UNIVERSIDAD POLITÉCNICA DE CARTAGENA

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

Estudio y evaluación de algoritmos de encaminamiento IP empleando routers Teldat

Autor
Juan Pedro Muñoz Gea

Director
José María Malgosa Sanahuja

Ingeniería Técnica de Telecomunicación, especialidad Telemática

Cartagena, Septiembre 2003

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Motivaciones y Objetivos

1 Motivaciones

El proyecto fin de carrera que a continuación se expone es un estudio teórico y experimental sobre el funcionamiento básico del router NUCLEOX PLUS de la firma española Teldat.

A partir de las características técnicas y funcionales de este router se va a proceder a realizar un estudio teórico de los principales servicios y modos de funcionamiento que ofrece, acompañado de experiencias concretas realizadas con el equipo y que sirven de guía para aprender a configurar y utilizar el dispositivo.

Ya que, como se ha dicho anteriormente, el punto de partida son los servicios básicos ofrecidos por el NUCLEOX PLUS, vamos a proceder a enumerarlos brevemente:

- Funciona como router IP, y por lo tanto sirve para la interconexión de redes. Implementa mecanismos de encaminamiento tanto estático como dinámico (RIP I y RIP II).

- Por las líneas serie se conecta mediante el protocolo PPP a enlaces punto a punto.

- Es un dispositivo de acceso a redes Frame Relay (FRAD).

- Utiliza NAT (Network Address Translation) para soportar el acceso por RDSI o RTB a Internet desde una LAN con direccionamiento privado, utilizando una única dirección IP pública.

- Es un Gateway H.323 y, por lo tanto, transporta voz proveniente de sus interfaces analógicos sobre redes IP. Puede capturar el tráfico saliente de una centralita y desviar el tráfico corporativo hacia una red IP y conmutar transparentemente el resto de las llamadas hacia salidas analógicas de RTC.

- Soporta las soluciones de Backup WRR (Wan ReRoute) y WRS (Wan ReStoral).

A partir los servicios ofrecidos por el router, el documento se estructura de la siguiente manera:

En el **Capítulo 1** se realiza una introducción al funcionamiento básico del protocolo IP. Ya que la característica fundamental del NUCLEOX PLUS es la de funcionar como router IP, es de gran utilidad analizar y comprender las características de este protocolo.

El **Capítulo 2** se dedica a exponer las características técnicas del NUCLEOX PLUS y los aspectos fundamentales sobre los modos de configuración y la forma en que debe realizarse dicha configuración.

Los **Capítulos 3 y 4** sirven de guía para la configuración de las dos tecnologías WAN soportadas por el equipo: PPP y Frame Relay, utilizando las interfaces WAN que posee el router: 2 interfaces serie y 2 accesos básicos RDSI.

En el **Capítulo 5** se aprende a utilizar el mecanismo NAT que incluye el equipo. Es una forma fácil de comprender el funcionamiento y la utilidad de este servicio.

En el **Capítulo 6** se expone una configuración sencilla de la tecnología de Voz sobre IP (VoIP). Con esta experiencia se van a poder apreciar los efectos que tienen diversos parámetros en la calidad de este servicio, tales como la variación del retardo (jitter), el eco, la compresión, etc.

En el **Capítulo 7** se ofrecen los pasos a seguir para poner el funcionamiento el protocolo RIP en el equipo. El router ofrece la posibilidad de observar cómo cambian las tablas de encaminamiento al provocar fallos o errores forzados en la red.

Por último, el **Capítulo 8** nos guía en la configuración de las dos facilidades de backup soportadas por el router: WRR y WRS. Con esta sencilla configuración se puede experimentar el funcionamiento de este servicio de gran utilidad en la actualidad.

2 Objetivos

El objetivo fundamental que se pretende conseguir con la realización de este proyecto fin de carrera es el de disponer de una guía básica del funcionamiento y configuración del router NUCLEOX PLUS de Teldat.

La utilidad de esta guía se puede aprovechar tanto para la docencia como para la investigación de diversos temas de gran importancia dentro del área de la ingeniería telemática.

Otro objetivo que se persigue es el de realizar una breve exposición teórica, necesaria para conocer los aspectos fundamentales que se configuran y se ponen en práctica con el router.

Capítulo 1
Introducción al protocolo IP

1.1 Internet y el conjunto de protocolos TCP/IP

TCP/IP es una colección de protocolos que proporcionan servicio en las capas de red y de transporte. Originalmente nacen del trabajo del Departamento de Defensa (DoD) de los EE.UU., concretamente en el Advanced Research Project Agency Network (ARPANET), y surgen como una necesidad para la interconexión fiable de redes de comunicación muy distintas entre si.

Los estudios arrancan a finales de los 60, cuando grupos de investigación empiezan a trabajar en tecnologías de interconexión de redes de conmutación de paquetes. A mediados de los 70 se crea la red ARPANET para proporcionar una red de comunicación fiable a los distintos agentes militares.

En 1974 nace la familia de protocolos TCP/IP que tratan de lograr conectividad universal, imponiéndose en poco tiempo como una solución estándar. Sobre 1980, ARPANET adopta TCP/IP como únicos protocolos.

En 1983 la red ARPANET se dedica a la investigación (a ella se conectan universidades y otras agencias gubernamentales), mientras que la nueva red MILNET se dedica exclusivamente a asuntos militares. En esta época hay una estandarización de TCP/IP en Internet a través de los RFC (Request For Comments).

Sin embargo, lo que de verdad impulsó a Internet en estos tiempos fue el software del sistema operativo UNIX de la Universidad de Berkeley. Se trataba de una implementación de bajo coste de los protocolos TCP/IP, y de esta manera el código fuente de TCP/IP fue de dominio público. Este software tiene una serie de utilidades para servicios de red, como la utilidad Socket.

En la actualidad, Internet es un sistema inacabado, en evolución y con requisitos cambiantes. Ahora estamos en IPv4, y se trabaja en IPv6 y en otra serie de mecanismos para solucionar los problemas que han surgido en los últimos años.

En resumen, podemos decir que Internet es un conjunto de redes conectadas que actúan como un todo coordinado. La ventaja es que proporciona interconexión universal independientemente del hardware de red. El software TCP/IP aísla las diferencias entre redes físicas distintas y hace al sistema de comunicación independiente de las tecnologías hardware.

1.2 Introducción al protocolo IP

Internet Protocol es un protocolo de nivel de red que define un mecanismo de entrega sin conexión, con el mejor esfuerzo y no confiable. El servicio se conoce como no confiable porque la entrega no está garantizada. Los paquetes se pueden perder, duplicar, retrasar o entregar sin orden. El servicio es llamado sin conexión porque no existe un proceso de señalización previo a la comunicación y consecuentemente cada paquete es tratado de manera independiente de todos los demás. Una secuencia de paquetes que se envían de una computadora a otra puede viajar por diferentes rutas; algunos de ellos pueden perderse mientras otros se entregan. Por último, se dice que el servicio trabaja con base en un best effort (entrega con el mejor esfuerzo) porque el protocolo IP intenta siempre entregar los paquetes hacia la red. Por supuesto, la red no descarta

paquetes caprichosamente; la no-confiabilidad aparece sólo cuando los recursos están agotados o la red subyacente falla.

El protocolo IP proporciona tres aspectos importantes. En primer lugar, define formalmente los campos de la cabecera del paquete IP. Segundo, el software IP realiza la función de encaminamiento, seleccionando la ruta por la que los datos serán enviados. En último lugar, además de aportar especificaciones formales para el formato de los datos y el encaminamiento, IP incluye un conjunto de reglas que caracterizan la forma en que los terminales y routers deben procesar los paquetes, cómo y cuando se deben generar los mensajes de error y las condiciones bajo las cuales los paquetes pueden ser descartados.

1.3 Direcciones IP

Las direcciones IP ayudan al software TCP/IP a ocultar los detalles de las redes físicas y hacen que Internet parezca como una sola entidad uniforme. De manera específica, una dirección IP codifica la identificación de la red a la que se conecta la máquina, así como la identificación de la máquina dentro de esa red.

Una dirección IP identifica el lugar donde una interfaz de red de un ordenador se conecta a la red. Por ejemplo, si un ordenador tiene más de una interfaz conectado a la red, se le debe asignar una dirección IP distinta para cada uno de ellos.

La dirección IP es un número de 32 bits. Normalmente se utiliza una notación especial para indicar dichas direcciones: los 32 bits se dividen en cuatro grupos de 8. Los valores de dichos grupos se expresan normalmente en decimal, separados por puntos.

Por ejemplo, una dirección IP que en notación binaria sea:

10000000 00101010 00001010 00010111

es equivalente a:

128.42.10.23

Cada dirección IP tiene una parte para identificación de la red que se denomina netid, y otra para identificar el terminal u ordenador conectado dentro de la netid, que se denomina hostid.

1.3.1 Tres tipos primarios de direcciones IP

Hay tres tipos primarios de direcciones IP: clase A, clase B y clase C. Los tipos se identifican por los bits más significativos de la dirección.

Las direcciones clase A se utilizan para las redes con más de 65.534 ordenadores. Se sabe que una dirección es clase A porque el bit más significativo vale 0. En clase A el campo netid ocupa los primeros 8 bits y el campo hostid los 24 restantes. Se deduce fácilmente que sólo hay 127 redes distintas de clase A.

La clase B se utiliza para redes de tamaño intermedio que tengan de 255 a 65.534 ordenadores. En estas direcciones los 16 primeros bits son el netid y los 16 restantes el hostid. Para reconocer una dirección como de clase B se tiene que cumplir que el primer y segundo bits sean 1 y 0 respectivamente.

Por último, la clase C se utiliza para redes con menos de 255 ordenadores. Con estas direcciones los primeros 24 bits son el netid y los 8 restantes el hostid. Los tres bits más significativos de una dirección clase C son 1, 1 y 0.

Además de estas clases con las que se organizan las direcciones de los sistemas finales existe una cuarta clase, la clase D, que identifica las direcciones multidestino o multicast. Para identificar una dirección multicast hay que comprobar que los cuatro bits más significativos sean 1, 1, 1 y 0. El resto de los bits de la dirección identifican el grupo multicast específico.

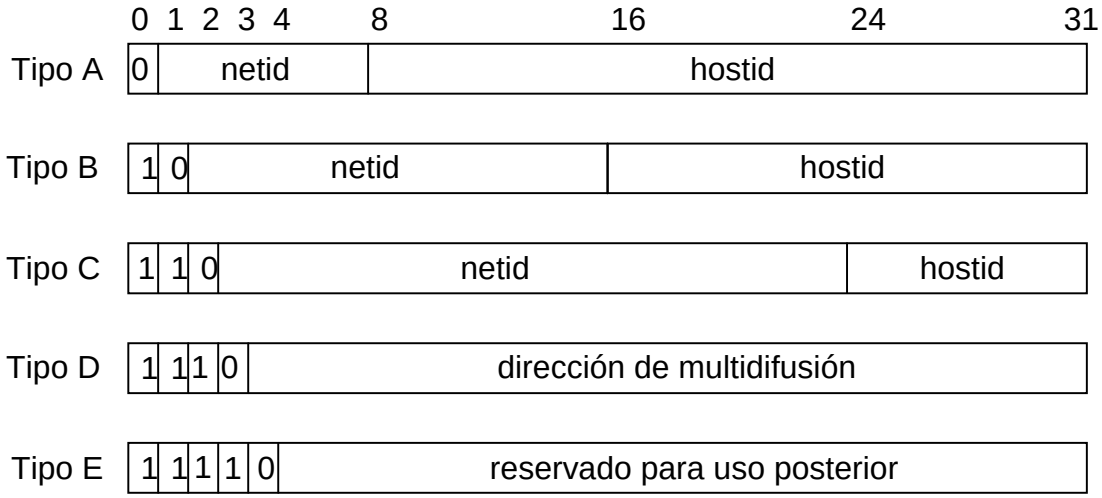

Figura 1.1: Las cinco formas de direccionamiento IP

Tipo	Dirección más baja	Dirección más alta
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tabla 1.1: Rango de direcciones IP

Este direccionamiento es hoy en día obsoleto. En la actualidad todos los terminales y routers trabajan con direcciones IP classless (ver apartado 1.3.6).

1.3.2 Direcciones de red y de difusión

Ya hemos mencionado que la mayor ventaja de codificar la información de la red en las direcciones IP es hacer posible que exista un encaminamiento eficiente. Otra ventaja es que las direcciones IP se pueden referir tanto a redes como a máquinas. Por regla general, nunca se asigna un campo hostid igual a 0 a una máquina individual. En vez de eso, una dirección IP con campo hostid de 0 se utiliza para referirse a la red en sí misma.

Otra ventaja significativa del esquema de direccionamiento en una red IP es que éste incluye una dirección de difusión que se refiere a todas las máquinas en la red. De acuerdo con el estándar, cualquier campo hostid formado solamente por unos, está reservado para la difusión. Este tipo de difusión se denomina difusión dirigida.

Otra forma de dirección de difusión, llamada dirección de difusión limitada o dirección de difusión en red local, proporciona una dirección de difusión para la red local, independientemente de la dirección IP asignada. La dirección de difusión local consiste en treinta y dos unos. Una máquina puede utilizar la dirección de difusión limitada como parte de un procedimiento de arranque antes de conocer su dirección IP o la dirección IP de la red local,

por ejemplo mediante el protocolo BOOTP. Sin embargo, una vez que el algoritmo conoce la dirección IP correcta para la red local, tiene que utilizar la difusión dirigida.
En la práctica, el IP utiliza sólo unas cuentas combinaciones de ceros o unos:

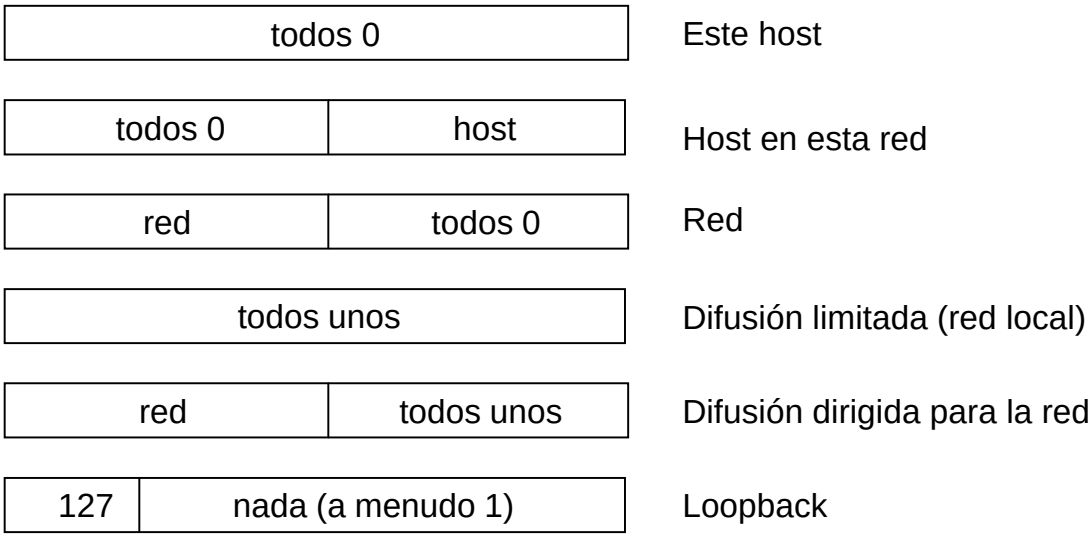

Figura 1.2: Formas especiales de direcciones IP

1.3.3 Dirección loopback

La dirección 127.0.0.0, valor del rango tipo A, se reserva para loopback; y está diseñada para utilizarse en escenarios de pruebas y para la comunicación de los procesos internos en la máquina local. Es decir, se trata de una dirección IP que nunca generará tráfico hacia la red. Todos los paquetes que se envíen a esta dirección son devueltos inmediatamente (como paquete de entrada) al driver de red. Por tanto, podríamos decir que se trata de una dirección que simula una interfaz de red virtual.

1.3.4 Debilidades del direccionamiento IP

El direccionamiento IP presenta cuatro debilidades fundamentales:

- La desventaja más obvia es que las direcciones se refieren a las conexiones de red, no a la computadora; si una computadora se mueve de una red a otra, su dirección IP debe cambiar.

- El método de manejo de direcciones de red del tipo A, B y C es bastante ineficiente.

- Por otra parte, el crecimiento explosivo en el uso de Internet ha hecho que las tablas de encaminamiento de los routers sean demasiado grandes, lo que a su vez conlleva un tráfico de encaminamiento elevado, con la consiguiente sobrecarga de la red.

- Otra debilidad es el escaso margen de direccionamiento, ya que 2^{32} es bastante inferior al número de ordenadores conectados a Internet.

1.3.5 Subnetting

La ineficiencia del manejo de direcciones de red del tipo A, B y C se soluciona con el uso de Subnetting.

Imagínese a una empresa que tiene 1000 equipos en una red. Con una dirección de clase C no tendría suficiente, ya que este tipo de direcciones sólo permite tener hasta 254 terminales dentro de una red; sin embargo, con una dirección de clase B estaría desperdiciando miles de direcciones (ya que este tipo permite direccionar más de 65.000 hosts). Lo ideal sería que cada uno pudiese elegir cuántos bits necesita realmente para direccionar cada uno de los equipos de una red. Además, otra ventaja que nos reportaría esta técnica sería el permitirnos manejar una única dirección de nivel de red para direccionar varías redes físicas distintas, con el consiguiente ahorro de direcciones de red que ello conllevaría.

La manera más sencilla de entender el direccionamiento de subred es imaginándose que una empresa tiene asignada una sola dirección de red IP tipo B, pero en realidad tiene dos o más redes físicas dentro de la empresa. Sólo los routers locales saben que existen muchas redes físicas y cómo encaminar el tráfico entre ellas; los routers exteriores a la empresa encaminan todo el tráfico como si sólo hubiera una red física.

Conceptualmente, agregar subredes sólo cambia ligeramente la interpretación de las direcciones IP. En vez de dividir la dirección IP de 32 bits en un prefijo netid y un sufijo hostid, ahora, el prefijo netid se mantiene, pero el sufijo hostid se divide en una parte subnetid (que identificará a una red física concreta) y en una parte hostid (que identificará a un host dentro de una red física determinada). El número de terminales que podemos tener por subred, en función del número de bits que destinemos al campo subnetid, utilizando una dirección IP de **clase B** son:

Bits de Subred	Número de Subredes	Hosts por Subred
0	1	65534
2	2	16382
3	6	8190
4	14	4094
5	30	2046
6	62	1022
7	126	510
8	254	254
9	510	126
10	1022	62
11	2046	30
12	4094	14
13	8190	6
14	16382	2

Tabla 1.2: Número de subredes posibles

Por otra parte, la máscara de red es la encargada de identificar la porción de la dirección ocupada por los campos netid y subnetid. La máscara es simplemente otra cadena de 32 bits representada en formato decimal separado por puntos, en el que se indica con “1” la porción ocupada por los campos netid y subnetid y con “0” el espacio reservado a hostid.

1.3.6 Direccionamiento Classless

A medida que Internet fue evolucionando a lo largo de los últimos años, dos de los problemas de escalabilidad de IP se han visto agravados. Por una parte, se produce un agotamiento de las direcciones de clase B, y por otra, el tamaño de las tablas de encaminamiento de los routers Backbone crece de manera desmesurada. Para solucionar estos problemas se utilizó el direccionamiento Classless.

Con este tipo de direccionamiento el número de bits de los campos hostid y netid se definen dinámicamente, según las necesidades del ISP; y de esta forma desaparece el concepto de clase A, B ó C. Para poder averiguar el tamaño del campo netid en este tipo de direccionamiento se utiliza el prefijo /X detrás de la dirección IP, donde X representa el tamaño de la porción de red. Esta representación se denomina Notación CIDR (Classless Interdomain Routing).

Visto de otra forma, esta notación también representa bloques contiguos de direcciones de red que pertenecen a una clase determinada (A, B ó C), de manera que el prefijo /X identifica el número de bits comunes, empezando por la izquierda, en el bloque de direcciones. Por ejemplo, supongamos que un ISP solicita el bloque de direcciones IP de clase C contiguas desde la 212.128.8.0 hasta la 212.128.15.0. Observemos la representación en notación punto decimal de estas direcciones:

212.128.8.0 212.128.**00001**000.00000000
212.128.9.0 212.128.**00001**001.00000000
212.128.10.0 212.128.**00001**010.00000000
212.128.11.0 212.128.**00001**011.00000000
212.128.12.0 212.128.**00001**100.00000000
212.128.13.0 212.128.**00001**101.00000000
212.128.14.0 212.128.**00001**110.00000000
212.128.15.0 212.128.**00001**111.00000000

Podemos observar que la parte común a todas las direcciones de red es 212.128.00001xxx.xxxxxxxx, esto en notación CIDR se representa como 212.128.8.0/21, por los 21 bits comunes a todas las direcciones. Esto aumenta la flexibilidad a la hora de distribuir los bits de la dirección IP, ya que ahora la porción de red de la dirección está representada por el prefijo CIDR, como indicamos anteriormente. Así, en el ejemplo anterior, la dirección de red 212.128.8.0/21, representa a los hosts que se encuentran entre las direcciones IP 212.128.8.0 y 212.128.15.254, lo que nos permite direccionar un total de 2^{11} hosts.

Esta técnica permite utilizar direcciones de red más ajustados a las necesidades de las organizaciones, como observamos en la siguiente tabla:

Prefijo CIDR	Nº de hosts
/17	$2^{15} - 2 = 32766$
/18	$2^{14} - 2 = 16382$
/19	$2^{13} - 2 = 8190$
/20	$2^{12} - 2 = 4094$
/21	$2^{11} - 2 = 2046$
/22	$2^{10} - 2 = 1022$
/23	$2^{9} - 2 = 510$
/24	$2^{8} - 2 = 254$

Tabla 1.3: Número de hosts en función del prefijo CIDR

Además, esta técnica también nos permite solucionar el problema del crecimiento de las tablas de encaminamiento de los routers, puesto que ahora podemos agregar las rutas a varias redes contiguas (que comparten el mismo prefijo CIDR) y también cercanas en cuanto a su situación topológica (que se llega a ellas a través del mismo gateway), en una sola entrada de la tabla de encaminamiento. Esto abre la puerta a un encaminamiento jerárquico, y de esta manera, lo que se pretende es que los routers Backbone tengan entradas con prefijos pequeños, que incluyan muchas redes a las que se llega por el mismo gateway.

Actualmente se asignan grandes bloques de direcciones IP contiguas a los grandes ISP, y estos utilizan el direccionamiento Classless y la notación CIDR para repartir estas direcciones IP entre sus abonados. Así, en el ejemplo del ISP anterior:

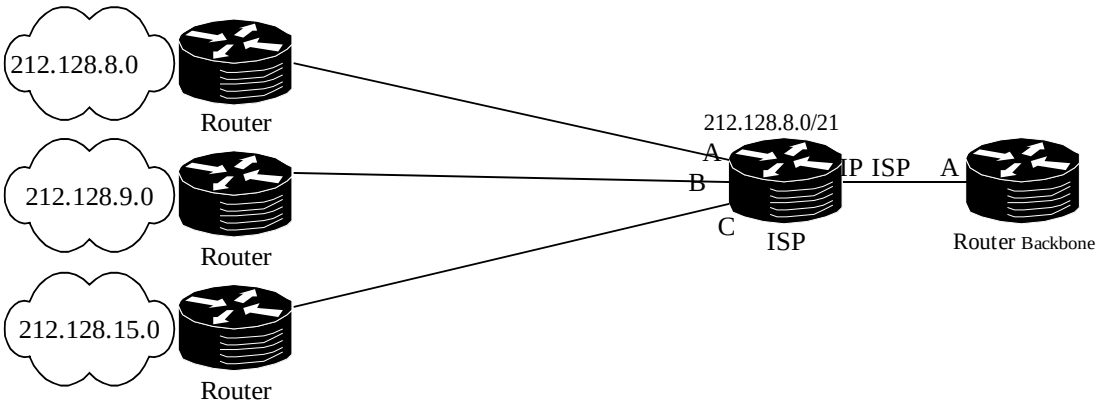

Figura 1.3: Ejemplo de direccionamiento Classless

Tabla de encaminamiento del Router Backbone:

IP destino	Máscara	Interfaz	GW
212.128.8.0	255.255.248.0	A	IP ISP

Tabla 1.4: Tabla de encaminamiento con direccionamiento Classless

El router Backbone encamina las redes contiguas, que se acceden por el mismo gateway, con una sola entrada en su tabla de encaminamiento.

1.3.7 Direccionamiento privado y NAT

El problema de escasez de direcciones IP se puede moderar mediante el uso de direccionamiento privado y de NAT. Existentes tres rangos de direcciones IP privadas:

DIRECCIÓN (Notación CIDR)	RANGO
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

Tabla 1.5: Direccionamiento privado

Estas direcciones se utilizan únicamente en las redes privadas, y no son válidas fuera de ellas. Es decir, no puede haber un datagrama IP circulando por Internet con una dirección IP privada. Dentro de las redes privadas, se pueden escoger cualquiera de las direcciones anteriores.

Por otra parte, la técnica NAT consiste en utilizar una única dirección IP pública en todo el tráfico generado por una red privada. Esta técnica se estudia con más detenimiento en el capítulo 5.

1.4 El datagrama IP

En una red la unidad de transferencia se denomina paquete y está compuesta por un encabezado (overhead) y por los datos. En Internet, a esta unidad de transferencia básica se llama *datagrama IP* (ver Fig. 1.4).

A continuación describiremos brevemente el significado de cada uno de los campos que conforman la cabecera de un datagrama IP.

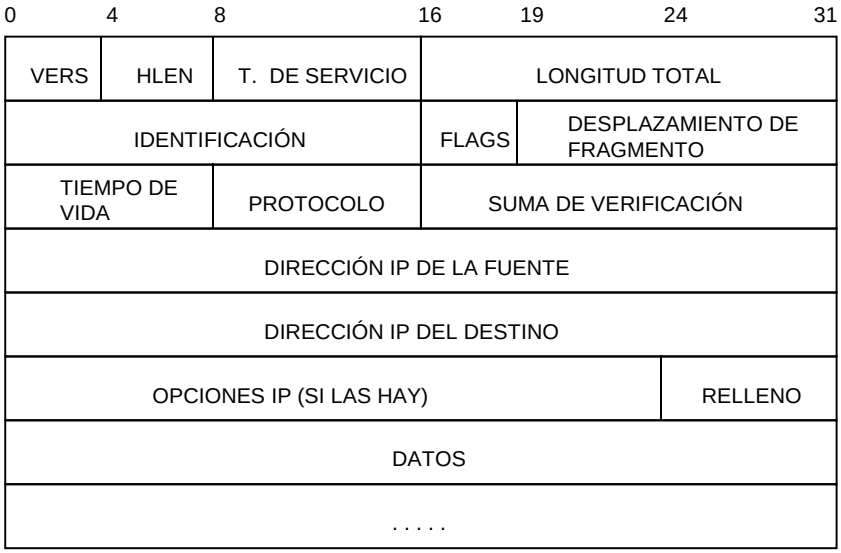

Figura 1.4: Formato de un datagrama IP

El primer campo de 4 bits *(VERS)* contiene la versión del protocolo IP que se utilizó para crear el datagrama. En general, el valor más habitual es 4 (es decir, versión 4), aunque las redes IPv6 (o también IP next generation) empiezan a utilizarse en entornos aislados (LAN).

El campo de longitud de encabezado *(HLEN)*, también de 4 bits, nos indica la longitud de la cabecera en múltiplos de 32 bits.

Type Of Service (TOS), es de 8 bits y especifica la manera en que debe manejarse el datagrama.

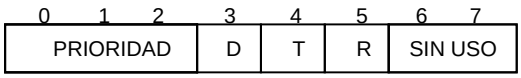

Figura 1.5: Campo Type Of Service

Los tres bits PRIORIDAD especifican la prioridad del datagrama, con valores que abarcan de 0 (prioridad normal) a 7 (máxima), permitiendo con ello indicar al emisor la importancia de cada datagrama. Si los routers responden a la prioridad, es posible implementar algoritmos de control de congestión.

Los bits D, T y R especifican el tipo de transporte deseado para el datagrama. Cuando está activado, el bit D solicita procesamiento con retardos cortos, el bit T solicita un alto caudal y el bit R solicita alta confiabilidad. Por supuesto, no es posible garantizar siempre el tipo de transporte solicitado. Se puede ver la especificación del tipo de transporte como una indicación para el algoritmo de encaminamiento que ayuda en la selección de una ruta entre varias hacia un

destino, con base en el conocimiento de las tecnologías de hardware disponibles en esas rutas. En realidad, la red no garantiza la realización del tipo de transporte solicitado.

El campo TOTAL LENGTH proporciona la longitud del datagrama IP medido en octetos, incluyendo los octetos del encabezado y los datos. Dado que el campo TOTAL LENGTH tiene una longitud de 16 bits, el tamaño máximo posible de un datagrama IP es de 2^{16} (65.535 octetos).

El campo TIME TO LIVE sirve para evitar que un datagrama concreto esté permanentemente circulando por la red (es decir, para evitar loops). Los routers que procesan los datagramas deben decrementar el campo TIME TO LIVE cada vez que procesan un datagrama y eliminarlo de la red cuando su valor llega a cero.

El valor en el campo PROTOCOL especifica qué protocolo de alto nivel se utilizó para crear el mensaje que se está transportando en el área DATA de un datagrama. Por lo general, dentro de un datagrama IP se encapsula una trama TCP ó UDP.

El campo HEADER CHECKSUM asegura la integridad de los valores de la cabecera. La suma de verificación IP se forma considerando a la cabecera como una secuencia de enteros de 16 bits, sumándolos juntos mediante el complemento aritmético a uno, y después formando el complemento a uno del resultado. Es importante notar que la suma de verificación sólo se aplica para valores de la cabecera IP y no para los datos.

Los campos SOURCE IP ADDRESS y DESTINATION IP ADDRESS contienen direcciones IP de 32 bits del emisor y del receptor involucrado. Son, sin duda, los campos más importantes de la cabecera.

El campo marcado con el nombre DATA muestra el comienzo del área de datos de un datagrama. Su longitud depende, por supuesto, del contenido de lo que se está enviando en el datagrama.

El campo OPTIONS aparece a continuación de la dirección de destino y no se requiere en todos los datagramas; las opciones se incluyen en principio para pruebas de red o depuración. La longitud del campo OPTIONS varía dependiendo de la opción que se selecciona. Algunas opciones tienen una longitud de un octeto. Otras tienen longitudes variables. En general, este campo se utiliza para funciones muy específicas que caen fuera del alcance de este proyecto.

Los campos FLAGS y DESPLAZAMIENTO DE FRAGMENTO se explicarán en la siguiente sección.

1.5 Fragmentación y reensamblado

Sabemos que, como los datagramas se mueven de una máquina a otra, éstos deben transportarse siempre a través de una red física subyacente. Para hacer eficiente el transporte en la red sería deseable que cada datagrama IP se correspondiera directamente con una trama de nivel físico. La idea de transportar un datagrama dentro de una trama de red es conocida como encapsulación. Para la red física subyacente, un datagrama es como cualquier otro mensaje que se envía de una máquina a otra. El hardware no reconoce el formato del datagrama ni entiende las direcciones IP.

1.5.1 Fragmentación

En un caso ideal, el datagrama IP completo se ajusta dentro de una trama física haciendo que la transmisión a través de la red física sea eficiente. Sin embargo, cada tecnología de conmutación de paquetes establece un límite superior fijo para la cantidad d e datos que puede transferir un paquete. Nos referiremos a estos límites como la unidad de transferencia máxima de una red (MTU). El software TCP/IP selecciona un tamaño de datagrama más conveniente y establece una forma para dividir datagramas en pequeños fragmentos cuando el datagrama necesita viajar a través de una red que tiene una MTU pequeña. Las pequeñas piezas dentro de un datagrama dividido se conocen con el nombre de fragmentos y el proceso de división de un datagrama se conoce como fragmentación. El tamaño de cada fragmento se selecciona de manera que cada uno de éstos pueda transportarse a través de la red subyacente en una sola trama. Los fragmentos se deben reensamblar para producir una copia completa del datagrama original, antes de que pueda procesarse en su lugar de destino.

Cada fragmento contiene un encabezado de datagrama que duplica la mayor parte del encabezado del datagrama original (excepto por un bit en el campo FLAGS que muestra que éste es un fragmento), seguido por tantos datos co mo puedan ser transportados en el fragmento, siempre y cuando la longitud total se mantenga en un valor menor a la MTU de la red en la que debe viajar.

1.5.2 Reensamblado de fragmentos

En una red TCP/IP, una vez que un datagrama se ha fragmentado, los fragmentos viajan como datagramas independientes hacia su destino final donde serán reensamblados. Lógicamente, si se pierde cualquier fragmento, el datagrama no podrá reensamblarse. La máquina de recepción arranca un temporizador de reensamblando cuando recibe el fragmento inicial. Si el temporizador termina antes de que todos los fragmentos lleguen, la máquina de recepción descartará los fragmentos sin procesar el datagrama.

1.5.3 Control de fragmentación

Tres campos en la cabecera del datagrama, IDENTIFICATION, FLAGS y FRAGMENT OFFSET, controlan la fragmentación y el reensamblado de los datagramas. El campo IDENTIFICATION contiene un entero único que identifica el datagrama. Cuando un router fragmenta un datagrama, éste copia la mayor parte de los campos de la cabecera del datagrama dentro de cada fragmento El campo IDENTIFICATION debe copiarse, ya que se utiliza para permitir que el destino tenga información acerca de los fragmentos que pertenecen a un mismo datagrama.

Para un fragmento, el campo FRAGMENT OFFSET especifica el desplazamiento en el datagrama original de los datos que se están transportando en el fragmento, medido en unidades de 8 octetos, comenzando con un desplazamiento igual a cero. Para reensamblar el datagrama, el destino debe obtener todos los fragmentos comenzando con el fragmento que tiene asignado un desplazamiento igual a 0 hasta el fragmento con el desplazamiento de mayor valor.

Los 2 bits de orden menor del campo de 3 bits FLAGS controlan la fragmentación. El primer bit de control especifica en qué momento se debe fragmentar un datagrama. Se le conoce como bit de no-fragmentación porque cuando está puesto a 1 especifica que el datagrama no debe fragmentarse. Cada vez que un router necesita fragmentar un datagrama que tiene activado el bit de no-fragmentación, el router descartará el datagrama y devolverá un mensaje de error a la fuente, mediante el protocolo ICMP. El bit de orden inferior en el campo FLAGS especifica si el fragmento contiene datos intermedios del datagrama original o de la parte final. Este bit es conocido como *more fragments*. Cada vez que en el destino se recibe un fragmento con el bit

more fragments desactivado, se sabe que este fragmento transporta datos del extremo final del datagrama original. De los campos FRAGMENT OFFSET y TOTAL LENGTH se puede calcular la longitud del datagrama original. Examinando FRAGMENT OFFSET y TOTAL LENGTH, en el caso de todos los fragmentos entrantes, un receptor puede establecer en qué momento los fragmentos que ha reunido contienen toda la información necesaria para reensamblar el datagrama original completo.

1.6 IP routing

En un sistema de conmutación de paquetes, el routing es el proceso que selecciona el camino que deberán seguir los datagramas desde la fuente de los datos hasta el destinatario, y el router es el dispositivo que hace dicha selección. Idealmente, el software de routing examinaría aspectos como la carga de red, la longitud del datagrama o el tipo de servicio que se especifica en el encabezado del datagrama, para seleccionar el mejor camino. Sin embargo, la mayor parte del software de routing en Internet es mucho menos sofisticado y selecciona rutas basándose en suposiciones sobre los caminos más cortos.

1.6.1 Entrega directa e indirecta

Podemos ver el encaminamiento de dos formas distintas: entrega directa y entrega indirecta.

ENTREGA DIRECTA: La transmisión de un datagrama IP entre dos máquinas dentro de una misma red física no involucra routers. El transmisor encapsula el datagrama dentro de una trama física, transforma la dirección IP de destino en una dirección física y envía la trama resultante directamente a su destino. Debido a que las direcciones IP de todas las máquinas dentro de una sola red incluyen un prefijo en común y como la extracción de dicho prefijo se puede realizar mediante unas cuantas instrucciones máquina, la comprobación de que una máquina se puede alcanzar directamente es muy eficiente.

ENTREGA INDIRECTA: La entrega indirecta es más difícil que la directa porque el transmisor debe identificar un router para enviar el datagrama. Después, el router debe encaminar el datagrama hacia la red de destino. Los routers en una red TCP/IP forman una estructura cooperativa e interconectada. Los datagramas pasan de un router a otro hasta que llegan a uno que los pueda entregar en forma directa.

1.6.2 Tablas de encaminamiento

El algoritmo usual de encaminamiento emplea una tabla de encaminamiento en cada máquina, que almacena información sobre posibles destinos y sobre cómo alcanzarlos.

Por lo común, una tabla de encaminamiento contiene pares (N,R) donde N es la dirección IP de una red de destino y R la dirección IP del “siguiente” router en el camino hacia la red N. El router R es conocido como el salto siguiente. La idea de utilizar una tabla de encaminamiento para almacenar un salto siguiente para cada destino es conocida como encaminamiento con salto al siguiente.

Otra técnica utilizada para mantener reducido el tamaño de las tablas de encaminamiento es asociar muchos registros a un router asignado por omisión. La idea es hacer que el software de encaminamiento IP busque primero en la tabla de encaminamiento para encontrar la red de destino. Si no aparece una ruta en la tabla, las rutinas de encaminamiento envían el datagrama a un router asignado por omisión (default gateway).

El procedimiento de encaminamiento es el siguiente. El router aplica la función AND a la dirección IP de destino de la trama y a la dirección IP de la primera entrada de la tabla de encaminamiento, con la máscara de esta entrada de la tabla, y si los resultados de las dos operaciones son iguales transmite la trama hacia el gateway de salida correspondiente a esa entrada de la tabla de encaminamiento; y si no son iguales, vuelve a aplicar la misma operación con la siguiente entrada de la tabla de encaminamiento.

1.6.3 Algoritmos de encaminamiento

Los routers IP realizan el encaminamiento en función de los valores que aparecen en la tabla de encaminamiento. Estos valores se deben calcular en función de la topología de la red: las conexiones entre routers y la carga de los enlaces. Valores erróneos en esta tabla pueden provocar que los datagramas no lleguen a su destino, que algunas partes de la red no puedan comunicarse con otras, que datagramas IP viajen formando ciclos entre routers gastando ancho de banda, empeorar el congestionamiento, etc.

Una red con un número alto de nodos tiene variaciones constantes en la topología. Las tablas de encaminamiento deben adaptarse a esos cambios. En caso de routers conectados a pocos enlaces, en un fragmento de red controlado por una misma organización, es posible controlar manualmente la tabla de encaminamiento (encaminamiento estático). Para casos no triviales es necesario que los routers se intercambien mensajes según algún algoritmo de encaminamiento (encaminamiento dinámico). Este algoritmo debe asegurar que todos los routers configuren las tablas con las rutas más cortas para cada destino. En general, al iniciarse un router, comienza con unos valores por defecto (sobre sus nodos vecinos normalmente). Comunicándose con otros routers va configurando la tabla de encaminamiento.

Se define el concepto de Sistema Autónomo (SA) como un conjunto de routers (y en definitiva de redes) administrados por una única organización. La IANA otorga un número identificativo para cada SA definido. De forma general, llamaremos IGP (Interior Gateway Protocol) a cualquier protocolo de encaminamiento que actúa dentro de un Sistema Autónomo, y que se encarga de gestionar los cambios sobre las tablas de encaminamiento de los routers interiores.

La información necesaria para configurar adecuadamente las tablas de encaminamiento es el estado de todos los enlaces de la red, lo que es muchas veces muy costoso. En una aproximación puramente centralizada, una máquina del SA recibe la información de estado de todos los enlaces, calcula las tablas de encaminamiento de todos los routers al mismo tiempo, y se las transmite. Se trata de un sistema poco escalable y poco tolerante a fallos.

Existen otras tendencias no centralizadas, como el RIP (estudiado en el capítulo 7), que es un protocolo que implementa un algoritmo del tipo vector-distancia; y el OSPF, que es un protocolo que implementa un algoritmo tipo SPF.

Capítulo 2
Introducción al *router* NUCLEOX PLUS

2.1 Introducción

El router NUCLEOX PLUS es un equipo de sobremesa, con fuente de alimentación interna, que consta de las siguientes interfaces:

- Puerto LAN, con 2 conectores:
  - 10BaseT.
  - AUI.
- 2 accesos básicos RDSI.
- 2 puertos serie V.24.
- Consola RS232C para configuración local.
- Disquetera 31/2“, para carga del perfil de configuración.
- 4 interfaces analógicos para el transporte de voz sobre IP.

El estado del equipo y de sus distintas interfaces se visualiza con facilidad mediante LEDs situados en la parte frontal.

El NUCLEOX PLUS actúa como conmutador de tráfico IP entre la interfaz LAN y las interfaces serie, WAN y RDSI, funcionando como router para la interconexión de redes locales. Implementa mecanismos de routing, tanto estáticos como dinámicos (RIP I, RIP II y OSPF), y también routing multicast. Por las líneas serie se conecta a enlaces punto a punto o conmutados, síncronos hasta 2 Mbps o asíncronos hasta 115.2 Kbps, mediante protocolo PPP. Las interfaces RDSI soportan agregación de canales hasta 256 Kbps mediante MPPP (Multilink Point-to-Point Protocol). En ambos casos se soportan mecanismos estándar de autentificación de usuarios PAP (Password Authentication Protocol) o CHAP (Challenge-Handshake Authentication Protocol).

Para la creación de VPN (redes privadas virtuales), se implementan túneles IP mediante el protocolo GRE (Generic Routing Encapsulation). Usando técnicas NAT se soporta el acceso por RDSI o RTB a Internet de una LAN con direccionamiento privado utilizando una única dirección IP pública. Implementa potentes controles de acceso (firewall), para filtrado de usuarios o servicios no deseados.

El NUCLEOX PLUS también es un dispositivo de acceso a redes Frame Relay (FRAD, FR Access Device). Se conecta mediante línea serie desde 300 bps hasta 2 Mbps, o por un canal RDSI, tanto a circuitos virtuales permanentes como conmutados. Admite los dos tipos de señalización LMI (Local Management Interface) más habituales (ANSI y UIT), con detección de circuitos huérfanos y monitorización de CIR para la localización de congestión. Permite el transporte de tráfico IP, X.25 y SNA mediante encapsulado RFC 1490.

Desde el punto de vista de la gestión, el NUCLEOX PLUS responde a las necesidades habituales de administración y control de redes, dotando al usuario de facilidades como configuración remota, envío y recepción de alarmas, monitorización, telecarga de software, etc. La gestión se ofrece en cuatro versiones: local desde consola, modo comando por Telnet y gestión SNMP sobre plataforma TELDAT o estándar. La conexión directa de un terminal

asíncrono a la línea de consola posibilita la configuración y monitorización de los parámetros de funcionamiento del NUCLEOX PLUS. Para la actualización local del perfil de configuración se utiliza el disquete de arranque. También es posible acceder al equipo mediante consola remota Telnet para tareas de configuración o monitorización (lógicamente, en este caso la configuración de la red TCP/IP debe estar funcionando). Mediante FTP se pueden realizar actualizaciones remotas de software.

El NUCLEOX PLUS soporta un abanico muy amplio de soluciones de backup:

- Backup extremo a extremo por canal B RDSI para protocolos de línea serie PPP, Frame Relay o X.25.
- Backup transparente (bit a bit) de enlaces punto a punto sin pérdida de sesión, basado en la detección de caída de señales físicas de la interfaz serie, e independiente del protocolo transportado.

En Voz sobre IP (VoIP), el NUCLEOX PLUS está ideado con intención de respetar al máximo las instalaciones existentes en planta de usuario. Aprovecha fácilmente todas las ventajas de la telefonía sobre IP, conectándose simultáneamente a la PABX convencional y la LAN de la oficina. Permite a las oficinas remotas realizar comunicaciones entre cualquier combinación de teléfonos convencionales, conectados directamente al NUCLEOX PLUS o a través de centralita, faxes convencionales y PCs multimedia. Soporta conversaciones full-duplex en tiempo real con calidad de sonido óptima, mediante algoritmos de cancelación de eco y controles de ganancia. Utiliza técnicas avanzadas de compresión/descompresión, implementadas según los estándares G.723.1 y G.729. Se soportan interfaces analógicos FXS/FXO y E&M, aunque este último ya está un poco anticuado. En cuanto a las llamadas sobre la red IP se implementan de acuerdo al estándar H.323 de la ITU-T, transportándose los paquetes de voz comprimida sobre protocolos RTP/UDP.

2.2 Características técnicas

Las características de las diferentes interfaces del router son las siguientes:

- Líneas WAN (2):
  - Conector standard DB25 macho.
  - Interfaz V.24. La línea 1 funciona como DTE y la línea 2 como DCE.
  - Velocidad: 300 bps a 2 Mbps.
- Líneas RDSI (2):
  - Interfaz: I.430TE, conector RJ45.
  - Canal D: Q.921, Q.931, X.25.
  - Canal B: X.25, transparente, MPPP, Frame Relay en Backup.
  - Circuitos conmutados y semipermanentes.
- Línea LAN:
  - Ethernet: IEEE 802.3
  - Conectores:
    - Puerto 10BaseT RJ45.
    - Puerto AUI DB15.
- Líneas analógicas de voz (4):
  - Conectores: 4 RJ11.
  - Interfaz: FXS/FXO, E&M.
  - Supresión de silencios.
  - Buffers de jitter dinámico.
  - Cancelación de eco.
- Línea de CONSOLA:
  - Conexión RS-232 a 9600 bps con conector DB9 hembra.

2.3 Configuración

El acceso al interfaz de configuración de los routers TELDAT puede realizarse mediante una conexión local al puerto serie de consola o de forma remota mediante una conexión vía telnet.

En caso de utilizar el puerto de consola, es necesario conectar éste al puerto serie de un PC, utilizando un cable serie RS-232 pin a pin con un conector DB9 macho. En el PC se debe arrancar alguna aplicación de emulación de terminales (por ejemplo, el HyperTerminal de Windows) y configurar la conexión con las siguientes características: terminal asíncrono a 9600 bps con 8 bits de datos y sin paridad.

Para acceder de forma remota utilizando telnet, es necesario haber configurado previamente los parámetros TCP/IP del equipo (dirección IP, máscara de red, etc). Para ello se deben seguir los pasos siguientes:

1. Acceder al router mediante el cable de consola.
2. Configurar los parámetros de IP del interfaz LAN (dirección IP, máscara, dirección IP interna, etc.) siguiendo los procedimientos descritos más adelante en este manual.
3. Salvar la configuración y rearrancar.
4. Establecer una sesión telnet contra la dirección IP del equipo desde algún ordenador remoto.

En cualquiera de los dos casos, tras establecer la conexión con el router, nos aparecerá en pantalla una serie de mensajes indicándonos ciertas características del equipo. Una vez iniciada la conexión con HyperTerminal, basta con pulsar “Enter” y nos aparecerá el símbolo “*” que nos indica que estamos en el menú principal.

La interfaz de configuración esta basada en cuatro procesos diferentes, cada uno de los cuales permite acceder a un conjunto distinto de comandos de configuración y monitorización. Cada proceso se identifica mediante un *prompt* diferente.

El proceso 1**,** que se identifica con el *prompt* “*****” y se denomina de gestión de consola (GESTCON), es el proceso que se activa nada más acceder al router. Desde él puede accederse al resto de procesos mediante la ejecución de los comandos “**process x**”, o de forma abreviada “**p x**”, siendo “x” el número del proceso deseado. Desde el proceso GESTCON se puede acceder a un conjunto de comandos que permiten comprobar el estado de los procesos, monitorizar la eficiencia de los interfaces de equipo y la transferencia de paquetes, así como la configuración de diversos parámetros. La mayoría de los cambios hechos en los parámetros de operación del Nucleox Plus en el proceso GESTCON tienen efecto inmediatamente sin necesidad de reiniciar el equipo.

Para volver al proceso 1 desde cualquier otro proceso se debe pulsar ‘Ctrl+p’. Es importante destacar que siempre se debe retornar al gestor de consola antes de ir a otro proceso.

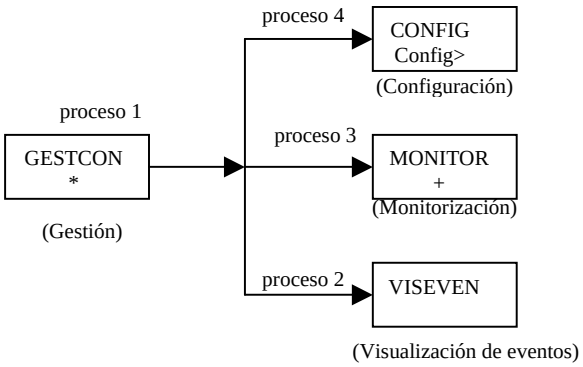

Figura 2.1: Procesos del Router Nucleox Plus

La utilidad del resto de procesos es la siguiente:

- **Proceso 2.** Se utiliza para visualizar eventos del sistema (trazas, errores, etc).
- **Proceso 3** (prompt "+"). Se utiliza para monitorizar el funcionamiento del router (por ejemplo, para ver las tablas de encaminamiento o conocer estadísticas de enlaces) o para acceder a las herramientas de diagnóstico (por ejemplo, ping y traceroute).
- **Proceso 4** (prompt "Config>"). Se utiliza para modificar o visualizar la configuración del equipo. El proceso de configuración permite configurar parámetros del router como los interfaces y los protocolos

Para introducir un comando sólo es necesario teclear las letras necesarias que lo distinguen de los demás, éstas están escritas en **negrita** en la sintaxis de cada uno de los comandos. Algunas veces se necesita una única letra del comando (y sus opciones) para ejecutarlo. Para borrar el último o los últimos caracteres tecleados en la línea de comandos se debe utilizar la tecla backspace.

A continuación tenemos una panorámica de los comandos de los diferentes procesos:

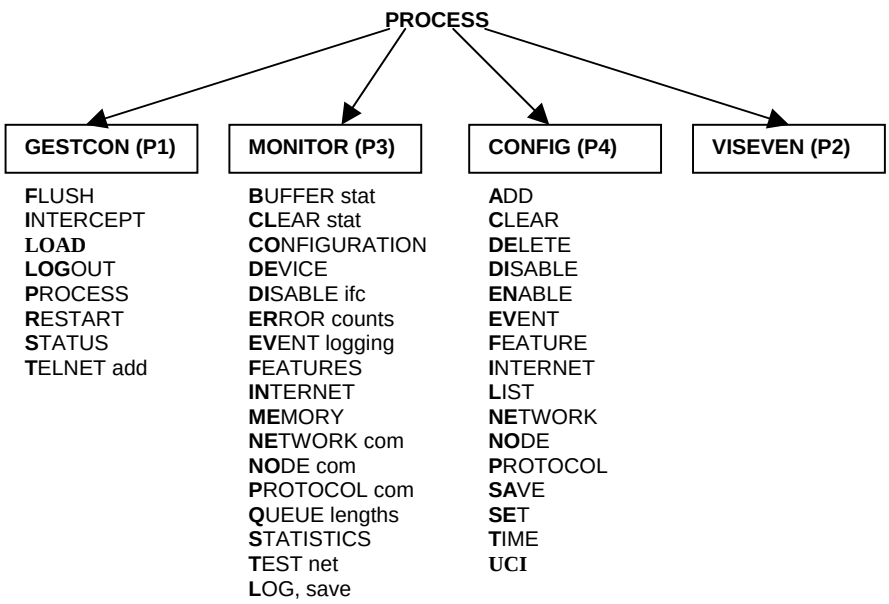

Figura 2.2: Comandos de los diferentes procesos

Por otra parte, el programa de configuración incluye un completo sistema de ayuda que permite conocer los comandos disponibles en cada proceso, así como el formato de sus parámetros. Tecleando **?** se muestran los comandos disponibles en cada momento. También se puede teclear **?** después del nombre de un comando específico para listar sus opciones.

En el caso de que queramos establecer una nueva configuración en el router, y borrar la configuración que tenga actualmente, debemos seguir los siguientes pasos. Desde el **Proceso 4** se utiliza el comando **CLEAR**, que permite borrar información de configuración del router. Para borrar la configuración de un protocolo teclear **CLEAR** y el nombre del protocolo. Para borrar toda la información, excepto información de interfaces teclear **CLEAR ALL**, y para borrar información de interfaces teclear **CLEAR DEVICE**. Para que los cambios hechos en este proceso se almacenen, se tiene que ejecutar el comando **SAVE**, que permite almacenar la configuración en disco. Así mismo, para que los cambios realizados en el proceso de configuración del equipo tengan efecto, se tiene que reiniciar el router mediante el comando **RESTART**, que se ejecuta desde el **Proceso 1**, o simplemente, apagando y encendiendo de nuevo el router. Hay que recordar que hay que reiniciar el equipo cada vez que se cambia la configuración del mismo para que los cambios tengan efecto. Esto provoca que:

- Los contadores software se ponen a cero.
- Se hace un test de las redes conectadas.
- Se borran las tablas de routing.
- Descarta todos los paquetes hasta que el reinicio se completa.
- Ejecuta la configuración actual.

Lógicamente, si este comando se usa en una conexión de terminal remoto, se pierde la sesión TELNET porque todos los procesos del equipo son reiniciados.

2.4 Configuración de las interfaces

Desde el punto de vista funcional, en el Nucleox Plus están integrados dos equipos virtuales:

1. Un router IP que realiza las funciones de internetworking.
2. Un conmutador de paquetes X.25 con entradas provenientes tanto del router como de los puertos X.25 y RDSI (cuando éstos transportan X.25).

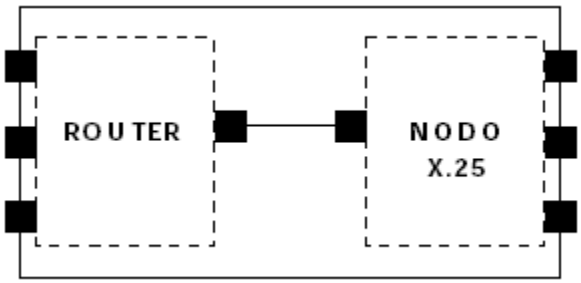

Figura2.3: Equipos virtuales del Nucleox Plus

Como se puede ver en la figura, cada equipo virtual gobierna su propio conjunto de interfaces. Es necesario pues poder identificar de forma precisa los distintos interfaces y saber si un interfaz pertenece al router o al nodo.

La forma en la que se identifican los interfaces en la configuración del Nucleox Plus es a través de un número.

Mediante el comando **LIST DEVICES** del proceso de configuración se obtiene la tabla de identificadores de interfaz. A continuación se muestra la salida de dicho comando al arrancar por primera vez el NUCLEOX PLUS:

```
Config>LIST DEVICES

Con    Ifc Type of interface                CSR     CSR2  int
---      1 Router->Node                       0             0
---      2 Node->Router                       0             0
ISDN 1   5 ISDN D channel: X25          A000000             1B
ISDN 1   7 ISDN B channel: X25          F001640  F000E00    9C
ISDN 2   6 ISDN D channel: X25          A200000             1B
ISDN 2   8 ISDN B channel: X25          F001660  F000F00    9B
LAN      0 Ethernet                     9000000             1C
WAN1     3 X25                          F001600  F000C00    9E
WAN2     4 X25                          F001620  F000D00    9D
Config>
```

La primera columna indica el conector físico al que corresponde el interfaz (*Con*), la segunda es el identificador de la interfaz (*Ifc*), la tercera columna especifica el tipo de interfaz programado, las columnas *CSR, CSR2* hacen referencia a posiciones de memoria dentro del equipo, y la columna *int* corresponde a las direcciones de interrupciones.

Como puede verse, los interfaces 5 y 7 comparten el conector RDSI 1, mientras que los interfaces 6 y 8 comparten el RDSI 2.

Otro aspecto importante es que hay interfaces que no tienen asociado un conector físico. Este es el caso de los interfaces 1 y 2 del ejemplo. Esto es debido a que son precisamente los interfaces que permiten unir las máquinas virtuales y por tanto no tienen asociado un conector externo, es decir, podríamos llamarlos conectores internos.

Con respecto a los números de interfaz hay que tener en cuenta que:

- Los interfaces gobernados por el nodo son: el Node->Router, los X.25 y los ISDN (que transporten X.25).
- Los interfaces gobernados por el router son todos los demás.
- Los interfaces del router empiezan por el 0 que suele corresponder al conector de LAN y terminan con el Router->Node. Los interfaces del nodo están a continuación.

Con toda esta información se puede rehacer la figura anterior para este caso:

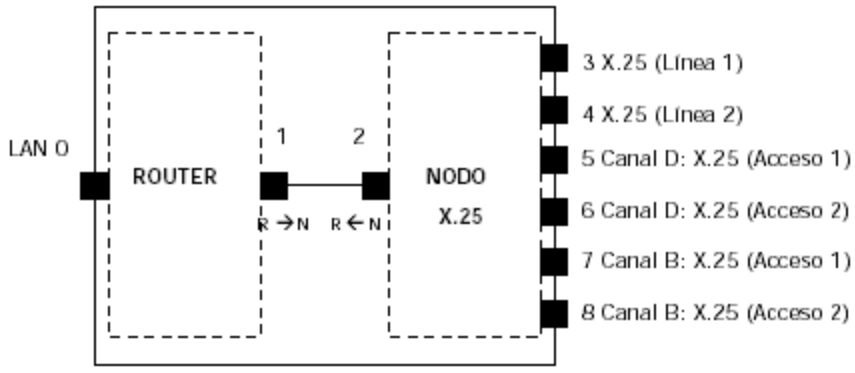

Figura 2.4: Estado Inicial del Nucleox Plus

Suponga ahora que se cambia el protocolo de una de las líneas WAN mediante el comando **SET DATA-LINK** y que a continuación se consulta la tabla de interfaces. En el siguiente ejemplo se asigna al interfaz WAN1 el protocolo Frame Relay:

```
Config>SET DATA-LINK FRAME RELAY
which port will be changed[1]? 2
Config>
Config>LIST DEVICES

Con    Ifc Type of interface                CSR     CSR2  int
---      2 Router->Node                       0             0
---      3 Node->Router                       0             0
ISDN 1   5 ISDN D channel: X25          A000000             1B
ISDN 1   7 ISDN B channel: X25          F001640  F000E00    9C
ISDN 2   6 ISDN D channel: X25          A200000             1B
ISDN 2   8 ISDN B channel: X25          F001660  F000F00    9B
LAN      0 Ethernet                     9000000             1C
WAN1     1 Frame Relay                  F001600  F000C00    9E
WAN2     4 X25                          F001620  F000D00    9D
Config>
```

Figura 2.5: Ejemplo de Configuración

Como se puede ver ahora hay un interfaz más, gobernado por el router y uno menos por el nodo. También se puede observar que el interfaz correspondiente a la línea 2 es el número 1 mientras que el de la línea 1 es el número 4. En este nuevo ejemplo el esquema del equipo queda:

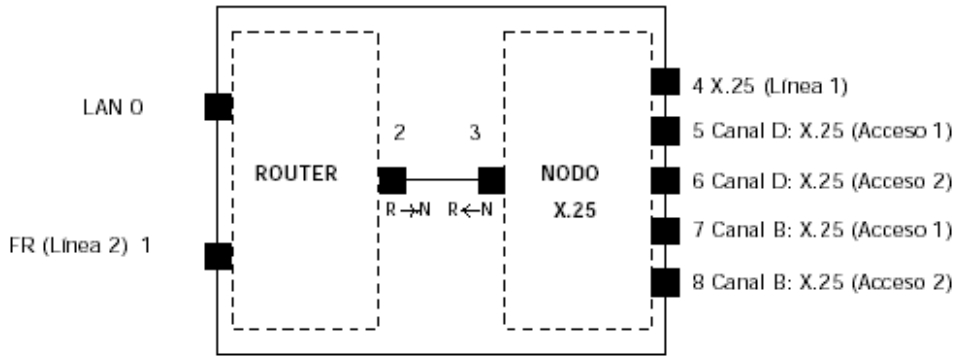

Figura 2.6: Ejemplo de Estado

Cuando se procede a configurar un equipo siempre hay que identificar correctamente los interfaces a través del identificador mostrado en la tabla del comando LIST DEVICES. No deberá por tanto utilizarse el número de conector.

Capítulo 3
Tecnologías WAN: PPP

3.1 Introducción a las tecnologías WAN

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área extendida. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN tales como las compañías telefónicas y proveedores de acceso a Internet.

Los protocolos de enlace de datos WAN describen la forma en que las tramas se llevan entre los sistemas de conmutación, utilizando un único enlace de datos.

Los estándares WAN son definidos y manejados por un número de autoridades reconocidas incluyendo las siguientes agencias:

- International Telecommunication Union-Telecommunication Standarization Sector (ITU-T).
- International Organization for Standardization (ISO).
- Internet Engineering Task Force (IETF).
- Electronic Industries Association (ETA).

Los protocolos WAN definen típicamente las características tanto del nivel físico como del nivel de enlace. Algunos, además, definen también especificaciones del nivel de red (como X.25).

1. Capa Física WAN

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo del circuito de datos (DCE). Típicamente, el DCE es el proveedor de servicio y el DTE es el dispositivo asociado al equipo de usuario. Por lo general los enlaces WAN son siempre circuitos serie puesto que se supone que tienen que cubrir distancias kilométricas largas.

Algunos estándares de la capa física que especifican esta interfaz son:

- EIA/TIA-232D: Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.

- EIA/TIA-449: Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.

- V.35: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha que operara en el intervalo de 48 a 168 kbps.

- X.21: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.

- G.703: Recomendaciones del ITU-T relativas a los aspectos generales de una interfaz.

- High-Speed Serial Interface (HSSI): Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

2. Capa de Enlace de Datos: Protocolos WAN

Se describen a continuación los protocolos DLC (Data Link Control) más utilizados en las actuales redes de comunicación. Por su falta de interés, no enunciaremos los protocolos orientados a carácter (como por ejemplo xmodem, kermit, etc.), a excepción del protocolo PPP, que se describirá con mayor detalle en siguientes apartados.

- Synchronous Data Link Control (SDLC). Es un protocolo orientado a bit y que fue desarrollado por IBM. SDLC define un entorno WAN en el que se permite que varias estaciones se conecten a un recurso dedicado. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.

- High-Level Data Link Control (HDLC). Soporta tres tipos de configuraciones: NRM (Normal Response Mode), ARM (Asynchronous Response Mode), ABM (Asynchronous Balanced Mode). Sin embargo, ARM está completamente en desuso. En modo NRM, HDLC se comporta de forma parecida a SDLC (es decir, comunicación entre una estación primaria y varias secundarias). El modo ABM es el más completo pues permite comunicación full-duplex.

- Link Access Procedure Balanced (LAPB). Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de tramas, así como también para intercambio, retransmisión, y reconocimiento de marcos. Es, en realidad, un subconjunto de HDLC.

- Frame Relay. Utiliza los recursos digitales de alta calidad con objeto de eliminar la verificación de errores LAPB. Al utilizar un marco simplificado sin mecanismos de corrección de errores, Frame Relay puede enviar la información de la capa 2 muy rápidamente, comparado con otros protocolos WAN.

- Point-to-Point Protocol (PPP). Descrito por el RFC 1661, un estándar desarrollado por el IETF y muy utilizado actualmente en Internet.

3.2 El protocolo PPP

Actualmente, cuando muchos usuarios piensan en Point to Point Protocol (PPP), lo hacen pensando en ordenadores personales (PCs), módems, y navegación por Internet. Sin embargo, PPP es un protocolo mucho más amplio que se emplea para transferir datos entre diversos tipos de computadoras y sistemas de telecomunicación. Este protocolo tiene la habilidad de manejar tasas de datos desde las más bajas a las más altas, y es compatible con prácticamente cualquier tecnología de redes.

PPP fue diseñado para permitir el intercambio de datagramas entre dos terminales a través de un enlace de comunicaciones. Dicho enlace debe ofrecer una comunicación full-duplex (bidireccional y simultánea) y un transporte ordenado de los datagramas.

El antecesor de PPP es el protocolo SLIP (Serial Line IP), pero algunas de sus restricciones lo hacen poco versátil para las necesidades actuales, por lo que ha ido perdiendo puestos frente a PPP. Las principales deficiencias de SLIP son las siguientes:

- SLIP no ofrece ningún procedimiento para obtener una dirección IP dinámicamente del servidor de acceso. Por ello, cada vez que se estable una conexión SLIP, el usuario debe indicar manualmente la dirección IP que se usará. De igual forma, SLIP no ofrece ningún mecanismo para que el servidor indique su propia dirección IP al cliente. Estas deficiencias no son importantes si las direcciones en cada extremo de la conexión son siempre fijas, pero hoy día lo normal es que la asignación de direcciones IP se haga de forma dinámica, obteniendo una IP diferente en cada conexión.

- SLIP no incluye ningún campo en su trama que permita identificar el protocolo de nivel superior que está transportando, por lo que es imposible que varios protocolos compartan el mismo enlace serie. SLIP está restringido al transporte del protocolo IP únicamente.

- SLIP originariamente no incluía ningún tipo de mecanismo de compresión de datos para mejorar la eficiencia. Para eliminar esta carencia se desarrolló posteriormente CSLIP (Compressed SLIP). El protocolo CSLIP no comprime los campos de datos, únicamente comprime las cabeceras TCP e IP en los segmentos TCP. Curiosamente, las cabeceras UDP e IP en los datagramas UDP no se comprimen.

Por el contrario el protocolo PPP:

- Permite la asignación dinámica de direcciones IP en ambas direcciones del enlace.
- Permite multiplexar un gran número de protocolos de nivel de red.
- Define mecanismos muy potentes para la detección de errores.
- Permite la verificación de autenticidad.
- Define una sesión de cuatro fases:
  - Establecimiento del enlace.
  - Determinación de la calidad del enlace (Autentificar Host).
  - Configuración del protocolo de capa de red.
  - Terminación del enlace.

3.3 Componentes principales

El protocolo PPP tiene tres componentes principales:

- Encapsulación, que ofrece la posibilidad de multiplexar diferentes protocolos de nivel de red sobre un mismo enlace serie.
- LCP (Link Control Protocol), que es un protocolo de control de enlace que configurará las opciones de encapsulación, el tamaño de los paquetes, detectará cualquier error de configuración en los hosts, autentificará al otro extremo del enlace y terminará el enlace.
- NCP (Network Control Protocol), que es el protocolo encargado de manejar las particularidades de los diferentes protocolos a nivel de red con los que PPP puede trabajar.

Además, PPP también ofrece:

- Protocolos de autenticación para exigir que el extremo remoto del enlace PPP se autentique antes de poder transmitir datos por el enlace. En la implementación actual se soportan los protocolos PAP (Password Authentication Protocol) descrito en la RFC-1172 y CHAP (Challenge-Handshake Authentication Protocol) definido en la RFC-1994.
- Protocolo Multilink PPP (MPPP) según la RFC-1990. El protocolo Multilink PPP permite dividir, recombinar y secuenciar datagramas a través de múltiples enlaces de

datos. La implementación actual permite agregar canales B de RDSI a uno o varios canales lógicos MPPP. También es posible agregar interfaces PPP sobre WAN (tanto síncrono como asíncrono) a un canal MPPP, aunque en este caso únicamente se deberá agregar una interfaz PPP en cada canal MPPP.

3.3.1 Encapsulación PPP

El paquete PPP tiene la siguiente estructura (los números representan el número de bytes):

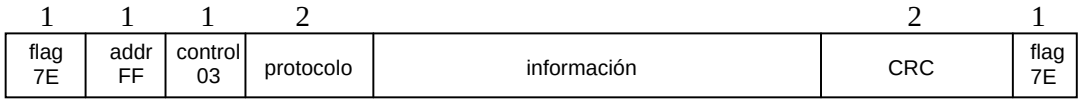

Figura 3.1: Formato del paquete PPP

A continuación se van a describir cada uno de los campos del paquete PPP.

PROTOCOLO. Este campo puede ser de 8 o 16 bits. Identifica al paquete encapsulado en el campo INFORMACIÓN. Hay algunos valores reservados para uso interno del protocolo:

Código	Protocolo	Código	Protocolo
0x0001	Reserved (transparency inefficient)	0x8021	Internet Protocol Control Protocol
0x0021	Internet Protocol	0x8023	OSI Network Layer Control Protocol
0x0023	OSI Network Layer	0x8025	Xerox NS IDP Control Protocol
0x0025	Xerox NS IDP	0x8027	DECnet Phase IV Control Protocol
0x0027	DECnet Phase IV	0x8029	Appletalk Control Protocol
0x0029	Appletalk	0x802B	Novell IPX Control Protocol
0x002B	Novell IPX	0x802D	Reserved
0x002D	Van Jacobson Compressed TCP/IP	0x802F	Reserved
0x002F	Van Jacobson Uncomprerssed TCP/IP	0x8031	Bridging NCP
0x0031	Bridging PDU	0x8033	Stream Protocol Control Protocol
0x0033	Stream Protocol (ST-II)	0x8035	Banyan Vines Control Protocol
0x0035	Banyan Vines	0x8037	Reserved till 1993
0x0037	Reserved (until 1993)	0x80FF	Reserved (compression inefficient)
0x00FF	Reserved (compression inefficient)	0xC021	Link Control Protocol
0x0201	802.1d Hello Packets	0xC023	Password Authentication Protocol
0x0231	Luxcom	0xC025	Link Quality Report
0x0233	Sigma Network Systems		

Tabla 3.1: Valores del campo PROTOCOLO

INFORMACIÓN. Este campo contendrá el datagrama para el protocolo de nivel de red indicado en el primer campo, y por lo tanto, es de tamaño variable. El tamaño máximo del campo de información viene fijado por el valor del MRU (Maximum Receive Unit), el cual tiene un valor por defecto de 1500 bytes, aunque puede tomar otros valores tras el proceso de negociación al establecer la conexión. El valor de 1500 se ha tomado por tratarse del máximo valor en una red Ethernet y Tokeng Ring.

CRC. Este campo, que también se puede ver como FCS (Frame Check Sequence), es una comprobación de redundancia cíclica para detectar errores en la trama.

Cada trama empieza y termina con un byte de FLAG cuyo valor es de 0x7E. Es seguido por un byte de ADDRESS cuyo valor siempre es de 0xFF, y a continuación un byte de CONTROL, cuyo valor es de 0x03.

3.3.2 Link Control Protocol

Para establecer el enlace, cada host debe en primer lugar enviar paquetes LCP que configuren y comprueben dicho enlace de datos. Una vez establecido, se procede a la autentificación, si ésta es necesaria. El siguiente paso es el envío de paquetes NCP (Network Control Protocol) para seleccionar aquellos protocolos de nivel de red que serán utilizados y encapsulados. Una vez realizada esta selección y configuración ya pueden proceder ambos extremos del enlace al envío de datagramas. El enlace se mantendrá hasta que se cierre explícitamente mediante un paquete LCP o NCP o algún suceso externo lo fuerce. El proceso seguido para el establecimiento del enlace puede resumirse en el siguiente diagrama:

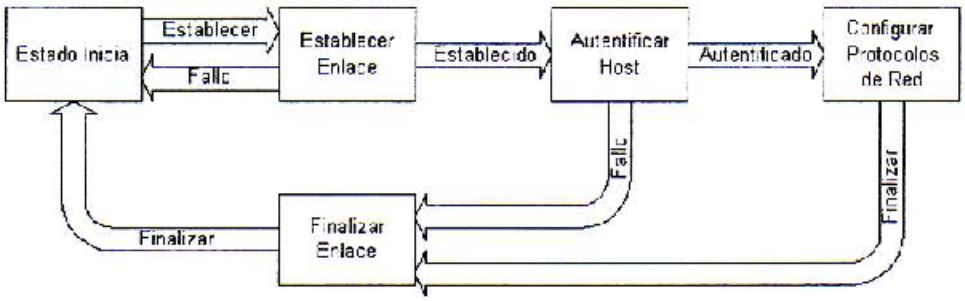

Figura 3.2: Fases de establecimiento del enlace.

Todo el proceso se inicia y finaliza en el *Estado Inicial*. En este estado se supone que el enlace físico no está disponible. Un suceso externo, como por ejemplo la detección de portadora, indicará que el enlace físico ya está disponible y se pasará a la fase *Establecer Enlace*.

En la fase *Establecer Enlace*, el protocolo de enlace (LCP) realizará un intercambio de paquetes de configuración entre los dos extremos. Si el proceso de configuración falla se volverá al *Estado Inicial*. En caso contrario se pasará a la fase de autentificación. En resumen, las acciones que se realizan en esta fase son:

- Cada dispositivo PPP envía paquetes LCP.
- Se establecen las opciones de:
  - Unidad de Transmisión Máxima (MTU).
  - Compresión de ciertos campos PPP.
  - Protocolo de autentificación del enlace.
- Terminación de la fase:
  - Se recibe y envía una trama de reconocimiento de la configuración.

La fase *Autentificar Host* es opcional. De requerirse un proceso de autentificación éste debe tener lugar antes de proceder a cualquier intercambio de paquetes de nivel de red. El protocolo usado para la autentificación se habrá negociado en la fase anterior de establecimiento del enlace. Si la autentificación falla, se procederá a la desconexión del mismo. En caso contrario se iniciará la configuración de los protocolos de red. En resumen, las características de esta fase son:

- Es una fase opcional.
- Se prueba el enlace para determinar si soportará protocolos de capa de Red.
- En esta fase se establece la autentificación del usuario.
- Los protocolos de autentificación utilizables son:
  - Password Authentication Protocol (PAP).
  - Challenge-Handshake Authentication Protocol (CHAP).

La fase *Configurar Protocolos de Red* permitirá configurar cada protocolo de red independientemente. A partir de ese momento ya podrán intercambiarse paquetes de datos. Las acciones que se llevan a cabo en esta fase son:

- Los dispositivos PPP envían paquetes NCP para escoger y configurar uno o más protocolos de Red.
- Si LCP cierra el enlace se informa a los protocolos de capa de Red.
- Verificación de los estados de LCP y NCP.

La fase *Finalizar Enlace* dará por terminado el enlace. Esta finalización se realizará de forma ordenada mediante los paquetes LCP correspondientes, indicando a los protocolos de nivel de red la finalización inminente del enlace, para que tomen las acciones apropiadas. Una vez superada esta fase, el nivel físico desconectará definitivamente el enlace de datos (por ejemplo, el módem colgaría), y se pasaría al *Estado Inicial*. LCP puede terminar el enlace en cualquier momento. Dos causas de terminación son: a petición del usuario y por un evento físico.

3.3.2.1 Formato de los paquetes LCP

Los paquetes LCP se encapsulan dentro del campo INFORMACIÓN de la trama PPP, identificándose con el valor 0xC021 dentro del campo PROTOCOLO.

El formato de un paquete LCP es el siguiente:

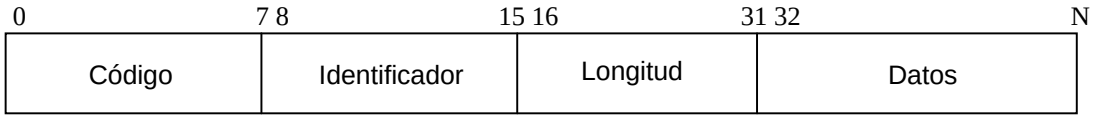

Figura 3.3: Formato de los paquetes LCP

A continuación se va a describir cada uno de los campos del paquete LCP.

CÓDIGO: Ocupa un byte e identifica el tipo de paquetes LCP. Los posibles valores para este campo son los siguientes:

Código	Paquete LCP
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject
8	Protocol-Reject
9	Echo-Request
10	Echo-Reply
11	Discard-Request

Tabla 3.2: Valores del campo CÓDIGO

IDENTIFICADOR: Permite la asociación de las peticiones con las respuestas.

LONGITUD: Indica la longitud del paquete LCP, la cual nunca deberá ser mayor que el MRU establecido para el enlace.

Hay 3 clases de paquetes LCP:

- Establecimiento y configuración del enlace:
  - Configure-Request
    Paquete que se transmite cuando se desea abrir un enlace. En él viajan las **opciones de configuración** del mismo. Después de su recepción se debe de enviar una respuesta apropiada, utilizando un paquete *ACK, NACK* o *Reject*.
  - Configure-Ack
    Las opciones de configuración recibidas son aceptadas (el campo de identificador de trama debe de coincidir con el del Configure-Request aceptado). Una vez que los dos extremos han recibido el *ACK* del extremo remoto, el enlace entra en estado *OPEN*.
  - Configure-Nak
    Alguna de las opciones de configuración recibidas en la trama con el identificador empleado no son aceptadas, pero se envía el valor recomendado o aceptado por el extremo. Cuando se recibe un *NAK*, el receptor debe de generar un nuevo *CONFIGURE-REQUEST* que contenga los valores aceptados indicados.
  - Configure-Reject
    Alguna de las opciones de configuración recibidas en la trama con el identificador empleado no son aceptadas ni reconocidas. Cuando se recibe un *REJECT*, el receptor debe de generar un nuevo *CONFIGURE-REQUEST* que no contenga los valores rechazados.

- Finalización del enlace:
  - Terminate-Request
    Paquete que se transmite cuando se desea finalizar una sesión.
  - Terminate-Ack
    Paquete que se transmite después de la recepción de un *TERMINATE-REQUEST*. La recepción de un paquete *TERMINATE-ACK* no esperado indica que el enlace ha sido cerrado.

- Administración y depuración del enlace:
  - Code-Reject
    Indica que se ha recibido un paquete LCP incompleto o con un valor en el campo código no reconocido. Si se persiste en la transmisión del citado paquete, el enlace terminará cerrándose.
  - Protocol-Reject
    Indica que se ha recibido una trama PPP con un campo de protocolo no implementado. El extremo receptor de la trama deberá de cesar en el envío del citado protocolo.
  - Echo-Request y Echo-Reply
    Proporcionan un mecanismo de mantenimiento del enlace. Cada cierto tiempo se genera una consulta con código ECHO-REQUEST que debe de ser devuelta con un ECHO REPLY.
  - Discard-Request
    Proporcionan un mecanismo para el descarte, eliminación de tramas. Es empleado para pruebas.

3.3.2.2 Opciones de configuración de LCP

Las opciones de configuración van incluidas en el campo de DATOS de los siguientes paquetes LCP: *CONFIGURE-REQUEST, CONFIGURE-ACK, CONFIGURE-NAK, CONFIGURE-REJECT, TERMINATE-REQUEST* y *TERMINATE-ACK.*

Si no se incluye una opción de configuración en un paquete de tipo Configure-Request entonces se asumirá su valor por defecto.

El formato de una opción de configuración es el siguiente:

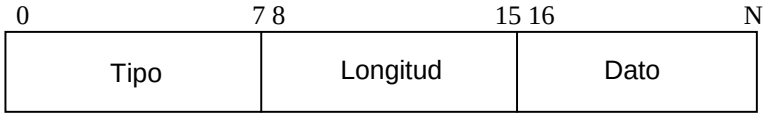

Figura3.4: Formato de una opción de configuración.

El campo TIPO es un byte indicando una opción de configuración concreta. Los posibles valores que puede tomar son los siguientes:

Tipo	Opción
0	Reservado
1	Maximum-Receive-Unit
2	Async-Control-Character-Map
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
6	Reservado
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression
9	FCS-Alternatives

Tabla 3.3: Opciones de configuración LCP

A continuación, se muestra una breve descripción de cada una de las opciones.

MAXIMUM-RECEIVE-UNIT (MRU). Con esta opción se indicará el tamaño máximo del paquete que se puede recibir. El valor por defecto es de 1500 bytes.

ASYNC-CONTROL-CHARACTER-MAP. Con esta opción se emplea para conseguir que la transmisión de los caracteres de control (como por ejemplo XON, XOFF) sea transparente, en caso de PPP asíncrono. Esto permite que cuando estos caracteres estén incluidos dentro de la trama no provoquen activación de los procesos de control de flujo en los módems o adaptadores empleados para la conexión.

AUTHENTICATION-PROTOCOL. Con esta opción se podrá negociar el protocolo que se usará para la autentificación de los terminales (por defecto no se realizará autentificación). En un mensaje de tipo *CONFIGURE-REQUEST* únicamente podrá haber una opción de configuración referente a la autentificación. En el caso de que el protocolo propuesto sea rechazado en un mensaje *CONFIGURE-NAK*, se podrá proponer otro protocolo diferente en otro mensaje *CONFIGURE-REQUEST*. Cuando se reciba un mensaje de tipo *CONFIGURE-ACK* para el protocolo de autentificación propuesto, significará que el otro extremo del enlace acepta autentificarse mediante el protocolo propuesto.

QUALITY-PROTOCOL. Por defecto no se establece ningún protocolo para monitorizar la calidad del enlace. Estos protocolos permiten saber cuándo se están perdiendo datos, así como con qué frecuencia se da esta situación. Cuando se envía esta opción en un paquete de tipo *CONFIGURE-REQUEST* se está solicitando al otro extremo que envíe información de monitorización de la calidad del enlace. Si el otro extremo acepta con un *CONFIGURE-ACK* entonces se podrá esperar la recepción de este tipo de información desde el otro extremo.

MAGIC-NUMBER. Es un número aleatorio que servirá para detectar bucles en el enlace así como otro tipo de anomalías. Por defecto tomará un valor de 0. Cuando se recibe un paquete de tipo *CONFIGURE-REQUEST* con una opción de configuración de Magic-Number, se debe comparar el número recibido con el número que se recibió en el último paquete de tipo *CONFIGURE-REQUEST*: si los números son diferentes entonces el enlace no tiene un bucle, y el paquete debe ser confirmado. Si los números son iguales entonces el enlace puede tener un bucle, ya que se interpreta que el paquete recibido en ese instante ya se recibió anteriormente. En este caso el paquete de configuración se debe rechazar enviando un paquete *CONFIGURE-NAK* con un Magic-Number diferente; el otro extremo deberá rechazar así mismo este paquete con otro *CONFIGURE-NAK* donde el Magic-Number haya cambiado.

PROTOCOL-FIELD-COMPRESSION (PFC). Esta opción permite negociar la compresión del campo PROTOCOLO en la trama PPP. Por defecto el campo PROTOCOLO tiene un tamaño de 2 bytes pero a través de esta opción de configuración se informa al otro extremo de que este campo podría tener un tamaño de un solo byte.

ADDRESS-AND-CONTROL-FIELD-COMPRESSION(ACFC). Igual que en el caso anterior, esta opción permite negociar la compresión de los campos de dirección y control.

3.3.3 Protocolos de autenticación

El PPP dispone de una serie de protocolos que permiten autenticar y verificar un enlace, el cual únicamente se establecerá en el caso de que se compruebe que los valores de login (usuario) y password (clave) esperados en un extremo son los adecuados. Este método es habitualmente empleado en enlaces en los que los routers se conectan a una red vía circuitos conmutados (RDSI o RTB), aunque también puede ser empleada en circuitos punto a punto.

Esta comprobación se realiza previamente al establecimiento de los protocolos de control de red (NCP). En caso de que la autenticación sea exigida y no se complete de forma correcta, se finalizará el establecimiento del enlace.

Existen dos métodos de autenticación definidos en la RFC-1334. Éstos son:

3.3.3.1 Password Authentication Protocol (PAP)

Proporciona un método simple para autenticar un enlace, usando un establecimiento de 2 vías:

1. Una vez que se alcanza el estado OPEN en la negociación de los LCP, el extremo que desea conectarse envía al autenticador un usuario (login) y una clave (password).
2. El extremo que la recibe comprueba si es válida y envía la respuesta adecuada, aceptando o denegando la llamada.

Los paquetes PAP se encapsulan dentro del *payload* de la trama PPP.

El formato de un paquete PAP es el siguiente:

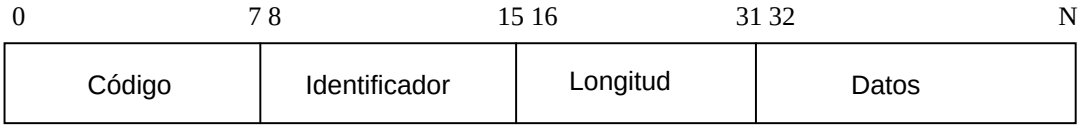

Figura 3.5: Formato de un paquete PAP

El formato es similar al de un paquete LCP. Sin embargo, el campo CÓDIGO sólo puede tener 3 valores:

Código	Paquete PAP
1	Authenticate-Request
2	Authenticate-Ack
3	Authenticate-Nak

Tabla 3.4: Valores del campo CÓDIGO en un paquete PAP

Como hemos visto en la tabla, los paquetes PAP los podemos agrupar en tres tipos:

AUTHENTICATE-REQUEST. Paquete que se transmite cuando se desea autenticar un enlace. En él viajan la clave y password empleados. Después de su recepción se debe de enviar una respuesta apropiada, utilizando un paquete de tipo *ACK* o *NACK*.

AUTHENTICATE-ACK. Los valores recibidos son aceptados. El campo de identificador de trama debe de coincidir con el del *AUTHENTICATE-REQUEST* aceptado. Una vez que se ha recibido el ACK del extremo autenticador se puede proceder con el establecimiento de los protocolos de red (NCP).

AUTHENTICATE-NAK. Los valores recibidos no son aceptados. El extremo que desea autenticar el enlace deberá de enviar un nuevo *AUTHENTICATE-REQUEST* con valores adecuados o finalizar el enlace.

3.3.3.2 Challenge-Handshake Authentication Protocol (CHAP)

El método de autenticación anterior no es muy seguro, debido a que tanto el login como la clave que se envían por la red viajan en “claro”. Este problema está resuelto por el otro método de autenticación: CHAP.

Proporciona un método mucho más seguro para autenticar un enlace. Se definen 3 fases claramente diferenciadas:

1. Una vez que se alcanza el estado OPEN en la negociación de los LCP, el extremo autenticador envía un reto (Challenge) al extremo que desea conectarse (también se puede transmitir en cualquier instante durante la comunicación para asegurar que la conexión no ha sido alterada). Este reto consiste en una cadena de bytes elegidos al azar, y que cambian en cada mensaje enviado.
2. El extremo que la recibe concatena el campo Identificador del paquete Challenge recibido, junto con su contraseña (Secreta) y con el reto recibido (Challenge), y aplica una función Hash a este flujo de bytes. Después enviará el resultado (Response) al extremo autenticador. El tamaño de la respuesta que se envía depende del algoritmo de Hash usado (16 bytes para MD5).
3. El extremo autenticador es capaz de calcular la respuesta que debe enviar el extremo que desea conectarse. Al recibir la respuesta, el autenticador verificará que lo recibido es lo esperado y permitirá (Success) o no (Failed) la continuación en el establecimiento de los protocolos de red.
4. A intervalos de tiempo aleatorios, el autenticador puede enviar nuevos retos al otro extremo. Después de enviar cada reto se repetirían los pasos del 1 al 3.

La seguridad de este método depende del secreto de la clave en ambos extremos, y el único problema es que ambos deben conocerla de antemano.

En este método, el password nunca viaja en "claro" por la red, y además, es imposible obtenerlo conociendo el Challenge y la respuesta enviada. Por otro lado, este método permite la autenticación del enlace incluso una vez que se hayan establecido los protocolos de red (por ejemplo IP), para verificar la seguridad del mismo.

Los paquetes CHAP se encapsulan dentro del campo INFORMACIÓN de la trama PPP. El campo PROTOCOLO tendrá el valor 0xC223 para indicar que el protocolo transportado es CHAP.

El formato de un paquete CHAP es el siguiente:

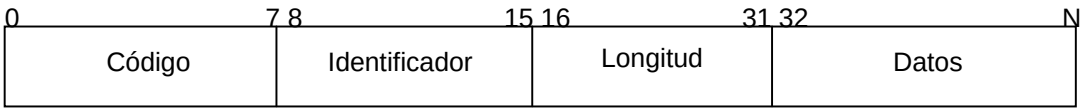

Figura 3.6: Formato de un paquete CHAP

El formato es similar al de un paquete LCP. Sin embargo, el campo CÓDIGO sólo puede tener 4 valores:

Código	Paquete CHAP
1	Challenge
2	Response
3	Success
4	Failed

Tabla 3.5: Valores del campo CÓDIGO en el paquete CHAP

El IDENTIFICADOR es un byte que cambia para cada mensaje Challenge enviado. En el mensaje de Response se debe copiar en el campo IDENTIFICADOR el identificador del Challenge recibido. De esta manera podemos saber a qué mensaje Challenge se refiere un determinado mensaje Response.

Como hemos visto en la tabla, los paquetes CHAP los podemos agrupar en cuatro tipos:

CHALLENGE. Paquete que transmite el extremo autenticador cuando se desea autenticar un enlace. En él viaja el reto con el que el otro extremo construirá la respuesta.

RESPONSE. Paquete que envía el extremo que desea conectarse, en el que viaja el resultado de la aplicar la función Hash a la cadena de bytes formada por la concatenación del campo Identificador, con el Challenge y el Password.

SUCCESS. El valor recibido es aceptado. Una vez que se ha recibido el SUCCESS del extremo autenticador se puede proceder con el establecimiento de los protocolos de red (NCP).

FAILED. El valor recibido no es aceptado. El extremo que desea autenticar el enlace deberá de enviar una nueva respuesta con valores adecuados o finalizar el enlace.

3.3.4 Protocolos de control de red (NCP)

Los protocolos de control de red o NCP ofrecen un medio de establecer y configurar los protocolos de nivel de red que se encapsularán en la trama PPP.

Este apartado se centrará en el NCP definido para el establecimiento y configuración de IP (IPCP), así como en el método usado para negociar la compresión de las cabeceras TCP/IP.

Como ya se ha explicado en apartados anteriores, para establecer una comunicación sobre un enlace punto a punto, cada extremo del enlace PPP debe enviar paquetes LCP que configuren y prueben el enlace de datos. Una vez establecido el enlace, se enviarán paquetes NCP para elegir y configurar aquellos protocolos de red con los cuales se quiere trabajar (en nuestro caso, IP). Superada esta fase ya se podrán enviar datagramas a través del enlace.

IPCP (Internet Protocol Control Protocol) es el protocolo NCP usado para configurar IP en enlaces PPP. El formato de un paquete IPCP es exactamente igual que el formato de los paquetes LCP:

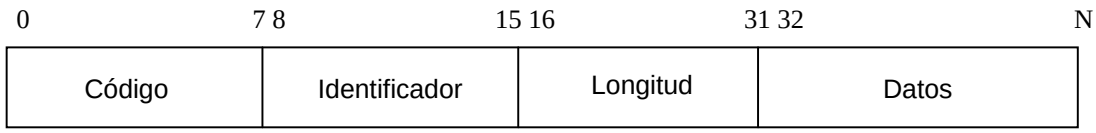

Figura 3.7: Formato de un paquete IPCP

El campo CÓDIGO aceptará únicamente valores entre 1 y 7:

Código	Paquete LCP
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject

Tabla 3.6: Valores del campo CÓDIGO en un paquete IPCP

El campo PROTOCOLO de la trama PPP debe tener el valor 0x8021 para indicar que se está transportando un paquete de tipo IPCP. Una vez que se ha negociado el uso del protocolo de red IP, mediante el correspondiente intercambio de paquetes IPCP, entre los dos extremos del enlace PPP, ya se puede pasar al intercambio de datagramas IP. Estos datagramas viajarán encapsulados dentro del campo INFORMACIÓN de la trama PPP (el campo PROTOCOLO de la trama PPP debe tener un valor de 0x0021 para indicar que lo que se está transportando es un datagrama IP). La longitud máxima del datagrama IP transmitido está limitada a la longitud máxima permitida para el campo INFORMACIÓN de la trama PPP. Si un datagrama IP tiene un tamaño mayor, debe ser fragmentado. Para evitar que se produzca fragmentación se puede limitar el tamaño máximo del segmento TCP, y con ello del datagrama IP, mediante la opción de configuración correspondiente de TCP.

3.3.4.1 Opciones de configuración IPCP

Las opciones de configuración de IPCP tienen el mismo formato que las opciones de configuración de LCP:

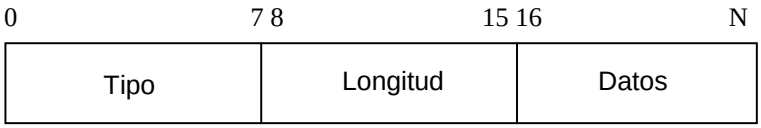

Figura 3.8: Formato de las opciones de configuración IPCP

Las dos opciones más importantes son las siguientes:

PROTOCOLO DE COMPRESIÓN IP. El campo TIPO debe tener un valor de 2. Esta opción de configuración permite la negociación de un protocolo de compresión específico. Por defecto no se usa ningún tipo de compresión.

DIRECCIÓN IP. El campo TIPO debe tener un valor de 3. Esta opción permite negociar la dirección IP que se le asignará al ext remo local del enlace PPP. El proceso comienza con el envío de un paquete *CONFIGURE-REQUEST* donde el emisor puede indicar la dirección IP que desea, o si no solicitar al otro extremo que le asigne una. Si la negociación de la dirección IP es necesaria, y n o se ha hecho referencia a esta opción de configuración en el paquete *CONFIGURE-REQUEST*, entonces esta opción se añadirá en el paquete *CONFIGURE-NAK* enviado por el otro extremo. Por defecto no se realiza negociación de las direcciones IP.

3.5 Desarrollo práctico

- Definir un interfaz PPP sobre línea serie que permita establecer un enlace síncrono con el otro extremo.
- Agregar un interfaz PPP sobre un interfaz de comandos AT, para poder conectarse a través de un módem con otro extremo. En este caso, el formato de los datos en la transmisión es asíncrono.
- Agregar un interfaz PPP sobre un acceso básico, para poder conectarse mediante RDSI con otro extremo. En este caso, el formato de los datos en la transmisión es síncrono.

3.5.1 Definir un interfaz PPP sobre línea serie en formato síncrono

3.5.1.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers NUCLEOX PLUS.
- 2 PC’s que funcionarán como clientes.
- 2 hubs.
- 2 latiguillos directos, para conectar cada PC al hub.
- 1 cable RS-232 DB25 punto a punto para conectar los 2 routers NUCLEOX PLUS, desde el puerto 1(DTE) de uno hasta el puerto 2 (DCE) del otro.

A continuación procedemos a montar la red según la siguiente topología:

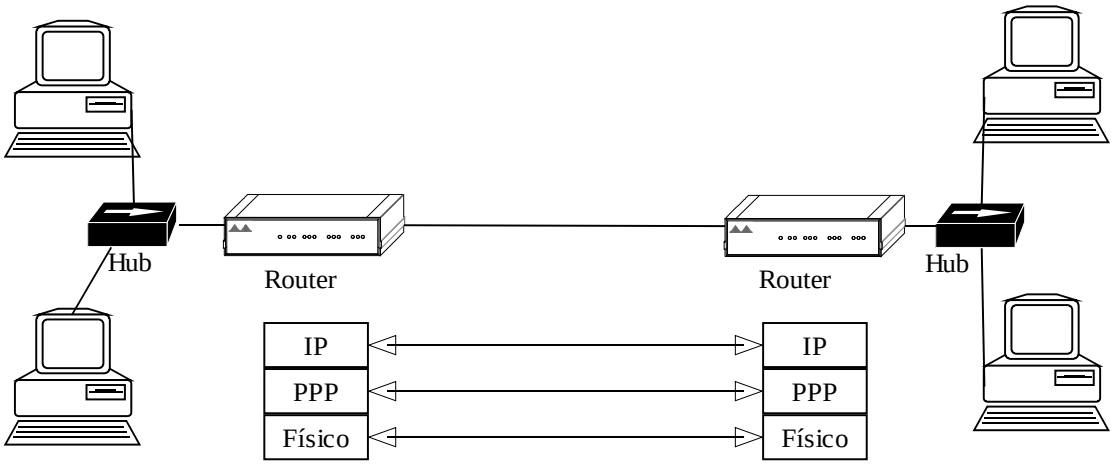

Figura 3.9: Topología de red

3.5.1.2 Configuración del interfaz LAN

Nuestro objetivo principal en este punto es asignarle una dirección IP a la interfaz LAN del router. Para ello en primer lugar debemos acceder al entorno de configuración del protocolo IP. El comando **PROTOCOL**, utilizado desde el **Proceso 4**, seguido de un número de protocolo o un nombre breve nos permite entrar en la configuración del protocolo deseado. Para saber el nombre o número de protocolo que tiene asignado IP, tecleamos **PROTOCOL ?**, y nos indica en una lista los distintos nombres de protocolos, con sus correspondientes números, que podemos teclear después de **PROTOCOL**:

```
Config>PROTOCOL ?
00  IP
03  ARP
06  DHCP
10  QLLC-FR
11  SNMP
12  OSPF
13  RIP
14  SDLC-QLLC
```

Cuando estamos en el entorno de configuración del protocolo IP, el prompt del sistema cambia y tiene la siguiente forma: *IP Config>*.

El comando **ADD ADDRESS** se debe utilizar para asignar direcciones IP a los interfaces hardware de la red. Los argumentos de este comando incluyen el identificador del interfaz (obtenido con el comando **LIST DEVICES**), la dirección IP, así como su máscara asociada.

```
IP config> ADD ADDRESS 0  128.185.123.22  255.255.255.0
IP config>
```

También se puede hacer introduciendo simplemente el comando **ADD ADDRESS**, y a continuación nos pregunta por los demás parámetros del comando.

Para retornar al menú del prompt *Config>* hay que teclear **EXIT.** Y para guardar esta dirección en memoria desde *Config>* teclear **SAVE**.

3.5.1.3 Configuración de la línea serie con PPP

Para configurar un interfaz serie como interfaz PPP SÍNCRONO, desde el menú de configuración teclear **SET DATA-LINK PPP.**

```
Config>SET DATA-LINK PPP
which port will be changed[1]? 1
Config>
```

A continuación indicaremos el puerto en el cual deseamos configurar el interfaz PPP, introduciendo el identificador de interfaz que queremos configurar (en este caso, el identificador 1). Seguidamente debemos guardar la configuración con el comando **SAVE,** y reiniciar con **RESTART.**

A continuación se debe asignar una dirección IP al interfaz PPP. Para ello debemos entrar en el menú de configuración del protocolo IP, y utilizar el comando **ADD ADDRESS** de la misma forma que en el apartado anterior, pero esta vez asignándosela al interfaz 1.

Para retornar al menú del prompt *Config>* hay que teclear **EXIT.** Y para guardar esta dirección en memoria desde *Config>* teclear **SAVE**.

Para comprobar que la asignación de direcciones IP se ha llevado a cabo correctamente podemos utilizar el comando **LIST ADDRESSES,** desde el menú de configuración de IP**,** que muestra las direcciones IP asignadas a cada interfaz.

3.5.1.4 Configuración de las tablas de encaminamiento

La dirección de destino se describe mediante la dirección de red IP y su máscara de red asociada.

Para crear, modificar y borrar rutas estáticas deben usarse los siguientes comandos (desde el menú de configuración del protocolo IP):

```
IP config> ADD ROUTE <red o subred o host, mascara, salto, coste>
```

```
IP config> CHANGE ROUTE <direccion-destino, mascara, salto, nueva-direccion-destino,
nueva-mascara, nuevo-salto, nuevo-coste>
```

```
IP config> DELETE ROUTE <direccion-IP-destino, mascara, siguiente salto>
```

Para comprobar que las rutas han sido agregadas, o borradas, correctamente podemos utiliza el comando **LIST ROUTES**, desde le menú de configuración de IP, que muestra las rutas estáticas configuradas.

Las rutas que debemos añadir, tomando como ejemplo la siguiente red, son:

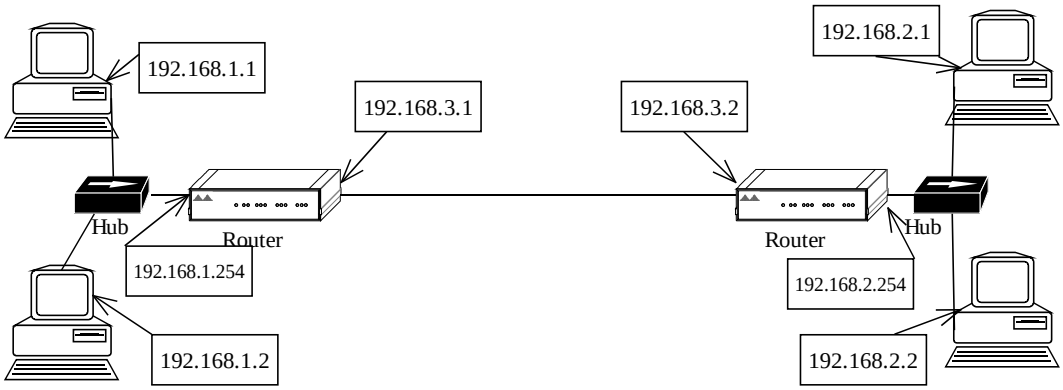

Figura 3.10: Topología con direcciones IP

para el router de la izquierda:

Destino	Netmask	Gateway
192.168.2.0	255.255.255.0	192.168.3.2
192.168.1.0	255.255.255.0	0.0.0.0
192.168.3.0	255.255.255.0	0.0.0.0

Tabla 3.7: Ejemplo de tabla de encaminamiento

3.5.1.5 Parámetros del protocolo PPP

En este apartado estudiaremos cómo configurar los 3 componentes más importantes de PPP: el LCP (Link Control Protocol), los NCPs (Network Control Protocols) y los protocolos de Autenticación. Estos 3 componentes quedan configurados por defecto de la siguiente forma:

- **LCP**
  Para ver la configuración del LCP debemos ejecutar el comando **LIST LCP**, y observamos lo siguiente:

```
PPP Config>LIST LCP

LCP Parameters
--------------
Tries Configure-Request           : 10
Tries Configure-Nak               : 10
Tries Terminate-Request           : 10
Timer between tries (sec)         : 3

LCP Options
-----------
Interface MRU (bytes)             : 1500
Magic Number                      : YES
Asynchronous Control Character Map : NO
Protocol Field Compression        : NO
Address Control Field Compression  : NO
PPP Config>
```

Parámetros LCP (LCP Parameters):

"Tries Configure-Request": indica las veces que se transmitirá un LCP CONFIGURE-REQUEST para establecer el enlace PPP.

"Tries Configure-Nak": indica el número máximo de rechazos de trama CONFIGURE-REQUEST durante el establecimiento del enlace que se transmitirán antes de finalizarlo por no encontrar configuración compatible entre ambos extremos.

"Tries Terminate-Request": indica el número de veces que se transmitirá la trama TERMINATE-REQUEST sin detectar respuesta de TERMINATE-ACK para finalizar un enlace de forma ordenada.

"Timer between tries": tiempo entre transmisiones consecutivas de LCPs CONFIGURE-REQUEST, TERMINATE-REQUEST y ECHO-REPLY cuando no se recibe la contestación de forma adecuada.

En caso de que deseemos modificar alguno de estos parámetros podemos utilizar el comando **SET LCP PARAMETERS**, y a continuación podremos modificarlos con el valor que deseemos.

```
PPP Config>SET LCP PARAMETERS
Tries Configure-Request            : [10]? 10
Tries Configure-Nak                : [10]? 10
Tries Terminate-Request            : [10]? 10
Timer between tries (sec)          : [3]? 3
PPP Config>
```

Opciones de configuración LCP (LCP Options):

Las opciones configurables son:

- *Interface MRU.*
- *Asynchronous Control Character Map.*
- *Magic Number.*
- *Protocol Field Compression.*
- *Address Control Field Compression.*

Todas estas opciones ya han sido explicadas en el apartado 3.3.2.2.

En el caso de que deseemos modificar alguna de estas opciones podemos utilizar el comando **SET LCP OPTIONS**, y a continuación podremos darles a las opciones los valores que deseemos.

```
PPP Config>SET LCP OPTIONS
Interface MRU (bytes)              : [1500]? 1500
Magic Number                       : (Yes/No)(Y)? Y
Asynchronous Control Character Map : (Yes/No)(N)? N
Protocol Field Compression         : (Yes/No)(N)? N
Address Control Field Compression  : (Yes/No)(N)? N
PPP Config>
```

- **NCP (IPCP)**

Para ver como queda configura el protocolo NCP debemos ejecutar el comando **LIST NCP** y observamos lo siguiente:

```
PPP Config>LIST NCP

NCP Parameters
--------------
Tries Configure-Request            : 10
Tries Configure-Nak                : 10
Tries Terminate-Request            : 10
Timer between tries (sec)          : 3
PPP Config>
```

Parámetros NCP:

"Tries Configure-Request": indica las veces que se transmitirá un NCP CONFIGURE-REQUEST para establecer el protocolo de red.

"Tries Configure-Nak": indica el número máximo de rechazos de trama CONFIGURE-REQUEST durante el establecimiento del protocolo de red que se transmitirán antes de finalizarlo por no encontrar configuración compatible entre ambos extremos.

"Tries Terminate-Request": indica el número de veces que se transmitirá la trama TERMINATEREQUEST sin detectar respuesta de TERMINATE-ACK para finalizar un protocolo de red de forma ordenada.

"Timer between tries": tiempo entre transmisiones consecutivas de NCP´s CONFIGURE-REQUEST y TERMINATE-REQUEST cuando no se recibe la contestación de forma adecuada

En caso de que deseemos modificar los valores de los parámetros NCP podemos utilizar el comando **SET NCP,** y a continuación introducir los valores que deseemos.

```
PPP Config>SET NCP
Tries Configure-Request          : [10]? 10
Tries Configure-Nak              : [10]? 10
Tries Terminate-Request          : [10]? 10
Timer between tries (sec)        : [3]? 3
PPP Config>
```

Para ver cómo quedan configuradas las opciones de configuración de IPCP ejecutamos el comando **LIST IPCP**, y observamos:

```
PPP Config>LIST IPCP

IPCP Options
------------
IP Van Jacobson Compression      :  NO
CRTP Compression                 :  NO
IP get local address             :  NO
IP mask local address            : 255.255.255.255
IP send address                  : YES
IP request remote address        : YES
IP remote address                : 0.0.0.0
PPP Config>
```

Opciones IPCP:

"IP Van Jacobson Compression": indica si se emplea compresión de Van Jacobson, como opción de protocolo de compresión IP.

"*CRTP Compression*": indica si se emplea o no la compresión CRTP (RFC-2508). Sólo es posible configurar una de las dos compresiones, como protocolo de compresión IP.

"IP get local address": indica si se solicita asignación de número IP al establecer el enlace, como es necesario en el caso de conexiones a un ISP. El valor por defecto es no.

"IP mask local address": en caso de solicitar asignación de número IP, indica la máscara a asociar. El valor por defecto es 255.255.255.255. Si se configura al valor 0.0.0.0, la máscara que se toma es la de la clase de la dirección.

"IP send address": en caso de que no exista petición de número IP, indica si se transmite o no el número IP configurado para el interfaz. El valor por defecto es sí.

"IP request remote address": indica si se requiere o no la transmisión del número IP del extremo remoto. El valor por defecto es sí.

"*IP remote address"*: en caso de que el extremo remoto solicite asignación de número IP, determina el número IP a transmitir.

En caso de que deseemos modificar algún valor de las opciones de IPCP, podemos introducir el comando **SET IPCP**, y a continuación introducir los valores que deseemos.

```
PPP Config>SET IPCP
IP Van Jacobson Compression        : (Yes/No)(N)? N
CRTP Compression                   : (Yes/No)(N)? N
IP get local address               : (Yes/No)(N)? Y
IP mask local address              : [255.255.255.255]? 255.255.255.255
IP send address                    : (Yes/No)(Y)? Y
IP request remote address          : (Yes/No)(Y)? Y
IP remote address                  : [0.0.0.0]? 0.0.0.0
PPP Config>
```

- **AUTENTICACIÓN**

  El comando **LIST AUTHENTICATION** permite visualizar las opciones programadas para realizar la autenticación del enlace. La autenticación implementada se realiza mediante el protocolo Password Authentication Protocol (PAP) o el protocolo Challenge-Handshake Authentication Protocol, descritos en la RFC-1334. Estos protocolos permiten establecer un enlace únicamente cuando se proporciona un login y un password correctos. Una vez finalizada la autenticación, se pasará a negociar los protocolos de red del enlace.

  El comando **SET AUTHENTICATION** permite programar el login y el password que serán enviados durante el proceso de autenticación en conexiones a Internet. Por defecto, tanto el usuario como la clave no están configurados. Si el extremo remoto solicita autenticación, serán estos valores los que se envíen para autentificar el enlace según el protocolo seleccionado: si es PAP serán enviados en claro, y si es CHAP será enviado el resumen MD5 del flujo de bytes resultado de la concatenación. Es importante destacar que la autenticación aquí configurada es la autenticación con la que el equipo se identifica ante el extremo remoto, en el caso en que el extremo remoto pida dicha autenticación.

  Para establecer que el router solicite autenticación al extremo que desea conectarse a él debemos utilizar los comandos **ENABLE AUTHENTICATION** (PAP o CHAP) y **ADD USERS**. Con este último comando configuramos los usuarios que van a poder establecer comunicación con nuestro router.

  El comando **ENABLE AUTHENTICATION** (PAP o CHAP) permite activar la facilidad de autenticación según el protocolo seleccionado: Password Authentication Protocol (PAP) o Challenge Authentication Protocol (CHAP). En caso de que la facilidad de autenticación se encuentre habilitada, se exigirá al extremo remoto que envíe el login y el password de acuerdo al método que se haya seleccionado. Solamente se podrá establecer el enlace en el caso de que el proceso se haya completado con éxito. En ambos casos, el usuario, con su correspondiente clave, debe haber sido añadido en la tabla de usuarios permitidos con el comando **ADD USERS.**

3.5.1.6 Comprobación de conexión en el enlace PPP

Los comandos de monitorización IP se deben introducir desde el prompt *IP*>. Para acceder a este prompt se debe entrar al **Proceso 3**, y una vez dentro de este proceso, que se identifica con el prompt "+", hay que teclear **PROTOCOL IP**:

```
*P 3
Console Operator
+PROTOCOL IP
IP>
```

2 de los comandos de monitorización más importantes son:

- *PING* address: Envía un mensaje ICMP a cualquier otro host cada segundo y espera una respuesta. Este comando se utiliza para aislar problemas en un entorno de múltiples redes. El comando *PING* finaliza cuando se pulsa cualquier tecla, o ya se han tratado todos los paquetes a enviar con sus correspondientes respuestas. En este momento se muestra un resumen de los paquetes transmitidos, recibidos, perdidos, y cuya respuesta ha superado time out, así como los retardos mínimos, medios y máximos.

- *TRACEROUTE* address: Enseña el camino completo, salto a salto, a una dirección destino concreta.

3.5.2 Agregar un interfaz PPP en un interfaz de comandos AT

3.5.2.1 El interfaz de comandos AT

Este interfaz va a ser empleado en el manejo del módem. El módem (Modulador-DEModulador) o ETCD (Equipo Terminal de Circuito de Datos) tiene por función adaptar los flujos de información digitales (esto es, los bits generados en cada equipo terminal de datos) a las características del medio de transmisión, y viceversa. Esto se consigue generalmente mediante el uso de alguna modulación específica que convierte los pulsos digitales producidos por un DTE en señales analógicas moduladas, ya sea en fase (PSK), frecuencia (FSK) o amplitud y fase (QAM), aptas para ser transmitidas a grandes distancias sobre líneas con anchos de banda vocales. En recepción, convierte las señales analógicas provenientes de las líneas de transmisión en señales digitales adecuadas para ser manejadas por los DTE´s.

Los módems se pueden clasificar atendiendo al modo de transmisión, técnicas de transmisión, tipo de línea, modulación, facilidades de corrección de errores, protocolos de compresión, etc. El CCITT ha normalizado un conjunto de recomendaciones para módems denominadas serie V, que definen los procedimientos para transmitir datos sobre líneas telefónicas conmutadas o punto-a-punto.

El módem se puede configurar desde el ETD, con los comandos AT (o Hayes), los comandos V.25-bis. Los comandos AT y V.25-bis tienen por misión establecer, mantener y finalizar la comunicación. Todos los comandos AT tienen una longitud de tres o cuatro caracteres seguidos opcionalmente por una cifra.

Los comandos se pueden clasificar, atendiendo a la función que realizan, en los siguientes tipos:

- Comandos de marcación
- Comandos de colgado y descolgado.
- Comandos que gobiernan el interfaz RS-232
- Comandos que manejan la configuración
- Comandos que gobiernan el circuito analógico
- Comandos que gobiernan el control de flujo
- Comandos que manejan los protocolos de control de errores MNP y V.42-bis
- Comandos que manejan el protocolo de compresión V.42-bis
- Comandos que monitorizan la fiabilidad del enlace.

A continuación explicaremos el funcionamiento de los comandos más importantes:

- Comandos de marcación.
La marcación puede ser por pulsos o por tonos, y con pausas entre dígitos, en caso que sea necesario. Los comandos más representativos involucrados en esta fase son:
ATDP: Marcación por pulsos. Ejemplo: ATDP 12459
ATDT: Marcación por tonos. Ejemplo: ATDT 12459

- Comandos que gobiernan el interfaz RS-232
AT&Cn: Control de la señal CD hacia el terminal. n=0 ON, n=1 normal, n=2 OFF

AT&Dn: Control de la señal DTR hacia el módem. n=0 DTR ignorada, n=1 con la transición on/off el módem pasa a modo comando sin colgar, n=2 una transición on/off hace colgar al módem, n=3 con una transición on/off el módem ejecuta un reset ATZ.

AT&Sn: Control de la señal DSR hacia el terminal. n=0 siempre activa, n=1 según V-24.

AT&Kn: Control de flujo entre DTE y módem. n=0 sin control de flujo, n=3 control de flujo por RTS/CTS, n=4 control de flujo mediante XON/XOFF, n=5 caracteres XON/XOFF transparentes para el control de flujo, n=6 control de flujo software y hardware.

- Comandos que manejan los mensajes y respuestas.
ATWn: Define el formato de los mensajes de conexión. n=0 solo devuelve la velocidad entre DTE y módem, n=1 devuelve la velocidad de línea, protocolo y velocidad entre DTE y módem, n=2 solo velociad de línea.

- Comandos de colgado y descolgado.
ATD: Pasa de modo comando a línea.
ATH: Desconectar el módem de la línea.

- Comandos que manejan la configuración.
AT&Fn: Reinicializa la memoria cargando los parámetros de fábrica por defecto.
AT&Wn: Almacena los parámetros en la RAM no volátil.

3.5.2.2 Configuración de los equipos

Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers NUCLEOX PLUS.
- 2 PC’s que funcionarán como clientes.
- 2 latiguillos directos, para conectar el router al hub.
- 2 hubs.
- 2 módems.
- 2 cables telefónicos (interfaz RJ-11).
- 2 cables serie para conectar el NUCLEOX PLUS al módem.

A continuación procedemos a montar la red según la siguiente topología:

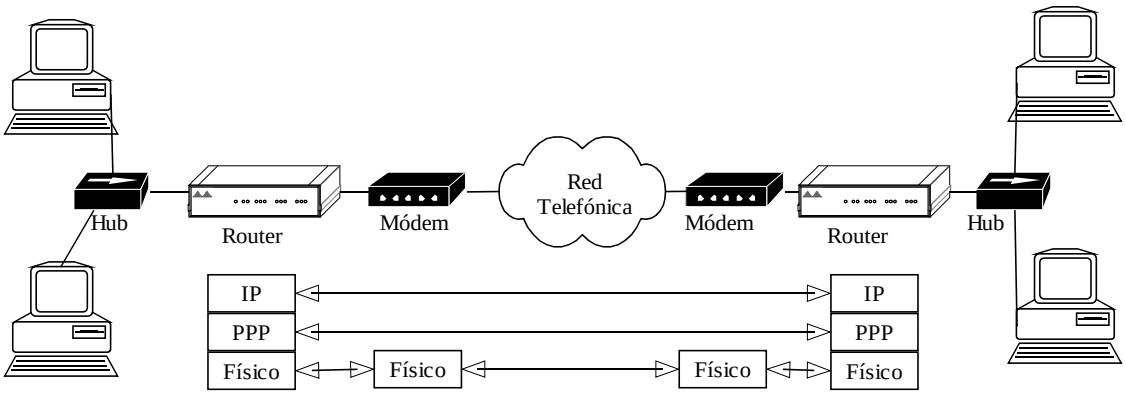

Figura 3.11: Topología de red

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

Configuración del NUCLEOX PLUS

Un interfaz de comandos AT permite manejar un módem externo para realizar la conexión. Sobre este interfaz podemos añadir un interfaz PPP asíncrono, sobre el cual se van a transmitir los comandos AT y posteriormente la información. Para ello desde el proceso 4 (**PROCESS 4**), ejecutamos **ADD DEVICE ATPPP-DIAL**. Para ver las interfaces que hemos añadido podemos ejecutar el comando **LIST DEVICES**.

```
Config>ADD DEVICE ATPPP-DIAL
which port will be changed[0]? 1
Added ATPPP-DIAL interface with num: 3
Config>
```

Cuando se ejecuta el comando **ADD DEVICE ATPPP-DIAL,** se nos pregunta qué puerto deseamos cambiar. Debemos decir que el puerto 1, ya que este puerto funciona como DTE.

Podemos observar que hemos añadido 2 interfaces. Un interfaz con el nombre AT COM, que es el interfaz de comandos AT, y otro con el nombre PPP AT COM, que es un interfaz PPP asíncrono sobre el interfaz de comandos AT. El interfaz AT COM, es un interfaz lógico, es decir, no tiene una correspondencia con un interfaz fisco, mientras que el interfaz PPP AT COM está asociado con el puerto serie número 1 del NUCLEOX PLUS.

A continuación debemos asignar las direcciones IP al router y configurar su tabla de encaminamiento. Para asignar las direcciones IP utilizamos el comando **ADD ADDRESS** desde el menú de configuración del protocolo IP, al que se accede tecleando **PROTOCOL IP** desde el Proceso 4 (Config>). Hay que añadirle una dirección tanto al interfaz LAN (Ethernet) como al interfaz serie (PPP AT COM).

```
IP config> ADD ADDRESS <nºinterfaz, direccion-IP, mascara-IP>
```

Seguidamente debemos añadir las rutas necesarias a la tabla de encaminamiento del router con el comando **ADD ROUTE**.

```
IP config> ADD ROUTE <red o subred o host, mascara, salto, coste>
```

Las rutas que debemos añadir, tomando como ejemplo la siguiente red, son:

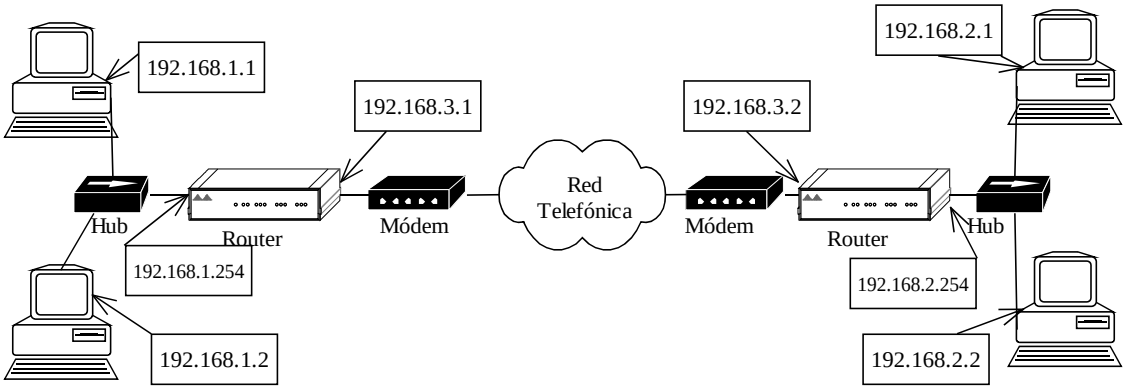

Figura 3.12: Topología con direcciones IP

para el router de la izquierda:

Destino	Netmask	Gateway
192.168.2.0	255.255.255.0	192.168.3.2
192.168.1.0	255.255.255.0	0.0.0.0
192.168.3.0	255.255.255.0	0.0.0.0

Tabla 3.8: Ejemplo de tabla de encaminamiento

Configuración del interfaz PPP

Para entrar en el menú de configuración del interfaz PPP AT COM debemos teclear **NETWORK (Número de interfaz asignado)**, este menú de configuración se identifica por el prompt *Circuit Config*>.

```
Config>NETWORK 2
Circuit Config
Circuit Config>
```

Si ejecutamos el comando **LIST** observamos la siguiente información:

```
Circuit Config>LIST
Base interface: 1
Destination address:
Inactive time: 60
Circuit Config>
```

Base interface: Nº de interfaz sobre el que se estable el interfaz de comandos AT.
Destination address: Número de destino, a través del cual se conecta al otro router.
Inactive time: La llamada se efectuará cuando haya tráfico IP, y si durante 60 segundos no hay tráfico de ningún tipo se colgará la llamada. Si estableciésemos *Inactive time: 0*, la llamada siempre estaría establecida.

Debemos de configurar la dirección de destino. Para ello ejecutamos el comando **SET DESTINATION-ADDRESS**, y a continuación introducimos el número de teléfono deseado. Una vez configurada esta dirección, debemos pasar a configurar parámetros propios del protocolo PPP, concretamente la velocidad de transmisión.

Para entrar al menú de configuración del protocolo PPP desde el prompt *Circuit Config*>, debemos introducir el comando **ENCAPSULATOR**. A continuación el prompt cambiará por el de *PPP Config*>. Aquí tecleamos **SET LINE LINE-SPEED**, este comando nos permite

configurar la velocidad a la que se enviarán los comandos de marcación y configuración al módem.

```
Circuit Config>ENCAPSULATOR
ASYNCHRONOUS PPP

-- Interface PPP. Configuration --
PPP Config>
```

Configuración del interfaz de comandos AT

Para entrar en el menú de configuración del interfaz AT COM debemos teclear **NETWORK (Número de interfaz asignado)**, este menú de configuración se identifica por el prompt *AT Config>*.

Este interfaz va a ser empleado en el manejo del módem. Los parámetros configurables para el módem externo y el valor que toman por defecto son los siguientes:

- Modo de conexión por comandos.
- Modo de marcación por tonos; manda ATDT <nº de Destination Address>.
- Comando de control de portadora (DCD): AT&C1.
- Comando de control de DSR: AT&S1, según la norma V-24.
- Comando de control de DTR: AT&D2, una transición on/off hace colgar al módem.
- Comando de control de CTS: AT&R1.
- Comando de activación de norma V-42/V.42bis: AT&Q5.
- Comando de selección de control de flujo: AT&K3, control de flujo por RTS/CTS.

En el caso de que queramos modificar alguno de los valores anteriores debemos utilizar el comando **SET**, y a continuación podremos seleccionar el valor que deseamos para cada comando.

```
AT Config>SET ?
CONNECTION
DIAL
DCD-CONTROL
DSR-CONTROL
DTR-CONTROL
CTS-CONTROL
V42-CONTROL
FLOW-CONTROL
```

Además debemos habilitar la RESPUESTA AUTOMÁTICA (AUTOMATIC ANSWER: AA), que permite que el interfaz ATDIAL acepte llamadas entrantes. Para ello ejecutamos el comando **ENABLE AUTO-ANSWER**.

Con esta configuración cada vez que se necesite reiniciar el enlace se enviarán automáticamente los comandos AT adecuados.

Asignación de direcciones IP a los PC Linux

Se ha utilizado Linux porque es lo que estaba instalado en el laboratorio. En Windows98 este proceso de configuración es tan fácil como acceder a un panel de control. Para asignar direcciones IP a los distintos PC's Linux, que funcionan como clientes, debemos entrar como root, y utilizar el comando **ifconfig** con el siguiente formato:

ifconfig (interfaz) (dirección-IP) **netmask** (máscara-de-red) **up**

de esta forma le asignamos a la <interfaz> la <dirección-IP> con la <máscara-de-red>; además con el comando parámetro **up** activamos la interfaz. De forma automática aparece una entrada en la tabla de encaminamiento del PC con destino a la red a la que se encuentra conectado directamente, es decir, a aquella ruta sin gateway.

Ejemplo:

ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up

Configuración de las tablas de encaminamiento de los PC Linux

Debemos crear las entradas de la tabla de encaminamiento, con destino a las diferentes redes de la topología, por el camino más corto.

Para introducir las tablas de encaminamiento en los PC's en Linux debemos utilizar el comando **route**, con el siguiente formato:

route add –net (IP-Red-Destino) **gw** (Gateway) **netmask** (Máscara-Red) (Interfaz)

Ejemplo:

route add –net 192.168.2.0 gw 192.168.3.2 netmask 255.255.255.0 eth0

Para comprobar que la configuración ha sido la correcta podemos visualizar las tablas de encaminamiento con el comando **route –n**.

Comprobación

Por último podemos comprobar mediante un ping si tenemos correctamente configurado el interfaz. Se deberá establecer la llamada RTB y obtener respuesta a los pings enviados.

3.5.3 Agregar un interfaz PPP sobre un acceso básico RDSI

3.5.3.1 Introducción

En los últimos años, la Red Digital de Servicios Integrados (RDSI) ha experimentado un increíble incremento en los servicios de telefonía básicos. Esta tecnología ha reemplazado a las conexiones telefónicas analógicas por conexiones digitales de alta velocidad, flexibles y fiables. Estas conexiones digitales hacen que la red telefónica sea mucho más fiable para transmitir datos, incluyendo el tráfico TCP/IP. PPP también posibilita a TCP/IP intercambiar mensajes a través de un enlace RDSI. Esta tecnología se denomina *RDSI de banda estrecha (RDSI-BE)*, para distinguirla de la *RDSI de banda ancha* que utiliza ATM.

Con RDSI de banda estrecha son posibles dos tipos de interfaces, llamados Basic Rate Interface (BRI) y Primary Rate Interface (PRI). La interfaz BRI (también llamada acceso básico 2B+D), es un acceso pensado para instalaciones de abonado pequeñas, con un máximo de 8 terminales. La interfaz PRI (también llamada acceso primario 30B+D), soporta los grandes volúmenes de tráfico de las grandes organizaciones. El acceso básico contiene 2 canales B a 64 Kbps y un canal D a 16 Kbps, mientras que el acceso primario contiene 30 canales B y un canal D, todos a 64 Kbps.

En la mayoría de los lugares, sólo los canales B transportan tráfico TCP/IP. En consecuencia, un ACCESO BÁSICO podrá transportar como máximo 128 Kbps de datos, mientras que un ACCESO PRIMARIO soporta 1,92 Mbps.

Aunque el canal D teóricamente puede transportar también datos, en España, éste se limita al control y la gestión de los canales B. A través del canal D los dispositivos RDSI transportan la información generada por el protocolo de señalización.

3.5.3.2 Configuración del interfaz usuario-red

Para facilitar el estudio del acceso de usuario, es preciso introducir una nomenclatura que permita redactar una normativa que designe con precisión y sin ambigüedades cualquier aspecto relacionado con la red, añadiendo como ventajas adicionales la posibilidad de un desarrollo técnico de los distintos bloques de un modo independiente y el poder escoger entre distintos fabricantes. Así, en el aspecto de usuario se definen Puntos de Referencia y Agrupaciones Funcionales.

Las Agrupaciones Funcionales representan entidades que realizan funciones de manera agrupada. Se pueden corresponder con un equipo físico en su totalidad, o con parte de él. Los Puntos de Referencia identifican las interfaces entre agrupaciones funcionales distintas y se pueden corresponder con interfaces reales, o con interfaces virtuales (internas en un equipo).

Puntos de Referencia:

- **Punto de Referencia S**: Punto de conexión física de los terminales RDSI.
- **Punto de Referencia T**: Representa la separación entre las instalaciones de usuario y equipos de transmisión en línea. Separación entre las funciones de transmisión y las funciones de conmutación local.
- **Punto de Referencia U**: Representa la línea de transmisión digital entre la instalación del cliente y la central telefónica y se corresponde físicamente con el bucle de abonado a dos hilos existente actualmente.

Grupos Funcionales:

- **Terminación de Red 1 (TR1)**: Realiza funciones de nivel físico e interconexiona la instalación interior del cliente a 4 hilos con la red exterior a 2 hilos. Físicamente localizado en el domicilio del cliente. Está bajo el control del operador de la red realizando funciones tales como verificación del bucle de abonado y monitorización de errores. Se conecta al punto de referencia U de cara a la red y proporciona el punto T; de no existir, TR2 proporcionaría el punto S/T.
- **Terminación de Red 2 (TR2)**: Realiza funciones de conmutación, concentración y control en el interior de las instalaciones del cliente. Un ejemplo de TR2 puede ser una centralita o una red de área local cuyos enlaces son del tipo RDSI y que se conectan por un lado a la TR1 y por el otro a los integrantes de dichas Centralitas o Redes. Se conecta al punto T y proporciona el punto S.
- **Equipo Terminal 1 (ET1)**: Terminales que admiten una conexión directa a la RDSI (teléfono digital, fax, equipo de videoconferencia, etc.)
- **Equipo Terminal 2 (ET2)**: Terminales que no admiten conexión directa a la RDSI (teléfono analógico convencional, ordenadores con interfaz RS-232,etc.) y precisan un adaptador de terminal.
- **Adaptador de Terminal (AT)**: Permite la conexión de los ET2 a la RDSI mediante adaptación de los niveles físico y de enlace, además de adaptar la velocidad binaria a 64 Kbps y multiplexar señales de menor velocidad.

La ITU-T ha propuesto varias configuraciones posibles para la interfaz del usuario-red. Las dos configuraciónes más sencillas y habituales son:

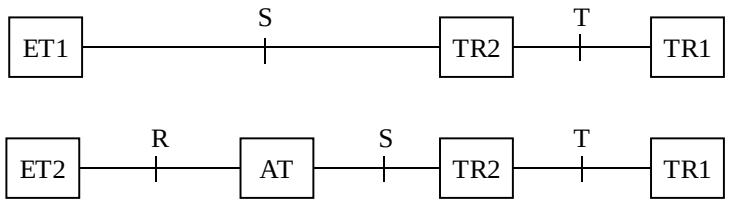

Figura 3.13: Configuración de referencia

Las características eléctricas de la interfaz usuario-red se determinan conforme a ciertos supuestos, sobre las diferentes configuraciones del cableado que pueden existir en las instalaciones de usuario. Se toman como referencia las dos configuraciones base siguientes:

Configuración punto a punto: Supone la existencia de una sola fuente (emisor) y un solo sumidero (receptor) que son interconectados por un circuito de enlace. Esta configuración de la capa 1 cumple la recomendación ITU-T I.430. En la figura siguiente se representa esta configuración tipo.

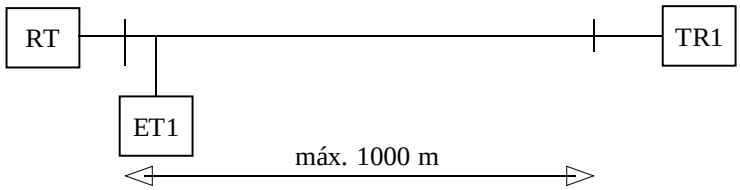

Figura 3.14: Configuración punto a punto

Donde RT es una resistencia de terminación de 100 Ω.

Configuración punto a multipunto: Supone la existencia de varias fuentes (emisores) conectadas a un único sumidero (receptor) por un circuito de enlace, e igualmente varios sumideros conectados a una sola fuente. En esta configuración no se contemplan elementos lógicos activos que realicen funciones. Esta configuración de la capa 1 cumple la recomendación ITU-T I.430. A esta configuración también llamada “bus pasivo”, se recurre cuando se desea conectar mas de un equipo terminal. Puede presentarse de dos formas: bus pasivo corto y bus pasivo extendido.

En la configuración **bus pasivo corto** los puntos de conexión de los terminales pueden situarse en cualquier parte a lo largo del bus y el máximo número de terminales a conectar es de **ocho** con una longitud de cable de conexión máxima de 10 m. La máxima longitud del bus es de 100 m en el caso de que el cable sea de baja impedancia (75 Ω) y de 200 m cuando el cable es de alta impedancia (150 Ω).

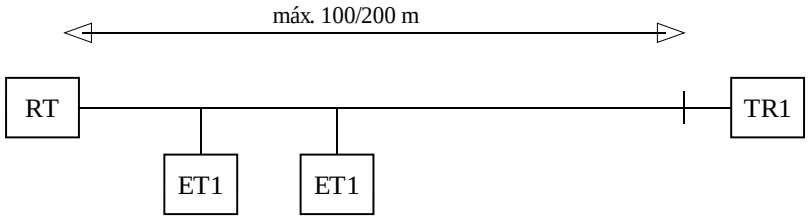

Figura 3.15: Configuración bus pasivo corto

En la configuración **bus pasivo extendido** los puntos de conexión de los terminales han de situarse agrupados en el extremo del bus mas alejado de la terminación de red TR y el número máximo de terminales a conectar es **cuatro** con una longitud de conexión máxima de 10 m. La longitud del bus es del orden de 100 m a 1000 m. En una configuración con 500 m de cable la distancia **d** entre los puntos de conexión de los terminales está comprendida entre 25 y 50 m.

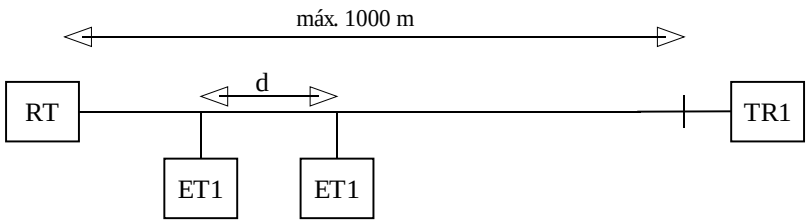

Figura 3.16: Configuración bus pasivo extendido

3.5.3.3 Trama de nivel físico

La transmisión del acceso básico (BRI) se estructura en tramas de longitud fija, que se repiten periódicamente. Cada trama tiene una longitud de 48 bits; a 192 Kbps, las tramas se deben repetir a una tasa de una trama cada 250 μs. La figura 3.36 muestra la estructura de la trama; la trama superior se transmite desde el equipo terminal del abonado hacia la red; la trama inferior se transmite desde la red hacia el equipo terminal del abonado. La transmisión se encuentra sincronizada, de forma que la transmisión desde el equipo terminal hacia la red se produce dos periodos de bit después que la transmisión en sentido contrario.

Cada trama de 48 bits incluye 16 bits de cada uno de los dos canales B y 4 bits del canal D. El significado del resto de los bits es:

- F: Bit comienzo de trama.
- L: Bit compensación de DC.
- B1: Ocho bits de información del canal B1.
- Fa: Siempre 0 lógico, excepto para estructura multitrama.
- D: Bits información canal D.
- E: Bit echo canal D. Retransmisión del último bit del canal D recibido por la terminación de red.
- N: Igual a Fa negado. Reservado uso futuro.
- B2: Ocho bits de información del canal B2.
- A: Bit de activación. Pone terminales en modo de bajo consumo.
- M: Estructura multitrama.
- S: Reservado uso futuro.

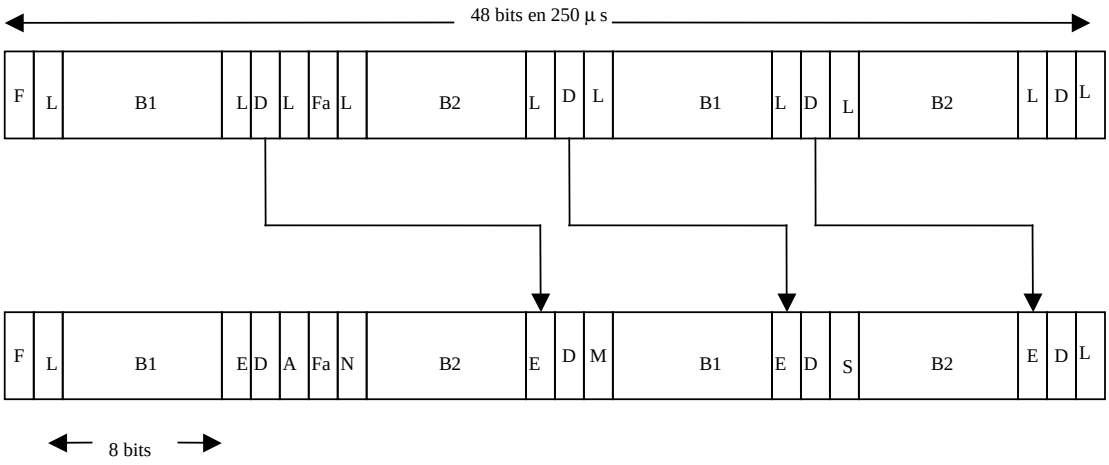

Figura 3.17: Formato de la trama física en RDSI.

3.5.3.4 Servicios RDSI

La ITU-T ha definido un total de 10 servicios básicos en modo circuito y 3 servicios básicos en modo paquete.

Los servicios básicos en modo circuito se caracterizan por la provisión de la transferencia de información de usuario sobre el canal B y de señalización sobre el canal D. Se distinguen los siguientes:

- **Servicio portador a 64 Kbps estructurado a 8 KHz sin restricciones:** El termino sin restricciones significa que la información se transfiere sin alteración y que no hay ninguna restricción en el patrón de bits a transmitir. El usuario puede utilizar este servicio para cualquier aplicación que necesite una tasa de datos de 64 Kbps.

  El termino estructurado quiere decir que, además de la transmisión de bits, se produce la transmisión de una estructura de sincronización entre los clientes. Cuando un usuario transmite información a otro usuario, la transmisión va acompañada por información de sincronización a 8 Khz, que delimita la información en unidades de 8 bits. Esta integridad estructural de 8 KHz implica que los octetos se reconocerán dentro del correspondiente espacio de tiempo.

- **Servicio portador a 64 Kbps estructurado a 8 KHz para conversación:** Este servicio define una modulación específica para crear la señal digital, llamada PCM (Pulse-Code Modulation). A causa de que la red asume que la información que se transmite es voz codificada, pude utilizar técnicas de procesamiento adecuadas (como cancelación de eco), y de esta forma la señal recibida producirá una alta calidad en su reproducción. Además, la red puede llevar a cabo conversiones en las reglas de codificación utilizadas, en función de la versión del algoritmo PCM utilizado: la ley μ o la ley a.

- **Servicio portador a 64 Kbps estructurado a 8 KHz para información de audio a 3,1 KHz**: Permite transmitir información musical (compatible con el estándar “hilo musical”) utilizando el ancho de banda analógico común en telefonía.

- **Servicio portador a 64 Kbps estructurado a 8 KHz alterno Conversación/Sin Restricciones:** Este servicio de usuario está pensado para los terminales de usuarios con múltiples capacidades, que pueden elegir entre la transmisión de Voz o la transmisión no restringida a 64 Kbps. El modo de transmisión de voz de este servicio básico es el mismo que el del servicio portador a 64 Kbps estructurado a 8 KHz para conversación; mientras que el modo no restringido es el mismo que el servicio básico identificado como servicio portador a 64 Kbps estructurado a 8 KHz sin restricciones.

- **Servicio portador a 64 Kbps estructurado a 8 KHz Multiusos**: Un terminal multiusos puede funcionar con varios servicios: terminales de voz (usando el servicio básico de transmisión de voz), terminales de audio a 3,1 KHz (usando el servicio básico de transferencia de audio) y con la red pública conmutada (usando el servicio básico alterno voz/no restringido).

- **Servicio portador a 2 x 64 Kbps estructurado a 8 KHz sin restricciones:** La información de usuario se transmite en dos canales B a 64 Kbps, lo que proporciona una transmisión a 128 Kbps.

- **Servicio portador a 384/1536/1920 Kbps estructurado a 8 KHz sin restricciones:** Estos tres servicios básicos proporcionan tasas de alta velocidad a 384, 1536 y 1926 Kbps.

- **Servicio portador de Tasa Múltiple estructurado a 8 KHz sin restricciones:** Este servicio básico le permite al usuario solicitar tasas de transferencia múltiplos de 64 Kbps hasta la tasa máxima de la interfaz.

3.5.3.5 El protocolo PPP en RDSI

Cuando un enlace RDSI es parte de una red TCP/IP, la conexión puede ser gobernada por el protocolo PPP. Sin embargo, para soportar cualquier tipo de enlace punto a punto, PPP también trabaja con otros tipos de protocolos. El protocolo LAPD de RDSI define el principio y el fin de cada trama, sin embargo no posee una técnica de identificación del protocolo de nivel de red que está transportando. Con el campo PROTOCOL del protocolo PPP se consigue este objetivo.

Multilink Protocol

La RDSI tiene potencial para soportar múltiples enlaces puesto que el acceso básico incluye dos canales B separados. El Protocolo Multilink de PPP (MPPP) permite que una estación se conecte usando estos dos canales B simultáneamente, de forma que ambos se comportan como un único enlace lógico. El enlace lógico, conocido como *bundle*, provee un ancho de banda igual a la suma de los anchos de banda disponibles para los enlaces individuales. En el caso del enlace básico, el bundle hace 128 Kbps de ancho de banda disponible.

El Protocolo Multilink (MPPP) posee un identificador dentro del campo PROTOCOLO de 0x003D. Además, cada enlace físico puede negociar la compresión del campo PROTOCOLO para reducirlo a un solo byte.

3.5.3.6 Configuración de los equipos

Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers NUCLEOX-PLUS.
- 2 PC's que funcionarán como clientes.
- 2 hubs.
- 2 latiguillos directos, que conectarán el PC a un hub.
- 2 latiguillos directos, que conectarán el router con una roseta con acceso RDSI.

A continuación procedemos a montar la red según la siguiente topología:

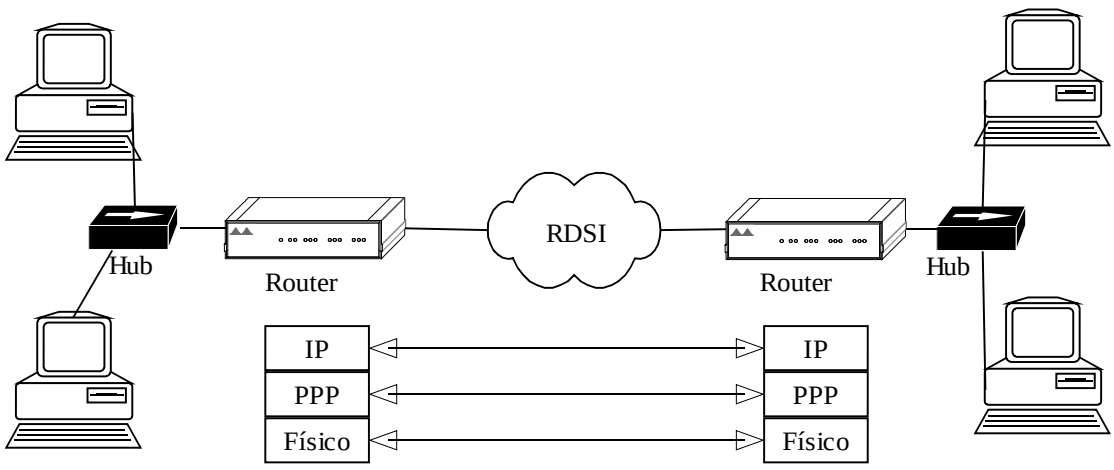

Figura 3.18: Topología de red.

Una vez que tenemos montada la red de la figura, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

Configuración del NUCLEOX PLUS

Para configurar un interfaz PPP sobre un acceso básico RDSI se deberá de introducir **ADD DEVICE PPP-DIAL** desde el proceso 4 (**PROCESS 4**). A continuación nos preguntará por el tipo de acceso básico RDSI, debemos introducir un 1. Durante el proceso de agregar el interfaz PPP-DIAL se pregunta el interfaz a eliminar. Dicho interfaz será siempre un canal B X.25. Por tanto los canales B PPP-DIAL se pueden agregar siempre a costa de perder canales B X.25.

```
Config>ADD DEVICE PPP-DIAL
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Ifc number to delete: [0]? 7
Added PPP-DIAL interface with num: 4
Config>
```

Para ver las interfaces que hemos añadido podemos ejecutar el comando **LIST DEVICES:**

```
Con     Ifc Type of interface                CSR      CSR2  int
---       3 Router->Node                       0                0
---       4 Node->Router                       0                0
ISDN 1    1 ISDN                         F001640  F000E00   9C
ISDN 1    2 B channel: PPP                     0                0
ISDN 1    7 ISDN D channel: X25          A000000           1B
ISDN 2    8 ISDN D channel: X25          A200000           1B
ISDN 2    9 ISDN B channel: X25          F001660  F000F00   9B
LAN       0 Ethernet                     9000000           1C
WAN1      5 X25                          F001600  F000C00   9E
WAN2      6 X25                          F001620  F000D00   9D
```

Podemos observar que se han creado 2 nuevas interfaces (1 y 2), una del tipo “ISDN” y otra del tipo “B channel: PPP”. El interfaz “ISDN” es un interfaz base RDSI. Si comprobamos su configuración, accediendo mediante el comando **NETWORK 1**, se verá que la conexión por defecto es del tipo conmutado, por lo que no es preciso configurar nada más.

```
*PROCESS 4
User Configuration
Config>NETWORK 1
ISDN Config
Config ISDN>LIST
Local destination:
Maximum frame size: 2048
ISDN Connection Type : Switched
Config ISDN>
```

El interfaz “B channel: PPP”, es virtual, no tienen asignado una posición física de memoria, y es el interfaz PPP sobre RDSI, propiamente dicho.

Para asignar las direcciones IP utilizamos el comando **ADD ADDRESS** desde el menú de configuración del protocolo IP, al que se accede tecleando **PROTOCOL IP** desde el Proceso 4 (Config>). Hay que añadirle una dirección tanto al interfaz LAN (Ethernet) como al interfaz virtual RDSI (B channel: PPP).

Seguidamente debemos añadir las rutas necesarias a la tabla de encaminamiento del router con el comando **ADD ROUTE**. Las rutas que debemos añadir, tomando como ejemplo la figura 3.19, son:

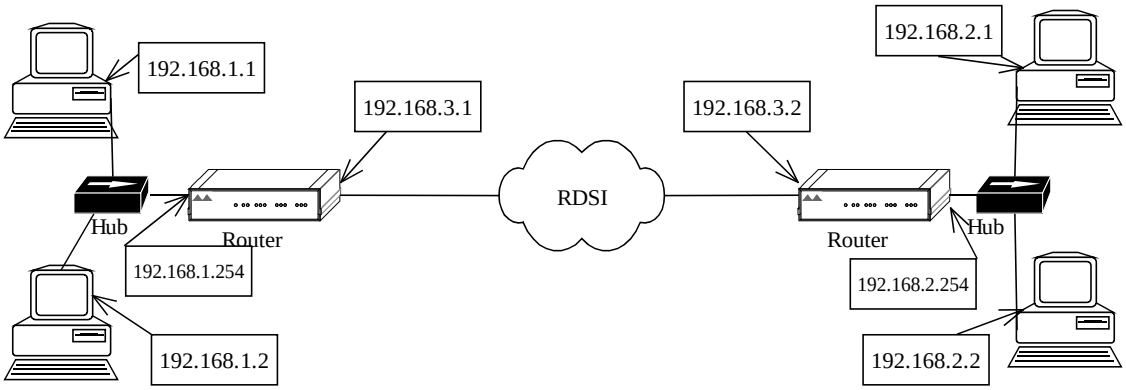

Figura 3.19: Topología de red con direcciones IP.

para el router de la izquierda:

Destino	Netmask	Gateway
192.168.2.0	255.255.255.0	192.168.3.2
192.168.1.0	255.255.255.0	0.0.0.0
192.168.3.0	255.255.255.0	0.0.0.0

Configuración del interfaz PPP

Para entrar en el menú de configuración del interfaz "B channel: PPP" debemos teclear **NETWORK (Número de interfaz asignado).** Este menú de configuración se identifica por el prompt *Circuit Config*>.

Si ejecutamos el comando **LIST** observamos la siguiente información:

```
Circuit Config>LIST
Base interface: -1
Destination address:
Inactive time: 60
Permitted caller:
Circuit name:
Outgoing calls allowed: Yes
Incoming calls allowed: No
Control access enabled: No
Circuit Config>
```

- *"Base interface":* se refiere al número del interfaz RDSI sobre el que se establece el enlace PPP. Por defecto toma el valor -1 indicando que el interfaz PPP utilizará el primer canal B del acceso básico que encuentre.
- *"Destination address":* es la dirección RDSI (número de teléfono) a la que se conectará el equipo.
- *"Inactive time":* permite determinar el tiempo tras el cual se liberará una llamada establecida en ausencia de tráfico IP.
- *"Permited caller":* con este parámetro se determina la dirección RDSI origen permitida. Por defecto (dirección vacía) se aceptan todas las llamadas RDSI.
- *"Circuit name":* este parámetro es meramente informativo. Permite asociar una cadena de caracteres al interfaz.
- *"Outgoing calls allowed"* e *"Incoming calls allowed":* indican la posibilidad de hacer y recibir llamadas.
- *"Control access enabled":* indica si se validará la pareja dirección destino/dirección origen con la lista global de parejas autorizadas. Dicha lista se configura en la facilidad global de control de acceso.

Debemos de configurar la dirección de destino. Para ello ejecutamos el comando **SET DESTINATION-ADDRESS**, y a continuación introducimos el número de teléfono deseado.

También debemos utilizar el comando **ENABLE INCOMING** para que el quipo pueda contestar a las llamadas entrantes.

Para entrar al menú de configuración del protocolo PPP desde el prompt *Circuit Config>*, debemos introducir el comando **ENCAPSULATOR**. A continuación el prompt cambiará por el de *PPP Config>*.

```
Circuit Config>ENCAPSULATOR

-- Interface PPP. Configuration --
PPP Config>
```

Aquí tecleamos **SET LINE LINE-SPEED**, este comando nos permite configurar la velocidad de transmisión. El resto de parámetros del protocolo PPP quedan configurados con sus valores por defecto al igual que en los dos apartados anteriores.

Asignación de direcciones IP a los PC Linux y Configuración de las tablas de encaminamiento de los PC Linux

Se realiza de la misma forma que en apartados anteriores.

Capítulo 4
Tecnologías WAN: Frame Relay

4.1 Introducción

Frame Relay es una red WAN de altas prestaciones que opera en las capas física y de enlace del modelo de referencia OSI. Originalmente fue diseñado para su uso a través de la Red Digital de Servicios Integrados (RDSI), aunque hoy es usado sobre una gran variedad tipos de interfaces de red. Frame Relay es una red de tecnología de conmutación de paquetes, por lo que se permite que las estaciones compartan dinámicamente el ancho de banda disponible.

Frame Relay emplea paquetes de longitud variable, para hacer la transferencia de datos más flexible y eficiente. Estos paquetes son conmutados entre los distintos nodos de la red hasta que se alcanza el destino. La multiplexación estadística controla el acceso a la red en redes de conmutación de paquetes. Como ya es sabido, la ventaja de esta técnica es que se acomoda más flexiblemente y más eficientemente al uso del ancho de banda.

4.2 Estandarización de Frame Relay

Las primeras propuestas de estandarización de Frame Relay fueron presentadas al CCITT en 1984. Sin embargo, Frame Relay no experimentó un avance significativo durante la década de los 80. Un mayor desarrollo de la red ocurrió en 1990 cuando Cisco, Digital Equipment (DEC), Northerm Telecom y StrataCom formaron un consorcio para centrarse en su desarrollo, al que se denominó Frame Relay Forum. Este consorcio desarrolló una especificación que conformó el protocolo básico Frame Relay y lo amplió con capacidades adicionales para entornos de interconexión complejos. Estas extensiones de Frame Relay se conocen como Local Management Interface (LMI). Desde que las especificaciones del consorcio fueron desarrolladas y publicadas, muchos vendedores han anunciado su soporte de la definición extendida de Frame Relay. La ANSI y la CCITT han estandarizado sus propias variaciones de la especificación original del LMI, y estas especificaciones estandarizadas ahora son usadas más comúnmente que la versión original. Internacionalmente, Frame Relay fue estandarizado por el ITU-T. En los Estados Unidos, Frame Relay es un estándar de la ANSI.

4.3 Dispositivos Frame Relay

Los dispositivos que conforman una red WAN Frame Relay se dividen en las siguientes dos categorías:

- FRAD (FR-Access Device).
- Conmutador Frame Relay (FRND, Dispositivo de Red Frame Relay).

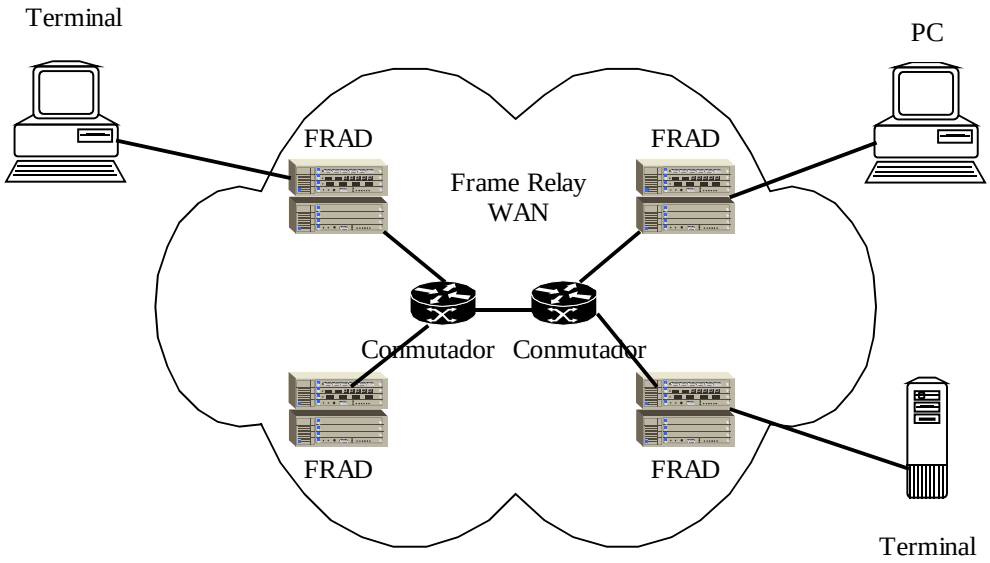

Figura 4.1: Red Frame Relay.

Los FRAD son un equipamiento de usuario que se encargan de empaquetar todas las tramas de los protocolos de nivel superior en tramas Frame Relay. De ahí el nombre que reciben, "dispositivos de acceso a redes Frame Relay".

Los conmutadores son los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, que identifica la ruta establecida para la conexión en la red. Estos conmutadores también se denominan FRND o Dispositivos de Red Frame Relay (Frame Relay Network Device).

Las redes Frame Relay están orientadas a la conexión (requieren de un mecanismo de señalización). Por lo tanto, cada circuito virtual establecido conserva en recepción el orden en que fueron emitidas las tramas. Esta característica hace que se simplifique mucho el funcionamiento de la red, ya que no se debe de implementar ningún mecanismo que garantice que las tramas llegan a su destino en el mismo orden en que fueron emitidas.

La calidad del substrato de transmisión permite que para lograr un mayor rendimiento del ancho de banda disponible, este tipo de redes no mandan asentimiento de los paquetes en su recepción, ni tampoco implementan ningún mecanismo de retransmisión de tramas. Esta es la principal diferencia de este tipo de redes con las redes X.25.

4.4 Circuitos virtuales Frame Relay

Frame Relay proporciona un enlace de datos orientado a conexión. Esto quiere decir que existe una comunicación establecida entre cada par de dispositivos y que esta conexión está asociada a un identificador de conexión. Este servicio se implementa usando circuitos virtuales Frame Relay, que es una conexión lógica entre dos dispositivos de usuario (FRAD) a través de una red de conmutación de paquetes Frame-Relay.

Con el establecimiento del circuito virtual se configura de antemano el camino por el cual van a circular los datos, entre los dos FRAD's. La causa de que este tipo de circuitos sean denominados virtuales, en contraposición a la conmutación de circuitos tradicional, es que en este caso el ancho de banda no es exclusivo, sino que es compartido con otras comunicaciones

de datos simultáneamente. En conmutación de circuitos, por el contrario, cada circuito tiene dedicado un ancho de banda de forma exclusiva.

Un circuito virtual puede atravesar un número indeterminado de conmutadores Frame Relay y se identifica por la sucesión de los identificadores DLCI establecidos entre cada par de dispositivos Frame Relay.

4.4.1 Circuitos Virtuales Conmutados

Los Circuitos Virtuales Conmutados (SVC, Switched Virtual Circuit) son conexiones temporales usadas en situaciones que necesitan únicamente transferencia de datos esporádica entre los dispositivos de usuario a través de la red Frame Relay. Una sesión de comunicación a través de un SVC consiste en los siguientes tres estados operativos:

- Establecimiento de llamada. Se estable el circuito virtual entre los dos dispositivos FRAD Frame Relay.
- Transferencia de datos. Se transmiten los datos entre los dispositivos FRAD sobre el circuito virtual. Si un SVC permanece inactivo durante un periodo de tiempo definido, se puede liberar la llamada.
- Terminación de llamada. El circuito virtual se libera.

Después de liberar el circuito virtual, los dispositivos FRAD deben establecer un nuevo SVC si hay datos adicionales para intercambiar. Se espera que los SVC se establezcan, mantengan, y terminen usando los mismos protocolos de señalización usados en RDSI. Pocos fabricantes de conmutadores Frame Relay soportan conexiones de circuito virtual conmutadas. Por lo tanto, su uso en las redes Frame Relay actuales es muy reducido.

4.4.2 Circuitos Virtuales Permanentes

Los Circuitos Virtuales Permanentes (PVC) son conexiones establecidas permanentemente que se usan para transferencias de datos consistentes y frecuentes entre dispositivos FRAD a través de la red Frame Relay. Las comunicaciones a través de un PVC no requieren los estados de establecimiento de llamada y de terminación que se usan con SVC. Los PVC siempre operan en uno de los dos siguientes estados:

- Transferencia de datos. Los datos se transmiten entre los dos dispositivos FRAD sobre el circuito virtual.
- Parado. La conexión entre los dispositivos FRAD está activa, pero no se transmiten datos. A diferencia de los SVC, los PVC no se liberan bajo ninguna circunstancia cuando están en el estado PARADO.

En este caso el establecimiento del circuito virtual es llevado a cabo por el administrador de la red de forma manual (estableciendo las tablas de encaminamiento de cada nodo manualmente). Y además, los FRAD pueden comenzar a transmitir datos en el momento en el que estén preparados, porque el circuito está establecido permanentemente.

Durante las operaciones de gestión de la red, puede ser que se aprendan PVC que no habían sido configurados en los dispositivos Frame Relay. A estos PVC se les denomina CIRCUITOS HUÉRFANOS. Si estos circuitos están habilitados los conmutadores tienen permiso para progresar paquetes por ellos, aunque en realidad no lo tengan configurado. Por ello es conveniente la deshabilitación de este tipo de circuitos. Además, con su deshabilitación también nos aseguramos que ningún intruso los va a utilizar como medio de acceso a nuestros equipos

4.4.3 DLCI

Los circuitos virtuales Frame Relay son identificados por los DLCI (Data-Link Connection Identifier). Los valores DLCI los asigna típicamente el proveedor de servicios Frame Relay (por ejemplo, la compañía telefónica) y tienen un significado local, es decir, sólo tienen significado en un enlace de la red.

La unión de los distintos DLCI´s desde el FRAD origen hasta el destinatario conforman el circuito virtual de la conexión.

Cuando el protocolo Frame Relay recibe un paquete para su encapsulamiento, compara la dirección IP de éste con las entradas de la caché del protocolo de resolución de direcciones (ARP – Address Resolution Protocol). Si la caché del ARP contiene el número de DLCI que coincide con la dirección IP, entonces el protocolo Frame Relay encapsula el paquete en una trama y lo transmite por el DLCI local especificado. Si el ARP no coincide con ninguno de los valores de la caché, la trama se descarta. Las direcciones de protocolo IP pueden ser asignadas de forma estática a las direcciones de los PVC de la red Frame Relay, sin necesidad de utilizar el ARP.

4.4.3.1 Asignación de DLCI

Con un DLCI de 10 bits hay 1024 posibilidades, teniendo en cuenta que los DLCI del número 16 hasta el 1007 son los disponibles para asignárselos a conexiones lógicas de usuario.

Número de DLCI	Asignación
0	Señalización
1-15	Reservados
16-1007	Conexiones lógicas de usuario
1008-10022	Reservados
1019-1022	Multicast
1023	Trama de control LMI

Tabla 4.1: Asignación de DLCI.

4.4.3.2 Funcionamiento de los conmutadores

Cuando un conmutador Frame Relay recibe una trama hace una serie de operaciones predefinidas, que vamos a describir a continuación:

En primer lugar, recalcula la secuencia de comprobación de trama (FCS), y si el FCS recalculado no coincide con el FCS de la trama, el conmutador descarta la trama.

Al mismo tiempo, el conmutador comprueba que el DLCI tenga un valor válido, así como la longitud de la trama. Si la trama es demasiado grande, demasiado corta, está desordenada, o tiene un DLCI inválido, se descarta. Nótese que al no haber ningún tipo de procedimiento para notificar dichos descartes, la recuperación de la información se delega a los protocolos de nivel superior (probablemente TCP).

Una vez que termina este procesamiento preliminar, el conmutador examina las tablas de encaminamiento para determinar el puerto por el que se transmitirá la trama. Cada tabla de encaminamiento del conmutador consiste en un par de valores (puerto-DLCI), asociado cada uno con un flujo de datos de entrada o de salida.

Input		Output	
Port	**DLCI**	**Port**	**DLCI**
1	16	2	33
2	8	1	16

Tabla 4.2: Tabla de encaminamiento de un conmutador.

La tabla de arriba muestra que una trama recibida por el puerto 1 que tenga un DLCI de 16 será transmitida por el switch a través del puerto 2, con un DLCI de 33.

Durante la fase de establecimiento de un circuito virtual, lo que se hace es modificar los valores de las tablas de encaminamiento de los conmutadores Frame Relay, en función de los extremos entre los que se va a establecer la comunicación, y de los conmutadores que se van a atravesar. Y de esta forma el camino que van a seguir los datos queda definido de forma única antes de comenzar a enviar los datos.

4.5 Formato de la trama

Los datos de usuario se transmiten en forma de tramas, usando un subconjunto del protocolo LAPF. Este protocolo es una versión mejorada del protocolo LAPD de la RDSI al que se le han añadido funciones de control de congestión.

El DLCI puede tener 10, 17 o 24 bits de longitud y, por lo tanto, podemos tener 3 tipos distintos de cabecera:

(segmento superior DLCI)			C/R	EA 0
(segmento inferior DLCI)	FECN	BECN	DE	EA 1

Figura 4.2: Cabecera con un DLCI de 10 bits

(segmento superior DLCI)			C/R	EA 0
DLCI	FECN	BECN	DE	EA 0
(segmento inferior DLCI)			D/C	EA 1

Figura 4.3: Cabecera con un DLCI de 17 bits

(segmento superior DLCI)			C/R	EA 0
DLCI	FECN	BECN	DE	EA 0
DLCI				EA 0
(segmento inferior DLCI)			D/C	EA 1

Figura 4.4: Cabecera con un DLCI de 24 bits

A continuación, describiremos brevemente la funcionalidad de cada uno de los campos que conforman la cabecera:

EA: El campo de EXTENSIÓN DE DIRECCIÓN se localiza siempre en la posición de bit 1 de cada byte de la CABECERA. Cuando está puesto a 0 indica que otro byte de la CABECERA sigue a este byte. Cuando está puesto a 1 indica que este byte es el último de la CABECERA.

C/R: El campo de COMANDO/RESPUESTA tienen una longitud de 1 bit. Este campo es transparente a la red y se incluyó en Frame Relay para ser usado por aplicaciones concretas.

FECN y BECN: El bit FECN (Forward Error Correction Notification) es puesto a 1 por la red para informar al receptor de que la red está experimentando congestión. De la misma forma, el valor de BECN (Backward Error Correction Notification) también se pone a 1 como un mecanismo para informar a la estación transmisora de que la red está congestionada en la dirección contraria. Su funcionamiento se verá en el apartado de mecanismos de control de congestión.

DE: El campo DE (Discard Eligible) provee un mecanismo para indicar a la red un esquema de prioridad para descartar tramas en periodos de congestión. Un valor de 0 en DE indica a la red que la trama no debe ser descartada, a no ser que no haya otra alternativa. Un valor de 1 indica que la trama puede ser descartada.

DLCI: El DLCI (Data Link Control Identifier) se usa en la red Frame Relay para permitir que múltiples sesiones compartan una línea común. El DLCI no representa una dirección de destino, sino la conexión resultante del establecimiento del circuito virtual y sólo tiene significado local. El tamaño más común del DLCI es de 10 bits. Algunos DLCI están reservados para funciones específicas de gestión de red.

4.6 Parámetros de Servicio

Estos parámetros de servicio incluyen el CIR, el B_c, el B_e, y el tiempo medio T_c usado para definir el CIR, el B_c y el B_e.

4.6.1 CIR (Comitted Information Rate)

El CIR es la tasa de transferencia binaria establecida para VCs bajo condiciones normales de funcionamiento (sin congestión de red). A cada VC se les asigna un CIR (establecido por el proveedor del servicio Frame Relay). EL CIR es una porción del caudal efectivo (throughput) total del enlace físico y varía entre 300 bps y 2 Mbps, siendo el valor más habitual el de 64 Kbps.

Es importante establecer que el CIR no es una medida instantánea de transmisión, sino una tasa media sobre el tiempo. Por ejemplo, si el CIR es de 256 Kbps, esto no quiere decir que el usuario no pueda transmitir a más de 256 Kbps. Lo que quiere decir es que el usuario no transmitirá más de 256 Kbits en un segundo (supueta una ventana de 1 segundo).

4.6.2 Comitted Burst Size (B_c)

En los terminales FRAD, el tamaño de ráfaga enviado a la red (Committed Burst Size) es la cantidad máxima de datos enviados (en bits) que puede ser transmitida a través de un VC durante un periodo de tiempo determinado de antemano (T_c). Este parámetro está relacionado con el CIR y se cuantifica según la siguiente expresión:

$$CIR=B_c/T_c$$

Por ejemplo, si se selecciona un CIR para un VC de 9.600 bps y un tamaño de ráfaga enviado de 14.400 bits, el periodo de tiempo es 1,5 segundos (14.400 bit /9.600 bps = 1,5 seg.). Esto quiere decir que el VC puede transmitir un máximo de 14.400 bits en cada segundo y medio.

4.6.3 Excess Burst Size (B_e)

El FRAD, durante un cierto intervalo de tiempo, puede transmitir más información de la marcada por el tamaño de ráfaga enviado. El exceso de información (en bits) es denominado Excess Burst Size. La red no garantiza que este exceso de información llegue al destinatario. De hecho, en situación de congestión, los conmutadores FR pueden descartar este tipo de tramas. Para distinguir este tipo de tramas, la cabecera de la trama Frame Relay contiene un bit DE (Discard Elegibility), puesto a 1.

Los emisores también pueden poner el valor del bit DE a 1 para indicar que la trama tiene menos importancia que otras tramas. Cuando la red está congestionada, los nodos de la red descartarán las tramas con el bit DE a 1 antes de descartar otras que no lo tienen. Esto reduce la probabilidad de descartar datos críticos en periodos de congestión.

Se deberá seleccionar un valor mayor que cero para el parámetro B_e sólo en aquellos casos en los que se desee aceptar el riesgo de que se descarten datos y el efecto que esto puede producir en el funcionamiento de las capas superiores del protocolo de comunicación.

Por lo tanto, Bc+Be representa la máxima cantidad de información que se puede transmitir durante un intervalo de tiempo Tc. Si un usuario transmite más de Bc+Be bits en un intervalo Tc, la red descartará inmediatamente el exceso de tramas.

4.7 Mecanismos de Control de Congestión

Debido a la naturaleza estadística del tráfico de datos, es posible que, en determinados instantes de tiempo, algunos de los nodos de la red se congestione. Frame Relay reduce la sobrecarga de la red mediante dos mecanismos simples de notificación de la congestión:

- FECN (Forward-Explicit Congestion Notification)
- BECN (Backward-Explicit Congestion Notification)

Tanto FECN como BECN se controlan por un solo bit situado en la cabecera de la trama Frame Relay (ver figura 4.2).

El mecanismo de FECN se inicia cuando el emisor envía tramas Frame Relay a la red. Si la red está congestionada, los nodos de la red ponen el valor del bit FECN a 1. Cuando las tramas alcanzan el receptor con un valor de FECN a 1 indica que la trama experimentó congestión en el camino de la fuente al destino. El dispositivo receptor puede retransmitir esta información a protocolos de capas más altas para procesarla. Dependiendo de la implementación, se puede iniciar el control de flujo, o se puede ignorar la indicación.

Los receptores ponen a 1 el valor del bit BECN en las tramas que viajan en sentido contrario a las tramas con el bit FECN a 1. Esto informa al emisor de que un camino particular a través de la red está congestionado. El dispositivo emisor puede retransmitir esta información a protocolos de capas más altas para que la procesen. Dependiendo de la implementación, se puede iniciar el control de flujo, o se puede ignorar la indicación.

4.7.1 Monitorización del CIR

La monitorización del CIR es una posibilidad opcional de Frame Relay que puede ser configurada para cada interfaz. Mediante esta opción se previene que la velocidad de transmisión de información sea mayor que la suma del tamaño de ráfaga enviado (Committed Burst Size) y del exceso sobre el tamaño de ráfaga (Excess Burst Size).

La velocidad de transmisión de información se denomina Tasa Variable de Información (VIR - Variable Information Rate). Dependiendo del grado de sobrecarga de la red, varía entre un mínimo de 0.25 veces el CIR y un máximo del tamaño de ráfaga enviado más el exceso sobre el tamaño de ráfaga ($B_c + B_e$).

Para impedir la sobrecarga inicial de la red, el VIR toma el valor del CIR al arranque de la misma.

4.7.2 Monitorización de Sobrecarga

La monitorización de sobrecarga es una característica opcional, que se configura para cada interfaz Frame Relay. Permite que el VIR de los VC varíe en respuesta a la sobrecarga de la red. El VIR puede tomar valores entre un mínimo de 0.25 veces el valor del CIR y un máximo de la velocidad de línea.

La monitorización del CIR, cuando está habilitada, anula la monitorización de sobrecarga. Si tanto la monitorización de sobrecarga como la monitorización del CIR están deshabilitados, el VIR para cada VC del interfaz será igual a la velocidad de línea y no decrecerá como respuesta a la sobrecarga de red.

4.7.3 Comprobación de Errores de Frame Relay

Frame Relay utiliza un mecanismo muy común de comprobación de errores conocido como Comprobación de Redundancia Cícilica (CRC). Nótese que en Frame Relay, si una trama es errónea, ésta es descartada inmediatamente sin realizar antes ningún proceso de corrección de errores.

4.8 LMI

El LMI (Local Management Interface) es un conjunto de mejoras a la especificación básica de Frame Relay. Fue desarrollado en 1990 por Cysco Systems, StrataCom, Northern Telecom, y Digital Equipment Corporation. Ofrece un conjunto de características (llamadas extensiones) para administrar las redes Frame Relay. El conjunto de las extensiones LMI de Frame Relay incluye direccionamiento global, mensajes de estado del circuito virtual, multicast y un control de flujo simple.

La extensión de direccionamiento global de LMI da al DLCI de Frame Relay un valor global en lugar de un significado local. Los valores DLCI se convierten en direcciones que son únicas en las redes WAN Frame Relay. Ahora, las interfaces de red individuales y los nodos de terminación unidos a ellas, por ejemplo, se pueden identificar usando resolución de direcciones estándar (protocolos ARP, Address Resolution Protocol) y técnicas de descubrimiento. Por lo tanto, la red Frame Relay entera parece como una red LAN.

Los mensajes de estado del circuito virtual de LMI proveen comunicación y sincronización entre los dispositivos FRAD y conmutadores. Estos mensajes se usan para informar periódicamente sobre el estado de los VC y se estudiarán en el apartado 4.9.

La extensión multicast de LMI permite asignar grupos multicast. También transmite informes sobre el estado de los grupos multicast en los mensajes de actualización.

4.8.1 Formato de la trama LMI

Los mensajes LMI utilizan un valor de DLCI de 1023. El formato de la cabecera de la trama LMI se representa a continuación:

<table>
<tr><td colspan="3">(segmento superior DLCI)</td><td>C/R</td><td>EA 0</td></tr>
<tr><td>(segmento inferior DLCI)</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA 1</td></tr>
</table>

Figura 4.5: Cabecera de la trama LMI

El bit C/R está a 1, mientras que los bits en las posiciones que representan los campos DE, FECN, y BECN, están a 0. La cabecera se encuentra situada en la trama LMI, justo después del Flag inicial. A continuación observamos el formato completo de una trama LMI:

<table>
<tr><td>1 Byte</td><td>2 Bytes</td><td>1 Byte</td><td>1 Byte</td><td>1 Byte</td><td>1 Byte</td><td>Variable</td><td>2 Bytes</td><td>1 Byte</td></tr>
<tr><td>Flag</td><td>Cabecera</td><td>Unnumbered Information Indicator</td><td>Protocol Discriminator</td><td>Call Reference</td><td>Message Type</td><td>Information elements</td><td>FCS</td><td>Flag</td></tr>
</table>

Figura 4.6: Formato de la trama LMI

La función de los distintos campos de la trama es la siguiente:

FLAG. Delimita el comienzo y el final de la trama.

CABECERA. Indicada anteriormente.

PROTOCOL DISCRIMINATOR. Tiene el valor 00000001 para identificar el mensaje LMI.

CALL REFERENCE. No tiene ningún objetivo. Está a 0.

MESSAGE TYPE. Etiqueta la trama con uno de los siguientes tipos:

- MENSAJE DE PETICIÓN DE ESTADO. Permite a un usuario solicitar información acerca del estado de la red.
- MENSAJE DE ESTADO. Respuesta a los mensajes de petición de estado. Los mensajes de estado incluyen mensajes de estado del VC y mensajes de actualización del estado.

INFORMATION ELEMENTS. Contiene un número variable de elementos de información individuales.

FCS. Campo de protección frente a posibles errores en transmisión.

4.9 Gestión de la Red Frame Relay

El proveedor de la red Frame Relay proporciona también el servicio de gestión de la red Frame Relay. Es responsabilidad de la gestión de red proveer a las estaciones finales Frame Relay con información de estado y configuración relativa a los VCs disponibles en el interfaz físico.

El protocolo Frame Relay admite tres tipos de gestiones: la descrita en el Anexo D de la ANSI, la del CCITT (hoy llamado ITU) y la del Interfaz de Gestión Local (Local Management Interface -LMI-). La red Frame Relay suministra específicamente la siguiente información:

- Notificación de VCs adicionales (huérfanos) y si están activos o inactivos así como la anulación de cualquier VC.
- Notificación del control de flujo según el valor de los bits de FECN y BECN.
- Notificación de la disponibilidad de un VC configurado.
- Verificación de la integridad del enlace físico entre la estación final y la red mediante el intercambio de una secuencia numérica de actividad.
- Inclusión del CIR como parte de la información del estado del VC.

4.9.1 Informe del estado de gestión

Bajo demanda, la gestión Frame Relay genera dos tipos de informes de estado, un informe de estado completo y un informe sobre la verificación de la integridad del enlace. El informe de estado completo proporciona información acerca de todos los PVCs conocidos por el interfaz Frame Relay. El informe sobre la verificación de la integridad del enlace comprueba la conexión entre una estación concreta y un conmutador de la red. Todas las peticiones de estado y respuestas a los mismos se realizan por el DLCI 0 para las entidades ANSI Anexo D y CCITT o bien por el DLCI 1023 para el Interfaz de gestión local provisional (LMI).

4.10 Desarrollo práctico

- Definir un interfaz Frame Relay sobre línea serie.
- Agregar un interfaz Frame Relay sobre un acceso básico, para poder conectarse mediante RDSI con otro extremo.

4.10.1 Definir un interfaz Frame Relay sobre línea serie

4.10.1.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers Frame Relay.
- 2 PC’s que funcionarán como clientes.
- 2 hubs.
- 2 latiguillos directos.
- 1 cable RS-232 DB25 punto a punto para conectar los 2 routers NUCLEOX PLUS, desde el puerto 1(DTE) de uno hasta el puerto 2 (DCE) del otro.

A continuación procedemos a montar la red según la siguiente topología:

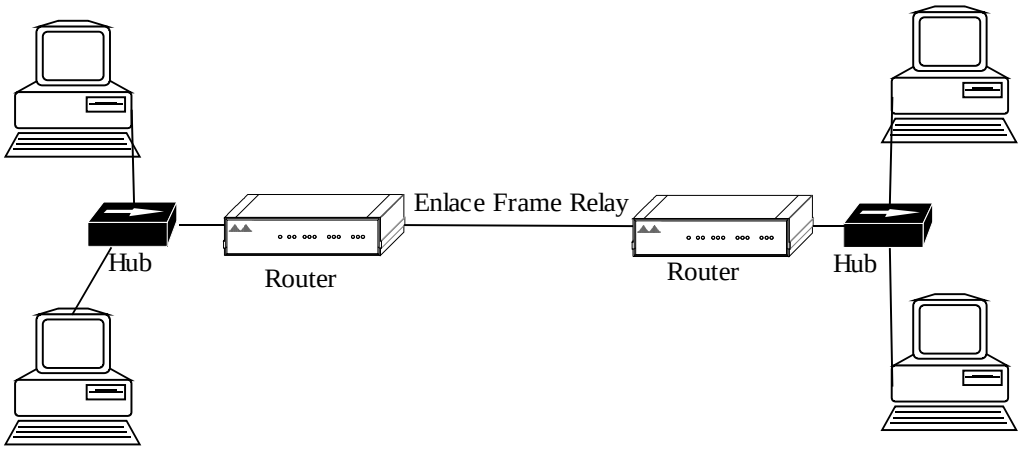

Figura 4.7: Topología de red

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

4.10.1.2 Configuración del NUCLEOX PLUS

En primer lugar, lo que debemos hacer es agregar el dispositivo Frame Relay. Para ello hay que ejecutar el comando **SET DATA-LINK FRAME-RELAY** una vez situado en el prompt de configuración Config>.

A continuación debemos asignar las direcciones IP al router y configurar su tabla de encaminamiento. Para asignar las direcciones IP utilizamos el comando **ADD ADDRESS** desde el menú de configuración del protocolo IP, al que se accede tecleando **PROTOCOL IP** desde el Proceso 4 (Config>). Hay que añadirle una dirección tanto al interfaz LAN (Ethernet) como al interfaz serie.

Seguidamente debemos añadir las rutas necesarias a la tabla de encaminamiento del router con el comando **ADD ROUTE**. Las rutas que debemos añadir, tomando como ejemplo la siguiente red, son:

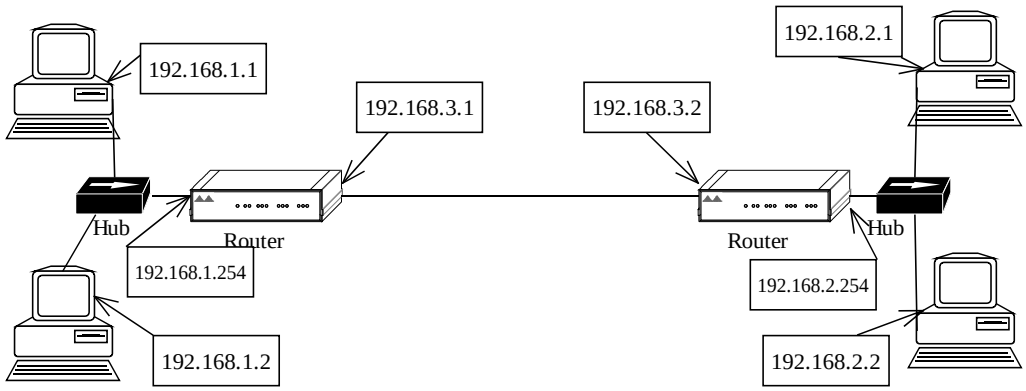

Figura 4.8: Topología de red con direcciones IP

para el router de la izquierda:

Destino	Netmask	Gateway
192.168.2.0	255.255.255.0	192.168.3.2
192.168.1.0	255.255.255.0	0.0.0.0
192.168.3.0	255.255.255.0	0.0.0.0

4.10.1.3 Configuración del interfaz Frame Relay

Para entrar en el menú de configuración del interfaz Frame-Relay debemos teclear **NETWORK (Número de interfaz asignado).** Este menú de configuración se identifica por el prompt *FR Config*>.

A continuación debemos añadir los circuitos virtuales permanentes (PVCs) que necesitemos. Para ello debemos utilizar el comando **ADD PVC-PERMANENT-CIRCUIT** desde el menú de configuración del interfaz Frame-Relay. Este comando añade un PVC al interfaz Frame Relay por encima de los circuitos por defecto (15). El número máximo de PVCs que pueden añadirse es de 991, aunque el número de PVCs admitidos por un interfaz depende del valor configurado para la longitud del buffer de recepción.

```
FR config> ADD PVC-PERMANENT-CIRCUIT
Circuit number [16]?
Outgoing Committed Information Rate (CIR) in bps [16000]?
Outgoing Committed Burst Size (Bc) in bits [16000]?
Outgoing Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)?
Assign circuit name []?
Inverse ARP (0-Default, 1-Off, 2-On): [0]?
FR config>
```

Además, al ejecutar el comando anterior, nos permite configurar una serie de parámetros:

- *Circuit number:* Es el número de circuito. Debe estar comprendido entre 16 y 1.007.

- *Committed Information Rate(CIR):* Es el valor de la tasa de información entregada y puede tomar valores entre 300 bps y 2.048 Mbps. El valor por defecto es 16 Kbps.

- *Committed Burst Size(B_c):* Es la máxima cantidad de datos, expresada en bits, que la red acepta para transmitir en un intervalo de tiempo igual a (Committed Burst Size/CIR) segundos. Puede tomar valores entre 300 y 2.048 Mbits. El valor por defecto es 16 Kbits.

- *Excess Burst Size(B_e):* Es la máxima cantidad de bits por encima del Committed Burst Size que la red trata de enviar durante un tiempo expresado en segundos igual a (Committed Burst Size/CIR). Los valores admitidos van desde 0 a 2.048 Mbits. El valor por defecto es 0.

- *Encrypt information:* Permite decidir si queremos que el campo de datos de la trama Frame Relay viaje en claro o cifrado.

- *Assign circuit name:* Es la cadena de caracteres ASCII utilizada para describir el circuito. Se recomienda utilizar un nombre de circuito que describa las características del mismo. El valor por defecto es *Unassigned*. El nombre puede tener hasta 23 caracteres.

- *Inverse ARP:* Permite definir si queremos habilitar/deshabilitar el protocolo ARP Inverso.

Cuando se está utilizando un protocolo de comunicaciones, como por ejemplo el protocolo IP sobre el interfaz Frame Relay, y se necesita conectar con dispositivos que no soportan el ARP (Address Resolution Protocol) sobre Frame Relay, hay que utilizar el comando **ADD PROTOCOL-ADDRESS.** Este comando se utiliza para asignar la dirección IP con el DLCI por el que se debe realizar la comunicación. Al añadir estas direcciones se evita la necesidad de utilizar ARP durante el proceso de establecimiento de comunicación para averiguar el DLCI que le corresponde a una determinada dirección IP destino. Al utilizar este parámetro se pide introducir una serie de parámetros:

- *IP Address:* Es la dirección IP de 32 bits.
- *Circuit number:* Es el número del DLCI (comprendido entre 16 y 1.007) que será utilizado por el protocolo.

```
FR config> ADD PROTOCOL-ADDRESS
Protocol name or number [0]?
IP Address [0.0.0.0]?
Circuit number [16]?
FR config>
```

A continuación se debe establecer la velocidad de línea utilizada por el interfaz en bits por segundo. Para ello utilizamos el comando **SET LINE-SPEED**. Esta velocidad es empleada por el control de CIR para regular el tráfico emitido y para el cálculo de los estadísticos de emisión y recepción. La velocidad seleccionada debe estar comprendida entre 300 y 2.048 Mbps. El valor por defecto es 64 Kbps.

```
FR config> SET LINE-SPEED
Access rate in bps [64000]?
FR config>
```

Debemos *deshabilitar la actividad de gestión* mediante el comando **DISABLE LMI**. Al deshabilitar este parámetro se permite el funcionamiento normal en pruebas Frame Relay extremo a extremo en ausencia de una red real.

```
FR config> DISABLE LMI
FR config>
```

También debemos utilizar el comando **ENABLE CIR-MONITOR** para habilitar la opción de monitorización de circuito impuesta por la tasa de transmisión configurada previamente mediante el comando **ADD PVC-PERMANENT-CIRCUIT**. Esta opción, por defecto, está deshabilitada.

La monitorización del CIR es uno de los mecanismos de control de congestión que posee Frame Relay. Mediante esta opción se previene que la velocidad de transmisión de información sea mayor que la suma del tamaño de ráfaga enviado (Comitted Burst Size) y del exceso sobre el tamaño de ráfaga (Excess Burst Size).

```
FR config> ENABLE CIR-MONITOR
FR config>
```

Con la configuración establecida hasta este momento podemos observar que quedan habilitadas por defecto otras características de Frame Relay como la monitorización de sobrecarga, que es uno de los mecanismos de control de congestión. Esta opción permite que la velocidad de transferencia de información varíe entre 0.25 veces el CIR y la velocidad de línea en respuesta a la sobrecarga de red.

Además, se permite el uso de todos los circuitos no configurados en el interfaz (circuitos huérfanos). Por defecto, estos circuitos están habilitados y su CIR es de 16 Kbps, el Committed Burst Size es 160 Kbits y el Excess Burst Size es 0.

También quedan habilitadas las opciones de transmisión de paquetes broadcast y la de emulación de difusión multicast en este interfaz. De esta manera, todo paquete de broadcast que llegue a este interfaz será transmitido por todos los circuitos que se encuentren activos.

Si se desea, se pueden habilitar otras propiedades que posee el interfaz Frame Relay, como la opción de compresión o la de fragmentación. El comando ENABLE COMPRESSION habilita la compresión de los datos para un DLCI determinado. Se puede elegir entre compresión **ADAPTATIVE** o **PREDICTOR, CONTINUOUS** o **PKT_BY_PKT** y **OWNER** o **COMPATIBLE**. El comando ENABLE FRAGMENTATION-FRF12 permite habilitar la fragmentación según la norma FRF.12 especificando el tamaño del fragmento en bytes.

4.10.1.4 Asignación de direcciones IP a los PC Linux y configuración de las tablas de encaminamiento

Se realiza de la misma forma descrita en el Capítulo 3.

4.10.1.5 Comprobación

Una vez configurados todos los parámetros anteriores, podemos realizar diversas pruebas para comprobar que se satisfacen las características de la comunicación que hemos configurado. Para ello podemos proceder a realizar un ftp desde uno de los clientes al otro cliente.

El FTP nos da información sobre el tiempo que tarda en transmitir un fichero de un determinado tamaño, y de esta forma podemos averiguar la velocidad de transmisión real en bits por segundo.

4.10.1.6 Medidas tomadas

CIR (bps)	B_C (bits)	B_e	TAMAÑO (bytes)	TIEMPO (segundos)	VELOCIDAD (bps)
16000	16000	0	50088	25,5	15700
16000	16000	8000	50088	16,5	24000
16000	16000	16000	50088	13	30000
48000	48000	0	50088	8	48000
48000	48000	8000	50088	7,5	54000
48000	48000	16000	50088	6	64000

Como podemos observar en la tabla superior, en todas las experiencias el parámetro T_c se ha tomado como 1 segundo. A partir de aquí, el trabajo ha consistido en modificar el CIR y el parámetro B_c, y en medir el tiempo que tarda en realizarse la transferencia completa de un fichero de tamaño conocido. Una vez conocido este tiempo se calcula la velocidad media a la que se ha realizado la transferencia.

Para cada una de las pruebas, se puede observar fácilmente como la velocidad de transferencia nunca es superior a la suma del CIR más el parámetro B_e / T_c, debido a que tenemos habilitada la opción de monitorización del CIR.

4.10.2 Definir un interfaz Frame Relay sobre RDSI

4.10.2.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers Frame Relay.
- 2 PC's que funcionarán como clientes.
- 2 hubs.
- 2 latiguillos directos, para conectar cada PC al hub.
- 2 latiguillos directos, para conectar el router a una roseta con acceso RDSI.

A continuación procedemos a montar la red según la siguiente topología:

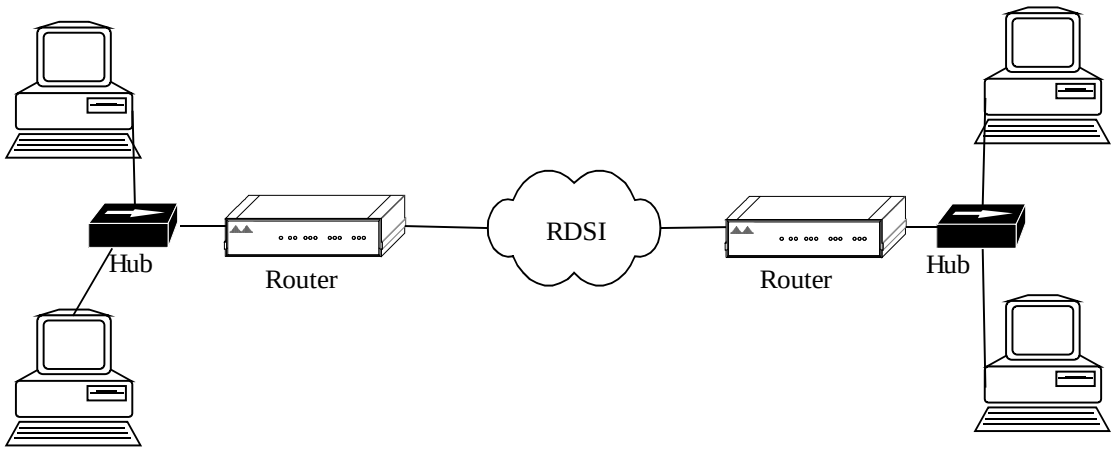

Figura 4.9: Topología de red

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

4.11.2.2 Configuración del NUCLEOX PLUS

En primer lugar lo que debemos hacer es agregar un interfaz Frame Relay sobre RDSI. Para agregar el dispositivo Frame Relay hay que ejecutar el comando **ADD DEVICE FR-ISDN** una vez situado en el prompt de configuración Config>.

```
Config> ADD DEVICE FR-ISDN
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Ifc number to delete: [0]? 7
Added FR-ISDN interface with num: 2
Config>
```

Si ejecutamos el comando **LIST DEVICES** podemos observar que se han creado 2 nuevas interfaces:

```
Config> LIST DEVICES

Con    Ifc Type of interface                CSR     CSR2  int
---      3 Router->Node                       0             0
---      4 Node->Router                       0             0
ISDN 1   1 ISDN                         F001640  F000E00   9C
ISDN 1   2 B channel: FR over ISDN           0             0
ISDN 1   7 ISDN D channel: X25          A000000            1B
ISDN 2   8 ISDN D channel: X25          A200000            1B
ISDN 2   9 ISDN B channel: X25          F001660  F000F00   9B
LAN      0 Ethernet                     9000000            1C
WAN1     5 X25                          F001600  F000C00   9E
WAN2     6 X25                          F001620  F000D00   9D
Config>
```

Éstos son el interfaz 1 (ISDN) que es el interfaz base RDSI, y el interfaz 2 (B channel: FR over ISDN), el interfaz Frame Relay sobre RDSI, que se trata de un interfaz lógico, carente de conector físico propio. Se debe añadir un interfaz Frame Relay sobre RDSI por cada destino potencial de las llamadas.

A continuación debemos asignar las direcciones IP al router y configurar su tabla de encaminamiento. Esto se realiza de la misma forma descrita en el apartado anterior.

4.10.2.3 Configuración del interfaz Frame Relay sobre RDSI

Para entrar en el menú de configuración del interfaz Frame Relay sobre RDSI debemos teclear **NETWORK (Número de interfaz asignado)**, este menú de configuración se identifica por el prompt *Circuit Config>*

```
Config> NETWORK 2
Circuit Config
Circuit Config>
```

Si ejecutamos el comando **LIST** observamos la siguiente información:

```
Circuit Config> LIST
Base interface: -1
Destination address:
Inactive time: 60
Permitted caller:
Circuit name:
Outgoing calls allowed: Yes
Incoming calls allowed: No
Enabled Access Control: No
Circuit Config>
```

Debemos de configurar la dirección de destino. Para ello ejecutamos el comando **SET DESTINATION-ADDRESS**, y a continuación introducimos el número de teléfono deseado.

```
Circuit Config> SET DESTINATION-ADDRESS
Destination address[]? 1018
Circuit Config>
```

También debemos utilizar el comando **ENABLE INCOMING** para que el equipo pueda contestar a las llamadas entrantes.

```
Circuit Config> ENABLE INCOMING
Circuit Config>
```

Una vez hecho todo lo anterior, sólo quedan por configurar aquellos parámetros específicos de Frame Relay. Para este ejemplo concreto, se va a crear un circuito permanente (PVC) con DLCI 16, se va a deshabilitar el LMI y se creará una asociación entre el DLCI 16 y la dirección IP 192.168.3.2 . Primero, se entra en el menú de configuración de Frame Relay:

```
Circuit Config> ENCAPSULATOR

-- Frame Relay user configuration --
FR config>
```

Ahora se crea el circuito virtual permanente que se desea tener disponible:

```
FR config> ADD PVC-PERMANENT-CIRCUIT
Circuit number [16]? 16
Committed Information Rate (CIR) in bps[16000]? 16000
Committed Burst Size (Bc) in bits[16000]? 16000
Excess Burst Size (Be) in bits[0]? 0
Encrypt information? [No]: (Yes/No)? NO
Assign circuit name[]? BARCELONA
FR config>
```

Hay que utilizar el comando **ADD PROTOCOL-ADDRESS** para agregar el protocolo estático y asignar el mapa de direcciones. Este comando añade las direcciones estáticas de destino de protocolo al interfaz Frame Relay.

```
FR config> ADD PROTOCOL-ADDRESS
IP Address [0.0.0.0]? 192.168.3.2
Circuit number[16]? 16
FR config>
```

Finalmente, se deshabilita la actividad de gestión de la red, ya que los routers están conectados directamente a través de la RDSI:

```
FR config> DISABLE LMI
FR config>
```

Se salva la configuración y se reinicia el equipo.

El interfaz “ISDN” es un interfaz base RDSI. Si comprobamos su configuración, accediendo mediante el comando **NETWORK 1**, se verá que la conexión por defecto es del tipo conmutado, por lo que no es preciso configurar nada más.

```
*PROCESS 4
User Configuration
Config>NETWORK 1
ISDN Config
Config ISDN>LIST
Local destination:
Maximum frame size: 2048
ISDN Connection Type : Switched
Config ISDN>
```

4.10.2.4 Asignación de direcciones IP a los PC Linux

Se realiza de la misma forma que en el capítulo 3.

4.10.2.5 Configuración de las tablas de encaminamiento de los PC Linux

Se realiza de la misma forma que en el capítulo 3.

Capítulo 5
NAT

5.1 Introducción

La necesidad de traducir una dirección IP surge cuando direcciones IP de redes internas no pueden ser usadas fuera de la red interna, ya sea por razones de privacidad o porque son inválidas para su uso en Internet.

La Traducción de Dirección Básica permite a los hosts en una red privada acceder de manera transparente a la red externa (Internet). Las organizaciones con una red configurada predominantemente para uso interno, con una necesidad ocasional de acceso externo, son buenos candidatos para este esquema.

Muchos usuarios de "Oficina Pequeña, Oficina en Casa" (SOHO) y empleados telecomunicados tienen múltiples equipos de red en sus oficinas, corriendo aplicaciones TCP/UDP. Sin embargo, tienen una sola dirección IP para su router de acceso, asignada por su proveedor de servicio. Mediante NAT, se puede conseguir que diversos usuarios (cada uno con su propia dirección IP privada) compartan dinámicamente la única dirección IP de acceso a Internet.

Hay limitaciones al uso del método de traducción. Es obligatorio que todas las solicitudes y respuestas pertenecientes a una sesión sean encaminadas por el mismo router NAT. Una manera de asegurar esto sería tener un NAT basado en un router frontera que fuera único para una zona del dominio, donde todos los paquetes IP son originados desde el dominio o destinados a él. Hay otras maneras de asegurar dicha integridad cuando existen múltiples dispositivos NAT. Por ejemplo, un dominio privado puede tener dos puntos de salida a proveedores diferentes y el flujo de la sesión desde los hosts en una red privada puede atravesar cualquiera de los dispositivos NAT que tenga la mejor métrica. Cuando uno de los routers NAT falla, el otro puede encaminar el tráfico para todas las conexiones.

Esta solución tiene la desventaja de quitar el significado extremo a extremo de una dirección IP. Otra consecuencia es que la seguridad del nivel de red IP extremo a extremo asegurada por IPsec no puede ser asumida con un dispositivo NAT de enrutado. La ventaja de esta aproximación, sin embargo, es que puede ser instalada sin cambios en los hosts o en los routers.

5.2 Funcionamiento NAT

En la figura 5.1 se ilustra el funcionamiento del mecanimo NAT.

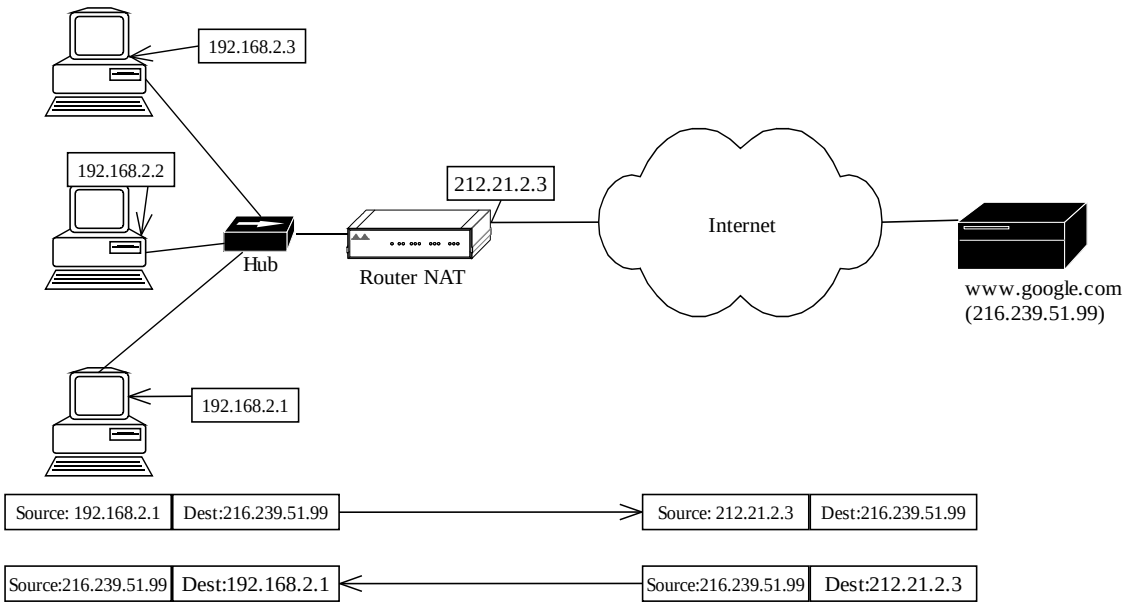

Figura 5.1: Mecanismo NAT

Cuando el host 192.168.2.1, en la red local 192.168.2.0 (dirección privada de clase C), desea enviar un paquete al host 216.239.51.99 (dirección IP pública), éste usa la dirección 216.239.51.99 como destino, y envía el paquete a su router primario. El router de la red tiene habilitado la facilidad NAT y sustituye la dirección origen a 212.21.2.3 (dirección IP pública), antes de que el paquete sea reenviado. Del mismo modo, los paquetes IP en la ruta de regreso van a pasar a través de traducciones de dirección en sentido contrario.

5.3 NAT Extendido

El mecanismo de NAT anterior no permite la conectividad desde el exterior, por ejemplo, tener un servidor web en la empresa y con acceso desde el exterior.

Imagínese que se desea facilitar acceso a un servidor FTP que está emplazado en el segmento de la red local del dominio privado. Si desde el dominio externo o global se intenta acceder al puerto FTP del servidor, los paquetes serán capturados por el router que da acceso, de tal modo que el servidor FTP inicial no podría ser alcanzado por el dominio externo. Para evitar esta situación lo que se hace es *"publicar"* el puerto FTP del servidor (que se encuentra en el dominio privado) en el router de acceso con otro puerto que queda reservado para este servidor. Para ello habría que establecer la siguiente asociación:

(Dirección Interna, Puerto Interno)→ Puerto Externo

que en el caso de un servidor FTP podría ser:

(192.168.1.21, 21)→ 6400

Así, las conexiones a la dirección pública del router al puerto destino 6400 (el publicado para hacer accesible el servidor FTP), mediante NAT Extendido se traducen a la dirección del propio servidor y al puerto destino 21 (puerto estándar del FTP) haciendo posible la conexión FTP con dicho servidor. De manera análoga se procede si se quisiera hacer públicos los puertos de Telnet de distintas máquinas de la red privada, u otros servicios en los que los paquetes destinados a puertos estándar sean capturados por el router de acceso.

5.4 Manipulación de encabezados IP, TCP, UDP e ICMP

En el modelo NAT, el encabezado IP de todos los paquetes debe ser modificado. Esta modificación incluye la dirección IP (dirección IP origen para paquetes salientes y dirección IP destino para paquetes entrantes) y la suma de control de redundancia cíclica (CRC).

Para las sesiones TCP y UDP, las modificaciones deben incluir la actualización de la suma de control en las cabeceras TCP/UDP. Esto es porque la suma de control de TCP/UDP también contiene las direcciones IP origen y destino. Para los paquetes de petición ICMP tampoco se requieren cambios adicionales en el encabezado ICMP, porque la suma de control en la cabecera ICMP no incluye las direcciones IP.

En el modelo NAT Extendido, las modificaciones en la cabecera IP son similares a las del modelo NAT. Para las sesiones TCP/UDP, las modificaciones deben ser extendidas para incluir la traducción del puerto (puerto origen para paquetes salientes y puerto destino para paquetes entrantes) en la cabecera TCP/UDP. La cabecera ICMP en los paquetes de petición ICMP deben también ser modificados para reemplazar el ID de petición y la suma de control del encabezado ICMP. El ID de petición del host privado debe ser traducido al ID asignado en los salientes y al revés en los entrantes. La suma de control del encabezado ICMP debe ser corregida para contar la traducción del ID de petición.

Las modificaciones del NAT son por paquete y puede ser un cómputo muy intensivo, ello involucra una o más modificaciones a la suma de control, inclusive para traducciones de un sólo campo. Afortunadamente, tenemos un algoritmo, que hace los ajustes a la suma de control para los encabezados IP, TCP, UDP e ICMP muy simple y eficiente. Todos estos encabezados usan una suma de complementos de uno, esto es suficiente para calcular la diferencia aritmética entre el antes de la traducción y el después de la traducción de direcciones y agrega esto a la suma de control.

5.5 Recomendación para el espacio de dirección privado

El RFC 1918 tiene recomendaciones sobre el espacio de dirección asignado para redes privadas. La Autoridad de Números Asignados de Internet (IANA) tiene tres bloques de espacio de dirección IP, llamados 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16 para redes privadas. En la notación CIDR, el primer bloque es sólo un número de dirección de clase A, mientras que el segundo bloque es un conjunto de 16 redes contiguas de clase B, y el tercer bloque es un conjunto de 256 redes contiguas de clase C.

Una organización que decide usar direcciones IP en el espacio de dirección definido anteriormente puede hacerlo sin una coordinación con IANA o con un registro de Internet. El espacio de dirección puede de este modo ser usado privadamente por muchas organizaciones independientes al mismo tiempo, con operaciones NAT habilitadas en sus routers frontera.

5.6 Encaminamiento a través de NAT

El router en el que se ejecuta NAT no debe anunciar el direccionamiento de las redes privadas al backbone. Sólo las redes con direcciones reales pueden ser conocidas fuera de la zona privada. Sin embargo, la información global que recibe NAT desde el router frontera de la zona puede ser anunciada en la zona privada.

Típicamente, el router NAT de la zona tendrá un encaminamiento estático configurado para reenviar todo el tráfico externo al router del proveedor de servicio a través de la conexión WAN, y el router del proveedor de servicio tendrá un encaminamiento estático dinámico.

5.7 Limitaciones de privacidad y seguridad

El NAT tradicional puede ser visto como algo que provee un mecanismo de privacidad, con sesiones unidireccionales desde los hosts privados y donde las direcciones verdaderas de los hosts privados no son visibles para los hosts externos.

La misma característica que brinda privacidad hace la depuración de problemas (incluyendo violaciones de seguridad) potencialmente más difícil. Si un host en una red privada está abusando de Internet de alguna manera (como tratando de atacar a otra máquina o enviando grandes cantidades de spam) es más difícil rastrear el origen actual de trastorno porque la dirección IP de los host es ocultada en un router NAT.

5.8 Traducción de paquetes salientes fragmentados TCP/UDP en configuración NAT Extendido

La traducción de fragmentos TCP/UDP en una configuración NAT extendida están condenados a fallar. La razón es la siguiente: sólo el primer fragmento contiene el encabezado TCP/UDP que sería necesario para asociar el paquete a una sesión para propósitos de traducción. Los fragmentos subsecuentes no contienen información del puerto TCP/UDP, simplemente llevan el mismo identificador de fragmentación que el especificado en el primer fragmento.

5.9 Implementaciones actuales

Muchas implementaciones comerciales que se adhieren a la descripción NAT provista en este documento están disponibles en la industria. El software de dominio público Linux contiene NAT bajo el nombre de "Enmascaramiento IP" (IP Masquerading). El software de dominio público FreeBSD tiene la implementación NAPT corriendo como un demonio.

Tanto el software Linux como el FreeBSD son libres, pero puede comprar los CD-ROMs de estos por mucho menos del costo de distribución. También están disponibles on-line desde muchos sitios FTP con los últimos parches.

5.10 Desarrollo práctico

5.10.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers NUCLEOX PLUS.
- 2 PC’s que funcionarán como clientes.
- 2 hubs.
- 2 latiguillos directos, para conectar cada PC al hub.
- 1 cable RS-232 DB25 punto a punto para conectar los 2 routers NUCLEOX PLUS, desde el puerto 1(DTE) de uno hasta el puerto 2 (DCE) del otro.

A continuación procedemos a montar la red según la siguiente topología:

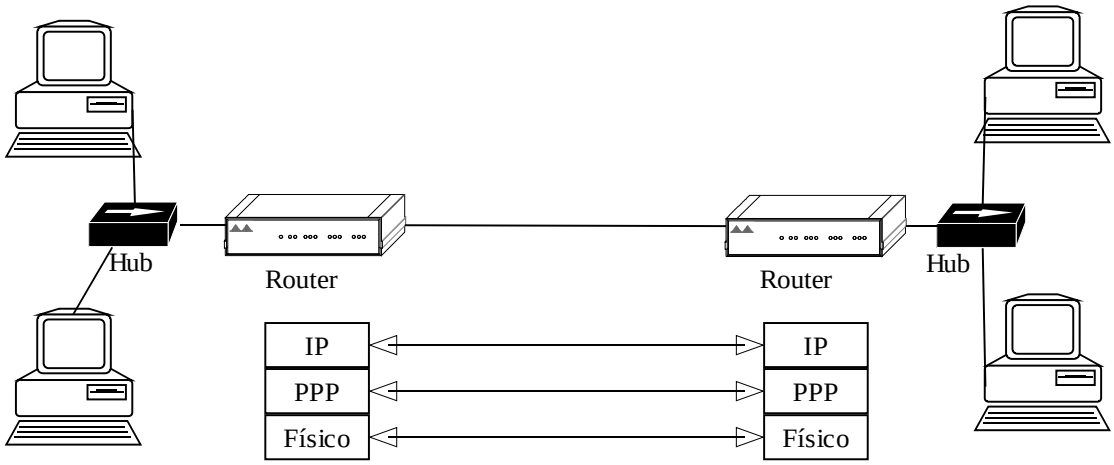

Figura 5.2: Topología de red

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con red física en la que se encuentren.

5.10.2 NAT

Aquí muchas direcciones locales son trasladadas en una misma dirección global. El problema principal de este tipo de NAT es que muchos servicios sólo aceptan conexiones provenientes de puertos privilegiados para así asegurar que no provienen de cualquier usuario. Otra limitación es que las conexiones entrantes no están permitidas.

En el router NUCLEOX PLUS existe una implementación de NAT que ***solo se puede utilizar para interfaces PPP***.

Para habilitar el NAT, simplemente utilizamos el comando **ENABLE NAT**, dentro de la configuración del interfaz PPP.

```
PPP Config>ENABLE NAT
PPP Config>
```

5.10.3 Comprobación

Una vez montada una red con el siguiente aspecto:

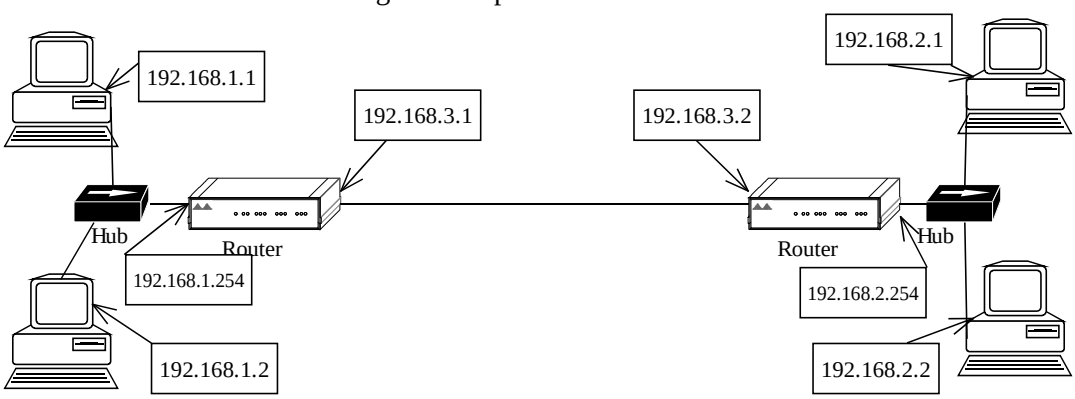

Figura 5.3: Topología de red con direcciones IP

1. Abrimos el Ethereal en los PCs con IPs 192.168.2.1 y 192.168.1.1.

2. Seguidamente procedemos a hacer un PING desde el PC con IP 192.168.1.1 hasta el PC con IP 192.168.2.1

3. Observamos en el PC con IP 192.168.1.1 las tramas capturas:

    a. Tramas emitidas: IPSource=192.168.1.1; IPDestination=192.168.2.1
    b. Tramas recibidas: IPSource=192.168.3.2; IPDestination=192.168.1.1

4. Las tramas capturas en el PC con IP 192.168.2.1:

    a. Tramas recibidas: IPSource=192.168.3.1; IPDestination=192.168.2.1
    b. Tramas emitidas: IPSource=192.168.2.1; IPDestination=192.168.3.1

Capítulo 6
Voz sobre IP

6.1 Introducción

La convergencia de las redes de telecomunicación actuales busca una tecnología que permita transmitir en la misma línea la voz y los datos. Esto obliga a establecer un modelo o sistema que permita empaquetar la voz para que pueda ser transmitida junto con los datos. Desarrollar una tecnología de ámbito mundial con este objetivo nos dirige claramente al protocolo IP y a encontrar el método que nos permita transmitir voz a la vez que datos sobre ese protocolo. El problema tiene una sencilla solución: VoIP (Voice over Internet Protocol).

Algo tan sencillo, en principio, no lo es en la realidad y para comprobarlo sólo hay que repasar la evolución que han sufrido los distintos desarrollos comerciales y los distintos estándares.

Aunque son conocidas distintas investigaciones en algoritmos avanzados de digitalización de voz desde 1970 y distintas experiencias de transmisión de voz sobre redes locales (LAN) en los años 80, es en febrero de 1995 cuando la empresa VocalTec da el pistoletazo de salida mostrando a través de su producto Internet Phone las posibilidades reales de establecimiento de llamadas telefónicas de PC a PC. Se utilizaba entonces un paquete de software instalado en el PC y como medio de transmisión Internet. Nacía así el término hoy acuñado como Telefonía IP.

En 1996 se dan las primeras experiencias de establecimiento de llamadas de Teléfono a PC y de Teléfono a Teléfono. A partir de 1997 empiezan a aparecer nuevos dispositivos y métodos que nos han llevado hoy en día a mantener el término XoIP (‘X’ over Internet Protocol) como la verdadera opción de futuro, o si se prefiere como la puerta hacia la convergencia de las redes. En este acrónimo, X significa cualquier contenido susceptible de ser transmitido por una red (D = data, V = voz, F = fax, M = multimedia, etc).

Es preciso definir de una forma simple y clara la situación actual para que a partir de este momento se puedan identificar claramente tanto los términos como los elementos que de alguna u otra forma intervienen en los distintos niveles del desarrollo de la convergencia de redes. Términos que posiblemente identifican el camino hacia los servicios de VoIP:

- Telefonía: servicios de telecomunicación prestados sobre la Red Telefónica Conmutada (RTC) ya sea Red Telefónica Básica (RTB) o Red Digital de Servicios Integrados (RDSI).
- Voz en Internet: servicios de telefonía prestados sobre la red pública global formada por la interconexión de redes de conmutación de paquetes basadas en IP.
- Voz sobre IP (VoIP): servicios de telefonía prestados sobre redes IP "privadas" sin interconexión a la RTC
- Telefonía IP: servicios de telefonía prestados sobre Redes IP "privadas" en interconexión con la RTC.
- Voz sobre Frame Relay (VoFR): servicios de telefonía prestados sobre redes soportadas por circuitos Frame Relay, orientados a la transmisión de datos.
- Voz sobre ATM (VoATM): servicios de telefonía prestados sobre redes ATM donde existe posibilidad de ofrecer una calidad de servicio (QoS).
- Multimedia sobre IP (MoIP): servicios multimedia (vídeo, audio, imagen, etc) prestados sobre redes IP
- Fax sobre IP (FoIP): servicios de transmisión de fax prestados sobre redes IP.

6.2 Telefonía IP frente a la telefonía tradicional

Aunque la telefonía IP aprovecha la infraestructura de telecomunicaciones ya existente, para su correcto funcionamiento necesita nuevos elementos. La telefonía IP necesita un elemento que se encargue de transformar las ondas de voz en datos digitales y que además los divida en paquetes susceptibles de ser transmitidos haciendo uso del protocolo IP. Este elemento es conocido como procesador de señal digital (DSP), el cual está integrado en los teléfonos IP o en los propios gateways encargados de transmitir los paquetes IP una vez paquetizada la voz. Cuando los paquetes alcanzan el gateway de destino se produce el mismo proceso a través del DSP pero a la inversa, con lo cual el receptor podrá recibir la señal analógica correspondiente a la voz del emisor.

El verdadero problema es que la telefonía conmutada establece circuitos dedicados entre el origen y el destino y ahí la calidad es innegable y segura. Por el contrario, la transmisión de voz sobre IP comparte el circuito y el ancho de banda con los datos, y los paquetes pueden atravesar multitud de nodos antes de llegar a su destino, lo que supone lógicas deficiencias en la transmisión de paquetes de voz (retardos y lo que es más grave, variaciones de retardo).

6.2.1 Muestreo digital

Aunque la comunicación analógica es la ideal para la comunicación humana, la transmisión analógica no es ni robusta ni eficaz para recuperarse del ruido de línea. En las primeras redes de telefonía, cuando se pasaba una transmisión analógica a través de los amplificadores para aumentar la señal, no sólo se incrementaba la voz, sino también el ruido de la línea.

La tecnología digital es mucho más robusta frente al ruido. Por tanto, cuando se generan las señales analógicas a partir de muestras digitales, se mantiene un sonido limpio. Cuando las ventajas de esta representación digital se hicieron evidentes, la red telefónica migró a la modulación por impulsos codificados (PCM).

La PCM convierte el sonido analógico en formas digitales muestreando el sonido analógico 8.000 veces por segundo y convirtiendo cada muestra en un código numérico. El teorema de Nyquist afirma que si se muestrea una señal analógica a una velocidad dos veces superior a la frecuencia de interés más alta, se puede reconstruir de nuevo de manera exacta esa señal en su forma analógica. Como la mayoría del contenido de voz está por debajo de 4.000 Hz (4 KHz), se requiere una velocidad de muestreo de 8.000 veces por segundo (125 ms entre muestras). En telefonía cada muestra tiene 8 bits, lo que nos da una velocidad de 64 Kbps (8 bits x 8.000 Hz = 64.000 bps).

6.2.2 Detección de la actividad de la voz (VAD)

En conversaciones de voz normales, uno habla y el otro escucha. Las redes de voz actuales contienen canales bidireccionales, de 64 Kbps, con independencia de si alguien está hablando o no. Esto significa que en una conversación normal se deja de utilizar, por lo menos, el 50% del total del ancho de banda. En realidad, la cantidad de ancho de banda que se pierde puede ser mayor si se toma un muestreo estadístico de las interrupciones y pausas de los patrones normales de voz en una persona.

Al utilizar VoIP, se puede utilizar este ancho de banda perdido para otros propósitos cuando está habilitada la detección de la actividad de voz (VAD, Voice Activity Detection). La VAD funciona detectando la magnitud de la voz para decidir cuando se debe comenzar a entramar la voz.

Normalmente, cuando la VAD detecta una disminución de la amplitud de la voz, espera un tiempo determinado antes de dejar de poner tramas de voz en paquetes. Este tiempo determinado se conoce como “hangover” y suele ser de 200 ms.

Sin embargo, la VAD padece determinados problemas a la hora de determinar cuando finaliza y empieza la voz, y a la hora de distinguir la voz de un ruido de fondo. Esto significa que si se está en un espacio ruidoso, la VAD es incapaz de distinguir la voz y el ruido de fondo.

6.2.3 Conversión digital a analógico

Los problemas de conversión de digital a analógico (D/A) abundan también en las redes de voz. A pesar de que todas las redes de backbone telefónico en los países del primer mundo son digitales, a veces ocurren conversiones D/A múltiples.

Cada vez que una conversión pasa de lo digital a lo analógico y viceversa, la voz o forma de onda es menos fiel a la forma original. Aunque las redes RTC actuales pueden manejar por lo menos siete conversiones D/A antes de que la calidad de voz se vea afectada, la palabra comprimida es menos robusta frente al ruido debido a esas excesivas conversiones.

6.3 Protocolos de transporte

Debido a la naturaleza sensible al tiempo del tráfico de voz, el protocolo UDP fue la elección lógica para transportar la voz. Sin embargo, se necesitaba más de lo que ofrecía UDP. Por tanto, para el tráfico en tiempo real o sensible al retraso, el Internet Engineering Task Force (IETF) adoptó el RTP (Real Time Protocol). VoIP se encapsula en la parte superior del RTP, que se encapsula a su vez en la parte superior del UDP. Por tanto, VoIP es transportado con una cabecera de paquete RTP/UDP/IP.

El RTP es el protocolo estándar para transmitir tráfico sensible al retraso en las redes basadas en conmutación de paquetes. RTP da a las estaciones receptoras información que no está en los protocolos UDP/IP. Como muestra la figura adjunta, dos campos de información importantes en la cabecera RTP son el Número de Secuencia y la Marca de Temporización. RTP utiliza la información de secuencia para determinar si los paquetes están llegando en orden, y la información de marca de temporización para determinar el tiempo de llegada entre paquetes. RTP consta de una parte de datos y una parte de control, ésta última se llama protocolo de control RTP (RTCP).

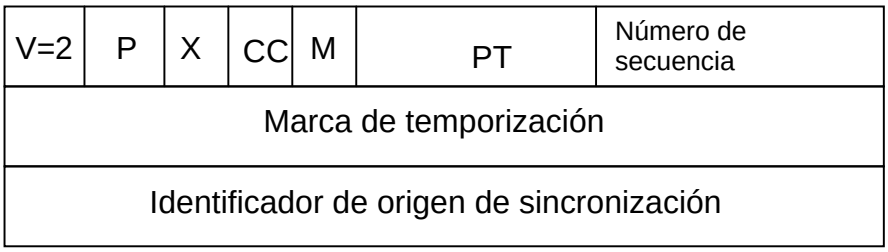

Figura 6.1: Cabecera RTP

La parte de datos de RTP es un protocolo limitado que proporciona soporte para aplicaciones con propiedades de tiempo real, como medios continuos (audio y video), incluida la reconstrucción de la temporización, la detección de pérdidas y la identificación de contenidos.

La utilización de RTP es importante para el tráfico en tiempo real, pero existen algunos inconvenientes. Las cabeceras RTP/UDP/IP tienen 8, 12 y 20 bytes, respectivamente, aunque se puede comprimir a 2 ó 4 bytes utilizando la compresión de cabecera RTP (CRTP).

6.4 Recomendación H.323

La recomendación H.323 nos proporciona el estándar necesario para que la evolución de la voz sobre IP sea común entre los diversos fabricantes. De esta forma los usuarios no deben preocuparse por problemas de compatibilidad. Esta especificación aprobada en 1996 por el ITU (International Telecommunications Union) y revisada en enero de 1998, tiene como objetivo definir un estándar para las comunicaciones multimedia sobre redes que no aseguran calidad del servicio.

Como logros principales de esta recomendación podemos señalar:

- La estandarización de los protocolos permite a los diversos fabricantes evolucionar en conjunto.
- Los usuarios no deben preocuparse sobre el ancho de banda disponible por su interlocutor, existiendo una negociación de las capacidades de cada punto de la línea.
- Debido al uso del protocolo IP, es independiente del tipo de red física que lo soporta, permitiendo la integración con las grandes redes IP actuales.
- La negociación previa permite conectar terminales de muy diversas características, como pueden ser teléfonos de voz, consolas de videoconferencia, ordenadores, etc.

6.4.1 Arquitectura

La recomendación H.323 determina como parte integrante de la comunicación tres bloques: terminales, gatekeepers y gateways.

6.4.1.1 Terminales

Como terminales, debemos entender el equivalente a los teléfonos actuales. Este punto es el que más diferencias puede ofrecer al usuario final.

El funcionamiento de todo terminal debe incluir el tratamiento necesario de la señal para su envío por la red de datos. Deben realizar la captación, digitalización, y compresión de la señal.

Existen principalmente dos tendencias en este tipo de elementos, terminales hardware y terminales software:

- Tanto la apariencia, como la funcionalidad de cara al usuario de los terminales hardware es igual a los teléfonos actuales. Esto permite eliminar la desconfianza inicial que puede producir el cambio. Ya existen en el mercado terminales que se conectan directamente a la red local (LAN).
- Por otro lado los terminales software, no son más que programas ejecutándose en nuestro ordenador personal. Puede producir un mayor rechazo inicial en el usuario, pero las capacidades del software pueden ser muy superiores a las aprotadas por una solución hardware.

Un terminal software, sin un incremento de costes importante, puede ofrecer al usuario características muy diversas, entre las que podemos señalar:

- Agenda compartida y personal enlazada a sistemas estándar como por ejemplo LDAP.

- Buzón de voz con características de programación muy superiores a las actuales.
- Manejo remoto del propio equipo con realización de tareas automáticas.
- Organizador de llamadas.
- Rellamada automática.
- Funciones de reconocimiento de voz.

6.4.1.2 Gatekeepers

Los gatekeepers deben sustituir a las actuales centralitas telefónicas, aunque normalmente se trata de una solución software. En realidad pueden convivir perfectamente con ellas si la configuración de la red así lo determina.

Dentro del esquema de Voz sobre IP, la funcionalidad principal que debe ofrecer todo gatekeeper se basa en el control de llamadas y gestión del sistema de direccionamiento. Este conjunto de tareas puede ser el más importante de todo el sistema.

Aunque los terminales pueden conectarse directamente sin intervención del gatekeeper, este tipo de funcionamiento es muy limitado. La potencia real del sistema se pone de manifiesto cuando dentro de cada zona H.323 existe el correspondiente gatekeeper. Todo terminal debe registrarse primero en una base de datos del gatekeeper. De esta forma desaparecen problemas de movilidad de los diversos puestos y usuarios. Incluso los distintos terminales pueden obtener direcciones dinámicas mediante DHCP (Dynamic Host Configuration Protocol). Este registro permite realizar la traslación antes señalada entre los identificadores de usuario y su localización física de forma automática.

Es responsabilidad del gatekeeper mantener un control de todo el tráfico generado por las diversas comunicaciones, a efectos de mantener un nivel aceptable de saturación de la red. El control de ancho de banda permite al administrador fijar un límite de utilización, por encima del cual se rechazan las llamadas.

En cuanto a otras capacidades añadidas, podemos pensar en el control de costes de llamadas, control de centros de atención al cliente, etc.

6.4.1.3 Gateways

Como último elemento del sistema nos encontramos con el eslabón de unión con toda la telefonía actual. Los gateways permiten que toda llamada dirigida a la red telefónica conmutada pueda establecerse sin intervención directa del usuario. Realmente todo el funcionamiento se produce de una forma totalmente transparente en ambos sentidos, pudiendo recibir y emitir llamadas directamente desde nuestro terminal hacia la RTC sin ningún problema.

6.5 Conjunto del protocolo H.323

El conjunto del protocolo H.323 está dividido en tres áreas de control principales:

- Señalización de registro, admisiones y estado (RAS). Proporciona un control de prellamadas en las redes basadas en gatekeeper H.323. El registro es el proceso que permite que los gateways alcancen una zona H.323 e informen al gatekeeper de sus direcciones IP, es un proceso necesario que ocurre antes de que se intente realizar ninguna llamada. Los mensajes de admisión entre puntos finales y gatekeepers proporcionan las bases para la admisión de llamadas y control de ancho de banda. Los gatekeepers autorizan el acceso a las redes H.323 confirmando o rechazando una petición de admisión. El gatekeeper puede utilizar el canal RAS para obtener

información de estado de un punto final, por ejemplo averiguar si el punto final está en línea o no, debido a una condición de fallo.

- Señalización de control de llamadas. Se utiliza para conectar, mantener y desconectar llamadas entre puntos finales. Los procedimientos de control de llamadas se basan en la recomendación H.225 de la ITU-T, que especifica la utilización y soporte de los mensajes de señalización Q.931. El canal de control de llamadas se crea en el puerto 1720 del protocolo TCP.

- Control y transporte de medios. Los mensajes de control de medios se transportan en un canal seguro H.245, mientras que el transporte de medios se realiza a través del protocolo RTP. RTCP (la parte de control de RTP) monitoriza la entrega de datos, y controla e identifica los servicios.

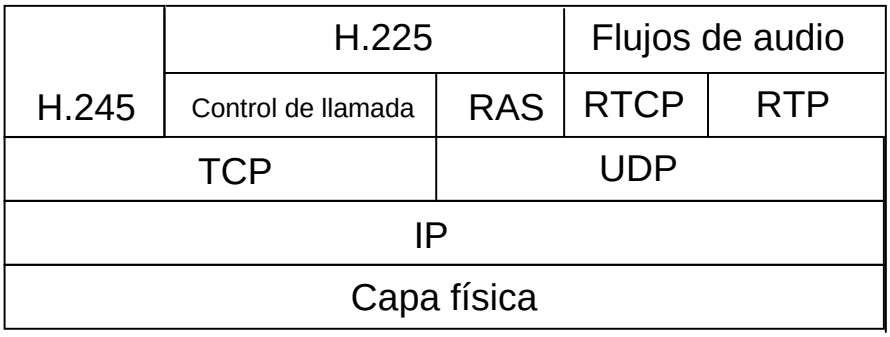

Figura 6.2: Capas del conjunto del protocolo H.323

6.6 Calidad

6.6.1 Retraso/Latencia

El retraso o latencia en VoIP se caracteriza por el tiempo que tarda la voz en salir del terminal del que está hablando hasta llegar al terminal del que está escuchando.

Existen tres tipos de retraso que son inherentes a las redes de telefonía actuales: retraso de serialización, retraso de propagación y retraso de manejo. El retraso de serialización es la cantidad de tiempo que se tarda en colocar un bit o byte en un interfaz. Su influencia en el retraso es relativamente pequeña. Por ejemplo, para rellenar una celda ATM de 53 bytes se requieren 2,72 μs ($2{,}72.10^{-6}$ s).

La luz viaja a través del vacío a una velocidad de 300.000 kilómetros por segundo y los electrones viajan a través del cobre a unos 200.000 kilómetros por segundo. Una red de cobre alrededor del mundo (21.000 kilómetros) induce un retraso de sentido único de unos 70 milisegundos que puede provocar una degradación apreciable de la voz.

Los dispositivos que envían tramas a través de la red provocan un retraso de manejo. Los retrasos de manejo pueden tener impacto en las redes telefónicas tradicionales, pero esos retrasos son un problema mayor en los entornos de paquetes. El DSP (Procesador Digital de Señal) genera una muestra de voz cada 10 ms cuando se utiliza G.729. Dos de esas muestras de voz (ambas con 10 ms de retraso) se colocan dentro de un paquete. El retraso de paquete es, por tanto, de 20 ms. Cuando se utiliza G.729, se produce un look-ahead inicial de 5 ms, lo que supone un retraso inicial de 25 ms para la primera trama de voz. Los fabricantes pueden decidir cuantas muestras de voz quieren enviar en un paquete. Como G.729 utiliza muestras de voz de 10 ms, cada incremento en las muestras por trama aumenta el retraso en 10 ms.

Una red basada en paquetes sufre, además, retrasos por otras razones. Dos de estas razones son el tiempo que se necesita para mover un paquete hasta la cola de salida y el retraso de la gestión de colas. Cuando los paquetes se guardan en una cola, debido a la congestión en una interfaz de salida, el resultado es un retraso en la gestión de colas. Este tipo de retrasos ocurre cuando se envían más paquetes que los que la interfaz puede manejar en un intervalo de tiempo dado.

6.6.2 Variación del retardo

La variación del retardo (jitter) es la variación del tiempo de llegada de un paquete. Es un problema que existe sólo en las redes basadas en conmutación de paquetes y es debido al retardo de gestión en las colas de salida de los nodos. Cuando se está en un entorno de voz por paquetes, el remitente espera transmitir de forma fiable paquetes de voz en un intervalo regular. Esos paquetes de voz se pueden retrasar por toda la red de paquetes y no llegar con el mismo intervalo de tiempo regular a la estación receptora. La diferencia entre el tiempo en que se esperaba recibir el paquete y cuando se recibe en realidad es lo que se llama variación del retardo. Éste es el parámetro fundamental para controlar la correcta recepción de la voz.

6.6.3 Compresión de voz

Un método de compresión utilizado a menudo es la modulación por impulsos codificados diferencial y adaptable (ADPCM, Adaptative Differential Pulse Code Modulation). Un ejemplo de utilización común de la ADPCM es la ITU-T G.726, que codifica utilizando muestras de 4 bits, lo que da una velocidad de transmisión de 32 Kbps. A diferencia de la PCM, los 4 bits no codifican directamente la amplitud de la voz, sino que codifican las diferencias de la amplitud entre dos muestras consecutivas, así como la velocidad de cambio de esa amplitud, empleando alguna predicción lineal rudimentaria.

La ITU-T normalizó los esquemas de codificación CELP, MP-MLQ PCM y ADPCM en sus recomendaciones de la serie G. Entre los estándares de codificación más populares para telefonía y voz por paquetes se incluyen:

- G.711. Describe la técnica de codificación de voz de PCM de 64 Kbps subrayada anteriormente; la voz codificada con G.711 está en un formato correcto para la entrega de voz digital en la red telefónica pública o a través de intercambio privado de tramas (PBX).
- G.726. Describe la codificación de ADPCM a 40, 32, 24 y 16 Kbps; también se puede intercambiar voz ADPCM entre voz por paquetes y telefonía pública o redes PBX, suponiendo que estas últimas tienen la capacidad ADPCM.
- G.729. Describe la compresión CELP que permite que la voz sea codificada en flujos de 8 Kbps.
- G.723.1. Describe una técnica de compresión que se puede utilizar para comprimir voz u otros componentes de señales de audio de servicios multimedia a una baja velocidad de bit.

En la tabla se muestra la relación existente entre los distintos algoritmos de compresión de voz utilizados y el ancho de banda requerido por los mismos:

Codecs	Ancho de Banda
G.711 PCM	64 Kbps
G.726 ADPCM	16, 24, 32, 40 Kbps
G.727 E-ADPCM	16, 24, 32, 40 Kbps
G.729 CS-ACELP	8 Kbps
G.728 LD-CELP	16 Kbps
G.723.1 CELP	6.4/5.3 Kbps

Tabla 6.1: Codecs de compresión

6.6.4 Eco

Oir la propia voz en el auricular mientras se está hablando es común y tranquilizador para la persona que está hablando. Oir la propia voz después de un retraso de unos 25 ms puede provocar interrupciones y romper la cadencia de la conversación. En una red de voz tradicional, el eco está normalmente provocado por un desajuste en la impedancia entre los cuatro cables del terminal y el bucle local de dos cables. En la red pública de telefonía conmutada, el eco está regulado con canceladores de eco y un firme control sobre los desajustes de la impedancia en los puntos de conversión de 2 a 4 hilos.

El eco tiene dos inconvenientes: puede ser alto y puede ser largo. Cuando más alto y largo es el eco, más incomodo resultará. Las redes telefónicas, en aquellas partes del mundo donde se utiliza principalmente la voz analógica, emplean supresores de eco, que eliminan el eco tapando la impedancia en un circuito. Éste no es el mejor mecanismo que se puede utilizar para eliminar el eco y, de hecho, provoca otros problemas.

En las actuales redes digitales, se pueden construir canceladores de eco mediante DSP´s. Imaginemos en este ejemplo que el usuario A está hablando con el usuario B. La voz del usuario A hacia el usuario B se llama G. Cuando G impacta con un desajuste de impedancia u otro entorno causante del eco, se refleja de nuevo hacia el usuario A. El usuario A puede oír el retraso varios milisegundos después de que haya hablado. Para eliminar el eco de la línea, el dispositivo a través del cual está hablando el usuario A guarda una imagen inversa de las palabras durante un cierto tiempo. Es lo que se llama voz inversa. Este cancelador de eco oye el sonido que viene del usuario B y sustrae –G para eliminar todo el eco.

6.7 Ventajas e inconvenientes

En esta sección se analizan por separado tanto las ventajas como los inconvenientes del uso de los servicios VoIP en los ámbitos más comunes. Así mismo se analizan los aspectos más relevantes que impiden una rápida implantación de estos servicios:

6.7.1 Ventajas

Los servicios de VoIP presentan una multitud de ventajas en todos los aspectos:

1. Amplia reducción en los costes de la factura telefónica. Los costes de todo tipo de llamadas se equipararán al de una llamada local de forma que la reducción en los costes del tráfico de voz será a todas luces muy importante.

2. Nuevas posibilidades de marketing directo y potenciación del servicio de atención al cliente. Podrán implantar la filosofía "Push 2 Talk" que consiste en un icono situado en una página Web a través del cual un navegante podrá dialogar con personal especializado de la compañía mientras continúa navegando por la red.

3. Potenciación del teletrabajo y de los teletrabajadores. Con una única conexión se podrá acceder a aplicaciones corporativas, al correo vocal, atender llamadas o buscar información sobre nuevos proyectos.

6.7.2 Inconvenientes

Si todo está tan claro, si ya existe tecnología, si los estándares están validados por organismos internacionales (caso del H.323 definido por la ITU), si la ley en principio no presenta inconvenientes y si además las consultoras internacionales presentan esta solución como la verdadera alternativa de negocio en el año 2005, la lógica hace pensar que la implantación de VoIP se realizará de forma inmediata. Pero el verdadero caballo de batalla se resume con tres letras: "QoS".

Garantizar calidad de servicio en base a retardos y ancho de banda disponible en una red IP no es nada fácil. Una vez digitalizada la voz y paquetizada, se envía al canal de transmisión y aquí no existen soluciones que nos garanticen o permitan establecer anchos de banda, orden de paquetes y retrasos asumibles en su transmisión. Las posibles soluciones pasan por diferenciar los paquetes de voz de los paquetes de datos, priorizar la transmisión de los paquetes de voz y hacer que los retrasos añadidos a la transmisión de los paquetes no superen en ningún caso los 150 milisegundos (recomendación de la ITU).

Las líneas de trabajo actuales de cara a conseguir calidad de servicio en una transmisión IP, están basadas en:

- Supresión de silencios y VAD (voice activity detection).
- Compresión de cabeceras.
- Reserva de Ancho de Banda: implantación del estándar RSVP (Protocolo de Reserva de Recursos) de la IETF (Internet Engineering Task Force).
- Priorizar: existen diferentes tendencias tales como:
    1. CQ (Custom Queuing): asignación de un porcentaje del ancho de banda disponible.
    2. PQ (Priority Queuing): establecer prioridad en las colas.
    3. WFQ (Weight Fair Queuing): asignar prioridad al tráfico de menos carga.
    4. DiffServ: definido en borrador por la IETF, evita tablas en routers intermedios y establece decisiones globales de rutas por paquete.
- Control de Congestión: uso del protocolo RED (Random Early Discard), técnica que fuerza descartes aleatorios

6.8 Desarrollo práctico

- Voz sobre IP a través de un interfaz serie Frame-Relay.
- Voz sobre IP a través de un interfaz LAN Ethernet.

6.8.1 Voz sobre IP a través de un interfaz serie Frame-Relay

6.8.1.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers Nucleox Plus.
- 2 PC's que funcionarán como clientes.
- 2 latiguillos directos.
- 2 hubs.
- 1 cable RS-232 DB25 punto a punto para conectar los 2 routers NUCLEOX PLUS, desde el puerto 1(DTE) de uno hasta el puerto 2 (DCE) del otro.
- 2 teléfonos analógicos.
- 2 latiguillos telefónicos, interfaz RJ-11.

A continuación procedemos a montar la red según la siguiente topología:

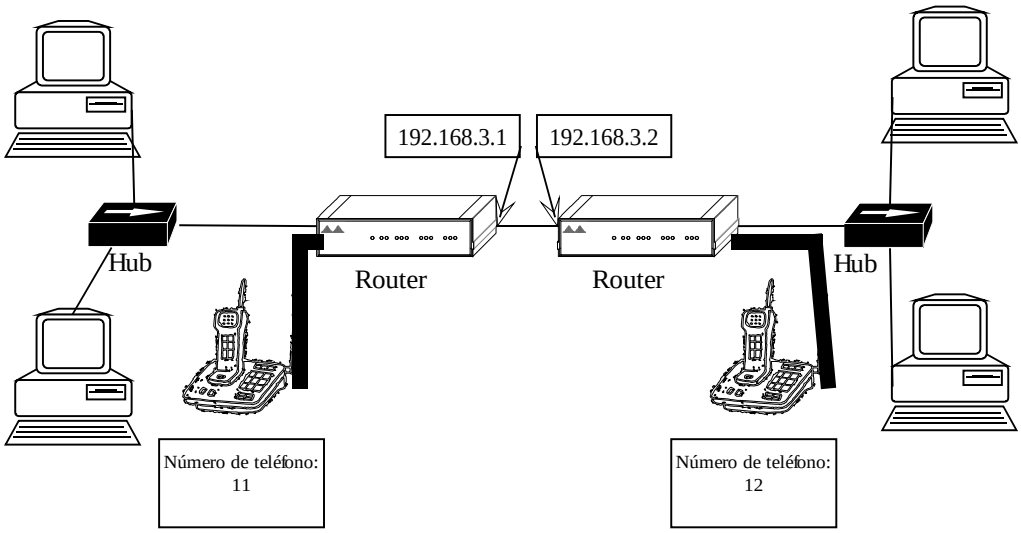

Figura 6.3: Voz sobre IP a través de un interfaz Frame-Relay

6.8.1.2 Configuración Frame-Relay

La comunicación entre los dos routers Nucleox Plus será a través de Frame-Relay. Por lo que en primer lugar se realizará todo el proceso necesario para la configuración de Frame Relay a través de un interfaz serie (vista en el capítulo 4).

6.8.1.3 Configuración de Voz sobre IP

Para entrar en la configuración del protocolo H.323 (Voz sobre IP), se accederá desde el menú principal de la siguiente forma:

1. En el prompt (*), teclee **PROCESS 4** (o P 4).
2. En el prompt de configuración (Config>), teclee **PROTOCOL H323** o **PROTOCOL 4**, o bien **P 4**.

Si desea borrar toda la configuración de H323 sin perder el resto de la configuración del equipo lo puede hacer con el comando **CLEAR H323** desde el prompt Config>.

```
Config> CLEAR H323
Config of H323 will be DELETED
Continue clearing? (Yes/No)? y
Config>
```

El Nucleox Plus soporta dos codecs de compresión, el G.729 y el G.723.1. Los dos codecs proporcionan un compromiso entre calidad y velocidad. La mejor calidad se obtiene con G.729,

que trabaja a 8 Kbps. G.723.1 puede trabajar a 6,4 y 5,3 Kbps y proporcionan una calidad de voz ligeramente inferior a la obtenida con el G.729.
Una vez comprimida la voz, se entregan a la CPU principal, en forma secuencial, tramas de longitud fija. La longitud y cadencia de estos paquetes en función de la norma empleada son:

G.729: 10 octetos cada 10 ms.
G.723.1 a 6,4 Kbps: 24 octetos cada 30 ms.
G.723.1 a 5,3 Kbps: 20 octetos cada 30 ms.

Posteriormente es la CPU principal la que se encarga del transporte de las tramas de voz sobre la pila IP. Cada paquete puede contener una o más tramas de voz, lo que es configurable. Si se encapsula más de una trama de voz en un paquete IP, el ancho de banda requerido para el flujo de voz es más bajo ya que varias tramas de voz comparten las cabeceras RTP/UDP/IP. El ahorro de ancho de banda puede no merecer la pena si se está utilizando algoritmos de compresión de cabeceras tales como CRTP.

Para conseguir una calidad de voz adecuada, esos paquetes deben tratar de ser entregados en el destino con el mismo orden y cadencia con que se generaron en el origen. Con el fin de minimizar la posible pérdida de alguna de esas muestras de voz, los algoritmos de compresión utilizan técnicas de interpolación para regenerar las muestras perdidas. Asimismo, y dado que el tiempo de propagación de un datagrama por la red no es fijo, (al contrario que en una red de conmutación de circuitos), los paquetes se van almacenando en un pequeño buffer y entregando posteriormente de forma secuencial de la forma más parecida posible a como fueron generados (cada 10 ms o 30 ms, según el codec empleado). Esto produce un cierto retardo en la voz, siempre tolerable dentro de unos límites, pero permite compensar los retardos introducidos por la red, y el jitter (variación de este retardo).

El comando **ADD ADDRESS** permite agregar una entrada a la tabla de asignación de números de teléfono a direcciones IP. Se utiliza para saber cómo acceder a un número de teléfono remoto. Además permite elegir el tipo de codec, VAD (Voice Activity Detection) y NOB (Número de tramas de voz por paquete RTP) a utilizar. El orden de aparición en la tabla es importante dado que se procesan de acuerdo con éste. Una vez que encuentra una entrada que se ajusta, deja de comprobar las siguientes. Para el router de la izquierda hay que ejecutar:

```
H323 Config> ADD ADDRESS
Telephone number? 12
Digits to Strip[0]?
Dial-Out Prefix?
IP address: [0.0.0.0]? 192.168.3.2
Codec-class Id[0]?
Tech-prefix[]?
H323 Config>
```

- *Telephone number:* Dígitos sobre los que se decide elegir una dirección IP. Puede ser el número de teléfono completo o sólo los primeros dígitos de acuerdo a un plan de numeración dado. Como máximo acepta 15 dígitos (0 a 9).
- *Digits to strip:* Número de dígitos del número de teléfono recibido que se eliminan empezando por la izquierda (prefijos). Admite valores entre 0 y 15.
- *Dial-out prefix:* Dígitos usados como prefijo del número resultante de aplicar el borrado del campo anterior sobre el número de teléfono solicitado. Admite hasta 15 dígitos (0 a 9).
- *IP address:* Dirección IP a la que se realizará la llamada.
- *Codec-class:* Identificador de la clase de codec a utilizar con ese destino. Esta clase define el codec, uso del VAD y el NOB de la llamada.
- *Tech-Prefix:* Prefijo tecnológico usado al realizar la llamada. Este campo sólo tiene sentido cuando el equipo opera bajo el control de un gatekeeper. Si no se especifica se

utiliza por defecto el prefijo asociado al gateway. Admite una cadena de caracteres de longitud máxima 11. Cadenas más largas se truncan a 11 caracteres.

Si se incluyen dos entradas en las que son exactamente iguales la dirección IP y el número de teléfono se da un mensaje de error. Por el contrario, se permite agregar una segunda entrada en la que coincida exactamente el número de teléfono: en este caso la segunda entrada se utiliza como dirección IP alternativa para acceder al teléfono remoto caso de que no se pueda acceder a la primera.

Con esta configuración al llamar al número 12 desde el gateway de la izquierda se realizará la llamada a la dirección IP 192.168.3.2 al numero de teléfono 12, utilizando el codec, VAD y NOB por defecto de la línea, que son los siguientes:

- Codec: G.723.1 a 5,3 Kbps.
- NOB: una muestra de voz por paquete RTP.
- VAD deshabilitado.

El comando **ADD LINE** agrega una entrada a la tabla de líneas. Esta tabla asocia número de teléfono a interfaces físicas del equipo (los Nucleox Plus disponen de 4 interfaces analógicos). Al recibirse una llamada se busca la interfaz a partir del número llamado y si se encuentra en la tabla se encamina la llamada hacia esa línea. En el caso de que no se encuentre, esté ocupada o esté deshabilitada se buscará una interfaz libre de acuerdo con las prioridades que se hayan configurado. Para el router de la derecha, suponiendo que el teléfono está conectado en el primer interfaz analógico, debemos ejecutar:

```
H323 Config> ADD LINE
Line?[1]? 1
Telephone number? 12
Digits to Strip[0]?
Dial-Out Prefix?
H323 Config>
```

- *Line:* Es el número de la línea a la que se le va a asignar el número de teléfono. Admite valores entre 1 y 4.
- *Telephone number:* Dígitos sobre los que se seleccionará una línea. Puede ser el número completo del teléfono asignado a esa línea o sólo un prefijo. Como máximo acepta 15 dígitos (0 a 9).
- *Digits to Strip:* Número de dígitos del número de teléfono recibido que se eliminan por la izquierda (prefijos). Admite valores entre 0 y 15.
- *Dial-Out Prefix:* Dígitos usados como prefijo del número resultante de aplicar el borrado indicado por el campo anterior sobre el número de teléfono recibido. Admite hasta 15 dígitos (0 a 9).

Con esta configuración al llamar en la dirección IP 192.168.3.2 al numero de teléfono 12, se encaminará hacia el primer interfaz analógico.

También es de gran utilidad utilizar el comando **ADD PREFIX** que permite agregar una entrada a la tabla de prefijos. Estas entradas definen el plan de numeración usado de manera que en función de los primeros dígitos marcados se decide cual es la longitud del número marcado y se indica el momento a partir del cual se inicia el proceso de llamada. En los dos routers debemos ejecutar:

```
H323 Config> ADD PREFIX
Prefix:? 1
Length:[0]? 2
H323 Config>
```

- *Prefix:* Dígitos sobre los cuales se realiza la decisión. Puede se un número completo o un prefijo común de un grupo de teléfonos. Admite hasta 15 dígitos (0 a 9).
- *Length:*. Longitud asignada a ese prefijo. Admite valores entre 1 y 15.

Con esta configuración al marcar como primer digito el número 1 estamos considerando que el número de teléfono va a tener sólo un dígito más, es decir, en total 2 dígitos, y al marcar estos 2 dígitos se iniciará el proceso de llamada.

Estas entradas se pueden obviar utilizando la tecla # del teléfono: cuando el usuario considera que ya ha marcado el número completo deberá marcar # para empezar el proceso de llamada.

El comando **SET GW ADDRESS** configura la dirección IP interna del gateway de voz. Ésta es la dirección IP origen utilizada en todas las tramas relacionadas con Voz sobre IP (tramas de establecimiento de llamada, de capacidades, de voz y de control de los canales de voz). Por defecto tiene el valor 0.0.0.0. Nosotros hemos optado por asignarle la misma dirección que tiene asignada la interfaz Frame-Relay. En el caso del router de la izquierda:

```
H323 Config>SET GW ADDRESS
Internal IP address? 192.168.3.1
H323 Config>
```

Para finalizar utilizaremos el comando **APPLY**. Este comando hace que los parámetros configurados se activen de forma inmediata. Los nuevos parámetros configurados no estarán activos hasta que se use este comando, a excepción de los relativos a las ganancias de volumen, que se activan de forma automática al configurarlos, con el fin de facilitar su ajuste. Los parámetros que se activan dinámicamente al usar el comando **APPLY** son:

- La tabla de asignación de números de teléfono a direcciones.
- La tabla de prefijos.
- La tabla de asignación de números de teléfono a líneas.
- Los temporizadores de tonos.
- Detección de actividad de voz.

6.8.1.4 Evaluación de la calidad

Tras realizar una prueba con 2 conversaciones simultáneas, los mayores problemas que hemos encontrado han sido el eco, el retardo y la variación del retardo (jitter). A continuación vamos a enumerar posibles soluciones a estos problemas.

El Nucleox Plus incorpora un **cancelador de eco**, pero sólo es capaz de funcionar efectivamente cuando la relación señal a eco es mayor o igual que 6 dB.

El único parámetro de configuración que afecta al eco es la ganancia del micrófono, de modo que a menor ganancia mayor relación señal a eco, y por lo tanto mejor funcionamiento del cancelador. La ganancia del altavoz no influye ya que se aplica tanto a la señal como al eco.

Si el eco se percibe en un extremo A de la conversación, el parámetro de la ganancia de micrófono se debe ajustar en el otro extremo B. Esto es debido a que el eco que se produce en el extremo B se transmite por IP al otro extremo de modo que llega con una diferencia temporal apreciable respecto a la señal original y por lo tanto se manifiesta como un eco perceptible.

Para configurar la ganancia del micrófono podemos utilizar el comando **SET LINE MIC-GAIN,** que indica la ganancia de entrada de la línea. Si se percibe una eco considerable,

debemos proceder a disminuir el valor que posee este parámetro, de la forma que se indicó anteriormente. Por defecto tiene el valor de 10 dB, y sus valores pueden variar entre -31 y 31.

```
H323 Config> SET LINE MIC-GAIN
Line?[1]? 1
Input Gain [-31 to 31 dB]: [10]?
H323 Config>
```

Por otra parte, el **retardo**, como se indicó anteriormente, puede ser debido a diversas causas. La más importante es el retardo de manejo, provocado por el DSP al generar muestras de voz según un codec de compresión determinado, y al colocar un determinado número de estas muestras de voz en un paquete.

Los codecs se diferencian por la velocidad a la que trabajan. G.729 trabaja a 8 Kbps, mientras que G.723.1 puede trabajar a 6,4 y 5,3 Kbps y proporcionan una calidad de voz ligeramente inferior a la obtenida con el G.729. Por otra parte, el número de muestras de voz colocadas en un paquete se pueden configurar con el comando **SET GW FRAMES-PACKET.** Este comando configura todas las líneas con el mismo número de tramas de voz por cada datagrama RTP. Aumentar dicho valor significa disminuir el ancho de banda requerido para enviar datos de voz, pero aumenta el retardo entre los mismos. Admite valores entre 1 y 6. Por defecto todas las líneas están configuradas con el valor 1.

```
H323 Config> SET GW FRAMES-PACKET
No of H323Frames/ RTP packet [1 - 6]: [1]? 2
H323 Config>
```

La **variación del retardo**, como se indicó anteriormente, es la variación del tiempo de llegada de un paquete, es decir, la diferencia entre cuando se esperaba recibir el paquete y cuando se recibe en realidad.

El Nucleox Plus, durante el proceso de recepción de las tramas, computa y actualiza de manera contínua el retardo admisible para la correcta reproducción de las tramas de voz, y este cómputo se realiza en función del retardo con el que llega cada trama de voz. La corrección del retardo admisible se realiza hasta que se sobrepasa el máximo retardo admisible, configurado con el comando **SET DELAY**. En cualquier caso, se elimina cualquier trama que llega con un retardo mayor del retardo admisible en curso. Admite valores comprendidos entre 60 y 1000 mseg. Por defecto tiene el valor 300 mseg.

```
H323 Config> SET DELAY
Maximum delay[300]? 400
H323 Config>
```

6.8.2 Voz sobre IP a través de un interfaz LAN Ethernet

6.8.2.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers Nucleox Plus.
- 2 PC’s corriendo bajo el sistema operativo Linux, que funcionarán como clientes.
- 4 latiguillos directos.
- 2 teléfonos analógicos.
- 2 latiguillos telefónicos, interfaz RJ-11.
- 1 hub.

A continuación procedemos a montar la red según la siguiente topología:

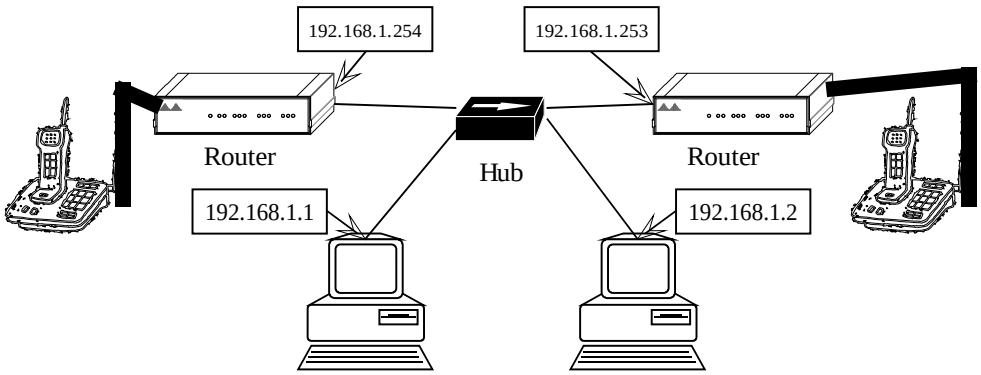

Figura 6.4: Voz sobre IP a través de un interfaz LAN Ethernet

6.8.2.2 Configuración de Voz sobre IP

La configuración de Voz sobre IP se realiza de la misma forma indicada en el apartado anterior.

6.8.3.3 Evaluación de la calidad

La prueba ha consistido en establecer una comunicación de voz sobre IP desde un teléfono, conectado a un gateway, hacia el otro teléfono, conectado al otro gateway. Una vez establecida la comunicación, se ha comenzado a realizar un ftp desde uno de los clientes hacia el otro.

Los resultados obtenidos demuestran que al comenzar a realizar la transmisión de datos, se produce un incremento considerable en el retardo y en la variación del retardo. Por lo que, al igual que en el apartado anterior, debemos proceder a solucionar estos dos problemas de la forma indicada anteriormente.

Capítulo 7
RIP

7.1 Introducción

Los hosts de las redes IP envían todo el tráfico IP hacia los routers, excepto el dirigido hacia destinos conectados directamente a la misma red. Estos routers están conectados a dos o mas redes físicas y encaminan datagramas IP entre estas, es decir, aceptan datagramas que llegan por medio de una interfaz de red y los encaminan hacia otra interfaz. De esta forma, los datagramas viajan de un router a otro hasta encontrar un router que se encuentre conectado directamente a la misma red física en la que se encuentra su destino final.

Los routers IP realizan el encaminamiento en función de los valores que aparecen en la tabla de encaminamiento. Cada entrada de información en la tabla de encaminamiento especifica la porción de red de una dirección de destino y establece la dirección de la siguiente máquina a lo largo de una ruta utilizada para alcanzar la red. Esta información se debe calcular en función de la topología de la red, es decir, de las conexiones ente routers y la carga de los enlaces. Valores erróneos en esta tabla pueden provocar que los datagramas no lleguen a su destino, que algunas partes de la red no puedan comunicarse con otras o que los datagramas IP estén constantemente dando vueltas (loops) por la red,gastando ancho de banda.

En el caso de routers conectados a pocas redes físicas (2, 3 ó 4), en un fragmento de red controlado por una misma organización, es viable controlar manualmente las tablas de encaminamiento. Para casos no triviales, es necesario que los routers se intercambien mensajes según algún algoritmo de encaminamiento, de forma que la asignación de los valores en la tabla de encaminamiento sea automática. A esta última opción se la denomina encaminamiento dinámico (frente al estático o manual).

El encaminamiento dinámico posee dos ventajas fundamentales frente al encaminamiento estático. En primer lugar, consigue optimizar automáticamente las rutas. Y por otra parte, se consigue que las rutas se redefinan cuando hay fallos en la red.

7.2 Sistemas Autónomos

Inicialmente Internet nació en torno a la red ARPANET. Los routers de esta red tenían información completa, es decir, una entrada para cada red conectada a Internet. Si recibían un datagrama que no sabían encaminar, automáticamente señalaban un error de encaminamiento. Los routers de este núcleo de Internet estaban gestionados por el INOC (Internet Networkss Operation Center), lo que los hacía un sistema altamente fiable.

En la actualidad, el conjunto de routers de las redes IP se encuentran estructurados en Sistemas Autónomos (SA), que se pueden definir como un conjunto de routers, y en definitiva de redes, administrados por una única organización. La IANA otorga un número identificativo único para cada SA. Se denomina Nodo Frontera al nodo que posee algún enlace hacia un nodo que no forma parte de su SA.

Cada SA debe gestionar un algoritmo de encaminamiento interno mediante un protocolo de tipo IGP (Interior Gateway Protocol), que configure las tablas de encaminamiento de sus routers. Este algoritmo debe ser independiente del usado en otros SA, y no intercambia información con routers externos. Los SA realizan un encaminamiento con información parcial, de forma que configuran sus tablas para encaminar hacia el nodo frontera aquellos datagramas que no pueden

manejar. Los nodos frontera tienen su algoritmo de encaminamiento propio, en primer lugar utilizó GGP (algoritmo de tipo Vector-Distancia) y desde 1988 utiliza SPREAD (algoritmo de tipo Shortest Path First).

Además, los SA se anuncian entre sí información sobre sus redes mediante protocolos del tipo EGP (Exterior Gateway Protocol). Los routers de cada SA elegidos para comunicarse con otros SA, deben recopilar periódicamente información sobre la topología de las redes del SA.

7.3 Interior Gateway Protocol (IGP)

De forma general, llamaremos IGP a cualquier protocolo de encaminamiento que actúa dentro de un Sistema Autónomo. Se encarga de gestionar los cambios sobre las tablas de encaminamiento de los routers internos.

La información necesaria para configurar adecuadamente las tablas de encaminamiento es el estado de todos los enlaces de la red, lo que es muchas veces muy costoso. En una aproximación puramente centralizada, una máquina del SA recibe la información de estado de todos los enlaces, calcula las tablas de encaminamiento de todos los routers al mismo tiempo, y se las transmite. Se trata de un sistema poco escalable y poco tolerante a fallos.

Existen otras tendencias no centralizadas, basadas en distintos modelos, como los algoritmos Vector-Distancia y los algoritmos SPF (Shortest Path First).

7.3.1 Algoritmos Vector-Distancia (Bellman-Ford)

Cada router maneja una tabla con una lista de todas las redes que conozca del SA, asociándole la distancia (a veces también se denomina coste y suele expresarse en términos de número de saltos o retardo estimado) hasta ella y la salida para ese destino:

Destino	Distancia	Ruta
Red 1	0	Directa
Red 2	0	Directa

Tabla 7.1: Ejemplo de Tabla Inicial

Un router al iniciarse conoce únicamente las redes a las que está conectado. Periódicamente, cada router enviará una copia de su tabla de encaminamiento a cualquier otro router que pueda alcanzar de manera directa, y se realizarán una serie de comprobaciones. Por ejemplo, cuando llega un mensaje al router K desde el router J, K examina el conjunto de destinos del mensaje y la distancia de cada uno. K actualizará la información en su tabla si:

- J conoce una ruta más corta para alcanzar un destino.
- J lista un destino que K no tiene en su tabla.
- K encamina actualmente un destino a través de J y la distancia de J hacia el destino ha cambiado.

Ejemplo:

Mensaje Vector-Distancia
(Enviado del router J al router K)

Destino	Distancia
Red 1	2
Red 4	3
Red 17	6
Red 21	4
Red 24	5
Red 30	10
Red 42	3

Tabla de encaminamiento existente
en el router K

Destino	Distancia	Ruta
Red 1	0	Directa
Red 2	0	Directa
Red 4	8	Router L
Red 17	5	Router M
Red 24	6	Router J
Red 30	2	Router Q
Red 42	2	Router J

Tras la recepción del mensaje, el router K modificará la entrada de la tabla de encaminamiento hacia la Red 4, incluyendo una nueva entrada con una distancia de 4 saltos y una ruta a través del Router J. Además, también incluirá una nueva entrada hacia la Red 21, con una distancia de 5 saltos y una ruta a través del router J.

7.3.2 Algoritmos Enlace-Estado (SPF)

Los protocolos que utilizan algoritmos Vector-Distancia tienen importantes desventajas que hacen que raramente sean empleados en grandes redes. En cada momento, las tablas de encaminamiento se calculan en función de la información que manejan los routers vecinos, lo que ralentiza mucho todos los cálculos, y que reaccione de manera oscilante e inestable ante cambios rápidos en la topología. Además, los protocolos Vector-Distancia pueden generar mensajes demasiado grandes, ya que el tamaño del mensaje crece con el número de redes del SA.

Una posible solución, es utilizar algoritmos de Enlace-Estado o SPF (Shortest Path First). En estos algoritmos, cada router envía al resto de routers del SA información sobre el estado de sus enlaces (en general, un costo relacionado con el tiempo de espera en cola para los datagramas enviados por ese enlace). Estos mensajes son cortos, ya que sólo se envía la información del número de interfaces de salida que tenga el router.

7.4 El protocolo RIP

Uno de los IGP más ampliamente utilizados es RIP (Routing Information Protocol), también conocido con el nombre de un programa que lo implementa, routed. El software routed fue originalmente diseñado en la Universidad de Berkeley en California para proporcionar información consistente de ruteo y accesibilidad entre máquinas en una red local.

La popularidad de RIP no reside en sus méritos técnicos. Por el contrario, es el resultado de que Berkeley distribuyó el routed junto con su popular sistema 4BSD de UNIX. Así, muchas redes TCP/IP adoptaron e instalaron routed y comenzaron a utilizar RIP sin considerar sus méritos o limitaciones técnicas.

Posiblemente el hecho más sorprendente relacionado con RIP es que fue construido y adoptado antes de que se escribiera un estándar formal. Finalmente, un RFC aparecido en junio de 1988 hizo posible que los vendedores aseguraran la interoperabilidad entre sus implementaciones.

El RIP es un protocolo de tipo Vector-Distancia, con métrica el número de saltos; es decir, la forma de medir la distancia hacia una red remota es contando el número de saltos existentes entre los dos extremos. En principio, divide las máquinas participantes en activas y pasivas. Los routers activos anuncian sus rutas al resto de máquinas; las máquinas pasivas listan y actualizan sus rutas con base en esos anuncios, pero nunca anuncian sus propias tablas. Sólo los routers pueden correr RIP de modo activo; los hosts deben utilizar el modo pasivo.

Las tablas de encaminamiento contienen 3 campos de información:

- Vector: Red de destino.
- Distancia: Número de saltos hacia la red destino. En la métrica RIP, un router define un salto hasta la red conectada directamente, dos saltos hacia la red que está al alcance a través de otro router, y así sucesivamente. De esta forma, el número de saltos a lo largo de una trayectoria desde una fuente dada hacia un destino dado hace referencia al número de routers que un datagrama encontrará a lo largo de la trayectoria. Es obvio que utilizar el conteo de saltos para calcular la trayectoria más corta no siempre produce resultados óptimos. Por ejemplo, una trayectoria con un total de saltos igual a 3 que cruza tres redes Ethernet puede ser notablemente más rápido que una trayectoria con un contador de saltos igual a 2 que atraviesa dos líneas serie lentas.
- Interfaz: Router vecino, donde comienza la ruta hacia el destino.

Los routers activos envían a sus vecinos cada 30 segundos los campos Vector y Distancia de sus tablas. Tanto los participantes RIP activos como los pasivos escuchan todos los mensajes difundidos y actualizan sus tablas de acuerdo al algoritmo Vector-Distancia descrito anteriormente.

Para prevenir que los routers oscilen entre dos o más trayectorias de costos iguales, RIP especifica que se deben conservar las rutas existentes hasta que aparezca una ruta nueva con un costo estrictamente menor.

Si falla un enlace de un router, los nodos que tienen instalada rutas a través de él deben enterarse. Por ello, todas las rutas aprendidas por medio de RIP permanecen activas sólo durante 180 segundos en la tabla; con ello conseguimos que el sistema reaccione adecuadamente frente a caídas de líneas en la red. Lógicamente, dicho contador se reinicia cada vez que se recibe un mensaje RIP nuevo.

7.4.1 Problemática RIP

RIP presenta tres inconvenientes importantes. En primer lugar, dado que el algoritmo no incorpora ningún mecanismo de detección de ciclos (loops), RIP debe asumir que el resto de routers son confiables o deberá tomar precauciones para prevenir los ciclos. En segundo lugar, para prevenir posibles inestabilidades, RIP debe acotar a 16 el nº máximo de saltos (distancia máxima). Así, para una red grande (con más de 16 saltos), los administradores deben dividir la red en secciones o utilizar un protocolo alternativo. Y en tercer lugar, el algoritmo Vector-Distancia empleado por RIP crea un problema de Convergencia Lenta (slow convergence), debido a que los mensajes de actualización de ruteo se difunden lentamente a través de la red. Seleccionando un infinito pequeño (16) se ayuda a paliar este problema, pero no se elimina completamente.

A continuación mostramos un ejemplo del problema de la Convergencia Lenta.

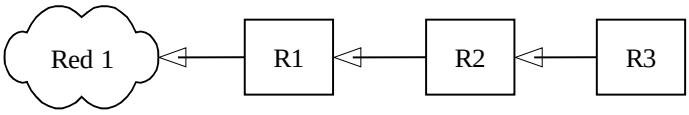

Figura 7.1: Problema de la Convergencia Lenta

Como se muestra en la figura, el router R1 tiene una conexión directa hacia la Red 1, así tiene una ruta en su tabla con distancia 1; éste incluye la ruta en sus difusiones periódicas. El router R2 ha aprendido la ruta desde R1, la recoge en su tabla de encaminamiento y la anuncia con una distancia igual a 2. Finalmente, R3 aprende la ruta desde R2 y la anuncia con una distancia 3.

Ahora, supongamos que la conexión de R1 hacia la Red 1 falla. R1 actualizará su tabla de encaminamiento inmediatamente para hacer la distancia igual a 16 (infinita). En la siguiente difusión, R1 anunciará a su vecino este cambio. Sin embargo, a menos que el protocolo incluya mecanismos extra para prevenirlo, cualquier otro router podría difundir sus rutas antes que R1. En particular, supongamos que R2 logra anunciar sus rutas justo después de que la conexión de R1 falle. Si esto sucede, R1 recibirá los mensajes de R2 y seguirá el algoritmo usual de Vector-Distancia: éste notará que R2 ha anunciado un camino hacia la Red 1 a un costo bajo, calculando que ahora se encuentra a 3 saltos par alcanzar la Red 1 (2 para que R2 alcance la Red1, más 1 par alcanzar R2) e instalará una nueva ruta a través de R2. En este tiempo, si R1 recibe un datagrama destino para la Red 1, encaminarán el datagrama hacia R2, y viceversa, y así sucesivamente hasta que su tiempo de vida limite (TTL) se alcance.

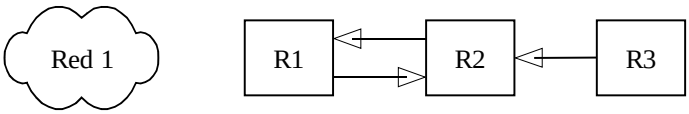

Figura 7.2: Problema de la Convergencia Lenta

En las siguientes difusiones de RIP no se resolverá el problema rápidamente. En el siguiente ciclo de intercambio de ruteo, R1 difundirá sus tablas de rutas completas. Cuando R2 aprenda que las rutas de R1 hacia la Red 1 tienen una longitud igual a 3, éste calculará una nueva longitud para tal ruta, haciéndola igual a 4. En el tercer ciclo, R1 recibe un mensaje del incremento desde R2 e incrementa la distancia en su tabla a 5. Este proceso continuará contando hasta llegar a 16 (el infinito de RIP).

7.4.2 Solución al problema de la Convergencia Lenta

Es posible resolver el problema de la convergencia lenta mediante una técnica conocida como **"split horizont update".** Cuando se utiliza esta técnica, un router registra la interfaz por la que ha recibido una ruta particular y no difunde esta información posteriormente por la misma interfaz. En el ejemplo, el router R2 no anunciará al router R1 su ruta de longitud 2 hacia la Red 1.

Otra técnica utilizada para resolver el problema de la convergencia lenta emplea un método conocido como **"hold down".** Esta técnica obliga a los routers a ignorar información acerca de una red durante un periodo de tiempo fijo después de la recepción de un mensaje que afirma que la red es inaccesible. Por lo general, el periodo hold down se establece en 60 segundos. La idea es esperar lo suficiente como para poder asegurar que todas las máquinas reciban la nueva información y que no se acepta un mensaje erróneo que está fuera de fecha.

Finalmente, otra técnica para resolver el problema de la convergencia lenta es el **"poisson reverse"**. Una vez que una conexión desaparece, el router sigue incluyendo dicha conexión durante varios periodos de actualización e incluye un costo infinito en la difusión. Para hacer el poisson reverse más efectivo, se debe combinar con las **"triggered updates"**. Las triggered updates obligan a un router a que envíe una difusión inmediatamente después de recibir nueva información, en lugar de esperar el próximo periodo de difusión. Al enviar una actualización inmediatamente, un router minimiza el tiempo en que es vulnerable por recibir la información nueva.

Por desgracia, mientras las técnicas anteriores resuelven algunos problemas, también inducen a otros:

- Con las "triggered updates", si una difusión cambia las tablas de encaminamiento de todos los routers presentes en una red, se activará un nuevo ciclo de difusión. Si este segundo ciclo de difusión cambia otra vez todas las tablas, activará más difusiones. Esto puede conducir a una avalancha de difusiones.
- La técnica "hold down" puede hacer que RIP sea muy ineficiente en una red de área amplia. En éstas, los periodos hold down son más largos que los temporizadores utilizados por los protocolos de alto nivel, lo cual puede consumir su periodo de tiempo y conducir a la ruptura de conexiones.

7.4.3 Formato del mensaje RIP

Los mensajes RIP pueden ser clasificados, a grandes rasgos, en dos tipos: mensajes de información de encaminamiento y mensajes utilizados para solicitar información. Ambos se valen del mismo formato, consistente en un encabezado fijo seguido por una lista opcional de de redes y sus correspondientes distancias.

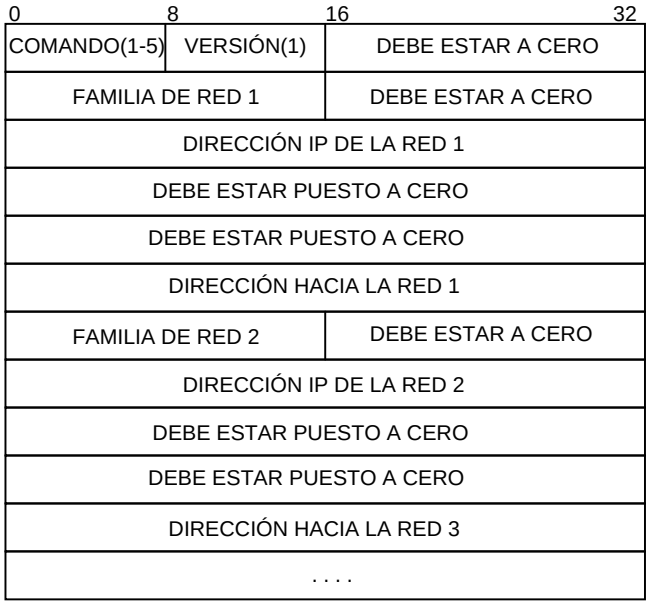

Figura 7.3: Formato del mensaje RIP

El campo COMANDO especifica una operación de acuerdo con la siguiente tabla:

Comando	Significado
1	(REQUEST) Solicitud para información parcial o completa de ruteo
2	(RESPONSE) Respuesta con distancias de red de pares desde la tabla de ruteo al emisor
3	Activar el modo de trazado (obsoleto)
4	Desactivar el modo de trazado (obsoleto)
5	Reservado

Tabla 7.2: Campo COMANDO del mensaje RIP

Un router o un host puede solicitar información de ruteo a otro enviando un comando REQUEST. El router responde a la solicitud mediante el comando RESPONSE. Sin embargo, en la mayoría de los casos, los routers difunden mensajes de respuestas periódicamente (es decir, sin necesidad de ser solicitados). El campo VERSIÓN contiene el número de versión del protocolo y lo utiliza el receptor para verificar que interpretará el mensaje de forma correcta.

7.4.4 Convenciones de direccionamiento RIP

La generalidad de RIP es evidente en la forma en que transmite direcciones de red. El formato de dirección no está limitado al uso con TCP/IP; puede utilizarse con múltiples conjuntos de protocolos de red. Cada dirección de red transportada por RIP puede tener una dirección de hasta 14 bytes. Por supuesto, las direcciones IP necesitan sólo 4; RIP especifica que los bytes restantes deben ser iguales a cero (los diseñadores seleccionaron el tercer octeto de este campo como inicio de la dirección IP a fin de asegurar una alineación de 32 bits). El campo FAMILIA DE RED identifica la familia de protocolo bajo la que la dirección de red deberá interpretarse. RIP utiliza un valor 2 para identificar las direcciones IP. Además de las direcciones normales IP, RIP utiliza la convención de que la dirección 0.0.0.0 representa la ruta por omisión.

El campo DISTANCIA HACIA LA RED contiene un contador con la distancia hacia la red especificada. La distancia es medida en saltos de router, pero los valores están limitados al rango entre 1 y 16, con la distancia 16 utilizada para dar a entender una distancia infinita.

7.4.5 Transmisión de mensajes RIP

Los mensajes RIP no contienen un campo de longitud explícito. De hecho, RIP asume que los mecanismos de entrega subyacentes dirán al receptor la longitud de un mensaje entrante. En particular, cuando se utiliza con TCP/IP, los mensajes RIP dependen del protocolo UDP para informar al receptor de la longitud del mensaje. RIP funciona en el puerto 520 de UDP. Sin embargo, aunque una solicitud RIP puede originarse en otro puerto UDP, el puerto de destino UDP para la solicitud es siempre el 520, que es el puerto de origen desde el cual, en principio, RIP difunde los mensajes.

7.5 Desarrollo práctico

7.5.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 4 routers NUCLEOX PLUS.
- 8 PC’s que funcionarán como clientes.
- 4 hubs Ethernet.
- 12 latiguillos directos.
- 4 cables RS-232 pin a pin para la conexión directa entre 2 routers NUCLEOX PLUS.

A continuación procedemos a montar la red según la siguiente topología:

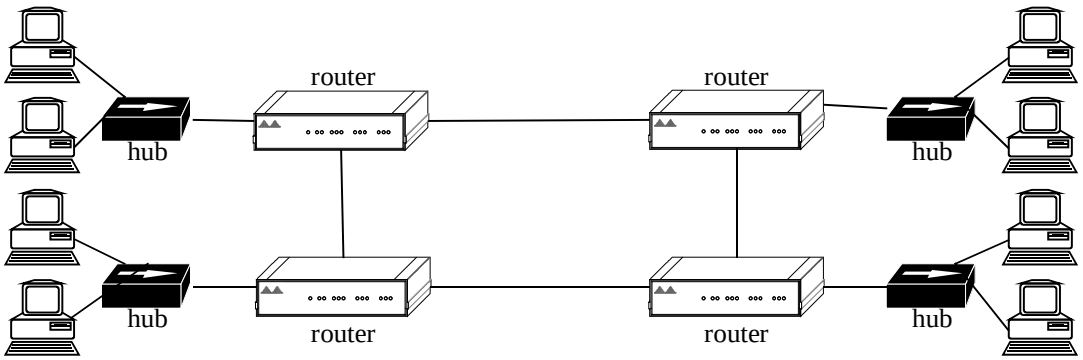

Figura 7.4: Topología de Red.

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

7.5.2 Configuración de las interfaces del router

En primer lugar configuramos la interfaz LAN del router. En este punto, nuestro objetivo es asignarle una dirección IP a este interfaz. Esto se realiza de la forma habitual, mediante el comando **ADD ADDRESS** desde el menú de configuración del protocolo IP.

Entre router y router estableceremos enlaces PPP síncronos. En primer lugar debemos establecer la existencia de un enlace de datos PPP ejecutando el comando **SET DATA-LINK PPP** desde el Proceso 4. Si a continuación procedemos a visualizar las interfaces existentes en el router, con el comando **LIST DEVICES**, podemos observar que una interfaz está configurada como enlace PPP.

A continuación, para asignar una dirección IP al interfaz PPP, debemos actuar de la misma forma que con los interfaces LAN; entramos en el menú de configuración del protocolo IP, y utilizamos el comando **ADD ADDRESS.** Siempre guardamos los cambios efectuados con el comando **SAVE**.

Llegados a este punto podemos comprobar si existe conectividad del router con los routers vecinos ejecuntando el comando **PING,** en uno de ellos, desde el proceso de monitorización del protocolo IP.

7.5.3 Configuración del protocolo RIP

El **NUCLEOX PLUS** soporta una implementación completa del protocolo RIP-2, tal y como se especifica en las recomendaciones RFC 1723 y RFC 1388. Esta versión es compatible con los routers que ejecuten la Versión 1 de RIP.

RIP-2 es una extensión de RIP-1. Utiliza el mismo formato de mensaje pero extiende el significado de alguno de los campos. Sin embargo, nosotros sólo vamos a utilizar RIP-1, por su mayor sencillez y facilidad de configuración.

El primer paso que debemos ejecutar es habilitar el protocolo RIP. Para ello, en primer lugar debemos entrar al menú de configuración del protocolo RIP, al que se accede desde el proceso 4, con el comando **PROTOCOL RIP**.

```
*P 4
User Configuration
Config>PROTOCOL RIP
RIP protocol user configuration
RIP config>
```

Para habilitar el protocolo RIP en los routers NUCLEOX PLUS debemos de ejecutar el comando **ENABLE RIP.** Con este comando habilitamos el protocolo RIP en todos los interfaces del router, es decir, todos los interfaces van a enviar mensajes RIP y también van a aceptar los mensajes RIP que le lleguen.

```
RIP config> ENABLE RIP
RIP config>
```

En caso de que no queramos que una determinada interfaz tenga habilitado el protocolo RIP debemos utilizar el comando **SET SENDING**. Mediante este comando definimos tanto las interfaces de red del router que tienen deshabilitado RIP como las que lo tienen habilitado; además también nos permite configurar los parámetros de envío por interfaz. Los parámetros de envío que se establecen por defecto son:

- Envío de las rutas de red.
- Envío de las rutas de subred.
- No envío de las rutas estáticas.
- Envío de las rutas directas.
- No envío de las rutas default.
- Poisoned-Reverse habilitado.

Para establecer si una interfaz tiene habilitado el protocolo RIP, y para configurar los parámetros de envío por interfaz se procede de la siguiente manera:

```
RIP config> SET SENDING
IP addresses for each interface:
intf 0 192.168.1.254 255.255.255.0 NETWORK broadcast, fill 0
intf 1 192.168.2.1   255.255.255.0 NETWORK broadcast, fill 0
intf 2 192.168.3.1   255.255.255.0 NETWORK broadcast, fill 0
Set for which interface address [0.0.0.0]? 192.168.2.1
Do you wish to send network routes? (Yes/No)(Y)? y
Do you wish to send subnetwork routes? (Yes/No)(Y)? y
Do you wish to send static routes? (Yes/No)(N)? n
Do you wish to send direct routes? (Yes/No)(Y)? y
Do you wish to send default routes? (Yes/No)(N)? n
Do you wish poisoned reverse ? (Yes/No)(Y)? y
RIP config>
```

- *Do you wish to send network routes?:* Si este flag está activado, el router incluye todas las rutas en las respuestas RIP.
- *Do you wish to send subnetwork routes?:* Si este flag está activado, el router incluye las rutas de subred en las respuestas RIP.
- *Do you wish to send static routes?:* Si este flag está activado, el router incluirá todas las rutas de las redes configuradas estáticamente en las respuestas RIP.
- *Do you wish to send direct routes?:* Si este flag está activado, el router incluirá todas las rutas de las redes conectadas directamente en las respuestas RIP. Si no está activado, sólo se enviarán las redes directamente conectadas que participen del protocolo RIP (que tengan habilitado RIP para envío o para recepción). Por defecto está activado.
- *Do you wish to send default routes?:* Si este flag está activado, el router incluye la ruta por defecto en las respuestas RIP, si es que existe un router por defecto. La ruta para el router por defecto se señala como una ruta al destino 0.0.0.0.

- *Do you wish poisoned reverse ?:* Este flag está activo por defecto. Habilita o deshabilita el poison reverse en el proceso del split-horizon.

De la misma forma también podemos configurar los parámetros de recepción por interfaz, mediante el comando **SET RECEIVING.** Los parámetros de recepción que se establecen por defecto son:

- Procesar rutas de redes recibidas.
- Procesar rutas de subredes recibidas.
- No sobrescribir las rutas default.
- No sobrescribir las rutas estáticas.

Para configurar los parámetros de recepción por interfaz se procede de la siguiente manera:

```
RIP config> SET RECEIVING
IP addresses for each interface:
intf 0 192.168.1.254 255.255.255.0 NETWORK broadcast, fill 0
intf 1 192.168.2.1   255.255.255.0 NETWORK broadcast, fill 0
intf 2 192.168.3.1   255.255.255.0 NETWORK broadcast, fill 0
Set for which interface address [0.0.0.0]? 192.168.2.1
Do you wish to process received network routes? (Yes/No)(Y)? y
Do you wish to process received subnetwork routes? (Yes/No)(Y)? y
Do you wish to overwrite default routes? (Yes/No)(N)? N
Do you wish to overwrite static routes? (Yes/No)(N)? N
RIP config>
```

- *Do you wish to process received network routes?:* Si está activado se aceptan rutas de red.
- *Do you wish to process received subnetwork routes?:* Si está activado se aceptan rutas de subred.
- *Do you wish to overwrite default routes?:* Previene que una ruta RIP por defecto, la cual es recibida por la dirección del Interfaz IP, sea almacenada como ruta por defecto.
- *Do you wish to overwrite static routes?:* Este comando previene que rutas RIP recibidas en la dirección IP del interfaz sobrescriban la rutas estáticas.

A continuación debemos configurar las compatibilidades de envío y recepción por interfaz, mediante el comando **SET COMPATIBILITY**. Ponemos como envío RIP-1: sólo paquetes RIP Versión 1 son enviados; y como recepción RIP-1 o RIP-2: se aceptan ambas versiones.

```
RIP config> SET COMPATIBILITY
IP addresses for each interface:
intf 0 192.168.1.254 255.255.255.0 NETWORK broadcast, fill 0
intf 1 192.168.2.1   255.255.255.0 NETWORK broadcast, fill 0
intf 2 192.168.3.1   255.255.255.0 NETWORK broadcast, fill 0
Set for which interface address [0.0.0.0]? 192.168.2.1
Available:
1.- Do not send
2.- RIP1
3.- RIP2 Broadcast
4.- RIP2 Multicast
What kind of sending compatibility do you wish? [3]? 2
Available:
1.- RIP1
2.- RIP2
3.- RIP1 or RIP2
4.- Do no receive
What kind of receiving compatibility do you wish? [3]? 3
```

El selector de envío posee 4 posiciones:

- Do not send: deshabilita el envío de paquetes RIP en este interfaz.

- RIP-1: sólo paquetes RIP versión 1 son enviados.
- RIP-2 broadcast: donde los paquetes RIP versión 2 son enviados por broadcast.
- RIP-2 multicast: donde los paquetes RIP versión 2 son enviados por multicast.

Se recomienda que el valor escogido sea *RIP-1* o *RIP-2 multicast*, y no *RIP-2 broadcast* para evitarnos posibles problemas de entendimiento con dispositivos *RIP-1*. *RIP-2 broadcast* sólo debe usarse cuando el administrador conozca y comprenda todas las consecuencias.

El selector de recepción posee 4 posiciones:

- RIP-1: sólo se aceptan paquetes RIP con versión 1.
- RIP-2: sólo se aceptan paquetes RIP con versión 2.
- RIP-1 o RIP-2: se aceptan ambas versiones.
- No recibir: deshabilitada escucha RIP en este interfaz.

Tal como queda definido RIP en su RFC, existen 3 temporizadores que controlan el funcionamiento de su algoritmo. Únicamente en casos excepcionales podría ser deseable cambiar sus valores mediante el comando **SET TIMERS.** Para ello el administrador debe estar seguro y entender las posibles consecuencias.

```
RIP config> SET TIMERS
Enter periodic sending timer [30]? 30
Enter route expire timer [180]? 180
Enter route garbage timer [120]? 120
RIP config>
```

- *Periodic sending timer:* Su valor por defecto es de 30 segundos y es el tiempo que transcurre entre envío de respuestas periódicas.
- *Route expire timer:* Su valor por defecto es de 180 segundos. Si transcurre dicho tiempo sin haber sido refrescada una ruta por una respuesta, dicha ruta pasará a ser inválida.
- *Route garbage timer:* Su valor por defecto es de 120 segundos. Una vez dada como inválida una ruta se mantiene en la tabla de rutas durante 120 segundos con métrica 16 (infinito) para que los routers RIP vecinos se den cuenta que va a ser borrada. Ésta es la técnica del poison reverse.

7.5.4 Visualización de las rutas aprendidas

Para visualizar las rutas aprendidas mediante el protocolo RIP en los routers NUCLEOX PLUS debemos situarnos en proceso de monitorización (**PROCES 3**), que se identifica con el prompt "+". Aquí ejecutamos el comando **PROTOCOL IP**, para entrar en el menú de monitorización del protocolo IP, y a continuación tecleamos **DUMP**. Nos mostrará por pantalla la tabla de encaminamiento del router, con todas las entradas que ha aprendido.

7.5.5 Fallos en la red

Antes posibles fallos en la red, que hacen que cambie la topología de la misma, el protocolo RIP se intenta adaptar. Éste hace que se produzcan cambios en la tabla de encaminamiento para adaptarse al fallo.

Los cambios en la tabla de encaminamiento pueden tener dos motivos:

1. Una ruta lleva más de 180 segundos sin aparecer en ningún mensaje RESPONSE que recibimos. Esa ruta cambia su métrica a 16 (infinito).

2. Forzados por la recepción de un mensaje RESPONSE:

i. Si el mensaje RESPONSE nos habla de una ruta más corta que la que tenemos a la red R, instalamos esa ruta.

ii. Si el mensaje RESPONSE proveniente de A habla de una ruta a la red R con métrica 16 (infinito), y nosotros teníamos apuntado en nuestra tabla de encaminamiento que para ir hacia R, pasábamos por A, entonces es borrada de nuestra tabla de encaminamiento.

Por lo tanto, si en nuestra red provocamos un fallo a propósito y esperamos un tiempo hasta que se alcance el régimen permanente en el protocolo RIP, podemos observar que las tablas de encaminamiento de los routers se han modificado para adaptarse a la nueva topología de la red.

Capítulo 8
Backup de redes WAN

8.1 Introducción

La facilidad de backup de redes WAN, permite establecer un encaminamiento alternativo en caso de fallo, tanto si el error se produce en los nodos de la red o en la red de acceso.

El enlace del que se hace backup, es decir, el que se encuentra normalmente en utilización, se denomina enlace primario, y por él irá el tráfico en condiciones normales de funcionamiento. Sólo si se detectan anomalías o deja de funcionar, será reencaminado por el enlace alternativo preparado a tal efecto. Para ello, en caso de estar activos ambos enlaces (primario y alternativo), será de mayor prioridad el primario, para que el tráfico sea cursado a través de él. El enlace primario puede ser cualquiera de los interfaces que comuniquen el estado de actividad en el que se encuentran, es decir, que pueda establecerse en un momento dado si están caídos o no, como por ejemplo, un interfaz Frame Relay, un interfaz PPP síncrono o asíncrono (pero no sobre RDSI en modo permanente, ya que siempre están activos), un interfaz LAN (Ethernet o Token Ring), etc.

El enlace de backup se denomina enlace secundario o alternativo. Es un enlace que en condiciones normales no debería estar activo, sino a la espera de que se produzca una alteración en el funcionamiento normal del enlace principal, al cual se encuentra monitorizando, para que en caso de que se produzca algún tipo de fallo en el mismo, activarse y servir de camino alternativo. Típicamente se suele poner de enlace secundario un interfaz de conmutación de circuitos (RDSI o analógico), como por ejemplo un enlace PPP sobre RDSI, un enlace PPP sobre comandos AT, un enlace Frame Relay sobre RDSI, etc.

El proceso de backup implica:

1. Detectar la caída del enlace primario.
2. Conmutar al enlace secundario.
3. Detectar la recuperación del enlace primario.
4. Volver a conmutar al enlace primario.

Dependiendo del tipo de backup que se utilice, el proceso descrito anteriormente será o no transparente a los protocolos de nivel de red (por ejemplo, IP). Si es transparente implica que toda la información de encaminamiento, las conexiones, etc., se mantienen iguales en los instantes en los que la conexión está establecida a través del enlace secundario. En caso que no sea transparente, se debe modificar la información de encaminamiento, establecer nuevas conexiones, identificar nuevos extremos de la comunicación, etc.

Por lo general se puede considerar la existencia de dos tipos de técnicas principales de realizar backup: WRR (Wan ReRoute), que no es transparente a los protocolos de nivel de red; y WRS (Wan ReStoral), que es transparten a los protocolos de nivel de red.

8.2 WRR (WAN Reroute)

El objetivo de este mecanismo es habilitar nuevos enlaces para posibilitar encontrar un camino alternativo, en el caso de que sea posible, para cursar el tráfico de un enlace primario que ha dejado de estar activo. El backup por reencaminamiento (Backup WAN Reroute, WRR) se denomina de esta manera porque el tráfico que experimenta el proceso de backup, en el periodo de caida del enlace principal, es reencaminado por un enlace alternativo.

Este enlace alternativo puede tener como destino el mismo que el enlace principal, u otro distinto. En la siguiente figura se muestra el caso en el que el enlace secundario tiene como destino un router distinto al del enlace primario:

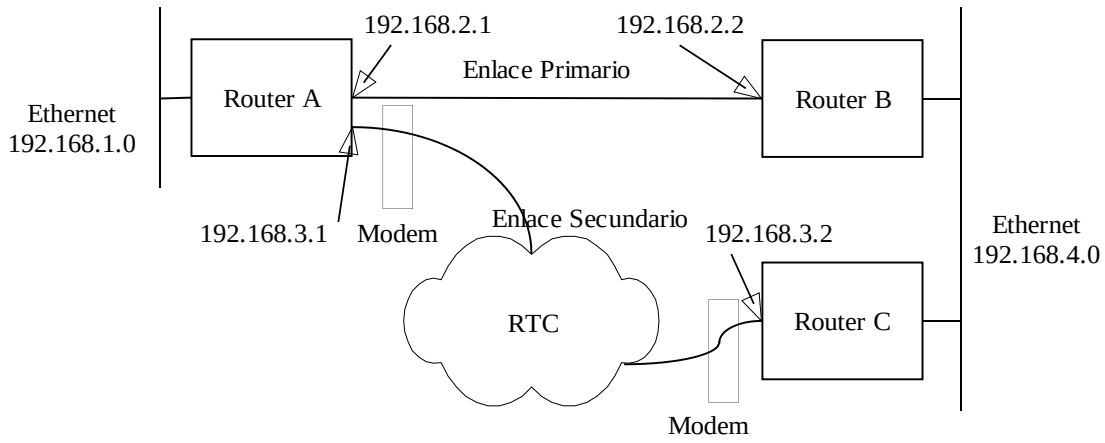

Figura 8.1: Ejemplo de WRR

En la figura las tablas de encaminamiento de los 3 routers son las siguientes:

ROUTER A

Destino	Gateway	Netmask
192.168.1.0	. . . .	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0
192.168.4.0	192.168.2.2	255.255.255.0
192.168.4.0	192.168.3.2	255.255.255.0

ROUTER B

Destino	Gateway	Netmask
192.168.1.0	192.168.2.1	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	192.168.4.253	255.255.255.0
192.168.4.0	. . . .	255.255.255.0

ROUTER C

Destino	Gateway	Netmask
192.168.1.0	192.168.3.1	255.255.255.0
192.168.2.0	192.168.4.254	255.255.255.0
192.168.3.0	. . . .	255.255.255.0
192.168.4.0	. . . .	255.255.255.0

Tabla 8.1: Tablas de encaminamiento de los routers

A continuación observamos un ejemplo en el que el enlace secundario tiene como destino el mismo que el enlace primario:

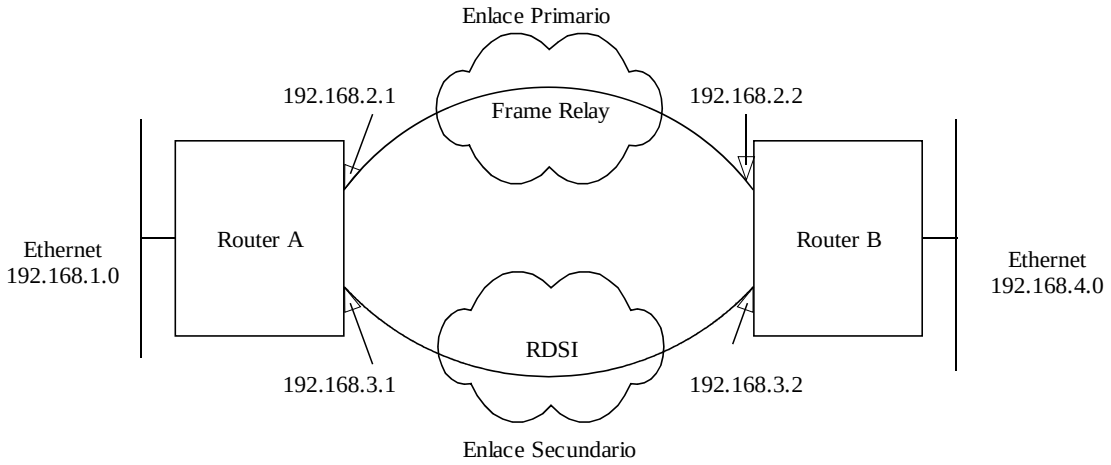

Figura 8.2: Ejemplo de WRR

En la figura las tablas de encaminamiento de los 2 routers son las siguientes:

ROUTER A

Destino	Gateway	Netmask
192.168.1.0	. . . .	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0
192.168.4.0	192.168.2.2	255.255.255.0
192.168.4.0	192.168.3.2	255.255.255.0

ROUTER B

Destino	Gateway	Netmask
192.168.1.0	192.168.2.1	255.255.255.0
192.168.1.0	192.168.3.1	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0
192.168.4.0	. . . .	255.255.255.0

Tabla 8.2: Tablas de encaminamiento de los routers

Como se puede observar en los dos ejemplos anteriores WRR no es un backup transparente desde el punto de vista de los protocolos de nivel 3, porque el enlace, tras pasar al proceso de backup, no es virtualmente el mismo. Es decir, cuando se establece la comunicación a través del enlace secundario, se trata de una nueva conexión, con una dirección IP origen nueva y una dirección IP destino nueva.

8.2.1 Funcionamiento

El modo en el que se realiza el backup WRR se describe a continuación. Se establece una asociación entre los interfaces del enlace principal y secundario para especificar el interfaz por el que se va a realizar el backup cuando el primero se “caiga”.

Se puede establecer el backup de varios interfaces principales por el mismo interfaz secundario. En cuanto uno de los principales se caiga, se activará el secundario y hasta que todos los principales no se hayan recuperado no se desactivará el secundario.

Análogamente, se puede configurar el backup de un interfaz principal por varios interfaces secundarios. En este caso, cuando el interfaz principal se caiga, se activarán todos los secundarios programados a tal efecto.

8.2.1.1 Estado de los Enlaces

Un interfaz cualquiera (sea primario o secundario) puede encontrarse en un momento dado en cualquiera de los estados siguientes:

- *No presente*.
- *No soportado*.
- *Activo*.
- *Inactivo*.
- *Realizando test*.
- *Deshabilitado*.

Además, el enlace **secundario** puede encontrarse también en el estado:

- *Disponible*, interfaz secundario monitorizando el estado de otro interfaz principal.

En condiciones normales, el interfaz primario se encontrará en estado *activo* y el tráfico irá a través suyo (cuando corresponda). El secundario permanece en estado *disponible* monitorizando el estado del primario.

8.2.1.2 Eventos

Pueden suceder distintos eventos que provocan cambios en el estado del sistema:

- *Activación de Primario (**PriUp**)*, alguno de los interfaces primarios asociados a un secundario ha anunciado una recuperación del enlace.
- *Caída de Primario (**PriDwn**)*, alguno de los interfaces primarios asociados a ese secundario ha anunciado una caída del enlace.
- *Primer Tiempo de Estabilización venció*, ha vencido el temporizador del primer tiempo de estabilización. El **Primer Tiempo de Estabilización** es el tiempo que debe estar caído el primario antes de activar el secundario (realizar el backup).
- *Tiempo de Estabilización venció*, ha vencido el temporizador del tiempo de estabilización. El **Tiempo de Estabilización** es el tiempo mínimo que debe estar activo el primario antes de desactivar el secundario (volver del backup y retornar a la situación inicial).
- *Desconocido (**Unk**)*, no se ha producido todavía ningún evento o el evento es desconocido.

8.2.1.3 Estado del Backup WRR en el enlace Secundario

El proceso de backup WRR puede encontrarse en diferentes estados:

- **Deshabilitado (---),** cuando no hay ninguna asociación habilitada o está deshabilitado globalmente el WRR.
- **Inicial (*Ini*),** estado en el que se encuentra el equipo al arrancar. El interfaz secundario se encuentra *disponible*; si llega el evento *Activación de Primario* entonces se pasa al estado **Directo**, mientras que si se produce el evento *Caída de Primario* se pasa a **Directo→Alternativo**.

- **Directo (*Dir*),** el secundario se encuentra *disponible* porque todos los enlaces primarios que controla están *activos*.
- **Directo→Alternativo (*Dir→Alt*),** cuando el secundario se encuentra *disponible*, pero se ha recibido un evento de *Caída de Primario* de alguno de los primarios que tiene asociado.
- **Alternativo (*Alt*),** cuando ha llegado el evento *Primer tiempo de Estabilización venció* con lo que se inicia un selftest del interfaz secundario para que se active.
- **Alternativo→Directo (*Alt→Dir*),** ha llegado el evento *Activación de Primario* de alguno de los primarios que tiene asociado.

8.2.1.4 Proceso de Backup WRR

El proceso de backup se inicia cuando estando el secundario en un estado de *disponible* se produce una *Caída de Primario.* Entonces pasa a estado **Directo→Alternativo** y después de esperar el tiempo mínimo que tiene que estar caído el primario (*Primer Tiempo de Estabilización*) y establecer que efectivamente entre en funcionamiento el secundario, se pasará al estado **Alternativo**.

Cuando el enlace secundario se encuentra *activo* (encaminando el tráfico que normalmente debería ir a través del enlace primario) con el backup en estado **Alternativo** y el primario al que está monitorizando vuelve a recuperarse (se produce el evento *Activación de Primario*), si éste es el último de los enlaces caídos que tienen a ese enlace configurado como secundario se pasa a **Alternativo→Directo**, y después de esperar el tiempo mínimo que debe estar activo el enlace primario (*Tiempo de Estabilización*) se activa de nuevo el enlace primario y se desactiva el secundario (y en el caso de enlaces secundarios conmutados, que requieren llamada para establecerse, se libera la llamada). El backup pasa a estado **Directo**.

8.3 WRS (WAN Restoral)

El proceso de backup WRS (WAN Restoral) es transparente a los protocolos de nivel 3, excepto por posibles retardos o cambios en la velocidad de un enlace secundario de menor capacidad. Toda la información de encaminamiento, las conexiones de protocolos, etc., se mantienen iguales.

En este tipo de backup, el enlace secundario sólo puede tener como destino el mismo que el enlace primario. En la siguiente figura se observa un ejemplo:

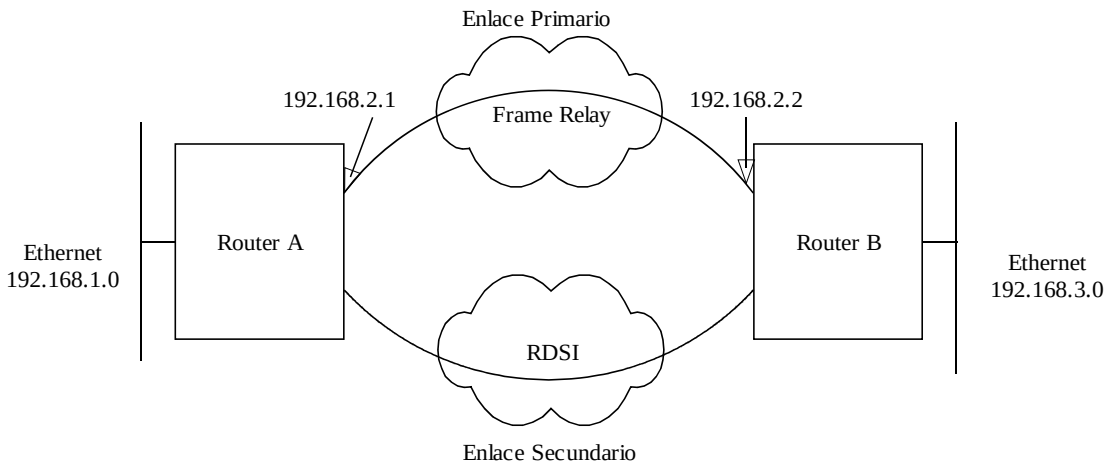

Figura 8.3: Ejemplo de WRS

En la figura las tablas de encaminamiento de los 2 routers son las siguientes:

ROUTER A

Destino	Gateway	Netmask
192.168.1.0	. . . .	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	192.168.2.2	255.255.255.0

ROUTER B

Destino	Gateway	Netmask
192.168.1.0	192.168.2.1	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0

Tabla 8.3: Tablas de encaminamiento de los routers

Cuando se entre en el proceso de bakcup la topología de la red quedará con la siguiente forma:

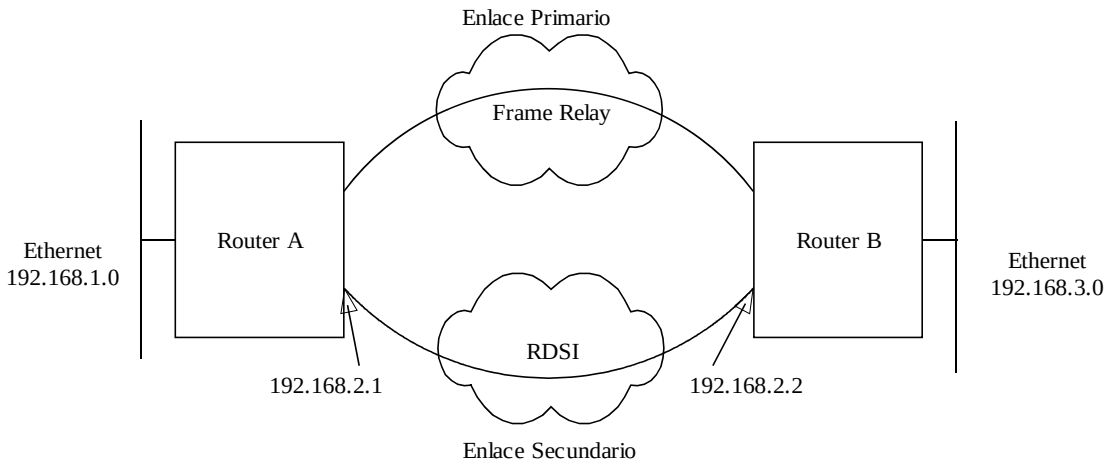

Figura 8.4: Funcionamiento de WRS

Como se puede observar este cambio no provocará ninguna modificación en las tablas de encaminamiento de los routers, ni en las conexiones establecidas por los protocolos de nivel superior. Es decir, el funcionamiento es idéntico al que había antes de comenzar el backup.

8.4 Desarrollo práctico

- Configuración de backup de PPP síncrono por PPP sobre RDSI, utilizando WRR.
- Configuración de backup de Frame Relay por RDSI, utilizando WRS.

8.4.1 Configuración de backup de PPP síncrono por PPP sobre RDSI, utilizando WRR

8.4.1.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers NUCLEOX PLUS.
- 2 PC’s que funcionarán como clientes.

- 2 hubs Ethernet.
- 8 latiguillos directos.
- 1 cables RS-232 pin a pin para la conexión directa entre 2 routers NUCLEOX PLUS.

A continuación procedemos a montar la red según la siguiente topología:

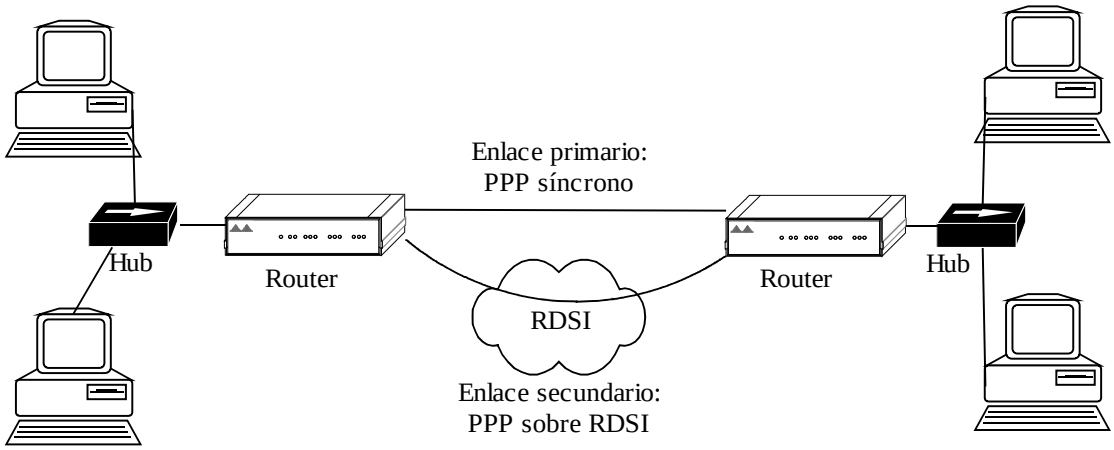

Figura 8.5: Topología de red

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

8.4.1.2 Configuración de las interfaces del router

En primer lugar configuramos la interfaz LAN del router. En este punto, nuestro objetivo es asignarle una dirección IP a este interfaz. Esto se realiza de la forma habitual, mediante el comando **ADD ADDRESS** desde el menú de configuración del protocolo IP.

Entre router y router estableceremos enlaces PPP síncronos. En primer lugar debemos establecer la existencia de un enlace de datos PPP ejecutando el comando **SET DATA-LINK PPP** desde el Proceso 4. Si a continuación procedemos a visualizar las interfaces existentes en el router, con el comando **LIST DEVICES**, podemos observar que una interfaz está configurada como enlace PPP.

A continuación, para asignar una dirección IP al interfaz PPP, debemos actuar de la misma forma que con los interfaces LAN; entramos en el menú de configuración del protocolo IP y utilizamos el comando **ADD ADRRESS.** Siempre guardamos los cambios efectuados con el comando **SAVE**.

Entre router y router también estableceremos enlaces PPP sobre RDSI. En primer lugar debemos establecer la existencia de un enlace de datos PPP sobre RDSI ejecutando el comando **ADD DEVICE PPP-DIAL** desde el Proceso 4. A continuación, igual que con el interfaz PPP síncrono, debemos asignarle una dirección a este interfaz; para terminar guardaremos los cambios efectuados con el comando **SAVE**.

Llegados a este punto podemos comprobar si existe conectividad desde un router con los routers vecinos, utilizando el comando **PING** desde el proceso de monitorización del protocolo IP. En este caso la conexión se establecerá a través del enlace primario, es decir, el enlace PPP síncrono.

Seguidamente, debemos configurar las tablas de encaminamiento de los routers. Las entradas que debemos incluir en estas tablas, tomando como ejemplo la red de la figura son:

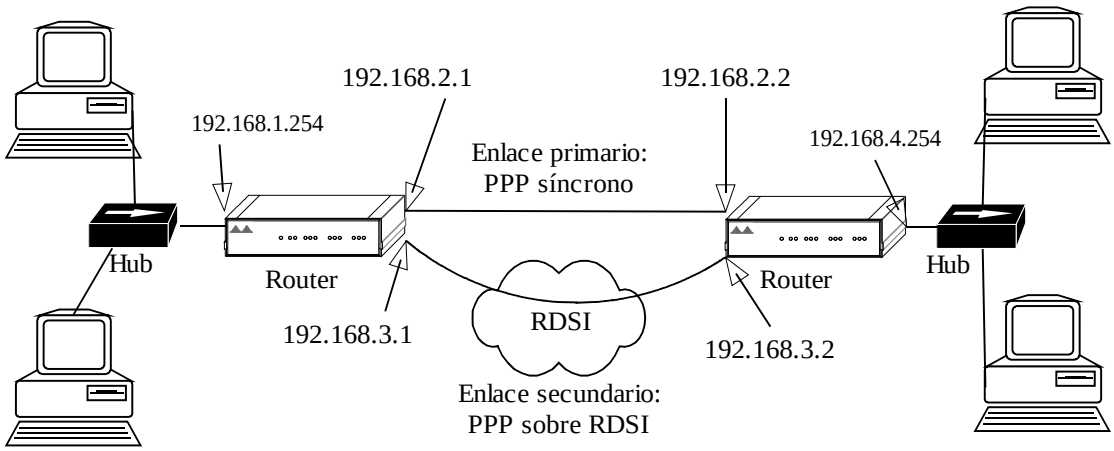

Figura 8.6: Topología de red con direcciones IP

ROUTER IZQUIERDA

Destino	Gateway	Netmask
192.168.1.0	. . . .	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0
192.168.4.0	192.168.2.2	255.255.255.0
192.168.4.0	192.168.3.2	255.255.255.0

ROUTER DERECHA

Destino	Gateway	Netmask
192.168.1.0	192.168.2.1	255.255.255.0
192.168.1.0	192.168.3.1	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0
192.168.4.0	. . . .	255.255.255.0

Tabla 8.4: Tablas de encaminamiento de los routers

8.4.1.3 Configuración del Backup WRR

Los comandos de configuración WRR están disponibles en el prompt de configuración asociado. Para acceder al prompt de configuración WRR hay que realizar los siguientes pasos:

1. Acceder al menú de configuración general, *Config>*.
2. Introducir el comando relacionado con la facilidad WRR, **FEATURE WRR-BACKUP-WAN**.

A continuación hay que utilizar el comando **ADD PAIR** que crea una nueva asociación para el backup WRR. Para ello se indica el interfaz primario que se quiere monitorizar, el subinterfaz (en su caso), el interfaz secundario y los tiempos de estabilización.

Si se quiere configurar el backup WRR de un interfaz principal sobre varios secundarios o el de varios interfaces primarios sobre el mismo secundario se añadirán tantas asociaciones con el mismo interfaz común como sea necesario.

```
Backup WRR> ADD PAIR
Primary Interface: [0]? 1
Primary Subinterface: ?
Secondary Interface: [0]? 2
First stabilization time: [-1]?
Stabilization time: [-1]?
Backup WRR>
```

Un valor de "-1" en los tiempos de estabilización indica que se configuran los valores que haya definido por defecto.

Seguidamente debemos utilizar el comando **ENABLE WRR** que habilita la funcionalidad de backup WRR. Si no se habilita la funcionalidad en general mediante este comando no se ejecutará nada relativo a la misma.

```
Backup WRR> ENABLE WRR
Backup WRR>
```

En este momento se puede salvar la configuración y reiniciar el router para que los cambios tengan efecto y el backup WRR esté funcional en la forma configurada.

Una vez establecida una configuración, puede ser que nos interese modificar los tiempos de estabilización de dicha configuración, sin modificar su funcionamiento. El comando **SET** se emplea para configurar los diferentes tiempos de estabilización. Se pueden configurar tanto los tiempos de estabilización que se emplean por defecto como los que utiliza una asociación determinada.

El comando **SET DEF-FIRST-TMP-STAB** configura el valor del primer tiempo de estabilización por defecto.

```
Backup WRR> SET DEF-FIRST-TMP-STAB
Default First Stabilization Time: [1]? 2
Backup WRR>
```

El comando **SET DEF-TMP-STAB** configura el valor del tiempo de estabilización por defecto.

```
Backup WRR> SET DEF-TMP-STAB
Default Stabilization Time: [1]? 2
Backup WRR>
```

El comando **SET FIRST-TMP-STAB** configura el valor del primer tiempo de estabilización de una asociación específica. Además del valor del primer tiempo de estabilización se indica a qué asociación se refiere. Un valor de "–1" establece el tiempo por defecto asociado (se toma el primer tiempo de estabilización por defecto).

```
Backup WRR> SET FIRST-TMP-STAB
Primary Interface: [0]? 1
Primary Subinterface: ? 16
Secondary Interface: [0]?
First stabilization time: [-1]? 1
Backup WRR>
```

El comando **SET TMP-STAB** configura el valor del tiempo de estabilización de una asociación específica. Además del valor del tiempo de estabilización se indica a qué asociación se refiere. Un valor de "–1" establece el tiempo por defecto asociado (se toma el tiempo de estabilización por defecto).

```
Backup WRR> SET TMP-STAB
Primary Interface: [0]? 1
Primary Subinterface: ? 16
Secondary Interface: [0]?
Stabilization time: [-1]? 2
Backup WRR>
```

8.4.1.4 Comprobación del funcionamiento

Para comprobar si el funcionamiento del backup es el correcto, podemos proceder a establecer una comunicación entre los dos routers a través del enlace primario, y posteriormente provocar un fallo en la red desconectando el cable en uno de los extremos y observar si el backup funciona correctamente.

Efectivamente, cuando cae el enlace primario, se activa el secundario. Si posteriormente se restablece el enlace primario, automáticamente se cuelga la llamada RDSI y continúa la comunicación por el enlace primario.

8.4.2 Configuración de backup de Frame Relay por RDSI, utilizando WRS

8.4.2.1 Montaje de la red

Para el montaje de la red se necesitan los siguientes materiales:

- 2 routers NUCLEOX PLUS.
- 2 PC's que funcionarán como clientes.
- 2 hubs Ethernet.
- 8 latiguillos directos.
- 1 cables RS-232 pin a pin para la conexión directa entre 2 routers NUCLEOX PLUS.

A continuación procedemos a montar la red según la siguiente topología:

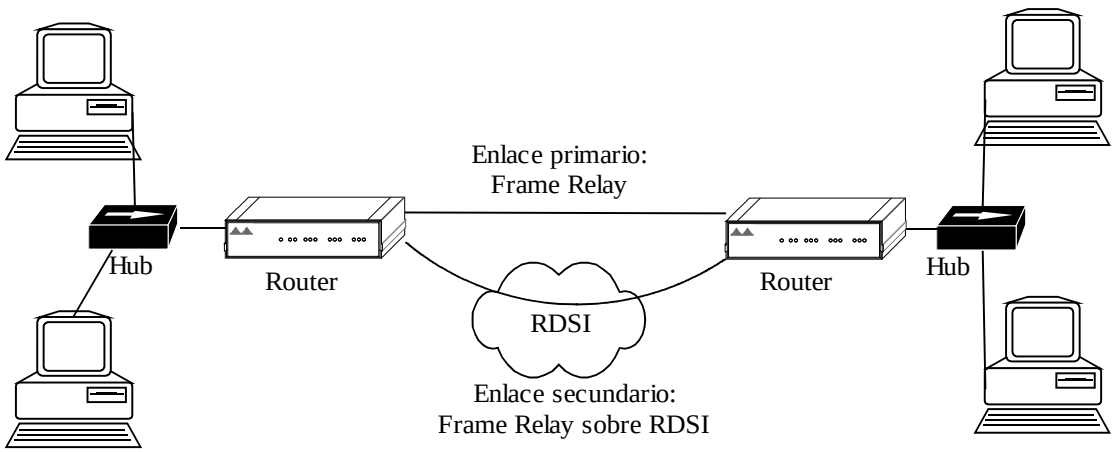

Figura 8.7: Topología de red

Una vez que tenemos montada la red de la imagen, hay que identificar las distintas redes físicas que existen en la misma, asignándole una dirección IP de clase C. A continuación procedemos a identificar las diferentes interfaces que existen y a asignarles una dirección IP, de acuerdo con la red física en la que se encuentren.

8.4.2.2 Configuración de los interfaces del router

En primer lugar, lo que debemos hacer es agregar el dispositivo Frame Relay. Para ello hay que ejecutar el comando **SET DATA-LINK FRAME-RELAY** una vez situado en el prompt de configuración Config>.

A continuación debemos asignar las direcciones IP al router y configurar su tabla de encaminamiento. Para asignar las direcciones IP utilizamos el comando **ADD ADDRESS** desde el menú de configuración del protocolo IP, al que se accede tecleando **PROTOCOL IP** desde el Proceso 4 (Config>). Hay que añadirle una dirección tanto al interfaz LAN (Ethernet) como al interfaz serie.

Seguidamente debemos añadir las rutas necesarias a la tabla de encaminamiento del router con el comando **ADD ROUTE**. Las rutas que debemos añadir, tomando como ejemplo la siguiente red, son:

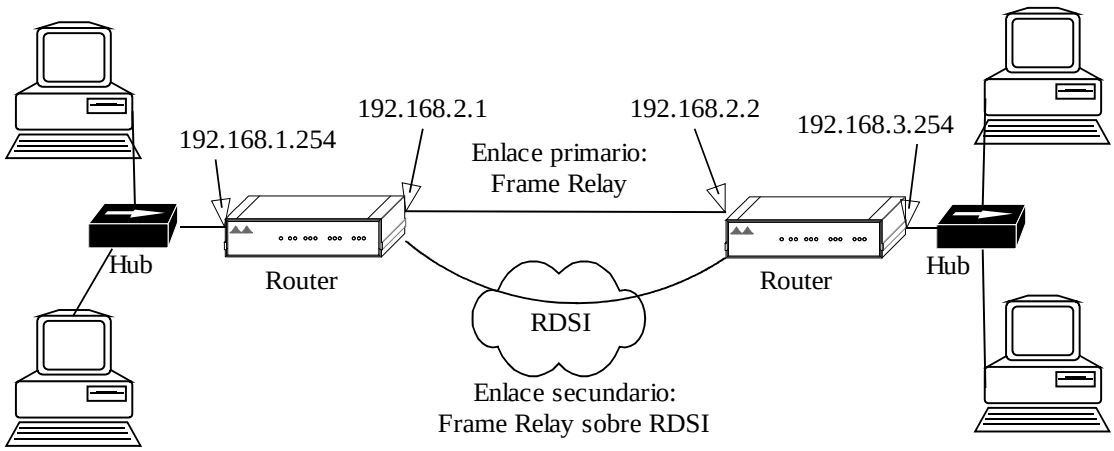

Figura 8.8: Topología de red con direcciones IP

ROUTER IZQUIERDA

Destino	Gateway	Netmask
192.168.1.0	. . . .	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	192.168.2.2	255.255.255.0

ROUTER DERECHA

Destino	Gateway	Netmask
192.168.1.0	192.168.2.1	255.255.255.0
192.168.2.0	. . . .	255.255.255.0
192.168.3.0	. . . .	255.255.255.0

Tabla 8.5: Tablas de encaminamiento de los routers

Para entrar en el menú de configuración del interfaz Frame-Relay debemos teclear **NETWORK (Número de interfaz asignado).** Este menú de configuración se identifica por el prompt *FR Config*>. A continuación debemos añadir los circuitos virtuales permanentes (PVCs) que necesitemos. Para ello debemos utilizar el comando **ADD PVC-PERMANENT-CIRCUIT** desde el menú de configuración del interfaz Frame-Relay. También hay que utilizar el comando **ADD PROTOCOL-ADDRESS** para agregar el protocolo estático y asignar el mapa de direcciones. Debemos *deshabilitar la actividad de gestión* mediante el comando **DISABLE LMI**. También debemos utilizar el comando **ENABLE CIR-MONITOR** para habilitar la

opción de monitorización de circuito impuesta por la tasa de transmisión configurada previamente mediante el comando **ADD PVC-PERMANENT-CIRCUIT**.

A continuación hay que crear el interfaz de backup. Para crear el interfaz de backup Frame Relay sobre RDSI hay que utilizar el comando **ADD DEVICE FR-DIAL**.

```
Config> ADD DEVICE FR-DIAL
Type basic access ISDN [2] : 1
Ifc number to delete: 7

If you are going to config more than two ISDN interfaces, you must config what
they have CSR:F011640 and CSR:F011660 over the ISDN 2 connector.
Added FR-DIAL interface with num: 3
Config>
```

Si utilizamos el comando **LIST DEVICES** se puede observar que se han creado dos nuevos interfaces, el interfaz base RDSI con el número 2, asociado al conector del acceso básico número 1, y el interfaz lógico de backup de Frame Relay con el número 3.

```
Config> LIST DEVICES

Con      Ifc   Type of interface    CSR      CSR2     int
---      4     Router->Node         0                 0
---      5     Node->Router         0                 0
LAN      0     Ethernet             9000000           1C
WAN1     6     X25                  F001600  F000C00  9E
WAN2     1     Frame Relay          F001620  F000D00  9D(Disabled)
ISDN 1   2     ISDN                 F001640  F000E00  9C
ISDN 1   3     Channel B: FR        0        0        0
ISDN 1   7     ISDN D channel       A000000           1B(Disabled)
ISDN 2   8     ISDN D channel       A200000           1B(Disabled)
ISDN 2   9     ISDN B channel       F001660  F000F00  9B
Config>
```

Si entramos en el menú de configuración del interfaz base RDSI, con el comando **NETWORK 2**, podemos observar que este interfaz es de tipo conmutado, por lo que no es necesario configurarle nada más.

```
Config> NETWORK 2
ISDN Config
Config ISDN>
```

Para configurar los parámetros asociados a un interfaz de backup de Frame Relay RDSI, hay que introducir en el prompt de configuración *Config>* el comando **NETWORK** seguido del número del interfaz de backup de Frame Relay a configurar.

```
Config> NETWORK 3
Circuit Config
Circuit Config>
```

Debemos utilizar el comando **SET DESTINATION-ADDRESS** para determinar la dirección RDSI a la que se efectuarán las llamadas RDSI de este interfaz de backup Frame Relay. También debemos introducir el comando **ENABLE INCOMING**, para que el router acepte las llamadas entrantes.

8.4.2.3 Asociar el interfaz principal Frame Relay al enlace de backup de Frame Relay secundario

Para asociar un interfaz principal Frame Relay a un enlace de backup de Frame Relay secundario, se debe introducir en el prompt de configuración:

```
Config> FEATURE WRS-BACKUP-WAN
WAN Back-up User Configuration
Back-up WAN>
```

A continuación se configura la asociación entre el interfaz principal y el de backup:

```
Back-up WAN> ADD
Primary Interface:1
Secondary Interface:3
Recovery Time:2
Back-up WAN>
```

El interfaz primario (Primary Interface) debe ser el número del interfaz Frame Relay del que se desea hacer backup, esto es, por el que en funcionamiento normal se transmiten los datos. El interfaz secundario (Secondary Interface) debe ser el número del interfaz de backup de Frame Relay por el que se realizarán las llamadas RDSI en caso de caída del enlace primario.

Una vez que se tiene asignada una red RDSI que permite realizar el backup del interfaz de Frame Relay, se pueden configurar los valores de los PVCs que se quieran utilizar para volver a direccionar el tráfico de backup. Se procede del modo siguiente:

```
FR config> SET CIRCUITS-BACK-UP
Circuit number[16]? 16
Frame Relay Back Up circuit number[17]? 0
ISDN Back Up to ISDN[17]?
Always Back Up to ISDN? [No]:(Yes/No)? Y
Encrypt Back up information? [No]:(Yes/No)? N
FR config>
```

De esta manera estamos configurando el router para que el PVC número 16 siempre realice el Backup hacia el interfaz Frame Relay sobre RDSI, y una vez que se restaure su conexión vuelva a establecer la comunicación.

8.4.2.4 Comprobación del funcionamiento

Para comprobar si el funcionamiento del backup es el correcto, podemos proceder a establecer una comunicación entre los dos routers a través del enlace primario, y posteriormente provocar un fallo en la red desconectando el cable en uno de los extremos y observar si el backup funciona correctamente.

Efectivamente, cuando cae el enlace primario, se activa el secundario. Si posteriormente se restablece el enlace primario, automáticamente se cuelga la llamada RDSI y continúa la comunicación por el enlace primario.

Conclusiones

Tras la realización de este documento se ha llegado a varias conclusiones sobre el router NUCLEOX PLUS:

- Este dispositivo nos da una solución sencilla para satisfacer las necesidades básicas de routing que pueden surgir en una red determinada. Sin embargo, tiene un nivel de funcionalidad limitado comparado con otros routers del mercado.

- El proceso de configuración del equipo es muy simple y nos ofrece la posibilidad de modificar la configuración establecida, o establecer nuevas configuraciones de una forma simple y rápida.

- Además, este dispositivo también nos da la posibilidad de poner en práctica y evaluar aspectos básicos de la redes IP actuales como es el caso del mecanismo de NAT, o de los protocolos de encaminamiento dinámico, como RIP.

- Las interfaces WAN del equipo (2 interfaces serie y 2 accesos básicos RDSI) nos ofrecen la posibilidad de experimentar con 2 de las tecnologías más utilizadas en la actualidad, como son PPP y Frame Relay.

- También se puede utilizar como introducción a una tecnología novedosa como es la Voz sobre IP (VoIP). El NUCLEOX PLUS nos sirve para poder comprender las necesidades de Calidad de Servicio (QoS) que se requiere en el tráfico de datos con requisitos temporales, como es el caso de la VoIP.

Bibliografía

Capítulo 1:

- D.E. Comer, "*Internetworking with TCP/IP. Volume I: Principles, Protocols and Architecture*", Ed. Prentice-Hall, 4ª edición, ISBN 0-13-018380-6.
- "*Router Teldat. Configuración TCP/IP*", Doc. DM502 Rev. 8.30, Febrero, 2000. Disponible en <www.teldat.es>.

Capítulo 2:

- "*Router Teldat. Configuración y Monitorización*", Doc. DM504 Rev. 8.30, Abril, 2000. Disponible en <www.teldat.es>.

Capítulo 3:

- "*Router Teldat. Interfaz PPP*", Doc. DM510 Rev. 8.31, Mayo, 2000. Disponible en <www.teldat.es>.
- A. López, A. Novo, "*Protocolos de Internet. Diseño e implementación en sistemas UNIX*", Ed. Ra-Ma, ISBN 84-7897-382-6.
- B.Lloyd, W.Simpson,"*PPP Authentication Protocols*", RFC 1334, Octubre 1992.
- W.Simpson, "*PPP Challenge Handsahke Authentication Protocol (CHAP)*", RFC 1994, Agosto 1996.
- "Práctica 2: Transmisión de datos en banda vocal vía módem. Laboratorio de Fundamentos de Telemática", F. Burrull, J. Garcia-Haro, F. Monzó-Sánchez.
- W. Stallings, "*ISDN and broadband ISDN with Frame Relay and ATM*", Ed. Prentice-Hall, 4ª edición, ISBN 0-13-973744-8.

Capítulo 4:

- "*Router Teldat. Frame Relay*". Doc. DM 503 Rev. 8.40, Septiembre, 1999. Disponible en <www.teldat.es>.
- G. Held, "*Frame Relay networking*", Ed. John Wiley & Sons, ISBN 0-471-98578-3.
- "*Internetworking Technologies Handbook*", 3rd ed., by Inc. Cisco Systems.

Capítulo 5:

- K. Egevang, P. Francis, "*The IP Network Address Translator (NAT)*", RFC 1631, Mayo 1994.
- P.Srisuresh, K. Egevang, "*Traductor de Dirección de Red Tradicional*", RFC 3022, Enero 2001.

Capítulo 6:

- "*Router Teldat. Voz sobre IP*", Doc. DM522 Rev. 8.4, Octubre, 2000. Disponible en <www.teldat.es>.
- J. Davidson, J. Peters, "*Fundamentos de voz sobre IP*", Ediciones Cisco, 2001.

Capítulo 7:

- D.E. Comer, "*Internetworking with TCP/IP. Volume I: Principles, Protocols and Architecture*", Ed. Prentice-Hall, 4ª edición, ISBN 0-13-018380-6.

- "*Router Teldat. Protocolo RIP*", Doc. DM518 Rev. 8.00, Julio, 1999. Disponible en <www.teldat.es>.

Capítulo 8:

- "*Router Teldat. Configuración de Backup de Frame Relay por RDSI*", Doc. DM511 Rev. 8.30, Febrero, 2000. Disponible en <www.teldat.es>.
- "*Router Teldat. Backup Wan Reroute (WRR)*", Doc. DM527 Rev. 8.30, Mayo, 2000. Disponible en <www.teldat.es>.