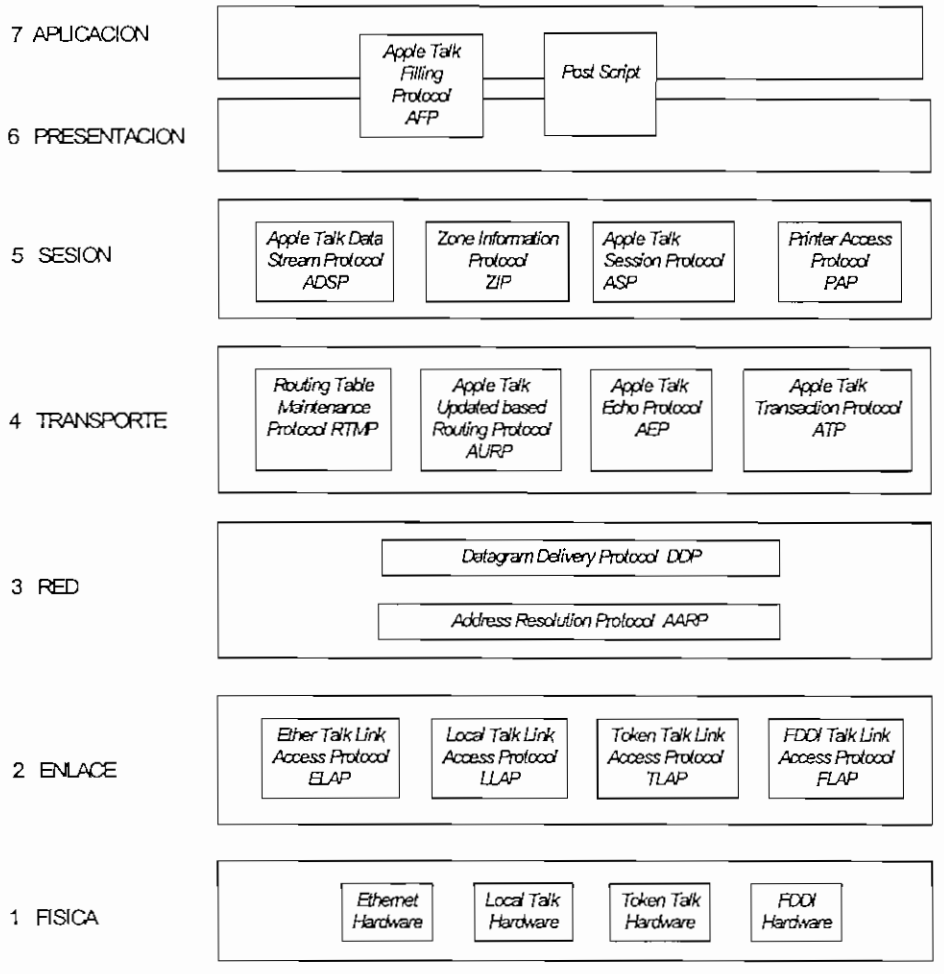


Figura 1.1 Relación de los protocolos *Apple Talk* con el modelo *OSI*

En la capa de red, el Protocolo de Liberación del Datagrama *(Datagram Delivery Protocol DDP)* provee un servicio sin conexión entre *sockets* de red.

[1] *Internetworking Technology Overview, Cisco* Capítulo 16

En la capa de transporte, los Protocolos de Mantenimiento de Tablas de Enrutamiento *(Routing Table Maintenance Protocol RTMP)* generan la tabla de rutas con las redes que se pueden alcanzar, las distancias, el puerto del ruteador local por el cual se accesa a la red destino, el siguiente ruteador que recibe el paquete y el estado de cada enlace.

Para el ejemplo de la figura 1.2 la tabla de rutas del Ruteador 1 se indica en el cuadro 1.1:

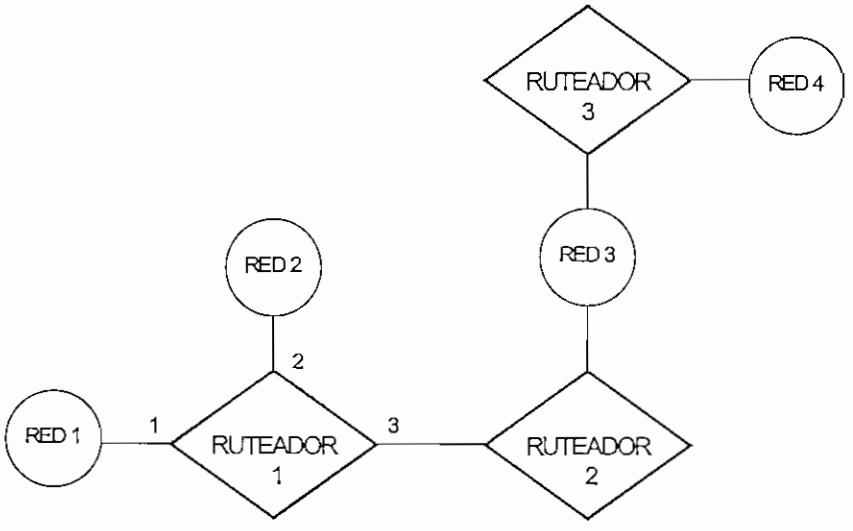


Figura 1.2 Enrutamiento en protocolo *Apple Talk*

Red destino	Distancia	Puerto	Siguiente ruteador	Estado
1	0	1	0	Bueno
2	0	2	0	Bueno
3	1	3	Ruteador 2	Bueno
4	2	3	Ruteador 2	Bueno

Cuadro 1.1 Tabla de rutas del Ruteador 1 y estado de cada enlace hacia los demás nodos

La distancia desde el Ruteador 1 hasta las redes adyacentes es 0.

Para llegar a la red 4 , la distancia es dos, se debe salir por el puerto local 3 y pasar primero por el Ruteador 2

1.1.2 PROTOCOLOS *DECNET*[2]

Es un conjunto de protocolos que conforman la Arquitectura de Red Digital *(Digital Network Architecture DNA)*.

La relación del modelo *DNA* con el modelo de referencia *OSI* se muestra en la figura 1.3.

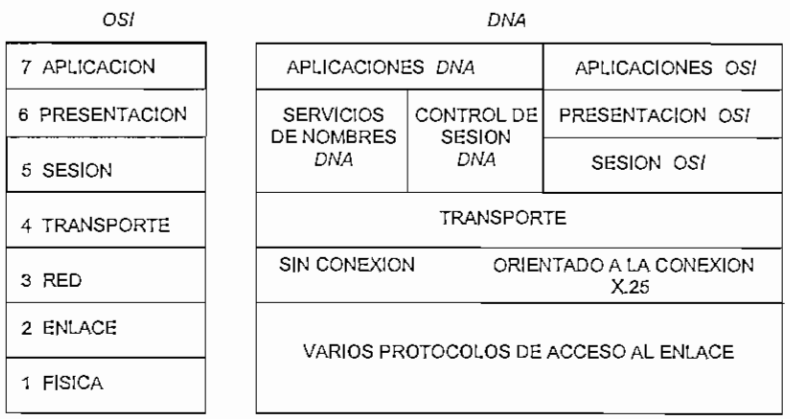


Figura 1.3 Relación del Modelo *DNA* con el modelo *OSI*

Como se observa en la figura 1.3 *DECnet* soporta capas red, tanto orientadas a conexión , como también no orientadas , a través de varios medios de enlace como *Ethernet, Token Ring , FDDI, y X.25.*

La capa red orientada a conexión usa el Protocolo de Nivel de Paquete X.25 (*Packet Level Protocol PLP*), el cual está en el nivel 3 del modelo X.25. Este protocolo es conocido también como Protocolo de Modo de Conexión de Red (*Connection Mode Network Protocol CMNP*).

La forma de enrutar los paquetes en la capa de transporte , es de la siguiente manera:

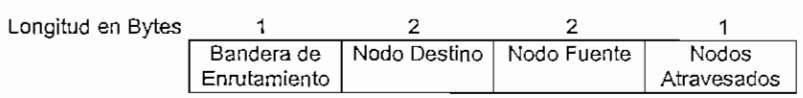


Figura 1.4 Formato de enrutamiento de la trama en la capa de transporte del modelo *DECnet*

[2] *Internetworking Technology Overview, Cisco* Capítulo 17

Para encontrar un *host* destino, DECnet divide a las redes en áreas.

La tabla de rutas se forma con pares de dirección **área / nodo**. En cada área se tiene ruteadores jerárquicos de nivel 1 y 2. Los del nivel 1, son los que se comunican con el *host*, y con otros ruteadores de nivel 1 o 2 pero en la misma área. Los de nivel 2, son los encargados de comunicarse con los ruteadores de nivel 2, pero de otra área diferente , para localizar un *host* remoto.

Este proceso se muestra en la red de la figura 1.5.

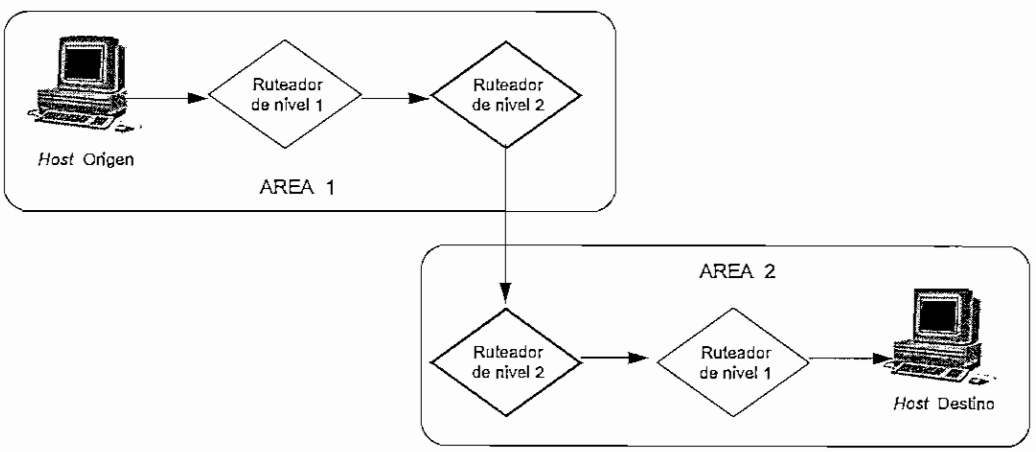


Figura 1.5 Ruteadores jerárquicos en los protocolos ruteables *DECnet*

1.1.3 PROTOCOLOS DE *NETWARE*[3]

Netware es un conjunto de protocolos cuya relación con el modelo de referencia OSI se muestra en la figura 1.6.

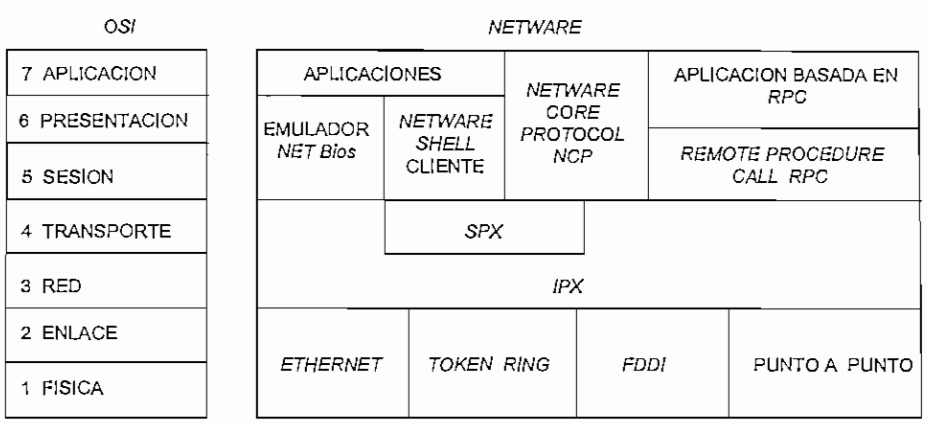


Figura 1.6 Relación de los protocolos *NETWARE* con el modelo *OSI*

[3] *Internetworking Technology Overview, Cisco* Capítulo 19

El protocolo de la capa red es *IPX* (*Internet Packet Exchange*), que es un protocolo no arientado a conexión , es decir, no provee reconocimiento de paquetes y control de las conexiones.

Los paquetes *IPX* viajan sobre varios medios como son *Ethernet, Token Ring, FDDI,*

Permite trabajar sobre enlaces *WAN* sincrónicos usando el protocolo Punto a Punto (PPP).

IPX emplea el protocolo *RIP (Routing Information Protocol*) para crear y mantener dinámicamente una base de datos con información de enrutamiento.

El formato del paquete IPX es el siguiente:

PAQUETE *IPX*

CHECKSUM	
LONGITUD DEL PAQUETE	
CONTROL DE TRANSPORTE	TIPO DE PAQUETE
RED DESTINO	
NODO DESTINO	
SOCKET DESTINO	
RED FUENTE	
SOCKET FUENTE	
DATOS DE CAPAS SUPERIORES	

Figura 1.7 Formato del paquete *IPX*

- El campo de Control de Transporte del paquete *IPX* indica el número de ruteadores por los que ha pasado el paquete.
- El Tipo de Paquete indica el protocolo de la capa superior que recibe el paquete.
- La capa transporte emplea el protocolo orientado a conexión llamado Intercambio de Paquetes Secuenciales *SPX (Sequenced Packet Protocol)* que permite el intercambio de paquetes *IPX* en forma confiable y segura entre los equipos de la red.

1.2 PROTOCOLOS INTERNET ADICIONALES

1.2.1 PROTOCOLO DE ASOCIACION DE DIRECCIONES (*ARP ADDRESS RESOLUTION PROTOCOL*) [4]

Es un protocolo de bajo nivel, que permite a un host encontrar la dirección física de otro *host* con solo proporcionar la dirección *IP* de su objetivo.

En el ejemplo de la figura 1.8, un host A desea conocer la dirección física del *host* B, para lo cual envía a toda la red un mensaje con la dirección IP_B de la estación B. Todos los anfitriones reciben el mensaje, pero sólo B reconoce su dirección IP_B y responde con su dirección física.
Cuando A recibe la respuesta, utiliza la dirección física, para enviar los paquetes directamente al *host* B.

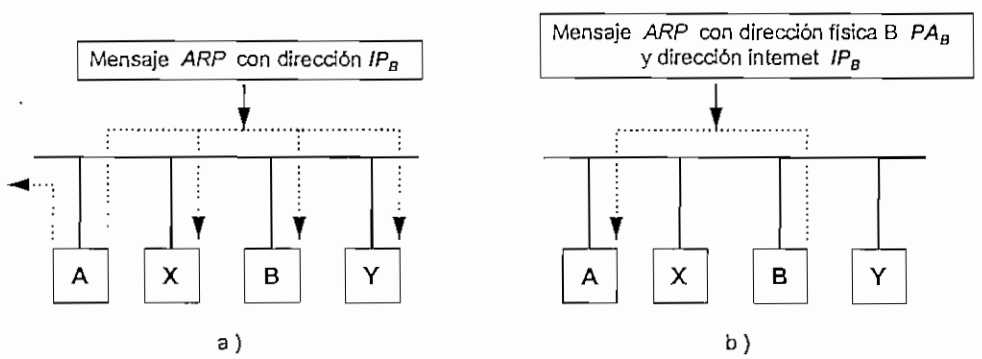


Figura 1.8 Proceso *ARP* a) pregunta, b) respuesta

Este protocolo permite asignar una dirección *IP* arbitraria a la máquina.

El encapsulamiento *ARP* es el siguiente:

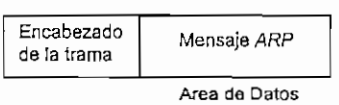
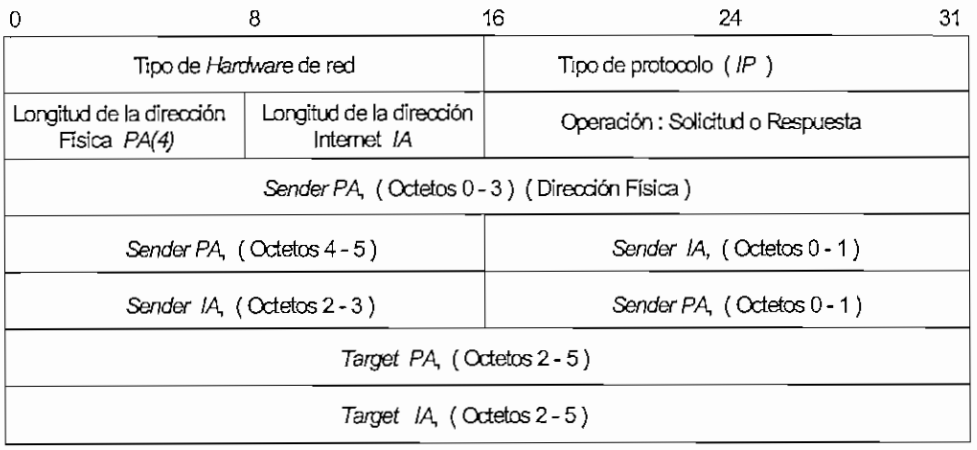


Figura 1.9 Formato del mensaje *ARP*

El formato del protocolo *ARP*, está formado por un número arbitrario de octetos como se indica en la figura 1.10.

[4] Redes Globales de Información con *Internet* y *TCP/IP*, Douglas Comer Capítulo 5



PA = Physical Address
IA = Internet Address

Figura 1.10 Formato del mensaje *ARP*

Para nuestro caso el tipo de protocolo es *IP*, cuya longitud de dirección física es 4. Sin embargo se puede emplear cualquier clase de direcciones físicas de red y cualquier tipo de protocolo de direcciones.

Sender Physical Address PA, se genera en el emisor y es repetida en el mensaje de respuesta.

Sender Internet Address IA , se genera en el solicitante y es repetida en el mensaje de respuesta.

Target Physical Address PA, se genera en el mensaje de respuesta.

Target Internet Address IA, generado en el mensaje de solicitud, donde se indica la dirección *IP* del destino y se repite en el mensaje de respuesta.

Cuando se envía un mensaje de solicitud (operación) *ARP*, se incluye en la trama las direcciones física e *internet* del solicitante y la dirección *internet* del destino.

El *Host* destino reconoce su dirección *internet*, y envía una respuesta (operación) *ARP*, donde se incluye las direcciones físicas y de *internet*, tanto del solicitante, como del destino.

En la estación solicitante se actualizan las tablas *ARP*, formando un mapa de parejas de direcciones físicas con direcciones *internet IP* como se indica en el cuadro 1.2.

Dirección Física *PA*	Dirección *Internet* *IA*
00:01:DD:F3	126.0.5.7
E4:35:4B:22	126.0.5.6
4C:00:21:45	126.0.5.4

Cuadro 1.2 Tabla de direcciones físicas con las respectivas direcciones *IP*

Una vez terminado este proceso, el emisor puede enviar paquetes *IP* directamente hasta el *host* destino.

1.2.2 PROTOCOLO REVERSO DE ASOCIACIÓN DE DIRECCIONES (*RARP REVERSE ARP*)[5]

Este protocolo es empleado por estaciones sin disco, para obtener su dirección de red *IP* , desde un servidor de direcciones *RARP,* a partir de su dirección física de tarjeta de red.

El formato del mensaje *RARP*, es el mismo que el de *ARP*, solo que al tipo de trama se le identifica como 8035.

Por ejemplo en la figura 1.11, un *host* A sin disco, envía un mensaje *RARP* con su dirección física, a toda la red, pidiendo su dirección *IP*. Los servidores *RARP*, buscan las transformaciones en las tablas de direcciones, y le responden con una dirección *IP* asignada, la misma que es guardada en la memoria de la estación A.

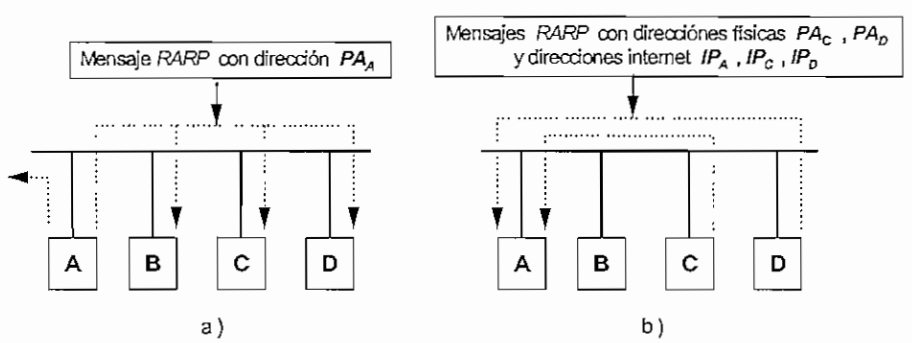


Figura 1.11 Proceso *RARP* a) Pregunta b) Respuesta

Una vez terminado este proceso *RARP*, la comunicación queda establecida , y la estación sin disco puede traer una copia del sistema operativo desde el servidor, hasta su memoria. Este proceso sólo se lo realiza en la inicialización de la estación.

[5] Redes Globales de Información con *Internet* y *TCP/IP*, Douglas Comer Capítulo 6

1.2.3 PROTOCOLO *INTERNET* DE MENSAJES DE CONTROL *(ICMP)*[6]

El protocolo de mensajes de control *internet*, permite que ruteadores y estaciones, envíen mensajes de error o de control hacia otros ruteadores o estaciones.

El mensaje *ICMP* es encapsulado en el datagrama *IP* para ser ruteado a varias redes, el cual a su vez, se encapsula en una trama para su transmisión, como se indica en la figura 1.12.

El campo del protocolo del datagrama *IP* que se describió en el capítulo 3 tiene el valor 1 que es asignado para los mensajes *ICMP*.

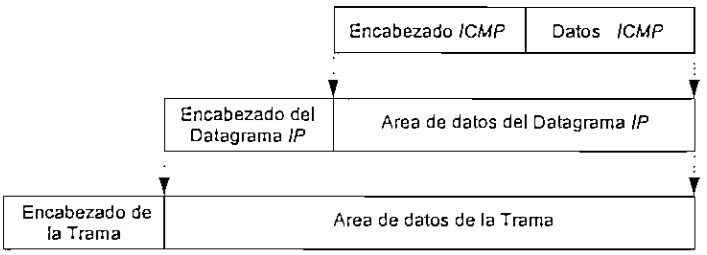


Figura 1.12 Encapsulado *ICMP*

El formato del mensaje *ICMP* es el siguiente:

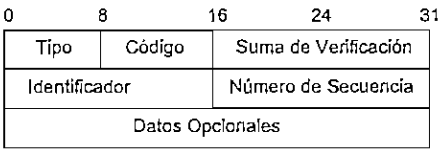


Figura 1.13 Formato del mensaje *ICMP*

Tipo de mensaje	Descripción
0	Respuesta de eco
3	Destino inaccesible
4	Disminución de origen
5	Redireccionar (cambiar una ruta)
8	Solicitud de eco
11	Tiempo excedido para un datagrama
12	Problema de parámetros en un datagrama
13	Solicitud de Time Stamp
14	Respuesta de Time Stamp
15	Solicitud de información
16	Respuesta de información
17	Solicitud de máscara de dirección
18	Respuesta de máscara de dirección

Cuadro 1.3 Tipos de Mensajes *ICMP*

[6] Redes Globales de Información con Internet Y TCP/IP, Douglas Comer Capítulo 9

1.2.3.1 PROTOCOLO INTERNET DE PRUEBA *PING* (*PROTOCOL INTERNET GROPER*)

Este protocolo es empleado para probar la accesibilidad y estado de un destino, empleando los mensajes *ICMP* de solicitud (8) y respuesta (0) de eco.

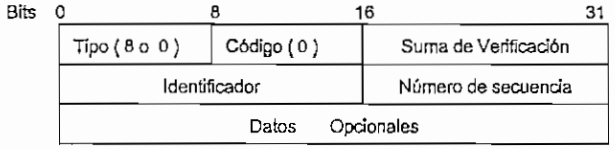


Figura 1.14 Formato del mensaje *ICMP PING*

El campo de datos opcionales, contiene datos que regresarán al transmisor, desde el destino.

1.2.3.2 DESTINOS NO ALCANZABLES

Cuando un datagrama no alcanza el destino, *IP* retorna un mensaje de, **red no accesible**, a la fuente original, utilizando el formato que se muestra a continuación.

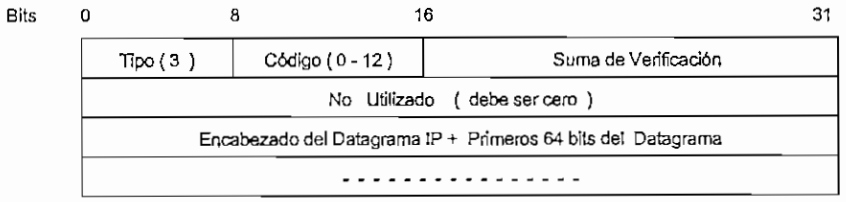


Figura 1.15 Formato del mensaje *ICMP* DESTINO INALCANZABLE

El campo código de un mensaje de destino no accesible, describe en detalle el problema.

Código	Descripción
0	Red inaccesible
1	Anfitrión inaccesible
2	Protocolo inaccesible
3	Puerto inaccesible
4	Se necesita fragmentación y configuración OF
5	Falla en la ruta de origen
6	Red de destino desconocida
7	Anfitrión de destino desconocido
8	Anfitrión de origen aislado
9	Comunicación con la red de destino - administrativamente prohibida
10	Comunicación con el anfitrión de destino - administrativamente prohibida
11	Red inaccesible por el tipo de servicio
12	Anfitrión inaccesible por el tipo de servicio

Cuadro1.4 Tipos de mensaje *ICMP* DESTINOS INALCANZABLES

1.2.3.3 DISMINUCIÓN DE LA TASA AL ORIGEN

Cuando el flujo de datagramas excede a la capacidad de proceso, *IP* descarta datagramas y envía un mensaje hacia la fuente, pidiendo que reduzca la velocidad de transmisión, por cada datagrama descartado.

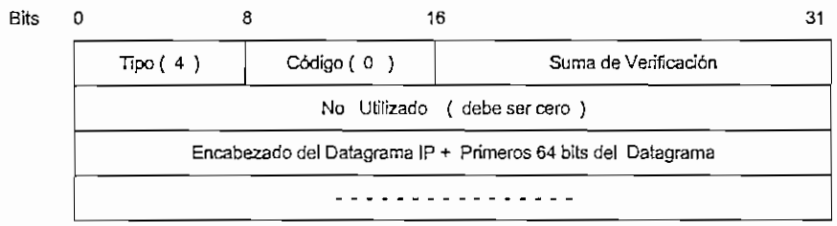


Figura 1.16 Formato del mensaje *ICMP* DISMINUCION DE LA TASA AL ORIGEN

1.2.3.4 SOLICITUD DE CAMBIO DE RUTA DESDE LOS RUTEADORES

Cuando un ruteador detecta una ruta más óptima que la sugerida por el *host*, le envía un mensaje, pidiéndole que cambie su ruta a la más conveniente.

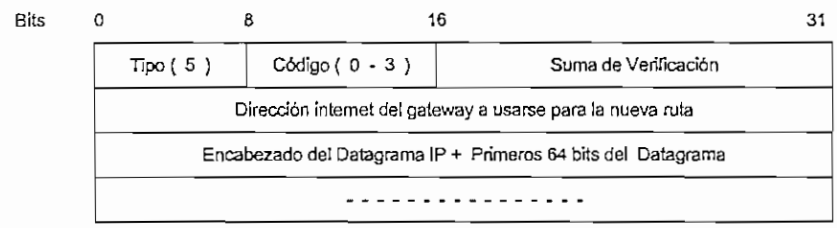


Figura 1.17 Formato de mensaje *ICMP* SOLICITUD DE CAMBIO DE RUTA

El código especifica la dirección de destino.

Código	Significado
0	Redireccionar datagramas para la red
1	Redireccionar datagramas para el anfitrión
2	Redireccionar datagramas para el tipo de servicio
3	Redireccionar datagramas para el tipo de servicio y el anfitrión

Cuadro 1.5 Tipos de mensaje *ICMP* de SOLICITUD DE CAMBIO DE RUTA

1.2.3.5 DETECCIÓN DE LAZOS Y RUTAS LARGAS

Es un mensaje que el ruteador envía al *host* origen, cuando éste descarta un datagrama, porque el tiempo de vida (*TTL*) en el encabezado del datagrama llega a cero, o cuando el temporizador de reensamblado expira mientras éste espera fragmentos.

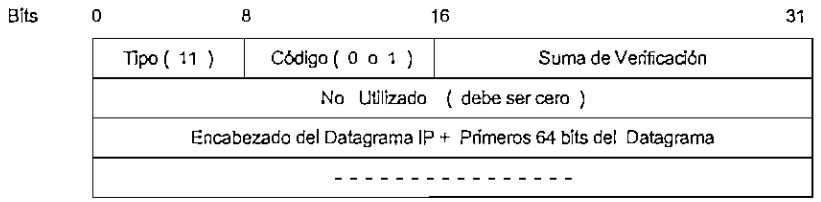


Figura 1.18 Formato de mensaje *ICMP* LAZOS Y RUTAS LARGAS

El código indica la razón por la cual terminó el tiempo.

Código	Significado
0	Conteo de tiempo de vida excedido
1	Tiempo para el reensamblado de fragmentos, excedido

Cuadro 1.6 Tipo de mensaje *ICMP* LAZOS o RUTAS LARGAS

1.2.3.6 SINCRONIZACIÓN DE RELOJES

Se utiliza para el cálculo del tiempo de retardo y sincronización de relojes entre estaciones, para lo cual se envía y recibe los tiempos de las estaciones.

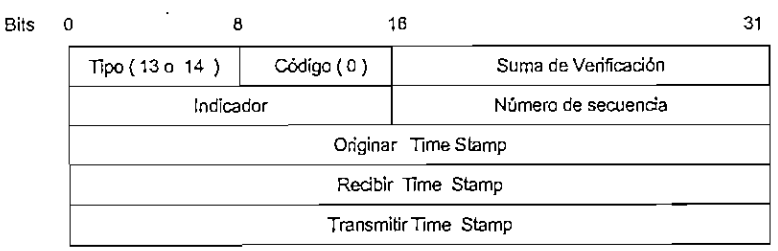


Figura 1.19 Formato de mensaje ICMP de SINCRONISMO DE RELOJES

Tipo	Significado
13	Solicitud
14	Respuesta

Cuadro 1.7 Tipo de mensaje *ICMP* para SINCRONISMO DE RELOJES

1.2.4 PROTOCOLO TRIVIAL DE TRANSFERENCIA DE ARCHIVOS *TFTP*

TFTP Trivial File Transfer Protocol

Es un protocolo sencillo que a menudo es utilizado con *RARP* en estaciones sin disco, en donde TFTP se encodifica en la ROM de la tarjeta de red para obtener una imagen del sistema operativo inicial cuando la máquina es inicializada. Se usa en aplicaciones que no requieren interacciones complejas entre cliente y servidor.

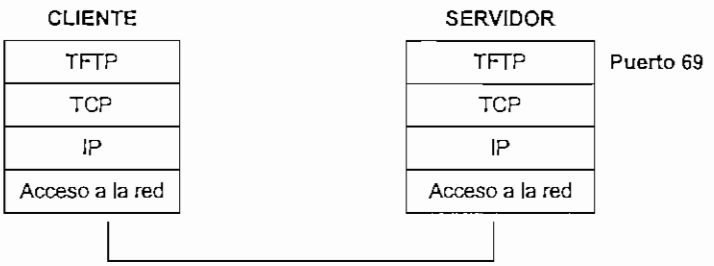


Figura 1.20 Proceso *TFTP* en el modelo *Internet* [7]

El primer paquete enviado solicita una transferencia de archivo y establece la interacción entre el cliente y el servidor. Se especifica el nombre del archivo que se va a transferir al cliente o al servidor.

1.2.5 PROTOCOLO *BOOTP* (*BOOTSTRAP PROTOCOL.*) [8]

Es un protocolo usado por estaciones sin disco, que permite determinar la dirección *IP y* luego utiliza *TFTP* para transferir el sistema operativo desde un servidor.

Al igual que *TFTP, BOOTP* utiliza interacciones cliente - servidor, para lo cual el protocolo se encuentra residente en una *ROM* para el arranque. *Bootp* se ejecuta sobre *UDP* e *IP* , para ser capaz de atravesar redes físicas.

El formato del mensaje es más complejo que *RARP* y tiene campos para información adicional como *gateways* , servidores de direcciones *IP* y máscaras de red , usadas para la comunicación entre redes .

---

[7] TCP/IP Technical Concepts, Open Strategies,Inc. and NCR , Capítulo 5, Pág.5
[8] TCP/IP Technical Concepts, Open Strategies,Inc. and NCR , Capítulo 5, Pág.5-6

1.2.6 INTERFACES TELNET

Telnet puede utilizar tres interfaces:

- *Telnet* a usuario
- *Telnet* a procesos de *host*
- *Telnet* a *TCP*

a) Interfaz Telnet a Usuario

Este interfaz tiene las siguientes características :

- Funciona en modo local y remoto. En modo local el interfaz permite invocar comandos locales antes de que se establezca la conexión al sistema remoto.

  Cuando la conexión al sistema remoto se establece, el usuario está en modo remoto.

- Tiene comandos locales para solicitar conexiones al servidor remoto, configurar las características de la terminal local y configurar parámetros del comando *TELNET*.

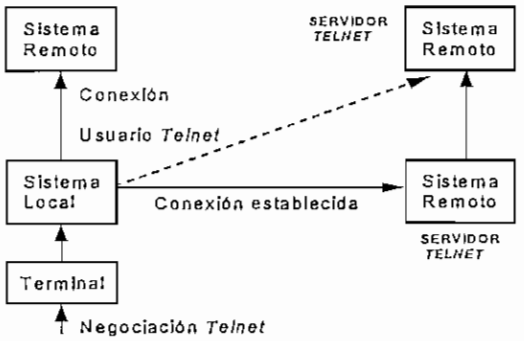


Figura 1.21 Conexión *Telnet* a sistemas locales y remotos

Cuando la conexión al servidor remoto se establece, todos los datos ingresados por el usuario se envían al servidor de *Telnet*. El mismo cliente puede abrir otra sesión *Telnet* con otro sistema remoto a través del servidor inicial.

b) Interfaz *Telnet* a procesos de *host*

Este interfaz realiza el control del terminal y provee de señales especiales para la transferencia de datos entre los procesos del usuario y del servidor a través de las conexiones establecidas por

Telnet. El interfaz permite la transmisión de datos y señales de control entre los procesos específicos y *Telnet*, como se muestra en la figura 1.22.

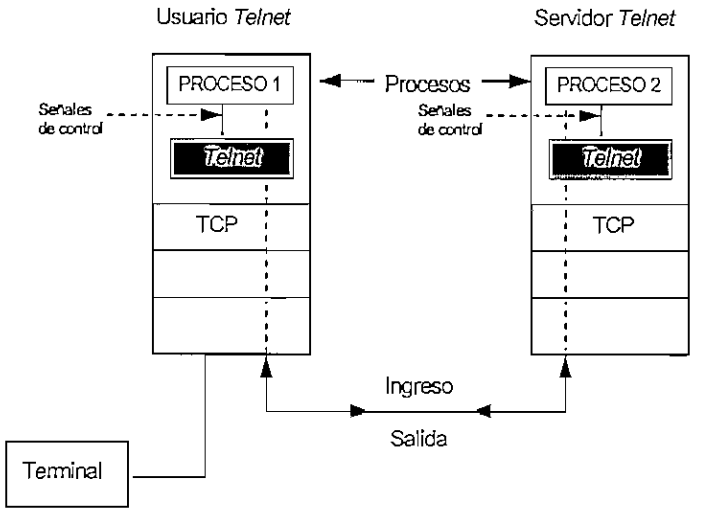


Figura 1.22 Interfaz *Telnet* a Procesos de Usuario y Servidor

c) Interfaz *Telnet* a *TCP*

Telnet reside en la capa de procesos del modelo *DoD* y utiliza el puerto 23. El servidor tiene un proceso "corriendo" el cual detecta una petición en el puerto 23. Una vez que la conexión se establece, *TCP* envía comandos y datos entre el usuario y el servidor *Telnet*.

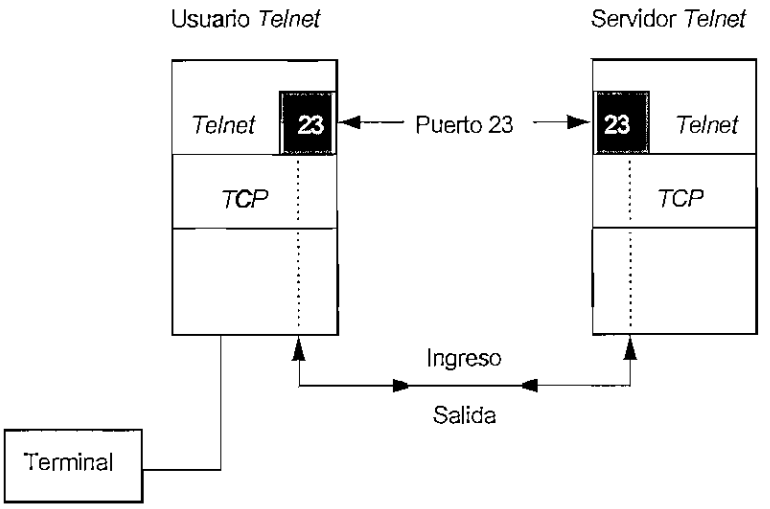


Figura 1.23 Conexión *Telnet* a través de *TCP*

ANEXO 2

2.1 REDES ATM [9]

La estructuración de la red ATM se muestra a continuación en la figura 2.1.

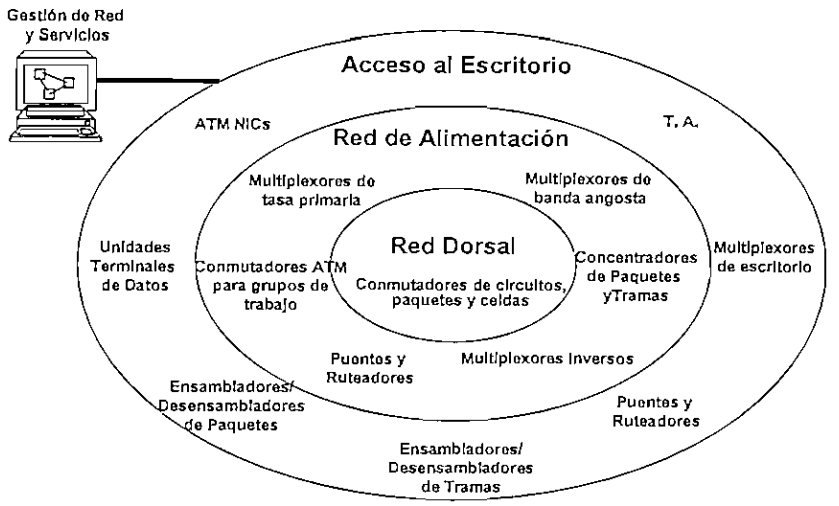


Figura 2.1 Estructuración de la red *ATM*

La unidad de transmisión en esta red es la **celda *ATM*** , que consta de 5 octetos de cabecera y 48 octetos de datos útiles .

Los conmutadores *ATM* analizan la información de la cabecera para conmutar la celda hasta su destino a través de otros conmutadores.

	Cabecera	Datos útiles
Longitud en octetos	5	48

Figura 2.2 Formato de la Celda ATM

ATM realiza la multiplexación de las celdas en forma *on demand* con la identificación de la fuente de transmisión contenida en la cabecera de cada celda . *On demand* significa que una estación puede enviar celdas con identificación siempre que sea necesario, sin necesidad de que tenga un tiempo preasignado para la transmisión.

[9] Internetworking Technology Overview, Cisco Systems Capitulo 15

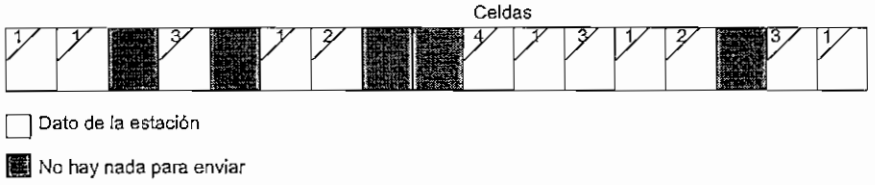


Figura 2.3 Transmisión de celdas *ATM*

2.1 FORMATO DE LA CABECERA *ATM*

Hay dos tipos de cabeceras que son:

- Cabecera *UNI* (Interfaz de Usuario a Red) que define la comunicación entre las estaciones *ATM* finales (estaciones y ruteadores) y los conmutadores *ATM.*
- Cabecera *NNI* (Interfaz de Red a Red) que define la comunicación entre conmutadores *ATM.*

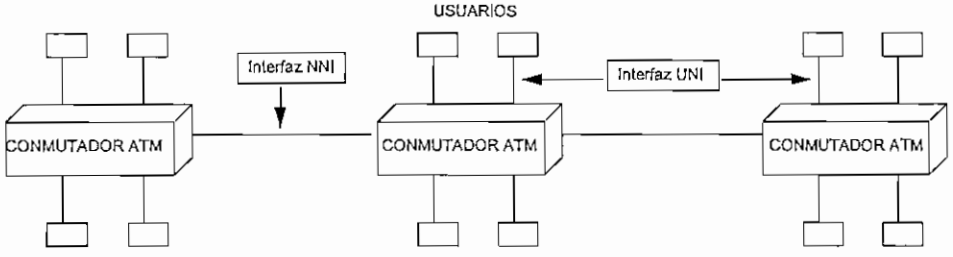


Figura 2.4 Interconexión de Conmutadores y Usuarios *ATM*

El formato de la cabecera ***UNI*** es el siguiente :

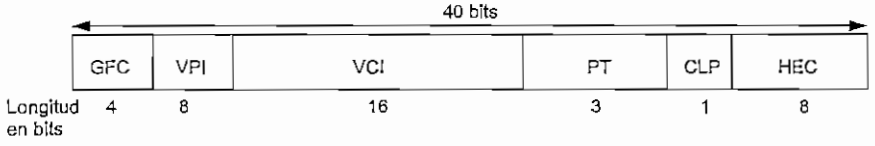


Figura 2.5 Cabecera *UNI*

. ***GFC*** Control de Flujo Genérico que identifica múltiples estaciones que comparten un simple interfaz *ATM.*

. ***VPI*** Identificación de Camino o ruta Virtual, el cual es usado junto con *VCI*, para identificar el siguiente destino de la celda a través de los conmutadores.

. ***VCI*** Identificación del Canal Virtual, el cual es usado junto con *VPI,* para identificar el siguiente destino de la celda a través de los conmutadores.

. ***PT*** Tipo de Dato, que identifica si la celda contiene datos de usuario o de control.

. ***CLP*** Prioridad de Pérdida por Congestión, que indica si la celda debe descartarse por congestión en la red.

. ***HEC*** Control de Error de Cabecera, que realiza una suma de verificación de la cabecera .

La cabecera ***NNI*** tiene el siguiente formato:

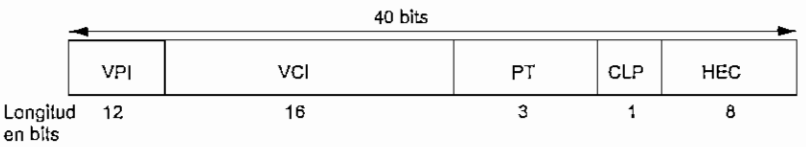


Figura 2.6 Cabecera *NNI*

Esta cabecera no tiene el campo *GFC*, pero el *VPI* es mayor, lo que permite asignar valores *VPI* mayores.

2.2 MODELO DE REFERENCIA *ATM*

La arquitectura de capas *ATM* se muestra en la figura 2.7:

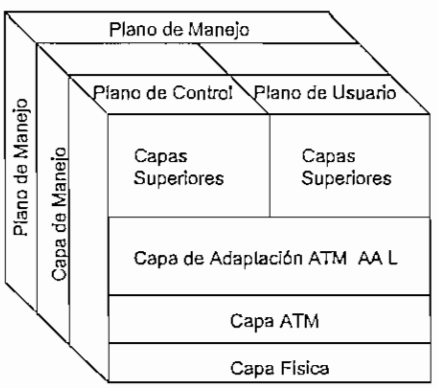


Figura 2.7 Modelo de referencia *ATM*

La capa *ATM* y la capa de Adaptación *ATM* son análogas a la capa de enlace en el modelo *OSI*.

2.2.1 Capa Física

La capa física se encarga de:

- La sincronización de la transmisión y la recepción del flujo de bits
- La generación y verificación de la Secuencia de Control de error de la Cabecera.
- Inserción o supresión de celdas para adaptarse a la tasa de transmisión.

2.2.2 Capa *ATM*

La capa *ATM* establece las conexiones y pasa las celdas a través de las redes, empleando la información de la cabecera de cada celda.

2.2.3 Capa de Adaptación *ATM AAL*

Esta capa recibe paquetes de los protocolos de las capas superiores *(IP, IPX)* y los divide en segmentos de 48 bytes que forman el campo de datos de la celda *ATM.*

Se incluye el número de secuencia de celda para que la capa de adaptación remota chequee si la celda se recibió en el orden correcto.

En el receptor se extrae la cabecera y los datos son reensamblados en el paquete original, para luego ser pasado a las capas superiores.

2.3 CONMUTACION *ATM*

Los conmutadores identifican el siguiente segmento de red por el que debe pasar la celda para ser enviado hasta su destino.

El conmutador *ATM* recibe la celda en un puerto y la conmuta hacia el puerto de salida correcto, basándose en los valores del Identificador de Camino o Ruta Virtual *VPI* y del Identificador del Canal Virtual de la cabecera de la celda.

El **canal virtual** es equivalente a un circuito virtual, es decir, es una conexión lógica entre dos puntos de comunicación.

El **camino o ruta virtual** es un grupo lógico de circuitos virtuales sobre los cuales se realizan operaciones comunes.

La conmutación de las celdas se realiza mediante una tabla que **mapea** los puertos de entrada hacia los puertos de salida para establecer una conexión virtual, en base a los valores de los campos *VPI* y *VCI* de la celda, como se muestra en la figura 2.8:

ENTRADA			SALIDA		
PUERTO	VPI	VCI	PUERTO	VPI	VCI
1	1	8	2	4	5
2	4	5	1	1	8
1	6	4	3	2	9
3	2	9	1	6	4

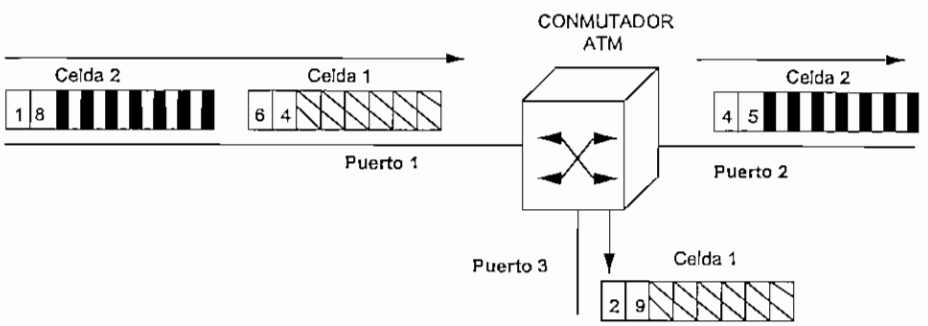


Figura 2.8 Ejemplo de Conmutación de celdas *ATM*

- Las dos celdas (1, y 2) arriban al puerto 1 del Conmutador *ATM*.
- El conmutador examina los campos *VPI* y *VCI* de la **celda 1** y determina sus valores
- El conmutador examina la tabla de mapeo, para determinar a cuál puerto debe enviar la celda. Encuentra que cuando recibe una celda en el puerto 1 con un *VPI* =6 y un *VCI* =4 , debe enviar la celda al puerto 3 con un valor *VPI* =2 y un *VCI* =9. De esta manera el conmutador cambia el *VPI* a 2 y el *VCI* a 9, y envía la celda hacia el puerto 3.
- Luego el conmutador examina la **celda 2** , la cual tiene un *VPI* de 1 y un *VCI* de 8. La tabla de conmutación indica que cuando recibe una celda en el puerto1 con *VPI* =1 y *VCI* =8 se debe dirigir al puerto 2 y los valores de *VPI* y *VCI* deben ser cambiados a 4 y 5 respectivamente.
- Si el conmutador recibe una celda en el puerto 3 con un *VPI* de 2 y un *VCI* de 9 , la tabla indica que la celda debe ir al puerto 1 con *VPI* y *VCI* de 6 y 4 respectivamente. Si la celda es recibida

en el puerto 2 con *VPI* y *VCI* de 4 y 5 respectivamente, la tabla conmuta la celda al puerto 1 y cambia los valores *VPI* y *VCI* a 1 y 8 respectivamente.

- Los valores *VPI* y *VCI* tienen significado sólo en el interfaz local.

Cuando la Identificación de Caminos o Rutas Virtuales *VPI* se emplea con un **grupo lógico** de canales virtuales, la *performance* de la conmutación se incrementa, por cuanto se reduce el número de campos a ser cambiados. Su funcionamiento se muestra en la figura 2.9:

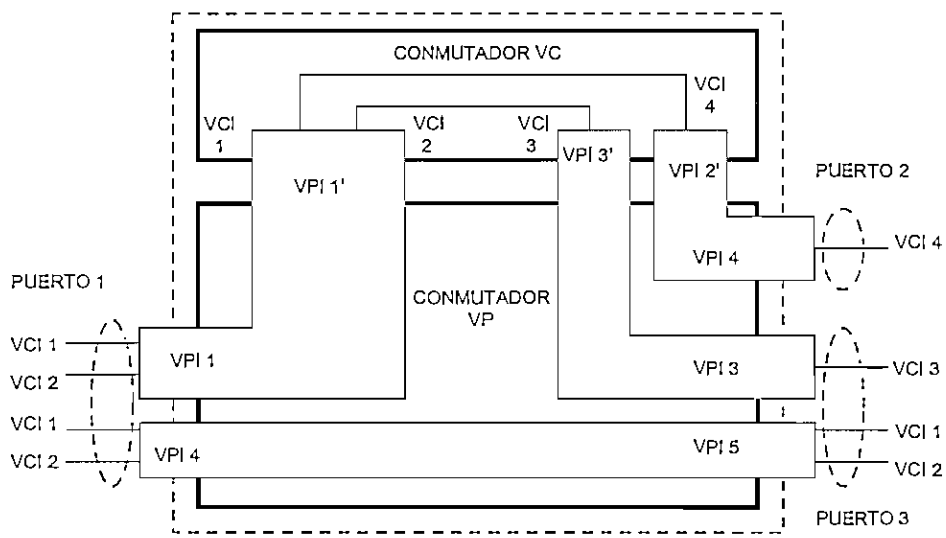


Figura 2.9 Conmutador *VP* y *VC*

- Las celdas que ingresan al puerto 1 que tienen un *VPI* de 4 son procesadas por el **Conmutador** *VP* el cual cambia el valor del *VPI* de la celda a 5, pero mantiene sin modificación los valores de *VCI,* y envía las celdas al puerto 3.
- Las celdas que tienen un *VPI* =1 son procesados por el **Conmutador** *VC* . A las celdas que tienen un *VCI* =1 , el conmutador *VC* cambia el *VPI* a 4 y el *VCI* a 4 y envía la celda al puerto 2. A las celdas que tienen un *VCI* =2 , el conmutador *VC* cambia el *VPI* a 3 y el *VCI* a 3 y dirige la celda al puerto 3. Es decir se puede multiplexar circuitos virtuales a través de una sola ruta en forma eficiente , con lo cual se reduce el costo de la transmisión por cuanto el alquiler de cada ruta es caro y depende de la cantidad de información que se envía por éste.

ANEXO 3

PROCEDIMIENTO PARA DETERMINAR NUMERO DE PROCESADORES, ESPACIO EN DISCO Y MEMORIA EN UN SERVIDOR DE RED

3.1 NUMERO DE PROCESADORES

Para determinar el número de procesadores, se deben realizar los siguientes pasos:

a) Calcular la carga equivalente del sistema.

b) Estimar la intensidad del *CPU* de las aplicaciones que se están ejecutando en el sistema.

c) Determinar el número óptimo de procesadores basados en los resultados de los pasos a y b.

a) Cálculo de la Carga Promedio

Para calcular la carga promedio se realizan los siguientes pasos:

1. Separar los usuarios por frecuencia de uso.
   - OCASIONAL: hasta 1.5 horas por día
   - PROMEDIO: hasta 3 horas por día
   - ALTO: sobre las 3 horas por día
2. Separar los usuarios por el tipo de sistema : multiusuario o cliente/servidor.
3. Calcular la carga equivalente utilizando la siguiente tabla:

	Multi-usuario	Cliente/Servidor	Total
# de usuarios *Ocasionales*	(_____ * 1) +	(_____ * 0.5) =	
# de usuarios *Promedio*	(_____ * 2) +	(_____ * 1) =	
# de usuarios *Alto*	(_____ * 3) +	(_____ * 1.5) =	
		TOTAL	
Dividir el **Total** por 3 y se obtiene la **Carga Equivalente**	——— /	3 =	

Cuadro 3.1 Cálculo de la Carga Promedio

b) Estimación de la intensidad del *CPU*

Para estimar la intensidad del *CPU*, se consideran el tipo de aplicaciones y el número de usuarios que usan dichas aplicaciones con cada nivel de intensidad.

- Para determinar la intensidad del *CPU* con las aplicaciones: se puede considerar el cuadro 3.2.

Tipo de Aplicación	Intensidad del CPU estimada	
	Multi-usuario	Cliente/Servidor
Contabilidad	MODERADA	BAJA
Desarrollo de Programas (Lenguajes Compilados)	MODERADA	BAJA
Desarrollo de Programas (Lenguajes Intérpretes)	ALTA	MODERADA
Hoja de cálculo	ALTA	MODERADA
Procesadores de palabras	MODERADA	BAJA
Base de Datos	ALTA	MODERADA
X Windows	ALTA	ALTA

Cuadro 3.2 Estimación de la Intensidad del CPU

- La siguiente tabla que provee la fórmula para determinar la intensidad del *CPU*.

Clasificación de Usuarios		Usuarios totales				Total
# de usuarios que usan aplicaciones de intensidad BAJA	.	# total de usuarios	*	1	=	
# de usuarios que usan aplicaciones de intensidad MODERADA	.	# total de usuarios	*	2	=	
# de usuarios que usan aplicaciones de intensidad ALTA	.	# total de usuarios	*	3	=	
			TOTAL			
Si TOTAL es una fracción, se debe redondearlo al valor más alto si la fracción es .5 o superior, y se debe truncarlo si la fracción es inferior a .5. El resultado de la intensidad de CPU del sistema es: 1=BAJA; 2=MODERADA; 3=ALTA						

Cuadro 3.3 Intensidad del CPU con el Sistema

c) Determinación del Número de Procesadores

Con los datos de la intensidad del *CPU* del sistema (filas) y la carga equivalente estimada, se lee el identificador de la columna para determinar el número de procesadores.

	Número de procesadores			
Intensidad del *CPU* del sistema	1	2	3	4
BAJA	Carga de 1-128	Carga de 129-256	Carga de 257-384	Carga de 385-512
MODERADA	Carga de 1-96	Carga de 97-192	Carga de 193-288	Carga de 289-384
ALTA	Carga de 1-64	Carga de 65-128	Carga de 129-192	Carga de 193-256

Cuadro 3.4 Número de Procesadores

3.2 CANTIDAD DE MEMORIA

Para determinar la cantidad de memoria requerida, se debe realizar los siguientes pasos:

a) Estimar el número de usuarios a tiempo completo en el sistema (carga equivalente)

b) Estimar el uso de memoria para aplicaciones y para el sistema.

c) Identificar aplicaciones mixtas que corren en el sistema.

d) Determinar la cantidad óptima de memoria, basados en el resultado de los pasos a, b y c.

a) Estimación del uso de Memoria

El uso de memoria depende del tipo de aplicación y el número de usuarios de la aplicación.

- Para estimar el uso de memoria de una aplicación se deben usar las siguientes guías:

  BAJA: usa menos de 1 MB de memoria

  MODERADA: usa 1-2 MB de memoria

  ALTA: usa más de 2 MB de memoria

  Si el uso de memoria no es conocido se puede estimar usando la siguiente tabla.

Tipo de Aplicación	Uso de memoria estimada	
	Multi-usuario	Cliente/Servidor
Contabilidad	MODERADA	BAJA
Desarrollo de Programas (Lenguajes Compilados)	BAJA	BAJA
Desarrollo de Programas (Lenguajes Intérpretes)	MODERADA	BAJA
Hoja de cálculo	BAJA	BAJA
Procesadores de palabras	MODERADA	BAJA
Base de Datos	ALTA	ALTA
X Windows	MODERADA	BAJA

Cuadro 3.5 Estimación del uso de memoria

- El uso de memoria por el sistema está determinado por la relación del número de usuarios en cada uno de los niveles, como se indica en el cuadro 3.6:

Clasificación de Usuarios		Usuarios totales				Total
# de usuarios que usan aplicaciones de memoria BAJA	,	# total de usuarios)	*	1	=	
# de usuarios que usan aplicaciones de memoria MODERADA	,	# total de usuarios)	*	2	=	
# de usuarios que usan aplicaciones de memoria ALTA	,	# total de usuarios)	*	3	=	
			TOTAL			
Si **TOTAL** es una fracción, se debe redondearlo al valor más alto si la fracción es .5 o superior, y se debe truncarlo si la fracción es inferior a .5. El resultado de la intensidad de *CPU* del sistema es: 1=BAJA; 2=MODERADA; 3=ALTA						

Cuadro 3.6 Determinación de memoria por usuarios

b) Determinación de aplicaciones mixtas

La aplicación mixta está determinada por la relación del número de usuarios para el total de número de aplicaciones diferentes utilizadas.

3.3 REQUERIMIENTOS DE DISCO

Para determinar los requerimientos de disco duro, se deben realizar los siguientes pasos:

a) Estimar los requerimientos de espacio en disco para usuarios

b) Estimar los requerimientos de espacio en disco para el sistema

c) Estimar los requerimientos de espacio en disco para aplicaciones.

d) Determinar el total de espacio de disco basados en los resultados de los pasos a, b y c.

a) Estimación de los requerimientos de espacio en disco para usuarios.

Si se conoce los requerimientos de espacio en disco, se usa la siguiente estimación:

- BAJA: uso hasta 10 MB de espacio en disco
- MODERADA: usa hasta 20 MB de espacio en disco
- ALTA: usa hasta 40 MB de espacio en disco

El cuadro 3.7 lista las fórmulas de cálculo del espacio en disco.

Usuarios		Espacio x usuarios		Total
# de usuarios con uso de disco BAJA	*	10 MB	=	
# de usuarios con uso de disco MODERADA	*	20 MB	=	
# de usuarios con uso de disco ALTA	*	40 MB	=	
		TOTAL		

Cuadro 3.7 Estimación de espacio en disco en función de los usuarios

b) Estimación de los requerimientos de espacio de disco del sistema.

Los requerimientos de espacio de disco del sistema deben incluir lo siguiente:

- El sistema operativo: Para ambiente Cliente/Servidor el espacio de disco requerido es aproximadamente 200 MB.
- El área de *Swap,* es el espacio de disco usado por el sistema operativo para simular memoria virtual, el cual se utiliza cuando la memoria RAM principal se agota. El tamaño va de 32 hasta 512 MB un solo disco. La cantidad total de espacio de *swap* necesario depende del sistema y del uso de la aplicación. El requerimiento mínimo de *swap* es dos veces la memoria para tamaños de *RAM* de 128 MB - 512 MB. Para tamaños mayor es que 512 MB, el espacio adicional de *swap* deber ser ubicado en un disco que no sea el *root.*

- Espacio de *dump*, es el espacio de disco que sirve para crear una imagen de la memoria principal, el cual se utiliza para recuperar datos cuando una falla catastrófica ocurre en el equipo y por tanto debe ser igual al tamaño de la memoria.

APLICACION	ESPACIO
Sistema Operativo	200 MB
Swap	32 - 512 en un sólo disco
Dump	igual al tamaño de la memoria
Stand	20 MB
Total	

Cuadro 3.8 Estimación de espacio en el disco de sistema

c) Estimación del espacio de disco para las aplicaciones:

Las aplicaciones a utilizarse son las siguientes:

APLICACION	ESPACIO
CONTABLES BANCARIAS	200 MB
SISTEMA DE BASE DE DATOS	300 MB
Total	**500 MB**

Cuadro 3.9 Estimación de espacio en disco para las aplicaciones

d) Determinación de la configuración de disco:

Para determinar el total de espacio de disco requerido, se consideran los siguientes aspectos:

REQUERIMIENTO DE DISCO INTERNO	VALOR
Usuarios	
Sistema	
Aplicaciones	500 MB
Subtotal disco interno	
% de crecimiento	40%
Total disco interno	

Cuadro 3.10 Espacio Total de disco

Empleando los criterios anteriores se obtiene la configuración óptima del Servidor Central de Producción y abastecer los requerimientos del *Software* Bancario.

ANEXO 4

4.1 POSIBLE DISTRIBUCION DE EQUIPOS EN UN BANCO

Una posible distribución de equipos en el Banco es la que se muestra en el cuadro 4.1.

Las controladoras de red *LAN* y *WAN* en los servidores tienen su propia dirección *IP*.

EQUIPOS	AREA	GRUPO	NOMBRE	RED IP 130.000.x.y
RUTEADORES	Cómputo	Cómputo		
GATEWAYS	Cómputo	Cómputo		
SERVIDORES				
UNIX PRODUCCION	Cómputo	Cómputo	SERVER001	*LAN*: 130.000.001.001 *WAN*: 133.254.001.002
UNIX DESARROLLO	Cómputo	Cómputo	SERVER002	*LAN*: 130.000.001.002 *WAN*: 133.253.001.002
NT	Cómputo	Cómputo	SRVNT00XX	*LAN*: 130.000.001.003 *WAN*: 133.252.001.002
CAJEROS	Cómputo	Cómputo	SRVATM00XX	*LAN*: 130.000.001.004 *WAN*: 133.251.001.002
BANRED	Cómputo	Cómputo	SRBRED00XX	*LAN*: 130.000.001.005 *WAN*: 133.250.001.002
ACCESO REMOTO	Cómputo	Cómputo	SRVRAS00XX	*LAN*: 130.000.001.006 *WAN*: 133.249.001.002
AGENCIA MATRIZ	Agencia Matriz	Agencia	MATRIZ	*LAN*: 130.000.001.007 *WAN*: 133.248.001.002
IMPRESION	Computo	Computo	SRMAIL00XX	130.000.001.y
MAIL	Computo	Computo	SRVIMP00XX	130.000.001.y
ARCHIVOS	Computo	Computo	SRVARC00XX	130.000.001.y
IMAGENES	Computo	Computo	SRVIMG00XX	130.000.001.y
USUARIOS				
Servidor y usuarios	Sistemas - Sistemas - Desarrollo	Sistemas	- SISTEM00XX - DESAR00XX	130.000.002.y
	Operaciones	Operaciones	OPER00XX	130.000.003.y
	Departamento Técnico	Técnico	TECNIC00XX	130.000.004.y
	Contabilidad	Contabilidad	CONTA0XX	130.000.005.y
	Departamento Financiero	Financiero	DPTFIN000XX	130.000.006.y
	Departamento Administrativo: - Administración - Recursos Humanos	Administración	 - DPTADM00XX - RECHUM00XX	 130.000.007.y 130.000.008.y
	Gerencia	Gerencia	GEREN00XX	130.000.009.y
	Cuentas Corrientes y Ahorros	Cuentas	CUENTA00XX	130.000.010.y
	Inversiones y Negocios	Inversiones	INVER00XX	130.000.011.y
	Cambios	Cambios	CAMBIO00XX	130.000.012.y
	Crédito	Crédito	CREDIT00XX	130.000.013.y
	Cobranzas	Cobranzas	COBRAN00XX	130.000.014.y
	Cartera	Cartera	CARTER00XX	130.000.015.y
	Banca Personal y Corporativa	Banca	BANCA00XX	130.000.016.y
	Mercadeo	Mercadeo	MERCAD00XX	130.000.017.y
	Comercio Interior y Exterior	Comercio	COMERC00XX	130.000.018.y
	Mesa de Dinero	Mesa	MESA00XX	130.000.019.y
	Tesorería	Tesorería	TESOR00XX	130.000.020.y
	Leasing	Leasing	LEASIN00XX	130.000.021.y
	Proveduría	Proveduría	PROVER00XX	130.000.022.y
	Auditoría	Auditoría	AUDIT00XX	130.000.023.y
	Departamento Jurídico	Jurídico	JURID00XX	130.000.024.y
Servicio al Cliente	- Terminales Financieras	Agencia	FINAN00XX	130.000.025.y
	- Terminales Administrativas	Agencia	ADMIN00XX	130.000.025.y
	- Cajas	Agencia	CAJA00XX	130.000.025.y
	- Servicio al Cliente	Agencia	SRCLTE00XX	130.000.025.y

Cuadro 4.1 Distribución de equipos en la matriz del Banco

4.2 ASIGNACION DE DIRECCIONES *IP* A LOS SERVIDORES Y USUARIOS EN LA MATRIZ

Las direcciones para los servidores se las asigna a partir de 130.000.**001**.001, conservando el primer factor de ***host*** y vamos variando el segundo factor para el resto de servidores, como se muestra en el cuadro 4.2.

DIRECCIONES IP DE LOS SERVIDORES EN LA MATRIZ	
SERVIDOR	**DIRECCION IP**
UNIX PRODUCCION	*WAN* : 133.254.001.**002** *LAN* : 130.000.001.**001**
UNIX DESARROLLO	*WAN* : 133.253.001.**002** *LAN* : 130.000.001.**002**
NT	*WAN* : 133.252.001.**002** *LAN* : 130.000.001.**003**
CAJEROS	*WAN* : 133.251.001.**002** *LAN* : 130.000.001.**004**
BANRED	*WAN* : 133.250.001.**002** *LAN* : 130.000.001.**005**
ACCESO REMOTO	*WAN* : 133.249.001.**002** *LAN* : 130.000.001.**006**
AGENCIA MATRIZ	*WAN* : 133.248.001.**002** *LAN* : 130.000.001.**007**
IMPRESION	130.000.001.**008**
MAIL	130.000.001.**009**
ARCHIVOS	130.000.001.**010**
IMAGENES	130.000.001.**011**

Cuadro 4.2 Direcciones IP de los servidores en la matriz

Para los departamentos se varía el primer factor de *host* para identificar al grupo. Para los usuarios se varía el segundo factor de *host* en cada departamento.

En los Servidores departamentales, el segundo factor de ***host*** tiene la dirección más baja , **001** , y el resto de usuarios se los coloca a partir de **011** en adelante.

Por ejemplo para el departamento de Sistemas , Contabilidad y Financiero se tienen las direcciones indicadas en los cuadros 4.3, 4.4.

Para el departamento de Contabilidad se varía el primer factor de *host* a 005 como se indica en el cuadro 4.3 con lo que queda la dirección 130.000.005.**yyy** donde yyy es el número de identificación de cada usuario.

Para los Servidores de departamento **yyy** tiene los valores más bajos y el resto de usuarios se los numera desde yyy=011

DIRECCIONES IP DE SISTEMAS		
EQUIPO	**DIRECCION IP**	*GATEWAY*
SERVIDORES		
Sistemas SRVSIS0001	130.000.**002**.001	130.000.001.001
Desarrollo SRVDES0001	130.000.**002**.002	130.000.001.001
.	.	
USUARIOS		
Sistemas		
SISTEM0001	130.000.**002**.011	130.000.001.001
SISTEM0002	130.000.**002**.012	130.000.001.001
.	.	"
SISTEM0XX	130.000.**002**.0XX	130.000.001.001
Desarrollo		
DESAR0001	130.000.**002**.101	130.000.001.001
DESAR0002	130.000.**002**.102	"
.	.	"
DESARnnn	130.000.**002**.nnn	"
Gateways adicionales para los equipos: - 130.000.001.002 - 130.000.001.003 - 130.000.001.004 - 130.000.001.005 - 130.000.254.254 puerto *ethernet* del ruteador maestro 1 - 130.000.254.253 puerto *ethernet* del ruteador maestro 2		

Cuadro 4.3 Direcciones IP en el departamento de Sistemas

DIRECCIONES IP DE CONTABILIDAD		
EQUIPO	**DIRECCION IP**	*GATEWAY*
SERVIDORES		
SRVCNT0001	130.000.**005**.001	130.000.001.001
SRVCNT0002	130.000.**005**.002	130.000.001.001
.	.	
USUARIOS		
CONTA0001	130.000.**005**.011	130.000.001.001
CONTA0002	130.000.**005**.012	"
.	.	"
CONTA00XX	130.000.**005**.0XX	130.000.001.001
Gateways adicionales para los equipos: - 130.000.001.002 - 130.000.001.003 - 130.000.001.004 - 130.000.001.005 - 130.000.254.254 puerto *ethernet* del ruteador maestro 1 - 130.000.254.253 puerto *ethernet* del ruteador maestro 2		

Cuadro 4.4 Direcciones IP de Contabilidad

Para el resto de departamentos se sigue un proceso similar.

Los Servidores *UNIX* deben tener una tabla de rutas para llegar a otras redes y para que los usuarios de otras redes puedan ingresar a su información.

- Esta tabla debe tener las direcciones *IP* de las redes existentes, la dirección *IP* del gateway a través del cual debemos pasar para llegar a la red destino, y el número de saltos requeridos para alcanzar el primer *gateway*.

- Las tablas de rutas del Servidor *UNIX* se generan empleando el siguiente comando:

route add net red *IP* destino máscara *gateway* local número de saltos

La distribución de los equipos es similar a la matriz como se muestra en el cuadro 4.5.

DISTRIBUCION DE EQUIPOS EN LA AGENCIA 1				
EQUIPOS	**AREA**	**GRUPO**	**NOMBRE**	**RED *IP*** **130.001.x.y**
RUTEADOR	Computo	Computo		
GATEWAYS	Computo	Computo		
SERVIDORES				
AGENCIA	Computo	Computo	SERAG001	*WAN* : 131.001.001.002 *LAN* : 130.001.001.001
IMPRESION	Computo	Computo	SRMAIL01XX	130.001.001.y
MAIL	Computo	Computo	SRVIMP01XX	130.001.001.y
ARCHIVOS	Computo	Computo	SRVARC01XX	130.001.001.y
BANRED	Computo	Computo	SRBRED01XX	130.001.001.y
ACCESO REMOTO	Computo	Computo	SRVRAS01XX	130.001.001.y
IMAGENES	Computo	Computo	SRVIMG01XX	130.001.001.y
USUARIOS				
	Operaciones	Operaciones	OPER01XX	130.001.003.y
	Departamento Técnico	Técnico	TECNIC01XX	130.001.004.y
	Contabilidad	Contabilidad	CONTA01XX	130.001.005.y
	Departamento Financiero	Financiero	DPTFIN01XX	130.001.006.y
	Departamento Administrativo: - Administración - Recursos Humanos	Administración	- DPTADM01XX - RECHUM01XX	130.001.007.y 130.001.008.y
	Gerencia	Gerencia	GEREN01XX	130.001.009.y
	Cuentas Corrientes y Ahorros	Cuentas	CUENTA01XX	130.001.010.y
	Inversiones y Negocios	Inversiones	INVER01XX	130.001.011.y
	Cambios	Cambios	CAMBIO01XX	130.001.012.y
	Crédito	Crédito	CREDIT01XX	130.001.013.y
	Cobranzas	Cobranzas	COBRAN01XX	130.001.014.y
	Cartera	Cartera	CARTER01XX	130.001.015.y
	Banca Personal y Corporativa	Banca	BANCA01XX	130.001.016.y
	Mercadeo	Mercadeo	MERCAD01XX	130.001.017.y
	Comercio Interior y Exterior	Comercio	COMERC01XX	130.001.018.y
	Mesa de Dinero	Mesa	MESA01XX	130.001.019.y
	Tesorería	Tesorería	TESOR01XX	130.001.020.y
	Leasing	Leasing	LEASIN01XX	130.001.021.y
	Proveduría	Proveduría	PROVER01XX	130.001.022.y
	Auditoría	Auditoría	AUDIT01XX	130.001.023.y
	Departamento Jurídico	Jurídico	JURID01XX	130.001.024.y
Servicio al Cliente	- Terminales Financieras	Agencia	FINAN01XX	130.001.025.y
	- Terminales Administrativas	Agencia	ADMIN01XX	130.001.025.y
	- Cajas	Agencia	CAJA01XX	130.001.025.y
	- Servicio al Cliente	Agencia	SRCLTE01XX	130.001.025.y

Cuadro 4.5 Distribución de equipos en la Agencia 1

Las direcciones *IP* de los servidores de la Agencia 1 son :

DIRECCIONES *IP* DE LOS SERVIDORES DE LA AGENCIA 1	
SERVIDOR	**DIRECCION *IP***
AGENCIA	*WAN* : 131.001.001.**002** *LAN* : 130.001.001.**101**
IMPRESION	130.001.001.**002**
MAIL	130.001.001.**003**
ARCHIVOS	130.001.001.**004**
CAJEROS	*WAN* : 130.001.001.**005** *LAN* : 130.001.001.**105**
BANRED	*WAN* : 130.001.001.**006** *LAN* : 130.001.001.**106**
ACCESO REMOTO	*WAN* : 130.001.001.**007** *LAN* : 130.001.001.**107**
IMAGENES	130.001.001.**008**

Cuadro 4.6 Direcciones IP de los servidores de agencia

Las direcciones *IP* de terminales y usuarios de la agencia 1 se indican en el cuadro 4.7:

DIRECCIONES *IP* DEL AREA DE ATENCION AL CLIENTE EN LA AGENCIA 1		
EQUIPO	**DIRECCION *IP***	*GATEWAY*
SERVIDORES		
SERAG01	*WAN* : 131.001.001.**002** *LAN* : 130.001.001.**101**	**131**.001.001.001
USUARIOS		
Terminal Financiera		
FINAN0101	130.001.**025**.011	**130**.001.001.001
FINAN0102	130.001.**025**.011	"
.	.	"
FINAN0150	130.001.**025**.050	"
Terminal Administrativa		
ADMIN0101	130.001.**025**.051	130.001.001.001
ADMIN0102	130.001.**025**.052	"
.	.	"
.	.	"
ADMIN0150	130.001.**025**.100	"
Servicio al Cliente		
SRCLTE0101	130.001.**025**.101	130.001.001.001
SRCLTE0102	130.001.**025**.102	"
.	.	"
.	.	"
SRCLTE0150	130.001.**025**.150	"
Cajas		
CAJA0101	130.001.**025**.151	130.001.001.001
CAJA0102	130.001.**025**.152	"
.	.	"
.	.	"
CAJA0150	130.001.**025**.200	"
Gateways adicionales para los equipos: - 130.001.254.254 puerto ethernet del ruteador de la Agencia 1		

Cuadro 4.7 Direcciones *IP* de terminales y usuarios

ANEXO 5

CONFIGURACION *TCP/IP* EN SERVIDORES Y USUARIOS

5.1 CONFIGURACION *TCP/IP* EN LOS SERVIDORES *UNIX*

En los servidores *UNIX* deben estar generadas todas las rutas anteriores, para que los usuarios locales y remotos puedan tener acceso a su información

- Las tablas de rutas del Servidor *UNIX* se generan empleando el siguiente comando:

  route add net red *IP* destino máscara *gateway* local número de saltos

- Las tablas de rutas formada en el servidor de *UNIX* de PRODUCCION y DESARROLLO se muestra en el siguiente cuadro:

TABLA DE RUTAS *IP* PARA LOS SERVIDORES *UNIX*			
DESTINO	MASCARA	*GATEWAY*	SALTOS
200.100.100	255.255.255.000	200.100.100.254	0
200.100.200	255.255.255.000	200.100.100.254	2
200.100.300	255.255.255.000	200.100.100.254	2
200.100.400	255.255.255.000	200.100.100.254	2
200.100.254	255.255.255.000	200.100.100.254	1
200.100.253	255.255.255.000	200.100.100.254	1
200.100.252	255.255.255.000	200.100.100.254	1

Cuadro 5.1 Tabla de enrutamiento *IP* en los servidores *UNIX*

La dirección 200.100.100.254 corresponde al puerto *ethernet* del ruteador QUITO 100 el cual está funcionando como *gateway* hacia las demás redes.

Todos lo servidores y usuarios deben tener configurado como dirección de *gateway* a la dirección del puerto *ethernet* del ruteador, tanto en la matriz como en las agencias.

5.2 CONFIGURACION *TCP/IP* EN SERVIDORES *NT*

Para configurar *TCP/IP* en *Windows NT* se siguen los siguientes pasos:

- Con el icono de Panel de Control , se escoge el icono de Red y aparece la pantalla que se muestra en la figura 5.1
- Aparecen los adaptadores de red *LAN* y *WAN* instalados e incluye un listado de protocolos de red instalados en *Windows NT* .

  Cuando el servidor no tiene instalado la tarjeta de *WAN* X25, aparece en el listado sólo la tarjeta ethernet.

- Se escoge una tarjeta de red y con la opción **Configurar** se establecen los parámetros de *hardware* .
- El protocolo *TCP/IP* ya viene instalado junto con *NT*, pero hay que seleccionarlo como protocolo de red, y con la opción **Configurar** se asignan las direcciones *IP* del *host* y del *gateway* , tanto para la tarjeta de red *LAN* como para la tarjeta de red *WAN*.

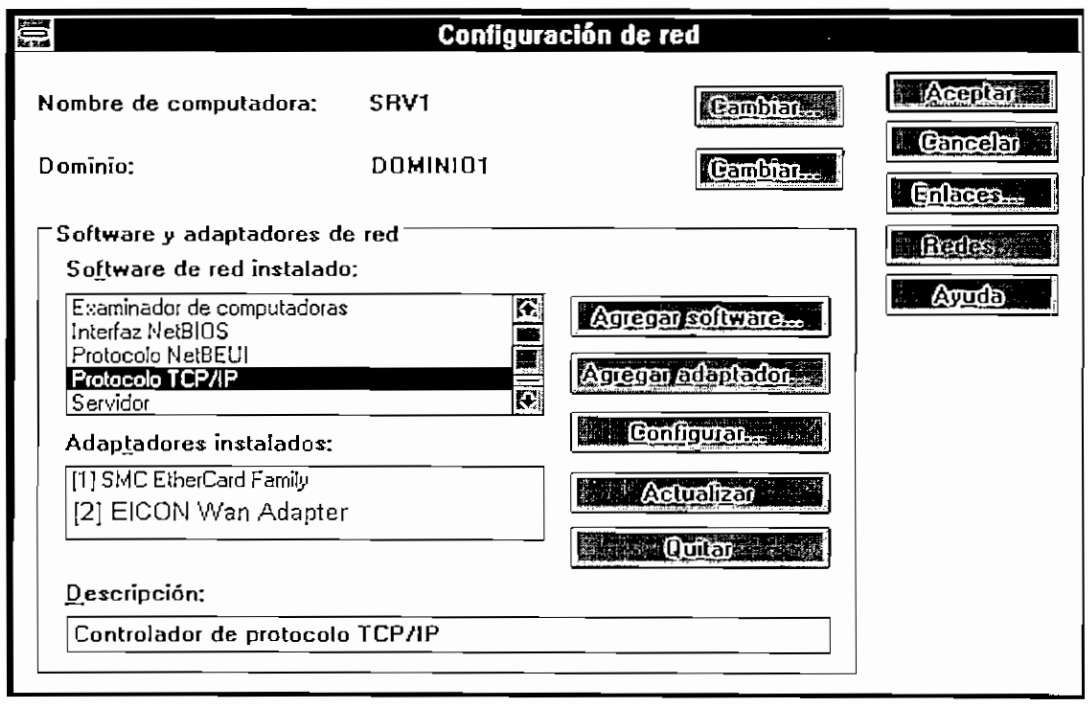


Figura 5.1 Configuración de red en Servidores *NT*

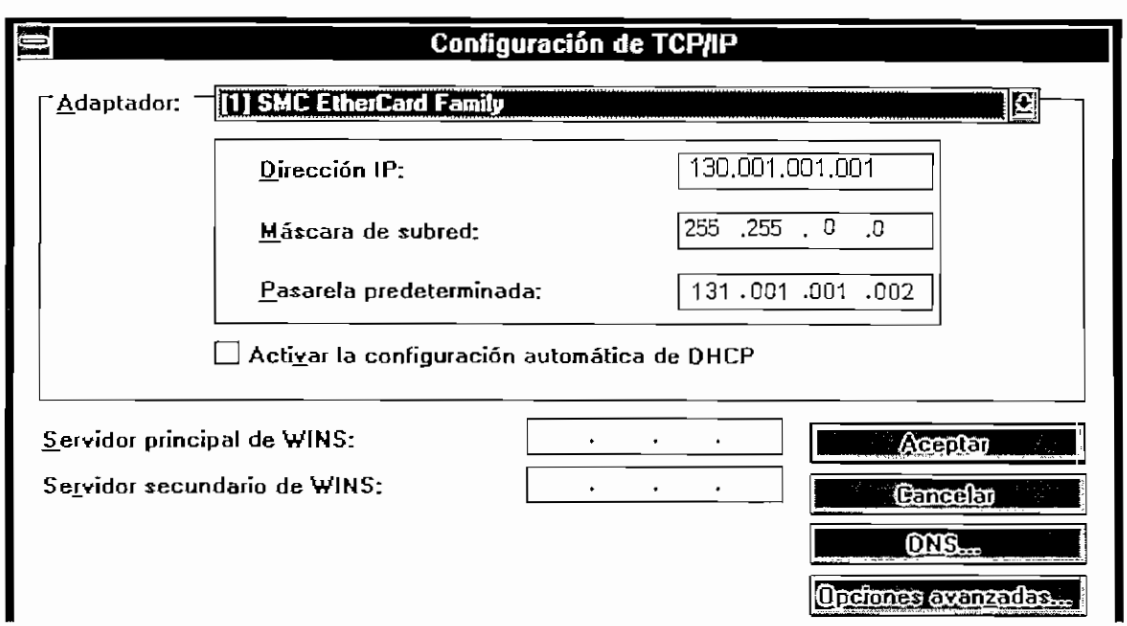


Figura 5.2 Configuración *TCP/IP* en Servidores *NT*

En este caso se ha escogido un servidor de agencia, donde la dirección de *gateway* para la tarjeta de red ethernet , tiene la dirección de la tarjeta de *WAN EICON* . Si no tiene la tarjeta *EICON* la dirección de *gateway* será la del puerto ethernet del ruteador.

- Si no se tiene tarjeta de red *ethernet*, se debe configurar Acceso Remoto por el puerto serial y poner como protocolo de red predeterminado al protocolo Punto a Punto. Con esto se puede enlazar al puerto serial de otro equipo que también tenga configurado su puerto serial como un puerto para enlace Punto Punto vía *RAS* (*Remote Access Services*).
- Para la tarjeta WAN, se selecciona la segunda tarjeta de red *EICON WAN Adapter* y con la opción Configurar se va al menú de configuración del adaptador.
- Con la opción de ***Port 1***, se escoge el protocolo de línea de bajo nivel, como por ejemplo:

  .X25 escogido para el enlace hasta el ruteador X25

  .SDLC

  .Frame Relay

  .Punto a Punto

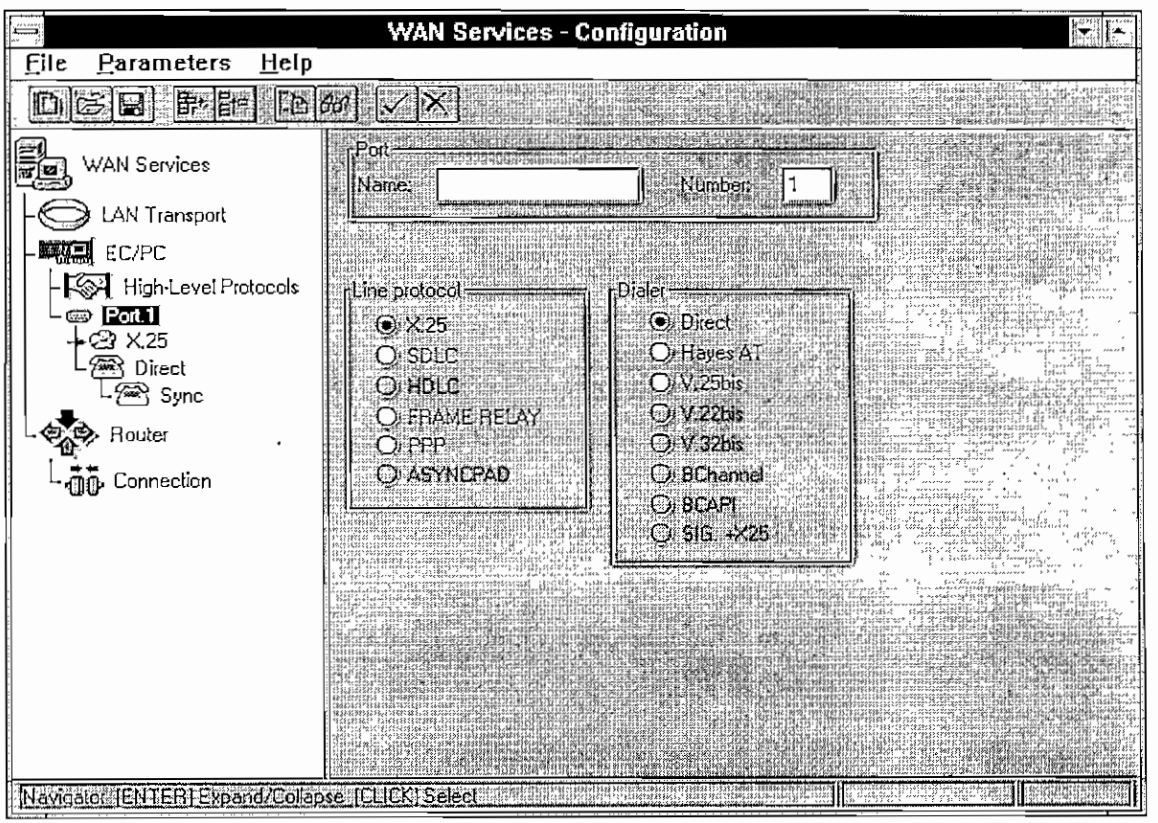


Figura 5.3 Configuración de la controladora de red *WAN*

- Con la opción **X.25** dentro de *Port 1* se ponen los parámetros X.25 del puerto *WAN* del servidor de Agencia como indica la figura 5.4, que en este caso tiene la siguiente configuración:

. *Node Type* : *DTE* , indica que el Servidor de Agencia actúa como *DTE*

. *Node Address* :101010 dirección del servidor de la AGENCIA 1

. *X.25 Version* : 1984

. *Window Size* : 2

. *Packet Size* : 128

. Circuitos virtuales temporales *TVC* = 32 que equivalen a los SVCs.

. Circuitos virtuales permanentes *PVC* = 0, lo cual permite generar circuitos virtuales solo cuando se realiza una llamada hacia el servidor.

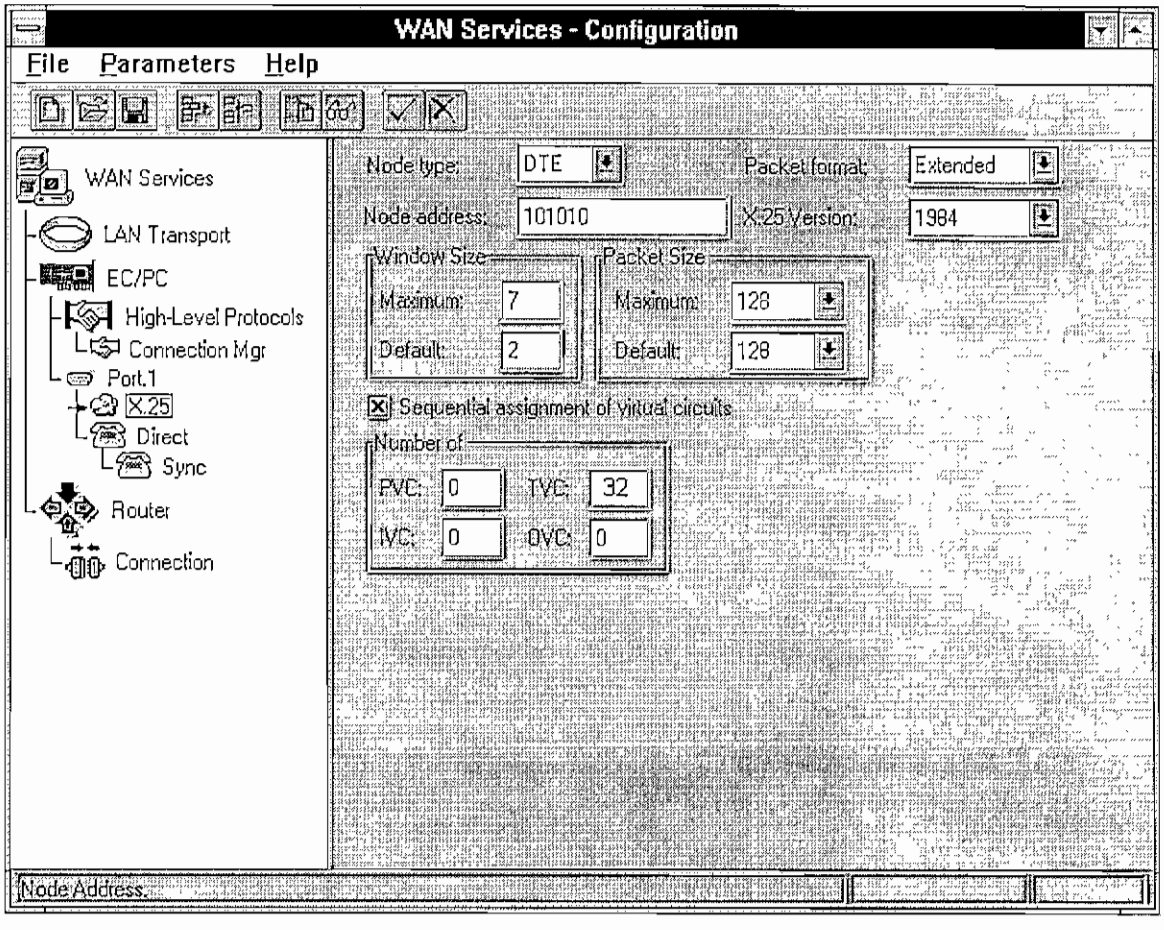


Figura 5.4 Configuración X.25 de la controladora de red *WAN*

- El transporte para *LAN* se escoge *TCP*, para emplear con TCP/IP configurado anteriormente.

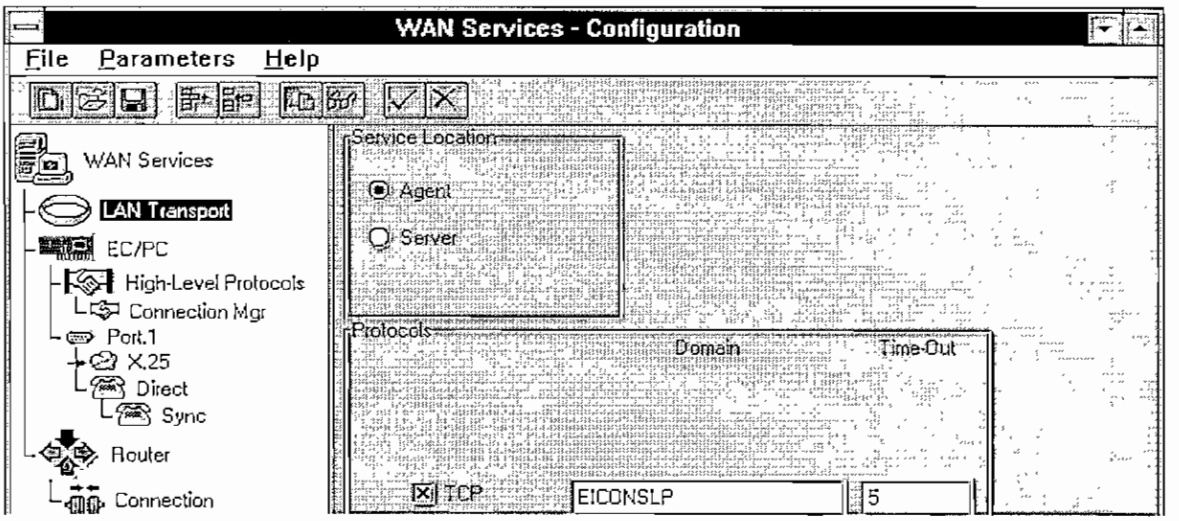


Figura 5.5 Configuración de protocolo de red extendida en la controladora *EICON*

- Para configurar el módulo de ruteador en la tarjeta *EICON* se escoge la opción **Connection**, para generar una conexión TCP/IP hacia el servidor UNIX que tiene la dirección X25 101000 y dirección IP 130.000.001.0001 como indican las figuras 5.6 y 5.7.

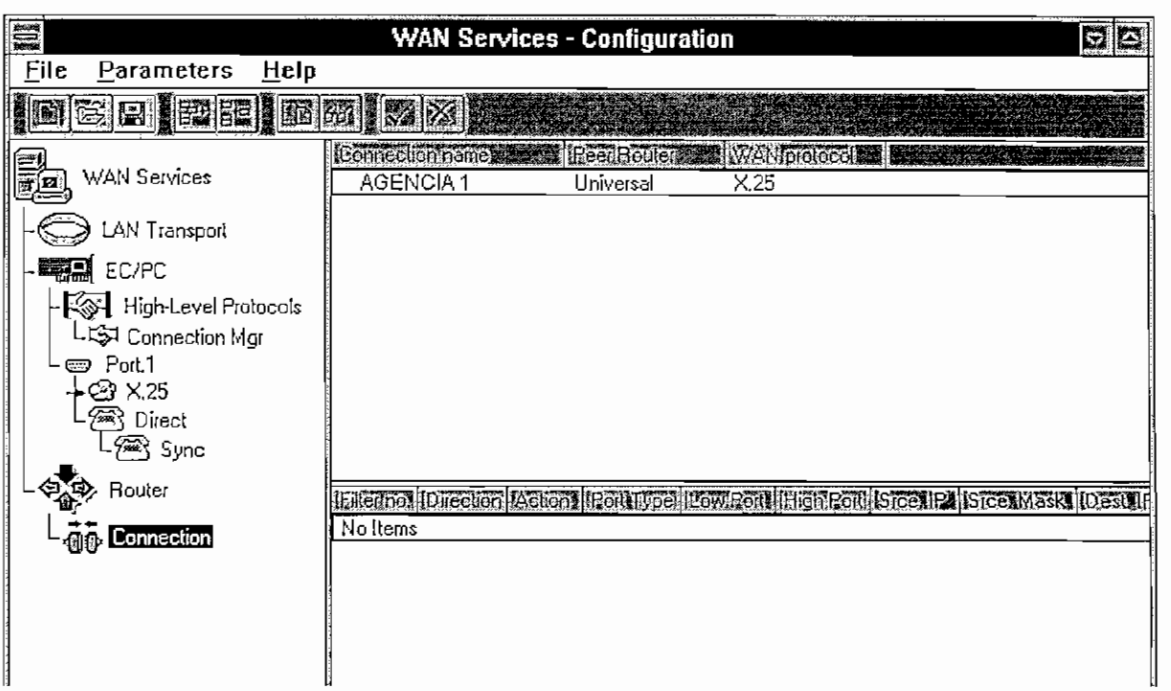


Figura 5.6 Configuración de la conexión TCP/IP en la controladora *EICON*

A la conexión con el *UNIX* se le nombra como AGENCIA 1.

El tipo de conexión debe ser *Two Way* , para que establezcan la conexión cualquiera de los dos servidores. Se debe especificar la dirección remota *IP* del servidor *UNIX* remoto y las direcciones X25 del *Windows NT* local y del *UNIX* remoto

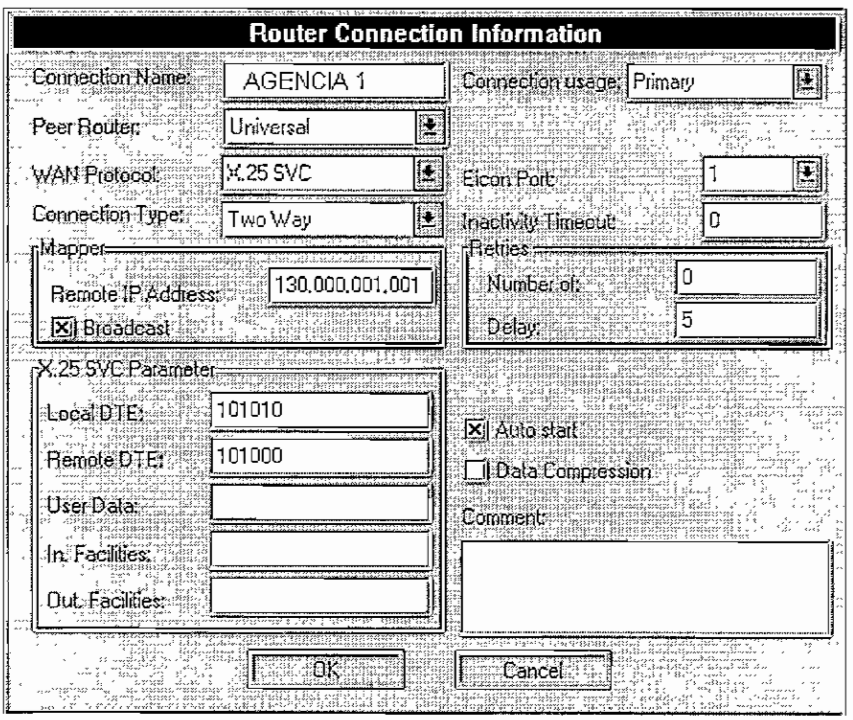


Figura 5.7 Configuración de la conexión TCP/IP sobre X.25 hasta el Servidor UNIX

El tamaño del datagrama se escoge con **Connection Manager**, que para este caso es 1514.

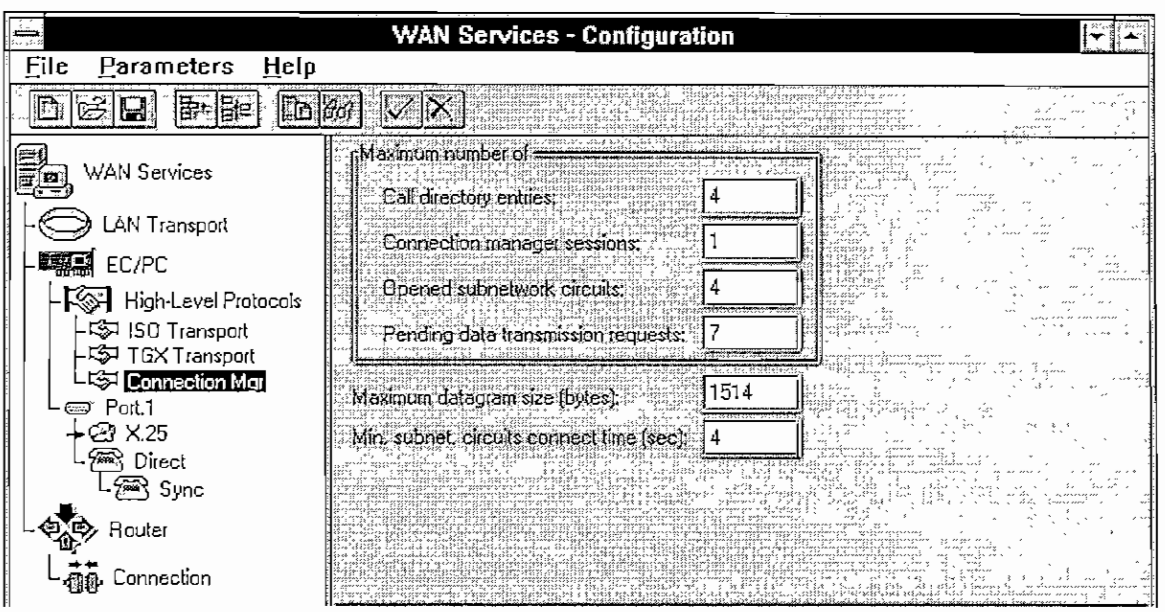


Figura 5.8 Parámetros X.25 de las conexiones X.25

5.3 CONFIGURACION *TCP/IP* EN *WINDOWS* PARA GRUPOS

El procedimiento para configurar *TCP/IP* en *Windows* para Grupos es el siguiente:

- Seleccionar icono de red
- Con el botón de Redes, se escoge : Instalar red Microsoft
- Con el botón de Controladores, se agrega y se configura la tarjeta de red y el protocolo de red a emplearse, en este caso *TCP/IP*, el cual debe estar como protocolo predeterminado.
- Con el botón Agregar Adaptador, se instala la tarjeta de red y con el botón Configurar se establecen parámetros de hardware de la tarjeta, como interrupción y dirección I/O .
- Con el botón Agregar Protocolo, se instala el *TCP/IP*. Con el botón Configurar se establece la dirección *IP* del *host* , con su respectiva máscara y dirección de *gateway*, que este caso es la dirección *IP* del ruteador.
- Cuando se instala la tarjeta de red, también se instalan por *default* los protocolos NetBEUI y IPX/SPX los cuales por lo general son retirados para que el acceso del computador a la red sea más rápido. En este caso se pone como protocolo predeterminado al TCP/IP.

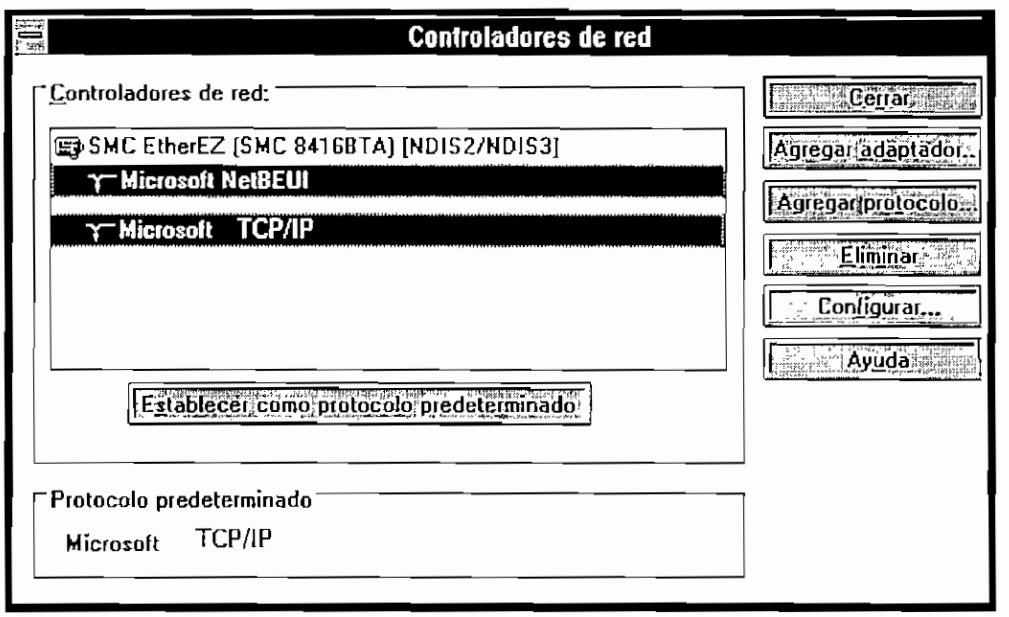


Figura 5.9 Configuración TCP/IP en Usuarios con Windows para Trabajo en Grupo

Mientras más protocolos de red estén instalados, el acceso a la red se torna más lento, por cuanto el computador debe hacer más procesos para escoger el protocolo de red.

ANEXO 6

CAPTURA DE DATOS MEDIANTE NETMONITOR

Los datos mostrados a continuación en el cuadro 6.1 pertenecen a un proceso *FTP* entre el usuario que tiene la dirección *IP* 200.100.200.26 con el servidor *UNIX* que tiene la dirección 200.100.100.1. Mediante Netmonitor se puede analizar los datos que transferimos entre pares de equipos.

En la captura se identifica el número de la trama, las direcciones *MAC* de las dos computadoras, los protocolos que emplean para la comunicación.

En el protocolo *IP* se identifica a *TCP* como el protocolo de la capa superior. *TCP* identifica el puerto origen (1061) y el puerto destino 21(*FTP*). 1061 equivale a 0x0425 en hexadecimal.
En cada nivel se muestran los parámetros estudiados en el capítulo 3 tanto de *IP* como de *TCP*.

En la trama 5 se observa que el servidor *Unix* responde y envía **'220 rchan.labor.com FTP server (Version 5.60 #1) r'** al puerto 1061 del usuario *FTP*.
En la trama 7 se determina que el nombre del *USER* es ***root*** en tanto que en la trama 10 se obtiene el *PASSWORD* del *root* el cual es ***rootcss9*** , lo cual es sumamente peligroso si el software es manejado por personas sin escrúpulos.

En la trama 23 se observa los nombres de los directorios que el servidor *Unix* envía al usuario para que este pueda observarlos ejecutando el comando *ls*. Estos directorios son : *dev* , *bin*, *usr*, *etc.*

Las tramas 50 y 51 corresponden al cierre del proceso *FTP* en donde se ejecuta el comando *QUIT* en el usuario y el servidor responde con ***Goodbye***.

Network Monitor para un proceso FTP

```
Frame  Time   Sre MAC Addr  Dst MAC Addr  Protocol  Description
2      3.364  WestDgC1289E  08003E00675C  TCP       ....S., len: 4, seq: 20548818, ack:        0, win: 8192
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1   IP


 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xC304; Proto = TCP; Len: 44
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: ....S., len: 4, seq: 20548818, aek: 0, win: 8192, src: 1061  dst: 21 (FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
    TCP: Sequence Number = 20548818 (0x1398CD2)
    TCP: Acknowledgement Number = 0 (0x0)
    TCP: Data Offset = 24 (0x18)
    TCP: Reserved = 0 (0x0000)
    TCP: Flags = 0x02 : ....S.
    TCP: Window = 8192 (0x2000)
    TCP: CheckSum = 0x28FC
    TCP: Urgent Pointer = 0 (0x0)
    TCP: Options
    TCP: Frame Padding

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 2C C3 04 40 00 20 06 DA E2 C8 64 C8 1A C8 64   .,..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8C D2 00 00 00 00 60 02   d..%...9......`.
00030:  20 00 28 FC 00 00 02 04 05 B4 20 20               .(.......

*******************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
3      3.485  08003E00675C  WestDgC1289E  TCP       .A..S., len:   0, seq: 939200001, ack:  20548819, win: 4096
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8D5; Proto = TCP; Len: 40
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .A..S., len: 0, seq: 939200001, ack: 20548819, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 00   ....(...>.g\..E.
00010:  00 28 A8 D5 00 00 3A 06 1B 16 C8 64 64 01 C8 64   .(....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 01 01 39 8C D3 50 12   .....%7....9..P.
00030:  10 00 0A AB 00 00 88 88 88 88 88 88               ............

*******************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
5      4.248  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '220 rchan.labor.com FTP server (Version 5.60
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8DE; Proto = TCP; Len: 97
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 57, seq: 939200002, ack: 20548819, win: 4096, src: 21(FTP) dst: 1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
 FTP: Resp. to Port 1061, '220 rchan.labor.com FTP server (Version 5.60 #1) r'
    FTP: FTP Error Return Code = 220
    FTP: FTP Command Arg1 = rchan.labor.com
    FTP: FTP Data: Number of data bytes remaining = 38 (0x0026)
```

```
00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 61 A8 DE 00 00 3A 06 1A C4 C8 64 64 01 C8 64   .a....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 02 01 39 8C D3 50 18   .....%7....9..P.
00030:  10 00 CC 3D 00 00 32 32 30 20 72 63 68 61 6E 2E   ...=..220 rchan.
00040:  6C 61 62 6F 72 2E 63 6F 6D 20 46 54 50 20 73 65   labor.com FTP se

*******************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
7      6.827  WestDgC1289E  08003E00675C  FTP       Req. from Port 1061, 'USER root' Src Other Addr  Dst Other Addr  Type
Other Addr
200.100.200.26  200.100.100.1  IP

 FRAME: Base frame properties
 ETHERNET: Destination address : 08003E00675C
 IP: ID = 0xC604; Proto = TCP; Len: 51
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .AP..., len: 11, seq: 20548819, ack: 939200059, win: 8519, src: 1061 dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
 FTP: Req. from Port 1061, 'USER root'
    FTP: FTP Command = USER
    FTP: FTP Data: Number of data bytes remaining = 7 (0x0007)

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 33 C6 04 40 00 20 06 D7 DB C8 64 C8 1A C8 64   .3..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8C D3 37 FB 0E 3B 50 18   d..%...9..7..;P.
00030:  21 47 50 84 00 00 55 53 45 52 20 72 6F 6F 74 0D   !GP...USER root.
00040:  0A                                                .

*******************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
8      7.010  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '331 Password required for root.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8DF; Proto = TCP; Len: 73
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 33, seq: 939200059, ack: 20548830, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
 FTP: Resp. to Port 1061, '331 Password required for root.'
    FTP: FTP Error Return Code = 331
    FTP: FTP Command Arg1 = Password
    FTP: FTP Data: Number of data bytes remaining = 21 (0x0015)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 49 A8 DF 00 00 3A 06 1A DB C8 64 64 01 C8 64   .I....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 3B 01 39 8C DE 50 18   .....%7..;.9..P.
00030:  10 00 33 EF 00 00 33 33 31 20 50 61 73 73 77 6F   ..3...331 Passwo
00040:  72 64 20 72 65 71 75 69 72 65 64 20 66 6F 72 20   rd required for

*******************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
10     10.601 WestDgC1289E  08003E00675C  FTP       Req. from Port 1061, 'PASS rootcss9'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xC804; Proto = TCP; Len: 55
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .AP..., len: 15, seq: 20548830, ack: 939200092, win: 8486, src: 1061 dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
 FTP: Req. from Port 1061, 'PASS rootcss9'
    FTP: FTP Command = PASS
```

```
    FTP: FTP Data: Number of data bytes remaining = 11 (0x000B)

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 37 C8 04 40 00 20 06 D5 D7 C8 64 C8 1A C8 64   .7..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8C DE 37 FB 0E 5C 50 18   d..%...9..7..\P.
00030:  21 26 9A AF 00 00 50 41 53 53 20 72 6F 6F 74 63   !&....PASS rootc
00040:  73 73 39 0D 0A                                    ss9..

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
11     10.797 08003E00675C  WestDgC1289E  TCP       .A....., len:   0, seq: 939200092, ack:  20548845, win: 4096
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8E0; Proto = TCP; Len: 40
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .A....., len: 0, seq: 939200092, ack: 20548845, win: 4096, src: 21 (FTP) dst: 1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 28 A8 E0 00 00 3A 06 1A FB C8 64 64 01 C8 64   .(....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 5C 01 39 8C ED 50 10   .....%7..\.9..P.
00030:  10 00 0A 38 00 00 88 88 88 88 88 88               ...8........

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
12     11.601 08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '230 User root logged in.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8E1; Proto = TCP; Len: 66
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 26, seq: 939200092, ack: 20548845, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
 FTP: Resp. to Port 1061, '230 User root logged in.'
    FTP: FTP Error Return Code = 230
    FTP: FTP Command Arg1 = User
    FTP: FTP Data: Number of data bytes remaining = 18 (0x0012)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 42 A8 E1 00 00 3A 06 1A E0 C8 64 64 01 C8 64   .B....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 5C 01 39 8C ED 50 18   .....%7..\.9..P.
00030:  10 00 13 FE 00 00 32 33 30 20 55 73 65 72 20 72   ......230 User r
00040:  6F 6F 74 20 6C 6F 67 67 65 64 20 69 6E 2E 0D 0A   oot logged in...

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
13     11.715 WestDgC1289E  08003E00675C  TCP       .A....., len:   0, seq:  20548845, ack: 939200118, win: 8460
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1   IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xC904; Proto = TCP; Len: 40
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .A....., len: 0, seq: 20548845, ack: 939200118, win: 8460, src: 1061  dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 28 C9 04 40 00 20 06 D4 E6 C8 64 C8 1A C8 64   .(..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8C ED 37 FB 0E 76 50 10   d..%...9..7..vP.
00030:  21 0C F9 11 00 00 02 04 05 B4 20 20               !.........
```

```
****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
14     13.846 WestDgC1289E  08003E00675C  FTP       Req. from Port 1061, 'PORT 200,100,200,26,4,38'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1   IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xCA04; Proto = TCP; Len: 66
    IP: Source Address = 200,100,200,26
    IP: Destination Address = 200.100.100.1
 TCP: .AP..., len: 26, seq: 20548845, ack: 939200118, win: 8460, src: 1061 dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
 FTP: Req. from Port 1061, 'PORT 200,100,200,26,4,38'
    FTP: FTP Command = PORT
    FTP: FTP Data: Number of data bytes remaining = 22 (0x0016)

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 42 CA 04 40 00 20 06 D3 CC C8 64 C8 1A C8 64   .B..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8C ED 37 FB 0E 76 50 18   d..%...9..7..vP.
00030:  21 0C 76 59 00 00 50 4F 52 54 20 32 30 30 2C 31   !.vY..PORT 200,1
00040:  30 30 2C 32 30 30 2C 32 36 2C 34 2C 33 38 0D 0A   00,200,26,4,38..

****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
15     14.014 08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '200 PORT eommand successful.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 30, seq: 939200118, ack: 20548871, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
 FTP: Resp. to Port 1061, '200 PORT command successful.'
    FTP: FTP Error Return Code = 200 (Command OK)
    FTP: FTP Command Arg1 = PORT
    FTP: FTP Data: Number of data bytes remaining = 22 (0x0016)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 46 A8 E2 00 00 3A 06 1A DB C8 64 64 01 C8 64   .F....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 76 01 39 8D 07 50 18   .....%7..v.9..P.
00030:  10 00 4C F6 00 00 32 30 30 20 50 4F 52 54 20 63   ..L...200 PORT c
00040:  6F 6D 6D 61 6E 64 20 73 75 63 63 65 73 73 66 75   ommand successfu

****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
16     14.018 WestDgC1289E  08003E00675C  FTP       Req. from Port 1061, 'NLST'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1   IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .AP..., len: 6, seq: 20548871, ack: 939200148, wiu: 8430, src: 1061  dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
 FTP: Req. from Port 1061, 'NLST'
    FTP: FTP Command = NLST
    FTP: FTP Data: Number of data bytes remaining = 2 (0x0002)

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 2E CB 04 40 00 20 06 D2 E0 C8 64 C8 1A C8 64   ....@. ....d...d
00020:  64 01 04 25 00 15 01 39 8D 07 37 FB 0E 94 50 18   d..%...9..7...P.
00030:  20 EE 4A 3F 00 00 4E 4C 53 54 0D 0A               .J?..NLST..
```

```
*******************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
21     14.390 08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '150 Opening ASCII mode data connection for f
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8E6; Proto = TCP; Len: 95
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 55, seq: 939200148, ack: 20548877, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
 FTP: Resp. to Port 1061, '150 Opening ASCII mode data connection for file li'
    FTP: FTP Error Return Code = 150
    FTP: FTP Command Arg1 = Opening
    FTP: FTP Data: Number of data bytes remaining = 44 (0x002C)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 5F A8 E6 00 00 3A 06 1A BE C8 64 64 01 C8 64   ._....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E 94 01 39 8D 0D 50 18   .....%7....9..P.
00030:  10 00 EE 83 00 00 31 35 30 20 4F 70 65 6E 69 6E   ......150 Openin
00040:  67 20 41 53 43 49 49 20 6D 6F 64 65 20 64 61 74   g ASCII mode dat

*******************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
22     14.514 WestDgC1289E  08003E00675C  TCP       .A....., len:   0, seq:  20548877, ack: 939200203, win: 8375
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1   IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xCD04; Proto = TCP; Len: 40
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .A...., len: 0, seq: 20548877, ack: 939200203, win: 8375, src: 1061  dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 28 CD 04 40 00 20 06 D0 E6 C8 64 C8 1A C8 64   .(..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8D 0D 37 FB 0E CB 50 10   d..%...9..7...P.
00030:  20 B7 F8 F1 00 00 4E 4C 53 54 0D 0A               .....NLST..

*******************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
23     14.642 08003E00675C  WestDgC1289E  FTP       Data Transfer To Client, Port = 1062, size 232
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8E7; Proto = TCP; Len: 272
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 232, seq: 940608002, ack: 20559635, win: 4096, src: 20  dst: 1062
    TCP: Source Port = FTP [default data]
    TCP: Destination Port = 0x0426
 FTP: Data Transfer To Client, Port = 1062, size 232
    FTP: FTP Data: Number of data bytes remaining = 232 (0x00E8)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 08   ....(...>.g\..E.
00010:  01 10 A8 E7 00 00 3A 06 1A 14 C8 64 64 01 C8 64   ......:....dd..d
00020:  C8 1A 00 14 04 26 38 10 8A 02 01 39 B7 13 50 18   .....&8....9..P.
00030:  10 00 BB 2C 00 00 2E 0D 0A 2E 2E 0D 0A 64 65 76   ...,.........dev
00040:  0D 0A 62 69 6E 0D 0A 75 73 72 0D 0A 65 74 63 0D   ..bin..usr..etc.

*******************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
24     14.691 08003E00675C  WestDgC1289E  TCP       .A...F, len:   0, seq: 940608234, ack:  20559635, win: 4096
Src Other Addr  Dst Other Addr  Type Other Addr
```

```
200.100.100.1  200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .A...F, len: 0, seq: 940608234, ack: 20559635, win: 4096, src: 20  dst: 1062
    TCP: Source Port = FTP [default data]
    TCP: Destination Port = 0x0426

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 08   ....(...>.g\..E.
00010:  00 28 A8 E8 00 00 3A 06 1A FB C8 64 64 01 C8 64   .(....:....dd..d
00020:  C8 1A 00 14 04 26 38 10 8A EA 01 39 B7 13 50 11   .....&8....9..P.
00030:  10 00 63 6D 00 00 88 88 88 88 88 88              ..cm........

*******************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
25     14.692  WestDgC1289E  08003E00675C  TCP       .A...., len:    0, seq:  20559635, ack: 940608235, win: 8344
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xCE04; Proto = TCP; Len: 40
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .A...., len: 0, seq: 20559635, ack: 940608235, win: 8344, src: 1062  dst: 20
    TCP: Source Port = 0x0426
    TCP: Destination Port = FTP [default data]

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 28 CE 04 40 00 20 06 CF E6 C8 64 C8 1A C8 64   .(..@. ....d...d
00020:  64 01 04 26 00 14 01 39 B7 13 38 10 8A EB 50 10   d..&...9..8...P.
00030:  20 98 52 D5 00 00 02 04 05 B4 20 32               .R..... 2

*******************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
26     14.754  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '226 Transfer complete.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1  200.100.200.26  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xA8E9; Proto = TCP; Len: 64
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
 TCP: .AP..., len: 24, seq: 939200203, ack: 20548877, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
 FTP: Resp. to Port 1061, '226 Transfer complete.'
    FTP: FTP Error Return Code = 226
    FTP: FTP Command Arg1 = Transfer
    FTP: FTP Data: Number of data bytes remaining = 12 (0x000C)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 40 A8 E9 00 00 3A 06 1A DA C8 64 64 01 C8 64   .@....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E CB 01 39 8D 0D 50 18   .....%7....9..P.
00030:  10 00 3A 93 00 00 32 32 36 20 54 72 61 6E 73 66   ..:...226 Transf
00040:  65 72 20 63 6F 6D 70 6C 65 74 65 2E 0D 0A         er complete...

*******************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
30     16.542  WestDgC1289E  08003E00675C  FTP       Req. from Port 1061, 'PORT 200,100,200,26,4,39'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1  IP

 FRAME: Base frame properties
 ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 IP: ID = 0xD104; Proto = TCP; Len: 66
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
 TCP: .AP..., len: 26, seq: 20548877, ack: 939200227, win: 8351, src: 1061 dst: 21(FTP)
```

```
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
  FTP: Req. from Port 1061, 'PORT 200,100,200,26,4,39'
    FTP: FTP Command = PORT
    FTP: FTP Data: Number of data bytes remaining = 22 (0x0016)

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   ..>.g\....(...E.
00010:  00 42 D1 04 40 00 20 06 CC CC C8 64 C8 1A C8 64   .B..@. ....d...d
00020:  64 01 04 25 00 15 01 39 8D 0D 37 FB 0E E3 50 18   d..%...9..7...P.
00030:  20 9F 76 38 00 00 50 4F 52 54 20 32 30 30 2C 31    .v8..PORT 200,1
00040:  30 30 2C 32 30 30 2C 32 36 2C 34 2C 33 39 0D 0A   00,200,26,4,39..

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
31     16.707  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '200 PORT command successful.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

  FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
  IP: ID = 0xA8EB; Proto = TCP; Len: 70
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
  TCP: .AP..., len: 30, seq: 939200227, ack: 20548903, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [eontrol]
    TCP: Destination Port = 0x0425
  FTP: Resp. to Port 1061, '200 PORT command sueeessful.'
    FTP: FTP Error Return Code = 200 (Command OK)
    FTP: FTP Command Arg1 = PORT
    FTP: FTP Data: Number of data bytes remaining = 22 (0x0016)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 46 A8 EB 00 00 3A 06 1A D2 C8 64 64 01 C8 64   .F....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0E E3 01 39 8D 27 50 18   .....%7....9.'P.
00030:  10 00 4C 69 00 00 32 30 30 20 50 4F 52 54 20 63   ..Li..200 PORT c
00040:  6F 6D 6D 61 6E 64 20 73 75 63 63 65 73 73 66 75   ommand successfu

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
38     17.143  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '150 Opening ASCII mode data connection for f
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

  FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
  IP: ID = 0xA8EF; Proto = TCP; Len: 95
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
  TCP: .AP..., len: 55, seq: 939200257, ack: 20548909, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
  FTP: Resp. to Port 1061, '150 Opening ASCII mode data connection for file li'
    FTP: FTP Error Return Code = 150
    FTP: FTP Command Arg1 = Opening
    FTP: FTP Data: Number of data bytes remaining = 44 (0x002C)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 5F A8 EF 00 00 3A 06 1A B5 C8 64 64 01 C8 64   ._....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0F 01 01 39 8D 2D 50 18   .....%7....9.-P.
00030:  10 00 ED F6 00 00 31 35 30 20 4F 70 65 6E 69 6E   ......150 Openin
00040:  67 20 41 53 43 49 49 20 6D 6F 64 65 20 64 61 74   g ASCII mode dat

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
43     17.507  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '226 Transfer complete.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

  FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protoeol
  IP: ID = 0xA8F2; Proto = TCP; Len: 64
    IP: Source Address = 200.100.100.1
```

```
    IP: Destination Address = 200.100.200.26
  TCP: .AP..., len: 24, seq: 939200312, ack: 20548909, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
  FTP: Resp. to Port 1061, '226 Transfer complete.'
    FTP: FTP Error Return Code = 226
    FTP: FTP Command Arg1 = Transfer
    FTP: FTP Data: Number of data bytes remaining = 12 (0x000C)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 40 A8 F2 00 00 3A 06 1A D1 C8 64 64 01 C8 64   .@....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0F 38 01 39 8D 2D 50 18   .....%7..8.9.-P.
00030:  10 00 3A 06 00 00 32 32 36 20 54 72 61 6E 73 66   ..:...226 Transf
00040:  65 72 20 63 6F 6D 70 6C 65 74 65 2E 0D 0A         er complete...

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
50     32.359  WestDgC1289E  08003E00675C  FTP       Req. from Port 1061, 'QUIT'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.200.26  200.100.100.1   IP

  FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
  IP: ID = 0xD804; Proto = TCP; Len: 46
    IP: Source Address = 200.100.200.26
    IP: Destination Address = 200.100.100.1
  TCP: .AP..., len: 6, seq: 20548909, ack: 939200336, win: 8242, src: 1061 dst: 21(FTP)
    TCP: Source Port = 0x0425
    TCP: Destination Port = FTP [control]
  FTP: Req. from Port 1061, 'QUIT'
    FTP: FTP Command = QUIT
    FTP: FTP Data: Number of data bytes remaining = 2 (0x0002)

00000:  08 00 3E 00 67 5C 00 00 C0 C1 28 9E 08 00 45 00   .>.g\....(...E.
00010:  00 2E D8 04 40 00 20 06 C5 E0 C8 64 C8 1A C8 64   ....@. ....d...d
00020:  64 01 04 25 00 15 01 39 8D 2D 37 FB 0F 50 50 18   d..%...9.-7..PP.
00030:  20 32 51 10 00 00 51 55 49 54 0D 0A               2Q...QUIT..

*****************************************************************************************
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol  Description
51     32.493  08003E00675C  WestDgC1289E  FTP       Resp. to Port 1061, '221 Goodbye.'
Src Other Addr  Dst Other Addr  Type Other Addr
200.100.100.1   200.100.200.26  IP

  FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
  IP: ID = 0xA8F4; Proto = TCP; Len: 54
    IP: Source Address = 200.100.100.1
    IP: Destination Address = 200.100.200.26
  TCP: .AP..., len: 14, seq: 939200336, ack: 20548915, win: 4096, src: 21 (FTP) dst:1061
    TCP: Source Port = FTP [control]
    TCP: Destination Port = 0x0425
  FTP: Resp. to Port 1061, '221 Goodbye.'
    FTP: FTP Error Return Code = 221
    FTP: FTP Command Arg1 = Goodbye.
    FTP: FTP Data: Number of data bytes remaining = 2 (0x0002)

00000:  00 00 C0 C1 28 9E 08 00 3E 00 67 5C 08 00 45 10   ....(...>.g\..E.
00010:  00 36 A8 F4 00 00 3A 06 1A D9 C8 64 64 01 C8 64   .6....:....dd..d
00020:  C8 1A 00 15 04 25 37 FB 0F 50 01 39 8D 33 50 18   .....%7..P.9.3P.
00030:  10 00 1A 10 00 00 32 32 31 20 47 6F 6F 64 62 79   ......221 Goodby
00040:  65 2E 0D 0A                                       e...
```

Cuadro 6.1 Análisis de captura de datos mediante *Netmonitor*

ANEXO 7
CRONOGRAMA DE INSTALACION DE LA RED DE DATOS
ANGEL CHINCHERO VILLACIS
as of Sat 12/07/97

Dates			
Start:	Mon 26/02/96	Finish:	Fri 9/08/96
Baseline Start:	Mon 26/02/96	Baseline Finish:	Fri 9/08/96
Actual Start:	Mon 26/02/96	Actual Finish:	Fri 9/08/96
Start Variance:	0d	Finish Variance:	0d

Duration			
Scheduled:	120d	Remaining:	0d
Baseline:	120d	Actual:	120d
Variance:	0d	Percent Complete:	100%

Work			
Scheduled:	4544h	Remaining:	0h
Baseline:	4544h	Actual:	4544h
Variance:	0h	Percent Complete:	100%

Costs			
Scheduled:	S 85.840,00	Remaining:	S 0,00
Baseline:	S 85.840,00	Actual:	S 85.840,00
Variance:	S 0,00		

Task Status		Resource Status	
Tasks not yet started:	0	Resources:	20
Tasks in progress:	0	Overallocated Resources:	0
Tasks completed:	88		
Total Tasks:	88	Total Resources:	20

Notes

RESUMEN DEL PROYECTO

PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	ANTERIOR	SOPORTE TECNICO
1	CRONOGRAMA DE INSTALACION DE RED DEL BANCO	120d	Mon 26/02/96	Fri 9/08/96		
2	Revisión de la Instalación Original en MATRIZ del BANCO	3d	Mon 26/02/96	Wed 28/02/96		
3	Revisión de cableado	1d	Mon 26/02/96	Mon 26/02/96		Ing Elec Q1;Téc. Elec. Q1
4	Revisión de Equipos	2d	Tue 27/02/96	Wed 28/02/96	3	Ing Elec Q1;Téc. Elec. Q1
5	Revisión Software	3d	Mon 26/02/96	Wed 28/02/96		Ing Sist Q1
6	Estudio de Factibilidad de Software y Hardware Originales	2d	Thu 29/02/96	Fri 1/03/96	2	
7	Factibilidad de uso de Hardware	1d	Thu 29/02/96	Thu 29/02/96		Ing Elec Q1
8	Factibilidad de uso del Software	1d	Fri 1/03/96	Fri 1/03/96	7	Ing Sist Q1
9	Diseño Topológico de la red de datos	8d	Mon 4/03/96	Wed 13/03/96	2;6	
10	Topología de la red WAN	2d	Mon 4/03/96	Tue 5/03/96		Ing Elec Q1
11	Topología de la red LAN	2d	Wed 6/03/96	Thu 7/03/96	10	Ing Elec Q1
12	Selección y Dimensión de Equipos de Comunicación	2d	Fri 8/03/96	Mon 11/03/96	11	Ing Elec Q1
13	Selección y Dimensión de Servidores y Terminales	2d	Tue 12/03/96	Wed 13/03/96	12	Ing Elec Q1
14	Entrenamiento de Técnicos	10d	Thu 14/03/96	Wed 27/03/96	9	
15	Entrenamiento en Hardware	10d	Thu 14/03/96	Wed 27/03/96		Ing Elec Q1,Ing Elec Q1
16	Entrenamiento en Software	10d	Thu 14/03/96	Wed 27/03/96		Ing Sist Q1,Ing Sist Q1
17	Instalación de cable de red UTP en MATRIZ del BANCO	13d	Thu 11/04/96	Mon 29/04/96	9	
18	Análisis de la estructura y facilidades del edificio	1d	Thu 11/04/96	Thu 11/04/96		Ing Elec Q2,Ing Elec Q3
19	Elección de cable para instalación de redes locales	1d	Thu 11/04/96	Thu 11/04/96		
20	Diseño de distribución física de la red en MATRIZ	2d	Fri 12/04/96	Mon 15/04/96	18;19	Ing Elec Q2,Ing Elec Q3

PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	ANTERIOR	SOPORTE TECNICO
21	Instalación del cable y puntos de red	10d	Tue 16/04/96	Mon 29/04/96	20	Téc. Elec. G1,Ing. Elec G2,Téc. Elec. G2,Téc. Elec. G3,Téc. Elec. G4,Ing. Elec G3
22	Instalación del cable UTP en las AGENCIAS	18d	Tue 30/04/96	Thu 23/05/96	9	
23	Análisis de facilidades de edificios en Guayaquil, Cuenca, Ambato	3d	Tue 30/04/96	Thu 2/05/96		Ing Elec G1;Ing Elec G4
24	Diseño de distribución física de la red en GUAYAQUIL, CUENCA, AMBAT	3d	Fri 3/05/96	Tue 7/05/96	23	Ing Elec G1;Ing Elec G4
25	Instalación del cable y puntos de red en GUAYAQUIL	3d	Wed 8/05/96	Fri 10/05/96	24	Téc. Elec. G1;Téc. Elec. G2,Téc. Elec. G3;Ing Elec G1
26	Instalación del cable y puntos de red en CUENCA	3d	Mon 13/05/96	Wed 15/05/96	25	Téc. Elec. G1;Téc. Elec. G2,Téc. Elec. G3;Ing Elec G1
27	Instalación del cable y puntos de red en AMBATO	6d	Thu 16/05/96	Thu 23/05/96	26	Téc. Elec. G1;Téc. Elec. G2;Téc. Elec. G3;Ing Elec G4
28	Instalación de Laboratorio de SOPORTE TECNICO	2d	Thu 11/04/96	Fri 12/04/96	14	
29	Red Local y Extendida	1d	Thu 11/04/96	Thu 11/04/96		Ing Elec G1
30	Configuración de Servidor UNIX y Windows NT	1d	Fri 12/04/96	Fri 12/04/96	29	Ing. Sist G1
31	Configuración de terminales Windows para Trabajo en Grupo	1d	Fri 12/04/96	Fri 12/04/96		Ing Sist G2
32	Pruebas de comunicación entre equipos	1d	Fri 12/04/96	Fri 12/04/96		Ing Elec G1
33	Instalación de Laboratorio en MATRIZ del BANCO	2d	Tue 30/04/96	Wed 1/05/96	17	
34	Laboratorio de red local y extendida	1d	Tue 30/04/96	Tue 30/04/96		Ing Elec G2
35	Instalación del Servidor UNIX de DESARROLLO	1d	Wed 1/05/96	Wed 1/05/96	34	Ing Sist G1
36	Intalación de Windows NT y Usuarios de DESARROLLO	1d	Wed 1/05/96	Wed 1/05/96		Ing Sist G2
37	Conexión del Servidor SANYO a la red Ethernet	1d	Wed 1/05/96	Wed 1/05/96		Ing Elec G2
38	Pruebas de conectividad	1d	Wed 1/05/96	Wed 1/05/96		Ing Elec G1
39	Instalación de RUTEADORES y HUBS	19d	Tue 30/04/96	Fri 24/05/96	17;22	
40	Instalación y pruebas en Matriz	1d	Tue 30/04/96	Tue 30/04/96		Ing Elec G1;Téc. Elec. G1

PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	ANTERIOR	SOPORTE TECNICO
41	Instalación y pruebas en Agencias	1d	Fri 24/05/96	Fri 24/05/96	40	Téc, Elec, O2,Ing Elec O2,Ing Elec O1;Téc. Elec, O1;Téc, Elec, O2,Ing Elec O1
42	Implementación de la red de datos en MATRIZ	5d	Fri 24/05/96	Thu 30/05/96	17	
43	Instalación de Servidor UNIX de PRODUCCION	1d	Fri 24/05/96	Fri 24/05/96		Ing Sist O4
44	Instalación de Aplicaciones Bancarias en el Servidor UNIX	2d	Mon 27/05/96	Tue 28/05/96	43	Ing Sist O3
45	Configuración e Instalación de Servidores NT	2d	Mon 27/05/96	Tue 28/05/96	44	Ing Elec O4,Ing Sist O4,Ing Sist O1
52	Configuración e Instalación de Usuarios de red	2d	Wed 29/05/96	Thu 30/05/96	45	Ing Elec O4,Ing Sist O4,Ing Sist O1
55	Instalación de red de datos en AGENCIAS	7d	Mon 3/06/96	Tue 11/06/96	22;39	
56	Configuración de Servidores NT en Laboratorio	1d	Mon 3/06/96	Mon 3/06/96		Ing Elec O4,Ing Sist O4
57	Servidores de AGENCIAS	1d	Mon 3/06/96	Mon 3/06/96		
58	Servidor de IMAGENES	1d	Mon 3/06/96	Mon 3/06/96		
59	Servidor de Correo Electrónico	1d	Mon 3/06/96	Mon 3/06/96		
60	Servidor de Servicio de Acceso Remoto RAS	1d	Mon 3/06/96	Mon 3/06/96		
61	Servidor DHCP , WINS y de Impresión	1d	Mon 3/06/96	Mon 3/06/96		
62	Configuración de Usuarios de AGENCIAS	2d	Tue 4/06/96	Wed 5/06/96	56	Ing Elec O4,Ing Sist O3
63	Terminales Financieras	1d	Tue 4/06/96	Tue 4/06/96		
64	Terminales Administrativas	1d	Wed 5/06/96	Wed 5/06/96		
65	Pruebas de comunicación con las Agencias Simuladas en Laboratorio	3d	Thu 6/06/96	Mon 10/06/96	62	Ing Elec O4,Ing Sist O3
66	Traslado de equipos probados a las Agencias	1d	Fri 7/06/96	Fri 7/06/96	65	
67	Instalación de equipos en los puntos de red	1d	Mon 10/06/96	Mon 10/06/96	66	Téc, Elec, O1,Ing Elec O1,Ing Elec O2;Téc. Elec, O1;Téc, Elec, O2,Ing Elec O3
68	Pruebas de red local y extendida en las Agencias	1d	Tue 11/06/96	Tue 11/06/96		Ing Elec O1;Ing. Sist O1;Ing Sist O2,Ing Elec O2;Ing Elec O3,Ing. Sist O3

PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	ANTERIOR	SOPORTE TECNICO
69	Pruebas de enlaces de red Extendida	2d	Wed 12/06/96	Thu 13/06/96	55	
70	Comunicación entre los Servidores NT y Servidores UNIX	1d	Wed 12/06/96	Wed 12/06/96		Ing Elec O3;Ing Sist O3
71	Comunicación entre usuarios locales y remotos	1d	Thu 13/06/96	Thu 13/06/96	70	Ing Elec O1;Ing Sist O1
72	Monitoreo de red LAN y WAN desde MATRIZ	5d	Fri 14/06/96	Thu 20/06/96	55;69	
73	Instalación de Software de Monitoreo	1d	Fri 14/06/96	Fri 14/06/96		Ing Elec O1
74	Monitoreo de red LAN Ethernet	2d	Mon 17/06/96	Tue 18/06/96		Ing Elec O1
75	Monitoreo de red WAN	2d	Wed 19/06/96	Thu 20/06/96	74	Ing Elec O1
76	Instalación de equipos adicionales	2d	Fri 31/05/96	Mon 3/06/96	42	
77	Clasificadora de cheques	1d	Fri 31/05/96	Fri 31/05/96		Ing Elec O3;Ing Sist O3
78	Arreglo de discos	1d	Mon 3/06/96	Mon 3/06/96	77	Ing Elec O3;Ing Sist O3
79	Actualización de Hardware y Software	15d	Fri 21/06/96	Thu 11/07/96	55	
80	Actualización en Servidores	5d	Fri 21/06/96	Thu 27/06/96		Ing. Sist O1;Ing Sist O1,Ing Sist O2;Ing. Sist O2,Ing Elec O1;Ing Elec O2;Ing. Elec O4,Ing Elec O1
81	Actualización en Usuarios	10d	Fri 28/06/96	Thu 11/07/96	80	Ing Sist O1;Ing. Elec O1;Ing Elec O2;Ing. Sist O2;Ing Sist O1,Ing Sist O2;Téc. Elec. O1;Téc. Elec. O2;Téc. Elec. O1;Téc. Elec. O2;Ing Elec O4,Ing Elec O
82	Afinamiento de la red	12d	Thu 25/07/96	Fri 9/08/96	72;79	
83	Afinamiento de comunicaciones	2d	Thu 25/07/96	Fri 26/07/96		Ing Elec O1;Ing Elec O2
84	Afinamiento de Sistemas Operativos en Servidores y Usuarios	10d	Mon 29/07/96	Fri 9/08/96	83	Ing Sist O3
85	Afinamiento de Aplicaciones	20d	Tue 4/06/96	Mon 1/07/96	76	Ing Sist O4
86	Entrenamiento al personal del BANCO	30d	Thu 2/05/96	Wed 12/06/96	14;33	Ing Elec O2;Ing. Sist O2;Ing. Sist O3
87	Elaboración de manual de RED DE DATOS del BANCO	20d	Mon 17/06/96	Fri 12/07/96	55	Ing Elec O3
88	Elaboración de manual respaldos y contingencias	10d	Mon 17/06/96	Fri 28/06/96	55	Ing. Sist O3

PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	% COMPLETADO	COSTO	TRABAJO
1	CRONOGRAMA DE INSTALACION DE RED DEL BANCO	120d	Mon 26/02/96	Fri 9/08/96	100%	S 0,00	0h
2	Revisión de la Instalación Original en MATRIZ del BANCO	3d	Mon 26/02/96	Wed 28/02/96	100%	S 1.320,00	72h
3	Revisión de cableado	1d	Mon 26/02/96	Mon 26/02/96	100%	S 280,00	16h
4	Revisión de Equipos	2d	Tue 27/02/96	Wed 28/02/96	100%	S 560,00	32h
5	Revisión Software	3d	Mon 26/02/96	Wed 28/02/96	100%	S 480,00	24h
6	Estudio de Factibilidad de Software y Hardware Originales	2d	Thu 29/02/96	Fri 1/03/96	100%	S 320,00	16h
7	Factibilidad de uso de Hardware	1d	Thu 29/02/96	Thu 29/02/96	100%	S 160,00	8h
8	Factibilidad de uso del Software	1d	Fri 1/03/96	Fri 1/03/96	100%	S 160,00	8h
9	Diseño Topológico de la red de datos	8d	Mon 4/03/96	Wed 13/03/96	100%	S 1.280,00	64h
10	Topología de la red WAN	2d	Mon 4/03/96	Tue 5/03/96	100%	S 320,00	16h
11	Topología de la red LAN	2d	Wed 6/03/96	Thu 7/03/96	100%	S 320,00	16h
12	Selección y Dimensión de Equipos de Comunicación	2d	Fri 8/03/96	Mon 11/03/96	100%	S 320,00	16h
13	Selección y Dimensión de Servidores y Terminales	2d	Tue 12/03/96	Wed 13/03/96	100%	S 320,00	16h
14	Entrenamiento de Técnicos	10d	Thu 14/03/96	Wed 27/03/96	100%	S 6.400,00	320h
15	Entrenamiento en Hardware	10d	Thu 14/03/96	Wed 27/03/96	100%	S 3.200,00	160h
16	Entrenamiento en Software	10d	Thu 14/03/96	Wed 27/03/96	100%	S 3.200,00	160h
17	Instalación de cable de red UTP en MATRIZ del BANCO	13d	Thu 11/04/96	Mon 29/04/96	100%	S 8.960,00	528h
18	Análisis de la estructura y facilidades del edificio	1d	Thu 11/04/96	Thu 11/04/96	100%	S 320,00	16h
19	Elección de cable para instalación de redes locales	1d	Thu 11/04/96	Thu 11/04/96	100%	S 0,00	0h
20	Diseño de distribución física de la red en MATRIZ	2d	Fri 12/04/96	Mon 15/04/96	100%	S 640,00	32h

PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	% COMPLETADO	COSTO	TRABAJO
21	Instalación del cable y puntos de red	10d	Tue 16/04/96	Mon 29/04/96	100%	S 8.000,00	480h
22	**Instalación del cable UTP en las AGENCIAS**	**18d**	**Tue 30/04/96**	**Thu 23/05/96**	**100%**	**S 8.160,00**	**480h**
23	Análisis de facilidades de edificios en Guayaquil, Cuenca, Ambato	3d	Tue 30/04/96	Thu 2/05/96	100%	S 960,00	48h
24	Diseño de distribución física de la red en GUAYAQUIL, CUENCA, AMBAT	3d	Fri 3/05/96	Tue 7/05/96	100%	S 960,00	48h
25	Instalación del cable y puntos de red en GUAYAQUIL	3d	Wed 8/05/96	Fri 10/05/96	100%	S 1.560,00	96h
26	Instalación del cable y puntos de red en CUENCA	3d	Mon 13/05/96	Wed 15/05/96	100%	S 1.560,00	96h
27	Instalación del cable y puntos de red en AMBATO	6d	Thu 16/05/96	Thu 23/05/96	100%	S 3.120,00	192h
28	**Instalación de Laboratorio de SOPORTE TECNICO**	**2d**	**Thu 11/04/96**	**Fri 12/04/96**	**100%**	**S 640,00**	**32h**
29	Red Local y Extendida	1d	Thu 11/04/96	Thu 11/04/96	100%	S 160,00	8h
30	Configuración de Servidor UNIX y Windows NT	1d	Fri 12/04/96	Fri 12/04/96	100%	S 160,00	8h
31	Configuración de terminales Windows para Trabajo en Grupo	1d	Fri 12/04/96	Fri 12/04/96	100%	S 160,00	8h
32	Pruebas de comunicación entre equipos	1d	Fri 12/04/96	Fri 12/04/96	100%	S 160,00	8h
33	**Instalación de Laboratorio en MATRIZ del BANCO**	**2d**	**Tue 30/04/96**	**Wed 1/05/96**	**100%**	**S 800,00**	**40h**
34	Laboratorio de red local y extendida	1d	Tue 30/04/96	Tue 30/04/96	100%	S 160,00	8h
35	Instalación del Servidor UNIX de DESARROLLO	1d	Wed 1/05/96	Wed 1/05/96	100%	S 160,00	8h
36	Intalación de Windows NT y Usuarios de DESARROLLO	1d	Wed 1/05/96	Wed 1/05/96	100%	S 160,00	8h
37	Conexión del Servidor SANYO a la red Ethernet	1d	Wed 1/05/96	Wed 1/05/96	100%	S 160,00	8h
38	Pruebas de conectividad	1d	Wed 1/05/96	Wed 1/05/96	100%	S 160,00	8h
39	**Instalación de RUTEADORES y HUBS**	**19d**	**Tue 30/04/96**	**Fri 24/05/96**	**100%**	**S 1.120,00**	**64h**
40	Instalación y pruebas en Matriz	1d	Tue 30/04/96	Tue 30/04/96	100%	S 280,00	16h

CRONOGRAMA 2 - 2

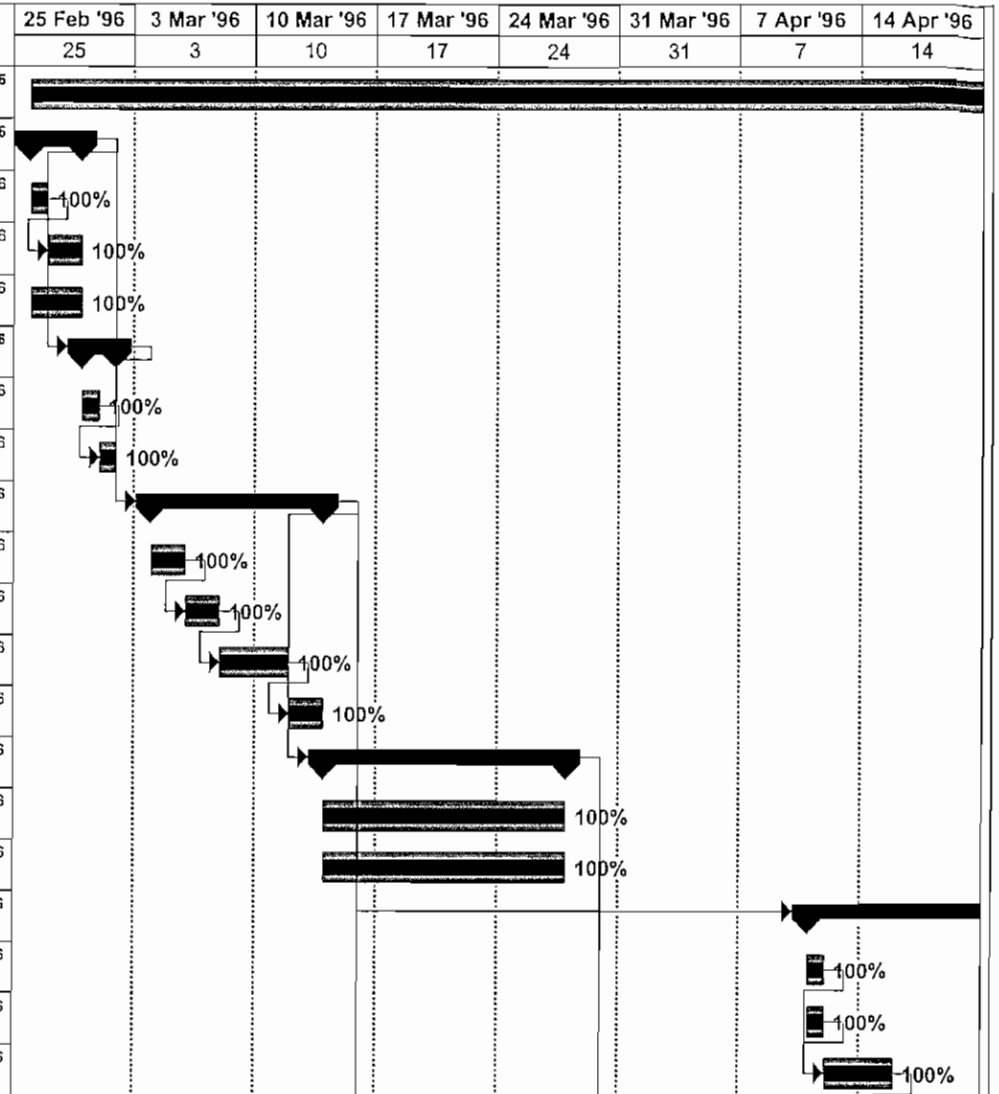
PROYECTO INVESPLAN

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	% COMPLETADO	COSTO	TRABAJO
41	Instalación y pruebas en Agencias	1d	Fri 24/05/96	Fri 24/05/96	100%	S 840,00	48h
42	Implementación de la red de datos en MATRIZ	5d	Fri 24/05/96	Thu 30/05/96	100%	S 2.400,00	120h
43	Instalación de Servidor UNIX de PRODUCCION	1d	Fri 24/05/96	Fri 24/05/96	100%	S 160,00	8h
44	Instalación de Aplicaciones Bancarias en el Servidor UNIX	2d	Mon 27/05/96	Tue 28/05/96	100%	S 320,00	16h
45	Configuración e Instalación de Servidores NT	2d	Mon 27/05/96	Tue 28/05/96	100%	S 960,00	48h
52	Configuración e Instalación de Usuarios de red	2d	Wed 29/05/96	Thu 30/05/96	100%	S 960,00	48h
55	Instalación de red de datos en AGENCIAS	7d	Mon 3/06/96	Tue 11/06/96	100%	S 3.720,00	192h
56	Configuración de Servidores NT en Laboratorio	1d	Mon 3/06/96	Mon 3/06/96	100%	S 320,00	16h
57	Servidores de AGENCIAS	1d	Mon 3/06/96	Mon 3/06/96	100%	S 0,00	0h
58	Servidor de IMAGENES	1d	Mon 3/06/96	Mon 3/06/96	100%	S 0,00	0h
59	Servidor de Correo Electrónico	1d	Mon 3/06/96	Mon 3/06/96	100%	S 0,00	0h
60	Servidor de Servicio de Acceso Remoto RAS	1d	Mon 3/06/96	Mon 3/06/96	100%	S 0,00	0h
61	Servidor DHCP , WINS y de Impresión	1d	Mon 3/06/96	Mon 3/06/96	100%	S 0,00	0h
62	Configuración de Usuarios de AGENCIAS	2d	Tue 4/06/96	Wed 5/06/96	100%	S 640,00	32h
63	Terminales Financieras	1d	Tue 4/06/96	Tue 4/06/96	100%	S 0,00	0h
64	Terminales Administrativas	1d	Wed 5/06/96	Wed 5/06/96	100%	S 0,00	0h
65	Pruebas de comunicación con las Agencias Simuladas en Laboratorio	3d	Thu 6/06/96	Mon 10/06/96	100%	S 960,00	48h
66	Traslado de equipos probados a las Agencias	1d	Fri 7/06/96	Fri 7/06/96	100%	S 0,00	0h
67	Instalación de equipos en los puntos de red	1d	Mon 10/06/96	Mon 10/06/96	100%	S 840,00	48h
68	Pruebas de red local y extendida en las Agencias	1d	Tue 11/06/96	Tue 11/06/96	100%	S 960,00	48h

PROYECTO INVESPLAN

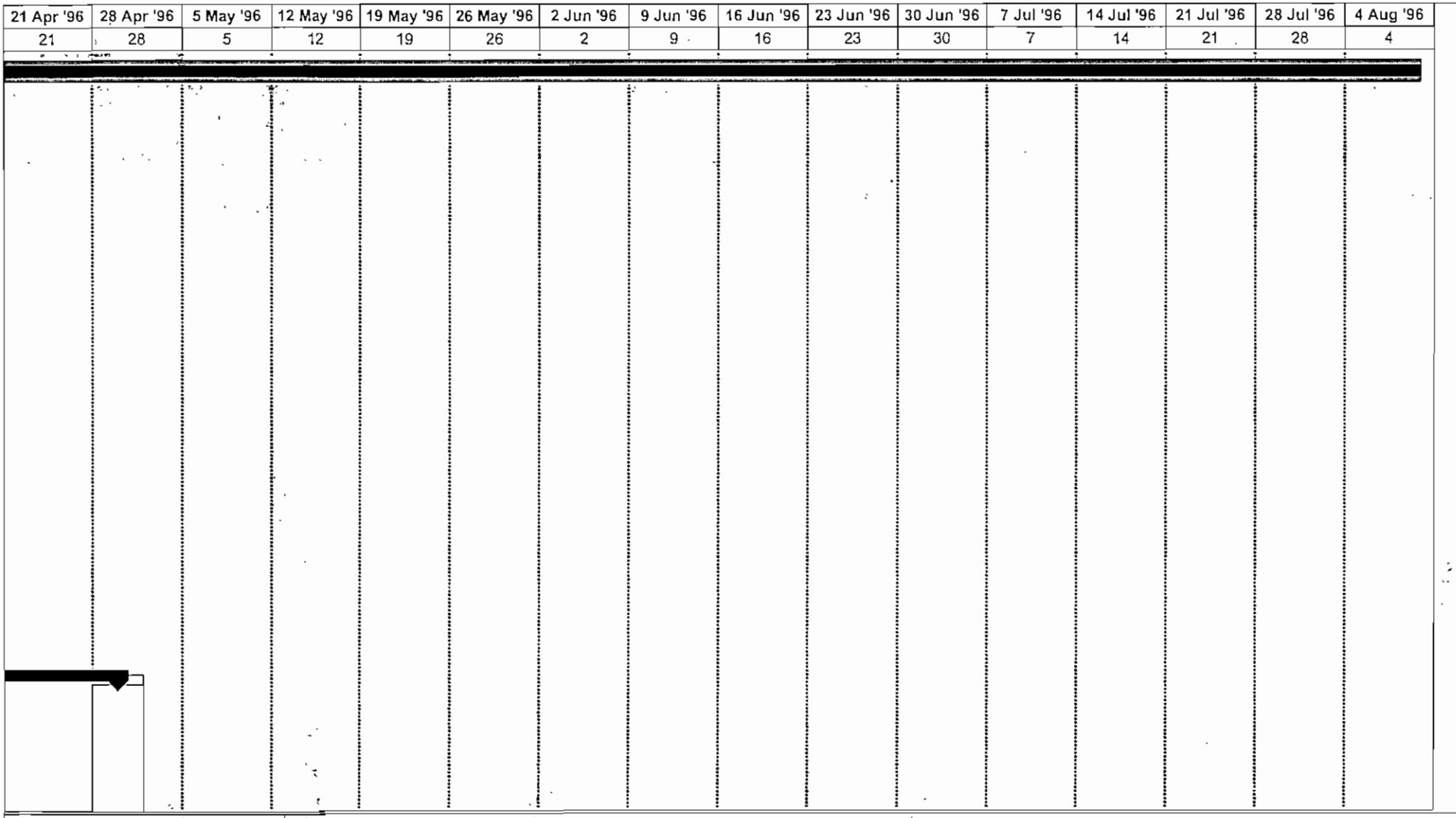
ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN	% COMPLETADO	COSTO	TRABAJO
69	Pruebas de enlaces de red Extendida	2d	Wed 12/06/96	Thu 13/06/96	100%	S 640,00	32h
70	Comunicación entre los Servidores NT y Servidores UNIX	1d	Wed 12/06/96	Wed 12/06/96	100%	S 320,00	16h
71	Comunicación entre usuarios locales y remotos	1d	Thu 13/06/96	Thu 13/06/96	100%	S 320,00	16h
72	Monitoreo de red LAN y WAN desde MATRIZ	5d	Fri 14/06/96	Thu 20/06/96	100%	S 800,00	40h
73	Instalación de Software de Monitoreo	1d	Fri 14/06/96	Fri 14/06/96	100%	S 160,00	8h
74	Monitoreo de red LAN Ethernet	2d	Mon 17/06/96	Tue 18/06/96	100%	S 320,00	16h
75	Monitoreo de red WAN	2d	Wed 19/06/96	Thu 20/06/96	100%	S 320,00	16h
76	Instalación de equipos adicionales	2d	Fri 31/05/96	Mon 3/06/96	100%	S 640,00	32h
77	Clasificadora de cheques	1d	Fri 31/05/96	Fri 31/05/96	100%	S 320,00	16h
78	Arreglo de discos	1d	Mon 3/06/96	Mon 3/06/96	100%	S 320,00	16h
79	Actualización de Hardware y Software	15d	Fri 21/06/96	Thu 11/07/96	100%	S 24.000,00	1280h
80	Actualización en Servidores	5d	Fri 21/06/96	Thu 27/06/96	100%	S 6.400,00	320h
81	Actualización en Usuarios	10d	Fri 28/06/96	Thu 11/07/96	100%	S 17.600,00	960h
82	Afinamiento de la red	12d	Thu 25/07/96	Fri 9/08/96	100%	S 2.240,00	112h
83	Afinamiento de comunicaciones	2d	Thu 25/07/96	Fri 26/07/96	100%	S 640,00	32h
84	Afinamiento de Sistemas Operativos en Servidores y Usuarios	10d	Mon 29/07/96	Fri 9/08/96	100%	S 1.600,00	80h
85	Afinamiento de Aplicaciones	20d	Tue 4/06/96	Mon 1/07/96	100%	S 3.200,00	160h
86	Entrenamiento al personal del BANCO	30d	Thu 2/05/96	Wed 12/06/96	100%	S 14.400,00	720h
87	Elaboración de manual de RED DE DATOS del BANCO	20d	Mon 17/06/96	Fri 12/07/96	100%	S 3.200,00	160h
88	Elaboración de manual respaldos y contingencias	10d	Mon 17/06/96	Fri 28/06/96	100%	S 1.600,00	80h

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN
1	CRONOGRAMA DE INSTALACION DE RED DEL BANCO	120d	Mon 26/02/96	Fri 9/08/96
2	Revisión de la Instalación Original en MATRIZ del BANCO	3d	Mon 26/02/96	Wed 28/02/96
3	Revisión de cableado	1d	Mon 26/02/96	Mon 26/02/96
4	Revisión de Equipos	2d	Tue 27/02/96	Wed 28/02/96
5	Revisión Software	3d	Mon 26/02/96	Wed 28/02/96
6	Estudio de Factibilidad de Software y Hardware Originales	2d	Thu 29/02/96	Fri 1/03/96
7	Factibilidad de uso de Hardware	1d	Thu 29/02/96	Thu 29/02/96
8	Factibilidad de uso del Software	1d	Fri 1/03/96	Fri 1/03/96
9	Diseño Topológico de la red de datos	8d	Mon 4/03/96	Wed 13/03/96
10	Topología de la red WAN	2d	Mon 4/03/96	Tue 5/03/96
11	Topología de la red LAN	2d	Wed 6/03/96	Thu 7/03/96
12	Selección y Dimensión de Equipos de Comunicación	2d	Fri 8/03/96	Mon 11/03/96
13	Selección y Dimensión de Servidores y Terminales	2d	Tue 12/03/96	Wed 13/03/96
14	Entrenamiento de Técnicos	10d	Thu 14/03/96	Wed 27/03/96
15	Entrenamiento en Hardware	10d	Thu 14/03/96	Wed 27/03/96
16	Entrenamiento en Software	10d	Thu 14/03/96	Wed 27/03/96
17	Instalación de cable de red UTP en MATRIZ del BANCO	13d	Thu 11/04/96	Mon 29/04/96
18	Análisis de la estructura y facilidades del edificio	1d	Thu 11/04/96	Thu 11/04/96
19	Elección de cable para instalación de redes locales	1d	Thu 11/04/96	Thu 11/04/96
20	Diseño de distribución física de la red en MATRIZ	2d	Fri 12/04/96	Mon 15/04/96



PROYECTO : RED INVESPLAN
ANGEL CHINCHERO VILLACIS
Date: Sat 12/07/97

Task
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Milestone
Rolled Up Progress

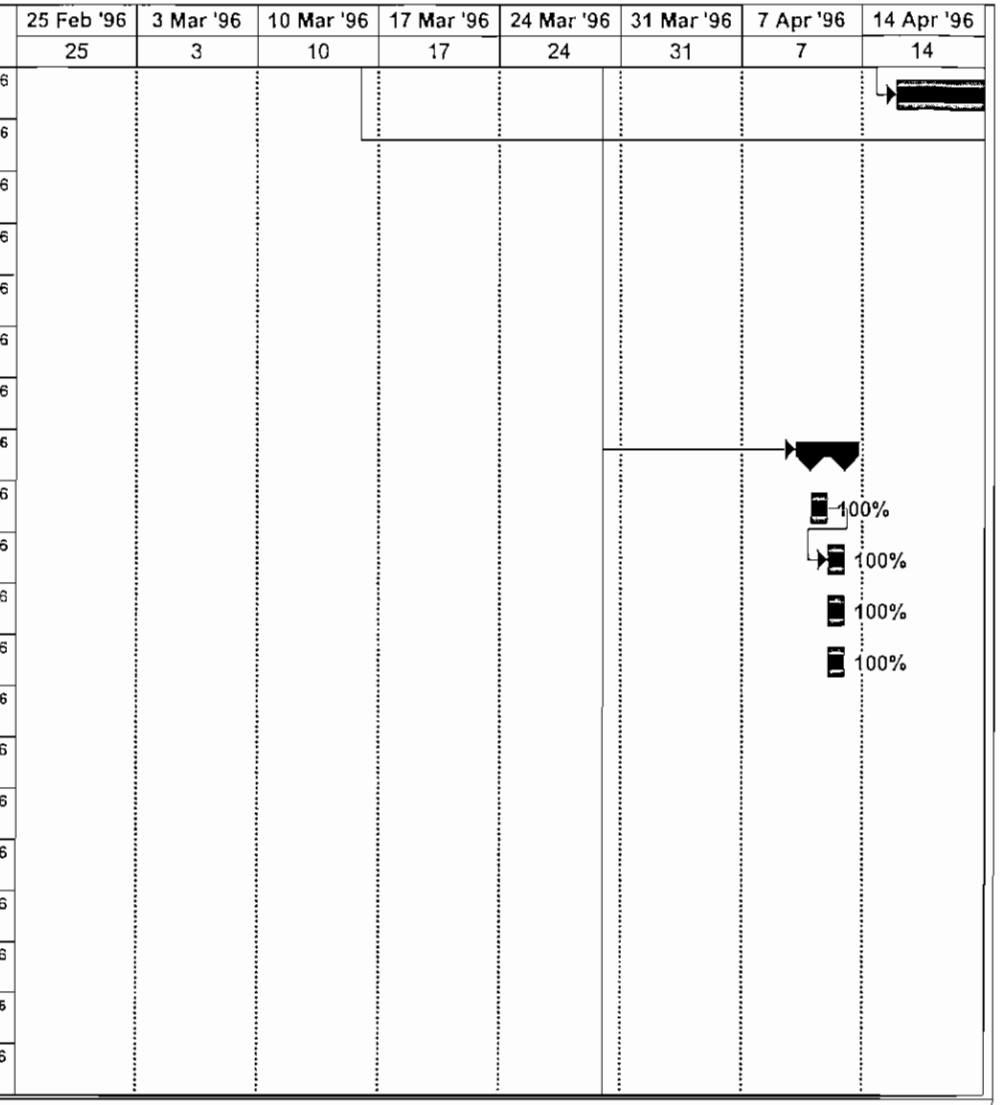


PROYECTO : RED INVESPLAN
ANGEL CHINCHERO VILLACIS
Date: Sat 12/07/97

Task
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Milestone
Rolled Up Progress

CRONOGRAMA 3 - 2

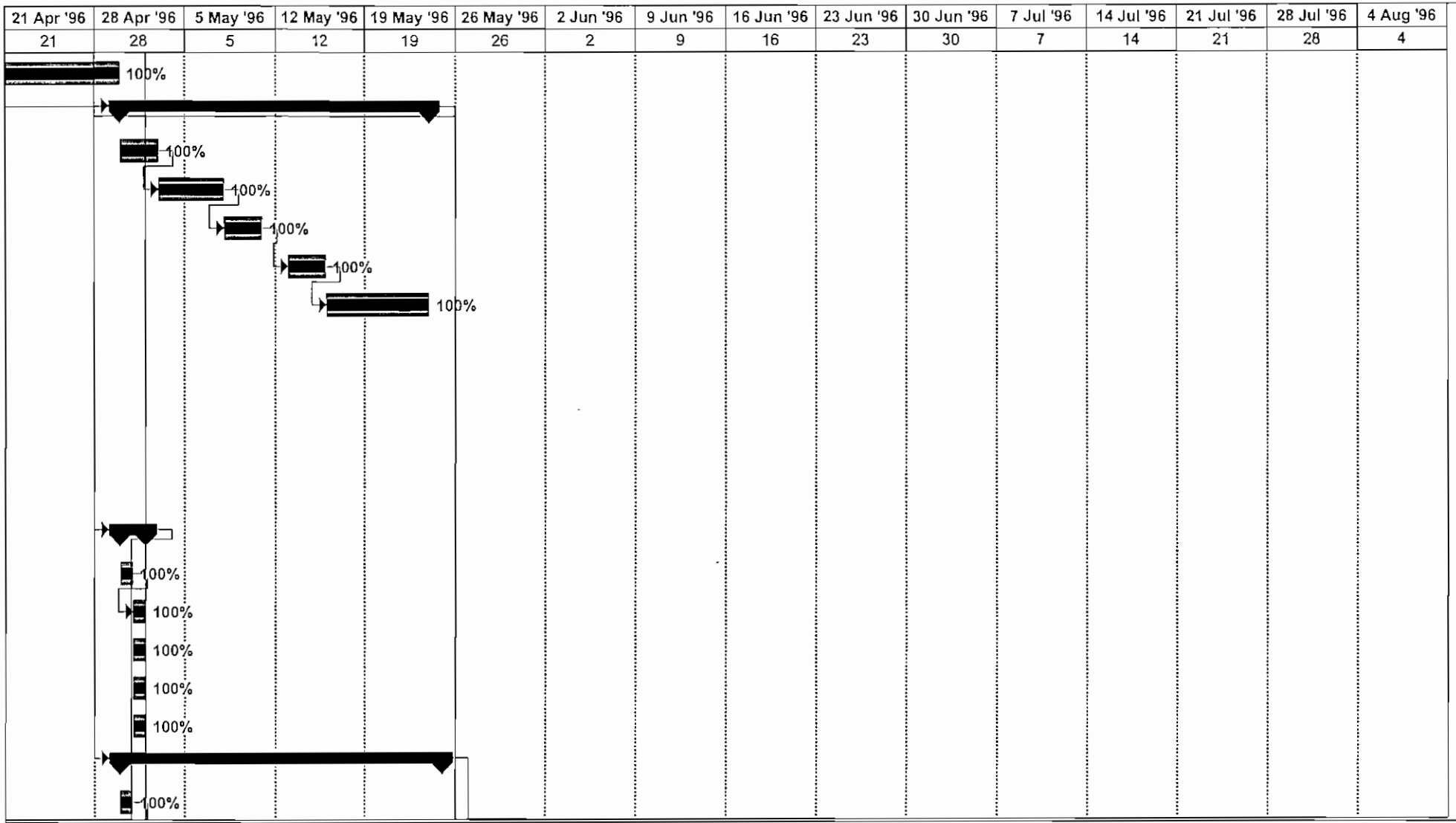
ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN
21	Instalación del cable y puntos de red	10d	Tue 16/04/96	Mon 29/04/96
22	Instalación del cable UTP en las AGENCIAS	18d	Tue 30/04/96	Thu 23/05/96
23	Análisis de facilidades de edificios en Guayaquil, Cuenca, Ambato	3d	Tue 30/04/96	Thu 2/05/96
24	Diseño de distribución física de la red en GUAYAQUIL, CUENCA, AMBAT	3d	Fri 3/05/96	Tue 7/05/96
25	Instalación del cable y puntos de red en GUAYAQUIL	3d	Wed 8/05/96	Fri 10/05/96
26	Instalación del cable y puntos de red en CUENCA	3d	Mon 13/05/96	Wed 15/05/96
27	Instalación del cable y puntos de red en AMBATO	6d	Thu 16/05/96	Thu 23/05/96
28	Instalación de Laboratorio de SOPORTE TECNICO	2d	Thu 11/04/96	Fri 12/04/96
29	Red Local y Extendida	1d	Thu 11/04/96	Thu 11/04/96
30	Configuración de Servidor UNIX y Windows NT	1d	Fri 12/04/96	Fri 12/04/96
31	Configuración de terminales Windows para Trabajo en Grupo	1d	Fri 12/04/96	Fri 12/04/96
32	Pruebas de comunicación entre equipos	1d	Fri 12/04/96	Fri 12/04/96
33	Instalación de Laboratorio en MATRIZ del BANCO	2d	Tue 30/04/96	Wed 1/05/96
34	Laboratorio de red local y extendida	1d	Tue 30/04/96	Tue 30/04/96
35	Instalación del Servidor UNIX de DESARROLLO	1d	Wed 1/05/96	Wed 1/05/96
36	Intalación de Windows NT y Usuarios de DESARROLLO	1d	Wed 1/05/96	Wed 1/05/96
37	Conexión del Servidor SANYO a la red Ethernet	1d	Wed 1/05/96	Wed 1/05/96
38	Pruebas de conectividad	1d	Wed 1/05/96	Wed 1/05/96
39	Instalación de RUTEADORES y HUBS	19d	Tue 30/04/96	Fri 24/05/96
40	Instalación y pruebas en Matriz	1d	Tue 30/04/96	Tue 30/04/96



PROYECTO : RED INVESPLAN
ANGEL CHINCHERO VILLACIS
Date: Sat 12/07/97

Task
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Milestone
Rolled Up Progress

CRONOGRAMA 3 - 3

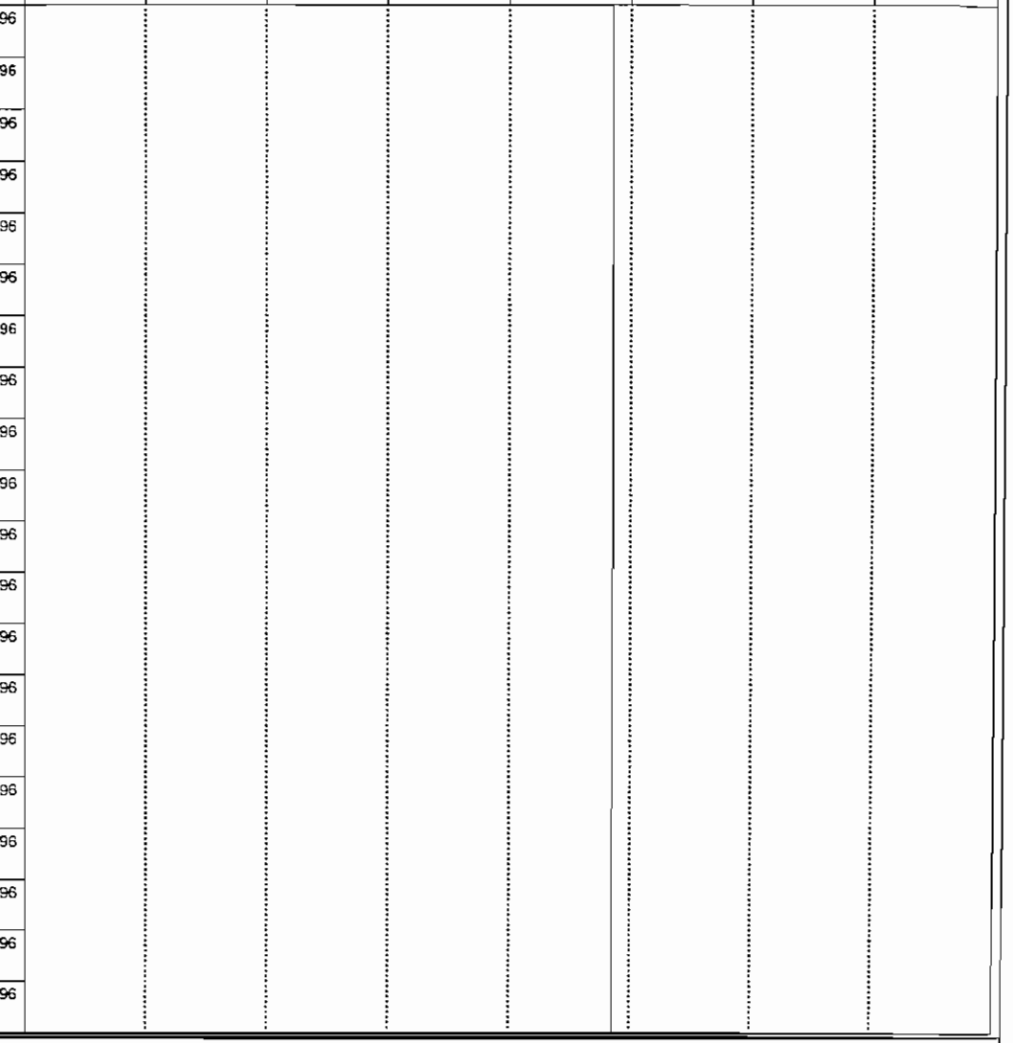


PROYECTO : RED INVESPLAN
ANGEL CHINCHERO VILLACIS
Date: Sat 12/07/97

Task
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Milestone
Rolled Up Progress

CRONOGRAMA 3 - 4

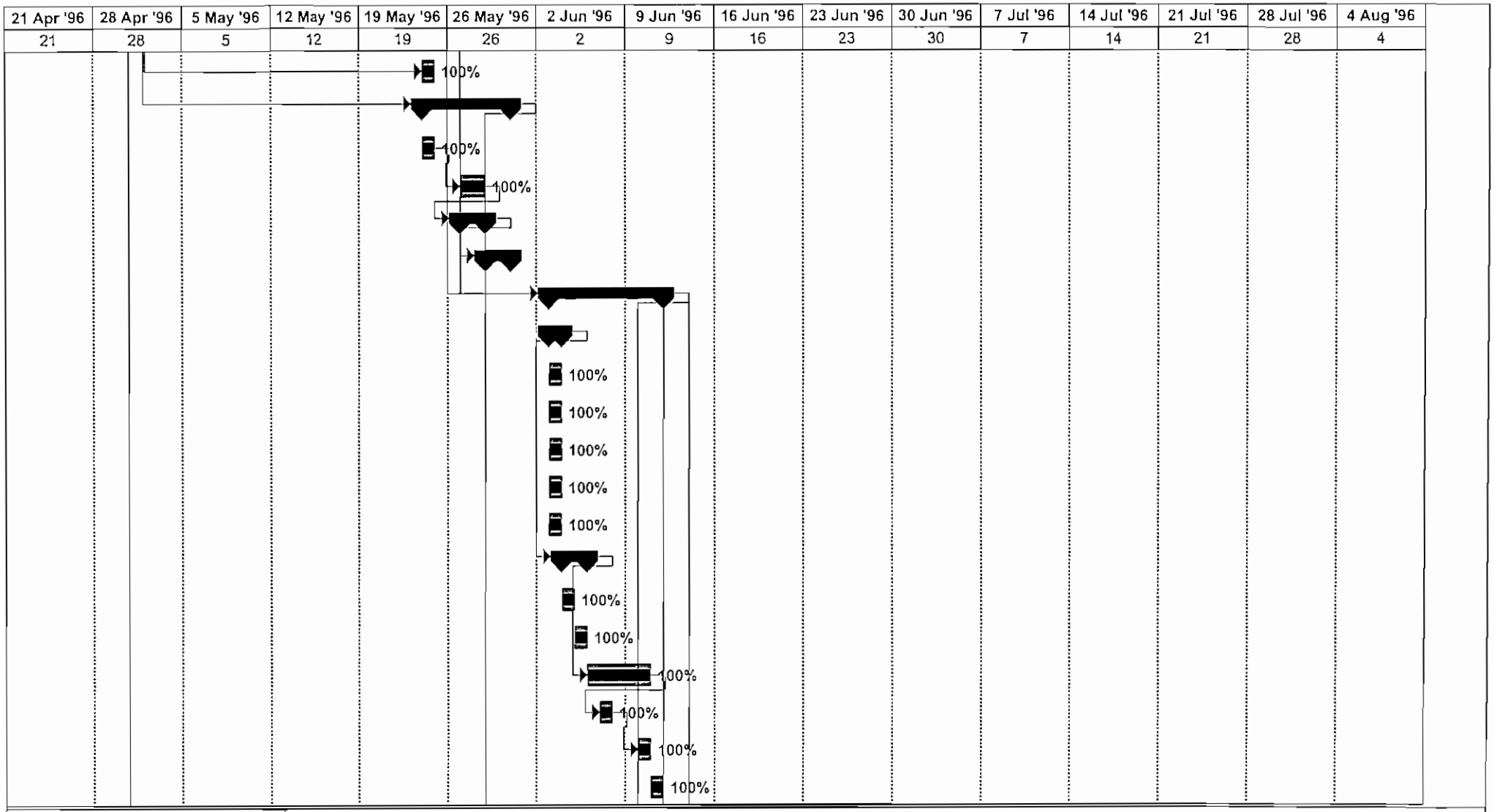
ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN
41	Instalación y pruebas en Agencias	1d	Fri 24/05/96	Fri 24/05/96
42	Implementación de la red de datos en MATRIZ	5d	Fri 24/05/96	Thu 30/05/96
43	Instalación de Servidor UNIX de PRODUCCION	1d	Fri 24/05/96	Fri 24/05/96
44	Instalación de Aplicaciones Bancarias en el Servidor UNIX	2d	Mon 27/05/96	Tue 28/05/96
45	Configuración e Instalación de Servidores NT	2d	Mon 27/05/96	Tue 28/05/96
52	Configuración e Instalación de Usuarios de red	2d	Wed 29/05/96	Thu 30/05/96
55	Instalación de red de datos en AGENCIAS	7d	Mon 3/06/96	Tue 11/06/96
56	Configuración de Servidores NT en Laboratorio	1d	Mon 3/06/96	Mon 3/06/96
57	Servidores de AGENCIAS	1d	Mon 3/06/96	Mon 3/06/96
58	Servidor de IMAGENES	1d	Mon 3/06/96	Mon 3/06/96
59	Servidor de Correo Electrónico	1d	Mon 3/06/96	Mon 3/06/96
60	Servidor de Servicio de Acceso Remoto RAS	1d	Mon 3/06/96	Mon 3/06/96
61	Servidor DHCP , WINS y de Impresión	1d	Mon 3/06/96	Mon 3/06/96
62	Configuración de Usuarios de AGENCIAS	2d	Tue 4/06/96	Wed 5/06/96
63	Terminales Financieras	1d	Tue 4/06/96	Tue 4/06/96
64	Terminales Administrativas	1d	Wed 5/06/96	Wed 5/06/96
65	Pruebas de comunicación con las Agencias Simuladas en Laboratorio	3d	Thu 6/06/96	Mon 10/06/96
66	Traslado de equipos probados a las Agencias	1d	Fri 7/06/96	Fri 7/06/96
67	Instalación de equipos en los puntos de red	1d	Mon 10/06/96	Mon 10/06/96
68	Pruebas de red local y extendida en las Agencias	1d	Tue 11/06/96	Tue 11/06/96



PROYECTO : RED INVESPLAN
ANGEL CHINCHERO VILLACIS
Date: Sat 12/07/97

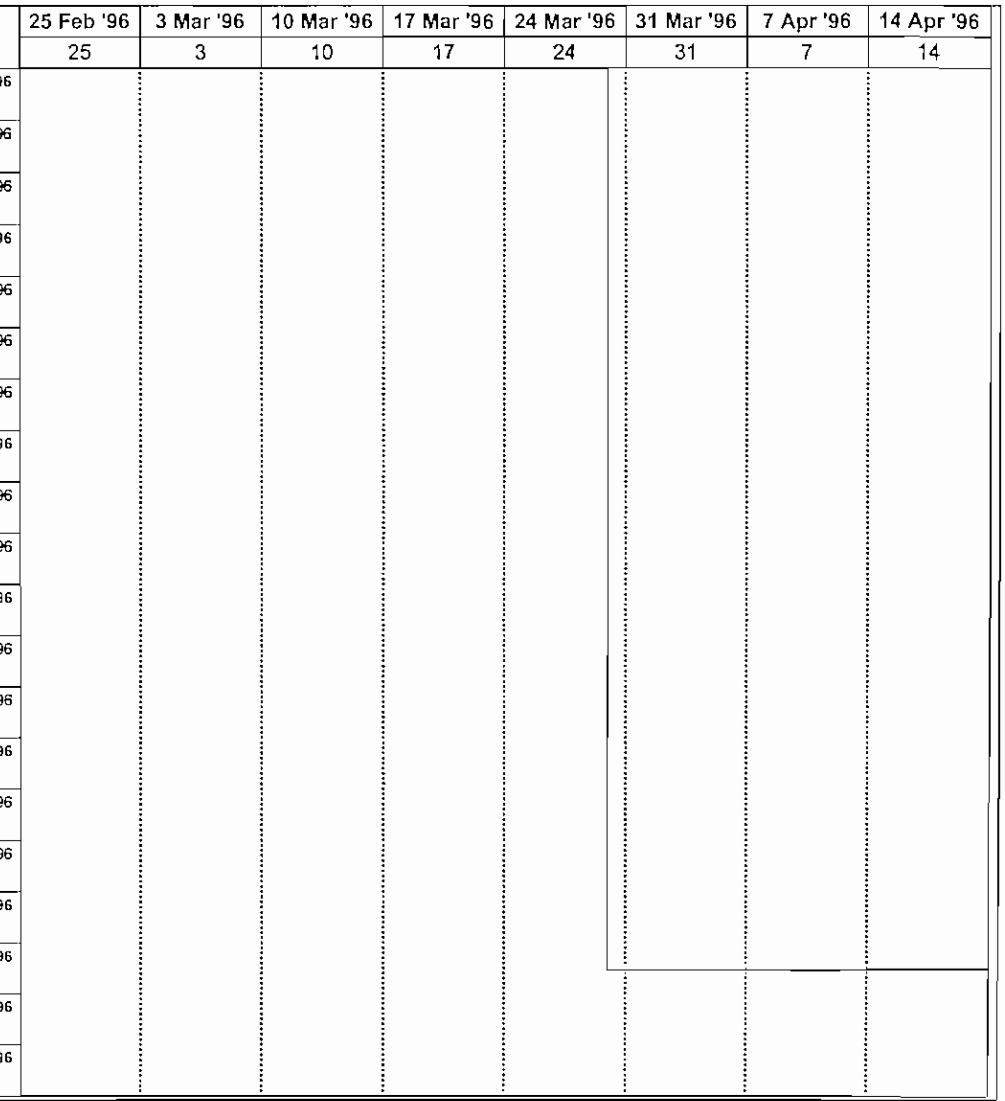
Task
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Milestone
Rolled Up Progress

CRONOGRAMA 3 - 5



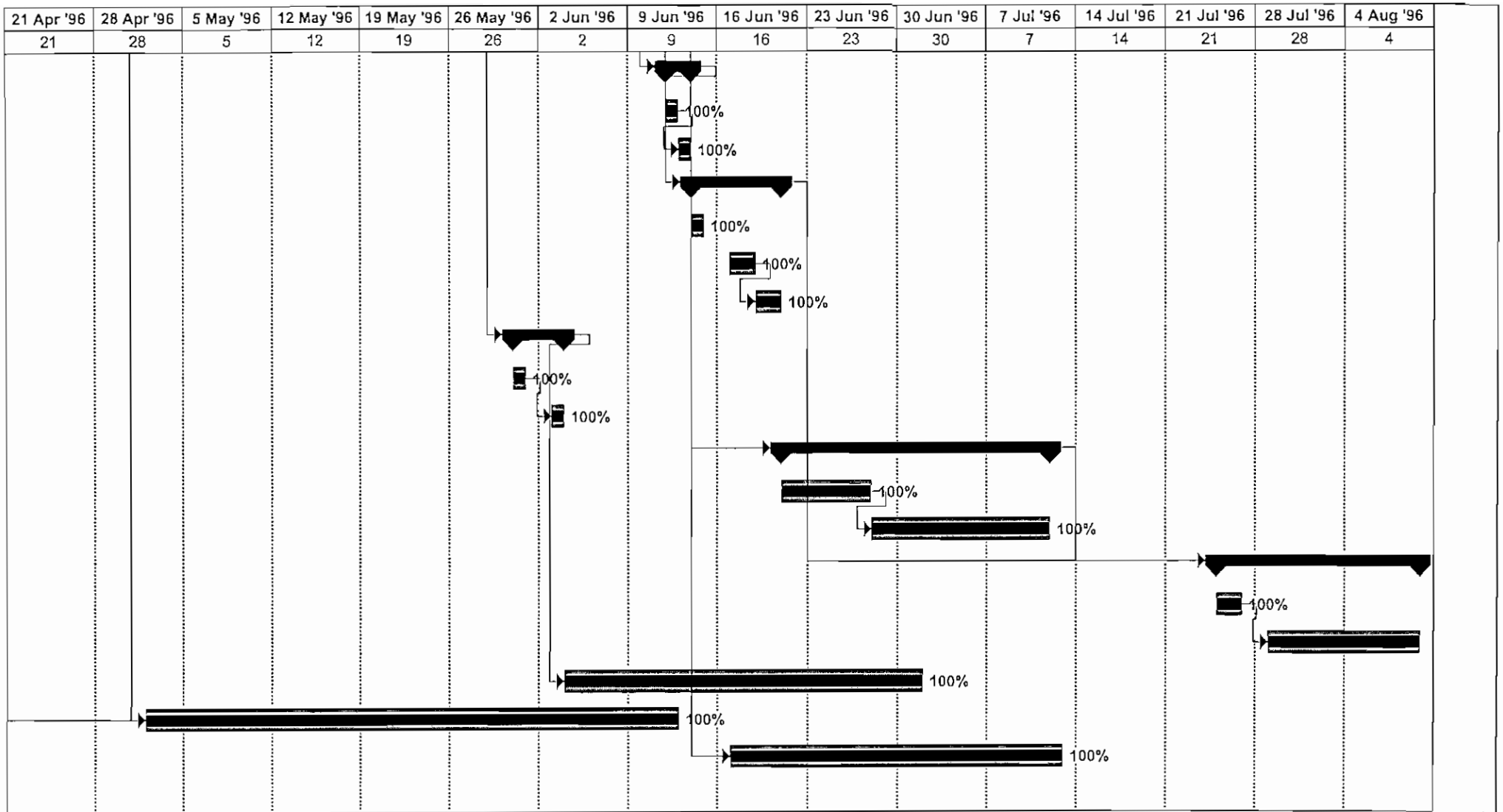
CRONOGRAMA 3 - 6

ID	NOMBRE DE LA TAREA	DURACION	INICIO	FIN
69	Pruebas de enlaces de red Extendida	2d	Wed 12/06/96	Thu 13/06/96
70	Comunicación entre los Servidores NT y Servidores UNIX	1d	Wed 12/06/96	Wed 12/06/96
71	Comunicación entre usuarios locales y remotos	1d	Thu 13/06/96	Thu 13/06/96
72	Monitoreo de red LAN y WAN desde MATRIZ	5d	Fri 14/06/96	Thu 20/06/96
73	Instalación de Software de Monitoreo	1d	Fri 14/06/96	Fri 14/06/96
74	Monitoreo de red LAN Ethernet	2d	Mon 17/06/96	Tue 18/06/96
75	Monitoreo de red WAN	2d	Wed 19/06/96	Thu 20/06/96
76	Instalación de equipos adicionales	2d	Fri 31/05/96	Mon 3/06/96
77	Clasificadora de cheques	1d	Fri 31/05/96	Fri 31/05/96
78	Arreglo de discos	1d	Mon 3/06/96	Mon 3/06/96
79	Actualización de Hardware y Software	15d	Fri 21/06/96	Thu 11/07/96
80	Actualización en Servidores	5d	Fri 21/06/96	Thu 27/06/96
81	Actualización en Usuarios	10d	Fri 28/06/96	Thu 11/07/96
82	Afinamiento de la red	12d	Thu 25/07/96	Fri 9/08/96
83	Afinamiento de comunicaciones	2d	Thu 25/07/96	Fri 26/07/96
84	Afinamiento de Sistemas Operativos en Servidores y Usuarios	10d	Mon 29/07/96	Fri 9/08/96
85	Afinamiento de Aplicaciones	20d	Tue 4/06/96	Mon 1/07/96
86	Entrenamiento al personal del BANCO	30d	Thu 2/05/96	Wed 12/06/96
87	Elaboración de manual de RED DE DATOS del BANCO	20d	Mon 17/06/96	Fri 12/07/96
88	Elaboración de manual respaldos y contingencias	10d	Mon 17/06/96	Fri 28/06/96



PROYECTO : RED INVESPLAN
ANGEL CHINCHERO VILLACIS
Date: Sat 12/07/97

Task
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Milestone
Rolled Up Progress



CRONOGRAMA 3 - 8