105

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

"ADMINISTRACIÓN DE REDES ATM".

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A N:

HUGO D. VALERIANO ROBLES
CARLOS ZUGASTI CRUZ

ASESOR:
ING. DAVID B. ESTOPIER BERMÚDEZ

MÉXICO, 2002.

Gracias

a DIOS,

a mi familia que siempre me han apoyado a realizar mis sueños y a la Familia Tapia

a la ENEP Aragón y a la DGSCA por la formación profesional que me brindaron

a todas las personas que me ayudaron a realizar este trabajo, los Ingenieros. Roberto Rodríguez, Esteban Rodríguez, Horacio Bocanegra, Javier Domínguez entre otros

al Ing. David Estopier por que nos ha servido de ejemplo con todas sus enseñanzas a ser unos excelentes ingenieros y por todo el apoyo brindado para esta tesis

a mi compañero de tesis y amigo de siempre, Hugo, por todo lo que hemos convivido

a mis amigos Raúl Gutiérrez Solis, Bernardo, Francisco, Ricardo

en fin a todos aquellos que de alguna manera pusieron su granito de arena

y en especial a la Ing. Irene Pérez que gracias a su cariño y compresión me ha dado la inspiración y el impulso que faltaba para poder concluir esta tesis entre otros muchos logros.

Gracias

a DIOS,

a mis Padres,

a mi familia por su apoyo, cariño y comprensión en todo momento,

a todos mis amigos que me han apoyado en mi carrera profesional y en lo personal (Horacio, Ricardo, Esteban, Ernesto, Javier, Arturo, etc.),

a la ENEP Aragón, a la UNAM, a la DGSCA y a la vida por la formación que me han dado,

al Ing. David B. Estopier Bermúdez por todo lo que hemos aprendido de él, su apoyo para hacer posible el presente trabajo y por lo que ha significado en nuestra vida, un ejemplo,

al Ing. Raúl Gutiérrez Martínez por su amistad y apoyo brindado,

a mi compañero de tesis y amigo de siempre, Carlos, por todo lo que hemos convivido,

en especial a Verónica por su apoyo que me ayudo a culminar esta tesis

A todos gracias por ser parte de este y muchos otros logros.

TESIS ADMINISTRACION DE REDES ATM

INDICE

INTRODUCCION

Hoy en día como la velocidad y el número de las redes de área local (LANs) continúa su crecimiento implacable, ha aumentado la demanda de las redes de conmutación para apoyar el rendimiento de procesamiento generado por estas LANs y su interconexión. En los primeros días del establecimiento de una red de área ancha o WAN, el X.25 entre otros fue diseñado para apoyar la conexión directa de las largas distancias de las terminales y de las computadoras (hoy en día se sigue utilizando). Al usar desde 64 Kbps, el X.25 hacía frente bien a esas demandas en los años 80's. Las LANs ha venido desempeñar un papel de aumento en el ambiente local , sin embargo, X.25 como otras tecnologías heredadas, han decaido en su uso, y el acceso se fue acelerando por encima de 2 Mbps. Día a día con el incremento de usuarios conectados a red como es el caso de Internet , los requerimientos de ancho de banda se hacen cada día mayores. Para acomodar estos requisitos enormes, han surgido diferentes tecnologías para transporte WAN ,una de ellas es ATM: Asynchronous Transfer Mode (Modo de Transferencia Asíncrona).

Esta tecnología esta básada en la conmutación de celdas de tamaño fijo y puede transportar voz, datos o video la que la hace versatil brindando calidad de servicio QoS . Utiliza fibra óptica y se maneja a velocidades de 155 Mbits por segundo y mas arriba, entre otras características, el unico inconveniente de utilizar redes de este tipo es el costo y puede ser la complejidad también dependiendo de como se construya la red, ya que una red Frame Relay por ejemplo provee características semejantes al poder transportar voz, datos o video de manera mas económica que ATM y puede resultar también eficiente.

CAPITULO 1 CONCEPTOS DE COMUNICACIONES.

1.1 SEÑALES EN SISTEMAS DE COMUNICACIÓN

En un sistema de comunicación la información es propagada de un punto a otro por medio de señales eléctricas o electromagnéticas. La exitosa transmisión de la información depende principalmente de dos factores: la calidad de la señal a ser transmitida y las características, del medio. Un medio de transmisión es el camino físico entre el transmisor y el receptor. Hay dos tipos de medios de transmisión, los guiados (cable, fibra óptica, etc.) y los no guiados (microondas). Estas señales pueden ser de tipo analógico o digital. Una señal analógica es aquella que es continua en el tiempo. Una señal digital es una secuencia de pulsos de voltaje. Los valores que puede tomar la señal digital son: 1 y 0. Generalmente la información analógica esta en función del tiempo y ocupa un espectro limitado de frecuencia, tal información puede ser representada en forma de señales electromagnéticas ocupando el mismo espectro. La información digital también puede ser representada por señales analógicas usando un módem. El módem (modulador/demodulador) convierte las señales digitales en forma de señales analógicas codificando la información digital dentro de una portadora de frecuencia. La señal resultante ocupa un cierto espectro de frecuencia sobre la portadora y así puede ser transmitida a través del medio de transmisión optimo para esa portadora. En el lado del receptor el módem demodula la señal para recobrar la información original. De forma similar la información analógica puede ser representada digitalmente. El dispositivo que hace esto se conoce como codec (coder-decoder). Este toma la señal analógica y la representa por una ráfaga de bits.

Existen cuatro formas diferentes de codificación con relación a la información y al tipo de señal empleada. Las razones para emplear cualquiera de ellas dependen del uso que se les dé:

- La información digital y señales digitales.- en general, el equipo para codificar la información digital dentro de una señal digital es menos complejo y menos caro que los equipos de modulación digital-analógico.

- La información analógica y señales digitales -. La conversión de la información analógica a una forma digital permite el uso de una transmisión digital y equipo de conmutación.

- La información digital y señales analógicas.- algunos medios de transmisión, tales como fibras ópticas y medios no guiados, utilizan solo propagación de señales analógicas.

- La información analógica y señales analógicas.- la información analógica en forma eléctrica puede ser transmitida fácilmente como señales de banda base y en forma barata. Por ejemplo la transmisión de voz. Un uso común de la modulación es para cambiar el ancho de banda de señales de banda base a otra porción del espectro y así poder compartir el mismo medio de transmisión, esto es conocido como multiplexión por división de tiempo que veremos más adelante.

1.2 CODIGOS DE LINEA:

Una señal digital es una secuencia de pulsos de voltaje discontinuos en el tiempo. Cada pulso es un elemento de señal. La información binaria es transmitida por codificación de cada bit dentro de los elementos de señal. En un caso simple hay una correspondencia de uno a uno entre los bits y los elementos de señal. Un ejemplo de esto es un 0 binario representado por un nivel de voltaje bajo y un 1 representado por un voltaje alto. Esta es una forma de representar los valores binarios y se conoce como código de línea.

Dentro de lo que es un código de línea intervienen varias definiciones. Si todos los elementos de señal tienen el mismo signo algebraico, esto es todos positivos o todos negativos, entonces la señal es unipolar. En una señal polar, un estado lógico es representado por un nivel de voltaje positivo y el otro por un nivel de voltaje negativo. La velocidad de la información de una señal es la velocidad en bit por segundo en que la información es transmitida. La longitud o duración de un bit es la cantidad de tiempo que toma el transmisor para emitir el bit. La velocidad de modulación en contraste es la velocidad en la cual el nivel de la señal es cambiado, esto dependerá del código de línea a emplear. La velocidad de modulación es expresada en bauds lo que significa un elemento de señal por segundo.

El uso de señales digitales puede ser menos costoso y bajo ciertas circunstancias provee una mejor utilización que las señales analógicas. Consideraremos cuatro familias de técnicas de codificación: NRZ, códigos binarios multinivel, códigos bifase y los que utilizan bits de relleno.

1.2.1 CÓDIGOS NO RETORNO A CERO (NON RETURN-TO-ZERO):

En estos códigos se utilizan dos diferentes niveles de voltaje, uno positivo y otro negativo, son usados como elementos de señal para los dos dígitos binarios. El nombre se refiere al hecho que el nivel de voltaje nunca retorna al valor de cero, pero este siempre es positivo o negativo. Estos códigos son los más comunes y los de más fácil forma para transmitir señales digitales. Sin embargo el uso de estos códigos no es apropiado para emplearse en redes de área local.

1.2.1.1 CÓDIGO NO RETORNO A CERO NIVEL (NRZ-LEVEL):

Este código utiliza un voltaje negativo constante para representar un 1 binario y un voltaje positivo constante para representar un cero binario. Este código es a menudo usado para conexiones muy cortas, tales como entre una terminal y un módem o una terminal y una computadora cercana.

1.2.1.2 CÓDIGO NO RETORNO A CERO INVERTIDO (NRZ, INVERT ON ONES)

Este código es otra variación del código NRZ. Así como el NRZ-L, el NRZI mantiene un pulso constante de voltaje para la duración de un tiempo de bit. La información misma es codificada como la presencia o ausencia de una transición de señal al principio del tiempo del bit. Una transición (de bajo a alto o viceversa) en el principio de la duración del bit denota un 1 binario para esa duración del bit, la no-transición indica un 0 binario.

Este tipo de código de línea es un ejemplo de codificación diferencial. En la codificación diferencial la señal es decodificada comparando la polaridad del elemento de señal adyacente y no es determinado por el valor absoluto de un elemento de señal. Un beneficio de este esquema es que puede ser más confiable para detectar una transición en presencia de ruido que para comparar un valor de un umbral. Otro beneficio es que al disponer de una transmisión compleja, es fácil perder el sentido de polaridad de la señal. Por ejemplo en un medio de transmisión de par torcido, si la punta de un dispositivo conectado es accidentalmente invertida, todos los 1's y 0's se invertirán. Esto no puede suceder con una codificación diferencial.

Existen diversas desventajas para la utilización de códigos NRZ. Una de ellas es la dificultad para determinar donde acaba un bit y empieza el otro. Por ejemplo considerando una larga cadena de 1's o 0's para NRZ-L, la salida es un voltaje constante sobre un largo período de tiempo. Bajo estas circunstancias cualquier variación de tiempo entre el transmisor y el receptor resultara perdida de la sincronización. Además hay una componente de cd durante cada tiempo de bit que puede acumularse si predominan pulsos positivos o negativos continuos.

1.2.2 CÓDIGOS BINARIOS MULTINIVEL

Este tipo de códigos cubre algunas deficiencias de los códigos NRZ. Estos códigos usan más de dos niveles de señal. Dos ejemplos de estos son el Bipolar-AMI y el Pseudoternario.

1.2.2.1 BIPOLAR-AMI (ALTERNATE MARK INVERTION)

En este tipo de código un 0 binario es representado por la ausencia de una señal lineal, y un 1 binario es representado por un pulso positivo o negativo. El pulso del 1 binario debe ser alternado en polaridad. Hay varias ventajas en este método. Primero no habrá perdida de sincronización si ocurre una larga cadena de unos. Cada uno introduce una transición. Una larga cadena de 0's seguiría siendo un problema. Segundo al alternar en polaridad los 1's de positivo a negativo no hay componente de cd. También el ancho de banda de la señal resultante es considerablemente menor que el del código NRZ. Finalmente al alternar pulsos se provee un medio simple de detección de errores. Cualquier error aislado, si se borra o añade un pulso causa una violación a esta propiedad.

1.2.2.2 PSEUDOTERNARIO

Esta técnica es igual a la anterior, con la diferencia que el 1 binario es representado por la ausencia de una señal lineal y el 0 por la alternación de los pulsos positivos y negativos. No hay una ventaja en particular de esta técnica y la anterior.

Como se mencionó anteriormente una cadena de 0's consecutivos en el código anterior o una cadena de 1's consecutivos en este presenta un problema. Algunas técnicas han solventado este problema mediante la

inserción de bits adicionales que forcen hacer transiciones. Al hacer esto para altas velocidades resulta costoso, para resolver esto se utilizan códigos de línea que utilizan bits de relleno o" scrambling".

1.2.3 CODIGOS BIFASE

Estos códigos son otra alternativa, la cual sobrepone algunas limitaciones de los códigos NRZ, dos de estas técnicas son: los códigos Manchester y Manchester Diferencial.

1.2.3.1 CÓDIGO MANCHESTER

Este es un código bifase que resuelve algunos de los inconvenientes anteriores. Este código requiere de al menos una transición por tiempo de bit y puede tener un máximo de 2 transiciones continuas. Así la razón de modulación máxima es el doble que en NRZ, esto significa que el ancho de banda o capacidad de transmisión requerida es mayor. Para compensar esto, los códigos bifase tienen varias ventajas:

* Sincronización: Porque hay una transición predecible durante cada tiempo de bit, el receptor se puede sincronizar en esa transición.
No hay componente de cd: Debido a que hay una transición en cada tiempo de bit, los códigos bifase no tienen componentes de cd.

* Detección de errores: La ausencia de una transición esperada puede ser usada para detectar errores. El ruido en la línea puede invertir ambas transiciones la anterior y la siguiente a la transición esperada y así causar un error indetectable.

En el código Manchester existe una transición a la mitad de cada periodo de bit. La transición del medio bit sirve como un reloj y como información, una transición de nivel bajo a nivel alto representa un 1, en el caso contrario de nivel alto a nivel bajo representa un 0.

1.2.3.2 CÓDIGO MANCHESTER DIFERENCIAL

Este código es similar al anterior pero la transición del medio bit solamente se usa para proveer un reloj. La codificación de un 0 es representada por la presencia de una transición en el comienzo de un periodo de bit. Este código tiene la ventaja que es una técnica de codificación diferencial. En la figura 1.1 se observan las diferentes formas de codificación mencionadas anteriormente.

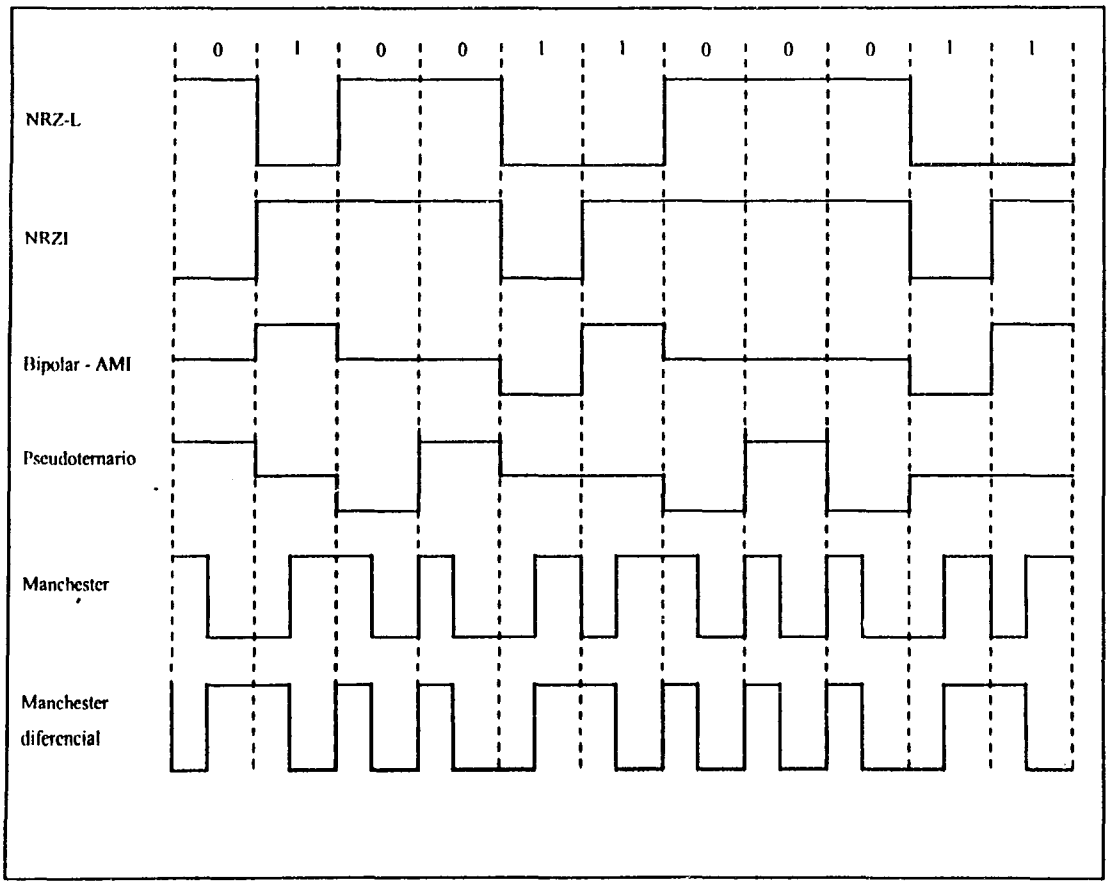


FIGURA 1.1 CODIGOS DE LINEA

1.2.4 CODIGOS QUE UTILIZAN BITS DE RELLENO

Aunque las técnicas bifase tienen un gran uso en redes de área local en aplicaciones a velocidades relativamente altas (arriba de 10 Mbps), estas no han sido ampliamente usadas en aplicaciones con grandes distancias. La principal razón de esto es que se requiere una alta velocidad de señalización relativa a la velocidad de la información. Hacer esto es más costoso en aplicaciones de larga distancia.

Otro método para hacer esto es usando los códigos que utilizan bits de relleno. La idea de este método es simple: secuencias que resultarían en un constante nivel de voltaje en la línea son remplazados por secuencias de relleno que proveerán suficientes transiciones para que el reloj del receptor se mantenga sincronizado. La secuencia de relleno debe ser reconocida por el receptor y reemplazada con la secuencia original de datos. La secuencia de relleno es de la misma longitud de la secuencia original, así no se incrementa la velocidad de los datos. Las metas de diseño para esto se resumen como sigue:

- no hay componente de cd
- no hay secuencias largas de señales de nivel cero
- no hay reducción en velocidad de información
- es capaz de detectar errores

Dos técnicas usadas en transmisiones de larga distancia son el *BIPOLAR WITH 8-ZEROS SUBSTITUTION (B8ZS) y el HIGH-DENSITY BIPOLAR-3 ZEROS (HDB3).*

1.2.4.1 BIPOLAR WITH 8-ZEROS SUBSTITUTION (B8ZS)

Esta codificación esta basada sobre bipolar-AMI, en este código una larga cadena de ceros puede hacer que se pierda la sincronización, para evitar esto sigue las siguientes reglas:

- Si en un octeto de todos ceros ocurre y él ultima pulso de voltaje del octeto anterior fue positivo, entonces los 8 ceros del octeto son codificados como 0 0 0 + - 0 - +.

- Si en un octeto de todos ceros ocurre y él ultimo pulso de voltaje del octeto anterior fue negativo, entonces los 8 ceros del octeto son codificados como 0 0 0 - + 0 + -.

Esta técnica forza a dos violaciones de código AMI.

1.2.4.2 HIGH-DENSITY BIPOLAR-3 ZEROS (HDB3).

Este código también esta basado en el código AMI. En este caso las cadenas de 4 ceros consecutivos son remplazadas con secuencias conteniendo uno o dos pulsos. En cada caso el cuarto cero es reemplazado por una violación. En adición, una regla es necesitada para asegurar que las sucesivas violaciones son de polaridad alternada y así no se introduce una componente de cd. Así, si la ultima violación fue positiva, esta violación será negativa y viceversa. La tabla 1.1 muestra las reglas de substitución para este código.

TABLA 1.1

Reglas de sustitución de HDB3

polaridad del pulso precedido	# de pulsos bipolares(1s) desde la ultima sustitución	
	par	impar
-	000-	+00+
+	000+	-00-

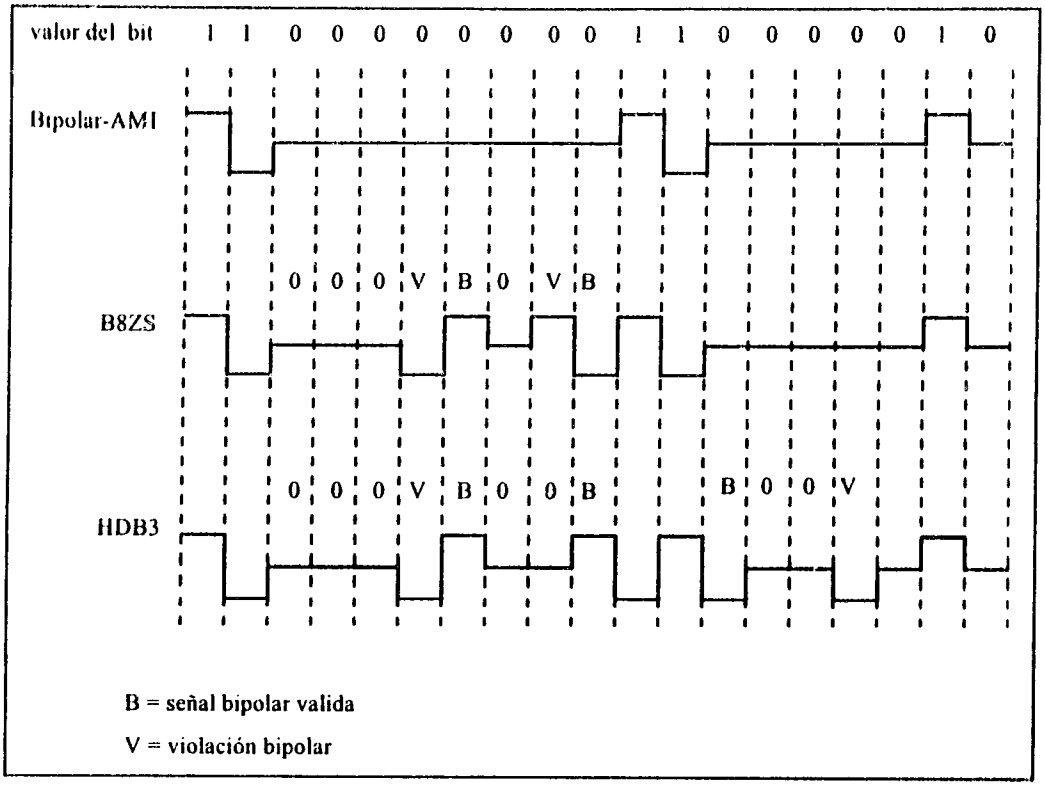


FIGURA 1.2 CODIGOS B8ZS Y HDB3

1.3 TRANSMISION DE INFORMACION DIGITAL

Para dos dispositivos enlazados por un medio de transmisión para intercambiar información, un alto grado de cooperación es requerido. Típicamente la información es transmitida un bit a la vez sobre el medio. El tiempo (velocidad, duración, espacio) de esos bits debe ser el mismo para el transmisor y el receptor. Dos técnicas comunes son asíncrona y síncrona. La transmisión de la información puede ser de dos formas serie y paralelo. La mas comúnmente usada es la serie por usar una sola línea en cambio que la transmisión en paralelo se requieren varias líneas lo que resulta costoso, esta forma se utiliza en dispositivos de I/O y en señales internas en una computadora. En una transmisión en serie los elementos de señal son enviados a través de la línea uno a la vez. Cada elemento de señal debe ser:

- Menor que un bit: por ejemplo en el código Manchester.
- Un bit: como en NRZ-L (digital) y FSK (analógico).
- Mas de un bit: como en QPSK (Quadrature Phase Shift Keying).

La sincronización es un elemento importante en las comunicaciones. El transmisor envía un bit de inicio a través del medio hacia el receptor. El receptor debe reconocer el principio y el final de un bloque de bits. Debe conocer también la duración de cada bit y así tomar el tiempo correspondiente para leer cada bit.

1.3.1 TRANSMISION ASINCRONA.

En esta transmisión la forma de sincronizar es discontinua, es decir, no se necesita una ráfaga constante de bits para sincronizar, la información es transmitida un carácter a la vez, donde cada carácter es de cinco a ocho bits de longitud. La sincronización es establecida y mantenida dentro de cada carácter, el receptor tiene la oportunidad de resincronizar al principio de cada carácter. Esto se muestra en la figura 1.3 a.

Cuando ningún carácter esta siendo transmitido la línea entre el transmisor y el receptor esta en un estado de espera "idle" (es decir se puede mantener con elementos de señal en 1). El empiezo de un carácter es señalado por un bit de inicio con un valor binario de cero. A este le siguen de cinco a ocho bits que completan al carácter. Los bits del carácter son transmitidos comenzando con el bit menos significante. El elemento final del carácter es un bit de parada el cual es un 1 binario. La longitud mínima para el bit de parada es usualmente de 1 a 2 tiempos de la duración ordinaria de un bit. No hay un valor máximo especificado. Cuando no hay mas caracteres a enviar en transmisor continuamente envía bits de parada "stop bit" (que son los mismos que los del estado en espera mencionado anteriormente) hasta que se envíe un nuevo bit de inicio "start bit". Figura 1.3 b.

Si una trama fija de caracteres es enviada, el intervalo entre dos caracteres es uniforme e igual al elemento de parada. Por ejemplo si el bit de

parada tiene una unidad de longitud y los caracteres ASCII A, B y C son enviados (sin bit de paridad) el patrón de bits es 0<u>1000001</u>1<u>0</u>0<u>1000001</u>1<u>0</u>1<u>1000001</u>111, el bit de inicio, empieza la secuencia de conteo para los próximos ocho elementos, los cuales son los del código ASCII de 7 bit y el bit de parada. En el estado de espera el receptor observa la transición de 1 a 0 para empezar el próximo carácter y entonces se muestrea la señal entrante a intervalos de un bit por 7 intervalos. Entonces se observa para la próxima transición de 1 a 0 la cual no ocurrirá en menos de un tiempo de bit.

Los requerimientos de tiempo son limitados. Por ejemplo, los caracteres ASCII son típicamente enviados como unidades de 8 bits, incluyendo el bit de paridad. Si el receptor es un 5% mas lento o más rápido que el transmisor, el muestreo de la octava información de bit será desplazada un 45% y aun así será correctamente muestreada. En la figura 1.3c se muestran los efectos de un error de tiempo de suficiente magnitud para causar un error en la recepción. En este ejemplo asumiremos una velocidad de 10 kbps, así cada bit tiene una duración de 0.1 miliseg. Asumimos que el receptor esta afuera por 7% o 7 microseg por bit de tiempo. Así el muestreo del receptor para el carácter entrante será de 93 microsegs (basado en el reloj del transmisor). Como se vio él ultimo muestreo es erróneo. Un error tal como este daría como resultado 2 errores. Primero él ultimo bit muestreado es incorrectamente recibido. Segundo, el conteo de bits puede estar ahora fuera de alineación. Si el bit 7 es un 1 y el bit 8 es un 0, el bit 8 podría ser confundido con el bit de inicio. A esta condición se le llama error de trama, un error de trama puede también ocurrir si el ruido causa una falsa apariencia de bit de inicio durante el estado de espera.

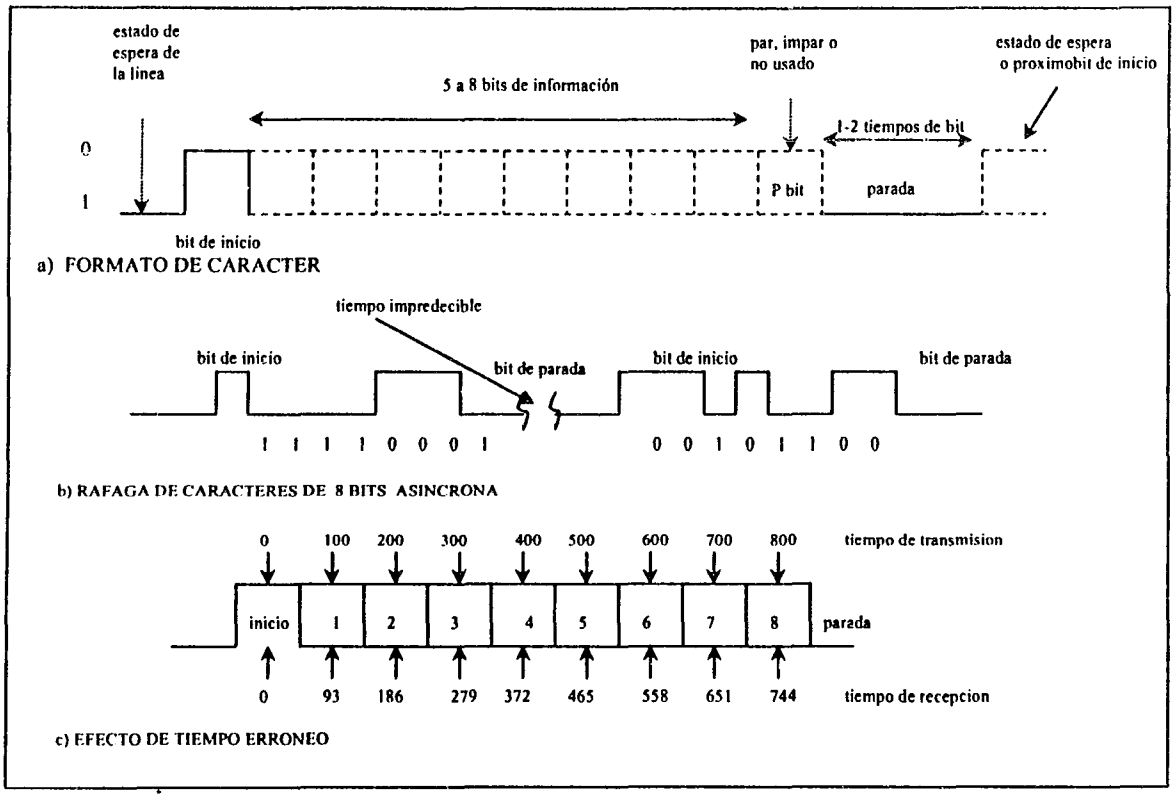


FIGURA 1.3 TRANSMISION ASINCRONA

La comunicación asíncrona es simple y barata pero requiere un sobreencabezado "overhead" de 2 a 3 bits por carácter. Por ejemplo para un código de 7 bits usando un bit de parada, 2 de 9 bit no llevan información pero son solamente para sincronización, así el sobreencabezado es de 2/9 = 0.22. Seguramente el porcentaje del sobreencabezado pudiera ser reducido mandando bloques grandes de bits entre los bits de inicio y de parada (largo de la trama). Sin embargo para usar un bloque grande de bits exitosamente se utiliza otra forma de sincronización, la síncrona.

1.3.2 TRANSMISION SINCRONA.

En este tipo de transmisión, bloques de caracteres o bits son transmitidos sin bits de inicio y de parada, y el tiempo de llegada de cada bit es predecible. Para evitar un diferencia de tiempo entre el transmisor y receptor, sus relojes de alguna forma deben estar sincronizados. Una posibilidad es proveer un reloj separado para cada uno. De otra forma, la información de reloj debe de estar dentro de la señal de información. Para señales digitales se puede utilizar códigos bifase, para señales analógicas dentro de la misma portadora de frecuencia puede sincronizar al receptor basado él la fase de la portadora.

Con la transmisión síncrona, hay otro nivel de sincronización requerido, para permitir al receptor determinar el comienzo y el fin de un bloque de información. Para lograr esto cada bloque comienza con un patrón de bits denominado preámbulo y finaliza con un patrón denominado " postamble". La información más el preámbulo y el postamble son llamados trama. La naturaleza del preámbulo y el postamble dependen si el bloque de información es orientado a carácter u orientado a bits.

Con la transmisión orientada a caracteres, el bloque de información es tratado como una secuencia de caracteres. Todo el control de la información es en forma de caracteres. La trama comienza con uno o más caracteres de sincronización usualmente llamados SYNC, y que es un patrón único de señales que el receptor reconoce como el principio de una trama. El postamble es otro carácter único. El receptor así es alertado para la entrada de una trama por los caracteres SYNC y acepta la información hasta que reconoce al postamble. Entonces el receptor esta en espera de otro SYNC. Alternativamente otra forma es para incluir la longitud de trama como parte de la información de control. El receptor entonces busca un carácter SYNC y determina la longitud de la trama, lee el número de caracteres y entonces busca por el próximo SYNC para empezar la próxima trama. Ver figura 1.4 a.

Con la transmisión orientada a bits, los bloques de información son tratados como una secuencia de bits. Ni la información de control necesita ser interpretada en unidades de ocho caracteres. Con los esquemas orientados a carácter, un patrón de bits especial comienza un bloque. En la transmisión orientada a bits, este preámbulo es de 8 bits de longitud y se le conoce como bandera. La misma bandera es también usada como un postamble. El receptor mira el patrón de la bandera y esta le indica que la trama comienza. Esto es seguido por algún campo con un número de control, un campo de longitud variable de información, más campo de control y finalmente la bandera se repite. La diferencia entre este método y orientado a carácter depende del formato y la interpretación de la información de control. Como se muestra en la figura 1.4 b.

Para bloques de longitud variable, la transmisión síncrona es más eficiente que la asíncrona. La transmisión asíncrona requiere de un encabezado 20% o más grande. El control de información en la transmisión síncrona es típicamente menor de 100 bits. Por ejemplo uno de los esquemas más comunes orientado a bits el HDLC utiliza 48 bits de información de control (incluyendo banderas), así para un mensaje de 1000 bits, el encabezado es de solo 48/1048 x 100% = 4.6%. Un ejemplo de bandera de HDLC es 01111110, este patrón de bits una vez concluida la bandera de inicio se puede repetir en los datos del resto de la trama lo que podría significar que la trama termina o perder sincronización, para evitar esto siempre se inserta un 0 después de cinco 1's consecutivos en los datos a ser transmitidos. Cuando el receptor detecta una secuencia de cinco 1's examina el sexto bit, si este es 0 el receptor lo borra. A este procedimiento se le conoce como relleno de bits "bits stuffing".

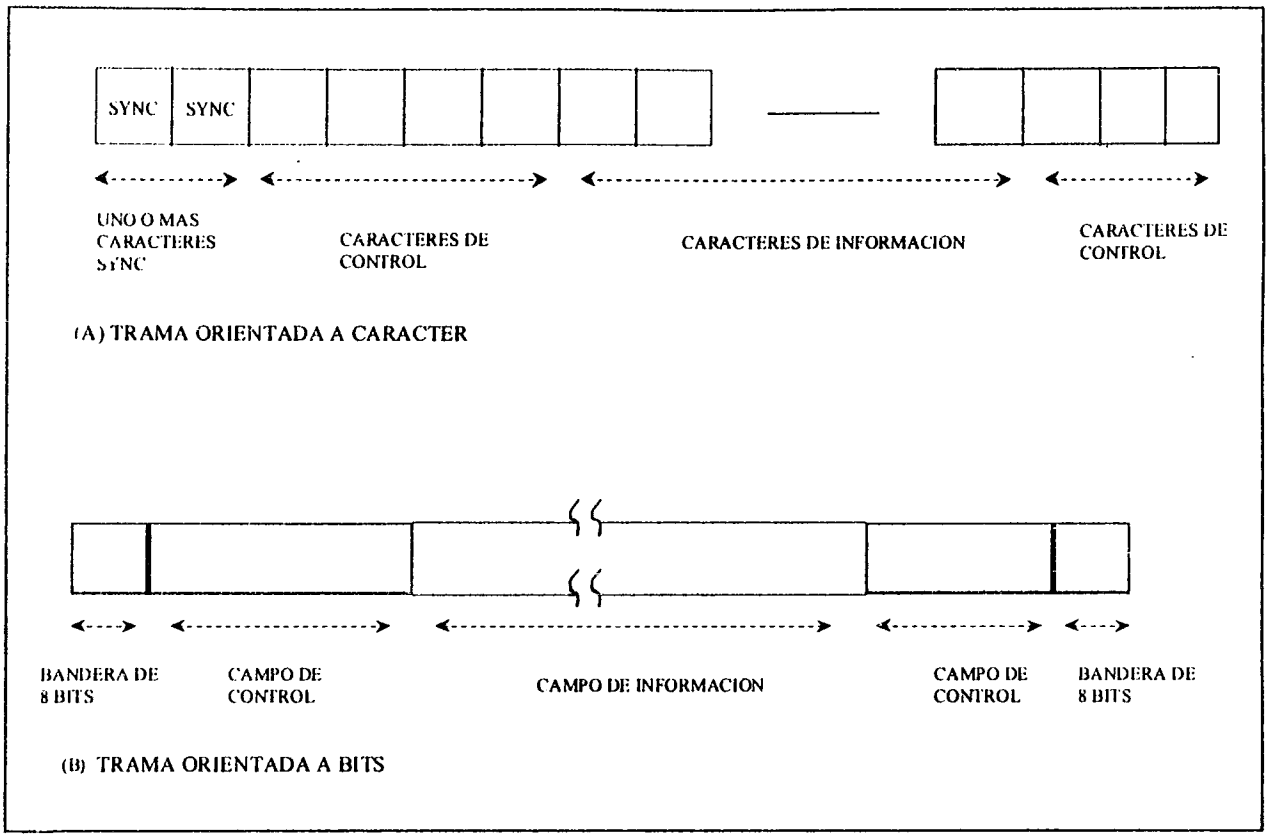


FIGURA 1.4 TRANSMISION SINCRONA

1.4. SISTEMAS DE MULTIPLEXADO

Se llama multiplexar a la combinación de 2 o más señales dentro de un canal o medio de transmisión. Se emplea principalmente para ahorrar costos y optimizar mejor los recursos, además existen limitaciones en la capacidad de cualquier canal de comunicación. Existen diversas formas de multiplexión, las más comunes son el multiplexaje por división de frecuencia para señales analógicas y multiplexión por división de tiempo para señales digitales.

1.4.1 MULTIPLEXAJE POR DIVISIÓN DE FRECUENCIA FDM (FRECUENCY DIVISION MULTIPLEXING)

Este tipo de multiplexaje es usado cuando el ancho de banda disponible del medio es excedido por el ancho de banda de las señales a ser transmitidas. Un número de señales puede ser portadas simultáneamente si cada señal es modulada dentro de una portadora de frecuencia diferente, y las portadoras de frecuencia están lo suficientemente separadas sin que sus anchos de banda se traslapen. Un caso general es mostrado en la figura 1.5. 6 fuentes de señal son introducidas a un multiplexor el cual modula cada señal dentro de una frecuencia diferente (f1 - f6).

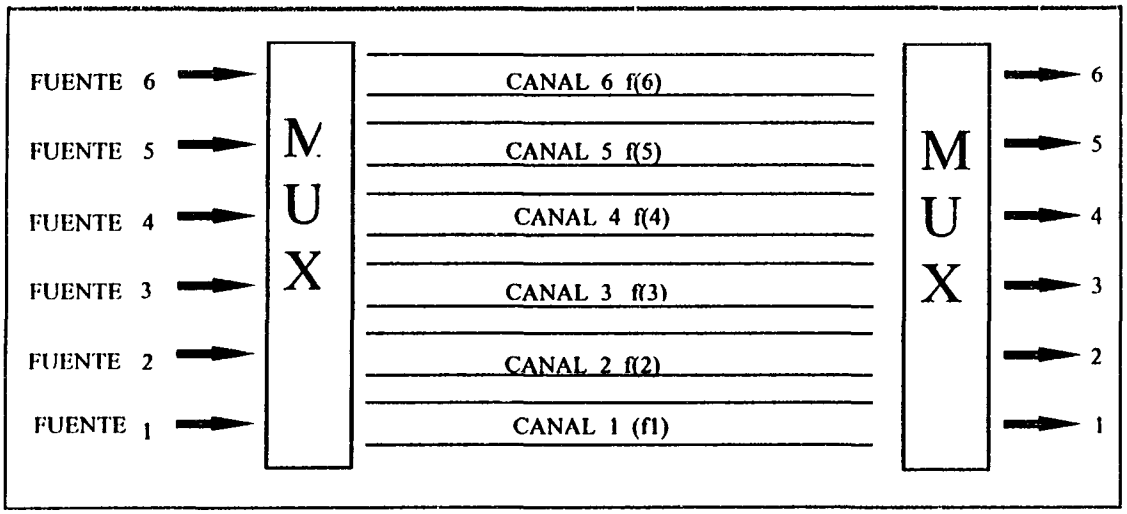


FIGURA 1.5 MULTIPLEXION POR DIVISION DE FRECUENCIA

Cada señal modulada requiere de un cierto ancho de banda centrado alrededor de su portadora de frecuencia, referido como canal. Para evitar interferencia, los canales son separados por bandas de guarda, las cuales son porciones sin uso en el espectro. La composición de la señal transmitida a través del medio es analógica. Sin embargo las señales que en ...n pueden ser

analógicas o digitales. Si es digital se entra en el caso de información digital y señales analógicas en el cual por ejemplo se utiliza FSK, y si es analógica se utiliza por ejemplo AM.

Una descripción general de un sistema FDM se muestra en la figura. Un número de señales analógicas o digitales *[mi(t),i=1,N]* están dentro del mismo medio de transmisión para ser multiplexados. Cada señal *mi(t)* es modulada dentro de una portadora *fcsi* desde donde están las portadoras a ser usadas cada una es referida como subportadora. Cualquier tipo de modulación puede ser usada. Las señales moduladas resultantes entonces son sumadas para producir la señal resultante compuesta *mc(t)*. La señal compuesta puede ser cambiada como un todo a otra portadora de frecuencia adicionando otro paso de modulación. Esta segunda modulación no necesita usar la misma técnica de modulación que la primera. La señal compuesta tiene un ancho de banda total de la suma de los anchos de banda parciales y esta señal esta lista para ser transmitida. En el lado del receptor, la señal compuesta pasa a través de N filtros pasabanda y la señal compuesta es separada sin las diferentes componentes. Cada componente es entonces demodulada para recobrar la señal original. Como se muestra en la figura 1.6.

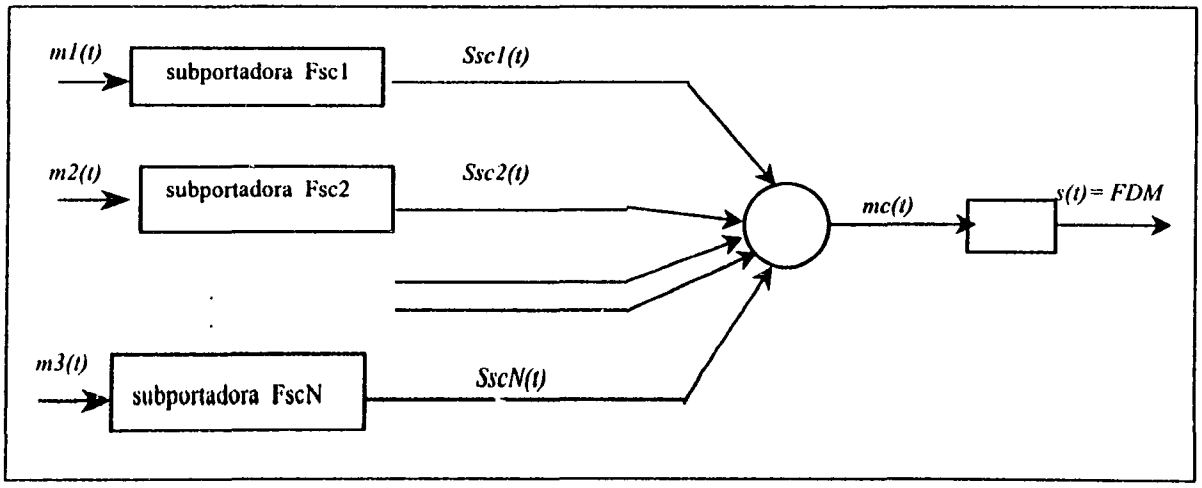


Figura 1.6 FDM

1.4.1.1 JERARQUÍA FDM

Esta jerarquía esta diseñada para la transmisión de señales de voz sobre enlaces de alta capacidad tales como los sistemas de microondas y los de cable coaxial. El CCITT la define de la siguiente manera: en el primer

nivel, sé multiplexan 12 canales de voz de 4 Khz cada uno para formar un grupo de señales con un ancho de banda de 12 x 4 = 48 Khz, en el rango de 60 a 108 Khz. El bloque que le sigue es de 60 canales (multiplexados 5 grupos de 12 canales) a este se le denomina supergrupo, en este paso cada grupo es tratado como una señal individual de 48 Khz de ancho de banda y modulada por una subportadora. La subportadora tiene frecuencias de 420 a 612 Khz en incrementos de 48 Khz. La señal resultante ocupa de 312 a 552 Khz. En adición, cualquier señal arriba de 48 Khz cuyo ancho de banda esta contenido dentro de 60 a 108 Khz puede ser usado como una entrada a un multiplexor de supergrupo. El próximo nivel de la jerarquía es el mastergrupo el cual combina 10 supergrupos. De nuevo, cualquier señal con un ancho de banda de 240 Khz en el rango de 312 a 552 Khz puede servir como una entrada a un MUX de mastergrupo. El mastergrupo tiene un ancho de banda de 2.52 Mhz y soporta 600 canales de voz.

Número de canales de voz	Ancho de banda	Espectro	AT&T	CCITT
12	48 Khz	60-108 Khz	Grupo	Grupo
60	240 Khz	312-552 Khz	Supergrupo	Supergrupo
300	1.232 Mhz	812-2044 Khz		Mastergrupo
600	2.52 Mhz	564-3084 Mhz	Mastergrupo	
900	3.872 Mhz	8.516-12.388 Mhz		Supermaster grupo
Nx600			Mastergrupo multiplex	
3600	16.984 Mhz	0.564-17.548 Mhz	Jumbogrupo	
10800	57.442 Mhz	3.124-60.566 Mhz	Jumbogrupo Multiplex	

Tabla 1.2 Estándares de portadoras FDM

1.4.2 MULTIPLEXAJE POR DIVISIÓN DE TIEMPO (TIME DIVISION MULTIPLEXING)

El multiplexaje por división de tiempo síncrono es posible cuando la velocidad de información alcanzable del medio excede la velocidad de la información de las señales digitales a ser transmitidas. Múltiples señales digitales (o señales portadoras de datos digitales) pueden ser portadas en un

mismo trayecto por porciones entrelazadas de cada señal en tiempo. Como se puede ver en la figura 1.7. El entrelazado puede ser a nivel de bit o en bloques de bytes.

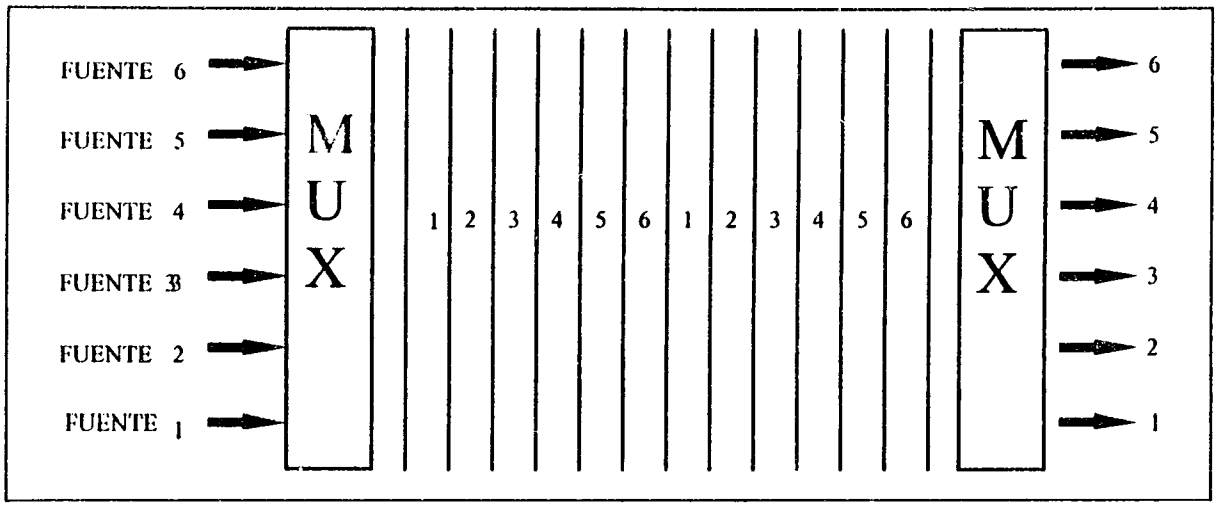


FIGURA 1.7 MULTIPLEXION POR DIVISION DE TIEMPO

Por ejemplo un multiplexor con 6 entradas de 9.6 kbps dan como resultado una línea de 57.6 kbps sí sé multiplexan.

Una descripción general de un sistema síncrono TDM se muestra en la figura 1.8 a. Un número de señales están por ser multiplexadas dentro del mismo medio de transmisión. Las dos señales tanto la de información como la portadora son digitales. La información entrante de cada fuente es brevemente almacenados en un "buffer". Cada buffer es típicamente de un bit o de un carácter en longitud. Los buffers son examinados secuencialmente para formar una señal compuesta de información digital en forma de ráfaga. La operación de exploración es lo suficientemente rápida que cada buffer es vaciado antes que otra información llegue. Así la señal digital puede ser transmitida directamente, o pasada a través de un módem para transmitir una señal analógica.

La transmisión de información puede tener un formato similar al de la figura 1.8 b. Los datos son organizados dentro de tramas. Cada trama contiene un ciclo de ranuras de tiempo (time slots). En cada trama, una o más ranuras son dedicadas a cada fuente de información. La secuencia de las

ranuras dedicadas a una fuente, de trama a trama, es llamado un canal. La longitud de la ranura de tiempo es igual a la longitud del buffer del transmisor, típicamente de un bit o un carácter.

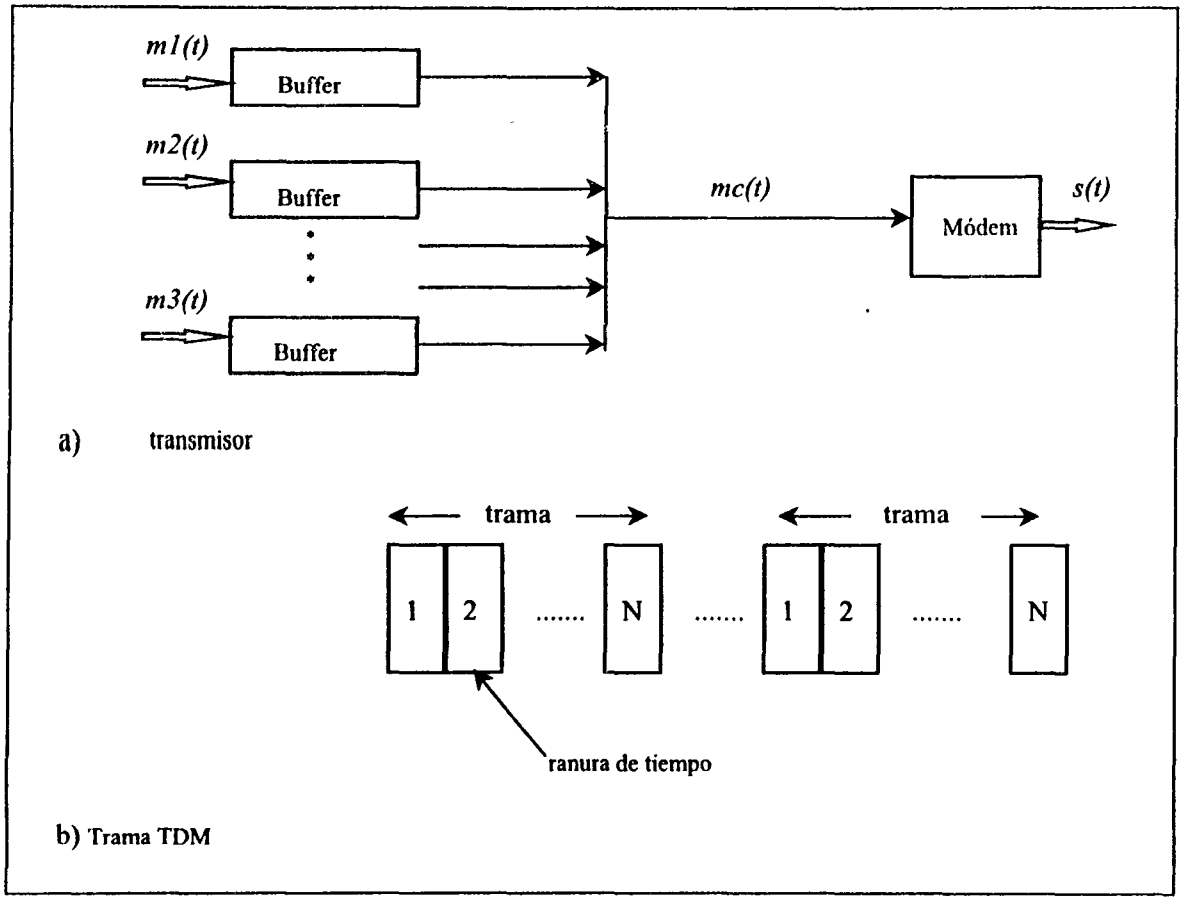


Figura 1.8 TDM síncrono

La técnica del entrelazado de caracteres es usada cuando las fuentes de la señal son asíncronas. Cada ranura de tiempo contiene un carácter de información. Típicamente los bits de inicio y de parada de cada carácter son eliminados antes de la transmisión y reinsertados por el receptor. La técnica de entrelazado de bits es usada con fuentes síncronas y también puede ser usado con fuentes asíncronas. Cada ranura tiempo contiene un bit.

En el receptor, la información entrelazada es demultiplexada y ruteada al buffer destino correspondiente. Para cada fuente de entrada existe una salida idéntica la cual recibe la información que entra a la misma velocidad

en la cual fue generada. TDM síncrono es llamado así no porque se use transmisión síncrona, sino por que las ranuras de tiempo preasignadas a las fuentes son fijas.

El mismo principio de agrupación que FDM es utilizado. La capacidad de un circuito de voz, expresado digitalmente, es convertida de 4000 Hz a 64000 bits por segundo. De hecho estos 64 kbps provienen del muestreo y codificación de la voz la cual requiere 8000 muestras de un byte por segundo, esto es un byte cada 125 microsegundos. La jerarquía Europea se compone de 32 canales o circuitos digitales para formar el primer nivel de la jerarquía o E1, este nivel se compone de 2048 kbps o 32 bytes cada 125 microsegs. Un E1 tiene capacidad de 30 circuitos de 64 kbps. Cuatro grupos de 32 bytes o E1's forman el segundo nivel con una velocidad de 8192 kbps, Un E2 tiene una capacidad de 120 circuitos. El tercer nivel o E3 tiene una velocidad de 34368 kbps, tiene capacidad de 480 circuitos_ y el cuarto nivel o E4 tiene una velocidad de 139264 kbps_con capacidad de 1920 circuitos. Ver tabla 1.3.

Esta técnica de agrupamiento no hace alguna suposición concerniente a la trama o al contenido de la señal. La transición es de un nivel dado a un nivel jerárquico mayor con la ayuda de justificación y relleno "padding . El porque de esto, accesar a señales de menor capacidad 8 (tributarias) requiere de demultiplexión, y esto implica operaciones de relleno y extracción de señales en todos los niveles intermedios.

Esta ausencia de flexibilidad virtualmente prohibe la extracción, e inserción de circuitos de baja capacidad para grupos de orden más grande de uno. El propósito de las operaciones de extracción e inserción es para habilitar la combinación de circuitos para responder a las variaciones de tráfico en las arterias de transmisión. Esta operación de conexión cruzada requiere de intervención manual con tecnologías corrientes. Esto es igual para FDM y TDM.

De hecho, usando TDM síncrono, y sacrificando algún tiempo de retardo en resincronizar, debe ser posible operar directamente en circuitos de baja velocidad los cuales ocuparan una posición precisa en tiempo. Sin embargo, si toda la red esta sincronizada, la fase de las señales es arbitraria y esta sujeta a variación debido a las diferencias en tiempos de propagación y diferencias de frecuencias entre los relojes transmisor y receptor.

1.4.2.1 JERARQUÍA TDM AMERICANA

La base de la jerarquía americana TDM es el formato de transmisión DS1, el cual multiplexa 24 canales. Cada trama contiene 8 bits por canal más 1 bit de sincronía, esto es 24 x 8 + 1 = 193 bits, para transmisión de voz se toman 8000 muestras por segundo teniendo entonces una velocidad de 8000 x 193 = 1.544 Mbps. Para cada 5 de 6 tramas los 8 bits son usados y para la sexta trama cada canal contiene 7 bits y el octavo es utilizado para control de red y ruteo de información, por ejemplo para establecer una conexión o terminar una llamada.

El mismo formato DS1 se utiliza para proveer servicios digitales. En este caso se utilizan solo 23 canales para información, el 24 es reservado para un byte especial de sincronía el cual permite una mas rápida y más confiable retransmisión de una trama errónea. Dentro de cada canal 7 bits son usados para información y el octavo es usado para indicar si el canal para esa trama contiene información del usuario o bits de control. Con 7 bits por canal y tomando 8000 muestras por segundo obtenemos una velocidad de 56 Kbps por canal.

El formato DS1 puede ser usado para llevar canales de voz y datos simultáneamente. En este caso los 24 canales son utilizados, no se provee un byte de sincronía. Después del nivel básico de 1.544 Mbps se pueden multiplexar para alcanzar niveles más altos con varias entradas DS1. Por ejemplo DS2 combina 4 DS1's dentro de una ráfaga de 6.312 Mbps. La información de las cuatro fuentes está entrelazadas por 12 bits a un tiempo, 1544 Mbps x 4 = 6.176 Mbps. La capacidad restante es usada para sincronía y bits de control. En la tabla se observan los demás niveles.

A)Norteamericano			B)Internacional CCITT		
Número de señal digital	Número de canales de voz	Velocidad de datos (Mbps)	Número de nivel	Número de canales de voz	Velocidad de Datos (Mbps)
DS-1	24	1.544	1	30	2.048
DS-1C	48	3.152	2	120	8.448
DS-2	96	6.312	3	480	34.368
DS-3	672	44.,736	4	1920	139.264
DS-4	4032	274.176	5	7680	565.148

Tabla 1.3 Estándares de portadoras TDM

Varios estándares de multiplexaje son empleados para usar una facilidad de transmisión de alta capacidad. Las designaciones DS1 y DS1C de aquí en adelante, son referidas a un esquema de multiplexaje usado para información de portadoras "carriers". AT&T y otras portadoras suministran facilidades de transmisión que soportan estas señales multiplexadas refiriéndose a ellas como sistemas de portadoras "carrier systems". Estas son designadas con una T, si la portadora T1 provee una velocidad de 1.544 Mbps y es capaz de soportar el formato multiplexado DS1 y de aquí en adelante para velocidades mayores.

1.4.3 MULTIPLEXAJE POR DIVISIÓN DE TIEMPO ASINCRONO O ESTADISTICO

En el multiplexaje estadístico las ranuras de tiempo son suministradas sobre demanda. Como en el multiplexaje síncrono, el estadístico tiene un número de líneas de I/O de un lado y una línea de alta velocidad en la otra. Cada línea de I/O tiene un buffer asociado a ella. En el multiplexaje

estadístico hay n líneas de I/O, pero solo k, donde k<n, ranuras de tiempo disponibles en la trama TDM. Para la entrada, la función del multiplexor es buscar en los buffers de entrada para recoger información hasta que una trama es llenada y entonces la trama es enviada. En la salida el multiplexor recibe una trama y distribuye las ranuras de información a su apropiado buffer de salida.

El TDM estadístico tiene la ventaja del hecho de que los dispositivos conectados no están todos transmitiendo a la vez, la velocidad de la información en la línea multiplexada es menor que la suma de las velocidades de información de los dispositivos conectados. Así un multiplexor estadístico puede usar una velocidad baja de información para soportar tantos dispositivos como un multiplexor síncrono. Alternativamente si un mux estadístico y uno síncrono van a usar la misma velocidad, el mux estadístico soporta más dispositivos.

En la figura 1.9 se muestran los contrastes del modo TDM síncrono y estadístico. En la figura tenemos cuatro fuentes de información y se muestran la información producida en los cuatro primeros tiempos (t0, t1, t2 y t3) en el caso del multiplexor síncrono, este tiene una salida efectiva de los cuatro tiempos, pero como se observa solo los dos primeros contienen información C y D no. A diferencia del muestreo estadístico este no envía ranuras vacías, así solo A y B son enviados durante el primer ciclo. Sin embargo, la significancia de la posición de las ranuras de tiempo en este esquema no importa, no toma en cuenta la posición de la ranura para la información (por ejemplo en el síncrono la ranura A1 le corresponde a A al igual que A2, etc). Se necesita un encabezado por ranura en el multiplexaje estadístico para asegurar la entrega. Ver figura 1.9.

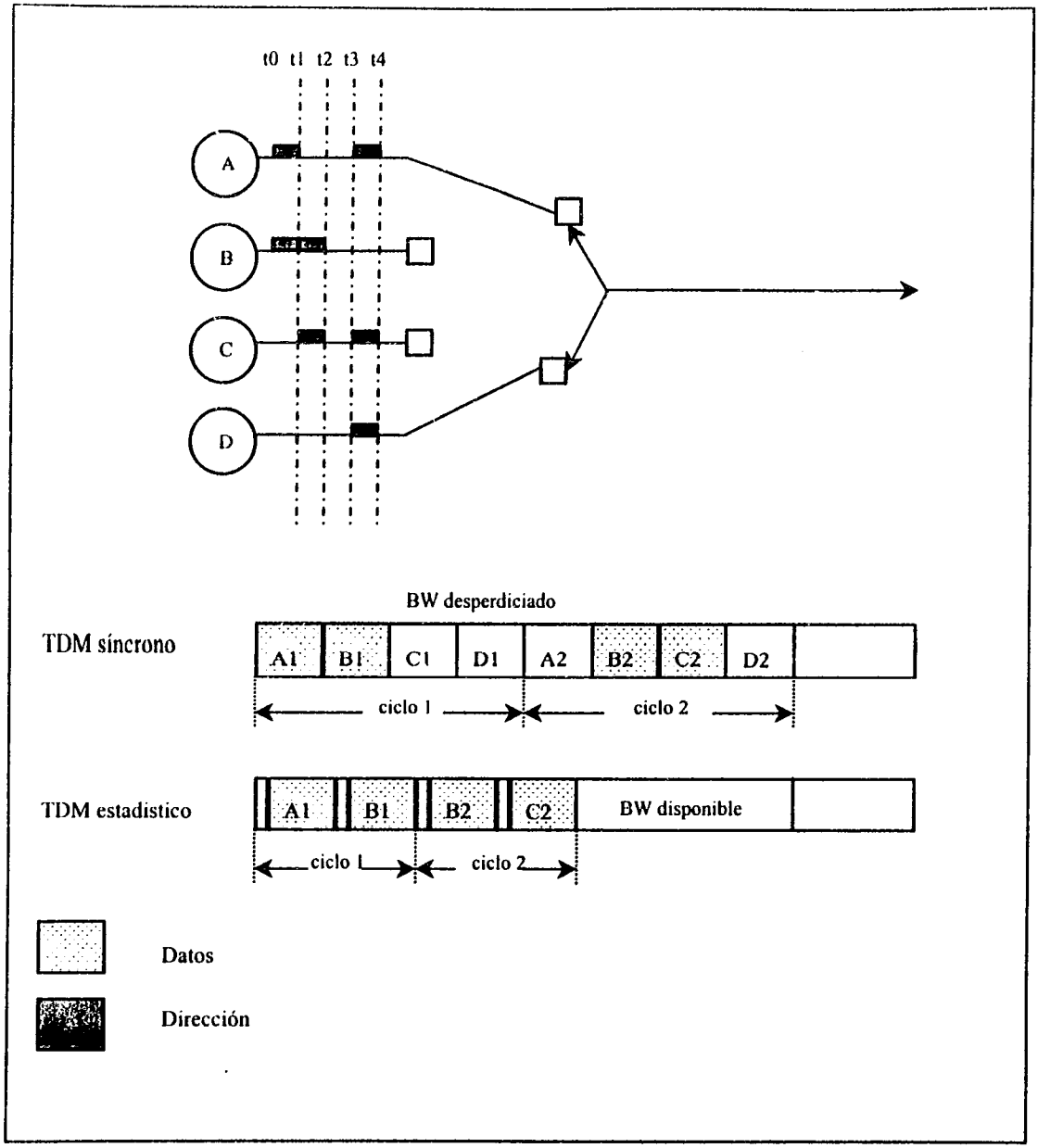


FIGURA 1.9 COMPARACION ENTRE TDM SINCRONO Y ESTADISTICO

1.5 TECNICAS DE CONMUTACION

Hemos analizado como la información puede ser codificada y transmitida sobre un enlace de comunicación. En su forma más simple, la información es transmitida entre dos dispositivos conectados directamente uno con otro por algún medio de transmisión. Sin embargo a menudo es impráctico tener conectados solo dos dispositivos, las causas de lo anterior son:

- los dispositivos estén alejados el uno del otro, esto seria costoso si la separación es de varios cientos de Km
- Hay un cierto grupo de dispositivos, cada uno de los cuales requiere un enlace para alguno de los otros en varias ocasiones, un ejemplo de esto son los teléfonos en el mundo y todas las terminales y computadoras propias de una misma organización. Excepto por el caso de pocos dispositivos, es impráctico proveer un cable dedicado entre cada par de dispositivos.

La solución a este problema es conectar cada dispositivo a una red de comunicación. La comunicación es lograda para transmitir la información de una fuente "transmisor" al destino "receptor" a través de una red con nodos intermediarios. Estos nodos no intervienen (son transparentes) con el contenido de la información, su función es proveer una facilidad de conmutación que moverá la información de un nodo a otro hasta que ellos lleguen a su destino. Un ejemplo de esto se muestra en la siguiente figura 1.10, donde se muestran una serie de dispositivos que desean comunicarse, se denominan genéricamente estaciones. Las estaciones pueden ser terminales, teléfonos y otros dispositivos de comunicación. También tenemos una serie de dispositivos que tienen el propósito de proveer la comunicación y se les conoce como nodos. Los nodos están conectados uno con otro de alguna forma por un enlace de transmisión (p.e. cable coaxial). Cada estación esta conectada a un nodo. La serie de nodos en conjunto es referida como una red de comunicaciones.

La figura 1.11 describe un espectro de técnicas de conmutación disponible para la información de transporte a través de la red. Los dos

extremos del espectro representan las dos técnicas tradicionales de conmutación: conmutación de circuitos y conmutación de paquetes, Las técnicas restantes son más recientes. En general las técnicas que van hacia la izquierda proveen transmisión con poca o sin variación y con un mínimo de demandas procesadas en las estaciones conectadas, mientras que las técnicas que van hacia la derecha proveen un incremento de flexibilidad para manejar velocidades variables y tráfico impredecible a expensas de incrementarla complejidad de procesamiento.

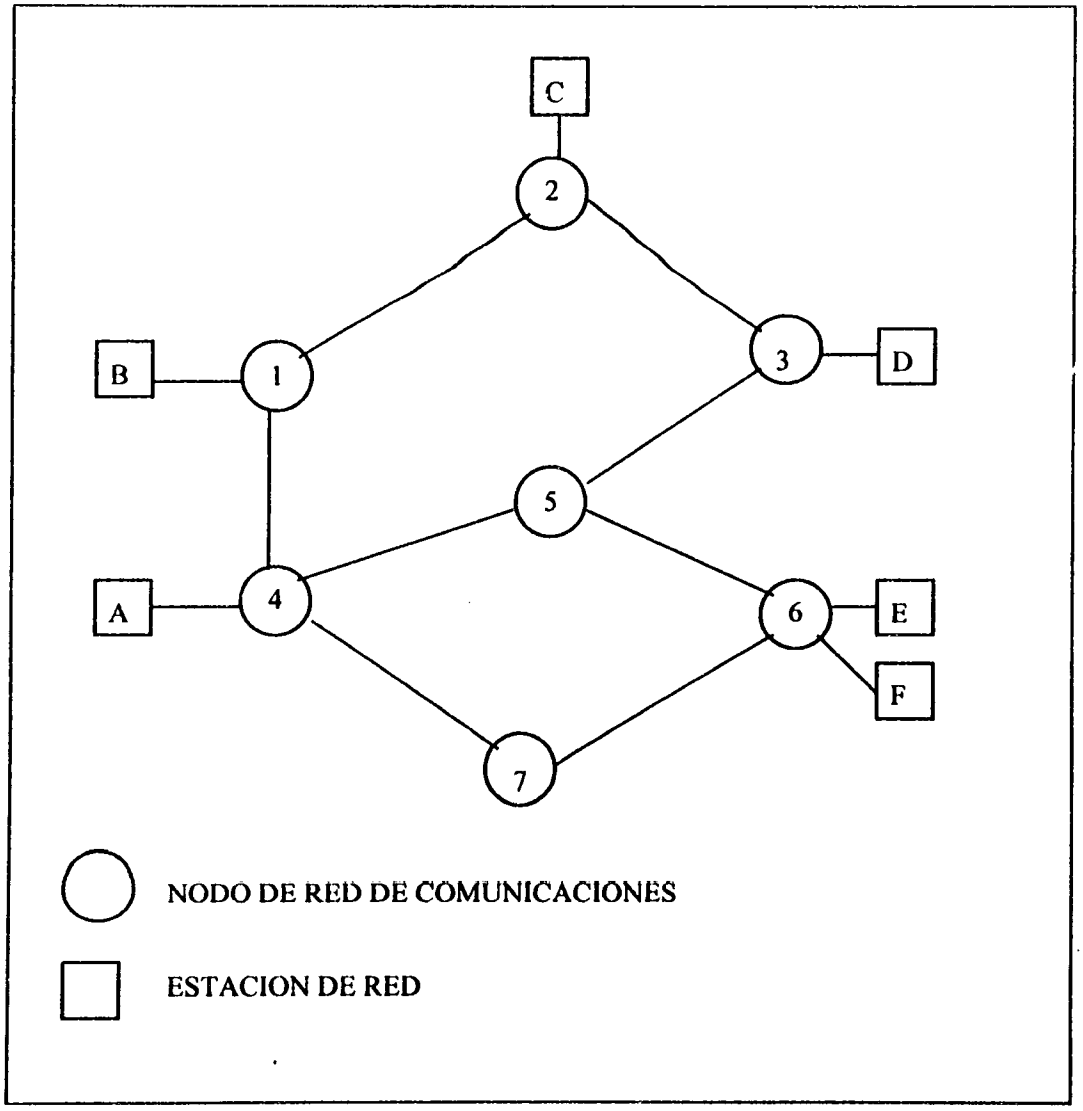


FIGURA 1.10 RED GENERICA DE CONMUTACION

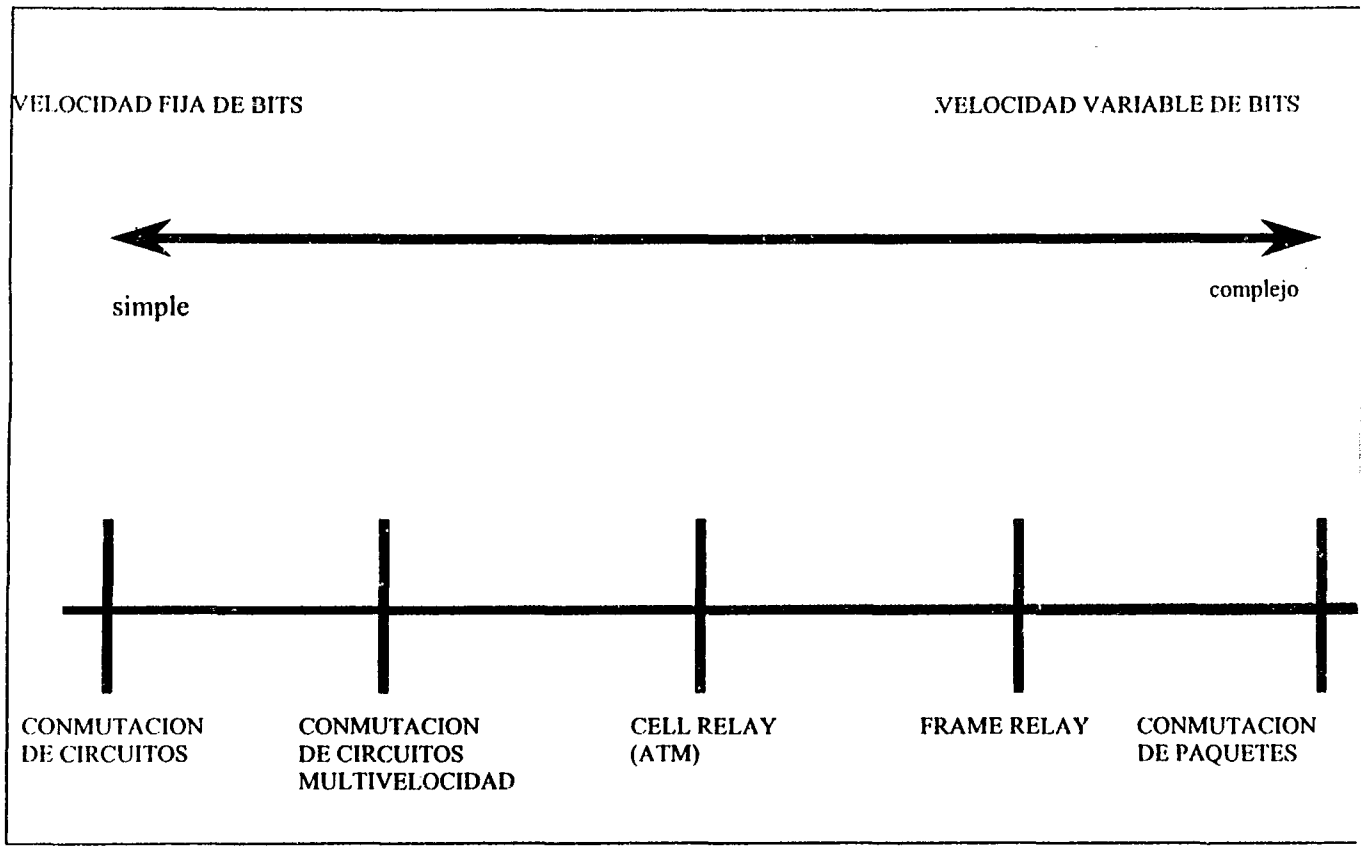


FIGURA 1.11 ESPECTRO DE TECNICAS DE CONMUTACION

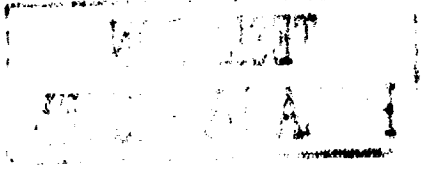
1.5.1 CONMUTACION DE CIRCUITOS

La comunicación vía conmutación de circuitos implica que haya un camino (path) de comunicación entre dos estaciones. Este camino es una secuencia de conexiones entre nodos para formar el enlace. En cada enlace físico un canal es dedicado para la conexión. El más común ejemplo de conmutación de circuitos es la red telefónica. La comunicación vía conmutación de circuitos envuelve tres fases las cuales se explican en la figura 1.10.

1.- Establecimiento del circuito. Antes de transmitir cualquier información en datos, una conexión punto a punto (estación con estación) debe ser establecida. Por ejemplo la estación A manda una petición al nodo 4 que solicita una conexión a la estación E. Típicamente el circuito de A hacia 4 es una línea dedicada, así que partimos del hecho que es una conexión que ya existe. El nodo 4 debe encontrar el próximo tramo en una ruta hacia el nodo 6. Basado en la información de ruteo y midiendo la disponibilidad de la red, el nodo 4 selecciona el circuito hacia el nodo 5 que tiene un canal libre (usando FDM o TDM) en el circuito, y manda un mensaje de petición a la estación E. Así se establece el camino dedicado de 4 hacia E vía nodos 4 y 5, siendo que un número de estaciones pueden establecer caminos internos de múltiples estaciones a múltiples nodos. El resto de los procesos son similares. El nodo 5 dedica un canal al nodo 6 e internamente une ese canal al canal del nodo 4. El nodo 6 completa la conexión hacia E. Para completar la conexión una prueba es realizada para determinar si E esta libre u ocupado para aceptar la conexión.

2.- Transferencia de información: Ahora las señales pueden ser transmitidas de A a través de la red hacia E .El camino del circuito A-4 esta conmutado internamente a través de 4, el canal 4-5 esta conmutado internamente a través de 5, el canal 5-6 esta conmutado internamente a través de 6 y finalmente 6-E. Generalmente la conexión es full-duplex y la información pueden ser transmitida en ambas direcciones.

3.- Desconexión del circuito: después de un período de transferencias de información, la conexión es terminada. Usualmente por la indicación de alguna de las dos estaciones. Señales deben ser propagadas a 4,5 y 6 para liberar los recursos dedicados. Hay que notar que el camino de la conexión es establecido antes que la transferencia de la información comience. Así la capacidad del canal debe estar disponible y reservada entre cada par de nodos en el camino, y cada nodo debe tener capacidad de conmutación interna para manejar la conexión. Los conmutadores deben tener inteligencia para hacer esas locaciones y escoger una ruta a través de la red. La conmutación de circuitos puede ser algo ineficiente. La capacidad del canal es dedicada durante la duración de la conexión, aún si la información no esta siendo transferida. Para una conexión de voz, la utilización puede ser aún mayor pero aun así no alcanza el 100 %. Para una conexión terminal a computadora la capacidad puede estar en espera durante más tiempo que el usuario para transmitir datos. En términos de eficiencia, hay un retardo antes para la transferencia de información para las llamadas de establecimiento.



Sin embargo una vez que el circuito es establecido la red es transparente a los usuarios. La información es transmitida a una velocidad fija sin retardo más que el de propagación a través del enlace de transmisión. El retardo entre cada nodo es despreciable.

1.5.2 CONMUTACION DE PAQUETES

Las redes de conmutación de circuitos fueron originalmente diseñadas para manejar trafico de voz, y la mayoría del trafico en esas redes es voz. Una característica de las redes de conmutación de circuitos es que los recursos dentro de la red son dedicados a una llamada en particular. Para conexiones de voz, el circuito resultante disfrutara de un elevado porcentaje de utilización utilizada en conversaciones. Sin embargo como las redes de conmutación de circuitos empezaron a ser usadas para conexiones de datos surgieron dos cuestiones:

1.- En una conexión típica servidor - terminal, mucho del tiempo de la línea esta en espera, así con las conexiones de datos el aprovechamiento de un circuito conmutado es ineficiente.

2.- En una red de conmutación de circuitos, la conexión provee para la transmisión una velocidad constante. Así cada uno de los dispositivos que están conectados deben transmitir y recibir a la misma velocidad la una de la otra, con lo cual limita la utilidad de la red al interconectar una variedad de computadoras y terminales.

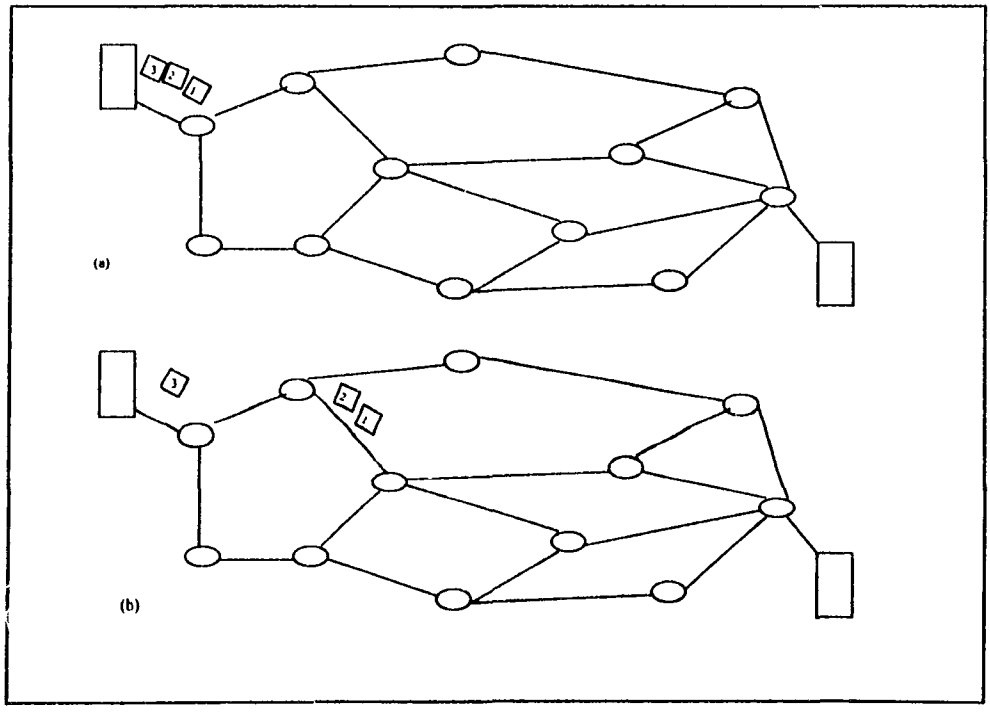
Una red de conmutación de paquetes utiliza bloques de información a transmitir denominados paquetes. Un tamaño típico de un paquete es de 1000 bytes. Si la fuente tiene un mensaje grande a transmitir, el mensaje es partido en una serie de paquetes, ver figura 1.12. Cada paquete consiste de una porción de datos (o todos si el mensaje es corto) que una estación desea transmitir, más un encabezado que contiene información de control. La información de control, a su mínimo, incluye la información que la red requiere en orden para direccionar el paquete a través de la red y lo lleva a su destino. En cada nodo, el paquete es recibido, almacenado brevemente y pasado al siguiente nodo.

La operación básica de una red de conmutación de paquetes es la siguiente: Una computadora transmisora u otro dispositivo envía un mensaje como una secuencia de paquetes (a). Cada paquete incluye información de control

indicando la estación destino (computadora, etc.). Los paquetes son inicialmente mandados al nodo al cual la estación esta conectada. Como cada paquete llega a ese nodo, este almacena brevemente el paquete, determina el próximo tramo de la ruta y pone en espera al paquete para después seguir con el enlace. Cada paquete es transmitido al próximo nodo (b) cuando el enlace este disponible. Todos los paquetes eventualmente toman su propio camino a través de la red y son entregados a su destino.

La conmutación de paquetes tiene un cierto numero de ventajas frente a la conmutación de circuitos:

1.- La eficiencia de la línea es grande, un simple enlace de nodo a nodo puede ser dinámicamente compartido por muchos paquetes sobre tiempo. Los paquetes son retenidos y transmitidos tan rápidamente como sea posible. Con conmutación de paquetes, el enlace nodo a nodo es asignado en tiempo usando TDM síncrono. Mucho de este tiempo, el enlace permanece en espera por que una porción de su tiempo dedicado a una conexión que esta libre.



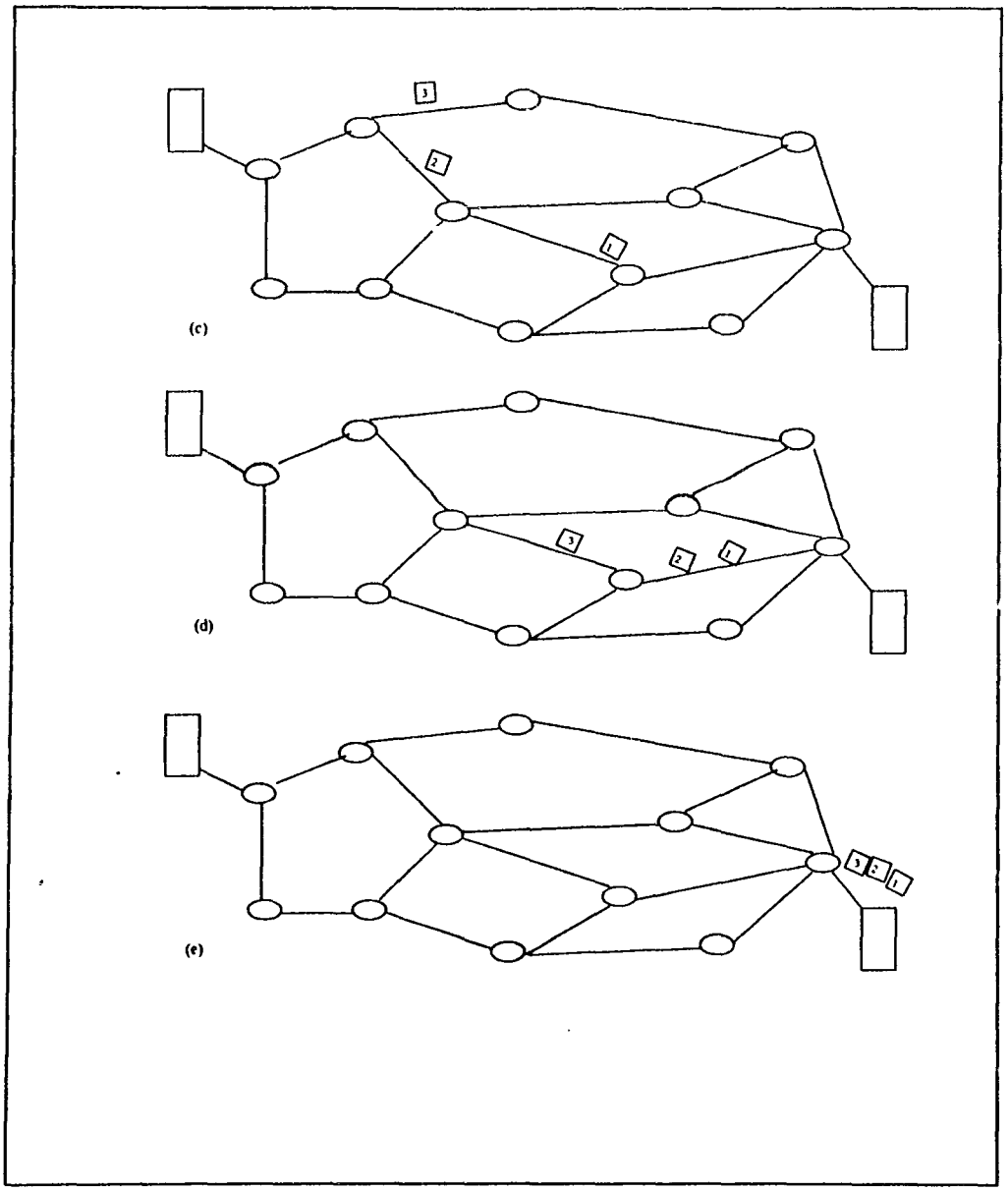


FIGURA 1.12 CONMUTACION DE PAQUETES (DATAGRAMA)

2.- Una red de conmutación de paquetes puede realizar conversión de velocidad de información. Dos estaciones de diferente velocidad de información pueden intercambiar paquetes entre nodos pero al llegar al nodo destino la velocidad será la del equipo.

3.- Cuando el trafico llega a ser elevado en una red de conmutación de circuitos, algunas llamadas se bloquean, esto es, que la red rehusa aceptar conexiones adicionales hasta que el trafico disminuya. En una red de conmutación de paquetes los paquetes son aun aceptados pero con un cierto retraso.

4.- Prioridades pueden ser usadas, así si un nodo tiene un numero de paquetes en la cola de espera para ser transmitidos, puede transmitir los paquetes de más alta prioridad primero. Estos paquetes tendrán menos demora que unos de menor prioridad.

Operación de una red de conmutación de paquetes. Considerando que una estación quiere enviar un mensaje a través de la red, el paquete es más grande que la longitud máxima de un paquete, el paquete es seccionado en varios paquetes más pequeños y mandados esos paquetes uno a la vez hacia la red. Hay dos formas para rutear los paquetes a través de la red para que lleguen a su destino. Estas formas o métodos son circuitos virtuales y datagramas.

En el método de los datagramas, cada paquete es tratado independientemente, sin tomar en cuenta que otros paquetes del mensaje hayan sido enviados antes. Esto se ilustra en la figura 1.13. Cada nodo escoge el camino del paquete hacia el próximo nodo, tomando en cuenta información recibida de nodos vecinos sobre trafico, fallas en la línea, etc. Así los paquetes cada uno con la misma dirección destino pueden no seguir la misma ruta (c), y entonces ellos pueden llegar en diferente secuencia al destino. En este ejemplo, el nodo de salida acomoda los paquetes en su orden original antes de entregarlos al destino. En algunas redes de datagramas el destino es el que reorganiza los paquetes. También es posible que un paquete sea destruido en la red, por ejemplo si un nodo cae todos los paquetes en la cola de espera se pueden perder. El nodo destino o el destino mismo debe de poder detectar la pérdida de un paquete y decidir como recobrar el paquete.

En el método de los circuitos virtuales una ruta preasignada es establecida antes de que cualquier paquete sea enviado, esta ruta sirve para soportar una conexión lógica entre dos puntos. Una vez que la ruta es establecida todos los paquetes siguen la misma ruta a través de la red figura 1.13. La ruta es fija para toda la duración de la conexión lógica, esto es similar a la formación de un circuito en una red de circuitos conmutados. Cada paquete ahora contiene un identificador de circuito virtual además de la información. Cada nodo en la ruta preestablecida sabe a donde dirigir los paquetes sin necesidad de tomar una decisión de ruteo. En cualquier tiempo una estación puede tener más de un circuito virtual a cualquier estación y puede tener circuitos virtuales a más de una estación.

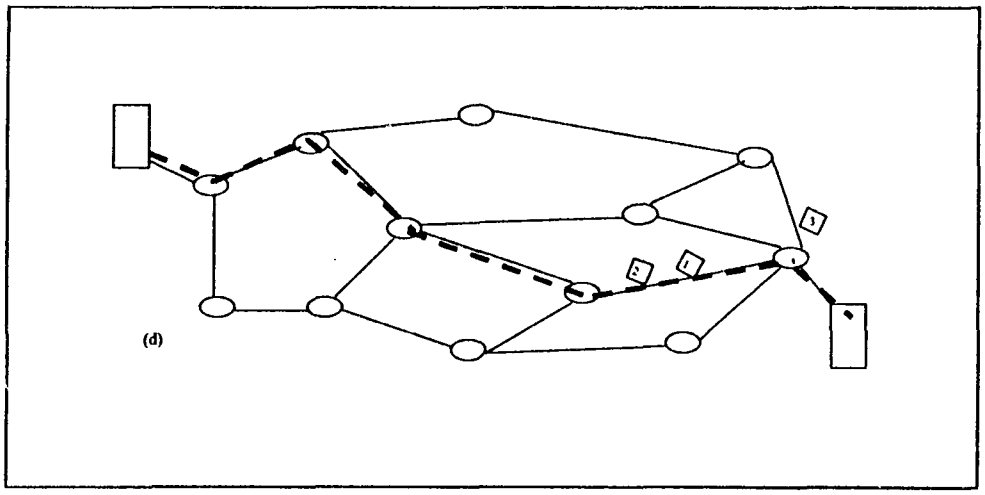


FIGURA 1.12 CONMUTACION DE PAQUETES (CIRCUITO VIRTUAL)

La principal característica de los circuitos virtuales es que la ruta entre estaciones es establecida primero. Esto no significa que la ruta es un camino dedicado como en conmutación de circuitos. Un paquete es almacenado en cada nodo y puesto en una cola de espera para mandarlo. La diferencia entre un

datagrama y un circuito virtual, es que el nodo no necesita tomar una decisión para cada paquete. Esto lo hace una sola vez usando un circuito virtual.

Si hay dos estaciones que desean intercambiar información sobre un periodo de tiempo extendido, hay ciertas ventajas de los circuitos virtuales. Primero la red puede proveer servicios relativos para servicios virtuales, incluyendo secuencia, control de errores y control de flujo. La secuencia es provista desde que todos los paquetes siguen la misma ruta y de ahí que lleguen en el mismo orden. Control de errores es un servicio que asegura que no solo los paquetes llegan en el mismo orden sino también que son correctos. Por ejemplo si un paquete en una secuencia del nodo 4 al nodo 6 falla al llegar al nodo 6, o llega con un error, el nodo 6 puede peticionar una retransmisión de ese paquete al nodo 4. Control de flujo es una técnica para asegurar que un camino no este sobresaturado para recibir información. Por ejemplo, si la estación E esta almacenando datos de la estación A y nota que no tiene espacio de almacenamiento en el buffer, puede solicitar a la estación A que suspenda momentáneamente la transmisión hasta nuevo aviso. Otra ventaja es que los paquetes se transmiten mas rápidamente ya que no es necesario tomar decisiones de ruteo.

Una ventaja de los datagramas es que la fase de llamadas no es requerido. Así si una estación desea mandar uno o más paquetes, la entrega de datagramas deben ser más veloces. Otra ventaja es si es más primitivo es más flexible. Por ejemplo, si una congestión se desarrolla en alguna parte de la red, los datos entrantes pueden ser ruteados por donde no hay congestión. Con el uso de circuitos virtuales los paquetes siguen la misma ruta y así es más difícil que se adapte a la congestión. Una tercera ventaja es que los datagramas entregados son más confiables. Con el uso de circuitos virtuales si un nodo falla todo el circuito virtual se pierde. Con los datagramas si un nodo falla sigue otra ruta sin pasar por ese nodo.

1.6 TIPOS DE CONEXION ENTRE SISTEMAS

1.6.1 DISPOSITIVOS DTE's y DCE's

Muchos de los dispositivos que procesan información digital tienen limitaciones de capacidad para transmitir: Típicamente ellos generan solo señales digitales y están son generalmente NRZ-L o sus variantes. La distancia a través de la cual ellos pueden transmitir información es también limitada. Consecuentemente es raro para tal dispositivo conectarse directamente al medio de transmisión. Una situación común se presenta en la figura 4.8. Los dispositivos como terminales y computadoras son referidos como DTE's (data terminal equipment) o equipo terminal de datos. Un DTE hace uso del sistema de transmisión a través de un dispositivo intermediario denominado DCE (data circuit-terminating equipment). Por un lado el DCE es responsable de la transmisión y recepción de bits, uno a la vez, sobre el medio de transmisión. Por el otro lado, el DCE debe interactuar con el DTE. En general esto requiere que ambos intercambien información e información de control. Esto es hecho sobre un grupo de cables referidos como circuitos de intercambio. Los dos DCE deben entenderse uno al otro, Esto es, el receptor de cada uno debe usar el mismo código de línea (p. e. Manchester) y el transmisor igual. En resumen cada par de DTE-DCE debe ser diseñado para tener interfaces complementarias y debe ser hábil para interactuar efectivamente.

1.6.2 SISTEMAS ORIENTADOS A CONEXIÓN

Hay dos formas en que un DTE se puede conectar con un DCE, la primera de ellas se denomina orientado a conexión. La segunda se denomina orientado a no conexión. Como se muestra en la figura 1.14 se ilustra un esquema de esta forma de conexión. La red orientada a conexión se caracteriza por que no hay conexión lógica inicial existente entre el DTE y la red. La conexión de red entre dos DTE esta inicialmente en estado de espera o desocupado. Si dos computadoras o terminales desean comunicarse mediante una red orientada a conexión, deben de establecer la conexión utilizando un intercambio de información denominado "handshake" que es parte de un protocolo de comunicaciones. Un protocolo de comunicaciones es una secuencia de pasos o reglas que se siguen para lograr un fin común entre dos o más entes. Una vez que se ha establecido la conexión, se entra en

el estado de transferencia de datos. Este estado también es posible utilizando el protocolo preestablecido. Finalmente los DTE liberan la conexión y vuelven al estado de espera.

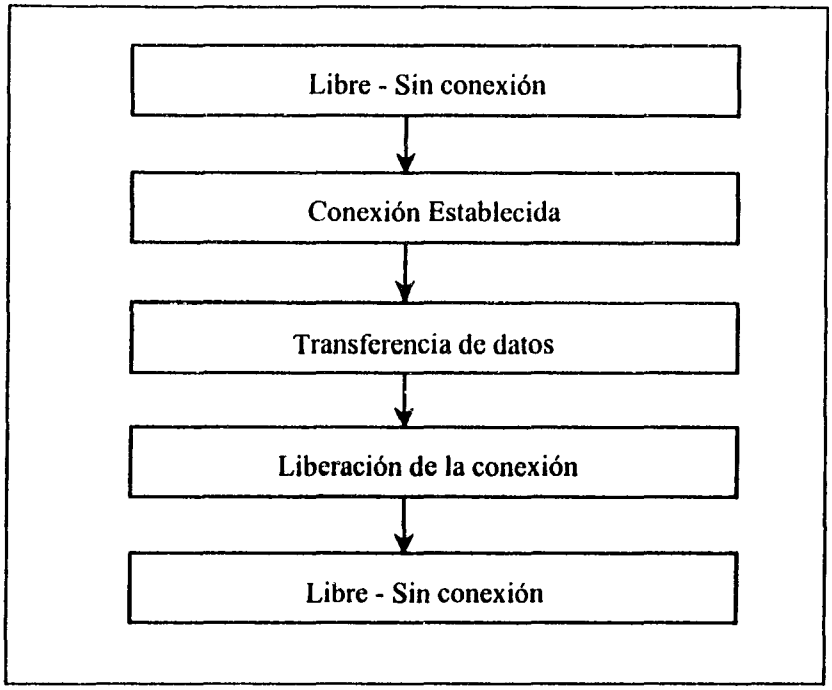


FIGURA 1.14. RED ORIENTADA A CONEXION

Las redes orientadas a conexión proveen un cierto cuidado de los datos de usuario. El procedimiento exige un reconocimiento especifico de que la conexión ha sido establecida, en caso contrario, la red informa a los DTE solicitantes de que no se ha podido establecer la conexión. También debe de existir un control de flujo, es decir, que la información llegue correctamente y en el orden adecuado y así no saturar a los DTE y DCE's. También se utilizan técnicas de corrección de errores. Las redes orientadas a conexión mantienen un constante control de las sesiones e intentan asegurar que la información del usuario no se pierdan en la red. El cuidado provisto por este tipo de redes requiere un considerable sobreencabezado para soportar muchas de las funciones.

Un ejemplo típico de una red orientada a conexión es el sistema telefónico. En este el abonado que llama sabe que se ha establecido la conexión, ya que puede hablar con la persona que esta al otro lado de la línea.

1.6.3 SISTEMA ORIENTADO A NO CONEXIÓN

Las redes orientadas a no conexión (también denominadas datagramas) pasan directamente del estado de espera (los dos DTE no están conectados lógicamente) al de transmisión de información, seguido de esto pasan al estado de espera. La diferencia es que no hay un establecimiento de la conexión y de la fase de liberación de la conexión. Además la red no orientada a conexión carece de reconocimientos (comandos para establecer una conexión), control de flujo detección y corrección de errores, aunque este servicio se puede proveer para un enlace determinado. Este tipo de redes no tienen sobrecarga. Ver figura 1.15.

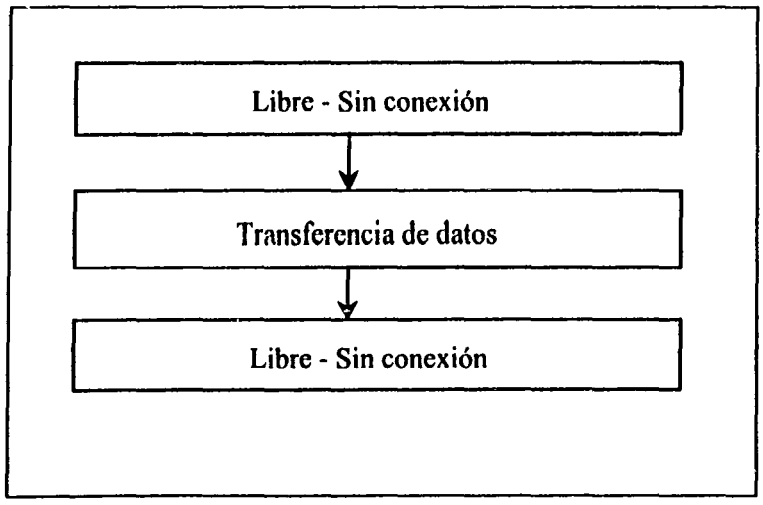


FIGURA 1.15 : RED ORIENTADA A NO CONEXION

Un ejemplo de una red orientada a no conexión es el proceso de escribir una carta. La carta se deposita en el buzón con la confianza de que llegara a su destino. Lo más habitual es que llegue sin problemas, pero el remitente no lo sabe en el momento de enviarla. La oficina de correos no envía ningún mensaje al remitente para decirle que la carta llega a su destino. No obstante el destinatario puede notificar la llegada de la carta al remitente escribiéndole otra carta.

Las bases de comparación y de selección entre redes orientadas y no orientadas a conexión se centran en la sobrecarga de trafico frente a las funciones que proporcionan. Las redes orientadas a conexión proporcionan muchas funciones, pero eso aumenta el costo del sistema. Por el contrario, la no orientadas a conexión tienen menos sobrecarga, pero dan menos soporte al proceso de aplicación de usuario. Muchas veces, la selección final viene condicionada por la integridad y seguridad que se desea proporcionar a los datos.

CAPITULO 2 REDES DE AREA LOCAL

2.1CONCEPTOS DE REDES LOCALES

2.1.1 DEFINICION DE REDES LOCALES

Una red local es una red de comunicación que provee la interconexión de una variedad de dispositivos de comunicación de información dentro de un área relativamente pequeña.

De esta definición podemos sacar 3 factores importantes. Primero, una red local es una red de comunicaciones lo que significa que facilita el movimiento de bits o datos de un dispositivo a otro, segundo, los dispositivos de comunicación pueden ser:

- computadoras
- terminales
- dispositivos periféricos
- sensores(de temperatura, humedad, seguridad, etc.)
- teléfonos
- etc.

Tomando en cuenta por supuesto que no todos los tipos de redes pueden manejar toda clase de dispositivos, y tercero, el alcance geográfico de una red local es reducido a unos kilómetros.

Estas son algunas características de LAN's:

- alta velocidad en la transmisión de datos (0.1 a 100 Mbps)
- distancias cortas (0.1 a 25 kms.)
- bajo índice de error (10^{-8} a 10^{-11})

Las dos primeras nos sirven para diferenciar a las redes locales de los sistemas multiprocesadores y de las redes de área ancha (WAN).

Las redes locales por lo general experimentan menor error en la transmisión de datos y menor costo en el proceso de comunicación que las redes que cubren grandes distancias.

Una diferencia entre las redes locales y los sistemas multiprocesadores es el grado de acoplamiento. Los sistemas multiprocesadores están

fuertemente acoplados, generalmente tienen algún control central e integrados completamente las funciones de comunicación. Las redes locales tienden a tener características opuestas.

Como ya habíamos dicho en el capitulo 1, hay 2 tipos básicos de redes locales: las que están basadas en la conmutación de circuitos y las que están basadas en la tecnología de transmisión de paquetes. La importancia de la transmisión de paquetes es el uso de un medio de transmisión compartido por un número de dispositivos. En una red local se requiere de la comunicación entre los dispositivos que cooperan.

Podemos observar las siguientes características:

- un medio de transmisión es compartido entre los dispositivos adjuntos
- la transmisión es en forma de paquetes
- la transmisión de cualquier estación es recibida por todas las demás estaciones
- no hay una estación maestra, en vez de eso todas las estaciones cooperan para asegurar el uso ordenado del medio de transmisión.

2.1.2 BENEFICIOS Y DESVENTAJAS

La tabla 2.1 nos muestra algunos de los principales beneficios de una red local.

Uno de los beneficios más importantes es la evolución del sistema, con una red local es posible reemplazar gradualmente aplicaciones o sistemas, y como consecuencia se puede aprovechar el equipo viejo al utilizarlo para aplicaciones que no justifican de gastos adicionales. Una red local tiende a aumentar la fiabilidad, disponibilidad y supervivencia de la facilidad del procesamiento de los datos. Con los sistemas de interconexión múltiple, la pérdida de cualquiera de los sistemas debe tener un mínimo impacto. Además los sistemas claves pueden ser redundantes y de esta manera otros sistemas pueden tomar esa carga de trabajo al presentarse una falla.

TABLA 2.1 Beneficios y desventajas de redes locales

Principales beneficios

- evolución del sistema
- fiabilidad, disponibilidad y supervivencia
- compartimiento de recursos
- soporte múltiple de proveedores
- mejor desempeño de respuesta
- los usuarios necesitan una sencilla terminal para accesar a diversos sistemas
- flexibilidad al establecer el equipo
- integración del procesamiento de datos
- aplicaciones complementarias de valor agregado (como por ejemplo el correo electrónico)

Principales desventajas

- la interoperabilidad no es garantizada
- una base de datos distribuida crea problemas de integridad seguridad/privacidad
- una lenta escalación
- perdida de control

El compartimiento de recursos también involucra a los datos. Los datos pueden ser alojados y controlados con una relativa facilidad desde la red y pueden estar disponibles para muchos usuarios.

Existen también algunos inconvenientes. Una red local no garantiza la interoperatividad entre los recursos, es decir; cuando dos dispositivos no cooperan para trabajar entre sí.

En ese caso se necesitaría de una aplicación especial. El que se pueda accesar a la red desde diferentes lugares pone en duda la integridad, seguridad y privacidad de la información.

2.2 CLASES DE REDES

Las redes de comunicación se pueden clasificar de muchas maneras. Una de ellas es clasificarlas dependiendo de la tecnología que usan, específicamente en términos de topología y medios de transmisión, pero al mismo tiempo estas tipologías y medios de transmisión pueden ser utilizados en una gran variedad de redes, así que la forma más común para clasificarlas es dependiendo del área geográfica que cubren.

Así tenemos:

- redes de área local (LAN)
- redes de área metropolitana (MAN)
- redes de área amplia (WAN)
- redes de área global(GAN)

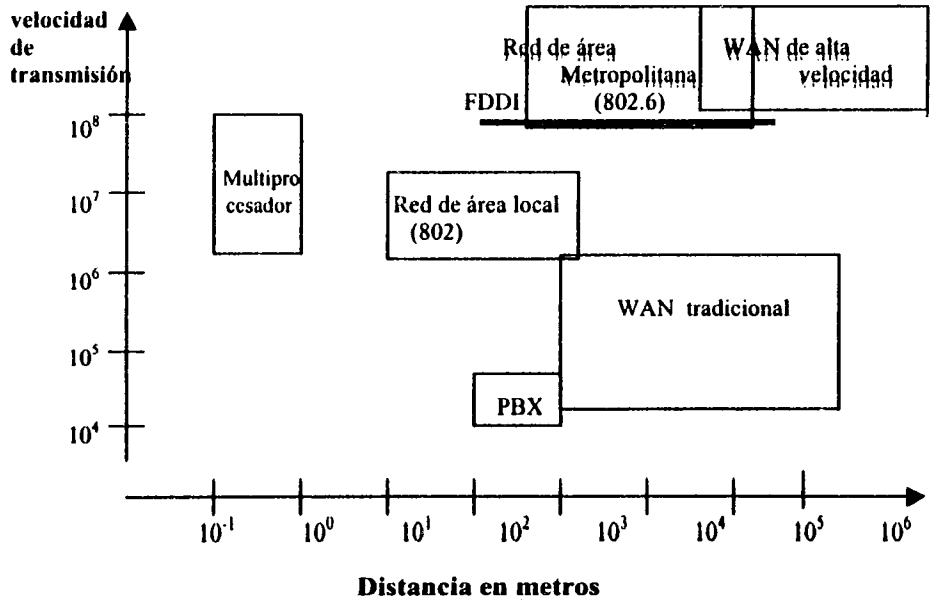


Figura 2.1 Comparación de los sistemas LAN's, MAN's, WAN's y GAN's.

2.2.1 REDES DE ÁREA LOCAL (LAN).

Una LAN se distingue de otros tipos de redes de datos en que están hechas para hacer rendir lo más posible los recursos de un área geográfica de dimensión moderada como un edificio. Una LAN es una red de comunicación que permite enviar y recibir información entre todas las estaciones que están conectadas. La LAN posibilita a las estaciones para comunicarse directamente usando un medio físico común sobre una base punto a punto sin que ningún nodo de comunicación intermedio sea requerido. La red generalmente es adquirida, usada y operada por una sola organización. Una LAN por lo regular usa una topología de medio compartido (bus, árbol, anillo, estrella) al contrario de la red conmutada, ambas usan la tecnología de transmisión de paquetes.

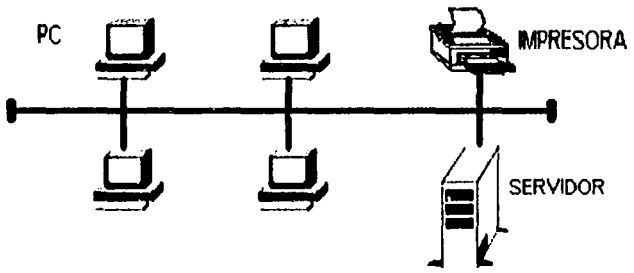


Figura 2.2 Red LAN

2.2.2 MAN

Una red MAN esta comprendida entre una LAN y una WAN, surgió a raíz del reconocimiento de que los enlaces punto a punto y las técnicas de las redes conmutadas usadas en WAN's pueden ser inadecuadas para las necesidades de crecimiento de las organizaciones. Una MAN cubre un área geográfica más grande que una LAN abarcando desde varios edificios hasta ciudades o campus. Dependen de los canales de comunicación, con velocidades de transmisión que van de moderadas a altas. Los índices de error y de retraso pueden ser un poco mas grandes que los que se pueden obtener en una LAN. Soporta tráfico de voz y datos y es proyectada para

proveer la capacidad requerida a un costo menor y a una mayor eficiencia que la obtenida en un servicio equivalente de la compañía local de telefonía. Usa transmisión de paquetes sobre un medio compartido. Soportan diferentes aplicaciones que se interrelacionan dentro del campus.

Como una alternativa del cable coaxial en aplicaciones de larga distancia se ha utilizado muy ampliamente la transmisión por radio microondas. Las antenas parabólicas se pueden montar sobre torres para enviar un haz de señales a otra antena que se encuentre a decenas de kilómetros de distancia. Este sistema es ampliamente utilizado en transmisiones telefónicas y de video; cuanta mayor altura tenga la torre, más grande será el enlace que la señal alcance a transmitir entre dos torres separadas por una distancia de 100 kms., que tienen línea de vista.

La transmisión mediante microondas se lleva a cabo en una escala de frecuencia que va desde 2 a 40 Ghz. Estas frecuencias se han dividido en bandas de portadoras comunes para aplicaciones de tipo gubernamental, militar y otras.

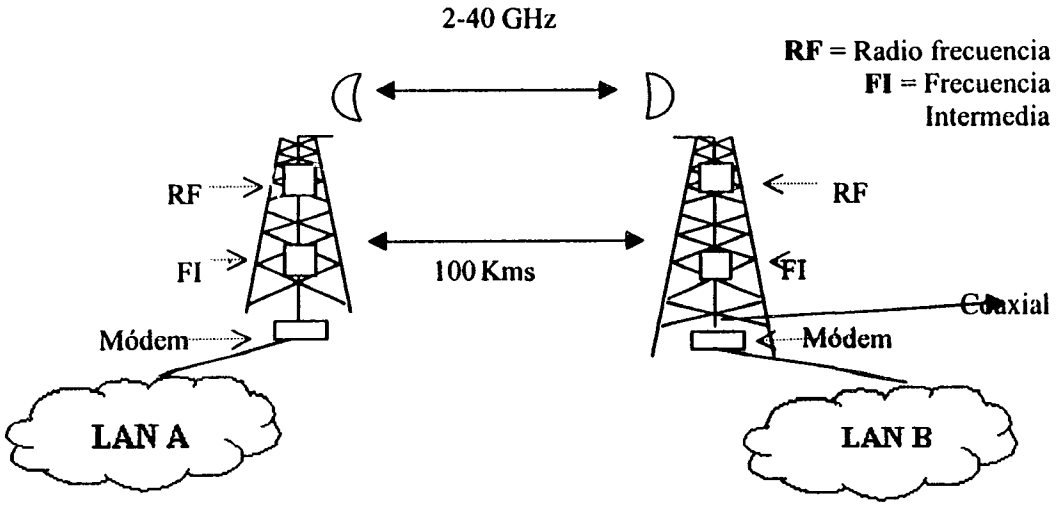


Figura 2.3 Enlace vía microondas.

2.2.3 WAN

Las redes WAN's son aquellas que cubren una gran área geográfica (como la red telefónica), típicamente son redes conmutadas, consisten de un conjunto interconectado de nodos conmutados. Una WAN puede ser de circuitos o paquetes conmutados, cada estación esta unida a uno de los nodos.

Hasta hace poco tiempo, las WAN's proveían una capacidad relativamente baja a los subscriptores. Para la transmisión de datos, tanto en una red de conmutación de paquetes como en una de circuitos conmutados por medio de un módem, eran comunes cantidades de 9600 bps o menos con un servicio como el E1 se podían obtener transmisiones mas altas, operando a 2.048 Mbps. El desarrollo más importante recientemente en WAN's ha sido el desarrollo de la red digital de servicios integrados (ISDN) de la cuál provee servicios de conmutación de paquetes y circuitos a velocidades de mas de 2.048 Mbps.

El continuo desarrollo de la fibra óptica ha conducido a la estandarización de altas transmisiones para WAN's. El esfuerzo más importante en este sentido es la estandarización de una red digital de servicios integrados de banda ancha (B-ISDN) que usa cell-relay (liberación de celdas) en vez de conmutación de circuitos.

Aparte de los medios de transmisión guiados las redes WAN se pueden comunicar mediante microondas y enlaces satelitáles.

La comunicación mediante satélite tiene algunas propiedades que la hacen atractiva para la comunicación en WAN's. El satélite esta constituido por uno o más dispositivos receptor, transmisor, para uno de los cuales escucha una parte del espectro, amplificando la señal de entrada y después la retransmite a otra frecuencia, para evitar los efectos de interferencia con las señales de entrada. El flujo dirigido hacia abajo puede ser muy amplio y cubrir una gran parte de kilómetros de diámetro.

Se encuentran a una altura aproximada de 36000 kms por encima de Ecuador, el periodo del satélite es de 24hrs, por lo cual giraría a la misma velocidad que lo hace la tierra. La capacidad que posee el satélite de recibir y transmitir se debe aun dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de gigahertz.

Se han establecido acuerdos internacionales sobre quien puede ser uso de que ranuras orbitales y de que frecuencias. Las bandas de 3.7 a 4.2 GHz y 5.923 a 6.425 GHz, se han designado como frecuencia de asignación de telecomunicación vía satélite, para flujos de información provenientes del satélite o hacia el satélite respectivamente. En la actualidad estas bandas a las que en general se les conoce como una banda 4/6 GHz, se encuentran superpobladas porque también se utilizan por los proveedores de servicios para enlaces terrestres de microondas. Las bandas superiores siguientes, se encuentran para la telecomunicación, son las de 12/14 GHz, las cuáles no se encuentran todavía congestionadas. Las bandas de frecuencia de 20/30 GHz también se han reservado para el área de telecomunicaciones, pero el costo del equipo necesario para utilizarlas es todavía elevado. La señal que transmite una estación terrestre tiene distinta frecuencia que la que devuelve el satélite. De ésta manera se impide que los canales de subida y de bajada se interfieran, ya que trabajan en bandas de frecuencias diferentes.

Un satélite típico divide su ancho de banda de 500 GHz en aproximadamente una docena de receptores-transmisores, cada uno con un ancho de banda de 36 MHz. Cada receptor-transmisor puede emplearse para codificar un flujo de información de 50 Mbps, 800 canales de voz digitalizada de 64 Kbps, o bien otras combinaciones diferentes. Además dos receptores-transmisores pueden utilizar señales con diferente polarización, de tal manera que emplee la misma banda de frecuencia sin que exista el problema de interferencia.

En los primeros satélites, la división de los receptores-transmisores en canales era estática, separando el ancho de banda de frecuencias fijas. En la actualidad, el canal se separa en el tiempo, primero una estación, después otra, y así sucesivamente siendo este esquema más flexible. A este sistema se le denomina multiplexión en el tiempo.

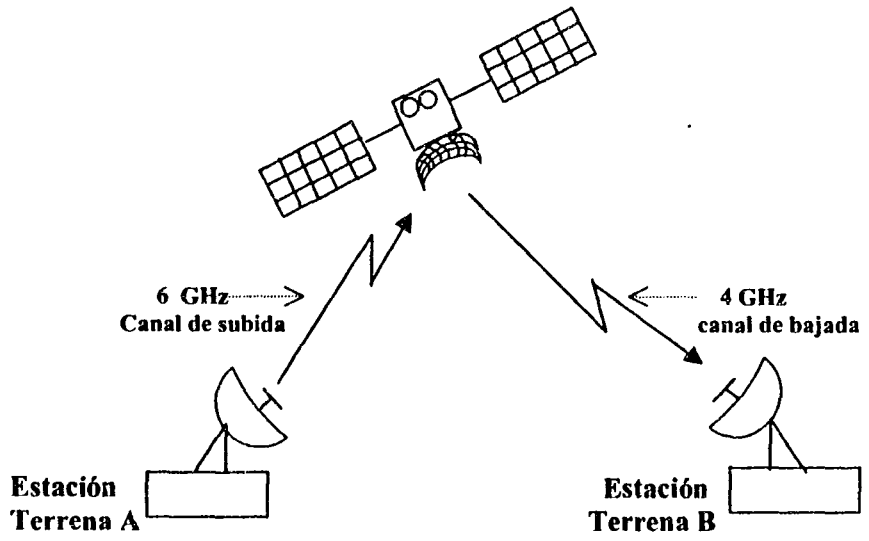


Figura 2.6 Comunicación vía satélite.

2.2.4 GAN

Una GAN (red de área global) se refiere a una red aún mayor que la WAN. Es un tipo de red que permite la comunicación en cualquier parte del mundo. Ejemplos de este tipo de red son: INTERNET, la red de American Express y el sistema IRIDIUM.

Dentro de muy poco tiempo, importantes sistemas satelitáles de órbita baja comenzarán a operar con el objetivo de proporcionar una red global de telecomunicaciones, las cuáles brindarán servicios de voz, datos, fax y radiolocalización en cualquier momento y lugar. Lo anterior revolucionará las comunicaciones para los viajeros de negocios, los residentes de áreas rurales y equipos de emergencia durante desastres naturales además de todas aquellas personas que requieran la conveniencia de un aparato telefónico inalámbrico con un solo número en todo el mundo (sin necesidad de familiarizarse con equipos diferentes) ya que seguirán gozando de los servicios a los que están suscritos en su lugar de origen. El sistema de telefonía (que cubre el planeta con comunicación ininterrumpida) satelital garantizará todo tipo de comunicación digital con excepción del video. El mecanismo de este tipo de sistemas es el siguiente: el satélite enruta la llamada al que se encuentre mas próximo del punto destino y baja la señal a una estación terrena para finalmente enviarla sobre las redes públicas hasta

el otro extremo. La mayoría de los aparatos de bolsillo serán bimodales, es decir, funcionarán tanto en redes satelitales como celulares, e incluso por PCS (sistemas personales de comunicación) y serán compatibles con normas terrestres.

Tabla 2.2 Características de LAN's, MAN's, WAN's y GAN's

RED	Velocidad de transmisión	Distancia cubierta
Red de Area Local (IEEE 802)	1-20 Mbps	< 25 km
FDDI	100 Mbps	<200 km
Red de área Metropolitana(IEEE 802.6)	30 Mbps- 1 Gps	<160 km
Red tradicional de área Amplia	10 Kbps-1.5 Mbps	ilimitada
Red de área Amplia de alta velocidad	50 Mbps-1Gbps	ilimitada

2.3 TOPOLOGIAS FISICAS

Las principales características en una tecnología que determinan la naturaleza de una red son:

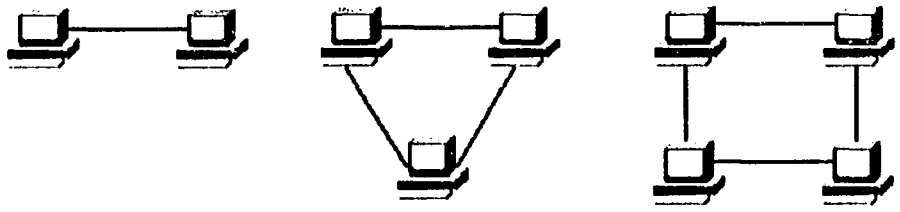
- topología
- medio de transmisión
- técnica de control de acceso al medio

Juntas determinan en gran medida el tipo de datos que pueden ser transmitidos, la velocidad y eficiencia de las comunicaciones, así como también las clases de aplicaciones que la red puede soportar.

La topología se refiere a la forma en la cuál los puntos terminales o estaciones de red están interconectados.

Una topología esta definida por la distribución de los enlaces de comunicación y los elementos de conmutación, y determina la ruta de los datos que pueden ser usadas entre cualquier par de estaciones.

Hagamos un breve paréntesis para explicar la diferencia entre tener una red de comunicación y conectar directamente cualquier par de dispositivos. Refiriéndonos a la figura 2.2, cada dispositivo tiene un enlace directo llamado enlace punto apunto con cada uno de los demás dispositivos. Si hay N dispositivos, entonces se necesitan N(N-1) enlaces, y cada dispositivo requiere (N-1) puertos de entrada y salida(I/O), incrementándose de esta manera el costo del sistema en cuanto a la instalación del cableado y



a) 2 estaciones b) 3 estaciones c) 4 estaciones

el hardware de I/O.

Figura 2.8 Problema con la conexión directa entre dispositivos

La solución fue introducir una red de nodos conmutados con habilidad para dirigir los mensajes, creando enlaces lógicos y eliminando la necesidad de muchas conexiones físicas directas (fig. 2.2). De esta forma cada dispositivo o estación se conecta directamente a un nodo de la red y se comunica a otras estaciones. Este método –el uso de una cantidad de nodos conmutados- generalmente no es usado en redes locales, debido a que como las distancias que cubre son pequeñas no se requieren nodos. Para esto se han desarrollado topologías que no requieren o requieren de solo un nodo de conmutación intermediario.

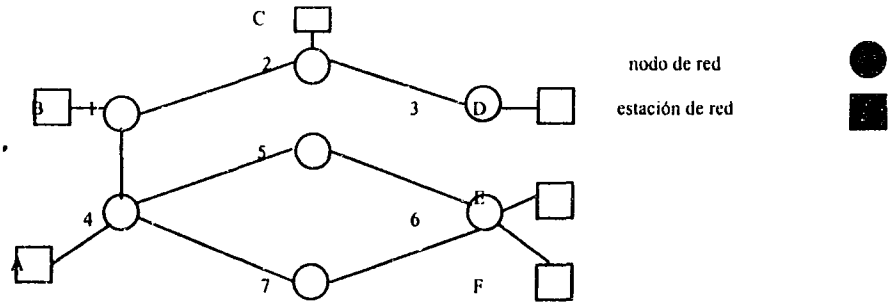
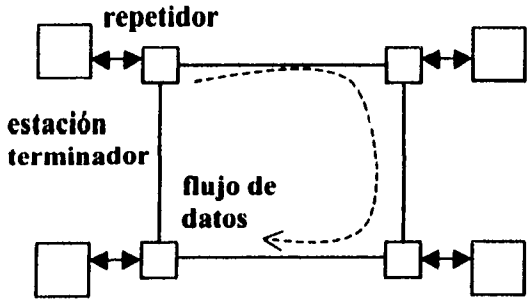


Figura 2.9 Red de conmutación

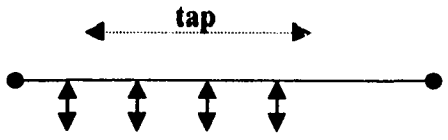
Las topologías mas utilizadas para construir redes son: estrella, bus, anillo y árbol (fig. 2.3). A su vez, estas pueden ser utilizadas como parte de otra red que utilice topologías mucho mas complejas.

Los factores que se deben considerar al analizar y elegir una topología son:

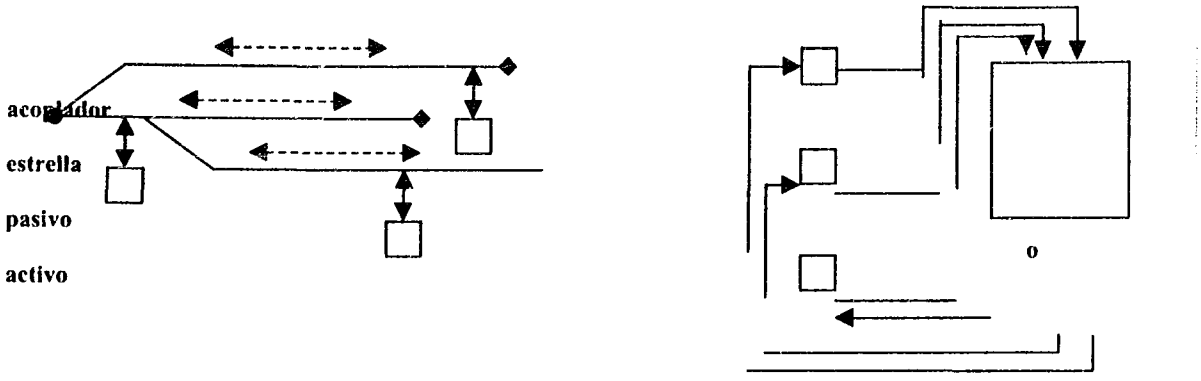
a) Flexibilidad para agregar o eliminar nodos.
b) Repercusiones de alguna falla sobre algún nodo.
c) Protocolo de comunicación física.
d) Problemas en el flujo de la información.
e) Versatilidad en el diseño del cableado.
f) Posibilidad de crecimiento.
g) Costo/beneficio



(a) anillo



(b) bus



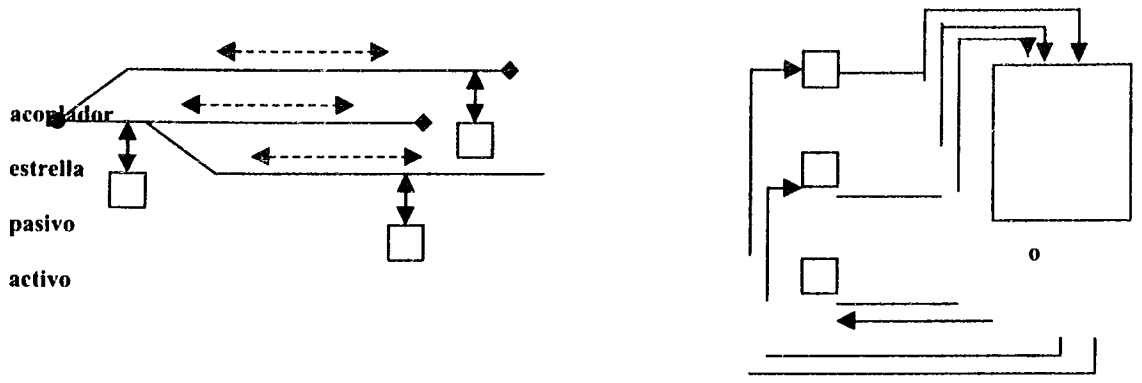
(c) árbol (d) estrella

Figura 2.10. Topologías físicas

2.3.1 ANILLO

La red consiste en un conjunto de repetidores unidos por enlaces punto a punto en donde el primero esta conectado al último. Así cada repetidor participa en 2 conexiones. El repetidor es un dispositivo capaz de recibir datos y transmitirlos bit por bit a otra conexión tan rápido como los recibe sin almacenarlos. Los enlaces son unidireccionales, los datos son transmitidos en una sola dirección y todos están orientados hacia el mismo sentido. Cada estación se une a la red por medio de un repetidor. Los datos son transmitidos en paquetes. Así por ejemplo, si la estación x desea trasmitir un mensaje a la estación y, ésta descompone el mensaje en paquetes. Cada paquete contiene una porción de los datos mas información de control incluyendo la dirección de la estación y. Los paquetes son introducidos al anillo uno a la vez y circula hacia el otro repetidor. La estación y reconoce su dirección y copia los paquetes como van pasando. Debido a que muchos dispositivos comparten el anillo, se necesita el control para determinar cuando cada estación puede insertar paquetes. Esto regularmente se hace con alguna forma de control distribuido, cada estación contiene un acceso lógico que controla la transmisión y recepción. El control de la red puede ser centralizado o distribuido entre varios nodos.

En caso de ser centralizado, uno de los nodos actúa como controlador de forma tal que, como todos los mensajes tienen que pasar a través de él, si no hay fallas, puede verificarse el correcto funcionamiento de la red en caso de que hubiera falla, tomar las medidas para solucionarlas.



(c) árbol (d) estrella

Figura 2.10. Topologías físicas

2.3.1 ANILLO

La red consiste en un conjunto de repetidores unidos por enlaces punto a punto en donde el primero esta conectado al último. Así cada repetidor participa en 2 conexiones. El repetidor es un dispositivo capaz de recibir datos y transmitirlos bit por bit a otra conexión tan rápido como los recibe sin almacenarlos. Los enlaces son unidireccionales, los datos son transmitidos en una sola dirección y todos están orientados hacia el mismo sentido. Cada estación se une a la red por medio de un repetidor. Los datos son transmitidos en paquetes. Así por ejemplo, si la estación x desea trasmitir un mensaje a la estación y, ésta descompone el mensaje en paquetes. Cada paquete contiene una porción de los datos mas información de control incluyendo la dirección de la estación y. Los paquetes son introducidos al anillo uno a la vez y circula hacia el otro repetidor. La estación y reconoce su dirección y copia los paquetes como van pasando. Debido a que muchos dispositivos comparten el anillo, se necesita el control para determinar cuando cada estación puede insertar paquetes. Esto regularmente se hace con alguna forma de control distribuido, cada estación contiene un acceso lógico que controla la transmisión y recepción. El control de la red puede ser centralizado o distribuido entre varios nodos.

En caso de ser centralizado, uno de los nodos actúa como controlador de forma tal que, como todos los mensajes tienen que pasar a través de él, si no hay fallas, puede verificarse el correcto funcionamiento de la red y en caso de que hubiera falla, tomar las medidas para solucionarlas.

Si es distribuido, el control se ejerce de manera conjunta entre varios nodos. El flujo de información estará limitado por el ancho de banda del medio de comunicación. Ya que cada estación de trabajo tiene que retransmitir cada mensaje, si existiera un número elevado de estaciones, el retardo introducido por la red puede ser muy grande para ciertas aplicaciones.

Ventajas:

- La capacidad de transmisión se reparte equitativamente entre todos los usuarios.
- Es fácil localizar los nodos y enlaces que originan errores.
- Se simplifica al máximo la distribución de mensajes.
- El tiempo de acceso no es muy grande.
- Se pueden conseguir velocidades muy altas
- Permite utilizar distintos medios de transmisión.
- Se requiere un mínimo de inteligencia en los nodos.

Desventajas:

- La confiabilidad de la red depende de los repetidores.
- Es necesario un dispositivo monitor.
- Es difícil incorporar nuevos dispositivos sin interrumpir la actividad de la red.

En una red en anillo el mensaje que entra debe contener la dirección física donde se debe entregar el mensaje en el anillo. Existen varios protocolos que pueden operar en comunicaciones punto a punto incluidas en un anillo por conmutación de paquetes y Token Ring. Estos protocolos son el CSMA (Acceso Múltiple por Detección de portadora) y el Token Passing Ring que veremos mas adelante.

Si es distribuido, el control se ejerce de manera conjunta entre varios nodos. El flujo de información estará limitado por el ancho de banda del medio de comunicación. Ya que cada estación de trabajo tiene que retransmitir cada mensaje, si existiera un número elevado de estaciones, el retardo introducido por la red puede ser muy grande para ciertas aplicaciones.

Ventajas:

- La capacidad de transmisión se reparte equitativamente entre todos los usuarios.
- Es fácil localizar los nodos y enlaces que originan errores.
- Se simplifica al máximo la distribución de mensajes.
- El tiempo de acceso no es muy grande.
- Se pueden conseguir velocidades muy altas
- Permite utilizar distintos medios de transmisión.
- Se requiere un mínimo de inteligencia en los nodos.

Desventajas:

- La confiabilidad de la red depende de los repetidores.
- Es necesario un dispositivo monitor.
- Es difícil incorporar nuevos dispositivos sin interrumpir la actividad de la red.

En una red en anillo el mensaje que entra debe contener la dirección física donde se debe entregar el mensaje en el anillo. Existen varios protocolos que pueden operar en comunicaciones punto a punto incluidas en un anillo por conmutación de paquetes y Token Ring. Estos protocolos son el CSMA (Acceso Múltiple por Detección de portadora) y el Token Passing Ring que veremos mas adelante.

2.3.2 TOPOLOGIAS DE ARBOL Y BUS

Con la topología de bus, la red de comunicación es simplemente el medio de transmisión –sin switches ni repetidores. Todas las estaciones se adhieren a través del hardware de interface adecuado, directamente a un medio de transmisión lineal o bus. La transmisión de cualquier estación se propaga a lo largo del medio y es recibida por todas las demás estaciones. La información viaja en ambos sentidos, por lo que es necesario prevenir las colisiones (antes de transmitir cada nodo debe verificar sí el bus esta disponible). Para ello el protocolo apropiado es el CSMA/CD(Carrier Sense Multiple Access/Collision Detection). Esta configuración presenta gran flexibilidad en cuanto a incrementar o disminuir el número de estaciones de trabajo.

Ventajas:

- El medio de transmisión es totalmente pasivo.
- Es fácil conectar nuevos dispositivos.
- Se puede utilizar toda la capacidad de transmisión disponible.
- Fácil de instalar.
- Es particularmente adecuada para tráfico muy alto.

Desventajas:

- La interfaz con el medio de transmisión ha de hacerse por medio de dispositivos inteligentes.
- Los dispositivos no inteligentes requieren unidades de interfaz muy sofisticadas.
- El sistema no reparte adecuadamente los recursos.
- La longitud de transmisión no sobrepasa los 2 km.

La topología de árbol es una generalización de la topología de bus. El medio de transmisión es un cable ramificado no cerrado, la ultima estación o estaciones no se conectan a la primera. La distribución del árbol empieza en un punto conocido como *headend.* Uno o más cables salen del *headend* y cada uno de ellos pueden tener ramificaciones. Esas ramificaciones a su vez

pueden tener a su vez más ramas lo que da paso a una distribución totalmente compleja. Y de igual manera, la transmisión de cualquier estación se propaga a través del medio y puede ser recibida por todas las demás estaciones. Para ambas topologías el medio es llamado multipunto.

2.3.3 TOPOLOGIA DE ESTRELLA

Cada estación esta conectada dispositivo central por medio de dos conexiones punto a punto, uno para la transmisión en cada dirección. La transmisión desde cualquier estación llega al nodo central y es retransmitida a todos los demás enlaces que salen de él. De esta manera, aunque la disposición física sea una estrella, lógicamente es un bus. Lo usual es que el nodo central ejerza todas las tareas de control y posea todos los recursos de la red.

Esta configuración presenta flexibilidad para incrementar o disminuir el número de estaciones de trabajo, ya que las modificaciones necesarias no representan ninguna alteración de la estructura. Si sé presentará una falla en alguna estación la repercusión en el comportamiento de la red es muy baja, en cambio si se presentara la falla en el nodo central se produciría un problema muy grande al afectar a toda la red.

El flujo de información puede ser elevado y los retardos introducidos por la red son pequeños si la mayor parte de ese flujo ocurre entre el nodo central y los nodos periféricos. Si la comunicación se produce entre las estaciones, el sistema se vería restringido por la posible congestión del nodo central.

Ventajas:

- Ideal para configuraciones en las que hay que conectar muchas estaciones a una misma estación.
- Se pueden conectar terminales no inteligentes.
- Las estaciones pueden tener velocidades diferentes dependiendo del medio de transmisión.
- Se puede obtener un alto nivel de seguridad.
- Es fácil detectar y localizar averías.

Desventajas:

- Es susceptible a averías en el nodo central.
- Elevado precio debido a la complejidad de la tecnología que se necesita en el nodo central.
- La instalación de los cables resulta muy cara.
- La actividad que debe soportar el nodo central hace que normalmente las velocidades de transmisión sean inferiores a las que se consiguen en las topologías de bus y anillo.

2.4 COMPONENTES DE UNA RED LAN

Los componentes de una red LAN son los siguientes:

- Estación de trabajo
- Tarjeta de red
- Sistema operativo
- Servidor
- Concentrador
- Repetidor
- Terminador de red
- Bridge
- Router
- Gateway
- Conmutador
- LAN switch

Estación de trabajo: es la máquina que tiene el usuario y que utiliza recursos de hardware y de software para comunicarse con otras máquinas y hacer uso de recursos compartidos por la red.

Tarjeta de red: para que una estación de trabajo se pueda comunicar en la red, se le debe agregar una tarjeta de interface de red que se inserta en algún slot libre del bus. Usan un protocolo de acceso que determina la topología de la red.
Las tareas que realiza son:

- Mover los datos entre la tarjeta de red y la memoria principal de la máquina.
- Generar los buffers para retener temporalmente que se encuentran en el cable o memoria de la estación de trabajo.
- Formar paquetes de información. Estos tienen 3 secciones: encabezado, datos y trailer. Los tamaños y formatos de los paquetes varían de acuerdo con el protocolo de acceso, esquema de direccionamiento y otras variables.
- Conversión paralelo – serial – paralelo. Los datos que se generan en la computadora vienen en paralelo (8 bits a la vez) pero deben viajar en el cable en forma serial asíncrona (1 bit a la vez). La tarjeta se encarga de llevar a cabo esta conversión.
- Codificar y decodificar los datos a enviar.
- Accesar al cable. Antes de que cualquier dato pueda ser enviado, la tarjeta debe conseguir el acceso al cable, dependiendo del tipo de protocolo de acceso que utilice.
- Antes de que el paquete pueda ser transmitido, otra tarjeta de red debe estar lista para recibirlo. Para esto existe un periodo corto de comunicación llamado reconocimiento (handshake).
- Cuando el paquete está listo es enviado a la línea por el transceiver, lo cuál le permite ir a su destino.

Sistema operativo: los sistemas operativos proveen la capacidad multiusuario a un conjunto de estaciones de trabajo, reside en el servidor y cada estación de trabajo tiene un componente de software que le permite accesar al servidor. Se incluye la administración del disco duro y funciones de comunicación, administración de la red para el manejo de seguridad. El software de la red está diseñado generalmente para una topología y protocolo de acceso en particular aunque actualmente se ofrece mayor flexibilidad.

Servidor: un servidor de red es una computadora que corre el sistema operativo de la red, el software de aplicación y tiene la función de administrar la red y sus recursos. Ahí se procesan las comunicaciones, acceso a usuarios, etc. Se pueden tener varios servidores para manejar varios recursos de hardware y software.

Concentrador: permite conectar estaciones y reconfigurar el sistema. También se encarga de aislar los nodos problemáticos mediante el punto de concentración. El concentrador puede incluir una interfaz en el que el

usuario instalará fibra óptica para una parte de la red y coaxial o par trenzado para otra región de la misma.

Repetidor: es usado para extender la longitud física del cable o el número de estaciones permitidas por segmento. Hace la función de amplificación de la señal. Esto permite que la señal original transmitida vaya mas lejos que lo que permitirían los límites de atenuación del medio de transmisión. Los repetidores dependen de dos variables: la arquitectura de red y el medio de transmisión usado.
En resumen:

- opera en la capa física de OSI
- regenera o repite señales físicas
- usado para extender una LAN

Terminador de red: es un dispositivo utilizado en redes que utilizan coaxial para balancear la impedancia en el sistema y no tener problemas de colisión en la información. Son impedancias de 50 ohms.

Bridge: son usados para segmentar redes basado sobre el tráfico de la red. La segmentación divide la red en subconjuntos lógicos, manteniendo el tráfico de las estaciones de trabajo que frecuentemente se comunican sobre una LAN. Son dispositivos los cuáles operan en la capa de enlace de datos y transmite tramas entre redes. Muchos puentes operan sobre redes de igual arquitectura, tal como de Token Ring a Token Ring o de ethernet a ethernet, sin embargo esto no es necesariamente una regla ya que el estándar IEEE 802 contiene un común denominador en el formato LLC 802.2 y el uso de 2 o 6 octetos de direccionamiento. Entonces, un puente puede ser construido entre LANs 802.x diferentes.
En resumen:

- opera en la capa de enlace de datos de OSI
- lógicamente separa segmentos de red
- independiente de protocolos de capas más altas
- usado para el manejo de tráfico de una LAN

Router: segmenta el tráfico de la red basado en la dirección de la red destino (no en la dirección física de la red destino (no en la dirección física de la estación de trabajo). Opera en la capa de Red de OSI y determina la dirección correcta de la red a la cuál va a enviar el paquete de datos. El router es un dispositivo de protocolo dependiente y opera co. ·ına dirección

jerárquica que es definida por ese protocolo. Un buen ejemplo de un sistema de direccionamiento jerárquico es el número telefónico, el cuál está dividido en varias secciones: clave del país, área, central telefónica y número de línea.

Entonces, un router IP tendría necesariamente dificultad para entender un esquema de direccionamiento que no corresponde a su propio formato, tal como uno usado por los protocolos ISO

En resumen:

- opera en la capa de red de OSI
- lógicamente separa subredes
- depende del protocolo de capa de red
- debe tener conocimiento de la topología de la red
- usado para la comunicación entre redes

Gateway: Son dispositivos de aplicación especifica que conectan diferentes arquitecturas de redes. Pueden operar en todas las capas de OSI. Puede ser responsable para conectar sistemas de e-mail incompatibles, convertir y transferir archivos de un sistema a otro o habilitar la interoperatividad entre sistemas operativos diferentes.

En resumen:

- opera en las capas más altas de OSI
- es dependiente de la aplicación del usuario
- usado para comunicación aplicación a aplicación

Switch: Dispositivos que organizan rápidamente la información por el manejo de hardware, entre puntos de contacto. No entiende información hacia arriba (capas superiores). En redes LAN es un dispositivo de alta velocidad que direcciona paquetes entre segmentos a nivel de enlace de datos. La mayoría de los switches LAN se suele llamar conmutación de tramas. Los switches LAN a veces se categorizan de acuerdo con el método que utilizan para reenviar el tráfico: conmutación rápida de paquetes y conmutación de paquetes almacenados y enviados. Los switches multicapa son un subconjunto inteligente de switches de LAN .

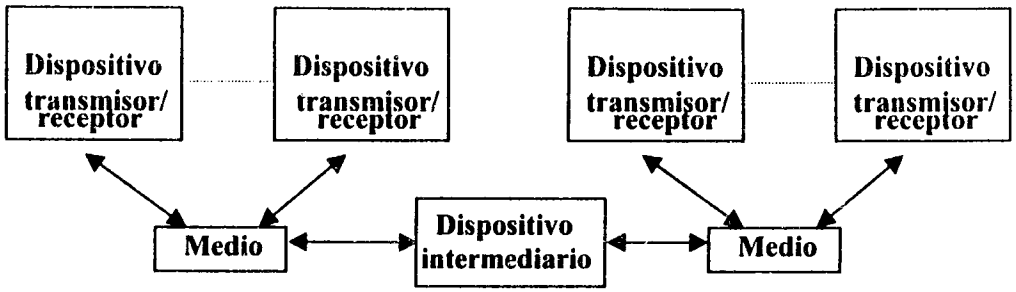
2.5 MEDIOS DE TRANSMISION

El medio de transmisión es la ruta física entre el transmisor y el receptor en una red de comunicación. En la figura 2.4 podemos observar los elementos básicos de un sistema de transmisión. La forma más común es el enlace punto a punto entre dos dispositivos transmisores/receptores. Se pueden utilizar uno o dos dispositivos intermediarios para compensar la atenuación o algunos deterioros en la comunicación. Los enlaces punto a punto son utilizados en la topología de anillo para conectar repetidores y en la de estrella para conectar dispositivos al conmutador central. También se utilizan para conectar dos redes locales que se encuentren ubicadas en diferentes lugares. Los enlaces multipunto son usados para conectar varios dispositivos, como en la topología de bus o árbol. Se pueden adherir algunos otros dispositivos al medio de comunicación como repetidores (señales digitales) o amplificadores (señales analógicas) para extender la longitud del medio.

Los medios de transmisión pueden ser clasificados como dirigidos o no dirigidos. En ambos casos la comunicación viaja en forma de ondas electromagnéticas. En el medio dirigido, las ondas son guiadas a lo largo de una ruta física (como por ejemplo el par torcido, el cable coaxial, y la fibra óptica), al contrario del medio no dirigido donde la atmósfera y el aire son ejemplos de medios de transmisión, los cuáles proveen un camino para transmitir ondas electromagnéticas pero no las guían.

teléfono	**cable coaxial**	**repetidor**
módem	**par torcido**	**amplificador**
multiplexor	**fibra óptica**	
etc.	**etc.**	

a) comunicación punto a punto



b) comunicación multipunto.

Figura 2.11 Diagrama de un bloque del sistema de transmisión

Algunas características que podemos utilizar para describir los medios de transmisión son:

- Descripción física: naturaleza del medio de transmisión.
- Características de transmisión: incluye las señales que son usadas sean analógicas o digitales, técnica de modulación, capacidad y rango de frecuencia sobre el cual ocurre la transmisión.
- Conectividad: punto a punto a multipunto.
- Alcance geográfico: la distancia máxima que puede haber entre los puntos de la red.
- Inmunidad al ruido: resistencia del medio a la contaminación en la transmisión de datos.
- Costo relativo: basado en el costo de los componentes, instalación y mantenimiento.
- Eficiencia (fallas mínimas)
- Soporte de servicios actuales y futuros con infraestructura económicamente óptima.

2.5.1 CABLE COAXIAL

Este es el medio de transmisión más versátil. Hay dos tipos de cable coaxial: el de 75 ohm, el cuál es el estándar utilizado en sistemas CATV y el de 50 ohm. Este es utilizado para la señalización digital con FDM llamada banda base, el de 75 ohm es usado para señalización analógica con FDM llamada de banda ancha.

Descripción física: Consiste de dos conductores uno exterior que por lo general se presenta en forma de malla y que cubre al conductor interior. Este último es lo que constituye el núcleo y consiste de un alambre de cobre duro el cual se encuentra rodeado por un material aislante se logrará una mejor percepción de este en la figura 2.5

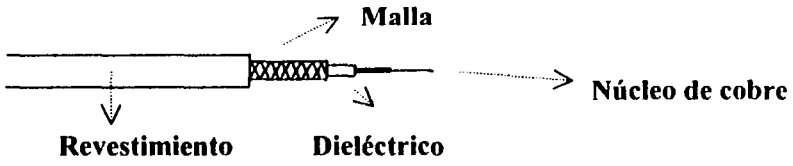


Figura 2.12 Cable coaxial

Características de transmisión: El cable de 50 ohms es utilizado para la transmisión digital. Generalmente se usa la codificación Manchester. Se logran velocidades de mas de 10 Mbps. El cable CATV es utilizado para señales analógicas o digitales, en el caso de señales analógicas se logran frecuencias de 300 a 400 Mhz. Los datos analógicos como video o audio, pueden ser manejados con cable CATV de la misma forma como se difunde el radio y la TV. Los canales de TV tienen asignado un ancho de banda de 6 Mhz y el canal de radio requiere mucho menos. Por lo tanto se pueden transmitir una cantidad de canales por el cable usando FDM. Cuando se utiliza FDM, al cable CATV se le conoce como coaxial de banda ancha. El espectro de frecuencias del cable es dividido en canales cada uno de los cuales transmite señales analógicas. Datos analógicos también pueden ser transmitidos por un canal, se han utilizado varios esquemas de modulación como ASK, FSK y PSK. La eficiencia del módem determinara el ancho de banda requerido para soportar una velocidad de datos dada. Para lograr

velocidades de mas de 20 Mbps, se han tomado dos métodos. Ambos requieren que el ancho de banda del cable de 75 ohms sea dedicado para esta transferencia de datos; no se utiliza FDM. Uno de estos métodos es usar la señalización digital en el cable y se logra una velocidad de 50 Mbps con este esquema. Otra alternativa es usar PSK; usando una transmisión de 150 Mhz y también se puede lograr una velocidad de 50 Mbps.

Conectividad: El cable coaxial es aplicable en configuraciones punto a punto y multipunto. El cable coaxial de banda base de 50 ohms puede soportar hasta 100 dispositivos por segmento, con la posibilidad de tener sistemas más grandes uniendo los segmentos con repetidores. El de banda ancha de 75 ohms puede soportar miles de dispositivos pero el uso de este a altas velocidades (50 Mbps) introduce problemas técnicos que limitan el número de dispositivos de 20 a 30. Los módems de RF se usan como interfaz de red. Los sistemas de banda ancha necesitan módems para convertir datos en señales analógicas y viceversa. El módem es capaz de transmitir y recibir utilizando una amplia gama de frecuencia. Cuando una red cubre largas distancias (por ejemplo un edificio de varios pisos) es necesario el uso de amplificadores, además es necesario el uso de acopladores de dirección para asegurar que las señales transmitidas por los dispositivos de la red sola se van a enviar en dirección al dispositivo de control. Existen también tomas independientes con dos conectores, uno para transmisión y otro para recepción. Las estaciones se pueden conectar sin que resulte afectado el resto de los usuarios. Para reducir el ruido y las señales no deseadas (armónicas) se utilizan terminadores instalados en los extremos de la línea. El cable coaxial utiliza conectores BNC o N (neil) con rosca.

Tipo		
RG-8 y RG-11	z= 50 Ω	(coaxial grueso)
RG-58	z=50 Ω	(coaxial delgado)
RG-59	z=75 Ω	
RG-62	z=93 Ω	(arcnet)

Alcance geográfico: Las distancias máximas en un cable típico de banda base son limitadas a unos cuantos kilómetros. Las redes de banda ancha pueden cubrir un radio de unas cuantas decenas de kilómetros. La transmisión a alta velocidad (50 Mbps), digital o analógica es limitada a 1 km aproximadamente. Debido a la alta velocidad de la transmisión de los

datos, la distancia física entre las señales sobre el bus es muy pequeña, por lo que solo se puede aceptar una atenuación muy pequeña o ruido.

Inmunidad al ruido: La inmunidad al ruido para el cable coaxial depende de la aplicación y la implementación. En general, es superior que la inmunidad que ofrece el par torcido para frecuencias más altas.

Costo: Se sitúa entre el costo del par torcido y de la fibra óptica.

Ventajas:

- Fácil instalación.
- Se puede aprovechar instalaciones existentes.
- Gran capacidad para soportar aplicaciones como voz, datos y video.
- Compatible con los estándares de redes de datos (Ethernet, Token Ring).
- No es susceptible a interferencias externas o ambientales.
- Buena relación costo beneficio.

Sin embargo, sobre todas estas ventajas cabe mencionar que el cable coaxial no es muy confiable en cuanto a conectividad ya que son sistemas muy susceptibles a fallas.

2.5.2 PAR TORCIDO

Es un medio de transmisión muy común tanto para señales analógicas como para digitales. Existen tres tipos de cable: el UTP (sin blindaje), el STP (con blindaje) y el FTP. La diferencia entre el UTP y el STP y FTP es que el primero solo cuenta con una cubierta protectora de plástico, y los últimos tienen además una malla tejida de hilos de metal además que el FTP tiene un alambre interno para eliminar emisiones electromagnéticas del cable. Este tipo de cables viene en conjuntos típicos de 2,3,4,6,12,16 y 25 pares de cables trenzados. Existen varias categorías de cable debido al grado y tipo de trenzado:

Categorías:

1 y 2: son utilizadas exclusivamente para tráfico de voz.
3: soporta 10 MHz en voz y datos, utilizado en los inicios de Ethernet.
4: 20 MHz utilizado en vos y datos, utilizado en los principios de Token Ring.
5: 100 MHz para voz y datos, utilizado para Fast Ethernet.

Cabe mencionar que el cable STP no esta como categoría 5. El cable UTP tiene una impedancia característica de 120 ohms a 100 MHz y 20°c. con una atenuación de 20 db/100 mts. Para el STP se tiene una impedancia de 85-112 ohms a 10 MHz con una atenuación de 11 db/110 mts.

Descripción física: Consiste en dos cables aislados puestos en forma de espiral con una inclinación calculada para reducir los efectos de la interferencia electromagnética que generan las señales de alta frecuencia. Pueden ir una cierta cantidad de esos pares juntos dentro de un cable envuelto por una capa protectora. Los pares tienen el grosor de 0.016 a 0.036 pulgadas.

Características de transmisión: Pueden ser usados para transmitir señales analógicas o digitales. Para las analógicas se requieren amplificadores casi cada 5 o 6 kms, para señales digitales se usan repetidores cada 2 o 3 km. El uso más común es para la transmisión analógica de voz. El par torcido tiene capacidad para mas de 24 canales de voz usando un ancho de banda mas de 268 Khz. Este tipo de medios de comunicación puede soportar frecuencias de transmisión de datos de mas de hasta 100 Mhz sin grado de atenuación alto.

Conectividad: El par torcido puede ser utilizado para aplicaciones punto a punto o multipunto. Como medio multipunto es una alternativa de menor costo y de menor desempeño que un cable coaxial pero soporta menos estaciones y el uso punto a punto es muy común. Los conectores mas utilizados son el RJ45 y el
RJ11. Existen varios tipos de configuración para RJ45 (recomendación ISO 8877) entre los que destacan el EIT/TIA, 568A y el de ATT:

Tabla 2.2 Configuraciones principales para RJ45

ATT	568 A	ATT
T1 +5	BCO/AZUL	T1 -5
R1 -4	AZUL	R1 -4
T2 +3	BCO/NARANJ	T2 +1
R2 -6	A	R2 -2
T3 +2	NARANJA	T3 +3
R3 -1	BCO/VERDE	R3 -6
T4 +7	VERDE	T4 +7
R4 -8	BCO/CAFÉ	R4 -8
	CAFE	

Alcance geográfico: Provee fácilmente transmisión de datos punto a punto en un rango de 15 kms o más. El par torcido para redes locales generalmente se utiliza para redes que se encuentran dentro de un mismo edificio.

Inmunidad al ruido: comparado con otros medios, el par torcido es limitado en distancia, ancho de banda y velocidad en la transmisión de datos. El medio es totalmente susceptible a la interferencia y al ruido debido a su fácil acoplamiento con los campos electromagnéticos. Las señales en los pares adyacentes pueden interferir con cada uno de los demás (éste fenómeno es conocido como cross-talk). Se han tomado algunas medidas para reducir esas imperfecciones como por ejemplo, cubriendo el cable con un trenzado metálico o enfundándolo, usando diferentes largos de trenzado, etc.

Costo: El par torcido es menos caro que el cable coaxial o la fibra óptica. Sin embargo, debido a sus limitaciones de conectividad, los costos de instalación pueden ser casi iguales a los otros medios.

Ventajas:

- Fácil y rápida instalación.
- Compatibilidad con los diferentes estándares de comunicación (Token Ring, Ethernet, Arcnet, StarLan, FDDI).
- Ancho de banda hasta 100 Mbps.
- Distancias máximas de transmisión: UTP 150 mts. , STP 500 mts.
- Buena relación costo/beneficio.

Existe una tecnología llamada HDSL (High Bit Rate Digital Subscriber Line), la cuál puede soportar 2.084 Mbps para una conexión digital en dos pares de cobre sobre una distancia superior a 4.8 kms. HDSL es una plataforma diseñada para alcanzar la hendidura entre limitantes de una red basada en cobre y las promesas de la fibra óptica y multimedia. La implementación de este sistema implica un costo bajo comparado con la reparación de enlaces de cobre y transmisión de fibra. La calidad de transmisión es buena. Esta plataforma puede ser utilizada para transportar una variedad de servicios que incluyen líneas privadas E1, conmutaciones E1, video comprimido, video en tiempo real, videoconferencia, televisión interactiva, interacción de estaciones de trabajo, acceso al rango primario ISDN (Red Digital De Servicios Integrados) y a las interconexiones LAN. Existen equipos con plataforma HDLS como E1 HDSL y CAMPUS 384 de la marca PAIR GAIN que incluyen unidades modulares remotas y de oficina central. La unidad de oficina central brinda soporte a mas de 16 módulos desplegados desde un bastidor estándar. La unidad remota ofrece más de 4 puertos fraccionarios E1 en G703, V.35 y V.36 sobre de uno a tres pares con grosor de cobre de 24/26 AWG. Además dentro de las capacidades de administración de redes, la plataforma E1 HDLS incluye características opcionales, administrativas, de mantenimiento y provisión entre algunas otras

Características y beneficios

- Largas distancias.
- Bajo costo.
- Instalación rápida.
- Alta confiabilidad.
- Flexible.
- Compacta y mínima energía.
- Puerto de mantenimiento (RS 232 o RJ 45 DCE).
- Indicadores de estado y alarma.
- Migración a implementación por fibra.
- Múltiples interfaces de red de datos.

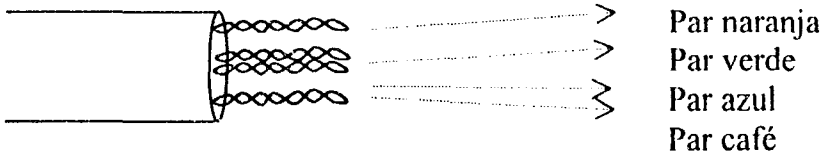


Figura 2.13 UTP de 4 pares.

2.5.3 FIBRA OPTICA

Uno de los progresos más importantes en la transmisión de información ha sido el desarrollo de sistemas de comunicación de fibra óptica. Las continuas mejorías en su desempeño y el decline de su precio junto con las ventajas que ofrece, la han hecho cada vez mas atractiva.

Construcción básica de un sistema de transmisión por medio de fibra óptica: los elementos básicos de un sistema de transmisión óptico son la fibra óptica, la fuente óptica y el detector (estos últimos operan como conversores eléctrico/óptico) y en especial desempeña un papel muy importante el desarrollo de diodos láser tan pequeños como transistores. Fig. 2.14

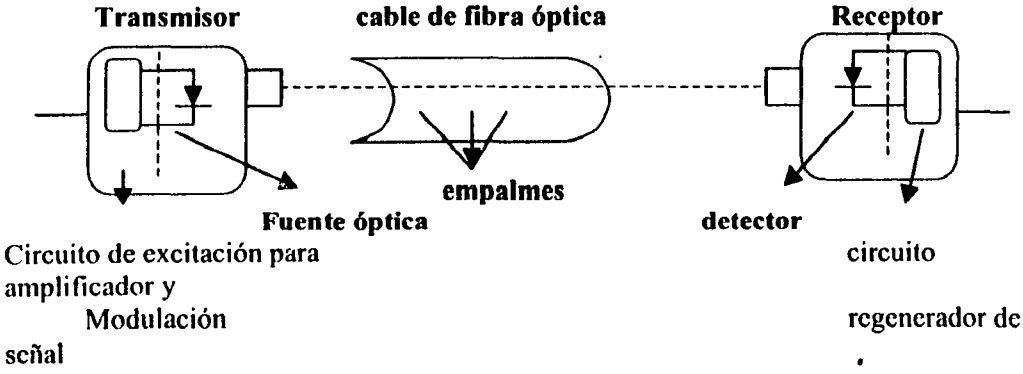


Figura 2.14 Construcción básica de un sistema de transmisión con fibra óptica.

Las siguientes características son las que distinguen a la fibra óptica del UTP o cable coaxial:

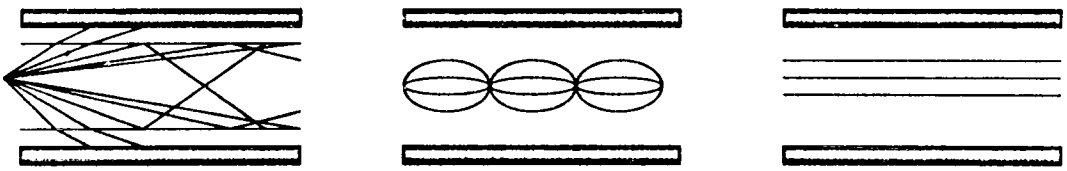
- Gran capacidad: el ancho de banda y por lo tanto la velocidad de datos son muy grandes; se han demostrado velocidades de 2 Gbps sobre varias decenas de km.
- Menor tamaño y peso más ligero: la fibra óptica es considerablemente mas delgada que el cable coaxial o que el para torcido. Esto implica una gran ventaja ya que al establecerlos en los conductos ocupan una cantidad de espacio mucho menor y la correspondiente reducción de peso reduce los requerimientos de estructuras de soporte (esto en fibras para interiores).
- Atenuación mas baja: la atenuación es relativamente mas baja para la fibra óptica que para el cable coaxial o el par torcido y es constante sobre un rango amplio.
- Aislamiento electromagnético: los sistemas de fibra óptica no son afectados por campos electromagnéticos externos. El sistema no es vulnerable a interferencia o impulsos de ruido. Igualmente las fibras no irradian energía.

Descripción física: una fibra óptica es un medio muy delgado (2 a 125 mm), flexible, capaz de conducir un rayo óptico. Se pueden utilizar varias clases de vidrio o plástico para su creación. La fibra de plástico no es muy cara y se pude utilizar en enlaces de distancias cortas para las cuáles, pérdidas moderadamente altas son aceptables. Un cable de fibra óptica es de forma cilíndrica y consiste de dos regiones con diferentes índices de refracción: el núcleo y el revestimiento. El núcleo es la parte mas interna, consiste de una o mas fibras muy delgadas de vidrio o plástico y cada una de estas tienen un recubrimiento de vidrio o plástico que tiene propiedades ópticas diferentes que las que tiene el núcleo. La capa más externa es el revestimiento y esta hecho de plástico y otros materiales puestos por capas para protegerlo contra la humedad, aplastamiento y otros riesgos que se puedan presentar en el medio ambiente.

Características de transmisión: la fibra óptica transmite una señal codificada como un rayo de luz mediante un reflejo total interno. Este reflejo puede ocurrir en cualquier medio que tenga un índice de refracción mas alto que el medio envolvente. La fibra óptica actúa como una guía de onda para

frecuencias en un rango de 10^{14} a 10^{15} Hz, la cual cubre el espectro visible y la parte del espectro infrarrojo.

La figura 2.15 muestra el principio de la transmisión por fibra óptica. La luz entra al núcleo, los rayos con ángulos poco profundos son reflejados y propagados a lo largo de la fibra; otros rayos son absorbidos por el recubrimiento. A esta forma de propagación se le conoce como multimodo de índice abrupto, haciendo referencia a la cantidad de ángulos que se reflejan. Cuando el radio del núcleo es reducido, se reflejan menos ángulos. Reduciendo el radio del ángulo en el orden de una longitud de onda, solo un ángulo o modo puede pasar: el rayo axial. Esto provee un desempeño superior que el multimodo: con la transmisión multimodo existen muchas rutas de propagación, cada una con una longitud diferente y por lo tanto con diferente tiempo para cruzar la fibra. Esto causa que las señales se propaguen fuera de tiempo y limita la velocidad a la cuál los datos pueden ser correctamente recibidos. Si hay una sola ruta de transmisión con solo un modo de transmisión tal distorsión no puede ocurrir. Finalmente, al variar el grado de refracción del núcleo, se logra un tercer tipo de transmisión conocido como multimodo de índice gradual. Como podemos ver se logran capacidades muy grandes, excediendo por mucho al cable coaxial y al par torcido.



(a) **Multimodo** **(b)Multimodo de índice gradual** **(c)Monomodo**

Figura 2.15 Modos de transmisión de fibra óptica

Se utilizan 2 tipos de fuentes de luz en los sistemas de fibra óptica: el diodo emisor de luz (LED) y el diodo de inyección láser (ILD). El LED es un dispositivo de estado sólido que emite luz cuando se aplica una corriente. El ILD trabaja sobre el principio del láser, es estimulado para producir un rayo super radiante de un ancho de banda estrecho. El LED es menos costoso, opera sobre un rango de temperatura más grande y tiene una larga vida operacional. El ILD es más eficiente y puede mantener velocidades de transmisión más grandes. El detector que se utiliza al final para convertir la

luz en energía eléctrica es el fotodiodo y de estos se utilizan dos tipos: el PIN y el APD. El PIN tiene un segmento de silicon intrínseco entre las capas P y N de un diodo. El APD, fotodiodo avalancha, es similar en apariencia pero usa un campo eléctrico mas fuerte. El PIN es menos caro y menos sensible que el APD.

Para transmitir información digital sobre fibra óptica se utiliza comúnmente AFK (modulación intensiva) Para un LED, el uno binario es representado por un breve pulso de luz y el cero por la ausencia de esta. En los transmisores láser se emite un bajo nivel de luz, este representa el cero binario, mientras que una onda de luz con amplitud más grande representa otra señal. Algunas aplicaciones prácticas actuales se encuentran en un rango de unos cuantos cientos de megabits por segundo sobre unos pocos kilómetros. Hay una relación entre la longitud de onda empleada, el tipo de transmisión y la velocidad lograda. Tanto en monomodo como multimodo soportan diferentes longitudes de onda de luz y pueden usar como fuentes de luz el LED o el láser. En la fibra la luz se propaga mejor en 3 diferentes ventanas de longitudes de onda, centradas sobre los 850, 1300 y 1500 nanómetros.

La pérdida es menor a altas longitudes de onda, permitiendo velocidades más altas sobre grandes distancias.

Muchas aplicaciones locales actualmente utilizan como fuente de luz al LED 850-nm. Además este es relativamente barato, generalmente esta limitado a velocidades que están por encima de los 100 Mbps y a distancias de unos cuantos kilómetros. Para lograr velocidades mas altas y mayores distancias se necesita un LED de1300 nm o láser. Aunque la fuente de 850 nm esta muy bien para LANs. Las capacidades de transmisión mas altas y distancias más grandes logradas en la actualidad requieren fuentes de luz de 1500 nm. Actualmente una simple frecuencia portadora se utiliza en la transmisión por fibra óptica.

Los avances en la transmisión por fibra óptica permitirán sistemas FDM (multiplexaje por división de longitud de onda) o multiplexación por división de color.

Conectividad: el uso más común de la fibra óptica es para enlaces punto a punto. Se han implementado sistemas experimentales multipunto usando una topología de bus pero resulta demasiado caro para ser práctico en la actualidad. Sin embargo un simple segmento de fibra óptica puede soportar mas conexiones que el par torcido o el coaxial debido a una pérdida de poder más baja, características de atenuación menores y a un potencial de ancho de

banda más grande. La fibra óptica utiliza acopladores y conectores ST, SC, bicónicos, SM con una fijación de la fibra óptica al conector por medio de curados epóxicos o luz ultravioleta. Las fibras ópticas normalmente se colocan en paneles dentro de un LIU (Unidad de Interconexión de luz) para su administración y soporte.

Alcance geográfico: la tecnología actual soporta transmisiones sobre distancias de 6 a 8 kms sin repetidores, por lo que la fibra óptica es comúnmente para enlaces de redes locales punto a punto.

Inmunidad al ruido: la fibra óptica no es afectada por interferencia electromagnética o ruido. Esta característica permite altas velocidades sobre grandes distancias y provee una excelente seguridad.

Costo: los sistemas de fibra óptica son mas caros que el par torcido y el cable coaxial en términos del precio por pie y los componentes que se requieren como son transmisores, receptores, conectores, etc. Si bien los costos del par torcido y el cable coaxial no están a la baja, los avances en la ingeniería deberán reducir el costo de la fibra óptica para ser competitivos con esos medios.

Ventajas:

- Aplicaciones de alta velocidad.
- Gran ancho de banda.
- Puede propagar una señal sin necesidad de amplificador desde 2 hasta 10 kms.
- Transmisión de voz, datos y video por el mismo canal.
- No genera señales eléctricas y/o magnéticas a su alrededor.
- Baja atenuación de menos de 1 dB/km.
- Inmune a interferencias electromagnéticas externas.
- Excelente tolerancia a factores físicos ambientales.
- Estándares que se han desarrollado o que han adoptado la fibra óptica (FDDI, Ethernet, Arcnet, Token Ring, etc.).
- Ofrece la mayor capacidad de adaptación a nuevas normas de comunicación.

2.6 SISTEMAS DE TRANSMISION

Los datos que se transmiten en una red usan 3 esquemas distintos: banda base banda ancha y banda portadora. Estos esquemas describen como se mueven los datos dentro del cable. Es importante decidir que método se va a tener en la red, debido a que estos varían en su flexibilidad, crecimiento de la red, costó de instalación y volumen del trafico que soportan.

2.6.1 SISTEMAS DE BANDA BASE

Una red de banda base es definida como aquella que usa señalización digital pero en general, el termino banda base se refiere a la transmisión de una señal analógica en su forma original sin modulación.

Las señales digitales son insertadas en la línea como pulsos de voltaje generalmente usando la codificación Manchester diferencial. El espectro de frecuencias del medio es usado para formar la señal, FDM no puede ser utilizado.

La transmisión es bidireccional, es decir, una señal insertada en cualquier punto sobre el medio se propaga en ambas direcciones a los extremos donde es absorbida. La señalización digital requiere una topología de bus. Los sistemas de banda base se pueden extender solo una distancia limitada, cerca de 1km. a lo mucho. Esto es debido a la atenuación de la señal, las cuales es muy pronunciada a altas frecuencias, causando en los pulsos una debilitación de la señal por lo que extender la comunicación sobre distancias mas grandes no es muy recomendable.

Coaxial banda base. Las formas mas conocidas del bus LAN de banda base usan cable coaxial. Muchos sistemas de cable coaxial de banda base usan un cable especial de 80-ohms en vez del cable estándar CATV de 75 ohms debido a la impedancia del cable. Impedancia es una medida de cuanto voltaje debe ser aplicado al cable para lograr la potencia de una señal dada. Para señales digitales, el cable de 50-ohms provee una mejor inmunidad contra el ruido electromagnético de baja frecuencia. El coaxial banda base simple consiste de un tramo no ramificado de coaxial con una resistencia en cada lado. El valor de la resistencia es igual a la impedancia del cable, esto previene la reflexión absorbiendo cualquier señal del cable.

Como en cualquier sistema de transmisión, existen factores que afectan la velocidad de transmisión de datos, como pueden ser la longitud

del cable, el número de conexiones y las características eléctricas de los receptores y transmisores de un sistema de coaxial banda base. Esto es cierto debido a la siguiente razón: cuando una señal se propaga a lo largo del medio de transmisión, la integridad de dicha señal se daña debido a la atenuación, al ruido y a otros factores.

A una velocidad de transmisión mas baja, los pulsos individuales de una señal digital duran mas y pueden ser recuperados si hubieran daños o deterioros de una manera más fácil que a velocidades más altas. La especificación ethernet y el estándar IEEE especifican el uso de cable de 50-ohm con un diámetro de 0.4 pulgadas y una velocidad de 10 Mbps. Con esos parámetros, la longitud máxima del cable es de 500 metros. Se permite un máximo de 100 conexiones. En IEEE este sistema se conoce como 10BASE5. Los dos primeros dígitos son la velocidad de transmisión dada en megabits por segundo, las cuatro letras son la abreviatura del medio (banda base); y los últimos dígitos dan la longitud máxima de cable en cientos de metros.

La figura 2.16 de la especificación ethernet, ilustra componentes típicos y sus funciones. Los principales componentes son:

- Transceiver
- Cable transceiver
- Controlador
- Cable coaxial de 50-ohms
- Terminadores de 50-ohms

TABLA 2.3 Especificaciones IEEE para redes locales de bus coaxial de banda base.

Parámetro	10 bases 5	10bases 2
Velocidad	10 Mbps	10Mbps
Longitud máxima de segmento	500m.	200m.
Alcance de la red	2500m.	1000m.
Nodos por segmentos	100	30
Espacio entre nodos	2.5m.	0.5m.
Diámetro del cable	0.4in	0.25in

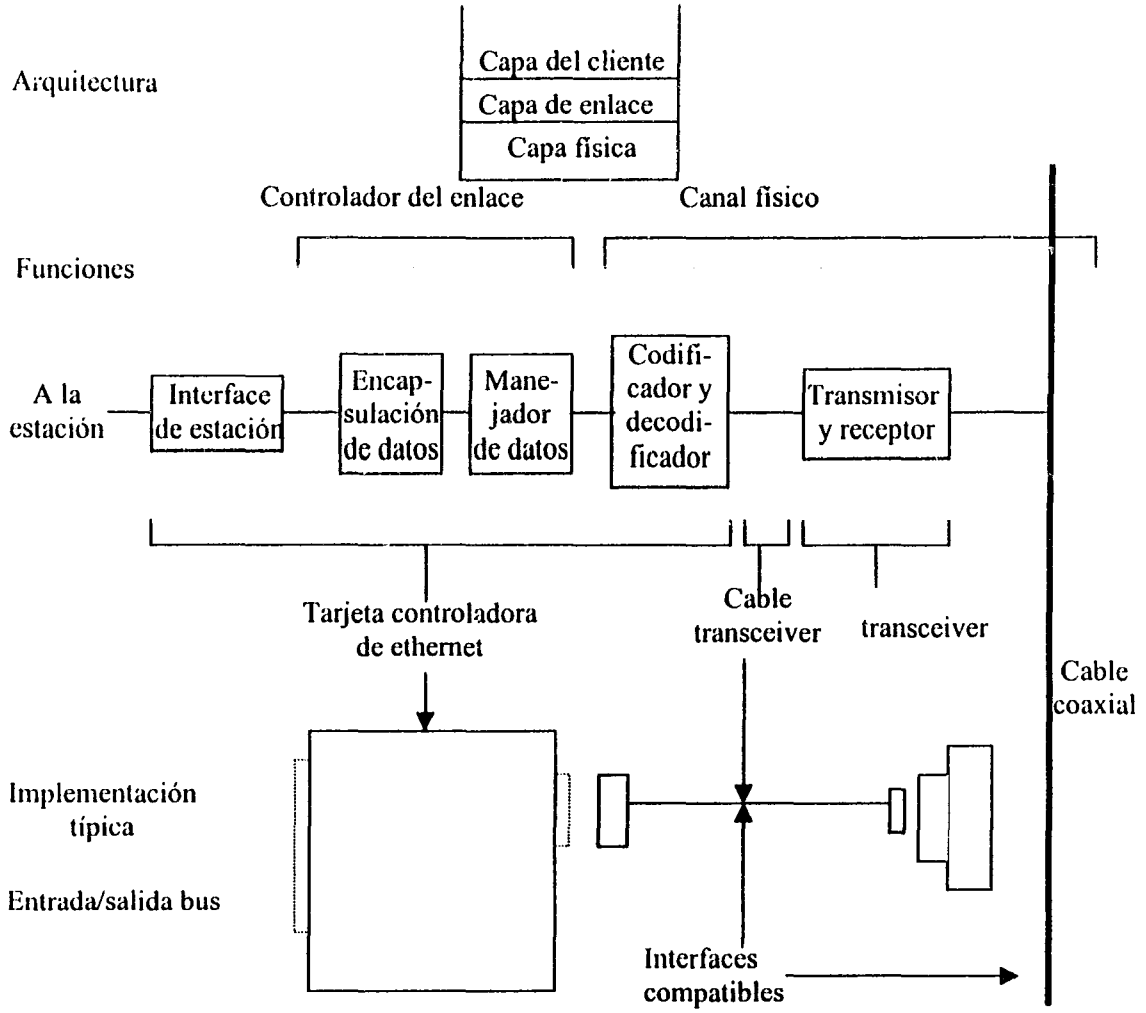


Figura 2.16 Arquitectura ethernet e implementación típica

El cable transceiver comprende 2 pares torcidos y conecta el MAU (transceiver) al controlador, el cuál contiene el volumen de inteligencia requerida para comunicarse sobre una LAN. El cable provee energía al MAU y pasa señales de datos entre éste y el controlador al igual que las señales de control. Incluye una señal de colisión del MAU al controlador.

El controlador es una implementación de todas las funciones requeridas para manejar el acceso al cable coaxial para el intercambio de paquetes entre el coaxial y la estación adjunta. Finalmente el cable de 50

ohms y los terminadores absorben señales, previniendo la reflexión de los extremos del bus.

Estos 5 componentes son suficientes para construir un bus LAN de banda base de mas de 1km. con mas de 100 estaciones. Para requerimientos más grandes, se necesita otro componente que es el repetidor. El estándar 802 permite un máximo de 4 repetidores entre 2 estaciones cualquiera, extendiendo la longitud efectiva del cable de 2.5 Km.

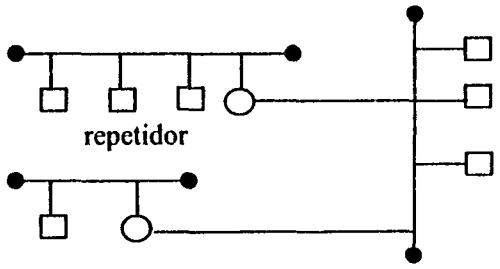


Figura 2. 17 Ejemplo de un sistema de banda base con 3 segmentos y dos repetidores.

2.6.2 SISTEMAS DE BANDA ANCHA

Este sistema permite que varias señales de información se transmitan en un solo cable simultáneamente ya que el cable se divide en varios canales, los cuáles, llevan cada uno una señal de frecuencia diferente, por lo tanto, este sistema puede transmitir datos, comunicaciones telefónicas señales de TV y otros tipos de tráfico electrónico.

Pueden cubrir mayores distancias que las de banda base. Estos ofrecen flexibilidad en la transmisión de señales, pero es mucho mas caro que los

anteriores debido al equipo necesario y al soporte técnico requerido para diseñar un sistema con un balance apropiado de las frecuencias de la banda para cada tipo de señal.

En general, banda ancha hace referencia a cualquier canal que tenga un ancho de banda más grande que un canal de voz(4KHz).

En el contexto de redes locales, el término se refiere al cable coaxial sobre el cuál se utiliza señalización analógica. Cuando utilizamos el término banda ancha nos referimos a sistemas que pueden manejar FDM, y cuando hablamos de portadora nos referimos a sistemas que manejan solo una señal analógica.

Tabla 2.4 Técnicas de transmisión

BANDA BASE	BANDA ANCHA
Señalización digital	Señalización analógica(requiere módem RF)
El ancho de banda es consumido por la señal. No se utiliza FDM	Se puede utilizar FDM-canales múltiples de datos, audio y video
Bidireccional	Unidireccional
Topología de bus	Topología de bus o árbol
Distancia: unos cuantos kms	Distancia: mas de 10 kms

Como ya habíamos mencionado, la banda ancha implica el uso de señalización analógica. Se puede aplicar FDM: el espectro de frecuencia del cable puede ser dividido en canales o secciones de ancho de banda. Los canales separados pueden soportar tráfico de datos, señales de radio y televisión. Los componentes del sistema de banda ancha permiten separar y unir operaciones; por lo tanto las topologías de bus y árbol son posibles.
Se logra una distancia mucho más grande (decenas de kms) comparada con la banda base. Esto es debido a que las señales analógicas que transporta los datos digitales se pueden propagar a distancias mas grandes antes que el ruido y la atenuación puedan dañar a los datos.

2.6.2.1 DIVISIONES DE FRECUENCIA DE CABLE COMÚN

Configuraciones dobles y divididas

Al igual que en sistemas de banda base, las estaciones que están en una LAN de banda ancha están unidas al cable por medio de un *TAP*. A diferencia de la banda base, la banda ancha es un medio unidireccional; las *TAPS* permiten que se inserten señales dentro del medio para propagarlas solo en una dirección. La razón fundamental de esto es que es *INFEASIBLE* construir amplificadores que pasen las señales de una frecuencia en ambas direcciones. Estos significa que solo aquellas estaciones que se encuentran conectadas de una estación transmisora pueden recibir sus señales. Pero para lograr una conectividad completa es claro que se necesita dos rutas de transmisión. Esas rutas están unidas a un punto de la red conocido como *HEADEND*. En la topología de bus, el *HEADEND* es simplemente el fin del bus, en la de árbol, es la raíz del árbol ramificado. Todas las estaciones transmiten sobre una ruta hacia el *HEADEND* (de entrada). Las señales llegan al *HEADEND* y se propagan a una segunda ruta hacia el *HEADEND* (de salida). Todas las estaciones reciben la ruta de salida.

Físicamente, se utilizan dos configuraciones para implementar las rutas de entrada y salida. En la configuración de cable doble, las rutas de entrada y salida están en cables separados y el *HEADEND* es un conector pasivo que se encuentra entre los dos. Las estaciones envían y reciben sobre la misma frecuencia.

Por el contrario, en una configuración dividida (*split*) las rutas de salida y entrada están en diferentes bandas de frecuencia sobre el mismo cable. Los amplificadores bidireccionales pasan frecuencias bajas de entrada y frecuencias altas de salida. Entre las bandas de frecuencia de entrada y salida hay una banda de guarda que no transporta señales y sirve como un separador únicamente. El *HEADEND* contiene un dispositivo que convierte las frecuencias de entrada en frecuencias de salida. Este dispositivo puede ser analógico o digital. Un dispositivo analógico, conocido como traductor de frecuencia, convierte un bloque de frecuencias de un rango a otro. Un dispositivo digital conocido como demodulador, recupera el dato digital de la señal analógica de entrada y lo transmite a la frecuencia de salida. De esta manera, un demodulador provee una mejor calidad de señal al remover todo el ruido y la atenuación acumulados y transmitir la señal limpia.

Los sistemas divididos están categorizados por la asignación de frecuencia de las dos rutas (tabla 2.5).

Tabla 2.5 Divisiones de frecuencia de cable común

FORMATO	BANDA DE FREC. DE ENTRADA	BANDA DE FREC. DE SALIDA	MAXIMO ANCHO DE BANDA DE LOS 2 SENTIDOS
Subsplit	5 a 30 Mhz	54 a 400 Mhz	25 Mhz
Midsplit	5 a 116 Mhz	168 a 400 Mhz	111 Mhz
High-split	5 a 174 Mhz	232 a 400 Mhz	168 Mhz
Dual-cable	40 a 400 Mhz	40 a 400 Mhz	360 Mhz

El formato *SUBSPLIT* provee la forma más fácil para mejorar los sistemas de cables de una sola dirección para operar en ambas direcciones. El *SUBSPLIT* tiene limitada su utilidad para las redes de área local debido a que un ancho de banda de solo 25 MHz esta disponible para la comunicación en ambos sentidos. *MIDSPLIT* es más conveniente para LAN's debido a que provee una distribución más equitativa del ancho de banda. La especificación *HIGH-SPLIT* ha sido desarrollada para proveer un mayor ancho de banda en los dos sentidos para sistemas de cables divididos.

Las diferencias entre las configuraciones son mínimas. El sistema *SPLIT* es útil cuando se encuentra ya una instalación de cable en la edificación. Si se necesita una gran cantidad de ancho de banda o se anticipa esta necesidad, entonces un sistema *DUAL-CABLE* es el indicado. Aparte de estas consideraciones, se toma en cuenta también el costo y el tamaño.

2.6.2.2 COMPONENTES DE BANDA ANCHA

Los sistemas de banda ancha utilizan los componentes del cable de TV, incluyendo el cable coaxial de 75 ohms. Todos los puntos terminales tienen un terminador de 75 ohms para absorber las señales. La banda anc

es conveniente para un radio de decenas de kilómetros desde el HEADEND y cientos e incluso miles de dispositivos. Los principales componentes del sistema son:

- Cable
- Terminadores
- Amplificadores
- Acopladores direccionales
- módems
- controladores

Los cables usados en redes de banda ancha son de tres tipos: cable troncal, cable de alimentación y cable de bajada.

El cable troncal forma la espina dorsal de un sistema LAN. Los cables troncales usan una construcción semirígida y por lo mismo no es flexible, puede ser doblado pero no muchas veces ni muy fácilmente. La parte externa del cable esta hecha de aluminio sólido. Líneas troncales vienen en seis tamaños, en un rango de 0.412 al pulgada de diámetro. Entre más grande sea el diámetro del cable es menor la atenuación. El cable semirígido tiene excelentes características de rechazo de ruido y puede ser usado dentro o fuera de la edificación. Típicamente un cable troncal se extenderá desde unos cuantos kilómetros hasta decenas de kilómetros. Los cables de distribución o de alimentación, son usados para distancias más cortas y para cables ramificados. Pueden ser semirígidos o flexibles y típicamente tienen un diámetro de 0.4 a 0.5 pulgadas. A diferencia del cable troncal, el cable de alimentación es generalmente para uso interno.

La elección del cable depende de varios criterios:

- Las limitaciones físicas de la ruta: cables de diámetro más angosto son más fáciles de instalar.
- El nivel de señal requerido para la distribución de la red: cables con un diámetro más grande tienen menor pérdida de señal.
- Normas de construcción locales y nacionales.

El cable flexible usado comúnmente como cable de alimentación tiene la designación RG-11. Con un diámetro de 0.405 pulgadas y con una

resistencia al ruido menor que el cable semirígido, la distancia es limitada a aproximadamente 800 metros.

Los cables de bajada son usados para conectar salidas y estaciones de distribución de cables. Son cortos (de 10 a 50 pies) y por lo tanto no necesitan un diámetro muy grande; aunque la atenuación por unidad de longitud es más grande para un cable más angosto, las distancia corta significa que el total de atenuación será más pequeña aún con un cable angosto. Los cables usados son flexibles e incluye los cables RG-59 (0.242 de diámetro), RG-6(0.332 pulgadas) y RG-11(0.405).

Los amplificadores pueden ser usados en cables distribuidos o troncales para compensar la atenuación. La atenuación en un cable es una función creciente de frecuencia. Para sistemas divididos, los amplificadores deben ser bidireccionales, pasando y amplificando frecuencias mas bajas en una dirección y aumentando frecuencias en otra.

Los acopladores direccionales proveen una forma para dividir una entrada dentro de dos salidas y combinando dos entradas dentro de una salida. *TAPS* son usados para conectar cables de bajada y por lo tanto estaciones a la LAN.

Los módems son necesarios para la conversión entre los datos digitales de las estaciones adjuntas y la señal analógica del medio. Están en uso una variedad de técnicas de modulación, las dos más comunes, las cuáles están endosadas para su uso en el estándar IEEE-802 son DPSK (Differential Phase-Shift keying) usada con IEEE-802.3 y duobinario AM/PSK, usado con IEEE-802.4.

. Una característica común de casi todos los módems LAN de banda ancha es el uso *SCRAMBLING*. Esto da a los datos una naturaleza pseudoaleatorea que ayuda al receptor a extraer la información (un bit en cada unidad de tiempo) También mejorar las características espectrales de la señal, dándole un mayor poder de distribución uniforme, oponiéndose a las potencialmente fuertes líneas espectrales discretas en datos NON SCRAMBLED. Esto da a la señal mejor resistencia al ruido finalmente, se necesitan controladores como en la banda base, para proveer el servicio LAN básico.

2.7 ORGANIZMOS DE ESTANDARIZACION.

2.7.1 ISO

En 1981, se estableció una relación formal entre IEEE y ECMA para desarrollar los estándares de comunicación. El resultado fue la Organización Internacional de Estándares (ISO) del modelo referencial de interconexión de sistemas abiertos (OSI: Open Systems Interconection). El modelo OSI define una estructura para la implantación de protocolos de comunicación en 7 capas o niveles para comunicarse a través de redes locales y metropolitanas. Las capas del modelo OSI están representadas jerárquicamente cada capa es dependiente directamente de la que está debajo de ella, manteniendo una interface con la de arriba y la de abajo. Esta interface es flexible y permite que los diseñadores puedan implementar varios protocolos de comunicación y continuar así bajo estándares.

La capa 1 del modelo OSI esta implementado por el hardware (incluye la especificación de las características mecánicas eléctricas de la conexión física), la capa 2 por una combinación de hardware y software, las 5 capas superiores están implementadas básicamente por el software y las capas 3, 4 y 5 se describen como el nivel subred de la red.

Las 7 capas son las siguientes:

1)capa física: aquí se lleva a cabo el intercambio de señales eléctricas que representan los datos y la información de control. Define que voltajes deben ser usados para representar un cero y un uno, cuantos pines debe tener un conector de red, etc., las especificaciones mecánicas y eléctricas de la conexión física. En síntesis esta capa define la topología de la red.

2)capa de enlace: toma la información a partir de los bits que da el nivel físico y la pone en un medio de transmisión. También se pueden incluir tareas de control de tráfico. En esta capa se involucra hardware (tarjetas de red, repetidores, bridges, multiplexores, etc.) y software (protocolos de bajo nivel como Token Passing, CSMA/CD, etc.). En resumen esta capa define el protocolo que se debe seguir para accesar a la red y poder enviar y recibir información.

3) capa de red: aquí se llevan a cabo operaciones de enrutamiento en la red y entre redes, control de direccionamiento de fuentes y destinos. Esta capa debe conocer la topología de la red de comunicaciones y elegir la trayectoria adecuada en una transmisión. Otras funciones incluyen los servicios que se proporcionan a la capa de transporte, congestión, control y conexión de múltiples redes al mismo tiempo.

4) capa de transporte: esta capa es el corazón de los protocolos jerárquicos. Su tarea es hacer posible y efectivo el transporte de datos sobre la capa de red de una máquina fuente a una máquina destino. Utiliza los servicios de la capa de red y proporciona servicios a la capa de sesión. Realiza funciones de segmentación de la información, calidad del servicio, administración de mensajes, secuencialización de mensajes y mapeo de transporte.

5) capa de sesión: establece, mantiene y termina una sesión con algún proceso en una máquina remota. Esta capa funciona como la interfase del usuario con el nivel de transporte. Este nivel debe dar un servicio fiable al nivel se presentación realiza tareas de: establecimiento y liberación de sesiones, administración de diálogo bidireccional alternado o simultáneo (comunicación dúplex o semidúplex), sincronización y recuperación durante la transferencia de información, aborto de tareas y el restablecimiento de la conexión en caso de que falle uno de los niveles mas bajos. Mientras se establece una conexión, el nivel de sesión debe poder negociar con la máquina remota ciertos parámetros de la conexión.

6)capa de presentación: proporciona servicios relacionados con la presentación de la información transmitida y recibida incluyendo conversión, encriptación y compresión.

7)*capa de aplicación*: se encarga de atender los procesos de aplicación del usuario final, y entonces, interactúa directamente con el software de aplicación. Contiene elementos de servicio, gestión de trabajos, intercambio de información, transferencia de archivos, acceso local y remoto, etc. Las demás capas están para satisfacer las necesidades de esta capa.

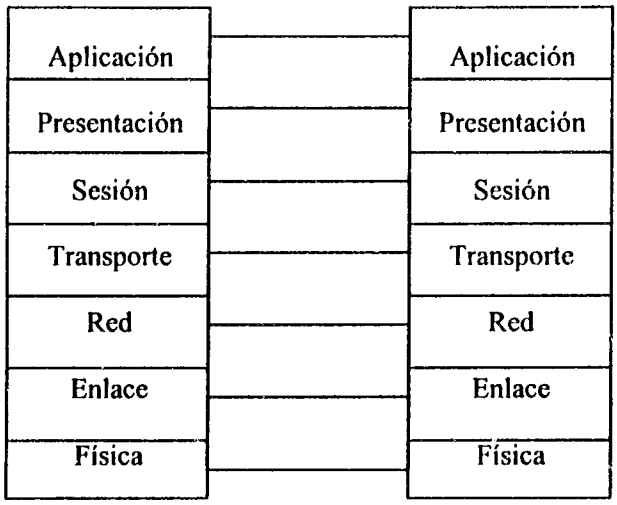


Figura 2.18 Capas del modelo OSI.

2.7.2 IEEE

Los primeros estándares para trabajo en redes LAN fueron desarrollados por la IEEE con un encabezado genérico de 802. Los trabajos desarrollos por el comité IEEE 802 ahora son organizados en los siguientes subcomités.

802.1 interfaz de alto nivel
802.2 control de enlace lógico
802.3 redes CSMA/CD
802.4 redes en Token bus
802.5 redes Token Ring
802.6 MAN-DQDB
802.7 Broadband Technical Advisory Group
802.8 Fiber Optic Technical Advisory Group
802.9 Redes de voz y datos integrados
802.10 Seguridad de la red

La razón de tener 10 grupos es debido a que las tareas para realizar la comunicación de información a través de la red es bastante complejo, por lo

cuál éstas deben ser divididas en tareas mas manejables. Esas tareas dependen extremadamente de la arquitectura de red.

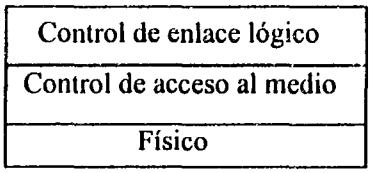


Figura 2.19 IEEE 802

La capa física es responsable de la codificación y decodificación de la señal, de la transmisión y recepción serial de bits y del medio de transmisión.

Los estándares IEEE dividen el nivel de enlace de datos en dos partes, el subnivel MAC (Media Acces Control) y el LLC (Logic Link Control). El subnivel de control de acceso al medio tiene mucho que ver con las dos funciones tradicionales del nivel, formato y detección de errores. El subnivel de control de enlace lógico extiende las funciones tradicionales del nivel de enlace de información proveyendo capacidad de multiacceso además de otras funciones.

Dentro del subnivel MAC se define tres estándares por la IEEE. El estándar 802.3 CSMA/CD (acceso múltiple por detección de portadora con detección de colisiones), el 802.4 Token bus y el 802.5 Token Ring. Cada estándar incluye algoritmos de control que permiten a las estaciones mantener control sobre el medio común, especifica la topología de la red, el medio de transmisión y la técnica de transmisión a emplear.

2.7.3 ANSI

El Instituto Nacional Americano de Estándares (ANSI) ha servido en su capacidad como administrador y coordinador del sector privado voluntario del sistema de estandarización de los Estados Unidos por 80 años. Fundado en 1918 por 5 sociedades de ingeniería y 3 agencias gubernamentales, el instituto sigue una organización de membresia privada y sin fines de lucro soportado por una diversidad de instituciones del sector público y privado. ANSI es miembro de la ISO y de la Comisión Internacional Electrónica (IEC). ANSI intenta coordinar y clarificar los estándares que se aplican, de manera voluntaria en E.U. Además de ser

FALTAN

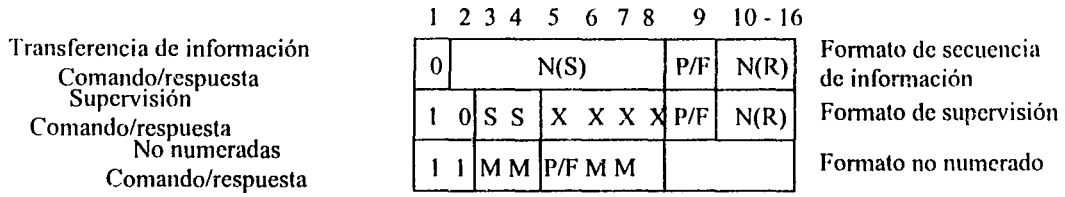
LAS

PÁGINAS

93

A

94



donde:

N(S): número de secuencia enviado
N(R): número de secuencia recibido
S: bit de supervisión

Respuestas/comandos:
00 RR (receiver ready)
01 REJ (reject)
10 RNR (receiver not ready)

M: bits modificables
X: reservado puesto en 0
P/F: comando (P)
respuesta(F)

Figura 2.21 Formatos del campo de control en tramas LLC

El formato de información se usa para la transmisión de datos secuenciales incluyendo un número de secuencia de la trama transmitida N(S) y el reconocimiento N(R) que indica la trama I esperada de la estación remota, el formato I es usado en el tipo 2. El supervisor es usado para supervisar el intercambio de tramas de información. El formato no numerado establece y desconecta el enlace lógico.

Las posibles combinaciones del formato no numerado son las siguientes:

1 2 3 4	5 6 7 8	bits		
1 1 0 0	P 0 0 0	UI	COMANDO	Tipo de operación 1
1 1 1 1	P 0 0 0	XID	COMANDO	
1 1 0 0	P 1 1 1	TEST	COMANDO	
1 1 1 1	F 1 0 1	XID	RESPUESTA	
1 1 0 0	F 1 1 1	TEST	RESPUESTA	
1 1 1 1	P 1 1 0	SABME	COMANDO	Tipo de operación 2
1 1 0 0	P 0 1 0	DISCCONECT	COMANDO	
1 1 0 0	F 1 1 0	UA		
1 1 1 1	F 0 0 0	RESPUESTA		
1 1 1 0	F 0 0 1	DM	RESPUESTA	
		FRMR	RESPUESTA	

2.8.2 IEEE 802.3 (CSMA/CD)

Este estándar se maneja en redes con una topología de tipo bus. Cuando una estación tiene un bloque de datos para enviar a través de la red, primeramente escucha si el canal se encuentra libre o alguna otra estación se encuentra transmitiendo, si este es el caso, la estación se mantiene en espera hasta que detecta que el canal se encuentra libre. Cuando no hay nadie transmitiendo, entonces la estación inicia la transmisión. Durante este proceso, la estación continúa monitoreando el canal, si el dato transmitido y el dato monitoreado en la línea difieren, entonces los datos han sido modificados y se dice que ha ocurrido una colisión. Esto es, al menos una estación inicia su transmisión de información antes de detectar que otra estación estaba accesando el canal.

Cuando se detecta una colisión, la estación detiene su transmisión de datos y emite una señal especial (jamming). Esta señal es transmitida por lo menos dos veces el tiempo que la señal tarda en recorrer toda la red de un extremo al otro para que todas las estaciones la reconozcan y detengan su transmisión de datos. Una vez que el canal se encuentra limpio, las estaciones se mantienen escuchando nuevamente. Sin embargo, las estaciones que provocaron la colisión, esperan un tiempo aleatorio, antes de reintentar su transmisión.

CSMA/CD presenta muchas ventajas por su facilidad de implementación, además con respecto a otros sistemas basados en algoritmos de contención, minimiza el desperdicio de ancho de banda del canal. Las estaciones sólo transmiten información si detentan que le canal se encuentra libre, y detienen su transmisión tan pronto como detentan que ha ocurrido una colisión en el canal.

La gran desventaja que presenta es que es eficiente solo cuando la carga de la red es baja. Si la carga de tráfico a través de la red se incrementa, la probabilidad de que ocurra una colisión incrementa. También, los intentos de retransmitir después de una colisión aumenta, incrementándose el tráfico en la red. Por consecuencia, un bloque de datos tardará un tiempo indeterminado para ser transmitido, o en algunos casos nunca se logrará transmitir.

Debido a que existen varias alternativas de configuraciones físicas, se ha desarrollado una notación concisa para distinguir las implementaciones que están disponibles:

<velocidad de transmisión en Mbps><método de señalización><longitud máxima del segmento en cientos de metros>

Las alternativas definidas son:

1. 10BASE5
2. 10BASE2
3. 1BASE5
4. 10BASET (T por par torcido)
5. 10BROAD36

La especificación 10BASE5 es el estándar original; especifica un cable coaxial de banda base a 10 Mbps, la longitud máxima de un segmento de cable es de 500 metros con un máximo de 100 conexiones por segmento. La longitud de la red puede ser extendida usando repetidores. Se permite un máximo de 4 repetidores entre cada par de estaciones, extendiendo la longitud efectiva de la red a 2.5 kilómetros.

La especificación 10BASE2 es un agregado al estándar IEEE 802.3 para cable coaxial delgado a la misma velocidad. La longitud del segmento se reduce a 185 metros con un máximo de 30 conexiones por segmento.

Otra opción, conocida como StarLAN, especifica una versión de par torcido sin blindaje y operando a 1 Mbps. Esta opción es de menor costo que las opciones de cable coaxial y es para instalaciones de computadoras que no requieren gran capacidad.

La especificación 10BASET define una topología de estrella. Un sistema simple consiste de un número de estaciones conectadas a un punto central llamado repetidor multipuerto. Las estaciones se unen al repetidor multipuerto por medio de un enlace punto a punto.
Ordinariamente; las conexiones consisten de dos pares de par torcido sin blindaje. La velocidad es de 10 Mbps usando codificación Manchester.

Finalmente se agregó la opción de banda ancha a una velocidad de 10 Mbps. Esta provee soporte para más estaciones sobre distancias más grandes a un costo mucho mayor.

La figura 2.22 nos muestra el formato de la trama:

OCTETOS	7	1	266	266	2	46 - 1500		
	PREAMBULO	SFD	DS	SA	LONGITUD	DATOS	PAD	FCS

donde:

Preámbulo: campo utilizado para la sincronización de comunicación, sigue un patrón de combinación de bits alternando 1s y 0s (1010....10)

SFD: indica el inicio de la trama y tiene una combinación fija de bits: 10101011

DA: indica la estación a la cual va dirigida la trama pudiendo ser una dirección física única, de grupo o global. Si se eligen 2 o 6 octetos de longitud esta debe ser la misma para todas las estaciones.

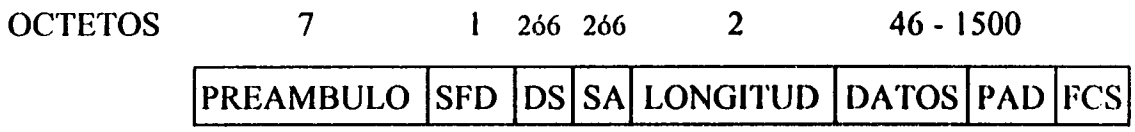
La especificación 10BASE2 es un agregado al estándar IEEE 802.3 para cable coaxial delgado a la misma velocidad. La longitud del segmento se reduce a 185 metros con un máximo de 30 conexiones por segmento.

Otra opción, conocida como StarLAN, especifica una versión de par torcido sin blindaje y operando a 1 Mbps. Esta opción es de menor costo que las opciones de cable coaxial y es para instalaciones de computadoras que no requieren gran capacidad.

La especificación 10BASET define una topología de estrella. Un sistema simple consiste de un número de estaciones conectadas a un punto central llamado repetidor multipuerto. Las estaciones se unen al repetidor multipuerto por medio de un enlace punto a punto.
Ordinariamente; las conexiones consisten de dos pares de par torcido sin blindaje. La velocidad es de 10 Mbps usando codificación Manchester.

Finalmente se agregó la opción de banda ancha a una velocidad de 10 Mbps. Esta provee soporte para más estaciones sobre distancias más grandes a un costo mucho mayor.

La figura 2.22 nos muestra el formato de la trama:

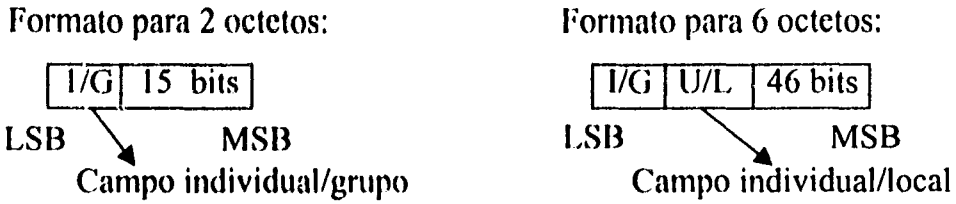


donde:

Preámbulo: campo utilizado para la sincronización de comunicación, sigue un patrón de combinación de bits alternando 1s y 0s (1010....10)

SFD: indica el inicio de la trama y tiene una combinación fija de bits: 10101011

DA: indica la estación a la cual va dirigida la trama pudiendo ser una dirección física única, de grupo o global. Si se eligen 2 o 6 octetos de longitud esta debe ser la misma para todas las estaciones.



SA: indica la estación que origino la trama, el DA y SA tienen la misma longitud

Longitud: longitud del campo de datos

PAD: se utiliza para asegurar que la trama es suficientemente grande para que opere correctamente. Cuando el campo de datos es menor a 46 octetos se usa el campo PAD. Se tiene como máximo una longitud de 1500 octetos entre el campo de datos y el PAD.

FCS: es un CRC (chequeo de redundancia cíclica) de 32 bits aplicable a DA, SA, longitud, datos y PAD.

Figura 2.22 Formato de trama IEEE 802.3 y formatos del campo de dirección

2.8.3 IEEE 802.4 TOKEN BUS

Este estándar especifica tres opciones de capa física. La primera es un sistema de banda ancha, la cuál soporta canales de datos a 1, 5 y 10 Mbps con anchos de banda de 1.5, 6 y 12 MHz respectivamente. El segundo es un esquema conocido como banda portadora o banda ancha de canal simple. Las velocidades de transmisión son de 1, 5 y 10 Mbps. El estándar más reciente es una especificación de fibra óptica. Se especifican tres velocidades de transmisión: 5, 10 y 20 Mbps. Para estar de acuerdo con el estándar para sistemas de fibra óptica, la banda ancha y portadora son especificadas en términos de longitud de onda en vez de frecuencia. Para las tres velocidades, el ancho de banda es de 270 nm y el centro de longitud de onda esta entre 800 y 910 nm. Esta especificación de fibra óptica puede ser usada con cualquier topología que sea lógicamente un bu-

Este estándar se basa en la transmisión de un paquete de datos (token) a través de un a red con topología de bus. Con lo cuál se elimina la gran desventaja que representa una red CSMA/CD, el cuál es provocado por colisiones. Este estándar maneja un algoritmo que opera de la siguiente manera.
Las estaciones conectadas al bus son secuenciadas para formar un anillo lógico. Un paquete de datos especial, el cuál es llamado token es transferido de estación en estación de manera secuencial. Cuando una estación recibe el token de la estación anterior, almacena la dirección de su predecesor y luego transmite cualquier dato que tenga. La estación puede transmitir tantos paquetes de datos como pueda, hasta que el tiempo máximo en que mantiene el token concluya. Es este punto, la estación debe pasar el token a la siguiente estación en el anillo lógico y almacenar sus datos no transmitidos para la siguiente vez que reciba el token.

2.8.4 IEEE 802.5 TOKEN RING

El algoritmo empleado para este estándar requiere que las estaciones se conecten físicamente en un anillo. Cada estación actúa como un relevador, permitiendo el flujo de datos a través del anillo de manera unidireccional. Una trama de datos libre (token) viaja a través del anillo de esta manera cuando todas las estaciones están sin transmitir. Cuando una estación que requiere enviar información reconoce el token libre, cambia un bit en él para marcarlo como un token ocupado, pasando el mismo a través del anillo. La estación transmite entonces el resto de su información, agregándola a los dos campos siguientes del token. Cuando una estación ve que los datos transmitidos van direccionados hacia ella, la estación duplica la información para procesarla, continúa con la transmisión hacia el anillo, y manda una señal de reconocimiento de la recepción del paquete de datos. Cuando una estación toma el token y comienza a transmitir una trama de datos, no existe token en el anillo, así que otras estaciones que desean transmitir deberán esperar.

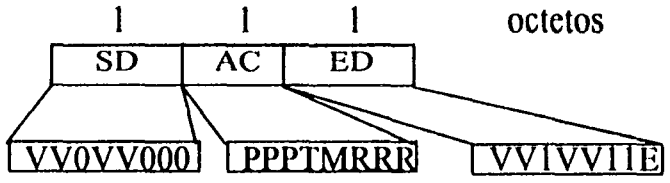
La estación que transmite un bloque de datos tiene por obligación eliminarlo del anillo en cuanto lo recupera, de otro modo el paquete continuaría dando vueltas a través de la red, así mismo puede continuar enviando información hasta concluir. Para asegurarse que solo un token se encuentre viajando a través de la red, la estación transmisora debe remover su información antes de poder transmitir un nuevo bloque de datos.

Existen tres formatos de trama:

a)token (compuesto por tres octetos)
b)trama LLC (de longitud variable)
c)secuencia de aborto (dos octetos)

a) Token

El formato de la trama lo indica la figura 2.23



donde:

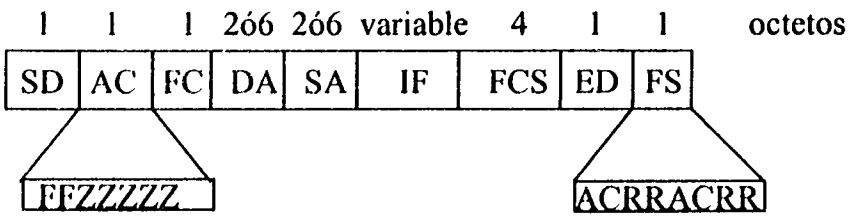
v: violación diferencial Manchester
T: bit de token
R: reservación de prioridad
P: modo de prioridad
M: monitoreo

Figura 2.23 Trama token

SD: delimitador de inicio
AC: control de acceso, los tres primeros bits son de prioridad debido a que cada estación tiene asignada una prioridad para su transmisión (donde 000 es la prioridad mas baja y 111 es la mas alta). Los bits R los puede utilizar la estación que quiera transmitir el siguiente token. El bit de token toma el valor 0 si es un token y 1 si es una trama. Finalmente, el bit de monitoreo se encarga de evitar que una trama circule continuamente por el anillo dándole el valor de 0 la estación que transmite y el valor de 1 la estación de monitoreo.
DE: delimitador de final. El bit E se utiliza cuando la trama tiene un error de chequeo de redundancia

b) trama MAC:

La figura 2.24 muestra el formato de trama MAC



Donde:

F. Define el formato de la trama

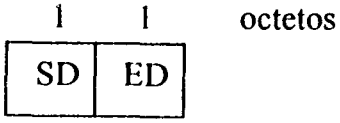
F	F	FORMATO
0	0	MAC (datos del anillo)
0	1	LLS (datos del usuario)
1	X	uso posterior

Z: bit de control
A: dirección conocida
C: trama recibida
R: bit reservado

Figura 2.24 Formato de trama MAC

SD: delimitación de inicio de trama
AC: control de acceso
FC: control de trama (LLC o MAC)
DA: estación destino
SA: estación fuente
IF: información del usuario si es trama LLC, datos del anillo si es MAC
FCS: chequeo de redundancia cíclica
DE: delimitación de fin de trama
FS: estado de trama
C) Trama de aborto

La trama de aborto esta representada en la figura 2.25



donde:

SD: inicio de trama
ED: fin de trama

Figura 2.25 Formato de trama de aborto.

Se utiliza solo cuando ha ocurrido un error que no garantice que la trama enviada sea recibida correctamente por la estación destino.

2.8.5 FDDI

ANSI desarrolló una especificación para redes locales con fibra óptica llamada FDDI. El canal de fibra óptica trabaja a 100 Mbps. Una anillo de fibra óptica puede incluir hasta mil nodos, estos pueden estar separados hasta 2 kms y la circunferencia del anillo puede llegar hasta 200 kms.

FDDI especifica una topología que incluye dos anillos de fibra óptica independientes que proporcionan una velocidad de 100 Mbps cada uno. El concentrador permite conectar estaciones y reconfigurar el sistema, también se encarga de aislar los nodos problemáticos mediante el punto de concentración. FDDI no exige necesariamente que todos los canales sean de fibra óptica. Se puede incluir en el concentrador una interfaz en donde se instalará fibra óptica para una parte de la red, y coaxial o par trenzado para otra parte.

Los conectores de las terminales y del concentrador son diodos láser, que hacen funcionar a la red a una velocidad de 100 MHz.

El estándar FDDI también abarca la capa MAC y la capa física, y soporta el uso del control de enlace lógico IEEE 802.3 (LLC). La figura 2.25 representa la arquitectura del protocolo FDDI, el cuá. nas abajo de' nivel LLC consiste de cuatro partes:

1)MAC: la capa MAC de FDDI es la parte de la capa de enlace de datos que regula el acceso al medio LAN
2) PHY (Physical Layer Medium Independent): esta es la parte del medio independiente de la capa física, la cuál incluye la codificación, decodificación y sincronización de las señales digitales
3)PMD (Physical Medium Dependent): especifica las señales ópticas y la forma de onda del medio dependiente de la capa física.
4)SMT (Station Management): provee el control necesario para manejar las funciones principales en las diferentes capas FDDI como pueden ser: administrar el anillo, localizar fallas, monitorear errores, etc.

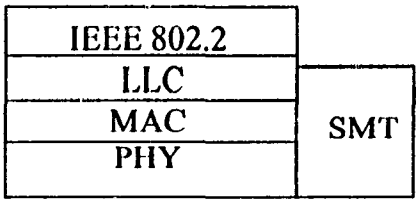


Figura 2.26 Arquitectura del protocolo FDDI

En resumen estas son algunas características con las que cuenta FDDI:

- utiliza fibra óptica
- velocidades de 100 Mbps
- especificación de fiabilidad
- utiliza el código 4B/5B
- reloj distribuido
- rotación del token de duración limitada
- nuevo token después de transmitir

2.8.5.1 FORMATO DE LA TRAMA FDDI

La figura 2.27 representa los formatos de la trama del protocolo FDDI. El estándar define el contenido de este formato en términos de símbolos, correspondiéndole a cada uno de estos 4 bits. Los símbolos se...

usados debido a que la capa física de datos codifica y transmite en paquetes de 4 bits mediante el código 4B5B.

64	8	8	16ó48	16ó48	4500	32	4	1
PREAMBULO	SD	FC	DA	SA	INFORMACION	FCS	DE	FS

a) formato general de trama

PREAMBULO	SD	FC	ED

b) formato del token

Figura 2.27 Formato de trama FDDI

Preámbulo: sincroniza la trama con el reloj de cada estación. El que origina la trama usa un campo de 26 símbolos ociosos (64 bits); las subsecuentes estaciones que la repiten pueden cambiar la longitud del campo de acuerdo con los requerimientos de sincronización. Los símbolos ociosos no son datos. La forma real de un símbolo que no es de datos depende de la codificación de la señal sobre el medio.

SD: delimitador de inicio, indica el inicio de la trama. Es codificado como JK donde J y K son símbolos que indican que nos son datos.

FC: control de trama, tiene el siguiente formato:

C	L	FF	ZZZZ

donde:

C: indica si es una trama sincronía o asíncrona
L: indica el uso de 16 ó 48 bits de direccionamiento
FF: indica si es una trama LLC, MAC de control o reservada. Para una trama de control, los 4 bits que faltan indican el tipo de control de la trama

Figura 2.28 formato del campo de control de la trama FDDI

DA: dirección destino, especifica la estación o estaciones hacia donde va dirigida la trama. Puede ser una sola dirección física, un grupo de estaciones o todas las estaciones. El anillo puede contener una mezcla de longitud de direcciones de 16 y 48 bits.

SA: dirección fuente, especifica la estación que envió la trama.

INFORMACION: contiene unidades de datos LLC o información relacionada con una operación de control.

FCS: trama de chequeo de secuencia, es un chequeo de redundancia cíclica de 32 bits aplicado a los campos FC, DA,SA y a los campos de información.

ED: delimitador de final de trama, contiene uno o dos símbolos que no son de datos, marca el final de la trama excepto para el campo FS. Tiene 8 bits de longitud para el token y 4 para las demás tramas.

FS: estado de trama, contiene detector de error (E), reconocimiento de dirección (A) e indicadores de copia de trama (F), cada indicador es representado por un símbolo, el cuál es R para "off" o "falso" y S para "on" o "verdadero".

2.8.5.2 ESPECIFICACIÓN DEL MEDIO FÍSICO

El estándar FDDI especifica un anillo de fibra óptica con una velocidad de transmisión de 100 Mbps usando el esquema de codificación NRZI-4B/5B. La longitud de onda especificada para la transmisión de información es de 1300 nm.

La especificación indica el uso de fibra óptica multimodo. Aunque en la actualidad las redes que cubren grandes distancias cuentan con fibra óptica monomodo, esa tecnología requiere generalmente el uso de láser como fuente de luz en vez de LEDS, lo cuál es adecuado para los requerimientos de FDDI. Las dimensiones de la fibra son especificadas en términos del diámetro del núcleo de la fibra y del diámetro externo de la capa que cubre el núcleo La combinación especificada en el estándar es 62.5 µm. El estándar menciona como alternativas 50/125, 8[illegible].25, y 100/[illegible] µm.

2.9 FAST ETHERNET

Debido a los recientes avances en la tecnología de computadoras, las aplicaciones de red locales han ido creciendo en velocidad, poder y habilidad para el proceso de información. Sin embargo estas nuevas aplicaciones demandan un mayor consumo de ancho de banda y las tecnologías como ethernet se han quedando rezagadas ante esto.

2.9.1 ESTANDAR 100 BASE T

Para solventar los requerimientos de ancho de banda en redes LAN se han desarrollado estándares como 100BASE-T o Fast Ethernet que es una mejora sobre el estándar del IEEE 802.3 o Ethernet basado sobre CSMA/CD "Carrier Sense Multiple Access, with Collision Detection" protocolo que define como transmitir, recibir y manejar los recursos en una red Ethernet. En adición a esto soporta aplicaciones sensibles al ancho de banda como aplicaciones multimedia, y además al estar basado sobre ethernet permite una suave migración y tener interfaces con las 2 velocidades 10 y 100 Mbps y permite utilizar la infraestructura de par trenzado utilizada en Ethernet. El mecanismo que se utiliza para tener una velocidad de 10 o 100 Mbps se llama autonegociación. Fast ethernet al estar basado en Ethernet inevitablemente es objeto de las mismas fallas como ser de medio compartido lo que significa compartir el ancho de banda entre los usuarios, otra es la distancia que se reduce en una red sin puentes a 210 m. Para cubrir las necesidades de distancia el empleo de LAN switches entre repetidores es necesario.

Hay otras tecnologías desarrolladas como 100anyVGLAN que utiliza un mecanismo denominado demanda de prioridad (estándar 802.12 del IEEE) al no estar basada en una tecnología de común uso por muchas empresas no han tenido el éxito que fast ethernet ha adquirido.

2.9.2 CARACTERÍSTICAS FÍSICAS

Fast ethernet cumple con el estándar EIA/TIA 568, soporta el uso de cable UTP categoría 3 o superior y fibra óptica. La codificación que emplea es 8B/6T.

Fast ethernet esta basado en una topología de estrella, y solo soporta dos repetidores lógicos. Cumple con el uso de SNMP para administración. Existen 2 tipos de repetidores Clase I y Clase II.

2.9.3 TIPOS DE REPETIDORES

2.9.3.1 REPETIDOR CLASE I

Este tipo de repetidor puede tener grandes retrazos de tiempo y funciona transformando las señales de la linea analógicas de un puerto de entrada a formato digital, y volviéndolas a transformar en analógicas cuando se envian a otros puertos. Esto hace posible repetir señales entre segmentos que utilizan diferentes técnicas de transmisión, tales como segmentos 100BaseTX/FX y segmentos 100Base-T4 permitiendo a estos mezclarse dentro de un hub repetidor. El proceso de transformación en un repetidor de Clase I utiliza un numero de tiempos de bit, de manera que un solo repetidor de Clase I puede ser usado en una colision cuando cables de máxima longitud sean usados.

2.9.3.2 REPETIDOR CLASE II

Este esta sujeto a retrasos de tiempo mas pequeños y repite inmediatamente las señales de entrada hacia otros puertos sin necesidad de un proceso de transformación . Para conseguir los retrasos de tiempo pequeños los repetidores solo se conectan a los segmentos con mismas técnicas de transmisión tales como 100Base-TX y 100Base-FX, un máximo de dos repetidores se pueden usar dentro de una colision cuando se usan cables de máxima longitud.

Fast ethernet tiene la capacidad de full duplex con el cual dobla el ancho de banda de un enlace entre una tarjeta de red y un switch o entre un par de switches (de 100 Mbps a 200 Mbps), deshabilita la detección de colisiones, así los dispositivos pueden transmitir y recibir concurrentemente a su completa velocidad. En el modo 100BASE-T4 no se soporta el modo full duplex.

El estándar 100BASE-T esta comprimido en 5 especificaciones: Control de Acceso al Medio (MAC), Interface Independiente del Medio

(MII) y tres capas físicas (100BASE-TX, 100BASE-T4 y 100BASE-FX). El siguiente diagrama muestra los componentes y sus relaciones.

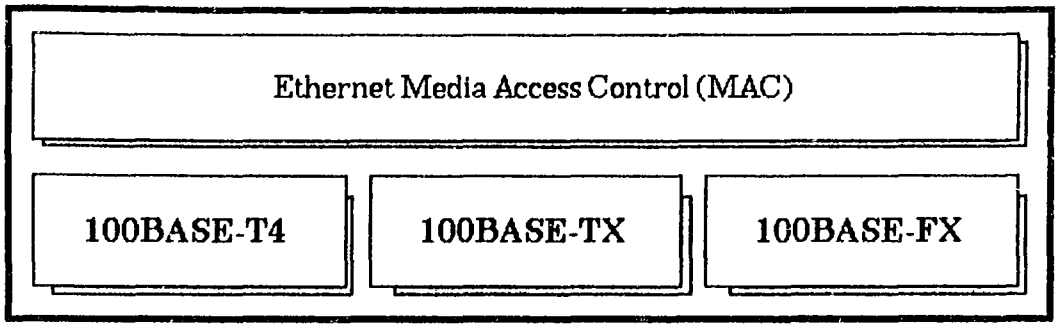


Figura 2.29 Componentes de fastEthernet

2.9.4 CONTROL DE ACCESO AL MEDIO (MAC)

La capa MAC esta basada en el protocolo CSMA/CD como en ethernet, la única diferencia es que corre 10 veces más rápido, fast ethernet retiene las características del ethernet.

2.9.4.1 INTERFACE INDEPENDIENTE DEL MEDIO (MII)

El MII es una nueva especificación que define una interface estándar entre la capa MAC y cualquiera de las 3 interfaces de capa física (100BASE-TX, 100BASE-T4 y 100BASE-FX). Es capaz de soportar velocidades de 10 o 100 Mbps. El MII es una parte electrónica opcional que proporciona un modo de unir las funciones de control de acceso al medio de ethernet en el dispositivo de red con el dispositivo de capa física que envia señales al medio de red . Puede ser implementado en el dispositivo de red internamente o externamente. El MII tiene un conector de 40 pines y puede tener una longitud máxima de 0.5 m.

2.9.4.2 CAPA FÍSICA 100BASE-TX

Esta capa define la especificación para 100BASE-T Ethernet sobre dos pares de cable UTP categoría 5 o STP tipo 1, un par para transmitir y uno para recibir con conector RJ-45 igual que en Ethernet. Permite segmentos de hasta 100 m de longitud. La interface dependiente del medio MDI (médium dependient interface) es un conector RJ-45.

2.9.4.3CAPA FÍSICA 100BASE-T4

Esta capa define la especificación para 100BASE-T Ethernet sobre cuatro pares de UTP categorías 3, 4 o 5. Con este método de señalización, tres pares son usados para transmitir y recibir y el cuarto para escuchar colisiones. Permite hasta 100 m de longitud, 90 metros desde el equipo hasta la roseta y 10 m para acomodar los cables en el closet. El la siguiente figura se muestra un esquema de las señales de los cuatro pares. La interface dependiente del medio MDI (médium dependient interface) es un conector RJ-45.

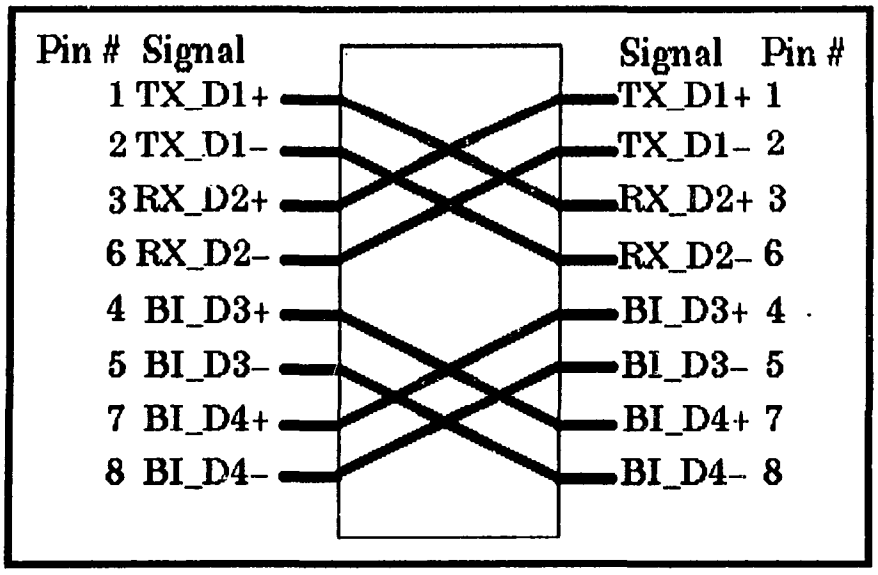


Figura 2.30 conector RJ-45

2.9.4.4 CAPA FÍSICA 100BASE-FX

Esta capa define la especificación para 100BASE-T Ethernet sobre dos hilos de fibra óptica multimodo de 62.5/125 micrones. Uno para transmitir y el otro para recibir, los conectores (MDI's) pueden ser ST, SC o MIC para FDDI. La longitud de onda es de 1350 nm, permite segmentos de 412 m , es posible tener distancias mas grandes pero esta es la máxima para garantizar el "round trip timing"

2.9.5 REGLAS DE CONEXION PARA FAST ETHERNET

Estas difieren un poco a las definidas en ethernet. En la siguiente figura se muestra las diferentes distancia soportadas por Fast Ethernet.

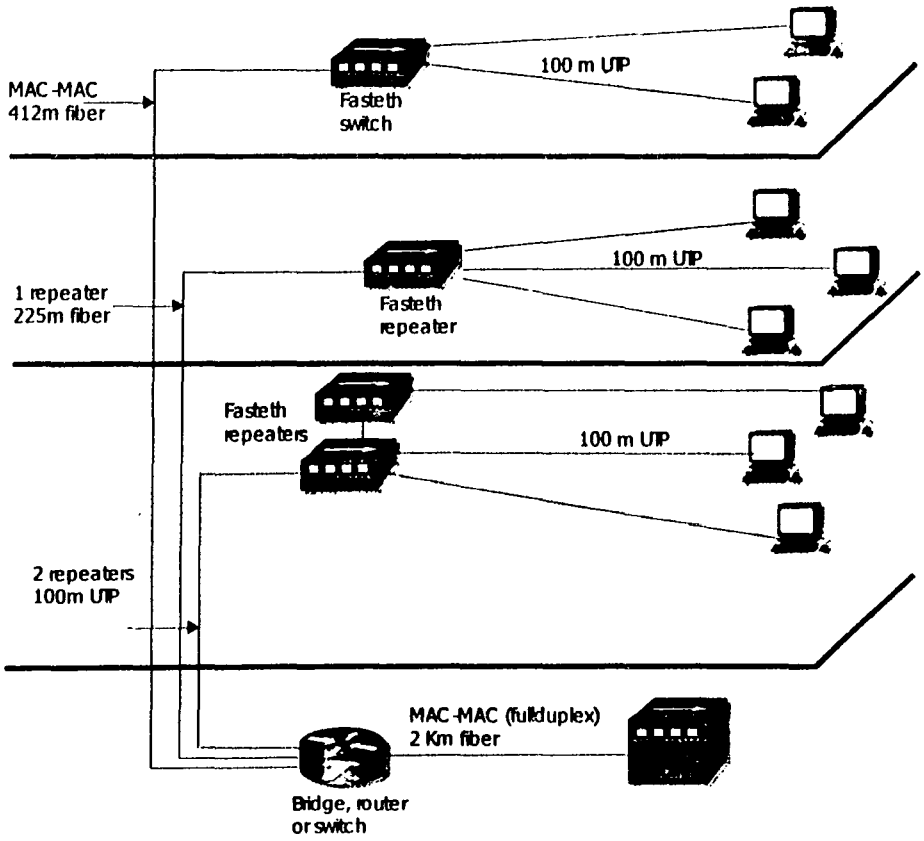


Figura 2.31 reglas de configuración de FasEthernet

- Máxima longitud 100m (328ft) sobre cable CAT 5
- 412 m (1352ft) de fibra conectando de un switch a otro, usando half duplex.
- Un alcance total de 325 m (1066ft) es permitodo en topologías de un solo repetidor, por ejemplo 225 m(738ft) de un enlace de fibra de un repetidor hacia un router o un switch mas 100 m (328ft) de un enlace con UTP de un repetidor hacia una estacion de trabajo.

2.10 GIGABIT ETHERNET

El funcionamiento de gigabit ethernet es el mismo al de 100-Mbps Ethernet. Gigabit Ethernet retiene el protocolo CSMA/CD (Carrier Sense Multiple Access/ Collision Detect) y el formato de trama de sus predecesores 10 y 100 Mbps. Asi es compatible con ethernet y fast ethernet y permite una suave migración. Asi la demanda de gigabit ethernet por empresas con backbone a 100 Mbps se ha ido incrementando.

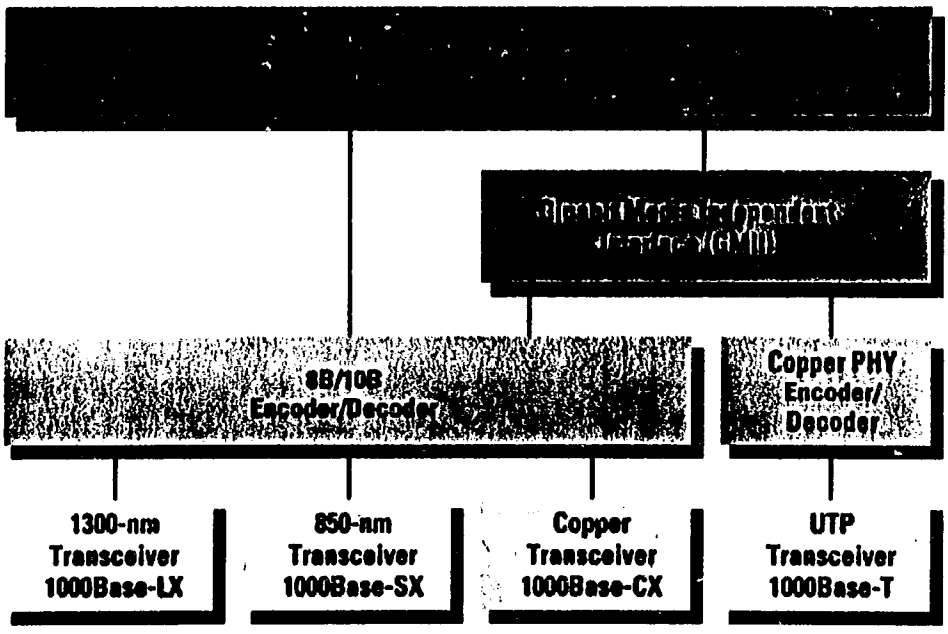


Figura 2.32 arquitectura de gigabit ethernet

El control de Acceso al Medio MAC es una versión mejorada de el algoritmo MAC 802.3 .Una interface gigabit de medio independiente (GMII) es definida para todos los medios excepto cable UTP. GMII define interfaces de datos sincronas de transmisión y recepción independientes de 8 bits paralelo. Esta implementada como una interface "chip-to-chip" que permite a diferentes vendedores mezclar los componentes MAC y la subcapa física (PHY) de diferentes manufacturas.

Dos esquemas de codificación estan definidos en la capa fisica. Un esquema 8B/10B es usado para fibra optica y medios de cobre blindados, y modulacion por amplitud de pulsos (PAM)-5 es usada para UTP.

2.10.1 CAPA DE ACCESO AL MEDIO

Las especificaciones de el formato de trama que CSMA/CD y del protocolo MAC es igual al empleado por las versiones del IEEE 802.3 para 10 y 100 Mbps. Para la operación de un hub Ethernet, en la cual solo una estación puede transmitir a la vez (half-duplex), el esquema basico CSMA/CD tiene dos mejoras:

- Extensión de portadora (Carrier extension):en esta son puestos al final de la trama MAC una serie de symbolos especiales, asi el bloque resultante es al menos de 4096 bits en duración, siendo el minimo de 512 bit como en 10 y 100 Mbps. Esta extension hace que la longitud trama mas grande transmitida sea el tiempo de propagación a 1 Gbps.
- Frame bursting: esta caracteristica permite multiples tramas cortas ser transmitidas consecuentemente indefinidamente sin abandonar el control por CSMA/CD entre tramas. Frame bursting evita el overhead de la extension de portadora cuando una estacion tiene un numero pequeño de tramas listas a enviar.

Con un LAN switch (en modo de operación full-duplex), el cual provee un medio dedicado en vez de permitir el acceso compartido al medio, la extension de portadora y el frame bursting no son necesitados. Son innecesarios por que la transmision y recepcion de datos en una estacion puede ocurrir simultameamente sin interferencia y sin contensiones para el medio compartido. Todos los productos gigabit en el mercado usan una tecnica de switching y de ahí no tienen que implementar las tecnicas anteriores.

Con el empleo de switches, se utiliza el modo de operación full-duplex y el protocolo CSMA/CD no es necesitado. La especificacion gigabit se extiende sobre las pausas en el protocolo que esta definido para 100 Mbps Ethernet permitendo control de flujo asimetrico. Usando el protocolo de autonegociación, un dispositivo puede indicar que si su otro extremi le esta mandando tramas pausadas no le va a responder.

2.10.2CAPA FISICA

La especificación para IEEE 802.3 incluye las siguientes altenativas mostradas en la siguiente figura.

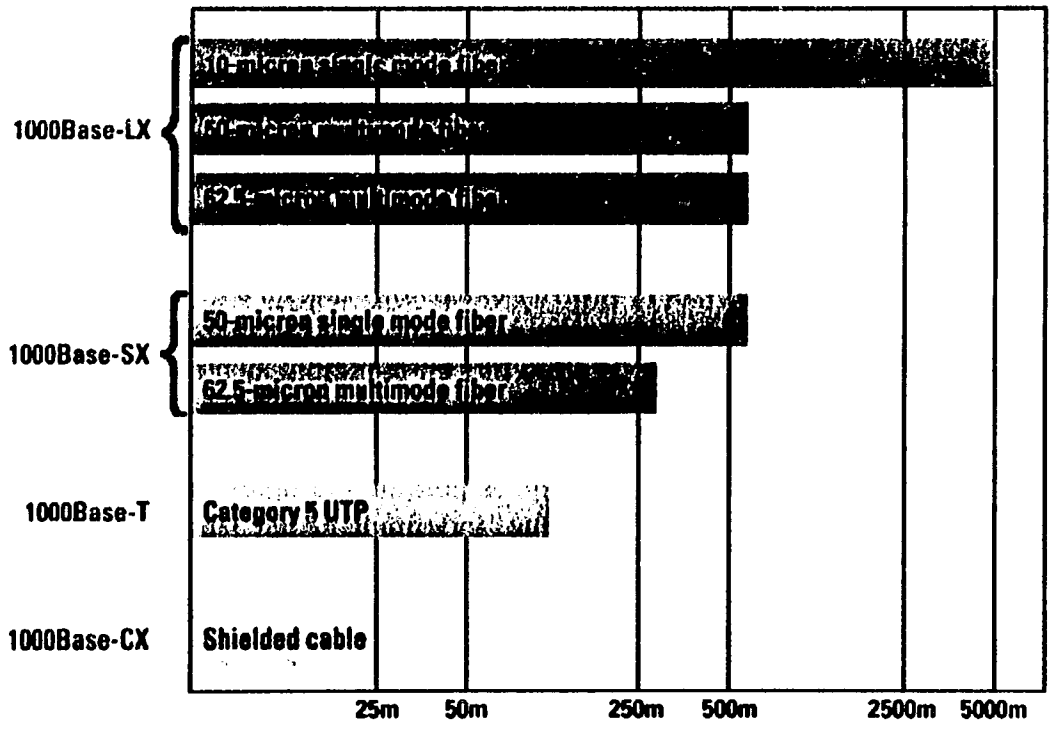


Figura 2.33 especificación para IEEE 802.3

- 1000Base-LX:esta opcion de longitud de onda larga soporta enlaces duplex de hasta 550 m utilizando fibra optica multimodo de 62.5 o 50 μm y hasta 5 Km utilizando fibra monomodo de 10 μm. Las longitudes de onda estan en el rango de 1270 a 1355 nm.

- 1000Base-SX: esta opcion de longitud de onda corta soporta enlaces duplex hasta 275 m utilizando fibra optica multimodo de 62.5 µm o hasta 550 m utilizando 50 µm. Las longitudes de onda estan en el rango de 770 a 860 nm.

- 1000Base-CX:esta opción soporta enlaces a 1Gbps entre dispositivos localizados dentro de un mismo cuarto o bastidor de equipo usando jumpers de cobre (cables STP especiales pueden llegar hasta 25 m). Cada enlace es compuesto de un cable STP en cada dirección.

- 1000Base-T:esta opcion hace el uso de cuatro pares de UTP categoria 5 para soportar dispositivos separados hasta 100 metros.

2.10.3TECNICAS DE CODIFICACION DIGITAL USADAS EN GIGABIT ETHERNET

El esquema de codificacion es usado para todas las opciones excepto la del UTP que es 8B/10B. Este esquema tambien es usado en canales de fibra. Con 8B/10B, cada 8 bits de datos son convertidos dentro de 10 bits para transmision. El esquema 8B/10B fue desarrollado y patentado por IBM para usarlo en su sistema de interconexión ESCON de 20 megabaud.

Los desarrolladores de este codigo listan las siguientes ventajas:

- puede ser implementado con simples y confiables transceivers de bajo costo.
- Esta bien balanceado,con una minima desviacion de la ocurrencia de un numero igual a 1 y 0 bits a traves de cualquier secuencia.
- Provee buena densidad de transicion para recobrar el reloj facilmente.
- Provee capacidad de deteccion de errores.

El codigo 8B/10B es un ejemplo de un codigo general mBnB, en el cual m es la fuente binaria de bits que es mapeada dentro de n bits binarios para transmision. La redundancia es construida dentro del codigo para proveer las caracteristicas deseadas de transmision haciando n > m. La figura 4 illustra la operación de este codigo. El codigo actual 8B/10B combina otros dos codigos 5B/6B y 3B/4B. El uso de estos dos codigos es simplemente un artificio que simplifica la definicion de el mapeo y la implementacion, el mapeo pudo haber sido definido directamente en

8B/10B. En cualquier caso, un mapeo es definido al mapear en un block cada uno de los 8 bits de la fuente posibles dentro de un block de codigo de 10 bits. Este complemento tiene el efecto de eliminar la disparidad o al menos moverlo en la direccion opuesta del flujo de la disparidad.

El mecamismo de codificación tambien incluye una entrada de control de linea, K, la cual indica si de la linea A a la H son bits de control o de datos. En el primer caso un bloque especial de 10 bit sin datos es generado. Un total de 12 de estos bloques sin datos estan definidos como validos en el estandar. Estos bloques son usados para sincronización y otros propositos de control.

Para 1000Base-T, el esquema de codificacion usado es el PAM-5, sobre cuatro pares de UTP. Asi cada enlace provee una velocidad de 250 Mbps. PAM-5 provee una utilizacion mejor del ancho de banda utilizando señalizacion binaria dentro de 5 niveles diferentes de señal. Cada elemento de señal puede representar 2 bits de informacion (usando cuatro niveles de señalizacion).En adicion un quinto nivel de señal es usado para el FEC (fordward error correction).

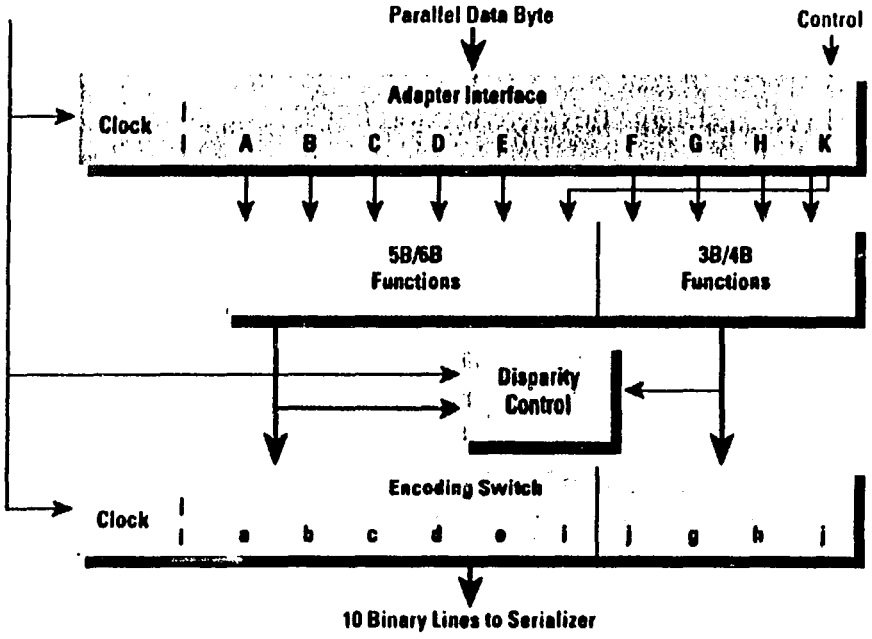


Figura 2.34

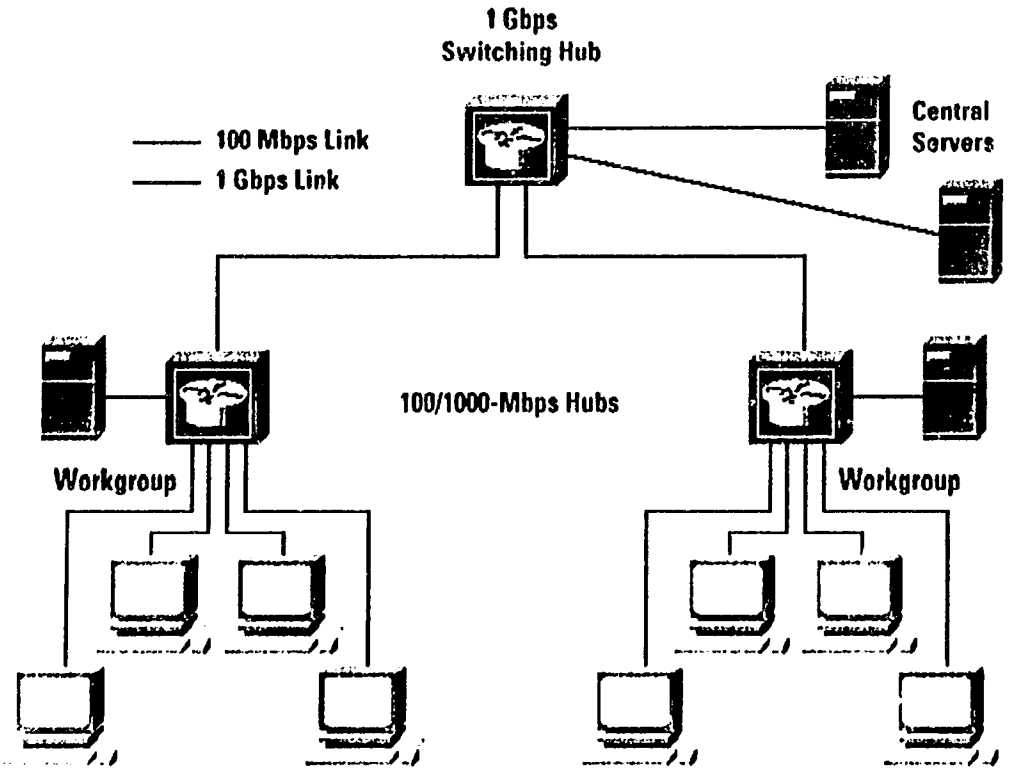


Figura 2.35 conexión tipica de una red con gigabit ethernet:

Tambien se ha desarrollado 10 Gigabit ethernet con el estandar P802.3ae, pero este tema no es cubierto en este trabajo

2.11 INTERFACES USADAS EN REDES LAN

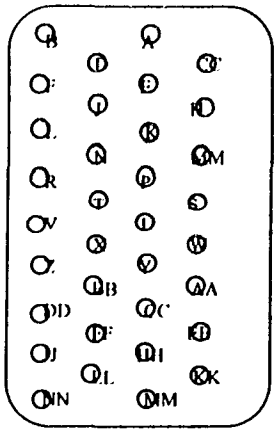
Las interfaces del nivel físico se utilizan para conectar dispositivos de usuario al circuito de comunicaciones. Para llevar a cabo esta función, en la mayoría de las especificaciones se describen tres atributos de la interfaz:

- eléctricos
- mecánicos
- procedimentales

Los atributos eléctricos son los que determinan los niveles de tensión o corriente y la temporización de los cambios eléctricos que representan los unos y ceros. Muchos de los protocolos del nivel físico clasifican estas funciones en cuatro grupos: control, sincronismo, datos y masa. Los atributos mecánicos describen los conectores y los hilos de la interfaz. Por lo general, todas las líneas de datos, de señalización y de control están incluidas en un mismo cable, y se conectan a enchufes terminadores situados en ambos extremos del cable. Por último, los atributos procedimentales describen lo que deben hacer los conectores, y la secuencia de eventos necesaria para llevar a cabo la transferencia efectiva de datos a través de la interface.

2.11.1 INTERFAZ V.35

Transmisión de datos a 48 kilobits por segundo utilizando circuitos de la banda de grupo entre 60 y 180 Khz



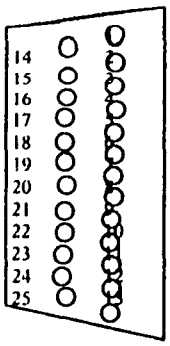
Asignación de pines mas usados:

A: tierra de protección
AA: reloj de transmisión
B: tierra de señal
C: permiso para transmitir
D: liberación de terminal
E: equipo de datos preparado
F: detección de señal de línea recibida
P: datos transmitidos
R: datos recibidos
S: datos transmitidos
T. datos recibidos
U: reloj de terminal
V: reloj de recepción
W: reloj de terminal
X: reloj de recepción
Y: reloj de transmisión

Figura 2.36 Conector M34. Norma V.35

2.11.2 INTERFAZ RS232-V.24

V.24 es otra interfaz estándar que se utiliza en muchas partes del mundo. Muchos de los productos que se pueden encontrar en oficinas están descritos como compatibles con la norma v.24. Esta norma incluye las definiciones de las líneas que unen los ETD y los ETCD.



Asignación de pines:

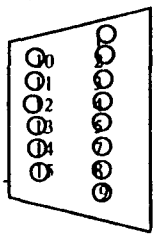
1: tierra de protección
2: datos transmitidos
3: datos recibidos
4: solicitud de transmisión
5: permiso para transmitir
6 equipo de datos preparado
7: tierra de señal
8: detección de portadora
9, 10 y11: reservado
12: detección de portadora secundaria
13: permiso para transmitir secundario
14: datos secundarios transmitidos
15: reloj de transmisión
16: datos recibidos secundarios
17: reloj de recepción
18: no asignado
19: solicitud de transmisión secundaria
20: terminal de datos preparado

21: detector de calidad de señal
22: timbre indicador
23: selector de velocidad de datos
24: reloj de transmisión
25: no asignado

Figura 2.37 Conector DB25. Norma V.24

2.11.3 INTERFAZ X.21

X.21 es otra interfaz estándar que tiene una atención considerable. Este estándar fue publicado por primera vez en 1972, y tuvo mejoras en 1976, 1980 y 1984. Emplea un conector de 15 pines. X.21 y otros estándares están diseñados en torno al concepto de estados, y su funcionamiento se explica mediante diagramas de estados.



Asignación de pines:

1: tierra común
9: tierra de protección
10: permiso para transmitir
11: nivel de recepción de datos
12: recepción de datos
13: transmisión de datos
15: terminal de datos preparada

Figura 2.38 Conector DB15 norma X.21

CAPITULO 3 ARQUITECTURAS DE RED

3.1 ARQUITECTURA XNS

3.1.1 INTRODUCCIÓN:

XNS fue desarrollado a finales de los años 70's por Xerox Corporation junto con Ethernet. A medida que las redes Ethernet crecían a finales de los años 70's surgío la necesidad de interconectarlas por lo que a principios del año de 1980 se culminó el sistema operativo de red de Xerox.

La arquitectura XNS contiene 2 puntos básicos: las capas inferiores tienen tecnología Ethernet y multiples redes Ethernet pueden existir. Estas redes están conectadas por varios canales de comunicación, tales como líneas dedicadas o telefónicas y la inteligencia para comunicarse entre ellas depende y reside en un ruteador. La unidad de información que se transfiere se conoce como paquete internet el cual debe contener una dirección para asegurar la entrega del paquete al destinatario (host). El paquete se entrega en un datagrama por lo que es necesario un protocolo de transporte.

La arquitectura XNS define 5 capas (de la 0 a la 4) y está dentro del modelo OSI como se muestra en la figura 3.1.

3.1.2 DIRECCIONAMIENTO DE DATAGRAMAS Y RUTEO EN XNS

El paquete (o datagrama) XNS debe ser entregado a el correcto destinatario para asegurar una comunicación eficiente. Si el destinatario y la fuente están en diferentes redes se requiere de información adicional.

El paquete internet incluye 3 capas de dirección:

1. Dirección de host de 48 bits que identifican a cualquier sistema que está conectado a la red y está dirección es de hardware grabada en una ROM.
2. Dirección de red que identifica a una red (por ejemplo una LAN) y es de 32 bits de longitud y está sirve para rutear el paquete.
3. Dirección de socket que específica un proceso en el host que puede envíar y recibir paquetes. De 65536 posibles números de sockets los primeros 3000 están reservados.

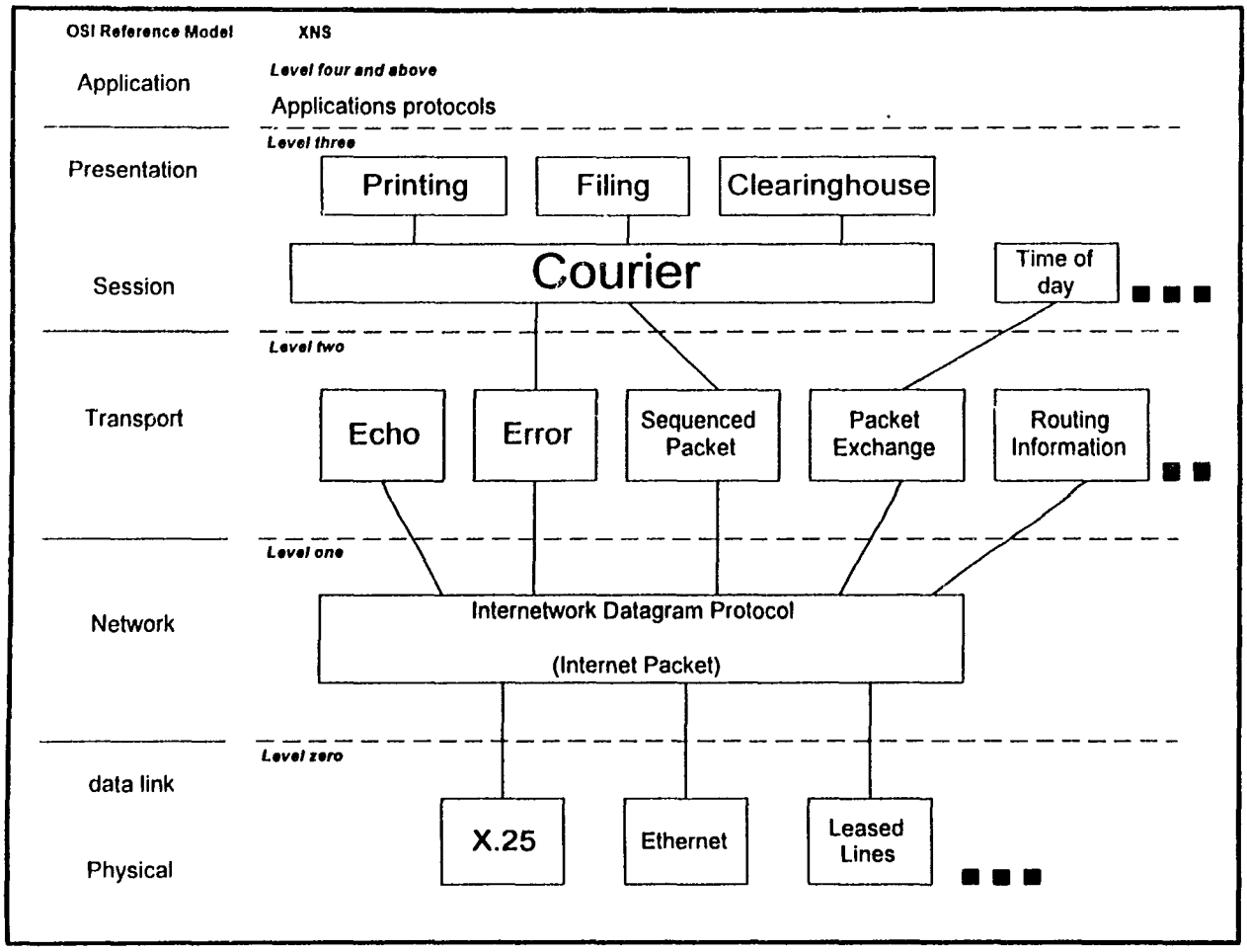


Figura 3.1 Protocolos de la arquitectura de XNS

3.1.3 XNS NIVEL 0 PROTOCOLOS DEL MEDIO DE TRANSMISIÓN

Está capa provee el transporte de los paquetes a nivel físico y corresponde a las capas 1 y 2 del modelo OSI y también incluye tecnologías tales como Ethernet, X.25, etc., y las interfaces típicas son RC 232-C, RS-449 y X.21 . Los distintos medios de transmisión pueden ser cable coaxial, fibra o UTP. El formato de trama a nivel de capa 2 puede diferir en longitud del paquete internet por lo que podemos fragmentar y encapsular el paquete

dentro de una trama. Ethernet es el más obvio de escoger para una LAN XNS.

La encapsulación de un paquete dentro de una trama Ethernet se muestra en la figura 3.2.

3.1.4 XNS NIVEL 1 PROTOCOLOS DE TRANSPORTE-INTERNET

Solo un protocolo es definido por XNS para el nivel 1, el Internet Protocol Datagram (IDP). La función de este es direccionar, rutear y entregar paquetes internet. La entrega del datagrama no esta garantizada.

El formato de un paquete internet se muestra en la figura 3.3 y sus campos se describen a continuación:

- checksum : (2 octetos) es el verificador del paquete internet aunque algunos vendedores lo suprimen con FFFFH para hacer la verificación con CRC.
- Longitud : (2 octetos) es la longitud del paquete. Está longitud es normalmente de 576 bytes , 30 de encabezado, 12 de encabezado SPP (Sequenced Packet Protocol) y 512 bytes de datos de usuario más 12 octetos de protocolo de nivel 3. Puede haber un bit de relleno para completar a 16.
- Control de Transporte: (1 octeto) es usado por los ruteadores y es inicializado a cero por el proceso fuente. Los ruteadores modifican este campo y rehacen el checksum. Los bits 4-7 corresponden al conteo de saltos que tiene un máximo de 16.
- Tipo de paquete: (1 octeto) identifican el formato del campo de datos similar al ethertype.
- Dirección destino y dirección fuente: (12 octetos cada una) definen la dirección internet y especifican la red (4 octetos), host (6 octetos) y socket (2 octetos). Los números de socket también pueden ser asignados y 2 son reservados: cero (desconocido) y todos unos.
- Datos: (0 – 546 octetos) información de capas superiores.
- Byte de relleno (garbage)(opcional 1 byte) completa a 16 bits los datos.

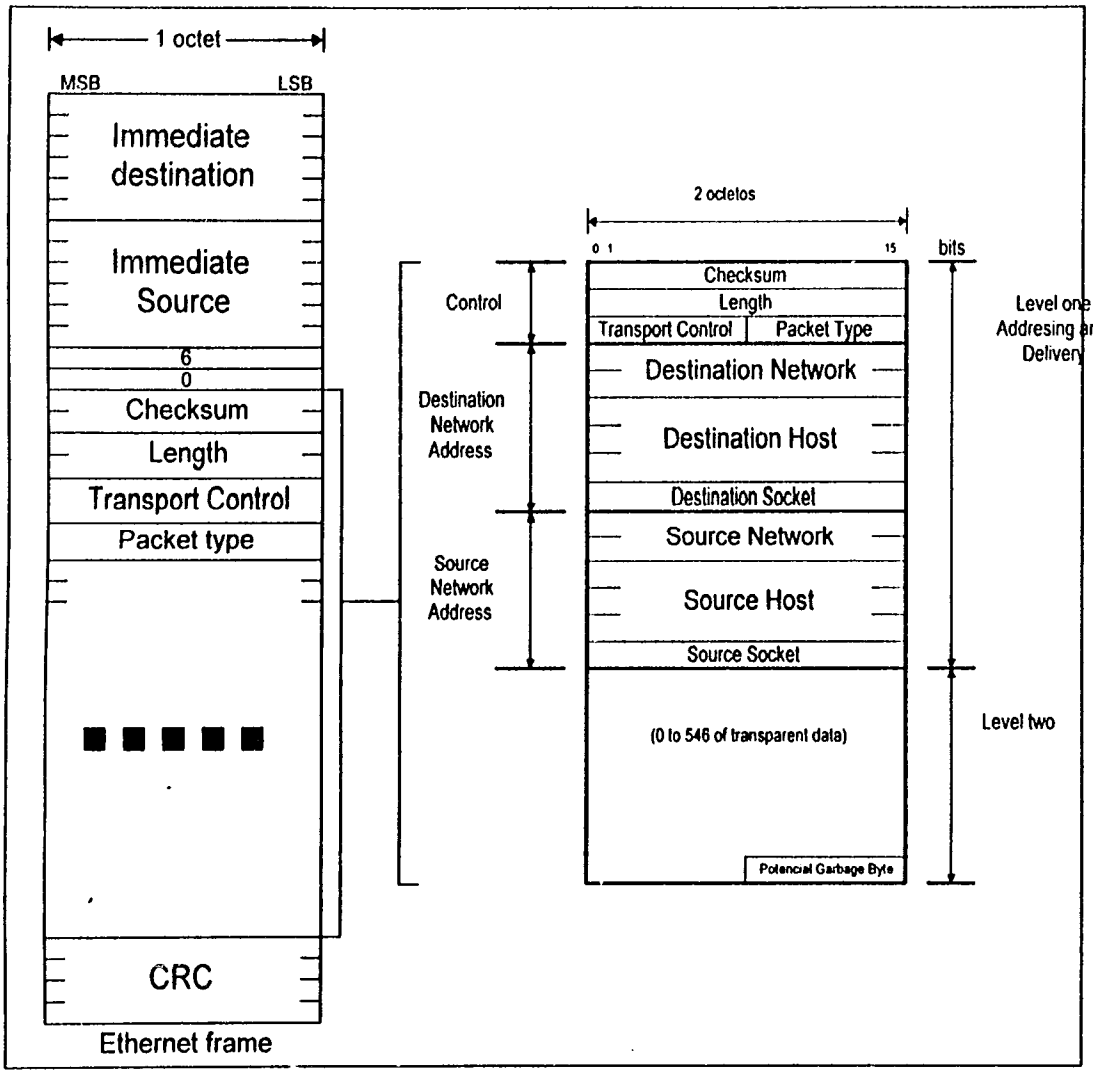


Figura 3.2: El paquete Internet dentro de una trama Ethernet

3.1.5 XNS NIVEL 2. PROTOCOLOS DE TRANSPORTE: INTERPROCESOS

Este nivel se compone de 5 protocolos y son implementados a nivel de interproceso.

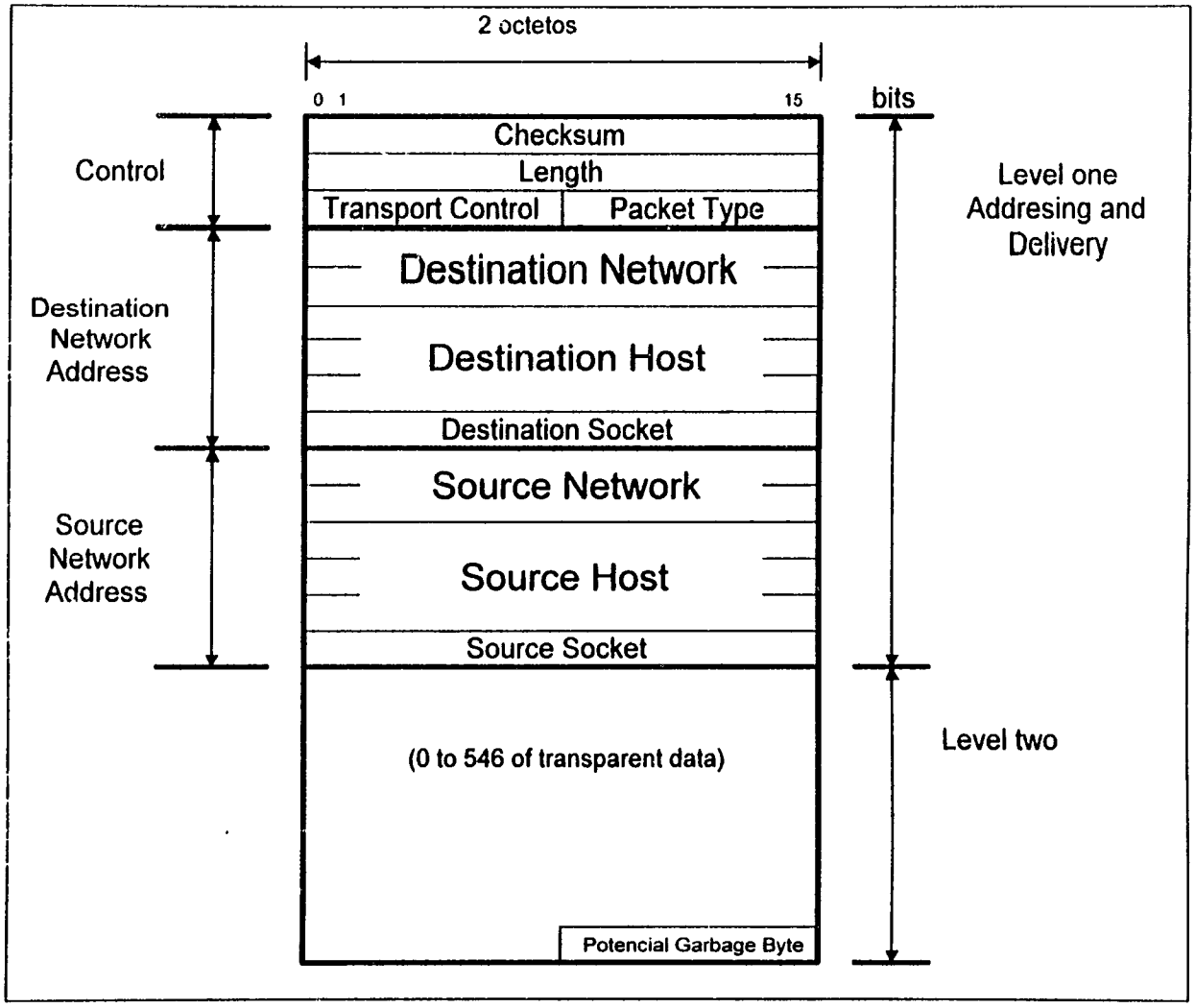


Figura 3.3 : Paquete Internet de XNS

3.1.5.1 RIP (ROUTING INFORMATION PROTOCOL)

Cada ruteador contiene una tabla que establece la ruta correcta para cada paquete internet. Esta tabla es mantenida con información transmitida o recibida por otros ruteadores para actualizar la topología.

El paquete RIP es especificado por el campo de tipo de paquete del encabezado IDP. El primer campo es de dos octetos e indica la operación si es una petición o una respuesta. La porción del contenido del paquete de RIP contiene uno o más "tuples" (de 6 octetos cada uno). Cada "tuple" consiste un número de objeto de red de 32 bits, y un retardo de 16 bits medido como saltos. El número de saltos permitidos es de 16.

Los paquetes de respuesta indican el número de saltos para llegar a su destino. El retardo de un ruteador directamente conectado es de 0 saltos.

3.1.5.2 ERROR PROTOCOL

El protocolo de error es usado para diagnósticos y es enviado desde el ruteador mediante un socket de error hacia el socket fuente que causa el error. El número de error (2 bytes) indica el tipo de error.

ERROR NUMBER (octal)	Description
0	error sin especificar es detectado en el destino
1	el checksum es incorrecto, o el paquete tiene alguna inconsistencia detectada en el destino.

Ciertos tipos de errores son elaborados dentro del campo de parámetros de errores. El paquete de error contiene una copia de la primer porción del paquete erróneo.

3.1.5.3 ECHO PROTOCOL

Este es un protocolo simple usado para verificar, la existencia de un camino de transmisión hacia un host designado. Dos operaciones son definidas. Petición de echo y repetición del echo. La porción de datos del paquete del protocolo de echo debera contener los datos del paquete que llega.

3.1.5.4 SEQUENCED PACKET PROTOCOL (SPP)

Este es el protocolo de transporte de los niveles 1 y 2 y provee transmisión confiable de los datos de procesos de capas superiores. Todas las transmisiones incluyen envío y recepción de números de secuencia para reensamblar el mensaje, control de flujo y control de errores. Ver figura 3.4

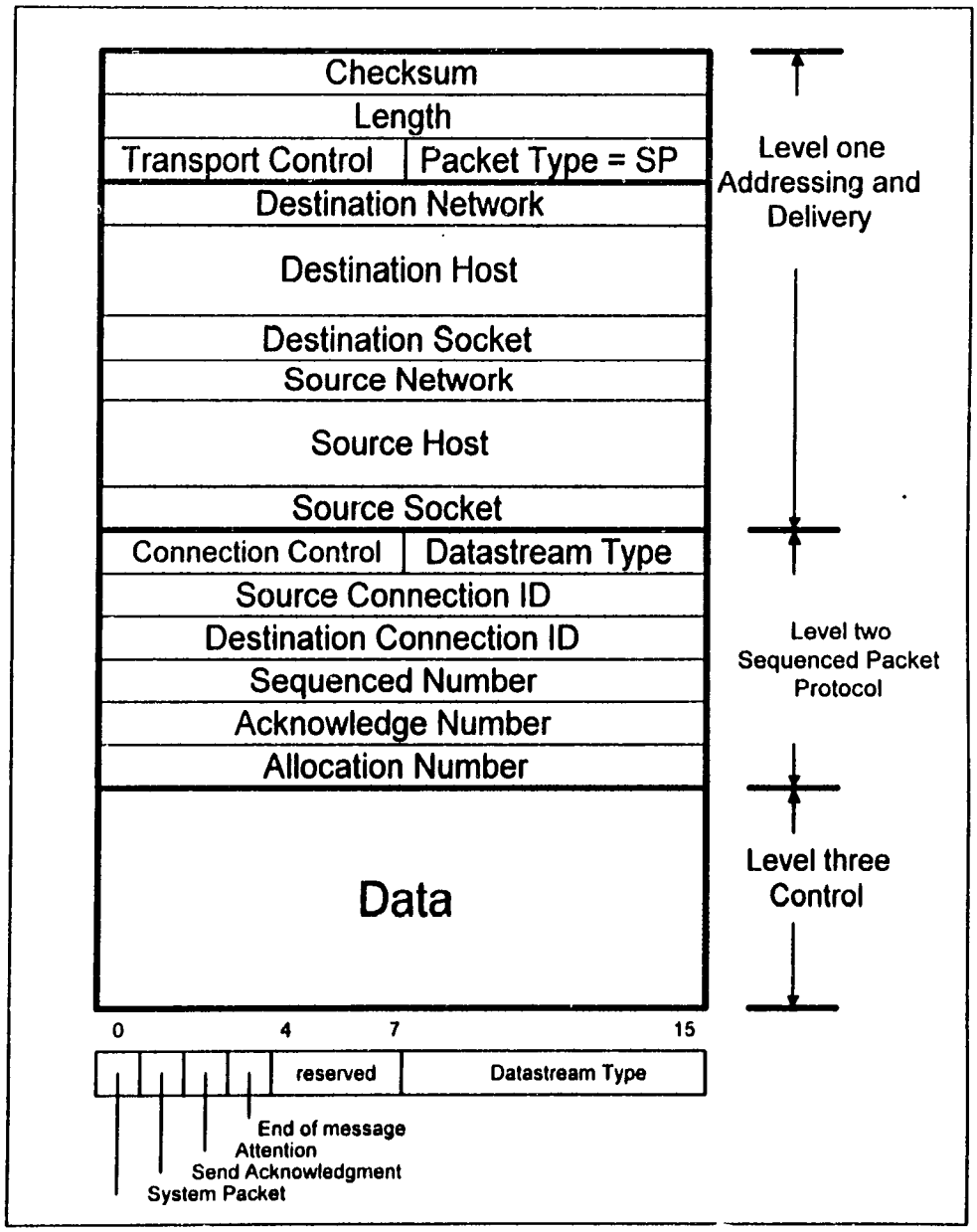


Figura 3.4 : Paquete del SPP de XNS

La base de la comunicación entre procesos es por una conexión abierta entre dos sockets. Los paquetes son intercambiados entre dos sockets.

El encabezado SPP es de 12 octetos y se transmite después del encabezado IDP. Arriba de 534 octetos de datos pueden completar el datagrama.

3.1.5.5 PACKET EXCHANGE PROTOCOL (PEP)

Este protocolo es usado para transmitir paquetes con gran confiabilidad que otros paquetes independientes pero sin el gran encabezado asociado con SPP. Este protocolo es similar a
UDP (de DoD). PEP opera usando un paquete simple usando cualquier socket y dirección fuente y destino.

Dos campos están incluidos en el encabezado PEP. El campo ID es de 32 bits e identifica la transacción (un par de paquetes) entre el transmisor y receptor. El campo de tipo cliente define el protocolo cliente de capas superiores.

3.1.6 XNS NIVEL 3 Y 4

El nivel 3 de XNS contiene los protocolos de control y equivale a la capa de sesión y presentación del modelo OSI y en nivel 4 contiene la capa de aplicación. El protocolo XNS Courier se utiliza mucho en sistemas operativos de LAN tales como Vines.

3.1.6.1 XNS COURIER PROTOCOL

El protocolo Courier define un mecanismo para transmisión entre varias entidades. Aquí se asumen 2 tipos de elementos existentes en una red. El elemento activo de sistema que hace llamadas con los argumentos necesarios para realizar una acción. El otro elemento llamado elemento pasivo de sistema es un proveedor de servicios de peticiones. El programa remoto responde con un resultado de retorno o un estado de error en el evento que se peticionó si la función no fue completada. El elemento activo de sistema (o cliente) y el EPS (o programa remoto) no deben estar situados

en la misma red física. Como resultado el protocolo Courier depende de los niveles 1 y 2 para facilitar la conexión del cliente con el programa remoto.

3.1.6.2 PROTOCOLO CLEARINGHOUSE

Para que el protocolo Courier pueda hacer llamadas remotas un mecanismo debe ser establecido para encontrar el sitio de el host remoto que contiene la información deseada. El protocolo Clearinghouse posee el servicio de directorio. Clearinghouse es una base de datos de objetos, los objetos tienen varias propiedades, el nombre de los objetos tiene una jerarquía de tres niveles: nombre, dominio y organización. La base de datos también puede ser distribuida a través de varios sitios.

Una petición Clearinghouse poe ejemplo puede ser un usuario que necesita encontrar un recurso en partícular como una impresora y hacer una petición para una dirección Clearinghouse. El Courier y el protocolo internet son usados y como resultado se envía un broadcast Ethernet. El servidor Clearinghouse específica donde encuentre el usuario la impresora en cuestión. Este protocolo es similar a SAP en Novell Netware.

3.2 NOVELL NETWARE

El sistema operativo de red Netware fue desarrollado e introducido en el mercado por Novell Inc., a principios de los 80's. Muchos de los elementos que componen a este, fueron derivados de XNS (Xerox Network System).

El sistema operativo de Netware esta basado en una arquitectura cliente/servidor, donde los clientes piden ciertos servicios desde servidores tales como acceso a archivos y acceso a impresoras. Dentro del ambiente de sistema operativo de red, el sistema operativo Netware especifica las 5 capas superiores del modelo OSI. Esto provee compartición de archivos e impresoras y soporte para varias aplicaciones tales como correo electrónico y bases de acceso. los protocolos que permiten el acceso a los usuarios a los servidores de archivos se conocen como NetWare Core Protocol (NCP) y el programa shell de la estación de trabajo.

La figura 3.5 ilustra los protocolos que utiliza Netware y su relación con el modelo OSI.

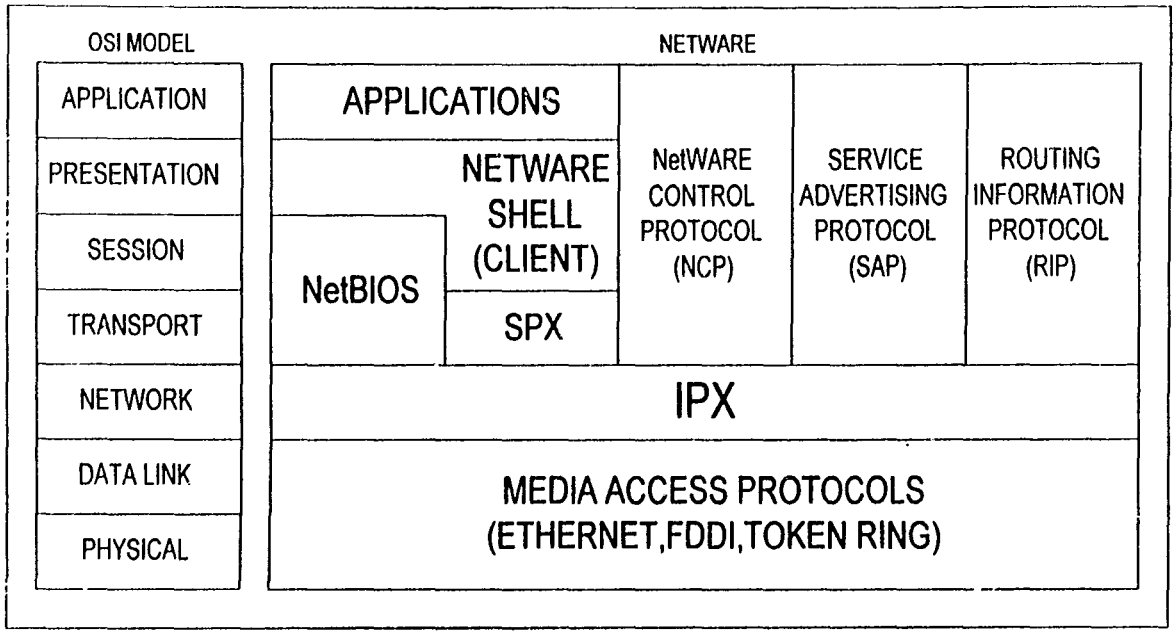


Figura 3.5 :Protocolos de la arquitectura Novell

Las dos primeras capas del modelo OSI son utilizadas para protocolos de acceso tales como Ethernet, Token Ring, FDDI, etc., La capa de red corresponde al protocolo IPX (Internet Packet Exchange) que es una derivación del protocolo IDP (Internet Datagram Protocol) de XNS.

3.2.1 INTERNET PACKET EXCHANGE (IPX)

IPX es el primer protocolo para enrutear en el ambiente Netware. IPX es una implementación del protocolo IDP de la arquitectura XNS con algunas modificaciones. Este datagrama es un protocolo sin conexión, cualquier reconocimiento o control de conexión debe ser provisto por un protocolo de capas superiores. IPX es la interface entre el software del servidor de archivos operando (NCP Network Control Program o shell de la estación de trabajo) y el protocolo de acceso. IPX define dos esquemas de enrutamiento de internetwork y de intranodos. El de internetwork se basa en

un número de red que se asigna a cada interface en una red IPX. El de intranodos es a nivel de número de socket, esto es, si varios procesos se estan corriendo dentro de un nodo, el número de socket provee un distintivo para correr el mismo proceso en diferentes puertos (asociando una aplicación a un número de puerto).

3.2.2 ROUTING INFORMATION PROTOCOL (RIP)

En una red Netware el protocolo de ruteo empleado es RIP. IPX mantiene sus tablas de ruteo dinamicamente. Un ruteador IPX manda paquetes broadcast conteniendo toda la información conocida por el ruteador, estos broadcast sincronizan todos los ruteadores en la red y se actualiza por si la topologia de la red llega a cambiar.

3.2.3 SEQUENCE PACKET EXCHANGE (SPX)

Novell Netware utiliza como protocolo de transporte SPX y se encarga de establecer comunicación punto a punto, además de programas de utilerias como RCONSOLE y SNA gateways,etc.

3.2.4 SERVICE ADVERTISING PROTOCOL (SAP)

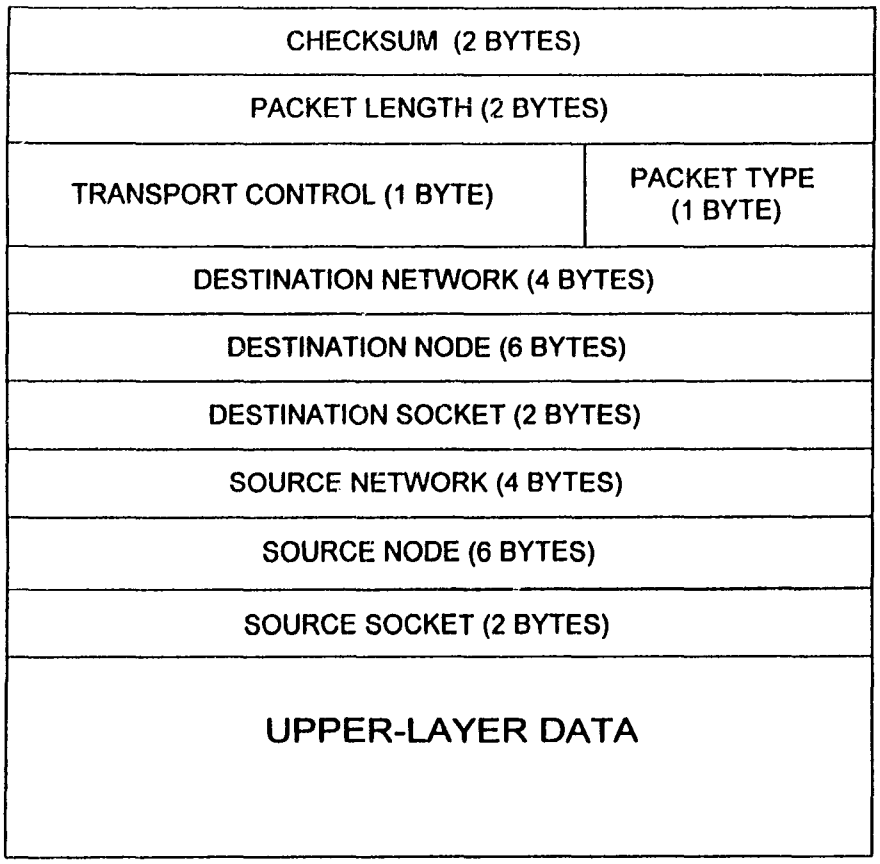
SAP provee a los ruteadores y servidores que contengan agentes SAP intercambiar información de servicios de red.

A través de SAP los servidores anuncian sus servicios y direcciones. Los ruteadores toman esta información y la comparten con otros ruteadores. Esto permite crear y mantener una base de datos de información de servicios de red. Los clientes en la red pueden determinar que servicios están disponibles y obtener direcciones de red de los nodos (servidores) en donde ellos pueden accesar a esos servicios. El cliente requiere de esta información para iniciar una sesión con unservidor de archivo.

3.2.5 FORMATO DEL PAQUETE IPX

El formato del paquete de IPX consiste de dos partes: un encabezado de 30 bytes y una porción de datos, IPX tiene un tamaño de paquete de 576 bytes aunque este valor no esta restringido.

La red, nodo y dirección de socket para el destino y la fuente estan dentro del encabezado.



La figura 3.6: Muestra el formato de paquete IPX.

- Checksum.- el paquete IPX comienza con un verificador de 16 bits puestos a 1´s.
- Packet Length.- este campo de 16 bits contiene la longitud en bytes del paquete completo. Este campo incluye el encabezado IPX y los datos. La longitud debe ser al menos de 30 bytes.
- Transport Control.- es de 1 byte de longitud, indica a traves de cuantos ruteadores ha pasado un paquete en su camino a su destino. Los paquetes son descartados cuando el valor llega a 16.
- Packet type.- es de 1 byte de longitud y especifica que protocolo de capa superior lleva.
- Destination Network.- este campo es de 4 bytes provee el número de red del nodo destino. Cuando el nodo transmisor tiene este campo en cero, el nodo destino esta en el mismo segemento que el nodo que lo manda.

- Destination Node.- es de 6 bytes de longitud y contiene la dirección física de el nodo destino.
- Destination Socket.- de 2 bytes de longitud y contiene la dirección del socket de el proceso del paquete destino.
- Source Network.- es de 4 bytes de longitud y provee el número de red del nodo fuente. Si este campo esta en cero indoca que la dirección local del nodo es desconocida.
- Source Node.- de 6 bytes de longitud y contiene la dirección física del nodo fuente. Las direcciones de broadcast no están permitidas.
- Source Socket.- de 2 bytes de longitud contiene la dirección del socket de el proceso que transmitió el paquete,
- Upper-layer Data.- contiene informacion de las capas superiores.

3.2.5.1 ENTREGA DE PAQUETES IPX

En una red Netware, la entrega exitosa de un paquete depende de el propio direccionamiento del paquete y de la configuración del internetwork. El direccionamiento del paquete es manejado por medio del Media Access Control MAC y los campos de dirección del encabezado IPX.

Para enviar un paquete a otro nodo, el nodo que enviará el paquete debe conocer la dirección de internetwork incluyendo red, nodo y socket de el nodo destino. Una vez que el nodo fuente tiene la dirección del nodo destino, lo que sigue es rutear el paquete. Sin embargo, la forma de que el header MAC de ese paquete sera direccionado depende en si el nodo fuente y el nodo destino estan separados por un ruteador. Como se muestra en la figura 3.7.

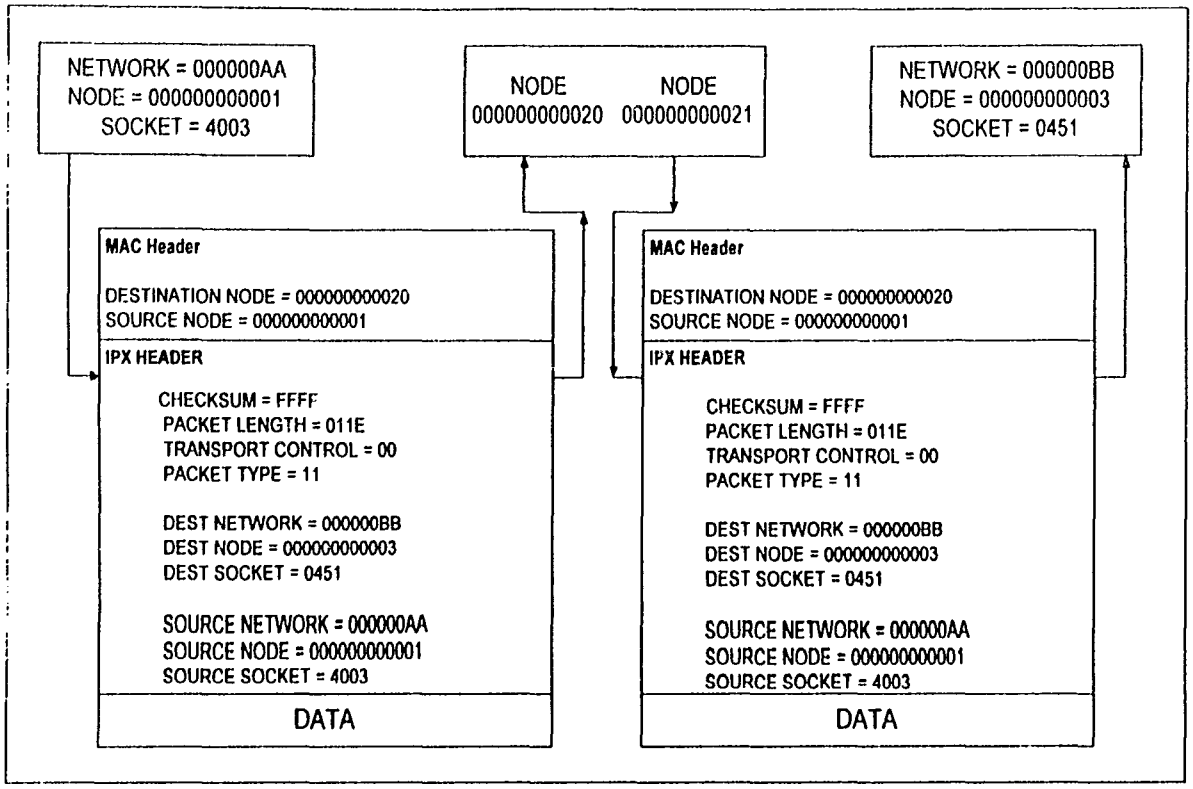


Figura 3.7 Estructura del paquete SAP

SAP usa IPX y protocolos de acceso al medio para su transporte. La estructura permite las siguientes funciones:

- Una petición hecha por una estación de trabajo para encontrar el nombre y la dirección del servidor más cercano de un cierto tipo.
- Una petición de un ruteador para los nombres y direcciones de todos los servidores o de todos los servidores de un cierto tipo en el internetwork.
- Una respuesta a una estación de trabajo o a una petición de un ruteador.
- Broadcast periodicos por servidores y ruteadores.
- Broadcast de información de algún cambio en un servidor.

La figura 3.8 nos muestra la estructura de un paquete SAP, hay que notar que el paquete esta encapsulado dentro del area de datos de IPX

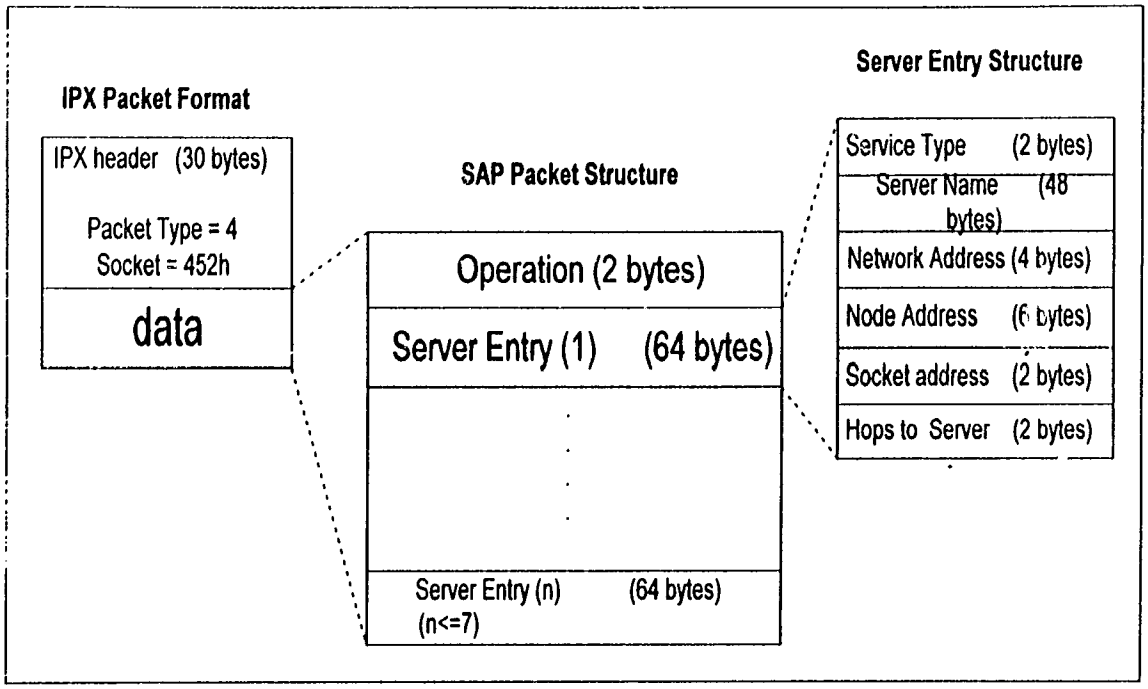


Figura 3.8 : estructura de un paquete SAP

Un paquete SAP tiene los siguientes campos.

- Operation .- este campo indica el tipo de operación que el paquete SAP ejecuta. Puede ser de alguno de los siguientes valores:

1 = Request
2 = Response
3 = Get Nearest Server Request
4 = Get Nearest Server Response

- Server Entry.- cada entrada de 64 bytes al servidor incluye información acerca de un servidor en particular. Este consiste de los siguientes campos:

- Service type.- de 2 bytes de longitud identifica el tipo de servicio que el servidor provee.
- Server name.- este campo contiene una cadena de caracteres de 48 bytes de longitud para asignar un servidor. El nombre del servidor, en combinación con el tipo de servicio, unicamente identifica un servidor en una internetwork.
- Network address.- es de 4 bytes de longitud y contiene la dirección de red del servidor.
- Node address.- es de 6 bytes de longitud contiene la dirección del nodo del servidor.
- Socket address.- es de 2 bytes de longitud y contiene el número de socket que el servidor usa para recibir peticiones de servicios.
- Hops to server.- es de 2 bytes de longitud e indica el número de redes intermediaria que debe de pasar para alcanzar el servidor asociado con este campo. Cada vez que el paquete pasa a traves de una red intermediaria, el campo se incrementa en 1.

Usando SAP, los servidores pueden anunciar sus servicios y sus direcciones. La información que ese servidor dispersa (broadcast) no es directamente usada por los clientes; más bien es recolectada por un agente SAP dentro de cada ruteador en el segmento del servidor. Los agentes SAP almacenan esta información en una tabla de información del servidor. Si el agente reside dentro de un servidor, la información es también almacenada en su tabla. Los clientes pueden contactar al ruteador más cercano o servidor de archivos mediante un agente SAP para informacion sobre el servidor.

El SAP broadcast a aquellos servidores y ruteadores locales y solo recibe de agentes SAP en sus segementos conectados. Sin embargo los agentes SAP periódicamente broadcast su servidor de información, así todos los agentes SAP en el internetwork tienen información acerca de todos los servidores que estan activos en el internetwork.

3.2.6 TABLA DE INFORMACIÓN DEL SERVIDOR

Una Tabla de información del servidor se muestra en la siguiente figura 3.9.

ERVER TABLE

Interface	Name	type	Network	Node	Socket	Hops	Age
1	LPX1102	4	4569f33	00-00-00-00-00-01	451	2	102
1	LPX1103	4	4569f44	00-00-00-00-00-01	451	5	65
2	LPX2001	4	45470001	00-00-00-00-00-01	451	4	33

Figura 3.9: Tabla de información de un servidor novell

La tabla contiene la siguiente información:

Interface, nombre del servidor, tipo de servidor, dirección de red, dirección de nodo, dirección de socket, número de saltos a otro servidor y edad del servidor.

3.3 SNA (SYSTEM NETWORK ARCHITECTURE)

SNA como arquitectura se encuentra orientado al procesamiento distribuido y a la administración de las comunicaciones. Representado un conjunto común de estándares de interconexión, para que una familia de productos de hardware y software se comuniquen.

SNA tiene como objetivo primordial de proveer:

- mecanismos de distribución de funciones, que realicen algunas tareas del computador central hacia los periféricos del sistema y equipos remotos.
- Libertad de conexión para que diferentes equipos puedan conectarse al mismo enlace, usando un protocolo común , SDLC.
- Independencia del dispositivo, ya que cuando las aplicaciones sean escritas no se tome en cuenta las caracterñisticas específicas del dispositivo a ser usado.

- Flexibilidad de configuración para cambiar facilmente la distribucion de la red.

3.3.1 TIPOS DE DATOS EN SNA

- datos de aplicación, pudiendo ser incompatibles de la forma de operar del usuario a quien va dirigido.
- Comandos SNA, activan, controlan y desactivan la red.
- Datos de respuesta, indicando que la formación recibida se acepta o se rechaza, en caso de que sea esta última decir la causa del rechazo.
- Datos de encabezamiento, estos existen dentro de los tres anteriores, indicadores de control o información para el correcto ruteo de mensajes.

SNA se organiza en capas sobrepuestas, en cada nodo de la red. SNA tiene 6 capas diferentes sin incluir la capa fisica.

Capa física.- se encarga de establecer las características físicas de la interconexión entre dos nodos adyacentes usando un protocolo propio para transportar las señales del origen al destino (establece especificaciones de los conectores).

Capa de control de enlace de datos (DLC).- organiza las reglas que gobiernan las comunicaciones en una línea que conecta dos nodos adyacentes a través del cual se transfieren los bits que forman el mensaje. Existe un componente en la capa DLC por cada línea de comunicación del nodo.

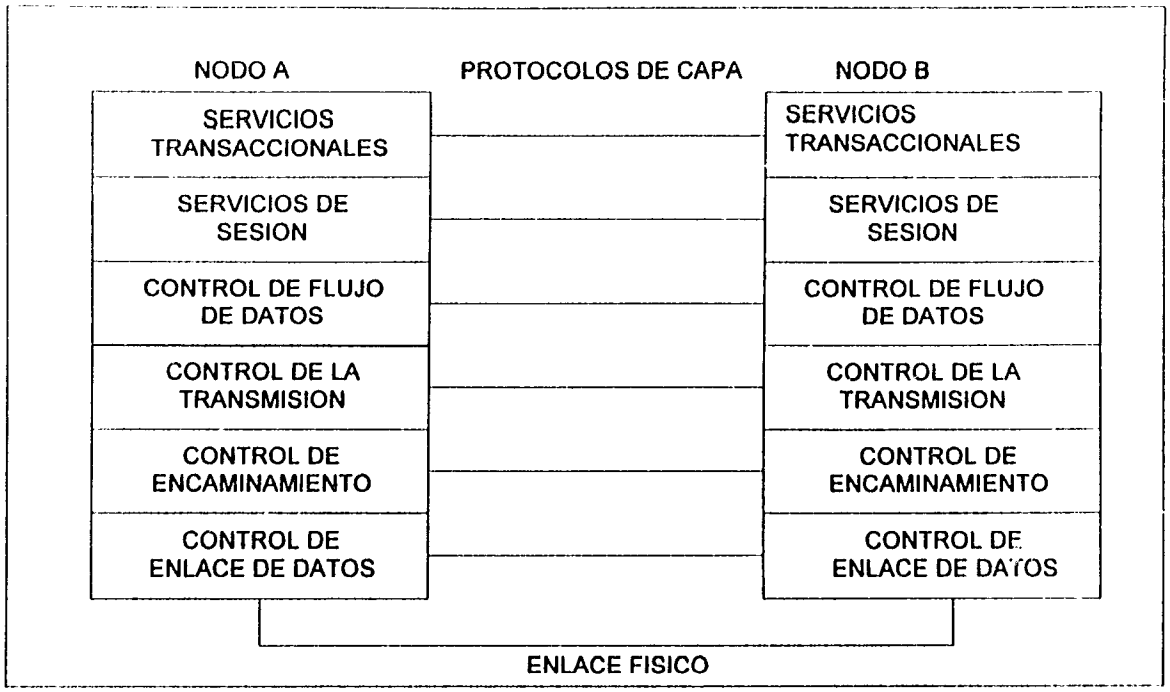


FIGURA 3.10: CAPAS DE SNA.

Capa de control de encaminamiento (PC).- esta ejecuta la función de ruteo dentro de los nodos, ademas de asignar a los mensajes un camino alternativo cuando existen condiciones que asi lo determinen.
Existen dentro de la capa dos funciones que determinan la próxima acción a seguir, llamados "ruta explicita" y "ruta virtual". En cada nodo el PC selecciona el proximo nodo a donde se le enviaran los datos y el enlace que se utilizará usando direcciones (NA: network address) y una tabla de ruteo (RT: routing table). Además encasilla los datos dentro de un tamaño con la capacidad del protocolo de comunicaciones.

Capa de control de transmisión.- es la responsable de mover los mensajes desde el nodo origen hasta el nodo destino.

Administra la tasa de transferencia de mensajes, previendo sobrecargas, mejorando la utilización de la línea. Administra la correcta secuencia de los mensajes hacia el usuario final o hacias otras capas de control (DFC y TC).

Capa de control de flujo de datos (DFC).- realiza la mayoría de las funciones de mantenimiento de la integridad de los datos transmitidos en una sesión de comunicaciones entre entidades de la red.

3.3.1.1 MODOS DE ENVÍO DE RECEPCIÓN:

- Modo "full-duplex". Flujo bidireccional entre las entidades involucradas en la sesión
- Modo "half-duplex flip-flop". Se alterna el sentido de transmisión entre las partes donde una dirige el trafico.
- Modo "full-duplex contention". Cualquiera de las partes puede comenzar el envio de datos a la otra.

3.3.1.2 ENCADENAMIENTO:

Mensajes relacionados que se envian en una misma dirección, puede agruparse lógicamente en una unidad mayor llamada "cadena". En caso de error en un "eslabón" de la cadena causa que el resto de la misma se ignore, llamando al procedimiento de recuperación.

3.3.1.3 OPCIONES DE RESPUESTA:

DFC realiza otras funciones. Por ejemplo , permite que un usuario final interrumpa temporalmente el flujo de datos sin finalizar la sesión de comunicaciones.

Servicios a las sesiones en la red.- estos servicios se encuentran ubicados en los puntos de control de los servicios del sistema (SSCP), en las unidades lógicas y en las unidades (PU).

- Servicios de configuración.- controlan los recursos asociados con la configuración física de la red SNA. Permite que el operador de la red altere la configuración de la misma.
- Servicios al operador de la red. Facilitan la comunicación entre el punto de control y los operadores de la red. Además de proveer los medios para ejecutar comandos para arrancar y detener la red SNA.
- Servicios de sesión.- Activan y desactivan sesiones cuando así se solicita. Convierte los "nombres" de los elementos que inician una sesión, en "direcciones de red".
- Servicios de gerencia y mantenimiento.- permite que un punto de control ejecute varias pruebas para verificar si un nodo o un enlace han fallado y por que razón.

Servicios a los usuarios finales (transacciones).- Estas se dividen en dos categorias: de "presentación" y de "aplicación a aplicación".

- Servicios de presentación: Definen el puerto a la red SNA por un usuario final:

- Requerimientos de traducción de códigos y comandos.
- Formato de pantalla, atributos de video,etc.
- Compresión y compactación de datos.
  Se encarga de que los mensajes sean compatibles con las características del usuario final del destino.

- servicios de aplicación a aplicación:

Estos servicios son definidos para las sesiones que vinculan dos sistemas de procesamiento transaccional. Se acceden desde programas de aplicación permitiendo que estos, en diferentes nodos, se comuniquen entre sí , sin tener en cuenta el protocolo. También permite que un programa de aplicación obtenga acceso a una base de datos, sin saber donde se encuentra está en la red.

3.3.2 CONCEPTOS DE SNA

SNA define las responsabilidades funcionales de cada componente en la red y las reglas de comunicación entre los mismos:

- Usuario final (EU: End User).- el termino "usuario final" hace referencia a una terminal de computador, al operador de la misma o a un programa de aplicación. El usuario final no forma parte de la red sino que se sirve de ella, es emisor y receptor de datos que fluyen por la red.
- Unidades Lógicas (LU: Logical Unit).- como los usuarios no son parte de la red no se identifican con esta, debe existir algún punto de conexión o contacto entre la red y el usuario llamada "unidad lógica".

Una LU es una pieza de software que permite que un usuario se conecte a la red para usar sus servicios, enviar y recibir datos por la red.

3.3.2.1 SESIONES ENTRE UNIDADES LÓGICAS:

Un usuario final accede a la red para comunicarse con otro usuario a través de una sesión LU-LU, permitiendo el intercambio de datos entre unidades lógicas. Cuando activamos una sesión LU-LU, la red provee recursos a disposición de las partes, tales como capacidad de memoria y del procesador.

3.3.2.2 ACTIVACIÓN DE UNA SESIÓN:

Una sesión entre dos unidades lógicas pueden ser iniciadas por una de las dos LU´s, por una de las LU diferente, por el operador de la red o por un procedimiento predefinido. Si se cumplen ciertas condiciones:

- existe un camino disponible entre las LU´s.
- Ambas LU´s cumplen con las necesidades de los usuarios.
- Hay una autorización para la conexión.

3.3.2.3 CONTROL DE FLUJO DE UNA SESIÓN:

Un aspecto importante para el control es el secuencionamiento del intercambio, el momento en que la LU se convierte de emisora en receptora, como se esperan las respuestas, la velocidad de arribo de los datos, para regular el flujo se utiliza la técnica llamada "Session Level Pacing".

3.3.2.4 DESACTIVACIÓN DE UNA SESIÓN:

Una sesión se desactiva apetición de una de las partes involucradas, o por causa de un evento ajeno a la sesión.

3.3.2.5 FLUJO DE DATOS EN UNA SESIÓN LU-LU:

Los datos transmitidos en una sesión LU-LU pueden viajar entre":

- un programa y una terminal.
- Dos programas, que residen.
- Dos terminales.

3.3.3 TIPOS DE UNIDADES LÓGICAS:

Una unidad lógica define el subconjunto de protocolos de capas y opciones sna, soportados por programas de aplicación durante una sesión.

LUT 0 (unidad lógica tipo cero).- llamada extremo abierto vincula dos programas.

LUT 1 (unidad lógica tipo uno).- refiriendose al flujo de datos entre una terminal y un programa.

LUT 2 (unidad lógica tipo dos).- vincula un programa con una terminal usando una corriente "datos 3270".

LUT 3 (unidad lógica tipo tres).- se refiere al flujo de datos entre un programa y una terminal.

LUT 4 (unidad lógica tipo cuatro).- define el flujo de datos entre dos terminales o un programa y una terminal.

LUT 6 (unidad lógica tipo seis).- se refiere al flujo de datos (complejo) entre programas.

LUT 6.2 (alias LU "C") .- unidad lógica tipo C diseñada para comunicaciones avanzadas entre programas de aplicación.

3.3.4 UNIDADES FÍSICAS (PU: PHYSICAL UNIT):

Representa las partes físicas que contiene el producto respecto a la red. Es un conjunto de componentes SNA que provee servicios usados para controlar enlaces, terminales, controladores y procesadores de la red.

El tipo de PU define la clase de nodo que representa en la red, determinando el rol de ese nodo dentro de la red.

PUT 5 .- unidad que representa un nodo central (host) conteniendo una PU, una LU y un SSCP.

PUT 4.- nodo que contiene software de control de encaminamiento (PC), una PU y una LU.

PUT 2 .- nodo final con funciones de ruteo limitadas, conteniendo una PU y LU.

PUT 1 .- dispositivos de dirección única conteniendo opcionalmente una

LU. Dispositivos simples, de bajo costo o dispositivos pre-SNA.

3.3.5 SSCP (SYSTEM SERVICES CONTROL POINT)

Conjunto de componentes SNA actuando como el cerebro de control e interactuando con los operadores de la red. Tres son las funciones principales que realiza:

- administra recursos de la red de acuerdo con los comandos emitidos por los operadores.
- Coordinación de la activación de sesiones entre unidades direccionables de la red.
- Activación de sesiones en la red física cuando ellas sean requeridas.

3.3.6 UNIDADES DIRECCIONABLES NAU (NETWORK ADDRESSABLE UNITS):

Conjuntos de componente SNA que proveen servicios permitiendo a los usuarios enviar datos a través de la red, además de ayudar a los operadores a ejecutar funciones de control y administración de la red.

Las NAU's contienen controladores, procesadores, piezas de hardware y software para terminales, comunicandose entre sí, a través de los caminos de control (PC). Cada NAU tiene una dirección que las identifica, llamada dirección de red.

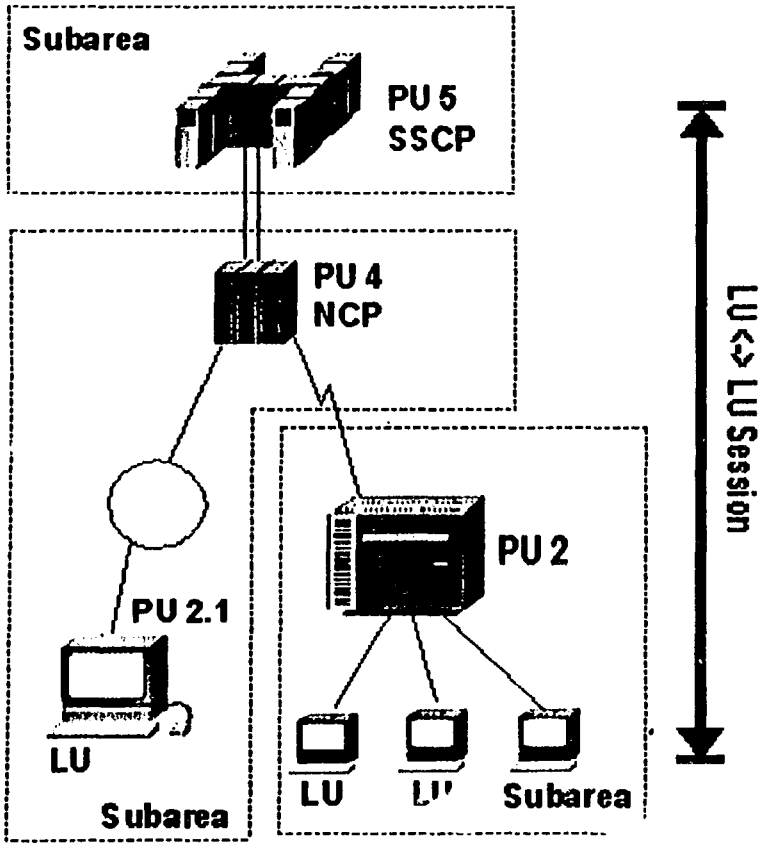


FIGURA 3.11: Ejemplo de una NAU

3.3.6.1 CLASES DE NAU`S

- Las unidades lógicas (LU), que representan a los usuarios finales dentro de la red.
- Las unidades físicas (PU), que representan en la red a las propiedades físicas de los dispositivos.
- El punto de control de los servicios del sistema (SSCP), que gobierna toda la red o parte de ella (dominio).

La comunicación entre NAU`s se da en cuatro clases de sesiones:

- Unidades lógicas entre sí (LU-LU).
- Unidades lógicas con el punto de control de los servicios del sistema (SSCP-LU).
- El punto de control de los servicios del sistema con unidades físicas (SSCP-PU).
- El punto de control de los servicios del sistema entre sí, cuando estan en dominios diferentes(SSCP-SSCP).

Un SSCPsesiona con las LU`s, permitiendo a los usuarios finales acceder, controlar y supervisar el procesamiento y los recursos de comunicaciones de la red.

Un SSCP tiene sesiones con las PU`s , para que los operadores de la red accedan y controlen la red.

En caso de tener la red dividida, los SSCP se comunican entre sí coordinando sus actividades. Las unidades físicas PU se comunican entre sí en una relación llamada flujo PU-PU.

Como en el caso de cuando se desea transferir un programa de un nodo a otro o también se usa en el manejo de rutas entre nodos.

3.3.7 DOMINIO

Un dominio es el grupo de nodos y recursos controlados por un único nodo central, consistiendo:

- un SSCP.
- Los sistemas aplicados y sus LU's.
- La PU del sistema central, CC's y controladores remotos.
- LU`s de los dispositivos terminales asociados con los PU's.

Una red SNA consiste de uno o más dominios SNA. En ACF/SNA, una red puede tener cualquier número de dominios. Un dominio es una colección de NAU's y las comunicaciones entre dominios son controladas y apoyadas por el software NCP que recide en los procesadores de comunicaciones (FEP).

3.3.8 NODO

Un nodo es un punto de la red conteniendo componentes SNA. Cada procesador, controlador y terminales que respete las especificaciones SNA, puede ser un nodo. Realmente un nodo no es una máquina sino que esta dentro de la máquina y esta puede contener varios nodos SNA.

Según sus propiedades y las características de su interrelación en SNA se definen en dos clases de nodos:

- de subárea
- periféricos

Una subárea es una parte es una parte de una red SNA que contiene un nodo (de subárea) y todos los nodos periféricos conectados a él. Un nodo de subárea puede recibir y mover mensajes desde y hacia cualquier destino dentro de la red. Mientras que un nodo periferico solo puede transferir mensajes entre una NAU contenida en él y el nodo de subárea del cual depende. Por lo cual un nodo periferico solo maneja direcciones locales.

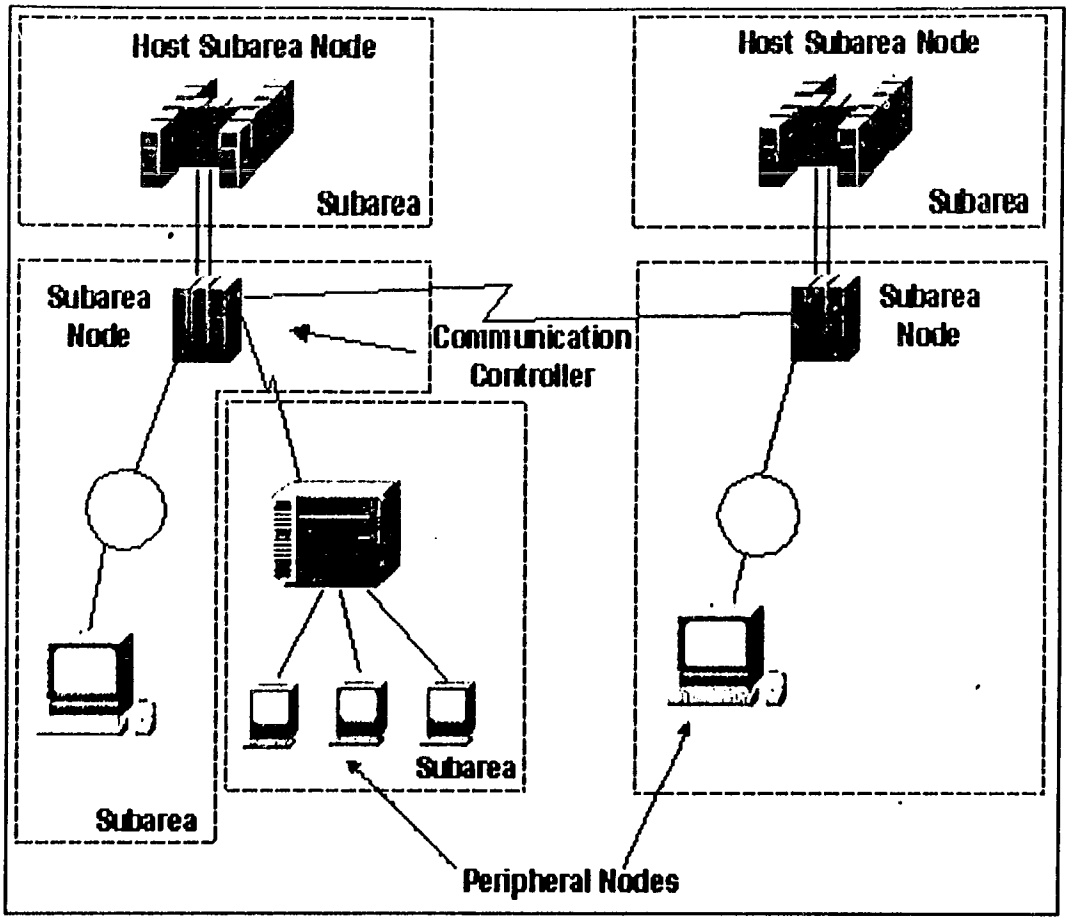


FIGURA 3.12: Ejemplo de nodos SNA

3.3.9 RUTAS EXPLICITAS Y RUTAS VIRTUALES:

Ruta explícita: cuando dos NAU que residen en nodos de subárea están en sesión, hay un camino entre los nodos quese llama "ruta explícita". Si una de las NAU se encuentra en un nodo periférico, el tramo entre el nodo de subárea y el periferico, se llama "enlace periferico".

Ruta virtual: el ruteo virtual es una técnica de ruteo de control de flujo, que controla la integrídad de los datos, mediante la asignación de números de secuencia.

Una ruta virtual conecta dos nodos de subarea finales que esten participando en una sesión. Cada ruta explicita puede alojar varias rutas virtuales.

3.4 TCP/IP

3.4.1 INTRODUCCION

TCP/IP es una familia de protocolos desarrollados a principios de los años 70's por el Departamento de Defensa de los Estados Unidos (DoD). Está arquitectura permite la interconexión de redes con diferentes arquitecturas basándose principalmente en dos protocolos: TCP (Transport control Protocol) de capa 4 del modelo OSI y el IP (Internet Protocol) de capa 3. Dentro del ambiente TCP/IP a todas las terminales, computadoras, servidores, etc., son referidos como "hosts". Los dispositivos que interconectan a las redes mediante IP son conocidos como "gateways" (estos son similares funcionalmente a lo que hace un ruteador en una red LAN). Los gateways también se conocen como ruteadores IP. La familia de protocolos TCP/ IP se muestra en la figura 3.13.

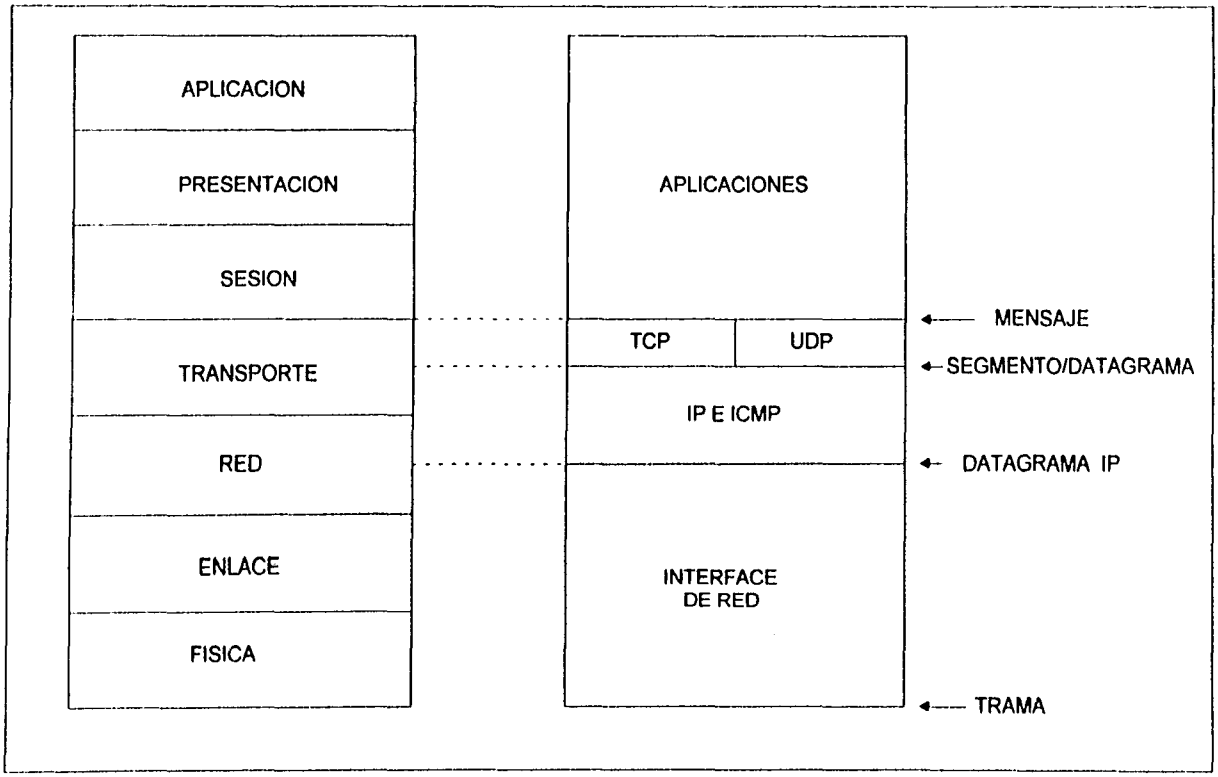


Figura 3.13: ARQUITECTURA TCP/IP (DoD)

La primer capa es la interface de red NI (Network Interface), esta capa puede tener Ethernet, X.25, Token Ring, etc. El acceso a los puertos se logra en la capa física, en la capa de enlace se utilizan direcciones físicas MAC y el LLC (logical link control). La capa que sigue es la de IP, después sigue la capa TCP y UDP, este último es muy usado para aplicaciones como FTP, SMTP, TELNET y SNMP.

3.4.2 DIRECCIONES IP

Una dirección consta de dos partes: el número de red y el número de host. Existen 5 clases de direcciones IP: A,B,C,D y E como se muestra en la figura 3.14.

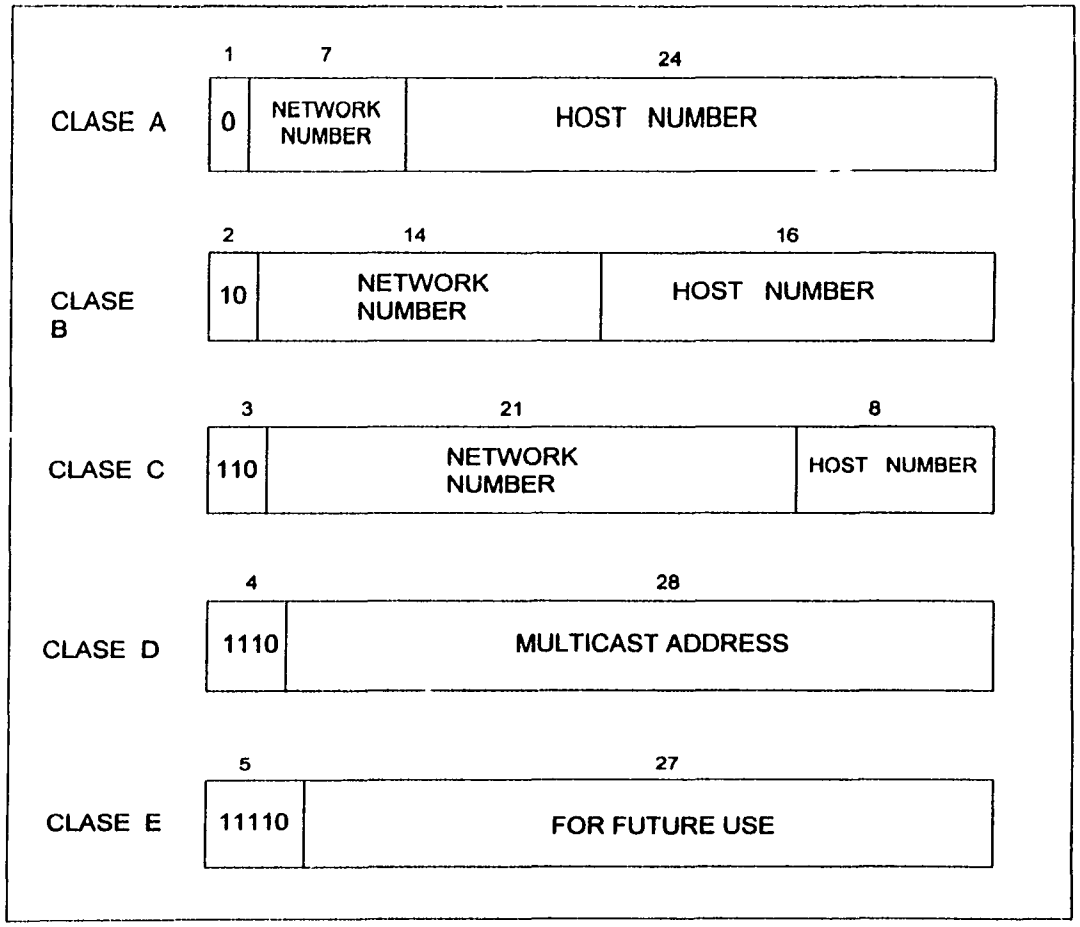


Figura 3.14: CLASES DE DIRECCIONES IP

La diferencia entre las distintas clases se basa en el número de bits que utiliza cada una para el host y para el número de red.

En la clase D los primeros 4 bits son 1110 y el resto se conoce como dirección de "multicast" que sirve para mandar información a un grupo de hosts. "broadcast" es una extensión de multicast en el cual todas las estaciones de una subred reciben la información. La clase E tiene en sus primeros bits 1111 y esta reservada para usos futuros.

Los 32 bits de una dirección IP están divididos en cuatro campos de un byte separados por puntos y los números utilizados son decimales. Además de utilizar notación decimal también podemos utilizar palabras las cuales se asocian a un número decimal (esta conversión la hace un servidor de dominio).

La clase A va del 1.0.0.0 al 126.0.0.0
La clase B va del 128.1.0.0 al 191.254.0.0
La clase C va del 192.0.1.0 al 223.255.254.0
La clase D es de broadcast

Un ejemplo de clase B es 132.248.190.243 y este número es asignado por el Network Information Center (NIC). En un futuro la dirección IP será de 128 bits en la versión de IP No. 6.

Un proceso de aplicación escoge el transporte que requiere, orientado a conexión TCP o sin conexión UDP. La capa TCP/UDP añade un encabezado a los datos que recibe de capas superiores. El proceso de añadir

Un encabezado se conoce como encapsulación. La capa IP en turno adiciona su encabezado y lo pasa a la capa NI y esta utiliza Ethernet o alguna otra tecnología de capa de enlace (2), como se muestra en la figura 3.15.

Si un paquete va a ser transmitido desde un host de una red hacia otra red, entonces una dirección IP local de un gateway debe ser encontrada y el paquete transmitido hacia su correcto gateway. El gateway revisa la dirección IP destino y si la encuentra anotada en su tabla no la envía hacia afuera, sino la manda al host destino en su red, si no la manda hacia otro gateway. Un paquete puede ser entregado a su destino pasando a través de

varias rutas. Para evitar esto los gateways tienen algoritmos para calcular el trayecto correcto.

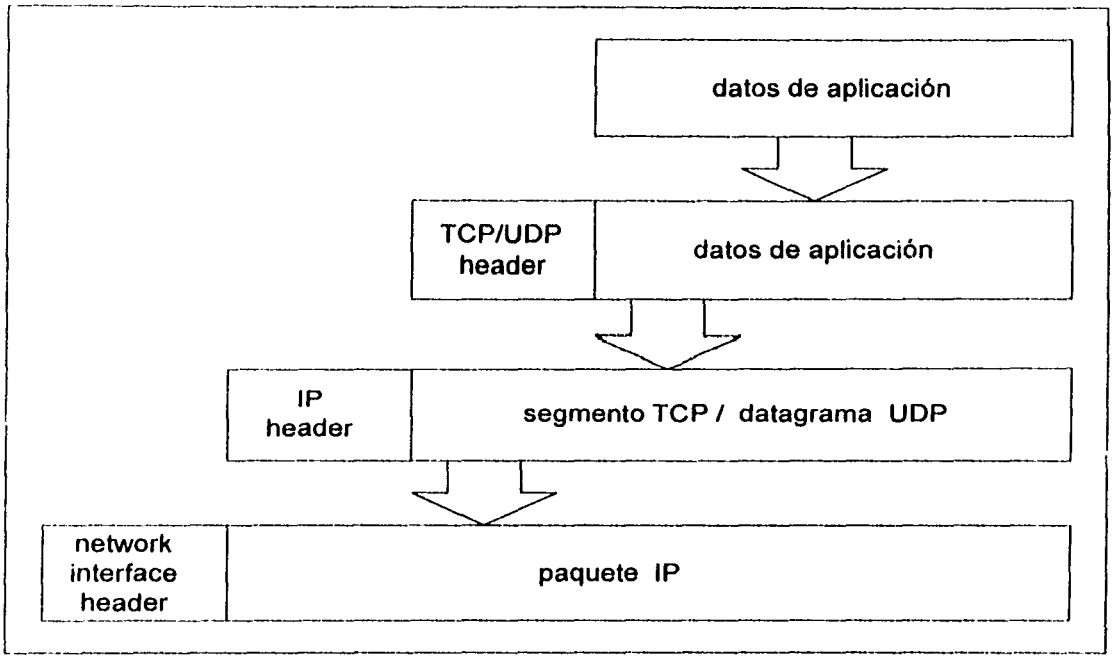


FIGURA 3.15: PROCESO DE ENCAPSULACIÓN

3.4.3 PROTOCOLO INTERNET (IP)

Este es un servicio de entrega de paquetes sin conexión, no hay una entrega punto a punto garantizada, ni control de flujo, ni reconocimiento o recobro de errores. Si se requiere conexión y control para que el paquete llegue a su destino eso lo debe proveer un protocolo de capas superiores (como TCP).

En la siguiente figura 3.16 se muestra un datagrama IP.

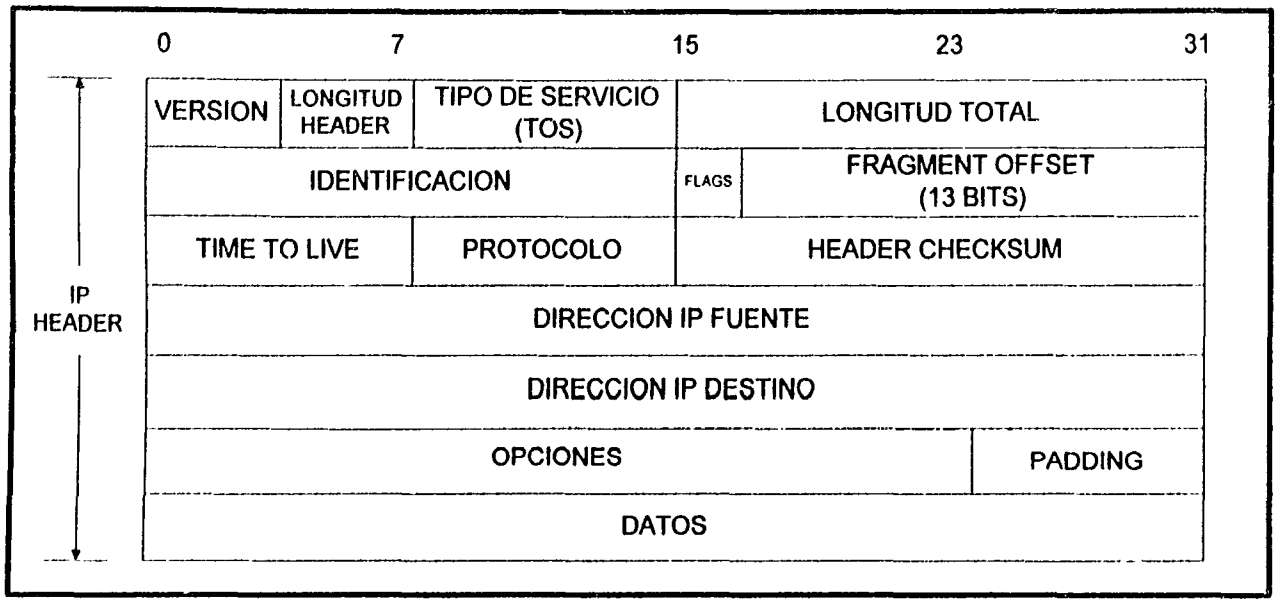


FIGURA 3.16: DATAGRAMA IP

Este consiste de un encabezado y una porción de datos, el encabezado es en múltiplos de 32 bits. En este se encuentran los siguientes campos:

Versión.- versión de IP (actual 4), intercambio de facilidades entre versiones.

Header Length (longitud del encabezado).- tamaño del encabezado o "header" incluyendo el PAD, está en octetos.

Type of service (TOS).- tipo de servicio, de 8 bits de longitud, los primeros 3 son de precedencia (prioridad) para lo cual diferentes niveles son definidos. El tráfico de mayor precedencia es más importante que el de menor precedencia. En la siguiente figura 5 se muestran 3 tipos de TOS según su RFC (Request For Comment).

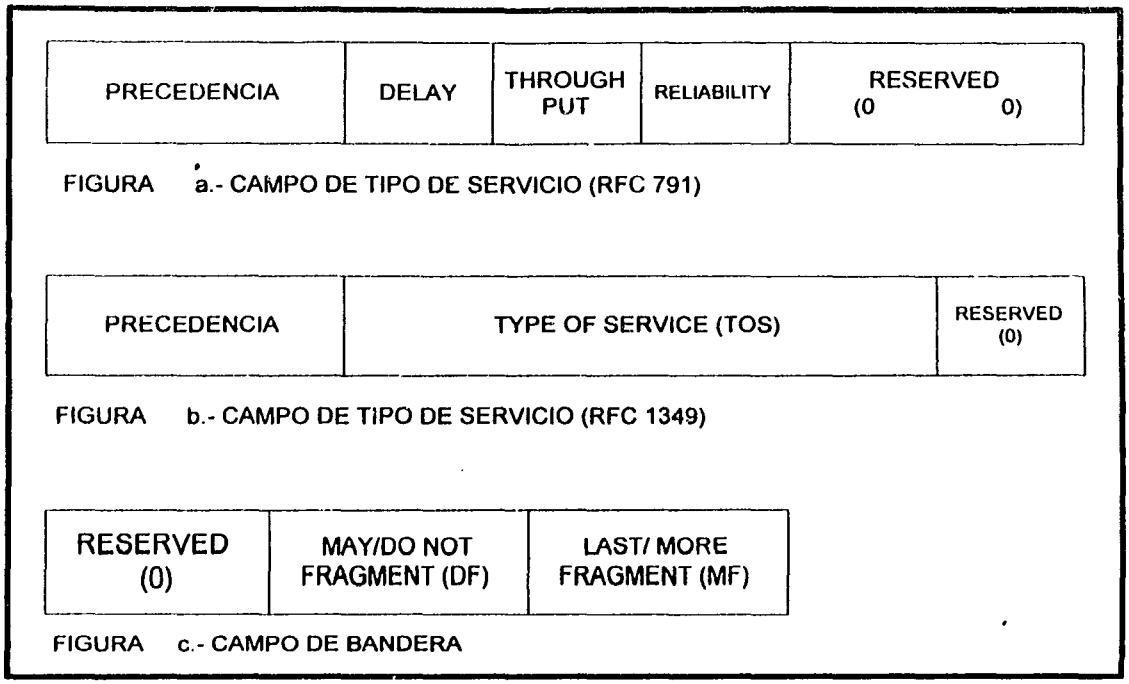


Figura 3.17: TIPOS DE SERVICIO

Figura 3.17a . RFC 791 que tiene campos de delay, throughput y reability y los últimos dos son para usos futuros.

Figura 3.17b . RFC 1349 redefine el campo TOS de 4 bits siendo el último cero.

Campo de identificación.- de 16 bits, sirve para darle una etiqueta al paquete o datagrama.

Campo de banderas (FF) y Fragment offset (FO).- el campo de banderas es de 3 bits y el F.O. es de 13 bits, el primer bit del F.F. es cero, el segundo (bit 1) tiene dos opciones: cero para fragmentar y uno para no fragmentar. El bit 1 es del último fragmento. Como se muestra en la figura 3.17c.

Fragmentation offset.- indica la posición de los fragmentos del datagrama dentro de la red.

Time to live (TTL).- tiempo de vida de un datagrama dentro de la red, es de 8 bits y el tiempo esta en segundos. Cada vez que pasa a través de un gateway el tiempo se decrementa en 1 hasta llegar a cero y destruirse, esto se hace para que no se sature la red con datagramas pérdidos.

Campo de protocolo.- es de 8 bits y contiene el número de protocolo de capas superiores que lleva, por ejemplo ICMP tiene el 1 y TCP el 6.

Header Chechsum.- de 16 bits y verifica el encabezado IP solamente.

Dirección IP fuente.- dirección IP del hosts origen que es de 32 bits.

Dirección IP destino.- dirección a la cual debe llegar el datagrama también de 32 bits.

Campo de opciones.- esta implementado en todos los gateways y hosts y es opcional en los datagramas. Hay dos tipos de opciones, el caso 1 y el caso 2. En la figura 3.18 se muestran los dos casos:

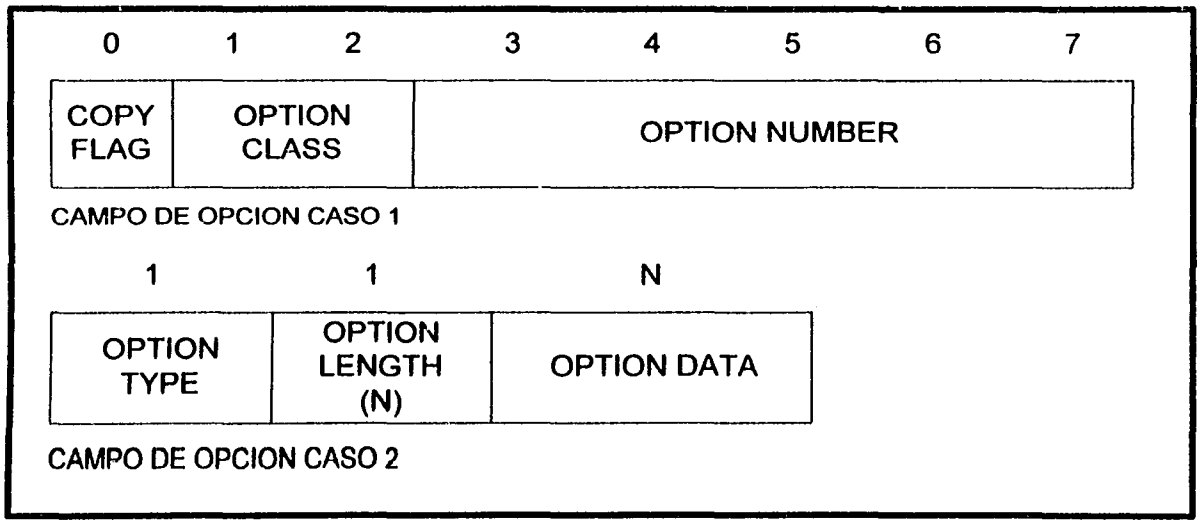


Figura 3.18 : CAMPO DE OPCION

El primer caso es de 1 byte de longitud. El caso 2 tiene un byte de tipo de opción, un byte de opción de longitud y uno de opción de datos. El byte de longitud incluye la longitud del de opción de datos y dos bytes que incluyen un byte de tipo de opción y uno de opción de longitud. El campo de opción tiene un bit de bandera, dos bits de opción de clase y 5 bits de opción

de número, hay que notar que un byte del tipo de opción en el caso 2 es el mismo que el campo de opción del caso 1.

Un bit de bandera indica si el campo de opción es copiado en fragmentos, Si es cero no es copiado y si es 1 se copia en todos los fragmentos.

Campo de PAD.- es usado para asegurar 32 bits si no se completa el de opción.

3.4.3.1 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMP es usado para utilizar mensajes de control de un host hacia otro para verificar si hay algún error.

El mensaje ICMP ocupa el campo de datos de la capa IP contiene un header y datos. Para un mensaje ICMP el campo de protocolo es puesto a 1.

El mensaje ICMP esta formado por las capas que se muestran en la figura 3.19.

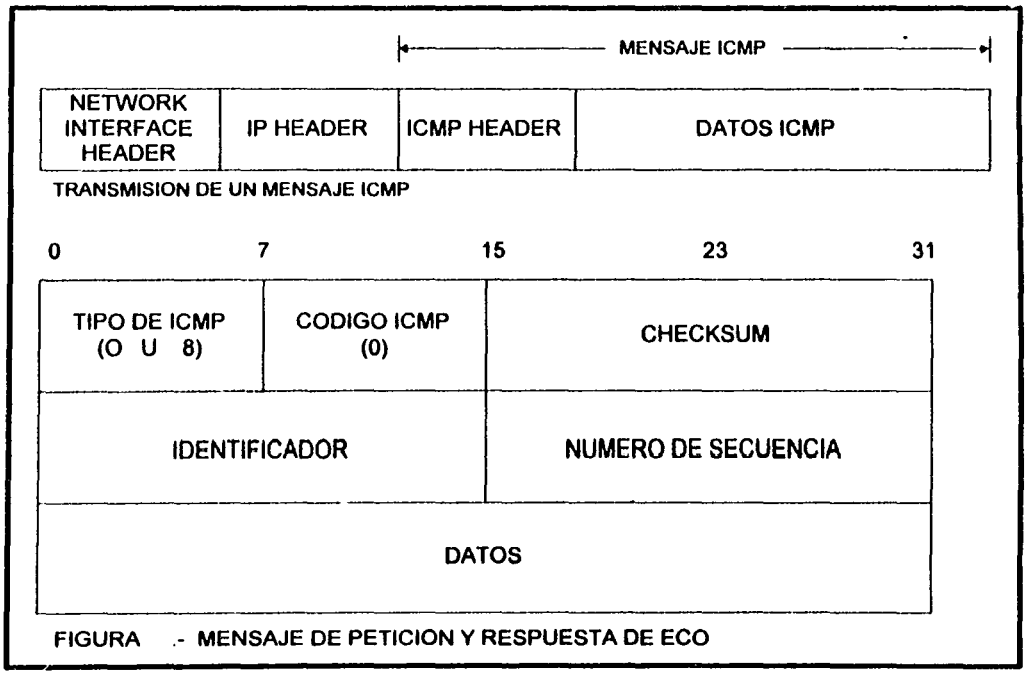


Figura 3.19: MENSAJE ICMP

Para ICMP el campo de TOS es 0000. La dirección fuente es la que genera el mensaje ICMP y la destino a la cual debe llegar el mensaje. El campo ICMP siempre tiene un tipo de campo ICMP en el cual puede haber diferentes mensajes ICMP, también hay un campo de código el cual detalla más acerca de los mensajes y también un campo de verificación (checksum).

Un ejemplo de mensaje ICMP es el PING (Packet InterNet Grouper) que es usado para checar la conectividad de un host desde otro host y obteniendo algunos detalles útiles para la administración de la red. El PING es una petición con respuesta de eco, el mensaje ICMP para esto se muestra en la figura 7. Cuando una petición de eco es enviada el tipo de ICMP es 8, y el de respuesta de eco es 0. El identificador y el número de secuencia son utilizados para identificar y comparar un mensaje y sus repeticiones.

3.4.4 TCP (TRANSFER CONTROL PROTOCOL)

TCP es un protocolo de conmutación de paquetes confiable, orientado a conexión usado para comunicación entre procesos y hosts de computadoras, la transferencia de datos es full duplex y es muy flexible.

No importa que protocolo este arriba o abajo aunque el de abajo generalmente es IP. La combinación de datos de TCP y su encabezado se conoce como segmento.

Otro concepto importante es el de conexión. TCP provee un número de direcciones o puertos en cada host. Muchos procesos pueden ser asociados con un puerto. A una dirección IP y un número de puerto se le denomina socket. Un par de sockets identifican a una conexión. Después de que la comunicación es establecida, una conexión debe ser establecida entre procesos, está conexión es referida como un circuito virtual.

TCP provee reconocimiento y retransmisión de segmentos. Cuando los datos se envían un número de secuencia de el primer byte de datos en el segmento también es enviado y al mismo tiempo se inicia un contador, el receptor al recibir los datos manda un número de reconocimiento para que el siguiente datagrama se envíe, si en un cierto tiempo no se recibe el reconocimiento se retransmite el segmento.

TCP cuenta con verificación de datos (checksum) para evitar errores. El control de flujo se logra por medio de variables de ventana que pueden ser enviados dentro del reconocimiento enviado por el receptor. Si el receptor no tiene espacio disponible en el buffer entonces pide una ventana

más pequeña y viceversa si se tiene espacio disponible se gestiona una ventana más grande.

Un segmento TCP se muestra en la figura 3.20 donde se muestran los siguientes campos:

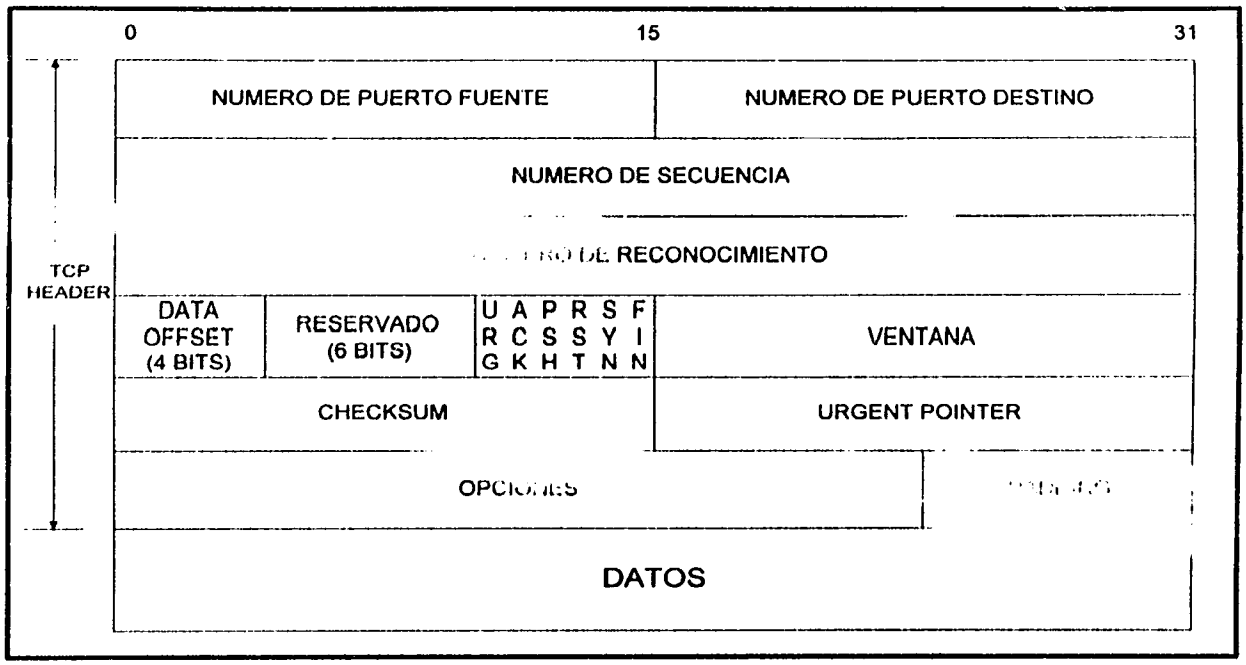


Figura 3.20. SEGMENTO TCP

- Número de puerto fuente.- de 16 bits de longitud y contiene un número de puerto fuente.
- Número de puerto destino.- de 16 bits con un número de puerto al que el segmento debe llegar.
- Número de secuencia.- es de 32 bits y el número de secuencia que espera el destino para pedir el siguiente segmento.
- Número de reconocimiento.- de 32 bits y es el acuse de recibo del segmento que espera, por ejemplo si el número enviado es 100 el que espera es el 101.
- Data offset.- de 4 bits, este campo contiene la longitud del encabezado TCP medido en términos de 32 bits. En un segmento se indica donde los datos empiezan.
- Reservado.- 6 bits para futuras aplicaciones, se ponen en ceros.

Los siguientes 6 campos son de 1 bit de longitud:

- URG.- cuando este bit es puesto a 1, el receptor espera procesar el segmento primero interrumpiendo todo lo demás que tenga pendiente.
- ACK.- cuando este bit es puesto a 1 el reconocimiento es enviado.
- PSH.- cuando este bit esta activado le indica al receptor que este datagrama no puede ser almacenado mucho tiempo en el buffer aunque tenga espacio.
- RTS.- para reiniciar la conexión.
- SYN.- para sincronizar números de secuencia, es usado para iniciar el establecimiento de una conexión por medio de un handshake.
- FIN.- se usa para finalizar una conexión.

- Window.- es de 16 bits, y es el número de octetos que el receptor espera recibir, el tamaño se establece al iniciar la conexión y el tamaño es el mismo para el transmisor y para el receptor.
- Checksum.- de 16 bits, sirve para verificar si el datagrama tiene errores.

- Urgent pointer.- de 16 bits, es tomado en cuenta cuando el bit URG esta activado, posee un número de secuencia al segmento que es urgente su entrega.

- Opciones.- de longitud variable en múltiplos de 8 bits, tiene dos opciones similares a IP.

- Padding (relleno).- longitud variable para completar el campo anterior a 32 bits.

3.4.5 UDP (USER DATAGRAM PROTOCOL)

UDP es un servicio no orientado a conexión, el cual no garantiza la entrega de datos.

UDP utiliza un esquema similar a TCP para la transmisión de datos. Los datos de aplicación son entregados con un header UDP, entonces en la capa IP el header IP es añadido, en la capa NI el encabezado de red es añadido a la trama IP. Esta trama es transmitida de una red a otra, en el extremo receptor la capa NI remueve el header NI y la capa IP remueve el

header IP. La capa UDP en turno remueve el encabezado UDP y manda los datos hacia la correspondiente aplicación. Si hay un error y la trama no es recibida se puede manda un mensaje ICMP para determinar la causa.

El datagrama UDP se muestra en la figura 3.21 y tiene 16 bits de puerto fuente y 16 bits de puerto destino. El campo de longitud contiene el número de bytes de la trama UDP e incluye la longitud del header UDP. El próximo campo es el de verificación, el cual es opcional si no se usa se pone en ceros.

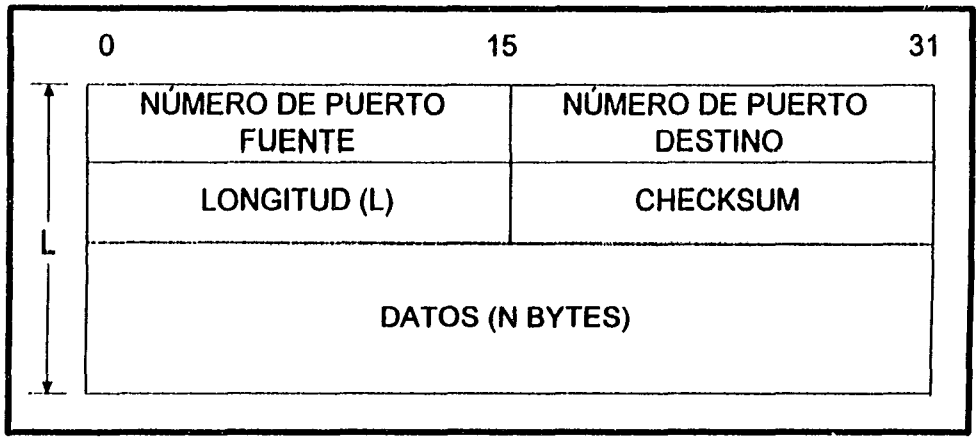


Figura 3.21: DATAGRAMA UDP

3.4.6 ARP (ADDRESS RESOLUTION PROTOCOL)

ARP es un protocolo de bajo nivel usado para localizar una dirección MAC mediante una dirección IP dada. Este protocolo permite a un host o a un ruteador hacer sus decisiones de ruteo usando direcciones IP mientras usa direcciones MAC para enviar paquetes de un salto hacia otro.

Una vez que el host o ruteador conocen la dirección IP del próximo salto hacia el destino, el host o router deben asociar esa dirección IP a su correspondiente dirección MAC antes de que el paquete sea enviado.

CACHE ARP	
IP ADDRESS	MAC ADDRESS
159.101.1.1	00308e3d0042
159.101.2.1	0080232b00ab

Figura 3.22: CACHE ARP

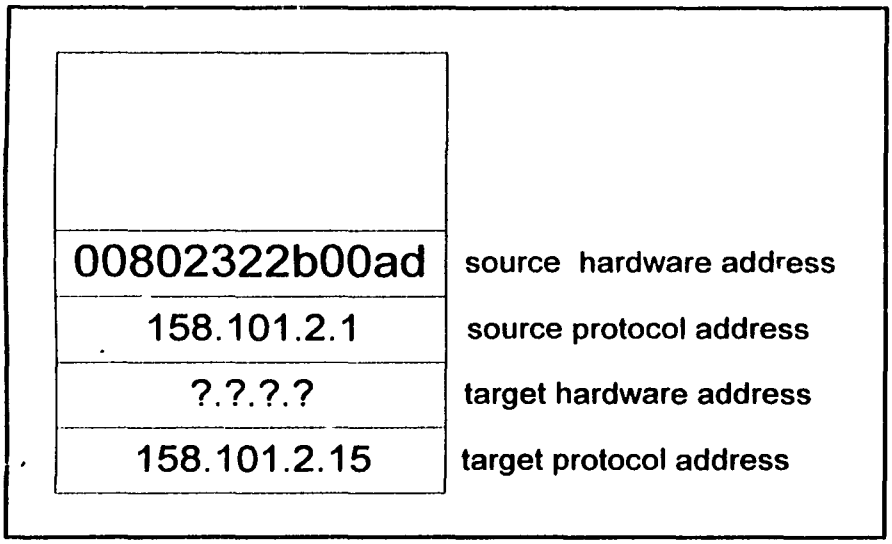


Figura 3.23: PETICION ARP

Para hacer está asociación, el host o ruteador primero mira su cache ARP en la que se encuentra una tabla de direcciones y su MAC correspondiente. Cada dispositivo participante en ruteo tiene un cache ARP, como se muestra en la figura 3.22.

Si la dirección IP no tiene una dirección MAC correspondiente en la tabla, el host o ruteador envía un "broadcast" hacia todos los dispositivos en la red con una petición ARP que contiene informació acerca del hardware y protocolo. Los dos elementos de una petición ARP son el objetivo 'target"

(dirección física destino), la dirección IP y MAC fuente y la dirección IP destino y el protocolo, como se muestra en la figura 3.23.

Cuando el dispositivo en la red recibe el paquete, lo examina y si su dirección no es la misma que la dirección objetivo, descarta el paquete.

Cuando un dispositivo recibe el paquete y confirma que la dirección IP es la misma, el dispositivo pone su dirección MAC en el campo de "target hardware add" y manda el paquete de regreso a la dirección hardware fuente. Cuando el host o ruteador orígen recibe la respuesta ARP actualiza su cache ARP.

3.4.7 RARP (REVERSE ADDRESS RELOLUTION PROTOCOL)

RARP es el proceso inverso de ARP, en el cual el mapeo es de una dirección física a una dirección IP. Una estación puede tener su dirección física, manda un RARP a un servidor dando su dirección IP, y el servidor mapea la dirección IP y manda de regreso la dirección física que se desconocía a la cual corresponde la dirección IP.

3.4.8 DIRECCIONES DE SUBRED

Una red que utiliza un protocolo simple bajo el control de un dominio administrativo se conoce como subred. Una subred puede ser una colección de redes pequeñas. Como se vio anteriormente, la dirección IP consiste de un número de red y un número de host, el número de red es usado para rutear de una red a otra. Esto provee el primer nivel de ruteo. La técnica de particionar una dirección de red para cubrir múltiples redes se conoce como "addressing subnet" o asignación de direcciones de subred. Aquí, un número de host es dividido en más de un nivel de partición de redes y esto ayuda en la formación de niveles de ruteo, como se muestra en la figura 3.24.

Al asignar direcciones de subred, para recobrar el número de red, se utiliza una máscara de subnet de 32 bits, la cual tiene en todo el número de red 1's y la parte del número de subnet es usado. La máscara de subnet tiene ceros en el resto de la máscara. Así cuando los datos serán enviados de una estación A otra, los manda al apropiado ruteador. El ruteador usa el número de subnet para mandar esos datos a la apropiada subnet o red, entonces el número de host es usado para entregar los datos al destino.

Si todas las redes no están usando una dirección de subnet, los ruteadores usan un agente "proxy" ARP. Acorde a esto, se utiliza un ARP con la dirección de una estación el ruteador responde dando su dirección física para la dirección de una estación y después este hace llegar los datos al correcto destino.

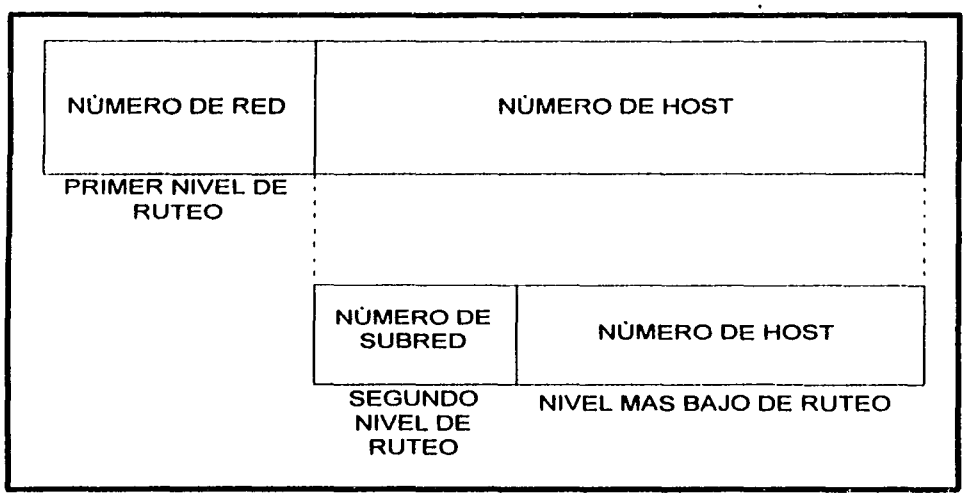


Figura 3.24: DIRECCIONES DE SUBRED

3.5 ARQUITECTURA APPLETALK

3.5.1 HISTORIA

A principios de los 80's, Apple Computer Inc. se preparaba para introducir las computadoras Macintosh, los ingenieros de Apple sabían que las redes llegarían a ser una necesidad, entonces buscaron que las redes basadas en computadoras Mac utilizaran la misma interface de usuario de las Mac. Apple decidió construir una interface de red dentro de cada Mac y así

integrar esa interface dentro del ambiente de escritorio. Esta nueva arquitectura de red fue denominada "AppleTalk".

Aunque AppleTalk es una red propietaria, Apple ha publicado especificaciones

en un intento para fomentar diversos desarrollos. Hoy, muchas compañias diseñan productos basados en appletalk, incluyendo Novell y Microsoft.

La implementación original de AppleTalk, fue diseñada para grupos de trabajo locales y estos son referidos como AppleTalk Fase 1. Con la instalación de más de 1.5 millones de computadoras Mac en los primeros 5 anos de vida del producto, sin embargo Apple encontró que grandes empresas excedían los limites de AppleTalk Fase 1, así que perfeccionaron el protocolo denominando a la nueva versión AppleTalk Fase 2 añadiendo capacidad de ruteo y permitiendo que AppleTalk corriera exitosamente en grandes redes.

3.5.2 TECNOLOGIA BASICA

AppleTalk fue diseñada como un sistema de red distribuido cliente-servidor. En otras palabras, los usuarios comparten recursos de la red (tales como impresoras y archivos) con otros usuarios. Las computadoras que proveen estos recursos de red son denominados servidores, las computadoras que usan estos recursos son llamados clientes. La interacción con los servidores es esencialmente transparente a el usuario porque la computadora en si determina la localización de el material requerido y lo accesa sin intervención del usuario. En adición a esa facilidad de uso, los sistemas distribuidos también tienen ventajas económicas sobre los sistemas punto a punto porque materiales importantes pueden ser localizados en pocas o muchas localidades .

En la figura 3.25 los protocolos de AppleTalk son mostrados junto con las capas del modelo OSI.

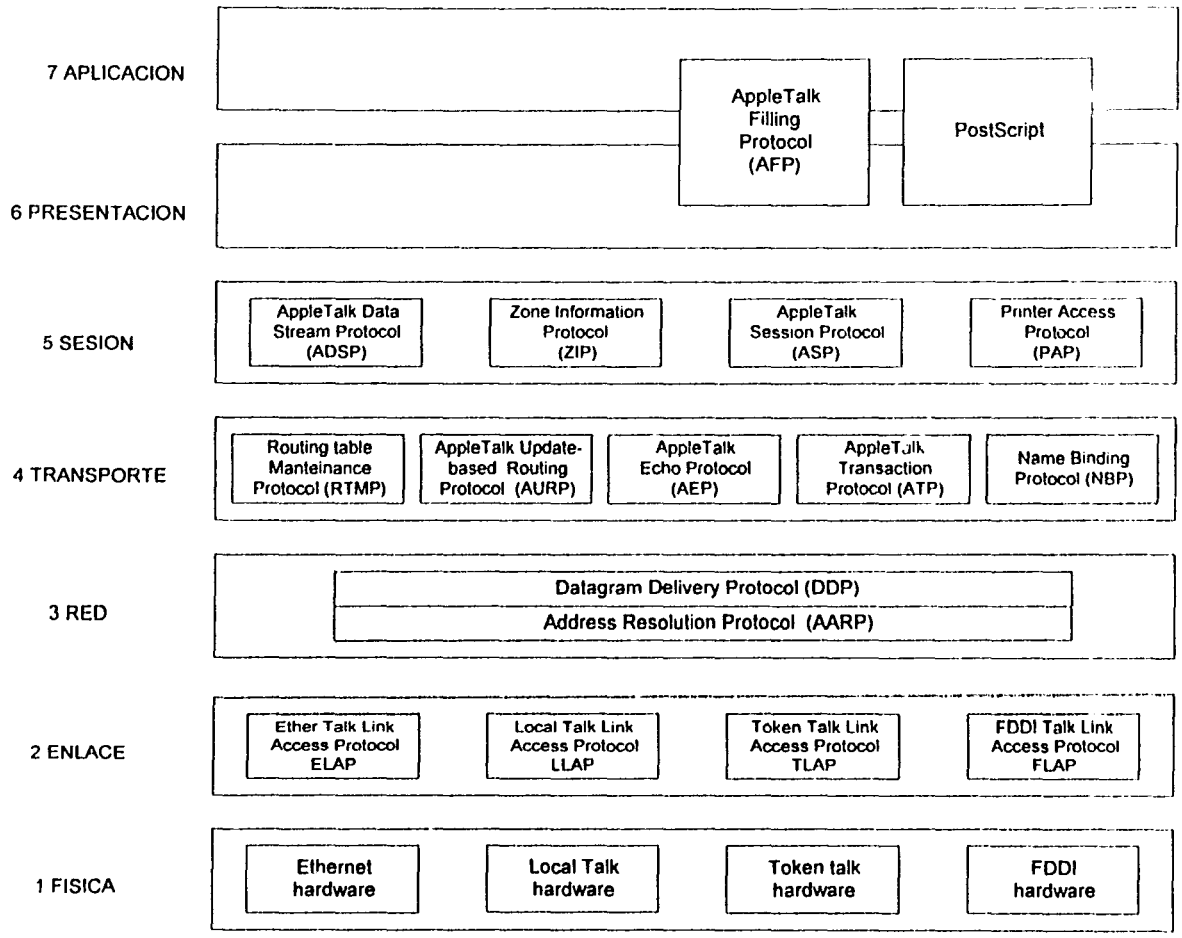


Figura 3.25 : APPLETALK y el modelo OSI

3.5.3 ACCESO AL MEDIO

Apple diseño AppleTalk para tener una capa de enlace independiente. En otras palabras, puede correr teóricamente por encima de cualquier tipo de tecnología de red LAN en la capa de enlace. Apple soporta una variedad de tipos de estas tecnologías como Ethernet, Token Ring, Fiber Distributed Data Interface

(FDDI) y LocalTalk. Apple refiere a AppleTalk sobre Ethernet como EtherTalk, AppleTalk sobre Token Ring como TokenTalk y AppleTalk sobre FDDI como FDDITalk. Los protocolos de capa de enlace que soporta AppleTalk sobre estos medios son : EtherTalk Link Access Protocol (ELAP), LocalTalk Link Access Protocol (LLAP), TokenTalk Link Access Protocol (TLAP) y FDDITalk Link Access Protocol (FLAP).

LocalTalk es el protocolo de acceso al medio propietario de Apple. Esta basado en acceso por contención , topología de bus, y señalización de banda base y corre sobre par torcido a 230.4 kbps. La interface física es EIA/TIA-422 (conocida como RS-422) una interface eléctrica balanceada soportada por EIA/TIA-449 (RS-449). Los segmentos pueden ser de hasta 300 mts y soporta un máximo de 32 nodos.

3.5.4 CAPA DE RED

Para asegurar una mínima sobrecarga en la red, las direcciones de nodo AppleTalk son asignadas dinámicamente. Cuando una computadora corriendo AppleTalk se inicializa, escoge un protocolo (de capa de red), una dirección y revisa si la dirección que escogió esta actualmente en uso. Si no esta en uso, el nuevo nodo es asignado exitosamente con esa dirección. Si la dirección que se escogió esta actualmente usada, el nodo de la dirección repetida manda un mensaje indicando un problema, y así el nuevo nodo escoge otra dirección y se repite el proceso. En la siguiente figura 3.26 se muestra el proceso de selección de una dirección.

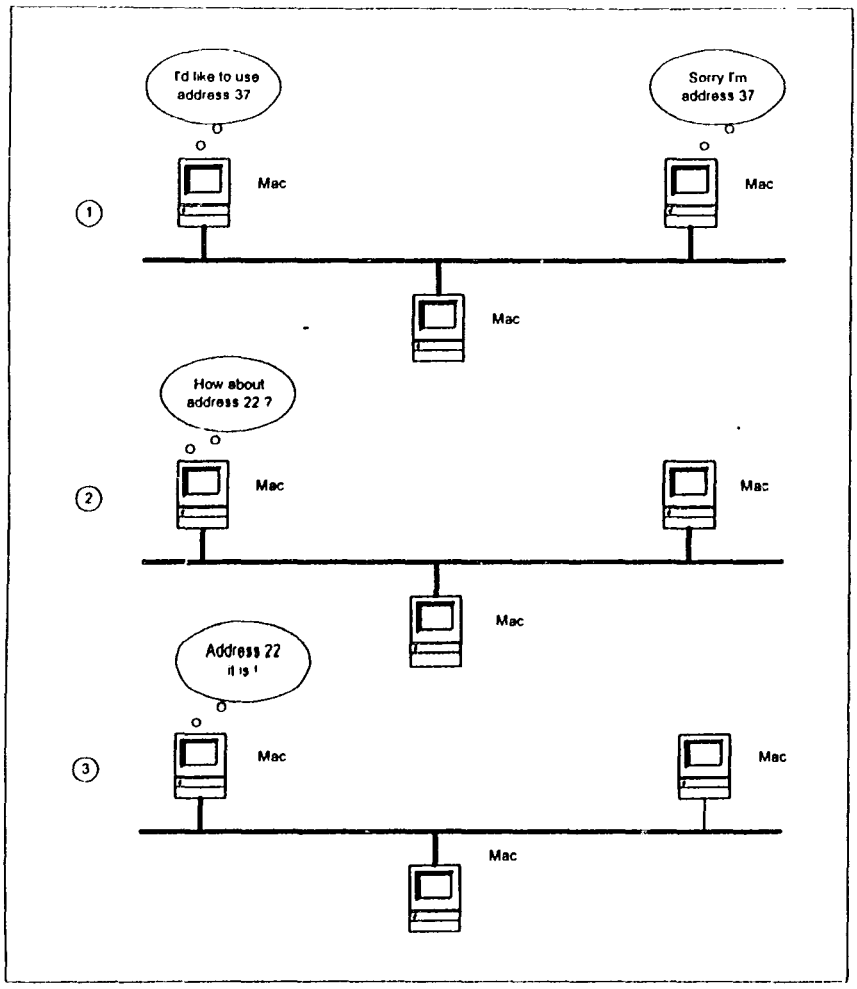


Figura 3.26 :Proceso de selección de direcciones APPLETALK

El actual mecanismo de selección de direcciones de AppleTalk es dependiente del medio. El protocolo de resolución de direcciones AppleTalk (AARP) es usado para asociar las direcciones AppleTalk con una dirección del medio particular. AARP también asocia otras direcciones de protocolo con direcciones de hardware. Cuando AppleTalk u otra pila de protocolos debe enviar un paquete a otro nodo de red, la dirección del protocolo es pasada hacia AARP. AARP primero revisa si la dirección en cuestión esta almacenada en su tabla de direcciones, si se encuentra, la pasa hacia el protocolo que la requiere. Si no, AARP inicia un broadcast o un mensaje multicast para preguntar acerca de la dirección de hardware para la dirección del protocolo en cuestión. Si el broadcast alcanza un nodo con la dirección del protocolo especificada, ese nodo retransmite con su direc. de

hardware. Esta información es pasada hacia el protocolo que pregunto, el cual usa la dirección de hardware para comunicarse con ese nodo.

3.5.5 ENTIDADES DE RED

AppleTalk identifica varias entidades de red. El mas elemental es un nodo, el cual es simplemente cualquier dispositivo conectado a una red AppleTalk. El nodo mas común es una computadora Macintosh e impresoras láser, pero otros tipos de computadoras también pueden entablar comunicación con AppleTalk, incluyendo IBM, Digital, VAX y otra variedad de estaciones de trabajo. La siguiente entidad que se define es la red. Una red AppleTalk es simplemente un cable lógico. Aunque el cable lógico es frecuentemente un cable físico, algunos sitios usan bridges para interconectar varios cables físicos. Finalmente se define una zona, una zona es un grupo lógico de redes. Estas entidades AppleTalk son mostradas en la

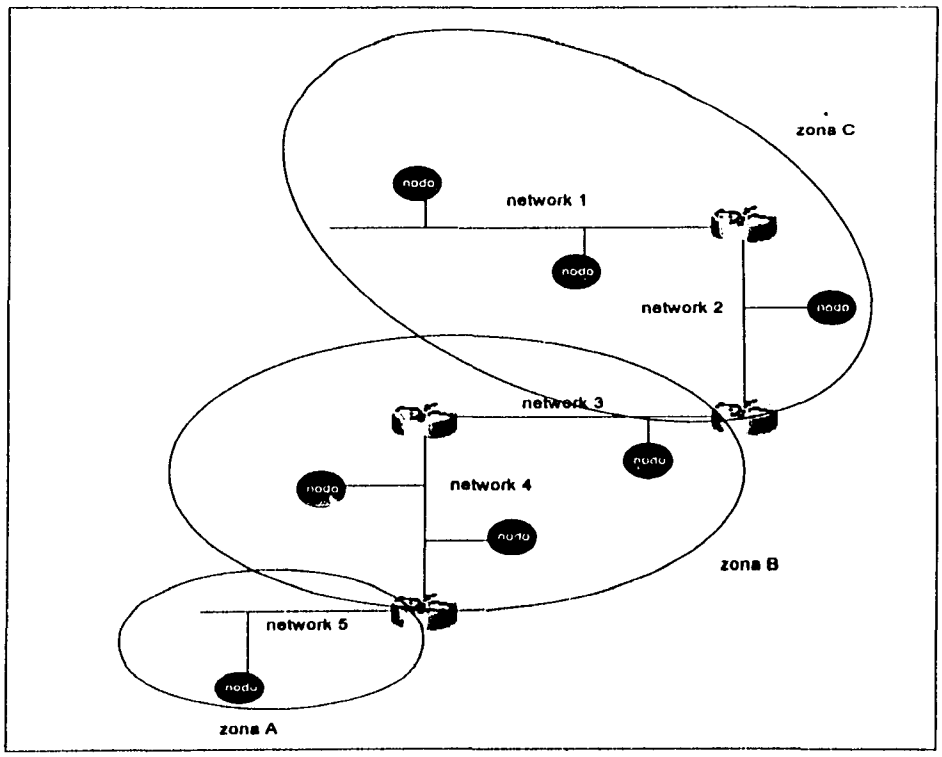


Figura 3.27 : Entidades de red APPLETALK

3.5.6 PROTOCOLO DE ENTREGA DE DATAGRAMAS (DDP)

El primer protocolo de la capa de red de AppleTalk es el protocolo de entrega de datagramas (DDP). Este protocolo provee servicio sin conexión entre "sockets" de red. Estos sockets pueden ser asignados estáticamente o dinámicamente.

Las direcciones AppleTalk, las cuales son administradas por el DDP, consisten de dos componentes : Un número de red de 16 bits y un número de nodo de 8 bits. Los dos componentes son usualmente escritos en notación decimal separados por un punto (por ejemplo, 10.1 significa red 10 y nodo 1). Cuando un socket de 8 bits esta identificando un proceso particular se añade un número de red y nodo de red, como un único proceso especificado en la red.

AppleTalk fase 2 distingue entre redes extendidas y no extendidas. En una red no extendida como LocalTalk, cada numero de nodo AppleTalk es único. Las redes no extendidas están definidas en AppleTalk fase 1. En una red extendida como EtherTalk o TokenTalk, cada combinación de red/nodo es único.

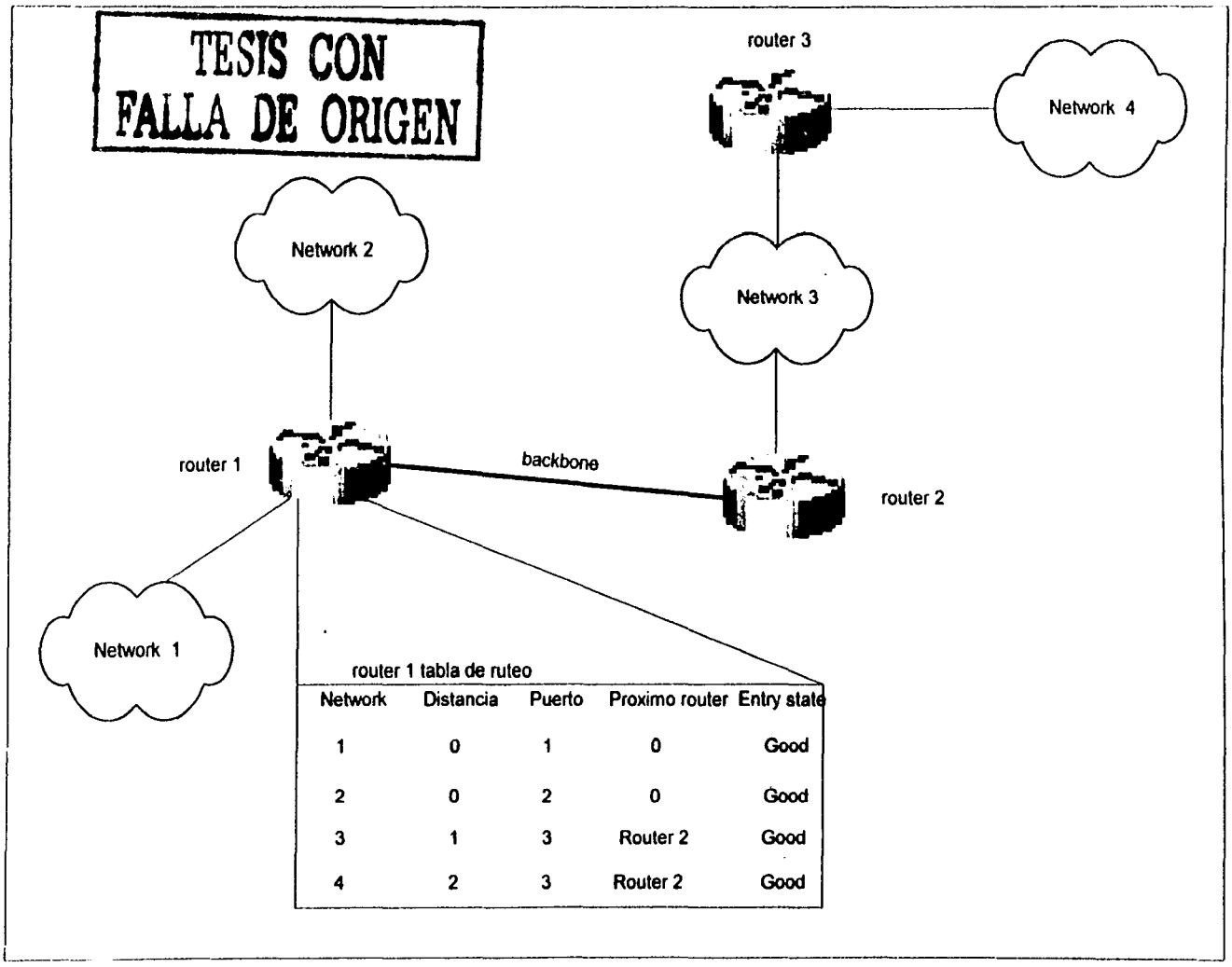
Las zonas son definidas por el administrador de red AppleTalk durante la configuración de ruteo. Cada nodo en la red pertenece a una zona simple especifica. Las redes extendidas pueden tener múltiples zonas asociadas a ellas. Los nodos en una red extendida pueden pertenecer a cualquier zona simple asociada con la red extendida.

3.5.7 CAPA DE TRANSPORTE

La capa de transporte en AppleTalk esta implementada por varios protocolos. Routing Table Maintenance Protocol (RTMP) o Protocolo de Mantenimiento de tablas de ruteo, AppleTalk Update-Based Routing Protocol (AURP) o Protocolo de Ruteo Basado en actualizaciones, AppleTalk Echo Protocol (AEP), AppleTalk Transaction Protocol (ATP) o Protocolo de Transacciones AppleTalk, y Name Binding Protocol (NBP) o Protocolo de Asociación de Nombres.

3.5.7.1 ROUTING TABLE MAINTENANCE PROTOCOL (RTMP)

Este protocolo establece y mantiene las tablas de ruteo. Las tablas de ruteo de RTMP contienen un valor para cada red que un datagrama puede alcanzar. Cada valor incluye un puerto de ruteo que lleva la dirección destino, el ID del nodo del próximo ruteador a recibir el paquete, la distancia en saltos a la red destino y el estado en que se encuentra (good, suspect or bad). Un intercambio periódico de tablas de ruteo permite a los ruteadores estar actualizados. La figura 3.28 muestra un ejemplo de una tabla RMTP y la correspondiente arquitectura de red.



router 1 tabla de ruteo

Network	Distancia	Puerto	Proximo router	Entry state
1	0	1	0	Good
2	0	2	0	Good
3	1	3	Router 2	Good
4	2	3	Router 2	Good

Figura 3.28:Ejemplo de tabla de ruteo APPLETALK

El protocolo Name Binding Protocol (NBP) asocia nombres AppleTalk (expresados como entidades visibles de red o NVE's) con direcciones. Una NVE es un servicio de direcciones AppleTalk tal como un socket. NVE's están asociados con una o más nombres de entidades y listas de atributos. Un nombre de entidad es una cadena de caracteres tal como printer@net1, mientras las listas de atributos especifican las características NVE.

Los nombres NVE son asociados con direcciones de red a través de un proceso que asocia o liga nombres. La liga de nombres puede ser hecha cuando el nodo de usuario es inicializado primero, o dinámicamente, inmediatamente antes del primer uso. NBP coordina el proceso de asociación de nombres, el cual incluye registro de un nombre, confirmación, borrado de un nombre y revisión de un nombre "lookup".

Las zonas permiten nombres en un grupo de nodos relacionados lógicamente. Para mirar nombres dentro de una zona, una petición NBP de revisión es enviada a un ruteador local, el cual envía una petición de "broadcast" a toda la red que tenga nodos pertenecientes a su zona. El protocolo de información de zona (ZIP) coordina esta tarea.

ZIP mantiene un número de red para el mapeo de los nombres de zona en las tablas de información de zona (ZIT's). Las ZIT's son almacenadas en ruteadores, en los cuales están los usuarios primarios de ZIP, pero los nodos finales usan ZIP durante el proceso de inicialización para escoger su zona y para conseguir información de interconexión hacia otras zonas.

ZIP usa tablas de ruteo RTMP para mantenerse actualizado cuando ocurran cambios de topología. Cuando ZIP encuentra una tabla de ruteo que no esta registrada en el ZIT la añade creando un nuevo ZIT.

3.5.7.2 APPLETALK UPDATE-BASED ROUTING PROTOCOL

El protocolo de ruteo basado en actualizaciones de AppleTalk (AURP) permite a un administrador de red conectar dos o mas redes AppleTalk a través de una red no AppleTalk (como p.ej. TCP/IP) para formar una red AppleTalk WAN. A esta conexión se le denomina tunel , el cual su función es como un simple enlace de datos virtual entre la interconexión de redes AppleTalk como se muestra en la figura 3.29.

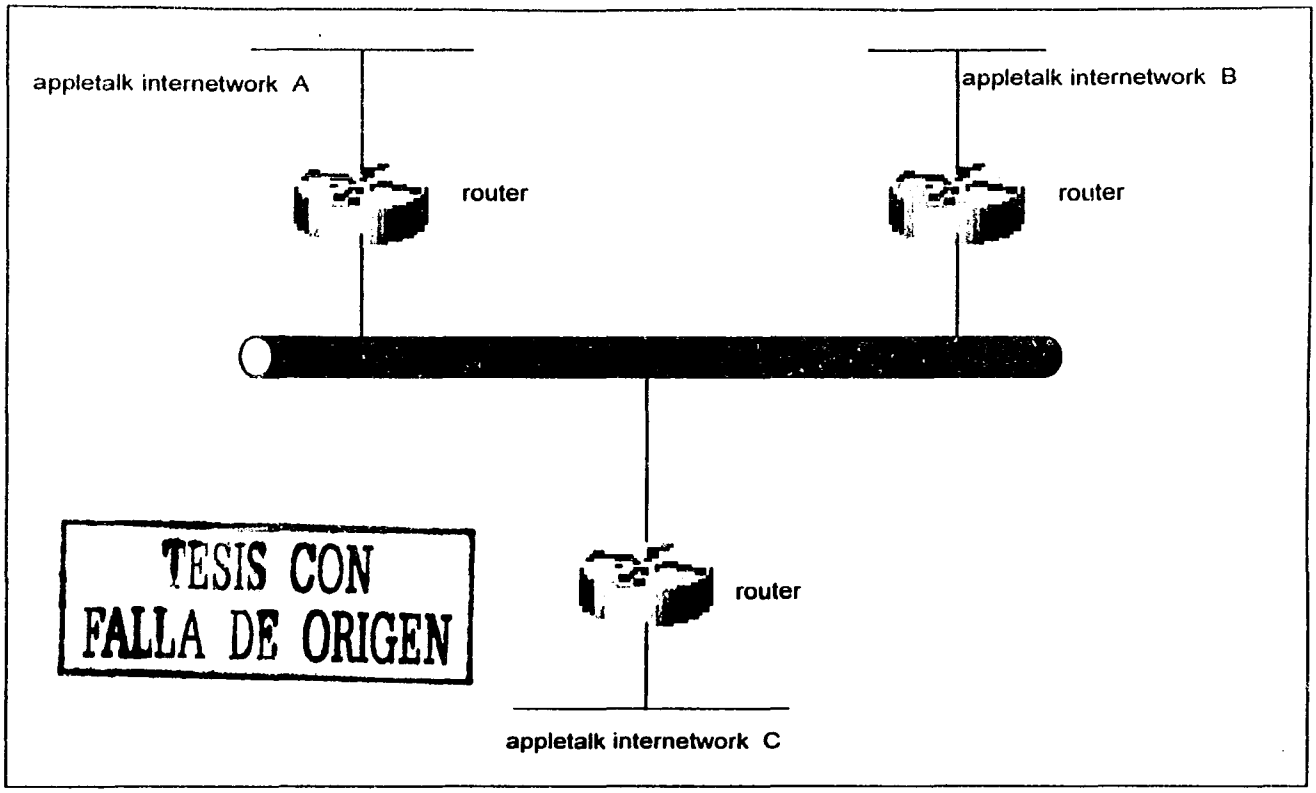


Figura 3.29: TUNEL APPLETALK

Un ruteador que interconecta redes AppleTalk hacia un tunel (esto es, un ruteador corriendo AURP) es llamado un ruteador exterior. Este manda paquetes de datos AppleTalk e información de ruteo a través de la red externa encapsulando los paquetes con la información de header requerida por el sistema externo. El ruteador externo receptor remueve el encabezado y manda los paquetes hacia la interface destino. Los paquetes son encapsulados por medio de el protocolo UDP (User Datagram Protocol) al iniciar la implementación de AURP.

Cuando solo dos ruteadores externos están conectados a un tunel, el enlace se llama tunel punto a punto. Cuando hay mas de dos ruteadores exteriores el tunel es llamado multipunto. Si todos los ruteadores exteriores conectados a un tunel multipunto pueden enviar paquetes hacia todos se dice que esta completamente conectado. Si uno o mas ruteadores exteriores no se pueden conectar hacia algún otro ruteador se dice que esta parcialmente

conectado. Cada ruteador exterior tiene ambas funciones: la de ruteador AppleTalk dentro

de su interred local y como un nodo final en la red externa que interconecta varias redes AppleTalk.

La función principal de AURP es mantener las tablas de ruteo para toda la red AppleTalk WAN mediante el intercambio de información entre ruteadores exteriores. En adición, AURP encapsula los paquetes de datos AppleTalk con los encabezados requeridos por la red externa.

El protocolo AURP usa el principio de partición de horizontes (split horizons, el cual nunca envía información de regreso hacia un ruteador que le manda información entrante) para limitar la propagación de información para actualizar las tablas de ruteo. Por tal razón, un ruteador exterior manda información de ruteo solo a las redes que abarcan su interconexión a la red local y a otras conectadas mediante un tunel.

Cuando un ruteador exterior llega a ver otro ruteador exterior en el tunel, los dos ruteadores intercambia sus listas de números de red y su información de zona asociada. Después un ruteador exterior manda información de ruteo solo si los siguientes eventos ocurren.

- Una red es añadida a la tabla de ruteo
- Un cambio en el trayecto hacia una red causa que el ruteador exterior para accesar a la red lo haga a través de su interred local en vez del tunel o viceversa.
- Una red es removida de la tabla de ruteo.
- La distancia a la red es cambiada.

Cuando un ruteador exterior recibe paquetes de datos AppleTalk o información de ruteo que necesita mandar sobre el tunel, El modulo AURP convierte esa información a paquetes AURP. Los paquetes AURP son encapsulados con la información del encabezado requerida por la red externa y enviada sobre el tunel hacia el ruteador exterior destino. Como se muestra en la figura 3.30.

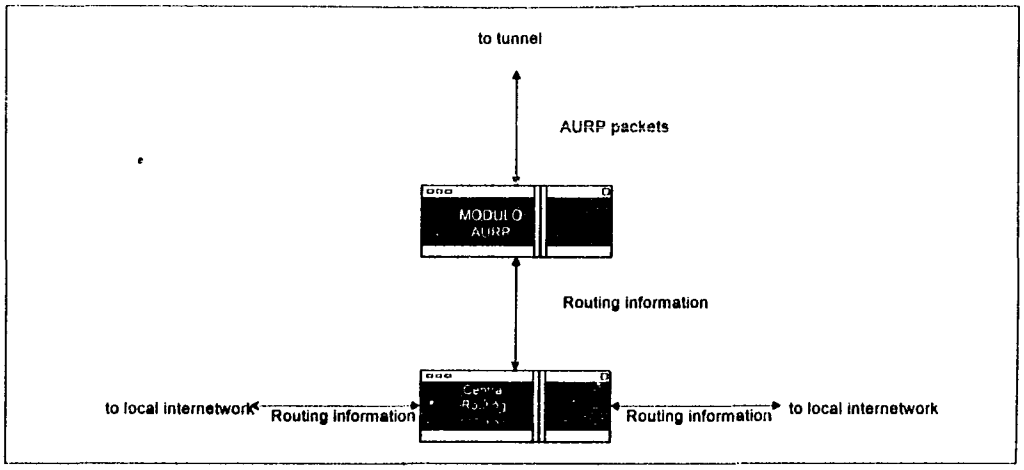


FIGURA 3.30: Modelo de arquitectura AURP

En el ruteador exterior destino, el modulo AURP remueve el encabezado requerido por el sistema externo de los paquetes AURP y manda paquetes de datos AppleTalk hacia su destino final. El ruteador exterior usa los paquetes AURP que contienen información de ruteo para actualizar su información de tablas de ruteo pero no propaga esa información a cualquier otro ruteador.

3.5.7.3 APPLETALK ECHO PROTOCOL (AEP)

AEP es un protocolo simple que genera paquetes que pueden ser usados para probar el alcance de varios nodos de red.

3.5.7.4 APPLETALK TRANSACTION PROTOCOL (ATP)

ATP esta disponible para aplicaciones basadas en transacciones tales como aquellas de los bancos o tiendas de ventas. Las transacciones ATP consisten de peticiones (de clientes) y respuestas (de servidores). Cada par de petición/respuesta tiene una particular transacción ID. Las transacciones ocurren entre dos sockets clientes. ATP usa dos tipos de transacciones: exactly once (XO) y at-least-once (ALO). Las transacciones XO son usadas en situaciones donde la ejecución de la transacción mas de una vez debiera ser inaceptable. Las transacciones de los bancos son ejemplos de este tipo de transacciones, si se ejecuta mas de una vez, resultarían datos inválidos.

ATP es capaz de manejar funciones de la capa de transporte, incluyendo reconocimiento de datos y retransmisión , secuencia de paquetes y fragmentación y reensamble. ATP limita la segmentación de un paquete en 8 y un paquete ATP no puede contener mas de 578 bytes de datos.

3.5.8 PROTOCOLOS DE CAPAS SUPERIORES

AppleTalk soporta varios protocolos de capas superiores:

AppleTalk Data Stream Protocol (ADSP) establece y mantiene ráfagas de datos de manera full duplex entre dos sockets en una interred AppleTalk. ADSP es un protocolo confiable el cual se garantiza que los bytes de datos son entregados en el mismo orden en el cual fueron enviados y que entre ellos no hay duplicados. Cada byte de datos contiene números ADSP para mantener la misma secuencia de los elementos individuales de las ráfagas de datos. ADSP también contiene control de flujo. El destinatario puede esencialmente disminuir la velocidad de transmisión reduciendo el tamaño de la ventana receptora. ADSP también proporciona control de mensajes fuera de banda. La atención de los paquetes son usados como vehículo para mover los mensajes fuera de banda entre dos entidades AppleTalk. Estos paquetes usan un numero de secuencia separado para diferenciar de los paquetes de datos normales ADSP.

- AppleTalk Session Protocol (ASP) establece y mantiene sesiones (conversaciones lógicas) entre un cliente AppleTalk y un servidor.
- AppleTalk's Printer Access Protocol (PAP) es un protocolo orientado a conexión que establece y mantiene conexiones entre clientes y servidores.
- AppleTalk Filing Protocol (AFP) ayuda a los clientes compartir recursos de red a través de la misma.

CAPITULO 4 SIMPLE NETWORK MANAGEMENT PROTOCOL

4.1 INTRODUCCION

Las redes y los sistemas de procesamiento distribuido han ido creciendo en importancia y han llegado a ser un factor crítico en los negocios. Dentro de una organización dada, los requerimientos hacen a las redes mas complejas soportando más aplicaciones y mas usuarios. Al crecer las redes dos factores se hacen evidentes:

- la red y sus recursos y aplicaciones distribuidas llegan a ser indispensables para una organización.
- Muchas cosas pueden ir mal, deshabilitando una parte o toda la red, o degradando el desempeño de la red.

Una gran red no puede ser manejada sola por el esfuerzo humano. La complejidad de tales sistemas dictamina el uso de herramientas de administración de red automatizadas. La urgencia de la necesidad de tales herramientas y la dificultad para suplirlas se incrementa si la red se compone por equipos de diferentes fabricantes.

En respuesta a estas necesidades se desarrollaron algunos estandares entre los que se encuentran SNMP y CMIP. SNMP forma parte de la familia de protocolos TCP/IP. CMIP fue desarrollado por ISO.

4.2 ¿QUE ES ADMINISTRACIÓN DE RED?

Administración de red puede tener diversos significados. En algunos casos involucra un consultor de red solitario monitoreando la actividad de la red con un analizador de protocolos. En otros casos la administración de red involucra una base de datos distribuida, dispositivos de red con auto-poleo y estaciones de trabajo que generan gráficas en tiempo real y vistas de la topología de la red y los cambios de tráfico . En general administración de red es un servicio que emplea una variedad de herramientas, aplicaciones y dispositivos que ayudan al administrador de la red a monitorear y dar mantenimiento a la red. (falta citar de quien es esta definicion)

4.2.1 METAS DE LA ADMINISTRACIÓN DE RED:

Entre las metas de la administración de una red tenemos:

Alta disponibilidad de la red
Distribuir los costos
Reducir los cuellos de botella
Incrementar la flexibilidad de operación e integración
Aumentar la eficiencia
Facilidad de uso
Mantener la seguridad

4.2.2 MODELOS DE ADMINISTRACIÓN:

Tenemos dos modelos de administración: administración distribuida de red y administración de red jerárquica o centralizada.

En el primer caso tenemos una forma de administración en la cual no tenemos un administrador central el administrador puede ser un nodo más de la red, un ejemplo de este tipo es un ambiente LAN.
En el segundo caso la administración es llevada a cabo desde un punto central como seria el caso de un mainframe.

4.2.3 ARQUITECTURA DE ADMINISTRACIÓN DE RED:

La mayoría de las arquitecturas de administración de redes usan la misma estructura básica y una serie de relaciones entre elementos. las estaciones finales (dispositivos administrados), tal como una computadoras y otros dispositivos de red, software que les manda alarmas cuando ellos reconocen problemas. Una vez recibiendo esta alarmas, las entidades de administración son programadas para realizar alguna función o grupo de acciones incluyendo dar aviso al operador, crear una bitácora de eventos, dar de baja el sistema e intentar reparar automáticamente el sistema, etc.

Las entidades de administración también pueden polear a las estaciones finales para verificar ciertas variables. El poleo puede ser automático o ser iniciado por el usuario, pero los agentes en los dispositivos administrados responden a todos los poleos. Los agentes son módulos de

software que primero compilan información acerca de los dispositivos administrados en el cual reside, entonces almacena la información en una base de datos de administración y finalmente las provee (activamente o reactivamente) a las entidades de administración dentro de un Sistema de Administración de Red (NMS) por medio de un protocolo de administración. Los protocolos de administración más conocidos son CMIP (Common Management Information Protocol) y SNMP (Simple Network Management Protocol).

Proxie de administración son entidades que proveen información de administración en favor de otras entidades. En la siguiente figura 4.1 se muestra una arquitectura típica de administración de red.

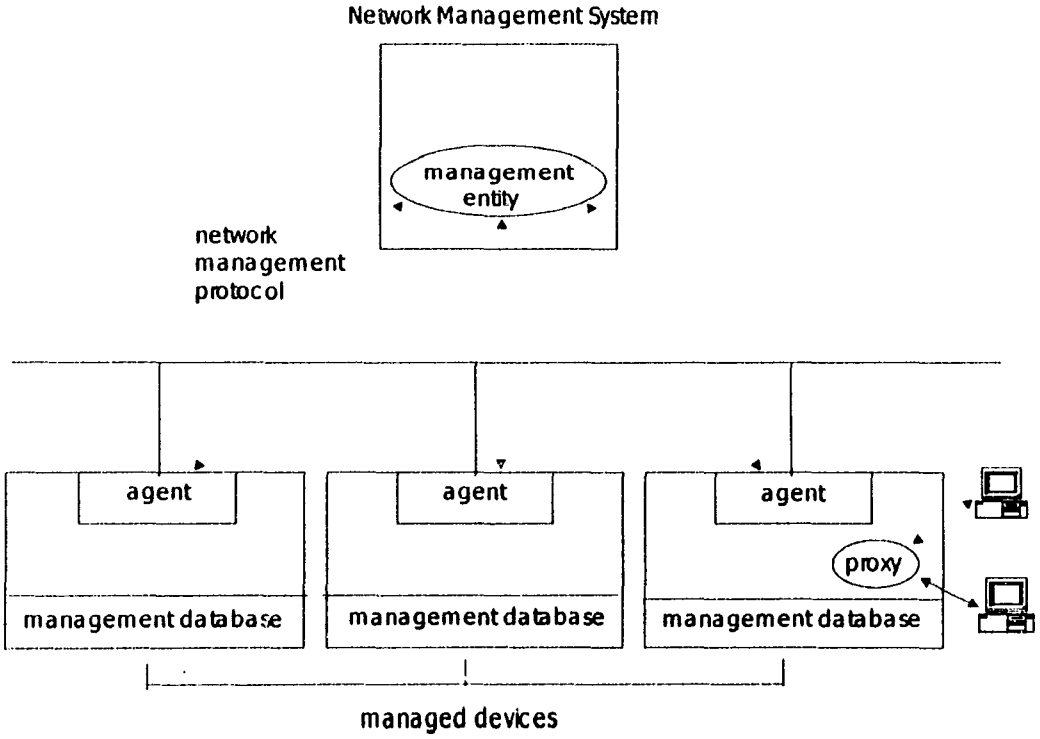


Figura 4.1 ARQUITECTURA DE ADMINISTRACIÓN DE RED

4.2.4 ARQUITECTURA DE ADMINISTRACION DE RED DEL MODELO TCP/IP

Esta arquitectura incluye los siguientes elementos:

- estación de administración
- agente de administración
- base de información de administración MIB
- protocolo de administración de red

Una estación de administración es típicamente un solo dispositivo el cual sirve como interfase para el administrador de red dentro de un sistema de administración de red. La estación debe estar equipada con aplicaciones de adminitración, una interfase para el administador de red, capacidad para transmitir comandos a través del protocolo de administración de red, y una base de datos donde es colocada la información extraida de las MIBs.

Los últimos dos son la base de la estandarización de SNMP.

Los agentes de administración son dispositivos de red, tales como host, bridges, routers y hubs, los cuales son capaces de comunicarse con y estar comunicados con la estación de administración . un agente responde a las peticiones de las estaciones, ejecuta una acción (en si mismo) mandada por la estación de adminitración, y puede mandar mensajes a la estación sin una petición.

Una base de administración de información MIB, es una colección de objetos, los cuales representan los recursos o aspectos del dispositivo en la red que pueden ser administrados. Cada objeto es, esencialmente , una variable de datos que representan un aspecto de el agente adminitrado.

Estos sistemas están estandarizados a través de sistemas de una clase en partícular (por ejemplo un grupo de objetos para administrar varios bridges).

La estación de adminitración y los agentes estan enlazados mediante el protocolo de administración de red. Tienen las siguientes capacidades: get (obtener), set (poner) y trap (mandar). Get permite a la estación de administración recobrar información de un objeto de un agente. Set habilita a la estación de administración poner el valor de un objeto de un agente .

trap permite a un agente notificar eventos inesperados a la estación de administración.

Los estandares no especifican el número de estaciones de administración pero para tener redundancia se deben de tener al menos dos sistemas en paralelo.

4.3 AREAS FUNCIONALES DE ADMINISTRACIÓN DE RED DEFINIDAS POR LA ORGANIZACIÓN DE ESTANDARES INTERNACIONALES (ISO).

Aunque esta clasificación fue desarrollada para el ambiente administración de OSI, ha ganado gran aceptación por vendedores y standarizadores de sistemas de administración de redes.

4.3.1 ADMINISTRACION DE FALLAS (FAULT MANGEMENT)

Para mantener la correcta operación de una red compleja, un administrador de red debe de tomar a los sistemas como un todo, cada componente esencial individualmente, con un cierto orden de trabajo. Cuando una falla ocurre, es importante tan rápido como sea posible para el administrador de red:

- Determinar exactamente donde esta la falla
- Aislar la falla del resto de la red
- Reconfigurar o modificar la red de tal manera que el impacto de la falla sea mínimo.
- Reparar o reemplazar los componentes que ocasionaron la falla y regresar la red a su estado inicial.

Dentro de la definición de administración de fallas es fundamental el concepto de falla. Es necesario distinguir una falla de un error. Una falla es una condición anormal que requiere atención o acción del administrador para ser reparada, mientras que un error es solo un evento simple. Una falla puede ser indicada por la no operación correcta o por errores excesivos.

4.3.2 ADMINSTRACION DE CUENTAS (ACCOUNTING MANAGEMENT)

En muchas redes corporativas, divisiones individuales o centros de costos, son cambiados por el uso de servicios de red. Estos son procedimientos internos de contabilidad en vez de transferencias de efectivo, pero sin embargo estos son importantes para la participación de los usuarios finales. Además, aun si no es empleado el cambio interno, el administrador de red necesita ser hábil para cuantificar el uso de los recursos por los usuarios finales u clases de usuarios finales por un nÚmero de razones incluyendo las siguientes:

- Un usuario final o un grupo de usuarios finales pueden abusar de sus privilegios de acceso y saturar la red a expensas de los otros usuarios.
- Los usuarios finales pueden estar haciendo un uso ineficiente de la red y el administrador de red puede asistir haciendo cambios para mejorar la eficiencia de la red.
- El administrador de red esta en una mejor posición para planificar el crecimiento de la red si es requerido.

4.3.3 ADMINISTRACION DE NOMBRES Y CONFIGURACION (CONFIGURATION AND NAME MANAGEMENT)

Las redes de datos de comunicación estan compuestas de componentes individuales y subsistemas lógicos (p.e. drivers en un sistema operativo) que pueden ser configurados para correr diversas aplicaciones. El mismo dispositivo por ejemplo, puede ser configurado para actuar como router o un nodo final o ambos. Una vez decidido como un dispositivo sera usado, el administrador encargado de la configuración puede escoger el software apropiado y los atributos correctos y valores para dicho dispositivo.

La administración de la configuración es referida con la inicialización de una red y dar de baja parte o toda la red. También es referida con el mantenimiento, adición y actualización de las relaciones entre componentes y el estado de los mismos durante la operación de la red.

4.3.4 ADMINISTRACION DE DESEMPEÑO (PERFORMANCE MANAGEMENT)

Las redes estan compuestas de diversos componentes, los cuales deben ser intercomunicados para compartir datos y recursos. En algunos casos, es crítica la efectividad de una aplicación que la comunicación sobre la red este dentro de ciertos límites de desempeño.

La administración del desempeño de una red de computadoras implica dos categorias funcionales : monitoreo y control. Monitoreo es la función que lleva el seguimiento de las actividades de la red. La función de control habilita al administrador del desempeño, hacer ajustes para aumentar el desempeño de la red. Algunos de los tópicos que conciernen al administrador de la red son los siguientes:

- cual es el nivel de utilización
- es excesivo el tráfico
- el throughput ha sido reducido a niveles inaceptables
- hay cuellos de botella
- el tiempo de respuesta se esta incrementando.

Para hacer esto posible, el administrador debe tomar una serie de valores iniciales en los recursos a ser monitoreados, en orden para formar niveles. Esto incluye la asociación de métricas y valores relevantes para la red asi como indicadores del desempeño de la red. Con la administración del desempeño, asi podemos monitorear muchos recursos para proveer información en un nivel determinado de operación de la red. Recolectando esta información en un cierto período de tiempo podemos sacar estadísticas y poder reconocer situaciones que indican una degradación de la red o un mal funcionamiento.

4.3.5 ADMINISTRACIÓN DE SEGURIDAD

La administración de seguridad es referida con la protección de la información que es manejada y proveer facilidades de acceso. Estas incluyen la generación, distribución y almacenamiento de llaves de encripción. Passwords y otra información de control de acceso o autorización debe ser mantenida y distribuida. La administración de seguridad tambien tiene que ver con el monitoreo y el control del acceso de la red o parte de la red de la información para administración obtenida de los nodos. Los logs es una

Otra ventaja es que no toma los desperfectos de SNMP en cuanto a direcciones, en cambio tiene contruido dentro dispositivos de seguridad de administración que soportan autorización, control de acceso y logs de seguridad. Debido a esto no necesita actualizaciones. La última ventaja es que fue desarollado por gobiernos y grandes corporaciones lo cual permite hacerlo disponible grandemente.

4.4.2 DESVENTAJAS DE CMIP

Aunque por sus características es un protocolo poderoso, tiene una gran desventaja . utiliza más recursos que SNMP en un factor de 10. Lo cual hace que no sea empleado. Y también es díficil su programación.

La estación de administración envía una petición concerniente de un dispositivo a su agente proxy. El agente proxy convierte cada petición dentro del protocolo de administración que el dispositivo este usando. Cuando el agente recibe una respuesta a la petición esperada esa respuesta es enviada a la estación de administración de manera similar, si una notificación de algún evento es enviada de un dispositivo al proxy, el proxy envía a la estación de administración la respuesta en forma de mensaje TRAP.

4.5 HISTORIA DE SNMP

A finales de los 70´s la herramienta mas usada para la administración fue el Internet Control Message Protocol (ICMP) comúnmente empleado con el programa PING (Paquet Internet Groper) para detectar hosts mediante el envio de mensajes de eco y su respuesta. Al aumentar el crecimiento de internet con un numero de hosts en una red en cientos de miles, y el numero de redes individuales en miles, no es posible manejar por unas cuantas personas los problemas de la red. Fue requerido estandarizar un protocolo más funcional que el PING y fácil de usar para los administradores de redes.

La primer herramienta utilizada para la administración de redes fué el Simple Gateway Monitoring Protocol (SGMP) desarrollado en noviembre de 1987. SGMP provee los medios para el monitoreo de gateways. la necesidad de una herramienta de administración de red de carácter general creció surgieron 3 aplicaciones:

figura muestra el ambiente operacional que será manejado. La parte sin sombrear provee soporte a las funciones de administrador de red.

4.5.3 OPERACIONES SOPORTADAS POR SNMP:

Son tres las operaciones generales que se ejecutan en objetos escalares por SNMP:

Get : una estación de administración obtiene un valor escalar de un objeto de una estación manejada, p.e. un router.

Set : una estación de administración actualiza un valor escalar de un objeto en una estación manejada, p.e. un router.

Trap: una estación manejada envía un valor escalar de un objeto a una estación de administración sin ser solicitada.

No es posible cambiar la estructura de una MIB adicionando o borrando instancias de objeto (por ejemplo borrando un renglón de una tabla.

Tampoco es posible emitir comandos para una acción a ser ejecutada. El acceso solo es provisto por la hoja de objetos en el árbol de identificador de objeto. Esto es que no es posible accesar a una tabla completa o renglón con una sola acción. Estas restricciones simplifican la implementación de SNMP.

4.5.4 LIMITACIONES DE SNMP

1. En una red grande el poleo podría afectar el desempeño de la red
2. SNMP no puede accesar a grandes volúmenes de datos como una tabla completa de ruteo
3. Los Traps SNMP no tienen acuse de recibo, el agente no puede saber si el mensaje llegó a la estación de administración.
4. tiene una trivial autentificación
5. No soporta comandos imperativos directamente, los hace a través de agentes cambiando los valores del objeto.
6. el modelo de la MIB es limitado.
7. No soporta la comunicación entre sistemas de administración.

4.5.5 PROXIES

Para utilizar dispositivos que no utilizan SNMP, el concepto de proxie es empleado. En este esquema un agente SNMP actúa como proxie (GESTOR) de uno o más dispositivos, esto es el agente actúa sobre los dispositivos gestionados. LA FIG 4.3 muestra lo anterior

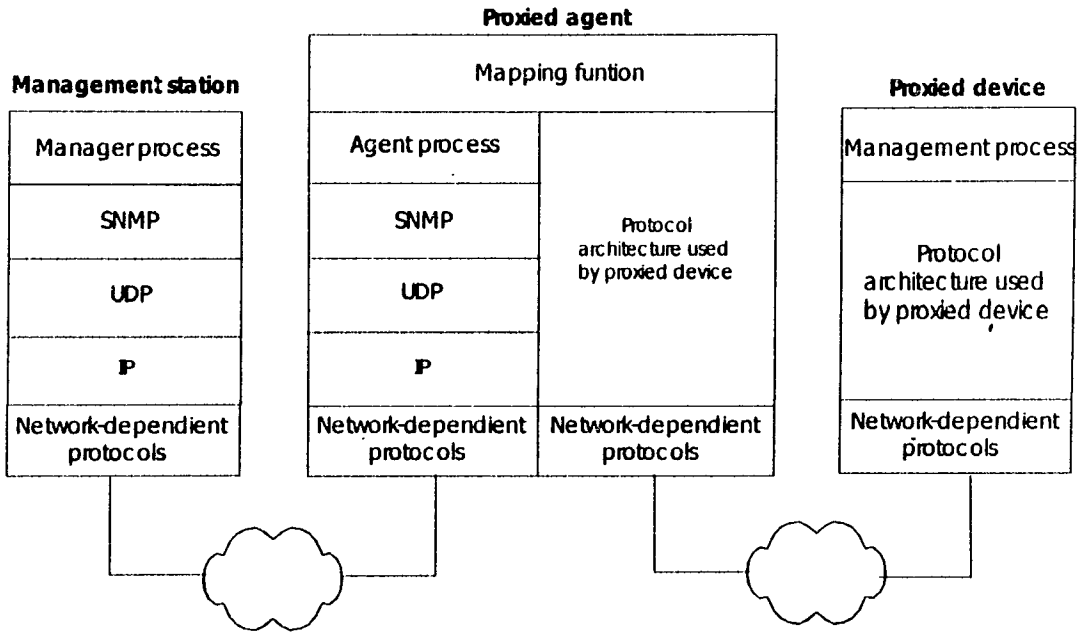


Figura 4.3 configuración proxy

La estación de administración envía una petición concerniente de un dispositivo a su agente proxy. El agente proxy convierte cada petición dentro del protocolo de administración que el dispositivo este usando. Cuando el agente recibe una respuesta a la petición esperada esa respuesta es enviada a la estación de administración de manera similar, si una notificación de algún evento es enviada de un dispositivo al proxy, el proxy envía a la estación de administración la respuesta en forma de mensaje TRAP.

4.5.5 PROXIES

Para utilizar dispositivos que no utilizan SNMP, el concepto de proxie es empleado. En este esquema un agente SNMP actúa como proxie (GESTOR) de uno o más dispositivos, esto es el agente actúa sobre los dispositivos gestionados. LA FIG 4.3 muestra lo anterior

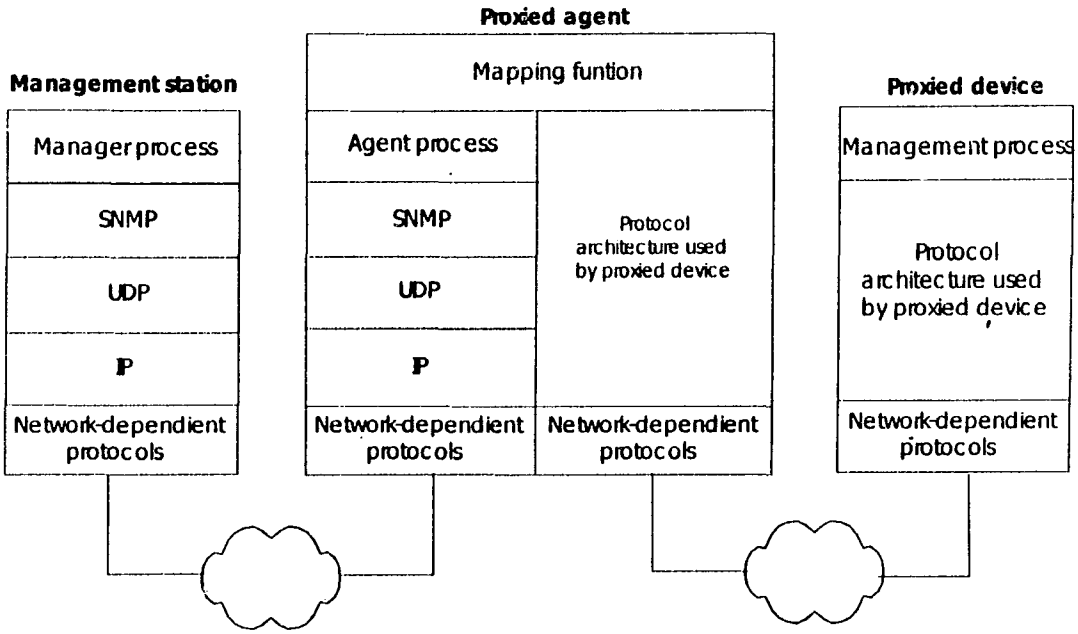


Figura 4.3 configuración proxy

La estación de administración envía una petición concerniente de un dispositivo a su agente proxy. El agente proxy convierte cada petición dentro del protocolo de administración que el dispositivo este usando. Cuando el agente recibe una respuesta a la petición esperada esa respuesta es enviada a la estación de administración de manera similar, si una notificación de algún evento es enviada de un dispositivo al proxy, el proxy envía a la estación de administración la respuesta en forma de mensaje TRAP.

4.6 ESTRUCTURA DE ADMINISTRACION DE LA INFORMACION

La estructura de administración de información (SMI), esta especificada en el RFC 1155 y define la estructura general dentro de la cual puede ser definida y construida una MIB. SMI identifica el tipo de datos que pueden ser usados dentro de la MIB y especifica como los recursos son nombrados y representados. Para proveer una estandarización el SMI debe de cumplir lo siguiente:

- Proveer una técnica estandarizada para definir la estructura de una MIB particular
- Proveer una técnica estandarizada para definir objetos individuales, incluyendo la sintaxis y el valor de cada objeto.
- Proveer una técnica estandarizada para codificar los valores de los objetos.

4.6.1 NOTACION DE SINTAXIS ABSTRACTA UNO (ASN.1)

La notación de sintaxis abstracta uno (ASN.1) es un leguaje formal desarrollado y estandarizado por CCITT (X.208) e ISO (ISO 8824). Puede ser usado para definir sintaxis abstractas de datos de aplicación. ASN.1 es usado para definir la estructura de aplicación y presentación de las unidades de datos de protocolos (PDU's). Finalmente es usada para definir las bases de información de administración tanto para SNMP como de OSI.

4.6.2 SINTAXIS ABSTRACTA

Existen dos grandes componentes:

Componente de transferencia de datos: concerniente a la transferencia de datos entre sistemas. Un ejemplo de este puede ser TCP o UDP.

Componente de aplicación: es el usuario del componente de transferencia de datos y concierne con la aplicación final del usuario. Un ejemplo de este puede ser FTP, Telnet, etc.

Sintaxis abstracta: describe la estructura genérica de datos independiente para cualquier técnica de codificación usada para representar datos. La sintaxis permite tipos de datos a ser definidos y valores de esos tipos para ser especificados.

Tipo de datos: un grupo de valores nombrados. Un tipo puede ser simple, el cual es definido especificando sus valores, o estructurado el cual es definido en términos de otros tipos.

Codificación: la completa secuencia de octetos usada para representar un valor de datos.

Reglas de codificación : Una especificación del mapeo de una sintaxis a otra. Específicamente se determinan algorítmicamente, para cualquier grupo de valores definidos en una sintaxis abstracta, la representación de esos valores es en una transferencia de sintaxis.

Transferencia de sintaxis: la forma en el cual los datos son representados en términos de patrones de bits entre entidades de presentación.

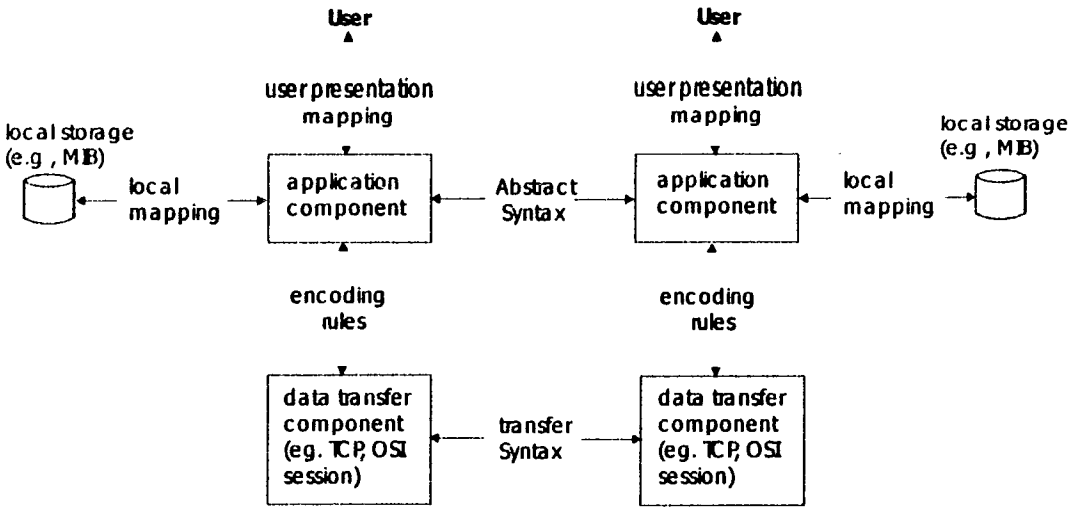


Figura 4.4 el uso de la sintaxis abstracta y transferencia

En La figura 4.4 tenemos un componente de aplicación, la información es representada en sintaxis abstracta que tiene que ver con tipos de datos y valores de datos. La sintaxis abstracta formalmente especifica datos independientemente de cualquier representación especifica. Así la sintaxis abstracta tiene muchas similaridades de definición de tipos de datos con los lenguajes de programación como Pascal, C, etc. y gramática como

Backus-Naur Form (BNF). Los protocolos de aplicación definen sus PDU's en términos de una sintaxis abstracta.

4.7 ADMINISTRACION DE INFORMACION EN SNMP

Cualquier sistema de administración de red, esta basado en bases de datos que contienen información de los elementos a ser manejados. En ambos ambientes TCP/IP y OSI, la base de datos es referida como una base de información de administración MIB. Cada recurso ser manejado es representado como un objeto siendo la MIB una colección de objetos. La MIB es una colección estructurada de objetos en forma de árbol. Cada sistema (workstation, bridge, router, etc.) mantiene una MIB que refleja el estado de los recursos manejados a dicho sistema. Un administrador de red puede monitorear los recursos de un sistema leyendo los valores de los objetos de la MIB y puede modificar esos valores.

Dentro de las MIB's tenemos:

1. El objeto u objetos usados para representar un particular recurso debe de ser el mismo en cada sistema.
2. Un esquema común para representación debe ser usado para soportar interoperabilidad.

4.7.1 ESTRUCTURA DE LA MIB

Todos los objetos en el ambiente SNMP están ordenados en orden jerárquico o de árbol. Los objetos hoja son los actuales objetos administrados, cada alguno representa algún recurso, actividad o información a ser manejada. La estructura de árbol en si define un grupo de objetos ordenados lógicamente. Figura 4.5

Una MIB contiene una lista de objetos que están referidos por un tipo de identificador de objeto (OBJECT IDENTIFIER), el cual sirve como el nombre del objeto. Como es jerárquico la convención de nombres también sirve para identificar la estructura de tipos de objeto.

Cada objeto dentro de una MIB SNMP esta definida en un formato: la definición especifica el tipo de datos de objeto, son permitidas formas y rangos de valores, y su relación hacia otros objetos dentro de la MIB. La notación ASN.1 es usada para definir cada objeto individual y también para definir la estructura completa de la MIB. Los valores de los objetos son enteros.

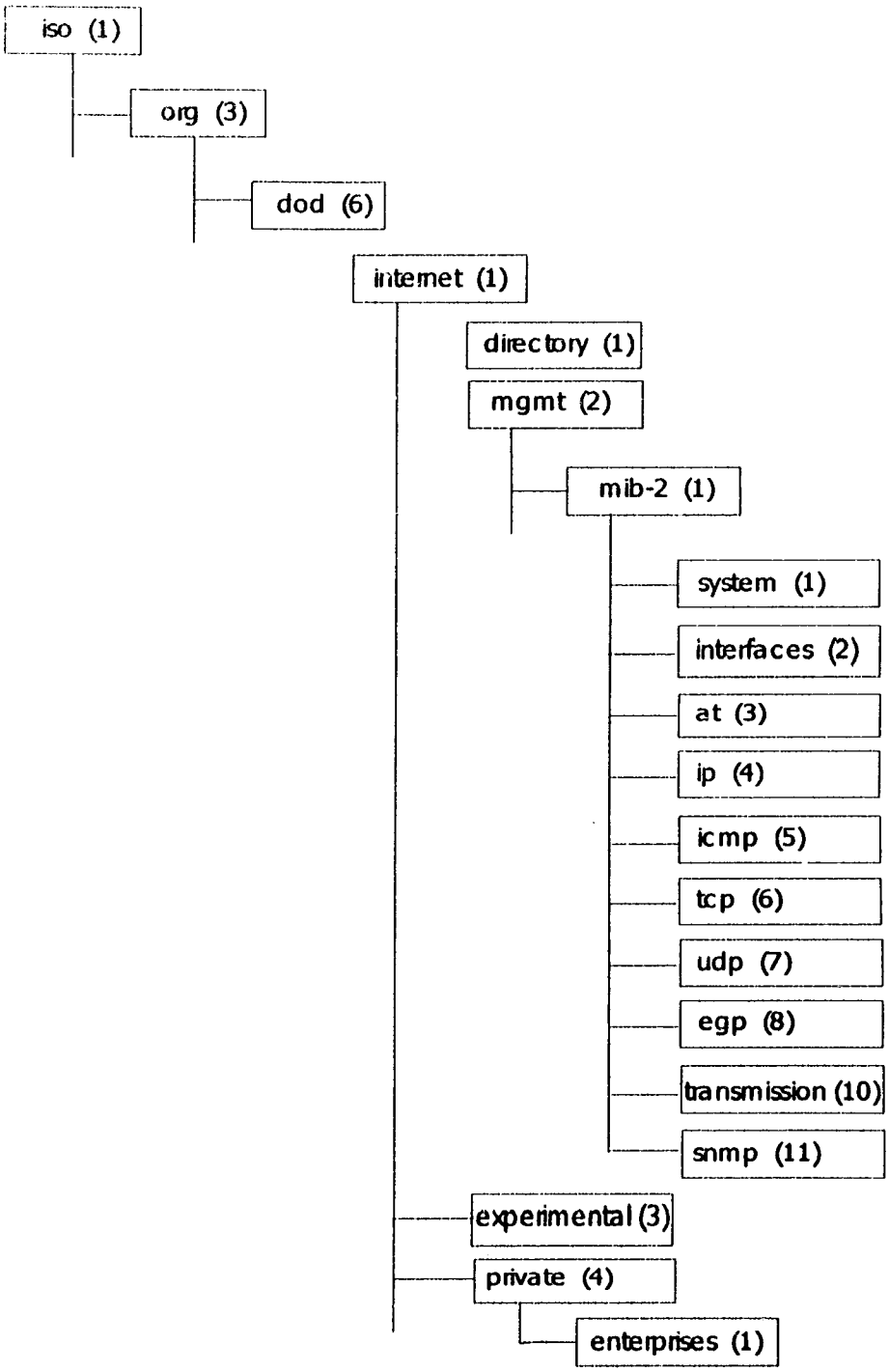


Figura 4.5 configuración de SNMP

Comenzando con la raíz del árbol identificador del objeto, cada objeto identificador esta compuesto de valores que identifican una rama en el árbol. Comenzando desde la raíz existen 3 nodos en el primer nivel: iso, ccitt y joint-iso-ccitt. Bajo el nodo de iso, un subárbol es para el uso de otras organizaciones una de las cuales es DoD. El RFC 1155 asume que un subárbol debajo de dod será puesto por el IAB como sigue:

Internet OBJECT IDENTIFIER ::= { iso (1) org (3) dod(6) 1 }

Así tenemos dos formas para acceder al valor del objeto en la MIB. Vía corta 1.3.6.1.2.1.2 ; Vía larga: iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(2).

4.7.2 SINTAXIS DE OBJETOS

Hay dos diferentes tipos de objetos de datos: universal y por aplicación. Los cuales son definidos con la notación ASN.1.

Tipos universales:

Los tipos de datos universales de ASN.1 consisten de tipos de datos independientes de la aplicación estos son de uso general, a continuación se muestran los tipos de datos permitidos para usarse en objetos de la MIB:

- *Integer* (UNIVERSAL 2)
- *Octectstring* (UNIVERSAL 4)
- *Null* (UNIVERSAL 5)
- *Object identifier* (UNIVERSAL 6)
- *Sequence, sequece-of* (UNIVERSAL 16)

El objeto identificador es único de cada objeto y es una secuencia de enteros que se conocen como subidentificadores, la secuencia se lee de izquierda a derecha y define la localización del objeto en la estructura de la MIB. Por ejemplo el objeto tcpConnTable esta definido como sigue:

Iso	org	dod	internet	mgmt	mib-2	tcp	tcpConnTable
1	3	6	1	2	1	6	13

o escrito 1.3.6.1.2.1.6.13

tipos de aplicación:

Consisten de tipos de datos que son relevantes a una aplicación particular. Cada aplicación incluyendo SNMP, es responsable para definir sus propios tipos de datos de aplicación. El RFC 1155 lista un número de tipos de aplicación. Los siguientes tipos están definidos:

Networkaddress: este tipo esta definido usando la construcción CHOICE, para permitir la selección de un formato de dirección de un numero de familias de protocolos, La única dirección definida es IpAddress.

Ipaddress: está es la dirección de 32 bits definida en IP

Counter: entero no negativo que puede ser incrementado pero no decrementado. Un valor máximo de 2 a la 32 – 1 esta especificado.

Gauge: entero no negativo que puede incrementar o decrementar.

Timeticks: entero no negativo que cuenta el tiempo en centésimas de segundo, este valor esta definido en las MIBs.

Opaque: este tipo soporta la capacidad para pasar datos arbitrariamente. Los datos son codificados como OCTET STRING para transmisión.

Otro importante valor es el threshold o umbral. Que se utiliza para designar un valor limite para disparar algún evento si es excedido dicho valor.

4.7.3 DEFINICIÓN DE OBJETOS:

Una base de información de administración consiste de un grupo de objetos. Cada objeto tiene un tipo y un valor. El tipo de objeto define una

clase particular de un objeto manejado. Una instancia de objeto es una instancia particular de un tipo de objeto que ha sido puesta a un valor especifico.

Para definir los objetos a sí mismos, la forma ASN.1 es usada. El bloque básico para la construcción de una especificación es el módulo. Un módulo tiene la siguiente forma básica.

```
<modulereference> DEFINITIONS ::=
        BEGIN

  EXPORTS
                IMPORTS
                AssignmentList
         End
```

El modulereference es un nombre de módulo seguido opcionalmente por un objeto identificador para identificar el módulo. La construcción EXPORTS indica cuales definiciones dentro del módulo pueden ser importadas por otros módulos. La construcción IMPORTS indica cual tipo y valor de las definiciones de otros módulos están para ser importadas dentro de su modulo. El assignment list consiste de tipos de asignaciones, valores asignados y macro definiciones.

En SNMP utilizamos macros para definir un grupo de tipos relativos usados para definir objetos manejados.

- Macro definición: define las instancias macro legales, especifica la sintaxis de un grupo relativo de objetos.
- Macro definición: una instancia generada de una definición macro especifica incorporando argumentos para los parámetros en la definición macro, especifica un tipo en particular.
- Valor de instancia macro: representa una entidad especifica con un valor específico.

La macro usada para las MIBs fue inicialmente definida en el RFC 1155 (para MIB I) y expandida en el RFC 1212 (para MIB II).

En la fig 4.5 se encuentra la definición macro de OBJECT TYPE del RFC 1212:

```
IMPORTS    ObjectName, ObjectSyntax FROM RFC-1155-SMI

OBJECT-TYPE MACRO ::=
BEGIN
     TYPE NOTATION ::=    "SYNTAX"    type (TYPE ObjectSyntax)
                          "ACCESS"  Access
                          "STATUS"    Status
                          DescrPart
                          ReferPart
                          IndexPart
                          DefValPart
     VALUE NOTATION ::= value (VALUE ObjectName)

     Access ::= "read-only" | "read-write" | "write-only" | "not-accessible"

     Status ::= "mandatory" | "optional" | "obsolete" | "deprecated"

     DescrPart ::= "DESCRIPTION" value (description DisplayString) | empty

     ReferPart ::= "REFERENCE" value (reference DisplayString) | empty

     indexPart ::= "INDEX" "{" IndexTypes "}"

     IndexTypes ::= IndexType | IndexTypes "," IndexType

     IndexType ::= value (indexobject ObjectName)     --if indextype, use the SYNTAX
                                                      --value of the correspondient
                                                      --OBJECT-TYPE invocation
                     | type *indextype)               --otherwise use named SMI type:
                                                      --must conform to IndexSyntax below

     DefValPart::= "DEFVAL" "{" value (defvalue ObjectSyntax) "}" | empty

     DisplayString ::= OCTET STRING SIZE (0..255)

END

IndexSyntax ::= CHOICE { number INTEGER (0..MAX),
                         string OCTEC STRING,
                         object OBJECT IDENTIFIER,
                         address NetworkAddress,
                         ipAddress IpAddress }
```

Figura 4.6 macro para objetos manejados (RFC. 1212)

- *Sintaxis*: la sintaxis abstracta para el tipo de objeto. Esta resuelve a una instancia del tipo *ObjectSyntax* definido en el RFC 1155 ver figura 4.6. Esencialmente la sintaxis debe estar construida usando los tipos de aplicación y universal permitidos en la SMI.
- *Acceso:* define la forma en la cual una instancia del objeto puede ser accesado, vía SNMP u otro protocolo. La cláusula de acceso especifica el mínimo nivel de soporte requerido por el tipo de objeto. Las opciones que tenemos son: *read only, read-write, write-only y not-accessible.*
- *Status*: indica la implementación del soporte requerido por el objeto. El soporte puede ser mandatorio u opcional. Alternativamente un objeto puede ser especificado como depreciado.
- *DescrPart*: descripción textual de la semántica del tipo de objeto, opcional.

```
RFC1155-SMI DEFINITIONS ::= BEGIN

EXPORTS -- EVERYTHING
        internet, directory, mgmt, experimental, private, enterprises, OBJECT-TYPE,
        ObjectName, ObjectSyntax, SimpleSyntax, ApplicationSyntax, NetworkAddress,
        IpAddress, Counter, Gauge, TimeTicks, Opaque;

-- the path to the root

internet        OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
directory       OBJECT IDENTIFIER ::= { internet 1 }
mgmt            OBJECT IDENTIFIER ::= { internet 2 }
experimental    OBJECT IDENTIFIER ::= { internet 3 }
private         OBJECT IDENTIFIER ::= { internet 4 }
enterprises     OBJECT IDENTIFIER ::= { private 1 }
-- definitio of object types

OBJECT-TYPE MACRO ::=
BEGIN
    TYPE NOTATION ::= "Syntax"   type (TYPE ObjectSyntax)
                      "ACCESS"   Access
                      "STATUS"   Status
    VALUE NOTATION ::= value (VALUE ObjectName)
    Access ::= "read-only" | "read write" | "write-only" | "not-accessible"
    Status ::= "mandatory" | "optional" | "obsolete"
END

--names of objects in the MIB

ObjectName :: OBJECT IDENTIFIER

--syntax of objects in the MIB

ObjectSyntax ::= CHOICE { simple SimpleSyntax,

      -- note that simple SEQUENCES are not directly mentioned here to keep things simple
      -- (i.e, prevent misuse). However, application-wide types which are IMPLICITly encoded
      -- simple SEQUENCEs may appear in the following CHOICE

                        application-wide ApplicationSyntax}

SimpleSintax ::= CHOICE {number INTEGER,
                         string OCTET STRING,
                         object OBJECT IDENTIFIER,
                         empty NULL }

ApplicationSyntax ::= CHOICE {address   NetworkAddress,
                              counter   Counter,
                              gauge     Gauge,
                              Ticks     TimeTicks,
                              arbitrary Opaque
                             -- other application-wide types, as they are defined, will be added here
                              }
```

```
--application-wide types

NetworkAddress ::= CHOICE {internet IpAddress}

IpAddress ::= [APPLICATION 0]                          -- in network-byte order
                IMPLICIT OCTET STRING (SIZE (4))

Counter ::= [APPLICATION 1] IMPLICIT INTEGER (0.. 4294967295)

Gauge ::= [APPLICATION 2] IMPLICIT INTEGER (0.. 4294967295)

TimeTicks ::= [APPLICATION 3] IMPLICIT INTEGER (0.. 4294967295)

Opaque ::= [APPLICATION 4] OCTET STRING      --arbitrary ASN.1 value, "double-wrapped"

END
```

Figura 4.7 *ObjectSyntax* definido en el RFC 1155

- *DefVal Part*: define un valor aceptable por default que puede ser usado cuando una instancia de objeto es creada a discreción del agente, opcional.
- *Value Notation*: esta indica el nombre usado para accesar al objeto vía SNMP.

4.7.3.1 IDENTIFICACION DE INSTANCIA

Cuando accesamos a una MIB vía SNMP o algún otro medio, buscamos una instancia específica de un objeto no un tipo de objeto.

4.7.4 DEFINICIÓN DE TABLAS:

El SMI soporta solo una forma de estructura de datos : una tabla simple de dos dimensiones con entrada de números escalares . la definición se usa con *Sequence y Sequence-of* de ASN.1 , *IndexPart* de la macro de *object-type* .

Para explicar la definición de las tablas lo haremos con un ejemplo:

Considerando el tipo de objeto tcpconnTable el cual tiene un identificador 1.3.6.1.2.1.6.13, este objeto contiene información acerca de las conexiones TCP mantenidas por la correspondiente entidad manejada. Para cada conexión tenemos lo siguiente:

- *State*: estado de la conexión TCP (existen 11 valores), el valor es puesto por la entidad TCP y es cambiado por la misma entidad para reflejar el estado de la conexión . cuando se aplica el valor de deleteTCB desde la estación de administración la conexión es terminada.
- *Local address:* dirección IP del final de la conexión
- *Local port*: puerto TCP del final de la conexión
- *Dirección remota*: dirección del otro fin de la conexión
- *Remote port*: puerto TCP del otro fin de la conexión.

La tabla de conexión de TCP es parte de la MIB y como tal esta representada como un objeto manejado en la estación de administración

De alguna identidad representada por el objeto manejado. En este caso el state de tcpConnTable tiene 22 artículos de información de conexión pero solo se utilizan 5 para mantener la administración simple . La figura 4.7 tomada del RFC 1213 muestra el tcpConnTable dentro de una MIB II, y esta definida con las siguientes construcciones:

```
        ACCESS   not-accesible
        STATUS   mandatory
        DESCRIPTION
                "A table containing TCP connection/specific information"
        ::= [tcp 13 ]

tcpConnEntry OBJECT-TYPE
        SYNTAX   TcpConnEntry
        ACCESS   not-accesible
        STATUS   mandatory
        DESCRIPTION
        "information about a particular current TCP connection. An object of this type is transient in that
         it ceases to exist when (or soon after) the connection makes the transition to the CLOSED state"
        INDEX      { tcpConnLocaladdress,
                     tcpConnLocalPort,
                     tcpConnRemAddress,
                     tcpConnRemPort }
      ::= { tcpConnTable 1 }

tcpConnEntry ::= SEQUENCE { tcpConnState INTEGER,
                            tcpConnLocalAddress IpAddress,
                            tcpConnLocalPort INTEGER (0...65535),
                            tcpConnRemAddress IpAddress,
                            tcpConnRemPort INTEGER (0..65535)

tcpConnState OBJECT-TYPE
        SYNTAX     INTEGER { closed (1),
                             listen (2),
                             synSent (3),
                             synReceived (4),
                             established (5),
                             finWait1 (6),
                             finWait2 (7),
                             closeWait (8),
                             lastAck (9),
                             closing (10),
                             timeWait (11),
                             deleteTCB (12) }
        ACCESS          read-write
        STATUS          mandatory
        DESCRIPTION
                "the state of this TCP connection

        ::= { tcpConnEntry 1 }

tcpConnLocalAddress OBJECT-TYPE
        SYNTAX     IpAddress
        ACCESS     read-only
        STATUS     mandatory
```

Figura 4.8 ***especificaci'on MIB II de la tabla de conexi'on TCP (RFC 1213)***

```
        DESCRIPTION
         "the local IP address for this TCP connection, in the case of a connection in the listen state
          which is willing to accept connections for any IP interface associated with the node, the
          value 0.0.0.0 is used"
       ::= { tcpConnEntry 2 }

tcpConnLocalPort  OBJECT-TYPE
       SYNTAX     INTEGER (0..65535)
       ACCESS     read-only
       STATUS     mandatory
       DESCRIPTION
             "the local port number for this TCP connection"
       ::= { tcpConnEntry 3 }

tcpConnRemAddress  OBJECT-TYPE
       SYNTAX     IpAddress
       ACCESS     read-only
       STATUS     mandatory
       DESCRIPTION
            "the remote IP address for this TCP connection"
       ::= { tcpConnEntry 4 }

tcpConnRem Port  OBJECT-TYPE
       SYNTAX     INTEGER (0..65535)
       ACCESS     read-only
       STATUS     mandatory
       DESCRIPTION
             "the remote port number for this TCP connection"
       ::= { tcpConnEntry 5 }
```

continuacion de la figura 4.8

- La mayor parte de la tabla consiste de la secuencia *SEQUENCE OF* TcpConnEntry. La secuencia *SEQUENCE OF* consiste de uno o mas elementos , todos del mismo tipo. En este caso (y en todos los casos SNMP SMI) cada elemento es un renglón de la tabla. Así una tabla consta de cero o mas renglones.
- Cada renglón consiste de una secuencia *SEQUENCE* que incluye 5 elementos escalares, una sequence consiste de un numero fijo de elementos que pueden ser de mas de un tipo. El SMI solo permite elementos mandatorios, en este caso cada renglón de la tabla contiene elementos del tipo *INTEGER, IpAddress, INTEGER* (..65535), *IpAddress, INTEGER* (..65535).

Finalmente el componente index determina cual valor de objeto(s) será usado para distinguir un renglón de la tabla.

La figura 4.9 es un ejemplo de una tabla que contiene tres renglones. La tabla entera representa una instancia sencilla de el tipo de objeto TcpConnTable. Cada renglón es una instancia de el tipo de objeto TcpConnEntry, para un total de tres instancias. También hay tres instancias de cada elemento escalar en la tabla, así hay tres instancias del tipo de objeto TcpConnState, etc. El SMI no permite definir un elemento de una tabla para hacer otra tabla.

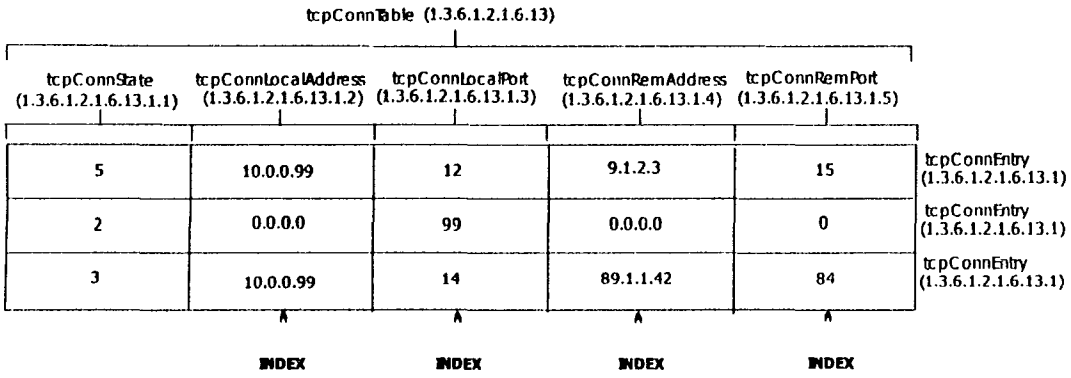


figura 5.8 instancia de una tabla de conexion TCP

Figura 4.9 instancia de una tabla de conexi'on TCP

4.7.5 OBJETOS COLUMNARES

Los objetos que aparecen en tablas los referimos como objetos columnares, el identificador de objeto no es suficiente para identificar la instancia. Existe una instancia de cada objeto en cada renglón de la tabla las instancias de un objeto no están definidas en la MIB. Necesitamos de alguna técnica para identificarla: existen dos. Técnica de acceso serial y técnica de acceso aleatorio. La primera esta basada en un orden lexicográfico de objetos en la estructura de la MIB.

Al tener una tabla un único identificador de objetos para cada renglón podemos tener objetos con el mismo identificador de objeto pero con diferentes instancias por ejemplo TcpConnTable 1.3.6.1.2.1.6.13.1.1, usando el valor del objeto index para distinguir un renglón de otro tenemos un objeto particular escalar y un objeto index en un renglón de la tabla. En SNMP podemos concatenar un objeto identificador con el valor de objeto index para diferenciarlo. Por ejemplo el valor de IfType es

1.3.6.1.2.1.2.2.1.3 y el valor de IfIndex es 2. concatenándolos tenemos el identificador de instancia para la instancia iftype tenemos 1.3.6.1.2.1.2.2.1.3.2. Si coincidiera al aplicar esto 2 valores de objeto iguales tendríamos que adicionar un subidentificador al identificador de instancia.

4.7.6 OBJETOS ESCALARES

Para distinguir entre instancia objeto y tipo de objeto. SNMP dictamina que el identificador de instancia de un objeto escalar consiste de su identificador de objeto concatenado a 0. p.e.

Object name	object identifier	instance identifier
TcpMaxConn	1.3.6.1.2.1.6.4	1.3.6.1.2.1.6.4.0

4.7.7 ORDEN LEXICOGRAFICO:

Como los identificadores de objeto son secuencias de números tienen un orden lexicográfico.

Este orden es generado a través del árbol de identificador de objeto en la MIB. Este orden es de forma numérica ascendente, se extiende a objetos identificadores de instancia. Con este tipo de arreglo una estación de administración puede recorrer el árbol de la MIB y saber que objeto sigue.

Tabla 4.1

Tabla 4.1 orden lexicografico de objetos e instancias de objeto de la figura 7.2

Object	Object identifier	Next Object Instance in lexicografic Order
ipRouteTable	1.3.6.1.2.1.4.21	1.3.6.1.2.1.4.21.1.1.9.1.2.3
ipRouteEntry	1.3.6.1.2.1.4.21.1	1.3.6.1.2.1.4.21.1.1.9.1.2.3
ipRouteDest	1.3.6.1.2.1.4.21.1.1	1.3.6.1.2.1.4.21.1.1.9.1.2.3
ipRouteDest.9.1.2.3	1.3.6.1.2.1.4.21.1.1.9.1.2.3	1.3.6.1.2.1.4.21.1.1.10.0.0.51
ipRouteDest.10.0.0.51	1.3.6.1.2.1.4.21.1.1.10.0.0.51	1.3.6.1.2.1.4.21.1.1.10.0.0.99
ipRouteDest.10.0.0.99	1.3.6.1.2.1.4.21.1.1.10.0.0.99	1.3.6.1.2.1.4.21.1.3.9.1.2.3
ipRouteMetric1	1.3.6.1.2.1.4.21.1.3	1.3.6.1.2.1.4.21.1.3.9.1.2.3
ipRouteMetric1.9.1.2.3	1.3.6.1.2.1.4.21.1.3.9.1.2.3	1.3.6.1.2.1.4.21.1.3.10.0.0.51
ipRouteMetric1.10.0.0.51	1.3.6.1.2.1.4.21.1.3.10.0.0.51	1.3.6.1.2.1.4.21.1.3.10.0.0.99
ipRouteMetric1.10.0.0.99	1.3.6.1.2.1.4.21.1.3.10.0.0.99	1.3.6.1.2.1.4.21.1.7.9.1.2.3
ipRouteNextHop	1.3.6.1.2.1.4.21.1.7	1.3.6.1.2.1.4.21.1.7.9.1.2.3
ipRouteNextHop.9.1.2.3	1.3.6.1.2.1.4.21.1.7.9.1.2.3	1.3.6.1.2.1.4.21.1.7.10.0.0.51
ipRouteNextHop.10.0.0.51	1.3.6.1.2.1.4.21.1.7.10.0.0.51	1.3.6.1.2.1.4.21.1.7.10.0.0.99
ipRouteNextHop.10.0.0.99	1.3.6.1.2.1.4.21.1.7.10.0.0.99	1.3.6.1.2.1.4.22.1.1.x

4.7.8 CODIFICACION

Los objetos en la MIB están codificados usando las reglas básicas de codificación (BER Basic encoding Rules) asociado con ASN.1. mientras no exista una forma má s compacta o eficiente de codificar, (VER) es el esquema estandarizado empleado.

4.7.9 MIBS PRIVADAS

Las MIBS han sido diseñadas para permitir el crecimiento y adicionar nuevos objetos. Extensiones privadas pueden ser adicionadas a un subárbol privado FIG 5.9 . esto permite a los fabricantes crear objetos para manejar entidades en sus productos y hacer estos objetos visibles a la estación de administración. El uso de SMI un esquema de objetos estandarizados, puede ser posible manejar objetos privados desde la estación de administración de diferentes fabricantes. En otras palabras interoperabilidad puede ser extendida la las extensiones privadas de la MIB.

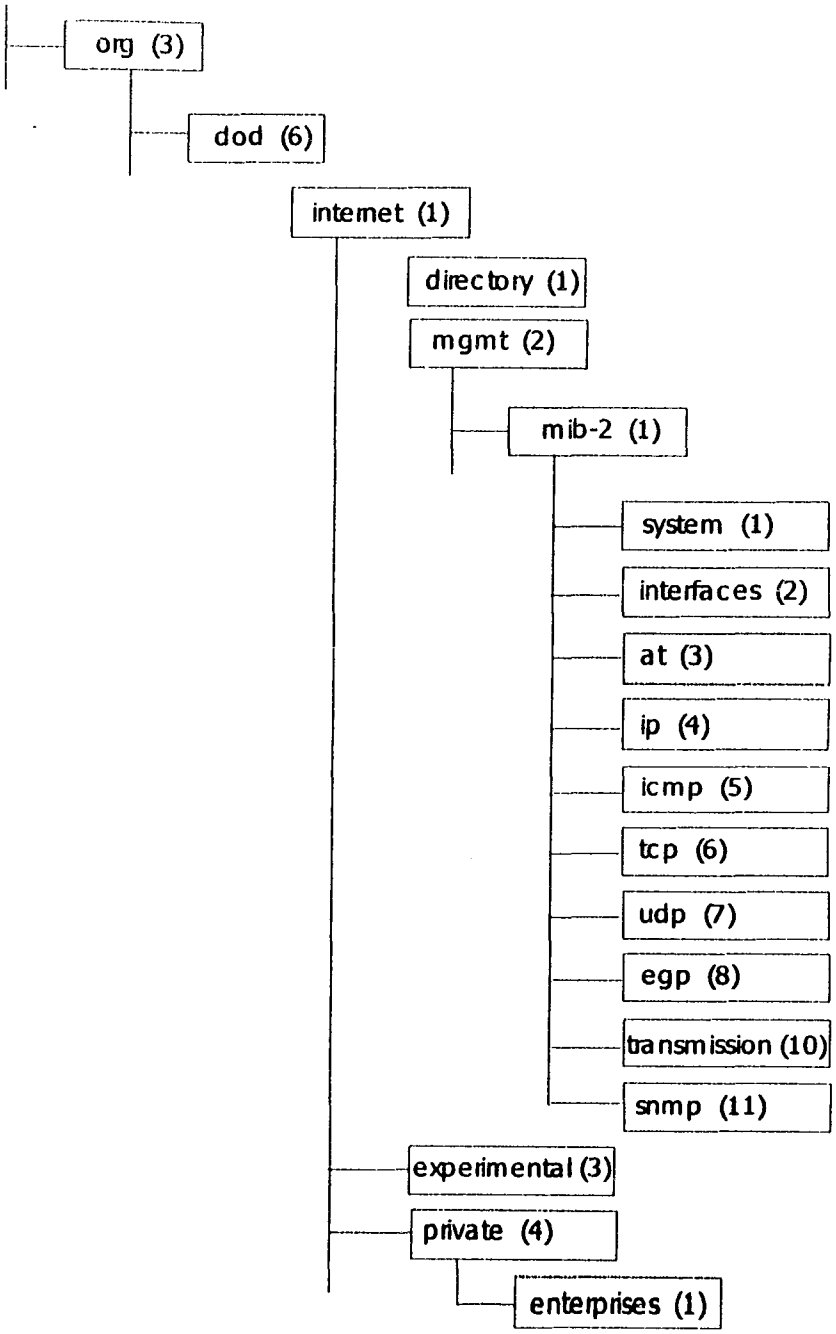


Figura 4.10 ObjectSyntax definido en el RFC 1155

Con SNMP, una estación de administración solo accesa a la información a la cual sabe llegar evitando un broadcast. Para que la estación de administración pueda manejar objetos MIB privados debe de tener la estructura privada MIB cargada. La estación de administración no puede

ofrecer al usuario los beneficios de las extensiones privadas por lo cual resulta difícil si se tienen fabricantes diferentes.

Para resolver esto muchos fabricantes proporcionan la versión textual y la descripción formal de sus extensiones MIB. Sin la descripción formal se tendrían que teclear cientos de definiciones en la estación de administración. Con la descripción formal la estación de administración es hábil para leer la MIB desde un disco y compilar dentro de una librería de la estación de administración de objetos manejados. Los fabricantes utilizan tres tipos de formatos para definir las MIBs privadas:

- Especificación SNMP SMI del RFC 1155
- Formato conciso MIB RFC 1212
- Specificación OSI SMI

4.7.10 BASE DE INFORMACION DE ADMINISTRACION II (MIB-II)

La definición de la segunda versión esta contenida en el RFC 1213. a diferencia de las MIB tiene objetos y grupos adicionales. Los siguientes criterios son utilizados:

- Un objeto necesita ser escencial para administración de configuración o fallas.
- Solo los objetos de control débiles estan permitidos. Este criterio refleja el hecho que los protocolos de administración no son lo suficientemente seguros para efectuar operaciones más poderosas.
- Evidencia de uso corriente y utilidad es requerida.
- No hay limite de objetos.
- Para evitar variables redundantes, los objetos no tienen que ser derivados de otras MIBs.

Desde que las MIB's tienen solo objetos escenciales, los grupos de MIB-II se subdividen en :

System: toda la información sobre el sistemas
Interfaces: información sobre interfases
At (address translation):descripción de translación de direcciones para el mapeo de direcciones.
Ip: implementación de ip en el sistema

Icmp: implementación de icmp en el sistema
Tcp: implementación de tcp en el sistema
Udp: implementación de udp en el sistema
Egp: implementación de egp en el sistema
Dot3 (transmission): esquemas de transmisión y protocolos de acceso en cada interfase
Snmp: implementación de snmp en el sistema

La estructura de cada grupo es determinada por el árbol estructurado de identificadores de objetos asignados a los miembros del grupo. Por ejemplo cada tabla dentro de un grupo aparece como un árbol de tres niveles. El nombre de la tabla es el nivel mas alto, el nombre de cada renglón es el segundo nivel y el nombre de cada elemento escalar del renglón de la tabla (objeto columnar) es el tercer nivel.

Ejemplo de grupo de interfases:

Grupo de interfases:

Este grupo contiene información genérica acerca de las interfases físicas de la entidad. Fig 4.11 incluye información de configuración y estadísticas de los eventos ocurridos en cada interfase. Cada interfase es añadida a una subred, aunque una interfase de un enlace punto a punto es también permitid.

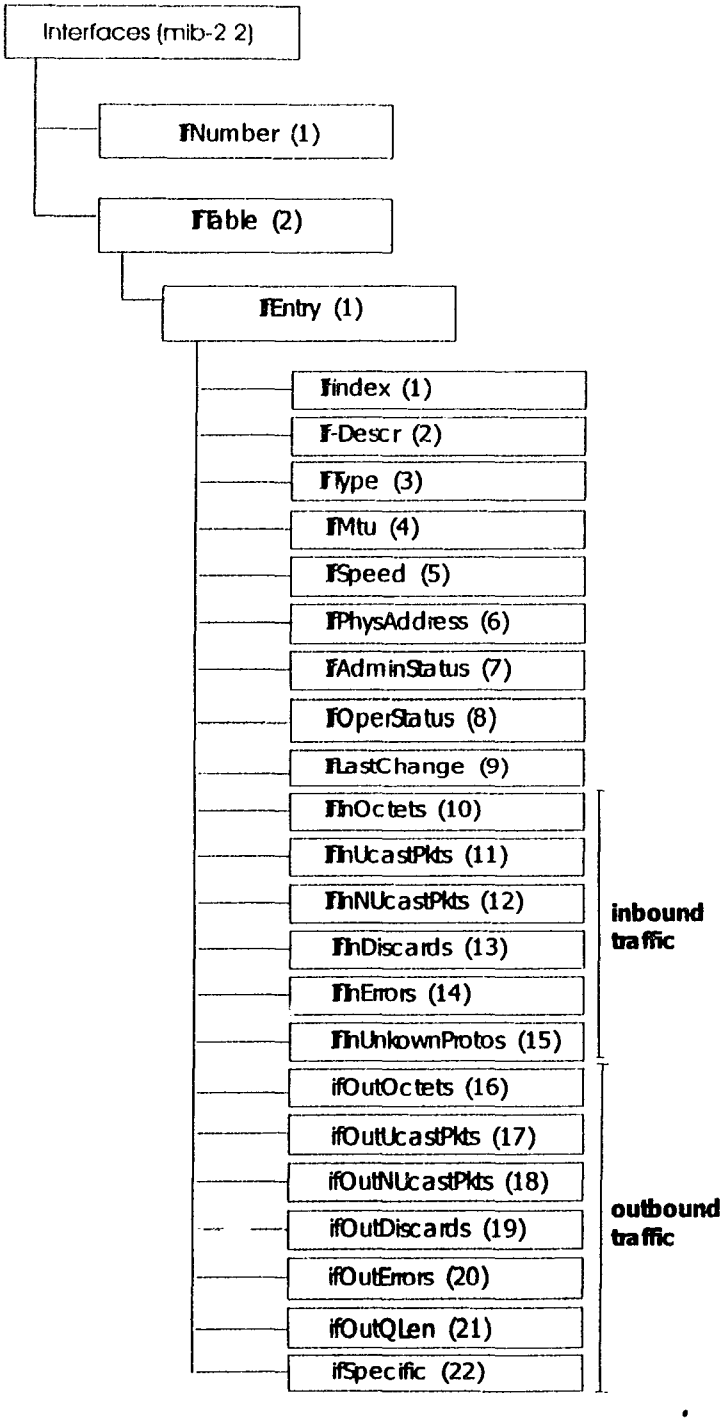


Figura 4.11 MIB II grupo de interfaces

4.7.11 GRUPOS SNMP

El grupo snmp esta definido como parte de MIB-II y tiene información relevante para la implementación y operación de SNMP. Fig 4.12 .Algunos de los objetos definidos en el grupo son valuados a 0 en aquellas implementaciones que solo soportan funciones de agente SNMP o funciones de estación de administración.

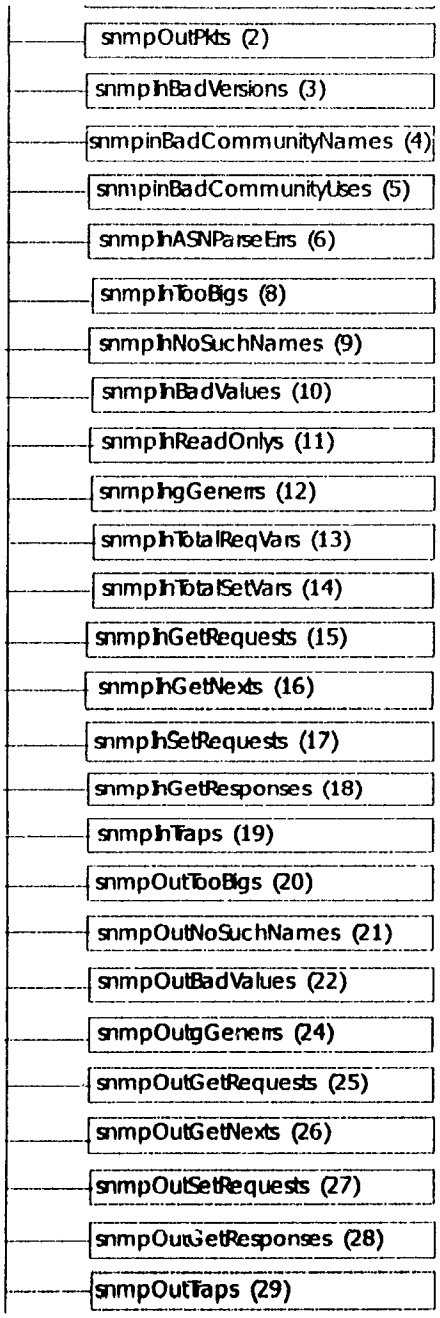


Figura 4.12 grupo snmp MIB II

4.7.12 ETHERNET INTERFACE MIB

La MIB de la interfase ethernet, es referida como EtherLike MIB (RFC 1643), es una de un número de MIB's definidas bajo el nodo de

transmision de la jerarquía MIB-II. La MIB EtherLike define objetos que representan atributos de una interfase a un medio de comunicación *ethernet*. Los siguientes esquemas son cubiertos:

- *Ethernet-csmacd*: este es el estandar ethernet para operación sobre 10 Mbps bus de coaxial.
- *Iso88023-csmacd:* este cubre un número de estandares desarrollados por el IEEE 802.3 y el ISO 8802-3. incluye operaciones a 10 y 100 Mbps sobre UTP, coaxial y fibra incluyendo topologías de bus y estrella.
- *StarLan*: este es el estandar obsoleto a 1 Mbps, par trenzado con topología de estrella desarrollado por AT&T y forma parte del estandar IEEE 802.3

Todos estos esquemas emplean control de acceso al medio (MAC) y CSMA/CD. La fig 4.13 ilustra la estructura de objetos de esta MIB:

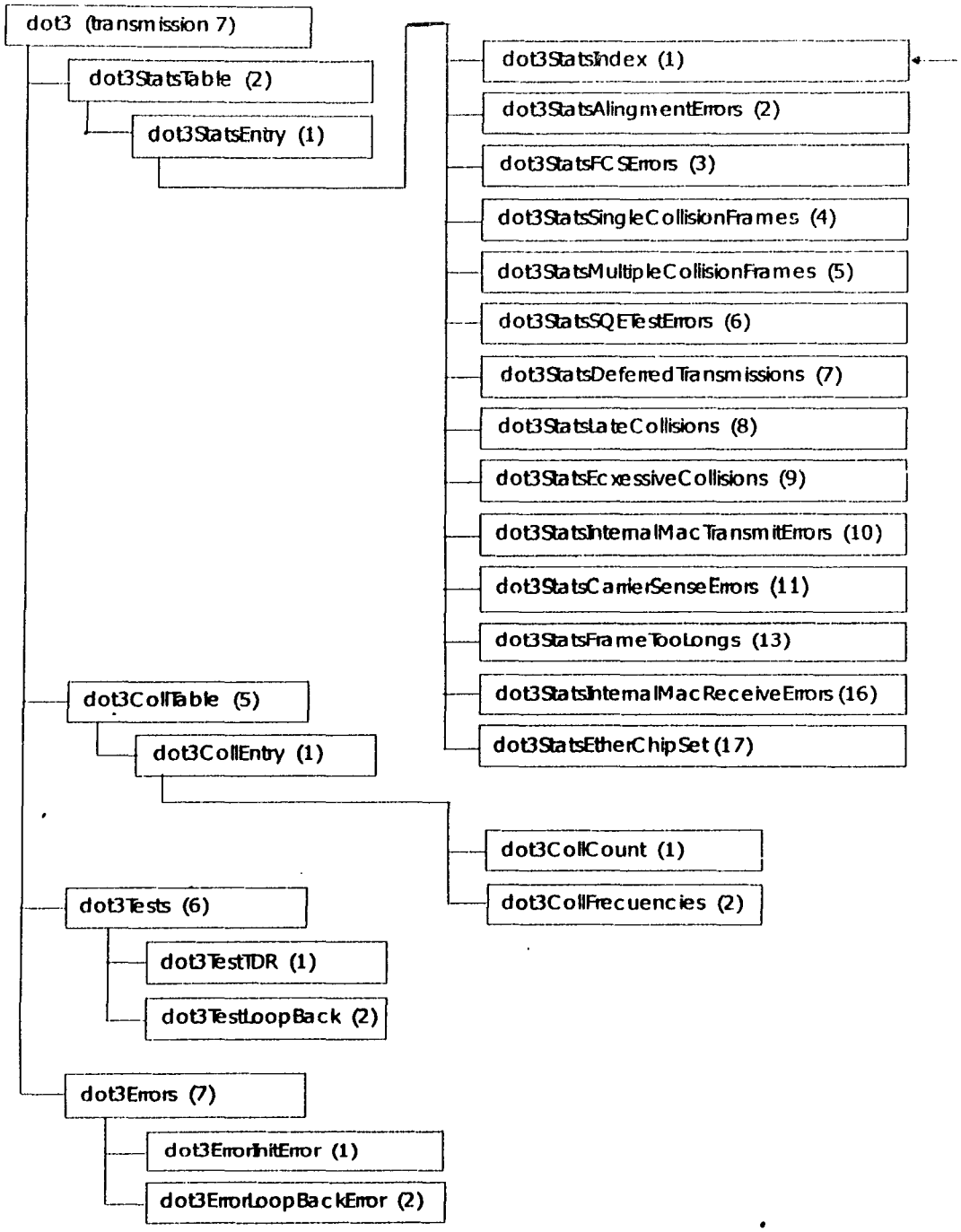


Figura 4.13MIB Etherlike

4.8 FORMATOS SNMP

La información intercambiada entre una estación de administración y un agente es en forma de mensaje SNMP. Cada mensaje incluye la versión de SNMP usada, un nombre de comunidad a ser usada para el intercambio y uno de 5 tipos de unidades de datos de protocolo (PDU's). Estos son mostrados en la fig 5.13 y la construcción de campos se muestra en la tabla 4.2

Version	Community	SNMP PDU

a) SNMP message

PDU TYPE	request-id	0	0	variablebindings

b) GetRequest PDU, GetNextRquest PDU, SetRequest PDU

PDU TYPE	request-id	error status	error index	variablebindings

c) GetResponse PDU

PDU TYPE	enterprise	agent addr	generic trap	specific trap	time stamp	variablebindings

d) Trap PDU

name1	value1	name2	value2	....	name n	value n

e) variablebindings

Figura 4.14 formatos snmp

field	Description
Version	SNMP version (RFC 1157 is version 1)
Community	A pairing of an SNMP agent with some arbitrary set of SNMP application entities the name of tje community act as a password to authenticate the SNMP message)
request-id	used to distinguish amoung outstanding requests by providing each request with a unique ID
error-status	used to indicate that an exception ocurred while processing a request, values are noError (0), tooBig (1), NoSuchName (2), badValue (3), readOnly (4), genErr (5)
error-index	when error-status in nonzero, may provide additional information by indicating which variable in a list caused the exception (a variable is an instance of a managed object)
variablebindings	a list of variable names and corresponding values (in some cases, such as GetRequest PDU, the value are null)
enterprise	type of object generating trap, based on sysObjectID
agent-addr	address of object generating trap
generic-trap	generic trap type, values are coldStart (0), warmStart (1), linkDown (2), linkUp (3),authenticationFailure (4), egpNeighborLoss (5), enterpriseSpecific (6)
specific-trap	specific trap code
time-stamp	time elapsed between the last (re)initialization of the network entity and the generation of the trap, contains the value of sysUpTime

Tabla 4.2 Campos de un mensaje SNMP

4.8.1 TRANSMISION DE UN MENSAJE SNMP

1. el PDU (Protocol Data Unit) es construido usando ASN.1 con una estructura definida en el RFC 1157
2. El PDU es pasado a un servicio de autentificación, junto con las direcciones de transporte fuente y destino y el nombre de la comunidad. El servicio de autentificación ejecuta cualquier transformación requerida para el intercambio, tal como encripción del código de autentificación y regresa el resultado.
3. La entidad de protocolo entonces construye el mensaje, consistiendo de una versión de campo, nombre de comunidad y el resultado del paso 2.
4. Este nuevo objeto ASN.1 es entonces codificado usando las reglas básicas decodificación y pasado al servicio de transporte.

4.8.2 RECEPCION DE UN MENSAJE SNMP

1. Se hace un chequeo básico de sintaxis del mensaje y se descarta el mensaje si tiene fallas.
2. Se verifica el número de versión y se descarta si no coincide.
3. La entidad de protocolo entonces pasa el nombre de usuario, la porción PDU del mensaje, y las direcciones de transporte origen y destino (tomando en cuenta el que servicio de transporte ha entregado el mensaje) a un servicio de autentificación.
   a) Si la autentificación falla, las señales del servicio de autentificación de la entidad de protocolo SNMP, generan un trap y descartan el mensaje.
   b) Si la autentificación es exitosa, el servicio de autentificación regresa un PDU en forma de objeto ASN.1.

4. La entidad de protocolo hace un chequeo básico de sintaxis del PDU y descarta si falla. Por otro lado usando el nombre de comunidad, la apropiada política de acceso SNMP es seleccionada y el PDU es procesado.

En la práctica los servicios de autentificación deben de verificar que el nombre de comunidad autoriza el recipiente de mensajes de la entidad SNMP origen.

4.8.3 LIGADURA DE VARIABLES

Es posible agrupar un número de operaciones del mismo tipo (get, set trap) dentro de un mensaje. Por ejemplo si queremos obtener los valores de todos los objetos escalares de un grupo en particular de un agente en particular mandamos un solo mensaje que pida todos los valores y obtenga una simple respuesta, listando todos los valores.

Para implementar el intercambio de objetos múltiple el PDU de SNMP incluye un campo de nombre variable-bindings. Este campo consiste de una secuencia de referencias para instancias de objeto, junto con los valores de esos objetos. Si el PDU lleva solo un nombre es ignorado el valor del campo, en este caso utilizamos el valor de NULL en el campo varible-bindings.

4.8.4 GETREQUEST PDU

Getrequest es usado por la aplicación y contiene los siguientes campos:

- *PDU type*: indica que es un PDU GetRequest
- *Request-id*: la entidad emisora asigna un numero que solo el mismo agente puede identificar, la aplicación SNMP correlaciona las respuestas con las preguntas y verifica la duplicidad de PDU.
- *Variablebindings*: lista de instancias de objeto cuyos valores son requeridos.

La entidad receptora SNMP responde con un GetResponse PDU que contiene el mismo request-id. La figura 4.15 muestra la secuencia de los PDU.

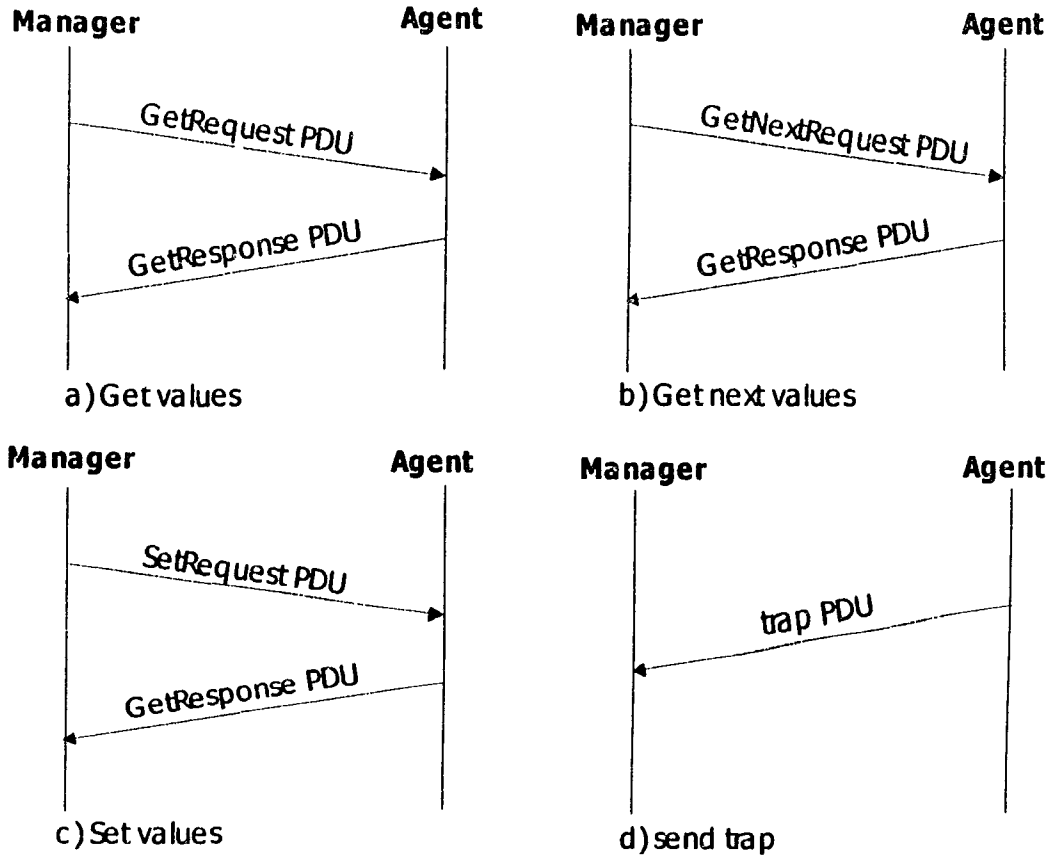


Tabla 4.15 secuencias de PDU SNMP

Como SNMP solo puede extraer objetos de las hojas del árbol de la MIB. No es posible extraer un renglón completo de una tabla (p, e la tabla de ruteo IP) solamente referenciando un objeto (p.e IpRouteEntry). Se podría obtener la tabla incluyendo cada instancia de objeto en una lista de variablebindings. Por ejemplo podemos extraer el primer renglón con:

GetRequest (ipRouteDest.9.1.2.3, ipRouteMetric1.9.1.2.3 ,
IpRouteNexHop.9.1.2.3)

4.8.5 SETREQUEST PDU

Tiene el mismo formato que GetRequest pero es usado para escribir un valor de un objeto en vez de leerlo y responde también con un GetResponse PDU.

El comando *set* puede ser usado para borrar una tabla. Un objeto puede ser usado para representar un comando poniéndole un valor específico, por ejemplo un agente puede incluir un objeto propietario *Reboto* con un valor inicial de 0, si la estación de administración cambia este valor a 1 el agente rebootea y resetea el equipo.

4.8.6 GETNEXTREQUEST PDU

Es casi idéntico al anterior pero cada variable en la lista de variablebindings refiere a una instancia de objeto cuyo valor tiene que ser retornado. La respuesta al valor de la instancia de objeto es el próximo en orden lexicográfico.

Una estación de administración usando GetNextRequest PDU puede descubrir la estructura de una MIB. También puede ser usado para buscar tablas

4.8.7 TRAP PDU

Contiene los siguientes campos:

PDU type: trap PDU
Enterprise: identifica al sistema que generó el trap
Agent address: ip del objeto que generó el trap
Generic-.trap: uno de los tipos de trap predefinido.
Especific-trap: código que indica mas específicamente la naturaleza del trap
Time-stamp: tiempo entre la ultima reinicialización de la entidad de red que genero el trap y La generación del trap.
Variablebindings: información adicional relacionada al trap

4.8.8 SOPORTE A NIVEL DE TRANSPORTE

Snmp requiere de algún servicio de transporte para entregar los mensajes SNMP. Requiere de un servicio orientado a no conexión.
Dentro de la arquitectura TCP/IP podemos usar UDP (User Datagram Protocol). Los puertos asignados para SNMP son el 161 y 162. los agentes escuchan los comandos GetRequest, GetNextRequest y SetRequest en el 161. las estaciones de administración escuchan los traps en el 162.

Para evitar la perdida de paquetes UDP, SNMP constantemente polea a los agentes para mantener contacto.

4.8.9 POLEO DE TRAPS

Si una estación tiene un gran número de agentes que manejan un gran número de objetos, llega ser impractico el polearlos a todos. Para evitar esto SNMP y la MIBs están diseñadas para usar una técnica denominada poleo directo de TRAP. Aquí en un cierto intervalo (una hora, un día, etc.) la estación de administración polea a todos los elementos para pedirles datos. Cada agente es responsable de notificar a la estación de administración si un suceso ocurre. Estos eventos son comunicados mediante mensajes Traps. Con esto no saturamos la red con información de poleo.

4.9 COMUNIDADES Y NOMBRES DE COMUNIDAD

La administración de redes envuelve la interacción de un número de entidades de aplicaciones soportadas por un protocolo de aplicación. En el caso de SNMP, las entidades de aplicación son las aplicaciones de la estación de administración y las aplicaciones de las estaciones manejadas (agentes) que usan SNMP, el cual es el protocolo soportado.

La aplicación envuelve manejar relaciones de uno a muchos entre la estación de administración y un grupo de estaciones manejadas. También tenemos relación entre una estación manejada y un grupo de estaciones de administración. Cada estación manejada controla su propia MIB y puede controlar las MIB's de un cierto número de estaciones administradas: hay tres aspectos para este control.

Servicio de autentificación: la estación administrada puede limitar el acceso a la MIB a estaciones administradas autorizadas

Políticas de acceso: la estación administrada puede dar diferentes privilegios para diferentes estaciones de administración.

Servicio de proxy: una estación manejada puede actuar como proxy de otras estaciones manejadas, esto puede envolver los dos anteriores.

SNMP provee una primitiva y limitada capacidad de seguridad lo que denominados comunidad. Una comunidad SNMP es la relación entre un agente SNMP y un grupo de administradores que definen autentificación, control de acceso y características proxy. El concepto de comunidad es local definido en el sistema manejado. El sistema manejado establece una comunidad para cada combinación de las características antes mencionadas. Cada comunidad tiene un único nombre de comunidad y las estaciones de administración usan este nombre de comunidad en todas sus operaciones get, set.

Como las comunidades están definidas localmente en el agente, el mismo número puede ser usado por diferentes agentes. La identidad de nombres es irrelevante y no indica ninguna similaridad entre las comunidades definidas. Así una estación de administración puede rastrear el nombre de la comunidad asociado a cada agente que desean acceso.

4.9.1 SERVICIO DE AUTENTIFICACIÓN

Como su nombre lo indica el servicio concierne a la autentificación. En el caso de un mensaje SNMP la función del servicio de autentificación deberá de asegurar el recipiente que el mensaje es de la fuente de la cual dice ser. Cada mensaje (get o put request) de una estación de administración hacia un agente incluye el nombre de la comunidad. Este nombre funciona como password y el mensaje es asumido para ser autentificado si el remitente conoce el password. La autentificación puede ser encriptada y desencriptada.

4.9.2 POLÍTICAS DE ACCESO

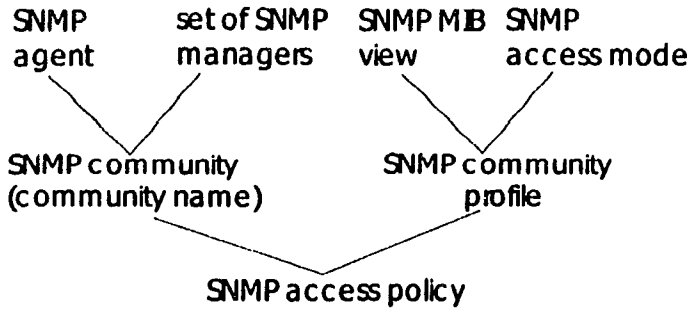
Por definición de comunidad, un agente limita su acceso a la MIB para un grupo seleccionado de estaciones de administración. Usando más de

una comunidad, el agente puede proveer diferentes categorías del acceso a diferentes estaciones de administración. Esto tiene dos aspectos:

SNMP MIB view: un subgrupo de objetos dentro de una MIB. Diferentes vistas a las MIBs pueden ser definidas para cada comunidad. El grupo de objetos en una vista no necesita pertenecer a un subárbol de la MIB.

SNMP access mode: Un elemento de un grupo (read-only read-write).Un modo de acceso es definido para cada comunidad.

La combinación de estos dos es conocida como perfil de comunidad SNMP. El pérfil está asociado con cada comunidad definida por un agente y se conoce como política de acceso SNMP.



La fig 4.16 ilustra una tabla con las relaciones anteriores

4.9.3 SERVICIO PROXY

Para cada dispositivo que el sistema proxy representa, se mantiene como una política de acceso SNMP. Así el proxy conoce cuales objetos MIB que pueden ser usado para manejar el sistema gestionado (MIB view) y su modo de acceso.

4.10 SNMPv2

Para cubrir las deficiencias de la primer versión se desarrollo la segunda versión denominada SNMPv2 y expande su funcionalidad para OSI. Se formuló una propuesta conocida como SMP (simple n.. agement protocol) desarrollada por las mismas personas que formularon SNMP, fue propuesta en julio de 1992 en ocho documentos. Estos documentos no

fueron RFC's. Fueron propuestos a la comunidad de internet para actualizar SNMP. Estos se tomaron como base para la realización de la segunda generación de SNMP en marzo de 1993. se formaron 2 grupos: Grupo de trabajo funcional y grupo de trabajo sobre seguridad. En 1996 se hizo una revisión y se rechazaron los aspectos de seguridad y se crearon nuevos RFC's. La coexistencia y transición entre SNMPv1 y SNMPv2 se encuentra en el RFC 1908. ver tabla 4.3

Number	title
1901	introduction to community-based SNMPv2
1902	structure of management information for SNMPv2
1903	textual conventions for SNMPv2
1904	conformance statements for SNMPv2
1905	protocol operations por SNMPv2
1906	transport mappings for SNMPv2
1907	management information base for SNMPv2
1908	coexistence between version 1 and version 2 of the Internet-standard Management Framework

Tabla 4.3 RFCs de SNMPv2

4.10.1 MEJORAS DE SNMPv2

Snmpv2 puede soportar administración de red centralizada o distribuida. Algunos sistemas pueden operar como administradores o como agentes.

Las mejoras de SNMPv2 caen dentro de lo siguiente:

- Estructura de la administración de la información (SMI)
- Capacidad de comunicación entre administrador y administrador
- Operaciones del protocolo

La SMI de SNMPv2 expande a la SMI SNMP. La macro usada para definir tipo de objeto ha sido expandida para incluir nuevos tipos de datos y tener mayor información asociada a un objeto.

La MIB SNMPv2 contiene información básica de tráfico acerca de la operación del protocolo SNMPv2, esto es análogo al grupo snmp en MIB II. También contiene otra información relacionada a la configuración de un *manager* o un agente SNMPv2.

El cambio más notable es la incorporación de dos nuevos PDU. El GetBulkRequest habilita al administrador para extraer grandes bloques de datos (múltiples renglones en una tabla). InformRequest PDU habilita a un manager para mandar traps con el tipo de información a otro.

4.11 ESTRUCTURA DE LA INFORMACIÓN DE ADMINISTRACIÓN SMI

El SMI esta basado en el SMI para SNMP. SMI para SNMPv2 provee especificaciones más elaboradas y documentación de objetos manejados y MIBs. SMI SNMPv2 introduce cuatro conceptos:

- Definición de objeto
- Tablas conceptuales
- Definiciones de notificación
- Módulos de información

4.11.1 DEFINICIÓN DE OBJETO:

También se usa para describir objetos manejados. La ASN.1 macro de *OBJECT-TYPE* es usada para convertir la sintaxis y semántica de todos los objetos manejados en una forma sistemática.

Prácticamente es el mismo tipo que el RFC 1155 con refinamientos en el RFC 1212.

La tabla 4.4 provee una comparación entre la macro definida en SNMPv2 y la macro definida en los RFC 1155 y 1212.

tabla 5.4 Comparacion de SMI entre SNMP y SNMPv2

SNMPv2	SNMP (RFC 1212)

TYPE NOTIFICATION ::= "SYNTAX" Syntax
Syntax ::= type(ObjectSyntax) | "BITS" "{" Kibbles "}"
ObjectSyntax ::= CHOICE { simple SimpleSyntax, application-wide Application Syntax }
SimpleSyntax ::= CHOICE {
integer-value INTEGER (-2147483648.. 2147483647),
string-value OCTETSTRING (SIZE (0..65535)),
objectID-value OBJECTIDENTIFIER }
applicationSyntax ::= CHOICE {
ipAddress-value IpAddress,
counter-value Counter32,
timeticks-value TimeTicks,
arbitrary-value Opaque,
big-counter-value Counter64,
unsigned/integer-value Unsigned32 }
UnitsPart ::= "UNITS" Text | empty
	TYPE NOTATION ::= "SYNTAX" type (ObjectSyntax)
	ObjectSyntax ::= CHOICE { simple SimpleSyntax, application-wide Application Syntax }
	SimpleSyntax ::= CHOICE {
	number INTEGER,
	string OCTETSTRING,
	object OBJECTIDENTIFIER,
	empty NULL }
	ApplicationSyntax ::= CHOICE {
	internet IpAddress,
	counter Counter,
	gauge Gauge,
	ticks TimeTicks,
	arbitrary Opaque }

"MAX-ACCESS" Access Access ::= "read-only" | "read-write" | read-create" | "not-accessible" | "accessible-for-notify"	"ACCESS" Access Access ::= "read-only" | "read-write" | "write-only" | "not-accessible"
"STATUS" Status Status ::= "current" | "obsolete" | "deprecated"	"STATUS" Status Status ::= "mandatory" | "optional" | "obsolete" | "deprecated"
"DESCRIPTION" Text	"DESCRIPTION" value (description DisplayString)
ReferPart ::= "REFERENCE" Text | empty	ReferPart ::= "REFERENCE" value (reference DisplyString) | empty
IndexPart ::= "INDEX" "{" Indextypes "}" | "AUGMENTS" "{" Entry "}" | empty IndexTypes ::= IndexType | IndexTypes "," IndexType IndexType ::= "IMPLIED" Index | Index Index ::= value (indexobject ObjectName) Entry ::= value (indexobject ObjectName)	indexPart ::= "INDEX" "{" IndexTypes "}" IndexTypes ::= IndexType | IndexTypes "," IndexType IndexType ::= value (indexobject ObjectName)
DefValPart ::= "DEFVAL" "{" value (defval Syntax) "}" | empty	DefValPart ::= "DEFVAL" "{" value (defvalue ObjectSyntax) "}" | empty
VALUE NOTATION ::= value (VALUE ObjectName)	VALUE NOTATION ::= value (VALUE ObjectName)

Tabla 4.4 comparación SMI entre SNMP y SNMPv2

4.11.2TIPO DE DATOS:

LA TABLA 4.5 lista los tipos de datos de SNMPv1 y SNMPv2, para ambos el tipo de un objeto puede estar basado en alguna aplicación. Los tipos simples de SNMPv2 son:

Data type	SNMPv1	SNMPv2
INTEGER	X	X
Unasigned32		X
Counter32	X	X
Counter64		X
Gauge32	X	X
TimeTicks	X	X
OCTET STRING	X	X
IpAddress	X	X
OBJECT IDENTIFIER	X	X
Opaque	X	X

Tabla 4.5 tipos de datos SNMPv1/SNMPv2

INTEGER (-2147483648. .2147483647)
OCTET STRING (0. .65535)
OBJECT IDENTIFIER: Identificador único de un objeto, consiste de una secuencia de números conocidos como subidentificadores, la secuencia se lee de izquierda a derecha y denota la localización del objeto en la estructura de árbol de la MIB.

Tipos de aplicación definidos en SNMPv2:

Ipaddress: esta es la dirección de 32 bits definida en IP

Counter32: entero no negativo que puede ser incrementado pero no decrementado. Un valor máximo de 2 a la 32 – 1 esta especificado. SNMPv2 especifica que el contador no tiene un valor inicial definido.

Counter64: entero no negativo que puede ser incrementado pero no decrementado. Un valor máximo de 2 a la 64 – 1 está especificado.

Gauge32: entero no negativo que puede crecer o decrecer. Si el máximo valor es alcanzado el *gauge* se queda en ese valor hasta un reset.

Unasigned32: representa un entero en el rango de 0 a 2 a la 32 –1.

Timeticks: entero no negativo que cuenta el tiempo en centésimas de segundo, este valor está definido en las MIBs.

Opaque: provee compatibilidad con SNMPv1

BITS: enumeración de los bits.

UNIT PART: Macro de ***OBJECT-TYPE*** en SNMPv2 que incluye una cláusula opcional UNITS la cual esta asociada con el objeto. Esta cláusula es útil para cualquier objeto que representa unidades de medida como el tiempo.

MAX-ACCESS clause: es similar a SNMP ACCESS. El prefijo MAX enfatiza un nivel máximo de acceso, independientemente de cualquier política de autorización. No incluye *write-only*. Una nueva categoría *read-create* es añadida. Las capacidades son:

Not-accessible: no accesible para el administrador par cualquier operación.
Accessible-for-notify: un objeto que es accesible solo vía notificación.
Read-only: acceso de lectura
Read-write: lectura y escritura
Read-create: lectura, escritura y crear acceso

STATUS clause: Es igual que la versión 1 pero no contiene las categorías de *opcional* o *mandatory*.

4.11.3 TABLAS SNMPv2:

Las mejoras se basan en el RFC 1212 y la especificación de RMON (RFC 1757) para facilitar la creación, borrado y acceso. Dos categorías son permitidas en SNMPv2:

Tablas que prohíben la creación o borrado de un renglón por el administrador: estas tablas son controladas por el agente.

Tablas que permite la creación o borrado de un renglón por el administrador: el administrador puede borrar o crear tablas.

Ambas tablas proveen convenios y facilidades para accesar a los renglones de la tabla por el índice.

4.11.4 INDICE DE TABLAS

Una diferencia entre la convención SNMPv2 para la cláusula de INDEX y la conversión del RFC 1212 es el uso opcional del modificador IMPLIED para un nombre de objeto en SNMPv2. Este modificador esta en juego al definir los identificadores de instancia.

4.11.5 CREACIÓN Y BORRADO DE RENGLONES:

Dos estrategias generales fueron creadas:

1. definir dos nuevos tipos de unidades de datos de protocolo, *Create* y *Delete*, para ser usados para borrado y creación de renglones
2. Pegar la semántica para creación y borrado de renglones dentro de la MIB con una nueva convención llamada *RowStatus*. El borrado y creación son ejecutadas con *set* y *get*.

Dos métodos de creación de renglones a partir de RowStatus: createandwait y createandgo:

Método createandwait: el administrador comienza por instruir al agente para crear una nueva columna con un identificador de instancia dado (valor de índice). Si es exitoso el agente crea el renglón y asigna valores a aquellos objetos en el renglón con valores por default. Si todos los objetos read-create tiene valores por default, el renglón es colocado en estado notinservice, indicando que el renglón esta creado pero no esta activo. Si los objetos read-create no tiene valores por default el renglón es puesto en estado notready indicando que el renglón no puede ser activado porque faltan algunos valores. El administrador entonces manda un get para determinar el status de los objetos read-create. El agente responde con un valor para cada objeto con un valor por default, nosuchiunstance para cada objeto que no tiene valor por default, nosuchobject para cada objeto definido en la MIB que no es soportado por el agente. El administrador entonces usa

un set para asignar un valor a todos los objetos nosuchinstance y puede asignar nuevos valores a los objetos por default.

El createandgo es más simple pero tiene dos restricciones:

Primero esta limitado a tablas con objetos que caben dentro de un PDU set o response, segundo el administrador no aprende automáticamente los valores default. El manager comienza por seleccionar un identificador de instancia. Puede entonces poner un PDU get para determinar cuales objetos read-create son nosuchinstance, o puede ya tener información por conocimiento previo del agente. El administrador entonces manda un set PDU que crea el renglón y asigna valores a los objetos en ese renglón. El administrador puede asignar valores a todos los objetos read-create que no tienen valores por default y puede asignar valores a los objetos read-create que tiene valores por default. Si la operación set es exitosa el renglón es creado y puesto en modo activo.

Ambas opciones están disponibles dentro de un agente y este puede decidir cual usa para cada tabla

Para borrar un renglón conceptual una estación de administración manda una operación set que pone el valor del estado de la instancia de la columna a destroy. Si la operación es exitosa, el agente remueve el renglón conceptual de la tabla.

Una estación de administración puede también suspender un renglón activo. Manda una operación set que pone el valor de la instancia de columna a not in service el agente responde con no error.

4.11.6 DEFINICION DE NOTIFICACION

La macro de NOTIFICATION TYPE es usado por SNMPv2 cuando un evento ocurre en una entidad. La cláusula opcional OBJECTS define el orden de secuencia de los objetos MIB que están contenidos dentro de cada instancia de la notificación. Los valores de esos objetos son comunicados a un administrador cuando una notificación ocurre. La cláusula DESCRIPTION contiene un texto con la semántica de la notificación. .

4.11.7 MÓDULOS DE INFORMACION

SNMPv2 introduce el concepto de modulo de información el cual especifica un grupo de definiciones relativas. Tres módulos de información son usados:

1. MIB módulos, los cuales contiene definiciones de objetos manejados interrelacionados y hace uso de las macros de *Object-type* y *notification-type*
2. Enunciados compliance para módulos MIB, los cuales hacen uso de las macro *module-compliance* y *object-group*
3. Enunciados de capacidad para implementaciones del agente que hace uso de la macro *AGENT CAPABILITIES*

En adición SNMPv2 incluye la definición de una macro object-identity la cual es usada para documentar los objetos usados en una MIB.

4.12 SIMPLE NETWORK MANAGEMENT PROTOCOL VERSION 3 (SNMPv3)

La tercera versión de SNMP esta basada en las dos anteriores. Todas las versiones tienen la misma estructura y componentes:

- Muchos nodos manejados cada uno con una entidad SNMP que provee acceso remoto hacia los agentes.
- Al menos una entidad SNMP con aplicaciones de administración (estación de administración)
- Un protocolo de administración usado para intercambiar información de administración entre entidades SNMP
- Información de administración.

4.12.1 ARQUITECTURA

Mantiene la misma arquitectura pero con componente mejor definidos:

- Definición de lenguaje de datos
- Definición de MIB

- Definición de protocolo
- Seguridad y administración

Usando los mismos principios en la definición de nuevas capacidades para la seguridad y administración.

La tercera versión de SNMP es descrita en los RFC´s 2570, 2571 ,2572 , 2573 , 2574 y 2575 . coexistencia entre las tres versiones es encontrada en el RFC 2576. fue producido por el IETF (Internet Engineering Task Force). Las nuevas funcionalidades de versión 3 con respecto a la 2 son:

- Seguridad
- Autentificación y privacidad
- autorización y control de acceso
- administración
- nombrado de entidades
- gente y políticas
- nombres de usuario y llaves de administración
- notificación del destinatario
- relaciones entre proxies
- configuración remota vía operaciones SNMP

4.12.2 DEFINICIÓN DEL LENGUAJE DE DATOS

La definición del lenguaje de datos se encuentra en el RFC 2578 "estructura de la administración de la información versión 2 (SMIv2). Aquí se definen los tipos de datos fundamentales, modelo de objetos y las reglas para crear los MIBs. Las especificaciones se encuentran en los RFC 2579 y 2580:

RFC 2579: "conversiones textuales para SMIv2" define un grupo inicial de abreviaciones, las cuales son disponibles para usarse dentro de los módulos MIB para la conveniencia de lectores y escritores.

RFC 2580:"anunciados de confirmancia para SMIv2" define los formatos de enunciados, los cuales son usados para describir los requerimientos para la implementación de agentes y enunciados de

capacidad que pueden ser usados para documentar las características de las implementaciones particulares.

4.13 MODULOS MIB

Los módulos MIB están definidos acorde a las reglas definidas en los documentos que especifican el lenguaje de definición de datos, principalmente el SMI como complemento por las especificaciones relacionadas.

Existe un gran número de módulos MIB definidos basados en estándar que periódicamente se actualizan en la lista de protocolos estándar (RFC 2400). Existen alrededor de 100 MIB basadas en estándares con un total de objetos definidos de 10000 aprox. existen además MIBs definidas por fabricantes lo que aumenta el número.

En general , la información de administración definida en cualquier Modulo MIB ,sin importar la versión del lenguaje de definición de datos usado, puede ser usado con cualquier versión del protocolo. La única excepción es el counter de 64 introducido en SNMPv2 al cual no puede acceder SMNPv1

4.13.1 OPERACIONES DE PROTOCOLO Y MAPAS DE TRANSPORTE

Para estas son definidas dentro de SNMPv2 en los RFC 1905 y 1906 respectivamente

4.14 SEGURIDAD Y ADMINISTRACION

Consiste de 6 documentos:

RFC 2570 "introducción a versión 3 del estándar de internet para la Administración de red" provee una introducción a SNMPv3

RFC 2571 "arquitectura para describir la administración de SNMP" describe todas la arquitecturas con énfasis en la arquitectura de seguridad y administración

RFC 2572 "proceso de mensajes y su envió para SNMP" describe la posibilidad de manejar múltiples mensajes y enviarlos hacia la parte del protocolo SNMP correspondiente de su entrega.

RFC 2573 "aplicaciones SNMPv3": describe los 5 tipos de aplicaciones que pueden ser asociadas con SNMPv3 y sus elementos.

RFC 2574"modelo de seguridad basado en usuarios para versión 3 del SNMPv3": describe mecanismos, amenazas, protocolos y los datos usados soportados para proveer seguridad a nivel de mensaje.

RFC2575" modelo de control de acceso basado en vistas (VACM) para SNMP": describe el VACM para ser usado en la arquitectura de SNMP

4.14.1 ARQUITECTURA DE SEGURIDAD Y ADMINITRACION

EL RFC 2571 define esta arquitectura. Define aspectos basados en la seguridad y administración, define un numero de términos usados para SNMPv3:

- motores y aplicaciones
- entidades (proveedores de servicio tales como motores en agentes y estaciones de administración)
- identidades (servicio de usuarios)
- información de administración, incluyendo soporte para múltiples contextos lógicos.

El documento contiene un pequeño modulo MIB que es implementado por todos los motores de protocolo autoritativos de SNMPv3. Un motor autoritativo es el receptor de un mensaje si el mensaje requiere una respuesta (como un get o set) o el emisor de el mensaje no requiere una respuesta.

4.15 PROCESO DE MENSAJES Y SU ENVIO (MPD)

El RFC 2572 define los procedimientos para la entrega de mensajes de múltiples versiones de SNMP hacia el modelo de procesamiento de mensajes correspondiente. Define los procedimientos para la entrega de PDU's hacia aplicaciones SNMP. describe el modelo de procesamiento de

mensajes SNMPv3. un motor de protocolo SNMPv3 debe soportar al menos un modelo de procesamiento de mensajes.

4.16 APLICACIONES SNMPV3

El RFC 2573 describe los 5 tipos de aplicaciones que pueden ser asociados a un motor SNMP. Las aplicaciones son: Generadores de comandos, respondedores de comandos,originadores de notificación, receptores de notificación y reenviadores proxy.

También define los módulos MIB para blancos específicos de operaciones de administración (incluyendo notificaciones), filtrado de notificaciones y proxies de reenvió.

4.17 MODELO DE SEGURIDAD BASADO EN USUARIOS (USM)

El RFC 2574 describe este modelo. Define los procedimientos de elementos para proveer seguridad a nivel de mensajes SNMP. El documento describe las dos amenazas primarias y secundarias contra las que se defiende este modelo. Estas amenazas son: modificación de información, mascarada, modificación de mensajes y divulgación.

El USM utiliza MD5 y el algoritmo secure Hash como llaves para proveer integridad de datos para proteger directamente contra ataques de modificación de datos, proveer indirectamente autentificación del origen de los datos y defender contra ataques de mascarada.

USM usa indicadores increméntales de tiempo sincronizados para defender contra ráfagas de ataque para modificación de mensajes. Mecanismos sincronizados de relojes automáticos basados sobre el protocolo que esta especificado sin dependencia entre muchas fuentes de tiempo y consideraciones de seguridad.

USM usa el estándar de encripción de datos (DES) en el bloque de cifras de modo encadenado (CBC) para proteger contra divulgación.

También se incluye una MIB para monitoreo remoto y administración de parámetros configurables para el USM, incluyendo una llave de distribución y llave de administración.

Una entidad de protocolo sencillo que puede proveer soporte simultáneo para modelos de seguridad múltiple , como protocolos de privacidad y autentificación. Todos los otros protocolos usados por USM están basados en criptografía simétrica. La arquitectura SNMPv3 admite el uso de llaves criptográficas públicas.

1. Un usuario y sus atributos se definen de la siguiente manera:

- ***userName***: una cadena que representa el nombre del usuario.
- ***securityName***: una cadena leíble representando al usuario en un formato que es modelo de seguridad independiente.
- ***authProtocol***: una indicación de si los mensajes enviados por estos usuarios pueden ser autenticados, y si es así, el tipo de protocolo de autenticación que es usado. Se definen 2 protocolos de autenticación en este artículo:
- el HMAC-MD5-96
- el HMAC-SHA-96.
- ***authKey***: si los mensajes enviados por el usuario pueden ser autenticado, se utiliza la llave de autenticación con el protocolo de autenticación.
- ***authKeyChange y AuthOwnKeyChange***: la única manera de actualizar remotamente la llave de autenticación. Hace en forma segura, que la actualización pueda ser completada sin necesidad de emplear protección de retiro.
- ***PrivProtocol***: una indicación de si los mensajes enviados por el usuario pueden ser protegidos de descubrimientos, y si es así, el tipo de protocolo de retiro que es usado. El Protocolo de Encriptación Simétrico CBC-DES es definido en este artículo.
- ***PrivKey***: si el mensaje enviado por el usuario puede ser encriptado y desencriptado, se usa la llave de retiro con el protocolo de retiro.
- ***privKeyChange y PrivOwnKeyChange***: la única manera de actualizar remotamente la llave de encriptación. Hace en forma segura, que la actualización pueda ser completada sin necesidad de emplear protección de retiro.
-

2.- Protección de la repetición

Cada máquina de SNMP mantiene 3 objetos:

- ***snmpEngineID***, el cual singularmente e inequívocamente identifica a la máquina de SNMP.
- ***snmpEngine Boots***, que es una cuenta del número de veces que una máquina de SNMP ha sido inicializado desde que el snmpEngineID se configuró por última vez.
- ***snmpEngineTime***, el cual, es el número de segundos desde que el contador snmpEngineBoots se incrementó la última vez.
  Cada máquina de SNMP siempre es autorizado con respecto a estos objetos en su propia entidad de SNMP. Es responsabilidad de una máquina SNMP no autorizada sincronizar con la máquina SNMP autorizada apropiadamente.

3.- Sincronización

El tiempo de sincronización requerido por una máquina de SNMP no autorizada, con el objeto de establecer comunicaciones auténticas ocurre cuando esta máquina ha obtenido ha obtenido una noción local de los valores de la maquina de SNMP autorizada. Estos valores deben estar dentro del Tiempo de Ventana de la Maquina de SNMP autorizada. Así la noción local de los valores de la maquina de SNMP autorizada deben guardarse libremente, sincronizado con los valores guardados de la maquina de SNMP autorizada.

4.- Mensaje de SNMP usando modelo de seguridad

El campo de mensajes msgSecurityParameters en SNMPv3, tiene un tipo de datos de cadena de octetos. Cuyo valor es la serialización de Tasa de Bit Erróneos (BER) de la secuencia ASN.1 siguiente:

```
USMSecurityParametersSyntax DEFINITIONS IMPLICIT TAGS ::=
        BEGIN
        UsmSecurityParameters ::=
        SEQUENCE {
-- global User-based security parameters
msgAuthoritativeEngineID OCTET STRING,
msgAuthoritativeEngine Boots INTEGER (0..2147483647),
msgAuthoritativeEngineTime INTEGER (0..2147483647),
msgUserName OCTET STRING (SIZE(0..32)),
```

-- authentication protocol specific parameters
msgAuthenticationParameters OCTET STRING,
-- privacy protocol specific parameters
msgPrivacyParameters OCTET STRING
}
END

5.- Servicios proporcionados por el Modelo de Seguridad User-based:
Los servicios son descritos como primitivos de un servicio abstracto de interfase, y las entradas y salidas son descritas como elementos de información abstracta cuando ellos pasan en estos servicios abstractos primitivos.

4.18 ELEMENTOS DE PROCEDIMIENTO

1.- Generación de mensaje SNMP saliente
Procedimiento seguido por una maquina de SNMP que genera un mensaje que contiene una operación de administración (como una solicitud, una respuesta, una notificación, o un reporte) por un usuario, con una particular securityLevel.
2.- Procesamiento de mensaje SNMP entrante
Procedimiento seguido por una maquina de SNMP cuando se recibe un mensaje que contiene una operación de administración por un usuario, con un securityLevel particular.

4.19 PROTOCOLOS DE AUTENTICACION

Como soporte a la integridad de datos, se requiere un compendio de algoritmo de mensajes. Un compendio se calcula encima de una parte apropiada de un mensaje y es incluido como parte del mensaje enviado al destinatario.

1.- HMAC-MD5-96
Es el primer protocolo de autenticación definido por el Modelo de Seguridad User-based, y es identificado a través de:
usmHMACMD5AuthProtocol
2.- HMAC-SHA-96
Este protocolo de autenticación es identificado por:
UsmHMAC-SHAAuthProtocol

PROTOCOLOS ENCRIPTAMIENTO

Se utiliza el Protocolo de Encriptación Simétrico CBC-DES, identificado por:

UsmDESPrivProtocol

- Para la confidencialidad de datos, se requiere un algoritmo de encriptación. Una parte apropiada del mensaje es encriptada antes de ser transmitido.
- Un valor confidencial en combinación con un valor *timeliness* es usado para crear el código de encriptación/desencriptación y el vector de inicialización. El valor confidencial es compartido por todas las máquinas de SNMP autorizadas para originar mensajes del usuario apropiado.

4.20 CONTROL DE ACCESO BASADO EN VISTAS (VACM)

El RFC 2575 describe el modelo de control de acceso basado en vistas para SNMP. Define los elementos de procedimiento para controlar el acceso a la información de administración. También incluye una MIB para administrar remotamente este modelo.

El VACM puede estar asociado simultáneamente dentro de un motor de implementación con múltiples modelos de procesamiento de mensajes y múltiples modelos de seguridad.

CAPITULO 5 ADMINISTRACION DE REDES ATM

5.1 INTRODUCCIÓN

La idea de integrar todos los servicios en una sola red viene desde hace tiempo, así como también se ha incrementado la demanda de aplicaciones multimedia que involucran procesamiento e intercambio de información de texto, audio, e imágenes. Aunado a esto se han desarrollado técnicas de conmutación de altas velocidades, medios rápidos como la fibra óptica, y nuevos protocolos han demostrado la factibilidad de crear redes de servicios integrados.

Existen dos tecnologías de "fast paquet" que dan soporte a tecnologías de banda ancha como son Frame relay y cell relay. Frame Relay es un protocolo de comunicaciones de datos de área amplia, para aplicaciones de datos tipo LAN principalmente, se basa en envíos por paquetes de tramas variables, posee estándares claros. Es una tecnología que se basa en la conmutación totalmente implementada en la capa de enlace de datos, medios de transmisión confiables y esta orientado a conexiones.

La tecnología Cell Relay utiliza celdas de tamaño fijo de 53 octetos usualmente de los cuales 5 son de encabezador y 48 de información de capas superiores. Esta estructura pose un tamaño adecuado para ser transmitida a intervalos regulares, lo cual es benéfico para aplicaciones tales como voz paquetizada, video o tráfico multimedia. Esta tecnología da soporte al Modo de Transferencia Asíncrono que tiene como principios básicos:

- las técnicas de transmisión y conmutación no están separadas
- los enlaces troncales y de acceso presentan un flujo constante de celdas, vacías y con información
- la transferencia de información por la red es esencialmente asíncrona con acceso aleatorio (la fuente de información puede o no accesar a la red) no hay posición fija en el tiempo para los paquetes de una fuente
- no hay recuperación de errores de transmisión por la capa ATM ocurriendo errores, puede pasar que se pierdan celdas
- no hay necesariamente una correspondencia entre las velocidades de la red de transporte de la fuente
- es una tecnología de conmutación de paquetes que soporta servicios múltiples y mezclados. Conmuta celdas individualmente
- presenta asignación del ancho de banda dinámico

- es proyectada para medios de transmisión digital de alto rendimiento (fibra óptica)
- presenta prioridad y calidad de servicio

5.2 MODELO B-ISDN

Una Red Digital de Servicios Integrados de Banda ancha (Broadband-Integrated Services Digital Network B-ISDN) tiene como función principal soportar un amplio rango de aplicaciones como voz, datos y video en la misma red. Un elemento clave de la integración de servicios para una red es proveerlos usando un número limitado de tipos de conexiones e interfaz multipropósito. B-ISDNs soporta conexiones conmutadas y no conmutadas así como la capacidad de transferir información en conmutación de circuitos y de paquetes, también brinda servicios orientados y no orientados a conexión. B-ISDNs provee características de servicio, mantenimiento y funciones de administración de redes.

El modelo de referencia de protocolo introduce el concepto de planos separados para la segregación de funciones de usuario, control y administración. El modelo de la arquitectura del protocolo B-ISDN se muestra en la figura 5.1. Este modelo consiste de un plano de usuario, uno de control y otro de administración.

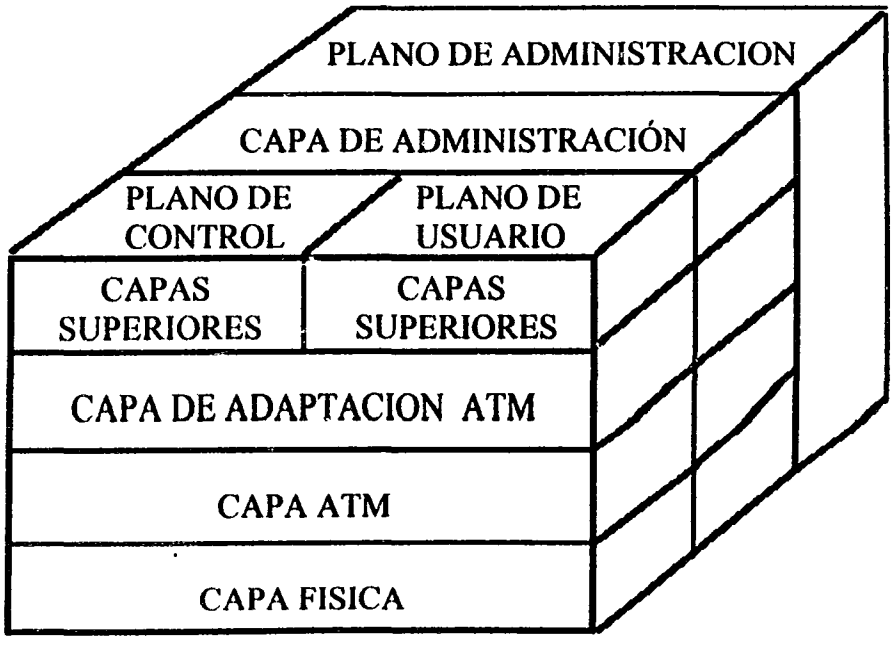


FIG. 5.1 MODELO DE LA ARQUITECTURA B-ISDN

PLANO DE USUARIO: Este plano provee una estructura de capas para el control del flujo de transferencia de información de usuario (control de flujo, y corrección de errores).

PLANO DE CONTROL: El plano de control tiene una estructura de capas, desempeña control de llamada y funciones de control de conexión. Intercambia las funciones de señalización necesarias para la realización de la llamada, habilitación de la conexión, funciones de supervisión y liberación.

PLANO DE ADMINISTRACION: Este plano provee dos tipos de funciones, llamadas funciones de administración de capa y funciones de administración de plano. La administración de plano provee la coordinación entre todos los planos. Esta administración no tiene una estructura de capas. La administración de capa realiza funciones de administración relacionadas con los recursos y parámetros residentes en sus entidades de capa de protocolo (metaseñalización es una función de administración de la capa ATM). La capa de administración maneja información de operación y mantenimiento específica de la capa concerniente. El modelo de la arquitectura en capas del protocolo puede ser descrito basándose en las funciones asociadas con cada capa.

5.2.1 CAPA FISICA

La capa física esta basada en DS3/E3 y SONET/SDH principalmente aunque en la practica se utilizan también velocidades menores.

5.2.2 CAPA ATM

La capa ATM provee la capacidad de transferencia de celdas. El campo de información de las celdas es transportado transparentemente por la capa ATM de la red. El encabezador de la celda y el campo de información cada uno consiste de un número fijo de octetos (5 y 48 octetos respectivamente). ATM es una técnica orientada a la conexión que puede ser usado para soportar servicios orientados y no orientados a la conexión. La señalización y la información de usuario son transportadas en canales virtuales separados. ATM esta diseñado para ofrecer capacidad de transferencia flexible común a todos los servicios.

5.2.3 CAPA DE ADAPTACION ATM (AAL)

Esta capa provee funciones dependientes del servicio a la capa ATM. La AAL soporta funciones de capas superiores de los planos de usuario y de control. La información es mapeada por AAL dentro de celdas ATM. En la transmisión final las unidades de información son reeensambladas de las celdas. La información especifica de AAL que debe ser intercambiada entre AALs es contenida en el campo de información de cada celda ATM. La AAL puede ser terminada en el equipo terminal (TE), adaptador de terminal (AT), terminal de red (NT2, NT1), terminación de intercambio (ET) y adaptador de red (NA). Funciones NA incluye esas funciones de adaptación que son necesarias entre ATM y no redes ATM. Las AALs son terminadas en la red para el servicio sin conexión, señalización, etc.

5.2.4 CAPAS SUPERIORES A AAL

Las capas arriba de AAL en el plano de control proveen control de llamada y control de la conexión. El plano de administración provee funciones de supervisión. Capas superiores a AAL en el plano de usuario son dependientes al servicio. Ejemplos de funciones provistas por esta capa incluyen funciones especificas de servicios de transporte interno.

5.3 MODO DE TRANSFERENCIA ASÍNCRONO (ATM)

El modo de transferencia asíncrono (ATM) es una tecnología basada en recomendaciones de la Unión Internacional de Telecomunicaciones para desarrollar B-ISDN a altas velocidades de transferencia de información de datos, voz y video; también es normalizada por el Instituto de Estándares Nacionales Americanos (ANSI) y por el Forum ATM. ATM es capaz de transferir voz, datos y video a través de redes publicas y privadas. ATM utiliza tecnología de fragmentación de información a altas velocidades en unidades llamadas celdas; es una tecnología de conmutación y multiplexaje basado en celdas. Cada celda consiste de 5 octetos de encabezador y 48 octetos de información como muestra la siguiente figura 5.2.

OCTETOS	5	48
	ENCABEZADOR	INFORMACION

FIG.5.2 FORMATO DE LA CELDA

En la siguiente figura podemos ver el funcionamiento de ATM.

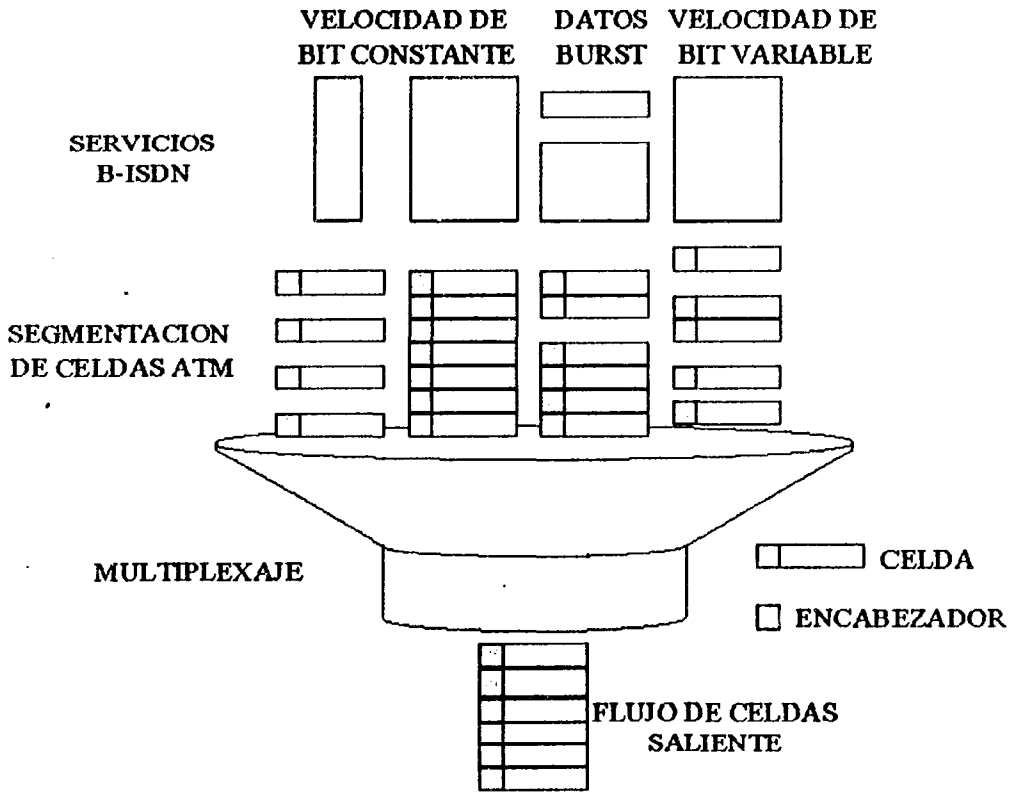


FIG.5.3 FUNCIONAMIENTO DE ATM

El flujo de celdas ATM inicia con señales de usuarios individuales estas pueden incluir servicios de velocidad constante (CBR) como un E1 por ejemplo, servicios de velocidad de bit variable (VBR) datos en ráfaga "burst" (trafico LAN). ATM fragmenta dichas señales en bloques de 48 octetos y les agrega un encabezador de 5 octetos para direccionamiento. ATM mezcla las celdas que toma de las señales individuales y las envía al switch ATM para que las multiplexe y puedan contender por ranuras de tiempo en el flujo de celdas saliente.

Las celdas transitan en las redes ATM atraves de dispositivos llamados switchs ATM, los cuales analizan la información contenida en el encabezador de la celda para realizar la conexión a la interfaz de salida para conectarse con el siguiente dispositivo que permitirá a la información llegar a su destino. ATM es una tecnología de conmutación de celdas y multiplexión, combina los beneficios de la conmutación de paquetes (retardo de transmisión constante y capacidad garantizada) con los de la conmutación de paquetes (flexibilidad y eficiencia para trafico intermitente).

5.4 CAPA FÍSICA

La capa física ATM controla la transmisión y recepción de bits en el medio físico. Mantiene los limites y paquetes de celdas en el tipo de trama adecuado para el medio físico usado. La capa física esta dividida en dos partes: la subcapa del medio físico y la subcapa de convergencia de transmisión. La subcapa del medio físico es responsable de enviar y recibir un continuo flujo de bits asociados con la información de sincronía entre el receptor y el transmisor. Debido a que incluye solo funciones dependiendo del medio físico, sus especificaciones dependen del medio físico usado. ATM puede usar un medio físico capaz de transportar celdas ATM. Algunos de los estándares que pueden transportar celdas ATM son PDH (Jerarquía Digital Plesiócrona), SONET (Red Optica Síncrona) y SDH (Jerarquía Digital Síncrona).

5.4.1 SUBCAPA DEPENDIENTE DEL MEDIO FISICO

La subcapa dependiente del medio físico (PMD) provee para la actual sincronización de la transmisión de bits y conectividad (define el medio físico de transmisión) sobre el medio físico. Se encarga del entramado sobre PDH, SONET y SDH teniendo sincronía al nivel de bit y provee codificación de línea, si es necesario conversión óptico-eléctrica.

5.4.1.1 PDH

La Jerarquía Digital Plesiócrona es el sistema de transmisión de redes publicas que se utilizan para transportar voz, también transportan datos y video sobre líneas dedicadas utilizando líneas de cobre, radioenlaces, fibra óptica con la ayuda de multiplexores y sistemas de interconexión digital. Hay variantes de PDH en el mundo las que se ilustran en la tabla siguiente.

VELOCIDAD MBPS	EUROPA	EEUU	JAPON
0.06	E0	DS0	
1.54		DS1	X
2.04	E1		
3.15		DS1C	
6.31		DS2	X
8.44	E2		
34.368	E3		
44.736		DS3	
139.264	E4		
274.176		DS4	100 MBPS
			400 MBPS

TABLA 5.1 VELOCIDADES PDH

El E1 es de uso europeo su trama consta de 32 ranuras de tiempo que se repiten cada 125 μs con una velocidad de cada ranura de tiempo de 64 Kbps. La ranura de tiempo TS0 tiene información de alineación de trama e información de alarmas así como un CRC-4. El TS16 tiene información de alineación de multitrama y señalización de linera de los TS1-15 y TS16-31. Las multitramas se forman con 16 tramas. El TS16 de la trama 0 de la multitrama se tiene la señal de alineación de multitrama y en las siguientes 15 tramas el TS16 sirve para señalización de línea como puede verse acontinuación.

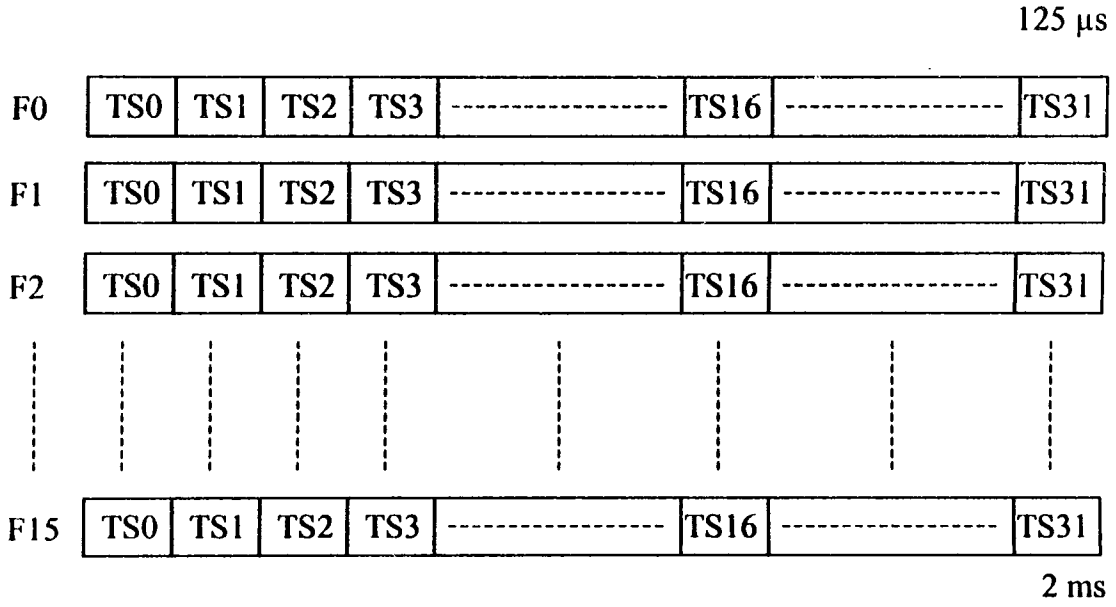


FIG.5.4 MULTITRAMA E1

La trama usada en norte América tiene 3ms de duración compuesta de 24 renglones de 193 bits cada uno. El primer bit de cada renglón, el bit F es usado para entramado y funciones de mantenimiento y operación como se muestra en la figura siguiente. Los bits D forman canales de 4 Kbps que es usado para llevar información de desempeño al otro extremo. El bit C es usado para CRC. El CRC que es usado es el CRC-6. Los bits F son usados para alineación de trama. La señal de alineación de trama es 001011.

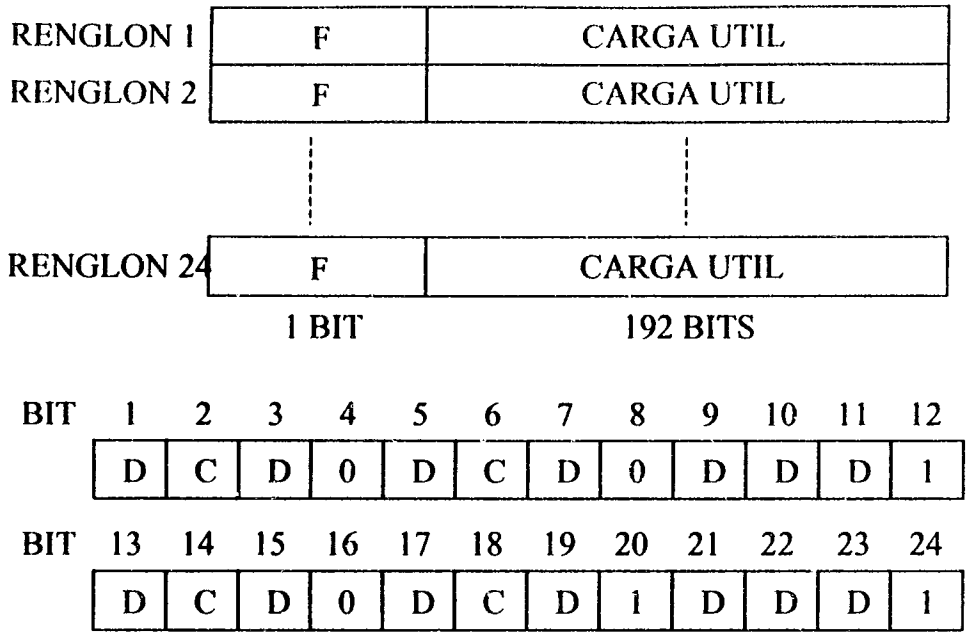


FIG. 5.5 PDH EN NORTE AMERICA

5.4.1.2 SONET

La especificación SONET define una jerarquía de velocidades de transferencia de datos digitales estandarizada, como lo muestra la tabla.

SONET DESIGNACION	SDH DESIGNACION	VELOCIDAD DE TRANSF. DE DATOS (MBPS)	VEL.DE TRANSF. INFORMACION
STS-1		51.84	50.112
STS-3	STM-1	155.52	150.336
STS-9	STM-3	466.56	451.008
STS-12	STM-4	622.08	601.344
STS-18	STM-6	933.12	902.016
STS-24	STM-8	1244.16	1202.688
STS-36	STM-12	1866.24	1804.032
STS-48	STM-16	2488.32	2405.376

TABLA 5.2 SEÑAL JERARQUIA SONET/SDH

El más bajo nivel referido como STS-1 (señal de transporte síncrono nivel 1), es de 51.84 Mbps. Esta velocidad puede ser usada para transportar una señal DS-3 o un grupo de señales de baja velocidad, tales como DS1, DS1C, DS2, E1, etc.

Múltiples señales STS-1 pueden ser combinadas para formar una señal N STS-1 que son mutuamente sincronizadas.

Para la jerarquía digital síncrona, la velocidad más baja es 155.52 Mbps, la cual es designada STM-1. Esta corresponde a SONET STS-3. La razón por la discrepancia es que STM-1 es la velocidad más baja que se puede acomodar una señal ITU-T de nivel 4(139.264 Mbps).

Las capacidades de SONET han sido mapeadas dentro de cuatro capas jerárquicas (figura 5.3.a):

5.4.1.2.1 PHOTONIC

Esta es la capa física, incluye una especificación del tipo de fibra óptica que puede ser usada y requerimientos de características de transmisión de láser tales como mínima potencia y dispersión y los requerimientos de sesitividad de los tranceivers.

5.4.1.2.2 SECCION

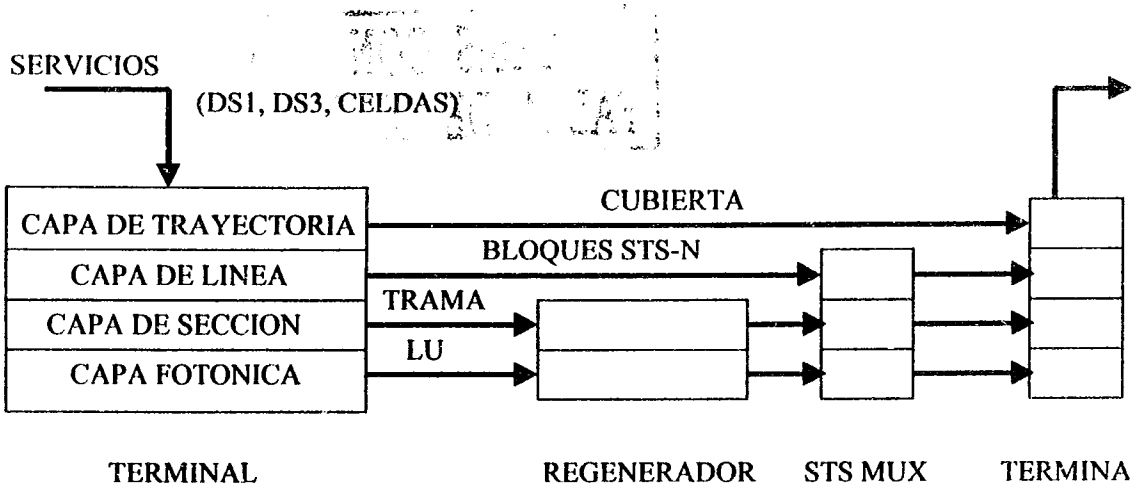
Esta capa crea las tramas básicas SONET, convierte señales eléctricas a señales ópticas y tiene algunas capacidades de monitoreo.

5.4.1.2.3 LINEA

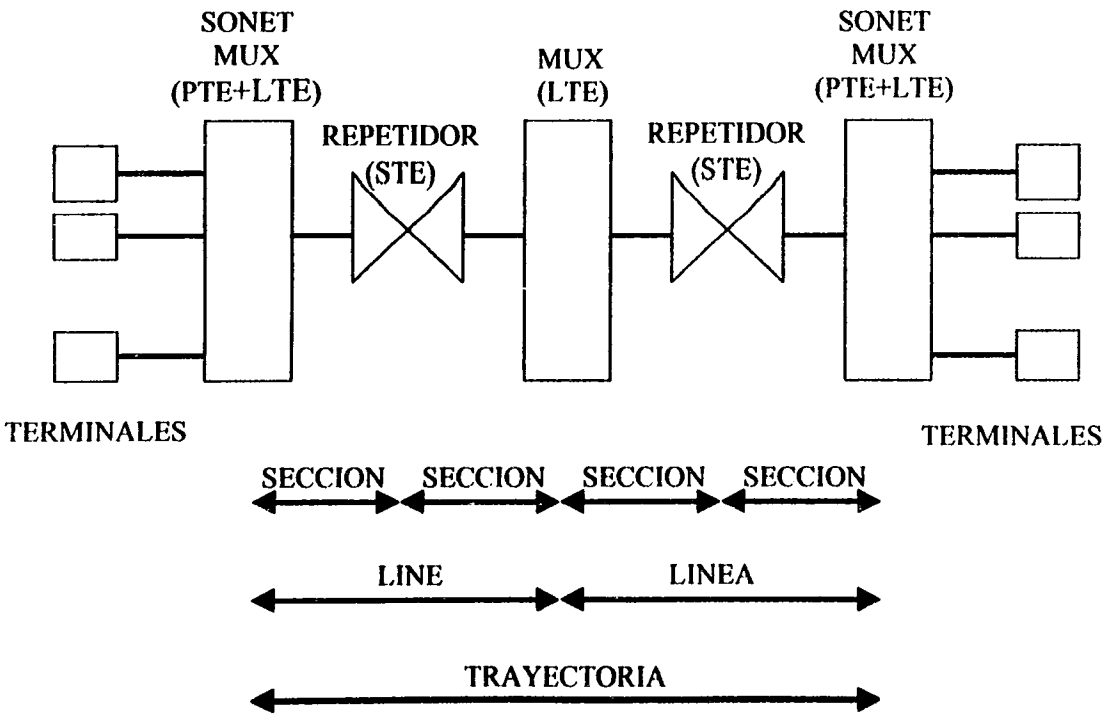
Esta capa es responsable de sincronizar, multiplexar los datos dentro de las tramas SONET, funciones de protección, mantenimiento y conmutación.

5.4.1.2.4 TRAYECTORIA

Esta capa es responsable de transportar punto a punto información a la velocidad de señalización apropiada.



A) JERARQUIA LOGICA

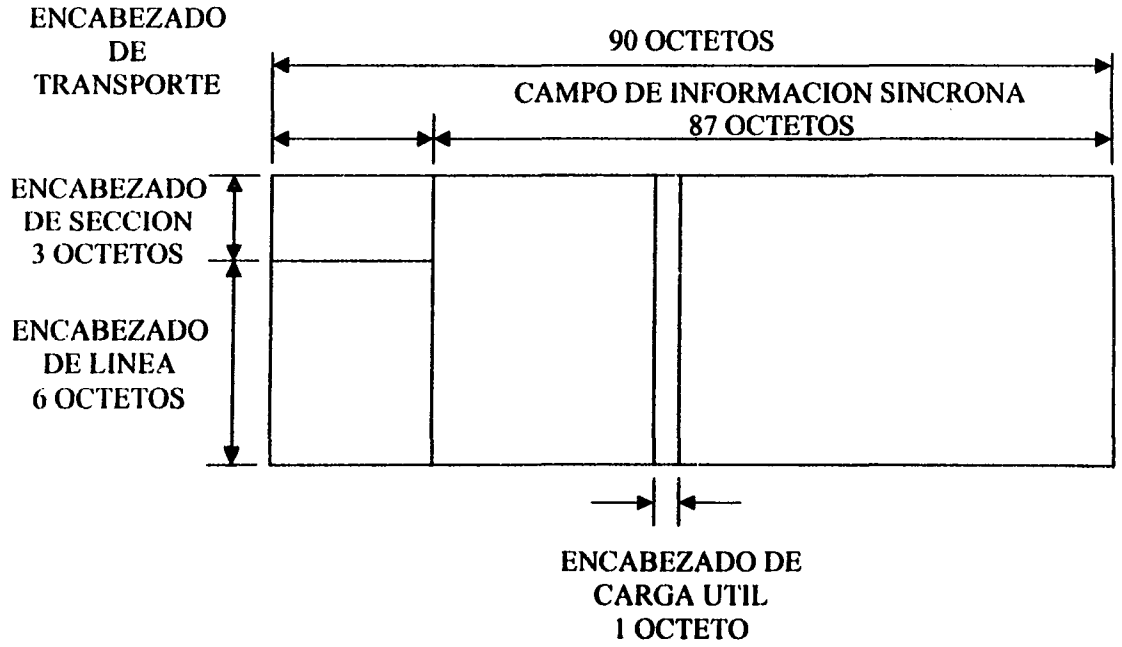


B) JERARQUIA FISICA

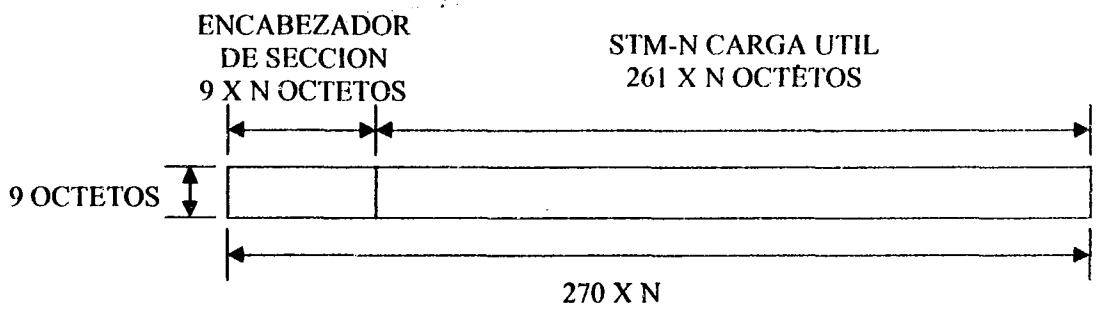
FIG 5.6 SISTEMA JERARQUICO

La figura 5.3.b muestra la realización física de las capas lógicas. Una sección es el bloque de construcción física básica y representa un sencillo cable que corre entre dos transmisor/receptores de fibra óptica. Para corridas cortas, el cable puede correr directamente entre dos unidades terminales. .Para distancias largas, repetidores que regeneren las señales son necesarios. El repetidor es un sencillo dispositivo que acepta un caudal digital de datos por un lado y regenera y repite cada bit por otro lado. La emisión de sincronización debe ser direccionada. Una línea es una secuencia de una o más secciones tal que la señal interna o estructura de canal de la señal permaneciendo constante. Puntos terminales y conmutadores/multiplexores intermedios que pueden agregar o dejar canales terminando una línea. Finalmente, una trayectoria conecta terminales finales, esto corresponde a un circuito punto a punto. Los datos son reensamblados en el comienzo de una trayectoria y no son accesados o modificados hasta que estén desensamblados en la otra terminal de la trayectoria.

El bloque de construcción básica SONET es la trama STS-1, la cual consiste de 810 octetos y es transmitida cada 125μs, para una taza de transferencia de datos de 51.84 Mbps. La trama lógicamente pude verse como una matriz de 9 filas por 90 octetos cada una, transmitiendo de izquierda a derecha y de arriba abajo.



A) FORMATO DE TRAMA STS-1



B) FORMATO STM-N

FIG. 5.7 FORMATO DE TRAMAS

Las primeras tres columnas (3 octetos por 9 filas = 27 octetos) son destinadas a encabezadores. Nueve octetos son dedicados al encabezador de sección y 18 octetos al encabezador de línea.

ENCABEZADOR DE SECCION	A1	A2	C1
	B1	E1	F1
	D1	D2	D3
ENCABEZADOR DE LINEA	H1	H2	H3
	B2	K1	K2
	D4	D5	D6
	D7	D8	D9
	D10	D11	D12
	Z1	Z2	E2

J1
A3
C2
G1
F2
H4
Z3
Z4
Z5

A) ENCABEZADO DE SECCION **B) ENCABEZADO DE TRAYECTORIA**

FIG 5.8 OCTETOS DE ENCABEZAMIENTO SONET STS-1

ENCABEZAMIENTO DE SECCION

A1, A2: bytes para alineación de trama = F6, 28 en hexadecimal, identifican inicio de trama.

C1: Identifica el número STS-1(1 o N) de cada STS-1 en un multiplexor STS-N (orden de aparición)

B1: Provee paridad sobre trama previa STS-N, monitoreo de errores de sección usando paridad par, es calculado sobre todos los bytes de la trama previa y el valor obtenido es colocado en este byte antes de mezclarse

E1: Nivel de sección orden de 64 Kbps PCM canal de comunicación de voz entre regeneradores y elementos de red

F1: Canal de 64 Kbps asignado para propósitos de usuario

D1-D3; Canal de comunicación a 192 Kbps de información de alarmas, mantenimiento, control, y administración entre secciones

ENCABEZAMIENTO DE LINEA

H1-H3: Bytes de apuntadores de alineación de trama y ajuste de frecuencia de la información.

B2: Provee paridad para monitoreo de errores en el nivel de línea calculado sobre todos los bits del encabezador de línea y la capacidad de información de la trama previa, el valor obtenido es colocado en este byte antes de mezclarse

K1, K2: Dos bytes para señalización de protección automática entre equipos de terminación de línea

D4-D12: Canal de comunicación de 576 Kbps de alarmas, mantenimiento, control, monitoreo y administración del nivel de línea

Z1, Z2: Reservado para uso futuro

E2: Canal de voz PCM de 64 Kbps para comunicaciones entre el equipo terminal de línea

ENACABEZADOR DE TRAYECTORIA

J1: Canal de 64 Kbps usado para enviar ráfagas de 64 bytes de tamaño fijo para que una terminal pueda verificar continuamente la integridad de una trayectoria, el contenido del mensaje es programado por el usuario

B3: Provee paridad al nivel de trayectoria para detección de errores de trayectoria, calculado sobre la SPE previa

C2: Etiqueta de señal de trayectoria STS para designar señales equipadas y no equipadas STS y para señales equipadas STS, el específico mapeo de la información STS que se necesita en la recepción terminal para interpretar la información

G1: Byte del estatus enviado de la terminal de trayectoria hacia el equipo originador para informar del estatus del equipo terminal y el desempeño de errores en la trayectoria

F2: Canal de 64 Kbps para uso de usuario

H4: Indicador de multitrama para información que necesita tramas más grandes que una trama STS; indicadores de multitrama son usados cuando se empaquetan canales de baja velocidad dentro del campo de información síncrona

Z3-Z5: Reservados para uso futuro

En redes de conmutación de circuitos muchos multiplexores y bancos de canales de las compañías telefónicas requieren multiplexar y remultiplezar para permitir el acceso a las piezas de información que son direccionadas a un nodo. SONET ofrece un estándar que tiene la capacidad de inserción y extracción para altas velocidades de transferencia de información. SONET hace uso de un conjunto de apuntadores que permiten localizar canales dentro del campo de información y la información en una trama, para que pueda ser accesada, insertada y removida con un simple ajuste de los apuntadores. La información del apuntador esta contenida dentro del encabezador de trayectoria que refiere a la estructura de multiplexaje de los canales contenidos en el campo de información. Un apuntador en el encabezador de línea proporciona la entrada al campo de información. El campo de información sincronía de una trama STS-1 puede estar desplazada con respecto a la trama. El actual campo de información (87 columnas x 9 filas) puede ocupar dos tramas. Los octetos H1 y H2 en el encabezador de línea indica el comienzo de la información.

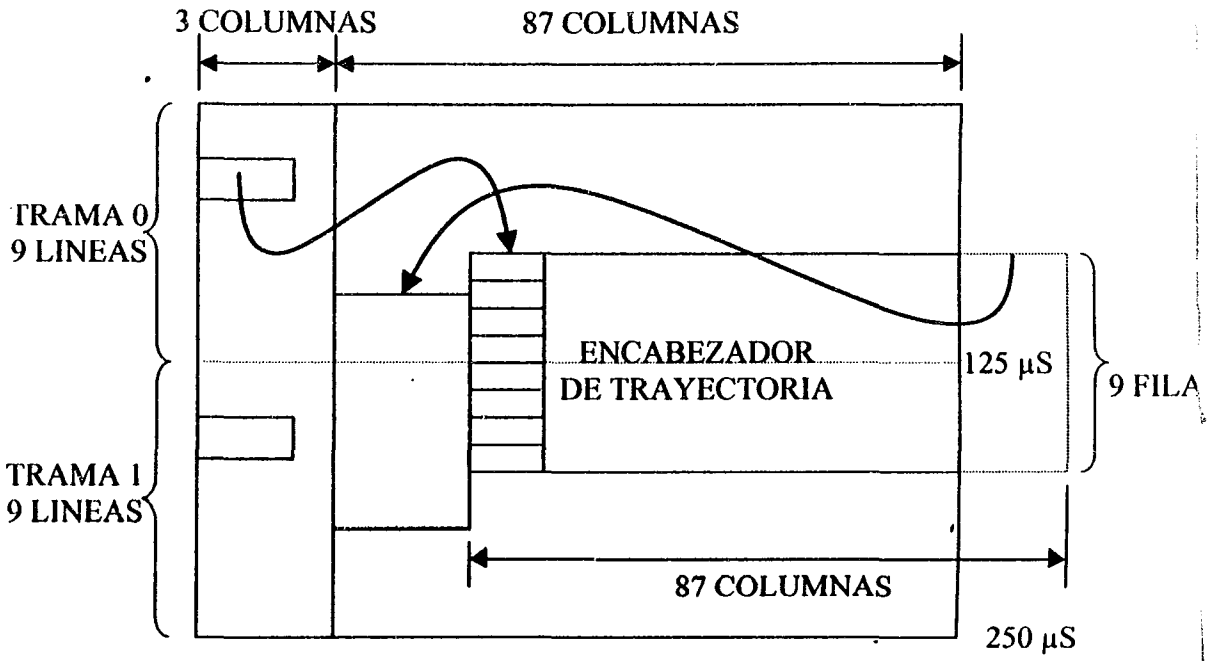
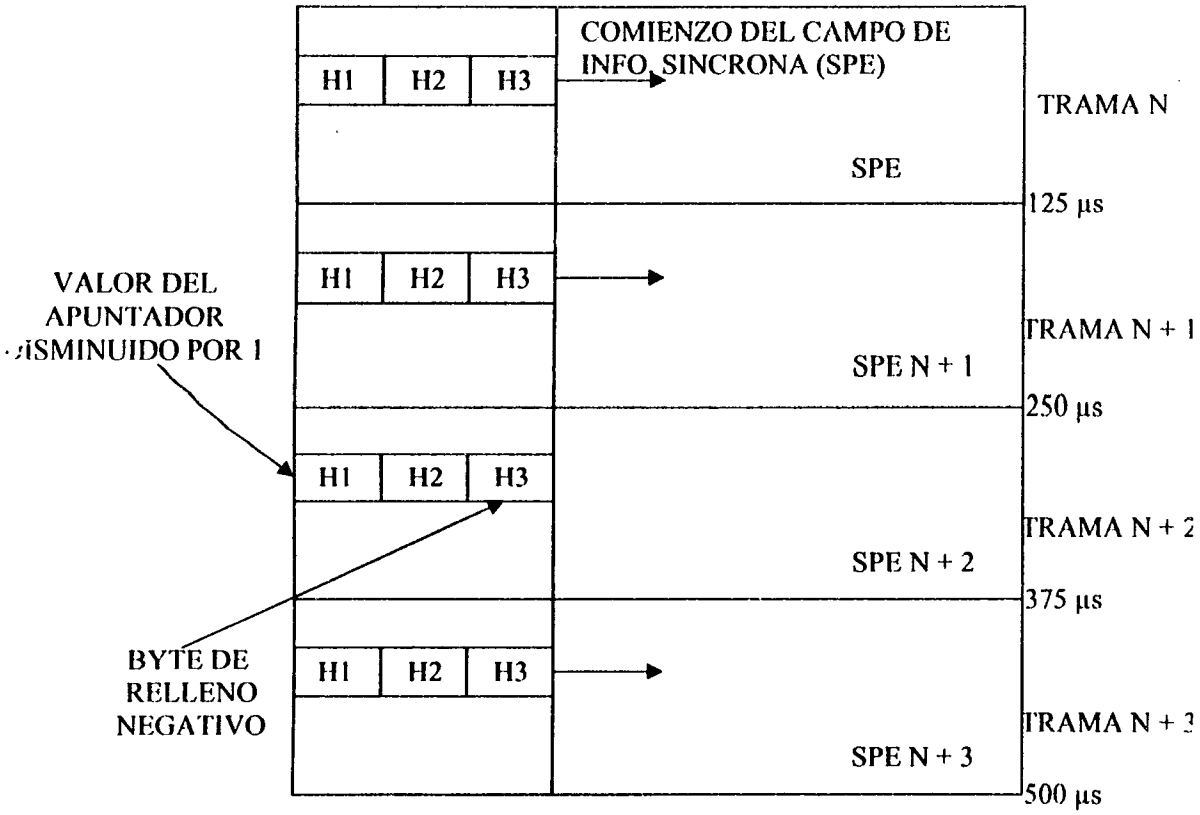


FIG.5.9 REPRESENTACION DE LA LOCALIZACION DEL CAMPO

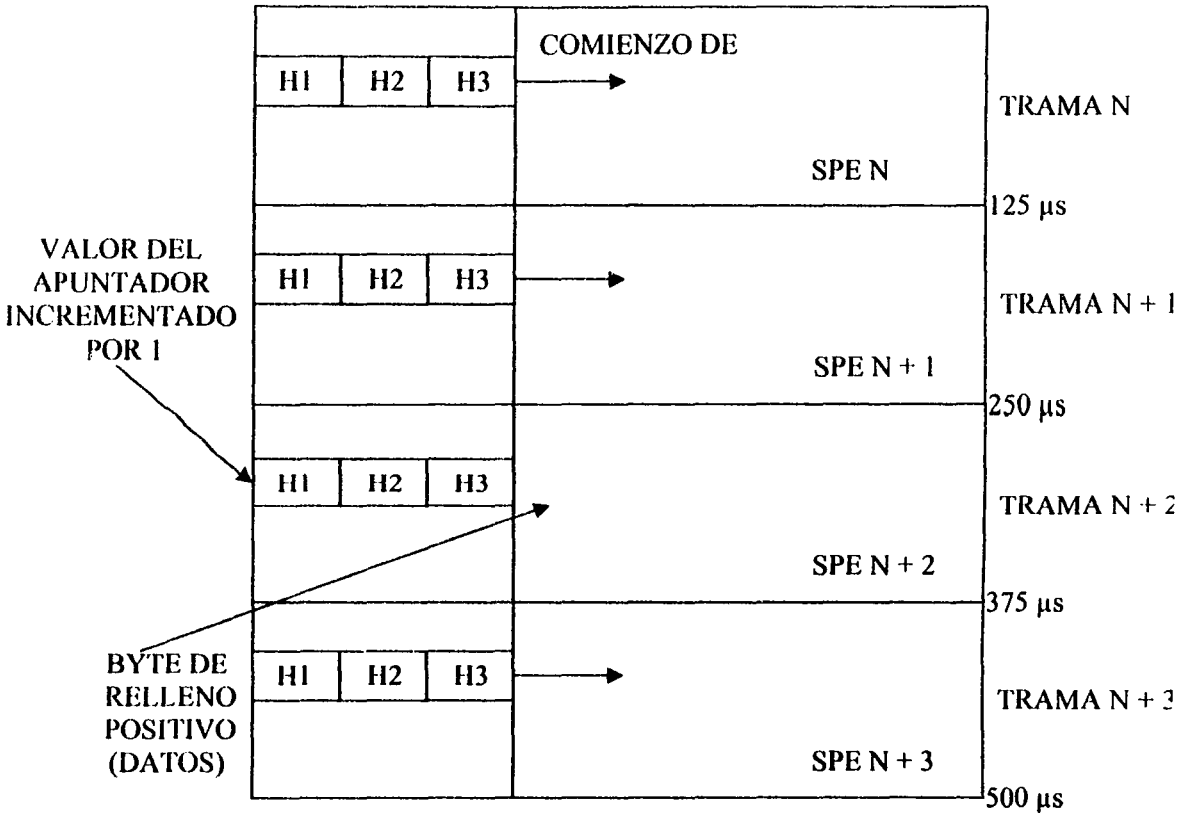
Debido a que hasta el mejor reloj atómico presenta variaciones en la señal de sincronía, cada nodo debe de recalcular el apuntador para alertar al siguiente nodo receptor de la exacta localización del comienzo de la información. Esto permite a la información deslizarse dentro de la trama STS-1, incrementando o disminuido el valor del apuntador a intervalos de un byte de posición.

Si la velocidad de la información es más alta que la de la trama STS, el apuntador es disminuido por un byte de posición así que la información siguiente comenzará un octeto después de la información más cercana. Para prevenir la perdida de un octeto de información esta es cubierta, el octeto H3 es usado para mantener el octeto extra para esa trama. Similarmente si la velocidad de la información es menor a la de la trama, la inserción de la

siguiente información es retrasada por un octeto. En este caso, el octeto en el campo de información síncrona que sigue al octeto H3 es dejado libre para permitir el movimiento de la información.



A) AJUSTE NEGATIVO DEL APUNTADOR



B) AJUSTE POSITIVO DEL APUNTADOR

FIG.5.10 AJUSTE DEL APUNTADOR

5.4.1.3 SDH

La capa física basada en SDH, el entramado impone una estructura en la corriente de celdas usando la trama STM-1 (STS-3). El campo de información podría ser compensado desde el comienzo de la trama como lo indica el apuntador en el encabezador de sección de la trama. El campo de información consiste de 9 octetos de una porción del encabezador de trayectoria y el resto contiene celdas ATM. La capacidad del campo de información (2,340 octetos) no es un múltiplo exacto de la longitud de la

celda (53 octetos), una celda puede rebasar él limite del campo de información.

El octeto H4 en el encabezador de trayectoria es colocado en el lado de envío para indicar la siguiente ocurrencia del limite de una celda. El valor de H4 indica el número de octetos para la primera celda de frontera que sigue al octeto H4. El rango permisible de valores es 0 a 52.

Puede ser usado para transportar información basada en ATM y STM (modo de transferencia síncrono), haciendo lo posible para utilizar una alta capacidad de transmisión basada en fibra para una variedad de conmutación de circuitos y aplicaciones dedicadas.

Una conexión especifica puede ser conmutación de circuitos usando un canal SDH. Por ejemplo una conexión transportando trafico de video a velocidad constante puede ser mapeada dentro de su propio campo de información de la señal STM-1, la cual puede ser conmutación de circuitos.

Usando técnicas de multiplexaje síncrono SDH, varios flujos ATM pueden ser combinados para construir interfaces para altas velocidades que soporten la capa ATM en un lugar particular. Por ejemplo cuatro flujos ATM separados a 155.52 Mbps cada uno pueden ser combinados para construir una interfaz de 622 Mbps (STM-4).

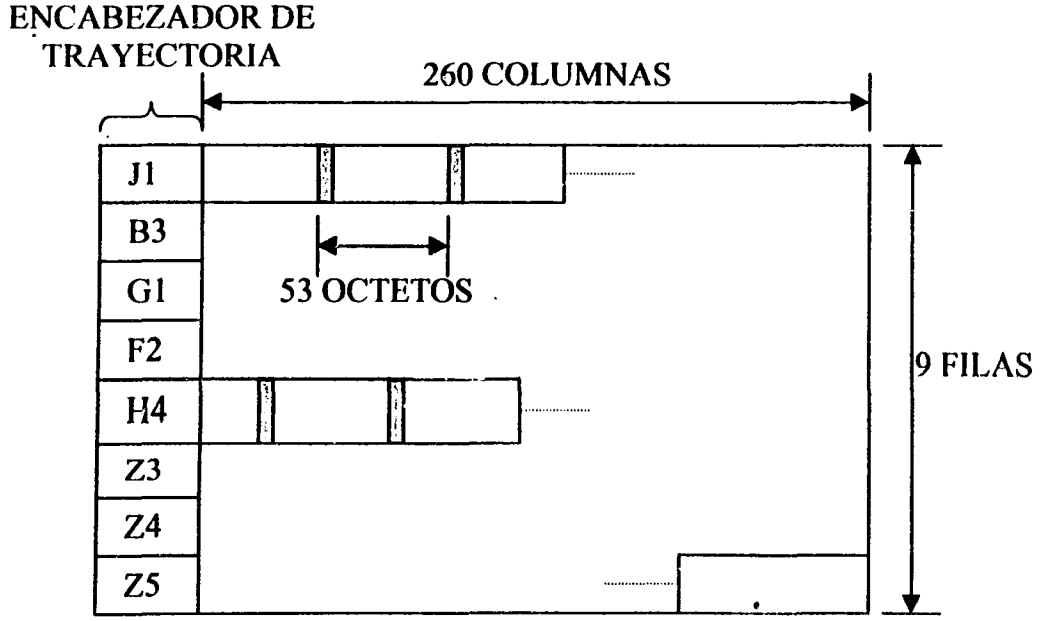


FIG.5.11 CAMPO DE INFORMACION STM-1 EN LA TRANSMISION DE CELDAS ATM BASADA EN SDH

5.4.2 SUBCAPA DE CONVERGENCIA DE TRANSMISION

La subcapa de convergencia de transmisión es responsable de las siguientes funciones:

5.4.3 GENERACION Y RECUPERACION DE TRANSMISION DE TRAMAS

La transmisión en la capa física consiste de tramas. Esta función es concerniente con la generación y mantenimiento de la apropiada estructura de la trama para una velocidad de datos dada. Su función es generar las tramas requeridas para que las celdas ATM puedan ser mapeadas. En el lado receptor la recuperación de la trama es ejecutada de tal forma que las celdas ATM puedan ser identificadas y recuperadas de la envoltura de la carga útil.

5.4.4 ADAPTACION DE LA TRANSMISION DE TRAMA

La información intercambiada en la capa ATM es un flujo de celdas. Esta subcapa es responsable de empaquetar esas celdas en tramas. Esto es para simplificar la recepción y transmisión de flujo de celdas dentro de la carga útil del sistema de transmisión.

5.4.5 DELINEACION DE CELDAS

Para propósitos de transmisión, el flujo de bits puede ser combinado. Esta capa es responsable de mantener los limites de la celda y así las celdas pueden ser recobradas en el flujo de celdas en el destino.

5.4.6 GENERACION DE SECUENCIA Y VERIFICACION DEL ENCABEZADOR DE CELDA

Cada encabezador de celda es protegido por un código de control de errores del encabezado (HEC). Esta subcapa es responsable de generar y checar el HEC. El código HEC es capaz de corregir errores de un solo bit en el encabezador. Este también es capaz de detectar muchos patrones de errores multibit. Si los errores son detectados en el encabezador, entonces la celda recibida es descartada. Dado que el encabezador le dice a la capa ATM que hacer con la celda es importante que no tenga errores; si así fuera podría ser entregada a un usuario erróneo. La subcapa también usa el HEC para localizar celdas cuando ellas son mapeadas directamente en el campo de

información de un sistema de transmisión TDM. El HEC no encontrará relación de los datos aleatorios de la carga útil de la celda cuando los 5 bytes que están siendo checados no son parte del encabezador. Así, esto puede ser usado para encontrar celdas en un flujo de bits recibidos. Una vez que varios encabezados de celda han sido localizados atraves de sus HEC, entonces la subcapa TC sabe que tiene que esperar 53 bytes de una celda. Este protocolo es llamado delineación de celdas basado en HEC.

5.4.7 DESACOPLAMIENTO DE LA VELOCIDAD DE CELDA

Esta incluye inserción y supresión de celdas libres en orden para adaptar la velocidad de celdas validas para la capacidad de información del sistema de transmisión que multiplexa múltiples ráfagas de celda VPI/VCI poniéndolas en una cola de espera, sí una ranura ATM no esta disponible inmediatamente. Si la cola esta vacía, debido a que no hay celdas para transmitir, para llenar la próxima ranura ATM de celda síncrona, entonces se inserta celdas desocupadas y distribuye las otras celdas asignadas a sus destinos.

5.5 CAPA ATM

Una red ATM consiste de un conjunto de switchs ATM interconectados punto-punto por medio de enlaces e interfaces ATM. Estos switchs soportan dos tipos de interfaces : interfaz usuario-red (UNI) e interfaz red-red (NNI) UNI conecta sistemas terminales (hosts, ruteadores, etc.) a un switch ATM. La interfaz NNI es un enlace físico o lógico a través del cual dos switchs ATM intercambian el protocolo NNI

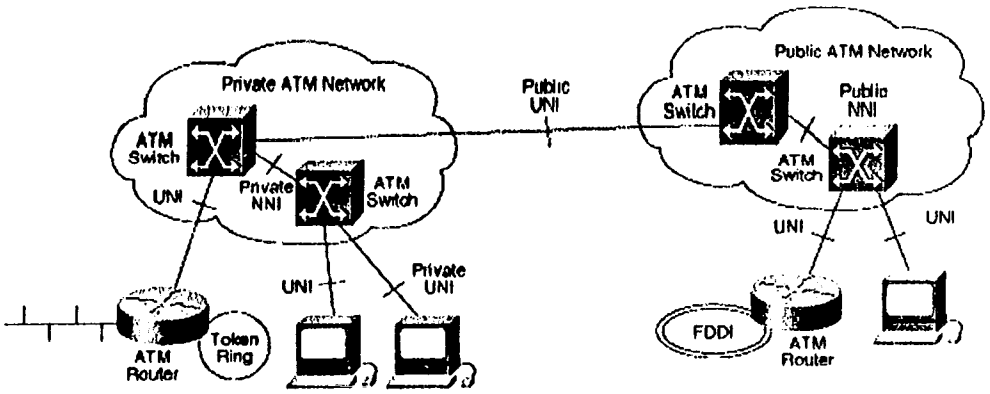


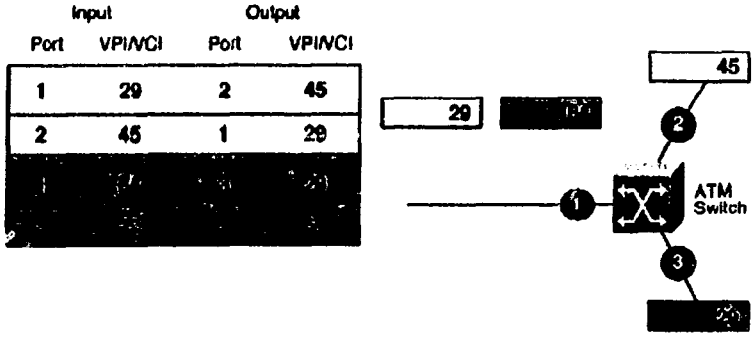
FIG. 5.12 INTERFACES DE RED ATM

Las redes ATM son orientadas a conexión, esto significa que un circuito virtual necesita ser establecido a través de la red ATM antes de transferir datos. Los circuitos en ATM son de dos tipos: trayectorias virtuales, identificadas por identificadores de trayectoria virtual (VPI); y canales virtuales (VCI),identificado por la combinación de un VPI y un identificador de canal virtual (VCI). Una trayectoria virtual es un grupo de canales virtuales, todos son conmutados transparentemente a través de la red ATM en base a un común VPI. Todos los VPI y VCI tienen solo significado a través de un particular enlace, y son reasociados en cada switch en la red. En operación normal switchs colocados todos en conexiones UNI en VPI = 0.

5.5.1 CONEXIONES VIRTUALES

El Identificador de Trayectoria virtual (VPI) y el Identificador de Canal Virtual (VCI) definen conexiones lógicas teniendo significado localmente. Consecuentemente, los valores podrían necesitar ser trasladados durante la conmutación.

La operación básica de un switch ATM es muy simple: recibe una celda a través de un enlace en un conocido valor VPI o VCI; se busca el valor de conexión en una tabla de translación para determinar el puerto de salida de la conexión y el nuevo valor VPI/VCI de la conexión en ese enlace; y transmite la celda en ese enlace con el correspondiente



identificador de conexión.

FIG. 5.13 OPERACIÓN DE SWITCH ATM

La manera en la cual esas tablas son configuradas determina dos tipos fundamentales de conexiones ATM:

CONEXIONES VIRTUALES PERMANENTES (PVC): Un PVC es una conexión establecida por un mecanismo externo, típicamente la administración de la red, en la cual un conjunto de switchs entre un sistema origen y un sistema destino ATM son programados en el correspondiente valor VPI/VCI. La señalización ATM puede facilitar el establecimiento de PVCs, pero, por definición, los PVCs siempre requieren de configuración manual.

Conexiones Virtuales Conmutadas (SVC): Un SVC es una conexión que se establece automáticamente por medio de un protocolo de señalización. SVCs no requieren de interacción manual para establecer PVCs. Todos los protocolos de capas superiores que operan sobre ATM primeramente usan SVCs.

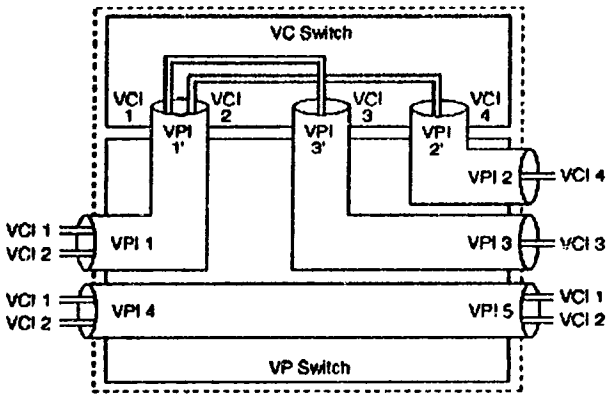


FIG. 5.14 CONMUTACION DE PVC Y SVC

GENERACION Y EXTRACION DEL ENCABEZADOR DE CELDA

En la transmisión un encabezador de celda es adicionado a los datos de usuario de AAL. Todos los campos son generados excepto el código HEC. También realiza la traslación de direcciones a un número de conexión lógico (VPI y VCI).

CONTROL DE FLUJO GENERICO

Esta función genera información de control de flujo de información y la deposita en el encabezado de la celda.

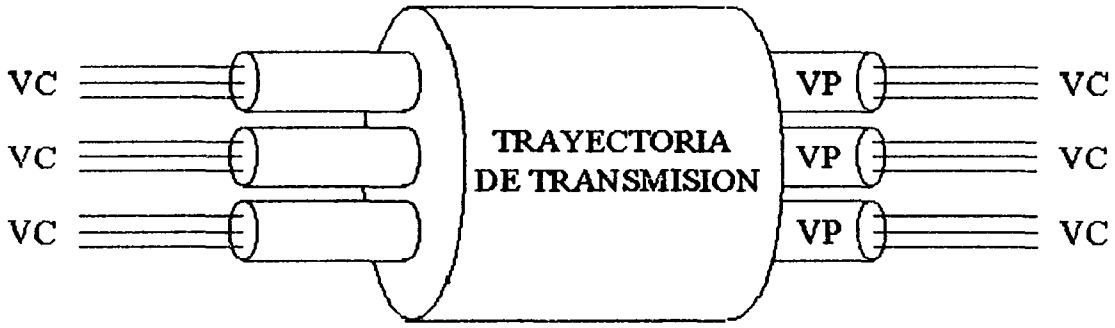
La capa ATM es responsable también de las siguientes funciones:

- construcción de celdas
- discriminación del tipo de carga útil de la celda

- interpretación de valores reservados predefinidos del encabezador de celda
- procesamiento de prioridad de perdida de celda
- soporte de múltiples clases de QoS
- indicación de congestión hacia delante explícito
- asignación de conexión y desconexión

Las conexiones lógicas en ATM son referidas a canales virtuales. Un canal virtual es activado entre dos usuarios finales atraves de la red, velocidad variable, flujo de celdas de tamaño fijo en modo full duplex son intercambiadas sobre la conexión. Los canales virtuales son también usado para intercambiar información de señalización de control entre el usuario y la red y para intercambiar información de ruteo y administración entre redes.

Para ATM una segunda capa ha sido definida como trayectoria virtual. Una trayectoria virtual es un conjunto de canales virtuales que tienen los mismos puntos terminales como se muestra a continuación.



VC = CANAL VIRTUAL
VP = TRAYECTORIA VIRTUAL

FIG. 5.15 RELACION ENTRE CONEXIONES

CANAL VIRTUAL (VC): Es un termino genérico para describir transporte unidireccional de celdas ATM asociadas por un común valor de identificador único.

ENLACE DE CANAL VIRTUAL: Significa transporte unidireccional de celdas entre un punto donde un valor VCI es asignado y otro donde ese valor es trasladado o terminado.

IDENTIFICADOR DE CANAL VIRTUAL (VCI): Identifica un enlace particular VC para un VPC dado.

CONEXIÓN DE CANAL VIRTUAL (VCC): Es una concatenación de enlaces VC que se extiende entre dos puntos donde la capa de adaptación es accesada. VCCs son propuestos para la transferencia de información entre usuarios, redes y usuario-red. La integridad de la secuencia de las celdas es preservada para celdas pertenecientes la mismo VCC.

TRAYECTORIA VIRTUAL: Termino genérico usado para describir transporte de celdas ATM pertenecientes a canales virtuales que son asociados a un común y único valor de identificador.

ENLACE DE TRAYECTORIA VIRTUAL: Un grupo de enlaces, identificados por un valor común de VPI, entre un punto donde un VPI es asignado y el punto donde ese valor es trasladado o terminado.

IDENTIFICADOR DE TRAYECTORIA VIRTUAL (VPI): Identifica un particular enlace VP.
CONEXIÓN DE TRAYECTORIA VIRTUAL (VPC): Una concatenación de enlaces que VP que se extiende entre el punto donde el VCI es asignado y el punto donde esos valores son trasladados o removidos.

Una conexión de canal virtual provee transferencia de celdas ATM punto a punto entre usuarios ATM. Los puntos terminales pueden ser usuarios o entidades de red. Cada punto terminal asocia un único VCI con cada VCC, los dos puntos terminales pueden emplear diferentes VCIs por el mismo VCC.
En adición en la red puede estar un número de puntos en los cuales los canales virtuales son conmutados, en esos puntos los VCIs son cambiados.

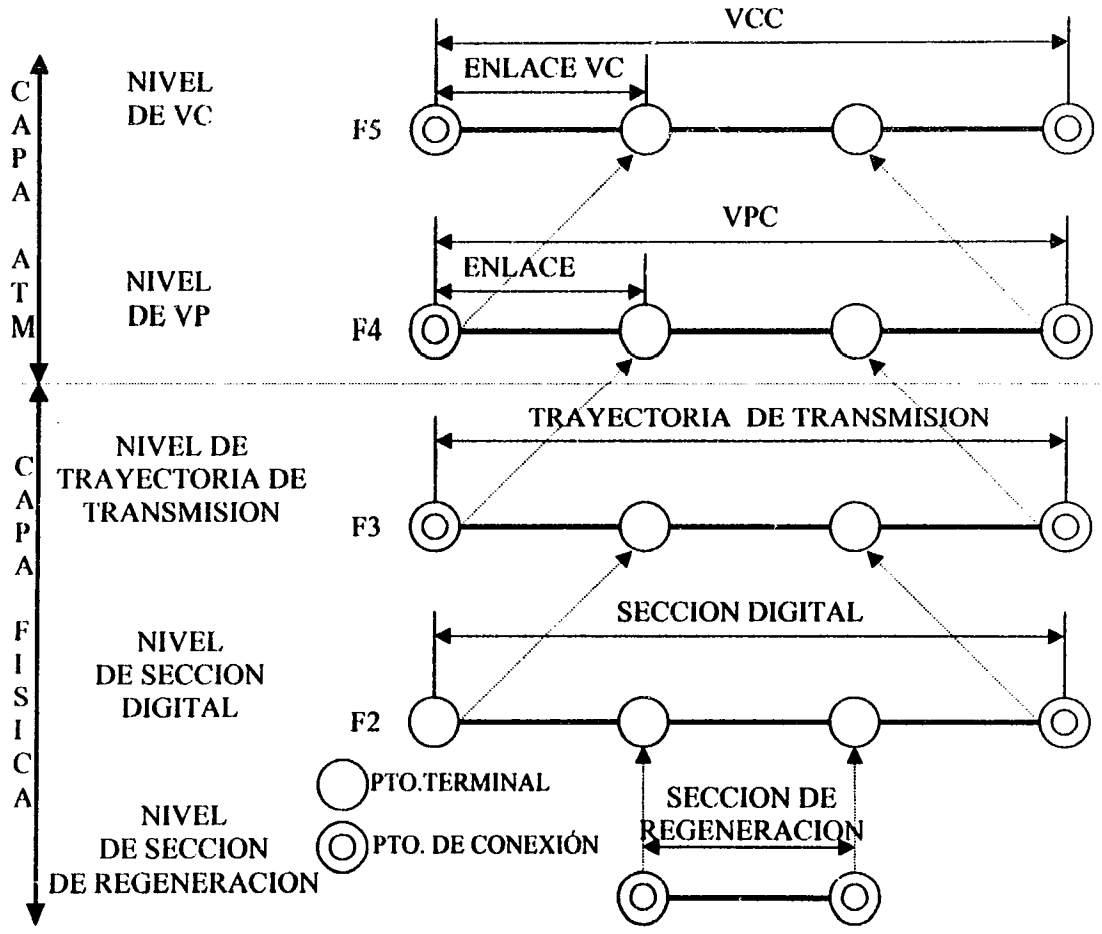
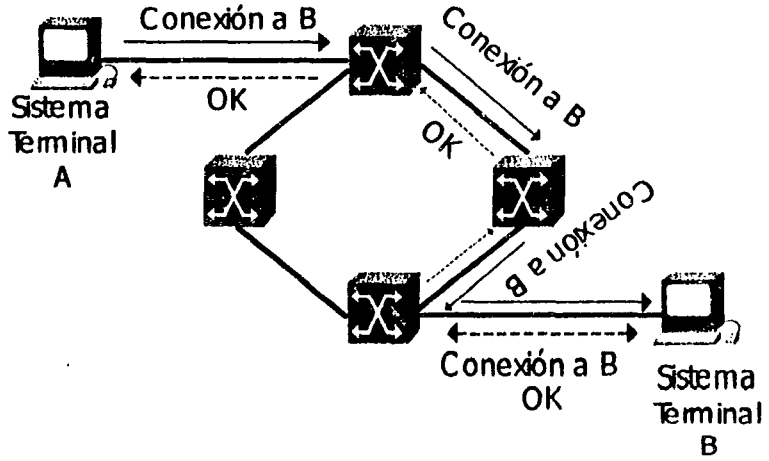


FIG. 5.16 RELACION JERARQUICA ENTRE CAPAS

La señalización ATM es comenzada por un sistema terminal ATM que desea establecer una conexión a través de una red ATM: paquetes de señalización son enviados en un canal virtual. Este canal virtual es reservado para tráfico de señalización y no se puede utilizar para enviar otro tipo de información. Todos los switchs son preconfigurados para recibir paquetes de señalización enviados a través de esta conexión y los pasa a un proceso de

señalización asociados al switch. En general todos los VCI a menores de 32 son reservados en cada VPI para propósitos de control: las conexiones de datos son localizadas en VCI fuera de este rango. La señalización es enrutada de switch a switch, hasta alcanzar el sistema terminal final. Los requerimientos de señalización son pasados entre la señalización o el proceso de control de llamada asociado con los switchs y esto es lo que hace



- Requerimiento de señalización
- Ruteo de conexión (establecimiento de la trayectoria)
- Rechazo/aceptación de la conexión
- Flujo de datos (a través de la misma trayectoria)

posible la conexión a través de los switchs. Después pueden cada uno aceptar y confirmar la petición de conexión, el flujo de datos fluye a través de la misma trayectoria.

FIG. 5.17 ESTABLECIMIENTO DE CONEXIÓN A TRAVÉS DE SEÑALIZACIÓN ATM (SVC)

Hay dos tipos de conexiones ATM fundamentales:
CONEXIONES PUNTO A PUNTO, las cuales conectan a dos sistemas terminal ATM de forma unidireccional o bidireccional.

CONEXIONES PUNTO MULTIPUNTO, las cuales conectan a un sistema terminal fuente (conocido como nodo raíz) a múltiples destinos terminales. Replicación de celdas es realizada en la red por los switchs ATM en el cual la conexión se deriva en varios trayectos. Tales conexiones son de manera

unidireccional , permitiendo al nodo raíz a todos sus destinos y no viceversa u otro en la misma conexión.

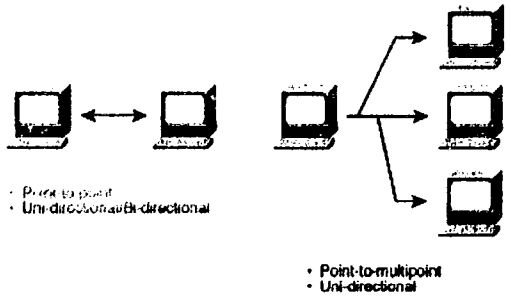


FIG. 5.18 TIPOS DE CONEXIONES ATM

5.5.2 DEFINICIÓN DE UNI, NNI (ESTRUCTURA DE CELDA)

Los grupos de estandarización ATM han definido dos formatos para el encabezador de celda. El formato para la interfaz usuario-red (UNI) y para la interfaz nodo-red (NNI). La especificación UNI define comunicación entre estaciones terminales ATM y switchs ATM en redes privadas ATM. El formato del encabezador de celda UNI es el siguiente:

	5 BYTES						48 BYTES
	GFC	VPI	VCI	PT	CLP	HEC	CAMPO DE INFORMACION
BITS	4	8	16	3	1	8	

FIG 5.19 CELDA UNI

GFC: Control de Flujo Genérico, provee funciones locales como identificar múltiples estaciones que comparten una sencilla interfaz ATM.

VPI: Identificador de Trayectoria Virtual, usado junto con el VCI para identificar el siguiente destino de una celda que pasa atraves de una serie de switchs ATM hacia su destino final

VCI: Identificador de Canal Virtual.

PT: Tipo de Carga útil, el primer bit indica cuando la celda contiene datos de usuario o de control. El segundo bit indica congestión y el tercero indica cuando la celda es la última en una serie de celdas que representan una trama sencilla. Un valor de 1 en el primer bit indica que esa celda transporta información de administración y mantenimiento.

CLP: Prioridad de perdida de celda es usada para poder descartar celdas en caso de congestión. Un valor de 0 indica una celda con mayor prioridad para no ser descartada a menos que no exista otra alternativa. Un valor de 1 indica que esa celda es candidata a ser descartada dentro de la red en caso de congestión. El usuario puede emplear este campo para información extra que puede ser insertada con un CLP = 1 y preguntando al destino sí la red no esta congestionada. La red puede poner este campo a 1 para varias celdas de datos que están en violación
de acuerdo al tráfico.

HEC: Control de errores en el encabezado:

- El transmisor calcula un código de error en base al encabezado de la trama a transmitir
- El transmisor inserta el código resultante en los datos a transmitir como un campo adicional
- El receptor calcula un código de error en base al encabezado recibido y usando el mismo algoritmo empleado por el transmisor ($x^8 + x^2 + x + 1$)
- El receptor compara este código resultante con el que viene en el campo HEC con lo que si es igual se descartan errores, de lo contrario se detecta una trama errónea y se descarta.

Esta información puede ser añadida en una etiqueta interna en cada celda. Esta etiqueta pude ser usada para propósitos de enrutamiento. La información de enrutamiento especifica como van a ser manejadas las celdas en el switch. El translador de encabezado puede generar información adicional (número de secuencia, timestamp, etc.) para incluirla en la etiqueta interna.

Los protocolos de señalización de ATM varían por el tipo de enlace, señalización UNI ATM es usada entre un sistema terminal ATM y un switch ATM a través de una UNI ATM; señalización NNI ATM es usada a través de enlaces NNI. El requerimiento de señalización UNI es transportada a través de UNI en la conexión por defecto: VPI = 0, VCI = 5.

Señalización ATM usa el método de establecimiento de conexión de un paso. Esto es, un requerimiento de señalización del sistema terminal fuente es propagada a través de la red hasta el destino final. El ruteo del requerimiento de conexión, y un subsecuente flujo de datos, es gobernada por los protocolos de ruteo de ATM. Tales protocolos de ruteo basan el requerimiento de conexión en la dirección destino, el tráfico y la calidad de servicio (QoS), parámetros requeridos por el sistema terminal fuente. El destino puede aceptar o rechazar la solicitud de conexión, sin embargo ya que el enrutamiento de la llamada es basado solo en los parámetros en el mensaje de solicitud de conexión inicial es limitada y el alcance de la negociación de los parámetros entre la fuente y el destino, pueden afectar el ruteo de la conexión.

Un número de tipos de mensajes son definidos en la especificación UNI 3.0/3.1, códigos de causa de error para las razones de falla de conexión, etc. Los elementos de datos usados en el protocolo de señalización , direcciones, en este caso, son transportados en elementos de información (IE) en los paquetes de señalización.

Un sistema fuente si desea establecer una conexión este deberá formular y enviar a la red un mensaje Setup, a través de su UNI, el cual contiene los parámetros de dirección destino, el tráfico deseado y la calidad de servicio. Este mensaje Setup es enviado, ingresa al switch, a través de UNI, el cual responde con un reconocimiento local (Call Proceeding). El switch ejecutará un proceso de enrutamiento ATM para propagar el requerimiento de señalización a través de la red, hasta que se llegue al switch que tiene conectado el sistema destino. Este switch deberá reenviar el

mensaje de Setup al sistema destino, a través de UNI. El destino decidirá si acepta o rechaza la solicitud de conexión; en el primer caso, se devuelve un mensaje de Connect, el cual regresa a través de la red, por la misma trayectoria en la que llego, al sistema origen. Una vez que el origen recibe el reconocimiento de conexión (Connect) ambos sistemas pueden transmitir datos a través de la conexión.. Si el destino rechaza la conexión, este envía un mensaje de Release al sistema origen, liberando la conexión. El mensaje Release es usado por cualquier sistema final o por la red para liberar una conexión establecida.

Un protocolo de señalización requiere de un esquema de direccionamiento que le permita identificar las fuentes y destinos de las conexiones. El foro ATM ha evaluado dos modelos fundamentales de direccionamiento diferentes.

Esos modelos difieren en la forma en la cual el protocolo de la capa ATM fue visto en relación con protocolos de capas existentes , en particular, protocolos de capa de red existentes tales como IP, IPX, etc. Esos protocolos tienen su propio esquema de direccionamiento y asociados protocolos de enrutamiento. Una alternativa era utilizar estos mismos esquemas de dirección dentro de redes ATM. Los puntos finales de la red ATM serían identificados por direccionamientos existentes de la capa de red (como direccionamiento IP) y las solicitudes de señalización serían transportados por ese direccionamiento. Existen protocolos de enrutamiento de la capa de red (tales como OSPF e IGRP) que serían utilizados para encaminar las solicitudes de señalización para la red ATM y estos podrían verse como paquetes no orientados a la conexión. Este modelo era conocido como el modelo del par, puesto que esencialmente trata la capa de ATM como par de las capas de red existentes.

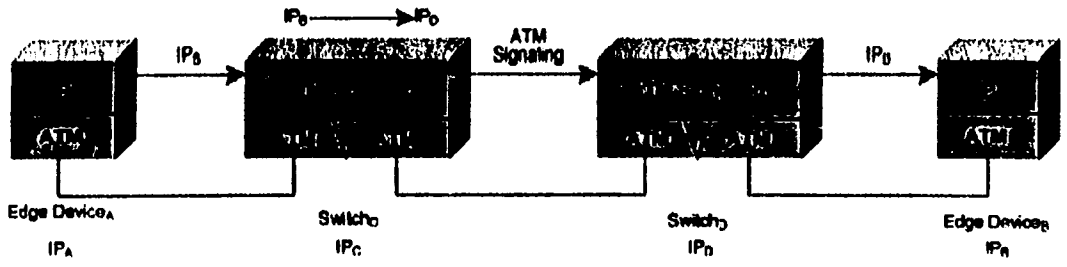


Fig. 5.21 Modelo par de direccionamiento ATM.

Un modelo alterno intentó independizar la capa de ATM de cualquier protocolo existente, definiendo para esta una nueva estructura de direccionamiento. Implícitamente, todos los protocolos existentes funcionarían sobre la red ATM. Por esta razón el modelo es conocido como modelo de subred o modelo overlay.. La operación de este modelo es la forma en la cual protocolos como IP operan sobre protocolos X.25 o líneas dial-up. En este modelo se requiere definir de la nueva estructura de direccionamiento y de protocolos de enrutamiento asociados a esto. Todos los sistemas ATM requieren de la asignación de direcciones ATM adicionalmente a el direccionamiento empleado en capas superiores. Ambos direccionamientos no estarían ligados. Por esta razón los protocolos que operan sobre ATM necesitan la resolución de direcciones ATM por algún protocolo de enrutamiento ATM y hacer la correspondencia de las direcciones de capas superiores (p.e. IP) con las direcciones ATM.

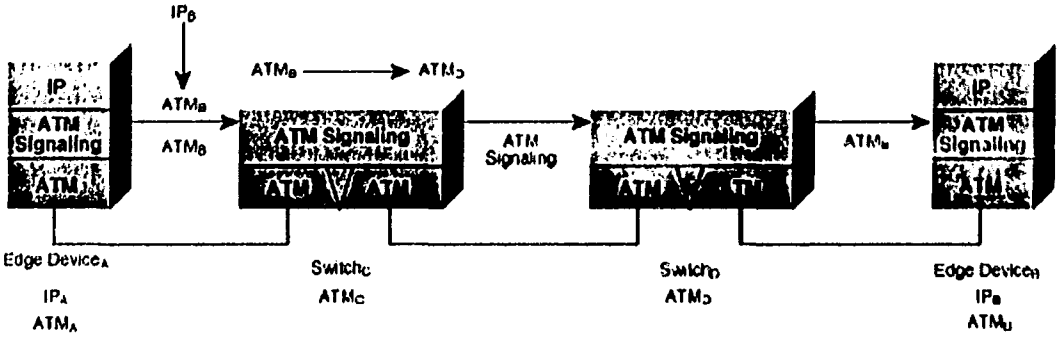


Fig. 5.22 Modelo overlay de direccionamiento ATM.

El foro ATM definió un formato de direcciones para las redes privadas basado en la sintaxis de la dirección punto de acceso a red OSI (NSAP) a pesar de que la dirección ATM tiene una estructura similar a NSAP no es lo mismo; Actualmente son utilizadas como direcciones NSAP, aunque son mejor descritas como direcciones de red privada ATM, o como identificadores de punto terminal ATM y no identifica NSAPs pero sí los puntos de conexión de acceso a la subred.

El formato de dirección ATM de 20 bytes esta diseñado para utilizarse en redes privadas ATM sin embargo el formato definido por la ITU-T (formato E.164) es de uso típico en las redes públicas. El foro ATM especificó un código NSAP para direcciones E.164. Este código fu utilizado

para codificar direcciones E.164 dentro de redes privadas pero puede también ser utilizado por algunas redes privadas. Este tipo de redes pueden basar su propio direccionamiento (formato NSAP) en direcciones E.164 de la UNI pública a la cual deben estar conectados y toman el prefijo de la dirección del número E.164 identificando nodos locales por los bits del orden más bajo o menos significativo.

Todos los formatos de direcciones ATM NSAP consisten de tres componentes: un identificador de formato y de área administrativa (autoridad) (AFI) el cual identifica el tipo y formato del identificador de dominio inicial (IDI); el IDI identifica la localización de la dirección y la autoridad administrativa y la parte de dominio específico (DSP) contiene información de ruteo actual. El protocolo Q.2931 define los campos de dirección origen y destino para las peticiones de señalización y también define los campos de subdirecciones para cada uno.

Existen tres formatos de direccionamiento ATM privado que se diferencian por la naturaleza de AFI e IDI:

- Formato NSAP de codificación E.164, en este caso el IDI es un número E.164

- Formato DCC: el IDI es un código de datos de país (DCC) ; identifica un país en particular, como se especifica en ISO 3166. Tales direcciones son administradas por el cuerpo nacional de miembros de ISO en cada país.

- Formato ICD: es un designador internacional de código (ICD); este es asignado por la autoridad de registros ISO 6523. Códigos ICD identifica particularmente organizaciones internacionales.

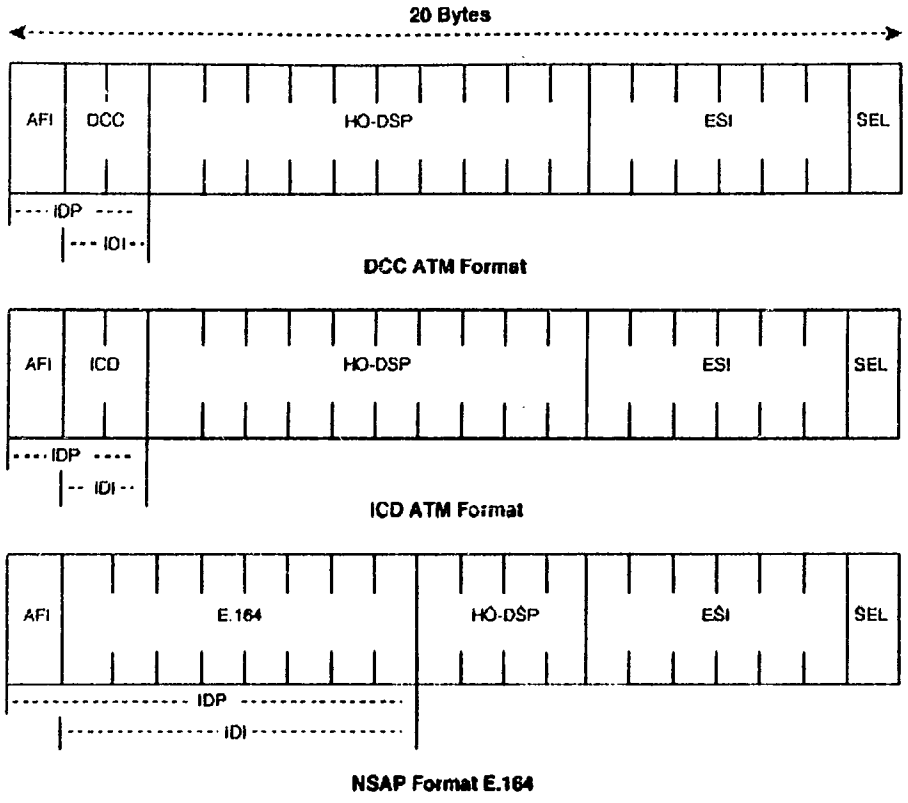


Fig. 5.243 Formato de direcciones de red privada ATM

El foro ATM recomienda que organizaciones o proveedores de servicio de red privada usen los formatos DCC o IDC para formar su propio plan de numeración. Organizaciones que deseen obtener direcciones ATM deben realizar el mismo mecanismo usado para obtener direcciones NSAP (por ejemplo, por medio de un organismo de administración local, para U.S. ANSI). Una vez obtenidas, esas direcciones pueden ser usadas para ambos formatos de dirección ATM y para direccionamiento NSAP.

En NSAPs, el DSP es subdividido en una jerarquía fija que consiste de un Dominio de Ruteo (RD), un identificador de Área (AREA) y un Identificador de Sistema Final (ESI). El foro ATM ha combinado los campos de RD y AREA dentro de un sencillo campo de DSP de alto orden (HO-DSP); el cual es usado para soporte flexible, direccionamiento multinivel jerárquico para protocolos de enrutamiento basados por prefijo.

La frontera para HO-DSP no es rígida, un rango de direcciones jerárquicas debe ser soportada, usando mascaras de prefijo, como subredes IP.

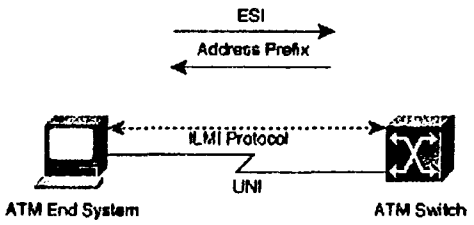


Fig. 5.24 Registro de direcciones usando el protocolo ILMI.

El campo ESI es especificado para representar una dirección MAC de 48 bits (administrado por IEEE). Las facilidades de soportar equipo LAN, hardware y dirección MAC, y de los protocolos tales del LAN como el IPX. Existe un octeto final Selector (SEL), este campo tiene significado en la multiplexación local en estaciones finales y no tiene significado en la red.

Para facilitar la administración y configuración de direcciones ATM en sistemas finales ATM a través de UNI, el foro ATM definió un mecanismo de registro de direcciones usando ILMI. Esto permite un sistema final ATM informar a un switch ATM a través de UNI, de su única dirección MAC y recibir el resto de las direcciones ATM de todos los nodos. Este mecanismo no solo facilita la autoconfiguración de dirección ATM de los nodos, sino también en el futuro, la autoconfiguración de otro tipo de información (como direcciones de capas superiores y servidores de direcciones). Específicamente, los nodos usarían una extensión del mecanismo de registro de dirección ILMI para informar a la red que soporta un particular grupo de direcciones. Como parte del registro el nodo también informa a la red del alcance deseado del registro, esto es, la extensión de la red para la cual la existencia del nodo multicast puede ser avisado (como parte de los protocolos de enrutamineto ATM). Este alcance es administrativo (edificio, sitio local o una empresa corporativa). La red debe mapear esta información a través de la política administrativa para la jerarquía propia del protocolo de enrutamiento ATM. Hasta que un nodo ha registrado su membresía en un grupo multicast, otros nodos pueden establecer conexiones a esos nodos. Si el nodo inicia la solicitud de conexión punto-multipunto al grupo de direcciones, la red conectará todos los nodos que están registrados en esa particular dirección ATM.

5.6.2 PROTOCOLO DE ENRUTAMIENTO ATM P-NNI.

Los protocolos para la Interfaz Nodo Red (NNI) son usados en ATM para enrutar solicitudes de señalización entre switchs ATM. Debido a que ATM es orientado a conexión , una solicitud de conexión necesita ser enrutada desde el nodo que la solicita a través de la red ATM hasta el nodo destino, muchos de esos paquetes son enrutados en un red de conmutación de paquetes. El foro ATM ha definido un protocolo para la Interfaz Nodo Red Privada (P-NNI). El propósito es definir protocolos NNI para uso en redes privadas ATM (o más específicamente, en redes que usen formato de direcciones ATM NSAP. Redes publicas que usen números E.164 para direccionamiento se interconectarán usando un diferente grupo de protocolos NNI basado en el protocolo de señalización ITU-T B-ISUP y el ITU-T MTP protocolo de enrutamiento de nivel 3. El protocolo P-NNI consiste de dos componentes: el primero es un protocolo de señalización P-NNI usado para liberar solicitudes de conexión ATM a la red, entre la UNI fuente y destino. La solicitud de señalización UNI es mapeada dentro de señalización NNI en el switch fuente. La señalización NNI es remapeada dentro de las señalización UNI en el switch destino. Los protocolos P-NNI operan entre los sistemas de conmutación ATM (los cuales pueden representar switchs o redes operando en una simple entidad P-NNI), los cuales están conectados por enlaces P-NNI. Los enlaces P-NNI pueden ser enlaces físicos o virtuales. Un ejemplo típico de un enlace virtual es una trayectoria virtual que conecta dos nodos. Todos los canales virtuales, incluyendo el que transporta la señalización P-NNI, será transportada transparentemente a través de switchs intermedios entre esos dos nodos en una trayectoria virtual, los dos nodos son adyacentes lógicamente en relación a los protocolos P-NNI.

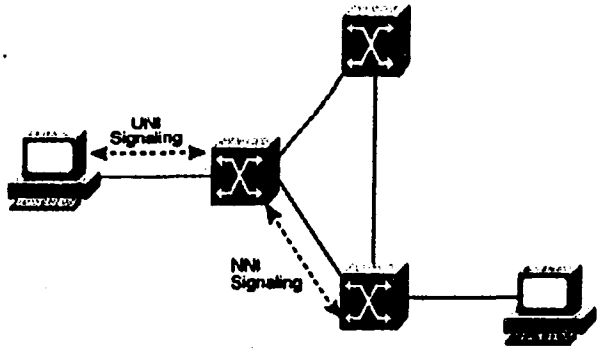


Fig 5.25 Señalización UNI y NNI.

El protocolo ILMI, definido primero para uso a través de enlaces UNI, es usado para enlaces NNI físicos y virtuales. El protocolo de señalización P-NNI es una extensión de señalización UNI e incorporados adicionalmente Elementos de Información (IE) como parámetros relacionados NNI como Listas de Transito Designado (DTL). La señalización P-NNI es transportada a través de enlaces NNI en el mismo canal virtual, VCI = 5, el cual es usado para señalización a través de UNI. El valor VPI depende de si el enlace NNI es físico o virtual.

El segundo componente del protocolo P-NNI es un protocolo de enrutamiento de circuito virtual. Este es usado para enrutar las solicitud de señalización hacia la red ATM. Esta es también la ruta en la cual la conexión ATM es establecida y por la cual fluirán los datos. La operación de enrutamiento de solicitudes de señalización a través de una red ATM, dada la naturaleza de ATM orientado a la conexión, es superficialmente similar al enrutamiento de paquetes no orientados a la conexión en una red existente de protocolos de capas superiores (como IP). El protocolo P-NNI tiene dos propósitos: ser escalable y soportar enrutamiento basado en la calidad de servicio (QoS). Una de las grandes ventajas de ATM es garantizar QoS en las conexiones. En una solicitud de conexión por parte de un nodo puede requerir un cierto QoS de la red y pueda ser garantizada durante todo el tiempo de la conexión. Estas conexiones son divididas por tipos de categorías de QoS ATM: CBR, VBR, ABR y UBR, dependiendo de la naturaleza del QoS deseado y de las características de los tipos de trafico esperado. Dependiendo del tipo de servicio ATM solicitado, la red esta expectante para liberar un particular QoS garantizado que esta especificado en el establecimiento de conexión (tal como taza de perdida de celda, retardo de celda y variación del retardo de celda). Para garantizar un QoS, los switchs ATM implementan una función denominada Control de Admisión a la Conexión (CAC). Una solicitud de conexión es recibida por el switch, el switch desempeña la función CAC. Esto es, basado en los parámetros y requerimientos de QoS de la conexión, el switch determina si el establecer la conexión viola el QoS garantizado (por ejemplo excesivas conexiones para el buffer del switch). El switch acepta la conexión solo si no son reportadas violaciones de las actuales garantías. CAC es una función local del switch es dependiente en la arquitectura del switch y de decisiones locales en la garantía del QoS.

El protocolo de enrutamiento de VC debe asegurar que una solicitud de conexión es enrutada por una trayectoria de salida hacia el destino y tiene una alta probabilidad de conocer el QoS requerido en el establecimiento de la conexión.

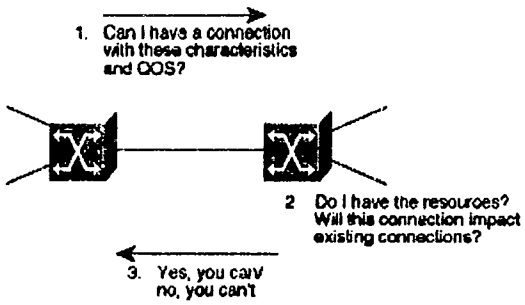


Fig. 5. 26 Control de Acceso a la Conexión.

Para hacer esto el protocolo usa un protocolo de enrutamiento de estado de la topología en la cual los nodos cubren el QoS y la información alcanza a todos los nodos obteniendo reconocimiento en la red y de los recursos de trafico disponible en la red. Esa información es pasada en los paquetes de estado de la topología P-NNI (PTSP), la cual contiene varios valores de tipo de tamaño (TLV) codificando elementos de estado de la topología P-NNI (PTSE). El protocolo P-NNI soporta un largo número de parámetros de estado de enlaces y nodos que son transmitidos a los nodos para indicar su actual estado a intervalos regulares, o cuando un particular evento a ocurrido.

Hay dos tipos de parámetros de enlaces: atributos de enlaces no adicionados usados para determinar cuando un nodo o enlace saben de una solicitud de QoS y adicionan métricas de enlace que se usan para determinar la selección de una trayectoria, consistente de un conjunto de enlaces y nodos concatenados (con métricas de enlace).

El conjunto de métricas de enlace son:

- Retardo máximo de transferencia de celdas (MCTD) por clase de trafico.
- Variación del retardo máximo de celdas (MCDV) por clase de trafico
- Taza máxima de perdida de celda (MCLR) para CLP=0, para las clases de trafico CBR y VBR.
- Peso administrativo: este es un valor dado por el administrador y es usado para indicar la preferencia de un enlace de red.

El conjunto de atributos de enlace son:

- Velocidad disponible de celda (ACR): una medida del ancho de banda disponible en celdas por segundo, por clase de trafico

- Margen de velocidad de celda (CRM): una medida de la diferencia entre el ancho de banda efectivo asignado por clase de trafico y la velocidad de celdas soportada; esta es una medida del margen de tolerancia a la velocidad soportada.
- Factor de varianza (VF): una medida relativa del margen CRM normalizado para la varianza del agregado de velocidades de celda en el enlace.

Todos los nodos de la red pueden obtener un estimado del estado actual de la red a través de PTSPs que contienen la información arriba descrita. El protocolo P-NNI avisa no solo las métricas de los enlaces. Típicamente PTSPs incluyen información bidireccional acerca del transito de nodos basado en las entradas y salidas de puerto y estado interno. Hay dos formas posibles de enrutamineto de conexión a través de la red: enrutamiento salto a salto y enrutamiento fuente. Enrutamiento salto a salto es usado por protocolos como IP o IPX, donde un paquete es enrutado en solo unos nodos dados a otro nodo (el siguiente salto) hasta el destino final. En el enrutamineto fuente, el nodo inicial en la trayectoria determina la ruta de entrada al destino final. El enrutamineto salto a salto es bueno para protocolos orientados a la no conexión ya que presenta el inconveniente de procesar pequeños paquetes en nodos intermedios. El protocolo P-NNI usa enrutamiento fuente. Es muy difícil hacer enrutamiento basado en QoS con protocolo salto a salto ya que cada nodo necesita desarrollar localmente CAC y evaluar el QoS a través de la red para determinar el siguiente salto. El enrutamiento salto a salto requiere un algoritmo de determinación de ruta estándar en cada salto para prevenir loops.

Un protocolo de enrutamiento basado en la fuente solo el primer nodo necesita determinar una trayectoria a través de la red, basado en el QoS requerido y el reconocimiento del estado de la red. El cual es obtenido por medio de PTSPs. Esto podría introducir una trayectoria completa en la solicitud de señalización para su enrutamineto hacia el destino final. Nodos intermedios desarrollarían un CAC antes de reenviar la solicitud. El CAC genérico (GCAC) es un algoritmo escogido para proveer una buena predicción de un algoritmo CAC de nodo especifico, requiriendo un número mínimo de métricas de estado de enlace. Usando el GCAC, un nodo presenta en un proceso de solicitud de conexión (el cual pasa su propio CAC) la solicitud como sigue:

- Todos los enlaces que no pueden proveer el ACR requerido y las que exceden el CLR requerido, son eliminados del conjunto de todas las posibles trayectorias usando GCAC.
- De este grupo reducido se procesa la trayectoria más corta para determinar la trayectoria o trayectorias posibles al destino.
- Esas trayectorias son seleccionadas en base a las métricas de enlace, tales como el retardo. Una de las trayectorias aceptables es escogida. Si múltiples trayectorias son encontradas el nodo puede realizar balanceo de carga.
- Una trayectoria es encontrada (note que solo una trayectoria es aceptable hacia el destino final, no la mejor trayectoria),el nodo construye una lista de transito designado (DTL) que describe la ruta completa al destino y la inserta dentro de la solicitud de señalización que se enviará a través de seta trayectoria.

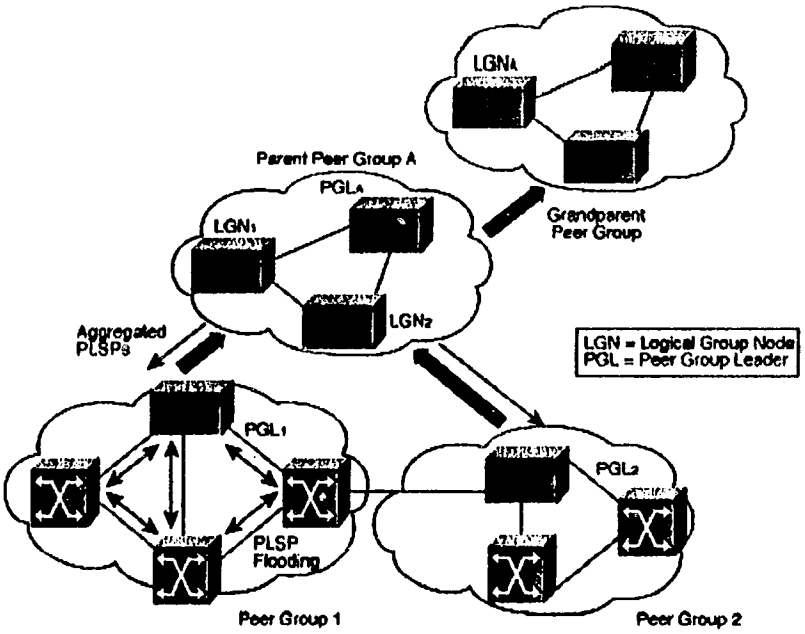
Cada nodo en la trayectoria desarrolla su propio CAC ya que su estado pude haber cambiado desde el ultimo aviso de su estado en el PTSP usado para el GCAC en el nodo fuente. Siempre existe la posibilidad que en una solicitud de conexión el CAC puede fallar en nodos intermedios. Esto ocurre con frecuencia en redes grandes con muchos niveles jerárquicos.

Adicionalmente para proporcionar QoS el foro ATM ha proporcionado un grupo de puntos para la escalabilidad del protocolo P-NNI. P-NNI esta pensado para redes pequeñas hasta en un futuro posiblemente una red ATM a nivel de Internet. Internet soporta muchos y diferentes protocolos de enrutamiento (protocolos de enrutamiento intradominio) como IGRP u OSPF, los cuales proporcionan escalabilidad a redes empresariales y protocolos de interdominio como BGP o IDRP. El foro ATM empezó hace algunos años a desarrollar un protocolo sencillo que pueda desarrollarse a todos los niveles en una red.

El protocolo P-NNI usa direcciones NSAP de 20 bytes para identificar niveles en la red jerárquica para soportar un número casi ilimitado de niveles; un máximo de 105 (el número de bits del byte 13 de alto orden de la dirección NSAP, excluyendo los campos ESI y SEL).

Para soportar esta jerarquia el modelo P-NNI define un modelo de red uniforme en cada nivel de la jerarquia. El modelo jerárquico P-NNI explica como opera cada nivel de la jerarquia, como múltiples dispositivos o nodos en un nivel pueden ser sumarizados dentro de un nivel superior y como información es intercambiada entre niveles. El modelo es recursivo y se extiende a otros niveles.

Cada nivel en la jerarquia consiste de un grupo de nodos lógicos interconectados por enlaces lógicos. En el más bajo nivel, cada nodo lógico representa un sistema switch fisico consistente de un switch físico o una red de switchs que internamente operan en un protocolo NNI propietario y soportan el protocolo P-NNI para interconectividad externa. En el nivel más bajo cada sistema switch debe ser asignado una única dirección NSAP. Nodos dentro de un nivel dado son agrupados dentro de un grupo conocido como grupo "par". La definición de grupo par es una colección de nodos los cuales tienen la misma base de datos topologica e intercambian información de estado de enlace con cada uno de los nodos del grupo. Los grupos par son organizados jerárquicamente y son asociados con un nivel padre mayor. En este grupo par padre cada grupo es representado por defecto como un



sencillo nodo lógico conocido como grupo de nodo lógico. En este grupo par padre, el grupo de nodo lógico actúa como un nodo normal, intercambiando PTSPs con los otros grupos par padres. Los grupos par representados por grupos de nodo lógico en un grupo par padre son conocidos como grupos par hijos de ese grupo.

Fig. 5.27 Modelo jerárquico de red P-NNI.

Normalmente los grupos par son identificados por direcciones privadas ATM prefijadas. En el más bajo nivel, por defecto todos los

sistemas finales obtienen sus direcciones de red, el (identificador ID) ID por defecto para los grupos par es a partir del byte 12 de orden más alto de la dirección NSAP del switch. Esto permite hasta 256 switchs en este nivel más bajo sin requerir configuración manual de IDs de grupo par de los switchs o configuración de sistemas finales.

En niveles mayores el ID por defecto para un grupo par es fijado en un ID de grupo par de nivel inferior. El ID de grupo par de un padre debe ser más corto que el del hijo, esto hace fácil la determinación la relación entre dos grupos par y previene loops de información de un grupo par jerárquico. El ID de grupo par comienza corto y se hace más grande a medida que va hacia niveles de mayor jerarquia.

Un grupo par es identificado por 22 bytes de identificador de nodo. En el nivel más bajo es en esencia el mismo que el sistema de direccionamiento del sistema de conmutación ATM. En niveles mayores el ID del nodo (el cual ahora identifica grupos de nodos lógicos) incluyendo dos indicadores de nivel que indican el nivel jerárquico del grupo par asociado y el grupo par hijo, más el ID del grupo par.

El protocolo P-NNI requiere que enlaces sean identificados ya que los enlaces entre grupos par necesitan ser identificados en PTSPs y pueden ser opcionalmente especificados en DTLs. Debido a que los atributos de enlace ATM pueden ser asimétricos (ya que conexiones pueden ser asimétricas), los enlaces son identificados por una combinación de ID de nodo transmitido y del ID localmente asignado. Los nodos intercambian esos Ids de puerto entre ellos mismos (usando el protocolo Hello) y hasta identificar enlaces particulares. En la practica, la identificación de enlaces es más o menos compleja, ya que múltiples enlaces físicos o virtuales necesitan estar conjuntados.

Cada grupo par elige un nodo sencillo en el grupo para desempeñar funciones de grupo de nodo lógico. Este nodo, conocido como grupo par líder (peer group leader PGL), es seleccionado a través de un mecanismo de elección y es basado en prioridad e ID del switch nodo. Cada PGL es identificado por una dirección ATM; si un nodo actúa como un PGL en múltiples niveles de grupos par, entonces este debe tener una única dirección ATM en cada uno de esos niveles. PGLs en cada grupo par tiene la responsabilidad de formular e intercambiar PTSPs en sus nodos pares en el grupo par padre para informar a esos nodos del alcance y atributos del grupo hijo. Similarmente, información recursiva obtenida por el PGL acerca del grupo par y de grupos del grupo padre son pasados al grupo hijo por el PGL. Los nodos hijo pueden entonces obtener conocimiento de toda a jerarquía de al red, en orden para construir todas las rutas fuente.

La información que es pasada del nivel mayor hasta el nivel más inferior. En el nivel más bajo tendrán toda la información de su propio grupo par, información adicional de su grupo padre, más información adicional de su grupo abuelo y en adelante. Para que PGLs se comuniquen con otros deben tener información del alcance y manera en la cual están interconectados entre sí.

Enlaces P-NNI (físicos o virtuales) están organizados en categorías en el modelo P-NNI. Horizontal o interior, enlaces conectan dos nodos en el mismo grupo par. Enlaces exteriores conectan nodos en un grupo par a otros nodos exteriores que no operan en el protocolo P-NNI. Enlaces de salida conectan dos nodos de frontera en dos diferentes grupos par, donde estos nodos de frontera son nodos en grupo par que tiene enlaces a nodos (vecinos foráneos) en otros grupos par. Los nodos descubren otros nodos primero por el protocolo P-NNI Hello en el cual los nodos intercambian paquetes hello a intervalos regulares entre sus nodos vecinos inmediatos.

Si dos vecinos descubren que están en el mismo grupo par, por comparación de sus Ids de grupo par, empiezan a enviar PTSPs a través del grupo par (por ejemplo a través de enlaces horizontales) para asegurar una rápida convergencia.

Los paquetes P-NNI hello y PTSPs son enviados en un canal virtual, VCI=18 con un VPI=0 para enlaces físicos y en correspondiente VPI para enlaces lógicos. Mecanismos como números de secuencia, reconocimientos y chequeo son usados para asegurar el alcance y el tiempo para liberar PTSPs.

Dos nodos de frontera podrían descubrir otros nodos, a través de enlaces de salida, por medio del protocolo Hello, el cual muestra que ambos nodos tienen diferente ID par. Dos nodos de frontera intercambian información ID a través de su enlace de salida para determinar el nivel más bajo en el cual los ancestros de los nodos es el mismo par (padre, abuelo, etc.). Cada nodo de frontera determina que el enlace de salida es un uplink hacia su grupo par ancestro. Los dos nodos de frontera intercambian información de métricas acerca del enlace de salida en el protocolo Hello, después avisan al uplink y sus características a sus respectivos grupos par a través de PTSPs.

En niveles superiores de la jerarquía P-NNI, múltiples enlaces deben ser adicionadas en grupo dentro de uplinks lógicos, sin embargo la información de acerca de la cobertura de uplinks lógicos y sus enlaces de salida que lo constituyen deben ser anunciados a esos nodos para poder hacer el mapa de un grupo lógico inter-par dentro de un enlace físico.

Nodos de frontera intercambian información acerca de PGLs de sus propios grupos par. Esto permite a los PGLs de grupos que descubren que están dentro del mismo grupo par padre para establecer conexiones a otros, a través de uplinks identificados y empiezan el intercambio de sus propios hellos y PTSPs. Entonces descubren la existencia de niveles de grupo par mayores hasta que todos los nodos descubran su entrada de jerarquía de red. A través de PTSPs, se envía información resumida de alcance y uplink, los PGLs descubren el estado total de la red.

Hasta que la información del estado total de la red es obtenida por todos los nodos, se puede entonces hacer uso de esta información para enrutar la solicitud de señalización. Cuando una solicitud de señalización es recibida por medio de UNI el switch debe usar un algoritmo de ruta corta, para determinar uno o más trayectorias que conectan el nodo fuente al destino deseado. Este algoritmo debe crear jerárquicamente una ruta fuente, esto es, un conjunto de DTLs, los cuales tendrán: trayectorias detalladas dentro del grupo par del nodo fuente; trayectorias menos detalladas dentro del grupo par padre y en menor detalle en niveles mayores de grupos pares, terminando en le nivel más bajo de grupo par, el cual es antecesor de los nodos fuente y destino.

Esos DTLs están contenidos dentro de un grupo dentro de la solicitud de señalización de P-NNI donde cada DTL contiene los elementos de trayectoria de un nivel en la jerarquia. Esto comprende una lista de nodos y opcionalmente, IDs de enlaces, agrupados con un apuntador que indica cual elemento en la lista es el siguiente a procesar. En un grupo par dado, ese DTL del grupo par es procesado por nodos hasta que alcance el nodo de frontera hacia el siguiente grupo par en la trayectoria. En este punto, el DTL de ese grupo par expira ya que el elemento final en ese DTL es el ID del nodo de frontera. El nodo de frontera remueve ese DTL, notar que el siguiente punto DTL al grupo par vecino (posiblemente en un diferente nivel dentro de la jerarquia) y reenviado a su nodo par de frontera dentro de su grupo par vecino.

Una vez que la solicitud llega al nodo de frontera dentro de su grupo par vecino, ese nodo descubre que la solicitud debe ser enrutada a través del grupo par del nodo. El DTL original solo ha adicionado información de su grupo par vecino. El nodo de frontera crea nuevos DTLs, describiendo ahora como enrutar la solicitud a través de su grupo par el cual desarrolla una función similar para el siguiente grupo par en la trayectoria y así adelante hasta que el grupo par destino sea alcanzado.

En este punto, el nodo de frontera construye un DTL que enrute la solicitud a el switch en el cual el sistema final esta conectado. El switch final (el DTL terminal) remapea la solicitud dentro de señalización UNI y la reenvía a través del indicado enlace UNI. DTLs son solo creados por el nodo fuente y por los nodos de frontera. Otros nodos intermedios solo procesan DTLs y mueven el apuntador DTL reenviando y pasando la solicitud al siguiente nodo en la trayectoria.

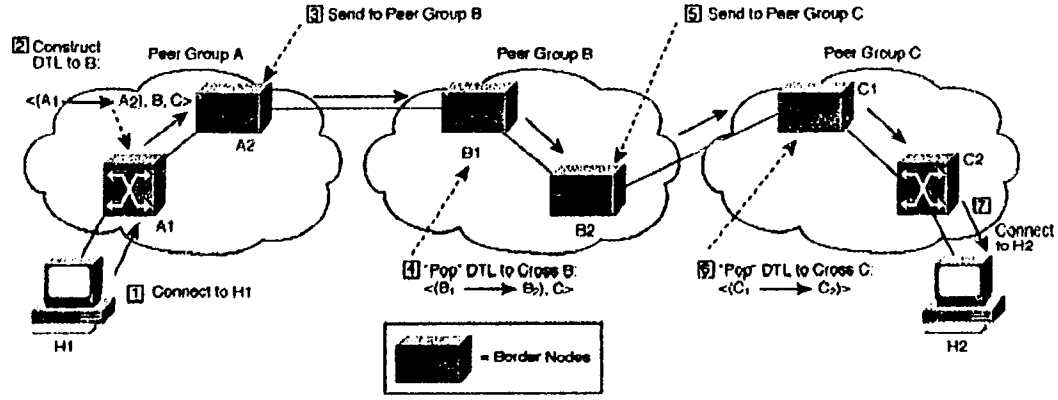


Fig. 5.28 Proceso DTL en el establecimiento de una conexión.

El protocolo P-NNI soporta establecimiento de conexiones virtuales permanentes suaves. Significa el establecimiento de PVCs y trayectorias virtuales permanentes (permanent virtual path PVP) usando procedimientos P-NNI. Por medio de la administración de la red, un PVC o PVP es establecido solo a través de la UNI fuente y destino, pero no a través de la red. Entonces, a través de la administración de la red el primer switch (ingreso al switch) es instruido para enrutar una conexión a través de la red hacia el destino (salida del switch) usando P-NNI. Esto es logrado con el proceso normal de P-NNI, en la señalización se instruye al switch destino para terminar la conexión en el PVC/PVP establecido, más que reenviar una solicitud de señalización UNI al sistema destino.

Dada la necesidad de usar conexiones permanentes (ya que los sistemas finales no soportan señalización, por ejemplo), un establecimiento de una conexión suave (totalmente no permanente) es mucho más conveniente y posible forma de establecer conexiones ...ás que us... lo

configuración salto a salto. Esto también permite establecer conexiones con un especifico QoS usando un proceso P-NNI.

Actualmente proveedores de servicio de redes publicas ATM están considerando el desarrollo de redes públicas ATM, el cual ofrece interconexión de servicio ATM a través de sistemas UNI públicos o privados. En primera instancia, es como que ese servicio ofrecido a través de seas redes no sería un servicio puramente ATM, pero sería en variantes basadas en ATM de las tecnologías WAN como Frame Relay o Servicio de Datos Multimegabit Conmutados (Switched Multimegabit Data Service SMDS).

El primer problema a encarar para la interconexión es que, para varias técnicas, administraciones y razones de tarificación, es que la mayoría de esos servicios públicos ATM iniciales no soportan conexiones virtuales conmutadas (SVCs) a través de UNI publica. Una forma de lograr esto es con el uso de túneles de Trayectorias Virtuales Permanentes (Permanent Virtual Path PVP). En este método, dos redes privadas ATM son enlazadas por medio de la red publica usando una trayectoria virtual en la cual la red publica transparentemente agrupa las colecciones de canales virtuales en el VP entre los dos sitios.

Las solicitudes de señalización de una red privada a la UNI publica podría entonces ser relacionada dentro del apropiado canal virtual (VCI=5) en el VP del usual canal virtual (VPI=0, VCI=5) por la salida del switch de la red privada y transportadas transparentemente a través de la entrada del switch de la otra red privada. En este punto, este switch podría asociar la solicitud dentro del canal usualmente usado y propagarlo a través de la red destino. Nótese que si las redes están corriendo protocolos P-NNI , entonces estos PVP a través de la red publica podrían ser tratadas como un enlace virtual. Por esta razón el enlace entre las redes publica y privada podría simultáneamente ser una UNI publica y un enlace virtual P-NNI. El cambio de túnel PVP se requiere operación normal de nodo, los procedimientos deben ser usados para ingresar y salir de switchs para alojar canales particulares dentro de PVP para una solicitud de conexión particular y de la misma forma son pasadas.

El túnel PVP permitiría que la señalización sea pasada a través de la red publica, esto aun requiere de configuración manual (tal como la suscripción) de conexiones a través de la UNI publica. Par eliminar esta

restricción y permitir ubicar la conectividad, necesidades de señalización para ser soportadas a través de la UNI publica.

Esto es que los proveedores de servicio de redes publicas no soportarán el protocolo P-NNI en sus redes, ya que usualmente no desean mostrar su estructura de red interna a los usuarios. Las redes publicas operan solo con números E.164, no con direcciones ATM formato NSAP e internamente corren sus propios protocolos NNI.

Han sido propuestos que variantes de protocolos de enrutamineto de frontera tales como Protocolo de enrutamiento de inter-dominio (Inter-Domain Routing Protocol IDRP) es usado para insertar información la conectividad dentro de redes P-NNI con rutas externas. Alternativamente, ha sido propuesto que la entrada a la red publica pueda ser vista como un simple grupo par en la jerarquia P-NNI. El resultado es que redes privadas tratarán las redes publicas como una subred y que la señal requerida pasará a través del túnel, como protocolos de red corren sobre redes como X.25 o dial-up.

Cada túnel puede usar los campos de subdirecciones definidos en los procedimientos de señalización UNI. En la salida del switch de un red privada, antes de reenviar la solicitud de señalización a través de la red publica, la salida del switch moverá la dirección en formato NSAP destino dentro del campo de subdirecciones y reemplazar el campo de la dirección destino con la dirección E.164 que corresponde a la UNI publica del switch que provee el ingreso a la red privada destino correspondiente, la dirección fuente con formato NSAP será movida dentro del campo de subdirecciones fuente y reemplazada con el número E.164 de la salida del nodo de la UNI publica.

Esta solicitud de señalización será reenviada dentro de la red publica, la cual la enrutará, usando el número E.164 destino, por medio de la UNI publica destino, usando protocolos internos NNI. En el ingreso al switch hacia la red privada destino, el switch de ingreso moverá las direcciones NSAP destino y origen dentro de los campos de direcciones principales y procesará la solicitud normalmente. Note que este procedimiento podría necesitarse para hacer la conexión inicial, igual si las redes privadas fueran subsecuentemente en túnel del protocolo P-NNI a través de la red publica.

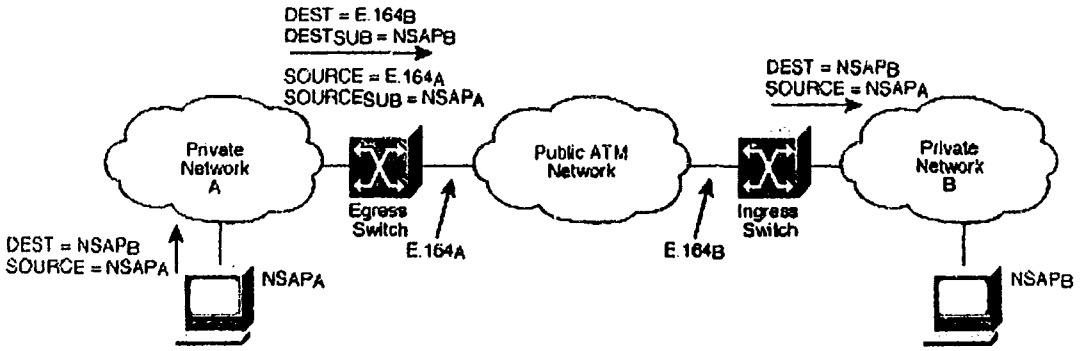


Fig. 5.29 Reasignación de direcciones en UNI publica.

Con este método los switchs de la red privada obtienen la información para relacionar la dirección destino ATM en formato NSAP a números E.164 de UNI a través de las cuales son alcanzados.

5.7 CAPA DE ADAPTACIÓN ATM

El empleo de ATM crea la necesidad de una capa de adaptación para soportar la transferencia de información de protocolos no basados en ATM. Lo que implica depositar en celdas ATM la información proveniente de dichos protocolos para poderlos transmitir a través de la red ATM.

5.7.1 SERVICIOS AAL

Los siguientes son ejemplos generales de los servicios provistos por AAL:

- Manejo de errores de transmisión
- Segmentación y reensamblaje, para hacer posible el transporte de largos bloques de información en celdas ATM
- Manejo de pérdida de condiciones de celda
- Control de flujo y reloj

La ITU ha definido cuatro clases de servicio para AAL que cubren una amplia gama de requerimientos. La clasificación es basada en si un reloj debe ser mantenido entre la fuente y el destino, si la aplicación requiere una

velocidad de transmisión constante y si la transmisión es orientada a conexión o no. Un ejemplo de servicio clase A es la emulación de circuito. En este caso, una taza de bits constante, la cual requiere de mantener la relación de tiempo y es orientada a conexión. Un ejemplo de servicio clase B es el vídeo de taza de bit variable usado en videoconferencias. Aquí la aplicación es orientada a conexión y la sincronía es importante pero la taza de transferencia es variable de acuerdo a la actividad de movimiento en la escena. Clases C y D corresponden a aplicaciones de transferencia de datos. En ambos casos la taza de transferencia puede variar pero no es necesario guardar sincronía en la conexión punto a punto y esto en modos orientados o no a la conexión.

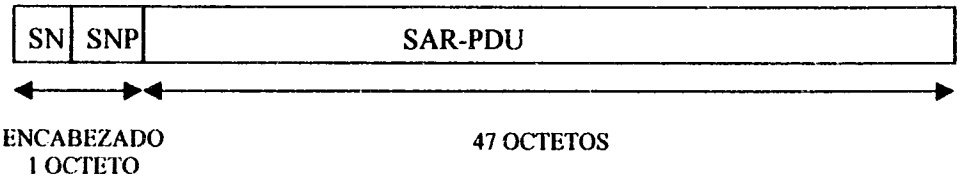
	Clase A	**Clase B**	**Clase C**	**Clase D**
Relación de sincronía entre la fuente y el destino	Requerida		No requerida	
Taza de información	Constante	Variable		
Modo de conexión	Orientada a conexión		No orientada a conexión	
Protocolo AAL	Tipo 1	Tipo 2	Tipo 3/4, Tipo 5	Tipo 3/4

Tabla 5.3 de clasificación de servicios para AAL

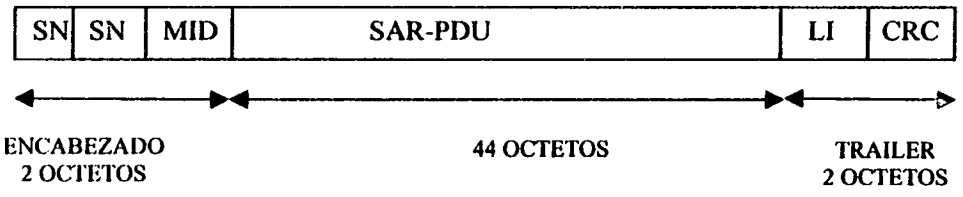
5.7.2 PROTOCOLOS ALL

La capa ALL esta organizada en dos subcapas lógicas: la subcapa de convergencia (CS) y la subcapa de segmentación y reensamblaje (SAR). La subcapa de convergencia provee las funciones necesarias para soportar aplicaciones especificas usando AAL. Cada aplicación conectada a AAL a un punto de acceso a servicio (SAP) el cual es simplemente la dirección de la aplicación. Así que la subcapa es dependiente del servicio.

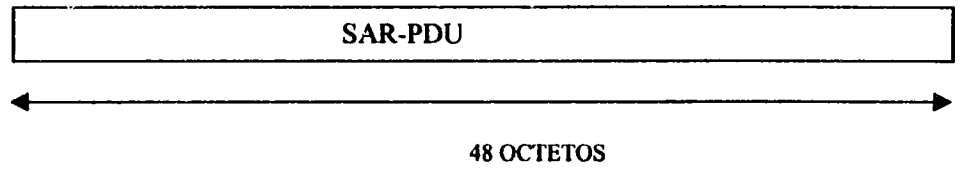
La subcapa de segmentación y reensamblaje es responsable de empacar la información recibida de CS dentro de celdas para transmitirlas y de desempacar la información en el otro extremo. Como hemos visto , en la capa ATM, cada celda consiste de 5 octetos de encabezado y 48 octetos del campo de información. Así, SAR debe empaquetar el encabezado y el acoplamiento de la información de CS dentro de bloques de 48 octetos. Inicialmente la ITU definió un tipo de protocolo para cada clase de servicio, nombrados desde Tipo 1 hasta Tipo 5. Actualmente cada tipo de protocolo consiste de dos subcapas, la CS y la SAR. Los tipos 3 y 4 fueron combinados y surgió el tipo 3/4.



A) AAL TIPO 1



B) AAL TIPO 3/4



C) AAL TIPO 5

SN = Número de secuencia (4 bits)
SNP = Protección de número de secuencia
ST = Tipo de segmento (2 bits)
MID = Identificación de multiplexado (10 bits)
LI = Indicador de longitud (6 bits)
CRC = Chequeo Cíclico Redundante (10 bits)

Fig. 5.30 Unidad de datos de Protocolo (PDUs) de Segmentación y reensamblaje (SAR)

5.7.3 AAL TIPO 1

La recomendación ITU-T I.363 especifica la capa de adaptación ATM AAL1 para soportar servicios de velocidad de bits constante en capas superiores a ATM. En AAL1, en el transmisor, un flujo continuo de información se divide en pequeños segmentos y se le agrega información de la capa AAL1 a cada segmento. Cada segmento es transportado por la capa ATM en celdas ATM. En el receptor, AAL1 extrae los segmentos de la s celdas ATM y reensambla el flujo continuo de información original usando la información de AAL. El receptor debe manejar la variación de retardo de celda, perdida de celda, detección de errores y recuperación de fuente de sincronía.

AAL1 consiste de dos subcapas: la subcapa de segmentación y reensamble (segmentaction and reassembly SAR) y la subcapa de convergencia (convergence sublayer CS). Las funciones de SAR y CS son descritas primeramente para transferencia de datos no estructurados. En este modo el usuario de datos es visto por AAL1 como un flujo continuo de información sin alguna estructura interna, tal como bloques de alineación de bytes o patrones de bits de tramas internos. La información de estructura interna de la información se transporta de un lado a otro. Las funciones de SAR y CS se muestran en la siguiente figura.

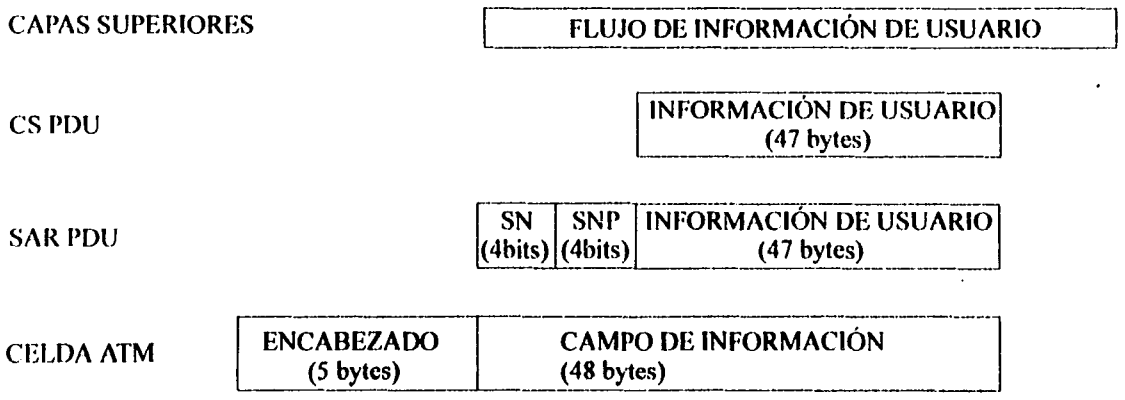


Figura 5.31 Unidad de datos de protocolo para AAL1

En el lado transmisor el flujo de la información es dividido en segmento de 47 bytes. Cada segmento forma una unidad de datos de protocolo (PDU) CS. El CS PDU es pasado a la subcapa de SAR. Cada segmento es etiquetado con un byte de información de SAR consistente de 4 bits del número de secuencia (secuence number SN) y 4 bits de protección

de número de secuencia (secuence number protection SNP). Los resultantes 48 bytes en el SAR PDU son enviados a la capa ATM para ser encapsulados en celdas.

El propósito del campo SN es para identificar el orden secuencial de los PDUs SAR para su reensamble. El campo de SN consiste de un bit para el indicador de la subcapa de convergencia convergence sublayer indicator CSI) y 3 bits de contador de secuencia (secuence count SC). El bit CSI es reservado para CS, para indicar la presencia o ausencia de la función CS. El contador de secuencia es asignado al PDU CS para detectar perdidas o desorden de PDUs.

El campo SNP provee corrección de errores del campo SN. El campo SNP consiste de 3 bits de CRC y un bit de paridad. El CRC es el resultado del calculo de CRC de los bits de SN y el bit de paridad es insertado después del calculo de CRC.

El receptor reemsambla el flujo de información a partir de los PDUs de SAR de la siguiente forma:

- Examina el CRC y el bit de paridad para detectar errores
- Corrige los errores de SN
- Reensambla los PDUs de CS en secuencia usando los números de secuencia
- Verifica PDUs de CS perdidos y lo notifica
- Establece un buffer para PDUs de CS compensar la variación de retardo de celda de la capa de ATM.

El flujo de información debe ser sacado del buffer igual como se transmitió. El receptor usa un servicio de reloj, el cual puede o no ser sincronizado con el de la red. Si el servicio de reloj no es sincronizado con la red, AAL1 debe pasar información de sincronía de 1 transmisor al receptor usando el método de synchronous residual time stamp (SRTS).

En el transmisor se asume que una referencia de reloj de red esta disponible pero el reloj fuente no es sincronizada con esta.

Un método de reloj adaptivo puede ser usado cuando un reloj de red no esta disponible. En el receptor los datos son recibidos en un buffer que es leído con un reloj local. AAL1 provee transferencia de datos estructurados para transportar información interna de la estructura de alineación de la información. AAL1 utiliza un apuntador para delinear la estructura de frontera. Este es soportado por dos tipos de PDUs de CS llamados formato no-P y P, como se muestra en la siguiente figura.

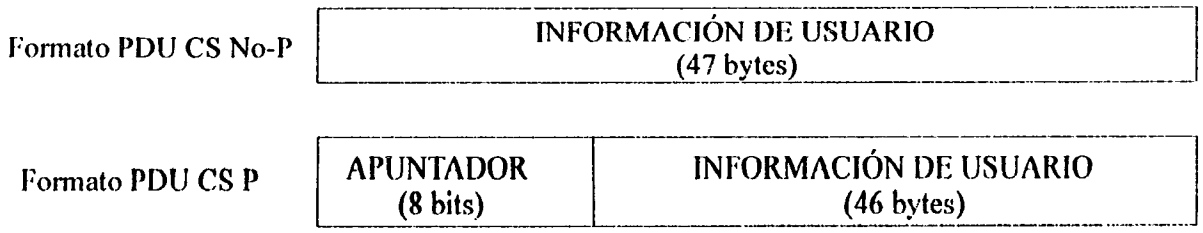


Figura 5.32 Formatos de PDUs de CS para transmisión de datos estructurados en AAL1

El formato PDU CS no-P es utilizado totalmente por información de usuario. En el formato P el primer byte es un apuntador y los restantes 46 bytes son usados para la información del usuario. El formato PDU de CS P es identificado por CSI=1, este formato es usado en PDUs de SAR con valores SN pares.

5.7.4 AAL TIPO 2

Este tipo es para aplicaciones analógicas tales como el vídeo o el audio, que requieren sincronía pero no una taza constante de información

5.7.5 AAL TIPO 3/4 Y 5.

El tipo de servicios provisto para AAL tipo 3/4 pueden ser caracterizados en dos dimensiones:

1. El servicio puede ser orientado o no a conexión. En el anterior caso, cada bloque de datos presentado a la capa SAR (SAR unidad de datos de servicio, o SDU) es tratado independientemente. En el último caso , esto es posible para definir múltiples conexiones SAR sobre una sencilla conexión ATM.

2. El servicio puede ser en modo mensaje o en modo flujo. El servicio en modo mensaje transfiere tramas de datos. Un sencillo bloque de datos de la capa arriba de AAL es transferida en una o más celdas. El servicio en modo de flujo soporta la transferencia de bajas velocidades continuas de datos con un bajo retardo requerido. Los datos entregados a AAL en bloques de tamaño fijo, los cuales podrían ser tan pequeños como un octeto. Un bloque es transferido por celda.

El AAL tipo 3/4 provee servicio de transferencia de datos aceptando datos de capas superiores y transmitiendo cada una a su respectiva terminal AAL destino. Desde la capa ATM se limita la transferencia de datos al campo de información de la celda de 48 octetos, la capa AAL provee las funciones de segmentación y reensamble.

Un bloque de datos proveniente de una capa superior, tal como una PDU (unidad de datos de protocolo), es encapsulada dentro de una PDU en la subcapa CS, esta es referida como la parte común de la subcapa de convergencia (CPSC), dejando abierta la posibilidad de agregar y desarrollar funciones especializadas en el nivel de CS. La CPCS PDU es pasada a la subcapa de SAR, donde es particionada dentro de bloques de información de 44 octetos. Cada bloque puede colocar dentro de una SAR PDU, la cual incluye un encabezado y un trailer de 48 octetos de longitud. Cada 48 octetos de una SAR PDU se coloca dentro de una celda ATM.

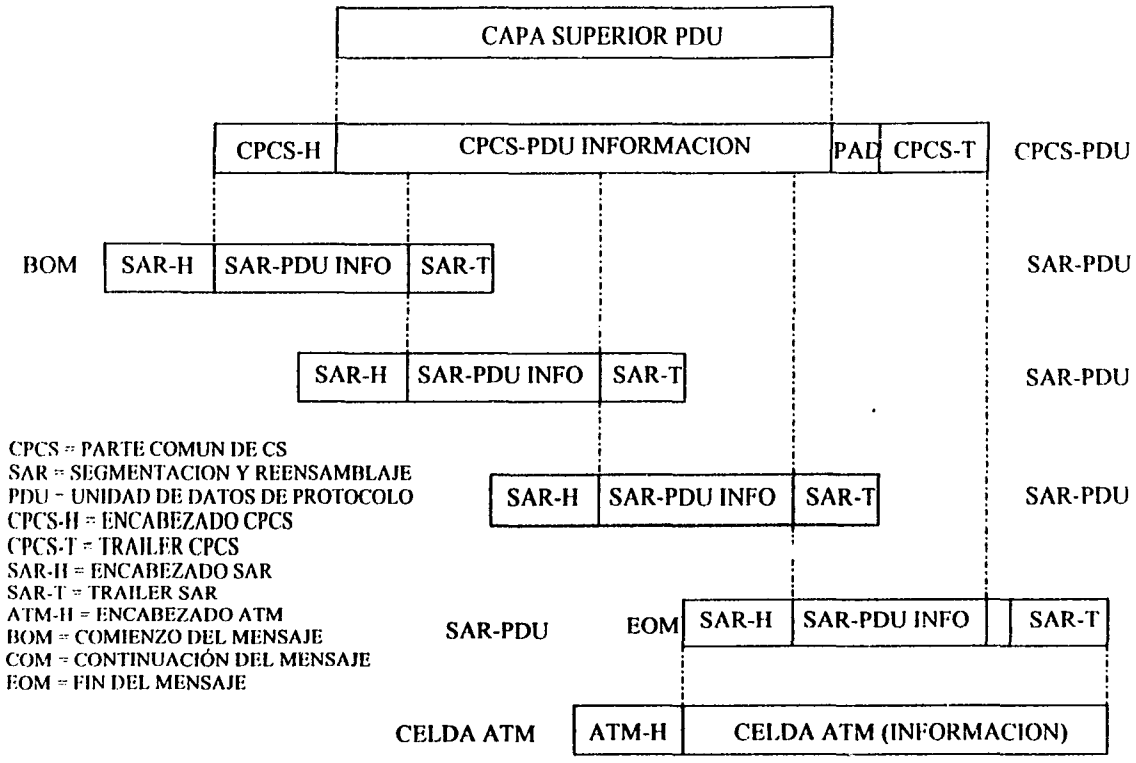
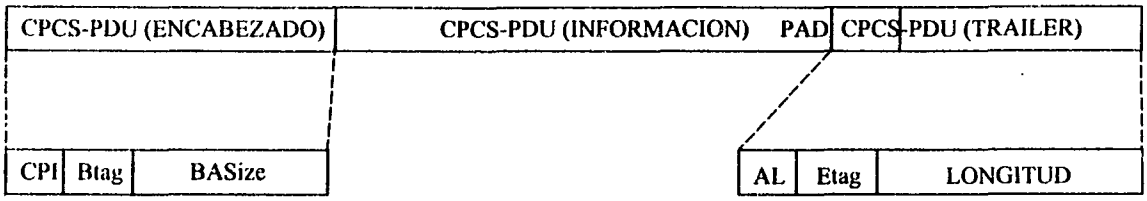


Figura 5.33 Ejemplo de transmisión de AAL 3 / 4

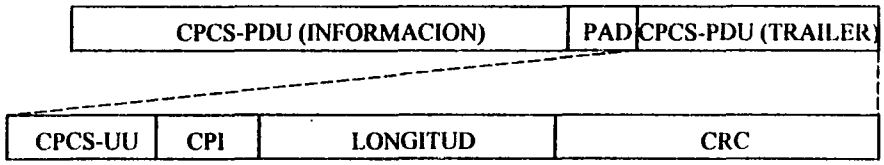
El encabezado de CPCS PDU consiste de tres campos:

- Indicador de parte común (CPI 1 octeto): indica la interpretación de los bits de los demás campos del encabezado de CPCS PDU.
- Etiqueta de comienzo (Btag 1 octeto): un número asociado a una CPCS PDU. El mismo valor aparece en el campo de Btag en el encabezado y en el Etag del trailer. El emisor cambia el valor de cada CPCS PDU sucesivo, haciendo posible que la asociación de encabezado y trailer sea correcta de cada CPCS PDU.



CPI = INDICADOR DE PARTE COMÚN (1 OCTETO)
Btag = ETIQUETA DE COMIENZO (1 OCTETO)
BASize = TAMAÑO DE ASIGNACIÓN DE BUFFER
AL = ALINEACION (1 OCTETO)
Etag = ETIQUETA DE FINALIZACIÓN (1 OCTETO)
LONGITUD = LONGITUD DEL CAMPO DE INFO. DE CPCS-PDU (2 OCTETOS)

AAL TIPO 3 / 4



CPCS-UU = INDICACION USUARIO-USUARIO CPCS (1 OCTETO)
CPI = INDICADOR DE CAMPO COMUN (1 OCTETO)
LONGITUD = LONGITUD DEL CAMPO DE CPCS-PDU (INFORMACION) (2 OCTETOS)
CRC = CHEQUEO DE REDUNDANCIA CICLICO

AAL TIPO 5

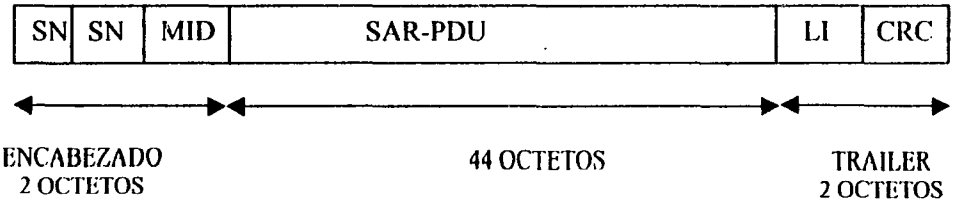
Fig. 5.34 CPCS PDU's

- Tamaño de asignación de buffer (2 octetos): indica a cada receptor el tamaño máximo de buffer requerido para reensamblar los CPCS SDU (unidad de datos de servicio). Para el modo mensaje, el valor es igual a la longitud del campo de información CPCS PDU. Para el modo streaming el valor es mayor o igual que la longitud del campo de información CPCS PDU.

La información de la siguiente capa superior es completada hasta 32 bits. El trailer CPCS PDU contiene los siguientes campos:

- Alineación (1 octeto): un octeto para alinear a 32 bits el CPCS PDU
- End tag (1 octeto): usado con el Btag en el trailer
- Longitud (2 octetos): Longitud de la carga útil del CPCS PDU.

El propósito de la capa CPCS es alertar al receptor que un bloque de datos esta entrando en segmentos y se debe reservar un espacio de buffer para su reemsamble. Esto prepara a la función CPCS para verificar la correcta recepción del CPCS PDU.



AAL TIPO 3/4

SN = Número de secuencia (4 bits)
SNP = Protección de número de secuencia
ST = Tipo de segmento (2 bits)
MID = Identificación de multiplexado (10 bits)
LI = Indicador de longitud (6 bits)
CRC = Chequeo Cíclico Redundante (10 bits)

Fig. 5.35 Formato SAR PDU's AAL 3/4

La figura anterior muestra el formato para el SAR PDU del tipo 3/4. La información de la capa superior siguiente, el CS arriva en bloques referidos a SAR SDUs . Cada SDU es transmitido en uno o varios SAR PDUs. Cada SAR PDUs en turno, es transmitido en una simple célula ATM. Los campos de encabezado de SAR PDU son usados para el proceso de segmentación de SDUs en la transmisión y de reensamblaje en la recepción.

- Tipo de segmento: hay cuatro tipos de SAR PDUs, un mensaje de secuencia simple (SSM) contiene una entrada SAR SDU. Si un SAR SDU es segmentado en dos o más SAR PDUs, el primer SAR PDU es el comienzo del mensaje (BOM), el último es el final del mensaje (EOM) y los intermedios SAR PDUs son la continuación del mensaje (COM).
- Número de secuencia: usado para el reemsamble de SAR SDU y verificar que todos los SAR PDUs han sido recibidos y concatenados

correctamente. Un valor de número de secuencia es colocado en el mensaje BOM e incrementado en los consecutivos COM y en el EOM para un sencillo SAR SDU.

- Identificador de mensaje: este es un único identificador asociado a un grupo de SAR PDUs que portan un sencillo SAR SDU, el cual es necesario para su reensamble.

El trailer de SAR PDU contiene los siguientes campos:

- Indicador de longitud: indica el número de octetos que ocupa el SAR SDU de la unidad de segmentación del SAR PDU. El número tiene un valor entre 4 y 44 octetos en múltiplos de 4. El valor debería ser siempre de 44 para BOM SAR PDU y COM SAR PDUs. Este es un número menor en SSM si el SAR PDU es menor de 44 octetos de longitud. Este es un número menor en un EOM si la longitud del SAR SDU no es un múltiplo integro de 44 octetos de longitud, necesitando el uso de una fijación parcial EOM.
- CRC: este es de 10 bits en la entrada SAR PDU.

Una característica distintiva de ALL 3/4 es que puede multiplexar diferentes ráfagas de datos en la misma conexión virtual ATM (VCI/VPI). Para los servicios orientados a conexión cada conexión lógica entre usuarios ALL es asignado un único valor MID. El tráfico de células de hasta 2^{10} diferentes conexiones pueden ser multiplexados sobre una simple conexión ATM. Para los servicios orientados a no conexión, el campo MID puede ser usado para comunicar un único identificador asociado a cada usuario sin conexión y tráfico de múltiples usuarios ALL pueden ser multiplexado.

AAL tipo 5 es un protocolo introducido para proveer facilidad de transporte para protocolos de capas superiores que son orientados a la conexión. Si se asume que las capas superiores toman cuidado del manejo de la conexión y que la capa de ATM produce errores mínimos, entonces varios de los campos del SAR y CPCS PDU no son necesarios. Por ejemplo para un servicio orientado a conexión, el campo MID no es necesario; el VCI/VPI es disponible multiplexar célula por célula y que las capas superiores soporten multiplexaje mensaje por mensaje.

El tipo 5 fue introducido para:

- Reduce proceso de sobreencabezado
- Reduce transmisión de sobreencabezado
- Asegura la adaptabilidad para el transporte de protocolos

Para entender las operación del tipo 5 comenzaremos con la capa CPCS. El CPCS PDU incluye un trailer con los siguientes campos:

- Indicador de usuario-usuario CPCS (1 octeto): usado para transmitir transparentemente información usuario-usuario.
- CRC (4 octetos): usado para detectar errores en el CPCS PDU
- Indicador de parte común (1 octeto): indica la interpretación de los bits de los demás campos del encabezado de CPCS PDU
- Longitud (2 octetos): longitud del campo de carga útil CPCS PDU.

Nótese que la facilidad de BASize ha sido eliminada. Si es necesaria para reservar espacio de buffer para reensamblar, esta información debe ser pasada a protocolos de capas superiores. Y varios protocolos de capas superiores negocien un tamaño PDU máximo; esta información puede ser usada por el receptor para reservar espacio en buffer. Un CRC de 32 bits protege la entrada CPCS PDU, por el contrario para tipo 3/4, un CRC de 10 bits es provisto para cada SAR PDU El CRC del tipo 5 provee mayor protección de los bits. El CRC de 32 bits provee mayor protección para la detección del desorden de células y solo en condiciones de falla de la red esto podría suceder.

La carga útil de la siguiente capa superior es acompletada a 48 octetos. El SAR PDU consiste de simplemente de 48 octetos de carga útil, transportando una porción del CPCS PDU. El encabezado tiene varias implicaciones:

- Debido a que no hay números de secuencia el receptor asume que todos los SAR PDU llegan en orden para su reensamble. El campo de CRC en el CPCS PDU esta para garantizarlo.
- La ausencia del campo de MID significa que no se puede intercambiar celdas entre PDUs de CPCS diferentes. Cada SAR PDU sucesivo transporta una porción del CPCS PDU actual o del primer bloque del siguiente CPCS PDU. Para distinguir entre esos dos casos, el bit de

indicación de usuario-usuario ATM (AAU) en el campo de carga útil del encabezado de celda ATM es usado. Un PDU CPCS consiste de cero o más SAR PDUs consecutivos con un AAU puesto a 0 seguido inmediatamente por un SAR PDU con AAU puesto a 1.

- La ausencia del campo LI significa que no hay forma para la entidad SAR, de distinguir entre octetos CPCS PDU y llenar en el último SAR PDU. Tampoco hay forma para la entidad SAR, de encontrar el trailer CPCS PDU en el último SAR PDU. Para resolver esta situación se requiere que la carga útil de CPCS PDU sea llenada fuera de el último bit en el trailer CPCS PDU.

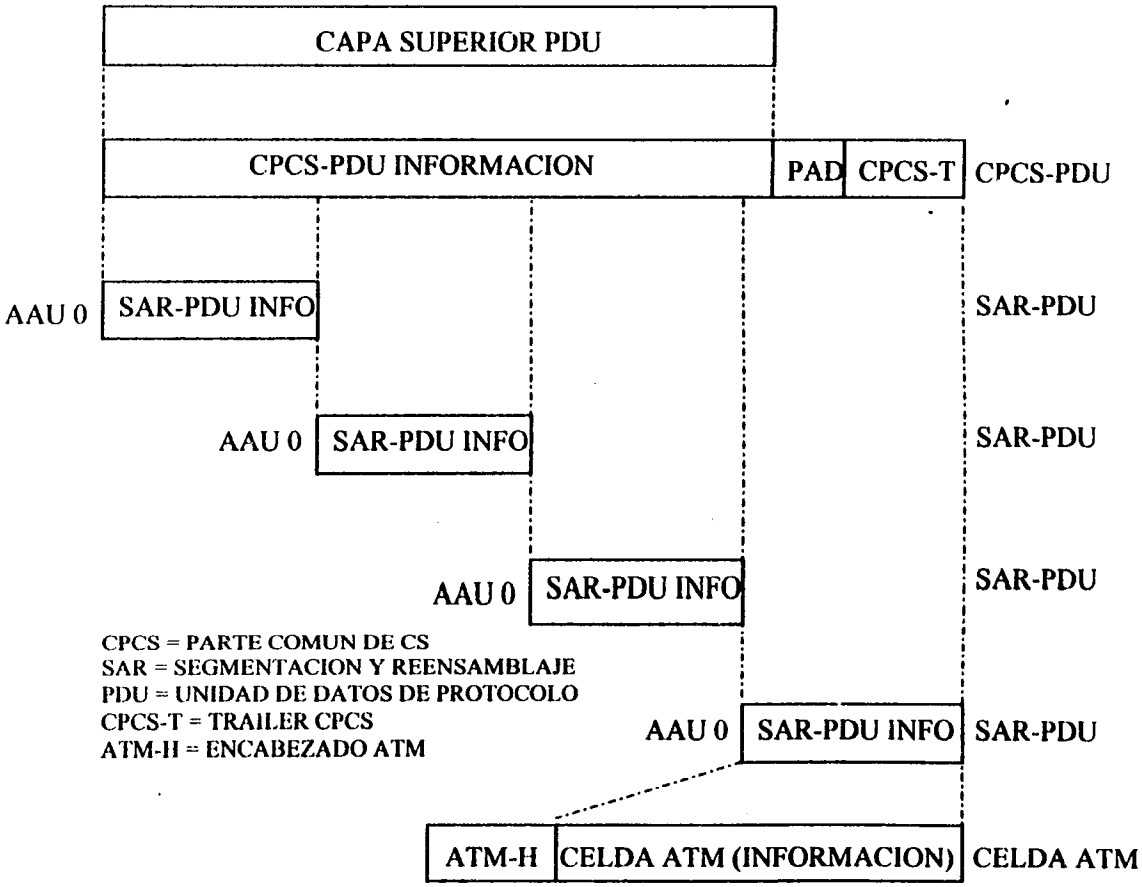


Fig. 5.36 Ejemplo de transmisión en AL5

5.8 MODELO DE ADMINISTRACIÓN DE RED ATM

La administración de red (Network Management NM) de una tecnología es una de las más complejas tareas para los grupos de estandarización, vendedores de equipos y soluciones de NM. La administración de red generalmente comprende: administración de la configuración (Configuration Management CM), administración de fallas (Fault Management FM), administración de desempeño (Performance Management PM), administración de alarmas (Accouting Management AM) y administración de seguridad (Security Management SM).

La estandarización de la administración de red se enfoca en la base de información de administración (Management Information Base MIB) el cual define manejo de objetos y asociación de atributos que son necesarios para implementar funciones de administración. Como se muestra en la siguiente figura, se necesitan plataformas abiertas y robustas para administrar redes ATM, para resolver los requerimientos del usuario de las funciones de la administración de la red ATM en un ambiente de múltiples proveedores.

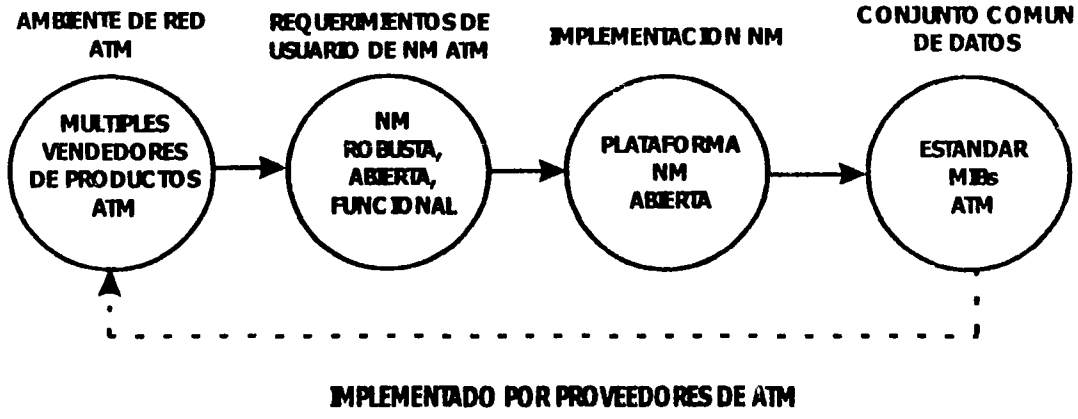


Fig. 5.37 Uso del estándar MIB ATM.

La clave para plataformas de NM abiertas es un protocolo de comunicaciones común y el manejo de objetos o elementos de información comunes que son usados para facilitar el monitoreo y el control de los elementos de red ATM. Esto es realizado a través de estándar MIB. En este contexto existen un número relevante de MIBs. Las MIBs están basadas en

estándares como el protocolo de administración de red simple (Simple Network Management Protocol SNMP) o protocolo de información de administración común (Common Management Information Protocol CMIP). A demás de las MIBs del Foro ATM (SNMP y CMIP), son definidas MIBs por otros organismos de estandarización como la fuerza de trabajo de los ingenieros de internet (Internet Engineering Task Force IETF) (SNMP), Foro NM (CMIP) e ITU (CMIP). Adicionalmente se desarrollan MIBs de fabricantes propietarias para manejar sus equipos. A pesar de que cada organismo de estandarización tiene objetivos específicos, existen MIBs que concuerdan. Por lo general se necesita la combinación de varias MIBs para cubrir una necesidad. Así pues, es importante entender las diversas MIBs que son aplicables a las redes ATM, su propósito, alcance e interrelaciones para manejar redes ATM.

Como la tecnología ATM va a través de redes publicas y privadas la administración de red tendrá diferentes perspectivas. El foro ATM ha definido un modelo jerárquico que comprende ambas áreas. Principalmente el modelo NM del foro ATM define cinco interfaces: M1, M2, M3, M4 y M5 como se puede apreciar en la figura.

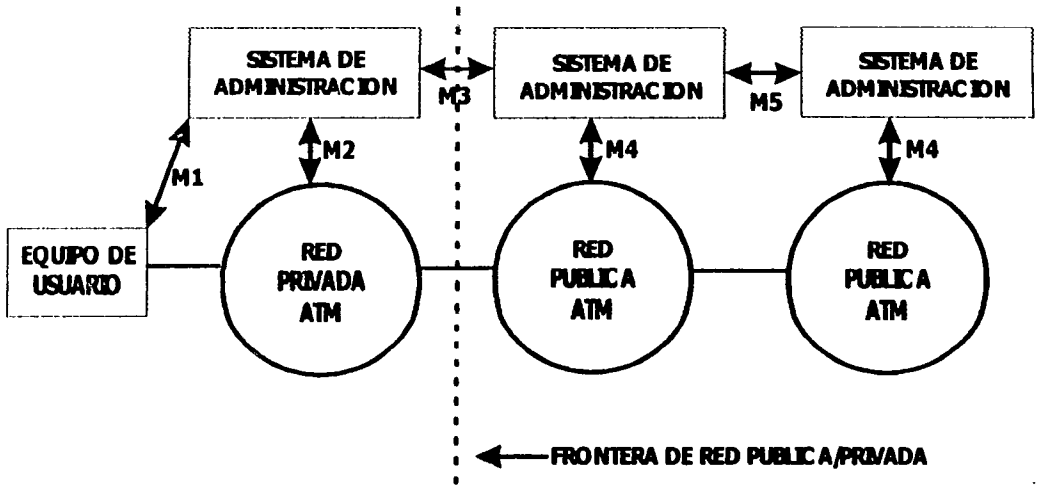


Fig. 5.38 Modelo de Administración del Foro ATM

La administración de la red privada ATM es llevada por M1 en combinación con M2. M1 concierne con la administración del equipo terminal de usuario conectado a switchs públicos o privados y M2 con la administración de switchs y redes ATM. M3 es el enlace entre las redes públicas y privadas para intercambiar información de fallas, desempeño y configuración. M4 pertenece a la administración de switchs y redes ATM públicos. M5 utiliza interacciones o intercambio de información de la administración entre dos redes públicas cualquiera. A continuación se muestra un resumen abreviado del foro ATM de las principales MIBs que pertenecen a las cinco interfaces.

- MIB interfaz de administración local integrada (Integrated Local Management Interface ILMI): Esta interfaz M1 provee información de estado, configuración y control para la interfaz ATM entre dos dispositivos ATM. La MIB ILMI cubre información de configuración, estado y estadísticas de desempeño de circuitos físicos y virtuales.
- MIB interface de intercambio de datos (Data Exchange Interface (DXI): define enrutamiento para unidades de servicio de datos ATM (DSU). La MIB DXI soporta administración de configuración y desempeño de la interface DXI la cual es básicamente una interface M1.
- MIB LAN Emulation: comprende a las MIB del cliente LANE y servidor LANE y están catalogadas en la interfaz M2. Soportan MIB de emulación de LAN (Emulated LAN ELAN) para administrar la configuración, fallas y desempeño de clientes y servidores.
- MIB M3: define objetos para la parte de los clientes de una red publica. M3 es una interfaz entre los sistemas de administración de red pública y privada. La interfaz del lado de la red privada utiliza SNMP y del lado de la red pública CMIP. Consecuentemente, una función de administración de interdominio es usada para su interoperabilidad.

Interfaz del Foro ATM	MIBs aplicables
M1	MIB AtoM, MIB LANE, MIB DIX, MIBs propietarias (MIBs adaptadas a ATM)
M2 (SNMP)	MIB AtoM, MIB LANE, MIB ILMI, MIB CBS, MIB PNNI, MIBs de y transmisión, MIB IMA, MIB RMON, MIBs propietarias.
M2 (CMIP)	MIB Visualización de Red M4, MIB de elementos de red M4, MIB SVC M2, MIB SONET ITU-T y MIBs E1/E3
M3	MIB M3 Y MIB AToM
M4 (SNMP)	MIB ILMI, MIB LANE, MIB CES, MIB SNMP M4, MIB AAL ATM, MIBs Transmisión, MIB IMA ATM Y MIB RMON
M4 (MIB (CMIP)	MIB NE M4, MIB ITU-T 1.751, MIB SVC M4, MIB AAL ATM, MIBs Transmisión, MIB Bellcore G.1114 y MIB del Foro NM.
M5 MIB	MIB Red – Red del Foro ATM y MIB carrier – carrier de ETSI NA5-2212

Tabla 5.4 de relación de MIBs con el Modelo del Foro ATM

Varios tipos de MIBs M4 se describen:

- MIB de elemento de red (Network Element NE): Define elementos del dominio de red y definiciones de subred, conexiones entre subredes, caracterización de trafico y estadísticas de tráfico. Esto es una MIB lógica común la cual es usada para definir la versión de SNMP y CMIP de MIB NE M4. Esta cubre la configuración de la interfaz ATM, administración de la conexión VP/VC y administración de desempeño.
- MIB de visualización de red M4: Soporta configuración de red de transporte (subred y aprovisionamiento de enlace), administración de conexión, administración de fallas de red, (incluyendo correlación, localización, notificación y pruebas) y admir tración de desempeño (monitoreo de congestión de la red).

- MIB de circuito virtual conmutado (SVC): define los objetos ATM relacionados a SVCs a través de NEs.
- MIB AAL ATM: Define los objetos relacionados con la capa de adaptación ATM para NEs en el dominio de la red publica.
- MIB PNNI: Define los objetos para PNNI
- MIB multiplexor inverso ATM: Define objetos para multepexaje ATM sobre sistemas de transmisión T1.
- MIB red – red M5: Define objetos para el intercambio de información de administración entre dos diferentes sistemas de administración de red de carriers ATM.
- MIB de pruebas de acceso: Permite accesar y controlar remotamente un switch para propósito de pruebas.

El IETF define MIBs SNMP para administrar redes ATM y sistemas de transmisión relacionados. Las de mayor importancia son:

- MIB AtoM (RFC 1695): Es generalmente usada para administrar configuración y desempeño terminal a terminal. El Foro ATM contribuyo al desarrollo de la MIB IETF AtoM para asegurar que objetos relevantes y atributos fueran alineados con la MIB ILMI.
- MIBs de transmisión: Estas MIBs definen administración de información de la configuración, fallas y desempeño para el manejo de los sistemas de transmisión que soportan ATM. Esta incluye: RFC 1406 para manejar T1-E1, RFC 1407 para manejar T3 – E3, RFC 1595 para administrar SONET.
- MIB RMON (Remote Monitoring): Define objetos para dispositivos ATM para pruebas, análisis de desempeño y análisis de patrones.

Varias organizaciones definen MIBs para administradores de red basados en estándares CMIP. Las MIBs ATM de interés de esas organizaciones están en resumen:

- MIBs de administración de NE de carrier: Corresponden a MIB NE M4. El estándar ITU I.751 define objetos para administración de NEs ATM usando CMIP. Esto esta basado en AF M4 NE. El Foro NM define MIBs para administración de servicio, desde la perspectiva del carrier.
- Interfaz inter carrier: ETSI NA5-2212 es una MIB carrier a carrier. Corresponde a la MIB M5 del Foro ATM.
- MIBs de Transmisión: Define objetos para administrar la configuración, fallas y desempeño para varios sistemas de transmisión que soportan ATM.

- Incluye: ANSI T1.247 para manejar T1, ITU-T G.704 y G.706 para la administración de SONET, SDH y E1, Bellcore GR.836 para el manejo de T3, ITU-T G.826 y G.832 para manejar E3.

5.8.1 PROTOCOLO DE ADMINISTRACIÓN DE RED SIMPLE (SNMP)

El protocolo SNMP es definido por el RFC 1157 consiste de cuatro tipos de operaciones, los cuales son usados para manipular la información de administración. Estos son:

- Get usado para traer información de administración específica
- Get-Next usado para traer información de administración a través de la MIB
- Set usado para modificar la información de administración
- Trap usado para reportar eventos extraordinarios

Esas cuatro operaciones son implementadas usando cinco tipos de PDUs:

- GetRequest-PDU usado para requerir una operación Get
- Get NextRequest-PDU usado para requerir una operación Get-Next
- GetResponse-PDU usado para responder a una operación Get, Get-Next o Set
- SetRequest-PDU usado para requerir una operación Set
- Trap-PDU usado para reportar una operación trap

5.8.2 INTERFAZ DE ADMINISTRACIÓN LOCAL INTEGRADA (ILMI)

La Interfaz de Administración Local Integrada (Integrated Local Management Interface ILMI) es un protocolo definido por el Foro ATM para guardar y capturar parámetros de la capa física, la capa ATM, de la trayectoria virtual y de los circuitos virtuales. ILMI utiliza SNMP. Esta organizada en cuatro Bases de Información de Administración (Management Information Base MIBs) para el manejo de objetos: MIB de convenciones de texto, MIB de administración de enlace, MIB de registro de direcciones y MIB de registro de servicios.

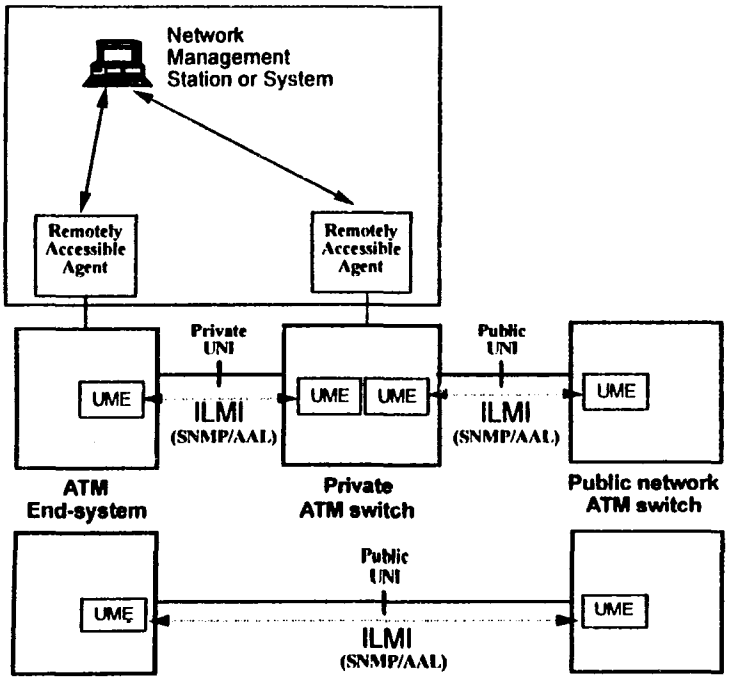


Fig. 5.39 Diagrama de la definición y contexto de ILMI

ILMI tiene las siguientes opciones y principios:

- Cada dispositivo ATM soporta una o más interfaces ATM.
- Las funciones de ILMI para una interfaz ATM proveen información de configuración, de estado y control acerca de los parámetros de la capa física ATM de la interfaz.
- Manejo de conjunto de objetos y atributos necesarias para soportar las funciones ILMI para cada interfaz ATM.
- Los atributos de la interfaz ILMI ATM son organizados en una estructura estándar MIB para cada interfaz ATM.
- Para cualquier equipo ATM existe una entidad de administración de interfaz ATM (Interface Management Entity IME) asociada con cada interfaz ATM que soporte funciones ILMI para esa interfaz ATM.
- Cuando dos equipos ATM se conectan punto a punto por sus interfaces ATM existen dos IMEs asociadas, una IME para cada interfaz de cada equipo ATM. Dos IMEs son definidas como IMEs adyacentes.
- La comunicación ILMI toma lugar entre IMEs adyacentes sobre enlaces físicos o virtuales.
- El protocolo de comunicación para ILMI es un protocolo abierto (por ejemplo SNMP).
- Una IME puede accesar vía el protocolo de comunicación ILMI a la información MIB de la interfaz ATM asociada con la IME adyacente.
- Funciones ILMI para UNI es el registro de direcciones a través de esta interfaz.
- Funciones ILMI para LAN Emulation provee auto configuración del cliente (LAN Emulation Client LEC).

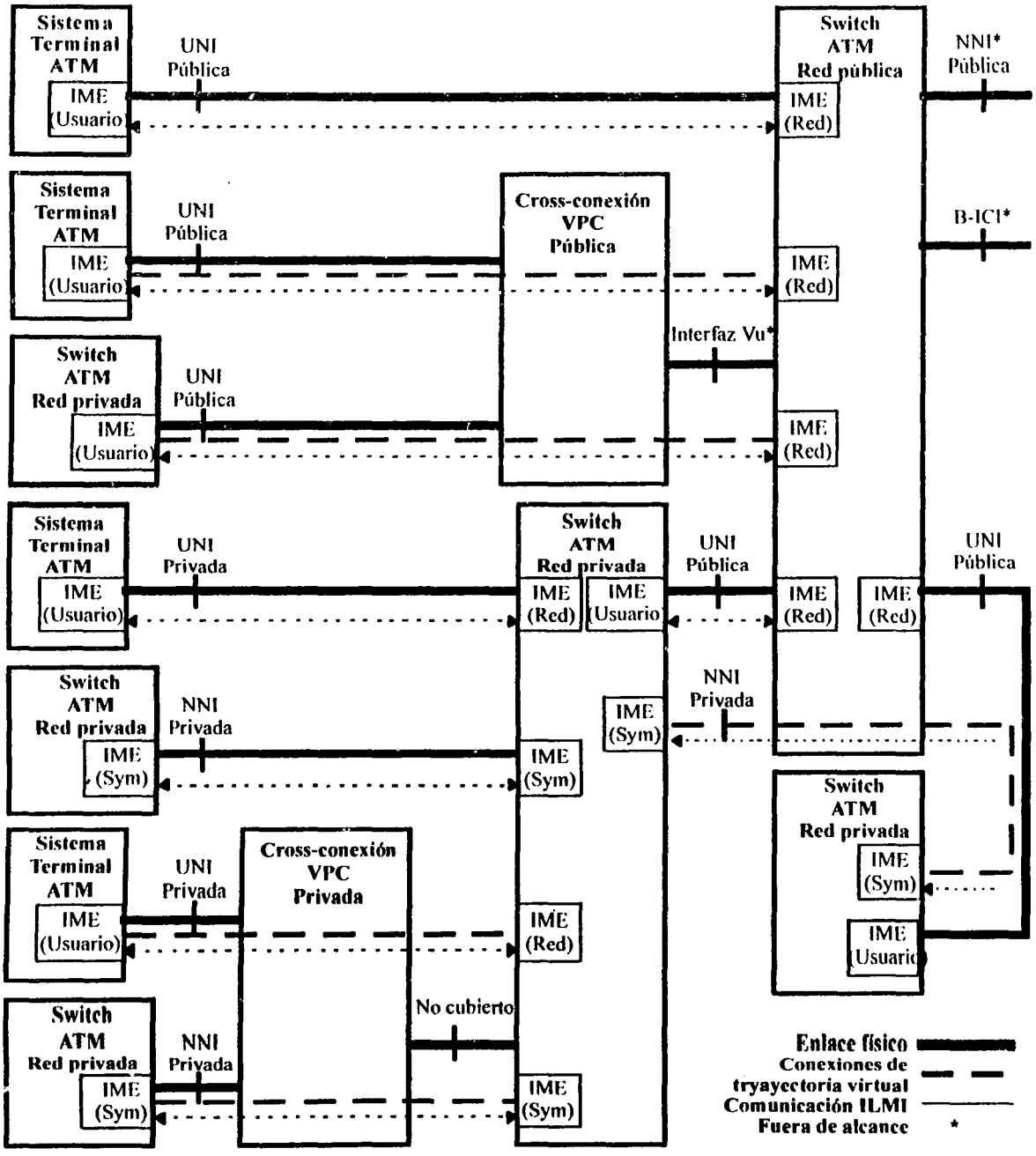


Fig. 5.40 Definición y contexto de ILMI

5.8.2.1 FUNCIONES ILMI.

ILMI soporta intercambio bidireccional de parámetros de interfaz ATM entre dos IMEs conectadas. Cada IME contiene una aplicación agente y una aplicación de administración. Para una porción especifica de ILMI cada IME contiene la misma MIB de la interfaz ATM. La semántica de algunos objetos MIB puede ser interpretada diferente de pendiendo del papel que desempeñe una IME individual.

Existen cuatro módulos MIB ATM principales: MIB de convenciones de texto, MIB de administración de enlace, MIB de registro de direcciones y MIB de registro de servicios.

El modulo MIB de convenciones de texto define varias convenciones textuales e identificadores de objetos tales como el número de octetos para la dirección de un sistema terminal ATM y el prefijo de red en un sencillo modulo para que se puedan importar mutuamente con otro modulo MIB y en forma consistente.

El modulo de MIB de administración de enlace provee facilidades de administración de enlace de propósito general en cuatro grupo de objetos para todas las interfaces ATM.

- Capa física. ILMI 4.0 discontinúa y deprecia los valores ILMI para la capa física y especifica el uso de la interfaz estándar MIB (RFC 1213). Ejemplos de estos valores son: atmfPortMyIfName, atmfPortMyIfIdentifier, atmfMyIpNmAddress, atmfMySystemIdentifier Este valor es un identificador de 48 bits definido por IEE administra universalmente el espacio de las direcciones MAC, las cuales identifican al dispositivo ATM como único), atmfTransmissionTypes, atmfSonetType, atmfSonetSTS3c, atmfDs3, atmfT1, atmfMediaTypes, atmfMediaUnknownType, atmfMediaCoaxCable y atmfMediaSingleMode.
- Capa ATM. Indica el número de bits disponibles para los valores de VPI y VCI en el encabezado de la celda ATM, el máximo número de VPCs y VCCs permitidos, el número de trayectorias virtuales configuradas permanentes, el número de canales virtuales, tipo de interfaz ATM, tipo de dispositivo ATM, versión de ILMI, UNI y NNI. Estos valores se

almacenan en la tabla atmfAtmLayerGroup y cada interfaz tiene una entrada atmfAtmLayerIndex en la tabla.

- Conexión de trayectoria virtual. Indica el estado de up o down de los VPC y sus parametros de QoS. Los atributos de un PVC del grupo PVC son almacenados en la tabla atmfVpcGroup (índice de interfaz, valor VPI, estado operacional, descriptor de trafico transmitido y recibido, indicador de best effort, clase de QoS transmitido y recibido y categoría de servicio). Cada PVC es indexado en la tabla por un atmfVpcPortIndex para identificar el puerto físico y un atmfVpcVpi para identificar el número VPI.
- Conexión de canal virtual. Indica el estado de up o down de los VCC y sus parametros de QoS. Los atributos de un PCC del grupo PCC son almacenados en la tabla atmfVccGroup (índice de interfaz, valor VPI, estado operacional, descriptor de trafico transmitido y recibido, indicador de best effort, clase de QoS transmitido y recibido y categoría de servicio). Cada VCC es indexado en la tabla por atmfVccPortIndex, valor VPI atmfVccVpi y valor VCI atmfVccVci. Solo los PVCs son representados en este grupo, incluyendo los reservados para señalización, ILMI y LECS VCCs.

El modulo MIB de registro de direcciones provee un mecanismo para el registro de direcciones ATM para una interfaz UNI lo cual permite que los switchs configuren automáticamente los prefijos de red en sistemas terminales.

El modulo MIB de registro de servicios provee un registro de servicios de propósito general para localizar servicios de red ATM tales como el servidor de configuración de LAN Emulation (LAN Emulation Configuration Server LECS).

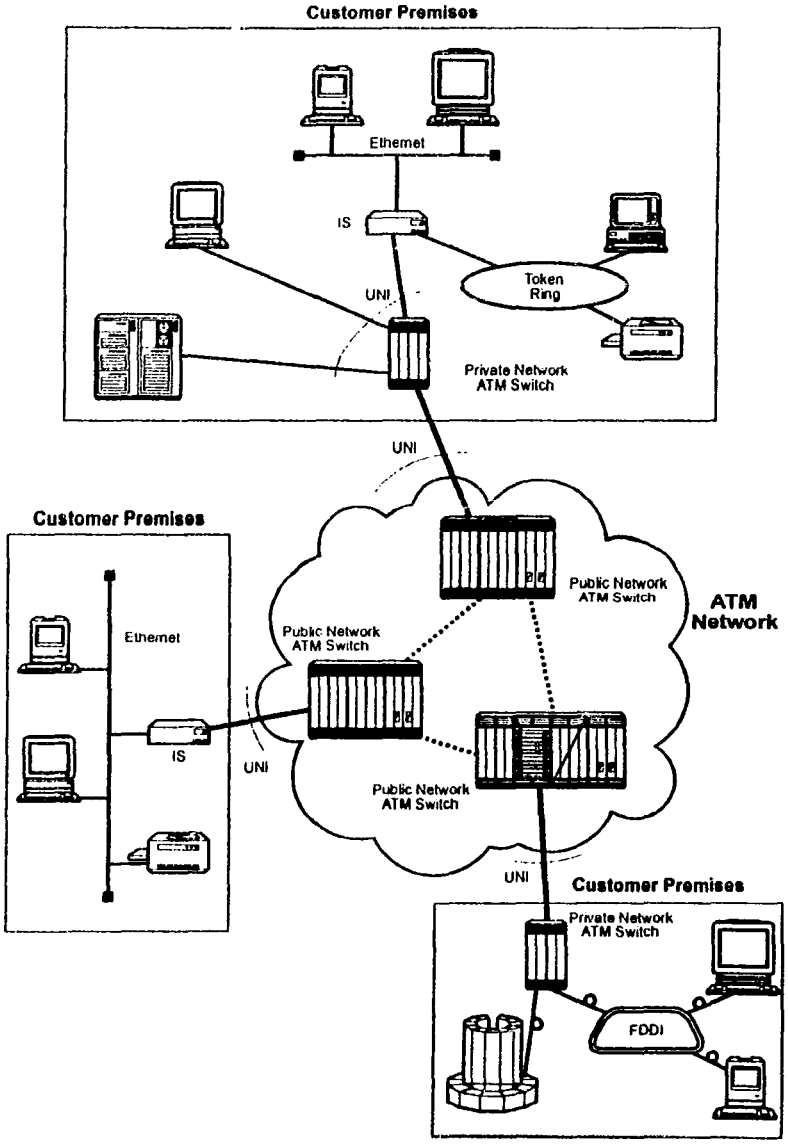


Fig. 5.41 Ejemplos de equipamiento para la implementación de ILMI UNI ATM

5.8.2.2 INTERFAZ DE SERVICIO ILMI.

Es importante entender ILMI ya que las interfaces ATM usan identificadores de objetos SNMP en funciones de red como auto configuración de LEC en ambientes LAN Emulation, keepalives y el descubrimiento de automático de PVC. Cuando dos interfaces ATM ejecutan el protocolo ILMI, intercambian paquetes ILMI a través de la conexión física. Esos paquetes consisten de mensajes de SNMP de 484 octetos de longitud. Las interfaces ATM encapsulan esos mensajes en un trailer de la capa de adaptación 5 de ATM, segmentan el paquete en celdas y las etiquetan para su transmisión. Desde que ILMI especifica valores particulares para el trailer AAL5, se define la encapsulación como ILMI cuando se crea el PVC que transportará los mensajes ILMI con valores por defecto de VPI=0 y VCI=16 los cuales se pueden modificar.

ILMI usa SNMP también para administrar y controlar operaciones de información a través de la interfaz ATM. La información de la interfaz ATM debe estar representada en la MIB. Los tipos de información que deben estar disponibles en la MIB es:

- Capa física
- Capa ATM
- Conexiones de Trayectoria Virtual (VPC)
- Conexiones de Canal Virtual (VCC)
- Información de registro de direcciones
- Registro de servicios

La estructura de árbol de la MIB ATM es descrita en la siguiente figura.

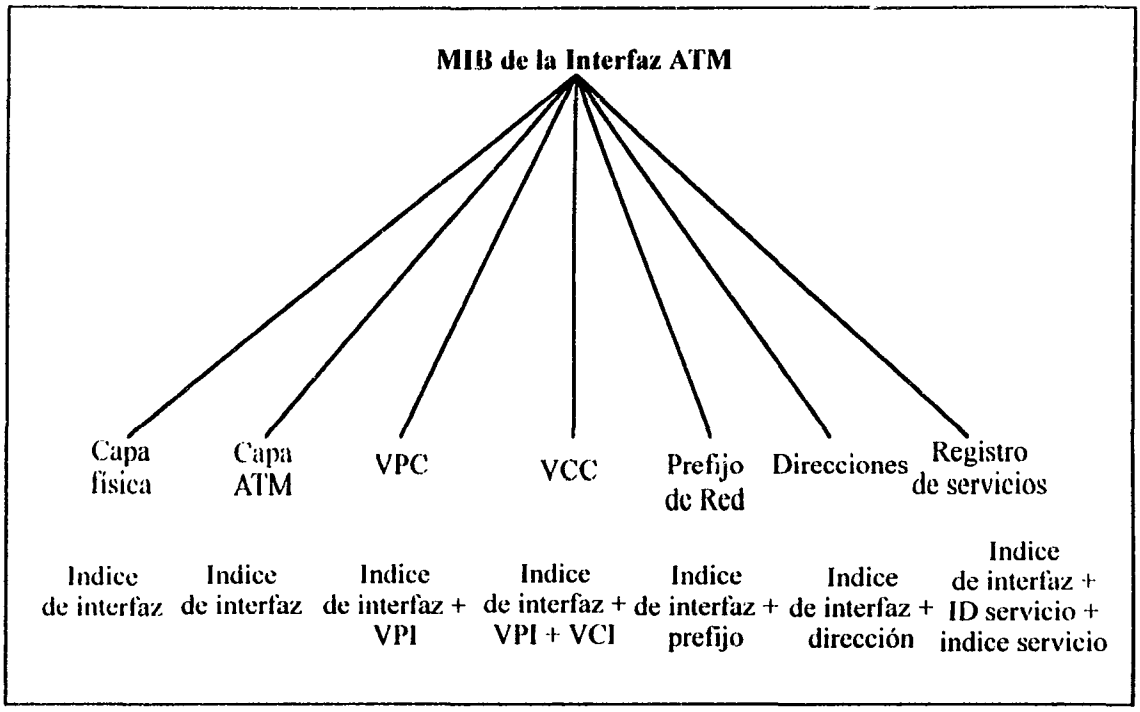


Fig. 5.42 Estructura de árbol de la interfaz ATM

La MIB ATM puede ser extendida a través del tiempo permitiendo agregar nuevos objetos sin que se requiera algún cambio en el protocolo de administración. En adición, proveedores pueden definir extensiones de MIBs de la interfaz privada ATM para soportar características adicionales o propietarias de sus equipos.

ILMI provee acceso a la información de administración que identifica la capa física de la interfaz. Cuando la comunicación ILMI toma lugar sobre un enlace físico, aquí se encuentra un grupo de capa física para esa interfaz física. Cuando la comunicación ILMI tiene lugar en un enlace virtual la información de administración de la capa física es presentada y representa la interfaz virtual. Cada interfaz física o virtual tiene un conjunto de atributos específicos e información asociada a ella. La especificación ILMI provee

información de configuración y estadísticas acerca de la interfaz ATM para la capa física.

ILMI provee acceso a la información de administración de la capa ATM. Aquí se encuentra un grupo de capa ATM para cada par de interfaz física o virtual. Los atributos de la capa ATM son comunes a lo largo de todas las conexiones de trayectoria virtual (VPCs) y conexiones de canal virtual (VCCs) a esa interfaz ATM. La información de configuración de la capa ATM muestra el tamaño de los campos de dirección VPI y VCI en el encabezado de la celda ATM, número de VPCs y VCCs configurados permanentes y el máximo número de VPCs y VCCs permitidos en esa interfaz ATM.

En el contexto de las funciones soportadas por ILMI, una conexión de trayectoria virtual (VPC) extendida entre dos interfaces ATM que terminan el VPC. En la interfaz de la capa ATM el VPC es identificado únicamente por el valor de VPI, cuando la comunicación ILMI toma lugar sobre un enlace físico. La información de estado indica el reconocimiento de IME del estado de VPC. La información de configuración muestra los parámetros de QoS para el VPC local del punto terminal.

ILMI provee un mecanismo para el registro de direcciones el cual permite a los switchs configurar automáticamente prefijos de red en los sistemas finales.

ILMI provee un mecanismo de registro de direcciones el cual permite a los sistemas finales configurar automáticamente direcciones ATM para las interfaces ATM en los switchs.

ILMI provee el registro de servicios de propósito general para localizar servicios ATM tales como LAN Emulation.

5.8.2.3 MODELO PARA MANEJO DE OBJETOS

El manejo de objetos es a través de una base de información MIB. La información relacionada con la operación de la interfaz ATM es organizada en la MIB en forma jerárquica. Cada interfaz ATM corresponde a una interfaz física. La MIB de la interfaz ATM es accesada a través de la ILMI correspondiente a la interfaz ATM/física.

Los objetos en la MIB de la interfaz ATM son definidos haciendo uso de un subconjunto de Notación de Sintaxis Abstracto 1(Abstract Syntax Notation One) definida por la estructura de información de administración (Structure of Management Information SMI). Cada objeto tiene un nombre, una sintaxis y un código. El nombre es un identificador de objeto el cual especifica un tipo de objeto. La sintaxis define la estructura de datos correspondiente al tipo de objeto. El código del objeto es como el tipo de objeto es representado usando la sintaxis del tipo de objeto cuando es transmitido en la red.

5.8.2.4 PROTOCOLO ILMI

Un VCC debe ser usado para enviar mensajes de SNMP de encapsulación AAL, entre IMEs. Este VCC es usado para requerimientos, respuestas y traps diferenciados de acuerdo al tipo de SNMP PDU.

Encapsulación de Mensajes de ILMI SNMP en AAL 5.
Encapsulación de mensajes de ILMI SNMP en la parte común de AAL 3 / 4.
Un VCC será provisto para ILMI. El valor por defecto de VCC es VPI=0, VCI=16, sin embargo el valor VPI/VCI debe ser configurado.
Las celdas que transportan mensajes ILMI tendrán prioridad de perdida de celda (CLP=0).
El trafico de SNMP en el VCC ILMI no debe exceder del 1 % del ancho de banda.

El formato del mensaje especificado en el RFC 1157 debe ser usado. En todos los traps de SNMP, el campo de time-stamp en el trap-PDU contendrá el valor de los IMEs sysUP Time objeto MIB en el tiempo de la generación del trap. Los traps soportados son el coldStart y

enterpriseSpecific. Todas las implementaciones ILMI deben ser capaces de aceptar mensajes SNMP de hasta 484 octetos. Los requerimientos relacionados con la conexión ATM usados para la comunicación ILMI son:

El VCC usado para la comunicación ILMI soportará una velocidad de celda sustentable, no más del 1 % de la velocidad de línea de la interfaz física ATM y una velocidad de celda pico no mayor del 5%. El trafico ILMI no debe sobrepasar de 484 octetos.

Un IME debe proveer acceso al grupo de sistema vía el protocolo de comunicación ILMI. El grupo de sistema consta de siete objetos:

sysDescr	descripción textual de la entidad, incluye nombre y versión que identifican el tipo de hardware, el sistema operativo y software de red del sistema.
sysObjectID	identifica al fabricante del subsistema de administración de Red.
sysUpTime	tiempo desde que el IME fue reinicializado.
sysContact	identificación textual de la persona que maneja el nodo.
sysName	nombre asignado administrativamente para el manejo del nodo.
sysLocation	descripción textual de la ubicación física del dispositivo.
sysServices	indica conjunto de servicios que la entidad ofrecerá primeramente. Las capas son:

Capa	Funcionalidad
1	física (p.e. repetidores)
2	enlace de datos/subred (p.e. switchs ATM puentes IEEE 802.3)

3 internet (p.e. routers IP)
4 end-to-end (p.e. hosts IP)
7 aplicaciones (p.e. correo)

5.8.2.5 CONVENCIONES DE TEXTO Y DEFINICIONES MIB

Las convenciones textuales MIB definen un número de identificadores de objetos en un simple módulo para que otros módulos las puedan importar en forma consistente.

Valores boléanos con datos del tipo RFC-1903

-- Categorias de servicio ATM:

```
AtmServiceCategory ::=
INTEGER {
other(1),
cbr(2),
rtVbr(3),
nrtVbr(4),
abr(5),
ubr(6) }
```

-- Direcciones del Sistema terminal ATM:

```
AtmAddress ::= OCTET STRING (SIZE (8 | 20))
```

-- Prefijo de red para direcciones ATM:

```
NetPrefix ::= OCTET STRING (SIZE (8 | 13))
```

-- Tanto para las convenciones AtmAddress, NetPrefix y Native E.164 las direcciones son representadas con 8 octetos usando el formato especificado en la especificación ATM Forum UNI Signalling 4.0. En

contraste para una dirección NSAP-encoded son 20 octetos, y para un prefijo de red NSAP-encoded son 13 octetos de longitud.

Grupos MIB

Sub árbol para definir tipo de objetos MIB ATM del Foro ATM

atmForum OBJECT IDENTIFIER ::= { enterprises 353 }

Sub árbol para definir administrativamente tipo de objetos

atmForumAdmin OBJECT IDENTIFIER ::= { atmForum 1 }
atmfTransmissionTypes OBJECT IDENTIFIER ::= { atmForumAdmin 2 }
atmfMediaTypes OBJECT IDENTIFIER ::= { atmForumAdmin 3 }
atmfTrafficDescrTypes OBJECT IDENTIFIER ::= { atmForumAdmin 4 }
atmfSrvcRegTypes OBJECT IDENTIFIER ::= { atmForumAdmin 5 }

Sub árbol para definir tipo de objetos para MIB de interfaz ATM

atmForumUni OBJECT IDENTIFIER ::= { atmForum 2 }
atmfPhysicalGroup OBJECT IDENTIFIER ::= { atmForumUni 1 }
atmfAtmLayerGroup OBJECT IDENTIFIER ::= { atmForumUni 2 }
atmfAtmStatsGroup OBJECT IDENTIFIER ::= { atmForumUni 3 }
atmfVpcGroup OBJECT IDENTIFIER ::= { atmForumUni 4 }
atmfVccGroup OBJECT IDENTIFIER ::= { atmForumUni 5 }
atmfAddressGroup OBJECT IDENTIFIER ::= { atmForumUni 6 }
atmfNetPrefixGroup OBJECT IDENTIFIER ::= { atmForumUni 7 }
atmfSrvcRegistryGroup OBJECT IDENTIFIER ::= { atmForumUni 8 }
atmfVpcAbrGroup OBJECT IDENTIFIER ::= { atmForumUni 9 }
atmfVccAbrGroup OBJECT IDENTIFIER ::= { atmForumUni 10 }
atmfAddressRegistrationAdminGroup OBJECT IDENTIFIER ::= {
atmForumUni 11 }

Definiciones de identificadores de objetos

-- Tipos de transmisión:

atmfUnknownType OBJECT IDENTIFIER ::= { atmfTransmissionTypes 1}
atmfSonetSTS3c OBJECT IDENTIFIER ::= { atmfTransmissionTypes 2 }
atmfDs3 OBJECT IDENTIFIER ::= { atmfTransmissionTypes 3 }
atmf4B5B OBJECT IDENTIFIER ::= { atmfTransmissionTypes 4 }
atmf8B10B OBJECT IDENTIFIER ::= { atmfTransmissionTypes 5 }
atmfSonetSTS12c OBJECT IDENTIFIER ::= { atmfTransmissionTypes 6 }
atmfE3 OBJECT IDENTIFIER ::= { atmfTransmissionTypes 7 }
atmfT1 OBJECT IDENTIFIER ::= { atmfTransmissionTypes 8 }
atmfE1 OBJECT IDENTIFIER ::= { atmfTransmissionTypes 9 }

-- Tipos de medio:

atmfMediaUnknownType OBJECT IDENTIFIER ::= { atmfMediaTypes 1 }
atmfMediaCoaxCable OBJECT IDENTIFIER ::= { atmfMediaTypes 2 }
atmfMediaSingleMode OBJECT IDENTIFIER ::= { atmfMediaTypes 3 }
atmfMediaMultiMode OBJECT IDENTIFIER ::= { atmfMediaTypes 4 }
atmfMediaStp OBJECT IDENTIFIER ::= { atmfMediaTypes 5 }
atmfMediaUtp OBJECT IDENTIFIER ::= { atmfMediaTypes 6 }

-- Tipos descriptores de trafico: Estos son combinados con

elementos vectores de parámetro para describirlos.
atmfNoDescriptor OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes 1 }
atmfPeakRate OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes 2 }
atmfNoClpNoScr OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes 3 }
atmfClpNoTaggingNoScr OBJECT IDENTIFIER ::= {
atmfTrafficDescrTypes 4 }
atmfClpTaggingNoScr OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes
5 }
atmfNoClpScr OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes 6 }
atmfClpNoTaggingScr OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes
7 }
atmfClpTaggingScr OBJECT IDENTIFIER ::= { atmfTrafficDescrTypes 8 }
atmfClpNoTaggingMcr OBJECT IDENTIFIER ::= {
atmfTrafficDescrTypes 9 }

La MIB de administración de enlace provee los siguientes grupos:

- Atributos por sistema
- Atributos por interfaz física
- Atributos por interfaz de la capa ATM
- Estadísticas por interfaz de la capa ATM
- Atributos por trayectoria virtual
- Atributos por ABR para la trayectoria virtual
- Atributos por canal virtual
- Atributos por ABR del canal virtual
- Traps de administración de enlace

Para los atributos por sistema los IMEs deben soportar el grupo de sistema del RFC 1213. Los atributos para la interfaz física están contenidos en el grupo de puerto físico (atmPhysicalGroup). La interfaz física esta definida por el índice de interfaz (atmfPortIndex). La información MIB en este nivel incluye:

- Indice de interfaz
- Dirección de interfaz
- Tipo de transmisión
- Tipo de medio
- Estado operacional
- Información específica de puerto
- Información de adyacencia

El índice de interfaz es usado para identificar una particular interfaz física o virtual en un equipo ATM. El objeto atmfPortIndex tiene el valor 0 en todos los mensajes de SNMP e implícitamente identifica la interfaz sobre la cual los mensajes ILMI son recibidos. El objeto de dirección de interfaz atmfPortAddress es obsoleto y se reemplazo por extensiones de registro de direcciones. El objeto para el tipo de transmisión atmfPortTransmissionType es depreciable y se implementa por requerimiento de compatibilidad. El objeto del tipo de medio atmfPortMediaType es depreciable y se implementa por requerimiento de compatibilidad. El objeto de estado operacional atmfPortOperStatus es depreciable y se implementa por requerimiento de compatibilidad. . El objeto de información específica de puerto atmfPortSpecific es depreciable y se implementa por requerimiento de compatibilidad. Los objetos atmfPortMyIfName, atmfPortMyIfIdentifier, atmfMyIpNmAddress, atmfMyOsiNmNsapAddress y

atmfMySystemIdentifier permiten a los sistemas vecinos mantener sus tablas de sistemas adyacentes para facilitar el auto descubrimiento y trazo de conexiones ATM por los sistemas de administración de red. Incluye el identificador de sistema que identifica al dispositivo ATM local a su IME, el identificador de interfaz que identifica la interfaz ATM administrada por su IME, la dirección a la cual la estación de administración ATM puede enviar mensajes del protocolo de administración de red y el nombre de la interfaz.

Los atributos para la interfaz de la capa ATM son localizados en el grupo de la capa ATM atmfAtmLayerGroup, la interfaz es identificada por el índice de interfaz atmfAtmLayerIndex. La información MIB en este nivel es:

- Índice de interfaz
- Número máximo de bits para VPI activos
- Número máximo de bits para VCI activos
- Número máximo de VPCs
- Número máximo de VCCs
- Número de VPCs configurados
- Número de VCCs configurados
- Máximo SVPC VPI
- Máximo SVCC VPI
- Máximo SVCC VCI
- Tipo de interfaz ATM (Pública/Privada)
- Tipo de dispositivo ATM (Usuario/Nodo)
- Versión ILMI
- Versión de señalización UNI
- Versión de señalización NNI

El objeto del índice de interfaz atmfAtmLayerIndex esta implícito en la interfaz ATM local. El objeto del número máximo de VPIs activos atmfAtmLayerMaxVpiBits es el número máximo de bits de VPI que pueden ser activados para esa interfaz. El objeto del número máximo de VCIs activos atmfAtmLayerMaxVciBits es el número máximo de bits de VCI que pueden ser activados para esa interfaz para el propósito de conmutación de

celdas en un VCC. El objeto del número máximo de VPCs atmfAtmLayerMaxVPCs es el número máximo de VPCs permanentes o conmutados que pueden ser soportados por esa interfaz. Este número incluye el número de PVCs permanentes pre configurados contados por atmfAtmLayerConfiguredVPCs. El objeto del número de VPCs configurados atmfAtmLayerConfiguredVPCs es el número actual de VPCs permanentes para los cuales la interfaz esta configurada a procesar. Este número representa el número de entradas en la atmfVpc. El objeto del número de VCCs configurados atmfAtmLayerConfiguredVCCs es el número actual de VCCs permanentes para los cuales la interfaz esta configurada a procesar. Este número representa el número de entradas en la atmfVcc, el cual debe incluir entradas para todos los VCCs permanentes (p.e. los de señalización, ILMI VCCs) y VCCs no estándar. La señalización en la interfaz ATM es configurada para soportar VPIs destinados para conmutar conexiones de trayectoria virtual de un sencillo y continuo rango de VPIs comenzando con el VPI=1 y terminando con el número indicado por el objeto de la conmutación máxima VPC VPI atmfAtmLayerMaxSvpcVpi como se muestra en la figura.

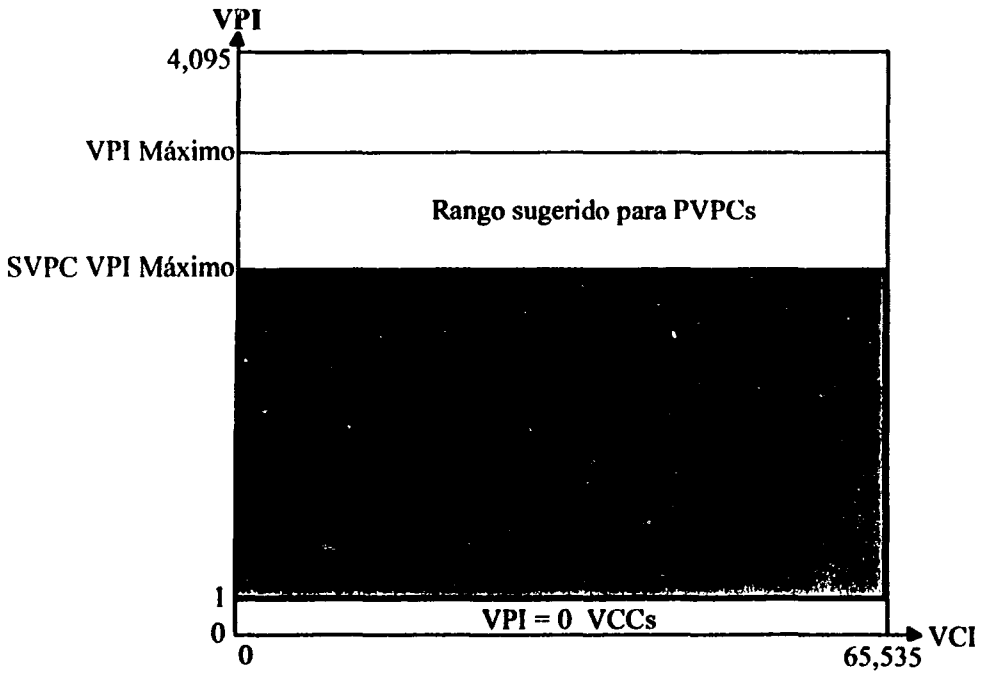


Fig. 5.43 Valores de conmutación VPC y VP

La señalización en la interfaz ATM esta configurada para soportar VPIs destinados para conmutar VCC de un rango continuo de VPIs comenzando con VPI=0 y terminando con el número indicado por el objeto de la máxima conmutación de VCC VPI atmfAtmLayerMaxSvccVpi. La señalización en la interfaz ATM esta configurada para soportar VCIs destinados para conmutar VCCs de un continuo rango de VCIs comenzando con el número indicado por el objeto de la conmutación mínima VCC VCI atmfAtmLayerMaxSvccVci y terminando con el máximo VCI. El mismo valor aplica para todos los valores de conmutación VCC VCI para lo cual la señalización fue configurada.

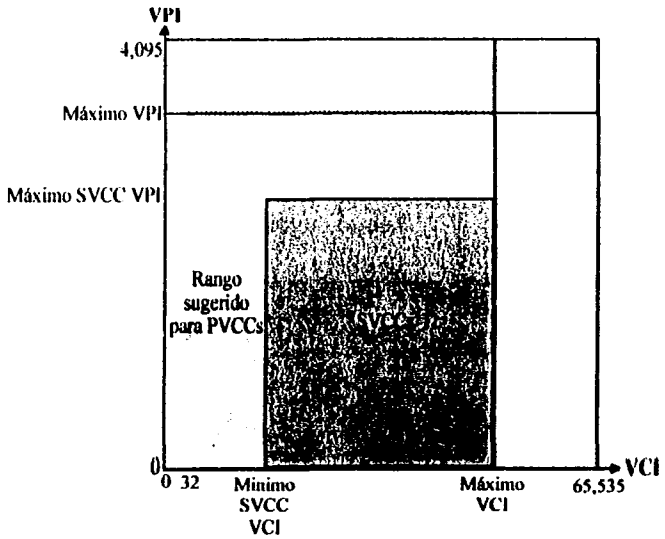


Fig. 5.44 Valores de conmutación VCC, VPI y VCI

El objeto indicador ATM Pública/Privada atmfAtmLayerUniType indica cuando el dispositivo ATM es de tipo público o privado. El objeto de tipo de dispositivo de interfaz ATM atmfAtmLayerDeviceType indica

cuando el dispositivo es de tipo usuario o nodo. El objeto de versión ILMI atmfAtmLayerIlmiVersion indica la última versión de ILMI del Foro ATM soportada en esta interfaz. El objeto de versión UNI atmfAtmLayerUniVersion indica la última versión de señalización ATM UNI soportada en esta interfaz. El objeto de versión NNI atmfAtmLayerNniSigVersion indica la última versión de señalización PNNI del Foro ATM soportada en esta interfaz. La versión de ruteo PNNI no se determinada por ILMI. El grupo de estadísticas de la capa ATM atmfAtmStatsGroup es depreciable y se implementa por requerimiento de compatibilidad. Los atributos de trayectoria virtual están alojados en el grupo de trayectoria virtual atmfVpcGroup. Este grupo es organizado por el índice de interfaz atmfVpcPortIndex y el valor VPI atmfVpcVpi y debe tener entradas atmfAtmLayerConfiguredVPCs. Solo conexiones de trayectorias virtuales permanentes son representadas en este grupo. Para interfaces virtuales (p.e. VPCs usado por PNNI) este grupo esta vacío.

La información MIB en este nivel incluye:

- Índice de interfaz
- Valor VPI
- Estado operacional
- Descriptor de tráfico transmitido
- Descriptor de tráfico recibido
- Indicador de Best Effort
- Clase de QoS transmitido
- Clase de QoS recibido
- Categoría de servicio

El objeto de índice de interfaz atmfVpcPortIndex es el mismo que el definido para la interfaz física. El objeto VPI atmfVpcVpi es el mismo que el definido para el VPI para ese VPC. El objeto de estado operacional atmfVpcOperStatus representa el estado del VPC conocido por el dispositivo local. Si estado punto a punto es conocido entonces un valor end2endUp(2) o end2endDown(3) es usado. Si solo el estado local es conocido entonces un valor de localUpEnd2endUnknown(4) o localDown(5) es usado. El descriptor de tráfico transmitido es una especi ación para el lado transmisor de la interfaz del VPC. El descriptor de tráfico recibido es una

especificación para el lado receptor de la interfaz del VPC. El objeto indicador de Best Effort atmfVpcBestEffortIndicator especifica cuando este es requerido para ese VPC. El objeto de clase de QoS transmitido atmfVpcTransmitQoSClass es depreciable y se implementa por requerimiento de compatibilidad. El objeto de clase de QoS recibido atmfVpcReceiveQoSClass es depreciable y se implementa por requerimiento de compatibilidad. El objeto de categoría de servicio atmfVpcServiceCategory indica la categoría de servicio de ese VPC. El objeto de indicación de descarte de tramas transmitidas atmfVccTransmitFrameDiscard especifica cuando la red esta permitida usar mecanismos de descarte de tramas en la dirección de transmisión de la conexión asociada. El objeto de indicación de descarte de tramas recibidas atmfVccReceiveFrameDiscard especifica cuando la red esta permitida usar mecanismos de descarte de tramas en la dirección de recepción de la conexión asociada. Los atributos ABR para trayectoria virtual se encuentran en el grupo de ABR de canal virtual atmfVccAbrGroup. Este grupo es organizado por el índice de interfaz atmfVccAbrPortIndex, el valor VCC VPI atmfVccAbrGroup y el valor VCC VCI atmfVccAbrVci. En cada entrada en el grupo ABR de canal virtual debe haber correspondencia uno a uno para una entrada en el grupo de canal virtual.

La información MIB en este nivel debe incluir:

- Índice de interfaz
- Valor VPI/VCI
- Parámetros de operación ABR

El objeto de índice de interfaz atmfVccAbrPortIndex es el mismo que el de la interfaz física. El objeto VPI atmfVccAbrVpi es el mismo valor que el de VPI para ese VPC. El objeto VCI atmfVccAbrVci es el mismo valor que el de VCI para ese VCC. Los parámetros usados con VCCs son idénticos a los usados con VPCs. Dos traps son definidos para ILMI, atmfVpcChange y atmfVccChange, para indicar que un VPC o VCC permanente ha sido configurado, modificado o borrado. El trap atmfVpcChange provee el valor VPI de un VPC nuevo o borrado en la interfaz ATM. El trap atmfVccChange provee los valores de VCI y VPI del VCC nuevo o borrado en la interfaz ATM.

5.8.2.6 PROCEDIMIENTOS ILMI
5.8.2.6.1 PROCEDIMIENTOS DE CONEXIÓN.

Los procedimientos de conectividad son usados para el establecimiento y subsecuentemente perdida de conectividad ILMI. Estos procedimientos son usados por los procesos de auto configuración y registro de direcciones. La conectividad ILMI debe ser probada periódicamente una vez establecida. Para propósito de establecer, verificar o restablecer conectividad ILMI el IME transmite un sencillo GetRequest o GetNextRequest para los objetos atmfPortMyIfIdentifier, atmfMySystemIdentifier y sysUpTime. Una coincidencia en el mensaje ILMI de respuesta indica que la conectividad esta establecida. Para detectar el establecimiento de conectividad ILMI el IME prueba esta con mensajes cada S segundos hasta que un mensaje ILMI de respuesta es recibido indicando que la conectividad es establecida. Esto se debe seguir haciendo con el fin de que la conectividad se mantenga. Una vez que el mensaje de ILMI se recibe la auto configuración puede tener comienzo. Para detectar subsecuentes perdidas de conectividad un IME prueba la conectividad con mensajes cada T segundos. La conectividad es declarada como perdida cuando el mensaje ILMI de respuesta no llega en k poleos consecutivos. Para recobrar la conectividad el IME probará con IME cada S segundos o hasta que una falla en el enlace ocurra. El IME indicará que la conectividad ILMI es restablecida después de recibir un mensaje de respuesta ILMI y reinicia la auto configuración y registro de direcciones. Los valores por defecto son k=4, S=1 y T=5 los cuales pueden ser configurados. La señalización puede tolerar fallas de capa física por un periodo de tiempo corto antes de liberar las conexiones existentes. Durante este tiempo un pequeño cambio existe para intercambiar dos enlaces sin que lo detecte la señalización pero los procedimientos de detección de cambio de punto de conexión son usados para detectar estos cambios. Si los procedimientos de detección de cambio de punto de conexión son implementados un IME debe guardar localmente copias de sus objetos atmfPortMyIfIdentifier atmfMySystemIdentifier y sysUpTime y debe inicializar esas variables a un valor ilegal al tiempo que se inicializa el establecimiento de conectividad ILMI. Un IME no debe reinicializar esas variables al tiempo de perdida o subsecuente restablecimiento de la conectividad ILMI. Un IME lee los valores actuales de los objetos atmfPortMyIfIdentifier, atmfMySystemIdentifier y sysUpTime en orden para establecer, verificar o restablecer conectividad ILMI. Un IME podría comparar esos valores retornarlos en un mensaje de respuesta ILMI con la copia local de esos

objetos. Si los valores atmfPortMyIfIdentifier, atmfMySystemIdentifier son diferentes de la copia local y si el valor de sysUpTime es menos que el de la copia el IME declararía que el punto de conexión ha cambiado y:

- Pondría lás copias locales de esos objetos en los valores de retorno
- Declararía que la conexión ILMI se perdió
- Informa su correspondiente entidad de señalización UNI para liberar todos los SVCs controlados por esa entidad.
- Enviaría un trap coldStart a su entidad IME para indicar que la interfaz se esta reiniciando.
- Declararía que la conectividad ILMI es restablecida.
- Reinvocará algún proceso de configuración automático.
- Desarrollaría el registro de direcciones si es necesario.

5.8.2.6.2 PROCEDIMIENTO DE CONFIGURACIÓN AUTOMÁTICA.

Un usuario o nodo privado puede configurar automáticamente sus interfaces ATM como UNI publicas, UNI privadas o PNNI y el tipo de IME como User-Side, Network-Side o Symmetric. Si la configuración automática es usada el usuario o nodo desarrollarían el procedimiento pudiendo no enviar algún mensaje no ILMI sobre la interfaz ATM hasta que el procedimiento de configuración se ha completado. Esta información de tipo de interfaz puede ser usada por otros protocolos ATM para su operación como la señalización UNI, PNNI y protocolos de enrutamiento. Como parte del proceso de auto configuración si el objeto atmfAtmLayerUniType para un puerto en un dispositivo ATM tiene el valor privado, entonces el IME traería los valores atmfAtmLayerDeviceType y atmfAtmLayerUniType y determina el valor del tipo de interfaz de acuerdo a la siguiente tabla.

Tipo de dispositivo Local[2]	Tipo de dispositivo par[3]	Tipo de UNI par[4]	Tipo de interfaz[5]	Tipo de IME[6]
User(1)	NoSuchName	Public(1)	Public UNI	User-Side
User(1)	NoSuchName	Private(2)	Private UNI	User-Side
User(1)	Node(2)	Public(1)	Public UNI	User-Side
User(1)	Node(2)	Private(2)	Private UNI	User-Side
User(1)	User(1)	N/A	Undefined[7]	Undefined[7]
Node(2)	NoSuchName	Public(1)	Public UNI	User-Side
Node(2)	NoSuchName	Private(2)	Private UNI	Network-Side
Node(2)	Node(2)	Public(1)[9]	Public UNI	User-Side
Node(2)	Node(2)	Private(2)[9]	Ver nota 10	Ver nota 11
Node(2)	User(1)	Public(1)	Undefined[8]	Undefined[8]
Node(2)	User(1)	Private(2)	Private UNI	Network-Side

Tabla 5.5 determinación del tipo de interfaz para dispositivos privados.

Nota 1 La determinación del tipo de interfaz para dispositivos públicos esta fuera del alcance de esta relación.
Nota 2 Valor retornado de los objetos locales atmfAtmLayerUniType y atmfAtmLayerDeviceType
Nota 3 Valor retornado del objeto remoto atmfAtmLayerDeviceType
Nota 4 Valor retornado del objeto remoto atmfAtmLayerUniType
Nota 5 Tipo de interfaz resultante
Nota 6 Tipo de IME resultante
Nota 7 El resultado de conectar un usuario a un usuario es indefinido
Nota 8 El resultado de conectar un nodo privado a un usuario publico es indefinido
Nota 9 Para que un switch ATM de red publica pueda soportar un tipo de interfaz PNNI debe indicar su atmfAtmLayerUniType como privada.
Nota 10 El tipo de interfaz resultante es IISP si el local y par atmfAtmLayerNniSigVersion es iisp o PNNI si el local y par atmfAtmLayerNniSigVersion es pnniVersion1point0.
Nota 11 El tipo de IME resultante es User-Side si el tipo de interfaz es IISP y el atmfMySystemIdentifier local es más grande que atmfMySystemIdentifier, Network-Side si el tipo de interfaz es IISP y el atmfMySystemIdentifier es más pequeño que el atmfMySystemIdentifier, y el tipo de interfaz es Symmetric si el tipo de interfaz es PNNI.

Un IME puede también configurar automáticamente un número de atributos de interfaz de capa ATM. UNI define valores de parámetro de trafico por defecto para la señalización VCC. Esta sección especifica procedimientos los cuales pueden ser usados para configurar automáticamente diferentes valores para uso en una interfaz en particular. Previamente para intentar el establecimiento de conectividad ILMI, el IME inicializará sus valores locales de los objetos atmfVccServiceCategory, atmfVccBestEffortIndicator, atmfVccReceiveTrafficDescriptorType,atmfVccReceiveTrafficDescriptorParam1,atmfVccReceiveTrafficDescriptorParam2,atmfVccReceiveTrafficDescriptorParam3,atmfVccReceiveTrafficDescriptorParam4 y atmfVccReceiveTrafficDescriptorParam5 para VPI=0, VCI=5. Antes de que la señalización de canal sea inicializada el IME leerá el valor de los objetos atmfVccServiceCategory,atmfVccBestEffortIndicator,atmfVccReceiveTrafficDescriptorType,atmfVccReceiveTrafficDescriptorParam1,atmfVccReceiveTrafficDescriptorParam2,atmfVccReceiveTrafficDescriptorParam3,atmfVccReceiveTrafficDescriptorParam4, and atmfVccReceiveTrafficDescriptorParam5 para VPI=0, VCI=5.

Si el objeto atmfVccServiceCategory no existe o si el valor leído no es valido pero un valor valido leído del objeto atmfVccReceiveTrafficDescriptorType el IME asumirá un valor para atmfVccServiceCategory como se muestra en la tabla:

atmfVccReceiveTrafficDescriptorType	**DefaultatmfVccServiceCategory**
atmfNoClpNoScr	ubr(6)
atmfNoClpScr	nrtvbr(4)
atmfClpNoTaggingScr	nrtvbr(4)
atmfClpTaggingScr	nrtvbr(4)
atmfClpNoTaggingMcr	abr(5)

Tabla 5.6 atmfVccServiceCategory por defecto.

Después de determinar la categoría de servicio el nodo determinará si uno de las combinaciones de la siguiente tabla han sido leídas.

atmfvccservicecategory	atmfvccreceivetrafficdescriptortype	atmfvccbesteffortindicator
cbr(2)	atmfnoclpnoscr	false(2)
rtvbr(3)	atmfnoclpscr o atmfclpnotaggingscr o atmfclptaggingscr	false(2)
nrtvbr(4)	atmfnoclpscr or atmfclpnotaggingscr o atmfclptaggingscr	false(2)
abr(5)	atmfclpnotaggingmcr	false(2)
ubr(6)	atmfnoclpnoscr	false(2)

Tabla 5.7 combinaciones de parámetros de transmisión validos.

Si una combinación valida ha sido leída y la categoría de servicio son las mismas en ambos IMEs para una particular dirección, entonces el IME determinará el contrato de trafico para la señalización VCC para tomar por cada parámetro de trafico el mínimo de su valor local atmfVccTransmitTrafficDescriptorParam y el valor atmfVccReceiveTrafficDescriptorParam excepto para el CDVT el cual es determinado solo por el valor de atmfVccReceiveTrafficDescriptorParam.

Cuando modificaciones locales son realizadas para el grupo de trayectoria virtual o el grupo de canal virtual un apropiado trap de administración de enlace es enviado para notificar el IME par. Cuando el valor de otros objetos por ejemplo los atributos de la interfaz de la capa ATM es modificado, el IME debe ser reinicializado para efectuar el cambio. El IME:

- Declarará la perdida de conectividad ILMI
- Informará a ala entidad de señalización UNI o PNNI para desconectar todas las conexiones.
- Reinicializar el sysUpTime a cero

- Enviará un trap coldStart a su entidad IME par para indicar el reinicio de la interfaz
- Reinvocar algún procedimiento de auto configuración
- Desarrollar registro de direcciones si es necesario
- Declarar que la conectividad ILMI será restablecida.

5.8.2.7 MIB DE REGISTRO DE DIRECCIONES

La MIB de registro de direcciones provee objetos SNMP para el intercambio de información de direcciones ATM. Esta información consiste de dos tablas:

- Prefijo de red. Implementado en el sistema final ATM vía el atmfNetPrefixGroup. El switch ATM envía un mensaje SetRequest en el prefijo del byte 13 de alto orden configurado en ese puerto del switch. En la inicialización los registros de prefijo de red ocurren primero.
- Dirección ATM. Implementada en el switch ATM vía el atmfAddressGroup. El sistema final ATM primero recibe un SetRequest en el prefijo de red y registra ese prefijo en su tabla de prefijos. Luego el sistema final ATM combina el prefijo con su identificador de estación final (end-station identifier ESI) y envía un SetRequest en el byte 20 de la dirección ATM. Finalmente el switch ATM escoge registrar la dirección en su tabla de direcciones ATM. La tabla de direcciones ATM usa dos objetos clave:

- AtmfAddressAtmAddress. Objeto de dirección ATM consistente del octeto 20 de la dirección privada ATM.
- AtmfAddressStatus. Es un objeto que indica la validación de una dirección ATM. Un sistema final ATM configura una nueva dirección ATM enviando un SetRequest y se coloca el objeto de estado de dirección ATM para validar el estado. Un sistema final ATM borra una dirección ATM existente por el envío de SetRequest y se coloca el objeto de estado de dirección ATM para validar el estado.

Tanto el switch ATM como el sistema final ATM necesitan mantener actualizadas las tablas de direcciones desde que las direcciones son usadas en número de parte llamada y número de parte que llama, campos de elementos de información de mensajes de señalización enviados cuando SVCs se comienzan a establecer.

El objeto atmfAddressRegistrationAdminStatus indica soporte para los grupos de prefijo y dirección. ILMI 4.0 propone el uso de los grupos de prefijo y dirección en la interfaz UNI privada. Si el equipo distante devuelve un error de noSuchName indicando que este es un equipo pre-ILMI 4.0, el equipo cercano debe asumir que el equipo distante soporta registro de direcciones. Si solo un lado soporta registro de direcciones, la especificación ILMI 4.0 sugiere que soporte de este lado reporte una condición de alarma UNI-misconfiguration o escoja obtenerla de otra manera, el otro extremo simplemente podría devolver el error noSuchName para cualquier requerimiento de registro.

Switch ATM (Lado - Red)	
Acción:	Cuando un sistema recibe un SetRequest del sistema final para la entrada de una dirección ATM en la tabla, el switch ATM valida la dirección anunciada para prevenir duplicación de direcciones.
Si la validación falla:	Responde con un GetResponse conteniendo un error badValue.
Si la validación es exitosa:	Responde con un GetResponse indicando noError y actualiza la tabla de direcciones.

Cuando un sistema final ATM da de baja un registro de dirección ATM, el switch ATM no debe liberar conexiones/llamadas asociadas con la dirección eliminada de la tabla.

Sistema final ATM (Lado - Usuario)	
Acción:	Valida un SetRequest para el objeto de prefijo de red.
Si la validación falla:	Responde con un GetResponse conteniendo el apropiado error.
Si la validación es exitosa:	Responde con un GetResponse indicando noError y actualiza la tabla de prefijos de red si este todavía no esta registrado.

5.8.2.8 MIB DE REGISTRO DE SERVICIOS

Esta especificación extiende la MIB de interfaz ATM para proveer un registro de servicio de propósito general para alojar servicios de red ATM tales como LAN Emulation Configuration Server (LECS) y el ATM Name Server (ANS). Para estos registros se tienen las siguientes definiciones MIB.

DEFINICIONES ATM-FORUM-SRVC-REG
IMPORTES
atmfSrvcRegTypes,
atmfSrvcRegistryGroup,
AtmAddress DE ATM-FORUM-TC-MIB
TIPO DE OBJETO DE RFC-1212;
-- Definiciones de identificador de objeto
Los siguientes valores son definidos para uso de valores probables del objeto atmfSrvcRegServiceID
-- LAN Emulation Configuration Server (LECS)
atmfSrvcRegLecs IDENTIFICADOR DE OBJETO ::= { atmfSrvcRegTypes 1 }
-- Cuando atmfSrvcRegServiceID tiene un valor de atmfSrvcRegLecs, el valor de atmfSrvcRegParm1 es ignorado.
-- ATM Name Server (ANS)
atmfSrvcRegAns IDENTIFICADOR DE OBJETO::= { atmfSrvcRegTypes 2 }
-- Cuando atmfSrvcRegServiceID tiene un valor de atmfSrvcRegAns,
el valor de atmfSrvcRegParm1 es ignorado.

-- Tabla de registro de servicio. La tabla de registro de servicio es implementada por el IME TIPO DE OBJETO atmfSrvcRegTable del lado – red.
SECUENCIA DE SINTAXIS atmfSrvcRegEntry
ACCESO not-accessible
ESTADO mandatory
DESCRIPCION
"La tabla implementrada por el IME en el lado – red en el puerto ATM UNI contiene todos los servicios que estan disponibles para el IME de lado – usuario indexados por el identificador de servicio."
::= { atmfSrvcRegistryGroup 1 }
atmfSrvcRegEntry OBJECT-TYPE
SYNTAXIS AtmfSrvcRegEntry
ACCESO not-accessible
ESTADO mandatory
DESCRIPCION
"Información a cerca de un proveedor de servicios que esta disponible para el IME lado - usuario."
INDICE {atmfSrvcRegPort, atmfSrvcRegServiceID, atmfSrvcRegAddressIndex}
::= { atmfSrvcRegTable 1 }
AtmfSrvcRegEntry ::=
SECUENCIA {
atmfSrvcRegPort
NÚMERO ENTERO,
atmfSrvcRegServiceID
IDENTIFICADOR DE OBJETO,
atmfSrvcRegATMAddress
AtmAddress,
atmfSrvcRegAddressIndex
NÚMERO ENTERO,
atmfSrvcRegParm1
SERIE DE OCTETOS}
atmfSrvcRegPort OBJECT-TYPE
SYNTAXIS DE NÚMEROS ENTEROS (0..2147483647)
ACCESO not-accessible
ESTADO mandatory
DESCRIPCION
"El valor de 0 es una forma especial de identificar la interfaz ATM sobre la cual el mensaje fue recibido."

::= { atmfSrvcRegEntry 1 }
atmfSrvcRegServiceID OBJECT-TYPE
SYNTAXIS IDENTIFICADOR DE OBJETO
ACCESO not-accessible
ESTADO mandatory
DESCRIPCION
"Este es el identificador de servicio el cual unicamente identifica el tipo de servicio a la dirección provista en la tabla."
::= { atmfSrvcRegEntry 2 }
atmfSrvcRegATMAddress OBJECT-TYPE
SYNTAXIS AtmAddress
ACCESO read-only
ESTADO mandatory
DESCRIPCION
"Esta es la dirección del servicio. El IME lado – usuario puede usar esta dirección para establecer una conexión con el servicio."
::= { atmfSrvcRegEntry 3 }
atmfSrvcRegAddressIndex OBJECT-TYPE
SYNTAXIS DE NÚMEROS ENTEROS (1..2147483647)
ACCESO not-accessible
ESTADO mandatory
DESCRIPCION
"Un número entero arbitrario diferencia múltiples conjuntos que contienen diferentes direcciones ATM para el mismo servicio en el mismo puerto."
::= { atmfSrvcRegEntry 4 }
atmfSrvcRegParm1 OBJECT-TYPE
SYNTAXIS SECUENCIA DE OCTETOS (TAMAÑO (1..255))
ACCESO read-only
ESTADO mandatory
DESCRIPCION
"El tamaño y significado de la serie de octetos es determinada por el valor de atmfSrvcRegServiceID."
::= { atmfSrvcRegEntry 5 }

5.8.3 FUNCIONES DE OPERACIÓN Y MANTENIMIENTO OAM.

La recomendación del ITU T I.610 describe las funciones de operación y mantenimiento de la capa física y de la capa ATM en la UNI. El mantenimiento es definido en la recomendación M.60 como la combinación de todas las tecnicas y correspondientes acciones administrativas (incluyendo funciones de supervisión) necesarias para mantener o restablecer un estado en la cual se pueda desempeñar una función requerida.

La siguiente figura muestra los procesos involucrados para las funciones OAM.

Fig. 5.45 Flujo de procesos de OAM

El monitoreo de la red ATM involucra observar las fallas e invocar acciones de mantenimiento y/o comandos correctivos para resolver las fallas. Esto involucra comparar mediciones de desempeño

La siguiente tabla muestra las cinco fases o tipos de acción que son utilizadas por la ITU para OAM.

Nombre	Acción	Resultado
Monitoreo de desempeño	Funcionamiento normal de la entidad administrada por un continuo o periódico chequeo de funciones	Es producida información de eventos de mantenimiento
Detección de fallas y defectos	Malfuncionamientos o predicción de los mismos es detectada por continuos o periódicos chequeos	Es producida información de eventos de mantenimiento o alarmas
Protección del sistema	El efecto de falla de una entidad administrada hacia otra entidad es minimizada al ser bloqueada	La entidad de falla es excluida de la operación
Información de falla o desempeño	Información de falla es proporcionada a otras entidades administradas	Indicadores de alarma son dados a otros planos de administración.
Localización de fallas	Determinación por pruebas internas o externas al sistema de una entidad de falla si la información es insuficiente	

Tabla 5.8 Acciones OAM

Las funciones son implementadas como flujos de información bidireccional que son definidas en cinco niveles, asociados con las capas física y ATM.

La fig. 5.16 relación jerárquica entre capas muestra la relación entre flujos con etiquetas desde F1 hasta F5 y la estructura jerárquica del modelo de referencia B-ISDN. Como ejemplo de un flujo OAM dos puntos podrían monitorear un VPC por medio de una prueba de loopback. Durante la fase de monitoreo cada celda recibida en un punto terminal podría ser retransmitida de regreso a la fuente que la envío.

La tabla 5.9 lista las funciones OAM en la capa ATM.

Nivel	Función	Flujo	Detección de falla	Sistema de protección e información de fallas
Trayectoria virtual	Monitoreo de trayectoria virtual disponible		Trayectoria no disponible	Para estudio futuro
	Monitoreo de desempeño	F4	Desempeño degradado	
Canal Virtual	Monitoreo de canal virtual disponible	F5	Canal no disponible	Para estudio futuro
	Monitoreo de desempeño		Desempeño degradado	

Tabla 5.9 Funciones OAM de la capa ATM

El monitoreo de la disponibilidad se lleva a cabo en el nivel de la trayectoria virtual y el monitoreo de desempeño en los niveles de trayectoria y canal virtual. Esos flujos de OAM son provistos por celdas dedicadas para funciones OAM en la capa ATM. Las celdas OAM de la capa ATM son identificadas por el campo del tipo de carga útil en el encabezado de la celda y por VPI/VCI.

Celdas ATM son usadas para levar información de operaciones OAM. Un VPI = 0 y un VCI = 9 identifican a las celdas OAM. La siguiente tabla es muestran funciones OAM para la capa física. Las celdas OAM son identificadas por valores prefijados de encabezado de celdas, uno para cada nivel de flujo de información.

Nivel	Función	Detección de falla
Sección de regeneración	OAM de la capa física (Physical-layer PLOAM) reconocimiento de celda	Perdida de PLOAM de reconocimiento de celda
Sección digital	PLOAM reconocimiento de celda	Perdida de PLOAM de reconocimiento de celda
	Sección de monitoreo de errores	Degradación de desempeño por errores
	Sección de reporte de errores	Degradación de desempeño por errores
Trayectoria de transmisión	Monitoreo de estado de red cliente (CN)	Señal de indicación de alarma de CN
	Delineación de celda	Perdida de sincronía de celda
	Detección/corrección de error de encabezado	Encabezado incorregible
	Monitoreo de desempeño por error de encabezado	Degradación de desempeño por errores de encabezado
	Desacoplamiento de la velocidad de celda	Falla de inserción y supresión de celdas libres

Tabla 5.10 Funciones OAM de la capa física

Una parte fundamental de la infraestructura de la administración de la red es la información de OAM.

5.8.4 FORMATO Y TIPOS DE CELDAS OAM.

La siguiente figura muestra el formato de celda OAM donde están los flujos F4 de trayectoria virtual y flujos F5 de canal virtual entre conexiones de puntos terminales que son definidos como flujos OAM punto a punto.

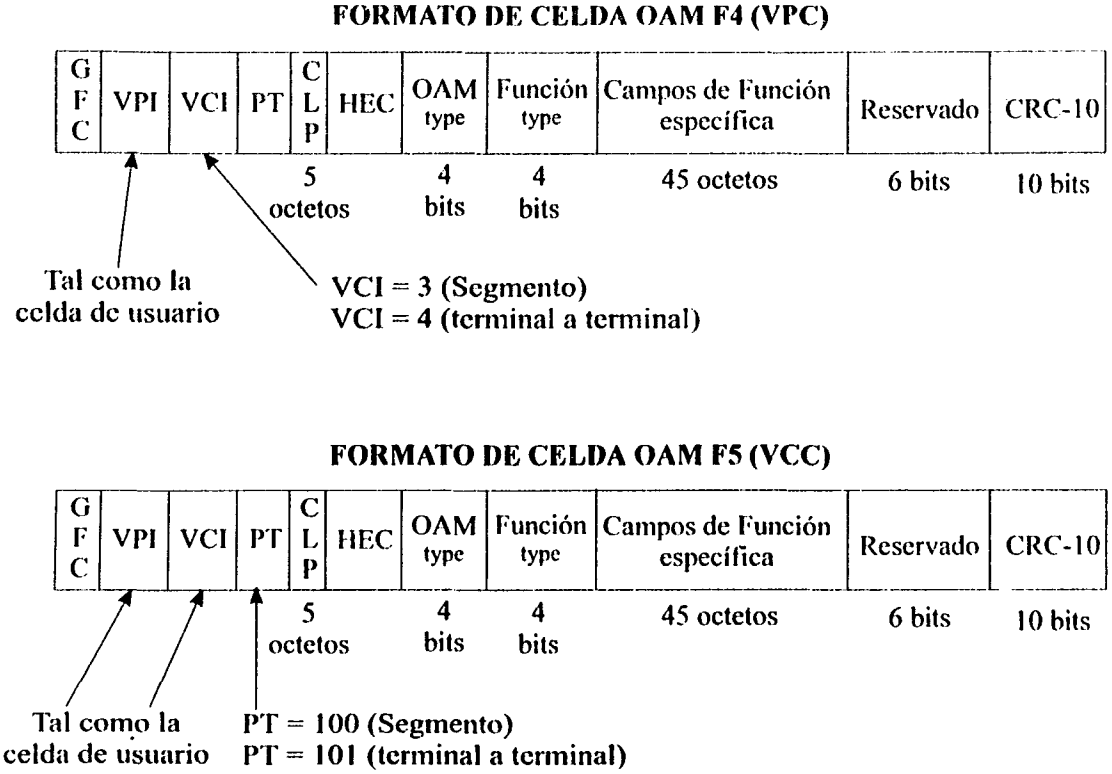


Fig. 5.46 Formato y tipos de celdas OAM

Los flujos de segmento OAM son los flujos F4 y F5 que ocurren a través de uno o más enlaces interconectados VC o VP. Los flujos VP utilizan diferentes VCIs para identificar si el flujo es terminal a terminal (VCI = 3) o si es de un segmento (VCI = 4). El tipo de carga útil (payload type PT) diferencia entre flujo terminal a terminal (PT = 100) y segmento (PT = 101) en un VCC.

La siguiente tabla sumariza los tipos y tipos de campos de funciones de celdas OAM mencionadas y referenciadas a la figura anterior.

Tipo de OAM		Tipo de función	
Administración de fallas	0001	AIS	0000
	0001	RDI/FERF	0001
	0001	Chequeo de continuidad	0100
	0001	Loopback	1000
Administración de desempeño	0010	Monitoreo hacia adelante	0000
	0010	Reporte hacia atrás	0001
	0010	Monitoreo y reportes	0010
Activación/Desactivación	1000	Monitoreo de desempeño	0000
	1000	Chequeo de continuidad	0001

AIS = Alarm Indication Signal
RDI = Remote Defect Indication
FERF = Far End Reporting Failure

Tabla 5.11 Tipos de OAM y tipos de funciones OAM

5.8.4.1 ADMINISTRACIÓN DE FALLAS

La administración de fallas determina cuando ocurre una, notifica a otros elementos de la conexión y provee los mecanismos para diagnosticar y aislar la falla. La siguiente figura muestra los campos de funciones especificas AIS, RDI/FERF.

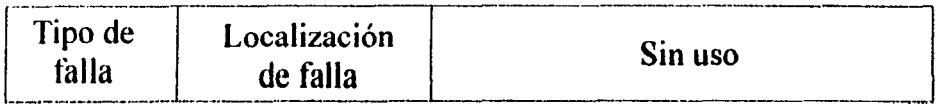


Fig. 5.47 Campos de funciones especificas AIS y RDI/FERF

El tipo de falla es una indicación del tipo de falla ha ocurrido. Cuando esta se presenta el equipo adyacente a esta envía una señal AIS hacia atrás indicando que ha ocurrido una falla hacia adelante y los extremos generan una señal RDI/FERF.

La localización de la falla es un indicador de donde ha ocurrido la falla. Una vez detectada una condición de falla la celda OAM es enviada periódicamente, el periodo de generación de estas celdas es del orden de segundos.

La siguiente figura muestra los campos de la función especifica de Loopback.

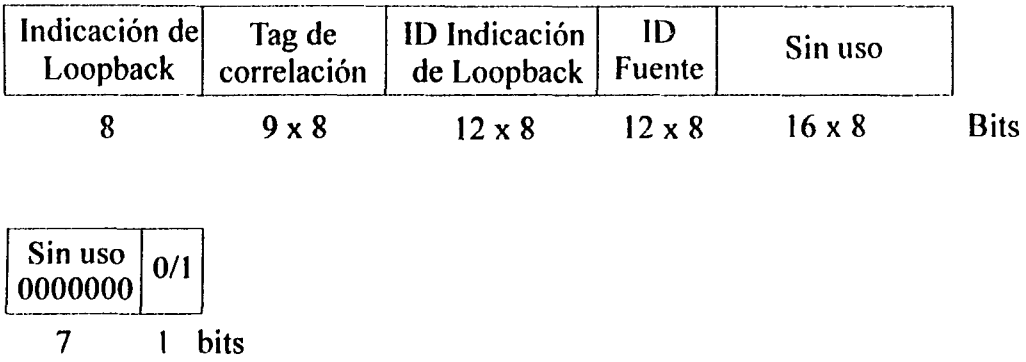


Fig. 5.48 Campos de función especifica Loopback

La indicación de loopback es un campo que contiene 01 cuando es originado y es decrementado por el receptor. Este es extraído cuando es recibido con un valor de 00.

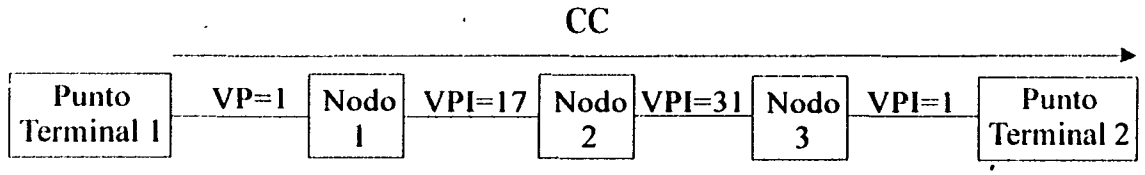
El tag de correlación es un campo definido para ser usado por el originador de la celda OAM para diferenciar celdas OAM dentro de un particular VPC/VCC y saber también cual ha sido recibida.

El ID de identificación de loopback es un campo que provee a la fuente y al receptor una manera de identificar donde un loopback puede ocurrir en un segmento. El valor por defecto es todos a 1 e indica que el loopback puede ocurrir en el punto terminal.

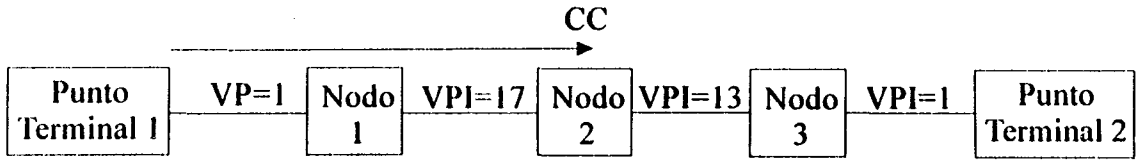
El ID fuente es provisto para que la fuente del loopback pueda ser identificada en la celda. Este puede ser usado por nodos para extraer las celdas OAM que se han insertado para extraerlas después de que han cumplido un lazo de regreso a la fuente.

La idea de checar continuidad es que los puntos terminales envíen una celda periódicamente en un intervalo predeterminado tal que la conexión de los puntos y los otros puntos terminales puedan distinguir entre una conexión que esta libre y una que tiene falla. Esta función es considerada para VPs. El checar la continuidad nos permite ver cosas que AIS no puede tal como un mal cambio en la interconexión de VPs. La siguiente figura muestra pruebas de continuidad.

A) Conexión de Trayectoria virtual inicial



B) Cambio erróneo



C) Notificación de falla

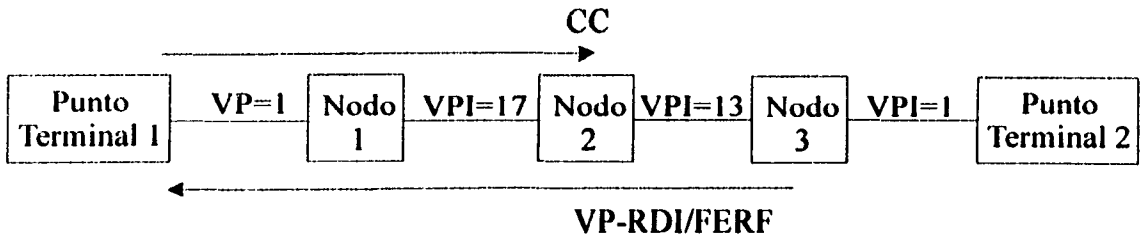


Fig. 5.49 Chequeo de continuidad CC usando celdas OAM

La parte A) muestra una conexión VP que atraviesa tres VPs que interconectan nodos con un mapa de VPI como se ve en la figura y transportando solo celdas CC. En la parte B) un error de interconexión es llevado a cabo en el Nodo 2 interrumpiendo el flujo de celdas CC. En la parte C) el Nodo 3 detecta esta falla de continuidad y genera una celda OAM VP-RDI/FERF en la dirección opuesta.

5.8.4.2 ADMINISTRACIÓN DE DESEMPEÑO

El desempeño de la red es observado por la red en varios puntos y la calidad de servicio (QoS) es vista por el usuario terminal a terminal. La figura siguiente muestra los campos de función específica de celda OAM Activación/Desactivación.

ID de Mensaje	Direcciones de acción	Tag de correlación	Bloque PM Tamaños A-B	Bloque PM Tamaños B-A	Octetos sin uso
6	2	8	4	4	42x8 bits

Fig. 5.50 Campos de celda OAM de la función específica de Activación/desactivación

El ID de mensaje es definido como:

000001	Requerimiento de activación
000010	Confirmación de activación
000011	Denegado el requerimiento de activación
000101	Requerimiento de desactivación
000110	Confirmación de desactivación
000111	Denegado el requerimiento de desactivación

La dirección de la activación es especificada como A-B (10) del activador o como B-A (01) del activador

Tamaño de bloque A-B identifica el tamaño del bloque de la medición de desempeño (PM) que puede ser soportado de A a B por una mascara de bit para tamaños de 1024, 512, 256 o 128 del bit más al menos significativo.

Tamaño de bloque B-A identifica el tamaño del bloque de la medición de desempeño (PM) que puede ser soportado de A a B por una mascara de bit para tamaños de 1024, 512, 256 o 128 del bit más al menos significativo.

Para los procesos de medición de desempeño y chequeo de la continuidad de la red entre sistemas terminales y segmentos se genera un requerimiento de activación que puede o no ser confirmado por la otra terminal extremo del proceso quedando activo o no el proceso ejecutado, intercambiando los mensajes y celdas arriba mencionados. Los procesos de activación y desactivación permiten medir el desempeño de la red en VPCs y VCCs.

La figura que sigue muestra la función específica de medición de desempeño en una celda OAM.

Número de Secuencia de Monitoreo (MSN)	Número total de celdas de usuario (TUC)	BIP-16	Marca de tiempo	Sin uso	Errores resultantes de bloque	Contador de Perdida/ mal inserción de celda
8	2x8	2x8	4x8	33x8	8	2x8 b

Fig. 5.51 Campos de celda OAM de la función específica de medición de desempeño

El tipo de función indica el tipo de función que comienza a ser ejecutada.

Monitoreo hacia adelante 0000
Reporte hacia atrás 0001
Ambos 0010

Número de secuencia de monitoreo (monitoring sequence number MSN) es el número de celda PM, módulo 256.

Número total de celdas de usuario (total user cell number TUC) es el total de celdas contenidas de datos de usuario enviadas desde la última celda PM.

BIP-16 es un código de detección de errores que se ejecuta sobre todas las celdas de usuario desde la última celda PM. Es sado para una estimación de los errores.

Marca de tiempo es un campo usado en el reporte hacia atrás para estimar el retardo. Esta especificada una exactitud de 1 microsegundo o menos.

Los errores resultantes de bloque es un contador de los errores detectados por BIP-16 en el último bloque del reporte hecho hacia atrás.

Las celdas mal insertadas o perdidas es un número que indica el número de celdas recibidas actualmente menos el número TUC desde la última celda PM.

La recomendación I.356 define los parámetro de desempeño para ATM como:

- Taza de error de celda
- Taza de errores severos de bloque de celda
- Taza de perdida de celda
- Taza de perdida de inserción de celda
- Retardo de transferencia de celda
- Retardo de transferencia de celda seria
- Variación del retardo de celda

La taza de errores de celda se define como:

$$\text{Taza de errores de celda} = \frac{\text{Celdas erróneas}}{\text{Celdas transferidas satisfactoriamente} + \text{Celdas erróneas}}$$

La taza de errores severos de bloque de celda para una o más conexiones esta definida como:

$$\text{Taza de errores severos de bloque de celda} = \frac{\text{Errores severos de bloque de celda}}{\text{Total de bloques de celdas transmitidas}}$$

Un bloque de celdas es una secuencia de celdas transmitidas consecutivamente en una dirección dada. Errores severos ocurren cuando más de un número específico de errores de celda, celdas perdidas o mal insertadas son observadas en un bloque de celdas recibido.

La taza de perdida de celda esta definida para una o más conexiones como:

$$\text{Taza de perida de celda} = \frac{\text{Perdida de celda}}{\text{Total de celdas transmitidas}}$$

La taza de perdida de inserción de celda esta definida para una o más conexiones como:

$$\text{Taza de perida de inserción de celda} = \frac{\text{Perdida de inserción de celda}}{\text{Intervalo de tiempo}}$$

El retardo de transferencia de celda esta definido como el tiempo entre un evento de salida de celda de la UNI fuente y un evento de entrada de celda en la UNI destino para una conexión en particular. Solo el retardo total puede ser estimado usando celdas OAM PM. La fuente y el destino tienen un reloj y una marca de tiempo en común. La fuente periódicamente envía celdas OAM PM e inserta su marca de tiempo . Las celdas entran a la red y experimentan variación de retardos. Con una celda OAM PM sale de la red y entra a su destino la marca de tiempo es extraída y varias operaciones son procesadas ahí. Primero el retardo absoluto es calculado como la diferencia entre la marca de tiempo local y la recibida en la celda OAM PM. Un valor de retardo almacenado anteriormente en memoria es sacado de esta y se calcula una diferencia entre este valor y el obtenido de las marcas de tiempo para verificar una diferencia de retardos. Este valor se guarda en memoria para cálculos posteriores de variación de retardo.

5.8.5 APLICACIÓN

Como hemos visto a lo largo de este trabajo una de las partes fundamentales de una red de datos es su administración. Una red grande o pequeña bien administrada tendra menos problemas y las fallas que pudieran ocurrir podran ser corregidas en menor tiempo.

5.8.5.1 REQUERIMIENTOS PARA ADMINISTRACION DE REDES

Uno de los requerimientos principales para un usuario es de que uso de la red sea fácil . esto implica para el administrador de red ciertas considesraciones para poder llevar esa tarea a cabo:

Controlar el creciemiento de la red: las redes y recursos distribuidos de computo estan incrementandose y se vuelven recurso vitales para muchas organizaciones. Sin un control efectivo estos recursos no se administran correctamente y no proveen las retribuciones esperadas por los administradores.

Controlar la complejidad: el continuo crecimiento en el número de elementos de la red hace que la red se haga dificil de controlar que esta conectado y que recursos se tienen.

Improvización de servicios: los usuarios finales esperan el mismo servicio
Sin importar que la red crezca y se distribuya.

Balancear necesidades: la información y recursos de computo de una organización debe de proveer una amplia variedad de applicaciones a diferentes niveles de soporte para los usuarios finales con requerimientos específicos en las areas de funcionamiento, disponibilidad y seguridad. El administrador de red debe controlar esos recursos para balancear esas necesidades.

Reducir tiempos de caída:los recursos deben de tener alta disponibilidad, es decir la red nunca debe de dejar de funcionar, debe para esto tener un cierto nivel de redundancia .

Control de costos: la utilización de recursos debe ser monitoriada y controlada para habilitar necesidades del usuario a un costo razonable.

Los puntos anteriores son prácticos para llevar a cabo una buena administración de recursos de una red. La Organización Internacional para Standarización (OSI) desarrollo 5 áreas funcionales para la administración de redes, aunque esta clasificación fue desarrollada dentro del ambiente OSI, ha sido aceptada por muchos vendedores para crear sistemas propietarios de administración de redes.

En este caso tenemos el uso de un protocolo de adminitración para administrar nuestra red , el SMNP (Simple Network Management Protocol) o Protocolo de Administración Simple de Red, el cual es una herramienta que nos sirve para obtener datos almacenados en los equipos de red que cuentan con este protocolo (actualmente la mayoría de los equipos de red o con conexión a red cuentan con este protocolo) dichos datos son extraidos mediante un poleo de una base de datos del equipo denominada MIB.

Las ventajas de utilizar un protocolo como SNMP para administrar una red son:

- Esta presente en casi todos los equipos de comunicaciones
- Es estandarizado
- Es simple
- No ocupa mucho tiempo de procesamiento del equipo

Las desventajas son:

- Es necesario un software adicional para utilizarlo adecuadamente y puede ser de costo elevado.
- Carece de la adecuada seguridad necesaria (aun utilizando SNMPv3)
- Mal configurado puede saturar la red con demasiados poleos de los equipos

Como en nuestro caso administraremos una red ATM , tenemos algunas formas de hacerlo. De la forma nativa de ATM , es decir a través de celdas OAM y con el protocolo ILMI o con una plataforma de administración que a traves de SNMP nos ayude a recoger información que nos ayude a administrar nuestra red. Para esto sera necesario contar con una

plataforma de administración o NMS propietaria de algun fabricante como es el caso de CISCOWORKS o de forma general tales como HP OpenView, Spectrum, etc. Estas plataformas generalmente son de ambiente gráfico para facilitar el uso de ventanas con gráficas, estadísticas, mapas de ubicación o topologías que la misma plataforma crea o que el usuario dependiendo de sus necesidades modela para administrar sus equipos y pueden ser utilizadas con sistemas operativos como UNIX o Windows NT.

La plataforma que debido a sus características de capacidad , gráficos , facilidad de uso ,etc con los que debe de contar una plataforma de administración elegimos a Spectrum de Cabletron Systems, para administrar nuestros equipos ATM.

Hay que tener en cuenta que el software de la plataforma de administración es costoso (el fabricante generalmente los vende modulares para que el usuario adquiera los modulos necesarios para su red) y adicionalmente tenemos que contar con el Hardware necesario (servidores) y también con las licencias que requiere el software como tal. Al estar hablando de una red ATM podemos deducir que el costo del software en custión no impacta tanto como lo es el adquirir los switches ATM y la infraestructura de la red en gneral como pueden ser routers, enlaces, etc. y el costo beneficio es mayor ya que estamos hablando de enlaces de gran capacidad como STM-1 el cual si se nos llega a caer y no es levantado en un tiempo considerable puede producir demasiadas pérdidas a la empresa u organización.

Es indispensable que contemos con una o varias personas capacitadas en el manejo del Spectrum , independientemente de sus actividades como administradores de red para poder darle mantenimiento a las bases de datos y en general a la plataforma en sí, agregar cambios, crear nuevas topologías , sacar estadísticas y tener una plataforma funcionando adecuadamente. La capacitación puede resultar costosa pero el costo-beneficio es grande al irse familiarizando con la plataforma.

Una vez que tenemos instalado el software de la plataforma de administración en este caso en un servidor UNIX debido a que es más estable que un servidor NT, procedemos a crear nuestra topología de la red de forma gráfica y agregando o quitando funcionalidades que tiene la plataforma como son el activar o desabilitar los parámetros que no queremos recopilar mediante el poleo debido a que un excesivo poleo en nuestra red la

puede saturar de información de adminitración y de la cual solo tengamos un cierto porcentaje útil .

Normalmente un NMS se divide en módulos funcionales dependiendo de que se requiera monitorear . Para el caso de ATM en Spectrum se utiliza el módulo SPECTRUM ATM Circuit Manager para visualizar los recursos ATM de la red y provee el manejo de la fábrica de conmutación (switched fabric) , canales y circuitos lógicos. Podemos incluir:

Administración dela infraestructura ATM
Descubrimiento automático de nuevos elementos
Aislamiento lógico de la red ATM en caso de falla
Administración de alarmas y eventos
Monitoreo de desempeño y reportes

En la siguiente figura podemos observar una pantalla de como se verían nuestros switches modelados con Spectrum además de una parte para VLAN´s y otra para una granja de servidores interconectados a través de enlaces.

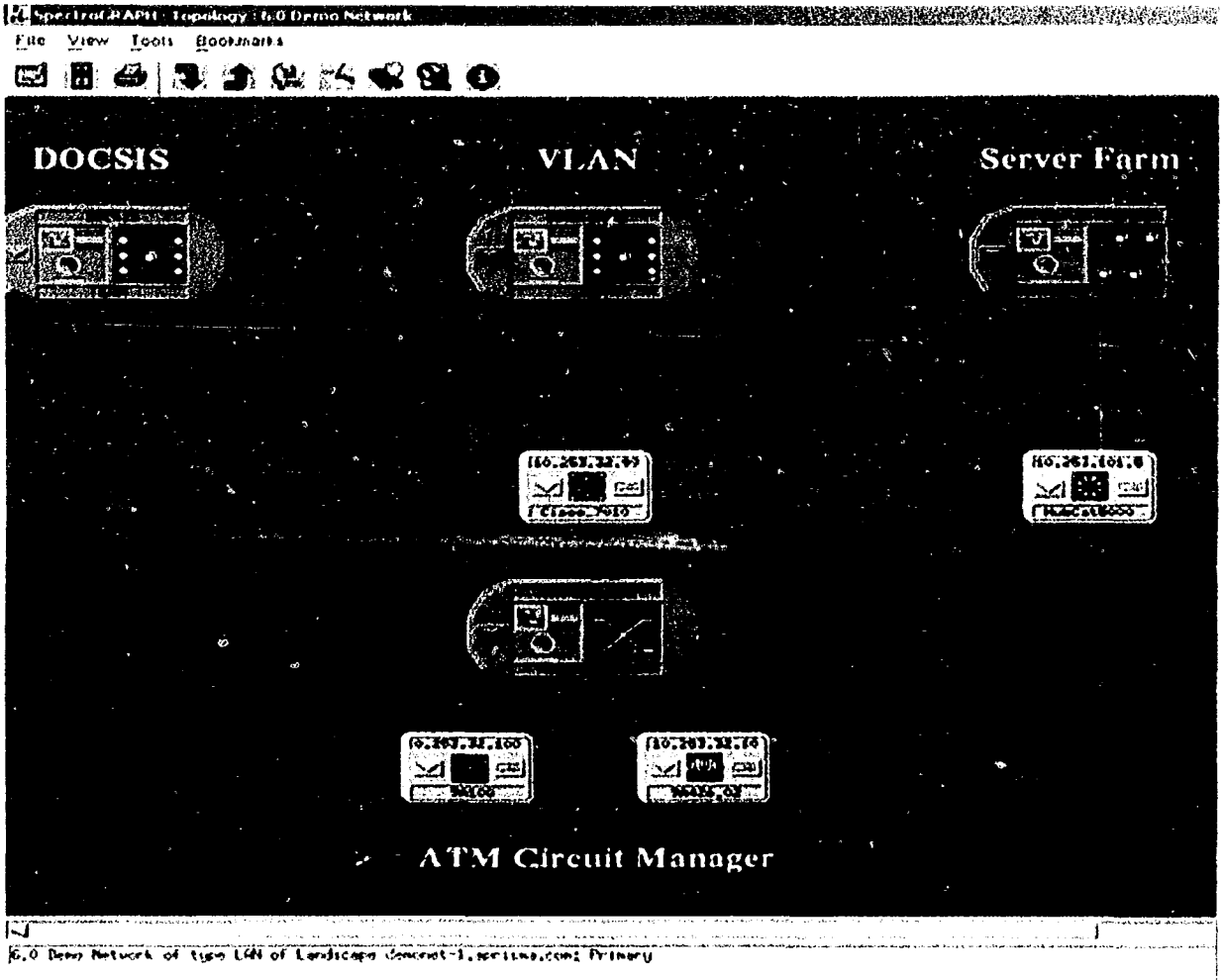


Fig. 5.52 Topología de una red ATM vista en el ATM circuit Manager

La ventana principal que utilizamos para visualizar alarmas generalmente empleamos la topología de la red en donde podemos visualizar un exágono en donde modificamos los parámetros del servidor de SPECTRUM, en esta ventana es donde partimos para realizar estadísticas o visualizar equipos que tenemos modelados . ver figura 5.53.

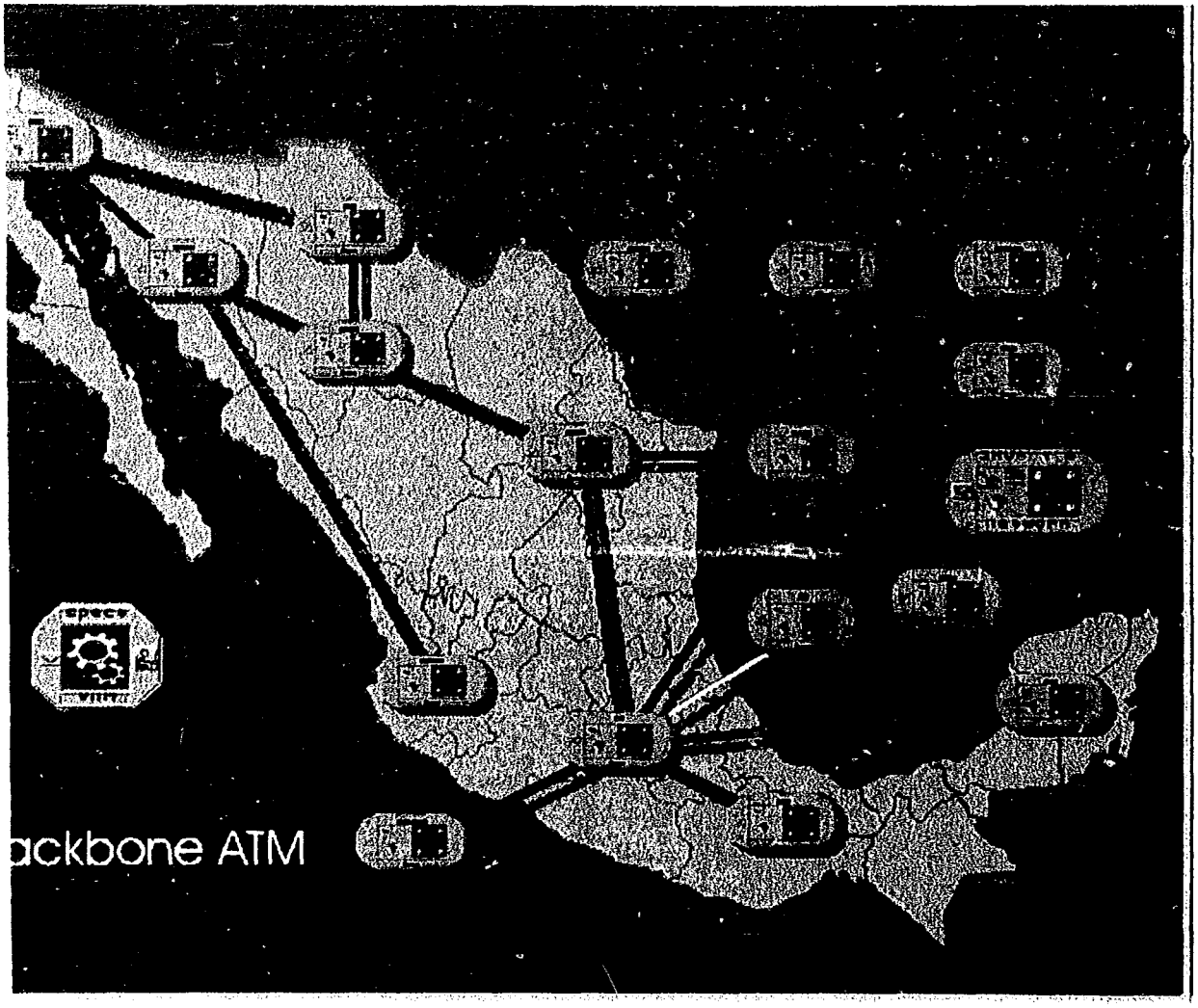


Fig. 5.53 vista de la topología de la red ATM

Una de las características que debe de tener una plataforma de administración es poder avisar mediante un pager o via correo electrónico o hasta mandando mensajes de voz a un celular si algun evento crítico sucede En el transcurso del día o de noche si es que no se tiene un administrador de la red nocturno para poder solvertar el problema rápidamente . esto se logra con el módulo denominado SPECTRUM Alarm Notification Manager. En este se pueden incluir mensajes de texto que se pasan a una llamada de celular .

Otra de las cosas que podemos monitorear en esta plataforma de nuestros switches es el de celdas de entrada y salida por una determinada interface o equipo como se muestra en la siguiente figura 5.54.

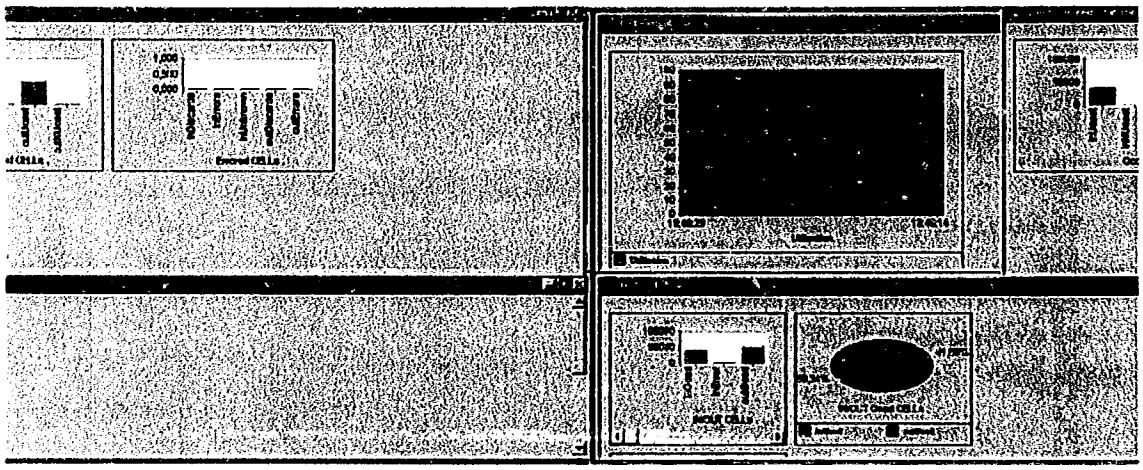


Fig. 5.54 celdas de entrada y salida

Podemos utilizar las herramientas para manejar las MIB´s con el programa denominado MIBTOOLS y editar los perfiles que requerimos tanto para ATM como para las demas tecnologías o protocolos como IP. En la siguiente figura 5.55 podemos visualizar una ventana de configuración de las MIB´s.

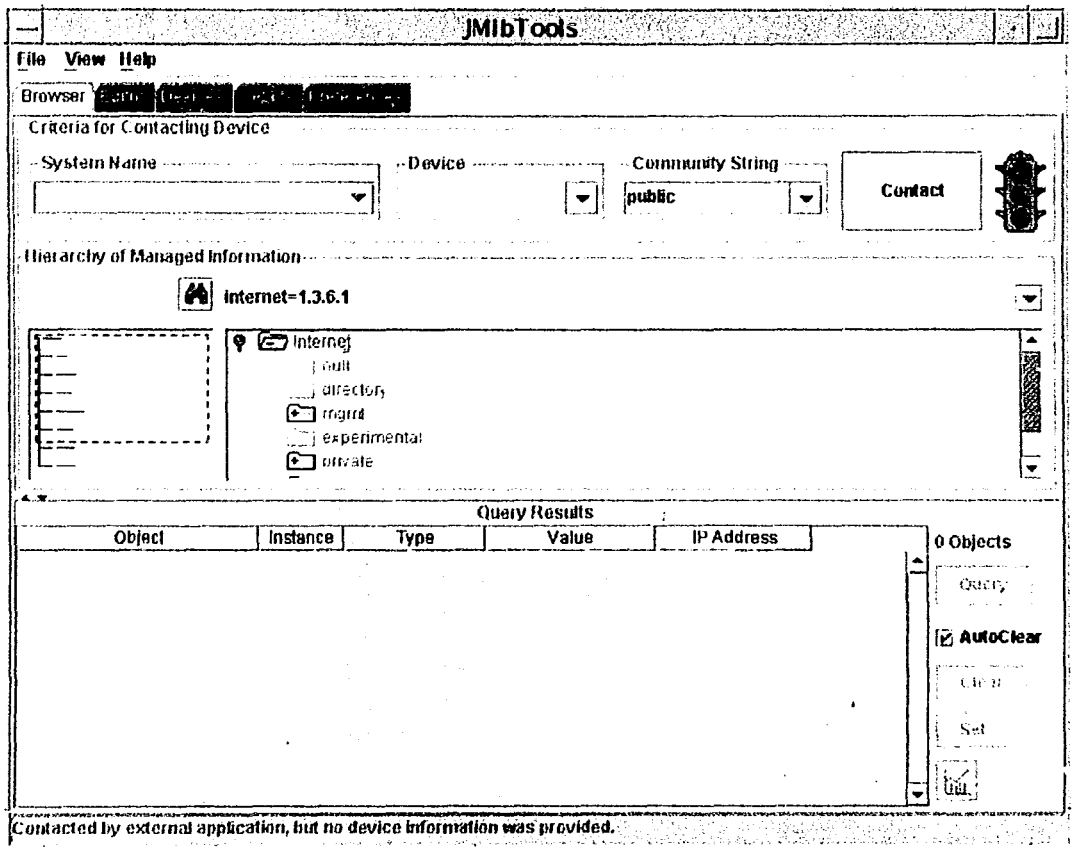


Fig. 5.55 ventana de configuración de MIB´s

Podemos también definir perfiles en MIB´s ATM como se observa en la siguiente figura 5.56, se puede visualizar los elementos del árbol como el atmInterfaceConfTable que no ayuda a visualizar la tabla de configuración de interfaces ATM. Podemos visualizar el orden para la identificación del objeto de la MIB como se describío en el capítulo 4.

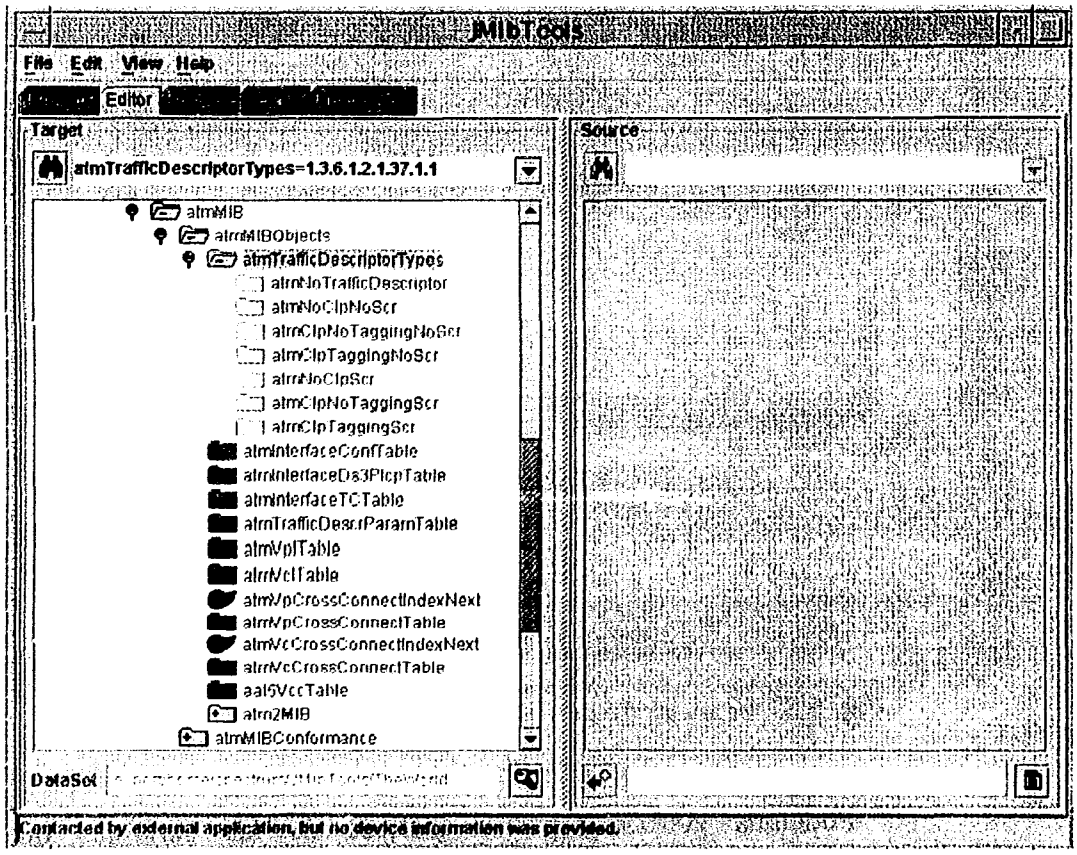


Fig. 5.56 ventana de configuración de MIB´s dentro del arbol ATM

Podemos definir perfiles para formatos de reportes según formatos preestablecidos o podemos crear nuestros propios formatos según nuestras necesidades. En la figura 5.57 podemos observar la ventana de configuración para formatos de reporte, esto se hace con el módulo Enterprise Configuration Manager.

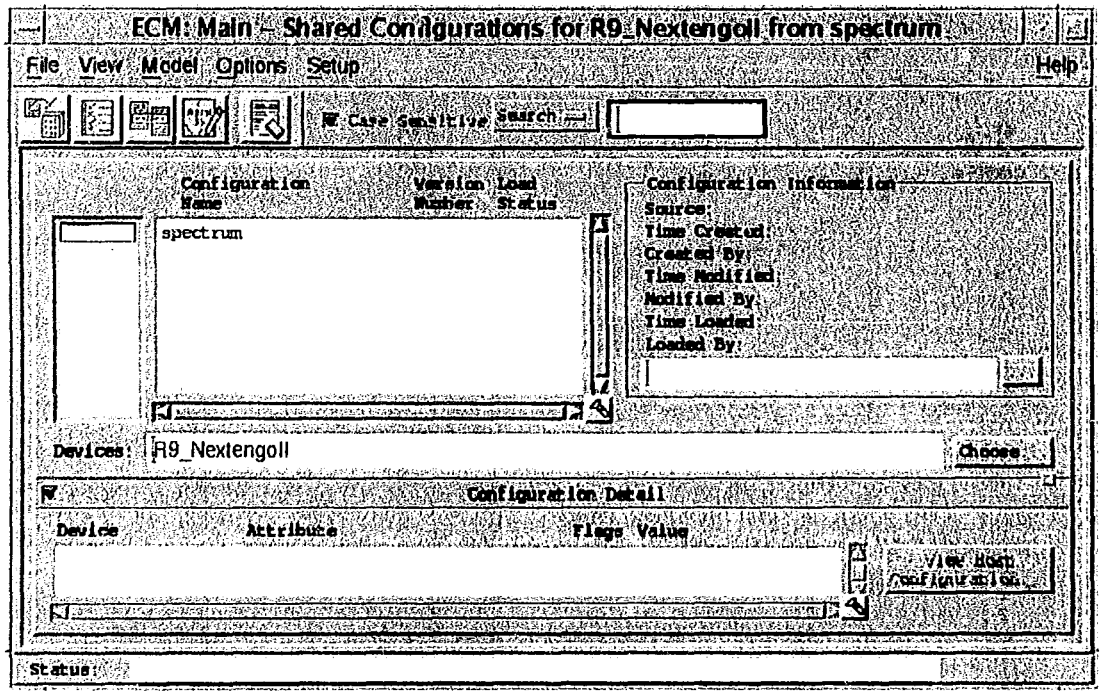


Fig. 5.57 ventana de configuración de formatos de reportes

Podemos generar reportes gráficos de las variables que hallamos definido como se muestra en la siguiente figura 5.58. Podemos crear muchos diferentes perfiles y formatos con variables diferentes dependiendo de que se requiera poner en el reporte.

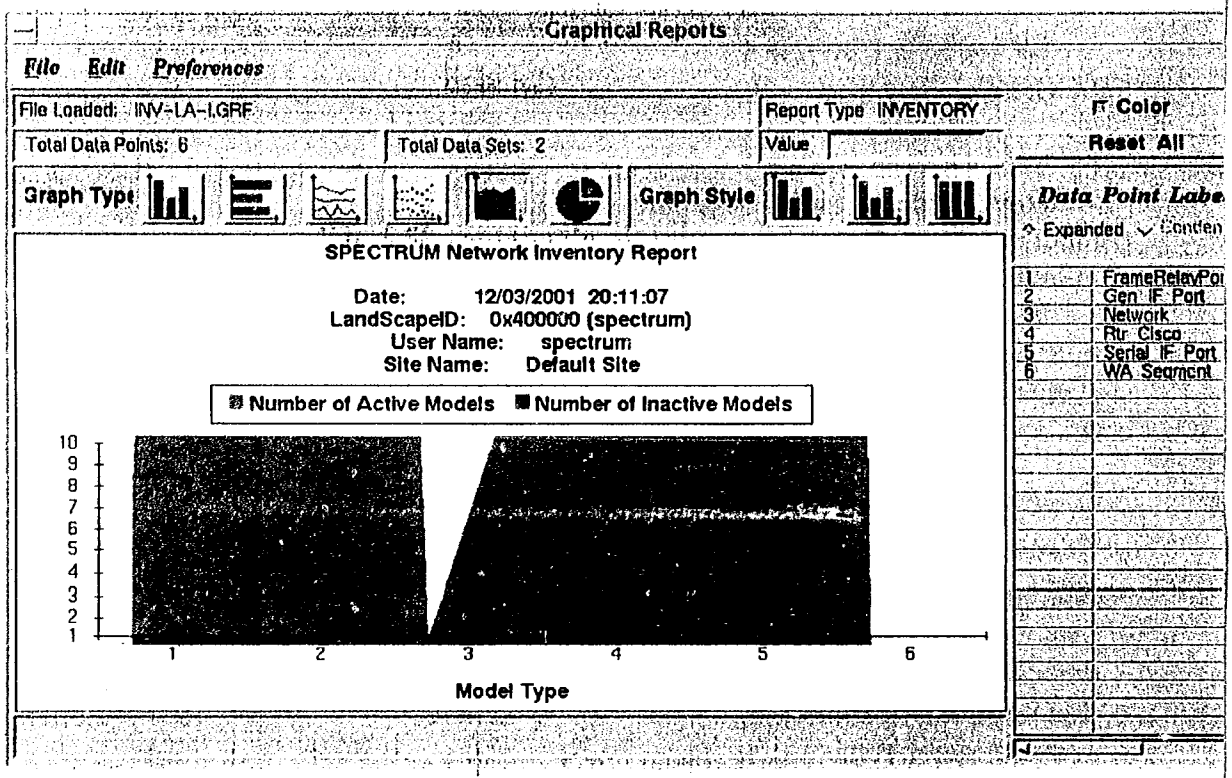


Fig. 5.58 ventana de un reporte grafico generado

5.9 CONCLUSIONES

Hoy en dia es imprescindible en una red de grandes dimensiones como lo son las redes ATM, el contar con un sistema de administración para el monitoreo, la gestión , la administración de cuentas, la obtención de estadísticas de desempeño y de la seguridad en las redes ATM. Con la ayuda de una plataforma de administración, en este caso *Spectrum,* se obtienen los siguientes beneficios en la administración de la red, tomando en cuenta el costo/beneficio de la plataforma de adminstración:

- Alta disponibilidad de la red
- Distribuir los costos
- Incrementar la flexibilidad de operación e integración
- Aumentar la eficiencia
- Facilidad de uso
- Mantener la seguridad
- Configuración remota
- Generación de reportes ejecutivos y operativos del desempeño de la red
- Visión global de la red y al correlacionar alarmas se detecta el problema rápidamente

Como desventajas se tiene que la plataforma de administración tiene un costo de implementación, operación y mantenimiento, ya que se requiere de licencias, personal capacitado, asitencia técnica y recursos asignados a la plataforma para su mantenimiento y crecimiento.

GLOSARIO

AAL	ATM Adaptation Layer
ABM	Asynchronous Balance Mode
ABR	Available Bit Rate
AFI	Authority and Format Identifier
ANSI	American National Standard Institude
ARM	Asynchronous Response Mode
ARPA	Advanced Research Projects Agency
AS	Autonumous System
ASCII	American Standard Code for Information Interchange
ASK	Amplitude Shift Keying
AU	Administrative Unit
AUI	Attachment Unit Interface
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BCD	Binary Code Decimal
BGP	Border Gateway Protocol
BICI	Broadband Inter-Carrier Interface
BIP-8	Bip Interleaved Parity
B-ISDN	Broadband ISDN
BRI	Basic Rate Interface
CAC	Control de Admisión de la Conexión
CBR	Constant Bit Rate
CCITT	Comite Consultivo de Telegrafia y telefonía
CDV	Variación de retardo de celda
CER	Cell Error Rate
CLP	Cell Lost Priority
CLR	Cell Lost Rate
CPCS	Subcapa de Convergencia de parte común
CPI	Indicador de parte común
CRC	Cyclic Redundancy Check
CS	Subcapa de convergencia
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CTD	Cell Transfer Delay
CMIP	Common Management Information Prc. col
DA	Destination Address
DARPA	Defense Advanced Project Research Agency
DCC	Data Country Code

DFI	Indicador de formato de parte específica de dominio
DoD	Department of Defense
DQDB	Distriubuited Queue Data Bus
DCE	Data Communication Equipment
DTE	Data Terminal Equipment
E1	Trama básica europea de voz (2.048 Mbps)
ED	Dispositivo de frontera
EGP	External Gateway Protocol
EIA	Electronics Industries Association
ESF	Extended Super Frame
FAS	Frame Align Signal
FC	Frame Control
FCS	Field Check Secuence
FDDI	Fiber Distribuited Data Interface
FDM	Frecuency Division Multiplexing
FIFO	First Input First Output
FS	Frame Status
FSK	Frecuency Shift Keying
FTP	File Transfer Protocol
GAN	Global Area Network
GFC	Generic Flow Control
HDLC	High-level Data link control
HEC	Header Error Control
HUB	Equipo concentrador de terminales en una red LAN
ILMI	Integrated Local Management Interface
IEEE	Institute Electrics and Electronics Engineers
IETF	Comisión de investigación de ingeniería de internet
IP	Internet Protocol
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standarization
IPX	Internet Packet Exchange
ITU-T	The Telecommunications Standarization Sector of the International Telecommunications
LAN	Local Area Network
LU	Logical Unit
LANE	Emulación de LAN
LAP-B	Link Access Protocol Balanced
LIFO	Last Input First Output
LIS	Logical IP Subnetwork

LTE	Line Terminal Equipment
LLC	Logical Link Control
MAN	Metropolitan Area Network
MAU	Mutistation Access Unit
MFAS	Multiframe Align Signal
MIB	Management Information Base
MID	Identificador de Mensaje
MPOA	Multiprotocolo over ATM
MPU	Maximum Trasnfer Unit
MAC	Medium Access Control
MIB	Management Information Base
NMS	Network Management System
NHRP	Protocolo de enrutamiento de próximo brinco
NIC	Network Information Center
NIC	Network Interface Card
NMS	Network Management System
NRZI	Non Return Zero Inverted
NSAP	Network Service Access Point
NNI	Network to Network Interface
OAM	Operation, Administration and Manteniance
OC-n	Optical Carrier
OSI	Open System Interconection
OSPF	Open Shortest Path First
P/F	Poll/Final
PAD	Paquet Assamber and Disassambler
PBX	Private Branch Exchange
PC	Personal Computer
PDH	Plesiochronous Digital Herarchy
PDM	Physical Depend Medium
PDU	Protocol Data Unit
PLCP	Protocolo de convergencia de capa física
PLR	Paquet Lost Rate
P-NNI	Protocol Network-Node Inteface
POH	Path Overhead
PRI	Primary Rate Interface
PSCS	Subcapa de convergencia de protocolo específico
PSK	Phase Shift Keying
PSP	Paquet Per Second
PT	Payload Type
PTE	Path Terminal Equipment

PTSP	Paquetes de estado de la topologia}
PVC	Circuito virtual permanente
QoS	Calidad de Servicio
RFC	Request For Comment
RAI	Indicador de alarma remota
RARP	Reverse ARP
RD	Dominio de enrutamiento
REJ	Reject
RFC	Request For Comments
RIP	Routing Information Protocol
RNR	Receive Not Ready
SDH	Synchonous Digital Hierarchy
SA	Source Address
SAP	Service Access Point
SD	Start delimiter
SDH	Sinchronous Digital Herarchy
SDU	Service Data Unit
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SN	Suscriber number
SNA	System Network Arquitecture
SNAP	Subnetwork Attachment Point
SNMP	Simple Network Management Protocol
SOH	Section overhead
SONET	Synchronous Optical Network
SPE	Synchronous Payload Envelop
SSCS	Subcapa de convergencia de servicio especifico
STDM	Multiplexaje por división de tiempo estadístico
STM-1	Synchronous Transport Module
STP	Shielded Twisted Pair
STS-n	Synchronous Transport Signal
SVC	Switched Virtual Circuit
SMI	Structure of Management Information
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
T1	Trama de voz básica norteamericana
TC	Convergencia de transmisión
TCP/IP	Protocolo de transporte/Protocolo Internet
TDM	Time Division Multiplex
TELNET	Protocolo para sesiones remotas

TFTP	Trivial File Tranfer Protocol
TS	Time Slot
UDP	User Datagram Protocol
UBR	Undefined Bit Rate
UME	Entidad de administración UNI
UNI	User Network Interface
UTP	Unshielded Twister Pair
UU	User to User
VBR	Variable Bit Rate
WAN	Wide Area Network

BIBLIOGRAFIA

- 1st, 2nd and Next Generation LAN's
Daniel Minoli
Mc Graw-Hill

- ATM Theory and Aplication
Mc Dysan & Spohn
Mc Graw-Hill Series on Computer Communications, 1995

- ATM
Walter Goralsky
Computer Technology Research Corp. 1994

- ATM Asynchronous Transfer Mode User's Guide
William Flanagan
Flaitron Publishing, Inc. Book, 1994

- ATM & MPEG-2 Integrating Digital Vídeo into Broadband Networks
Michael Orzessek and Peter Sommer
Hewlett Packard

- ATM (User-Network Interface Specification)
The Forum ATM

- ATM The Future of High-Speed Networking
Walter Goralski
Computer Technology Research.

- ATM Theory and Application
David E. Mcdysan and Darren L. Spohn
McGraw-Hill

- Broadband LAN Technology
Gary Kim
Artech House

- CISCO LAN Switching
Kennedy Clark, Kevin Hamilton
Cisco-Press, 1999

- Data and Computer Communications
William Stallings
Mc Millan Publishing Company, 1985

- Data and Computer Communications
William Stallings
Mc Millan Publishing Company, Fourth Edition , 1994

- Digital Telephony
John Bellamy
John Wiley & Sons, Sec. Edition, 1990

- Diseño de Redes Locales
Hoppper & Temple
Addison-Wesley Iberoamericana, 1994

- FastEthernet
Howard W. Johnson
Prentice Hall

- Gigabit Networking
Partridge Craig
Adison Wesley Publishing Company

- High Performance Networking, V
S. Frida
North Holland

- High Speed Networks
Boisseau M
John Wiley & Sons, 1994

- ISDN and Broadband ISDN with Frame Relay and ATM
William Stallings
Addison Wesley Publishing Company, 3er ed, 1995

- Internetworking with TCP/IP
Douglas Comer
Prentice Hall, Sec. Edition, 1991

- Internetworking
Mark A. Miller
A Guide to Network Communivcations LAN to LAN, LAN to WAN
M&T Books, 1990

- Local Area Networks
James Martin
Prentice Hall, Sec Edition, 1994

- Local and Metropolitan Area Network
William Stallings
Mc Millan Publishing Company, Fourth Edition, 1993

- Local and Metropolitan Area Network
William Stallings
Mc Millan Publishing Company, Fifth Edition, 1996

- Networking Standards
William Stallings
Addison Wesley Publishing Company

- Network Management Systems Essentials
Divaraka K. Udupa
mc graw-hill

- Redes de Computaddoras
Uyless Black
Macrobit Editores, 1990

- Redes de Computadoras
Andrew S. Tanenbaum
Prentice Hall

- Redes Globales de Información con Internet y TCP/IP
Douglas Comer
Prentice Hall, 1996

- SNMP,SNMPv2 and RMON
William Stallings
Mc Millan Publishing Company, 1996

- TCP/IP and Related Protocols
Uyless Black
Mc Graw Hill

- Understanding ATM
Stan Schatt
Computer Mc Graw-Hill, 1996

- Virtual LAN's
Gilbert Held
John Wiley & Sons Inc.

RFC's

- RFC 2575: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

- RFC 2574: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

- RFC 2573: SNMP Applications

- RFC 2572: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

- RFC 2571: An Architecture for Describing SNMP Management Frameworks

- RFC 2275: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

- RFC 2274: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 2273: SNMPv3 Applications
- RFC 2013: SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
- RFC 2012: SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
- RFC 2011: SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 1910: User-based Security Model for SNMPv2
- RFC 1909: An Administrative Infrastructure for SNMPv2
- RFC 1908: Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
- RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1906: Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1905: Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1904: Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1903: Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1902: Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)

- RFC 1901: Introduction to Community-based SNMPv2
- RFC 1450: Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1352: SNMP Security Protocols
- RFC 1351: SNMP Administrative Model
- RFC 1283: SNMP over OSI
- RFC 1271: Remote Network Monitoring Management Information Base
- RFC 1270: SNMP Communications Services
- RFC 1215: Convention for defining traps for use with the SNMP
- RFC 1214: OSI internet management: Management Information Base
- RFC 1213: Management Information Base for Network Management of TCP/IP-based internets:MIB-II
- RFC 1212: Concise MIB definitions
- RFC 1189: Common Management Information Services and Protocols for the Internet (CMOT and CMIP)
- RFC 1187: Bulk Table Retrieval with the SNMP
- RFC 1158: Management Information Base for network management of TCP/IP-based internets: MIB-II
- RFC 1157: Simple Network Management Protocol (SNMP)

URL's:

http://www.snmp.com
http://www.3com.com
http://www.asante.com
http://www.lantronix.com
http://wwwhost.ots.utexas.edu/ethernet/index.html
http://www.specialty.com
http://www.webcom.com
http://www.clarktech.com/al202.htm
http://hpcc920.external.hp.com/rnd/technol/whtpaper/switch/switch.htm
http://www.zeinet.com/atm/lan1-2.html
http://www.ipsilon.com/technology/papers/newman0001.htm
http://www.cisco.com/univercd/data/doc/cintrnet/idg3/idglans.htm
http://www.cisco.com/cpress/data/cpress/fund/ith.htm
http://www.hp.com:80/rnd/technol/whtpaper/switch/abc.htm
http://www.ij.com/univercd/data/doc/harware/wbu/ls1010/rel_11_2/sw_cfg/pnni_cnf.htm
http://www.xyplex.com/product/white-paper/swexcpt.html
http://cio.cisco.com/warp/public/729/c5000/netdn_wp.htm
http://www.baynetworks.com/more/index.html
http://www.moose.byu.edu/~christof/Fast_Ethernet.html
http://www.3com.com/nsc/500617.html
http://a01-unix.gsyc.inf.uc3m.es/~fperez/lro9798
http://www.atmforum.com
http://www.gdc.com
http://www.nortelnetworks.com
http://www.gigabit-ethernet.org/