UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTA DE ESTUDIOS SUPERIORES

CAMPUS ARAGÓN

TEMA **IMPLEMETACION DE SISTEMAS REDUNDANTES CISCO PARA UNA RED FRAME RELAY Y ACCESO DE INTERNET**

ESPECIALIDAD **COMUNICACIONES Y ELECTRONICA**

ALUMNO.- **LUIS FELIPE MARIN LOPEZ**

PROFESOR.- **ING. PABLO LUNA ESCORZA**

CARRERA.- **ING. MEC. ELEC.**

NO. CTA.- **09201909-8**

AGRADECIMIENTOS

Este trabajo es un producto del gran esfuerzo que ha infundido en mi familia, en particular mis padres que me dieron la oportunidad de crecer como persona y profesionista; y no olvidando a mis hermanos que me dieron el apoyo en cada momento en la Universidad y en la elaboración de la tesis.

Agradeciendo también a mis profesores dentro de la Universidad, que con su esfuerzo de cada uno de ellos dieron paso al camino como profesionista. Así como al asesor de esta tesis que tuvo la flexibilidad de apoyarme en cada capitulo.

Finalmente, agradeciendo a esta Institución, la Universidad Nacional Autónoma de México (UNAM), y en consecuencia a la Facultad de Estudios Superiores Aragón, (FES ARAGON); por dirigirme a un camino de bien para ser profesionista de la carrera Ingeniería Mecánica Eléctrica (IME), de la cual me siento orgulloso.

INDICE

INTRODUCCION

Cuando cursaba la carrera de Ingeniería Mecánica Eléctrica, en la FES Aragón, iniciaba el consumo de computadoras por alumnos de las Universidades, y me incursione en el mundo tecnológico de la computación que ofrece grandes beneficios como universitarios y profesionales. Sin embargo, ahí no se detuvo el descubrimiento de nuevos horizontes en materia de tecnología, y creo que lo que me motivo en realizar esta tesis, fue el sentirme afortunado en vivir en el inicio de la era de la inmensa red compartida en todo el mundo, que es Internet. Para mi fue un salto quántico, ver como se revolucionaba el modo de transferir datos, que puedo atreverme a decir, que también modifico el modo de vivir de mucha gente e incluso en nuestro país es una realidad con transferencias vía Internet, intercambio de información día a día, como el correo electrónico, charlas en línea con tus amigos, transacciones de cuentas bancarias, y más. Este rápido cambio de la industria de cómputo y la industria de telecomunicaciones dio paso a consolidarse como una herramienta muy poderosa. También en mis días como universitario, solamente utilizaba este servicio sin considerar lo implica toda la infraestructura que hay detrás de esta red, así como miles de personas que utilizamos telefonía celular, telefonía convencional, televisión por cable, etc., que solamente utilizamos sin tener algún interés de cómo funcionan estos sistemas. Por lo que estoy convencido que la red de Internet ya no es tan solo un sistema aislado a ciertos grupos o industrias sino que ha sido globalizado para todo tipo de población e industria que tenga la infraestructura para acceder a esta. Aunque para mí, la elaboración de esta tesis fue más que un interés por la red de Internet, mas bien fue como las industrias salvaguardan este servicio como parte de su estrategia financiero y tecnológico, esto ha sido algo tan común, que muchas industrias protegen este servicio que tenga las menos averías posibles o cortes de comunicación, ya que de esto depende su ingreso económico de manera directa o indirecta, haciendo transacciones, anuncios publicitarios, catálogos de productos, etc.

Por esta situación tuve la inquietud de investigar sobre sistemas redundantes, que pudieran ser efectivos y de gran utilidad en las industrias, y sin costo elevado, es decir aprovechar los recursos que se tiene en las industrias y adaptarlos a ella. Pero para poder entender estos sistemas, necesitamos adentrarnos a los campos de telecomunicaciones. Donde yo recabo información en el Capitulo I que habla de las redes LAN, donde se inicia una red aunque geográficamente pequeña, es donde se generan la transmisión de datos. Luego mencionara en el Capitulo II el terreno de cómo dos rede LAN pueden interactuar mutuamente aun geográficamente con distancias amplias, por ello el estudio de las redes WAN. Por otro lado, para poder integrar estas redes necesitamos de un direccionamiento para saber como dirigir los datos por ello la necesidad del uso del protocolo TCP/IP que se indicara en el Capitulo III.

Ahora no tan solo es necesario implementar redes, sino que ahora también se necesita rapidez y alta disponibilidad de rendimiento de redes que presenten las menores fallas posibles para garantizar el servicio. Pero cabe señalar que las empresas hoy en día requieren servicios de redes publicas, y han puesto la mira en redes con alto rendimiento como Frame Relay, que es una buena opción para integrar estaciones remotas a un nodo central, es en el Capitulo IV que se hablara de los detalles de conectividad y beneficios que nos proporciona Frame Relay. Otro de los interés de cualquier industria es crear sistemas casi infalibles a múltiples variables que podrían interrumpir el servicio de red, es

por ello que en el Capitulo V se describa el sistema redundante HSRP de Cisco Systems, que sin duda solo realiza un sistema redundante en hardware, es decir, el sistema de redundancia recae sobre el dispositivo denominado ruteador que se vera con precisión, en este mismo capitulo, desde sus características de hardware hasta el sistema operativo que invoca a los comando para poder configurarlo. Pues las industrias medianas y grandes utilizan estos dispositivos para obtener comunicación entre dos o más oficinas que están separadas geográficamente. Con estos argumentos se puede plantear esta tesis, el cliente que tenga un acceso de Internet y utilice un sistema de Router Cisco System puede aprovechara redundar su enlace, pero como antes lo menciones solo esta para hardware, es decir, si falla un router el otro inmediatamente tomara el mando, pero el enlace es uno de los principales motivos de falla. Por ello aquí se plantea una redundancia de enlace y de dispositivos que daría una mayor fiabilidad en el servicio de Internet, teniendo en cuenta que usuarios del corporativo y usuarios externos acceden a este sistema por lo que es vital para una empresa este servicio.

Por ultimo, el planteamiento anterior solo resolvería el problema de acceder a Internet para los usuarios externos, pero para los usuarios internos tendría la limitante de que solo podrían acceder a este acceso si estuvieran en el mismo segmento de red, ya que si están en otra oficina o sucursal que los separa geográficamente y el servicio de la red Frame Relay estuviera caída en tan solo ese punto, se vería afectada ya que no podrían revisar el servicio de Internet desde ese punto o tal vez mas si dependen de otro servidor que no sea precisamente de Web, entonces por eso se mostrara en esta tesis el otro sistema de respaldo DDR de Cisco Systems, que se mencionara en el Capitulo VI, ultimo de la tesis. Con esto se podrá garantizar servicios fiables.

CAPITULO I REDES LAN

I.1 REDES DE ÁREA LOCAL

En la sociedad actual es difícil no saber como usar una computadora personal (PC). Muchas personas crecen usando la PC y algunas se vuelven competentes. Históricamente, una PC había estado bastante aislada, permitiendo a un solo usuario trabajar en un proyecto sin tener acceso a recursos externos o el beneficio de comunicarse con otros colaboradores.

Una red de área local (LAN) es una forma de conectar PCs individuales de manera que puedan compartir recursos limitados. Estos recursos incluyen elementos como unidades de disco, archivos (base de datos) e impresoras. Además, la red permite una mayor interacción y comunicación entre los miembros de una red. Una red LAN se grafica limitada. Las PCs conectadas a la red están localizadas dentro de un área geográfica limitada. Las PCs conectadas a la red se llaman nodos. De esta manera característica los nodos que forman una LAN están en una sola habitación o en un solo edificio. Esta relación de computadoras se muestra en la figura 1.1.

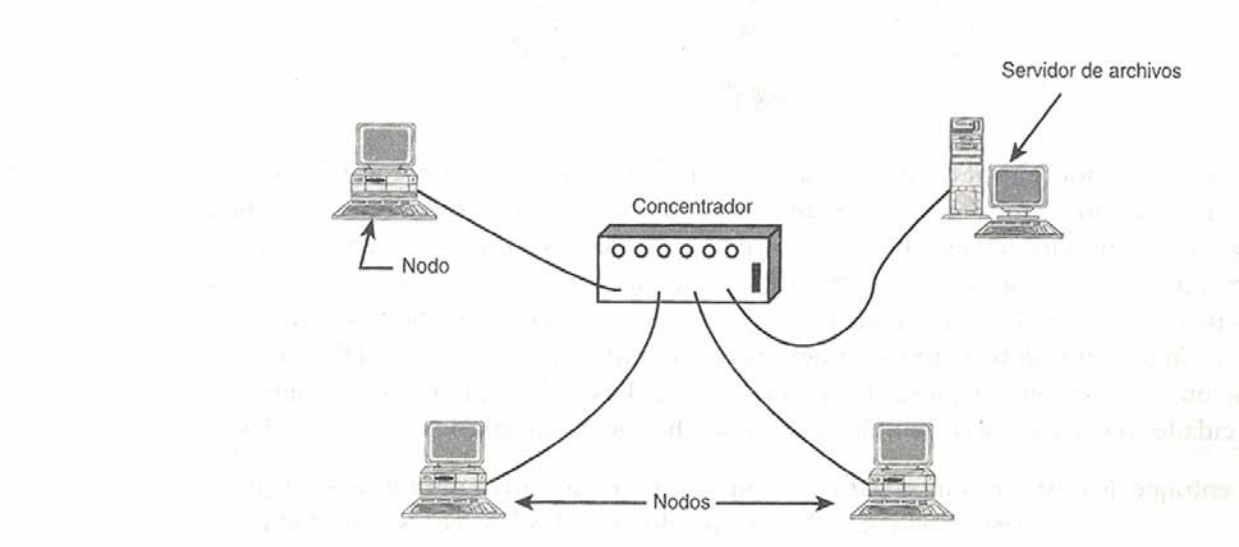


FIGURA 1.1 RED LAN POR PC´s INDIVIDUALES

Una red LAN difiere del enfoque antiguo de host y terminal en que cada PC conectada a la LAN es una computadora hecha y derecha por si misma. Las computadoras individuales pueden ser menos potentes que un mainframe, pero permiten mayor libertad de computación a los usuarios individuales. También es mas fácil ampliar una LAN; comúnmente todo lo que necesita hacer es conectar otra PC y asegurarse de que puede comunicarse con otras computadoras en la LAN.

I.1.1 EVOLUCIÓN HISTÓRICA

En las décadas de los 60 y 70 la informática se concebía como un servicio estructurado jerárquicamente, reflejando en gran medida la estructura interna de las organizaciones. En la década de los 80 surgieron las redes de área local a la vez que

nuevos métodos de organización, proponiendo una estructuración de las organizaciones basada en grupos de trabajo especializados y coordinados entre sí mediante mecanismos más dinámicos y flexibles. En la década de los 90 las redes de área local están dejando de ser entes aislados y ofrecen a las grandes organizaciones la posibilidad de crear redes virtuales extensas mediante nuevas tecnologías de interconexión de redes.

El ordenador personal (PC, ***Personal Computer***) cambió las ideas: Se pasó de utilizar un ordenador central, concebido para una serie de trabajos específicos, hacia el uso de herramientas en el puesto de trabajo que permitieran asimilar la información, soportar decisiones y, más recientemente, mejorar la eficiencia del personal y en consecuencia la productividad de las empresas. El crecimiento del número de ordenadores y la llegada del proceso distribuido generó nuevas necesidades en las comunicaciones entre ordenadores. Anteriormente esto se basaba en conectar terminales a un gran ordenador central, frecuentemente a largas distancias. La llegada del PC empezó a introducir necesidades de compartir información y recursos, como pueden ser impresoras y discos, dentro de un área local, y normalmente realizando operaciones de alta velocidad.

Esta necesidad condujo al desarrollo de la Red de Área Local (***Local Area Network***, LAN). Inicialmente se pensaba que una red de área local podría extenderse a través de una planta de un edificio o como mucho a lo largo de éste. A partir de ese instante, y en respuesta al meteórico crecimiento de las implantaciones de redes, se desarrollaron nuevas capacidades que han colocado a las redes de área local al nivel de los métodos de comunicaciones más sofisticados de la actualidad. Desafortunadamente el mercado creció dejando a las organizaciones de estándares rezagadas respecto a los programas de desarrollo de las organizaciones comerciales. Como consecuencia de ello, aparecieron muchos tipos de redes locales diferentes unas de otras, creando un complejo mercado.

I.1.2 ENFOQUES PARA LA CONECTIVIDAD

Cuando una compañía u organización busca establecer una LAN, debe decidir un enfoque para desarrollar la red. Hay dos enfoques: redes cliente/servidor y redes punto a punto. Ambos enfoques se exponen en las secciones I.4.2.1 y I4.2.2; respectivamente.

I.2 MEDIOS DE TRANSMISION

Los medios de transmisión son un importante pieza para las redes LAN ya que en ella crea la facilidad de trafico de información y dependiendo el hardware que se utilice será el tipo de medio que integraremos a nuestra red LAN, en el diseño se tendrá que poner énfasis en costos, tecnología utilizada y velocidad de transmisión requerida. Como se describen en los siguientes temas.

I.2.1 CABLES

Los cables son el medio físico para conectar las estaciones de trabajo con los servidores de archivo y con otros componentes de la red. Esto se observa en la parte posterior de una computadora; se puede ver el cable que usa la red. Los administradores de la red y los planificadores de red necesitan preocuparse, sobre todo, por el tipo de cable instalado en una red, pero también puede haber otras preocupaciones.

I.2.1.1 TIPO DE CABLES

Se encuentran disponibles muchos tipos de cable, pero solo hay unas cuantas categorías importantes. Estas categorías incluyen las siguientes:

- Coaxial
- Par trenzado
- Línea telefónica digital
- Fibra óptica

I.2.1.1.1 CABLES COAXIALES

El término de coaxial significa que tiene un eje compartido. Esta es la forma exacta como esta construido un cable coaxial. Consiste en un solo alambre sólido aislado alrededor. Este aislamiento lo rodea a su vez un alambre en malla y el cable entero esta rodeado por aislamiento adicional. La figura 1.2 muestra un ejemplo de la apariencia de un cable coaxial.

Observara que el cable coaxial es muy parecido al cable usado para la televisión por cable. Casi idéntico, aunque hay unas cuantas diferencias técnicas en las especificaciones. Por lo general se usan tres tipos de cable coaxial en las redes, RG-8 y RG-11 son los cables más gruesos y los que se confunden con mayor frecuencia con los cables para televisión por cable. RG-58 es un poco mas delgado y mas fácil de trabajar con el.

El cable coaxial, aunque bastante aceptable para propósitos de conectividad, rara vez se usan en las instalaciones de red nuevas. La razón es que es más fácil trabajar con otros cables y pueden proporcionar el mismo (o mejor) rendimiento.

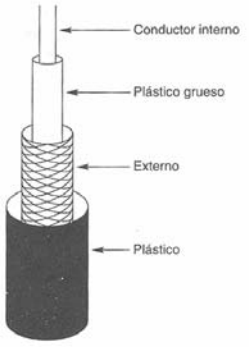


FIGURA 1.2 EL CABLE COAXIAL

Se conocen dos tipos de cable coaxial:

- El cable de Banda Base

- El cable de Banda Ancha

Las señales eléctricas de Banda Base se pueden transmitir por medio de cables coaxiales a velocidades de 10 Mbits/s en distancias de hasta 1 Km. La Banda Base utiliza la técnica denominada CSMA/CD (Carrier Sense Mutiple Access / Collision Dectection, Acceso Múltiple con Sensibilidad de Portadora con Detección de Colisiones) para acceder al medio. Todos los dispositivos de la red usan los mismos protocolos para acceder y utilizar el medio físico.

En Banda Ancha, las señales se modulan sobre una onda portadora sinusoidal. Puede transmitirse muchas señales simultaneas utilizando varias frecuencias portadoras suficientemente separadas entre si como para evitar los efectos de íntermodulación. El cable coaxial de Banda Ancha opera sobre una serie de canales sin relación. A cada canal se asigna una frecuencia y puede operar con diferentes protocolos. Estos sistemas se utilizan en operaciones punto a punto en grandes distancias.

I.2.1.1.2 CABLES DE PAR TRENZADO

Los cables de par trenzado se llaman así debido a que constan de varios alambres de cobre sólido trenzados entre si. El cable comúnmente contiene cuatro pares de alambre sólido para un total de ocho cables. Cada par esta trenzado y, luego, los cuatro pares se trenzan entre sí. Existen dos categorías de par trenzado: UTP (par trenzado desprotegido; Unshielded Twisted Pair) y STP (par trenzado protegido; Shielded Twisted Pair). La única diferencia entre los dos es que el cable STP tiene una capa de asilamiento extra entre los pares: esto ayuda a reducir la interferencia eléctrica potencial a velocidades altas de datos.

En la actualidad, hay en el mercado cinco categorías de cables de par trenzado:

Categoría 1 y 2. Estas categorías están consideradas para transmisiones de voz y datos lentos (hasta 1 Mbps). La mayor parte del cableado telefónico (que también usa el cable de par trenzado) queda dentro de estas categorías y es inadecuado para el uso de redes modernas.

Categoría 3. Esta categoría esta considerada para velocidades de red hasta de 10 Mbps.

Categoría 4. Esta categoría esta considerada para velocidades hasta de 16 Mbps.

Categoría 5. Esta categoría esta considerada para velocidades hasta de 100 Mbps.

No existe una gran diferencia de precio entre las categorías de cable y, la labor para instalar cada categoría es la misma. Por esta razón, es un buen consejo instalar cableado de la categoría 5 si esta haciendo alguna instalación de red nueva. Esto es válido aunque no vaya a usar la velocidad completa especificada para el cable; la idea es permitir el crecimiento futuro de su red sin tener que reinstalar cable mas adelante.

I.2.1.2 ESTÁNDARES EIA/TIA

De todas las organizaciones aquí, la EIA/TIA tiene el mayor impacto en las normas relacionadas con los medios de red. Específicamente, los estándares EIA/TIA 568A y EIA/TIA 569-A han sido y continúan siendo las más ampliamente utilizadas para la actuación técnica de los medios de red. Los estándares EIA/TIA especifican los requisitos mínimos para entornos de múltiples productos y de múltiples fabricantes. Permiten la planificación y la instalación de sistemas LAN sin dictar el uso de equipos específicos, de modo que dan a los diseñadores de LAN la libertad de crear opciones de mejora y expansión.

Esta norma establece dos estándares (A y B) para el cableado Ethernet 10Base-T determinado que color corresponde a cada pin del conector RJ-45. El estándar 568B, también llamado especificación AT&T es usado mas frecuentemente, pero muchas instalaciones están diseñadas con el estándar 568-A, también denominado RDSI. Normalmente un cableado esta armado respetando el mismo estándar (A o B) en ambos extremos del cable. Estos cables se utilizan para:

- ✓ Conectar una estación de trabajo a la roseta de una instalación de cableado estructurado.
- ✓ Conectar la patchera con el hub o switch en el armario del cableado.
- ✓ Conectar directamente una estación de trabajo a un hub o a un swicth.
- ✓ Conectar un hub con el puerto “crossover” de otro dispositivo.

Como se muestran en las siguientes figuras 1.3 Y figura 1.4 los dos estándares:

Norma de cableado 568-A

Pin#	Par #	Función	Color del Cable	10/100 Base-T Ethernet	100 Base-T4 y 1000 Base-T Ethernet
1	3	Transmite	Blanco/Verde	Si	Si
2	3	Recibe	Verde/Blanco	Si	Si
3	2	Transmite	Blanco/Naranja	Si	Si
4	1	Telefonía	Azul/Blanco	No	Si
5	1	Telefonía	Blanco/Azul	No	Si
6	2	Recibe	Naranja/Blanco	Si	Si
7	4	Respaldo	Blanco/Marrón	No	Si
8	4	Respaldo	Marrón/Blanco	No	Si

FIGURA 1.3 NORMA DE CABLEADO 568-A

Norma de cableado 568-B

Pin#	Par#	Función	Color del Cable	10/100 Base-T Ethernet	100 Base-T4 y 1000 Base-T Ethernet
1	2	Transmite	Blanco/Naranja	Si	Si
2	2	Recibe	Naranja/Blanco	Si	Si
3	3	Transmite	Blanco/Verde	Si	Si
4	1	Telefonía	Azul/Blanco	No	Si
5	1	Telefonía	Blanco/Azul	No	Si
6	3	Recibe	Verde/Blanco	Si	Si
7	4	Respaldo	Blanco/Marrón	No	Si
8	4	Respaldo	Marrón/Blanco	No	Si

FIGURA 1.4 NORMA DE CABLEADO 568-B

I.2.1.2.1 CABLE RECTO

Un cable recto mantiene la conexión pin a lo largo de todo cable. Por lo tanto, el hilo conectado al pin 1 es el mismo en ambos extremos del cable. La figura 1.5 ilustra que el conector RJ-45 en ambos extremos tiene todos sus hilos en el mismo orden. Si mantiene los dos extremos RJ-45 de un cable de lado en la misma orientación, podrá ver los hilos de colores (o strips o pins) en cada extremo del conector. Si el orden de los hilos de colores es el mismo en cada extremo, el cable es recto.

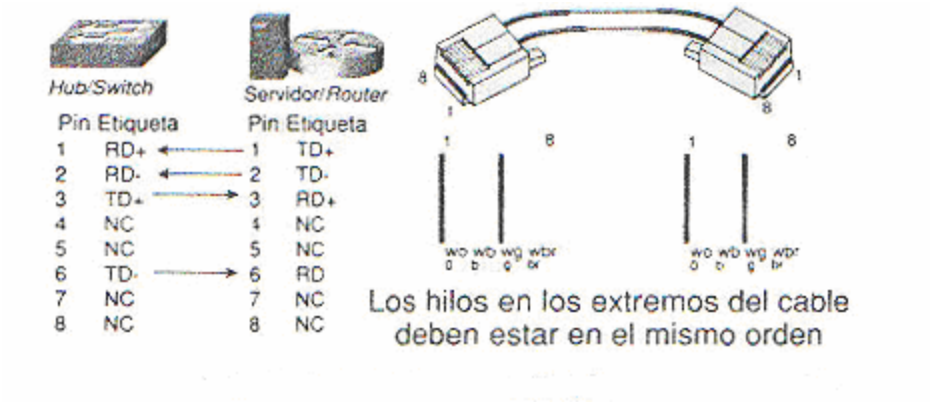


FIGURA 1.5 DIAGRAMA DE CABLE RECTO

Utilice un cable recto para conectar dispositivos tales como PC o Ruteadores a otros dispositivos, como hubs o switches. La figura 1.6 muestra las pautas de conexión cuando se emplea cable recto.

FIGURA 1.6 CONEXIÓN DE UN CABLE RECTO

I.2.1.2.2 CABLE CRUZADO

Se denomina así al patch armado utilizando el estándar A en un extremo y el B en el otro. Estos cables responden al estándar 568, y se utilizan para:

- ✓ Conectar hubs o switches entre sí.
- ✓ Conectar dos estaciones de trabajo aisladas, a modo de una mini-LAN.
- ✓ Conectar una estación de trabajo y un servidor sin necesidad de un hub.

Como se muestra en la siguiente figura 1.7 la configuración del cable Cruzado.

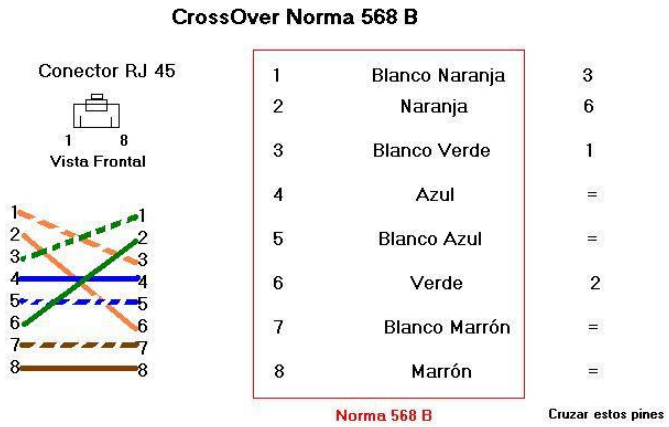


FIGURA 1.7 CONFIGURACION DE UN CABLE CRUZADO.

I.2.1.3 LÍNEAS TELEFÓNICAS

En este medio de comunicación de datos, el usuario conecta su terminal sobre una línea telefónica: la interfaz entre la terminal y el circuito telefónico es un MODEM. El portador de los datos es la red telefónica Pública.

La red telefónica ofrece dos tipos de circuitos para la transmisión de datos.

1. Línea Conmutada. Opera dentro de la red pública conmutada y el usuario puede ocupar aleatoriamente cualquier circuito de la red. La principal ventaja que se puede obtener de una línea conmutada es su bajo costo cuando el volumen de tráfico a cursar es pequeño. La lentitud de respuesta, la posibilidad de bloqueo y la

mala calidad de la línea son los principales inconvenientes que presentan una línea conmutada.

2. Línea dedicada. Las líneas dedicadas o privadas suelen ser de gran utilidad para aquellos usuarios que no pueden permitirse el retardo que supone establecer la conexión, o que no puede tolerar que la llamada se bloquee si todas las líneas están ocupadas. Además, los usuarios cuyo tráfico ocupa varias horas de enlace, puede ahorrar bastante dinero utilizando una línea dedicada.

I.2.1.4 CABLE DE FIBRA ÓPTICA

El cable de la fibra óptica es la solución de cableado más costosa disponible en la actualidad, pero también es la más capaz en función del rendimiento. Como podría suponer por el nombre de cable, la información se transmite a lo largo del cable por pulsaciones de luz en lugar de impulsos eléctricos. La luz es generada ya sea por un láser o por un LED y produce una señal que casi no es susceptible a la interferencia normal. El cable de fibra óptica puede soportar velocidades de transmisión de datos hasta de 800 Mbps.

Debido a que el cable de fibra óptica se hace con vidrio o con plástico de grado óptico no se pueden usar las mismas herramientas como las que usan cuando se trabaja con cobre. Además, el cable es menos tolerante al maltrato. Por estas razones es aconsejable dejar la instalación de la fibra óptica a instaladores profesionales que tienen experiencia para cumplir las necesidades especiales del cable.

Se conocen dos tipos de modalidades de fibra óptica:

- Unimodal
- Multimodal

La fibra óptica unimodal permite la propagación de un solo haz de luz a través del cable, mientras que la fibra óptica multimodal permite varias señales ópticas propagarse a través de él. El cable unimodal permite manejar datos a mayores distancias, utilizando un Ancho de Banda también mayor. El cable unimodal opera en conexiones punto apunto. La fibra óptica unimodal emplea generalmente un rayo láser como fuente emisora.

Debido a que el cable mutimodal permite la propagación de varias señales luminosas (que viajan a diferentes ángulos), llegan a diferentes distancias, por lo tanto causa que cada señal arribe a diferente tiempo. La fuente emisora de luz que utiliza es un LED (Light Emisor Diode, Diodo Emisor de Luz). Las características del cable multimodal le permiten operar en conexiones de grupo.

- Los cables de fibra óptica ofrecen muchas ventajas frente a los cables que utilizan señales eléctricas para transmitir datos:

- Mayor velocidad y capacidad de transmisión (en el orden de Gigabits/s).

- Inmunidad total ante las interferencias electromagnéticas.

- Los costos de instalación y mantenimiento para grandes y medianas distancias son menores que las que se derivan de las instalaciones de cables eléctricos.

- La fibra óptica es le medio de transmisión ideal donde se necesita de mucha seguridad, puesto que es prácticamente imposible intervenir.

I.2.2. CONECTIVIDAD INALÁMBRICA

Para propósitos especiales las redes inalámbricas están ganado terreno, donde el cable físico es poco práctico o imposible. Se usa una amplia variedad de métodos técnicos para establecer redes inalámbricas, incluyendo microondas, amplio espectro, infrarrojo y celular (como en los teléfonos celulares). Este tipo de redes es bueno para distancias cortas entre edificios (como del otro lado de la calle) o en situaciones móviles.

Muchas personas se preocupan de la conectividad inalámbrica no sea segura, pero la amenaza a la seguridad se exagera mucho. La conectividad inalámbrica usa precauciones hacen mas segura la conectividad inalámbrica que el uso de cable de cobre no protegido.

Las soluciones de conectividad inalámbrica pueden ser costosas. Aunque no tan costosas como la fibra óptica, no obstante le pesan a la carrera. Investigue todas sus opciones de cableado antes de comprometerse con el inalámbrico.

I.3 TECNOLOGIAS DE LAN

A continuación de definirán las diferentes tecnologías LAN, en la actualidad.

I.3.1 ETHERNET

Ethernet Es el método de acceso más común en el entorno de LAN. La amplia aceptación de Ethernet como método de acceso se debe al bajo costo de hardware de Ethernet y al alto rendimiento que se logra. El hardware Ethernet esta disponible con cientos de fabricantes y al parecer los precios están bajando todo el tiempo.

La especificación Ethernet fue desarrollada originalmente mediante los esfuerzos de Digital Equipment Corporation, Intel y Xerox. Más tarde, a mediados de la década de 1980, Ethernet fue codificado por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE; Instutute for Electrical and Electronic Engineers) como IEEE 802.3. Ahora, todos los que producen cualquier cosa diseñada para una red Ethernet siguen esta norma.

La forma como funciona Ethernet puede describirse mejor explicando como ocurre la comunicación. Ethernet usa tecnología conocida como CSMA/CD, lo cual significa Transportador Sensible de Acceso Múltiple/Detección de Colisión (Carrier Sense Multiple Acces/Collision Detection). La comunicación sigue estos pasos generales:

1. El hardware de acceso que espera transmitir una trama debe escuchar el cable para ver si alguien más ya esta transmitiendo.

2. Si nadie más esta transmitiendo, envía unas cuantas tramas y, luego, hace una pausa breve para que otros puedan transmitir, si lo desean.

3. Si ocurre una colisión entre dos piezas de hardware de acceso que transmiten al mismo tiempo, ambas piezas esperan un tiempo de duración aleatoria, y luego, comienzan de nuevo en el paso 1.

Estos tres pasos se repiten con tanta frecuencia como sea necesario hasta que el mensaje completo termina de transmitirse. La idea de estos tres pasos es sencilla, lo cual es la causa de que puedan llevarse a cabo con facilidad en el hardware y por eso los precios son tan bajos.

La velocidad característica a la que se refiere la información por medio de Ethernet es de 10 Mbps, pero puede variar, dependiendo del tipo de especificación de cableado para la que este diseñada la implementación Ethernet. Estas especificaciones incluyen las siguientes:

- 10Base2. Este es un Ethernet de 10 Mbps basado en un cable coaxial RG-58 (delgado) de 50 Ohms. Los segmentos de cable pueden tener hasta 182 metros de largo con hasta 30 nodos a lo largo del segmento. Ambos extremos del cable deben estar determinados y un extremo debe estar aterrizado.

- 10Base5. Este es un Ethernet de 10 Mbps basado en un cable coaxial RG-11 de 50 Ohms. (Puede usar cable RG-8 si hay un transceptor entre la conexión del cable y la NIC). Los segmentos de cable pueden tener hasta 492 metros con hasta 100 nodos por segmento. Ambos extremos del segmento deben estar terminados y un extremo debe estar aterrizado.

- 100BaseVG. Este es un Ethernet de 100 Mbps basado en cuatro pares de cables de par trenzado categoría 3 (o mejor). Esta especificación es diferente de la 100BaseT4 (véase la sección de FastEhternet) por que usa una tecnología de acceso llamada de demanda en lugar de CSMA/CD.

Las demás se verán en la sección de FAST Ethernet.

I.3.2 FDDI Y CDDI

Aunque tanto Ethernet como Token-Ring permiten velocidades para redes de trabajo pequeño y mediano, algunas velocidades de las redes son mucho mayores.

Aquí es donde entran en escena FDDI (Interfaz de Datos Distribuidos por Fibra [como en fibra óptica]; Fiber Distribuited Data Interfcace) y CDDI (Interfaz de Datos Distribuidos Por Cobre [Cooper Distribuited Data Interfaz]). Estos métodos de acceso todavía son relativamente nuevos y por consiguiente, bastante costosos.

Las redes FDDI y CDDI tipo I permiten velocidades de transmisión de datos de 100Mbps, en tanto el tipo II permiten velocidades de transmisión hasta de 600 Mbps. Estas velocidades se logran a través de cables de cobre comunes para (CDDI) con las longitudes de segmento de red ya mencionadas para Ethernet. Cuando se usa fibra óptica (para FDDI), las longitudes del segmento pueden tener hasta varios kilómetros de longitud, dependiendo del grado de cable de fibra óptica usado.

Tanto FDDI como CDDI pueden verse como una extensión de la especificación Token-Ring. Sin embargo, difieren en el número de señales que se pasa en cualquier momento determinado. Mientras que Token-Ring se basa en una sola señal, FDDI y CDDI se basan en muchas señales que dan vuelta. El resultado son las capacidades de rendimiento efectivo dinámico de Ethernet sin desventaja de las colisiones.

I.3.3 FAST ETHERNET IEEE 802.3/100 MBPS

Desde los principios de operación, las redes Ethernet son muy simples, y cabe mencionar que alrededor del 80% de las estaciones de trabajo conectadas en red son Ethernet 802.3. Esta cantidad se debe; desde luego, a su bajo costo, pero también a este tipo de redes opera en la práctica con mejores resultados que los proporcionados por los modelos analíticos. La razón es que estos modelos se fundamentan en una serie de hipótesis teóricas sobre las características del tráfico, que son conservadoras para las aplicaciones reales en producción, que presentan otro tipo de comportamiento.

Las hipótesis teóricas de los modelos analíticos son esencialmente:

- La red local esta constituida por una población infinita de estaciones, lo que evidentemente dista mucho de ser cierto.

- El tráfico de las estaciones tiene una distribución aleatoria.

- El tráfico es del tipo Todos con Todos, lo que no es correcto, pues el esquema más utilizado en las redes de área local es del tipo Cliente/Servidor.

La operación Cliente/Servidor determina normalmente un tipo de tráfico interactivo. Aún en el caso de transferencia de archivos, un servidor transmite un número determinado de bloques y espera hasta recibir una respuesta del cliente. En definitiva, la operación cliente/servidor produce los siguientes efectos autorreguladores:

- Cuando la red tiende a la congestión, las peticiones a los servidores se dilatan en el tiempo, ya que hasta que no se atiende una petición no se realiza otra, con lo que disminuye la carga presentada a la red. De esta forma se crea una capa virtual de control de congestión.

- La velocidad de las operaciones en la red esta determinada por la capacidad de los servidores, derivada por ejemplo del subsistema de archivos, que normalmente es muy inferior a los 10 Mbps de velocidad de Ethernet.

Una vez hechas estas consideraciones, complementaria a las del apartado anterior, es también cierto que determinadas redes y determinados servicios pueden demandar velocidades muy superiores a los 10 Mbps.

Una de las opciones más simples para obtener alta velocidad en redes de área local consiste en adaptar el estándar IEEE 802.3 para CSMA/CD a la velocidad de 100 Mbps. La idea básica es conservar el método de acceso (MAC) con objeto de mantener la máxima compatibilidad de la extensa base instalada en redes Ethernet e IEEE 802.3/ISO 8802-3. Pueden destacarse las siguientes características:

- Costo reducido, en línea con la norma Ethernet/IEEE 802.3

- Mantener el MAC, para simplificar la interoperación con las redes existentes y poder utilizar el mismo software.

- Utilización de cable UTP (Par Trenzado Sin Apantallar), por ser el más utilizado y económico.

- Fácil coexistencia y migración con los estándares existentes. La situación ideal seria disponer de tarjetas que operen a 10/100 Mbps.

Frente a los mencionados aspectos positivos, las limitaciones fundamentales se derivan del propio método de acceso CSMA/CD: distancia, tiempo de respuesta no controlado en condiciones de alta carga, poca adecuación a aplicaciones con tiempo de respuesta crítico y gestión de red y prioridades no incluidas en la arquitectura.

A continuación se comentan las opciones de IEEE 802.3 para operar a 100 Mbps.

- 100Base-T, es el nombre genérico que se emplea para referirse a dicho estándar sobre cualquier medio en banda base, manteniendo todas las características y temporizadores de 10Base-T e incluso la topología utilizada es también en estrella, como en 10Base-T, si bien con limitaciones. La conexión entre la estación y el Hub será punto a punto y no superara los 100 metros.

- 100Base-TX, designa al estándar cuando se usa cable del tipo UTP-5.
- 100Base-T4, designa al estándar cuando se utiliza cable UTP-3. debido a que la oferta de UTP-3 más utilizada es con 4 pares, 100Base-T4, utiliza todos ellos. Los datos se transmiten sobre 3 pares, con lo cual la velocidad por par es de 33 Mbps, con el consiguiente ahorro en asuntos de la electrónica. El cuarto par se utiliza para detectar colisiones. Las características básicas de 100Base-T4 son:

    - ✓ La conexión entre estación y el hub es punto a punto.

    - ✓ La distancia máxima del cable es de 100 metros.

    - ✓ El protocolo puede operar tanto 100 Mbps, como a los 10 Mbps de la Ethernet clásica. Para ello los adaptadores pueden identificar el tipo de hub

al que están conectados y seleccionar dinámicamente el modo de operación.

- 100Base-T2 es un intento de conseguir utilizar el cable UTP-3 con 2 pares. En teoría, se puede conseguir 100Mbps para distancias limitadas, hasta 100metros, con un par UTP-3. Sin embargo, los adaptadores serian complejos y costosos. Por otra parte, puesto que los cables UTP-3 normalmente se suministran con 4 pares, lo lógico seria poder utilizar los restantes para otro tipo de tráfico como el telefónico. Sin embargo, el limitar las diafonías a límites aceptables es también un importante problema; en consecuencia, muy poca utilidad tendría utilizar 2 pares de UTP-3 si no se puede utilizar los otros 2. Por ello, la opción que prevalece en la actualidad es 100Base-T4.

- 100Base-FX, es un borrador de estándar para utilizar el cableado propio de fibra multimodo (MMF de FDDI).

En la figura 1.8 se ilustra un ejemplo de configuración con Fast Ethernet.

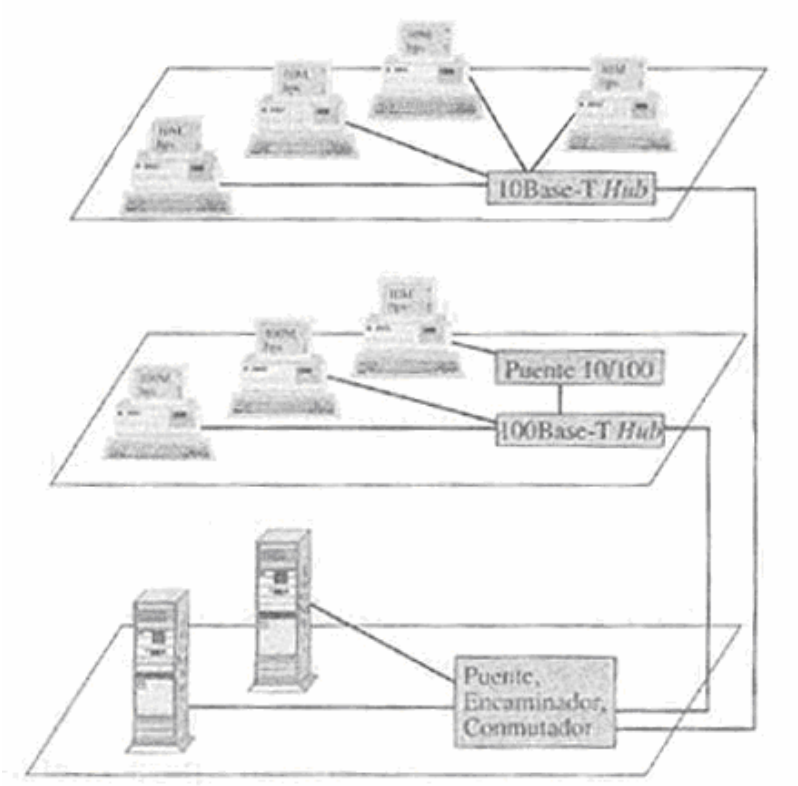


FIGURA 1.8 CONFIGURACION DE FAST ETHERNET

I.3.4 VIRTUAL LAN

Esta es una de las facilidades valoradas de las nuevas redes conmutadas. Estas redes pueden ser configuradas como un segmento único, ya que la disponer de enlaces dedicados no tiene necesidad de segmentar para aumentar el throughput, ya que el medio

de transmisión nunca será el cuello de botella. Sin embargo, la segmentación proporciona algunas ventajas organizativas, operativas e incluso de seguridad y queda muchas transmisiones limitadas a los miembros de un mismo segmento. Las virtual LAN están estrechamente relacionadas con el groupware o trabajo en grupo. Las VLAN unen lógicamente usuarios separados físicamente para formar parte de uno o múltiples grupos de trabajo, eliminando las limitaciones físicas y de un único entorno propio al grupo. Además, proporcionan seguridad y protección en los envíos de información entre los miembros de cada grupo de trabajo dentro de cada red virtual. De este modo, los empleados de los diferentes departamentos consiguen un óptimo tiempo de respuesta dentro de su grupo o con otros departamentos de la corporación, evitando problemas de inseguridad.

La formación de grupos lógicos consigue también solventar los problemas de tramos de red congestionados por exceso de tráfico ajeno al grupo (broadcast de toda la organización, tramos no aislados que pueden ser filtrados, etc.) permitiendo aprovechar el ancho de banda. El administrador de la red también obtendrá ventajas, ya que la red puede ser transformada de una forma mas sencilla, se reducen los costos de añadir, cambiar o eliminar usuarios y podrá controlar y optimizar el ancho de banda.

Los objetivos de las VLAN es conseguir redes que:

- ✓ Integren usuarios remotos móviles
- ✓ Den seguridad y flexibilidad a los grupos virtuales de trabajo.
- ✓ Permiten el más alto rendimiento en todos los nodos de la red corporativa.
- ✓ Logren organizaciones más flexibles.
- ✓ Eliminen limitaciones geográficas al crear grupos virtuales de trabajo en toda la red.
- ✓ Permitan añadir, eliminar o cambiar usuarios vía software.

I.3.5 REDES INALÁMBRICAS (WIRELESS LAN)

Sin demasiada penetración en el mercado el estándar IEEE 802.11 se considera como una solución para la implantación de redes de área local sin hilos tanto en edificios como en espacios abiertos con amplia cobertura y rendimiento.

Esta norma especifica un sistema para la conexión de equipos dentro de la red de área local pero no establece un método de cómo los productos, bien dispositivos o puntos de acceso, de diferentes empresas pueden interactuar.

Los medios físicos sobre el que en principio se soportará esta tecnología son:

- Espectro Ensanchado Secuencial Directo
- Espectro Ensanchado con Salto de Frecuencia
- Infrarrojos

El desarrollo del estándar para la capa de acceso al medio es, por lo tanto, bastante complejo, y proporcionará funciones de:

- Gestión de potencia

- Encaminamiento multicanal
- Seguridad

Hasta la fecha la tecnología desarrollada trabaja en el rango de frecuencias de 2.4 GHz con velocidades de 2Mbps para los protocolos de Espectro Ensanchado. El siguiente paso supondrá un avance a velocidades de 20 Mbps y el desarrollo de una versión internacional de Protocolos de Puntos de Acceso para pasarelas sin hilos.

Las principales ventajas de esta tecnología son:

- **Movilidad y flexibilidad** de cobertura y ubicación de usuarios.
- **Bajo coste en infraestructura** al no discurrir por un medio guiado.

Las mayores desventajas:

- **Menor fiabilidad** que otras soluciones sobre medios guiados
- Actualmente **baja velocidad de proceso**

I.4 ELEMENTOS DE CONECTIVIDAD

Para realizar la interconexión entre equipos y tengamos una red LAN que pueda ser con facilidad compartir recursos se debe emplear elementos de conectividad para una conexión física que conlleve posteriormente a una conexión lógica.

I.4.1 HARDWARE DE CONECTIVIDAD

En este apartado se hablará de los componentes más importantes que existen en el mercado para la conectividad de una red LAN y forme una red estable y capaz de ser flexible a los cambios de tecnologías que se desea utilizar en cada red LAN que se diseñe, en los siguientes temas se describirá cada uno de ellos.

I.4.1.1 TARJETA DE INTERFAZ DE RED (NIC)

Una tarjeta de interfaz de red, a veces llamada NIC o adaptador de red, se usa para conectar una PC a un cable de red. En el mercado literalmente hay cientos de tipos diferentes de NICs, producidas por docenas de fabricantes. (La figura 1.9 muestra un ejemplo de una NIC común). Los precios pueden variar desde tan poco como 40 dólares hasta mas de 500 dólares, dependiendo del método de acceso usado por la tarjeta y el tipo de bus (ISA, EISA, MCA o PCI) para el que esta diseñada la tarjeta.

FIGURA 1.9 TARJETA COMÚN DE INTERFAZ DE RED

I.4.1.2 REPETIDORES

Una de las desventajas del tipo de cable que se usa principalmente, es el CAT5 UTP, es la longitud del mismo. La longitud máxima para un cable UTP en una red es de 100 metros (aproximadamente 33 pies). Si necesita extender la red mas allá de este limite, deberá añadir un dispositivo a la red. Dicho dispositivo se llamado repetidor.

El término repetidor viene de los días de la comunicación visual, cuando un hombre que estaba situado en una colina recibía una señal de otra persona que estaba en la colina de su izquierda, y después repetía la señal a la persona que estaba situada en la colina de la derecha. También viene del telégrafo, teléfono, microondas y comunicaciones ópticas, las cuales emplean repetidores para fortalecer sus señales en las largas distancias y evitar que se debiliten o mueran.

Al igual que los medios de red, los repetidores son dispositivos de red que existen en la Capa 1, la capa física, del modelo de OSI. Para comenzar a comprender como funciona un repetidor, es importante comprender primero que un dato abandona el origen y se traslada por la red, transformándose en pulsos de luz o eléctricos que pasan por los medios de red. Estos pulsos se llaman señales. Cuando las señales abandonan un puesto de transmisión, están limpias y son fácilmente reconocibles, Sin embargo, la longitud del cable deteriora y debilita las señales mientras pasan por los medios de red. Por ejemplo, las especificaciones del cable Ethernet de par trenzado de categoría 5, establecen que la máxima distancia a la que pueden viajar las señales de red es de 100 metros. Si una señal viaja a esa distancia, no existen garantías que una NIC pueda leerla. Un repetidor puede proporcionar una solución sencilla si existe este problema.

El propósito del repetidor es regenerar y reenviar las señales de red, a un nivel de bits para hacer posible que estas viajen largas distancias por los medios. Tenga cuidado con la regla de los cuatro repetidores para Ethernet 10 Mbps, también conocida como Regla 5-4-3, cuando extienda segmentos LAN. Esta regla dice que se pueden conectar cinco segmentos de red de extremo a extremo usando cuatro repetidores, pero solo tres segmentos podrán tener hosts (computadoras).

El término repetidor originalmente se refería a un dispositivo de puerto “in” único y a un dispositivo de puerto “out” único. Hoy existen los repetidores de puerto múltiples. Los repetidores se clasifican como dispositivos de Capa 1 del modelo OSI, por que actúan solo a nivel bits y no se fijan en ninguna otra información.

I.4.1.3 CONCETRADORES (HUBS)

En general, el término concentrador se conoce en campo de la informática como hub (por su termino en ingles, y para evitar confusiones; en este trabajo se menciona como “hub”). Y se emplea en lugar de repetidor cuando se refiere al dispositivo que sirve como centro de la red, como se puede observar en la Figura 1.10. Aunque un hub opera en una topología física en estrella, crea el mismo entorno de contención que en bus. Esto se debe a que cuando un dispositivo trasmite, el resto de los dispositivos escuchan y la contención crea un bus lógico.

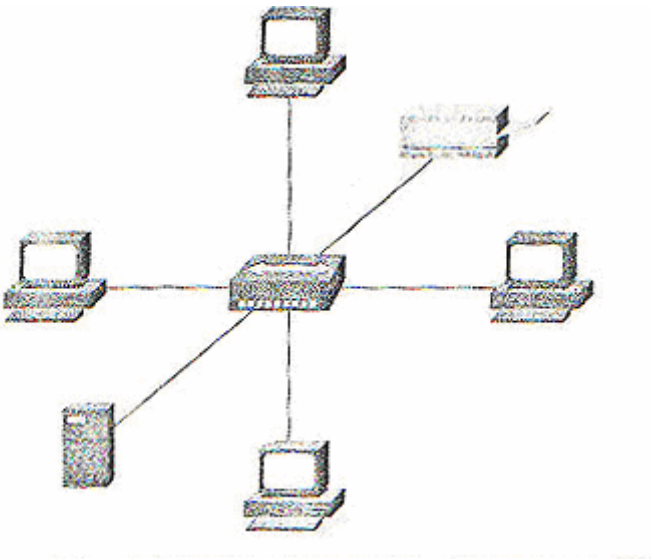


FIGURA 1.10 TOPOLOGIA ESTRELLA CON HUB CENTRAL

El propósito de un hub es regenerar y reenviar señales de red. Esto hace a nivel de bits con un gran número de hosts (por ejemplo 4, 8 o incluso 24). Esta acción se conoce como concentración. Estas son las propiedades más importantes de los hubs:

- Regenerar y repetir las señales.
- Propagar las señales en la red.
- No pueden filtrar el tráfico de la red.
- No pueden determinar la mejor ruta.
- Se utilizan como puntos de concentración de la red.

Los hubs emplean normalmente en la redes Ethernet 10BaseT o 100BaseT. El papel de los hubs en la red Token Ring lo ejecuta la Unidad de Conexión al Medio (MAU). Físicamente, se parece a un hub, pero la tecnología de Token Ring es muy diferente. En FDDI, el dispositivo de conexión se llama concentrador. Las MAU y los concentradores son también dispositivos de la Capa 1.

I.4.1.4 CONMUTADORES (SWITCHES)

Un switch (en castellano conmutador, pero en este trabajo lo mencionaremos como “switch”, ya que así se conoce en campo de la informática y redes; y se evitará la confusión con el término de conmutador telefónico) es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (***Open Systems Interconection***). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un ***filtro*** en la red, mejoran el rendimiento y la seguridad de las LANs (***Local Area Network***- Red de Área Local).

I.4.2 TIPOS DE REDES

Es necesario tener en cuenta que tipo de red vamos a diseñar, de acuerdo a las necesidades de la institución, empresa, negocio, etc., se deberá analizar el tipo, ya que debemos verificar si solo será algo simple como consulta de algunos datos o algo más complejo como hoy en día son bases de datos a través de servidores, o consultas a través del Internet, etc, por esto se describirá en los siguientes temas.

I.4.2.1 REDES CLIENTE/SERVIDOR

Las redes cliente/servidor se usan comúnmente en entornos LAN mayores, incluyendo colegios y universidades. En este enfoque de la conectividad, la red se compone de uno o más servidores especializados, y varios clientes diferentes, como se muestra en la figura 1.11. Los servidores están diseñados para proporcionar servicios centralizados y los clientes son los diferentes nodos de la red. En un entorno cliente/servidor, las PCs conectadas a la red pueden llamarse clientes, nodos o estaciones de trabajo; existe poca diferencia técnica entre los términos en este tipo de red.

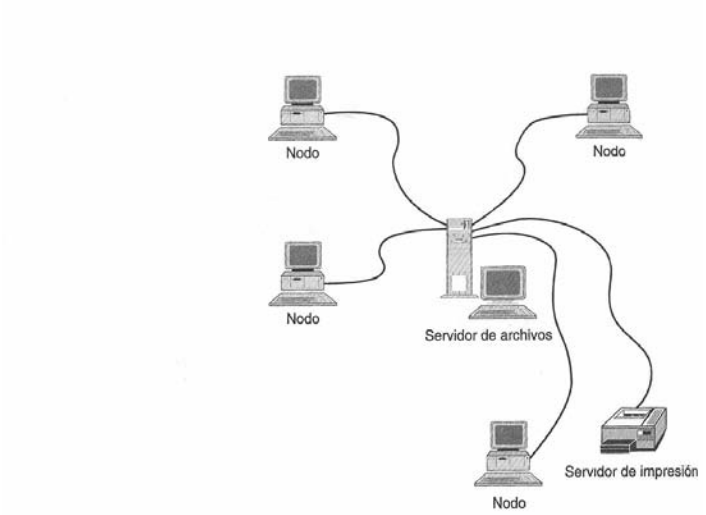


FIGURA 1.11 RED CLIENTE / SERVIDOR

Muchos tipos de diferentes servidores se pueden usar en una red cliente/servidor. Estos servidores se agregan a la red; lo dictan las necesidades de esta. Tipos comunes de servidores incluyen los siguientes:

- Servidor de archivo: Esta computadora esta dedicada a proporcionar almacenamiento y administración centralizados de archivos.
- Servidor de impresión: Esta computadora o dispositivo proporcionan servicios de impresión centralizados.
- Servidor de comunicaciones: Esta computadora esta dedicada a proporcionar servicios de MODEM, fax y correo electrónico.
- Servidor de base de datos: Esta computadora esta dedicada a ejecutar un programa de base de datos centralizado.

I.4.2.2 REDES DE PUNTO A PUNTO

En un entorno de conectividad de punto a punto no hay servidores centralizados. En su lugar, cada nodo en la red proporciona que puedan tener acceso a otros nodos en la red. Por ejemplo, un nodo puede tener una impresora que pueden usar otros nodos, en tanto que un nodo diferente puede tener archivos de datos a disposición de otros usuarios de la red. La figura 1.12 muestra un ejemplo de conectividad de punto a punto.

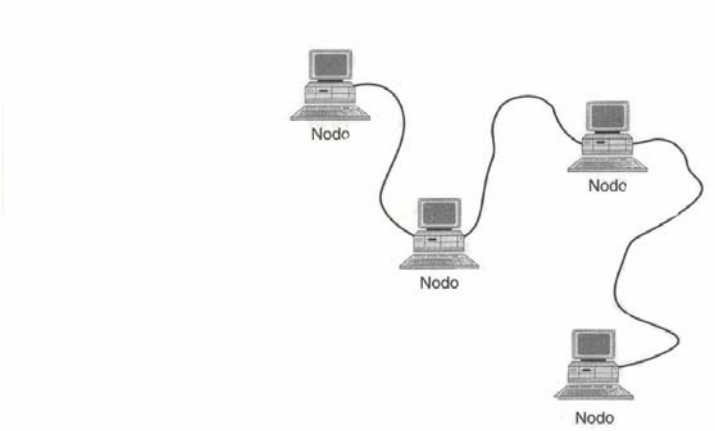


FIGURA 1.12 CONECTIVIDAD PUNTO A PUNTO

La conectividad de punto a punto se usa de manera tradicional para redes o grupos de trabajo menores. Por ejemplo, su salón de clases, si no esta conectado a una red mayor, puede usar el enfoque de red punto a punto. Este enfoque elimina varias desventajas inherentes en el enfoque cliente/servidor. Por ejemplo, si una de las computadoras en la red falla, no se desactiva la red completa. Por supuesto, los recursos compartidos por eso nodo no están disponibles, pero pueden usarse servicios alternativos por medio de otros nodos en la red. Además, de manera característica no es necesario un administrador de red por que cada persona que usa la red, por lo general mantiene su propia computadora y administra sus propios recursos compartidos.

I.4.3 TOPOLOGÍAS

Como se ha definido anteriormente, para que el tráfico de información pueda ser rápido y no tengamos averías en la red, o tener precaución que solo algunos segmentos puedan estar afectado y no toda la red completa, se determina en los siguientes temas los tipos de topologías que actualmente existen, sin embargo debemos tomar en cuenta el tipo de hardware de conexión y la velocidad que deseamos transmitir.

I.4.3.1 TOPOLOGÍA JERÁRQUICA

La topología jerárquica es una de las más comúnmente utilizadas hoy en día. El software para controlar la red es relativamente simple y la propia topología proporciona un punto de concentración para control y resolución de errores. En la mayor parte de los casos, el ETD de mayor jerarquía (raíz) es el que controla la red. En esta topología; el flujo de datos entre los ETD lo inicia un ETD A. En algunos diseños, el concepto de

control jerárquico se distribuye ya que se proponen métodos para que algunos ETD subordinados controlen los ETD por debajo de ellos en la jerarquía. Así se reduce la carga del procesador central del nodo A.

Aunque la topología jerárquica es atractiva desde el punto de vista de la simplicidad de control, presenta problemas serios de cuellos de botella. El ETD situado en la raíz de la jerarquía, que típicamente es una computadora de altas prestaciones, controla todo el tráfico entre los ETD. El problema no son sólo los cuellos de botella, sino también la fiabilidad. En el caso de un fallo en la máquina situada en la raíz, la red queda completamente fuera de servicio, a no ser que otro nodo asuma las funciones del nodo averiado. Permite una evolución simple hacia redes más complejas, ya que es muy sencillo añadir nuevos componentes.

La topología jerárquica también se denomina “red vertical” o “red en árbol”. La palabra “árbol” es utilizada, ya que la topología recuerda físicamente a un árbol. La raíz sería el nodo principal y las ramas, los nodos secundarios. Las ventajas y desventajas de las redes de comunicación de datos verticales son las comunes que las de una estructura jerárquica de un centro de trabajo. Líneas de autoridad muy claras con cuellos de botella muy frecuentes en los niveles superiores, y a menudo delegación insuficiente de responsabilidades.

I.4.3.2 TOPOLOGÍA HORIZONTAL (BUS)

La topología horizontal o en bus es una disposición muy popular en redes de área local. El control del tráfico entre los ETD es relativamente simple, ya que el bus permite que todas las estaciones reciban la transmisión. Es decir, cada estación puede difundir la información a todas las demás. El principal inconveniente de esta topología es que habitualmente sólo existe un único canal de comunicaciones al que se conectan todos los dispositivos de la red. En consecuencia, si falla dicho canal la red deja de funcionar. Algunos fabricantes suministran un canal redundante que se pone en funcionamiento en el caso de fallo en el canal primero. En otros casos se proporcionaran procedimientos para evitar los nodos que fallan. Otro problema que presenta esta configuración es la dificultad de aislar los componentes defectuosos conectados al bus, debido a la ausencia de puntos de concentración. Como muestra la siguiente figura 1.13:

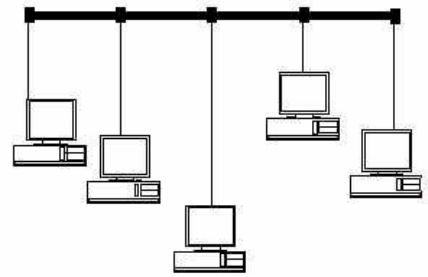


FIGURA 1.13 TOPOLOGIA BUS

I.4.3.3 TOPOLOGÍA EN ESTRELLA

Es otra estructura ampliamente usada en sistemas de comunicación de datos. Una de las principales razones para su uso es fundamentalmente histórica. Todo el tráfico surge del centro de la estrella. El nodo A, típicamente un computador controla completamente los ETD conectados a él. Es por tanto, una estructura muy semejante a la estructura jerárquica, con la diferencia de que la estructura en estrella tiene mucho más limitadas las posibilidades de procesamiento distribuido.

El nodo A es el responsable de encaminar el tráfico entre los otros componentes. Es también responsable de ocuparse de los fallos. La localización de averías es relativamente simple en redes en estrella ya que es posible ir aislando las líneas para identificar el problema. Sin embargo, como sucedía en la estructura jerárquica, la red en estrella sufre de los mismos problemas de fallos y cuellos de botella, debido al nodo central. Algunos sistemas poseen un nodo central de reserva, lo que incrementa considerablemente la confiabilidad del sistema. . Como muestra la siguiente figura 1.14:

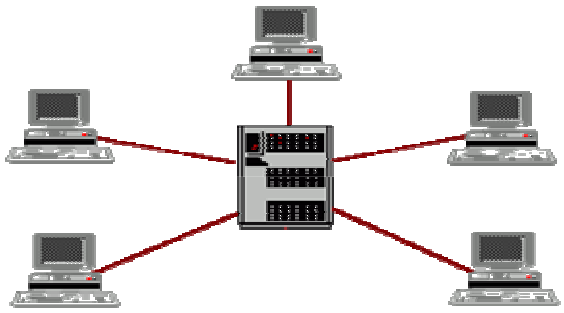


FIGURA 1.14 TOPOLOGIA ESTRELLA

I.4.3.4 TOPOLOGÍA EN ANILLO

Este tipo de topología recibe su nombre del aspecto circular del flujo de datos. En muchos casos el flujo de datos va en una sola dirección, es decir, una estación recibe la señal y la envía a la siguiente estación del anillo. La lógica necesaria en una red de este tipo es relativamente simple. Las tareas que deben realizar el nodo componente son aceptar los datos, enviarlos al ETD conectado a él, o bien enviarlos al siguiente componente intermedio en el anillo. Como todas las redes, el anillo tiene también sus inconvenientes. El principal de ellos es que un único canal une a todos los componentes del anillo. Si falla el canal entre dos nodos, falla toda la red. En consecuencia algunos sistemas incorporan canales de reserva. En otros casos se proporciona la posibilidad de evitar el enlace defectuoso, de forma que la red no quede fuera de servicio. Otra solución puede ser utilizar un doble anillo. Como muestra la siguiente figura 1.15:

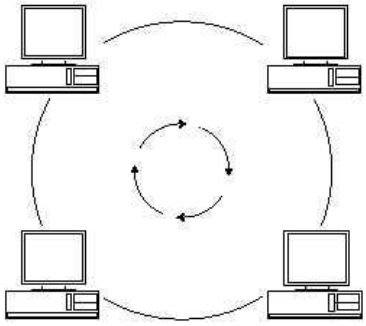


FIGURA 1.15 TOPOLOGIA ANILLO.

I.4.3.5 TOPOLOGÍA EN MALLA

La topología en malla apareció en los últimos años. Su principal atractivo es una relativa inmunidad a problemas de fallos o cuellos de botella. Dada la multiplicidad de caminos entre los ETD y los ECD, es posible encaminar el tráfico evitando componentes que fallan o nodos ocupados. Aunque esta solución es costosa algunos usuarios prefieren la gran fiabilidad de la topología en malla frente a las otras (especialmente para las redes de pocos nodos).

Como muestra la siguiente figura 1.16:

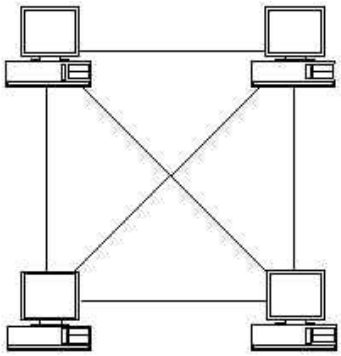


FIGURA 1.16 TOPOLOGIA MALLA

I.5 SISTEMAS OPERATIVOS

Un sistema operativo es un conjunto especial de programas de computación que administra todo lo que ocurre dentro de un sistema de computación. El sistema operativo proporciona la interfaz para comunicarse con la computadora, permite el procesamiento de información en segundo plano y administra la salida de información hacia el monitor, la impresora u otro dispositivo de salida. Sin un sistema operativo la computadora no seria nada más que un pisapapeles de tamaño descomunal.

I.5.1 MS-DOS

Son las siglas de Microsoft Disk Operating System. Es el sistema operativo más usado por las computadoras personales compatibles con IBM, tuvo varias versiones,

hasta llegar a la 6.22, de la cual Microsoft dio el brinco para hacer que el sistema operativo tuviera un ambiente grafico. Como sistema operativo, MS-DOS coordina a la unidad central de proceso (CPU) de la computadora, con el resto del hardware. En esta función el MS-DOS toma el caracter que pulsa el usuario en el teclado, lo codifica en forma entendible para el CPU y a continuación lo visualiza en el monitor en forma comprensible para el usuario.

Dentro de MS-DOS, existen comandos (palabras clave que requieren una acción de sistema operativo), internos y externos. Los comandos internos residen en la memoria del sistema como parte del archivo COMMAND.COM; estos son cargados en memoria cuando el sistema operativo es cargado. Cuando listamos el directorio de nuestro disco de MS-DOS no pueden ser vistos ya que forma parte del archivo llamado COMMAND.COM. Los comandos externos son cargados en memoria desde el disco, solo cuando los necesitamos.

Comandos internos: DIR, COPY, PATH, etc.

Comandos externos: FORMAT, DISKCOPY, etc.

I.5.2 WINDOWS

Es un entorno gráfico, en las versiones anteriores de Windows 95 se instala sobre MS-DOS, ocultándolo desde ese momento y actuando como intermediario entre el usuario y la computadora. La razón más importante para el usuario es la facilidad de uso. Windows es fácil e intuitivo para una persona inexperta, pues no hay que memorizar comandos ni parámetros de estos comandos. En lugar de aprender a trabajar como la computadora. Windows enseña a la computadora a trabajar como nosotros. Crea una pantalla que el equivalente a nuestra propia mesa de trabajo. Windows copia el interfaz gráfico de las computadoras Macintosh. Además Windows emplea continuamente el ratón (Mouse), cuyos movimientos en la mesa se transmiten fielmente a una señal visible en pantalla, llamada puntero, que nos permite seleccionar objetos u operaciones.

MS-DOS es un sistema mono-tarea, mientras que Windows puede estar realizando varias acciones simultáneamente. Además estandariza algunas aplicaciones, haciendo que los programas sean compatibles entre sí al ser diseñados para la misma interfaz de aplicación.

I.5.2.1 WINDOWS 3.1 Y 3.11

Windows 3.1 se puso a la venta en abril de 1992, casi dos años después de la aparición del Windows anterior. Los requerimientos del sistema operativo eran DOS 3.1, un sistema basado en 80286 (o superior), 640 KB de memoria convencional, 256 KB de memoria extendida (1 MB recomendado), unidad de disco flexible de alta densidad, unidad de disco duro con 6 MB de espacio libre (10 MB recomendado) y adaptador gráfico. La actualización presentaba un programa de instalación bastante mejorado, un curso práctico en línea, mayor consistencia en los cuadros de diálogo, un sistema de ayuda mejorado, un administrador de archivos mejorados y controladores de impresora y de video adicionales. También agrego soporte para fuentes TrueType.

Windows 3.11 apareció en diciembre de 1993, pero no estuvo disponible sino hasta enero de 1994. Los requerimientos del sistema eran los mismos que para la versión

3.1. Esta actualización menor incluyo algunos controladores nuevos, archivos de soporte NetWare (Novell) y algunos arreglos de errores. Sin embargo, las “mejoras” mayores se encontraban en el empaque. Microsoft agrego un holograma a la caja e incluyo un certificado de autenticidad. Estos cambios eran para compartir un problema creciente de piratería en el mercado internacional.

I.5.2.1.1 WINDOWS PARA TRABAJO EN GRUPO 3.1 Y 3.11

Windows para Trabajo en Grupo 3.1 apareció en octubre de 1992, y represento un gran cambio de dirección para la corriente principal de la línea de productos de Windows. Antes las versiones de Windows se diseñaban para PCs solas, en tanto que Windows para Trabajo en Grupo 3.1 fue diseñado para usarse en un entorno de red. La aparición de Windows para Trabajo en grupo también constituyó un cambio en versión previa de Windows reemplazaba a la versión anterior. Esto no sucedió con Windows para trabajo en Grupo. No reemplazo 3.1, simplemente estaba dirigido a un diferente mercado. De pronto el panorama de Windows fue transformado, como se muestra en la figura 1.17.

La razón por la que Windows para Trabajo en Grupo fue diseñado para su uso en una red doble:

- Las redes estaban comenzando a hacer incursiones en negocios pequeños. Los competidores de Microsoft estaban haciéndose de renombre al proporcionar conectividad de punto a punto que funcionaria incluso con Windows.

- Microsoft estaba planeando sacar Windows NT en un futuro cercano. Este producto se colocaría como el servidor en redes de tamaño mediano, lo cual significaba que eran necesarios clientes (estaciones de trabajo).

Windows para Trabajo en Grupo 3.11, una actualización menor, se puso a la venta en noviembre de 1993. Los requerimientos del sistema eran los mismos que para la versión anterior, pero había unas cuantas características nuevas. Estas incluían controladores mejorados (compatibles con la especificación NDIS 3.0), soporte adicional a Novell Netware, Servidor de Acceso Remoto (RAS; Random Access Server)), soporte para fax, soporte para comunicaciones, mejorado y un acceso a archivos en modo protegido de 32 bits, mejorado. Además se abandono el soporte para la operación en modo estándar (real).

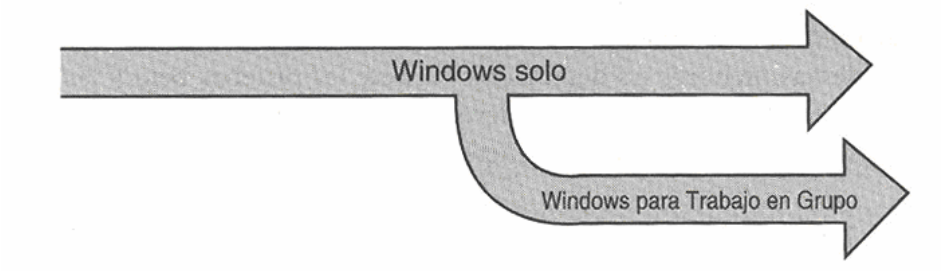


FIGURA 1.17 DIVISION DE WINDOWS PARA PC OFICINA Y GRUPO DE TRABAJO

I.5.2.2 WINDOWS NT

El desarrollo de Windows NT comenzó en 1988 y se puso a la venta por fin en julio de 1993. La razón para el ciclo de desarrollo tan largo (el cual en realidad comenzó al mismo tiempo que estaba trabajando Windows 2.X), fue que Windows NT era un sistema operativo completamente nuevo, de principio a fin. Microsoft se percato de que no podía abandonar el sendero regular de Windows (el cual estaba basado en el legado del sistema operativo DOS), pero Microsoft necesitaba un sistema operativo con fuerza industrial diseñado para sistemas de terminado de calidad. Ahora el árbol genealógico de pronto aparecía como se muestra en la figura 1.18.

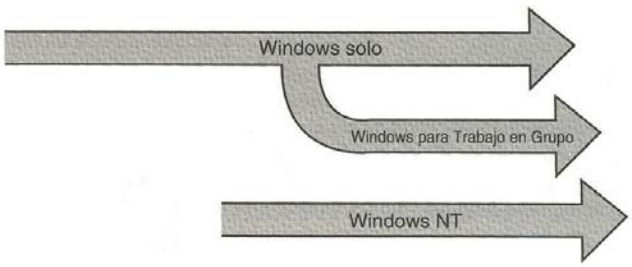


FIGURA 1.18 WINDOWS NT PLANTÓ UN ÁRBOL GENEALÓGICO NUEVO JUNTO AL ANTIGUO.

Observe que el árbol genealógico ya no es un solo árbol. Esto debe a que Windows NT comenzó desde su propia raíz. Lo único que era igual era la interfaz de usuario. La forma exacta como la interfaz y la tecnología subyacente ponían en práctica era nueva por completo. La NT en Windows significa “Nueva Tecnología”, lo cual es a forma como Microsoft veía al sistema operativo. Debido a que estaba diseñado para PCs de determinada calidad, los requerimientos del sistema incrementaron. Los requerimientos mínimos eran una CPU 80386 ejecutándose a 33 MHz, 8MB de RAM, unidad de disco duro de 85 MB y una tarjeta VGA. Comparé estos requerimientos con los Windows 3.1 y puede empezar a ver como se esperaba que fuera los sistemas de Windows NT de “terminado de calidad”.

La versión inicial de Windows NT salió con varios nombres. El primero fue simplemente ese: Windows NT. Un poco mas tarde el producto se renombro como Windows NT 3.1, lo cual puso el número de versión del producto más o menos en sincronía con el producto de Windows común, el cual estaba en la versión 3.1. Desde un punto de vista de mercado esto no tenía sentido, sobre todo por que la interfaz de usuario tanto en Windows NT como en Windows 3.1 era la misma.

Poco después de salir Windows NT, Microsoft puso a la venta una versión mejorada del producto, la cual fue diseñada para usarse de manera explícita como un servidor. Esta se llamo de manera bastante apropiada Windows NT Advanced Server. Esta disparidad entre los nombres de los productos (Windows NT 3.1 y Windows NT Advanced Server) fue simplificada más adelante cuando los nombres de los productos se volvieron Workstation y Server. Por tanto, siempre salía una nueva versión., el número de la versión se aplicaba a Windows NT Workstation 4.0 y Windows NT Server 4.0.

I.5.2.3 WINDOWS 95

Esta versión tan anticipada apareció a finales de de agosto de 1995. Una vez más, el tiempo transcurrido desde la versión anterior fue casi dos años, mucho mayor incluso del que se había anticipado Microsoft. Los requerimientos de hardware cambiaron de nuevo y ahora Windows 95 requería al menos una CPU 80386. (Sin embargo, se adapta mejor a maquinas 80486 o Pentium). Windows 95 no funcionara con sistemas basados en RISC ni sacara ventaja de multiprocesadores.

Los cambios en Windows 95 representaron los cambios más arrolladores en la historia del producto. La relación entre DOS y Windows se invirtió, la interfaz de Windows de usuario se cambio por completo, gran parte del sistema operativo se escribió de nuevo en código de 32 bits y muchas aplicaciones fuero modificadas. Se agrego soporte de OLE 2.0, ya que era un soporte integral para una amplia variedad de redes. Windows 95 era mucho más estable que versiones anteriores de Windows, con la notable excepción de Windows NT. Windows 95 también presento el desplome de dos miembros del árbol genealógico de Windows, como se muestra en la figura 1.19, Windows 95, con sus capacidades de conectividad integradas, se diseño para reemplazar tanto a Windows 3.11 como a Windows para Trabajo en Grupo 3.11.

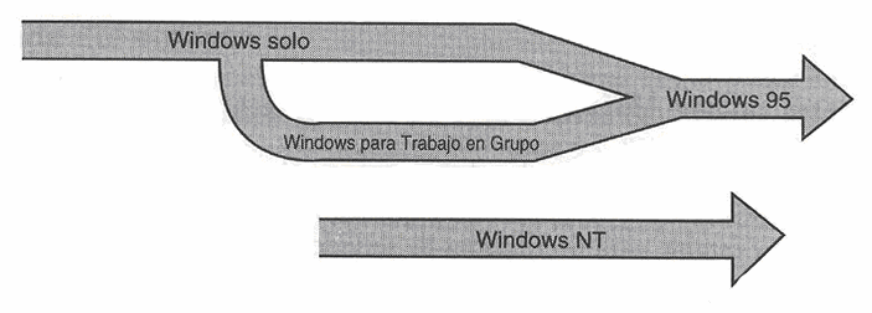


FIGURA 1.19 CONSOLIDACION DE LA VERSION A WINDOWS 95

I.5.2.4 WINDOWS 98

Windows 98 no representó para los usuarios "comunes" ningún cambio significativo. Sólo un poco de "maquillaje" gráfico y alguna que otra utilidad nueva o mejorada (como el "liberador de espacio" o el viejo "defrag"). Pero si trajo algunas "cositas" nuevas "bajo la manga": el soporte completo para los 32 bits (al fin), y la "eliminación" del DOS como sistema independiente (ya que no incluye una nueva versión, sino un emulador del mismo), son algunos ejemplos. La única gran virtud de Windows 98 es la de seguir "enganchando" a los usuarios finales y hacer que Microsoft mantenga el liderazgo mundial en sistemas operativos.

Además, es la "antesala de entretenimientos" para que no pase tanto tiempo antes de la aparición de Windows 2000, que promete ser la "unión" con Windows NT (Windows Nueva Tecnología). Windows NT es un sistema operativo de 32 bits especializado en redes que utiliza otro sistema para el manejo de los archivos, y por lo tanto "incompatible" por el momento con Windows 95/98.

I.5.2.5 WINDOWS 2000 /WINDOWS ME

La empresa de Gates ha dado un nuevo paso en sus principales productos y nacieron así Windows 2000 y Windows ME. El primero, es el sucesor de NT, por lo que está orientado a empresas y hereda muchas de las características de este.

Su gran estabilidad, su soporte para varios procesadores, su alto nivel de seguridad, además de sus impresionantes capacidades para desenvolverse como “Servidor” lo hacen, como dije, la mejor opción para una empresa. Es rápido y lo suficientemente fácil de configurar casi para cualquier persona, pero hay que tener en cuenta que tiene poco soporte para el agregado de periféricos como tarjetas de video o de sonido. Es decir, este no es un sistema operativo totalmente apto para la multimedia. Al ser de esta manera, es muy probable que no se use en hogares, donde comúnmente encontraremos juegos, música en la PC, enciclopedias multimedia y demás. Ahí es donde entra Windows Millennium (ME), sucesor de Windows 98 (aunque muchos dicen que es la tercera edición de éste después de Windows SE).

Es un sistema operativo donde prima la facilidad de uso, la robustez y las mejoras en multimedia, comunicaciones e Internet. Aunque no cuenta con la estabilidad de Windows 2000 es más seguro que Windows 98 y 98 SE (segunda edición) ya que se han incorporado una serie de utilidades para proteger el sistema operativo y hacerlo más resistente a las instalaciones de programas y drivers de terceros que, en definitiva, son las principales causas de cuelgues y pantallas azules en sus predecesores. Una de las cosas interesantes con que nos encontramos en Windows ME es que el modo DOS, tal como lo conocemos, ha dejado de existir. Ya no es posible iniciar el sistema en "sólo símbolo del sistema" o apagar el sistema "reiniciando en modo MS-DOS". Tanto es así, que los archivos AUTOEXEC.BAT y CONFIG.SYS ya no tienen ninguna función en ME (salvo durante la instalación).

I.5.2.6 WINDOWS XP, LA NUEVA GENERACIÓN DEL ESCRITORIO

Este sistema operativo es la mejora más importante técnicamente desde Windows 9x, y unifica las versiones separadas que hubo estos años: WINDOWS 9x/ME para usuarios hogareños y SOHO contra Windows NT/2000 para usuarios corporativos con requerimientos de trabajo en redes de alto nivel. Windows XP se distribuye en 2 versiones principales: Windows XP Home Edition y Windows XP Profesional. La versión Home no tiene tanto soporte para redes, lo que si incluye la versión Profesional. Windows XP además de constituirse en la unión de los entornos mencionados, es en realidad la continuación de Windows NT/2000. Se destaca en este producto su alto grado de integración con las redes e Internet, además de proveer una nueva interfaz gráfica que se hace notar ni bien se comienza a utilizar. Los cambios de interfaz son básicamente estéticos. La diferencia real con sus predecesores esta dada por el soporte LAN, software de grabación de CDs, multimedia, escritorio remoto y manejo de usuarios.

Algo muy importante es el hecho de que Microsoft con esta versión de su Sistema Operativo ha puesto especial énfasis en los controladores de los dispositivos (drivers). Windows XP ahora es muchísimo más renuente que sus predecesores al instalar controladores de los dispositivos no certificados para el mismo. Con esto Microsoft

pretende reducir al máximo las ya tan conocidas (y sufridas) "pantallas azules", aduciendo que la mayoría de las causas de inestabilidad de las versiones anteriores estaba dada por el uso de controladores de los dispositivos no certificados, obsoletos o mal desarrollados. Se destaca la búsqueda inteligente que hace el Sistema Operativo al momento de instalar un dispositivo nuevo, escaneando unidades en busca de los drivers correctos. En resumen Microsoft de nuevo se presenta muy fuerte con este nuevo Sistema Operativo, el cual seguramente estará de nuevo destinado a mantener la hegemonía de la empresa de Redmond.

I.5.3 UNIX

Sistema operativo transportable de 32 bits, multiusuario, multitarea, desarrollado originalmente por AT&T. UNIX fue desarrollado por Dennos Ritche y Ken Thompson en los laboratorios Bell a principio de la década de los años setenta. Ha sido mejorado a través de los años, especialmente por científicos de computación en la Universidad de California, en Berkeley.

Las redes en forma del conjunto de protocolos TCP/IP, han estado disponibles en UNIX desde la etapas iniciales. UNIX esta disponible en un amplio rango de hardware computacional, desde una PC, hasta una supercomputadora Cray; también esta disponible en otras formas relacionadas. Por ejemplo, AIX corre en estaciones de trabajo IBM, A/UX es la versión gráfica que se ejecuta en computadoras Macintosh poderosas y Solares de Sun corre en procesadores Intel.

I.5.4 LINUX

Linux, es un sistema operativo de UNIX, es un sistema multiusuario que ofrece características de multitarea preferentes. Linux esta disponible como producto libre de distribución (shareware) y como producto libre de distribución no tiene costo pero si para un soporte técnico que implicara un costo. En otras palabras, podemos empezar a utilizarlo gratuitamente, pero si queremos actualizaciones y controladores especiales, tendremos que desembolsar una determinada cantidad.

Linux soporta todas las más importantes herramientas, protocolos y aplicaciones, incluido TCP/IP y clientes de publicaciones y correo electrónico. Es una herramienta de red excelente, y es una buena elección para las actividades Internet e intranet. Puesto que Linux esta respaldado por la licencia pública de la Fundación de software gratuito, los autores deben comercializar de forma gratuita como RedHat Software y Caldera Inc., vienen en CD-ROM e incorporan herramientas de desarrollo, librerías, gestión de red, óptimos servidores Web y demás prestaciones Internet muy útiles y a un precio pero muy asequible.

I.5.5 NET WARE

En 1982, es una pequeña oficina de una fábrica siderurgia en Orem en el estado de UTA, Ray NORAD, Judith Clarke, Craig Burton y programadores de una compañía llamada Superset intuyeron el futuro de las redes. En esta época les hacían la competencia principalmente compañías como Corvus Systems, que estaban sobre todo

interesadas en la venta de discos duros; sin embargo, desde sus comienzos, Novell estuvo orientado a la venta de software para sistemas de computadoras integradas.

Los tiempos fueron difíciles y la financiera de NORAD presiono, para dar beneficios cuanto antes, pero Novell persevero en sus objetos a largo plazo de suministrar software, herramientas de sistemas y soporte. Mientras estuvo NORAD a la cabeza de Novell, la estrategia de sus productos era clara y coherente: comercializar un sistema operativo con buenas prestaciones y un buen rendimiento, y crear un entorno favorable para su funcionamiento. Novell es sobre todo una empresa de software, aunque hay hecho varias incursiones en el mercado hardware con el fin de desarrollar nuevos productos o provocar una baja de los precios del hardware haciendo la competencia. Novell nunca hizo gala de estrategia de << control contable >> (de la que IBM hizo un arte) para acaparar el mercado. Al contrario, ha tenido que sufrir como para conseguir soporte exterior y estimular la competencia. Aunque Novell podía haberse convertido en la cabecilla del movimiento << Todos menos Microsoft >> de 1996 y 1997, su cruzada por vencer las barreras corporativas acabo siendo un fracaso.

I.6 MODELO OSI (OPEN SYSTEM INTERCONNECTION)

La Organización Internacional de Estandarización (ISO: Internacional Standard Organization) desarrollo un modelo de referencia para las arquitecturas de sistemas. Le llamo OSI: Open System Interconnection. Este modelo es estratificado y se estructura en 7 capas. En el concepto de OSI, un sistema es un conjunto de una o más computadoras, el software asociado, los periféricos, las terminales, los operadores humanos, los procesos físicos, los medios de transferencia de información, etc., que forman un ente autónomo con capacidad de realizar el procesamiento de la información.

OSI pone atención al intercambio de información entre sistemas y no el funcionamiento interno de cada sistema en particular. En otras palabras, el Modelo de Referencia OSI constituye el marco de trabajo para el desarrollo de protocolos estándares para la comunicación entre dos capas homónimas ubicadas en equipos separados. Los formatos y protocolos para la comunicación de capas adyacentes dentro de un sistema no serían estandarizados. El objetivo, a largo plazo, de OSI es desarrollar una compatibilidad total Intersistemas, entre los muchos productos y servicios ofrecidos por los proveedores y las redes transportadoras alrededor del mundo. Por esto se desarrollo las 7 siguientes capas de OSI.

I.6.1 LA CAPA DE APLICACIÓN

La capa de aplicación proporciona la interfaz y servicios que soportan las aplicaciones de usuario. También se encarga de ofrecer acceso general de la red.

Esta capa suministra las herramientas que el usuario, de hecho ve. También ofrece los servicios de red relacionados con estas aplicaciones de usuario, como la gestión de mensajes, la transferencia de archivos y las consultas de datos. La capa de aplicación suministra cada uno de estos servicios a los distintos programas de aplicación con los que cuenta el usuario en su computadora. Entre los servicios de intercambio de información que gestiona la capa de aplicación se encuentran la Web, los servicios de correo electrónico (como el Protocolo Simple de Transferencia de Correo, comúnmente

conocido como SMTP- Simple Mail Transfer Protocol – incluido en TCP/IP), así como aplicaciones especiales de bases de datos cliente/servidor.

I.6.2 LA CAPA DE PRESENTACION

La capa de presentación puede considerarse el traductor del modelo OSI. Esta capa toma los paquetes (la creación del paquete para la transmisión de datos por la red empieza en realidad en la capa de aplicación) de la capa de aplicación y los convierte a un formato genérico que pueden leer todas las computadoras. Por ejemplo, los datos escritos en caracteres ASCII se traducirán a un formato más básico y genérico.

La capa de presentación también se encarga de cifrar los datos (si así lo requiere la aplicación utilizada en la capa de presentación) así como de comprimirlos para reducir su tamaño. El paquete que crea la capa de presentación contiene los datos prácticamente con el formato con el que viajaran por las restantes capas de la pila OSI (aunque las capas siguientes irán añadiendo elementos al paquete, lo cual puede dividir los datos en paquetes más pequeños).

I.6.3 LA CAPA DE SESION

La capa de sesión es la encargada de establecer el enlace de comunicación o sesión entre las computadoras emisora y receptora. Esta capa también gestiona la sesión que se establece entre ambos nodos (véase la Figura 1.20).

FIGURA 1.20 GESTION DE SESION.

Una vez establecida la sesión entre los nodos participantes, la capa de sesión pasa a encargarse de ubicar puntos de control en la secuencia de datos. De esta forma, se proporciona cierta tolerancia a fallos dentro de la sesión de comunicación. Si una sesión falla y se pierde la comunicación entre nodos, cuando después se restablezca la sesión solo tendrán que volver a enviarse los datos situados detrás del último punto de control recibido. Así se evita el tener que enviar de nuevo todos los paquetes que incluían la sesión.

Los protocolos que operan en la capa de sesión pueden proporcionar dos tipos distintos de enfoques para que los datos vayan del emisor al receptor; la comunicación orientada a la conexión y la comunicación sin conexión. Los protocolos orientados a la conexión que operan en la capa de sesión proporcionan un entorno donde las computadoras conectadas se ponen de acuerdo sobre los parámetros relativos a la

creación de los puntos de control de datos, mantienen un dialogo durante la transferencia de los mismos, y después terminan de forma simultánea la sesión de transferencia.

Los protocolos orientados a la conexión operan de forma parecida a una llamada telefónica; en este caso, la sesión se establece llamando a la persona con la que se desea hablar. La persona que llama y la que se encuentra al otro lado del teléfono mantiene una conexión directa. Y cuando la conversación termina, ambos se ponen de acuerdo para dar por terminada la sesión y cuelgan el teléfono a la par.

El funcionamiento de los protocolos sin conexión se parece más bien a un sistema de correo regular. Proporciona las direcciones pertinentes para el envío de los paquetes y estos pasan a enviarse como si se echaran a un buzón de correo. Se supone que la dirección que incluyen permitirá que los paquetes lleguen a su destino, sin necesidad de un permiso previo de la computadora que va a recibirlos.

I.6.4 LA CAPA DE TRANSPORTE

La capa de transporte es la encargada de controlar el flujo de datos entre los nodos que establecen una comunicación; los datos no sólo deben entregarse sin errores; sino además en la secuencia que proceda. La capa de transporte se ocupa de también de evaluar el tamaño de los paquetes con el fin de que estos tengan el tamaño requerido por las capas interiores del conjunto de protocolos. El tamaño de los paquetes lo dicta la arquitectura de red que se utilice.

La comunicación también se establece entre computadoras del mismo nivel (el emisor y el receptor); la aceptación por parte del nodo receptor se recibe cuando el nodo emisor ha enviado el número acordado de paquetes. Por ejemplo, el nodo emisor puede enviar de un sólo golpe tres paquetes al nodo receptor y después recibir la aceptación por parte del nodo receptor. El emisor puede volver a enviar otros tres paquetes de datos de una sola vez.

Esta comunicación en la capa de transporte resulta muy útil cuando la computadora emisora manda demasiados datos a la computadora receptora. En este caso, el nodo receptor tomará todos los datos que pueda aceptar de una sola vez y pasará a enviar una señal de “ocupado” si se envían más datos. Una vez que la computadora receptora haya procesado los datos, y está lista para recibir más paquetes, enviará a la computadora emisora un mensaje de “luz verde” para que envíe los restantes.

I.6.5 LA CAPA DE RED

La capa de red encamina los paquetes además de entregarlos. La determinación de la ruta que deben seguir los datos se produce esta capa, lo mismo que el intercambio efectivo de los mismos dentro de dicha ruta. La Capa de Red es donde las direcciones lógicas (como las direcciones IP de una computadora de red) pasan a convertirse en direcciones físicas (las direcciones de hardware de la NIC, la tarjeta de Interfaz para Red, para esa computadora específica).

Los Ruteadores operan precisamente en la capa de red ó utilizan los protocolos de encaminamiento para determinar la ruta que deben seguir los paquetes de datos.

El modo en que se determinan los Ruteadores y la forma en que estos convierten las direcciones lógicas en direcciones físicas son temas que más adelante se mencionarán.

I.6.6 LA CAPA DE ENLACE DE DATOS.

Cuando los paquetes de datos llegan a la capa de enlace de datos, estos pasan a ubicarse en tramas (unidades de datos), que vienen definidas por la arquitectura de la red que se esta utilizando (como Ethernet, Token Ring, etc.). La capa de enlace de datos se encarga de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor, e identifica cada computadora incluida en la red de acuerdo con su dirección de hardware., que viene codificada en la NIC.

La información de encabezamiento se añade a cada trama que contenga las direcciones de envío y recepción. La capa de enlace de datos también se asegura de que las tramas enviadas por el enlace físico se reciben sin error alguno. Por ello, los protocolos que operan en esta capa adjuntarán un Chequeo de Redundancia Cíclica (Cyclical Redundancy Check o CRC) al final de la trama. El CRC es básicamente un valor que se calcula tanto en la computadora emisora como la receptora. Si dos valores CRC coinciden significa que la trama se recibió correcta e íntegramente y no sufrió error alguno durante su transferencia.

Una vez más y tal como se mencionó anteriormente, el tipo de trama que genera la capa de enlace de datos dependerá de la arquitectura de red que este utilizando., como Ethernet, Token Ring de IBM o FDDI. La figura 1.21 muestra una trama Ethernet 802.2 y la Tabla 1-1 describe cada uno de sus componentes. Aunque es posible que ahora no comprenda todas las partes que integra la trama representada esta se compone básicamente de un encabezado que la describe, de los datos que incluyen, y de la información referente a la capa d enlace de datos (como los puntos de Acceso al Servicio de Destino, Destination Service Access Point y Punto de Acceso al Servicio, Service Access Point), que no sólo definen el tipo de trama de que se trata (en esta caso, Ethernet), sino que también contribuyen a que la trama llegue a la computadora receptora.

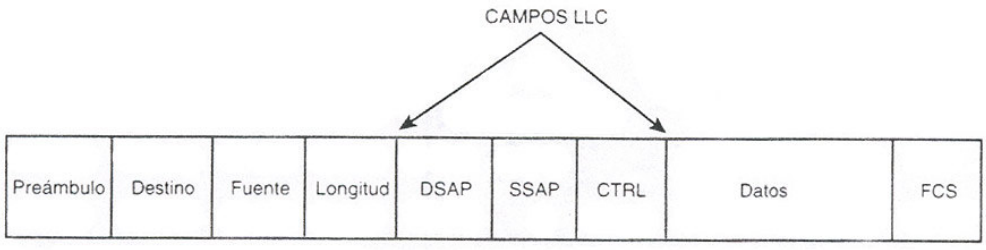


FIGURA 1.21 TRAMA DE ETHERNET 802.2

TABLA 1-1 SEGMENTOS DE LA TRAMA ETHERNET.

Segmento	Función
Preámbulo	Bits de alternación (1 y 0) que indican que se han enviado una trama.
Destino	La dirección de destino
Fuente	La dirección de origen
Longitud	Especifica el número de bytes de datos incluidos en la trama.
DSAP	Destination Server Access Point o Punto de Acceso al Servicio de Destino, indica a la tarjeta de red de la computadora receptora donde tiene que ubicar la trama dentro de la memoria intermedia
SSAP	Proporciona la información de Punto de Acceso al Servicio (Service Access Ponit) para la trama (los Puntos de Acceso al Servicio se tratan en más detalle en el apartado de "Las subcapas del enlace de datos"
CTRL	Un campo de Control Lógico de Enlace. (El enlace lógico se explica en más detalle en el apartado "Las subcapas de enlace de datos "
Datos	Este segmento de la trama mantiene los datos que se han enviado.
FCS	El campo de Secuencia de Comprobación de la Trama (Frame Check Sequence) contiene el valor CRC para la trama.

La capa de enlace de datos también controla la forma de enlace de datos en que las computadoras acceden a las conexiones físicas de la red. Nos detendremos en este aspecto de la Capa 2 en el apartado "las subcapas del enlace de datos" incluido en este mismo capítulo.

I.6.7 LA CAPA FISICA.

En la capa física las tramas procedentes de la capa de enlace de datos se convierten en una secuencia única de bits que puede transmitirse por el entorno físico de la red. La capa física también determina los aspectos físicos sobre la forma en que el cableado esta enganchado a la NIC de la computadora. En la computadora receptora de datos, la capa física es la encargada de recibir la secuencia única de bits (es decir, información formada por 1 y 0).

I.6.7.1 LAS SUBCAPAS DEL ENLACE DE DATOS

Antes de dar por finalizada nuestra explicación del modelo de red OSI, es preciso que volvamos atrás y comentemos con más detalle algunas especificaciones desarrolladas por el IEEE para la capa de enlace de datos del modelo OSI. La especificación IEEE 802 dividía la capa de enlace en dos subcapas, el Control Lógico del Enlace (Logical Link Control o LLC) y el Control de Acceso al Medio (Media Access Control o MAC).

La subcapa de Control Lógico del Enlace establece y mantiene el enlace entre las computadoras emisora y receptora cuando los datos se desplazan por el entorno físico de la red. La subcapa LLC también proporciona Puntos de Acceso al Servicio (Service Access Points o SAP), que no son más que puntos de referencia a las que otras computadoras que envíen información pueden referirse y utilizar para comunicarse con las capas superiores del conjunto de protocolos OSI dentro de un determinado nodo receptor. La especificación IEEE que define la capa LLC es la 802.2. La subcapa de Control de Acceso al Medio determina la forma en que las computadoras se comunican dentro de la red, y cómo y dónde una computadora puede acceder, de hecho, al entorno físico de la red y enviar datos. La especificación 802 divide a su vez la subcapa MAC en una serie de categorías (que no son más que formas de acceder al entorno físico de la red), directamente relacionadas con la arquitectura especifica de la red, como Ethernet y Token Ring (véase la figura 1.22).

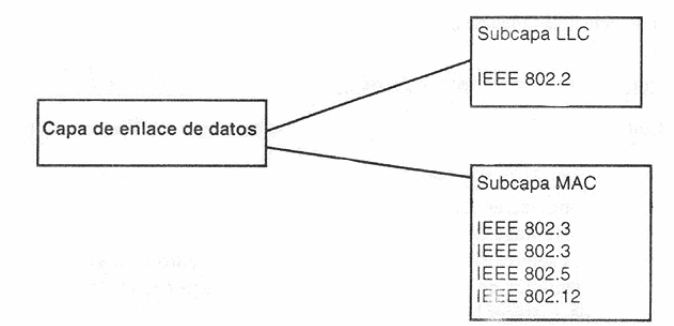


FIGURA 1.22 CAPA DE ENLACE COMPUESTA POR DOS SUBCAPAS.

I.7 PROTOCOLOS

En el siguiente apartado se verán los siguientes tipos de protocolos que existen para una Red LAN.

Para que un paquete de datos viaje desde un origen hasta su destino en una red, es muy importante que todos los dispositivos de dicha red hablen el mismo lenguaje o protocolo. Protocolo esta definido como un conjunto de normas que hacen posible y más eficiente la comunicación de la red.

I.7.1 NETBEUI

Es el protocolo utilizado en las antiguas redes basadas en Microsoft LAN Manager. Es muy rápido en pequeñas redes que no llegan a la decena de equipos y no muevan ficheros de gran tamaño, a partir de ahí es mejor que te inclines por otra opción y lo desinstales de tus clientes y tus servidores, esto ultimo siempre que no tengas ningún equipo que utilice LAN manager.

I.7.2 IPX/SPX

Este protocolo, implementado por Novell, se ha demostrado sobradamente su valía en redes de área local, es rápido, fácil de configurar y requiere pocas atenciones. Es el

protocolo que Microsoft recomienda para redes de área local basadas en DOS, Windows 3.X, Windows 95 y Windows NT. El principal inconveniente que presenta para redes medianas y grandes es que no se puede enrutar o sea que no puede pasar de una subred a otra; si entre ambas hay un Ruteador, por lo que no puede usarse en redes WAN. Otro inconveniente que presenta en redes con un cierto número de equipos es que puede llegar a saturar la red los broadcast que lanzan los equipos para anunciarse en la red.

El termino IPX, significa; Intercambio de Paquetes en Red/Intercambio Secuencial de Paquetes. La principal función del protocolo IPX es la de entrega de paquetes de nodo a nodo en una comunicación entre redes. El termino SPX; es el protocolo de transporte de Novell el cual proporciona aviso de entrega e intercambio de paquetes.

I.7.3 TCP/IP

Este protocolo cuenta con una gran ventaja; pues en la mayoría de redes se utiliza y además se hace imprescindible si estas conectado a Internet o quieres crear una intranet. La capacidad de TCP/IP para mover información en una red, por grande que sea, sin perder datos, su sistema de nombres y direcciones, y su facilidad para saltar de una red a otra lo convierten en el candidato ideal para cualquier red de ordenadores dispuesta a no quedarse dentro de las paredes de un edificio. No obstante pueden achacársele algunos inconvenientes como a dificultad de configuración para el usuario y la necesidad de un mantenimiento constante por parte del administrador de la red.

El primer inconveniente se debe a la necesidad que tiene el usuario de conocer algunos datos imprescindibles antes de que el sistema empiece a funcionar en red: dirección IP, mascara de red, dirección de servidor de nombres, y dirección del Ruteador, afortunadamente este problema puede resolverse utilizando el servicio de configuración dinámica de equipos (DHCP), que viene incluido en Windows NT Server, este servicio asigna los datos mencionados arriba; a cada equipo en el momento en que este se conecta en red de manera transparente para el usuario. El trabajo de mantenimiento por parte del administrador tampoco es fácil: asignación de IP a los nuevos equipos, mantenimiento de la tabla de nombres en el servidor de nombres si existe o, peor aún, en cada equipo si no existe y vigilar que no hay direcciones duplicadas por citar sólo algunos. De nuevo NT Server nos da una mano si combinamos la potencia de DHCP con el servicio de nombres para Windows (WINS) y el reciente servicio de nombre de dominio (DNS).

Otro inconveniente que aún no hemos mencionado es la falta de seguridad de TCP/IP frente a los “mirones” que tengan acceso físico de la red, ya que las tramas TCP/IP no van codificadas y con un software adecuado podría capturarse parte de la información que estamos enviando. Para este problema comienzan a surgir soluciones como el protocolo punto a punto apantallado (PPTP), que encripta las tramas TCP/IP que enviamos, estableciendo de esta forma un canal seguro incluso a través de Internet.

I.7.4 APPLETALK

La computadora Apple dispone de un grupo propio de protocolos de la familia AppleTalk. El protocolo de clasificación de AppleTalk AFP (AppleTalk Filing Protocol) es el único que permite compartir archivos distribuidos por la red. AFP esta conectado al

Sistema de archivo jerárquico HFS (Hierarchical File System) en el sistema operativo Macintosh.

I.8 ORGANISMOS DE ESTANDARIZACION

Entre los principales organismos internacionales que se ocupan de actividades relacionadas al desarrollo de estándares para la implementación de sistemas distribuidos en el área de transmisión de información, a través de redes públicas de datos encontramos a CCITT, IEEE e ISO.

I.8.1 CCITT

El CCITT (Consultive Comité Internacional Telegragh and Telephone; Comité Consultivo Internacional de Telegrafía y Telefonía) esta conformado por organismos nacionales de correo y telecomunicaciones así como de compañías privadas que ofrecen servicios públicos de comunicaciones.

En lo que se refiere a la transmisión de datos, el CCITT estableció dos comisiones: la Comisión de Estudios XVII encargada de elaborar las recomendaciones sobre la transmisión de datos a través de una red telefónica, conocidas como las recomendaciones de la serie V y la Comisión de Estudio VII, la cual se encarga de las recomendaciones sobre la transmisión de datos a través de redes publicas para transmisión de datos, que se denominan normas X.

I.8.2 LA ITU-T

La ITU (Unión de Telecomunicaciones Internacional; International Telecommunication Union) fue creada en 1934, y con la creación de la ONU se vinculó a ésta en 1947. La ITU tiene tres sectores de los cuales sólo nos interesa el conocido como ITU-T que se dedica a la estandarización de las telecomunicaciones. Desde 1956 a 1993 la ITU-T se conoció con el nombre CCITT, acrónimo del nombre francés Comité Consultatif International Télégraphique et Téléphonique. En 1993 el CCITT fue reorganizada y se le cambió el nombre a ITU-T; estrictamente hablando el cambio de nombre tiene efectos retroactivos, es decir, los documentos vigentes, aún cuando fueran producidos antes de 1993, son hoy documentos de la ITU-T y no del CCITT.

Los miembros de la ITU-T son de cinco clases:

- Representantes de los países.
- Operadores privados reconocidos (por Ej. British Telecom, Global One, AT&T).
- Organizaciones regionales de telecomunicaciones (p. ej. el ETSI).
- Empresas que comercializan productos relativos a telecomunicaciones y organizaciones científicas.
- Otras organizaciones interesadas (bancos, líneas aéreas, etc.).

Entre los miembros hay unos 200 representantes de países, unos cien operadores privados y varios cientos de miembros de las otras clases. Sólo los representantes de los países tienen derecho a voto, pero todos los miembros pueden participar en el trabajo.

Para desarrollar su trabajo la ITU-T se organiza en Grupos de Estudio, que pueden estar formados por hasta 400 personas. Los Grupos de Estudio se dividen en Equipos de Trabajo (Working Parties), que a su vez se dividen en Equipos de Expertos (Expert Teams).

Las tareas de la ITU-T comprenden la realización de recomendaciones sobre interfaces de teléfono, telégrafo y comunicaciones de datos. A menudo estas recomendaciones se convierten en estándares reconocidos internacionalmente, por ejemplo la norma ITU-T V.24 (también conocida como EIA RS-232) especifica la posición y el significado de las señales en el conocido conector de 25 contactos utilizado en muchas comunicaciones asíncronas. La ITU-T denomina a sus estándares "recomendaciones"; con esto se quiere indicar que los países tienen libertad de seguirlas ó no. Ignorarlas puede suponer quedar aislado del resto del mundo, por lo que en la práctica a menudo las recomendaciones se traducen en obligaciones.

Todos los estándares de la ITU-T se nombran mediante una letra seguida de un punto seguido a su vez de números. La letra identifica la serie, por ejemplo todo lo relativo a módems se encuentra en la serie V (V.32, V.42,…); la serie X trata sobre redes de datos y OSI (X.25, X.400,...), las series I y Q definen la RDSI, la serie H comprende todo lo relativo a codificación digital de vídeo y videoconferencia (H.263, H.323, etc.).

I.8.3 IEEE

El IEEE (Institute of Electrical and Electronic Enginners; Instituto de Ingenieros Eléctricos y Electrónica) es una organización profesional que ha desarrollado un número considerable de estándares en la redes de datos.

Entre los estándares implementados por el IEEE en el área de las redes LAN son actualmente predominantes e incluyen protocolos muy similares y virtualmente equivalentes a Ethernet y Token Ring.

I.8.4 ISO

La ISO (Internacional Standarization Organization; Organización Internacional de Normalización) es una federación de organismos nacionales de normalización y se encarga de la elaboración de recomendaciones internacionales a partir de propuestas de sus países miembros y de otros organismos profesionales. Sus trabajos se organizan en Comités Técnicos en grandes áreas de trabajo y estos a su vez se subdividen en subcomités para el estudio de temas específicos.

Del campo de la informática se ocupa el Comité Técnico de Computadoras y el Tratamiento de la Información. Como consecuencia del creciente interés por el tema de los sistemas distribuidos en 1977 se creo un subcomité denominado "Interconexión de Sistemas Abiertos". Los trabajos de dicho Subcomité han dado lugar a la elaboración de un modelo de referencia conocido como OSI (Open System Interconnection; Interconexión de Sistemas Abiertos), el cual constituye una pauta al adentrarse en el estudio de los sistemas distribuidos.

En este trabajo se revisará algunos estándares que se utilizan en las tecnologías de LAN y WAN, por lo que es importante tener presente los organismos anteriores, para saber el contenido a detalle de los estándares se tendrían que verificar las publicaciones de los estándares.

CAPITULO II REDES WAN

II.1 REDES WAN

En este trabajo es muy importante describir lo que conlleva realizar una Red WAN (Red de Área Amplia, en ingles Wide Area Network), que es ampliar nuestras redes LANs hasta otros limites geográficos más extensos, para poder realizar intercambio de información a distancia, lo que nos da la ventaja de establecer comunicación más eficiente y confiable entre oficinas a distancia, sin tener que viajar en oficina a oficina.

II.1.1 INTRODUCCIÓN

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la red de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales (como DBP en Alemania o British Telecom en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como Frame Relay y SMDS - Synchronous Multimegabit Data Service) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han llamado autopistas de la información.

II.1.2 REDES DE ÁREA EXTENSA (WAN)

Como podría suponer por el nombre, una red de área amplia (WAN) es una red de PC dispersa en un área amplia. Recuerde que una LAN de manera característica esta en un área geográfica limitada, como una habitación o un edificio. Cuando se dispersa la red es llamada Red de Area Amplia. Ejemplos de estas redes de computadoras pueden encontrarse en colegios y universidades muy grandes, o en compañías que tienen oficinas en más de un área geográfica. La figura 2.1 describe las características de una red WAN.

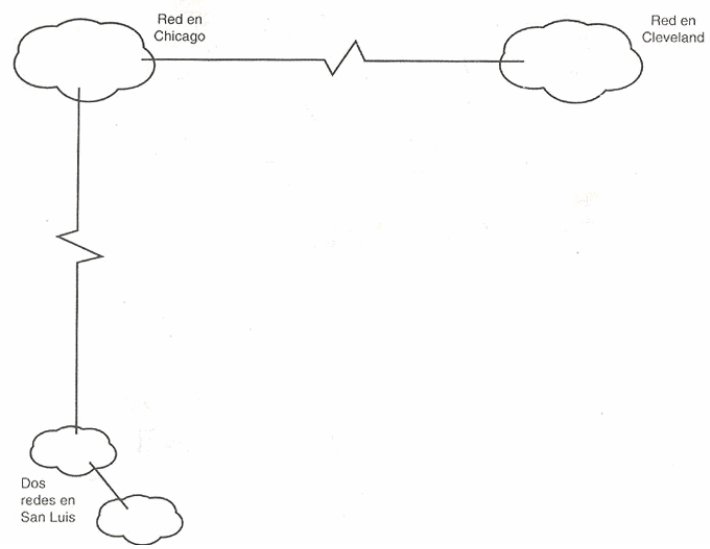


FIGURA 2.1 CARACTERISTICAS DE UNA RED WAN.

Muchas veces las redes comienzan como una LAN, pero pronto se vuelven WAN conforme la compañía o la organización crecen. Por ejemplo, si una compañía tiene una sola oficina en Chicago, puede desarrollar una LAN para su oficina. Si la compañía abre una oficina en Cleveland o San Luis, la compañía puede tender a duplicar la misma clase de oficinas en esas localidades; incluyendo la LAN. Cuando las LAN en Chicago y Cleveland o San Luis se conectan entre sí, la compañía ha desarrollado su propia WAN.

II.1.3 CONSTITUCION DE UNA RED DE AREA AMPLIA (WAN)

La red consiste en ECD (computadores de conmutación) interconectados por canales alquilados de alta velocidad (por ejemplo, líneas de 56 kbps). Cada ECD utiliza un protocolo responsable de encaminar correctamente los datos y de proporcionar soporte a los computadores y terminales de los usuarios finales conectados a los mismos. La función de soporte ETD (Terminales / computadores de usuario). La función de soporte del ETD se denomina a veces PAD (Packet Assembly / Disasembly – Ensamblador / Desensamblador de Paquetes). Para los ETD, el ECD es un dispositivo que los aísla de la red. El centro de control de red (CCR) es el responsable de la eficiencia y fiabilidad de las operaciones de la red.

II.2 MEDIOS DE TRANSMISION

Definiendo a un medio de transmisión como el canal físico donde se llevará nuestra información a una distancia amplia, que se definen de acuerdo a la velocidad de transmisión y la eficiencia de ninguna ruptura en él, para ser más integra nuestra red, es importante saber como debemos aprovechar estos medios en nuestra red.

II.2.1 HILOS DE TRANSMISIÓN

En comunicaciones telefónicas se utiliza con frecuencia el termino "pares" para describir el circuito que compone un canal. Uno de los hilos del par sirve para transmitir o recibir los datos, y el otro es la línea de retorno eléctrico.

II.2.2 MICROONDAS

En un sistema de microondas se usa el espacio aéreo como medio físico de transmisión. La información se transmite en forma digital a través de ondas de radio de muy corta longitud (unos pocos centímetros). Pueden ser direccionados múltiples canales a múltiples estaciones dentro de un enlace dado, o pueden establecerse enlaces punto a punto. Las estaciones consisten de una antena tipo plato y de circuitos que interconectan la antena con terminal del usuario.

Cuando el sistema de microondas pertenece a la compañía de teléfonos, parte de la red telefónica por cables intervienen en el circuito. Dependiendo del país y de su legislación, a veces es necesario obtener una licencia especial para uso privado y esto puede constituirse en un contratiempo. También puede decirse que por el momento, los componentes resultan bastante costosos y no están disponibles fácilmente. La transmisión es una línea recta (lo que esta a la vista) y por lo tanto se ve afectada por accidentes geográficos, edificios, bosques, mal tiempo, etc. El alcance promedio es de 40 Km., en la Tierra. Una de las ventajas importantes es la capacidad de poder transportar miles de canales de voz a grandes distancias a través de repetidoras, a la vez que permite la transmisión de datos en su forma natural. Como se muestra en la figura 2.2.

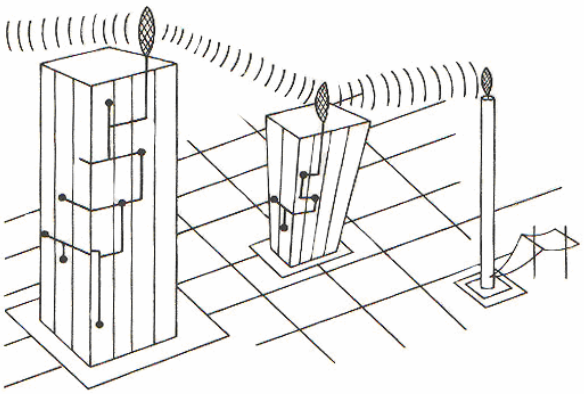


FIGURA 2.2 TRANSMISION DE MICROONDAS CON REPETIDORAS

II.2.3 SATELITES

Muy amplia es actualmente la difusión del uso de satélites en redes de procesamiento de datos y se espera, además, un futuro muy promisorio en lo que concierne a una cobertura total del globo terráqueo, que elimine definitivamente la barrera de los océanos y las montañas.

II.2.3.1 CARACTERÍSTICAS DEL MEDIO

El satélite de comunicaciones es un dispositivo que actúa principalmente como “reflector” de las emisiones terrenas. Podríamos decir, que es la extensión al espacio del concepto de “torre de microondas”. Al igual que estas, los satélites “reflejan” un haz de

microondas que trasportan información codificada. Realmente, la función de “reflexión” se compone de un receptor y un emisor, que opera a diferentes frecuencias: recibe a 6 GHZ y envía (refleja) a 4GHZ, por ejemplo.

Físicamente, los satélites giran alrededor de la Tierra en forma sincrónica con esta a una altura de 35680 Km., en un arco directamente ubicado sobre el ecuador. Esta es la distancia requerida para que un satélite gire alrededor de la Tierra en 24 horas, coincidiendo entonces con una vuelta completa de un punto en el ecuador. Esta es la característica que en definitiva determina el objetivo geoestacionario que tienen los satélites de comunicaciones. Algunos menos de la mitad del globo queda en “el cono de mira” de un satélite, con lo cual, es obvia la importancia del alcance que tiene cada uno de estos dispositivos. Como ejemplo, digamos que un satélite ubicado sobre el ecuador en cualquier punto latinoamericano, actuaría como una altísima torre de microondas que permitiría interconectar todo el continente. Muchos satélites en los Estados Unidos usan la misma frecuencia que las torres terrenas de microondas, que operan en la línea de vista. En la figura 2.3 se muestra la posición de un satélite.

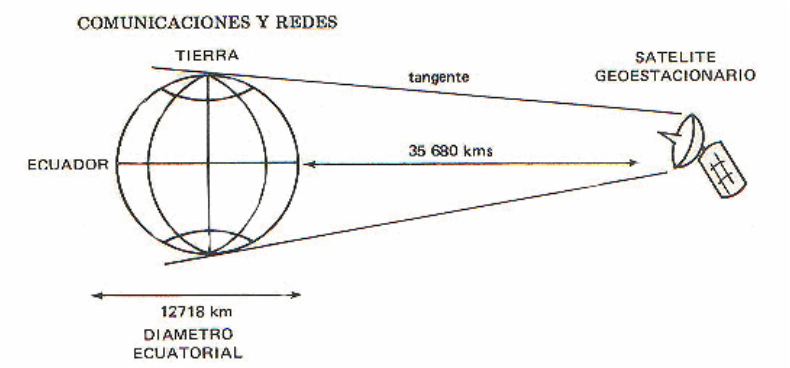


FIGURA 2.3. POSICION DE UN SATELITE RESPECTO A LA TIERRA.

El esparcimiento o separación entre dos satélites de comunicaciones, es de 2880 Km. equivalente a un ángulo de 4^0, visto desde la Tierra. La consecuencia inmediata es que el número de satélites posibles a conectar de esta forma es finito (y bastante reducido aunque tal vez suficiente si se saben aprovechar).

II.3 TIPOS DE ENLACE

Los enlaces sirven para la interconexión de redes, es decir desde una Red A, como haré el enlace entre mi Red B, existiendo un gran número que empresas dedicadas a estos servicios proporcionan de acuerdo al tipo de datos de información y velocidad que se requiera, dando como resultado diferentes costos por la infraestructura utilizada.

II.3.1 LÍNEAS PUNTO A PUNTO

Enlazan dos DTE

II.3.2 LÍNEAS MULTIPUNTO

Enlazan tres o más DTE

II.3.3 LÍNEA DEDICADA

Este servicio puede ser analógico ó digital. Una red analógica usa muchas de las técnicas de transmisión analógica convencionales y consecuentemente adolece de muchas de las limitaciones del sistema analógico conmutado. Las redes digitales de línea dedicada mantienen la señal en forma digital a través del circuito.

II.3.4 CIRCUITO ANALOGICO CONMUTADO

Normalmente proporcionado por la red telefónica pública. Usa el mismo principio de discado del sistema telefónico.

II.3.5 CIRCUITO DIGITAL CONMUTADO

Este servicio proporciona únicamente circuitos “Full dúplex”, punto a punto. Sus principales características son: bajos porcentajes de error, tiempo rápido de establecimiento de llamada y la estructura que facilita la determinación de tarifas de una red conmutada.

II.3.6 LINEAS TELEFONICA DIGITALES

Si una red va a cubrir un área geográfica grande (una WAN), entonces se necesita ver otras soluciones de cable, además de apropiadas para una LAN. De esta manera característica esto implica trabajar con la compañía telefónica o algún otro transporte común para rentar líneas de datos dedicadas entre sitios.

Las líneas de datos dedicadas vienen en diversas variedades, cada una se distingue por la capacidad (ancho de banda) del canal. En general existen tres tipos de conexiones dedicadas:

II.3.6.1 CANAL DEDICADO

Este es un canal dedicado común de capacidad pequeña. El ancho de banda que utiliza este canal es de acuerdo a la normatividad que rigen en el país donde se encuentra ya que los valores típicos son de 56 Kbps y 64 Kbps (en México se utiliza el termino DS0 que implica un canal de 64 Kbps), según el sistema que maneja cada empresa que lo proporciona, como se muestra en las dos secciones siguientes.

II.3.6.2 SISTEMA AMERICANO

Canal T1. Este tipo de conexión es equivalente a 24 canales de 56Kb, que opera en un ancho de banda de 1,544 MBPS. Cuando use un canal T1, necesitará equipo especial de la compañía telefónica en su oficina, ya que la transmisión se hace por cable de fibra óptica. El canal comienza en su localidad y termina en el conmutador de la compañía telefónica, donde su señal de datos se comprime en las líneas de gran capacidad de la compañía telefónica. Esta señal termina en el conmutador de la compañía telefónica sirve a su sitio remoto, donde se separa de las líneas telefónicas normales y se envía en forma directa a su sitio remoto.

Canal T3. El circuito dedicado mas rápido que puede obtener es su canal T3, el cual opera a 44736 Mbps. Con este ancho de banda la conexión tiene 28 veces la capacidad del canal T1 y 672 veces la capacidad de la línea de 56 Kb. El costo de rentar circuitos dedicados puede ser bastante alto y variara con base en la distancia recorrida por el circuito. Cuando compre una conexión así, es buena idea discutir las alternativas con las compañías de larga distancia que pueden proporcionarle el servicio.

II.3.6.3 SISTEMA EUROPEO

Troncales digitales de 64 KBPS para un conmutador con conexión de 2048 MBPS.

Líneas privadas para conducción de señales punto a punto o multipunto tipo E0 (64 KBPS) y E1 (2,048 MBPS). Circuitos Privados para conducción de señales nacionales e internacionales Tipo E0 y E1. Sin embargo existe un canal más rápido que se denomina E3 que opera con un ancho de banda de 34368 Mbps, que por lo general este servicio se proporcionan a empresas con un nodo central que debe proporcionar servicios centrales a sus estaciones remotas para mejor el rendimiento en la red.

II.4 TECNICAS DE INTERCONEXION

Para establecer mi comunicación de redes, se tiene que tomar en cuenta la técnica de interconexión en mi red, ya que conocerlas nos sirve para saber el proceso que sigue nuestros paquetes que llevan de una red hasta otra y así definir los posibles problemas y rendimiento de la misma.

II.4.1 CONMUTADAS POR CIRCUITOS

Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

II.4.2 CONMUTADAS POR MENSAJE

En este tipo de redes, el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

II.4.3 CONMUTADAS POR PAQUETES

Las redes de paquetes brindan un “circuito” virtual, es decir, un circuito que parece ser una conexión punto a punto para un par de terminales. En realidad es un circuito compartido por muchas terminales mediante técnicas múltiplex de división de tiempo, proporcionado por una transportadora de paquetes. Las redes de paquetes ofrecen únicamente dos servicios básicos de conmutación:

1. Llamada virtual, en la que se establece un circuito virtual temporario entre terminales (similar a una llamada de circuito conmutado)

2. Circuito Virtual Permanente, en el que las terminales están asociadas permanentemente por medio de un circuito virtual (similar a un circuito dedicado).

En ambos casos, el usuario debe transmitir sus datos a la transportadora común en un formato específico de la transportadora, que se conoce como paquete. En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

II.4.4 REDES ORIENTADAS A CONEXIÓN

En estas redes existe el concepto de multiplexión de canales y puertos conocido como ***circuito o canal virtual***, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

II.4.5 REDES NO ORIENTADAS A CONEXIÓN

Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es INTERNET.

II.4.6 RED PÚBLICA DE CONMUTACIÓN TELEFÓNICA (PSTN)

Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

II.5 LA TECNOLOGIA DE COMUNTACION DE PAQUETES

Una de las tecnologías más utilizadas en la actualidad es la conmutación de paquetes ya que proporciona un rendimiento eficiente y han llegado a alcances económicos para muchas empresas, como se describe en los siguientes temas.

II.5.1 INTRODUCCION

Los términos “conmutación de paquetes” y “conmutación de circuitos” son comúnmente usados como sinónimos siendo términos diferentes. La conmutación de paquetes permite que múltiples usuarios compartan las facilidades de la red de datos y Ancho de Banda, en lugar de ofrecer cantidades determinadas.

II.5.2 REDES DE CONMUTACION PARA LA TRANSMISION DE DATOS.

La tecnología de conmutación se ha desarrollado por la necesidad de compartir los recursos de la red entre los diferentes usuarios del sistema y hacerla más eficiente desde

el punto de vista económico, de esta manera podemos mencionar tres clases de redes de conmutación:

1. Redes de Conmutación de Circuitos
2. Redes de Conmutación de Mensajes
3. Redes de Conmutación de Paquetes

II.5.2.1 REDES DE CONMUTACION DE CIRCUITOS

La conmutación de circuitos se origina en la red de telefonía pública; cuando se realiza una llamada y, cuando desde ambos extremos comienzan a comunicarse, lo están realizando sobre un circuito temporal. Este circuito esta dedicado a las dos personas hasta que concluya la llamada. Si ellos cuelgan y vuelven a llamar se establecerá otro circuito de la misma manera, pero no necesariamente sobre la ruta anterior. De esta manera, pueden compartirse entre los usuarios recursos comunes de la red (circuitos).

El proceso de comunicación entre computadoras es igual. Una llamada de punto a punto es establecida como un circuito virtual y se mantiene vigente hasta que toda la información ha sido transmitida. Entonces el circuito es desactivado. El Ancho de Banda asignado a la llamada es dedicado a ella hasta que la información es transmitida y recibida en su totalidad. La conmutación de circuitos es la tecnología ideal para el tráfico que requiere un constante Ancho de Banda y tiempos mínimos de generación y terminación de la llamada.

II.5.2.2 REDES DE CONMUTACION DE MENSAJES

En los años 60’s y 70’s, el método mas extendido en la transferencia de datos era la conmutación de mensajes. Esta tecnología sigue empleándose todavía en aplicaciones como el correo electrónico. A diferencia de la conmutación de circuitos, la conmutación de mensajes es una tecnología que permite grabar la información para atenderla después, gracias a la capacidad de almacenamiento que posee este tipo de conmutador. Puesto que los datos suelen estar almacenados, el tráfico no puede considerarse interactivo o en tiempo real, aunque también es posible cursar mensajes a gran velocidad, estableciendo prioridades para las distintas clases de tráfico, de esta forma, el tráfico de más alta prioridad permanece menos tiempo en cola.

II.5.2.3 REDES DE CONMUTACION DE PAQUETES

Como respuesta a los problemas presentados por la conmutación de mensajes, en los años 70’s la industria busco una nueva estructura de conmutación para el envió de datos. Frente a la conmutación de mensajes, la conmutación de paquetes distribuye el riesgo a más de un conmutador, reduce la vulnerabilidad de las fallas en la red y permite un mejor aprovechamiento del canal de comunicaciones. Mientras que existe una mayor saturación con la conmutación de paquetes comparada con la conmutación de circuitos, esta saturación garantiza en envió libre de errores por el uso de paquetes diseccionados que se transmiten por la red. Debido a que la conmutación de paquetes no requiere conexión, en contraste con la conmutación de circuitos, la inteligencia de los nodos de la red enruta los paquetes alrededor de los otros nodos en situaciones de falla. Se puede

alcanzar velocidades mucho más altas por medio de la conmutación de circuitos que la conmutación de los paquetes convencional X.25, la cual es limitada a 64 Kpbs.

La conmutación de paquetes es únicamente un servicio que no requiere de conexiones y que es efectivo para la transmisión cuya información no dependa del tiempo de respuesta pero es poco recomendable para las conexiones orientadas y de voz y video que requieran velocidad. La conmutación de paquetes pasa información de nodo a nodo empleando un esquema de encolamiento. La información es recibida y procesada si el Ancho de Banda se encuentra disponible, si no lo esta, la información es almacenada en la cola de espera hasta que el Ancho de Banda este disponible.

El tráfico puede ser clasificado también por prioridades. Los nodos de los extremos son los responsables de la detección y corrección de errores, así como de iniciar su recuperación. La conmutación de paquetes es un amplio término que comenzó con los servicios de X.25. Ahora es utilizado de una u otra forma para presentar tecnologías actuales como “Frame Relay”.

II.5.2.3.1 PRINCIPIOS DE TRANSMISON DE PAQUETES

Un **paquete** es una secuencia continua de bits transmitidos en una red como una unidad. Los bits pueden representar una colocación de caracteres individuales y representar información de control de la llamada o simplemente la información que el usuario desea transmitir. Estas cadenas de bits proceden de un dispositivo sincrono o asíncrono, y están contenidas en un formato preestablecido.

Un **paquete conmutado** es un paquete diseccionado, con lo cual un canal de transmisión es ocupado durante el envió del paquete. El canal esta disponible para los paquetes que están siendo transferidos entre los diferentes equipos terminales de datos.

Un **Circuito Virtual** es un circuito lógico utilizado en la comunicación entre dispositivos terminales en una red o entre dos redes. El término “virtual” se refiere al hecho de que sin ser un circuito físico establecido., funciona como tal. La ventaja que proporciona este tipo de circuito, es que permite el ahorro de Ancho de Banda, pues a través de un solo canal físico es posible establecer una gran cantidad de Circuitos Virtuales.

Un **PVC (Permanent Virtual Circuit; Circuito Virtual Permanente)** es, como su nombre lo indica, un circuito lógico permanente establecido. Los PVC son ideales para situaciones en donde la necesidad de contar con un medio de comunicación constante.

Un **SVC (Switched Virtual Circuit; Circuito virtual Conmutado)** es un circuito virtual que puede ser establecido dinámicamente de acuerdo a la demanda, en contraste con el PVC.

Entre los tópicos y conceptos involucrados en la transmisión de un paquete desde un dispositivo de origen hasta otro de destino, podemos mencionar:

1. Ensamble de un paquete en le punto origen.
2. Identificación del paquete

3. Transporte del paquete
4. Recepción y desensamblaje del paquete en el punto de destino.

Los siguientes términos, son utilizados ampliamente para describir el proceso de ensamblaje y transporte de un paquete:

Conversión de protocolo. Conversión de un Protocolo Nativo (como el Asíncrono) hacia un protocolo de Interfaz (por ejemplo el Modo Paquete) y viceversa.

PAD (Packet Assembly/Disammbly: Ensamblador/Desensamblador de Paquetes). Es un software utilizado en forma de módulos que realiza principalmente las funciones representadas por estos términos, se muestra en la figura 2.4.

II.5.2.3.2 ENSAMBLE DEL PAQUETE

La transmisión de los datos, a través de una red de paquetes, comienza con la conversión del protocolo de Modo Nativo (esta dado en la aplicación) hacia le Modo Paquete. Los paquetes ensamblados comienzan cuando el primer caracter es recibido en la terminal fuente, y colocado en la memoria (búfer) del convertidor de protocolos. Cada caracter adicional es recibido y almacenado en el búfer: este procedimiento continúa hasta que una condición indica el final del paquete.

Una vez que el paquete sale, es “encapsulado” y se le adiciona un encabezado de paquete. En este instante, el paquete esta preparado para ser transmitido a través de la red.

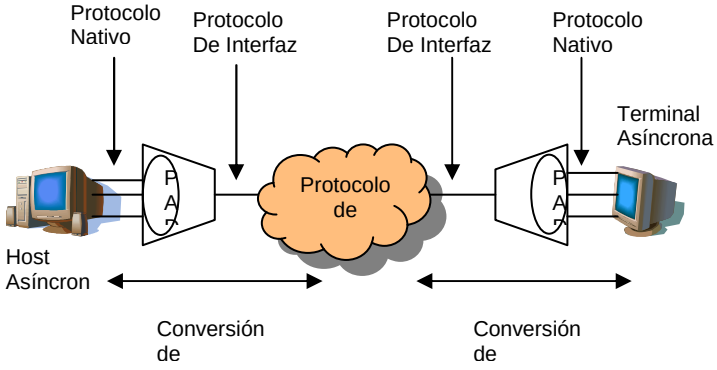


FIGURA 2.4 FUNCIONES DEL PAD.

II.5.2.3.3 ENCABEZADO DEL PAQUETE

El encabezado de paquete contiene la información necesaria para su manejo a través de la red. La información contenida en el encabezado incluye por lo general:

Identificación de información. Incluye un número identificador del paquete. La función de identificador del paquete, asigna un número de identificación, conocido como LCN (Logical Channel Number, Número de Canal Lógico).

Número de secuencia. También es asignado en el encabezado del paquete de datos. El número de secuencia identifica el orden en el cual los paquetes son transmitidos. Este número es usado para el reconocimiento del paquete, y para identificar la secuencia en la cual los paquetes están siendo desempeñados en el dispositivo de destino.

II.5.2.3.4 CAMPO DE INFORMACION

Los datos del usuario están contenidos en este campo. El tamaño del paquete de datos esta determinado por el número de caracteres que el administrador del sistema asigne.

II.5.2.3.5 TRANSPORTE DEL PAQUETE

Una vez que el paquete es ensamblado, es enviado a través de un enlace de comunicaciones. En seguida de que el paquete es transportado, este debe ser puesto en la trama. El mecanismo de entramado es responsable de transportar el paquete libre de errores a través del enlace.

II.5.2.3.6 RECONOCIMIENTO DE TRAMA

El reconocimiento de trama es un mecanismo usado por una red de paquetes para asegurar la entrega de datos a través del enlace. Una vez recibida la trama, el dispositivo receptor checa que la trama sea correcta. Si no ocurren errores durante la transmisión, un paquete de reconocimiento regresa al dispositivo fuente, cuando este recibe el reconocimiento de trama, borra la copia de la trama que mantenía almacenada en memoria. Si al dispositivo receptor detecta un error en el Chequeo de Secuencia de Trama, descarta la trama incorrecta y no le envía el reconocimiento. Las tramas subsecuentes llegaran fuera de sincronía y serán rechazadas por el nodo receptor, causando retransmisiones.

II.5.2.3.7 DESENSAMBLE DEL PAQUETE

La función de desensamble del paquete es responsable de convertir los datos del usuario contenidos en el Modo Paquete a su formato (Modo Nativo) y transmitirlo hacia el dispositivo de destino, el cual se encargara de recuperar la información del usuario.

II.6 LAS REDES PÚBLICAS Y PRIVADAS

En la siguiente sección, se describirán las diferencias de redes públicas y privadas, para conocer la operabilidad, así como los conceptos para realizar el diseño de una WAN y tener en cuenta la seguridad e integridad del servicio.

II.6.1 LAS REDES PÚBLICAS

Las redes públicas son los recursos de telecomunicación de área extensa pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción.

Estas operadoras incluyen a:

- Compañías de servicios de comunicación local. Entre estas compañías tenemos a TELCOR.
- Compañías de servicios de comunicación a larga distancia. Una compañía de comunicación a larga distancia (IXC: IntereXchange Carriers) es un operador de telecomunicaciones que suministra servicios de larga distancia como AT&T, MCI y US SPRINT.
- Proveedores de servicios de valor agregado. Los proveedores de servicio de valor agregado (VACs: Value-Added Carriers) como CompuServe Information y GE Information Services, ofrecen con frecuencia, servicios de comunicación de área amplia como complemento a su verdadero negocio.

II.6.2 REDES PRIVADAS

Una red privada es una red de comunicaciones privada construida, mantenida y controlada por la organización a la que sirve. Como mínimo una red privada requiere sus propios equipos de conmutación y de comunicaciones. Puede también, emplear sus propios servicios de comunicación o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus propias líneas de comunicaciones.

Aunque una red privada es extremadamente cara, en compañías donde la seguridad es imperante así como también lo es el control sobre el tráfico de datos, las líneas privadas constituyen la única garantía de un alto nivel de servicio. Además, en situaciones donde el tráfico de datos entre dos puntos remotos excede de seis horas al día, emplear una red privada puede ser más rentable que utilizar la red pública.

II.7 INTERNETWORKING UNITS (IWU) EN LAS NUEVAS FRONTERAS

Se podrá definir a InternetWorking como la colección de redes interconectadas mediante Ruteadores y otras Unidades que funcionan generalmente como una red única, que basa para referir productos, procedimientos y tecnologías como se describe a continuación.

II.7.1 INTRODUCCION

El Internetworking permite la conexión de redes separadas, física o lógicamente, ayuda a superar sus ámbitos de operación y mejora su rendimiento global. El internetworking puede ser visto como metodología que permite estructurar una red de forma coherente distribuyendo, o centralizando, la información de la forma más adecuada, independientemente de su localización geográfica; también puede proporcionar anchos de banda dedicados e interconectar segmentos de diferente tecnología. (Figura 2.5).

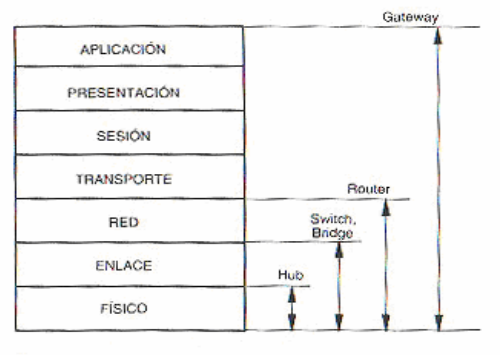


FIGURA 2.5 NIVEL DE RUTEO DE LAS INTERNETWORKING UNITS

El internetworking se realiza mediante las InternetWorking Units (IWU) que engloban una amplia gama de dispositivos entre los que cuentan los hubs (concentradores), los bridges (puentes), los Ruteadores (encaminadotes) y los gateways (pasarelas):

II.7.2 DESCRIPCION DE DISPOSITIVOS WAN

A continuación se enlistarán algunos de los dispositivos más conocidos, como los más usados en la conexión de una red WAN, por lo que se llevará a cabo una descripción de los mismo, así como sus características de cada uno.

II.7.2.1 PUENTES (BRIDGES)

Los bridges permiten extender de forma transparente los límites de los segmentos de una LAN, véase figura 2.4. Tienen la importante ventaja de ser transparente a los protocolos de nivel superior de la redes (TCP/IP, Appletalk o IPX), soportan protocolos no enrutables como NetBIOS, son fácilmente de instalar y configurar. Existen versiones con capacidad de unir segmentos geográficamente distantes utilizando las versiones de bridges remotos. En definitiva, permiten una extensión de las LAN sin necesidad de modificar el software instalado.

II.7.2.2 CONMUTADORES (SWITCHES)

Los conmutadores son unos dispositivos de reciente aparición y que amplia la gama de posibilidades existentes para interconectar LAN. Por sus características son más asimilables a un bridge que un Ruteador, ya que operan en el nivel 2 y son transparentes a los protocolos que transportan.

Existen diversos tipos de conmutadores dependiendo del tipo de red que soportan; así, existen conmutadores para tramas. Token Ring, Ethernet y FDDI. A menudo realizan función de backbone soportando los diferentes segmentos LAN ya existentes. Como principal ventaja que presenta su instalación es que protegen la base instalada, pues la mayor parte de los adaptadores pueden seguir siendo utilizados en una configuración en las que se introduce un conmutador.

II.7.2.3 RUTEADORES (ROUTERS)

Encaminan paquetes de información hasta la estación destino utilizando el nivel red del modelo OSI. Los Ruteadores deben ser direccionados explícitamente; las estaciones deben conocer la dirección de los mismos para poder acceder a nodos remotos. Esta es una característica que los diferencia de los bridges, cuyas estaciones conectadas no necesitan conocer las direcciones de los mismos, lo único importante es la dirección de la estación remota con la que quieren hablar.

Los Ruteadores proporcionan servicios más sofisticados que los bridges; pueden seleccionar una ruta basándose en parámetros tales como la latencia de los enlaces, el estado de congestión, la distancia entre nodos, etc., de modo que se pueden aplicar diferentes políticas según los requerimientos específicos de cada aplicación permitiendo unas topologías más complejas y descentralizadas ya que pueden manejar diversos esquemas de direcciones, diferentes velocidades y tamaños de trama. No obstante, todos ejecutan funciones similares:

II.7.2.3.1 ELIGEN EL CAMINO MAS ADECUADO

Mantienen las tablas internas que proporcionan información de los enlaces de la red. Estas tablas son fundamentales, pues en ellas basan la decisión para realizar el ruteo de la información.

II.7.2.3.2 DISPONEN DE MECANISMOS PARA EL CONTROL DE FLUJO

La congestión es algo común cuando dos redes de diferente velocidad están interconectadas, pues la más rápida excede la capacidad de la más lenta. Cuando esto ocurre y es detectado, el Ruteador envía una señal a la estación fuente, indicando congestión e invitándole a reducir la velocidad de transmisión.

II.7.2.3.3 UNEN REDES HETEROGÉNEAS

Los Ruteadores pueden conectar redes de diferente nivel MAC (Token Ring, Ethernet, etc.). Su tarea es la de mapear las direcciones del protocolo de comunicaciones (por ejemplo, IPX) en las direcciones destino de la red utilizada (por ejemplo, Frame relay), siendo esta una de las razones que dificultan las funciones de multicasting pues las WAN suelen ser redes orientadas a la conexión.

II.7.2.4 MODEM ANALOGICO

En la actualidad existen numerosos dispositivos que se pueden conectar a la WAN y a la red LAN doméstica. El primero de ellos es el MODEM. Un MODEM es un dispositivo que permite la transmisión de datos entre una LAN y una WAN sobre una red cableada o inalámbrica. El MODEM convierte las señales recibidas desde la WAN en señales que son distribuidas por toda la red LAN doméstica. Cada método de acceso a Internet de alta velocidad que llegue a la casa debe utilizar un MODEM de algún tipo para convertir la señal.

Un MODEM puede usar una gran variedad de protocolos distintos para convertir señales; sin embargo, los protocolos son específicos según las velocidades particulares de de transmisión de datos. Además de la designación del protocolo, las siguientes características distinguen las distintas capacidades del MODEM:

- **Bit por segundo (bps).** Velocidad a la que el MODEM puede transmitir y recibir datos.
- **Voz y capacidades de fax, además de la transmisión de datos**. Utilizados en ampliaciones de la red doméstica.
- **Compresión de datos**. Para velocidades más rápidas de transferencia de datos.

II.8 TECNOLOGIAS DE REDES WAN

A continuación se describirán las tecnologías WAN más importantes de la actualidad.

II.8.1 PROTOCOLO HDLC

SDLC fue desarrollado por IBM a mediados de la década de los 70's. Este protocolo fue la base para el desarrollo de nuevos protocolos de la capa de enlace de datos, creados para operar en el modo sincrono orientado a bit. De esta manera la ISO modifico el protocolo SDLC para crear el protocolo HDLC. Posteriormente CCITT modifico el protocolo HDLC para crear el procedimiento LAP (Link Access Procedure; Procedimiento de Acceso al Enlace) y posteriormente el LAPB (Link Access Procedure Balanced; Procedimiento de Acceso al Enlace Balanceado). El IEEE modifico el protocolo HDLC para crear el estándar IEEE 802.2.

Cada uno de estos protocolos ha llegado a ser importante para la operación en el ambiente LAN (IEEE 802.2) y en el ambiente WAN (SDLC, HDLC, LAPB).

II.8.1.1 ESTACIONES Y CONFIGURACIONES LOGICAS

Los protocolos orientados a bit reconocen la existencia de cuatro tipos de estaciones lógicas que pueden operar en cualquiera de las tres configuraciones que se mencionan a continuación y se observan en la figura 2.6.

Estación Lógica Primaria. Una estación lógica primaria asume la responsabilidad de organizar el flujo de datos y de recobrar el nivel de enlace en caso de error. Las tramas transmitidas por esta estación son referidas como tramas de control.

Estaciones Lógicas Secundarias. Una estación lógica secundaria no tiene directamente la responsabilidad de control de enlace, en lugar de ello, esta estación responde a los comandos enviados por la estación primaria.

Estación Lógica Balanceada. Una estación lógica balanceada esta diseñada para compartir equitativa y complementariamente las funciones de control de enlace con otra estación balanceada. Una estación balanceada no se identifica ni como estación ni como estación secundaria.

Estación Lógica Configurable. Una estación configurable tiene la capacidad de funcionar en diferente momento y según se requiera (por que puede responder a diferentes grupos de comandos) como estación primaria, estación secundaria o estación balanceada.

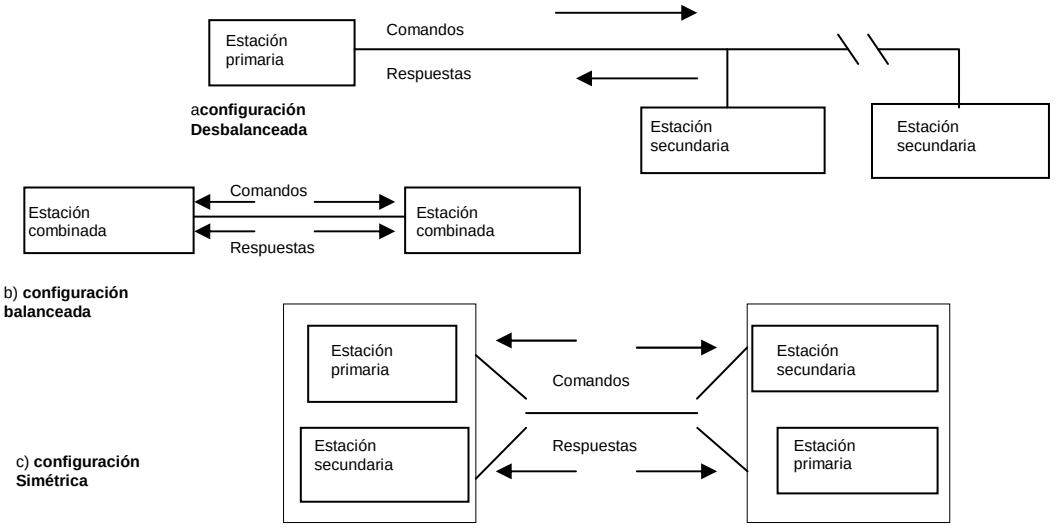


Figura 2.6 MODOS LÓGICOS DE CONFIGURACIÓN.

Configuración Desbalanceada. Una configuración desbalanceada consiste de una estación lógica primaria y una ó más estaciones lógicas secundarias. Esta configuración se considera desbalanceada en el sentido de que la prima de responsabilidad reside en la estación primaria.

Configuración Balanceada. La configuración balanceada consta de dos estaciones balanceadas conectadas por un circuito dedicado o por un circuito punto a punto conmutado. En la configuración balanceada cada terminal tiene igual y complementaria responsabilidad del control del enlace de datos.

Configuración Simétrica. Esta es posible combinar una estación lógica primaria y una estación lógica secundaria en una estación física, para con ello obtener una combinación de dos configuraciones punto a punto desbalanceadas operando de manera independiente.

II.8.1.2 PROCEDIMIENTOS RELACIONADOS CON EL ACCESO AL ENLACE

Un protocolo de control de enlace de datos es un grupo especifico de reglas que gobierna el proceso de intercambio que pueden ser computadoras personales, terminales y conmutadores de paquetes entre otros.

Los protocolos de control de enlace de datos residen en el nivel de Enlace del modelo OSI. Las funciones de un protocolo de control de enlace de datos incluyen la inicialización de un enlace físico, el control de intercambio de datos y la terminación del enlace y, la que seria la función más importante desde el punto de vista del usuario: manejar técnicas de recuperación de información en caso de presentarse alguna condición de mal funcionamiento en la red.

II.8.1.3 MODOS DE TRANSFERENCIA

HDLC comparte los campos del formato de la trama SDLC al igual que SDLC soporta el modo de operación sincronía y "Full Dúplex". La diferencia principal entre estos dos protocolos es que SDLC soporta únicamente un solo modo de transferencia, mientras que HDLC soporta tres. Los tres modos de transferencia que soporta HDLC son:

Modo de Respuesta Normal. Este modo de transferencia es usado por SDLC. En este modo, una estación secundaria no puede comunicarse con una estación primaria hasta que le otorga permiso.

Modo de respuesta Asíncrona. Este modo de transferencia permite a la estación secundaria intercomunicarse con la estación primaria sin esperar permiso de esta.

Modo Asíncrono Balanceado. Este modo de transferencia introduce un nodo combinado. Un nodo combinado puede actuar como una estación primaria o secundaria de la situación.

II.8.1.4 FORMATO DE LA TRAMA HDLC

El formato de la trama HDLC esta representado por la figura 2.7

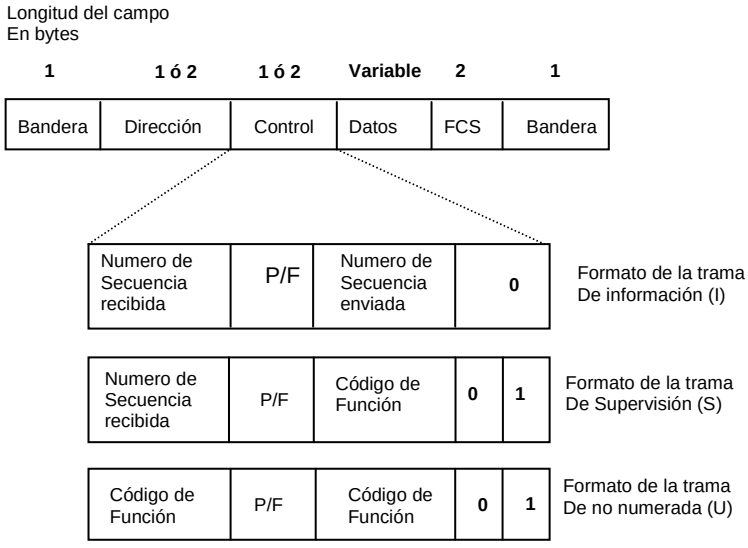


FIGURA 2.7 FORMATO DE LA TRAMA HDLC.

Como se muestra en la figura anterior, la trama HDLC esta delimitada por dos banderas con longitud de un byte cada una. El campo de dirección contiene siempre la dirección de la estación secundaria involucrada en el proceso de comunicación. Puesto

que la estación primaria es la fuente o destino del proceso de comunicación, no se requiere incluir su dirección.

En la figura anterior se muestra que el campo de control puede usar tres diferentes formatos dependiendo del tipo de trama HDLC requerida. Las tres tramas se describen a continuación:

Trama de Información (I). Esta trama transporta información de control relacionada con la operación “Full Dúplex” hacia las capas superiores. Envía y recibe números de secuencia además del bit de poleo, información de control de flujo, chequeo de errores. El número de secuencia se refiere al conteo de tramas enviadas y recibidas a través del canal de la red. Este conteo permite esperar una numeración consecutiva. En la operación “Full Dúplex” el envío y recepción de información se mantiene permanente. La estación primaria usa el bit de poleo (P/F) para decir a la estación secundaria si esta requiere de una respuesta inmediata. La estación secundaria utiliza este bit para decir a la estación primaria si la actual trama es la última respuesta enviada por esta.

Trama de Supervisión (S). Esta trama proporciona información de control. Estas no tienen un campo de información. Las tramas de supervisión solicitan y suspenden la transmisión, reporte de estado y reconocimiento de las tramas de información.

Trama no numerada (U). Esta trama como su nombre lo sugiere, no sigue ninguna secuencia. Esta trama puede tener un campo de información. Las tramas no numeradas son usadas con fines de control. Por ejemplo, en ellas se especifica si el campo de control es uno de dos bytes, inicialización de una estación secundaria y otras funciones similares.

La trama FCS (Frame Check Secuency; Chequeo de Secuencia de Trama) precede al delimitador de la bandera final. Esta trama puede tener un campo de información. Las trama FCS utiliza un algoritmo denominado CRC (Cyclic Redundancy Check; Chequeo de Redundancia Cíclica) cuya función es realizar un cálculo algebraico de cada trama, tanto en el lado de la estación transmisora como el de la estación receptora para posteriormente compáralas y determinar si ha ocurrido algún error en la transmisión. El formato de la trama HDLC es compartida por la trama SDLC.

II.8.2 RDSI (ISDN)

Una tecnología versátil es la Red Digital de Servicios Integrados (Integrated Services Digital Network [ISDN]), generalizada, históricamente importante. Fuel el primer servicio de conexión telefónica completamente digital. El costo es moderado, el ancho de banda máximo es de 128 KBPS para la interfaz de acceso básico (BRI) de menor costo, y sobre los 3 MBPS para la interfaz de acceso principal (PRI). El medio corriente es el cable de cobre de par trenzado.

Es el primer paso para acceder a unos servicios digitales de alta calidad y ya se encuentra plenamente disponible en todo Occidente. Dada la progresiva implantación y los acuerdos de interoperatividad alcanzados en Europa, hacen que este territorio sea especialmente propenso para su desarrollo y progresiva implantación sustituyendo ventajosamente las actuales redes conmutadas de voz y datos.

Las posibilidades de los usuarios múltiples. Desde centralitas PBX hasta Ruteadores.

Desde videotelefónos hasta multiplexores, pasando por una amplia gama de dispositivos como adaptadores, teléfonos digitales, fax, videocámaras, nodos de comunicaciones. Las aplicaciones pueden ser también muy variadas; aplicaciones cliente-servidor, circuitos de back-up, interconexión de LAN, sistemas de televigilancia, telebanco, telecompra, en algunos casos es incluso la única opción si es que necesita una red digital conmutada basada en 64 KBPS.

Algunas ventajas adicionales para los usuarios son las facilidades para reasignar las líneas con total flexibilidad, dada su característica de conexión universal, pudiendo variar su uso según las necesidades de cada momento, evitando los tramites necesarios para dar continuas altas o bajas de determinados servicios con la consiguiente perdida de tiempo y dinero que ello significa.

II.8.3 ATM (B-ISDN)

Es, sin duda, la estrella que más brilla en el firmamento de las comunicaciones. La historia de ATM es tan reciente que remontarse mas allá de 1988 significa desempolvar archivos de ciertos experimentos realizados en los años setenta y ochenta que no sobrepasaron el ámbito del laboratorio. Sin embargo, es sorprendente la popularidad adquirida, sobre todo teniendo en cuenta que apenas existen unos pocos servicios operativos.

En su origen guarda ciertos paralelismos con el Frame Relay al haber nacido también en el seno del RDSI, esta vez en la banda ancha, y haberse constituido en tecnología independiente.

Bajo una concepción celular de las comunicaciones una red ATM es capaz de transferir cualquier tipo de información entre dos puntos sin modificar su naturaleza íntima. Ya sea voz, imagen o datos, el ATM cose un traje a la medida de las necesidades de cada tipo de tráfico. Su implantación se va a verificar en todo tipo de entornos tanto locales como extensos aunque estos últimos serán una realidad situada en el horizonte del año 2000.

II.8.4 FRAME RELAY

Apareció como un método para optimizar el uso de los canales de la RDSI. La posterior evolución le llevo a constituirse en un servicio independiente que podía ser soportado por redes de diversas tecnologías y, paradójicamente, muy pocas redes RDSI han llegado a implementarlo.

El Frame Relay (FRL), fue la primera red de área extensa en adaptar su arquitectura a las nuevas tecnologías de transmisión y los avances en informática, vinculando a los dispositivos de los usuarios en el proceso de transmisión al hacerlos responsables del control de flujo y control de errores. Esta estrategia, posteriormente asumida por la redes ATM, convierte al FRL en la solución más eficiente para la transmisión de datos, y la puerta más segura para garantizar una migración suave hacia

la banda ancha, existiendo ya estándares para su soporte e interconexión con redes B-ISDN.

El FRL es apropiado para la transmisión de datos a velocidades inferiores a 2 MBPS posicionándose en un segmento actualmente ocupado por las redes X.25 y los enlaces permanentes.

II.8.5 REDES INALAMBRICAS

Seguramente la segunda mitad de la década de los noventa va a estar marcada por la investigación y el desarrollo de las comunicaciones inalámbricas. Ya esta en funcionamiento en Europa la segunda generación de redes inalámbricas cuyos máximos representantes son el GSM (Global System for Mobile communications) para áreas extensas y el DECT (Digital European Cordeless Telecommunications) para entornos departamentales. Ambos vienen a sustituir a sus precursoras analógicas que ya encontraban próximas a la saturación. Una tercera generación de redes inalámbricas, conocidas por el nombre genérico de UMTS (Universal Mobile Telecommunications System), esta dispuesta para saltar a la arena de las comunicaciones hacia el año 2000 con objetivos tan ambiciosos como la integración de estaciones móviles con la RDSI de Banda Ancha con soporte global de voz, datos y video. Los entornos locales no son ajenos a este nuevo mercado emergente y ya desde principios de los años noventa se dispone de redes locales inalámbricas o WLAN (Wíreless LAN) que progresivamente van incrementando sus prestaciones hasta acercarse a las de sus equivalentes.

II.8.6 PPP

Como el acceso remoto es de tanta importancia, existen muchos protocolos de seguridad y control. El Grupo para tareas de ingeniería de Internet desarrollo el Protocolo Punto a Punto, PPP (Point to Point Protocol) como medio primario de autentificación y de control de sesiones de acceso remoto. PPP es un protocolo de enlace de Datos diseñado específicamente para acceso telefónico por MODEM, RDSI y otros circuitos digitales similares.

PPP encapsula los paquetes IP o IPX en paquetes especializados de Protocolo de control de red. El protocolo proporciona protección por contraseña utilizando PAP, Protocolo de autentificación de contraseña (Password Authentication Protocol) y CHAP, protocolo de autentificación y acuerdo mutuo (Challenge Handshake Authentication Protocol). Si bien PPP, PAP y CHAP dan mucho respeto, la buena noticia es que el software para realizar estas funciones está integrado en Windows y está disponible para clientes Macintosh y UNIX. Tras la autentificación propia en el sistema operativo de escritorio, las prestaciones del sistema operativo autentifican para el servidor de acceso remoto automáticamente.

Sin embargo, para alcanzar el grado máximo de seguridad es posible llamar a un servidor de autentificación para comprobar que los que llaman son efectivamente quienes alegan ser y para elaborar una lista de las personas que han llamado, cuando lo han hecho y durante mucho tiempo. Livingston Enterprises of Pleasanton, CA. Cuenta con mucho soporte para el protocolo RADIUS, Servicios de usuario de llamada de acceso remoto (Remote Access Dial-In User Service), que combina la autentificación y la

autorización con funciones de contabilidad. Se puede acceder directamente a los binarios y códigos fuente de UNIX desde Livingston. RADIUS es soportado por un amplio espectro de dispositivos, como sistemas de acceso remoto y cortafuegos de Cisco Systems, Ascend Communications, Bay Networks, Shiva Corp., U.S. Robotics y Raptor Systems.

PPP ha sido la referencia obligada de muchos protocolos de acceso remoto. El protocolo PPP multienlace (abreviado MP, MPPP o MLPPP) puentea dos o más puertos serie o canales B RDSI para una operación a mayor velocidad. Por ejemplo, BRI, la interfaz de velocidad básica (Basic Rate Service) de RDSI, alcanza los 128 KBPS con PPP multienlace. MP es un estándar que forma parte de Windows y del popular software de comunicaciones para computadoras Macintosh y UNIX.

II.8.7 SONET/SDH

SONET (***Synchronous Optical Network***, Red Óptica Síncrona) y SDH (***Synchronous Digital Hierarchy***, Jerarquía Digital Síncrona) en terminología UIT-T, es un estándar internacional, desarrollado por el Working Group T1X1 de ANSI para líneas de telecomunicación de alta velocidad sobre fibra óptica (desde 51,84 MBPS a 2,488 Gbps). SONET es su nombre en EE.UU. y SDH es su nombre europeo. Son normas que definen señales ópticas estandarizadas, una estructura de trama síncrona para el tráfico digital multiplexado, y los procedimientos de operación para permitir la interconexión de terminales mediante fibras ópticas, especificando para ello el tipo monomodo.

Para entender el funcionamiento de SDH es conveniente hacer una introducción previa a PDH ***(Plesiochronous Digital Hierachy).***

II.8.7.1 PDH

PDH surgió como una tecnología basada en el transporte de canales digitales sobre un mismo enlace. Los canales a multiplexar denominados módulos de transporte o contenedores virtuales se unen formando tramas o módulos de nivel superior a velocidades estandarizadas 2 MBPS, 8 MBPS, 34 MBPS, 140 MBPS y 565 MBPS. Es una jerarquía de concepción sencilla, sin embargo contiene algunas complicaciones, que han llevado al desarrollo de otras jerarquías más flexibles a partir del nivel jerárquico más bajo de PDH (2 MBPS) equivalente a una trama MIC de RDSI (30B+D).

La principal problemática de la jerarquía PDH es la falta de sincronismo entre equipos. Cuando se quiere pasar a un nivel superior jerárquico se combinan señales provenientes de distintos equipos. Cada equipo puede tener alguna pequeña diferencia en la tasa de bit. Es por ello necesario ajustar los canales entrantes a una misma tasa de bit, para lo que se añaden bits de relleno. Sólo cuando las tasas de bit son iguales puede procederse a una multiplexación bit a bit como se define en PDH. El demultiplexor debe posteriormente reconocer los bits de relleno y eliminarlos de la señal. Este modo de operación recibe el nombre de plesiócrono, que en griego significa casi síncrono.

Los problemas de sincronización ocurren a todos los niveles de la jerarquía, por lo que este proceso ha de ser repetido en cada etapa de multiplexación. Este hecho genera un gran problema de falta de flexibilidad en una red con diversos niveles jerárquicos. Si a un punto de la red se le quieren añadir canales de 64 KBPS, y el enlace existente es de 8

MBPS o superior, debe pasarse por todas las etapas de demultiplexación hasta acceder a un canal de 2 MBPS y luego volver a multiplexar todas las señales de nuevo.

La falta de flexibilidad dificulta la provisión de nuevos servicios en cualquier punto de la red. Adicionalmente se requiere siempre el equipamiento correspondiente a todas las jerarquías comprendidas entre el canal de acceso y la velocidad del enlace, lo que encarece en extremo los equipos. Otro problema adicional de los sistemas basados en PDH es la insuficiente capacidad de gestión de red a nivel de tramas. La multiplexación bit a bit para pasar a un nivel de jerarquía superior y con bits de relleno convierte en tarea muy compleja seguir un canal de tráfico a través de la red.

II.8.7.2 JERARQUÍA DIGITAL SÍNCRONA (SDH)

Una red síncrona es capaz de incrementar sensiblemente el ancho de banda disponible y reducir el número de equipos de red sobre el mismo soporte físico que otro tipo de tecnologías. Además la posibilidad de gestión de red dota a ésta de mayor flexibilidad.

El desarrollo de equipos de transmisión síncronos se ha visto reforzada por su capacidad de interoperar con los sistemas plesiócronos (PDH) existentes destinados principalmente al transporte de telefonía vocal. SDH define una estructura que permite combinar señales plesiócronas y encapsularlas en una señal SDH estándar. Las facilidades de gestión avanzada que incorpora una red basada en SDH permiten un control de las redes de transmisión. La restauración de la red y las facilidades de reconfiguración mejoran la incorporación y prestación de nuevos servicios.

Este estándar de transmisión síncrona se recoge en las recomendaciones G.707, G.708, y G.709 del ITU (Unión Internacional de Telecomunicaciones) bajo el epígrafe SDH (Synchronous Digital Hierachy).

Las recomendaciones del ITU definen un número de velocidades de transmisión básicas en SDH:

- 155 MBPS, STM - 1 (“Synchronous Transport Module”)
- 622 MBPS, STM - 4
- 2,4 Gbps, STM - 16
- 10 Gbps, STM - 64 (en desarrollo)

Estas recomendaciones definen también una estructura de multiplexación, donde una señal STM-1 puede portar señales de menor tráfico, permitiendo el transporte de señales PDH entre 1,5 MBPS y 140 MBPS.

SDH define un número de contenedores, cada uno de ellos correspondiente a una velocidad de transmisión PDH. La información de la señal PDH se introduce en su contenedor correspondiente y se añade una cabecera al contenedor, que permite monitorizar estas señales. Cabecera y contenedor forman un denominado contenedor virtual. En una red síncrona todo el equipamiento se sincroniza con un mismo reloj de red. Variaciones de retardo asociadas a un enlace de transmisión inciden en una posición

variable de los contenedores virtuales, lo que se resuelve asociándoles un puntero en la trama STM -1.

Las redes de transmisión de telecomunicaciones que se desarrollan e implantan en la actualidad se basan principalmente en soluciones técnicas de jerarquía digital síncrona (SDH). Tanto las operadoras o PTT's en sus redes públicas, como empresas y organismos oficiales en sus redes privadas, están implantando SDH, que permite una integración de todos los servicios de voz, datos y vídeo a nivel de transmisión, lo que facilita la gestión de las redes y las beneficia de los niveles de protección y seguridad intrínsecos a SDH. Otra ventaja adicional de esta tecnología es que sobre ella se pueden desarrollar otras soluciones del tipo FRAME RELAY o ATM.

En conclusión cabe decir que actualmente SDH es la alternativa tecnológica de más futuro para la transmisión en las redes de comunicaciones. La tecnología PDH juega un papel todavía importante en la transmisión, al permitir segregar el tráfico en canales de comunicación de baja velocidad (menores de 64 KBPS). Es por ello que los equipos PDH se integran en el denominado acceso de usuario a las redes de transmisión en su jerarquía más baja (PDH a 2 MBPS). No obstante el resto de niveles de jerarquía superior en PDH (8, 34, 140 MBPS) están siendo desplazados por equipos de tecnología SDH, compatibles con PDH, pero más versátiles y económicos

II.8.8 X.25

X.25 fue el primer protocolo estándar de red de datos pública. Se definió por primera vez en 1976 por el CCITT (Comité Consultatif International Télégraphique and Téléphonique). Aunque el protocolo ha sido revisado múltiples veces (la última en 1993) ya se ha quedado algo anticuado y no es en la actualidad un servicio interesante en general, debido a su baja eficiencia y velocidad; normalmente no supera los 64 Kb/s, aunque se pueden contratar conexiones de hasta 2.048 Kb/s. A pesar de estas desventajas conviene conocer los aspectos básicos de X.25 pues aun existe una gran cantidad de usuarios de este tipo de redes. Además, en el protocolo X.25 se definieron por primera vez muchos de los conceptos en que se basa Frame Relay y ATM, que podemos considerar en cierto sentido como el X.25 versión 2 y versión 3, respectivamente. El conjunto de estándares que definen X.25 ha sido adoptado como parte del modelo OSI para los tres primeros niveles.

X.25 es un servicio fiable orientado a conexión; los paquetes llegan en el mismo orden con que han salido. Una vez establecido un circuito entre dos NSAPs la información se transfiere en paquetes que pueden ser de hasta 128 bytes (aunque en muchas redes se permiten tamaños de hasta 4 KBytes). En la red los paquetes son transferidos de cada conmutador al siguiente por la técnica de almacenamiento y reenvío y sólo son borrados cuando se recibe la notificación de recepción; es necesario que se produzca una confirmación de la correcta recepción del paquete en cada salto que éste realiza en la red. Un mismo NSAP puede tener establecidos varios VCs (PVCs y/o SVCs) hacia los mismos o diferentes destinos.

A nivel físico se definen en X.25 dos interfaces, la X.21 cuando se usa señalización digital (cosa poco habitual) y la X.21bis (un subconjunto de la EIA-232D/V.24) cuando es analógica.

A nivel de enlace se utiliza un protocolo llamado LAP-B (Link Access Procedure-Balanced) que es una versión modificada del estándar ISO HDLC (High-level Data Link Control), que vio antes.

El rendimiento que se obtiene de un VC X.25 depende de muchos factores: velocidad de los accesos físicos implicados, número de VC simultáneos, tráfico en cada uno de ellos, carga de la red, infraestructura, etc.

Los protocolos X.25 se diseñaron pensando en los medios de transmisión de los años setenta, líneas de baja velocidad con tasa de errores elevada. El objetivo era aprovechar lo mejor posible las lentas líneas de transmisión existentes, aún a costa de hacer un protocolo de proceso pesado. Por si esto fuera poco, las redes X.25 casi siempre se utilizan para ***encapsular*** tráfico correspondiente a otros protocolos, por ejemplo TCP/IP, SNA o DECNET (podríamos decir que los paquetes de estos protocolos viajan "disfrazados" en paquetes X.25); cuando se encapsula un protocolo como TCP/IP en X.25 se realizan de forma redundante las tareas de la capa de red, con lo que el resultado es aún mas ineficiente. Para resolver este tipo de problemas a partir de 1990 se empezaron a crear redes basadas en Frame Relay.

II.9 POR QUE RUTEADORES EN REDES WAN

Una breve explicación por que los Ruteadores son centro de una red WAN, ya que estos dispositivos fueron creados para realizar la conexión de redes LAN con una Red WAN como se describe a continuación.

II.9.1 LA FUNCION DEL RUTEADOR EN UNA WAN

Los Ruteador son útiles para dividir las LAN en dominios de difusión separados, y se debe utilizar al conectar estas LAN sobre una área amplia (véase la figura 2.8). Los Ruteadores tienen interfaces LAN y WAN. Las tecnologías WAN se emplean frecuentemente para conectar Ruteadores. Los Ruteadores se comunican entre sí sobre conexiones WAN, y conectan redes dentro de sistemas autónomos, así como el backbone de Internet. Los Ruteadores operan en la Capa 3 del modelo OSI, tomando decisiones basadas en direcciones de red (en Internet utilizando el Protocolo Internet, o IP).

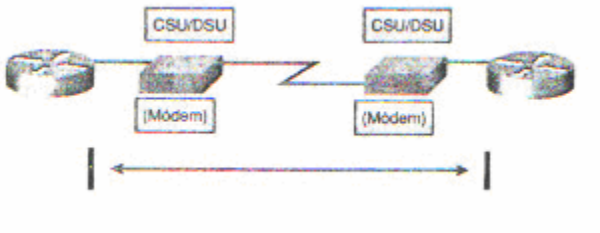


FIGURA 2.8 FUNCION DE UN RUTEADOR

Las dos funciones principales de los Ruteadores son la determinación de las mejores rutas para los paquetes de datos entrantes y la conmutación de paquetes a la interfaz saliente correcta. Los Ruteadores lo llevan a cabo, construyendo tablas de

enrutamiento e intercambiando la información de red que estas contienen con otros Ruteadores. Se pueden configurar tablas de enrutamiento, pero generalmente se mantienen dinámicamente utilizando un protocolo de enrutamiento que intercambia información sobre la topología de la red (ruta) con otros Ruteadores.

Por ejemplo, si quiere que cualquier computadora (X) pueda comunicarse con cualquier lugar de la Tierra, y con cualquier otra computadora (Z) en cualquier lugar del sistema Luna-Tierra, debe incluir un elemento de enrutamiento para el flujo de información y rutas redundantes para la fiabilidad. Se pueden trazar muchas decisiones y tecnologías de diseño de redes con este deseo para las computadoras X, Y y Z puedan comunicarse ó intercomunicarse. Cualquier internetworking también incluye normalmente lo siguiente:

- Direccionamiento consistente extremo a extremo.
- Direcciones que representan topologías de red.
- Selección de la mejor ruta.
- Enrutamiento dinámico.
- Conmutación/envío.

CAPITULO III EL PROTOCOLO TCP/IP

III.1 TCP/IP

Uno de los principales protocolos que hoy en día revoluciona la vida de las comunicaciones es el TCP/IP, teniendo un buen rendimiento en las redes por la fiabilidad de la información. Mientras mas grandes las redes se deben crean subredes que definan a un grupo de computadoras y pueda ser mas rápido la identificación de cada equipo, para ello se ha desarrollado un cálculo para esto.

III.2 INTRODUCCIÓN DE TCP Y UDP.

TCP es un protocolo orientado a conexión, que proporcionan una extensa verificación de error, y control, de flujo y UDP es un protocolo no orientado a conexión con mucho menos chequeo de error sofisticado. Se podría decir que TCP esta construido para fiabilidad y UDP para velocidad. La aplicación es que podrían soportan sesiones interactivas, tal como Telnet y FTP, tienden a utilizar TCP. Las aplicaciones que hacen su propia verificación de error o que no necesiten de mucha verificación de error utilizan UDP. Un software diseñado para desarrollo de una aplicación de red puede usar TCP o UDP como un protocolo de transporte. El simple control del mecanismo UDP, debería no ser necesariamente considerando a las limitantes.

Por otro lado, la calidad que menos se asegura, no necesariamente significa menos calidad. Las verificaciones extra y los controles provistos por TCP son enteramente innecesarios, para muchas aplicaciones. En estos casos donde la verificación de error y el flujo de control son necesarios, algunos desarrollos prefieren proveer aquellas características de control en las aplicaciones de sí mismos – donde ellos pueden ser controlados para necesidades específicas – y usar el angosto transporte UDP para acceder a la red. Los servicios basados en UDP como el Remote Procedure Call (RPC) de TCP/IP pueden soportar avanzadas y sofisticadas aplicaciones, pero estas aplicaciones deben tomar más responsabilidad en el chequeo de error y control de flujo de tareas que si ellos alcanzaron el montón por TCP

III.2.1 UDP: PROTOCOLO DE TRANSPORTE NO ORIENTADO A CONEXIÓN.

UDP es mucho más simple que TCP. Aquí hay, sin embargo, un par de observaciones acerca de UDP.

Primero, aunque UDP en algunas veces descrito como que no tiene la capacidad de verificación de error. De hecho, UDP es capaz de un rendimiento de verificación de error rudimentario. Este es el mejor para caracterizar a UDP como que tiene la capacidad para la limitada verificación de error. El datagrama UDP incluye un valor en la suma de la verificación que la computadora recibe para poder usarlo para probar la integridad de los datos. El datagrama UDP, incluye una cabecera pseudo que abarca la dirección destino para el datagrama, así proporcionando un medio de comprobación para datagramas mal dirigidos. También si el módulo receptor de UDP recibe un datagrama directo para un puerto UDP inactivo o indefinido, este regresa un mensaje ICM notificando a la computadora fuente que el puerto es inalcanzable.

Segundo, el UDP no ofrece el resecuenciamiento de datos provistos por TCP. El resecuenciamiento es más significativo en una red grande, tal como Internet, donde los segmentos de datos deben tomar diferentes rutas y experiencia significativa de retrasos en los buffers de los Ruteadores. En las redes locales, la carencia de una característica de resecuenciamiento en conductos típicamente UDP para una recepción no fiable.

III.2.1.1 PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)

El principal propósito del protocolo UDP es exponer datagramas para la capa de aplicación. Tal como el protocolo UDP por sí mismo, es muy pequeño, y sin embargo, emplea una simple estructura de cabecera. El RFC que describe el protocolo, RFC 768, es solamente 3 páginas en longitud. UDP no retransmite datagramas perdidos ó corruptos, la secuencia de los datagramas recibidos fuera de orden, elimina los datagramas duplicados, da un acuse de recibo de datagramas o lo establece, o conexiones terminadas. UDP es primordialmente un mecanismo para programas de aplicación para enviar o recibir datagramas sin encabezado de una conexión de TCP.

III.3 INTRODUCCION AL PROTOCOLO TCP/IP

Los mensajes subyacentes que se transfieren entre su computadora y los diversos servidores con los que se puede comunicar, tal como los servidores Web y el correo electrónico. Este conocimiento, a su vez, nos proporcionara un mejor entendimiento de los mensajes de error con los que se pueden encontrar cuando proporcione sus propios servicios TCP/IP. Si procede del mundo de la programación, puede incluso intentar escribir su propio software de cliente para alguno de estos protocolos.

Será difícil abordar todos los protocolos TCP/IP disponibles que se pueden usar en la redes, pero si podemos ver algo sobre los más comunes. Estos protocolos, a su vez, pueden ampliarse mediante otros protocolos más comunes. Estos protocolos, a su vez, pueden ampliarse otros protocolos. Por ejemplo, los protocolos de correo electrónico se pueden ampliar con una autenticación de seguridad basada en TCP/IP. Una ampliación de un protocolo de servidor Web puede permitir a los exploradores cliente cargar archivos completos en un servidor. Hoy en día, existe un protocolo en uso denominado RPC (Remote Procedure Calls) Llamadas a Procedimientos Remotos, que permiten a los programadores ejecutar partes de sus programas en diferentes computadoras, permitiendo a una red trabajar coordinadamente para procesar la información más rápidamente.

III.3.1 TCP: PROTOCOLO DE TRANSPORTE ORIENTADO A CONEXIÓN.

Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados a la red Internet. Es un protocolo orientado a conexión ya que utiliza un método más sofisticado y una extensiva verificación de error, y control, de flujo. Este nombre viene dado por los dos protocolos estrella de esta familia:

El Protocolo TCP (Protocolo de Control de Transmisión), funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

El Protocolo IP (Protocolo Internet), funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras computadoras. Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores, además de los que proporciona los protocolos TCP e IP.

TCP/IP se basa en software utilizado en redes. Aunque el nombre TCP/IP implica que el ámbito total del producto es la combinación de dos protocolos: Protocolo de Control de Transmisión y Protocolo Internet. El término TCP/IP no es una entidad única que combina dos protocolos, sino un conjunto de programas de software más grande que proporciona servicios de red, como registro de entrada remota, transferencia de archivo remoto y correo electrónico, etc., siendo TCP/IP un método para transferir información de una computadora a otra. Además TCP/IP maneja los errores en la transmisión, administra el enrutamiento y entrega de los datos, así como controlar la transmisión real mediante el uso de señales de estado predeterminado.

III.3.2 LA ESTRUCTURA DE TCP/IP

El modelo de comunicaciones de OSI esta definido por siete capas a diferencia del modelo TCP que define cuatro.

1. Capa de Aplicación.
2. Capa de Transporte.
3. Capa de Internet.
4. Capa de Red.

A medida que obtenga más información acerca de las capas, tenga en cuenta el propósito original de Internet. El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la ***capa de Internet*** y la capa de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. No confunda las capas de los dos modelos, porque la capa de aplicación tiene diferentes funciones en cada modelo.

III.3.3 CAPA DE APLICACIÓN

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa.

III.3.4 CAPA DE TRANSPORTE

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de

error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a la conexión no significa que el circuito exista entre los computadores que se están comunicando (esto sería una conmutación de circuito). Significa que los segmentos de la Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes, como ya se había visto anteriormente.

III.3.5 CAPA DE INTERNET

El propósito de la ***capa de Internet*** es enviar paquetes origen desde cualquier red en Internetwork de redes y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando envía una carta por correo, usted no sabe cómo llega a destino (existen varias rutas posibles); lo que le interesa es que la carta llegue.

III.3.6 CAPA DE RED

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN y todos los detalles de la capa física y de enlace de datos del modelo OSI. El diagrama que aparece en la siguiente figura 3.1 se denomina ***gráfico de protocolo***. Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP. En la capa de aplicación, aparecen distintas tareas de red que probablemente usted no reconozca, pero como usuario de Internet, probablemente use todos los días. Estas aplicaciones incluyen las siguientes:

- ***FTP*** : File Transfer Protocol (Protocolo de transporte de archivos)
- ***HTTP***: Hypertext Transfer protocol (Protocolo de transferencia de hipertexto)
- ***SMTP***: Simple Mail transport protocol (Protocolo de transporte de correo simple)
- ***DNS***: Domain Name Service (Servicio de nombre de dominio)
- ***TFTP***:Trival File transport protocol(Protocolo de transporte de archivo trivial)

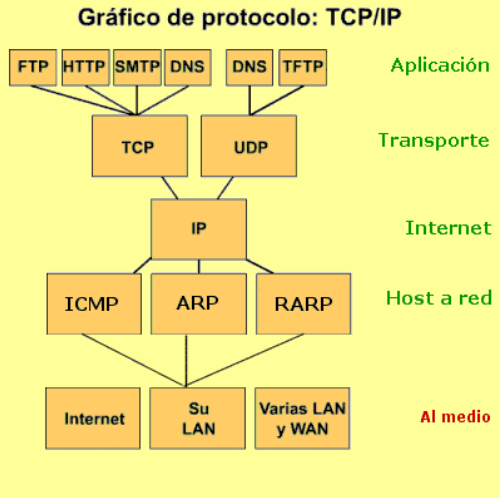


FIGURA 3.1 GRAFICO DE PROTOLOCOS

El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los diseñadores de software. La capa de transporte involucra dos protocolos: el protocolo de control de transmisión (TCP) y el ***protocolo de datagrama (UDP)***. La capa inferior, la capa de red, se relaciona con la tecnología LAN o WAN que se utiliza en particular. En el modelo TCP/IP existe solamente un protocolo de red: el protocolo Internet, o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. ***IP*** sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

Si compara el modelo OSI y el modelo TCP/IP, observará que ambos presentan similitudes y diferencias. Los ejemplos incluyen:

Similitudes

- Ambos se dividen en capas
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos
- Ambos tienen capas de transporte y de red similares
- Se supone que la tecnología es de conmutación de paquetes (no de conmutación de circuitos)
- Los profesionales de networking deben conocer ambos

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- Los protocolos TCP/IP son los estándares entorno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, no se crean redes a partir de protocolos

específicos relacionados con OSI, aunque todo el mundo utiliza el modelo OSI como guía.

III.4 ARQUITECTURA TCP/IP

La figura 3.2 muestra una comparación de los modelos TCP/IP y OSI, donde indican las diferencias entre las capas que componen a cada modelo.

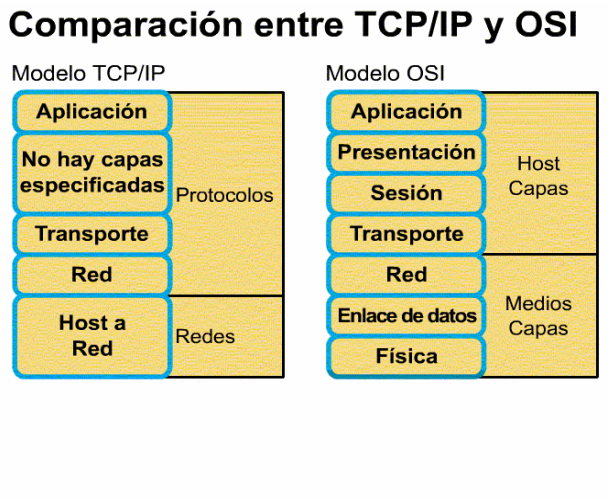


FIGURA 3.2 COMPARACION ENTRE TCP/IP Y OSI

El modelo básico en Internet es el modelo Cliente/Servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (International Standard Organization) para la interconexión de sistemas abiertos (OSI). (Ver Fig. 3.3).

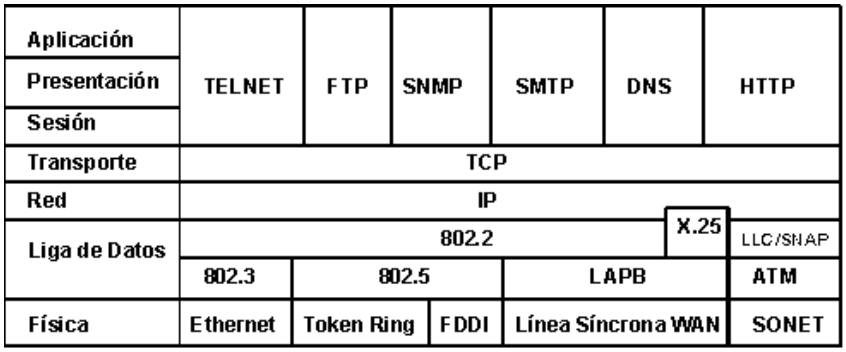


FIGURA 3.3 RELACIÓN DEL MODELO TCP/IP CON EL MODELO OSI

No hace mucho tiempo, ATM era visto por todos los operadores de telecomunicaciones como la única tecnología integradora de todo tipo de tráficos: datos, vídeo y por supuesto voz. Sin embargo, ATM ha visto como su desarrollo e implantación han ido más lentos de lo esperado y su extensión sobre todo al entorno LAN está en duda. A la vez, IP a surgido como un protocolo de LAN de transmisión de datos, el cual ha ido extendiéndose hacia las redes MAN y las WAN de un modo imparable debido en parte a su sencillez, su bajo costo en equipos y por su transporte tanto a través de redes IP como de Internet.

El protocolo IP ha tenido su origen en transmisión de datos y no está demasiado adaptado a la transmisión de datos e imágenes. La tecnología de transmisión de paquetes, en la que está basada IP, ofrece tamaño de celdas variable, que en comparación con tecnologías de tamaño de celda fija como ATM, introduce ineficiencias y necesidad de procesos extras. Además IP es un protocolo que solamente ofrece un tipo de calidad de servicio (QoS) basado en proporcionar el mejor rendimiento posible en el enlace disponible.

III.4.1 CONEXIONES

Una conexión son dos pares: dirección ***IP y puerto***. No puede haber dos conexiones iguales en un mismo instante en toda la Red. Aunque bien es posible que un mismo ordenador tenga dos conexiones distintas y simultáneas utilizando un mismo puerto. El protocolo TCP utiliza el concepto de conexión para identificar las transmisiones. En el siguiente ejemplo se han creado tres conexiones. Las dos primeras son al mismo servidor Web (puerto 80) y la tercera a un servidor de FTP (puerto 21). La figura 3.4 muestra la conexión entre dos hosts.

Host 1	Host 2
194.35.133.5:1256	135.22.8.165:80
184.42.15.16:1305	135.22.8.165:80
184.42.15.16:1323	135.22.10.15:21

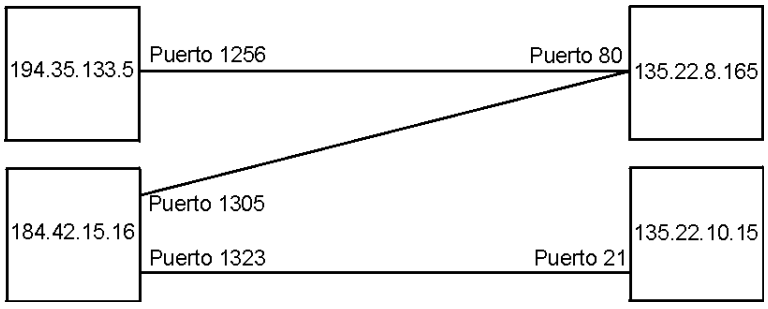


FIGURA 3.4 CONEXIÓN ENTRE DOS HOSTS.

Para que se pueda crear una conexión, el extremo del servidor debe hacer una ***apertura pasiva*** del puerto (escuchar su puerto y quedar a la espera de conexiones) y el

cliente, una ***apertura activa*** en el puerto del servidor (conectarse con el puerto de un determinado servidor).

Nota: El comando NetStat muestra las conexiones abiertas en un ordenador, así como estadísticas de los distintos protocolos de Internet.

III.4.1.1 ESTABLECIMIENTO DE UNA CONEXIÓN

Antes de transmitir cualquier información utilizando el protocolo TCP es necesario abrir una conexión. Un extremo hace una ***apertura pasiva*** y el otro, una ***apertura activa***. El mecanismo utilizado para establecer una conexión consta de ***tres vías***. La figura 3.5 muestra la apertura de conexión.

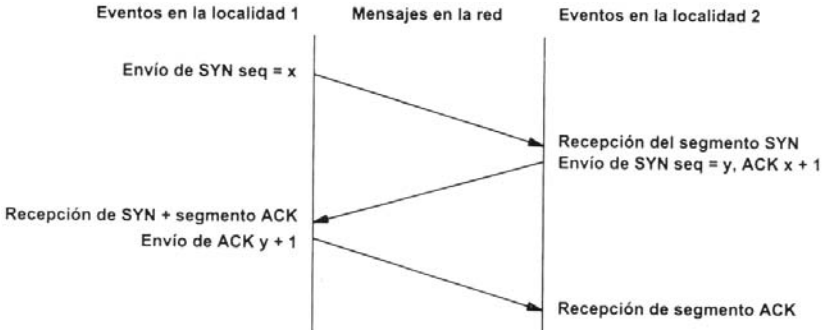


FIGURA 3.5 APERTURA DE UNA CONEXIÓN TCP.

1. La computadora que quiere iniciar la conexión hace una apertura activa enviando al otro extremo un mensaje que tenga el bit SYN activado. Le informa además del primer número de secuencia que utilizará para enviar sus mensajes.
2. La computadora receptora (un servidor generalmente) recibe el segmento con el bit SYN activado y devuelve la correspondiente confirmación. Si desea abrir la conexión, activa el bit SYN del segmento e informa de su primer número de secuencia. Deja abierta la conexión por su extremo.
3. La primera computadora recibe el segmento y envía su confirmación. A partir de este momento puede enviar datos al otro extremo. Abre la conexión por su extremo.
4. La computadora receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión. A partir de este momento puede enviar ella también datos. La conexión ha quedado abierta en los dos sentidos.

Observamos que son necesarios 3 segmentos para que ambas computadoras abran sus conexiones y sepan que la otra también está preparada.

Números de secuencia. — Se utilizan números de secuencia distintos para cada sentido de la comunicación. Como hemos visto el primer número para cada sentido se acuerda al establecer la comunicación. Cada extremo se inventa un número aleatorio y envía éste como inicio de secuencia. Observamos que los números de secuencia no comienzan entonces en el cero. ¿Por qué se procede así? Uno de los motivos es para evitar conflictos: supongamos que la conexión en un ordenador se interrumpe nada más empezar y se crea una nueva. Si ambas han empezado en el cero es posible que el

receptor entienda que la segunda conexión es una continuación de la primera (si utilizan los mismos puertos).

III.4.1.2 CIERRE DE UNA CONEXIÓN

Cuando una aplicación ya no tiene más datos que transferir, el procedimiento normal es cerrar la conexión utilizando una variación del mecanismo de 3 vías explicado anteriormente. La figura 3.6 muestra el cierre de una conexión.

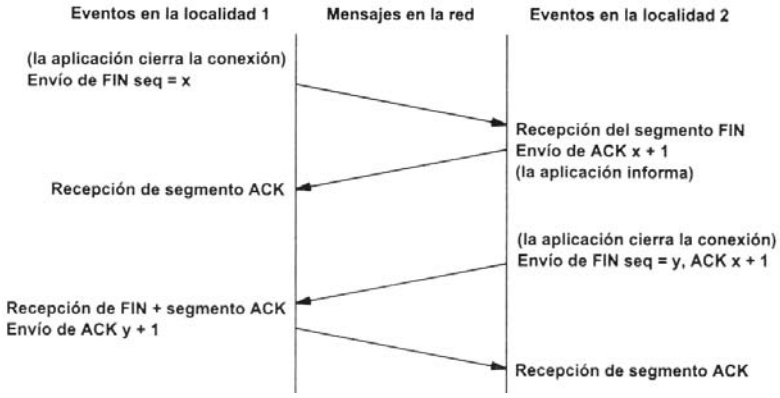


FIGURA 3.6 CIERRE DE UNA CONEXIÓN TCP.

El mecanismo de cierre es algo más complicado que el de establecimiento de conexión debido a que las conexiones son full-dúplex y es necesario cerrar cada uno de los dos sentidos de forma independiente.

1. La computadora que ya no tiene más datos que transferir, envía un segmento con el bit FIN activado y cierra el sentido de envío. Sin embargo, el sentido de recepción de la conexión sigue todavía abierto.
2. La computadora receptora recibe el segmento con el bit FIN activado y devuelve la correspondiente confirmación. Pero no cierra inmediatamente el otro sentido de la conexión sino que informa a la aplicación de la petición de cierre. Aquí se produce un lapso de tiempo hasta que la aplicación decide cerrar el otro sentido de la conexión.
3. La primera computadora recibe el segmento ACK.
4. Cuando la computadora receptora toma la decisión de cerrar el otro sentido de la comunicación, envía un segmento con el bit FIN activado y cierra la conexión.
5. La primera computadora recibe el segmento FIN y envía el correspondiente ACK. Observemos que aunque haya cerrado su sentido de la conexión sigue devolviendo las confirmaciones.
6. La computadora receptora recibe el segmento ACK.

III.5 DIRECCIONES IP

Una de los temas importantes de TCP/IP, es saber como simplifica el proceso de direccionamiento para la búsqueda de computadoras en la red. De acuerdo a los análisis complejos de las redes, el hardware utilizado y la dirección de red definida, nos lleva a

pensar sobre el método que realiza para la localización de cada una de las computadora, por ello describamos el panorama general que se recurrió hasta establecer la solución.

En primer lugar, una computadora emisora no puede conocer cual es la dirección hardware de una computadora remota, ni tampoco sabrán cual es la información debe pasar a través de sí para alcanzar su destino. Para que la dirección hardware se pudiera utilizar como dirección definitiva. Las pasarelas tendrían que conocer en que lugar, geográficamente hablando, se encuentran las distintas direcciones. Debido a que la dirección hardware le asignan los fabricantes y estos no disponen de ningún método para controlar el lugar en que se instalará o venderá su producto, es absolutamente imposible averiguar la ubicación física de un determinado dispositivo de red.

En otro esquema, las pasarelas sabrían ahora como enviar paquetes IP hacia sus destinos, basándose en la dirección IP. Sin embargo, una vez que el paquete alcance la red local, existiría un pequeño problema. Cada máquina debería tener implementada su dirección IP en el nivel de alcance de datos, para reconocer los paquetes destinados a ella. Considere que ocurriría en este sistema si dos computadoras distintas tuvieran la misma dirección IP en la red. Ambas computadoras recibirían y procesarían la información a medida que llegara (ver figura 3.7).

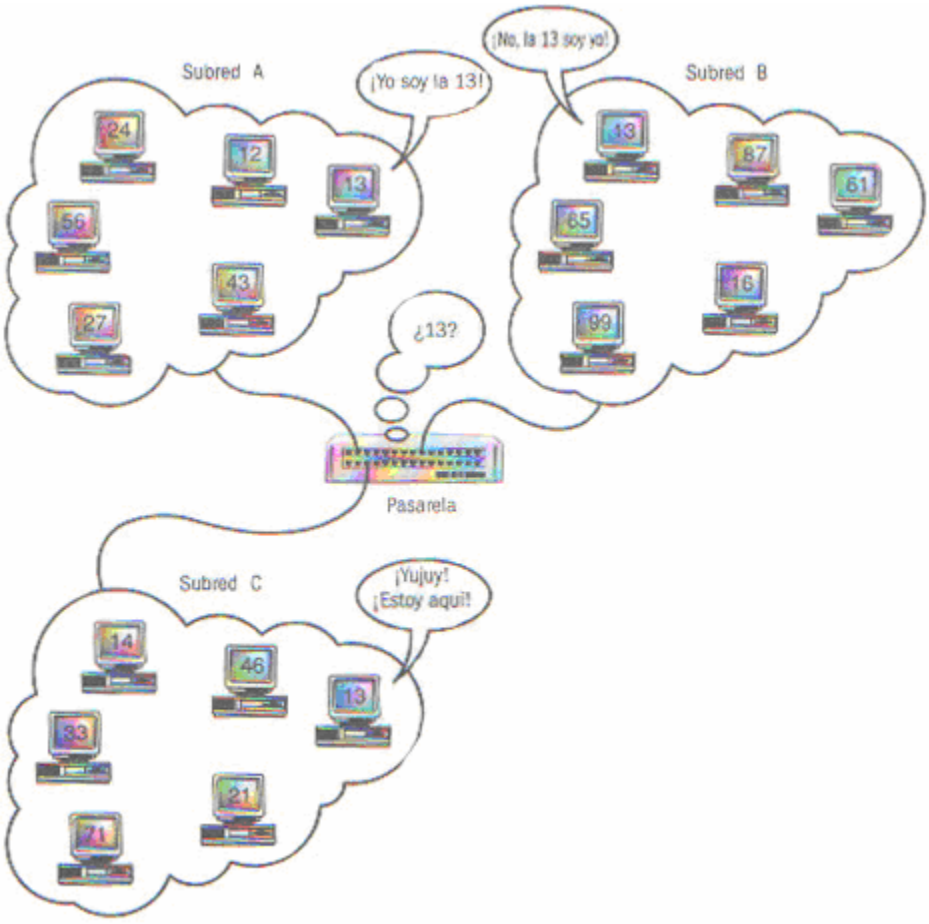


FIGURA 3.7 DECISIÓN DE PASARELA CON BASE EN LA DIRECCION IP.

El resultado seria un tráfico de red absolutamente caótico, sin ninguna forma de identificar el problema. Esto se debería a que el único identificador de las computadoras sería la dirección IP y, en este caso, ni siquiera seria única. Algún usuario malicioso de la red (si, aunque no se lo crea, existen) podría configurar su dirección IP de manera que fuera idéntica a la del servidor central de su compañía y causar estragos en la red. Aunque el resultado de esto podría redundar en unos cuantos días sin poder ir al trabajo, quizá muchos no lo considerasen nada bueno. Actualmente, es perfectamente posible que alguien asigne una dirección IP duplicada en la red. Sin embargo, también es posible identificar la dirección hardware de la que provienen los paquetes duplicados, identificar al fabricante del dispositivo y llegar hasta el culpable. Si no existieran las direcciones de hardware, seria un auténtico rompecabezas.

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

III.5.1 DIRECCIONES IP PÚBLICAS. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

III.5.2 DIRECCIONES IP PRIVADAS (RESERVADAS). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por Ruteadores. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un Ruteador (o ***proxy***) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

III.5.3 DIRECCIONES IP ESTÁTICAS (FIJAS). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

III.5.4 DIRECCIONES IP DINÁMICAS. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma A.B.C.D donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99. Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00

hasta la FF.FF.FF.FF ó en binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

Las tres direcciones siguientes representan a la misma computadora en diferentes sistemas numéricos.

(decimal) 128.10.2.30
(hexadecimal) 80.0A.02.1E
(binario) 10000000.00001010.00000010.00011110

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las computadoras conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el ***identificador de red*** y el ***identificador de host***.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las **clases primarias A**, **B** y **C**. La **clase D** está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de **clase E** no se pueden utilizar (están reservadas). Como se muestra en la Tablas 3-1 con número de hosts y Tabla 3.2 que muestra las direcciones IP.

TABLA 3-1 CLASES DE REDES CON NUMERO DE HOSTS POSIBLES.

	0 1 2 3 4	8	16	24	31
Clase A	0 Red	Host			
Clase B	1 0 Red		Host		
Clase C	1 1 0 Red			host	
Clase D	1 1 1 0 Grupo de multicast (multidifusión)				
Clase E	1 1 1 1 (direcciones reservadas: no se pueden utilizar)				

TABLA 3-2 CLASES DE REDES CON RANGO DE DIRECCIONES IP

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	Máscara de subred
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	Grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	No válidas	-	-	240.0.0.0 - 255.255.255.255	-

Difusión (broadcast) y multidifusión (multicast).-- El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión para referirse a un único host.

III.5.5 DIRECCIONES IP ESPECIALES Y RESERVADAS

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla 3-3. Su interpretación depende del host desde el que se utilicen.

TABLA 3-3 PRINCIPALES DIRECCIONES ESPECIALES

Bits de red	Bits de host	Significado	Ejemplo
Todos 0		Mi propio host	0.0.0.0
Todos 0	Host	Host indicado dentro de mi red	0.0.0.10
Red	Todos 0	Red indicada	192.168.1.0
Todos 1		Difusión a mi red	255.255.255.255
Red	Todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1

Difusión o ***broadcasting*** es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de ***loopback*** (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (***intranets***). Una dirección IP que pertenezca a una de estas redes se dice que es una ***dirección IP privada***. La tabla 3-4 muestra las direcciones reservadas en las redes, que son privadas.

TABLA 3-4 RANGO DE DIRECIONES RESERVADAS EN LAS REDES

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

III.6 PROTOCOLO IP

IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes.

Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados ***datagramas IP***) que tiene las siguientes características:

Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados. Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

III.6.1 FRAGMENTACIÓN

Ya hemos visto que las tramas físicas tienen un campo de datos y es aquí donde se transportan los datagramas IP. Sin embargo, este campo de datos no puede tener una longitud indefinida debido a que está limitado por el diseño de la red. El MTU de una red es la mayor cantidad de datos que puede transportar su trama física. El MTU de las redes Ethernet es 1500 bytes y el de las redes Token-Ring, 8192 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo. Un encaminador ***(Ruteador)*** fragmenta un datagrama en varios si el siguiente tramo de la red por el que tiene que viajar el datagrama tiene un MTU inferior a la longitud del datagrama. Veamos en la siguiente figura 3.8 cómo se produce la fragmentación de un datagrama.

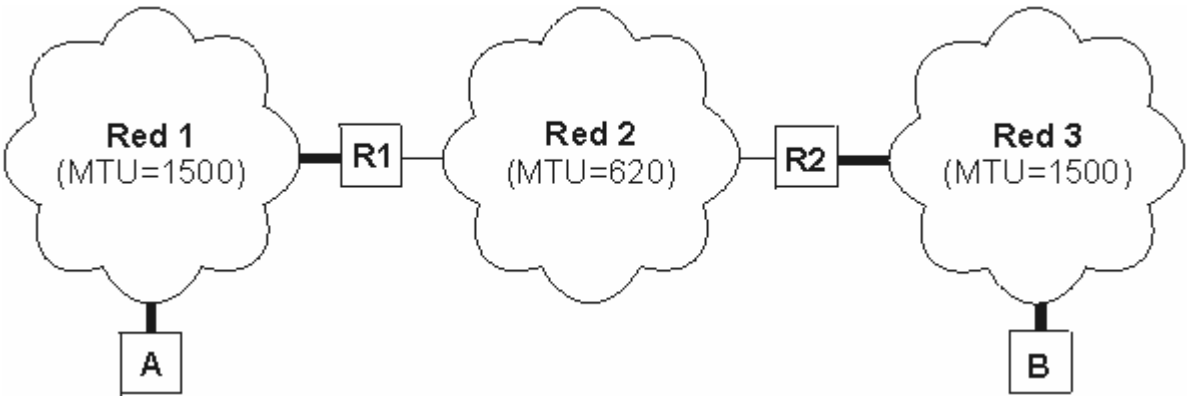


FIGURA 3.8 FRAGMENTACION DE UN DATAGRAMA

Supongamos que el host A envía un datagrama de 1400 bytes de datos (1420 bytes en total) al host B. El datagrama no tiene ningún problema en atravesar la red 1 ya que 1420 < 1500. Sin embargo, no es capaz de atravesar la red 2 (1420 >= 620). El Ruteador R1 fragmenta el datagrama en el menor número de fragmentos posibles que sean capaces de atravesar la red 2. Cada uno de estos fragmentos es un nuevo datagrama con la misma ***Identificación*** pero distinta información en el campo de ***Desplazamiento de fragmentación*** y el bit de ***Más fragmentos (MF)***. Veamos el resultado de la fragmentación:

- ✓ **Fragmento 1:** Long. total = 620 bytes; Desp = 0; MF=1 (contiene los primeros 600 bytes de los datos del datagrama original)

- ✓ **Fragmento 2:** Long. total = 620 bytes; Desp = 600; MF=1 (contiene los siguientes 600 bytes de los datos del datagrama original)
- ✓ **Fragmento 3:** Long. total = 220 bytes; Desp = 1200; MF=0 (contiene los últimos 200 bytes de los datos del datagrama original)

El Ruteador R2 recibirá los 3 datagramas IP (fragmentos) y los enviará a la red 3 sin reensamblarlos. Cuando el host B reciba los fragmentos, recompondrá el datagrama original. Los encaminadores intermedios no reensamblan los fragmentos debido a que esto supondría una carga de trabajo adicional, a parte de memorias temporales. Nótese que el ordenador destino puede recibir los fragmentos cambiados de orden pero esto no supondrá ningún problema para el reensamblado del datagrama original puesto que cada fragmento guarda suficiente información.

Si el datagrama del ejemplo hubiera tenido su bit ***No fragmentar (NF)*** a 1, no hubiera conseguido atravesar el Ruteador R1 y, por tanto, no tendría forma de llegar hasta el host B. El encaminador R1 descartaría el datagrama.

III.7 PROTOCOLOS DERIVADOS DE TCP/IP

A continuación se mencionaran los diferentes protocolos que se derivan de TCP/IP ya que es una gama extensa que solo se describirán los mas importantes en cuanto este trabajo y en los sistemas actuales de redes que se ocupan para un servicio necesario en las empresas, para diagnosticar ó evaluar las redes de una manera inicial y poder definir las posibles fallas o analizar los cambios en una red.

III.7.1 PROTOCOLO ARP

Dentro de una misma red, las computadoras se comunican enviándose tramas físicas. Las tramas Ethernet contienen campos para las direcciones físicas de origen y destino (6 bytes cada una):

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

El problema que se nos plantea es cómo podemos conocer la dirección física de la máquina destino. El único dato que se indica en los datagramas es la dirección IP de destino. ¿Cómo se pueden entregar entonces estos datagramas? Necesitamos obtener la dirección física de un ordenador a partir de su dirección IP. Esta es justamente la misión del protocolo ARP (Protocolo de Resolución de Direcciones, Address Resolution Protocol).

Nota: El protocolo ARP está definido en la RFC 826

La Tabla 3-5 muestra las direcciones físicas así como la dirección IP que le corresponde.

TABLA 3-5 RELACION DE DIRECCION FISICA CON LAS DIRECCION IP EN LOS HOSTS.

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
	A3-BB-05-17-29-D0	10.10.0.1	Red 2
B	00-E0-4C-33-79-AF	10.10.0.7	
R2	B2-42-52-12-37-BE	10.10.0.2	
	00-E0-89-AB-12-92	200.3.107.1	Red 3
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	

Vamos a tomar un ejemplo, como es el siguiente. Un host A envía un datagrama con origen 192.168.0.10 y destino 10.10.0.7 (B). Como el host B se encuentra en una red distinta al host A, el datagrama tiene que atravesar el Ruteador 192.168.0.1 (R1). Se necesita conocer la dirección física de R1.

Es entonces cuando entra en funcionamiento el protocolo ARP: A envía un mensaje ARP a todas las computadoras de su red preguntando "¿Cuál es la dirección física de la computadora con dirección IP 192.168.0.1?". La computadora con dirección 192.168.0.1 (R1) advierte que la pregunta está dirigida a ella y responde a A con su dirección física (00-E0-4C-AB-9A-FF). Entonces A envía una trama física con origen 00-60-52-0B-B7-7D y destino 00-E0-4C-AB-9A-FF conteniendo el datagrama (origen 192.168.0.10 y destino 10.10.0.7). Al otro lado del Ruteador R2 se repite de nuevo el proceso para conocer la dirección física de B y entregar finalmente el datagrama a B. El mismo datagrama ha viajado en dos tramas físicas distintas, una para la red 1 y otra para la red 2.

Observemos que las preguntas ARP son de difusión (se envían a todas las máquinas). Estas preguntas llevan además la dirección IP y dirección física de la computadora que pregunta. La respuesta se envía directamente a la computadora que formuló la pregunta.

III.7.2 DHCP

Recientemente se ha empezado a utilizar una técnica diferente para asignar direcciones IP a las computadoras cliente. Esta técnica se conoce como asignación dinámica y la gestiona una computadora que tenga en ejecución lo que se denomina servidor DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host). Los servidores DHCP se puede preparar para que efectúen la configuración TCP/IP de un usuario automáticamente cuando encienda su computadora. También proporcionan al administrador el poder de ajustar remotamente la configuración de las computadoras cliente.

Las ventajas del DHCP son obvias; no es necesaria ninguna configuración por parte del usuario final, ni tampoco hay que mantener una enorme y voluminosa base de datos con direcciones IP. DHCP libera al administrador de red de una tarea poco

productiva, y que requiere mucha dedicación. Sin embargo, también puede limitar su capacidad para resolver los problemas de los usuarios individuales. Las direcciones se actualizan según una unidad de tiempo, denominada duración de la asignación del DHCP. Las computadoras alquilan direcciones al servidor. Cuando la asignación caduca, el número se puede reasignar a la misma computadora, o a otra computadora diferente. Es responsabilidad del cliente la renovación de la licencia de la dirección IP asignada, cuando haya transcurrido la mitad del tiempo de asignación. Por lo general, la dirección se puede renovar indefinidamente. Si una asignación caduca y no se renueva, es posible que el servidor DHCP asigne una configuración IP diferente a la misma computadora. Esta acción de saber quien tiene una determinada dirección en un determinado instante de tiempo, y en su lugar, lo único que posee es una lista de direcciones IP y las direcciones hardware a las que están asignadas.

III.7.3 PROTOCOLOS DE CORREO

Hoy en día el correo electrónico es una de las herramientas más utilizadas en la industria por ello ha desarrollado algunos protocolos que definen la seguridad de la información así como la rapidez de la misma, que a continuación se describen.

III.7.3.1 POP3

Comenzaremos con los protocolos de correo de nivel sesión, en concreto con el protocolo POP3, Post Office Protocol.

El propósito del servidor POP3 es proporcionar un punto de recolección para su correo electrónico. Su computadora se conecta al servidor POP3 a través de una conexión TCP/IP en el puerto 110. Luego, ejecuta una serie de ordenes que identifican al usuario, recopila información acerca de los mensajes disponibles y los carga en la computadora local. El correo electrónico basado en POP3 se desarrollo para disminuir la sobrecarga derivada de mantener múltiples conexiones en un servidor de correo. Anteriormente, los clientes tenían que conectarse directamente al servidor de correo y utilizar el software de servidor, generalmente a través de la línea de órdenes, para leer los mensajes de correo. Para una organización ó Universidad de tamaño considerable, este esquema colocaba gran parte de la carga en el servidor (en algunos casos, todavía es así). Además, una vez que se había leído el correo, este no se eliminaba automáticamente del servidor, sino que podía dejarse allí todo el tiempo que se deseara. POP3 elimina estos problemas estableciendo conexiones cortas y rápidas con el servidor, durante las que el correo se traspasa del servidor a la computadora local de cliente. Cuando se usa el sistema de correo POP, las necesidades de recursos del servidor se reducen significativamente.

III.7.3.2 SMTP

Hemos visto el protocolo POP3, pero ¿Cómo enviar un correo electrónico? Algunos servidores y clientes POP3 pueden enviar correo electrónico desde una conexión POP3, pero esta operación no debe considerarse como norma. La mayoría de los clientes se conectan a un servicio TCP/IP separado, denominado SMTP, para realizar el envío de mensajes.

SMTP (Simple Mail Transfer Protocol) Protocolo Simple de transferencia de Correo, es la red troncal par todo el correo electrónico. Acepta mensajes entrantes en el puerto 25 y los almacena en buzones de correo individuales, o transporta el correo a otra máquina para su suministro.

III.7.3.3 IMAP

IMAP (Internet Message Access Protocol) Protocolo de Acceso de Mensajes de Internet, es un protocolo recientemente añadido a los protocolos de correo TCP/IP y uno de los más útiles. Permite a los clientes conectarse a un servidor IMAP y manipular remotamente los buzones de correo, como si estuvieran localmente ubicados en cada cliente. IMAP se ha diseñado para eliminar la frustración muchas personas tienen con el servidor de correo POP: demasiadas copias de mensajes en demasiados lugares. El correo electrónico basado en POP es efectivo cuando se esta trabajando con una única computadora cliente. Sin embargo, si se tiene una computadora en casa y otra en la oficina y comparten cuentas de correo electrónico entre ellas, pueden surgirle algunos problemas. El autor, frecuentemente, recibe solicitudes de ayuda cuando esta en casa leyendo su correo. Cuando todavía utilizaba un servidor POP3, volvía al trabajo y se olvidaba completamente (hasta que sonaba el teléfono) de que había recibido el mensaje de correo electrónico en un servidor y permitiendo al usuario acceder a él, en el momento que desee. Cuando el autor pone en marcha Outlook Express en casa, su buzón de correo electrónico es exactamente el mismo que en la oficina. Algunos servidores IMAP permiten incluso configurar reglas para almacenar los mensajes IMAP entrantes en diferentes buzones de correo de forma automática.

III.7.4 PROTOCOLOS DE ENTREGA DE DOCUMENTOS

También se ha desarrollado protocolos de entrega de documentos que hoy, es importante ya que electrónicamente son importantes pero la alta cantidad de bytes en cada uno de ellos; hace que la transferencia sea más tardada, por lo que con estos protocolo se define seguridad y rapidez en la información.

III.7.4.1 GOPHER

El protocolo Gopher fue diseñado para permitir a las computadoras navegar a través de un conjunto de información almacenada con un interfaz de usuario amigable e independiente de la plataforma. Los datos se organizan en formato jerárquico con diferentes niveles de directorio por lo que el usuario puede desplazarse. Es un cliente típico, estos niveles se representan mediante menús. Seleccionar una opción de menú puede hacer una de las tres cosas siguientes: redirigirnos a un servidor Gopher distinto, llevarnos a un submenú del menú actual, o visualizar o descargar un documento. Gracias a su capacidad para redirigir el cliente hacia el otro servidor, el sistema Gopher se comporta de una forma muy similar a un sencillo explorador Web. Sin embargo, la diferencia entre el servidor Web y el servidor Gopher esta en la interfaz directa y estructurada. Normalmente, el explorador para la World Wide Web es una herramienta muy gráfica y abstracta, mientras que el sistema Gopher proporciona información de forma directa y basada en texto. Sin embargo, los servidores Web pueden estructurar sus datos siguiendo el mismo estándar jerárquico que el servidor Ghoper, y los exploradores

Web pueden actuar como exploradores Gopher. Debido a estas razones, los servidores Gopher están comenzando a ser extremadamente raros.

III.7.4.2 HTTP

Frecuentemente, se considera la Web como una creación asombrosa pero, ¿Cómo de asombrosa es la red que lo hace posible? La respuesta probablemente le sorprenda. La especificación del protocolo HTTP es extremadamente larga e implica una gran cantidad de condiciones que pueden existir entre el servidor y el cliente; sin embargo, es conceptualmente fácil de seguir e ilustrar.

III.7.4.3 IRC

Internet Relay Chat (IRC) se desarrollo para ser el más moderno protocolo de conversación por Internet y ha demostrado ser precisamente eso. IRC es la MBONE (red troncal multimedia) de la conversación en Internet. IRC es un grupo de servidores interconectados que permiten a miles de clientes conectarse simultáneamente y conversar entre ellos. Como la red troncal de multimedia de Internet, IRC interconecta servidores esparcidos por todo el mundo. Cuando se envían mensajes a un servidor, IRC los retribuye a través de la red IRC.

La utilización de un servidor IRC puede ser poco confusa al principio, pero esto es porque todavía no se ha escrito un software de cliente que oculte completamente el protocolo IRC. La mayor parte de los clientes requieren que el usuario realmente conozca la mayor parte del conjunto de ordenes IRC, para usarlo de una forma eficiente. Los servidores IRC se definen canales y operadores. Los canales son los famosos salones de conversación de los que todos hemos oído hablar. Cualquier persona puede crear un canal, probablemente se desee ser el operador del mismo. Ser operador de un canal proporciona la capacidad de controlar a los usuarios que intentan unirse al mismo. Pueden negarles el acceso, echarlos y otras muchas cosas. Se puede incluso intercambiar archivos con otros usuarios directamente a través de la interfaz IRC. Sin embargo, hay advertencias a seguir: IRC tiene una enorme cantidad de funciones ocultas y agujeros. Los usuarios de IRC con experiencia pueden hacer estragos en su canal si se les provoca. IRC es un excelente lugar para el trabajo cooperativo pero también es un lugar de encuentro principal para muchos piratas informáticos.

III.7.4.4 FTP

FTP es el todo terreno de la red para transferir archivos a través de conexiones TCP/IP. Se han escrito servidores y clientes para todas las plataformas imaginables y, a pesar de la popularidad de HTTP para la transferencia directa de archivos, FTP se ha mantenido como el rey para la transferencia directa de archivo entre distintas plataformas.

Si nunca ha utilizado FTP, una de las primeras cosas que observará es muy rápido. El protocolo fue diseñado para ser extremadamente sencillo y para transferir datos lo más rápidamente posible. Pruebe a copiar un archivo en una computadora remota usando FTP y luego empleando un protocolo específico de sus sistemas operativos. Quedará bastante sorprendido por la diferencia de velocidad que observará.

FTP emplea un método diferente de comunicación del que hemos visto hasta el momento. Podemos comunicarnos con un servidor FTP a través de una conexión Telnet, aunque no completamente. La razón, de ello es que una misma sesión FTP mantiene una conexión de dos puertos distintos: el puerto 20, denominado “conexión de datos” y el puerto 21, denominado “conexión de órdenes”. Como es de esperar, las órdenes se envían al puerto 21 y los datos suministrados al cliente desde el servidor se envían a través del puerto 20.

III.7.4.5 NTP

FTP es el primer protocolo introducido anteriormente en el que no existe un formato por completo legible. Sin embargo, FTP sigue siendo un protocolo TCP/IP de muy alto nivel. Se puede ver las órdenes que se envían y reciben para realizar tareas en la red. Nuestros ejemplos han demostrado que muchos protocolos trabajan según el modelo de solicitud del cliente y respuesta del servidor. Es importante darse cuenta de que no todos los protocolos siguen este modelo. Pueden no haberse percatado pero, realmente, hasta este momento hemos visto dos de estos protocolos: SNMP y DHCP. Veamos un último protocolo que es útil y no tiene un formato comprensible para el usuario: NTP (Network Time Protocol), el protocolo de temporización de red.

NTP proporciona un mecanismo mediante el cual un reloj interno del dispositivo de red se puede sincronizar con el reloj de un servidor NTP. El reloj del servidor NTP considera como la autoridad para las cuestiones de temporización, incluso aunque él, en sí no sea preciso. Para evitar este error, muchos servidores NTP se sincronizan; así mismos conectándose a otros servidores NTP, que están directamente vinculados a relojes atómicos; no es posible conseguir algo más preciso que esto. Por tanto, conectando ambas computadoras al servidor NTP de forma periódica, se pueden suponer que sus relojes permanecerán sincronizados y el software del autor continuara ejecutándose como debiera.

III.8 INTERNET: LA RED INFORMÁTICA

La llamada "autopista de la información" es, realmente, un conjunto de miles de redes informáticas unidas entre sí. Comenzó con el propósito de crear una infraestructura comunicativa entre computadoras con fines militares. Hoy en día existen miles de redes que interconectan por vía telefónica millones de computadoras personales de todo el mundo. El espíritu inicial de las primeras experiencias era simplemente académico: pretendían unir bases de datos de centros de investigación de todo el mundo para intercambiar información. Es una red de computadoras interconectadas entre sí que ofrecen acceso y comparten información a través de un lenguaje común. En la actualidad es la red de computadoras más grandes que existe en el mundo; se conecta por teléfono (a través de un módem) o por fibra óptica y transmite toda clase de información.

La palabra Internet es el resultado de la unión de dos términos: Inter, que hace referencia a enlace o conexión y Net (Network) que significa interconexión de redes. Es decir, Internet no es otra cosa que una conexión integrada de redes de computadores o redes interconectadas.

Por medio de todo este conjunto de componentes de hardware y software. Se crearon y continúan desarrollándose numerosos servicios, aplicaciones y usos de toda índole que son aprovechados para diferentes fines, los que conforman el infinito mundo Internet.

III.8.1 DNS

Los servidores DNS no contienen información de todas las computadoras en Internet. En lugar de ello, tiene autoridad únicamente sobre determinadas subredes y contiene solo la información de los nombres de host de estas subredes. También disponen de la capacidad de consultar información de otros servidores DNS y así dar respuesta a solicitudes referentes a computadoras sobre las que no tiene autoridad. Para minimizar el trafico de red, la mayoría de los servidores DNS guardan en caché la información sobre otros servidores y responderán a las solicitudes directamente, como si ellas tuvieran autoridad sobre las redes remotas. Sin embargo, deberán identificar su respuesta como no-vinculante. Para mantener la información almacenada en el caché del DNS <<actualizada>>, cada elemento de la base de datos DNS tiene un tiempo de vida (Time To Live, TTL) especifico. Una vez que el TTL ha transcurrido, el elemento se borra de la cache. El TTL suele estar configurado a varias horas, ya que los hombres de host suelen ser relativamente estables.

La resolución de nombres puede ser un proceso muy costoso en términos de tiempo de proceso. Aunque la mayoría de los nombres se resuelven en una fracción de segundo (o dos), el tiempo de proceso depende por completo de lo rápido que puedan responder los servidores DNS primarios de dominio a una solicitud. El servicio DNS se creó para facilitar la ubicación de los dominios. Un dominio es una colección de nodos relacionados de alguna manera. De esa manera es como DNS organiza los nombres de los nodos en una jerarquía de dominios.

Dependiendo de su localización en la jerarquía, un dominio puede ser de primer, segundo o tercer nivel. También DNS tiene otras ventajas: permite delegar la autoridad sobre un determinado subdominio a sus administradores. La delegación de un subdominio implica el control total del mismo por parte de la organización en la que se delegó, con total libertad para crear nuevos subdominios internos, asociar nombres a nodos, etc. Los DNS organizan los nombres de los nodos en una jerarquía de dominios. Un dominio es una colección de nodos relacionados de alguna manera. Dependiendo de su localización en la jerarquía, un dominio puede ser de primer, segundo o tercer nivel. Otros niveles pueden existir pero no son frecuentes. Por ejemplo, algunos dominios de primer nivel muy usuales son los siguientes:

- edu: Aquí se incluyen casi todas las universidades o centros de investigación.
- com: Compañías u organizaciones con fines comerciales.
- org: Organizaciones no comerciales. Las redes UUCP privadas se encuentran aquí.
- net: Pasarelas y otros nodos administrativos de la red.
- mil: Nodos militares.
- gov: Nodos del gobierno.

III.8.2 ISP

Un proveedor de servicios de Internet o ISP (***Internet Services Provider***), es una empresa que presta servicios de conexión a Internet. Los ISP también están siempre conectados, de forma que sus clientes pueden acceder a Internet en cualquier momento. Además de hacer posible la conexión de sus clientes, un ISP suele prestar otros servicios, como el hospedaje de páginas o una cuenta de correo electrónico, de donde resulta que suelen ser a la vez proveedores de conexión y servidores de hospedaje.

La conexión entre el usuario final y el ISP, se realiza normalmente mediante RTB (Red Telefónica Básica), siendo nuestra llamada conducida por la Compañía Telefónica hasta un host en la sede del ISP. A partir de este punto, comienza para nosotros el universo Internet. Este host del ISP que permite al cliente conectarse a la Red se dice que es su pasarela ("Gateway") a Internet. Sin embargo también existe el acceso de Internet a través de enlaces dedicados, es decir, de mayor capacidad para el tráfico demandante de la empresa, utilizando medios alternativos como fibra óptica, BNC, o satélites, para una amplia cantidad de ancho de banda.

III.8.3 COMERCIO ELECTRÓNICO

El comercio electrónico ha adquirido rápidamente una gran importancia económica y política al proseguir la notable expansión mundial de Internet. Los derechos de propiedad intelectual son de importancia fundamental para el mantenimiento de un entorno estable y favorable al desarrollo continuo del comercio electrónico.

El comercio electrónico consiste en realizar electrónicamente transacciones comerciales. Está basado en el tratamiento y transmisión electrónica de datos, incluidos texto, imágenes y vídeo. El comercio electrónico comprende actividades muy diversas, como comercio electrónico de bienes y servicios, suministro en línea de contenidos digitales, transferencia electrónica de fondos, compraventa electrónica de acciones, conocimientos de embarque electrónicos, subastas, diseños y proyectos conjuntos, prestación de servicios en línea (on line sourcing), contratación pública, comercialización directa al consumidor y servicios posventa. Por otra parte, abarca a la vez productos (p.ej., bienes de consumo, equipo médico especializado) y servicios (p.ej., servicios de información, financieros y jurídicos), actividades tradicionales (p.ej., asistencia sanitaria, educación) y nuevas actividades (p.ej., centros comerciales virtuales).

III.8.4 INTRANET

Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet ó no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (Web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "Internets" en miniatura ó lo que es lo mismo, Internet es una intranet pública gigantesca.

III.8.5 EXTRANET

Unión de dos ó más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

Una extranet proporciona varios niveles de accesibilidad a los usuarios foráneos. Y tu solo puedes acceder a una extranet si cuentas con un usuario y una contraseña. Es decir se maneja seguridad.

CAPITULO IV FRAME RELAY

IV.1 INTRODUCCION

El crecimiento del tráfico de datos originado por la gran cantidad de nuevas aplicaciones tales como el correo electrónico, la transferencia de archivos y los programas elaborados para diseño y manufactura, creados para trabajar en el ambiente LAN, han traído la necesidad de transmitir grandes volúmenes de información en forma de patrones de tráfico impredecibles conocidas como “ráfagas”. Frame Relay es un protocolo de acceso a la red diseñado para transportar este tipo de información. Tanto las anteriores aplicaciones, como las actuales que requieren de alta velocidad de transmisión, no pueden tolerar excesivos retardos a través de los enlaces WAN; Frame Relay también fue diseñada para cubrir esta necesidad.

El protocolo Frame Relay trabaja en los dos primeros niveles del modelo OSI ya que parte del hecho de que los dispositivos conectados alrededor de él, y los medios de comunicación son de muy alta confiabilidad, trayendo como consecuencia un menor procesamiento de información. Esta capacidad permite a los nodos Frame Relay la transmisión de altos volúmenes de tráfico a través de canales de mayor velocidad, sin tener que incrementar el tamaño del equipo.

Los protocolos orientados a paquete tienen como característica, la posibilidad de administrar el Ancho de Banda de manera inteligente haciendo uso de su capacidad para manejar la totalidad del tráfico proveniente de diferentes fuentes, el cual será lógicamente multiplexado a través de una interfaz única en la red. Los paquetes serán enviados tan pronto como el canal este disponible.

En esencia, Frame Relay es un mecanismo de señalización y transferencia de datos entre dispositivos finales y la red. El dispositivo transmisor, coloca un número identificador en cada trama de datos antes de que esta sea enviada al nodo Frame Relay de destino, el cual lo interpreta como una dirección de destino y envía la trama hasta él. Este proceso también hablita a cada dispositivo terminal para comunicarse con varios destinos utilizando un solo enlace de acceso a la red.

IV.2 CONCEPTO GENERAL

Frame Relay es un protocolo WAN de alto rendimiento que opera en la capa física y capa de enlace del modelo OSI. Frame Relay originalmente fue diseñado para usarse a través de las interfaces de Red Digital de Servicios Integrados (Integrated Services Digital Network [ISDN]). Hoy, este es usado sobre una variedad de otras interfaces de red como buena tecnología. En esta sección se enfoca en las especificaciones de Frame Relay y aplicaciones en el contexto de servicios WAN.

Frame Relay es un ejemplo de la tecnología de conmutación de paquetes. Las redes de conmutación de paquetes habilitan a las estaciones finales para compartir dinámicamente los medios de la red y el ancho de banda disponible. Las siguientes dos técnicas son usadas en la tecnología de conmutación de paquetes:

- Paquetes de longitud variable

- Múltiplexación estadística

Los paquetes de longitud de variable son usados para transferencias de datos más flexibles y eficientes. Esos paquetes son conmutados entre varios segmentos en la red hasta que el destino es alcanzado.

La Técnica de la múltiplexación estadística controla el acceso de la red en un paquete de la red conmutada. La ventaja de esta técnica es que esta acomoda más flexibilidad y eficiencia en el uso del ancho de banda. El más popular de LAN, tal como son Ethernet y Token Ring, son redes de paquetes conmutados.

Frame Relay frecuentemente es descrito como una línea aerodinámica de la versión de X.25, ofreciendo algunas más de las capacidades robustas, tal como el ventaneo y la retransmisión del último dato que son ofrecidos en X.25. Este es el porque Frame Relay típicamente opera sobre las facilidades WAN que ofrece mas servicios de conexiones seguras y un alto grado de seguridad que las facilidades disponibles durante el termino de los 70s y cercano a los 80s que sirven como plataforma común para WANs de X.25. Como se menciono anteriormente, Frame Relay es estrictamente un protocolo de Capa 2, mientras que X.25 proporciona servicios en la Capa 3 (Capa de Red). Esto habilita a Frame Relay para ofrecer el más alo rendimiento y la mejor eficiencia que X.25, y lo hace adecuadamente Frame Relay para actuales aplicaciones WAN, tal como la interconexión LAN.

IV.3 ESTANDARIZACION DEL PROTOCOLO FRAME RELAY

La necesidad de manejar estándares que regulen el protocolo Frame Relay entre los diferentes diseñadores de equipos de telecomunicaciones llevo a Estados Unidos a crear un comité conocido como T1S1 acreditado por ANSI a trabajar en el desarrollo de los estándares. T1S1 dio entrada al protocolo Frame Relay a los estándares de CCITT en los grupos de Estudio XI y XVII.

Un mayor desarrollo en la historia de Frame Relay ocurrida en 1990 cuando Cisco, Digital Equipment Corporation (DEC), Northern Telecom, y StrataCom formado un consorcio para concentrarse en el desarrollo de tecnología Frame Relay. Este consorcio desarrollo una especificación que conformada al protocolo básico de Frame Relay que estuvo siendo discutida en CCITT, pero este extendido protocolo con características que proporciona capacidades adicionales para los entornos de internetworking complejo. Estas extensiones de Frame Relay son referidas colectivamente como la Interfase de Administración Local (Local Management Interface [LMI]).

Después que la especificación de consorcio fue desarrollada y publicada, muchos vendedores han anunciado sus definiciones de soporte del Frame Relay extendido. ANSI y CCITT han subsecuentemente estandarizado sus propias variaciones de la especificación original de LMI, y estas especificaciones estandarizadas ahora son más comúnmente usadas que la versión original.

Internacionalmente, Frame Relay fue estandarizado por la International Telecommunication Union—Telecommunications Standards Section (ITU-T). En los

Estados Unidos, Frame Relay es un estándar de American National Standards Institute (ANSI).

El trabajo técnico de los estándares para Frame Relay concluyo en 1991.

Por su parte, CCITT determino dividir las funciones y características del protocolo Frame Relay en 5 estándares por separado.

Descripción del servicio (CCITT I.233, ANSI T1.606). Describe el propósito y características generales de una red Frame Relay.

Administración de la Congestión. (CCITT I.370, ANSI T1.606-1) define la velocidad y manejo del tráfico de las ráfagas de datos. Describe también los procedimientos de administración y control de la congestión en la red.

Aspectos Esenciales. (CCITT Q.922, ANSI T1.618). Da una amplia explicación de los procesos que ocurren en Frame Relay.

Señalización de Acceso. (CCITT Q.933, ANSI T1.617). Especifica un protocolo para establecimiento de llamadas virtuales del nodo Frame Relay y proporciona un medio para informar a los usuarios a cerca de la asignación, detección de fallas y reestablecimiento de la llamada virtual.

Control de Enlace de Datos. (CCITT Q.922, no estandarizado por ANSI). Proporciona un mecanismo de enlace final punto a punto para asegurar la entrega correcta de información a través de la red.

La recomendación Q.922 Anexo A de CCITT define los aspectos centrales que dieron origen a la estructura de la trama LAPF (Link Acess Procedure for Frame relay; Procedimiento de Acceso al Enlace para Frame Relay) para el control y transporte de datos entre dos dispositivos finales en el nivel 2 del modelo OSI.

El anexo A contiene la estructura de la trama, procedimientos y formatos de los protocolos de los campos para a operación apropiada del servicio proporcionado en el nivel 2 como son descritos en la recomendaciones I.222 e I.223.

El protocolo definido en el Anexo A es un subgrupo del protocolo LAPF. Este intenta compartir las funciones principales del protocolo LAPF definidas en la recomendación I.233 que ha sido utilizado convenientemente por el protocolo LAPD, así como también en la recomendación Q.921. Estas funciones se refieren a la delimitacion, alineamiento y transparencia de la trama, el procedimiento de múltiplexaje y desmultiplexaje de la trama usando el campo de dirección, detección (pero no corrección) de errores y las funciones de administración de la congestión.

Q.922A fue escogido para Frame Relay por que virtualmente todos los protocolos de datos pueden ser adaptados a dicho formato para transportarse a través de redes WAN, SNA, TCP/IP, X.25 y virtualmente todos los protocolos propietarios, pueden ser usados con el formato Q.922A; esto hace a una red Frame Relay compatible con una gran variedad de protocolos de alto nivel.

IV.4 DISPOSITIVOS DE FRAME RELAY

Los dispositivos que unen a red WAN de Frame Relay están dentro de las dos categorías generales siguientes:

- Equipo Terminal de Datos (DTE)
- Equipo de Comunicaciones de Datos (Data circuit-terminating equipment [DCE])

Los DTEs generalmente son considerados para ser equipos terminales para especificar una red y típicamente son ubicados premisas de un cliente. De hecho, estos pueden ser poseídos por el cliente. Ejemplos de dispositivos DTE son terminales, computadoras personales, Ruteadores, y puentes.

Los DCEs son dispositivos de interconectividad de las portadoras poseídas. El propósito del equipo DCE es proporcionar el reloj y servicios de conmutación en una red, en el cual son los dispositivos que actualmente transmiten datos a través de la WAN. En muchos de los casos, esos son los paquetes conmutados. Como muestra la Figura 4.1 la relación entre las 2 categorías de los dispositivos.

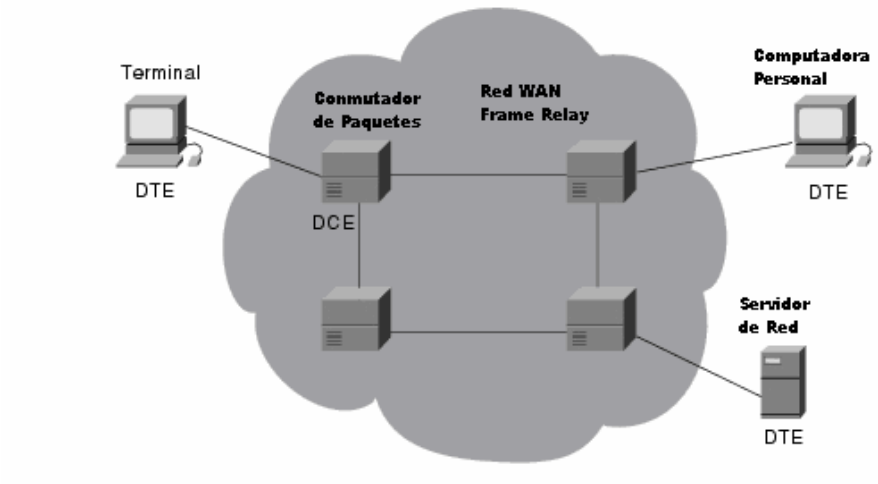


FIGURA 4.1 DCEs GENERALMENTE RESIDE CON LAS WANS DE LAS PORTADORAS OPERADAS.

La conexión entre un dispositivo DTE y un dispositivo DCE consiste en ambos componentes de capa física y capa de enlace. Los componentes físicos definen las especificaciones mecánicas, eléctricas, funcionales, procedimientos para la conexión entre los dispositivos. Uno de los más comúnmente usados en las especificaciones de la capa física es el estándar recomendado de la especificación (RS)-232. El componente de la capa de enlace define el protocolo que establece la conexión entre el dispositivo DTE, tal como un Ruteador, y el dispositivo DCE, tal como un Switch. En esta sección examinaremos una especificación de protocolo comúnmente usado en la red WAN: el protocolo Frame Relay.

IV.5 CONCEPTOS BASICOS DE FRAME RELAY

La técnica tradicional de conmutación de paquetes tiene características básicas:

- Señalización dentro de banda. Los paquetes de control de llamada, utilizados por establecer y terminar los circuitos virtuales, se transmiten por el mismo canal y el mismo circuito virtual que los paquetes de datos.

- Múltiplexación de los circuitos virtuales a nivel de red.

- Control de flujo y control de errores tanto a nivel 2 como a nivel 3.

Estas características suponen una gran carga para el sistema. La figura 4.2 a) muestra el flujo de tramas necesarias para la transmisión de un único paquete de datos, con su correspondiente paquete de reconocimiento desde el sistema final origen hasta el sistemas final destino. Para cada salto en la red, el protocolo de control de enlace de datos necesita del intercambio de una trama de datos y una trama de acuse de recibo. Más aun para cada nodo intermedio es necesario mantener tablas de estado por cada circuito virtual que administren la gestión de llamadas y los aspectos de control de errores y de flujo del protocolo X.25. Para simplificar se supone que el tamaño de la ventana es 1. Toda esta carga puede ser ajustada si existe una posibilidad importante de aparición de errores en cualquiera de los enlaces de red, pero este no es el caso de la mayoría de las redes actuales.

Frame Relay esta diseñada para eliminar en lo posible todos aquellos procesos no necesarios hoy en día de X.25 y que generan una importante carga del sistema. Los puntos principales en los que Frame Relay se diferencia de un servicio de conmutación de paquetes convencional X.25 son:

- Control de llamadas fuera de banda. La señalización del control de llamada se realiza en una conexión lógica separada de la conexión para la transmisión de los datos del usuario.

- La múltiplexación y conmutación de conexiones lógicas tiene lugar a nivel 2 en vez de a nivel 3, eliminando de esta manera un nivel entero de procesamiento.

- La red deja de preocuparse del control de errores y del control de flujo. Estos, si se emplean, pasan a ser responsabilidad del nivel superior y se realizan extremo a extremo.

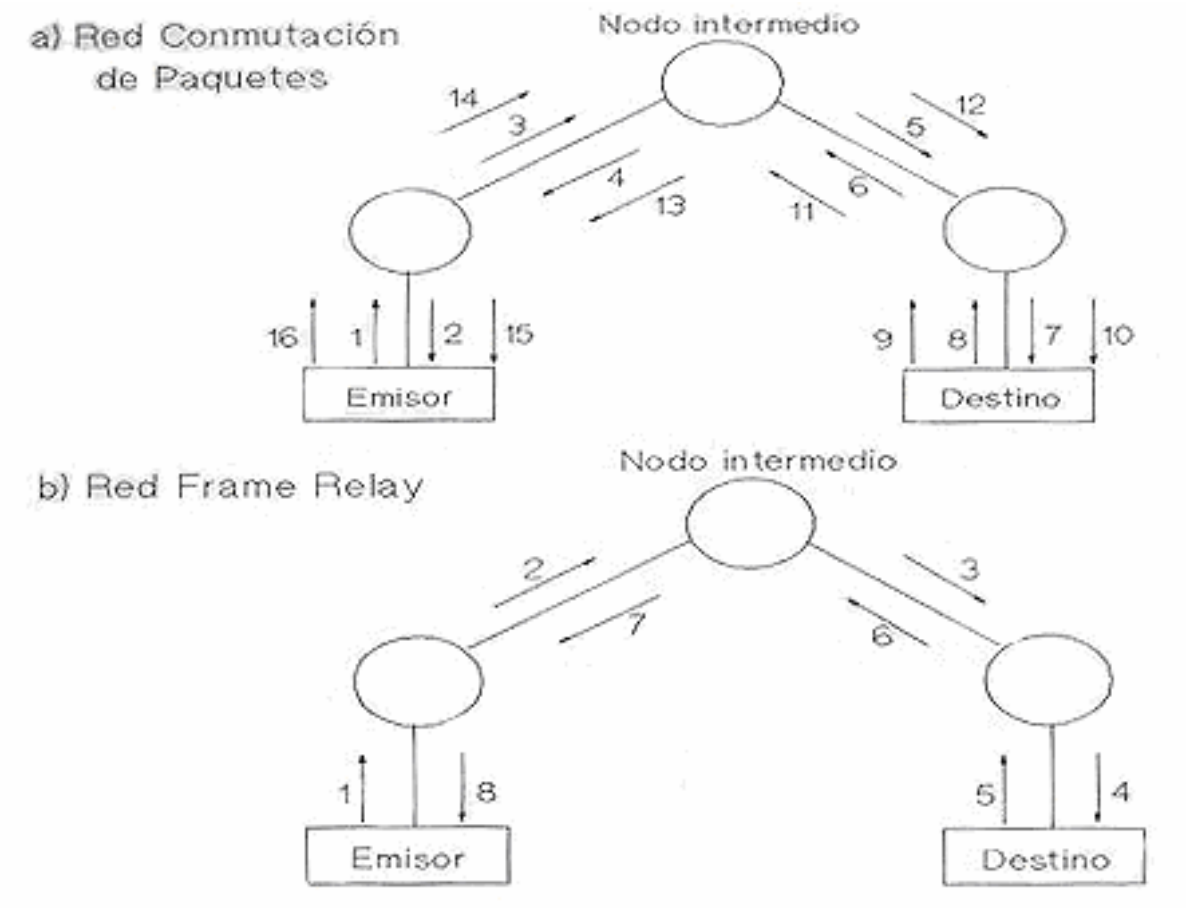


FIGURA 4.2 A) Y B) COMPARACIÓN DE TRANSMISIONES X.25 Y FRAME RELAY.

La figura 4.2 b) muestra la operación de Frame Relay, en la que manda una única trama de datos del origen al destino y se genera un acuse de recibo en el nivel superior, transmitido de vuelta a otra trama.

La conmutación de tramas (ó frame switching) opera también a nivel 2; sin embargo, realiza las funciones de control de errores y control de flujo de este nivel.

A continuación se analizan las ventajas e inconvenientes de la utilización de Frame Relay frente a X.25.

IV.5.1 INCONVENIENTES

- El inconveniente principal de Frame Relay frente a X.25 es que se pierde la capacidad de realizar el control de flujo y el control de errores en cada uno de los enlaces de la red, pero esta funcionabilidad puede ser proporcionada, extremo a extremo, por nivel superior.

- Es necesaria la disponibilidad de líneas de alta calidad.

- No existe un estándar para la interconexión de servicios Frame Relay, como X.75 para las redes X.25.

- Si la conexión es directa, es decir, si no hay nodos intermedios, el FRL no ofrece ninguna ventaja frente a SDLC o HDLC, con los que guarda gran semejanza.

- Si la probabilidad de error (BER) fuese alta, sería necesario retransmitir tramas enteros de extremo a extremo, por lo que las ventajas iniciales quedarían neutralizadas. En este punto es destacable que, si bien es cierto que se pueden utilizar instalaciones existentes, estas han de poder ofrecer un mínimo nivel de calidad para poder soportar servicios FRL.

- Otra desventaja deriva de la facilidad para transmitir tramas de tamaño variable que introduce retardos y tiempos de respuesta imprevisibles, lo que imposibilita a las redes totalmente FRL para el transporte de datos isocronicos (voz y video en tiempo real). No obstante, sería posible su soporte limitando el tamaño de los tramas y utilizando internacionalmente infraestructuras RDSI o ATM.

- Otro inconveniente es el mecanismo utilizado para el control de flujo muy simple pero obliga a disponer de unos amplios tamaños de ventana en ambos extremos de la red. Si hay congestión persistente, el único método viable es el de modificar el tamaño de la ventana dinámicamente según el estado de la red, para obtener la máxima eficacia y evitar congestiones severas.

IV.5.2 VENTAJAS

- La mayor ventaja de Frame Relay es que hace más eficiente el proceso de comunicación. La funcionabilidad del protocolo requerida en la interfaz usuario-red se reduce, así como el procesamiento interno de la red. Esto conlleva un menor retador y mayor rendimiento. El tiempo de proceso de la trama es del orden de la décima parte que en X.25.

- La velocidad de acceso puede alcanzar normalmente los 2 MBPS, frente a los 64 KBPS de X.25.

- La interfaz de usuario es sencilla y conlleva a una, relativamente simple migración desde X.25.

- Ahorro de costes. El acceso unificado a través del cual pueden enviar todos los tráficos de datos por un solo puerto de acceso que multiplexa los diferentes flujos de datos permiten la simplificación en la gestión de los servicios. Las aplicaciones relacionadas con las comunicaciones no necesitan realizar grandes cambios en la arquitectura de sus comunicaciones, gracias al bajo nivel de transparencia del FRL (nivel 2 del modelo OSI) que permite encapsular la mayoría de los protocolos existentes (IP, SDLC, IPX, etc.) (Figura 4.3). Diversos acuerdos internacionales garantizan tales encapsulamientos.

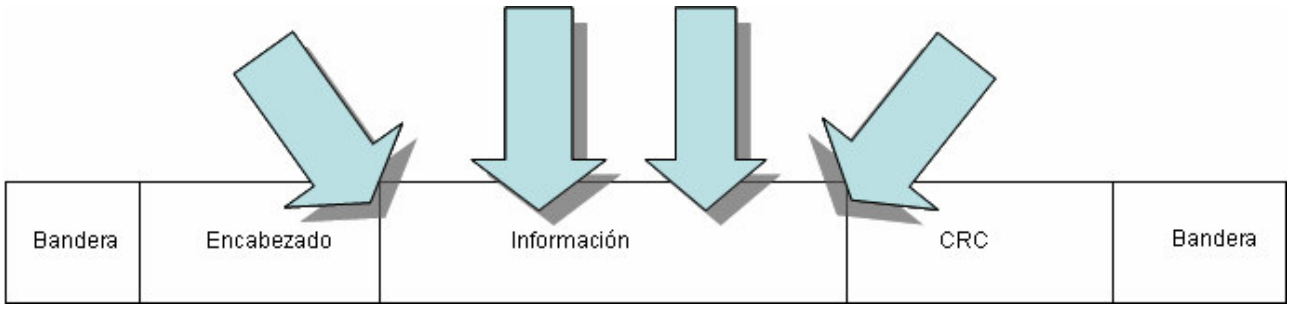


FIGURA 4.3 ENCAPSULAMIENTOS DE DIFERENTES PROTOCOLOS

También las operadoras pueden incrementar el rendimiento de sus instalaciones gracias a la posibilidad de poder ofrecer un volumen de tráfico muy superior al que realmente pueden soportar. Esta afirmación, casi una paradoja, esta basada en la presunción estadística de que la probabilidad de que todos los usuarios empiecen a transmitir simultáneamente son muy pequeños. Aun en el caso de que esto ocurriese y se llegará a un estado de congestión, la red dispone de mecanismos estandarizados para gestionarla.

- Eficiencia en el uso del ancho de banda. Los usuarios FRL disponen de ciertas calidades de servicio a veces inéditas en las actuales redes de comunicaciones. Facilidades como posibilidad de acomodar tráfico o ráfagas, tan común en nuestros días, o contratar un CIR apropiado a sus necesidades o disponer de un solo puerto de acceso que multiplexe los diferentes flujos de datos.

IV.6 ARQUITECTURA FRAME RELAY

Al igual que en otras arquitecturas de comunicaciones, los planos de una arquitectura Frame Relay, representados en la Figura 4.4 son:

- Plano de Control (Plano C), cuyas funciones esta la señalización y el establecimiento y liberación de las conexiones.

- Plano de Usuario (Plano U), cuya función es la transferencia de información entre usuarios.

- Plano de Gestión (Plano G), cuya misión es el control y la gestión de las operaciones de la red, y puede dividirse en gestión de planos y gestión de capas.

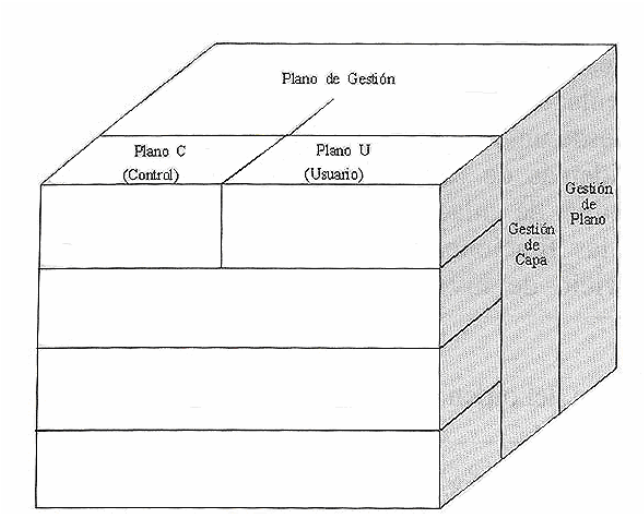


FIGURA 4.4 MODELO DE REFENCIA DE PROTOCOLOS

En la actualidad, para la transmisión de información entre usuarios finales, el protocolo utilizado en el plano de usuario es el Q.922, una nueva recomendación, versión adaptada del protocolo LAP-D. Frame Relay sólo utiliza las funciones consideradas esenciales de este protocolo:

- Delimitación, alineación y transparencia de tramas.
- Múltiplexación y demultiplexacion de tramas utilizando el campo de dirección.
- Inspección de la trama para asegurar que esta formada por un número entero de octetos antes de la inserción de un bit o después de la extracción de un bit cero.
- Inspección de la trama para comprobar que no es demasiado corta o demasiado larga.
- Detección de la transmisión de errores.
- Funciones de control de congestión.

Todas las funciones anteriores se encontraban ya en el estándar I.441/Q.921 (LAP-D), anterior al Q.922, a excepción de la última. También hay diferencias en los campos de dirección de las tramas.

Estas funciones centrales de Q.922 en el plano de usuario constituyen un subnivel del enlace. Proporcionan los servicios mínimos para la transmisión de las tramas de enlace desde un usuario a otro, sin tener en cuenta el control de flujo o el control de errores. Además de esto, el usuario puede elegir funciones adicionales extremo a extremo a nivel de enlace o de red, que no forman parte del servicio RDSI ofrecido. Basado en las funciones centrales (core), RDSI ofrece retransmisión de tramas como un servicio de nivel dos, orientado a conexión, con las siguientes propiedades:

- Preservación del orden de las tramas transmitidas desde un extremo de la red al otro.

- Tramas no duplicadas.

- Pequeña probabilidad de pérdida de tramas.

En el plano de control, Q.922 proporciona un servicio de control de enlace de datos fiable, con control de errores y de flujo, a los mensajes de control de llamada I.451/Q.931 (que son también utilizados en RDSI).

Los niveles de protocolo de los Planos U y C se representan en la figura 4.5

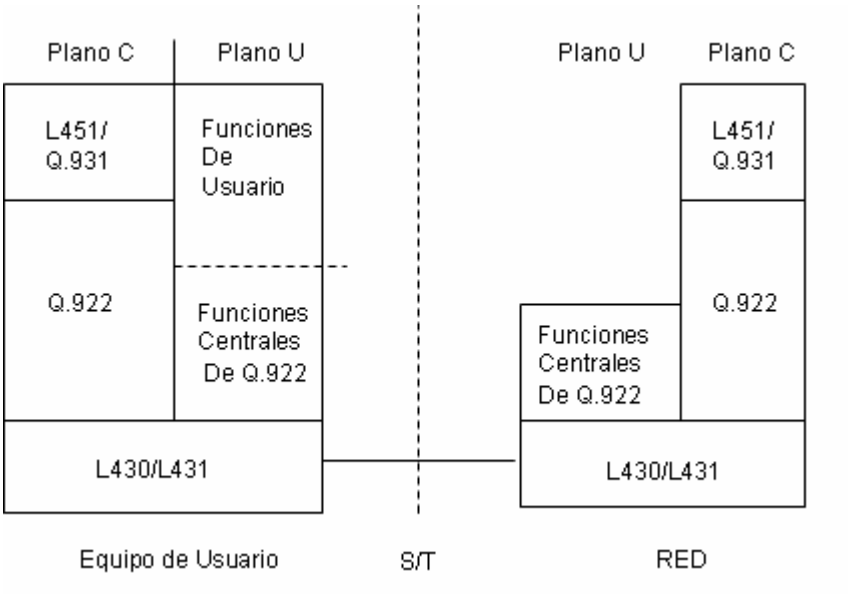


FIGURA 4.5 NIVELES DE PROTOCOLO FRAME RELAY

Esta arquitectura reduce al mínimo el trabajo a realizar por la red. Los datos de usuario se transmiten en tramas que prácticamente no son procesadas por los nodos intermedios de la red, a excepción hecha de la detección de errores y el encaminamiento en base al identificador de conexión. El proceso es como sigue: Cuando una trama llega a un nodo, este automáticamente la envía a su destino una vez analizada la cabecera ¿Qué ocurre si se produce un error? Sencillamente se interrumpe la transmisión. Si la trama esta todavía en la red, los nodos se encargan de eliminarla; si hubiera llegado a su destino; es el DTE el que; mediante los protocolos de nivel superior, se encarga de solicitar la retransmisión. La figura 4.6 compara la arquitectura Frame Relay con la X.25.

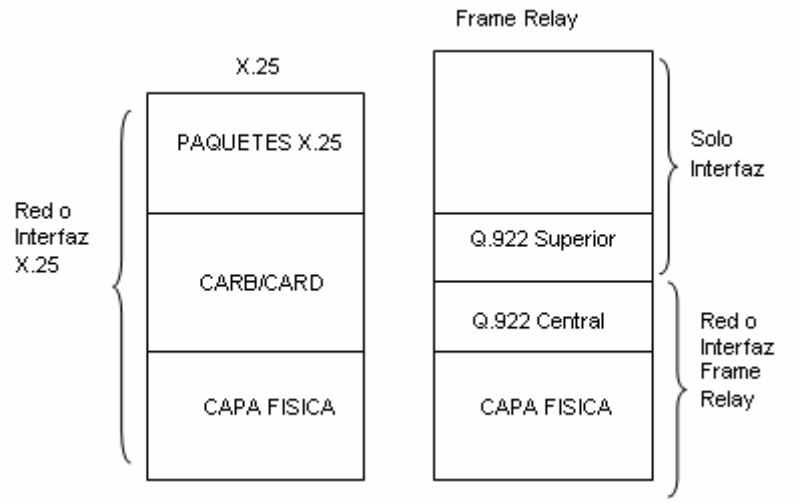


FIGURA 4.6 COMPARACION DE FRAME RELAY Y X.25

Frame Relay se concibió originalmente como un servicio opcional de RDSI. El usuario envía tramas al nodo de la red sobre un canal B, H o D y estas tramas se pasan al usuario de destino a través de la red. Sin embargo, las implementaciones reales de Frame Relay suelen ser independientes de RDSI. En este caso se utiliza el concepto de Frame Relay cuando la red proporciona interfaces Frame Relay a los usuarios. Internamente la red puede utilizar técnicas Frame Relay para la transmisión entre sus nodos y de hecho se están desarrollando estándares para este fin. Sin embargo, la transferencia interna dentro de la red puede ser de otro tipo, incluso X.25.

En la figura 4.7, se representan varias posibles situaciones de operación de Frame Relay. En las figuras 4.7 a) y 4.7 b) el acceso a Frame Relay es a través de RDSI. En 4.7 c) la red proporciona interfaces Frame Relay a los DTE. En definitiva, una pared Frame Relay, es un sentido amplio, es una red que proporciona al usuario una interfaz FR y que provee los servicios necesarios para soportar una comunicación entre interfaces FR.

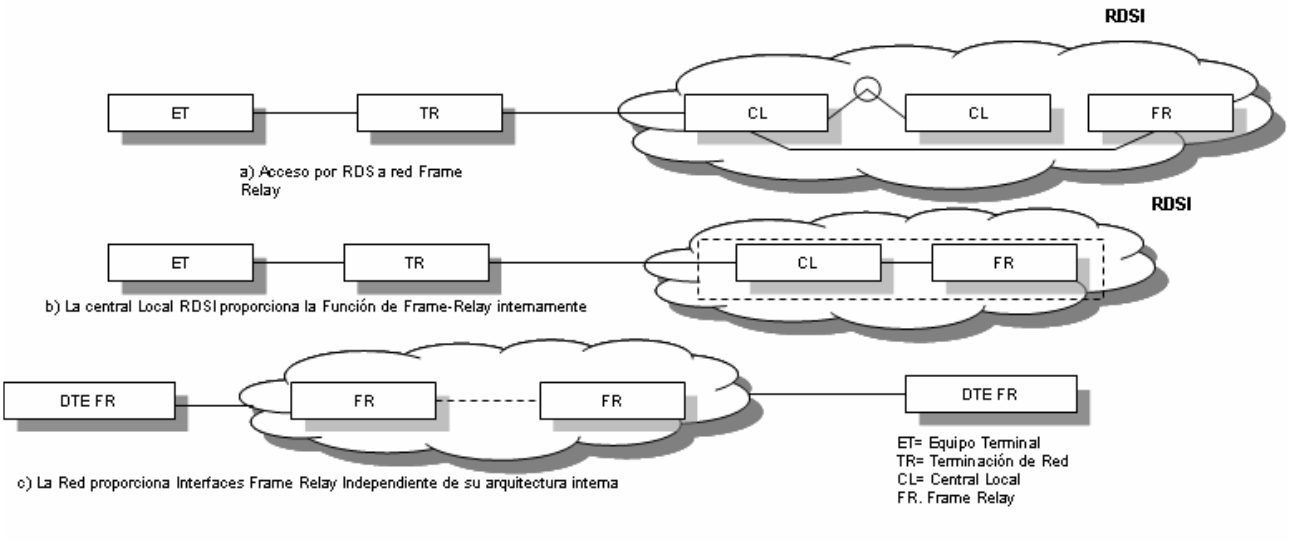


FIGURA 4.7 a), b) y c) UTILIZACIONES DE FRAME RELAY

Un ejemplo característico es la Red Iberpac española. Originalmente toda la arquitectura estaba basada en la Recomendación X.25 y X.75 para transferencias internas. En la actualidad facilita a los usuarios, interfaces X.25 y FR (aparte de EDP para terminales modo caracter). La estructura interna combina arquitecturas X.25, FR y ATM en función de las necesidades de trafico y CdS (véase figura 4.8).

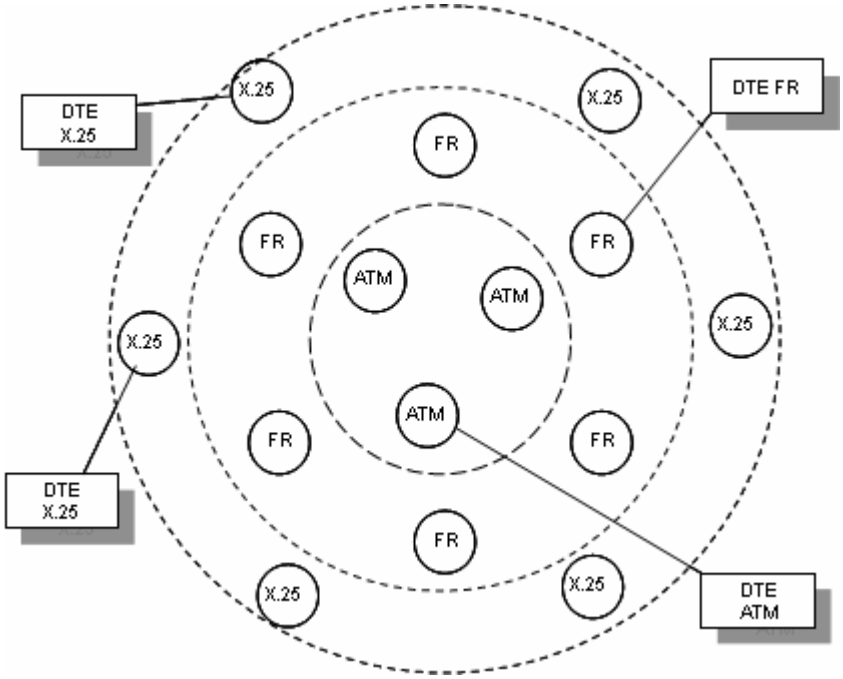


FIGURA 4.8 VISION ESQUEMATICA DE RED DE ARQUITECTURA MIXTA (INTERNA Y EXTERNA) X.25, FR Y ATM

IV.7 LOS CIRCUITOS VIRTUALES DE FRAME RELAY

Frame Relay proporciona Comunicacion de conexión Orientada en la capa de enlace de datos. Este significa que una conexión definida existe entre cada par de estas conexiones son asociadas con un identificador de conexión. Este servicio es implementado por un Circuito Virtual de Frame Relay, en el cual es una conexión lógica creada entre dos dispositivos el Equipo Terminal de Datos (DTE) a través de una red de conmutación de paquetes Frame Relay (PSN).

Los Circuitos Virtuales proporcionan una ruta de comunicacion bidireccional del dispositivo del uno de los dispositivos DTE para otro y son identificadores únicos para el Identificador de Conexión de Enlace de Datos (Data-Link Connection Identifier [DLCI]). Un número de circuitos virtuales pueden ser multiplexados dentro de un circuito físico para la transmisión a través de la red. Esta capacidad frecuentemente puede reducir el equipo y la red compleja requerida para conectar múltiples dispositivos DTE.

Un circuito virtual puede pasar a través de cualquier número de dispositivos DCE intermedios (switches) ubicados dentro de la PSN de Frame Relay.

Los Circuitos Virtuales de Frame Relay caen dentro de dos categorías: Los Circuitos Virtuales Conmutados (Switched Virtual Circuits [SVCs]) y los Circuitos Virtuales Permanentes (Permanent Virtual Circuits [PVCs]).

IV.7.1 CIRCUITOS VIRTUALES CONMUTADOS

Los Circuitos Virtuales Conmutados (Switched virtual circuits [SVCs]) son conexiones temporales usadas en situaciones requeridas solamente esporádicamente en la transferencia de datos entre los dispositivos DTE a través de la red Frame Relay. Una sesión de comunicación a través de un SVC consiste de los siguientes 4 estados operacionales:

- **Configuración de Llamada (call setup)** — El Circuito Virtual entre los dos dispositivos DTE de Frame Relay es establecido.

- **Transferencia de Datos (Data transfer)** — Los datos transmitidos entre los dispositivos DTE sobre el Circuito Virtual.

- **Ocupado (Idle)** — La conexión entre los dispositivos DTE esta todavía activos, pero no los datos entran transferidos. Si un SVC permanece en un estado ocupado (idle) para un periodo definido de tiempo, la llamada puede ser terminada.

- **Termino de Llamada** (**Call termination)** — El Circuito Virtual entre los dispositivos DTE es terminado.

Después de que el Circuito Virtual es terminado, los dispositivos DTE deben establecer un nuevo SVC si hay un dato adicional para ser intercambiado. Estos esperan que los SVCs sean establecidos, manteniendo, terminando de usar la misma señalización de protocolos usada en RDSI.

Algunos constructores de equipo DCE de Frame Relay soportan las conexiones que Circuitos Virtuales Conmutados. Por lo que, sus actuales desplegados son mínimos en las red Frame Relay, hoy en día. Previamente no es ampliamente soportado los equipos Frame Relay, los SVCs son ahora la norma. Las compañías han encontrado que los SVCs ahorran dinero en el extremo del circuito por que no esta abierto todo el tiempo.

IV.7.2 CIRCUITOS VIRTUALES PERMANENTES

Circuitos Virtuales Permanentes [Permanent virtual circuits (PVCs)] son permanentes conexiones establecidas que son usadas para que frecuentemente y consistentemente los datos transferidos entre los dispositivos DTE a través de la red Frame Relay. La Comunicacion a través de un PVC no requiere la configuración de llamada (call setup) y los estados de terminación son usados con SVCs. PVCs siempre opera uno de los dos siguientes estados operacionales:

- **Transferencia de Datos** (**Data transfer)** — Los datos son transmitidos entre los dispositivos DTE sobre el Cicuito Virtual.

• **Ocupado** (**Idle)** — La conexión entre los dispositivos DTE esta activa, pero no los datos transferidos. A diferencia de los SVCs, los PVCs no serán terminados bajo algunas circunstancias cuando estén en estado ocupado (idle).

Los dispositivos DTE pueden empezar a transferir datos siempre y cuando estén listos por que el circuito esta permanentemente establecido.

IV.8 FUNCIONAMIENTO DE LA RED

La función de retransmisión de tramas realizada por Frame Relay consiste en el encaminamiento de las tramas, antes descritas, de acuerdo a los valores de sus DLCI.

Por lo general, el encaminamiento es controlado mediante las entradas de una tabla de conexión que utiliza DLCI. El manejador conmuta las tramas de un canal de entrada a otro de salida mediante la apropiada entrada de la tabla de conexión y traduce DLCI de la trama antes de la transmisión.

Hay que reseñar que todas las terminales finales tiene una conexión lógica con valor DLCI=0, que esta reservada par el control de llamadas. Esto se utiliza cuando en el canal D no se usa I.451/Q.931 para el control de llamadas.

Como parte de la función de retransmisión de tramas, se verifica el campo FCS de cada trama. Si se detecta un error, la trama simplemente se descarta, siendo responsabilidad de los usuarios finales la recuperación de este error.

La figura 4.9 es otra forma de ver los protocolos implicados en Frame Relay desde el punto de vista de sus conexiones individuales. Hay un nivel físico y un subnivel de Frame Relay comunes. Se puede incluir sobre este subnivel un protocolo de control de enlace de datos a nivel dos. Esta elección depende de la aplicaciones y puede variar en las distintas conexiones Frame Relay (DLCI i). Si los mensajes de control de llamadas se mandan en tramas Frame Relay, estas tramas se envían en el DLCI 0, que proporciona una conexión Frame Relay entre el usuario y el manejador de tramas. El DLCI 8191 esta dedicado a posprocedimientos de gestión.

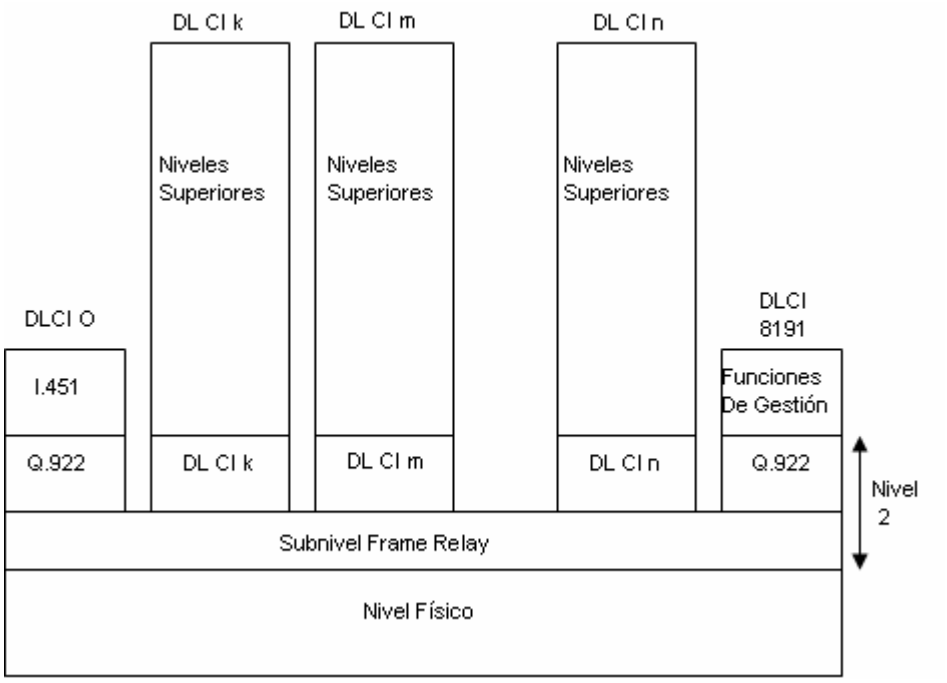


FIGURA 4.9 MULTIPLEXACION EN FRAME RELAY

En la figura 4.10 se representa la operación de FR. Se supone que hay un circuito físico entre DTE y el nodo de la red. Este circuito multiplexa varios circuitos virtuales permanentes (PVC), identificados por su DLCI.

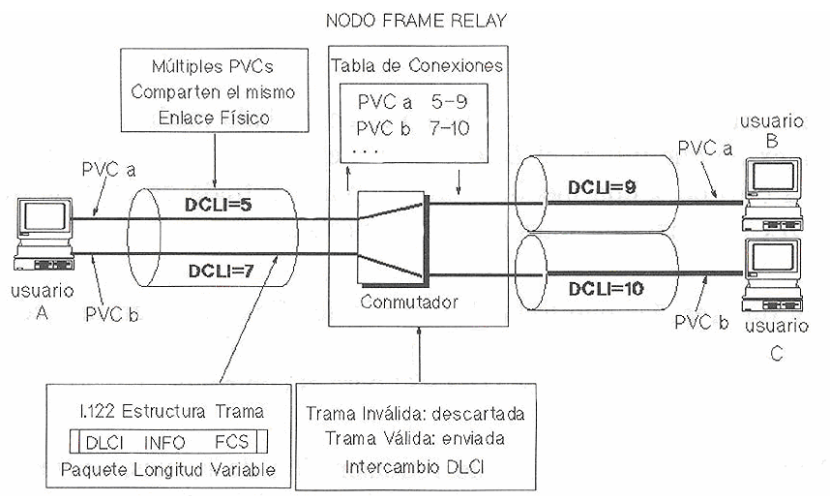


FIGURA 4.10 OPERACIÓN DE FRAME RELAY

Supongamos que el usuario A desea comunicarse con el usuario B. Primero deberá asegurase que dispone de un circuito virtual (CV) en ambos usuarios. La información, antes de ser entregada a la red, deberá ser segmentada en tramas a las que le añade un identificador común llamado DLCI. Ya que n la red las tramas son conmutadas de acuerdo con las tablas de encaminamiento que asocian cada DLCI de entrada con un puerto de salida y un nuevo DLCI, hasta que llegan a su destino donde

son de nuevo ensambladas. Es obvio que estos identificadores solo tienen significado dentro del contexto de cada enlace; ya que van siendo sustituidos a lo largo de todo el circuito virtual.

IV.9 CONTROL DE CONGESTION

A continuación se dará los conceptos del control de congestión que se lleva a cabo en Frame Relay.

IV.9.1 CONCEPTOS BÁSICOS DE CONTROL DE CONGESTIÓN

Una red Frame Relay es una red de conmutación de paquetes en la que los "paquetes" son tramas de nivel 2. Como cualquier red de conmutación de paquetes, una de las áreas clave en el diseño de una red Frame Relay es el control de congestión. Para entender algunos términos relacionados con el control de congestión, debemos acudir a algunos resultados de la teoría de colas. Básicamente, una red Frame Relay es una red de colas. En cada manejador, hay una cola de tramas por cada enlace de salida. Si la velocidad de llegada de las tramas excede la velocidad de transmisión de las mismas, el tamaño de la cola crece sin límite y el retraso sufrido por una trama tiende a infinito. Incluso si la velocidad de llegada de las tramas es menor que la velocidad de transmisión, la longitud de la cola crecerá muy rápidamente a medida que la velocidad de llegada se aproxime a la velocidad de retransmisión.

En la figura 4.11 se representa la situación de las colas en un manejador de tramas o nodo Frame Relay.

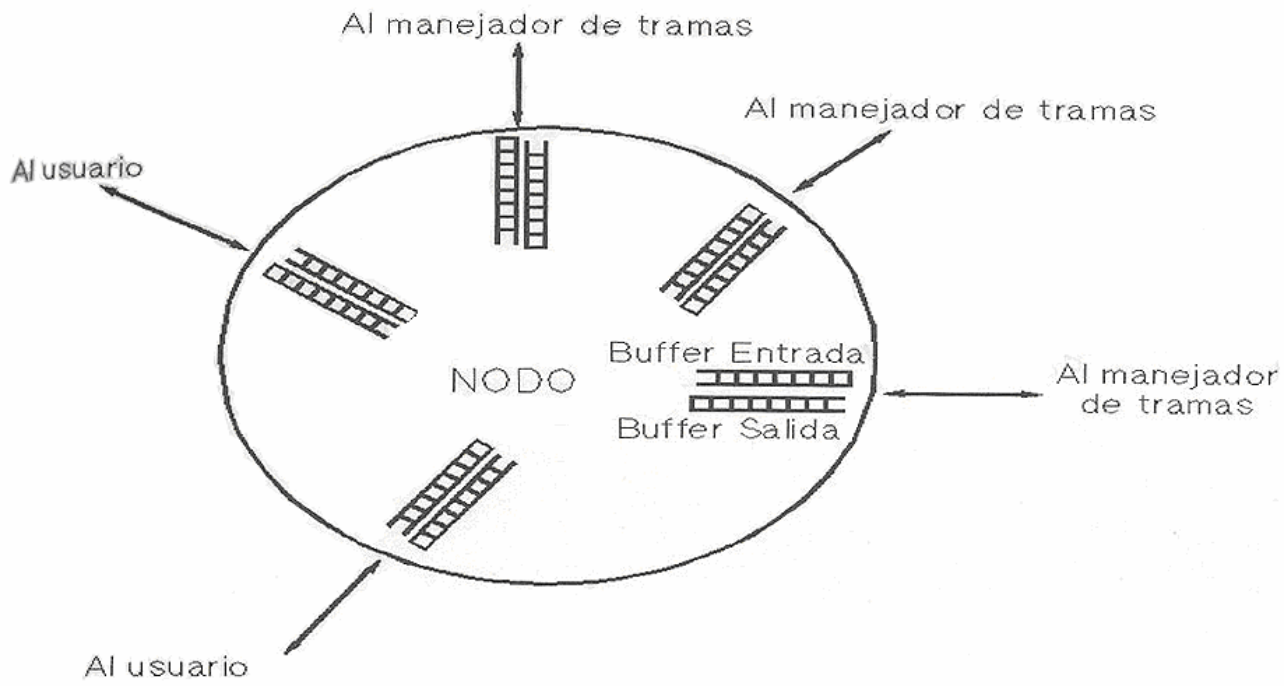


FIGURA 4.11 COLAS EN UN NODO FRAME RELAY

Cualquier manejador tiene conectado un determinado número de enlaces de transmisión a otros manejadores y directamente a usuarios finales. En cada enlace, las

tramas entran y salen. Pueden considerarse que hay dos búferes en cada enlace; uno que recibe las tramas que llegan y otro que guarda las tramas que están esperando ser transmitidas. Podemos imaginarnos cada enlace como dos búferes de tamaño variable, con la única limitación que la suma de sus tamaños debe ser siempre constante.

De cualquier manera, cuando llega una trama, se almacena en el buffer de entrada del enlace correspondiente. El manejador examina cada trama de entrada para tomar la decisión de encaminamiento y entonces mueve dicha trama al buffer de salida más apropiado. Las tramas encoladas para salir se transmiten rápidamente al manejador para que sea posible. Pero si las tramas llegan demasiado rápidamente al manejador para que este pueda procesarlas, o llegan más rápido de lo que parten las tramas de los buffers de salida, entonces habrá un momento en el que no dispondrá de memoria para nuevas tramas de entrada.

Cuando alcanza su punto de saturación, se puede adoptar dos estrategias. La primera consiste simplemente en descartar cualquier trama de entrada para la que no haya espacio en el buffer. Pero este método no es aconsejable, ya que las tramas descartadas deber ser transmitidas, aumentando de este modo la congestión de la red. La otra alternativa es utilizar algún mecanismo que limite la velocidad a la que las nuevas tramas entran a la red. Este procedimiento es realmente el conocido como control de congestión.

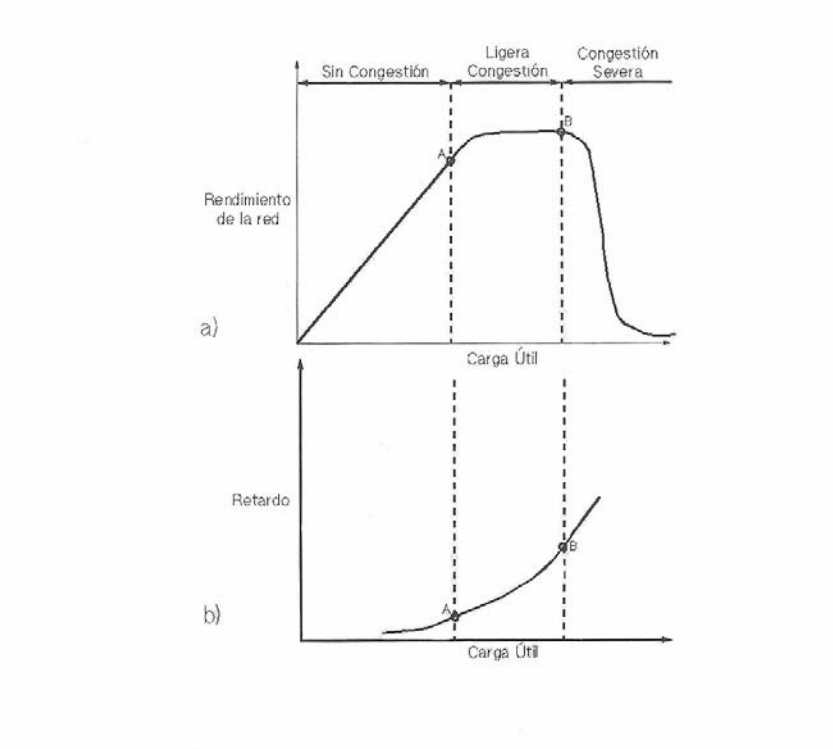


FIGURA 4.12 a) y b) ANALISIS DE CONGESTION.

La figura 4.12 a) y 4.12 b) muestran los efectos de la congestión en términos de generales. La primera muestra el rendimiento de una red (número de tramas transmitidas a la estación de destino por unidad de tiempo) frente a la carga ofrecida (número de tramas transmitidas por todos los abonados); mientras que la segunda presenta el retraso

medio a través de la red, desde la entrada a la salida. Con poca carga, el rendimiento aumenta proporcionalmente al aumento de la carga ofrecida. A medida que la carga va creciendo, se alcanza un punto (punto A en el gráfico) a partir del cual el rendimiento de la red crece más lentamente que el crecimiento de la carga ofrecida. Esto debido a que la red esta entrando en un estado de congestión ligera. En esta región, la red continúa encargándose de toda la carga aunque con retardos mayores.

A medida que la carga de la red aumenta, la longitud de las colas de los manejadores crece y se alcanza un punto (punto B en el grafico) más allá del cual el rendimiento disminuye a medida que aumenta la carga ofrecida. Esto es debido a que los buffers de cada manejador son de tamaño finito y cuando se llenan deben descartar tramas. Estas tramas deben ser retransmitidas por el origen, sumándose a las nuevas que entran en la red. Lo único que se consigue con este hecho es empeorar la situación; a medida que transmiten más tramas, la carga del sistema crece y se saturan más buffers. Incluso las tramas que mandan con éxito tienen que ser retransmitidas, por que el mensaje ACK tarda tanto tiempo en llegar que el origen asume que la trama no ha llegado al destino. Bajo estas circunstancias, la capacidad efectiva del sistema es virtualmente cero.

Es evidente que es necesario evitar este tipo de situaciones y, precisamente esa la misión del control de congestión. El objetivo de todas las técnicas de control de congestión es limitar la longitud de las colas en los manejadores de tramas para evitar el colapso del rendimiento.

IV.9.2 EL CONTROL DE CONGESTION EN FRAME RELAY

UIT-T, en la serie I.3xx, define los objetivos de control de congestión en Frame Relay de la siguiente manera:

- Minimizar el descarte de tramas.
- Mantener, con una probabilidad alta y mínima variación, la calidad de servicio acordada.
- Minimizar la posibilidad de que un usuario monopolice los recursos de la red a expensas de otros usuarios.
- Ser fácil de implementar y suponer poca carga para los usuarios finales de la red.
- Crear el menor tráfico adicional posible en la red.
- Distribuir los recursos de la red equitativamente entre los usuarios.
- Limitar la transmisión de la congestión a otras redes y elementos dentro de la red.
- Operar con efectividad, sin depender del flujo de tráfico, en cualquier dirección entre los usuario diferentes.

- Tener la mínima interacción con, ó impacto sobre, otros sistemas en la red Frame Relay.

- Minimizar la variación de la calidad del servicio debida a las conexiones Frame Relay individuales durante la congestión.

El control de congestión es especialmente importante en este tipo de redes. El protocolo Frame Relay esta orientado a conseguir el máximo rendimiento y eficacia. Esto tiene como consecuencia que los manejadores de tramas no puedan controlar el flujo que llegan de un abonado o de un manejador adyacente mediante el típico protocolo de ventana deslizante, como ocurre, por ejemplo en LAP-D.

El control de congestión es una responsabilidad compartida entre la red y los usuarios finales. La red es la mejor que puede monitorizar el grado de congestión, mientras que los usuarios son los que mejor pueden controlar esta congestión limitando el tráfico. Teniendo esto en cuenta, podemos considerar dos estrategias generales para el control de congestión:

- Los procedimientos para evitar la congestión se utilizan cuando esta se inicia, a fin de minimizar sus efectos sobre la red. Estos procedimientos se inician antes, o en el punto A en la figura 4.12 a), para evitar el tratamiento de la congestión que se produce en el punto B. Cerca del punto A, es difícil para el usuario final advertir que la congestión se esta incrementando, por lo que debe existir un mecanismo de señalización explícito en la red que dispare estos procedimientos.

- Los procedimientos de recuperación de la congestión se utilizan para prevenir el colapso de la red en la fase de congestión severa. Se inician generalmente cuando la red empieza a eliminar tramas debido a la congestión. Estas tramas sirven como un mecanismo de señalización implícito.

UIT-T y ANSI consideran estas dos estrategias como formas complementarias de control de congestión en el servicio portador de retransmisión de tramas.

IV.10 IDENTIFICADOR DE CONEXIÓN DEL ENLACE DE DATOS (DLCI)

Los Circuitos Virtuales de Frame Relay son identificados por los identificadores de conexión del enlace de datos (***data-link connection identifiers [DLCIs]***. Los valores de DLCI típicamente son asignados por el proveedor de servicio de Frame Relay (por ejemplo. La compañía telefónica).

Los DLCIs de Frame Relay tienen un significativo local, el cual indica que sus valores son únicos en la LAN, pero no necesariamente en la WAN de Frame Relay.

Se puede configurar en dos diferentes dispositivos DTE pueden ser asignados el mismo valor de DLCI dentro de una red WAN de Frame Relay. La figura 4.13 A ilustra un solo Circuito Virtual de Frame Relay puede ser asignados diferentes DLCIs en cada final de un VC.

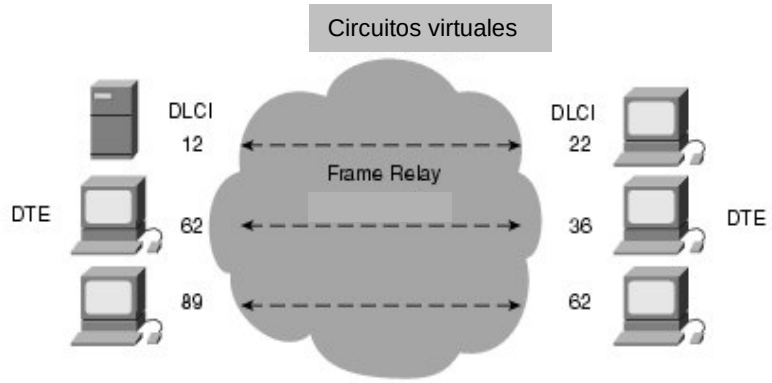


FIGURA 4.13. CIRCUITOS VIRTUALES CON DIFERENTES DLCI

IV.11 IMPLEMENTACION DE LA RED FRAME RELAY

Una implementación de red Frame Relay privada común es para un equipo multiplexor T1 o E1 con ambas interfaces Frame Relay y NO Frame Relay. El trafico Frame Relay es enviado hacia fuera de la interfaz Frame Relay y sobre la red de datos. El trafico NO Frame Relay es enviado a la aplicación apropiada o servicio, tal como un Conmutador (private branch exchange [PBX]) para servicio de telefonía o para la aplicación de video-teleconferencia.

Una red típica de Frame Relay consiste de un número de dispositivos DTE, tal como los Ruteadores, conectados a los puertos remotos en un equipo multiplexor vía un servicio tradicional punto a punto tal como circuitos T1, T1 fraccional o 56K o E1, o E1 fraccional y 64 K. Un ejemplo de una simple red Frame Relay es mostrada en la Figura 4.13.

Pero en la figura 4.14. Una red simple de Frame Relay de varias conexiones de dispositivos a diferentes servicios sobre una WAN.

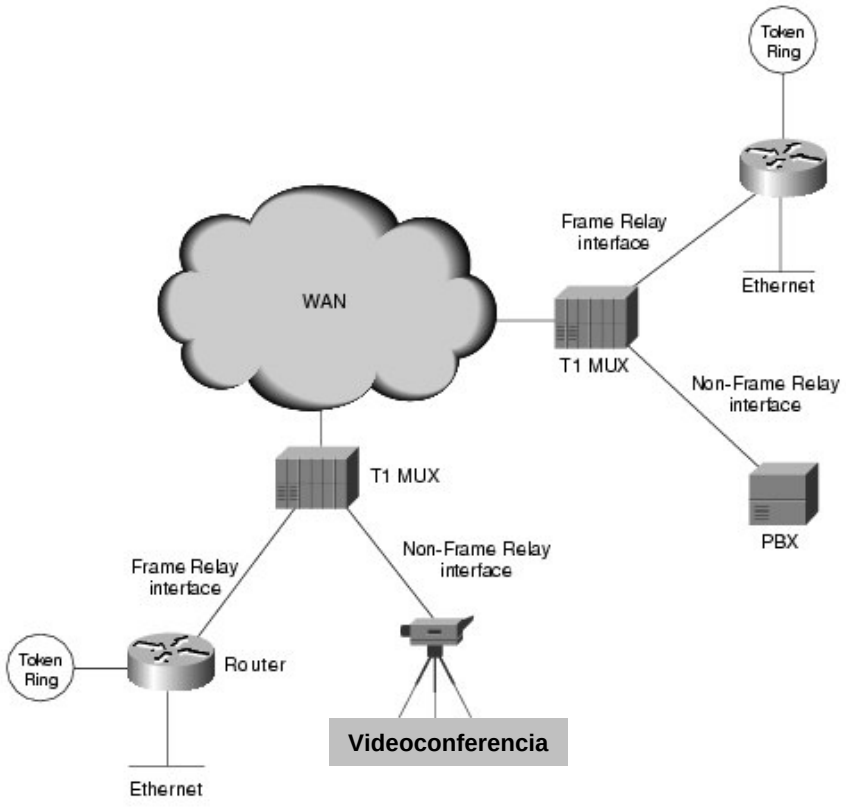


FIGURA 4.14 RED SIMPLE DE FRAME RELAY DE VARIAS CONEXIONES DE DISPOSITIVOS

La mayoría de las redes Frame Relay despliegan hoy en día son proporcionadas por proveedores de servicio que intentan ofrecer servicios de transmisión hacia sus clientes. Esto es frecuentemente referido como un servicio publico de Frame Relay. Frame Relay es implementado en ambas redes como las proporcionadas de portadora pública y las redes privadas. En la siguiente sección examina 2 metodologías para desplegar Frame Relay.

IV.12 LAS REDES QUE PROPORCIONAN PORTADORAS PÚBLICAS

En las redes que proporcionan portadoras públicas de Frame Relay, el equipo de conmutación Frame Relay es localizado en las oficinas centrales de una portadora de telecomunicaciones. Los subscriptores son cargados en base al uso de sus redes pero son revelados en los equipos y servicios de administración y mantenimiento de la red Frame relay

Generalmente, el equipo DCE también es dueño por el proveedor de Telecomunicaciones. El equipo DTE podría ser propiedad del cliente o podría ser propiedad del proveedor de telecomunicaciones como un servicio para el cliente. La mayoría de las redes Frame Relay hoy en día son redes públicas de Frame Relay que proporcionan la portadora.

IV.13 REDES PRIVADAS DE FRAME FRAME RELAY PARA EMPRESAS

Es más frecuente, a lo largo del mundo las organizaciones son desplegadas por redes privadas de Frame Relay. En las redes privadas de Frame Relay, la administración y mantenimiento de la red son responsabilidades de la empresa (una compañía privada). Todos los equipos, incluye el equipo de conmutación, es propiedad del cliente.

IV.14 FORMATOS DE LA TRAMA DE FRAME RELAY

Para entender mucho de la funcionabilidad de Frame Relay, será de gran ayuda entender la estructura de la trama de Frame Relay. En las siguientes secciones se describirán el formato básico de la trama de Frame Relay, y la versión de LMI de la trama de Frame Relay.

IV.14.1 FORMATO ESTÁNDAR DE LA TRAMA DE FRAME RELAY

El formato de trama, como se muestra la figura 4.15, es similar al de otros protocolos de nivel 2 como LAP-D y LAP-B, con una diferencia fundamental, en este caso no hay campo de control.

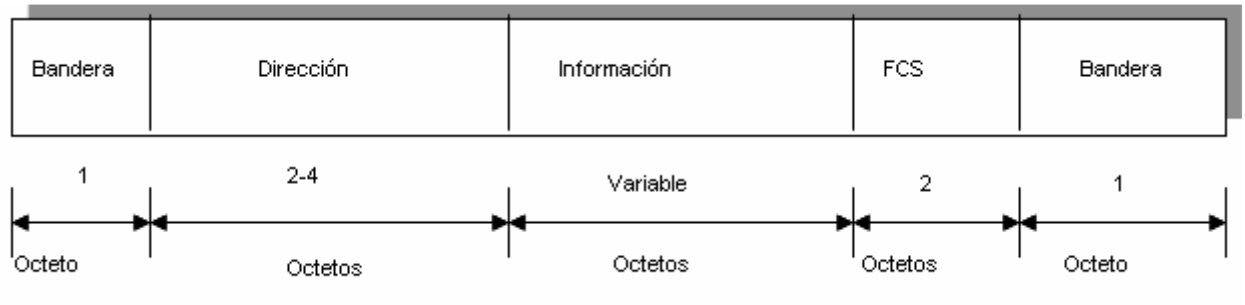


FIGURA 4.15 FORMATO DE TRAMA

Esto se supone que:

- ✓ Solo existe un tipo de trama, utilizada para transmitir información de usuario.
- ✓ No se puede utilizar señalización dentro de banda; una conexión lógica solo puede transmitir datos de usuario.
- ✓ Tampoco existen tramas que permitan a la red ejecutar control de flujo, enviar ACK's o pedir retransmisiones, ya que no hay número de secuencia.

Todas estas funciones deben ser implementadas en los equipos terminales tales como encaminadores, puentes o controladores de comunicaciones, que deberán disponer de los mecanismos necesarios para el secuenciamiento, el control de flujo, el envío de reconocimientos y la recuperación de errores, que permitan garantizar la integridad de los datos transmitidos.

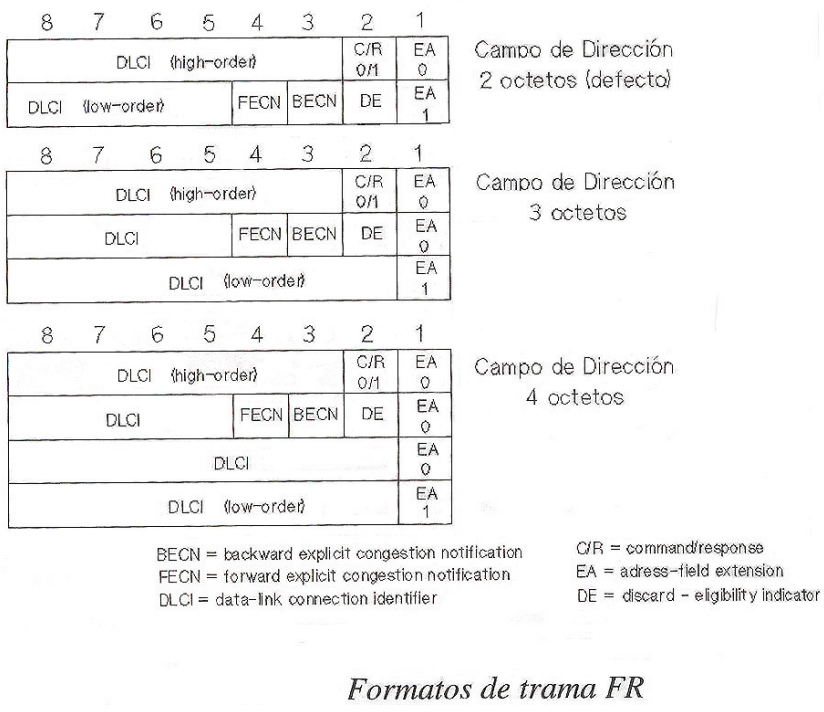
- ✓ La red detecta pero no recupera errores; los nodos de la red tienen capacidad de detectar errores y en determinados casos de eliminar tramas, pero nunca recuperarlos.

A continuación se describen uno por uno los distintos campos que componen la trama:

- **Bandera (Flag):** Este campo funciona igual que en los protocolos LAP-D y LAP-B. Todas las tramas comienzan y terminan con la secuencia de bits 01111110. Para garantizar la transparencia de la información, el nivel de enlace que va a transmitir la trama de Frame Relay debe encargarse de comprobar el contenido de la trama entre el delimitador de apertura y cierre e insertar un bit 0 cada vez que aparezca una secuencia de cinco bits 1 consecutivos. Por su parte el nivel de enlace de la entidad receptora se encargara de eliminar dichos bits una vez que obtenga los datos de la trama comprendidos entre ambos delimitadores.

- **Dirección (Address)**: El campo de dirección esta formado por defecto por dos octetos, pero puede extenderse hasta tres o cuatro. Los posibles formatos de este campo se muestran en la figura 4.16.

Mantiene un identificador de conexión de enlace de datos (DLCI) de 10, 17 o 24 bits, que desempeña la misma función que el número de circuito virtual en X.25. Permite multiplexar múltiples conexiones lógicas Frame Relay sobre un único canal. Como en X.25 el identificador de conexión tiene un significado puramente local; cada parte final de la conexión lógica asigna su propio DLCI, tomando de un conjunto de números locales no utilizados, y la red se encarga de establecer su correspondencia.



Formatos de trama FR

FIGURA 4.16 FORMATOS DE TRAMA FRAME RELAY

Para Frame Relay en el canal D, se asume un campo de dirección de dos octetos, y los valores de DLCI están limitados al rango 480-1.007. Esto equivale a un SAPI (Identificador de SAP, Punto de Acceso al Servicio) de 32-62. Así que las tramas Frame Relay pueden multiplexarse con las tramas LAP-D en el cual D, distinguiéndose por los bits 8 al 3 del primer octeto del campo de dirección.

La longitud del campo de dirección, y por lo tanto del DLCI, esta definida por el campo EA (Extended Ardes), que indica si el campo de dirección continua en el siguiente octeto (1) o ha terminado (0). El campo C/R es de uso especifico en cada aplicación y el protocolo estándar Frame Relay no lo utiliza. El resto de los bits de este campo están relacionados con el control de congestión que tratara más tarde en este capitulo.

- **Información**. El campo de información transmite datos del nivel superior. Si el usuario elige implementar funciones adicionales de control del nivel de enlace extremo a extremo, entonces en este campo encontraremos una trama de enlace de datos. Por ejemplo, una elección muy normal será utilizar el protocolo LAP-D mejorando (Q.922) para realizar funciones adicionales a las que proporciona el estándar. En este caso, la trama entera LAP-D se transmitiría en el campo de información.

- **FCS (Frame-Check Sequence):** Es una secuencia de 16 bits que permite verificar la correcta transmisión de la trama y la futura recuperación de posibles errores en la misma. Su funcionamiento es el mismo que en los protocolos LAPD y LAPB.

IV.14.2 FORMATO DE TRAMA LMI

Tramas de Frame Relay que conforman a las especificaciones que consisten de los campos ilustrados en la Figura 4.17.

FIGURA 4.17 NUEVE CAMPOS QUE COMPRENDEN A FRAME RELAY QUE CONFORMAN EL FORMATO LMI

Las siguientes descripciones resumen los campos ilustrados en la Figura 4.16.

- **Bandera**—Delimita el comienzo y el término de la trama.

- **LMI DLCI**— Identifica la trama como una trama LMI en lugar de una trama básica de Frame Relay. El valor DLCI del especifico LMI definido en la especificación del consorcio LMI es el DLCI = 1023.

- **Indicador de Información no-numerado**— Pone el bit de la lista final a cero.

- **Protocolo Discriminador**— Siempre contiene un valor indicativo que la trama es una trama LMI.

- **Referencia de Llamada**— Siempre contiene ceros, este campo actualmente no es usado para algún propósito.

- **Tipo de mensaje**— Etiquetas de la trama como son los siguientes tipos de mensajes:

  – **Mensaje de búsqueda de estado**— Permite un dispositivo de usuario pueda investigar acerca del estado de la red.

  – **Mensaje de estado**— Responde a los mensajes de interrogación de estado. Los mensajes de estado incluye los “keepalives” y los mensajes de estado del PVC.

- **Elementos de Información**— Contiene un número variable de los elementos de la información Individual (IEs). El IEs consiste de los siguientes campos:

  – **Identificador IE** — Únicamente identifica el IE.

  – **Longitud de IE** — Indica la longitud del IE.

– **Datos**— Consiste de 1 ó más bytes que contienen la encapsulación de datos de capa superior.

• **Secuencia de Verificación de Trama (FCS)** — Asegura la integridad de los datos transmitidos.

IV.15 ADMINISTRACION DEL SISTEMA

La administración de una red Frame Relay implica tanto una administración interna como la interfaz del usuario de la red. Esta responsabilidad ha sido distribuida entre diferentes protocolos, esta administración incluye los siguientes aspectos:

- Administración de los parámetros de servicio de usuarios suscritos.
- Administración del ancho de Banda
- Administración de la congestión
- Ruteo de datos a través de la red.

IV.15.1 PARÁMETROS DE SERVICIO

Los parámetros de servicio determinan los procedimientos que realizan el conmutador Frame Relay para colocar, controlar y administrar el Ancho de Banda, la congestión y el ruteo para cada PLL dado.

El cliente o usuario suscribe los parámetros para cada PLL definidos en el lado de acceso a la red. Los parámetros del usuario y los parámetros de la red deberán corresponder entre sí. Dichos parámetros se mencionan a continuación.

IV.15.1.1 CIR

El parámetro CIR (Committed Information Rate; Tasa de Información Comprometida) representa la cantidad de información (expresada en bit por segundo) configurada para que el dispositivo del usuario transmita su información a través de la línea de Acceso de Frame Relay. El valor CIR tendrá que ser menor a la capacidad de transmisión de la línea de Acceso y de la línea Troncal, para lo cual se tendrá que asignar un valor CIR para un PLL de entrada y otro un PLL de salida.

IV.15.1.2 BC

El parámetro BC (Committed Bursa Size: Tamaño de Ráfaga Comprometida) define la cantidad máxima de datos de usuario que la red pondrá transmitir bajo condiciones normales en un tiempo determinado (TC). Este lapso no es asignado por el usuario y solo es una medida del tiempo en que el dispositivo del usuario utiliza el Ancho de Banda en relación al resto de los dispositivos. De esta manera, se desprende la siguiente fórmula que relaciona a los parámetros CIR, BC y TC.

TC= BC/CIR

BE

El parámetro BE (Excess Burts Size: Tamaño de Ráfaga Excedida) especifica la máxima cantidad de datos que el usuario de la red podrá transmitir en condiciones no especificadas. Lo anterior significa que el usuario podría transmitir una cantidad “extra” de información hacia la red Frame Relay es un momento en el que el tráfico de la red lo permita. El parámetro BE representa dicha cantidad “extra”.

Las redes Frame Relay pueden usar esta noción de velocidad para implementar una “velocidad forzada” hacia la interfaz de usuario. La velocidad forzada significa que la tramas en exceso del CIR serán transmitidas solamente si el Ancho de Banda esta disponible y descartado si este es insuficiente.

El bit DE es puesto en tramas de baja prioridad, de esta manera, son descartadas en primer término en caso de tramas perdidas. El bit DE es puesto por la red Frame Relay en algunas tramas recibidas con valor CIR alto; a dichas tramas se les asigna un valor de baja prioridad. El bit DE puede también ser puesto en el equipo del usuario final si este es capaz de reconocer que algunas tramas son más importantes que otras.

IV.15.2 ADMINISTRACION DE ANCHO DE BANDA

La distribución del Ancho de Banda es una función muy importante en la administración de la red. La red regula el flujo de datos entrantes para asegurar que el Ancho de Banda que requieran estos no exceda a la capacidad de la red. Los enlaces lógicos son establecidos basándose en la capacidad disponible tanto en la Troncal como la línea de Acceso. Las reglas y consideraciones que sigue la red en la administración son:

- La cantidad de bits asignada al parámetro BC en el tiempo TC es transmitida de manera transparente.

- La cantidad de bits excedente del parámetro BC y menor a la cantidad asignada al parámetro BE durante el tiempo TC es transmitida como una trama susceptible a ser descartada en caso de congestión.

- La cantidad de bits excedente de los parámetros BC y BE será descartada.

- Cualquier trama con el bit DE puesto en 1 será considerada por la red como susceptible a ser descartada.

IV.15.3 MECANISMOS DE CONTROL DE CONGESTIÓN

Frame Relay reduce el sobre encabezado de la red por la implementación de simples mecanismos de notificación de control de congestión más que al explícito flujo de control por circuito virtual. Frame Relay típicamente esta implementado en el medio de la

red segura, entonces la integridad de los datos no son sacrificados por que el control de flujo, pueden ser dejados a los protocolos de capas más altas. Frame Relay implementa dos mecanismos de notificación de congestión:

- Notificación de Congestión Explicita de Envíos (Forward-explicit congestion notification [FECN])

- Notificación de Congestión Explicita Retrasada (Backward explicit congestion notification [BECN])

Cada FECN y cada BECN son controlados por un solo bit contenido en la trama del encabezado de Frame Relay. El encabezado de la trama de Frame Relay también contiene un bit de Elegibilidad de Descarte (Discard Eligibility [DE]), el cual es usado para identificar el tráfico menos importante que puede ser tirado durante los periodos de congestión.

El bit de ***FECN*** es parte del campo de dirección en el encabezado de la trama de Frame Relay. El mecanismo de FECN es iniciado cuando un dispositivo DTE envía tramas de Frame Relay dentro de la red. Si la red esta congestionada, los dispositivos DCE (conmutadores [switches]) ponen el valor del bit de la trama de FECN a 1. Cuando las tramas alcanzan el destino del dispositivo DTE, el campo de dirección (con el bit FECN puesto) indica que la trama experimenta una congestión en la ruta de la fuente al destino. EL dispositivo DTE puede revelar esta información a los protocolos de capas más altas para el procesamiento. Dependiendo de la implementación, el control de flujo puede ser inicializado, o la indicación puede ser ignorada.

EL bit ***BECN*** es parte del campo de la dirección en el encabezado de la trama de Frame Relay. Los dispositivos DCE ponen el valor del bit BECN a 1 en la tramas viajando en dirección opuesta de la tramas con sus bits FECN puestos. Esto informa que el dispositivo DTE recibido en una particular ruta a través de la red congestionada. El dispositivo DTE puede entonces revelar esta información a los protocolos de capas más altas para el procesamiento. Dependiendo de la implementación, el control de flujo puede ser iniciado, o la indicación puede ser ignorada.

IV.15.4 ELEGIBILIDAD DE DESCARTE DE FRAME RELAY

El bit Eligibilidad de Descarte ***(Discard Eligibility [DE])*** es usado para indicar que una trama tiene la más baja importancia que la otras tramas, El bit DE es parte del campo del dirección en el encabezado de Frame Relay.

Los dispositivos DTE pueden poner el valor del bit DE de una trama a 1 para indicar que la trama tiene la importancia más baja que las otras tramas. Cuando la red llega a congestionarse, los dispositivos DCE descartaran tramas con el bit DE que pone antes de ser descartado a esos. Esto reduce la probabilidad de los datos críticos siendo tirados por los dispositivos DCE de Frame Relay durante los periodos de congestión.

IV.15.5 VERIFICACIÓN DE ERROR DE FRAME RELAY

Frame Relay usa un mecanismo de verificación de error conocido como es la Verificación de Redundancia Cíclica (***cyclic redundancy check [CRC])***. El CRC compara dos valores calculados para determinar si los errores ocurridos durante la transmisión de la fuente al destino. Frame reduce el sobreencabezado de la red para la implementación de la verificación de error más que a la corrección de error. Frame Relay típicamente esta implementada en el medio de la red segura, entonces la integridad de los datos no es sacrificada por que la corrección de error puede ser dejada a los protocolos de capas más altas operando en la cima de Frame Relay.

IV.16 RUTEO

El ruteo es realizado en dos áreas funcionales:

Generación de la Ruta. Un conmutador Frame Relay tiene la habilidad de aprender la topología de la red y generar tablas de ruteo. Las tablas de ruteo generadas por la red son actualizadas o modificadas en tres situaciones:

- Cuando se adiciona ó se borra una línea de Acceso o troncal.
- Cuando un nodo es adicionado ó borrado.
- Cuando una línea es puesta en servicio ó cuando se pone fuera de servicio de manera temporal.

Selección de la Ruta.- El nodo Frame Relay utiliza su capacidad de enrutar un enlace lógico basado en la mejor trayectoria posible.

IV.17 FRAME RELAY FRENTE A OTROS SERVICIOS

La oferta de servicios de telecomunicaciones es cada vez más amplia y el FRL deberá hallar su propio hueco, unas veces en calar competencia con otros servicios y otras completándolos.

IV.17.1 ATM

No es una tecnología con la que pretenda competir, al menos en los servicios multimedia y de muy alta velocidad en los que ATM puede ofrecer unas cualidades de servicio no comparables en FRL. No ocurre lo mismo para transferencia de datos, donde FRL es más eficiente que el ATM. Por otro lado, el FRL cuenta a su favor el ser un estándar actualmente disponible en redes extensas y demostradamente competitivas, cosas que de momento no podemos decir del ATM.

IV.17.2 RDSI

También puede ser servicios complementarios con la posibilidad de utilizar RDSI como vía de acceso al FRL e incluso como backup. Para la transferencia de datos, el FRL es adecuado cuando el volumen de información a transmitir es elevado y el número de puntos a conectar está limitado. La RDSI resultara más apropiada si el volumen de

información es bajo, la dispersión de los usuarios es elevada y, por supuesto, si lo que se pretende es integrar voz, datos e imágenes haciendo uso de los mismos equipos y las mismas infraestructuras. Si lo que se pretende es la interconexión de LAN mediante Ruteadores, el FRL suele resultar más adecuado debido al alto volumen de información de control generada, adecuándose a los esquemas de tarificación no conmutados.

IV.17.3 X.25

Las redes de paquetes como X.25 son más lentas e ineficaces que el FRL. No hay que olvidar que fueron concebidas cuando las infraestructuras de comunicaciones eran de peor calidad, que obligaron a diseñar reiterados procedimientos de control, mientras que el FRL saca el máximo partido de los nuevos equipos de conmutación y medios de transmisión. En cierto modo FRL es el heredero natural de las redes X.25 a las que supera claramente en prestaciones e incluso disminuye en complejidad.

IV.17.4 ENLACES PERMANENTES

El rendimiento obtenido por los canales permanentes pueden llegar a ser similar, por lo que se debe analizar con detalle cada caso particular y evaluar parámetros como: el volumen de trafico (si es muy elevado los enlaces permanentes pueden ser más adecuados); puntos a conectar (si son muchos y mallados el FRL es superior); y costes de equipos, donde FRL facilita la múltiplexación de los enlaces. Una ponderación de cada uno de estos parámetros puede señalar la opción correcta.

CAPITULO V IMPLEMENTACION DE REDUNDANCIA EN ACCESO DE INTERNET

V.1 INTRODUCCION

Antes de comenzar la implementación redundancia en el acceso de Internet debemos detenernos para considerar como se conecta un sitio de una empresa con un acceso de Internet de alta demanda; y llegaremos a la conclusión que invariablemente se tendrá que instalar un Ruteador para alcanzar la red e Internet, en las condiciones mencionadas anteriormente. Ya que este uno de los elementos más importantes para considerar su redundancia en el sistema, por ello se mencionará a través de este Capitulo, sus características, su estructura de hardware y su lenguaje de programación, esenciales para determinar el enrutamiento de la red; y cabe señalar que una de las empresas más sólidas en estos dispositivos es Cisco Systems a nivel mundial. Así que iniciemos comentado que los Ruteadores son otro tipo de dispositivo de internetworking. Estos dispositivos pasan paquetes de datos entre las redes en base a la información de la capa de protocolo de red o capa 3. Los Ruteadores tienen la capacidad de tomar decisiones inteligentes respecto de cuál es la mejor ruta para entregar los datos a través de la red.

V.2 ESTRUCTURA DE LOS RUTEADORES DE CISCO

Los Ruteadores de Cisco tienen que ser capaces de construir tablas de encaminamiento ejecutar comandos y encaminar paquetes por las interfaces de red mediante el uso de protocolos de encaminamiento. Esto significa que el Ruteador debe tener potencia de procesamiento, algún tipo de capacidad de almacenamiento y memoria disponible de acceso aleatorio. También requiere de un software adecuado, como un sistema operativo que permita configurar los protocolos los protocolos encaminados y de encaminamiento.

V.2.1 LA CPU DE UN RUTEADOR

Los Ruteadores no son distintos a los PC en cuanto a que también integran un microprocesador. Y al igual que la PC, los distintos modelos de Ruteadores de Cisco incorporan procesadores diferentes. Por ejemplo, el Ruteador 2505 de Cisco, contiene un procesador 68EC030 de Motorola a 20 MHz. Un Ruteador de gama alta, como el Ruteador Cisco 7010, incorpora una CPU MC68040 de Motorota a 25 MHz. (muchos Ruteadores de gama más baja utilizan los mismos procesadores Motorota que usan algunas computadoras Macintosh de Apple. Algunos Ruteadores de gama alta utilizan, en cambio, procesadores RISC, que son los que suelen integrar las microcomputadoras o los servidores de gama alta).

V.2.2 COMPONENTES DE LA MEMORIA DE UN RUTEADOR.

Como comentamos al principio, los Ruteadores no sólo necesitan potencia de procesamiento, sino también un sitio donde almacenar la información de configuración un lugar donde arrancar el sistema operativo del Ruteador (IOS), y memoria que puede utilizarse para mantener la información dinámica que se genere cuando el Ruteador mueve los paquetes por la interconexión. Los Ruteadores de Cisco contienen de hecho, distintos tipos de componentes de memoria que proporcionan la capacidad de

almacenamiento y la caché dinámica requerida. El listado siguiente ofrece la información acerca de los distintos componentes de memoria que integra un Ruteador de CISCO:

V.2.2.1 ROM. Contiene el Auto-Test de Encendido (POST) y el programa de carga del Ruteador. Los chips de la ROM también contiene parte o todo el sistema operativo (IOS) del Ruteador (por ejemplo, la ROM del Ruteador 2505 sólo contiene una parte del IOS, mientras que la serie 7000 incluye el IOS completo). Puesto que el IOS se encuentra en la ROM, puede recuperarse en caso de desastre grave de borrado de la memoria flash. Los chips de la ROM en los Ruteadores de Cisco son extraíbles y pueden actualizarse o reemplazarse.

V.2.2.2 NVRAM (RAM no volátil). Almacena el archivo de configuración del arranque para el Ruteador. La NVRAM puede borrarse, y puede copiarse en ella la información básica de configuración del Ruteador. Lo bueno de la NVRAM es que mantiene la información incluso si se interrumpe la corriente en el Ruteador (algo realmente útil, teniendo en cuenta lo pesado que sería tener que reconfigurar el Ruteador cada vez que hubiera un apagón).

V.2.2.3 FLASH RAM. La memoria flash es un tipo especial de ROM que puede borrarse y reprogramarse. La memoria flash se utiliza para almacenar el IOS de Cisco que se ejecuta en el Ruteador. También se pueden almacenar aquí versiones alternativas del IOS (como una actualización por ejemplo). La memoria flash viene de hecho, en forma SIMMS (Single-Inline Memory Modules o Módulos Sencillos de Memoria en Línea) y en función del Ruteador que se tenga, se puede instalar memoria flash adicional.

V.2.2.4 RAM. Parecida a la memoria dinámica que se utiliza en una PC, la memoria RAM proporciona el almacenamiento temporal de la información (los paquetes se guardan en la RAM mientras el Ruteador examina su información de direccionamiento), además de mantener otro tipo de información, como la tabla de encaminamiento que se este utilizando en ese momento. La RAM también almacena la configuración del Ruteador que esta ejecutando (los cambios que se introduzcan en la configuración se mantiene en la RAM hasta que se guardan en la NVRAM).

Todos estos componentes de memoria desempeñan un papel fundamental en todo lo que ocurre al arrancar el Ruteador. Las distintas posibilidades referentes al arranque del sistema del Ruteador y a las ubicaciones del IOS y de los archivos de configuración del arranque se trataran más adelante.

V.3 SECUENCIA DE ARRANQUE DEL RUTEADOR

En el tema anterior comentamos los distintos tipos de memoria que incluye un Ruteador (como RAM, NVRAM, Flash RAM, y ROM). Todos estos equipos de memoria participan en la secuencia de arranque de un Ruteador. Por ello, y antes de adentrarnos en la configuración de un Ruteador, vamos a explicar la secuencia de arranque que sigue y los sitios a los que se remite para encontrar un archivo de configuración.

Cuando se enciende un Ruteador, los chips de la memoria ROM, ejecutan un auto-test de Encendido (Power On Self Test o POST) que comprueba el hardware del Ruteador como el procesador, las interfaces y la memoria. Este test es muy parecido al

que se ejecuta al encender una PC (y en el también se comprueba la RAM, la CPU y demás elementos de hardware:

El paso siguiente en la secuencia de arranque es la ejecución de un programa de carga busca el IOS de CISCO. El IOS puede cargarse directamente desde la ROM (los Ruteadores incluyen una copia parcial o integra del CISCO IOS en la ROM), desde la FLASH RAM del Ruteador, o desde un servidor TFTP incluido en la red (los comandos para cargar el IOS desde todas estas aplicaciones los veremos más adelante). El IOS suele estar almacenado en la memoria flash del Ruteador.

Una vez cargado el IOS del Ruteador, este pasa a buscar el archivo de configuración. El archivo de configuración normalmente se encuentra almacenado en la memoria NVRAM (se utiliza un comando de copia para copiar la configuración de ejecución en la NVRAM). Al igual que el IOS, el archivo de configuración depende de la información almacenada en la NVRAM del Ruteador).

Una vez cargado el archivo de configuración en el Ruteador, la información incluida en el archivo activa las interfaces y proporciona los parámetros relacionados con los protocolos encaminados y de encaminamiento vigentes en el Ruteador. En la figura 5.1 se ofrece un esquema del proceso de arranque de un Ruteador. No debe olvidarse que si se carga el IOS desde otra fuente que no sea la memoria Flash RAM, se tiene que incluir una anotación en el Registro de Configuración ROM. Igualmente, para cargar el archivo de configuración desde otra fuente distinta a la memoria NVRAM, debe incluirse en la NVRAM información acerca de la ubicación del archivo.

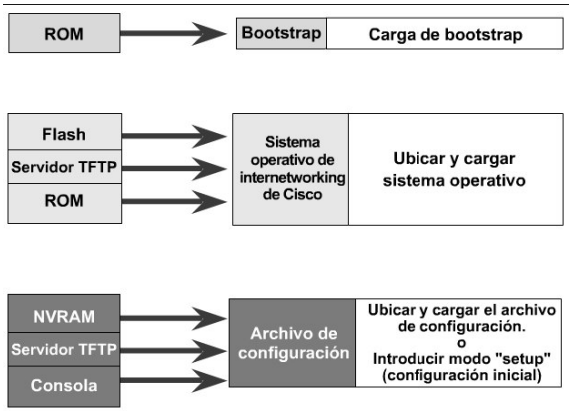


FIGURA 5.1 SECUENCIA DE ARRANQUE DEL RUTEADOR

Si no se encuentra un archivo de configuración en la NVRAM o en cualquier otro lugar previamente especificado (como un servidor TFTP), se incluirá el modo **Setup** (arranque) y aparecerá el cuadro de dialogo System Configuration (Configuración del sistema) en la pantalla de la consola del Ruteador.

V.4 DESCRIBIENDO EL RUTEADOR A CONECTAR

La siguiente tabla, lista las interfaces soportadas para este modelo.

Tabla 5-1 Interfaces del Ruteador.

Modelo	Ethernet / AUI (DB-15)	Token Ring	Serial (DB-60)	ISDN BRI (RJ-45)
Cisco 2501	1	-	2	-

AUI= Attachment Unit Interface
ISDN= Integrated Services Digital Network.
BRI= Basic Rate Interface

V.4.1 CARACTERISTICAS DE HARDWARE

Además de las interfaces listadas en la tabla anterior, el Ruteador incluye las siguientes características de hardware:

- Memoria de Acceso Aleatorio Dinámico (DRAM) para la memoria principal y memoria compartida.

- Memoria de Acceso Aleatorio No Volátil (NVRAM) para almacenar la información de configuración.

Memoria Flash, para correr el software CISCO IOS.
Puerto de Consola EIA/TIA -232, para el acceso del sistema local usando una Terminal de consola.
Puerto Auxiliar EIA/TIA-232 para el acceso remoto usando un MODEM.

Nota: EIA/TIA-232 y EIA/TIA-449 fueron conocidas como estándares recomendadas RS-232 y RS-449 antes de su aceptación como estándares por la Electronic Industries Association (EIA) y Telecommunications Industry Association (TIA).

La siguiente figura 5.2 muestra los paneles posteriores del modelo antes discutido.

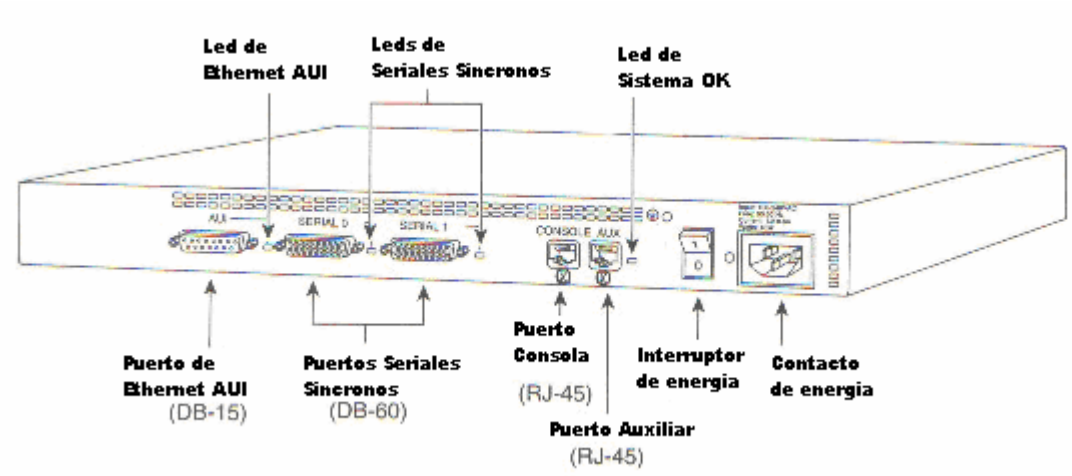


FIGURA 5.2 PANELES POSTERIORES DEL RUTEADOR SERIE 2500

V.4.2 ESPECIFICACIONES DEL SISTEMA.

Las especificaciones del sistema del Ruteador esta listado en la tabla 5-3 siguiente:

TABLA 5-2 ESPECIFICACIONES DEL RUTEADOR

Descripción	Especificación
Dimensiones	1.75x17.5x10.5 in (4.44x44.45x28.82 cm.) Unidad de Rack.
Peso	10 lb (4.5 Kg.)
Voltaje de alimentación AC.	100 a 240 AC.
Corriente	1.2 a 0.6 A
Frecuencia	50/60 Hz.
Disipación de Potencia	40 W (máximo), 135.5 Btus/hr
Voltaje de Entrada de Alimentación DC	40 W, 40 a 72 DC
Corriente	1.5 a 1.0 A
Disipación de Potencia	40 W (máximo), 135.5 Btus/hr
Procesador	20 MHz Motorola 68EC030
Ambiente de Operación	32 a 104 ^{o} F (0 a 40^{o} C)
Temperatura No Operativa	-40 a 185 ^{o} F (-40 a 85 ^{o} C)
Humedad de Operación	5 a 95%, no condesado
Conformidad Regulatoria	FCC Clase A y DOC Canadiense Clase A

Btus= British Thermal Units.

V.5 CONFIGURAR UN RUTEADOR

Establecer la configuración básica de un Ruteador no es as que activar las distintas interfaces del Ruteador y configurar los parámetros de software para los protocolos encaminados y de encaminamiento. Por ejemplo, si esta encaminando IP, las interfaces deben de tener asignadas las direcciones IP correspondientes. Los protocolos de encaminamiento también tienen que estar debidamente configurados (si se va a utilizar RIP o IGRP, deberán configurarse estos dos protocolos). Lo mismo que cualquier interfaz en serie que vaya a utilizarse, que deberá configurarse con el correspondiente protocolo WAN de capa 2 (como HDLC, o Frame Relay). Entre la información acerca de la configuración básica deberá así mismo incluirse el ancho de banda y la sincronización para conexiones WAN.

El archivo de configuración del Ruteador sirve de parámetros de software para indicarle al Ruteador lo que debe encaminar y el modo en que debe hacerlo. Todos los comandos que se utilizan para configurar el Ruteador forman parte del sistema operativo IOS de Cisco. Existen distintas formas de llevar a cabo la configuración del Ruteador, ya sea directamente utilizando la consola del Ruteador, o bien de forma indirecta, cargando un archivo de configuración ubicado en un servidor de Protocolo Trivial de Transporte de

Archivos (Trivial File Transport Protocol o TFTP) dentro de la red. El listado siguiente muestra algunas de las opciones disponibles para cargar la información de configuración dentro de un Ruteador:

- ***Consola del Ruteador***. El Ruteador puede configurarse directamente desde una PC (la consola del Ruteador) que este conectado al puerto de la consola del Ruteador por medio del cable enrollado de incorpora el Ruteador. El PC tiene asimismo que ejecutar algún tipo de software de emulación de Terminal que le permita conectar con el Ruteador a través del puerto serie del PC. También se puede conectar directamente con el Ruteador utilizando el puerto auxiliar del Ruteador, que normalmente se encuentra junto al puerto de la consola en la parte trasera del Ruteador.

- ***Terminal virtual***. Si ya se configuro el Ruteador a nivel básico activa algunas de las interfaces en la red (como un puerto Ethernet), se puede conectar con el Ruteador vía Telnet por medio de una Terminal virtual. Esto significa sencillamente que una computadora de la red que esta ejecutando un programa Telnet se conectara con el Ruteador y pasara a configurarlo (siempre que faciliten las contraseñas correctas, de lo que hablaremos en detalle más adelante)

- Estación de trabajo para la gestión de la red. Los Ruteadores también pueden configurarse desde una estación de trabajo incluida en la red que ejecute un software especial para la gestión de redes, como la Cisco Works de Cisco (como se muestra en la figura 5.3) o el HP Open View de Hewlett Packard (Como se muestra en las figuras 5.4a y 5.4b).

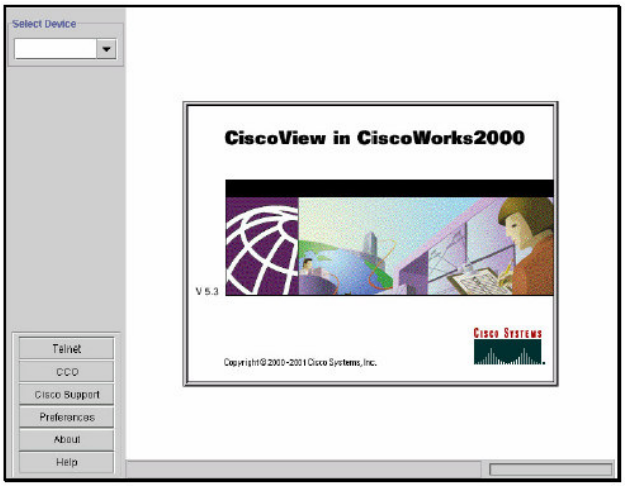


FIGURA 5.3 VERSION DE HERRAMIENTA DE CISCOWORKS

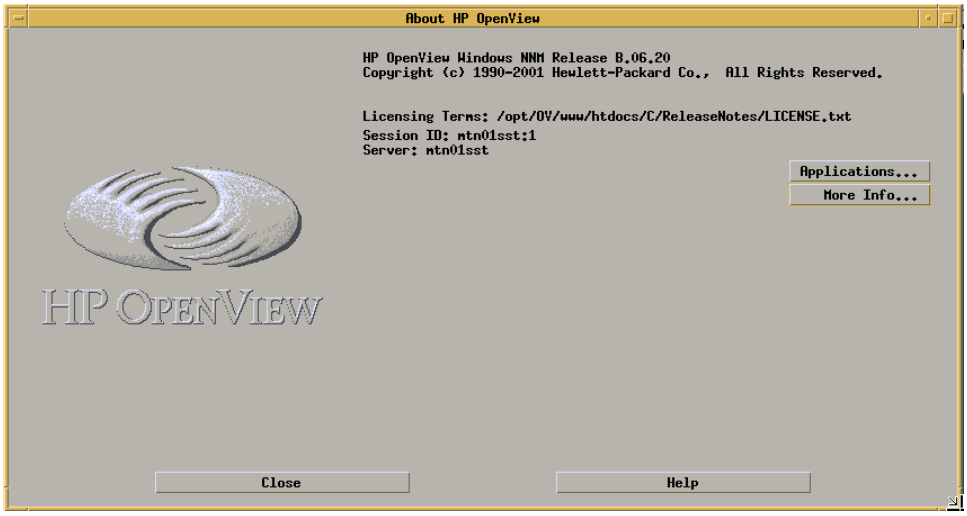
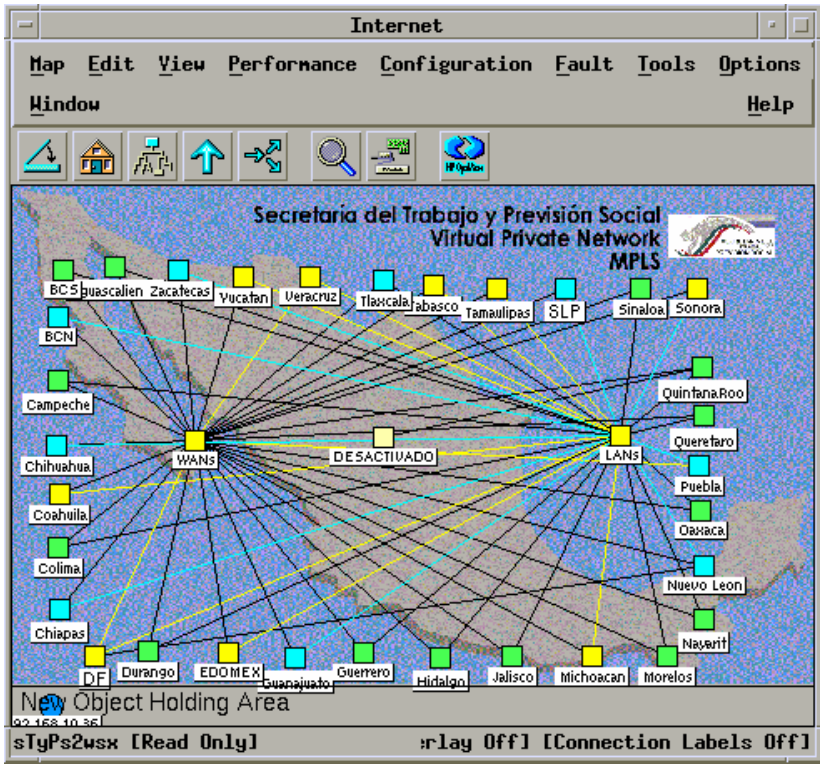


FIGURA 5.4a VERSION DE HP OPEN VIEW



5.4b MONITOREO A TRAVES DE HP OPEN VIEW PARA REDES VPN Y FRAME RELAY

- ConfigMarker de Cisco. Este programa basado en gráficos, permite construir una configuración para el Ruteador o Ruteadores en la red y después cargar la configuración a un Ruteador que este directamente conectado a una consola de Ruteador (el PC que este ejecutando ConfigMarker) a otros Ruteadores conectados a la red. Para que ConfigMarker pueda cargar las configuraciones del

Ruteador de la red, las interfaces de red en dichos Ruteadores tienen que estar ya configurados.

- Servidor TFTP. Se puede cargar una configuración de Ruteador desde un servidor TFTP incluido en la red. Si se guardan las configuraciones en un servidor TFTP, después podrán descargarse sin problemas en un determinado Ruteador. (Como se muestra en la figura 5.5)

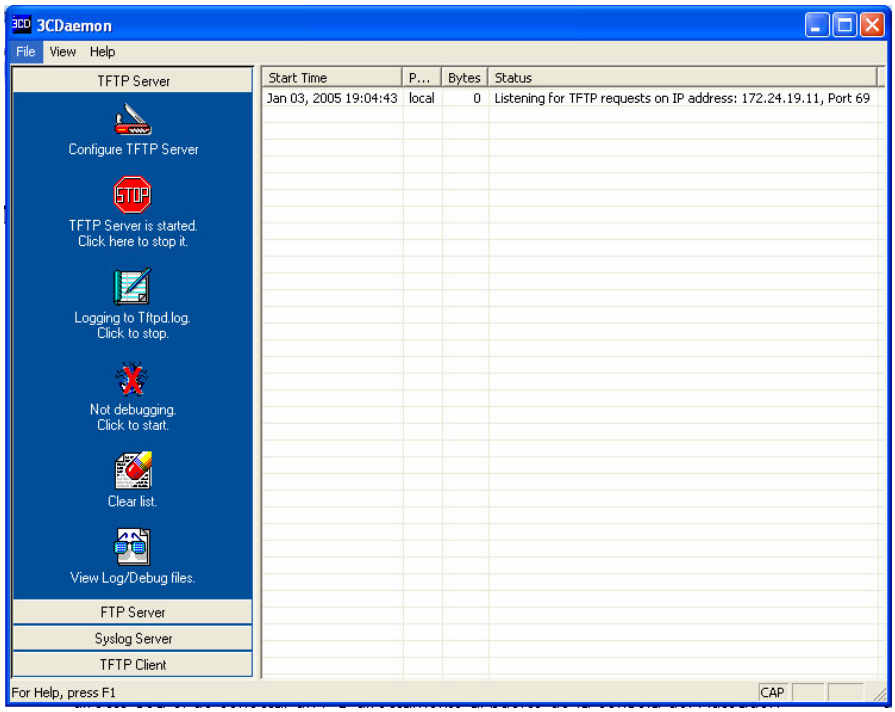


FIGURA 5.5 SOFTWARE DE EMULACION DE SERVIDOR TFTP

De entre todos estos métodos de configuración, probablemente el más sencillo y directo sea el de conectar un PC directamente al puerto de la consola del Ruteador. Con ello no sólo se puede construir rápidamente una configuración básica del Ruteador gracias al cuadro de dialogo **System Configuration** (Configuración del sistema), sino que además permite ajustar los parámetros de configuración en el modo **Configuration** (Configuración) del Ruteador.

Con el comando **show version** podemos observar la configuración del sistema cuando inicia o enciende el Ruteador como se muestra en la siguiente figura 5.6:

```
Router>sh ver
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 29-Nov-99 14:52 by kpma
Image text-base: 0x03051C3C, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c)XB1, PLATFORM SPECIFIC RELEASE SOFTWARE
(fc1)
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB1, PLATFORM
SPECIFIC RELEASE SOFTWARE (fc1)

Router uptime is 2 hours, 26 minutes
System restarted by reload
System image file is "flash:/c2500-js-l_120-8.bin"

cisco 2500 (68030) processor (revision M) with 6144K/2048K bytes of memory.
Processor board ID 17048803, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102
Router>
```

FIGURA 5.6 EJEMPLO DE COMANDO "SHOW VERSION "

Aquí muestra mucha de la información como:

- El tipo de Ruteador, en este caso es de series 2500
- La versión del software IOS que es 12.0
- El tiempo en el que fue prendido por ultima vez, aquí indica 2 horas con 26 minutos
- Que cuenta con un puerto de LAN Ethernet
- Y además cuenta con dos interfaces seriales.

V.5.1 CONECTAR LA CONSOLA

Para iniciar la conexión del Ruteador, conviene asegurar que se tenga lo necesario, después de ello, debe conectar primero el cable de alimentación del Ruteador y a una toma de alimentación (asegúrese de que el Ruteador este apagado); después, tiene que conectar un PC al Ruteador para que actúe como consola del mismo. La consola puede ser cualquier PC que tenga un puerto serie y pueda ejecutar algún tipo de software de emulación de Terminal. Este PC, de hecho, pasara a convertirse en una Terminal tonta y suministrara la interfaz que deberá utilizarse para configurar y controlar el Ruteador.

La computadora consola y el Ruteador deben conectarse por medio del cable enrollado que se incluye junto al Ruteador. El cable viene cerrado en ambos extremos con un conector RJ-45. (Véase Figura. 5.7)

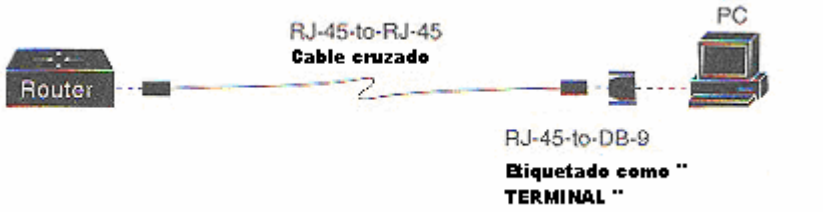


FIGURA 5.7 COMO CONECTAR EL CABLE DEL RUTEADOR AL PC PARA CONFIGURARLO.

El Ruteador también incluye varios adaptadores en serie diferentes que contienen un puerto RJ-45 para que puedan conectarse al cable enrollado y después al puerto serie del PC que vaya a utilizarse como consola del Ruteador. Una vez seleccionado el adaptador en serie apropiado, ya puede conectar el Ruteador a la consola.

V.5.1.1 CONECTAR EL RUTEADOR A LA CONSOLA

1. Conecte el adaptador macho RJ-45 al cable enrollado del puerto situado en la parte trasera del Ruteador marcado como CONSOLE. (véase Figura 5.8)
2. Conecte el adaptador en serie al puerto serie pertinente en el PC que vaya utilizar como consola.

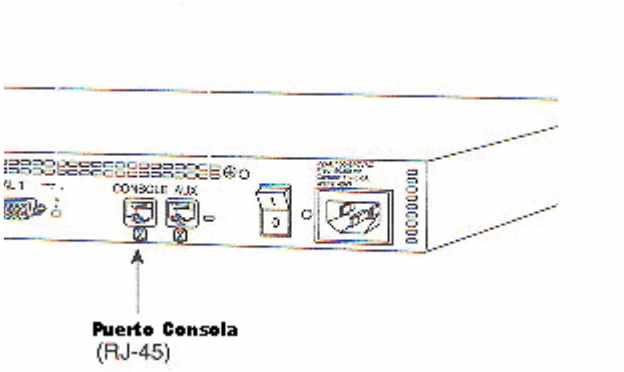


FIGURA 5.8 EL CABLE ENROLLADO SE CONECTA AL PUERTO CONSOLE DEL RUTEADOR UTILIZANDO EL CONECTOR MACHO RJ-45.

Una vez realizada la conexión física entre el Ruteador y el PC, debe configurarse al software de emulación de Terminal en el PC. El software de emulación de Terminal y los parámetros para comunicar con el Ruteador se explican en el apartado siguiente.

V.5.1.2 CONFIGURAR LA CONSOLA DEL RUTEADOR

La PC que se utilice como consola se comunica con el Ruteador por medio del software de emulación de Terminal. Existen varios paquetes de software de este tipo, como Hyper-Terminal (que viene incluido en los sistemas operativos Windows 95/98, Windows 2000 y XP). También existen otros tipos de software disponibles en Internet que

pueden descargarse como freeware o shareware (como Terra Term Pro, un emulador de Terminal de configuración y uso muy sencillos).

Una vez instalado un determinado paquete de software de emulación de Terminal, deben configurarse los parámetros de configuración para el puerto serie que vaya a utilizar para comunicarse con el Ruteador. La tabla 5-1 refiere al listado de los parámetros de comunicación que debe utilizarse el software de emulación de Terminal.

TABLA 5-3 PARÁMETROS DE COMUNICACIÓN EN EMULADOR DE TERMINAL

Parámetro	Configuración
Emulación de Terminal	VT100
Velocidad en baudios	9600
Paridad	Ninguna
Bits de datos	8
Bits de parada	1 (2 bits de parada para la serie 2500)

V.5.1.3 TRABAJAR CON EL SOFTWARE DE EMULACION DE TERMINAL

Cada paquete de emulación de Terminal de distinta forma, pero todos proporcionan un sistema de menús y cuadros de dialogo para acceder a los distintos parámetros del software. En la figura 5.9 se muestra el dialogo **serial port setup**. Los parámetros de comunicación se configuran utilizando cuadros desplegables donde viene incluidas las distintas opciones.

Después de configurar correctamente el emulador de Terminal de la consola, resulta muy sencillo establecer comunicación con el Ruteador.

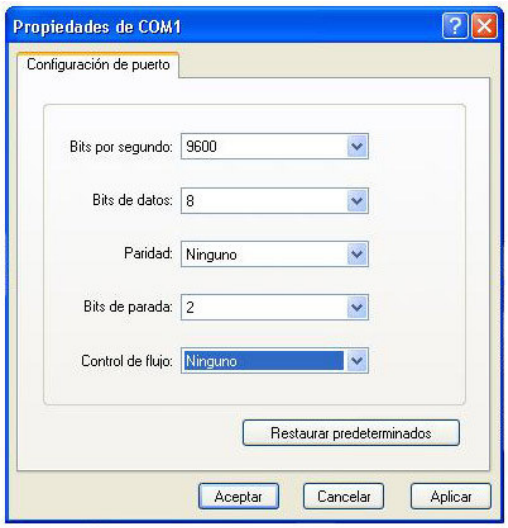


FIGURA 5.9. LOS PARÁMETROS DE COMUNICACIÓN PARA EL PUERTO SERIE SUELEN INCLUIRSE EN CUADROS DE DIALOGO EN LA MAYORÍA DE EMULADORES BASADOS EN WINDOWS.

V.5.1.4 ESTABLECER LA COMUNICACIÓN ENTRE EL RUTEADOR Y LA CONSOLA

1. Inicie su emulador de Terminal y asegúrese de que ha seleccionado el puerto serie adecuado para la comunicación (así como los parámetros de configuración que se detallan en la tabla 5-3)
2. Encienda el Ruteador (pulse el interruptor situado en la parte posterior del Ruteador, o en la parte izquierda en los Ruteadores de la serie 2500)

V.6 PREPARANDO AL USUARIO PARA CONECTAR EL RUTEADOR.

Cuando configuras tú Ruteador, considera las limitaciones de distancia y la interfaz electromagnética potencial (EMI) como es definida por EIA.

V.6.1 CONEXIONES SERIALES SINCRONAS.

Antes de que conectes un dispositivo para el puerto serial sincrono (etiqueta "SERIAL"), tú necesitaras conocer lo siguiente:

- Tipo de dispositivo DTE ó DCE, que estas conectando a la interfaz serial sincrona.
- El tipo de conector, macho ó hembra, requerido para conectar al dispositivo.
- La señal estándar requerido por el dispositivo.

V.6.2 DTE o DCE

Un dispositivo que comunica sobre una interfaz serial sincrona es cualquier dispositivo DTE o DCE. Un dispositivo DCE proporciona una señal de reloj que pasa las comunicaciones entre el dispositivo y el Ruteador. Un dispositivo DTE no provee una señal de reloj. Los dispositivos DTE usualmente conectan a los dispositivos DCE. La documentación que viene con el dispositivo debería indicar si este es un dispositivo DTE o DCE. (Algunos dispositivos tiene un puente seleccionador para indicar cualquier modo). Si tú no puedes encontrar la información en la documentación, refiérase a la Tabla 5-4 para auxiliarse a seleccionar el tipo apropiado de dispositivo.

TABLA 5-4 DISPOSITIVOS TÍPICOS DTE O DCE.

Tipo de Dispositivo	Genero	Dispositivo Típico
DTE	Macho	Terminal, PC, Ruteador
DCE	Hembra	MODEM, CSU/DSU, Multiplexor

Las consideraciones de si son machos o hembras son:

Si los pines sobresalen de la base del conector, el conector es macho.
Si el conector tiene agujeros para insertar pines, el conector es hembra.

Nota: CSU / DSU = Unidad de Canal de Servicio / Unidad de Datos de Servicio.

V.6.3 LIMITACIONES DE DISTANCIA Y VELOCIDAD.

Las señales seriales pueden viajar a una distancia limitada en cualquier velocidad de bits dada, generalmente, la velocidad de datos es muy baja y la distancia es muy grande. Todos las señales seriales son sujetas a limitaciones de distancia, más allá de la cual la señal se degrada significativamente ó es una pérdida completa.

La tabla 5-5 lista las máximas velocidades y distancias para señales en el estándar EIA/TIA-232. la señalización estándar soporta un desbalance de circuitos en señal con velocidad arriba de 64 KBPS.

TABLA 5-5 EIA/TIA-232 LIMITACIONES DE VELOCIDAD Y DISTANCIA.

Velocidad	Distancia (Pies Ft)	Distancia (m)
2400	200	60
4800	100	30
9600	50	1.5
19200	50	1.5
38400	50	1.5
64000	25	7.6

Los controladores de Balance permiten señales EIA/TIA-449 para viajar a distancias más grandes que las señales EIA/TIA-232. Tabla 5-6 lista para las máximas velocidades y distancias para EIA/TIA-449, V.35, X.21 y señales EIA/TIA-530.

TABLA 5-6. EIA/TIA-449, V.35, X.21 Y EIA/TIA-530. LIMITACIONES DE VELOCIDAD Y DISTANCIA.

Velocidad de datos	Distancia (Pies ft)	Distancia (metros m)
2400	4100	1250
4800	2050	625
9600	1025	312
19200	513	156
38400	256	78
56000	102	31

Precaución: El EIA/TIA-449 e interfaz V.35 soporta velocidades de datos arriba de 2048 MBPS, excediendo este el máximo podría resultar en perdida de datos y no es recomendado.

V.6.4 ESTANDARES DE SEÑALIZACIÓN.

El puerto serial sincrono soporta la siguiente señalización estándar: EIA/TIA-232, EIA/TIA-449, V.35, X.21 y EIA/TIA-530. Tú puedes ordenar un cable blindado serial de transición DB-60 que tiene un conector apropiado para el estándar de tu especificación. El final del extremo del Ruteador el cable blindado serial de transición tiene un conector DB-60, el cual conecta al puerto serial sobre el panel posterior Ruteador. El extremo del otro

cable serial de transición está disponible con el conector apropiado al estándar de tu especificación. En la documentación del dispositivo que tú quieres conectar debería indicarle el estándar usando para este dispositivo. El puerto serial sincrono puede ser configurado como DTE o DCE (excepto el EIA/TIA-530, el cual es solamente DTE), dependiendo del cable de conexión.

Nota: Todos los puertos seriales configurados como DTE, requieren un reloj externo de un CSU/DSU u otro dispositivo DCE.

La siguiente figura 5.10 muestra los cables seriales de transición que tú puedes conectar al puerto serial en el panel posterior del Ruteador.

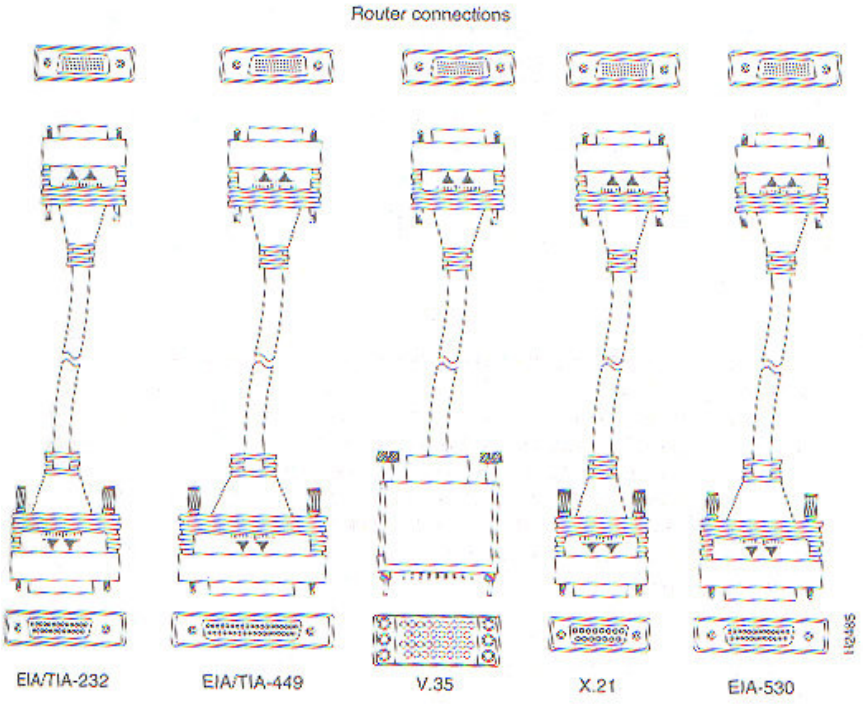


FIGURA 5.10 ESTANDARES DE CONEXIÓN DE EQUIPOS

Comentemos dos estándares más conocidos y que este equipo utiliza.

V.6.4.1 CONEXIONES EIA/TIA-232.

El estándar EIA/TIA-232 soporta un desbalance de circuitos en la señal a una velocidad de 64 KBPS. El puerto serial (etiquetado “SERIAL”) soporta conexiones sincronas. La consola y los puertos auxiliares también usan una conexión EIA/TIA-232, sin embargo, la consola y el puerto auxiliar soporta conexiones asíncronas.

En el extremo de la red del cable serial de transición EIA/TIA-232 proporciona un conector DB-25, como se muestra en la Figura 5.11. El extremo conecta al puerto serial en el panel posterior del Ruteador, que tiene un conector DB-60. Los cables seriales de transición están disponibles con una conexión DB-25 o un receptáculo en cada modo DTE o DCE.

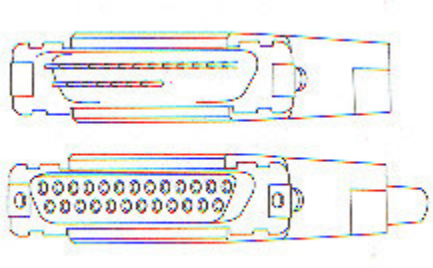


FIGURA 5.11 CONEXIÓN DEL ESTANDAR EIA/TIA-232

V.6.4.2 CONEXIONES V.35.

El estándar V.35 es recomendado para velocidades de 48 KBPS, aunque en la práctica es satisfactoriamente usada hasta en 4 MBPS.

El extremo de la red del cable serial de transición V.35 proporciona un estándar en conector de tipo Winchester de 35 pines, como se muestra en la figura 5.12. La terminación que conecta al puerto serial en la parte posterior del panel del Ruteador, tiene un conector DB-60. los cables V.35 están disponibles con un estándar de conexión V.35 o un receptáculo en cualquier modo DTE o DCE.

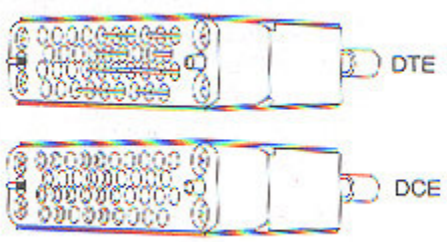


FIGURA 5.12 CONEXIÓN DE ESTANDAR V.35

V.7 CONEXIONES DE RUTEADOR

En los siguientes apartados se describiran las conexiones necesarias para el Ruteador, asi como de la interfaces y dispositivos necesarios.

V.7.1 INTERFAZ G.703

La interfaz G.703 es un estándar de CCITT para transmitir voz sobre portadoras digitales como T1 y E1. La interfaz G.703 proporciona las especificaciones de Modulación de Código de Pulso (PCM) y a tasas de datos de de 64 Kbps a 2.048 Mbps. El servicio típico de G.703 es usado para el equipo de Comunicacion de datos de interconexión tales como puentes, Ruteadores, y multiplexores. La interfaz G.703 es trasportada sobre cable balanceado (en par trenzado 120 ohm) o cable desbalanceado (coaxial dual a 75). Si la interfaz G.703 es balanceado o desbalanceado depende de tu localización geográfica y la portadora que te proporciona el servicio. El servicio balanceado es el más común en el mundo con la excepción de Reino Unido y Países Bajos.

V.7.2 TRANCEPTOR

Dispositivo que realiza, dentro de una misma caja ó chasis, funciones tanto de transmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones. Dado que determinados elementos se utilizan tanto para la transmisión como para la recepción, la comunicación que provee un transceptor solo puede ser semiduplex, lo que significa que pueden enviarse señales entre dos terminales en ambos sentidos, pero no simultáneamente. En el caso de este Ruteador se utiliza para realizar una conversión de interfaces de AUI a RJ45, a través de este dispositivo para poderlo integrar a la red LAN del cliente que utilizará un hub ó switch.

V.7.3 DESCANALIZADOR

Definiremos a un descanalizador como un CSU/DSU (Unidad de Canal de Servicio / Unidad de Datos de Servicio), que pueden ser de dos tipos. Uno de ellos es para de multiplexar la señal, es decir, en tantos canales como sean necesarios, por ejemplo cuando se utiliza un medio como un Microondas o Fibra Óptica y en estos medios se utiliza un ancho de banda completo como un E1, pero solo se requiere un ancho de banda de 512K, el proveedor de medio configura el equipo a ese ancho de banda por canales (slots), solo en el caso de Microondas por que es posible, en el caso de Fibra Óptica solo puede proporcionar un E1 completo ya que el proveedor no lo puede configurar.

Por lo que ahí entra el otro tipo del descanalizador, que es el de transconectar las interfaces para el posible manejo del medio y el Ruteador, ya que en este caso particular de implementación el proveedor de Fibra Óptica proporciona la interfaz G.703 y nuestro Ruteador tiene interfaz V.35, para llevar la conversión de interfaces se utiliza un descanalizador para dicho propósito.

Los descanalizadores son configurables, es decir, utilizan un emulador de consola para configurar sus parámetros (en la mayoría de los casos son para el primer tipo, multiplexores) ya que necesitan administrar cuantos canales estarán activos, según el ancho de banda. Y por otro lado existen los de autodeteccion (autosense) ya que estos no necesitan configurar los parámetros sino que autodetectan la señal y los canales activos; y así se establece la configuración (en la mayoría de los casos son para el segundo tipo, transconectores). En este proyecto se utilizará este tipo como se menciono antes, el descananalizador transconector, ya que el proveedor de Fibra Óptica dejará una interfaz G.703 y en el Ruteador tendrá V.35, por lo que se resuelve con un descanalizador de autodeteccion con entrada G.703 y salida a V.35 (en este caso es de marca Nokia).

V.7.4 CONSOLA Y PUERTOS DE CONEXIONES AUXILIARES.

El Ruteador incluye un puerto de consola serial asíncrono y un puerto auxiliar. La consola y los puertos auxiliares proporcionan acceso al Ruteador en cualquier localidad (con la Terminal de consola) o remotamente (con el MODEM).

La principal diferencia entre la consola y los puertos auxiliares es que el soporte auxiliar soporta el hardware de control de flujo y el puerto de consola no. Los pasos de control de flujo en la transmisión de datos entre el dispositivo que emite y el dispositivo receptor. El control de flujo asegura que el dispositivo receptor pueda absorber los datos

enviados a este antes de que el dispositivo pueda emitir; y envíe más. Cuando el búfer esta lleno en el dispositivo receptor, un mensaje es enviado al dispositivo que emite para suspender la transmisión hasta que los datos en los búferes hallan sido procesados. Por que el puerto auxiliar soporta el control de flujo, esto es ideal para usarse con transmisiones de alta velocidad de un MODEM. Las terminales de consola transmiten a velocidades más bajas que los MODEMs; por lo tanto, el puerto de la consola es ideal para usarse con terminales de consola.

V.7.5 CONEXIONES DEL PUERTO DE CONSOLA.

El Ruteador incluye un EIA/TIA-232 puerto de consola serial asíncrono (RJ-45). Los cables y adaptadores para conectar una Terminal de consola (una Terminal ASCII o el software de emulación de Terminal de PC) para el puerto de consola están incluidos. Para conectar una Terminal ASCII para el puerto de la consola, el cable cruzado RJ-45 a RJ-45 (similar en cables de telefónicos) con adaptador hembra RJ-45 a DB-25 (etiquetado “TERMINAL”). Para conectar el software de emulación de Terminal en una PC al puerto de consola, use un cable cruzado RJ-45 a RJ-45 con un adaptador hembra RJ-45 a DB-9 (etiquetado “TERMINAL”). Los parámetros por omisión para el puerto de la consola son 9600 baudios, 8 bits de datos, no paridad, 2 bits de parada. El puerto de la consola no soporta hardware de control de flujo.

V.7.6 CONEXIONES DE PUERTOS AUXILIARES.

El Ruteador incluye un EIA/TIA-232 puerto auxiliar serial asíncrono (RJ-45) que soporta hardware de control de flujo. Un cable o adaptador a conectar a un MODEM para el puerto auxiliar están incluidos. Para conectar un MODEM a un puerto auxiliar, use el cable cruzado RJ-45 a RJ-45 (similar en cables telefónicos) con el adaptador macho RJ-45 a DB-25 (etiquetado “MODEM”).

V.8 INTERFACES DEL RUTEADOR

Una interfaz del Ruteador suministra la conexión física entre el Ruteador y un tipo de medio físico en la red. Las interfaces de Cisco a menudo se denominan puertos, y cada puerto viene designado físicamente de acuerdo con la topología de red a la que sirve. Por ejemplo, una interfaz LAN, como puerto Ethernet en el Ruteador, se compone de un conector hembra RJ-45 (que está conectando a un hub Ethernet por medio de un cable de par trenzado con conectores machos RJ-45 en cada extremo).

Los puertos incorporados se designan por su tipo de conexión seguido de un número. Por ejemplo, si el primer puerto Ethernet en un Ruteador se designa como E0, el segundo se designaría como E1 y así sucesivamente. Los puertos serie se designan siguiendo este mismo procedimiento, donde S0 corresponde al primer puerto serie.

Los Ruteadores Cisco como los de la serie 2500, son básicamente Ruteadores estándar que viene con un número predeterminado en puerto LAN y WAN y en serie. Los Ruteadores gama alta, como el 4500 de Cisco, son modulares y, de hecho, contienen ranuras abiertas en las que pueden instalarse varias tarjetas de interfaz.

No sólo pueden conectarse distintos tipos de tarjetas de interfaz (como LAN ó WAN), sino que además puede seleccionarse el número de puertos deseados en cada tarjeta. Por ejemplo, en una de las tres ranuras abiertas del Ruteador 4500 se puede instalar una tarjeta Ethernet que contenga seis puertos Ethernet.

Para saber que interfaces (así como su estado actual) se están utilizando en un determinado Ruteador se utiliza el comando **show interfaces,** como se muestra en la siguiente figura 5.13.

```
Router>sh inter
Ethernet0 is administratively down, line protocol is down
  Hardware is Lance, address is 0010.7b81.65e9 (bia 0010.7b81.65e9)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 252/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 02:11:34, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     77 packets output, 4620 bytes, 0 underruns
     77 output errors, 0 collisions, 13 interface resets
     0 babbles, 0 late collision, 0 deferred
     77 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0 is administratively down, line protocol is down
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  More
```

FIGURA 5.13 EJEMPLO DE COMANDO "SHOW INTERFRACE"

Aquí muestra información como:

- Que tanto la LAN como los seriales están administrativamente dadas de baja.
- Por tanto la línea del protocolo están abajo (down)
- En la parte de interfaces seriales cuentan con una encapsulación HDLC, como se vera más adelante.

La configuración de una determinada interfaz depende del tipo de protocolo de red que utilice la red al que esta conectando el puerto de la interfaz. Por ejemplo, un puerto Ethernet conectado a una red IP tendrá que configurarse para el encaminamiento IP. En cambio, un puerto Ethernet conectado a una red Apple Talk deberá configurarse para el encaminamiento Apple Talk.

V.8.1 INTERFACES LAN

Los Ruteadores Cisco soportan varias redes LAN ampliamente utilizadas. Las interfaces de Ruteador más comunes para redes LAN son Ethernet, Fast Ethernet, Token Ring de IBM, la Interfaz de Datos Distribuidos por Fibra Óptica (Fiber Distribuited Data Interfaz FDDI).

Todos estos protocolos LAN utilizan el mismo sistema de direccionamiento físico de la capa de enlace de datos (es decir, la dirección MAC de hardware en una NIC, o la dirección MAC de hardware ubicada en el controlador de la interfaz del Ruteador). Estas direcciones son únicas para cada dispositivo.

Todos los protocolos de LAN requieren una interfaz que coincida con la del Ruteador que utilizan. Por ejemplo, una red Token Ring sólo puede estar enganchada a un Ruteador que cuente con la interfaz apropiada Token Ring.

V.8.2 INTERFACES SERIE

Las interfaces en serie de un Ruteador permiten conectar varias redes LAN utilizando tecnologías WAN: Los protocolos WAN transmiten datos a través de interfaces asincrónicas y sincrónicas en serie (dentro de los Ruteadores), que están conectadas entre sí mediante líneas encontradas y otras tecnologías de conectividad suministradas por terceros.

Las tecnologías WAN de la capa del enlace de datos que más se utilizan en la actualidad son el Control de Enlace de Datos de Alto Nivel (High Level Data Link Control o HDLC, el X.25, Frame Relay) la Red Digital de Servicios Integrados (Integrated Services Digital Network o ISDN) y el Protocolo Punto a Punto (Point to Point Protocol o PPP). Todos estos protocolos WAN se configuran en determinadas interfaces del Ruteador (como interfaz en serie o en una interfaz RDSI) cuando el Ruteador se encuentra en el modo de configuración. Los comandos necesarios para dicha configuración, se tratará más adelante.

V.8.3 INTERFACES LOGICAS

Antes de dar por concluida esta explicación sobre la interfaces, conviene comentar brevemente las interfaces lógicas. Una interfaz lógica es una interfaz únicamente de software que se crea mediante el IOS de un Ruteador. El IOS (Sistema operativo de Interconexión de Redes) de Cisco se trata más adelante.

Las interfaces lógicas no existen como tales, es decir, no son interfaces de hardware de un Ruteador. Para entender el concepto de interfaz lógica, se puede considerar como una interfaz virtual creada por medio de una serie de comandos del software del Ruteador.

Los dispositivos reconocen estas interfaces virtuales como interfaces reales, lo mismo que una interfaz de hardware, como puerto serie. Se pueden configurar distintos tipos de interfaces lógicas en un Ruteador, como interfaces de retrobucle, interfaces nulas, e interfaces túnel.

V.8.4 INTERFACES RETROBUCLE

Una interfaz de retrobucle es una interfaz que emula una interfaz física real en el Ruteador. Los retrobucles suelen configurarse en un Ruteador de gama alta como un Ruteador de núcleo entre dos interconexiones corporativas de red o entre una red corporativa e Internet. Los Ruteadores que sirven como Ruteadores de núcleo se configuran con un protocolo externo de pasarela, como el Protocolo de Pasarela Fronteriza (BGP), que encamina los paquetes entre dos interconexiones distintas de redes.

Puesto que el Ruteador sirve como enlace fundamental entre interconexiones de redes, los paquetes de datos no deberían volcarse si una determinada interfaz física del Ruteador deja de funcionar. Por esto mismo, la interfaz virtual de retrobucle se crea y configura como la dirección de finalización para las sesiones del Protocolo de Pasarela fronteriza (BGP). De esta forma, el tráfico se procesa localmente en el Ruteador, lo que garantiza la recepción integra de los paquetes en su destino final.

V.8.5 INTERFACES NULAS

Otro tipo de interfaz lógica es la interfaz nula. Esta interfaz se configura en un Ruteador utilizando determinados comandos de Ruteador y sirve como muro de contención par impedir el paso de un determinado tráfico de red. Por ejemplo, si no desea el tráfico de una determinada red pase por un determinado Ruteador (y que lo haga por otros Ruteadores incluidos en la interconexión) se puede configurar la interfaz nula de forma que reciba y vuelque todos los paquetes que la red envíe en dicho Ruteador. Por lo general los listados de acceso se utilizan para filtrar el tráfico en una interconexión de redes y definir los Ruteadores que pueden utilizarse para determinadas redes. Comparada con los listados de acceso de interfaz nula sería como utilizar un mazo grande de hierro para tratar una gema en vez de utilizar los finos instrumentos de los que sirven los joyeros.

V.8.6 INTERFACES TUNEL

Una interfaz túnel es otra interfaz lógica que puede utilizarse para conducir un determinado tipo de paquetes a través de una conexión que normalmente no soporta dicho tipo de paquetes. Por ejemplo, se puede configurar una interfaz de túnel en cada uno de los dos Ruteadores que se encargan de encaminar paquetes AppleTalk desde sus respectivas redes LAN. Ambos Ruteadores estarían conectados por medio de una conexión en serie, como se muestra en la figura 5.14. La interfaz de túnel se configuraría para encaminar IP. Y aunque AppleTalk, no puede encaminarse normalmente a través de una interfaz IP., los paquetes AppleTalk se encapsularían (es decir, se meterían todos dentro de un sobre genérico) y después se conducirán a través del túnel como si fueran IP. Los Ruteadores de Cisco ofrecen el Protocolo Genérico de Encapsulacion del Ruteador (Generic Route Encapsulation Protocol o GRE), que se encarga de gestionar la encapsulación de paquetes transmitidos a través de una interfaz de túnel.

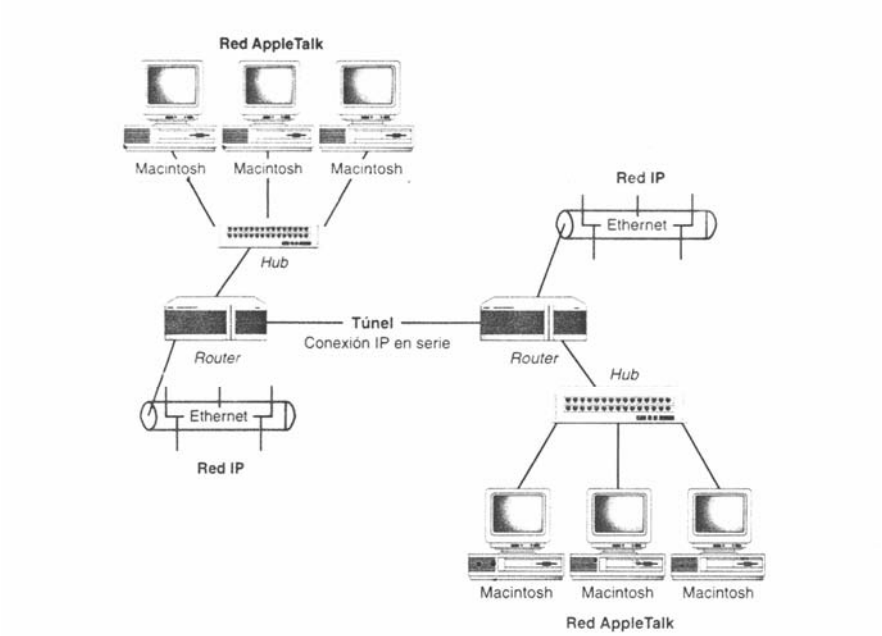


FIGURA 5.14 FLUJO DE PAQUETES APPLETALK EN UN TUNEL IP

V.9 INTRODUCCION AL SISTEMA OPERATIVO DE INTERCONEXION DE REDES

El Sistema Operativo de Interconexión de Redes (Internetworking Operating System ó IOS) de Cisco es el software que permite al hardware del Ruteador encaminar paquetes por una conexión entre redes. El IOS, como cualquier otro sistema operativo, proporciona el conjunto de comandos y funciones de software con lo que puede controlarse y configurarse el Ruteador, además de ofrecer la funcionabilidad que requieren los distintos protocolos, tanto encaminados como de encaminamiento, para hacer realidad la interconexión de redes.

Configurar un Ruteador significa activar las distintas interfaces y protocolos que lo integran. Deben utilizarse una serie de comandos para que interfaces como Ethernet o en serie puedan ejecutarse. También debe suministrarse información de configuración para los protocolos que se encaminan, como IP o IPX/SPX. Y tienen que configurarse igualmente los protocolos de encaminamiento, como RIP e IGRP. Una vez configurado el Ruteador, deben gestionarse los archivos de configuración. El listado que se ofrece a continuación presenta algunas de las tareas que tiene que ejecutar con el conjunto de comando del IOS:

- Configurar las interfaces LAN del Ruteador. La configuración de las interfaces LAN del Ruteador deben hacerse después de realizar las conexiones físicas, ensamblar el hardware del Ruteador y conectar los distintos cables a las redes LAN o WAN. Las interfaces del Ruteador deben configurarse para su uso en estas redes. Por ejemplo, una red que encamine IP, cada interfaz Ethernet que se utilice debe configurarse con la dirección IP y la mascara de subred que proceda.

- Configurar las conexiones en serie y los protocolos WAN. En aquellos casos en que el Ruteador este conectado a una red WAN por medio de una línea contratada o cualquier otra tecnología WAN, el protocolo WAN que se utilice en las interfaces en serie del Ruteador debe configurarse.

- Gestionar los archivos de configuración del Ruteador. Una vez configurado el Ruteador, conviene guardar alguna copia del mismo. La configuración de ejecución del Ruteador se almacena en la memoria NVRAM donde viene incluida como la configuración de arranque. También puede resultar oportuno conservar una copia de un archivo de configuración o cargarlo desde un servidor TFTP.

- Controlar y mantener el Ruteador. También tendrá que utilizarse el conjunto de comandos del IOS para controlar y resolver los posibles problemas que puedan surgir con el Ruteador. Asimismo; pasando un tiempo, resultará necesario actualizar el IOS del Ruteador dentro de la memoria Flash RAM. El conjunto de comandos proporciona todas las herramientas que se requieren para controlar el Ruteador y actualizar el IOS y el conjunto de características que este incluye.

Aunque este listado puede parecer exhaustivo, lo cierto es que no lo es en absoluto. El conjunto de comandos del IOS de CISCO es tan grande que serían necesarios varios temas para poder abarcarlos en su totalidad. Cisco publica en resumen de comandos de software para cada versión de IOS que comercializa. La referencia de comandos para la versión 11.3 del IOS contiene más de 1000 páginas. Aunque el volúmen pueda parecer increíble, lo cierto es que sólo se utilizan pocos comandos de IOS, incluso si uno se aficiona al encaminamiento y acaba trabajando con Ruteadores de gama alta en una gran conexión entre redes.

Cisco proporciona una Interfaz de Línea de Comandos (Command-Line Interfaz o CLI) que puede utilizarse para configurar y mantener el Ruteador. Para acceder a la CLI debe utilizarse una consola de Ruteador o conectar el Ruteador vía Telnet utilizando una Terminal virtual.

Si conoce DOS ó UNIX, la CLI le resultara muy similar. Se trata de una interfaz muy común de línea de comando. Si no está acostumbrado a trabajar con interfaces de línea de comandos, las figuras que se ofrecen a lo largo de los temas ayudarán a comprender los distintos comandos.

V.9.1 ESTRUCTURA DE COMANDOS

Los comandos del IOS se utilizan en los distintos modos del Ruteador: Usuario, Privilegiado y Configuración. Cada uno de estos modos proporciona su propio conjunto de comandos:

El modo Usuario sólo ofrece comandos básicos para visualizar la información sistema y ejecutar pruebas básicas.

El modo Privilegiado suministra un conjunto más amplio de comandos para visualizar la información del Ruteador, además de proporcionar acceso al modo Configuración.

El modo Configuración ofrece el conjunto de comandos que permiten configurar las interfaces y protocolos que se utilizan en el Ruteador.

V.9.2 COMANDOS EXEC

El IOS de Cisco utiliza un interpréte de comandos para ejecutar los comandos (interpreta el comando) denominado Exec. El modo Usuario y el modo privilegiado se consideran niveles distintos del interprete Exec. Por ello, cuando se lanza alguno de estos modos, los comandos allí disponibles revisten una determinada estructura básica: el comando seguido del parámetro del Ruteador. El comando no es más que uno de los comandos que incluye el IOS, como “show”, y el parámetro del Ruteador corresponde al elemento en el que se desea que actúe el comando.

Y así, y a modo de ejemplo, el comando show Ethernet 0 presenta los parámetros relacionados con la primera interfaz Ethernet del Ruteador. En la Fig. 5.15 se muestra este comando.

```
Router#show interface ethernet 0
Ethernet0 is administratively down, line protocol is down
  Hardware is Lance, address is 0010.7b81.65e9 (bia 0010.7b81.65e9)
  Description:
  Internet address is 0.0.0.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 252/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 02:11:34, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     77 packets output, 4620 bytes, 0 underruns
     77 output errors, 0 collisions, 13 interface resets
     0 babbles, 0 late collision, 0 deferred
     77 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

FIGURA 5.15 EJEMPLO DEL COMANDO “SHOW INTERFAZ ETHERNET 0”

Para ejecutarse los comandos que se utilizan en los distintos modos del Ruteador, siempre debe pulsarse la tecla Intro después de introducir el comando. Los resultados de dicho comando pasan entonces a mostrarse en la consola del Ruteador ó en la pantalla de la Terminal virtual.

V.9.3 EL SISTEMA DE AYUDA DEL IOS

Al margen del modo en el que se encuentre, el IOS puede proporcionarle ayuda. No nos estamos refiriendo al típico sistema de ayuda con ventanas y mensajes emergentes a los que nos tiene acostumbrados Microsoft y los programas basados en Windows, sino a un tipo de ayuda más sútil y bastante aceptable teniendo en cuenta que se trata de una interfaz de línea de comandos.

Supongamos que se encuentra en el modo Usuario y desea ver el listado completo de los comandos disponibles. Para ello, sólo tiene que introducir el signo de interrogación “?” y después pulsar Intro. El listado de comandos aparecerá en la pantalla de la consola como se muestra en al figura 5.16.

```
Router>?
  Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
--More--
```

FIGURA 5.16 EJEMPLO DEL COMANDO DE AYUDA EN IOS

Una vez consultados los comandos disponibles en el modo Usuario, decide utilizar un determinado comando, pero no sabe exactamente como debe introducirse ese comando en el indicador. Por ejemplo, quiere saber como se utiliza el comando **show.** Para ello, tiene que escribir show (o el comando del que se desea obtener ayuda) en el indicador seguido del signo “?” (No olvidar insertar un espacio entre ***show*** y el signo de interrogación; en caso contrario, aparecerá un mensaje de comando erróneo), y después pulse Intro. El sistema le proporcionara la ayuda específica para el comando seleccionado, como se muestra en la figura 5.17.

```
Router>show ?
  alps           Alps information
  backup         Backup status
  clock          Display the system clock
  compress       Show compression statistics
  dialer         Dialer parameters and statistics
  drip           DRiP DB
  flash:         display information about flash: file system
  fras-host      FRAS Host Information
  history        Display the session command history
  hosts          IP domain-name, lookup style, nameservers, and host table
  kerberos       Show Kerberos Values
  location       Display the system location
  management     Display the management applications
  modemcap       Show Modem Capabilities database
  ncia           Native Client Interface Architecture
  ppp            PPP parameters and statistics
  rmon           rmon statistics
  rtr            Response Time Reporter (RTR)
  sessions       Information about Telnet connections
  sgbp           SGBP group information
  snmp           snmp statistics
  tacacs         Shows tacacs+ server statistics
  terminal       Display terminal configuration parameters
  traffic-shape  traffic rate shaping configuration
  users          Display information about terminal lines
  version        System hardware and software status
  vpdn           VPDN information

Router>show |
```

FIGURA 5.17 EJEMPLO DE AYUDA DESPUES DE COMANDO "SHOW"

Una vez obtenida la ayuda sobre un comando específico, el propio comando se insertará automáticamente en el indicador de comandos (véase la figura 5.14). Puede entonces especificar parámetros para el comando y después pulsar Intro para que se ejecuten. Por ejemplo, en el caso del comando "***show",*** puede añadir **versión** al comando y después pulsar Intro. Los parámetros relacionados con la versión instalada del IOS se mostraran en pantalla.

Como dijimos anteriormente, el sistema de ayuda también esta disponible en los modos Privilegiado y Configuración. La ayuda del modo Privilegiado se parece a la suministrada en el modo Usuario. Para obtener información general sólo tiene que introducir "¿"; si desea información más especifica, tiene que escribir el comando seguido de "?".

V.10 UTILIZAR LOS DISTINTOS MODOS DEL RUTEADOR

Puede empezar a examinar los distintos modos de los que dispone el Ruteador. El Ruteador ofrece tres modos básicos de acceso. El modo **User** (Usuario), el modo **Privileged** (Privilegiado) y el modo **Configuration** (Configuración).

Cada uno de estos modos básico de Ruteador proporciona un grado más alto de acceso a la configuración del Ruteador y permiten, en mayor ó menor grado, modificar la configuración del Ruteador. El listado siguiente presenta una breve descripción de cada uno de estos tres modos:

Modo Usuario: Este modo proporciona un acceso limitado al Ruteador. Se ofrece una serie de comandos no destructivos que permiten examinar algunos parámetros de configuración del Ruteador.

Modo Privilegiado. Conocido también como modo de Activación (Enable), este modo permite examinar en más profundidad el Ruteador y proporciona un conjunto de comandos más robustos que le modo Usuario. Tras acceder al modo Privilegiado utilizando la contraseña secreta ó de activación (si no se especifico una contraseña secreta cifrada), se puede acceder a los comandos de configuración que proporciona el modo de Configuración y editar, por tanto, la configuración del Ruteador.

Modo Configuración. También llamado modo de Configuración Global, este modo se lanza desde el modo Privilegiado y proporciona todos los comandos de configuración del Ruteador. Existen además subconjuntos del modo Configuración para los protocolos, interfaces y otros aspectos relativos a la operación del Ruteador.

V.10.1 MODO USUARIO (NO PRIVILEGIADO)

Como acabamos de decir, el modo Usuario permite examinar, de forma limitada, la configuración del Ruteador. El modo Usuario es el modo que se activa por defecto al volver a arrancar el Ruteador. El acceso a este modo también puede protegerse por medio de una contraseña de consola.

En la figura 5.18 se muestra el indicador del modo Usuario para el Ruteador que hemos configurado antes utilizando el cuadro de dialogo **System.** El indicador corresponde del nombre Ruteador seguido del signo “>” (mayor que). En esta figura también se muestra una parte de los resultados del comando **show interfaces.**

```
Router>sh inter
Ethernet0 is administratively down, line protocol is down
  Hardware is Lance, address is 0010.7b81.65e9 (bia 0010.7b81.65e9)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 252/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 02:11:34, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     77 packets output, 4620 bytes, 0 underruns
     77 output errors, 0 collisions, 13 interface resets
     0 babbles, 0 late collision, 0 deferred
     77 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

FIGURA 5.18 EL MODO USUARIO PERMITE EXAMINAR LA INFORMACIÓN DE CONFIGURACIÓN DEL RUTEADOR UTILIZANDO UN NÚMERO LIMITADO DE COMANDOS.

El funcionamiento del modo Usuario puede equiparse a la conocida formula de “se puede mirar pero no tocar”. Sin embargo, lo que si ofrece es una gran cantidad de información del Ruteador y de su actual estado.

V.10.2 MODO PRIVILEGIADO

El modo Privilegiado proporciona todos los comandos incluidos en el modo Usuario, además de ofrecer un amplio conjunto de comandos para examinar el estado del Ruteador (como el comando **show running-config** que permite examinar la configuración actual de ejecución para e Ruteador). El modo Privilegiado también proporciona el comando **config** que permite lanzar el modo de Configuración del Ruteador.

Como el modo Privilegiado se puede de hecho controlar el Ruteador. Por ello, es importante asignar una buena contraseña de activación para impedir que alguien modifique la configuración de su Ruteador (si alguien tiene que acceder a algunos de los parámetros del Ruteador, siempre podrá hacerlo desde el modo Usuario).

Para lanzar el modo Privilegiado en un Ruteador, se debe escribir **enable** en el indicador del modo Usuario y después pulsar Intro. Después, deberá introducirse la contraseña (la contraseña secreta y cifrada que asigno el Ruteador) y volver a pulsar Intro. En la Figura 5.19 se muestra el modo Privilegiado del Ruteador después de invocar el comando **show running-config**. El indicador del modo Privilegiado es el nombre de Ruteador seguido por el carácter de gato "#" (numero).

```
Router#show running-config
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
ip subnet-zero
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
--More--
```

FIG. 5.19 EL MODO PRIVILEGIADO PERMITE EXAMINAR LA CONFIGURACIÓN DEL RUTEADOR GRACIAS A UN AMPLIO CONJUTO DE COMANDOS, LANZAR EL MODO CONFIGURACIÓN.

Una vez finalizado el trabajo en el modo Privilegiado, lo normal es volver al modo Usuario. Si no lo hace, dejara la configuración del Ruteador al descubierto y cualquiera que accediera por la Terminal podría modificarla. Para ver al modo Usuario, introduzca **disable** y pulse Intro. Si desea desconectarse del Ruteador, escriba **logout** y pulse Intro. De esta forma, la próxima persona que utilice la consola tendrá que introducir la contraseña del Ruteador (si existe una) para lanzar el modo Usuario.

V.10.3 MODO CONFIGURACION

El modo Configuración permite determinar todos los parámetros relacionados con el hardware y el software del Ruteador. Aquí pueden configurarse las interfaces los protocolos encaminados y de encaminamiento. También puede establecerse las contraseñas del Ruteador y configurar los protocolos WAN que utilizan las interfaces en serie del Ruteador Algunas de las opciones de configuración referidas al Ruteador pueden establecerse en un Ruteador nuevo desde el cuadro de dialogo System Configuration. El modo Configuración permite acceder a todos los comandos que requieren para configurar ó ajustar la configuración del Ruteador.

Al modo de Configuración se accede desde el modo Privilegiado. Para ello, debe escribirse **config** en el indicador del modo Privilegiado y después pulsar Intro.

V.10.3.1 UTILIZAR EL MODO DE CONFIGURACION

En el indicador del modo Privilegiado, introduzca **config** y pulse intro.

El sistema le preguntará si desea realizar la configuración desde la Terminal, la memoria o la red. La opción predeterminada es la consola, así que pulse Intro para continuar.

Para cambiar el nombre al Ruteador, escriba hostname [nombre], donde “nombre” se refiere al nuevo nombre que desee asignar al Ruteador. Una vez introducido el comando, pulse Intro. El nombre nuevo del Ruteador se mostrará en el indicador del modo Configuración (véase la figura 5.20).

```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname prueba
prueba(config)#
```

FIGURA 5.20 EN EL MODO CONFIGURACIÓN PUEDE CAMBIAR EL NOMBRE DEL RUTEADOR.

V.11 TABLAS DE RUTEO

Las tablas de ruteo sobre las que se basan las decisiones de enrutamiento pueden ser configuradas de dos modos:

a) Estáticamente, definidas en el momento de la instalación y manipulables por los administradores de la red. Los Ruteadores que las utilizan son eficientes, aunque obligan a un procedimiento de configuración largo y tedioso.
b) Dinámicamente, utilizado algoritmos automáticos. Los Ruteadores son más fáciles de configurar, pero pueden llegar a incrementar el sobreencabezado de la red por los continuos intercambios de información de control entre los Ruteadores instalados.

V.11.1 ALGORITMOS DE RUTEO

Existen varios algoritmos de ruteo; algunos de ellos ya empiezan a estar diseñados para trabajar adecuadamente con las nuevas redes digitales a velocidades medias y altas:

V.11.1.1 RIP (ROUTING INFORMATION PROTOCOL) describe la red en términos de saltos (hops) que indican el número de Ruteadores que un paquete debe atravesar antes de llagar a su destino. Una versión modificada fue la adoptada por el TCP/IP. No es apropiado para redes muy grandes pues sobrecargan en exceso los enlaces por el intercambio frecuente de tablas de ruteo.

V.11.1.2 OSPF (OPEN SHOREST PATH FIRST) más sofisticado que el anterior, utiliza tablas configuradas por los administradores de red con parámetros como retardo, ancho de banda, coste de las comunicaciones, etc. Permite topologías complejas y es apropiado para redes grandes, pues soporta bien los cambios de topologías. El MOSPF es la versión multicast.

V.11.1.3 PPP (POINT TO POINT PROTOCOL) es un protocolo propuesto por Internet que permite a los Ruteadores intercambiar información a través de enlaces punto apunto. Es casi un estándar hecho como protocolo de enlace de redes extensas y en entornos cliente-servidor. La principal ventaja es que puede negociar parámetros referentes a la configuración, calidad de la línea, autentificación de acceso y protocolos de red.

V.11.1.4 MLPPP (MULTILINK PPP) es la evolución del PPP hacia los nuevos entornos digitales, conmutados y mutiprotocolo como RDSI, FRL y ATM. (Figura 5.21). Permite configurar múltiples enlaces y CV independientemente de la red WAN utilizada que pueden ser activados dinámicamente según el ancho de banda requerido. Además limita el tráfico entre Ruteadores estrictamente necesario, evitando que los paquetes de control atraviesen continuamente la WAN consiguiendo así un ahorro económico importante.

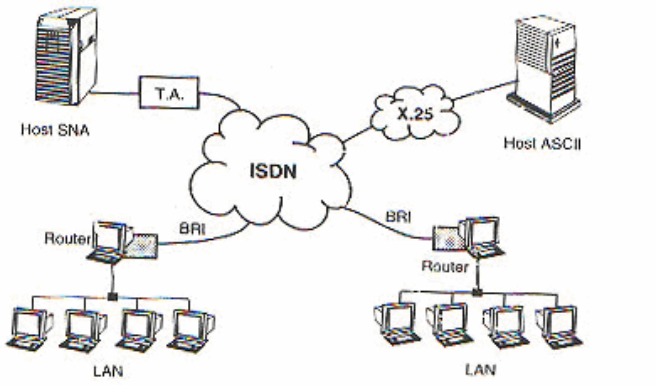


FIGURA 5.21 EJEMPLO DE RED MULTIPROTOCOLO

V.12 CONFIGURACION DE HDLC

A continuación se dará la configuración en el Ruteador en la Interfaz Serial para protocolos HDLC.

V.12.1 COMPRENDER LAS INTERFACES EN SERIE Y WAN

Los Ruteadores también pueden conectarse a varias tecnologías WAN y protocolo WAN. Las interfaces en serie en el Ruteador proporcionan la conectividad que requieren

las distintas tecnologías WAN, por ejemplo, los Ruteadores que estén conectados remotamente a otros Ruteadores mediante RDSI, utilizarán normalmente interfaz RDSI.

Vamos a describir los comandos del IOS de Cisco que permiten configurar distintos protocolos de WAN en el Ruteador o Ruteadores. La conectividad WAN, en general, ha mejorado en estos últimos años su relación coste-eficiencia. Donde antes las compañías tenían que utilizar una línea de conexión conmutada a 56K dado su relativo bajo costo, ahora pueden permitirse utilizar Frame Relay a través de una línea E1 por prácticamente el mismo coste.

El tipo de conexión que debe utilizar depende, sin duda alguna del coste y la velocidad de la línea. Antes de tomar una decisión sobre una conexión WAN, es preciso evaluar todas las posibilidades.

Por lo general, los Ruteadores funcionan como Equipo Terminal Digital (Digital Terminal Equipment o DTE), por lo que se requiere de un cable DTE que este conectado al puerto serie del Ruteador y de ahí a un dispositivo CSU/DSU, que normalmente se conoce como Equipo Digital de Comunicaciones (Digital Communication Equipment o DCE), que esta enganchado a la línea que proporciona la compañía telefónica. El dispositivo CSU/DSU proporciona la velocidad de reloj para la transmisión sincrónica.

Puede consultar rápidamente la encapsulación (el protocolo WAN determinado) para una interfaz en serie utilizando el comando **show interfaz serial** [***numero de interfaz***]. El número interfaz corresponde a la interfaz en serie que desee examinar. Por ejemplo, para consultar la interfaz en serie 0, debería utilizar el comando show interfaz serial 0 (recuerde que puede abreviar sus comandos). En la figura 5.22 se muestra los resultados de este comando.

```
Router Con0 is now available

Press RETURN to get started.



Router>sh inter s0
Serial0 is administratively down, line protocol is down
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 17 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
Router>
```

FIGURA 5.22 EJEMPLO DE COMANDO "SHOW INTERFAZ SERIAL0"

V.12.2 ENCAPSULACION

Como ya sabemos, todas las comunicaciones de la red se crean en un origen y se envían a un destino. La información que se envía por la red se denomina datos o paquetes de datos. Si una computadora (Host A) quiere enviar datos a otra computadora (Host B), los datos deben empaquetarse primero mediante un proceso llamado encapsulación. La encapsulación envuelve los datos con la información de protocolo necesaria antes de su transito por la red.

Por lo tanto, mientras el paquete de datos baja por las capas del modelo OSI, recibe las cabeceras, la información final y otra información.

Para ver como se muestra en la Figura 5.23. Cuando los datos se envían desde el origen, como se puede ver, el empaquetamiento y el flujo de datos se intercambian mientras la red realiza su servicio para los usuarios finales.

Los datos, con forma de señales eléctricas, deben viajar por el cable hasta la computadora destino y, después, convertirse en su formato original para que puedan ser leídos por el destinatario. Como se puede imaginar, este proceso se realiza mediante varios pasos. Por este motivo, los diseñadores de hardware, software y protocolos han reconocido que la manera más eficiente de implementar las comunicaciones de red sería un proceso de creación de capas.

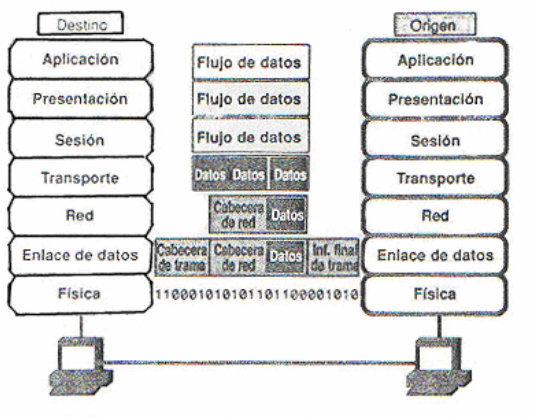


FIGURA 5.23 PROCESO DE ENCAPSULACIONDE DATOS

Como se muestra en la figura 5.24, las redes deben realizar los siguientes pasos de conversión para encapsular los datos:

1. **Construir los datos**. Cuando un usuario envía un correo electrónico, sus caracteres alfanuméricos se convierten en datos para que puedan viajar por la internetwork.
2. **Empaquetar los datos para el transporte de extremo a extremo**. Los datos se empaquetan para el transporte por la internetworking de redes. Usando segmentos, la función de transporte asegura que los hosts de ambos extremos del sistema de corre electrónico pueden comunicarse con total fiabilidad.
3. **Añadir la dirección de red a la cabecera**. Los datos se colocan en un paquete, o datagrama, que contiene una cabecera de red con direcciones lógicas de origen y

destino. Dichas direcciones ayudan a los dispositivos de red a enviar paquetes a través de la red a lo largo de una ruta seleccionada dinámicamente.

4. **Agregar (añadir) la dirección local a la cabecera de enlace de datos**. Cada dispositivo de la red debe colocar el paquete en una trama. La trama incluye una cabecera con la dirección física del siguiente dispositivo conectado directamente en la misma ruta.
5. **Convertir los bits para la transmisión**: La trama se debe convertir en un modelo de 1 y 0 (bits) para su transmisión por medio (normalmente un cable). Una función de cronometraje permite a los dispositivos distinguir a los bits mientras viajan por el medio. El medio de la internetworking física puede variar a lo largo de la ruta que se haya empleado. Por ejemplo, un correo electrónico puede originarse en una LAN, cruzar el backbone de un campus y salir a un enlace WAN hasta que alcance su destino en otra LAN remota.

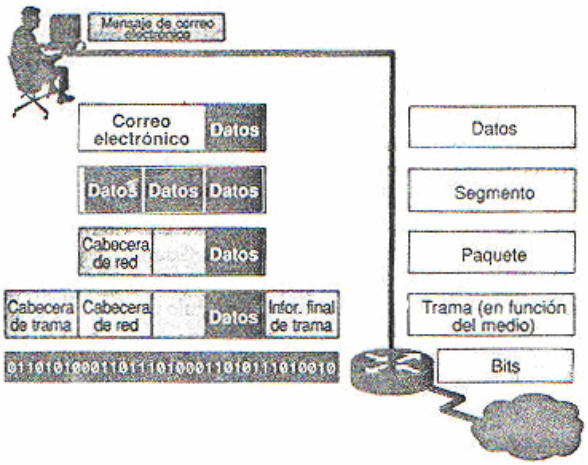


FIGURA 5.24 PASO A PASO EL ENCAPSULAMIENTO DE DATOS

V.12.2.1 ENCAPSULACION NO ES SÓLO UNA PALABRA BONITA

Cuando se configura interfaces en serie con determinado protocolo WAN, esta utilizando de hecho el comando de encapsulación seguido del nombre de protocolo. La encapsulación es el proceso de empaquetar datos en un determinado encabezado de protocolo. Por ejemplo, los datos Ethernet se encapsulan en un encabezado Ethernet antes de ser transmitidos por la red. En aquellos casos en que se transmiten tramas Ethernet por una conexión WAN, toda la trama se ubica (o se encapsula) en un tipo de trama determinado por el protocolo WAN utilizado, como el HDLC o PPP.

V.12.3 DESENCAPSULACION

Cuando el dispositivo remoto recibe una secuencia de bits, la pasa de enlace de datos para manipular las tramas. Cuando la capa de enlace de datos recibe la trama, hace lo siguiente:

- Lee la dirección física y otras informaciones de control que proporciona la capa enlace de datos conectada directamente.
- Interpreta la información de control de la trama, creando el datagrama.

- Pasa el datagrama a la siguiente capa, siguiendo las instrucciones que aparecen en la zona de control de la trama.

Este proceso se conoce como desencapsulación. Cada capa subsiguiente realiza un proceso de desencapsulación similar.

V.12.4 CONFIGURAR EL CONTROL DE ENLACE DE DATOS DE ALTO NIVEL (HDLC)

HDLC es un protocolo WAN de punto a punto que se utiliza como protocolo WAN predeterminado en los Ruteadores de Cisco. Por defecto viene siempre activado. Si no esta activado en su Ruteador, un sencillo comando de encapsulación activa HDLC. Otro parámetro que debe facilitarse al configurar HDLC es el ancho de banda. Corresponde al rendimiento efectivo de la línea que se ha contratado (por ejemplo, una línea de 56 K tiene un ancho de 56). El ancho de banda se mide en kilobits por segundo y es un parámetro necesario si se utiliza IGRP como protocolo, ya que IGRP utiliza el ancho de banda como una de sus métricas.

Si HDLC no esta como un protocolo WAN configurado para una determinada interfaz, se puede activar fácilmente siguiendo los pasos que se especifican a continuación.

V.12.4.1 CONFIGURAR HDLC EN UNA INTERFAZ SERIE

1. En el indicador del modo Privilegiado escriba config t, y después pulse Intro. Se lanzará el modo Configuración Global.
2. Para configurar una determinada interfaz WAN, introduzca el nombre de la interfaz en el indicador, como **interfaz serial 1**, después pulse Intro. El indicador se pasará al modo **config-if.**
3. Escriba ***encapsulación HDLC***, y después pulse Intro.
4. Si tiene que especificar el ancho de banda para la interfaz, escriba ***bandwidth [kilobits/segundo]***, donde kilobits/segundo corresponde a la velocidad de transmisión de la línea. Por ejemplo, para una línea de 56K, tendría que escribir ***bandwidth 56***, y después pulsar Intro para hacer efectivo el comando (vease la figura 5.25)
5. Para cerrar la sesión de configuración de la interfaz, pulse Ctrl.+Z.
6. Pulse de nuevo Intro para volver al modo privilegiado.

```
Router Con0 is now available

Press RETURN to get started.


Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial 1
Router(config-if)#encapsulation HDLC
Router(config-if)#bandwidth 56
Router(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

FIGURA 5.25 EJEMPLO DE CONFIGURACION HDLC EN RUTEADOR

V.13 ALGORITMO DE PROTOCOLO IGRP (Interior Gateway Routing Protocol)

Ahora vamos a describir el algoritmo de protocolo IGRP

V.13.1 INTRODUCCION

El Protocolo de Ruteo de Pasarela Interior (Interior Gateway Routing Protocol [IGRP]) es un protocolo de ruteo que fue desarrollado a la mitad de los 80's por Cisco Systems, Inc. La principal meta de Cisco en la creación de IGRP fue proporcionar un protocolo robusto para el ruteo con un Sistema Autónomo (AS). Tales protocolos son conocidos como Protocolos de Ruteo de Pasarela Interior.

En la mitad de los 80's, el Protocolo de Ruteo de Pasarela Interior más popular fue el Protocolo de Información de Ruteo (Routing Information Protocol [RIP]). Aunque RIP fue bastante usado para ruteo con un pequeño tamaño moderado, relativamente interredes homogéneas, los límites estuvieron siendo empujados por las redes crecientes. En particular, el limite de saltos es pequeño es de 16 en RIP restringido al tamaño de las interredes, la única métrica (cuenta de saltos) soportada de solamente el igual del costo de la carga balanceada (solamente en redes Cisco) no permitió para mucho ruteo flexible en complejos entornos. La popularidad de los Ruteadores Cisco y la robustez del IGRP incito muchas organizaciones con extensas interredes para reemplazar RIP por IGRP.

La inicial implementación IGRP de Cisco trabajo en las redes con Protocolos de Internet (Internet Protocol [IP]). IGRP fue diseñado para operar en cualquier entorno de red, sin embargo, Cisco pronto lo porto para operar en OSI para redes con Protocolo de Redes sin Conexiones (Connectionless-Network Protocol [CLNP]). Cisco desarrollo el IGRP Mejorado (Enhanced IGRP) a principio de los 90's para mejorar la eficiencia de la Operacion de IGRP.

V.13.2 CARACTERISTICAS DEL PROTOCOLO IGRP

IGRP es una vector de distancia Interior Gateway Protocol (IGP). El vector de distancia rutea a los protocolos matemáticamente comparando ruteos usando medidas de distancia. Esta medida es conocida como el vector de distancia. Los Ruteadores usan un protocolo de vector de distancia debe ser enviado a todas o a una porción de sus tablas de ruteo en un mensaje de actualización de ruteo en intervalos regulares para cada de sus Ruteador vecinos. Como una información de ruteo prolifera a través de la red, los Ruteadores pueden identificar nuevos destinos como ellos agreguen a la red, aprenden de las fallas de la red, y lo más importante, calculan distancia para todos los destinos conocidos.

El vector de distancia de los protocolos de ruteo es frecuentemente contrastado con el estado del enlace de los protocolos de ruteo, el cual envía una información local para todos los nodos de la interred. IGRP usa una métrica compuesta que es calculada por la factorizacion del peso matemático de los valores para el retraso de la red, ancho de banda, seguridad y carga. Administradores de red pueden poner los factores de peso para cada una de estas métricas, aunque con gran cuidado debe ser tomado antes de

cualquier valor por omisión sea manipulado. IGRP proporciona un amplio rango para estas métricas. La seguridad y la carga, por ejemplo, pueden tomar cualquier valor entre 1 y 255, el ancho de banda puede tomar valores de velocidades reflejantes de 1200 bps a 10 Gbps, mientras el retraso puede tomar cualquier valor de 1 a 224. Estos rangos amplios de métricas están mas allá complementados por una serie de constantes definidas por el usuario que habilita a un administrador de red para influenciar la selección de ruta. Estas constantes son disueltas contra las métricas, y cada uno, en un algoritmo que produce uno solo, la métrica compuesta. Entonces, el administrador de red puede influir en la selección de ruta para dar el más alto o el más bajo peso especifico de métricas. Esta flexibilidad permite a los administradores un tono fino de la selección automática del IGRP.

Para proporcionar la flexibilidad adicional, IGRP permite el ruteo de multicamino. Múltiples caminos pueden tener métricas desiguales todavía para ser validas a rutas multicamino. Por ejemplo, si un camino es 3 veces mejor que otro camino (esta métrica es tres veces más bajo), el mejor camino será usado tres veces como sea necesario. Solamente en rutas con métricas que están dentro de un cierto rango ó con variancia con la mejor ruta están usando como multicaminos. La variancia es otro valor que puede ser establecido por el administrador de red.

V.13.3 CARACTERICITICAS DE ESTABILIDAD

IGRP proporciona un número de características que son diseñadas para mejorar la estabilidad. Estos incluyen caídas sostenidas (holddowns), división horizontal (split horizons), actualizaciones de revocación venenoso (poison-reverse).

Las caídas sostenidas (holddowns) son usadas para prevenir los regulares mensajes de actualización de la inapropiada rehabilitación de una ruta que habría ido mal. Cuando el Ruteador se cae, los Ruteador vecinos detectan esta vía la falta de regulares mensajes de actualizaciones programados. Estos Ruteadores pueden calcular nuevas rutas y enviar los mensajes actualización de ruteo para informar a los vecinos de la carga de la ruta. Esta actividad comienza con una oleada de actualizaciones disparadas que filtran a través de la red. Estas actualizaciones disparadas no llegan instantáneamente a cada dispositivo de red. Por lo que, esto es posible para un dispositivo que todavía debe ser informado de la falla de red para enviar un regular mensaje de actualización, el cual advierte una ruta fallida como siendo válida para un dispositivo que ha sido notificado de la falla de la red. En este caso, el dispositivo sustituirá el contenido (y advierte potencialmente) de la información de ruteo incorrecta. Las caídas sostenidas dicen a los Ruteador sostener la caída en cualquier cambio que podría afectar rutas de algunos períodos de tiempo. El período de la caída sostenida usualmente es calculado para ser más grande que el período de tiempo necesario para actualizar a la red entera del cambio de ruta.

División horizontal (split horizons) deriva de la premisa que este nunca es útil para enviar información acerca de la ruta de regreso en la dirección del cual este regreso. La Figura 5.26 ilustra la regla de la division horizontal. El Ruteador 1 (R1) advierte que tiene una ruta a la Red A (Network A). No hay razón para que el Ruteador 2 (R2) incluya esta ruta en la actualización de regreso para el R1 por que el R1 esta más cerca a la Red A. La regla de división horizonal dice que R2 debe debe parar esta ruta de cualquier

actualización que este envía a R1. La regla de división horizontal ayuda a prevenir rutas cíclicas. Considerar, en el ejemplo, el caso en el cual la interfase del R1 a la Red A cae. Sin división horizontal, R2 continua informando a R1 que puede obtener la Red A (a través de R1). Si R1 no tiene suficiente inteligencia, de hecho recogería la ruta de R2 como una alternativa para esta falla de conexión directa, causando una ruta cíclica. Aunque la caída sostenida debe prevenir esto, la división horizontal es implementada en IGRP por que proporcionan estabilidad extra al algoritmo.

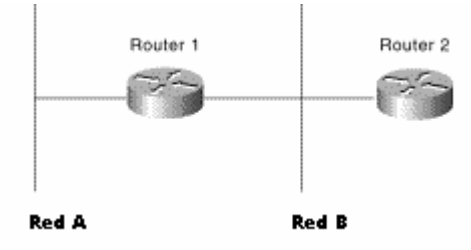


FIGURA 5.26 LA REGLA DE DIVISION HORIZONLA AYUDA A PROTEGER CONTRA RUTAS CILCICAS.

Las divisiones horizontales deben prevenir rutas cíclicas entre los Ruteador adyacentes, pero las actualización de revocación de veneno (poison-reverse) son necesarias para vencer largas rutas cíclicas. Incrementos en las rutas métricas generalmente indican rutas cíclicas. Las actualizaciones de revocación de veneno las envían para remover la ruta y situarlo en una caída sostenida. La implementación de Cisco de IGRP, las actualizaciones de revocación de veneno son enviadas si una ruta métrica ha incrementado por un factor de 1.1 o mayor.

V.13.4 TEMPORIZADORES (TIMERS)

IGRP mantiene un número de temporizadores y variables que contienen intervalos de tiempo. Estos incluyen un temporizacion de actualización, un temporizador inválido, un período de tiempo sostenido, y un temporizador de cadena. El temporizador de actualización específica que tan frecuente los mensajes de actualización de ruteo deben ser enviados. El valor por omisión en IGRP de este variable es de 90 segundos. El temporizador inválido específica cuanto una ruta debe espera la ausencia de los mensajes de actualización de la ruta acerca de una ruta específica antes de declarar la ruta inválida. El valor por omisión para este variable es de 3 veces el periodo actual. La variable de tiempo sostenido, específica el periodo de caída sostenida. El valor por omisión IGRP para esta variable es 3 veces el período del temporizador de actualización más 10 segundos. Finalmente, el temporizador de cadena indica cuanto tiempo debe pasar antes de que una ruta deba ser encadenada de la tabla de rutas. El valor por omisión IGRP de esta variable es de 7 veces el periodo de la actualización de ruta.

V.13.5 CONCEPTO GENERAL

IGRP ha probado ser uno de los más exitosos protocolos de ruteo de todo el tiempo. No para pequeñas redes de este éxito debido a la funcional similitud a RIP, un simple grande y amplio éxito desplegado en el protocolo de ruteo. Cisco tomo los grandes dolores para cuidar y preservar muchas de las características de RIP, mientras una gran

expansión de estas capacidades. Hoy, IGRP esta mostrando en esta época: la falta de soporte por Mascara de Subredes de longitud variable (variable-length subnet masks [VLSM]). Se prefirió un desarrollo del IGRP versión 2 para incorporar esta capacidad, Cisco ha construido una mejora del legado IGRP de éxitos con IGRP Mejorado (Enhanced IGRP).

V.13.6 CONFIGURANDO IGRP

IGRP es un dinámico protocolo de ruteo de vector de distancia diseñado por Cisco en la mitad de 80's para un ruteo en un Sistema Autónomo que contiene redes amplias y complejas arbitrariamente con un diverso ancho de banda y características de retraso.

V.13.7 LA IMPLEMENTACION IGRP DE CISCO

IGRP usa una combinación de métricas configurable por el usuario, incluyendo el retraso de la interred, ancho de banda, seguridad y carga.

IGRP también advierte 3 tipos de rutas: interior, sistema y exterior, como se muestra en la Figure 5.27. Las rutas interiores son las rutas entre subredes en la red adjunta a una interfaz del Ruteador. Si la red adjunta a un Ruteador no es una subred, IGRP no avisa de las rutas interiores.

Las rutas de sistema son rutas para redes con un Sistema Autónomo. El software IOS de Cisco deriva rutas de sistema de las interfaces de la red conectada directamente y la información de la ruta de sistema proporcionada por otros Ruteadores que operan IGRP ó servidores de acceso. Las rutas de sistema no incluyen la información de la subred.

Las rutas exteriores son rutas para redes fuera del Sistema Autónomo que son considerados cuando identifican una pasarela del último extremo. El software IOS de Cisco escoge una pasarela para el último extremo de la lista de rutas exteriores que IGRP proporciona. El software usa la pasarela (Ruteador) del último extremo si no tiene una mejor ruta para un paquete y el destino no está a una red conectada. Si el Sistema Autónomo tiene más que una conexión a una red externa, los diferentes Ruteadores pueden escoger diferentes Ruteadores exteriores como la pasarela del último extremo.

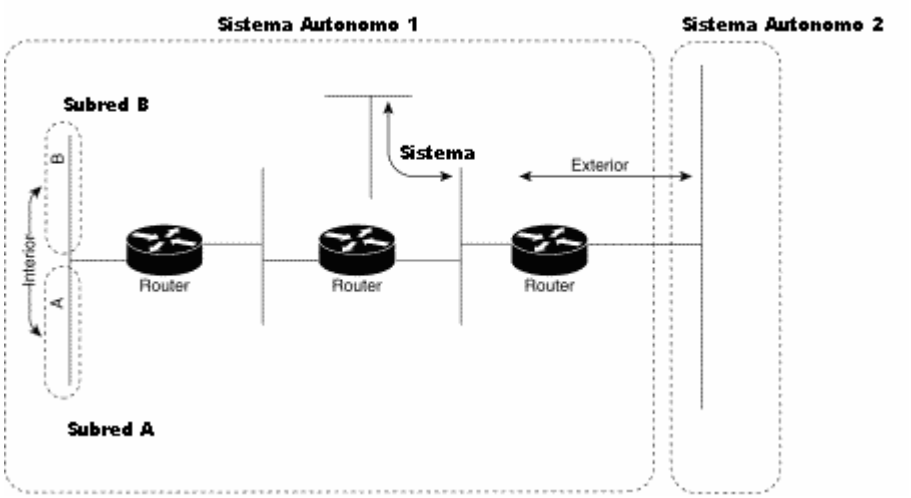


FIGURA. 5.27 RUTAS INTERIORES, SISTEMA Y EXTERIORES

V.13.8 ACTUALIZACIONES IGRP

Por omisión, un Ruteador que opera IGRP envía una difusión de actualización (broadcast) cada 90 segundos. Este declara una ruta inaccesible si no recibe una actualización del primer Ruteador en la ruta con tres períodos de actualización (270 segundos). Después de 7 periodos de actualización (630 segundos), el software IOS de Cisco remueve la ruta de la tabla de ruteo.

IGRP usa la actualización rápida y la actualización de revocación de veneno para acelerar la convergencia del algoritmo de ruteo. La actualización rápida es el envío de una actualización más rápida que el periódico estándar del intervalo de actualización de notificación de otros Ruteadores de un cambio de métrica. Las actualizaciones de revocación de veneno son enviados a remover una ruta y situarla en la caída sostenida, el cual mantiene nueva la información de ruteo del que esta siendo usado por un cierto periodo de tiempo.

V.13.9 CREANDO EL PROCESO DE RUTEO IGRP

Para crear el proceso de ruteo de IGRP, usa los siguientes comandos, comenzando desde el modo de configuración global:

	Comando	Objetivo
Paso 1	Ruteador(config)# **Ruteador igrp** as-number	Habilita un proceso de ruteo de IGRP, el cual te sitúa en el modo de configuración del Ruteador.
Paso 2	Ruteador(config-Ruteador)# network ***network-number***	Asocia las redes con un proceso de ruteo IGRP.

IGRP envía actualizaciones a las interfaces en las redes específicas. Si la red de una interfase no esta especificada, la interfaz no será avisada en cualquier actualización IGRP.

No es necesario tener registrado el número de Sistema Autónomo para usar IGRP. Si tú no tienes el número registrado, tú eres libre de crear el propio. Los sistemas Cisco recomiendan que si tú tienes un número registrado, lo utilices para identificar el proceso IGRP.

V.14 REDUNDANCIA DE SISTEMAS

En un sentido estricto, en ingeniería, la duplicación de componentes críticos de un sistema con la intención de incrementar la disponibilidad del sistema es llamado redundancia. Los sistemas de seguridad crítica, tal como el cableado de un avión, algunas partes del sistema de control pueden ser triplicadas. Un error en uno de los componentes puede entonces estar fuera de elección para los otros dos. En un sistema de redundancia triple, el sistema tiene 3 componentes, todos ellos deben fallar antes de que falle el sistema.

La redundancia es la parte del mensaje que podría omitirse sin que se produzca pérdida de información. Cualquier sistema de comunicación introduce algún grado de redundancia, para asegurar que no hay pérdida de información esencial, o sea para asegurar la perfecta recepción del mensaje. Como sabemos un Ruteador es un dispositivo de ***propósito general*** diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN. Además el diseño de la red determina cuales son otros requerimientos (redundancia, seguridad ó limitar el tráfico de broadcast) que justifique el gasto extra y la complejidad de instalar un ruteador dentro de dicho ambiente.

En una conexión de WAN, la fiabilidad debe asegurarse en dos puntos: la línea de transmisión y el ruteador. Para que el tráfico de su red no se interrumpa aunque falle el medio de transmisión, los ruteadores Cisco utilizan la tecnología de marcado, que les permite activar automáticamente un módem de acceso telefónico o una conexión RDSI como sistema auxiliar hasta que se restablece la línea. Para las sedes más importantes, es posible que desee instalar un ruteador de reserva que tome el relevo en el caso de que falle el ruteador principal. Cabe señalar, que los modelos redundantes se deben tener en cuenta que son para sistemas críticos, así mismo se debe determinar el grado de criticidad de los servicios para aplicar algún tipo de redundancia.

Los tipos de redundancia en la red son:

- Redundancia de Workstation-Ruteador: Se refiere en la relación de cómo descubre el Workstation al Ruteador, puede incluir un default gateway, ARP, HSRP, etc.
- Redundancia de servidores: Mirrioring que significa sincronizar discos, duplexing que es igual al mirrioring pero además que los tienen en diferentes tarjetas controladoras.
- Redundancia de Rutas: Se refiere al balance de carga y minimizar el downtime.

- Redundancia de Medios: Se refiere a la evitar la pérdida de tráfico del medio que se utilice.

V.15 IMPLEMENTACIÓN DE HSRP EN UNA RED EMPRESARIAL

A continuación se dará el concepto general de redundancia HSRP desarrollada por Cisco para obtener redundancia en el sistema.

V.15.1 INTRODUCCIÓN

El alcance del establecimiento de una red de la empresa abarca todas las localizaciones del establecimiento de una red que un negocio utilice alcanzar a sus clientes y proveer productos o servicios. Dentro de la red de la empresa, la atención se ha centrado en dos ambientes separados, la red de área amplia y la red del campus, y los arquitectos de la red han sido acertados en el abastecimiento de una infraestructura directa para ambos ambientes. Uno de los desafíos más grandes que permanece, sin embargo, está prolongando este nivel de la redundancia entre los sitios de trabajo y el equipo de la red en el nivel de la sesión. El Cisco Systems ha estado proporcionando soluciones “extremo a extremo” dentro de la área de la interred y, con la disponibilidad del Protocolo de Ruteo de Espera en Caliente (Hot Standby Routing Protocol [HSRP]) puede quitar esta última valla de la viveza dentro de la red de la empresa.

V.15.2 CONVERGENCIA DE RED

Una red de la empresa es comprada por varios departamentos dentro de una organización. El propósito primario de la red es proporcionar a usuarios finales dentro de estos departamentos tiene acceso a sus datos y usos. Los usuarios finales típicamente no tienen cuidado sobre los Ruteadores, líneas de telecomunicaciones, conmutadores Frame Relay, o conmutadores LAN, o el hecho es que no lo saben. Su opinión de la red de la empresa es que es un sistema total. Inyectando varios niveles de la redundancia en la red, el arquitecto de la red permite la red, como sistema total, para mantener conexiones y converger alrededor de fallas. Conocido como convergencia de la red, esta característica es una medida del tiempo que toma para recuperar el acceso a los datos de los usuarios finales; considera la recuperación de todos los dispositivos, acoplamientos, y protocolos que un usuario emplea para tener acceso a datos.

V.15.3 REDUNDANCIA DEL PROTOCOLO

Los protocolos de red los datos de aplicación cruza la red empresarial. Estos protocolos confían sobre una arquitectura para proveer jerarquía para el direccionamiento de estaciones de trabajo y topología de la información sobre la red. Un gateway o Ruteador multiprotocolo otorga esta información. Estaciones de trabajo, Ruteadores, servidores de archivo podría hablar a cada uno, y para este propósito, los protocolos han implementado en la búsqueda de métodos para encontrar y almacenar la dirección del gateway. Algunos protocolos hacen este procedimiento dinámico, mientras que otros requieren la dirección gateway para ser “hardcoded” en la configuración de las estaciones del trabajo como se ilustra en la tabla 5-7. Después el gateway ha encontrado las comunicaciones entre las aplicaciones del servidor y la estación del trabajo que están

establecidos sobre un específico gateway, la ruta es formada. Las últimas rutas para la duración de la sesión, hay un solo punto de falla. Si cualquier cosa en las rutas cambiadas, tal como el gateway, las terminales de sesión. Aunque un redundante gateway es agregado a la red incrementa la disponibilidad de la red, los protocolos tendrán efectividad en tiempos fuera de las sesiones antes de establecer otra ruta a través de un segundo gateway.

TABLA 5-7: SOPORTE DE REDUNDANCIA EN RELACIÓN AL PROTOCOLO

Protocolo	***Soporte Redundante de Gateway***	***Tiempo de Recuperación***
IP	**Si con IRDP**	**Configurable**
IPX	**Si**	**10 seg.**
NetBIOS	**No**	
Banyan	**No**	
DECNet	**No**	
AppleTalk	**Si**	**30 seg.**

HSRP otorga un método de un provisionamiento de una ruta directa de redundancia por el Internet Protocol (IP) para compartir el protocolo y la dirección Media Access Control (MAC) entre gateways redundantes. HSRP fue introducido dentro del software Cisco IOS™ en la Versión 10 para realizarlo con su salida. El protocolo consiste de una dirección virtual y una dirección de protocolo que están compartiendo entre dos Ruteadores y un proceso que monitorea ambas LAN y las interfaces seriales vía un protocolo multicast. La característica está activada con los siguientes comandos:

Standby [group number] **ip**
[***ip-address***(***secondary***)]
Standby [***group number***] **timers** ***hellotime***
holdtime

Standby [***group number***] **priority** priority number
Standby [***group number***] **preempt**

Standby [***group number***] **track** ***type number***
[***interface priority***]
Standby [***group number***] **authentication** ***string***

Los ruteadores que están participando en un grupo HSRP comunica a cada uno de los grupos vía User Datagram Protocol (UDP) multicast basado en paquetes “hello”. Durante el comienzo, ó a través del uso comandos “prioritary” y “preempt”, uno de los ruteadores esta escogiendo ser el ruteador activo y el segundo ruteador es diseñado como respaldo. Si el Ruteador de respaldo falla para recibir el paquete “hello” del ruteador activo, también el segmento local de LAN es inestable ó el ruteador activo ha tenido una falla. También en este caso el Ruteador de respaldo asume el control virtual de la dirección MAC y de protocolo. Dentro del software Cisco IOS™, en ambos tiempos entre el HSRP los paquetes “hello” (hellotime) y asciende el tiempo antes que el Ruteador de respaldo declara al Ruteador activo estar inoperativo (holdtime) que son configurables.

Cuando implementamos HSRP en cualquier ambiente, uno regla específica necesita ser seguida, de otro modo la red no funcionará correctamente. La regla es simple: " La conectividad debe ser garantizada entre los puertos de los ruteadores**."** Si el ambiente del LAN se rompe, después ambas ruteadores asumen la dirección IP primaria y anuncian el alcance al resto de la red. Si los ruteadores se unen a un grupo de switches, la misma regla se aplica; los switches se deben considerar como sólo segmento Ethernet/Token Ring.

V.15.4 PROTOCOLO DE RUTEO DE ESPERA EN CALIENTE (HSRP)

HSRP es un protocolo de redundancia inter-VLAN o inter-ELAN que permite la detección y recuperación automática ante la caída del ruteador activo. HSRP funciona entre los ruteadores que hagan sistemas primarios y de respaldo (backup), y por medio de ese protocolo ambos ruteadores comparten la misma dirección MAC e IP (la configurada en el gateway por omisión de las PCs), de tal modo que la caída del ruteador principal es totalmente transparente para los PCs.

El protocolo HSRP permite balanceo de carga en cuanto a las tareas de ruteo de inter-VLAN (cada ruteador puede estar activo para una VLAN y en modo de espera "standby" para otra cuyo ruteador activo sea el otro componente del par redundante) de forma que los rendimientos de ambos ruteadores pueden sumarse para calcular el rendimiento global de la solución.

V.15.5 USANDO HSRP PARA TOLERANCIA DE FALLA CON RUTEO DE IP

En esta caso se examina el Hot Standby Routing Protocol (HSRP) de Cisco, el cual provee automáticamente el respaldo cuando lo configure sobre los Ruteadores Cisco que opera con Internet Protocol (IP) sobre Ethernet, Fiber Distributed Data Interface (FDDI), y Token Ring en redes de área local (LANs). HSRP es compatible con el protocolo de Novell Internetwork Packet Exchange (IPX), AppleTalk, y Banyan VINES, y este es compatible con DECnet y Xerox Network Systems (XNS) en ciertas configuraciones. Para IP, HSRP permite a uno de los Ruteadores automáticamente asumir la función del segundo Ruteador si el segundo Ruteador falla. HSRP es particularmente útil cuando los usuarios sobre una subred requieren continuamente accesos a recursos en la red.

Considerando la red mostrada en la Figura 5.28. El ruteador A es responsable para el manejo de paquetes entre el segmento Tokyo y el segmento Paris, y el ruteador B son responsable por el manejo de paquetes entre segmento Tokyo y segmento New York. Si la conexión entre el Ruteador ruteadores A y C se cae ó si también el ruteador comienza a estar indisponible, rápidamente cubierto por el protocolo de ruteo, tal como el Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) y Open Shortest Path First (OSPF) puede responder dentro de segundos tal que el ruteador B es preparado para transferir paquetes y por oro lado iría a través del ruteador A.

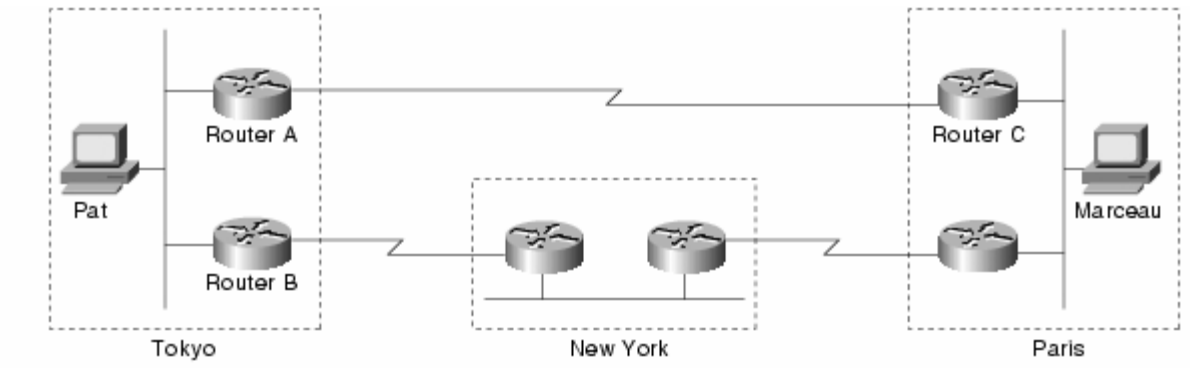


FIGURA 5.28 UNA RED WAN TÍPICA.

Sin embargo, a pesar de la rápida convergencia, si la conexión entre el ruteador A y ruteador C se cae, o si también esta indisponible, el usuario Pat en el segmento Tokio podría no ser capaz de para comunicar con el usuario Marceau incluso después que el protocolo de ruteo ha convergido. Eso es por que el Host IP, tal como la estación de trabajo de Pat, usualmente no participa en protocolos de ruteo. En lugar, se configuran estáticamente con la dirección de un solo Ruteador, tal como el Ruteador A. Hasta alguno manualmente modifica la configuración del host de Pat para usar la dirección del Ruteador B en lugar del Ruteador A, Pat no puede comunicarse con Marceau.

Algunos hosts IP usan un proxy Address Resolution Protocol (ARP) para seleccionar un Ruteador. Si la estación de trabajo de Pat estuviera operando con un proxy ARP, este enviaría un requerimiento ARP para la dirección de la estación de Marceau. El Ruteador A respondería a favor de la estación del trabajo de Marceau y daría a la estación de trabajo Pat esto en su propia dirección de Media Access Control (MAC) (en lugar de la dirección IP de la estación de trabajo de Marceau). Con el proxy ARP, la estación de trabajo de Pat se comporta como si la estación de trabajo Marceau estuvieron conectados al mismo segmento de la red tal como la estación de trabajo de Pat. Si el Ruteador A falla, la estación de trabajo de Pat continuará para el envío de paquetes destinado para la estación de trabajo de Marceau para la dirección MAC del Ruteador A incluso a través de esos paquetes deben ir a ninguna parte y están perdidos. Pat tampoco espera por ARP para adquirir la dirección MAC del Ruteador B para ser enviado otro requerimiento ARP o reinicia la estación de trabajo para forzarlo a enviar un requerimiento ARP. En esta caso también, por un significativo período de tiempo. Pat no puede comunicarse con Marceau—incluso también el protocolo de ruteo ha convergido, y el Ruteador B esta preparado a transferir paquetes que por otro lado irían a través del Ruteador A.

Algunos hosts de IP usa el Routing Information Protocol (RIP) para descubrir Ruteadores. El inconveniente de usar el RIP es lento para adaptarse para cambiar en la topología. Si la estación de trabajo de Pat esta configurada para usar RIP, 3 a 10 minutos debe transcurrir antes del RIP hace otro Ruteador disponible.

Algunos hosts IP más nuevos usan el ICMP Ruteador Discovery Protocol (IRDP) para encontrar al Nuevo Ruteador cuando una ruta comienza a estar disponible. Un host que opera IRDP escucha un mensaje multicast “***hello”*** esta configurado el Ruteador y usa un Ruteador alterno cuando este no tan distante recibe esos mensajes “hello”. Si la

estación de trabajo de Pat estuviera operando IRDP, este detectaría que el Ruteador A no tan distante enviando mensajes “hello” y comenzarían a enviar estos paquetes para el Ruteador B.

Para los Hosts IP que no soportan IRDP, el HSRP de Cisco provee una manera de mantener comunicando cuando un Ruteador llega a ser indisponible. HSRP permite 2 ó más Ruteadores configurados HSRP para usar la dirección MAC y la dirección IP de red de un Ruteador virtual. El virtual Ruteador no esta físicamente existente, en lugar, este representa la común tarjeta para los Ruteadores que están configurados para proveer el respaldo para cada uno. Figura 5.29 muestra el segmento Tokio de la WAN tal como debe ser configurado para HSRP. Cada Ruteador actual es configurado con la dirección MAC y la dirección IP de red del Ruteador virtual.

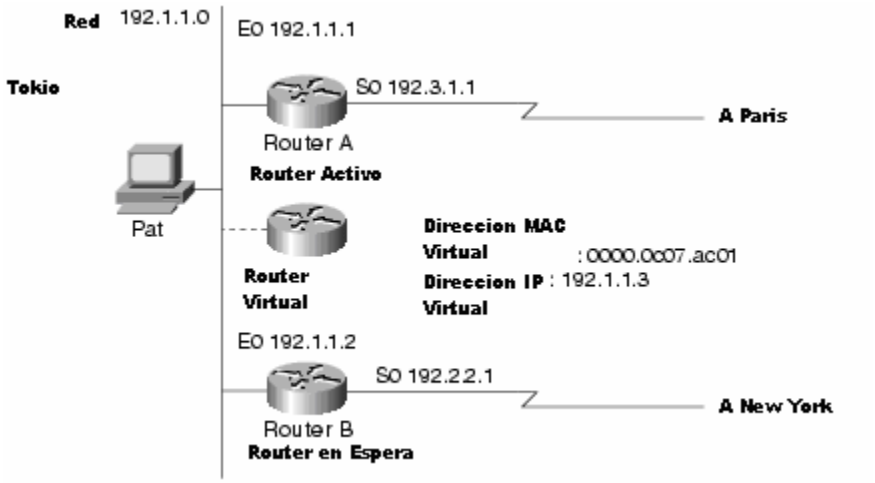


FIGURA 5.29 DIRECCIONAMIENTO DE HSRP SOBRE EL SEGMENTO DE TOKYO.

En la Figura 5.29, la dirección MAC del virtual Ruteador es 0000.0c07.ac01. Cuando tú configuras HSRP, el Ruteador automáticamente selecciona uno de la dirección virtual MAC de un rango de direcciones en el software de Cisco IOS que está dentro del rango de un bloque de direcciones MAC de Cisco. Las LANs Ethernet y FDDI usan una de las direcciones preasignadas MAC tal como una dirección virtual MAC. Las LANs Token Ring usan la dirección funcional tal como una dirección virtual MAC.

En la Figura 5.29, en lugar de la configuración de los hosts en la red 192.1.1.0 con la dirección IP del Ruteador A, están configurados con la dirección IP del Ruteador virtual como su gateway de omisión. Cuando la estación de trabajo Pat envía paquetes para la estación de trabajo de Marceau sobre el segmento de Paris, este los envía a la dirección MAC del Ruteador virtual.

En la Figura 5.29 El Ruteador A esta configurado tal como el Ruteador activo. Este está configurado con la dirección IP y la dirección MAC del Ruteador virtual y envía cualquier paquete diseccionado al Ruteador virtual hacia fuera de la interfaz 1 para el segmento Paris. Como el Ruteador en espera, el Ruteador B esta también configurado con la dirección IP y la dirección MAC del Ruteador virtual. Si por alguna razón el

Ruteador A detiene la transferencia de paquetes, el protocolo de ruteo converge, y el Ruteador B asume el mando del Ruteador A y llega a ser el Ruteador activo. Eso es, el Ruteador B ahora responde a la dirección IP virtual y la dirección MAC virtual. La estación de trabajo de Pat continúa para usar la dirección IP del Ruteador virtual para la dirección de paquetes destinados para la estación de trabajo Marceau, en el cual el Ruteador B recibe y envía al segmento de Paris vía el segmento de New York. Hasta que reanuda la operación el Ruteador A, HSRP permite al Ruteador B proveer un servicio ininterrumpido para los usuarios sobre el segmento Tokyo que necesita comunicar con usuarios del segmento Paris. Mientras que el Ruteador activo, el Ruteador B continúa actuando en función normal: el manejo de paquetes entre el segmento Tokyo y el segmento de New York.

HSRP también trabaja cuando los hosts están configurados por el proxy ARP. Cuando el Ruteador activo HSRP recibe una petición para un host que no está localmente en la LAN, el Ruteador contesta con la dirección MAC del Ruteador virtual. Si el Ruteador activo llega a ser indisponible o la conexión remota a la LAN se avería, el Ruteador que llega a ser el Ruteador activo recibe paquetes direccionado al Ruteador virtual y los transfiere consecutivamente.

Nota. Tu puedes configurar HSRP sobre cualquier Ruteador Cisco que esta operando con Cisco Internetwork Operating System (Cisco IOS) Software Release 10.0 ó mayor. Si tú configuras HSRP para un Ruteador Cisco sobre una LAN Token Ring, todos los Ruteadores Cisco sobre esta LAN debe operar con Cisco IOS Software Release 10.0 ó mayor. Cisco IOS Software Releases 10.2 (9), 10.3 (6), y 11.0 (2) permite la dirección IP en espera para responder los requerimientos al ping. Cisco Software Release 11.0 (3) (1) proporciona mejora el soporte para el uso de la dirección IP secundaria con HSRP.

V.15.6 ENTENDIENDO COMO TRABAJA HSRP

HSRP usa un esquema prioritario para determinar cual Ruteador está configurado con HSRP para ser el Ruteador activo por omisión. Para configurar como un Ruteador activo, tú lo asignas una prioridad que es más alto, que la prioridad de todos los otros Ruteador configurados HSRP. La prioridad por omisión es 100, si tú configuras un Ruteador para tener la más alta prioridad, será el Ruteador activo por omisión.

HSRP trabaja con el intercambio de mensajes multicast que advierte alrededor de los Ruteadores configurados con HSR. Cuando el Ruteador falla envía un mensaje “hello” dentro del periodo de tiempo configurable, el Ruteador en espera con la más alta prioridad llega a ser el Ruteador activo. La transición de la función de los paquetes entregados entre los Ruteadores es completamente transparente para todos los hosts de la red.

Los Ruteadores configurados con HSRP intercambian 3 tipos de mensajes multicast:

- ***Hello***—El mensaje “hello” transmite a otros Ruteador con HSRP la prioridad de los Ruteador con HSRP y el estado de información. Por omisión, un Ruteador HSRP envía mensajes “hello” cada 3 segundos.

- ***Coup***— Cuando un Ruteador en espera asume la función de Ruteador activo, este envía un mensaje “coup”.

• ***Resign***— Un Ruteador que es el Ruteador activo envía este mensaje cuando este es apagado ó cuando un Ruteador que tiene mayor prioridad envía un mensaje “hello”.

En cualquier momento, los Ruteadores configurados con HSRP están en uno de los siguientes estados:

• ***Active***— El Ruteador esta actuando sobre la transferencia de paquetes.

• ***Standby***— El Ruteador esta preparado para asumir funciones de transferencia de paquetes si el Ruteador activo falla.

• ***Speaking and listening***— EL Ruteador esta enviando y recibiendo mensajes “hello”.

• ***Listening***— El Ruteador esta recibiendo mensajes “hello”.

Nota. Cuando está configurado sobre AGS, AGS+, y Ruteadores series Cisco 7000, HSRP toma ventaja de características especiales de hardware que no están disponibles sobre otros Ruteadores Cisco. Esto significa que HSRP opera de manera ligeramente diferente sobre otros Ruteadores.

V.16 IMPLEMENTACION DE REDUNDANCIA EN ACCESO DE INTERNET

En las siguientes secciones se darán los requerimientos de la empresa que desea realizar redundancia en sus sistemas de acceso a Internet, ya que es una de las herramientas más importantes que utilizan los usuarios para realizar cualquier consulta de información general, así como para ingresar sistemas de la misma empresa.

V.16.1 ANALISIS DE INFRAESTRUCTURA DE RED ACTUAL

La empresa ha realizado una análisis de requerimientos que conlleva a la redundancia de su sistema de Internet, teniendo en cuenta que se optimicen los recursos de acceso a Intenert que cuentan en su infraestructura de red, pero teniendo en cuenta que es prioritario garantizar el servicio que contenga una disponibilidad del 99.99 % de efectividad en operación. Por lo que se enumerarán los recursos con que se cuentan antes de la implementación y posteriormente dar una solución confiable y de seguridad a la red interna, para cualquier ataque o inconsistencia del sistema.

Actualmente se cuenta con una red Frame Relay que abarca toda la republica Mexicana, por lo que es necesario que todos los usuarios de la empresa puedan acceder a Internet bajo este canal.

Además se cuenta con un ancho de banda de un E1 (2048 Mbps) para el acceso de Internet, que esta en la utilización de un 40 a 50% de tráfico. Sin embargo harán una actualización de la base de datos que se maneja a través de Internet y estiman que suba en un 70 a 80% de tráfico, por lo que se desea dar una opción de mantener en un 15% al 20% de tráfico disponible en sistuaciones criticas y en un 30% a 40% en situaciones normales que conlleven a un nuevo acceso que se integre a este servicio.

La ubicación de los edificios importantes en la republica Mexicana se encuentra en la CD de México y Monterrey, que a través de la red Frame Relay se comunican sin problema de tráfico.

La mayor importancia para una fiabilidad, y de seguridad de operación del sistema de la empresa será del público en general que accederá de cualquier medio al portal Web que radica su base de datos en México desde cualquier acceso que tenga el usuario, línea telefónica, red corporativa, banda ancha, es decir, el portal es de uso comercial, por lo que se requiere la mejor redundancia para hacer efectiva la operación al un 99.99% como la seguridad del portal como de los servidores del corporativo.

Cuentan con un conjunto de servidores DNS, primarios y secundarios que están bajo plataforma Windows 2000 que son servidores internos, así como Servidor de correo electrónico que utilizan protocolos POP3 y SMTP para la transferencia de archivos, servidor FTP en cuanto transferencia de archivo por el corporativo, además de un Firewall que es un Cisco Pix 550, Base de datos con sistema operativo Windows 2000 utilizando motores de consulta de Oracle y SQL para diferentes aplicaciones del corporativo y el servidor Linux para el alojo de la base de datos en ASP y PHP que se accede a través del buscador Internet Explorer.

La parte de la infraestructura del hardware de la red, en su totalidad es cable UTP categoría 5, y en sitio de Comunicaciones y servidores cuenta con un backbone de fibra óptica en su nodo principal en la vertical hacia sus pisos, y su horizontal se encuentra con cable UTP categoría 5. Manejando una red FastEthernet 802.3 con una topología bus, así mismo cuenta con UPS redundantes con capacidad de mantener los servidores y equipos de comunicaciones por 12 horas continuas sin interrupción. Cuentan con conmutadores Cisco catalys 1900 y 2900, así como un ruteador Cisco modelo 2501 para su acceso a Internet que actualmente opera.

V.16.2 REQUERIMIENTOS DE REDUNDANCIA DEL SISTEMA DE INTERNET

La empresa desea realizar una conexión de redundancia en el sistema de Internet, donde se determine las menores variables de interrupción de servicio, así como de accesos, equipos, etc., ya que la empresa tiene un giro comercial y financiera que debe contar con el mejor servicio posible.

Se deben utilizar los recursos que se tiene actualmente en la red, y si se desea agregar algunos otros, debe mantener el objetivo que el sistema proporciona sea la mejor inversión financiera y tecnológica para la empresa.

La seguridad es el factor de esencial que establezca fronteras exteriores e interiores que actualmente se tiene, pero con la idea de no afectar la topología de la red en lo más posible que indicaría configurar demás dispositivos y que cambiaria sensiblemente a sistemas de bases de datos o aplicaciones que accedan ó modifiquen día a día, y mucho menos repercuta en estaciones de los usuarios.

V.16.3 IMPLEMENTACION DE LA SOLUCION DEL ANALISIS DEL SISTEMA DE REDUNDANCIA.

Tomando en cuenta todos los parámetros y solicitudes, así como recursos con que cuenta la empresa se realiza la siguiente solución de un sistema redundante con HSRP de Cisco.

Teniendo en cuenta el hardware de la infraestructura tenemos los siguientes:

Conjunto de Servidores: Correo electrónico con protocolo POP3 y SMTP con sistema operativo Windows 2000, DNS con sistemas Operativos Windows 2000, y Bases de datos con SQL y Oracle, bajo plataforma Windows 2000, y además servidores FTP con sistemas operativos con Windows 2000, así como servidor Web Linux con ASP y PHP.

Análisis 1: Aquí podemos definir que no existe ningún problema de tráfico de datos ni de ruteo, ya que las plataformas Windows e incluso Linux utilizan TCP/IP así como los mismo protocolos que utilizan en cada uno de ellos como POP3, SMTP, y en cuanto a las bases de datos, Oracle, SQL, ASP y PHP son aplicaciones que sólo se manifiestan como motores de bases de datos pero que necesitan de una plataforma de sistemas operativos y los cuales operan con TCP/IP

También podemos definir los accesos, como el cableado del la red que:

Tenemos un E1 (2048 Mbps) y también una topología en bus FastEthernet 802.3 y por tanto cableado UTP categoría 5, y cabe mencionar respaldo de UPS en cuanto a energía eléctrica se refiere.

Análisis 2: Aquí aprovecharemos el acceso E1 que es de fibra óptica y colocaremos otro acceso E1 pero con diferente proveedor para que aseguremos la continuidad del servicio, esto implica que si un medio de algunos de los dos diferentes backbones de proveedores diferentes, implicaría que uno tomaría todo el tráfico mientras se diagnostica y se corrige el problema. En cuanto a la topología de la red y cableado que utilizaran será referirá más a la administración de la red LAN, ya que sólo esto determina el tipo de interfaz que utilizara los equipo de comunicaciones que se instalarán. Y la velocidad con que se decida propagar el tráfico desde los ruteadores hacia la LAN, es decir, se tiene en cuenta que los ruteadores deben tener una interfaz FastEthernet.

Así mismo podemos ubicarnos en la parte de seguridad de la red con el conjunto de dispositivos que cuenta la empresa.

Como tema central tenemos a un Firewall, que es un Cisco Pix 515, que como sabemos realiza la función de implementar las políticas de seguridad en cuanto al flujo de la red, es decir, de quien tendrá permisos para acceder a la red ó quien no los tendrá. Por lo que esta caso se delimitara la frontera interior con el Firewall y la seguridad exterior lo administración a través del ISP, aunque como un ISP su función es entregar los mayores beneficios del Internet, cabe señalar que en este punto se tendrá abierto todos los servicios y puertos que se pueden ocupar en el Internet, por ello como un pequeño paréntesis se colocan Firewalls dentro de la red LAN para que ellos formen las políticas informáticas que rijan a cada uno de los clientes o empresas que tengan este tipo de servicio. Por lo que la parte del sistema redundante, solo establece la mejor topología de la red y entregar el servicio con todos los beneficios y servicios de la Internet, así como la

configuración de los equipos y sistemas, por consecuencia, solo en este punto se puede señalar que el mejor punto estratégico y conveniencia de la topología de la red es que se coloque el Firewall delante de los dos Ruteadores (teniendo la perspectiva de dirección a la red LAN) que se necesitan para establecer la redundancia HSRP.

La parte final se refiere al hardware que se requiere y son accesos que se requieren para implementar el sistema se tiene un Cisco 2501. Y además tiene una descanalizador NOKIA autosense, sin embargo, se necesita colocar otro Cisco 2501 y otro descanalizador NOKIA. Así que el otro punto es generar la parte de la solución integral en equipo y configuración.

Solución: Para determinar la solución debemos enlistar con los que se cuenta, en cuanto a equipos, Acceso a Internet, aplicaciones de sus sistemas, y seguridad en la red, que son los siguientes.

1 Ruteador 2501, con puerto AU1 y 2 puertos Seriales.
1 Descanalizador NOKIA Autosense
1 Transciver de puerto AUI a RJ45 (FastEthernet)
1 Acceso de Fibra Óptica con 1 E1 (2048 Mbps)
Se cuenta con acceso de Internet con el ISP, DNS externo, IP Pública.
Conjunto de servidores con protocolo de comunicacion TCP/IP
1 Firewall Cisco Pix 515
Switches Catalys 1900 y 2900 propagados en su corporativo.

Con lo que debemos contar además de lo que tenemos, para la implementación de la redundancia de HSRP de Cisco es el siguiente:

Otro Ruteador 2501, con puerto AU1 y 2 puertos Seriales.
Otro Descanalizador NOKIA Autosense
Otro Transciver de puerto AUI a RJ45 (FastEthernet)
Otro Acceso de Fibra Óptica con 1 E1 (2048 Mbps)
Un Switch como mínimo de 8 puertos FastEthernet
Otra IP Pública que debe proporcionar el ISP
Balanceo de carga a través de equipos DCE del ISP

Al final quedarían:

2 Ruteador 2501, con puerto AU1 y 2 puertos Seriales.
2 Descanalizador NOKIA Autosense
2 Transciver de puerto AUI a RJ45 (FastEthernet)
2 Acceso de Fibra Óptica con 1 E1 (2048 Mbps)
Se cuenta con acceso de Internet con el ISP, DNS externo, IP Publica.
Conjunto de servidores con protocolo de comunicacion TCP/IP
1 Firewall Cisco Pix 515
Switches Catalys 1900 y 2900 propagados en su corporativo.

Primeramente la parte del hardware y conexiones se deben realizar de la siguiente manera, 2 Ruteadores 2501 en la parte de la WAN se conectará hacia 2 descanalizadores (un Ruteador con un descanalizador respectivamente), ya que como es entregado en una

interfaz G.703 el descanalizador hará la conversión del esta interfaz de G703 a V.35 para conectarlo a cada Ruteador, y a cada uno de los dos diferentes proveedores de acceso, con esto hacer la primer redundancia de medio y de Ruteador, después conectamos la parte de LAN del Ruteador, de su puerto AUI al transciver y de este al nuevo switch con puertos FastEthernet, con cables UTP categoría 5 con configuración de cable directo.

Después de esto se solicitara al cliente 3 direcciones IPS LAN que estén en el mismo segmento de su red de conexión. Esto será para configurar 2 de ellas en cada Ruteador (una por Ruteador), que serán direcciones IPS diferentes, ya que la tercera será común en la configuración de los dos Ruteador, ya que esta será dirección IP virtual que se genera para indicar el estado de cada uno de los Ruteadores, si ha existido una caída en alguno de ellos.

Posteriormente a esto, se debe configurar el Ruteador con el protocolo de comunicación más simple como es HDLC en la parte de la WAN (en la interfaz serial del Ruteador) y así como utilizar el protocolo de ruteo que es el IGRP, y anunciar la red que se propagará en la LAN. Así como el direccionamiento de IPS públicas en cada uno de los Ruteadores, esto en la parte de WAN. Y por último el balanceo que realizará el ISP en ambos conexiones que se definirá como se observará como si fuese el mismo enlace y esto implica que si alguno de los dos accesos con diferentes proveedores se cae el servicio el otro tomará todo el tráfico del servicio de Internet, y así se podría redundancia del medio. Por otro lado si no hay falla, y como el servicio esta balanceado la carga de tráfico se distribuirá en los dos accesos.

Por otro lado la redundancia HSRP de Cisco, esta dirigida a los equipos Ruteadores Cisco, quiere decir, que si alguno sufre alguna avería ó caída del medio, el otro se encuentra en espera de la falla y en ese momento se activará como el Ruteador primario mientras se restablece la falla. Finalmente, para dar la solución integral, se realiza el diagrama a seguir, así como la configuración de cada uno de los Ruteadores en las siguientes secciones.

V.17 IMPLEMENTACION DOS RUTEADORES CISCO 2501 CON PROTOCOLO HDLC Y REDUNDACIA HSRP

En la figura 5.30 se muestra el diagrama de cómo se colocaran el sistema redundante HSRP.

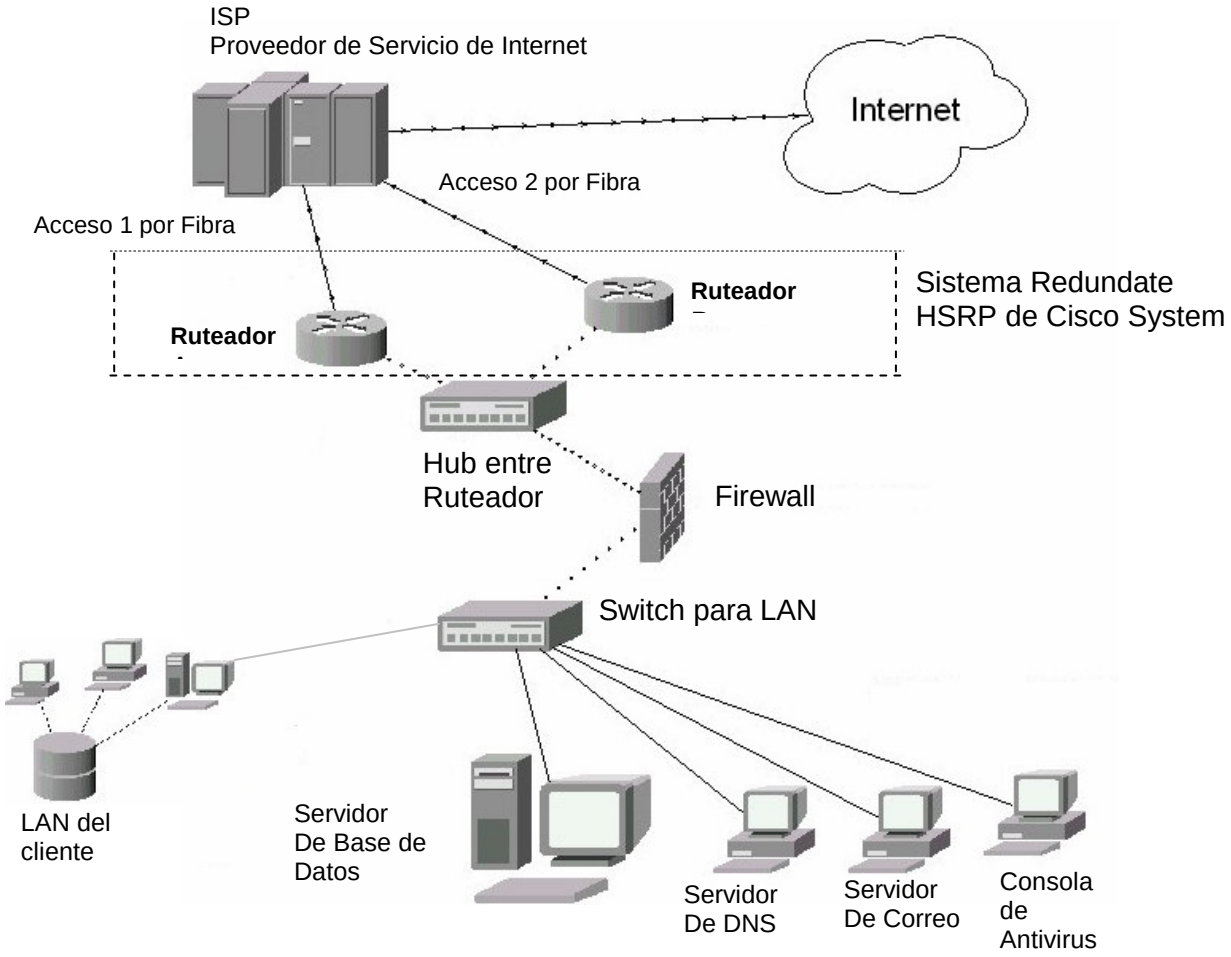


FIGURA 5.30 DISEÑO DE LA RED CON SISTEMA REDUNDANTE HSRP

CONFIGURACION DE RUTEADOR A (CISCO 2501):

```
version 12.2
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname RUTEADOR_INTERNET_A
!
logging buffered 4096 debugging
enable password 7 08734F41040C0B1E160A0852
!
clock timezone CST -6
clock summer-time Horario.de.verano date Apr 6 2003 2:00 Oct 26 2003 2:00
ip subnet-zero
!
!
```

```
!
interface FastEthernet0/0
 description LAN
 ip address 192.168.4.31 255.255.255.0
 duplex auto
 speed 10
 standby 1 ip 192.168.4.1
 standby 1 priority 115
 standby 1 preempt
 standby 1 track FastEthernet0/0
 standby 1 track Serial0/0
!
interface Serial0/0
 description RED WAN
 ip address 148.245.32.66 255.255.255.248
 ip load-sharing per-packet
!
router igrp 100
 network 172.16.0.0
 !
!
ip route 0.0.0.0 0.0.0.0 148.245.32.65
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
ntp clock-period 17179890
ntp server 200.33.213.236
!
end
```

CONFIGURACION DE RUTEADOR B (CISCO 2501):

```
version 12.2
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname RUTEADOR_INTERNET_B
!
logging buffered 4096 debugging
no logging console
no logging monitor
enable password 7 06540C2E415B07100116165D
!
clock timezone CST -6
```

```
clock summer-time Horario.de.verano date Apr 6 2003 2:00 Oct 26 2003 2:00
ip subnet-zero
!
!
interface FastEthernet0/0
 description LAN Datacenter
 ip address 192.168.4.32 255.255.255.0
 duplex auto
 speed 10
 standby 1 ip 192.168.4.1
 standby 1 preempt
standby 1 track FastEthernet0/0
 standby 1 track Serial0/0
!
interface Serial0/0
 description RED WAN
 ip address 148.245.32.68 255.255.255.248
 ip load-sharing per-packet
!
router igrp 100
 network 172.16.0.0

!
ip route 0.0.0.0 0.0.0.0 148.245.32.67
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
ntp clock-period 17179890
ntp server 200.33.213.236
!
end
```

V.17.1 EXPLICACION DE LAS CONFIGURACIONES

En la Figura 5.30 se debe realizar configuraciones básicas para identificación del Ruteador como colocar el nombre del Ruteador, utilizando el comando "**hostname nombre_Ruteador**", en donde nombre_Ruteador es Ruteador Internet A, lo cual se tendría que dar con los siguientes comandos de configuración:

```
Ruteador>
Pasamos al modo privilegiado
Ruteador>en
Ruteador#
Entramos en modo configuración
Ruteador#config t
```

Ruteador(config)#
Damos el comando que cambia el nombre
Ruteador(config)#hostname RUTEADOR_INTERNET_A

Y queda como sigue:

RUTEADOR_INTERNET_A#

Así aparece en el archive de configuración como se muestra arriba.

hostname RUTEADOR_INTERNET_A

Ahora para dar la IP de la FastEhternet, como su descripción, la velocidad y el modo de transmisión de se debe hacer desde el como de configuración como sigue:

RUTEADOR_INTERNET_A#
RUTEADOR_INTERNET_A#config t
RUTEADOR_INTERNET_A(config)#
RUTEADOR_INTERNET_A(config)#interface Fast0/0
RUTEADOR_INTERNET_A(config-if)#

En este momento ya entramos a la interfase de LAN
Ahora vamos a dar la descripción de la interfaz, es para identificarla

RUTEADOR_INTERNET_A(config-if)#descripcion LAN

Por consiguiente vamos a dar la ip address que nos proporcionara el administrador de RED LOCAL

RUTEADOR_INTERNET_A(config-if)#ip address 192.168.4.31 255.255.255.0

Ahora vamos a dar el modo de trasmisión en la interfaz, que será duplex de manera automática, lo que significara que entre el switch o hub, y la interfaz ethernet del Ruteador, harán una negociación para la sincronización de ambos.

RUTEADOR_INTERNET_A(config-if)#duplex auto

Por ultimo de dará la velocidad en que se comunicaran la interfaz con el swicth.

interface FastEthernet0/0
description LAN
ip address 192.168.4.31 255.255.255.0
duplex auto
speed 10

Como se muestra en la Figura 5.30; según este diseño la red, se debe crear la Redundancia tanto en los enlaces con el proveedor (Carriers), y también Redundancia en

los Ruteadores para cualquier avería física. El panorama es que el cliente cuenta con dos accesos de Fibra óptica, con dos diferentes proveedores, que por obvias razones tienen una trayectoria diferente y no dependen del mismo backbone, esto nos permitirá en primera instancia la redundancia de enlaces, es decir, si un enlace de fibra cae el otro estará activo para llevar consigo el tráfico. Los enlaces con que se cuentan con un ancho de banda de 1 E1, cada uno. El proveedor de servicio realiza un proceso de balanceo, esto significa, que estabiliza los dos circuitos para que el tráfico de ellos se equilibre, y para el cliente lo vería como un solo acceso, sin embargo cuando un enlace cae. Un solo acceso llevara el flujo total de la información. Por ello la importancia de configurar un arreglo del HSRP que tomaría las siguientes decisiones, por la inactividad de la interfaz Serial o la interfaz Ethernet que serian las siguientes posibilidades:

Inactividad de Interfaz Serial:

Falla en el acceso de enlace de fibra optica. El sistema HSRP toma la decisión, por la líneas configuradas; el comando "**standby ip**"; indica la ip virtual que en este caso se refiere a la dirección 192.168.4.1, que como se muestra esta configurada en ambos ruteadores para que se indique la relación que existe entre ellos, y como esta en el mismo grupo del sistema HSRP, por omisión es 0, ya que no se configuro, así que después el comando "**standby preempt**", indica que existe una prioridad según el nivel que se configuro, en este caso el que tiene mayor prioridad es el que se configura 115 dando como resultado que es el que tiene el control, pero cuando el enlace falla, la serial queda inactiva, la detectara con el comando "**standby track serial0/0**" que determinara si es la que estaba en uso al verificarlo y dar como resultado verdadero, el sistema HSRP buscara el siguiente ruteador con la prioridad siguiente y tomara el control de esta misma.

La interfaz serial sufrió un daño: Realizara lo antes mencionado.

El ruteador se apago. Realizara lo antes mencionado

Inactividad de Interfaz Ethernet:

Problema en el switch: El sistema HSRP toma la decisión, por la líneas configuradas; el comando "**standby ip**"; indica la ip virtual que en este caso se refiere a la dirección **192.168.4.1**, que como se muestra esta configurada en ambos ruteadores para que indica la relación que existe entre ellos, así como esta en el mismo grupo del sistema HSRP, por omisión es 0, ya que no se configuro, así que después el comando "**standby preempt**", indica que existe una prioridad según el nivel que se configuro, en este caso el que tiene mayor prioridad es el que se configura 115 dando como resultado que es el que tiene el control, pero cuando el enlace falla, la serial queda inactiva, la detectara con el comando "**standby track FastEthernet0/0**" que determinara si es la que estaba en uso al verificarlo y dar como resultado el verdadero del sistema HSRP buscara el siguiente Ruteador con la prioridad siguiente y tomara el control de esta misma.

La interfaz Ethernet sufrió un daño: Realizara lo antes mencionado.

El cable LAN sufrió un daño. Realizara lo antes mencionado

La configuración antes descrita queda definida con el siguiente procedimiento:

```
Ruteador_Internet_A#config t
Ruteador_Internet_A(config)#interf fast0/0
Ruteador_Internet_A(config-if)#
```

Y se da los siguientes comandos:

```
Ruteador_Internet_A(config-if)#standby 1 ip 192.168.4.1
Ruteador_Internet_A(config-if)#standby 1 priority 115
Ruteador_Internet_A(config-if)# standby 1 preempt
Ruteador_Internet_A(config-if)# standby 1 track FastEthernet0/0
Ruteador_Internet_A(config-if)# standby 1 track Serial0/0
```

Y queda de la siguiente manera:

```
interface FastEthernet0/0
 description LAN Datacenter
 ip address 192.168.4.32 255.255.255.0
 duplex auto
 speed 10
 standby 1 ip 192.168.4.1
 standby 1 priority 115
 standby 1 preempt
 standby 1 track FastEthernet0/0
 standby 1 track Serial0/0
```

En tanto, que en la serial se realiza una configuración de protocolo HDLC, ya que en Internet no se tiene una misión critica de envío y recepción de información, claro hablamos de los Web sites de orden publico, que pueden ser visitados por cualquier persona que lo desee, sin embargo, el protocolo HDLC tiene una estabilidad de operación fiable. Es importante aclarar que la anterior configuración de ambos Ruteador en sus respectivos seriales, no muestra la configuración de encapsulación HDLC. Pero no por que no se halla configurado, esto se verifica al escribir el comando "**show running-config"** no se mostrara esta configuración. Para verificar si el protocolo de encapsulación es HDLC, se debe escribir el comando "show interfaces", donde se visualizara en la interfaz serial correspondiente la encapsulación HDLC.

Ahora vamos a configurar los cambios en la interfaz serial como sigue:

Entramos en modo de configuración

```
Ruteador_Internet_A#config t
```

Entramos a la interfaz serial

```
Ruteador_Internet_A(config)#interf ser0/0
```

Damo s la descripcion para identificarla

```
Ruteador_Internet_A(config-if)#description RED WAN
```

Ahora damos la dirección IP pública que nos proporciona el proveedor de Internet, que será pública para que nuestro portal sea visible por Internet.

Ruteador_Internet_A(config-if)#ip address 148.245.32.66 255.255.255.248

Posteriormente a esto daremos el comando que se utilice para balancear la carga en el Ruteador local, ya que el ISP lo hara desde sus equipos.

Así quedara configurado:

interface Serial0/0
description RED WAN
ip address 148.245.32.66 255.255.255.248
ip load-sharing per-packet

Para verificar el enrutamiento que debe hacerse del ISP al Router será con una ruta estática, que se configura desde el modo de configuración global como sigue:

ip route 0.0.0.0 0.0.0.0 148.245.32.65

Entramos en modo de configuración:

Ruteador_Internet_A#config t

Después agregamos el algoritmo de protocolo con el siguiente comando:

Ruteador_Internet_A(config)#ip route 0.0.0.0 0.0.0.0 148.245.32.65

Lo que significa que cualquier tráfico que venga hacia el router (0.0.0.0 0.0.0.0, esto se entiende que cualquier host con cualquier mascara podrá pasar), resuelva el direccionamiento a través del ISP (148.245.32.65, esta dirección la da el ISP y por lo regular es una antes de la configurada en la serial).

A su vez, se tiene configurado el algoritmo de protocolo IGRP; que en realidad su configuración es muy fácil ya que se tiene dos líneas de configuración, uno que se declara el algoritmo de protocolo como la red interna que resolvera, es decir, la red LAN que toma ese camino para su comunicación, y el procedimiento es el siguiente:

Entramos en modo de configuración:

Ruteador_Internet_A#config t

Después agregamos el algoritmo de protocolo con el siguiente comando:

Ruteador_Internet_A(config)#Router igrp 100

Por ultimo se agrega la red que anunciara en este algoritmo:

Ruteador_Internet_A(config-Ruteador)#network 172.16.0.0

Finalmente en el desplegado de configuración quedara:

Ruteador igrp 100
network 172.16.0.0

NOTA: El otro Ruteador tiene la misma configuración, con la diferencia que las direcciones IP que se agregan en la interfaz Fastethernet0/0, así como también en la interfaz Serial0/0, y el nivel de prioridad en el sistema HSRP para definir que Ruteador es el primario.

Este arreglo, para algunos podría ser costoso en cuanto a la infraestructura, sin embargo la importancia de los clientes, hoy en día, a parte del costo monetario, también se tiene un costo de tecnología; ya que es necesario transferir información, con la menor probabilidad de falla, para que sus comunicaciones tengan una red segura. Y puedan llevar los usuarios a cabo sus tareas y rutinas financieras sin ningún contratiempo.

CAPITULO VI IMPLEMENTACION DE REDUNDANCIA EN FRAME RELAY

VI.1 DESCRIPCION DE FRAME RELAY

A continuación se dará los conceptos generales y como los pasos a seguir para configurar un Ruteador Cisco para Frame Relay, así como la implementación de redundancia de la red.

VI.2 FRAME RELAY

Frame Relay es un protocolo de acceso de red similar en principio al X.25 (un protocolo es un sistema de procedimientos o las reglas que gobierna la transferencia de la información entre los dispositivos). La diferencia principal entre Frame Relay y el X.25 es la integridad de datos (detección de error) y control de flujo del error de la red (corrección de error).

X.25 hace que todos sus datos se comprueban y que corrijan en el nivel de red. Eso significa que los dispositivos de la red corrigen los datos corruptos o que piden para que los datos sean retransmitidos. El coste de tal comprobación y retransmisión es una red con retrasos.

El rendimiento de Frame Relay se basa solamente en detección de error y no en corrección de error. De tal modo deja la tarea de la corrección de error a los protocolos usados por los dispositivos inteligentes en cada extremo de la red. Estos dispositivos inteligentes proporcionarán integridad de datos extremo a extremo. Pues Frame Relay confía en el equipo final para actuar a la retransmisión y recuperación de error, hay significativamente menor procesamiento requerido para la red y menor retraso total.

VI.2.1 CONFIGURACIONES DE HARDWARE DE FRAME RELAY

Tú puedes crear conexiones Frame Relay usando uno de las siguientes configuraciones de hardware:

- Ruteadores y access servers conectados directamente para el switch de Frame Relay

- Ruteadores y access Server conectados directamente al channel service unit/digital service unit (CSU/DSU), el cual después conecta a un switch remoto de Frame Relay.

Nota Los Ruteadores pueden conectar a redes Frame Relay también por conexión directa a un switch Frame Relay o a través de un CSU/DSUs. Sin embargo, una sola interfaz del Ruteador configurad a para Frame Relay puede ser configurado por solamente uno de estos métodos.

El CSU/DSU convierte a señales V.35 o RS-449 para un código apropiado de señalización de transmisión T1 para la recepción exitosa para la red Frame Relay. La Figura 6.1 ilustra las conexiones alrededor de los componentes.

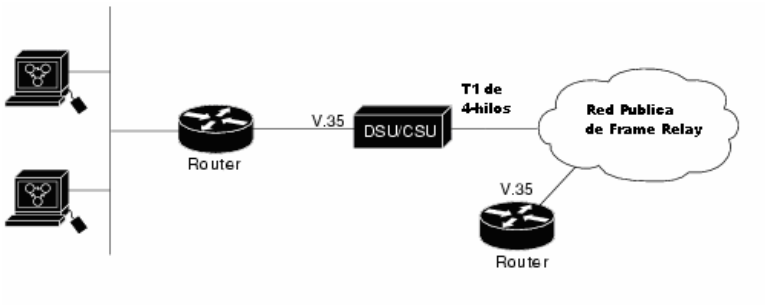


FIGURA 6.1 CONFIGURACIÓN TÍPICA DE FRAME RELAY

La interfaz Frame Relay actualmente consiste de una conexión física entre el servidor de red y el switch que proporciona el servicio. Esta única conexión física proporciona conexión directa a cada dispositivo en la red.

VI.2.2 CONFIGURAR FRAME RELAY

El Frame Relay es un protocolo de enlace de datos para la conmutación de paquetes que se utiliza para conectar dispositivos DTE (Ruteadores) con dispositivos DCE. Los dispositivos DCE en las redes de Frame Relay están formados por conmutadores de portadoras propietarias (véase la figura 5.23). La red de Frame Relay (una red telefónica conmutada, pública o privada) suele representarse como una nube.

El Frame Relay utiliza circuitos virtuales permanentes para las sesiones de comunicación entre los distintos puntos de la WAN. Estos circuitos virtuales se identifican por medio de un DLCI (data link connection identifier o identificador de la conexión de datos), un valor que proporciona el proveedor del servicio de Frame Relay. El DLCI tiene que especificarse para la conexión entre el Ruteador y el conmutador (véase en la figura 6.2), y debe introducirse en un numero DLCI cuando se configura el Frame Relay en el Ruteador.

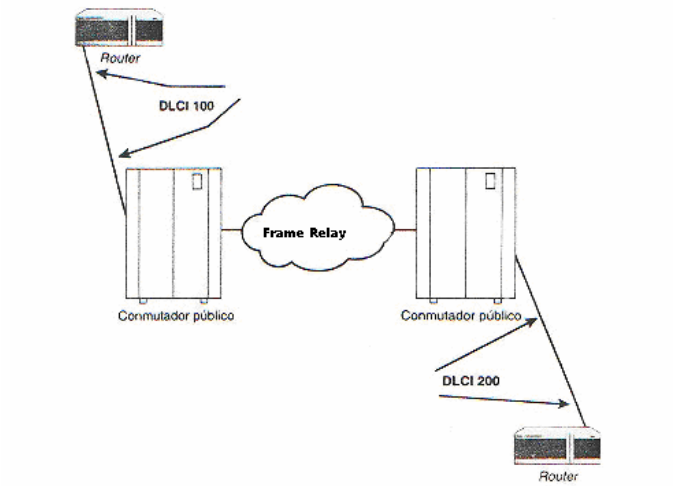


FIGURA 6.2 PROCESO DE ENLACE DE DATOS SOBRE FRAME RELAY

Otro parámetro que puede configurarse para el Frame Relay es la LMI (Local Management Interfaz o Interfaz Local de Gestión). LMI es el estándar de señalización que

se utiliza entre el Ruteador y el conmutador de Frame Relay: los Ruteadores de Cisco soportan tres tipos de LMI:

- Cisco: tipo LMI de Cisco, Northern Telecom, DEC y StrataCom.
- ANSI: tipo LMI del ANSI (el organismo estadounidense de normalización).
- q933a: tipo LMI del estándar Internacional de Telecomunicaciones.

La configuración del Frame Relay en el Ruteador es bastante parecida a la configuración de los protocolos WAN vistos anteriormente.

VI.2.2.1 CONFIGURAR FRAME RELAY EN UNA INTERFAZ SERIE

1. En el indicador del modo Privilegiado, escriba ***config t*** y después pulse Intro. Se lanzará el modo Configuración Global.
2. Para configurar una determinada interfaz WAN, introduzca el nombre de la misma en el indicador, por ejemplo **interfaz en serie 0**, y después pulse Intro. El indicador pasara al modo **config-if.**
3. Escriba la dirección IP con el comando **IP address 172.16.10.1 255.255.255.252**
4. Después escriba ***encapsulation frame*** y después pulse Intro.
5. Para determinar el DLCI para la conexión entre el Ruteador y el conmutador de Frame Relay, escriba ***frame-relay interfaz dlci [#],*** en donde "#" corresponde al número DLCI que se haya proporcionado a la línea que se conecta el Ruteador y el conmutador. Si el número DLCI es igual a 100, el comando que debería introducirse sería **frame-relay interfaz-dlci 100**. Pulse Intro para continuar.
6. El comando **frame- relay interfaz-dlci 100** le lanzara de hecho al indicador **dlci** desde donde pueden configurarse los parámetros avanzados relacionados con el circuito **virtual** dlci. Para volver el modo Configuración de la interfaz, escribe int s0 y pulse Intro.
7. Para configurar la LMI (sólo ejecute este paso si tiene una versión del IOS anterior a la versión 11.2), escriba ***frame relay lmi type [tipo LMI],*** donde tipo LMI puede ser el tipo cisco, ANSI, o q933a. Para determinar ansi como el tipo de LMI, debería introducir el comando "***frame-relay lmi-type ANSI"***. Después pulse Intro (véase la Figura 15.7).
8. Para cerrar la sesión de configuración pulse Ctrl.+Z.
9. Pulse de nuevo Intro para volver al indicador del modo privilegiado. Como se muestra abajo.

```
Ruteador>en
Ruteador#config t
Enter configuration commands, one per line. End with CNTL/Z
Ruteador (config)# int s0
Ruteador (config-if) # ip address 172.16.10.1 255.255.255.252
Ruteador (config-if) # encap frame
Ruteador (config-if) # frame-relay interface-dlci 100
Ruteador (config-if) # frame-relay lm-type ansi
Ruteador (config-if) #
```

Una vez configurado el Ruteador, puede utilizar el comando **“show interfaz serial [número de interfaz]”** para consultar los parámetros de configuración para el Frame Relay. Otro comando que puede resaltarle de gran ayuda para comprobar la configuración del Frame Relay en el Ruteador es show frame-relay lmi.

El comando **“show frame–relay lmi”** proporciona un listado de los mensajes no validos que el Ruteador haya recibido o enviado, además de mostrar los mensajes LMI validos también enviados y recibidos. En la figura 6.4 se muestra el resultado de este comando (puede utilizarlo tanto en el modo Usuario como Privilegiado).

```
Router#sh frame-relay lmi
LMI Statistics for interface Serial0 (Frame Relay ) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Rcvd 1748             Num Status msgs Sent 1748
  Num Update Status Sent 0              Num St Enq. Timeouts 0
Router#
```

FIGURA 6.4 EJEMPLO DE COMANDO PARA MOSTRAR EL LMI

Un consejo muy útil que debe recordarse es que puede configurar una sola interfaz de Ruteador para múltiples números DLCI (circuitos virtuales) mediante el uso de subinterfaces. Por ejemplo, después de configurar la interfaz en serie 0, se puede especificar en el indicador de configuración que se desea configurar la interfaz en el indicador de configuración que se desea configurar la interfaz en serie **serial 0.1**, donde el 1 corresponde a la primera subinterfaz. Después sólo tendría que configurar dicha subinterfaz con un determinado numero DLCI.

VI.2.2.2 VERIFICACION DE CONEXION

Con el siguiente comando nosotros verificamos la integridad del enlace que es **“show ip interface brief”**, en el siguiente caso tenemos todas interfaces arriba, pero considerando que nosotros tenemos configuración en la serial0 es la que nos interesa, en este momento, se encuentra el enlace de Frame Relay activo.

Nosotros podemos ver las direcciones IP en la Interfaz:

Ruteador#sh ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
BRI0	unassigned	YES	NVRAM	down	down
Ethernet0	10.1.1.1	YES	NVRAM	up	up
Serial0	172.16.10.1	YES	NVRAM	up	up

El procedimiento para configurar la interface Ethernet es el mismo en cuanto a la configuración de la dirección IP, pero aquí no se realiza la encapsulación de datos, ya que a nivel LAN solo basta con agregar el direccionamiento.

Conectado otro Ruteador en la red; nosotros deberíamos agregar una dirección IP a la interfaz Ethernet.

```
Ruteador>
Ruteador>en
Ruteador#config  t
Enter configuration commands, one per line. End with CNTL/Z.
Ruteador(config)#int e0
Ruteador(config-if)#ip address 10.1.1.2 255.255.255.0
Ruteador(config-if)#no shut
%SYS-5-CONFIG_I: Configured from console by console
Ruteador(config)#exit
Ruteador#exit
```

Ahora que nosotros tenemos una dirección en ambos lado de la conexión Ethernet, nosotros podemos llegar entre Ruteador con el comando PING.

VI.2.2.3 PRUEBAS DE PING

Se mencionará a uno de los comandos más importantes para la verificación de una conexion de redes. Se trata del comando que comprueba el estado de la conexión con uno o varios equipos remotos, por medio de los paquetes de solicitud de eco y de respuesta de eco, para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

El comando PING, de sus siglas en ingles, es el Packet Inter Net Groper, permite al usuario realizar una prueba básica de conectividad. La sintaxis es:

ping *ip-address*

El Ruteador enviara 5 requerimientos hacia la dirección IP destino; si este recibe la respuesta, este lo denotará con un símbolo de admiración **“!”**, en caso contrario de no recibir respuesta denotara con el símbolo de puntos suspensivos **“….”**

Un ping exitoso:

```
Ruteador#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/44 ms


Ruteador#
```

Un ping fallido:

```
Ruteador#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Ruteador#
```

Ping es uno de las más comunes pruebas utilizadas como herramienta. PING usa el protocolo ICMP (Internet Control Message Protocol), para comunicar con otros Ruteadores.

Cuando un dispositivo se le ejecuta por primera vez el comando “PING”. Este comando podría fallar la primera vez al tratar de buscar una respuesta. Esto es por que el Ruteador no ha sido completado por la resolución ARP.

Tú puedes también ver tu dirección IP usando el comando **“*show running-config”*** ó **“*show ip interface”*.**

VI.3 PERSONALIZANDO TU RED FRAME RELAY

A continuación se definirá como personalizar la red Frame Relay para tener un mejor rendimiento en la transmisión de datos.

VI.3.1 ENTENDIENDO LAS SUBINTERFACES DE FRAME RELAY

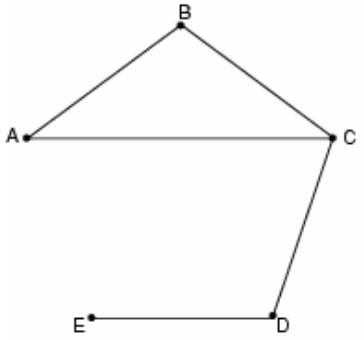
La interfaces de Frame Relay proporciona un mecanismo para soportar parcialmente una malla de redes Frame Relay como subinterfaces. La mayoría de protocolos asumen transitividad en una red lógica; esto es, si la estación A puede hablar con la estación B, y la estación B puede hablar con la estación C, entonces la estación A seria capaz para hablar a la estación C directamente. La transitividad es veraz en las LANs, pero no sobre redes Frame Relay a menos que A sea directamente conectado a C.

Además, ciertamente que los protocolos tales como AppleTalk (el protocolo nativo de MAC y se reviso en la sección I.7.4) y el Puente Transparente (protocolo que utilizan los puentes) no pueden soportar parcialmente mallas de redes porque requieren una división horizontal. La división horizontal es una técnica de ruteo en la cual el paquete recibido en la interfaz no puede ser enviada de la misma interfaz incluso si son recibidos ó transmitidos en diferentes VCs.

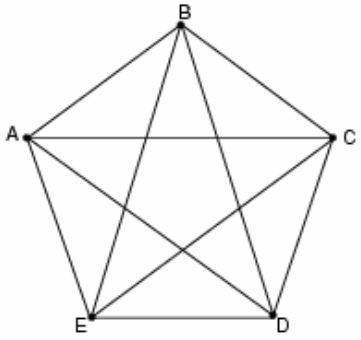
Configurando las subinterfaces de Frame Relay aseguran que una sola interfaz física es tratada como múltiples interfaces virtuales. Este trato te permite sobreponerte para dividir las reglas horizontales. Los paquetes recibidos en una interfaz virtual pueden ser enviados a otra interfaz virtual incluso si ellos están configurados sobre la misma interfaz física.

Las direcciones de las Subinterfaces son las limitaciones de las redes Frame Relay para proporcionar una camino para subdividir un malla particionada en la red Frame Relay dentro de un número más pequeño, una malla completa de subinterfaces (o point-to-point). Cada subred asignada es un propio número y aparece a los protocolos como si este fuera alcanzable a través de una interfaz separada. (Nota esas subinterfaces “point-to-point” pueden ser innumerables para la el uso IP, reduciendo el direccionamiento voluminoso que debe por otro lado resultar)

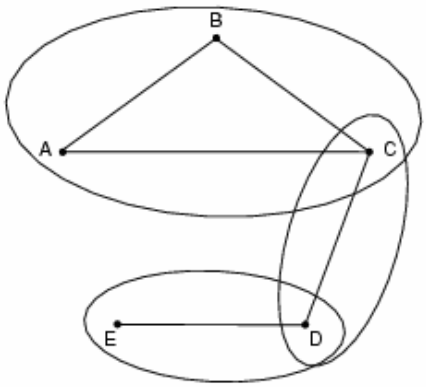
La figura 6.5 muestra 5 nodos de una red Frame Relay que es particionalmente en malla. (Red A). Si la entera red es vista como una sola subred (con el único número asignado) la mayoría de los protocolos sumen que un nodo A puede transmitir un paquete directamente al nodo E, cuando en el hecho este debe cambiar a través de los nodos C y D. Esta red puede ser hecha para trabajar con protocolos (por ejemplo, IP), pero no trabajaremos del todo con otros protocolos (por ejemplo, AppleTalk) por que los nodos C y D no cambiarán el paquete fuera de la misma interfaz sobre el cual este fue recibido. Una manera para hacer que esta red trabaje completa es crear una red malla completa (red B), pero haciendo esto requiere un largo número de PVCs, en el cual no puede económicamente ser factible.



Red A: Red Frame Relay parcialmente mallada sin conectividad completa.



Red B: Red Frame Relay completamente mallada, con conectividad completa



Red C: Red Frame Relay parcialmente mallada, con conectividad completa. (Configuracion de subinterfaces).

FIGURA 6.5 USANDO LAS SUBINTERFACES PROPORCIONA UNA CONECTIVIDAD COMPLETA MALLA PARCIAL DE RED FRAME RELAY.

Usando las subinterfaces, tú puedes subdividir la red Frame Relay dentro de 3 más pequeñas subredes (Red C) con números separado de red. Nodos A, B, y C están conectadas a un red malla completa, y los nodos C y D, como también los nodos D y E, son conectados vía red point-to-point. En esta configuración, los nodos C y D pueden acceder a 2 subinterfaces y puede por lo tanto enviar paquetes sin violación de las reglas de división horizontal. Si el puenteo transparente esta siendo usado, cada subinterfaz es vista como una puerta del puente separado.

Las subinterfaces pueden ser configuradas para comunicacion multipunto o punto-a-punto. (No hay por omisión.) Para configurar las subinterfaces sobre una red Frame Relay, usa los siguientes comandos comenzando en un modo de configuración global:

	Comando	**Objetivo**
Paso 1	Ruteador(config)# **interface *type number.subinterface-number*** {**multipoint** | **point-to-point**}	Crea una subinterfaz punto a punto ó multipunto (point-to-point ó multipoint)
Paso 2	Ruteador(config-subif)# **encapsulation frame-relay**	Configura la encapsulación de Frame Relay en la interfaz serial.

VI.3.2 DEFINIENDO EL DIRECCIONAMIENTO DE SUBINTERFACES

Para interfaces punto a punto (point-to-point), el destino es asumido para ser conocido y es identificado ó implicado en el comando **frame-relay interface-dlci**. Para interfaces multipunto (multipoint), los destinos pueden ser dinámicamente resueltos a través del uso de ARP Inverso de Frame Relay Inverse ARP ó puede ser estáticamente mapeado a través del comando **frame-relay map**.

VI.3.3 DIRECCIONAMIENTO DE SUBINTERFACES PUNTO A PUNTO (POINT-TO-POINT)

Si tú especificas una subinterfaz punto a punto (point-to-point) en el procedimiento precedente, usa el siguiente comando en el modo de configuración de la interfaz:

Comando	**Objetivo**
Ruteador(config-subif)# **frame-relay interface-dlci *dlci***	Asocia la subinterfaz seccionada point-to-point con un DLCI.

Nota Este comando es típicamente usado en la subinterfaces; sin embargo, este puede también ser aplicado a la interfaces principales. El comando **“frame-relay interface-dlci”** es usado para habilitar los protocolos de ruteo sobre las interfaces principales que están configuradas para usar el ARP Inverso. Este comando es también de mucha ayuda para asignar una clase específica a un solo PVC sobre la subinterfaz multipunto (multipoint).

Si tú defines una subinterfaz para una comunicación punto a punto (point-to-point), tú no puedes reasignar el mismo número de subinterfaz para ser usado para la comunicacion multipoint sin primero reiniciar el Ruteador o el acceso al servidor. En lugar, tú puedes simplificar al eludir usando ese número de subinterfaz y usar un diferente número de subinterfaz.

VI.4 MÉTODOS DE NOTIFICACIÓN DE CONGESTIÓN DE FRAME RELAY

La diferencia entre los métodos de notificación de congestión de BECN y ForeSight es que BECN requiere unos paquetes de usuario para ser enviado en la dirección de la congestión DLCI para transportar la señal. El envió de los paquetes de usuario no es predecible y, por lo tanto, no es seguro como un mecanismo de notificación. Más que una espera de los paquetes de usuario para proporcionar la notificación de congestión, el tiempo de mensajes ForeSight garantiza que el Ruteador recibe notificación antes de que la congestión llegue a ser un problema. El tráfico puede ser lento en la dirección del congestionado DLCI.

VI.4.1 CONFIGURANDO EL LMI

Este parte ya se habia configurado en la sección anterior, cuando configuramos Frame Relay, pero aquí se explica más a detalle de lo que representa en la red. Ya que con el inicio de la liberación del Cisco 11.2, el software soporta la autodeteccion de la Interfaz de Administración Local (LMI), el cual habilita la interfaz para determinar el tipo de LMI que es soportado por el conmutador (switch) de Frame Relay.

VI.4.2 ACTIVANDO LA AUTODETECCION DEL LMI

La autodeteccion del LMI esta activo en las siguientes situaciones:

- El Ruteador está encendido ó la interfaz cambia de estado operativo activo (UP).
- La línea de protocolo está caída (DOWN) pero la línea esta activa (UP).
- La interfaz es un DTE Frame Relay.
- El tipo de LMI no esta explícitamente configurado.

Ver las siguientes secciones para información adicional de interés para la activación del autodeteccion del LMI:

- Estado Requerido
- Mensajes de Estado
- Autodeteccion del LMI
- Opciones de Configuración

VI.4.3 ESTADO REQUERIDO

Cuando la autodeteccion de LMI esta activo, este envía un completo estado requerido, en los 3 tipos de LMI, al switch. La orden es ANSI, ITU, cisco, pero es hecho en una rápida sucesión. El software Cisco IOS proporciona la habilidad para escuchar en ambos DLCI 1023 (cisco LMI) y DLCI 0 (ANSI y ITU) simultáneamente.

VI.4.4 MENSAJES DE ESTADO

Uno ó más de los estados requeridos reproducirán una respuesta (estado de mensaje) del switch. El Ruteador decodificadará el formato de la respuesta y se configura automáticamente a sí mismo. Si más de uno responde a la recepción, el Ruteador se configura a sí mismo con el tipo de la última respuesta recibida. Este se acomoda a los switches inteligentes que pueden soportar múltiples formatos simultáneamente.

VI.4.5 AUTODETECCION DEL LMI

Si la autodeteccion del LMI no es exitosa, un reintento inteligente del esquema es construido. Cada intervalo N391 (por omisión es 60 segundos, el cual mantiene el intercambio de 6 a 10 segundos cada uno), la autodeteccion de LMI intentará para verificar el tipo de LMI.

La única indicación visible para el usuario de la autodeteccion del LMI es bajo la manera de que el comando este encendido que es **“debug frame lmi”.** A cada intervalo N391, el usuario ahora verá tres investigaciones rápidas del estado al salir de la interfaz serial: uno en el ANSI, uno en ITU, y uno en LMI-tipo del Cisco.

VI.4.6 OPCIONES DE CONFIGURACIÓN

Sus opciones de configuración son proporcionados; la autodeteccion del LMI es transparente para el usuario. Tu puedes apagar la autodeteccion LMI por la configuración explicita un tipo de LMI. El tipo de LMI debe ser escrito dentro de la NVRAM y que la próxima vez el encendido del Ruteador, la autodeteccion del LMI será inactiva. Al final de la autoinstalación, una declaración de **“frame-relay lmi-type *xxx”*** es incluido dentro de la configuración de la interfaz. Esta configuración no es automáticamente escrita a la NVRAM; debes explícitamente escrita la configuración a la NVRAM para usar el comando **“copy system:running-config”** ó **“copy nvram:startup-config”.**

VI.4.6.1 LA CONFIGURACIÓN EXPLICITA DEL LMI

El software de Frame Relay soporta los estándares de la industria para la dirección del LMI, incluyendo la especificación Cisco. Si tú quieres configurar el LMI y entonces la autodeteccion se desactiva el LMI, actúa las tareas en las siguientes secciones:

- Configuración el tipo LMI (Requerido)
- Configuración el Intervalo del Keepalive LMI (Requerido)

- Configurando el enlistado del LMI y los Intervalos del Tiempo (Opcional)

VI.4.6.2 CONFIGURACIÓN DEL TIPO DEL LMI

Si el Ruteador ó el servidor de acceso son unidos a la Red de Datos Publico (PDN), el tipo del LMI debe igualar el tipo usando sobre la red pública. De lo contrario, el tipo de LMI puede ser configurada para cuadrar las necesidades de tu red privada Frame Relay.

Tú puedes configurar uno de los tres siguientes tipos de LMIs sobre los dispositivos Cisco: ANSI T1.617 Anexo D, Cisco, y ITU-T Q.933 Anexo A. Para hacerlo, use los siguientes comandos de inicio en el modo de configuración de la Interfaz:

	Comando	Objetivo
Paso 1	Ruteador(config-if)# **frame-relay lmi-type** {**ansi** | **cisco** | **q933a**}	Configura el tipo de LMI.
Paso 2	Ruteador# **copy nvram:startup-config** ***destination***	Escribe el tipo de LMI a la NVRAM.

VI.5 CONFIGURANDO UN MAP CLASS

Para configurar un map class, usa los siguientes comandos empezando en el modo de configuración global:

	Comando	Objetivo
Paso 1	Ruteador(config)# **map-class frame-relay** ***map-class-name***	Específica un nombre de map class de Frame Relay y entra al modo de configuración del map class.
Paso 2	Ruteador(config-map-class)# **frame-relay cir in** ***bps***	Específica la entrada de la tasa de información comprometida (committed information rate [CIR]), en bits por segundo.
Paso 3	Ruteador(config-map-class)# **frame-relay cir out** ***bps***	Especifica la salida del CIR, en bits por segundo.
Paso 4	Ruteador(config-map-class)# **frame-relay mincir in** ***bps***[2]	Pone la mínima entrada aceptable CIR, en bits por segundo.
Paso 5	Ruteador(config-map-class)# **frame-relay mincir out** ***bps*** [2]	Pone la mínima salida aceptable CIR, en bits por segundo.
Paso 6	Ruteador(config-map-class)# **frame-relay bc in** ***bits*** [2]	Pone la entrada de tamaño de ráfaga comprometida (committed burst [Bc]), en bits.
Paso 7	Ruteador(config-map-	Pone la salida del Bc, en bits.

	class)# **frame-relay bc out *bits*** [2]	
Paso 8	Ruteador(config-map-class)# **frame-relay be in *bits*** [2]	Pone la entrada de tamaño de la ráfaga excesiva (excess burst [Be]), en bits.
Paso 9	Ruteador(config-map-class)# **frame-relay be out *bits*** [2]	Pone la salida del Be, en bits.
Paso 10	Ruteador(config-map-class)# **frame-relay idle-timer *seconds*** [2]	Pone el intervalo de tiempo fuera ocupado, en segundos.

[1] En este comando reemplaza al comando **frame-relay becn-response-enable**, el cual será removido en un futuro por Cisco IOS release. Si tú usas el comando **frame-relay becn-response-enable** en los argumentos, debes reemplazarlo con el comando **frame-relay adaptive-shaping becn**.

[2] La claves **in** y **out** son opcionales. Configurando el comando sin las claves **in** y **out** que aplicaran ese valor a ambos, a los valores de tráfico de entrada y salida para la instalación de SVC. Por ejemplo, **frame-relay cir 56000** aplica 56000 para ambos valores de tráfico de entrada y salida para configurar la actividad el SVC.

Tú puedes definir múltiples map classes. Un “map class” es asociado con un mapa estático, no con la interfaz ó subinterfaz misma, Por que la flexibilidad de esta asociación permite, que tú puedas definir diferentes map class para diferentes destinos.

VI.6 MONITOREANDO Y MANTENIENDO LAS CONEXIONES DE FRAME RELAY

Para monitorear las conexiones de Frame Relay, usa cualquiera de los siguientes comandos en el modo EXEC:

Comando	Objetivo
Ruteador# **show interfaces serial *type number***	Despliega la información acerca de los DLCIs de Frame Relay y el LMI.
Ruteador# **show frame-relay lmi** [***type number***]	Despliega las estadísticas del LMI.
Ruteador# **show frame-relay map**	Despliega las actuales entradas de mapeo de Frame Relay.
Ruteador# **show frame-relay pvc** [***type number*** [***dlci***]]	Despliega las estadísticas de los PVC.
Ruteador# **show frame-relay traffic**	Despliega las estadísticas de tráfico de Frame Relay.
Ruteador# **show frame-relay lapf**	Despliega la información acerca del estado del LAPF.

VI.7 LAS INTERNETWORKS DE RUTEO DE MARCADO BAJO DEMANDA (DDR)

El servicio de Ruteo de Marcado Bajo Demanda (Dial-on-Demand Routing [DDR]) proporciona interconexiones de red que cruzan la Red Telefónica Publica (Public Switched Telephone Networks [PSTNs]). Esta dedicado para las redes de área amplia que son típicamente implementadas en líneas rentadas u opciones de servicios más modernos como son Frame Relay, SMDS, ó ATM. El servicio DDR proporciona una sesión de control para conectividad de áreas amplias sobre redes de circuitos conmutados, en el cual se gira a proporcionar servicios sobre demanda y reducen costos de red.

DDR pueden ser usadas sobre interfaces seriales sincronas, interfaces RDSI (Integrated Services Digital Network [ISDN]), ó interfaces seriales asíncronas. EL estándar V.25bis y el marcado DTR son usados para conmutar CSU/DSUs de 56, Adaptadores Terminales RDSI (ISDN [TAs]), ó módems sincronos. Las líneas de seriales asíncronas están disponibles en el puerto auxiliar de Ruteadores Cisco y servidores de Comunicación para conexiones a MODEM. DDR es soportado en RDSI usando interfaces BRI y PRI.

VI.7.1 CONCEPTO GENERAL DE SERVIDOR DE ACCESO REMOTO

Las redes locales actuales pueden extenderse más allá de los límites de la propia oficina. Ya sea por la proliferación de Internet, ó por las opciones de teletrabajo, las redes entran y salen por las líneas telefónicas para que la red no se encuentre aislada del resto del mundo.

Con la informática móvil y la proliferación de las redes locales, se hizo necesario, que cuando un usuario se encuentra fuera de sus oficinas, exista alguna posibilidad de conectar con la red local de la oficina, ya sea para consultar el correo electrónico, editar ficheros ó imprimir un informe en un dispositivo de la empresa para que lo pueden ver otras personas de la compañía. El concepto de acceso remoto a redes es relativamente antiguo; no obstante en el último año está cobrando auge gracias al empuje que las comunicaciones están recibiendo por parte de la telefonía móvil con transmisión de datos, e Internet.

VI.7.2 QUE ES UN SERVIDOR DE ACCESOS REMOTO (RAS)

Aunque cada fabricante puede dar distintos nombres a sus productos, el término que más se maneja actualmente es el de RAS, siglas que significan Remote Access Server ó Servidor de Acceso Remoto. Básicamente se trata de un dispositivo que da servicio a ordenadores que conectan a través de líneas de entrada no permanentes. Con "no permanentes" se quiere decir que se trata de líneas de comunicaciones que no están conectadas con un ordenador concreto de forma continua, como sucedería con líneas punto a punto, si no que son conexiones que se pueden realizar desde puntos diferentes en cada momento.

Típicamente las conexiones de entrada se realizan a través de líneas telefónicas atendidas por módems, pudiendo ser líneas RDSI o líneas telefónicas analógicas. No se

incluyen en este concepto las conexiones a través de líneas punto a punto o líneas frame relay, cuya filosofía y aplicación es muy distinta (normalmente para unir de forma permanente ubicaciones distintas de una misma compañía).

Los usuarios remotos podrán acceder al servidor RAS utilizando sus líneas RDSI ó analógicas, o utilizando terminales de telefonía móvil, con lo que la conexión se puede realizar desde cualquier punto en el que este servicio tenga cobertura. La conexión por medio de líneas telefónicas, se puede realizar desde cualquier punto de la tierra en el que exista algún tipo de servicio telefónico.

El costo de la comunicación resultará tanto mayor cuanto más lejano se encuentre el país en cuestión (siempre atendiendo a las tarifas de la compañía telefónica que se utilice). Por ello, hay compañías con gran implantación mundial, que disponen de servidores locales en varios países del planeta, permitiendo que un trabajador de la empresa pueda entrar en la red global desde cualquier lugar en el que se encuentre desplazado, sin que suponga un excesivo coste telefónico.

VI.7.3 INTRODUCCION A DDR

El Ruteo por Marcado Bajo Demanda de Cisco IOS (Dial-on-Demand Routing [DDR]) proporciona algunas funciones. Las primeras tablas de ruteo DDR proporcionan la imagen de conectividad todo el tiempo usando Interfaces de Marcado. Cuando la tabla de ruteo envía un paquete a la Interfase de Marcado, DDR entonces filtra hacia fuera los paquetes interesantes para establecer, mantener y liberar la conexiones conmutadas. El Internetworking es alcanzado en la conexión mantenida DDR usando PPP u otra técnica de encapsulación (tales como HDLC, X.25, SLIP).

VI.7.4 NUBES DE MARCADO

La red formada por los dispositivos interconectados DDR puede generalmente ser etiquetados como Medios de marcado o nubes de marcado (***dialer media*** or ***dialer cloud)***. El objetivo de la nube de marcado incluye solamente los proyectados dispositivos conectados y no incluyen los medios de conmutación (la RDSI entera se extiende al mundo y esta más allá del objetivo de la nube de marcado). La exposición del RDSI debe ser considerada cuando se diseña seguridad:

Las características fundamentales de las nubes de marcado son las siguientes:

- Las nubes de marcado están colectivamente en grupos de potencial y conexiones activas punto a punto.
- En las conexiones activas, las nubes de marcado forman un medio NBMA (non-broadcast multiaccess) similar a Frame Relay.
- Para el marcado de salida en circuitos conmutados (tal como RDSI) la dirección de protocolo de red para el mapeo del número de directorio debe ser configurado.
- Las conexiones inactivas DDR son espaciadas para aparecer como activas a las tablas de ruteo.
- El broadcast no deseado u otro tráfico causado sin necesidad de conexiones puede ser prohibitivamente caro. El potencial de costo en los medios tarifados (tal como

RDSI) deben ser cercanamente analizados y monitoreados para prevenir tal pérdida.

Las características de las nubes de marcado afectan cada escenario del diseño de internetworking DDR. Un sólido entendimiento del direccionamiento de protocolo de red, ruteo y estrategias de filtrado pueden resultar en un robusto y costo efectivo de internetworks.

VI.7.5 TOPOLOGIAS

El factor más importante en seleccionar la topología es el número de sitios que deberá soportar. Si solamente 2 sitios son involucrados, la topología usada es punto a punto (point-to-point). Si hay más de 2 sitios son soportados, la topología típica utilizada es hub-and-spoke. Para números pequeños de sitios con un muy bajo tráfico de volúmenes, la topología es la malla completa (Full meshed) que puede ser la más apropiada.

Topologías para DDR:

- Point-to-point
- Fully meshed
- Hub-and-spoke

La figura 6.6 muestra la topología Hub-and-spoke, que es la que se utilizará.

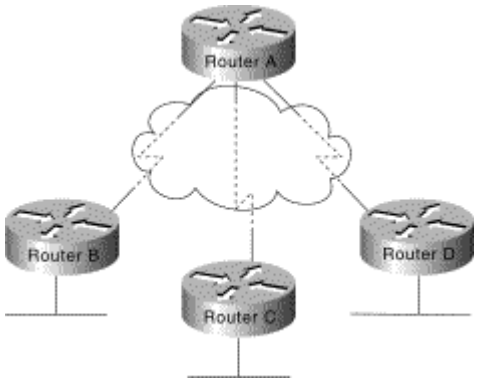


FIGURA 6.6: TOPOLOGIA HUB-AND-SPOKE.

Las topologías hub-and-spoke son muy fácil de configurar que la de malla completa cuando topologías de múltiple puntos son requeridas porque el sitio remoto de las interfaces marcadas son solamente mapeadas en el sitio central. Esto permite mejor el diseño complejo (tal como el direccionamiento, enrutamiento, y autentificación) para ser administrado en el Hub DDR. La Configuración soporta sitios remotos que pueden ser simplificados maravillosamente (similares a una topología de punto a punto).

VI.7.6 ANALISIS DE TRÁFICO

Para el análisis de tráfico, se desarrolla una tabla en la cual los protocolos necesitados son capaces de soportar el marcado basado en DDR de los siguientes equipos. Este formara la base para el resto de diseño. Por ejemplo, una compañía llamada KDT ha seleccionado una topología hub-and-spoke (para proporcionar escalabilidad) y ha desarrollado la tabla que se muestra en Tabla 6-1 para los requerimiento de la nube DDR.

TABLA 6-1: REQUERIMIENTOS DDR PARA PROTOCOLOS DE CONECTIVIDAD PARA KDT

Sitios Remotos	Protocolos de Dial-In	Protocolos Dial-Out	Notas
c700A	IP, IPX	None	
c700B	IP	None	
c1600A	IP, AppleTalk	IP	
c2500A	IP, IPX, AppleTalk	IP, IPX, AppleTalk	
C2500B	IP, IPX	IP	
NAS3600A	IP, IPX, AppleTalk	IP, IPX, AppleTalk	

El propósito de la tabla identifica en cuales sitios y protocolos se requieren la capacidad para iniciar las conexiones DDR. Una vez la conectividad establecida, cada protocolo requiere 2 caminos de conectividad vía las tablas de ruteo y el mapeo de dirección de la nube de marcado. EL Dial-in contra el Dia-out es de la perspectiva del Hub.

A menudo una meta primaria de una red DDR es ofrecer un mejoramiento de costo sobre los cargos asociados WAN con conexiones dedicadas. Adicionalmente al análisis de tráfico debe ser realizado por cada protocolo a este o a la etapa de diseño de Filtro de Marcado. Las aplicaciones de red usan la infraestructura proporcionada por el internetwork en muchas diferentes y a menudo de manera no esperadas.

VI.7.7 INTERFACES DE MARCADO (DIALER)

Al acceder a los medios de marcado es vía Interfaces de Marcado de Cisco ISO. Los canales ISDN B, Interfaces Seriales Sincronas, e Interfaces Asíncronas puede todas

ser convertidas a interfaces de marcado usando los comandos de configuración de interfaz de marcado.

VI.7.8 CONEXIONES DE MODEM ASINCRONOS

Conexiones asíncronas son usadas por servidores de Comunicacion ó a través del Puerto auxiliar en un Ruteador. Las conexiones asíncronas DDR pueden ser soportadas por múltiples protocolos de capa de red. Cuando se considera soluciones asíncronas DDR, los diseñadores deben considerar si las aplicaciones internetworking pueden tolerar el más largo tiempo de llamada configurada y el más bajo throughput de módems analógicos (en comparación con RDSI). Para algunas aplicaciones de diseño, DDR sobre conexiones de MODEM asíncrona puede proporcionar una opción de efectividad en el costo.

Para marcar hacia afuera usando conexiones asíncronas, los argumentos de charla deben ser configurados tal que el marcado del MODEM y los comandos de acceso son enviados al sistema remoto. Para diseñar flexibilidad, múltiples argumentos de charla pueden ser configurados en ***"dialer maps".*** Los argumentos de MODEM pueden ser usados para configurar módems para llamadas de salida. Los argumentos de acceso son proyectados para negociar con el acceso de sistemas remotos y preparar el enlace para el establecimiento de PPP. Los argumentos de charla son configurados con la espera de envío y claves para modificar las configuraciones, tal como sigue:

chat-script dialnum "" "atdt\T" TIMEOUT 60 CONNECT \c

Si tú estas usando DDR asíncrono y llamando un sistema que requiere un acceso de modo de caracter, usa la clave **"system-script"** con el comando **"dialer map"**.

Los argumentos de charla a menudo encuentran problemas con el tiempo debido al hecho que ellos operan con una gran precisión que cuando una persona esta controlando la conexión. Por ejemplo, algunas veces cuando un MODEM envía el mensaje de CONNECT, este no esta listo para enviar datos, y puede incluso desconectar si alguno dato es recibido en el circuito TX. Para evitar estos modos de falla, las pausas son agregadas a la cabeza de alguna de las cadenas enviadas

Cada cadena enviada es terminada con un carro de retorno, incluso cuando esta cadena es nula (""). A menudo el argumento de charla será configurado sin la cadena final "send". De esta manera puede producir resultados no esperados. Asegurar que todos los argumentos de charla han sido completados en pares de espera de envíos. Si al final del elemento en el argumento de charla lógico va hacia fuera para ser una espera (como en el previo ejemplo), use la **\c** como el envió final para suprimir la salida no deseada.

Use el comando **"debug chat"** para identificar los problemas de argumento de charla.

VI.7.9 METODOS DE ENCAPSULACION

Cuando un enlace de datos limpio esta establecido entre 2 DDR peers, los datagramas de internetworking deben ser encapsulados y ser tramados para cruzar los

medios de marcado. Los métodos de encapsulación disponibles dependen de la interfase física utilizada. Cisco soporta la encapsulación de enlace de datos como el Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), Serial Line Interface Protocol (SLIP), y X.25 para DDR:

- PPP es el método de encapsulación recomendada, porque este soporta múltiples protocolos y es usado para conexiones sincronas, asíncronas o RDSI. Además, PPP realiza direccionamiento de negociación y autenticación y es operable con diferentes vendedores.
- HDLC es soportado con líneas seriales sincronas y conexiones RDSI solamente. HDLC soporta múltiples protocolos. Sin embargo, HDLC no proporciona autenticación, en la cual puede ser requerida si utiliza grupos rotatorios de marcado.
- SLIP trabaja en interfaces asíncronas solamente y es soportada por IP solamente. Las direcciones deben ser configuradas manualmente. SLIP no proporciona autenticación y es operable solamente con otros vendedores que use SLIP.
- X.25 es soportado en interfaces seriales sincronas y un solo canal RDSI B.

VI.7.10 AUTENTICACION

La autenticación en una red DDR proporciona dos funciones: seguridad y estado de marcado. Como las mejores redes DDR conectadas a la PSTN, es imperativo que un modelo de seguridad fuerte se implemente para prevenir el acceso inautorizado para recursos sensitivos. La Autenticación también permite el código DDR permita rastrear de que sitios están actualmente conectados y proporciona la construcción de grupos de MultiLink PPP.

- CHAP
- PAP
- ISDN Security
- DDR Callback
- IPX Access Lists

VI.7.11 GENERALIDADES DEL ENCAPSULADO PPP

A diferencia de HDLC, el encapsulado no es propietario de Cisco. Por esta razón, se utiliza a menudo para conectar dispositivos de diferentes fabricantes. La figura 6.7 ilustra como el protocolo punto a punto (PPP) ofrece conectividad extremo a extremo para múltiples protocolos.

FIGURA 6.7 GENERALIDADES DE PPP.

Los desarrolladores de Internet diseñaron PPP para realizar la conexión de enlaces punto a punto. PPP.

Puede ser configurado sobre los siguientes tipos de interfaces físicas:

- Seriales asíncronos.
- HSSI (Interfaz serial de alta velocidad)
- RDSL
- Seriales sincronías.

VI.7.12 COMPONENTES PPP: NCP Y LCP

Desde el punto de vista funcional, el protocolo punto a punto (PPP) es un protocolo de capa de enlace de datos con los servicios de capa de red. Como resultado de esta característica, el protocolo PPP puede ser dividido en dos subcapas. Estas subcapas mejoran la funcionalidad del protocolo PPP. La figura 6.8 muestra el desglose de estas capas.

El protocolo PPP utiliza el componente NCP (Programa de Control de Red) para encapsular múltiples protocolos. Además otro componente fundamental, el LCP (Protocolo de Control del Enlace), para negociar y configurar opciones de control sobre el enlace de datos de la WAN.

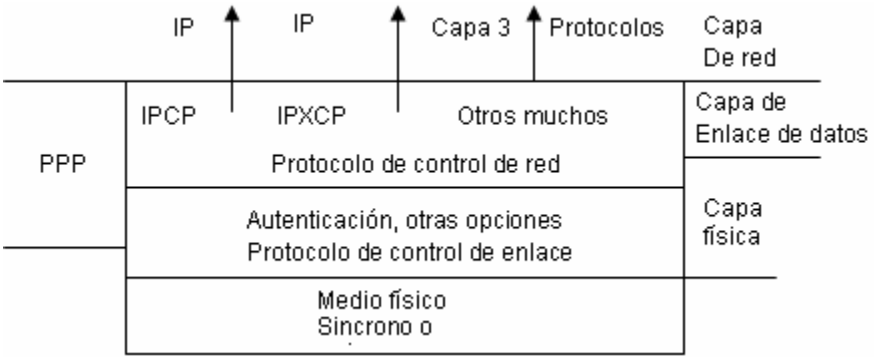


FIGURA 6.8. SUBCAPAS PPP

Con estas funciones de bajo nivel, el protocolo PPP puede utilizar los siguientes:

- Medios físicos sincronos
- Medios físicos asíncronos como los que utiliza el servicio telefónico básico para las conexiones de acceso telefónico con MODEM
- RDSI

El protocolo PPP ofrece un amplio conjunto de servicios que controlan la configuración de un enlace de datos. Estos servicios son opciones de LCP, que se utilizan principalmente para negociar y comprobar tramas, con el fin de implementar los controles punto a punto que un administrador específico para la llamada.

Con estas funciones de alto nivel, el protocolo PPP transporta paquetes de varios protocolos de capa de red en los que NCP actúa. Éstos son campos funcionales que contienen códigos estandarizados para indicar el tipo de protocolo de capa de red que encapsula.

Una de las ventajas principales del protocolo PPP es la funcionalidad de las opciones LCP, como se muestra en la tabla 6-2

TABLA 6-2 OPCIONES LCP

Característica	**Como funciona**	**Protocolo**
Autenticación	Solicita una contraseña. Realiza intercambio de desafíos.	PAP CHAP
Compresión	Comprime los datos en el origen; descomprime en el destino.	Stacker o Predictor
Detección de errores	Comprueba los datos del enlace. Evita bucles de trama.	Magic Number Quality

Los Ruteadores Cisco que utilizan el encapsulado PPP pueden incluir las opciones LCP que muestra la tabla 11.1:

- Las opciones de autenticación requieren que la parte del enlace que efectúa la llamada introduzca la información necesaria para garantizar que la llamada tiene el permiso del administrador de red. Ruteadores homólogos intercambian mensajes de autenticación. Existen dos alternativas
  - Protocolo de Autenticación por Contraseña (Password Authentication Protocol [PAP])
  - Protocolo de Autenticación por Acuerdo de Reto (Challenge Handshake Authentication Protocol [CHAP])
- Las opciones de compresión incrementan el rendimiento efectivo en las conexiones PPP reduciendo la cantidad de datos de la trama que deben viajar a través del enlace. El protocolo descomprime la trama en el destino. Los dos protocolos de compresión disponibles en los Ruteadores Cisco son Stacker y Predictor.

- Los mecanismos de detección de errores del protocolo PPP permiten que un proceso identifique condiciones de error. Las opciones Quality y Magic Number ayudan a garantizar un enlace de datos fiable sin bucles.
- El software Cisco IOS Release 11.1 y posteriores soportan PPP multienlace. Esto permite el equilibrado de la carga sobre las interfaces del Ruteador que usan PPP.

  La fragmentación y secuenciación de paquetes, divide la carga para PPP y envía sobre fragmentos sobre circuitos paralelos. En algunos casos, este “mazo” de conducto PPP multienlace funciona como un enlace individual lógico, mejorando el rendimiento y reduciendo la latencia entre pares de Ruteadores.

VI.7.13 ESTABLECIMIENTO DE UNA CONEXIÓN PPP

Para que los dispositivos se comuniquen utilizando PPP, el protocolo debe abrir primero una sesión. La figura 6.9 ilustra este establecimiento de conexión.

El establecimiento de una sesión PPP consta de tres fases:

Paso 1. Fase de establecimiento del enlace. En esta fase, cada dispositivo PPP envía paquetes LCP para comprobar el enlace de datos. La compresión de ciertos campos PPP y el protocolo de autenticación del enlace. Si una opción de configuración no esta incluida en un paquete LCP, se asume su valor predeterminado.

FIGURA 6.9 ESTABLECIMIENTO DE UNA CONEXIÓN PPP.

Paso 2. Fase de autenticación (opcional). Una vez establecido el enlace y elegido el protocolo de autenticación, el par puede ser autentificado. La autenticación, caso de ser utilizada, tiene lugar antes de la entrada en la fase de protocolo de capa de red.

Paso 3. Fase de protocolo de capa de red. En esta fase, los dispositivos PPP del enlace envían paquetes NCP para elegir y configurar uno o más protocolos de capa de red, como IP. Una vez configurado cada protocolo de capa de red elegido, se puede enviar datagramas desde cada protocolo de capa de red sobre el enlace.

VI.7.14 CONFIGURACION DEL ENCAPSULADO PPP Y LA AUTENTICACION CHAP

Cuando se configura la autenticación PPP, se puede seleccionar PAP o CHAP. En este trabajo solo se verá CHAP, por lo que solo se describirá a este. A continuación se describe el método de autenticación.

VI.7.15 AUTENTICACION DE PROTOCOLO DE AUTENTICACIÓN POR CONTRASEÑA (CHAP)

CHAP es un método de autenticación más robusto que PAP. CHAP se utiliza en el inicio de un enlace y, periódicamente, para comprobar la identidad de un nodo remoto utilizando un intercambio de señales de tres direcciones. CHAP tiene lugar en el establecimiento inicial del enlace y puede repetirse en cualquier momento posterior al establecimiento del enlace y puede repetirse en cualquier momento posterior al establecimiento del enlace. La figura 6.10 ilustra las transacciones que tienen lugar durante la autenticación CHAP.

Una vez terminada la fase de establecimiento del enlace PPP, el Ruteador local envía un mensaje “desafió” al nodo remoto. El nodo remoto responde con un valor calculado utilizando una función hash de una dirección (normalmente MD5). El Ruteador local comparará la respuesta del valor hash esperado con su propio cálculo. Si el valor coincide, la autenticación es reconocida. En otro caso, la conexión se termina inmediatamente.

CHAP ofrece protección contra ataques de reproducción sistemática mediante el uso de valor de desafió variable que es único e imprevisible. La utilización de desafíos repetidos se hace con la intención de limitar el tiempo de exposición a cualquier ataque individual. El Ruteador local (o servidor de autenticación de terceros como TACAS) controla la situación de la frecuencia y temporizacion de los desafíos.

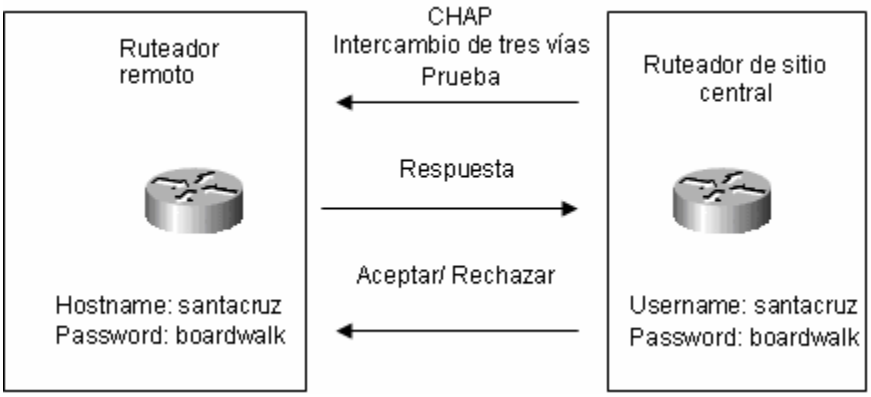


FIGURA 6.10 AUTENTICACIÓN CHAP.

VI.7.16 HABILITACION DEL ENCAPSULACION PPP Y LA AUTENTICACION CHAP

Para habilitar el encapsulado PPP y la autenticación CHAP, hay que configurar los elementos listados en la tabla 6-3

TABLA 6-3 TAREAS DE LA AUTENTICACIÓN PPP

Ruteador que autentifica (Ruteador	**Ruteador que será autentificado**

recibe la llamada)	**(Ruteador que inicia la llamada)**
Encapsulado PPP	Encapsulado PPP
Nombre de host	Nombre de host
Nombre de usuario	Nombre de usuario
Autenticación PPP	Autenticación PPP

Para habilitar el encapsulado PPP, entre en el modo de configuración de interfaz, Introduzca el comando de configuración de interfaz ***encapsulation ppp*** para especificar el encapsulado PPP en la interfaz (o en serial asíncrono como el puerto auxiliar del Ruteador).

Ruteador(config-if)#**encapsulation ppp**

Antes de configurar la autenticación PPP, es necesario configurar la interfaz para el encapsulado PPP. Para habilitar la autenticación CHAP, siga los siguientes pasos que se detallan a continuación:

Paso 1 Comprobar que cada Ruteador tiene un nombre de host asignado. El nombre de host se utilizara como “nombre de usuario” en la identificación del Ruteador con su par PPP. Para asignar un nombre de host, introduzca el comando **hostname nombre** en el modo global (ya antes descrito):

Ruteador(config)#hostname nombre

La opción ***nombre*** debe coincidir con un nombre de usuario que este configurado en el Ruteador par del otro extremo del enlace.

Paso 2 Definir en cada Ruteador el nombre de usuario y contraseña que se espera desde el Ruteador remoto, con el comando de configuración global **username nombre password contraseña:**

Ruteador(config)#username nombre password contraseña

La opción ***nombre*** es el nombre de host del Ruteador remoto. Tenga en cuenta que en este caso se distingue entre mayúsculas y minúsculas. La opción ***contraseña*** establece la contraseña que será utilizada para la conexión. En los Ruteadores Cisco, la contraseña debe ser la misma para ambos Ruteadores. En el software anterior al IOS Release 11.2, la contraseña aparecía en la configuración, como contraseña cifrada, o secreta. A partir de Release 11.2, la contraseña aparece como contraseña legible, no cifrada. Para ocultar las contraseñas y evitar que aparezca en la configuración del Ruteador IOS, introduzca el comando ***service password-encryption*** en el modo de configuración global. (Este comando afecta sólo al modo en que se muestran las contraseñas en la configuración del Ruteador. Las contraseñas CHAP se siguen intercambiando como valores MD5 cifrados).

Añadir una entrada de nombre de usuario para cada sistema remoto con el que el Ruteador local se comunique y requiera autenticación. El dispositivo remoto debe tener también una entrada de nombre de usuario para el Ruteador local. Recuerde que el

Ruteador comparara estos nombres de usuario con los nombres de host del Ruteador remoto para la autenticación.

Paso 3 Configurar la autenticación PPP con el comando de configuración de interfaz **ppp authentication**. Esta es una sintaxis completa:

Ruteador(config-if)#ppp authentication {chap | chap pap | pap chap | chap}

Nota: Si PAP y CHAP están habilitados a la vez, el primer método especificado se demandará durante la negociación del enlace. Si el Ruteador remoto sugiere el uso del segundo método ó simplemente rechaza el primer método, entonces se intentará el segundo método.

VI.8 GENERALIDADES DE RUTEO DE MARCADO BAJO DEMANDA (DDR)

Los servicios RDSI pueden ser utilizados para una gran variedad de servicios de red. Una aplicación muy habitual de RDSI es el DDR. Una vez que se tiene en mente la redundancia de enlace, ahora se tiene oportunidad de aprender a configurar esta interfaz cuando necesite transferir tráfico, por otro medio cuando el principal falle.

El DDR es un conjunto de características CISCO que permiten a dos ó más Ruteadores Cisco establecer una conexión dinámica sobre un único acceso telefónico, para enrutar paquetes e intercambiar actualizaciones de enrutamiento conforme se necesite. El DDR se utiliza en conexiones de redes intermitentes de poco tráfico sobre el POTS (Servicio telefónico analógico convencional) o en una RDSI. La figura 6.11 ilustra una configuración DDR típica.

Tradicionalmente, las redes se han interconectado por las líneas WAN dedicadas. DDR responde a la necesidad de conexiones de redes intermitentes sobre un servicio WAN de conmutación de circuitos. Si se usan conexiones WAN sólo cuando se necesitan, el DDR reduce el coste del uso de WAN.

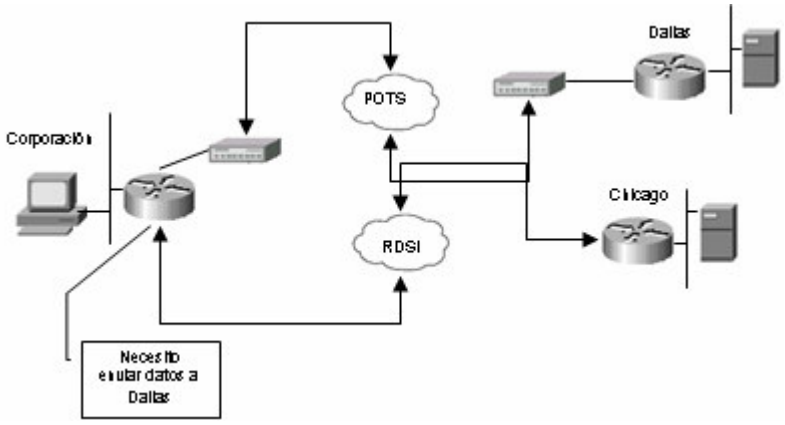


FIGURA 6.11 RUTEO DE MARCADO BAJO DEMANDA.

Este trabajo no trata a todas las configuraciones avanzadas del DDR. Entre estas características están las siguientes:

- **Perfiles de la llamada**: Posibilidad de configurar DDR para que las configuraciones de la interfaz física estén separadas de las configuraciones lógicas requeridas para realizar una llamada DDR.

- **Multienlace PPP**. Posibilidad de agregar tráfico sobre múltiples canales RDSI simultáneamente.

- **Línea telefónica de respaldo**. Posibilidad de habilitar una línea secundaria cuando falla el enlace principal. Esta última es la que veremos.

VI.8.1 EL COMANDO "CHAT-SCRIPT"

Para crear un argumento que situará una llamada sobre un MODEM, utiliza el comando "**chat-script"** en modo de configuración global. Usa la forma "**no"** de este comando para deshabilitar el argumento de charla especificado. El valor por omisión no está definido en los argumentos de charla por las diferentes variables a configurar.

chat-script *script-name expect-send*

no **chat-script *script-name expect-send***

La descripción de sintaxis

script-name	Nombre del argumento de charla.
expect-send	Contenido del Chat script.

Los argumentos de charla son usados en dial-on-demand routing (DDR) para dar comando de marcado al MODEM y los comandos para acceder a los sistemas remotos. El argumento definido será usado para situar una llamada a un MODEM.

Algunas características de argumentos son los siguientes:

- Los argumentos de charla son del caso sensitivo.

- Tú puedes tener cualquier número de secuencias activas de ABORT a la vez.

- Cuando un argumento de charla comienza, el tiempo fuera por omisión es de 5 segundos. Cambia el tiempo fuera para persistir hasta el próximo tiempo, tú los cambias en el argumento.

- Una cadena dentro de comillas se trata de una sola entidad.

La tabla 6-4 muestra los argumentos posibles para la secuencia de escape en una charla entre módems.

TABLA 6-4 ARGUMENTO DE CHARLA DE SECUENCIAS DE

ESCAPE	
Secuencia de Escape	**Descripción**
" "	Se espera de cadena nula.
EOT	Envía un carácter de finalización de transmisión.
BREAK	Causa una pausa (BREAK). Esta secuencia es algunas veces simulada con una línea de velocidad y caracteres nulos. Puede no trabajar en todos los sistemas.
\c	Suprime una nueva línea al final del la cadena enviada.
\d \K	Retardo por 2 segundos. Inserta una pausa (BREAK)
\n	Envía una nueva línea o caracter de línea de alimentación.
\p	Pausa por .25 segundos.
\r	Envía un retorno.
\s	Envía un caracter de espacio.
\t	Envía un caracter de tabulación.
\\	Envía un caracter de diagonal invertida [backslash (\)]
\T	Resitua por el número telefónico.
\q	Reservado, todavía no usado.

La tabla 6-5 muestra algunos ejemplos de ejecución en un argumento de MODEM.

TABLA 6-5 EJEMPLO DE EJECUCION DE UN ARGUMENTO DE MODEM	
Par de Espera y Envio	**Implementación**
ABORT	Finalizar la ejecución del argumento si el texto

ERROR	"ERROR" es encontrado. (Tú puedes tener como muchos entradas abortadas activas como desees)
" " "AT Z"	Sin espera de nada, envía un comando "AT Z" para el MODEM. (Nota el uso de la comillas para permitir un espacio en la cadena de envío)
OK "ATDT \T	Espera ver "OK." Envía "ATDT 96837890."
TIMEOUT 60	Espera 60 segundos para la próxima cadena esperada.
CONNECT \c	Espera "connect," pero no envíes nada. (Nota que **\c** es efectivamente nada; " " habría indicado nada seguido por el retorno de carro.)

VI.8.2 CREAR ARGUMENTOS DE CHARLA PARA INTERFACES ASÍNCRONAS

Para especificar un argumento de charla para una línea, realiza la siguiente tarea en el modo fe configuración de línea:

Tarea	Comando
Especifica un argumento de MODEM para una línea.	**script dialer *regexp***

Un máximo de un comando **script dialer** puede ser configurado por línea. El argumento de charla te permite especificar un argumento de charla por el tipo de MODEM adjunto a la línea como sigue:

script dialer *modem-type**

Este es recomendado que un argumento de charla (un argumento de charla “dialer") es escrito para colocar una llamada y otro argumento de charla (un argumento de charla "system" o "login") es escrito para autenticarse en los sitios remotos, donde es requerido.

El estilo regular de las expresiones en UNIX son usadas para comparar patrones y seleccionar entre muchos argumentos. Este ser muy útil si tú especificas argumentos del MODEM en una interfaz que es usada para marcar múltiples destinos.

Tú puedes también asignar argumentos de charla para interfaces asíncronas para otros propósitos que los de DDR.

VI.8.3 CONFIGURANDO LLAMADAS PARA UN SOLO SITIO

El argumento de charla llega a ser por omisión el argumento de charla para una interfaz. Esto significa que este llega a ser por omisión el argumento de charla para los comandos **dialer string** y **dialer map** presentados en esta sección.

Para configurar una interfaz para llamar a un solo sitio, realiza los siguientes pasos:

Paso 1 Habilita el DDR en la interfaz.

Paso2 Para la interfaces sincronas, específica la cadena de marcado.
Para interfaces asíncronas, especifica el argumento de charla y la cadena de marcado.

Para habilitar DDR y también especifiques el marcado del DTR o el marcado del in-band, realiza uno de las siguientes tareas en el modo de configuración de línea:

Tarea	**Comando**
Configura una interfaz serial para usar el marcado del DTR.	**Dialer dtr**
Configura una interfaz serial para el marcado del in-band.	**Dialer in-band** [**odd-parity** | **no-parity**]

Para un solo sitio sobre líneas seriales conectadas por MODEM sin uso del V.25bis usando solamente la señalización EIA (específicamente, la señal DTR [Data Terminal Ready]), tú habilitas el DDR usando el comando **dialer dtr**. Una interfaz configurada para la señalización DTR puede colocar solamente llamadas, esto no las puede aceptar. Los grupos rotativos de marcado arrendados no pueden ser configurados por la señalización DTR.

Para llamar a un solo sitio en las seriales conectadas por interfaces conectadas por interfaces asíncronas o por Modems V.25bis o interfaces sincronas, tú habilitas el DDR usando el comando **dialer in-band**. Si usas Modems V.25bis, tú puedes opcionalmente especificar en parte. La versión de 1984 de los estados de especificaciones V.25bis que los caracteres deben tener extrañamente la paridad. Sin embargo, por omisión NO tiene paridad.

VI.8.4 EL COMANDO “DIALER IN-BAND”

Específica que DDR es soportado, usa el commando “**dialer in-band”** en el modo de configuración de la interfaz. Usa la forma “**no”** de este comando para deshabilitar el DDR para la interfaz.

El comando **dialer in-band** específica que argumentos de charla serán usados en las interfaces asíncronas. Las palabras claves de igualdad no aplican en la interfaces asíncronas.

VI.8.5 EL COMANDO "DIALER IDLE-TIMEOUT"

Para especificar el tiempo de espera antes de que la línea sea desconectada, se debe usar el comando "**dialer idle-timeout"** en el modo de configuración de interfaz. Usar la forma "**no"** de este comando para reiniciarlo al valor por omisión que es de 120 segundos.

La forma es:

dialer idle-timeout *segundos*

no **dialer idle-timeout**

La descripción de sintaxis

segundos	Tiempo de espera, en segundos, que debe ocurrir en la interfaz antes de que la línea sea desconectada. Los valores aceptables son positivos no cero.

VI.8.6 EL COMANDO "DIALER ENABLE-TIMEOUT"

Configura la longitud de tiempo en la interfaz que esta caída después una llamada es completada ó fallida y antes de que este disponible para marcar otra vez. Use el comando "**dialer enable-timeout"** en el modo de configuración de la interfaz. Para regresar al valor de omisión utilice la forma "**no"** de este comando. El valor de omisión es de 15 segundos.

dialer enable-timeout *segundos*

no **dialer enable-timeout**

La descripción de sintaxis

Segundos	Tiempo en segundos que software de Cisco IOS espera antes de la próxima llamada que puede ocurrir en la interfaz especifica. Los valores aceptables son positivos, no cero en el rango de 1 hasta 2147483.

Nota Para interfaces asíncronas no requiere un argumento de sistema, un argumento de MODEM debe ser definido por la línea asociada para el uso del comando **script dialer** en la configuración de línea.

Para colocar una llamada a un solo sitio en una interfaz de línea asíncrona para el cual el argumento de MODEM no ha sido asignado o un argumento de sistema debe ser especificado, realiza la siguiente tarea en el modo de configuración de la interfaz:

Tarea	**Comando**
Especifica argumentos de charla y una cadena de marcado.	**dialer map *protocol next-hop-address*** [**modem-script**

	modem-regexp] [**system-script** ***system-regexp***] ***dial-string*** [***isdn-subaddress***]

Usa el comando **dialer map** para especificar un argumento de charla si no es el argumento de MODEM es especificado para la línea o un adicional argumento de charla (sistema) es requerido para autenticar en el sitio remoto.

Tú no necesitas especificar un argumento de sistema si uno de los siguientes puntos se cumple:

El argumento de MODEM puede se usado para marcar y autenticarse en el sistema remoto.

Tú estas llamando a un sistema que no requiere un argumento de autenticación, esto es, un sistema que responde e inmediatamente que va dentro del modo del protocolo.

Si tú quieres llamar a un solo sitio remoto por interfaz, el comando **dialer string** es muy útil. Tu no necesitas el comando **dialer map** para la autenticación. Los marcados pasan la cadena que tú has definido para el DCE externo.

Para especificar la cadena (número telefónico) para ser llamado en interfaces seriales (asíncronas y sincronas), realiza la siguiente tarea en el modo de configuración de interfaz:

Tarea	Comando
Especifica una cadena de números para marcar.	**dialer string** ***dial-string***

VI.8.7 EL COMANDO “DIALER MAP”

Configurar una interfaz serial para llamar a uno ó múltiples sitios o recibir llamadas de múltiples sitios, utilice el comando “**dialer map”** en el modo de configuración de la interfaz, las opciones son mostradas en la descripción de sintaxis. Para eliminar una entrada particular de dialer map, utilice la forma “**no”** de este comando.

La descripción de sintaxis

Protocol	Palabras claves; uno de los siguientes: **appletalk**, **bridge**, **clns**, **decnet**, **ip**, **ipx**, **novell**, **snapshot**, **vines**, y **xns**.
next-hop-address	Dirección de protocolo usada para igualar contra la dirección en los cuales los paquetes son destinados. Este argumento no se usa con la palabra clave **bridge**.
Name	(Opcional) Indica el sistema remoto con el cual el Ruteador local al comunica al access server. Usada para autenticar el sistema remoto en llamadas de entrada.

hostname	(Opcional) Para casos sensitivos del nombre o ID del sitio remoto del dispositivo remoto (usualmente el Hostname).
broadcast	(Opcional) Indica que los broadcasts deben ser enviados a esta dirección del protocolo.
MODEM-script	(Opcional) Indica el argumento del MODEM para ser usado para la conexión (para interfaces asíncronas).

VI.8.8 EL COMANDO "DIALER-GROUP"

Para controlar el acceso por la configuración de una interfaz permitida a un específico grupo de marcado, usa el comando "**dialer-group"** en el modo de configuración de la interfaz. Usa la forma "**no"** de este comando para removerla de la interfaz del grupo de acceso de marcado.

dialer-group *group-number*

no **dialer-group**

La descripción de la sintaxis.

Group-number	Número de grupo de acceso de marcado para una específica interfaz perteneciente. Este grupo de acceso es definido con el comando "**dialer-list"**. Los valores aceptables son positivos de 1 a 10.

VI.8.9 EL COMANDO "ASYNC DEFAULT ROUTING"

Para habilitar al Ruteador para pasar las actualizaciones de ruteo a otro Ruteador sobre el Puerto Auxiliar configurada como una interfaz asíncrona, usa el comando "**async default routing"** en el modo de la configuración de interfaz. Usa la forma "**no"** de este comando para deshabilitar el direccionamiento dinámico.

async default routing

no **async default routing**

VI.8.10 EL COMANDO "ASYNC MODE DEDICATED"

Para situar una línea dentro del modo asíncrono dedicado usando Serial Line Internet Protocol (SLIP) o encapsulación PPP, usa el comando "**async mode dedicated"** en el modo de configuración de la interfaz. Usa la forma "**no"** de este comando para regresar la línea al modo inactivo.

async mode dedicated

no **async mode dedicated**

Syntax Description

VI.8.11 EL COMANDO "DIALER-LIST PROTOCOL"

Para definir una lista de marcado de dial-on-demand routing (DDR) para la marcación por el protocolo o por una combinación de un protocolo y una lista de acceso previamente definida, usa el comando "**dialer-list protocol"** en el modo de configuración global. Usa la forma "**no"** de este comando para borrar una lista de marcado.

dialer-list *dialer-group* protocol *protocol-name* {**permit** | **deny** | **list *access-list-number*** | ***access-group***}

no **dialer-list *dialer-group*** [**protocol *protocol-name*** [**list *access-list-number*** | ***access-group***]]

La descripción de sintaxis.

dialer-group	Número de un grupo de acceso de marcado identificado en cualquier comando **dialer-group** en la configuración de interfaz.
protocol-name	Uno de las palabras claves siguientes de protocolos son: **appletalk**, **bridge**, **clns**, **clns_es**, **clns_is**, **decnet**, **decnet_Ruteador-L1**, **decnet_Ruteador-L2**, **decnet_node**, **ip**, **ipx**, **vines**, o **xns**.
permit	Permite el acceso a un protocolo completo.
deny	Deniega el acceso a un protocolo complete.
list	Específica que una lista de acceso será usado para definir una fina granularidad que un protocolo completo.
access-list-number	Números de lista de acceso especificado en cualquier DECnet, Banyan VINES, IP, Novell IPX, ó XNS, en listas de acceso estándar ó extendidas, incluyendo listas de acceso de Novell IPX en el punto de acceso de servicio extendido (SAP) y tipos de puente.
access-group	Nombre de una lista de filtro usada en el "**clns filter-set"** y comandos **clns access-group**.

VI.9 CONFIGURACION EN EL PUERTO AUXILIAR

Se debe puntualizar que para que se tome el puerto auxiliar como el puerto de respaldo cuando se cae la señal principal en nuestra serial, se debe tomar en cuenta que debemos configurarlo, y para ellos debemos considerar la señalización como la interfaz que va a interconectar a nuestro MODEM, así que se mostrará de manera general estas señales y para su mejor entendimiento lo hacemos refiriéndonos de la señalización del MODEM con una computadora.

Comúnmente utilizan el interfaz del conector RS-232D (DB25) y esta dividido en grupos distintos de señales como son:

- Señales de Datos.

- TXD (Transmit Data): Los datos son enviados desde la computadora al módem por este pin para transmisión.
- RXD(Received Data): Los datos son recibidos por la computadora.

- Señales de Control.

- DTR (Data Terminal Ready): La computadora usa DTR para decirle al módem que está encendida, el software esta cargado, y esta lista para comunicarse.
- DSR (Data Set Ready) o MR (módem Ready): El módem local le dice a la computadora que esta encendido en modo normal de operación.
- DCD (Data Carrier Detect) o CD (Carrier Detect): Una indicación de que el módem remoto esta en línea y esta listo para intercambiar datos. (la presencia de una portadora no implica que la portadora tiene datos). Esta señal es proporcionada a la computadora desde el módem local.
- RI (Ring Indicator): El módem sensa el timbrado en la línea.
- RTS o RS (Request to Send): La computadora es preguntando al módem si esta listo para empezar a transmitir datos.
- CTS o CS (Clear To Send): El módem le dice a la computadora que continúe y empiece a enviar datos

VI.9.1 EL COMANDO “MODEM INOUT”

Configura el Puerto Auxiliar del MODEM (AUX) para entrada/salida. Esto significa que tú debes configurar el MODEM para proporcionar la Detección de la Portadora (CD) por que el Ruteador se desconecta cuando la señal de CD cae. También, el Ruteador tira la señal Terminal de Datos Preparada (Data Terminal Ready [DTR]) si esta quiere que el MODEM se desconecte. El programa del MODEM cuelga cuando tira la señal DTR.

```
modem inout
```

VI.9.2 EL COMANDO “FLOWCONTROL HARDWARE”

Usa el Control de Flujo de Hardware (hardware flow control [RTS/CTS]). El Puerto auxiliar (AUX) lanza la señalización de Requerimiento para Envío (Request To Send [RTS]) cuando este quiere que el MODEM se desconecte, y el MODEM debe lanzar la señalización de Limpiado para Envío (Clear To Send [CTS]) si este quiere un control de flujo en el puerto Auxiliar (AUX). El Programa del MODEM para RTS/CTS.

```
flowcontrol hardware
```

VI.9.3 EL COMANDO “TRANSPORT INPUT ALL”

Define cual de los protocolos pueden ser usados para conectarse a una línea especifica.

```
Transport input all
```

V.10 IMPLEMENTACION DE LA SOLUCION DEL ANALISIS DEL SISTEMA DE REDUNDANCIA.

Aquí también se tomará en cuenta todos los parámetros y solicitudes, así como recursos con que cuenta la empresa se realiza la siguiente solución de un sistema redundante de su red Frame Relay.

Teniendo en cuenta el hardware de la infraestructura tenemos los siguientes:

Aquí debemos hacer un análisis ya que estamos considerando que los sitios que queremos realizar la redundancia es en sitios remotos que acceden a través de la red Frame Relay a su corporativo o nodo central, donde cada sitio remoto tiene aproximadamente de 15 PC's a 20 PC's. Con switches Catalys y necesitan acceder a los sistemas de Web o aplicaciones de bases de datos, sin embargo, la circunstancia es que necesitan una mínimo índice de falla en la red, por lo que se necesitará realizar el sistema redundante DDR para Frame Relay. Así como también el cliente requiere una mejoría en su ancho de banda.

Análisis 1: Como sabemos que sus equipos requieren protocolos TCP/IP están cubiertos sin problema, ya que el acceso de los servidores de bases de datos ó a portales Web, no tendrán problemas con este acceso.

El punto radica de cómo se no se vería afectado con alguna interrupción del enlace.

Tenemos que son 31 sitios que utilizan 384 Kbps a lo largo de la Republica Mexicana, en cada uno de los Estados; y no tienen ningún problema por realizar sus actividades, dando como resultado que no se realizara ninguna ampliación de ancho de banda, lo que se requiere realizar es que a través de una línea telefónica directa se logre realizar la redundancia solo que aquí estamos limitados a la velocidad del MODEM externo que será de 56 Kpbs, lo que significaría que habría suficiente ancho de banda para utilizar base de datos en línea y correos electrónicos (solo para casos de suma importancia, es decir, las actividades indispensables para que opere el sitio remoto).

Análisis 2: Aprovecharemos el Ruteador Cisco 2501 que se encuentra en cada uno de los sitios remotos por lo que se utilizara su puerto auxiliar para realizar el respaldo de Frame Relay que en termino generales se activará cuando la interfaz serial primaria tenga una falla. De esta manera se garantiza la continuidad del enlace.

Esto se realiza a través de DDR de Frame Relay cuando el enlace primario cae, el puerto auxiliar a través del MODEM externo conectado a este, que solicitará una petición al Servidor de Acceso para poder entrar por este canal a la red Frame Relay.

Aquí el tema central es que la línea telefónica que se conecta al MODEM externo siempre está al puerto auxiliar, por lo que se tendrá que rentar una línea telefónica analógica que estará en espera de ser ocupada, solo que aquí estamos hablando de que los sitios se encuentran dispersos en los estado de la República y como dato del cliente

se encuentra en la capitales de los Estados de la República Mexicana por lo que no se torna difícil que algún proveedor de telefonía local en cada Estado la proporcione; pero se debe tomar en cuenta que la llamada se realizara a través de larga distancia por lo que será un costo mayor, pero esto no debe ser una limitante para no crear un respaldo del enlace, ya que la falta de continuidad del enlace y por tanto las actividades de la empresa sería más costoso, la espera de falla del enlace. Y se realiza una mejora de ancho de banda con los métodos de congestión de Frame Relay, así mismo como generar subinterfaces. Por lo tanto, se debe plantear la solución de este respaldo a continuación.

Solución: Para determinar la solución debemos enlistar con los que se cuenta, en cuanto a equipos, Acceso a Internet, aplicaciones de sus sistemas, y seguridad en la red, que son los siguientes.

- 1 Ruteador 2501, con puerto AU1 y 2 puertos Seriales.
- 1 Transciver de puerto AUI a RJ45 (FastEthernet)
- 1 Acceso de par de cobre con 384 Kbps
- 1 puerto auxiliar asíncrono
- 15 a 20 PC’s cada sitio
- Switches Catalys 1900 o 2900.

Con lo que debemos contar además de lo que tenemos para la implementación de la redundancia de DDR para Frame Relay de Cisco que es el siguiente:

- 1 MODEM externo por localidad
- 1 Línea analógica contratada
- Configuración de conexión hacia Servidor de Acceso
- 1 Servidor de Acceso (Acces Server), este lo configura el proveedor de la red de Frame Relay por la seguridad que implica en la red del proveedor.

Al final quedarían:

- 1 Ruteador 2501, con puerto AU1 y 2 puertos Seriales.
- 1 Transciver de puerto AUI a RJ45 (FastEthernet)
- 1 Línea Analógica contratada
- Switches Catalys 1900 o 2900
- 1 Servidor de Acceso (aunque este será proporcionado por el proveedor)
- 1 MODEM externo por localidad

Primeramente la parte del hardware y conexiones se deben realizar de la siguiente manera, el Ruteadores 2501 en el puerto auxiliar se conectará el MODEM que a su vez se conectará a la línea telefónica analógica, que esto completa el respaldo DDR de Frame Relay.

Por lo que respecta al Servidor de Acceso lo configura el proveedor de la red Publica de Frame Relay, por lo que solo nos indicara los usuarios y la contraseñas que autenticara al MODEM con el Servidor de Acceso, para que sea configurado en el Ruteador y pueda tener acceso.

El Ruteador contendrá la configuraciones de la autenticación, como las configuraciones del MODEM, así como el argumento de charla, y también el teléfono que se configurara, y también el Servidor de Acceso estará en la ciudad de México, será el mismo número, pero con larga distancia.

Por último se verá en la siguiente sección, donde se observará con detenimiento en cada uno de los comandos utilizados en el Ruteador para que pueda respaldar el enlace a través de la línea telefónica analógica con apoyo del MODEM, que estará solicitando una conexión en el Servidor de Acceso. Por la parte de mejorar el ancho de banda se realiza la creación de subinterfaz, y configurar el map-class de Frame Relay de manera personalizada como se muestra a continuación.

En la figura 6.12 se muestra el diagrama de cómo se colocaran el sistema redundante DDR para Frame Relay de Cisco.

VI.11 EL DIAGRAMA Y CONFIGURACION DE LA IMPLEMENTACION DE UN RUTEADOR CISCO CON FRAME RELAY Y REDUNDACIA DDR

En la figura 6.12 se muestra el arreglo del esquema redundante para Frame Relay con DDR en una localidad remota hacia el nodo principal de la red.

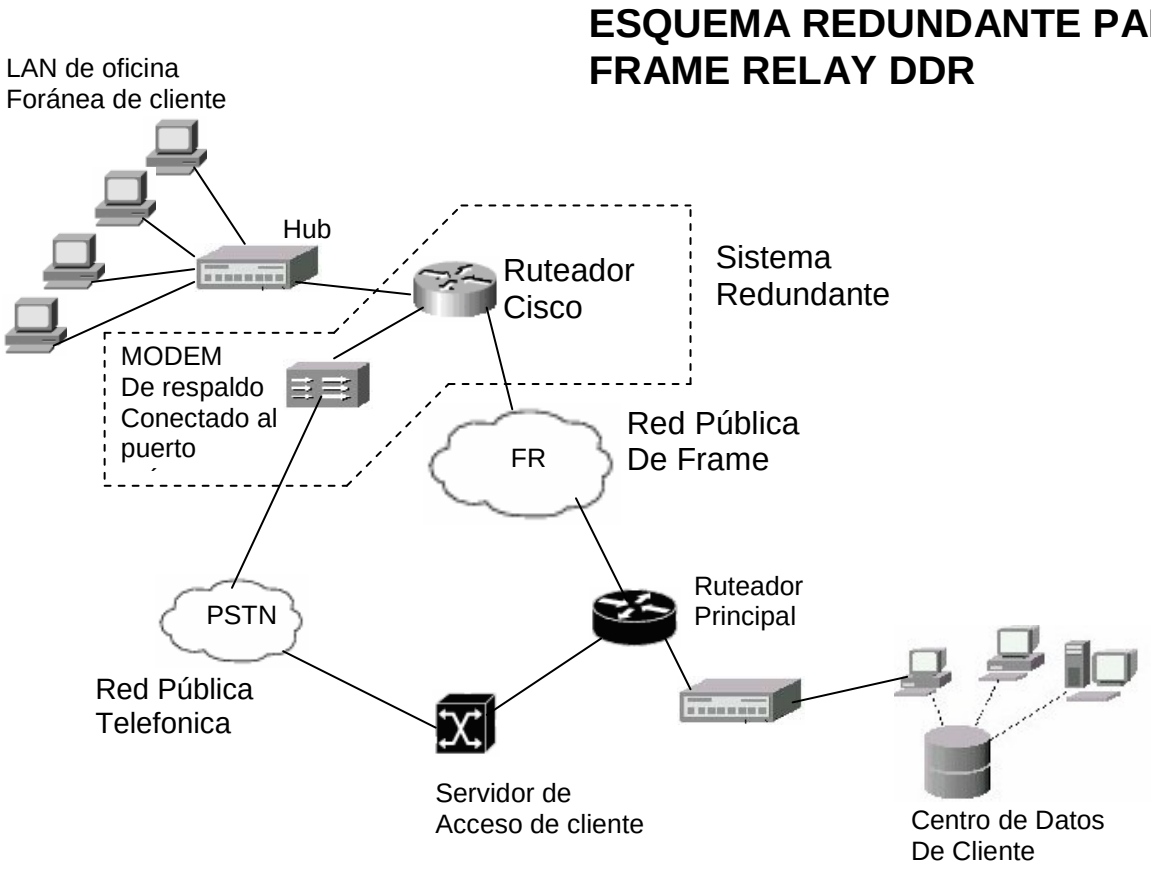


FIGURA 6.12 DISEÑO DE RED FRAME CON REPALDO DDR

CONFIGURACION DE UN RUTEADOR CISCO DE UNA OFICINA FORANEA:

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RUT_DDR1
!
logging rate-limit console 10 except errors
enable password avant3lgetr0
!
memory-size iomem 25
ip subnet-zero
no ip finger
!
!
interface FastEthernet0
 ip address 172.16.31.1 255.255.255.0
 speed auto
!
interface Serial0
 no ip address
 encapsulation frame-relay
 no ip mroute-cache
 frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
  ip address 10.10.11.62 255.255.255.252
 no ip mroute-cache
 frame-relay interface-dlci 27
  class bw384
!
interface Async1
 ip unnumbered FastEthernet0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 180
 dialer enable-timeout 180
 dialer map ip 172.18.116.50  AcSer RUT_DDR1 modem-script dialnum broadcast
015557345678
 dialer-group 1
 async default routing
 async mode dedicated
```

```
 ppp authentication chap
!
dialer-list 1 protocol ip permit
!
!
chat-script dialnum "" "atdt, 015557345678" TIMEOUT 60 CONNECT \c
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.11.61
no ip http server
!
!
map-class frame-relay bw384
 frame-relay cir 38400
 frame-relay mincir 384000
 frame-relay fair-queue
 frame-relay fragment 160
 logging trap debugging
logging 192.168.100.6
!
snmp-server community STgLgF8bI1vEQnC RW
snmp-server chassis-id RUTEADOR_RESPALDO
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server host 192.168.100.2 STgLgF8bI1vEQnC
!
!
line con 0
 transport input none
line aux 0
 modem InOut
 transport input all
 flowcontrol hardware
! line vty 0 4
 password mypwdlost
 login
!
no scheduler allocate
end
```

VI.11.1 EXPLICACION DE LA CONFIGURACION

Como se muestra en la figura 6.12 el diseño de la red, es también asegurar la integridad de servicio en las oficinas foráneas del cliente, ya que muchas empresas que retoman este diseño es por que están comprometidas a dar un servicio seguro y eficiente en ciudades expandidas en la nación. Sin embargo para bajar los costos de sistemas redundantes, se dio una solución de tomar una línea telefónica para respaldo. Para

obtener una mejor rendimiento cuando el circuito de Frame Relay se encuentre inactivo, tomará un camino por la interfaz asíncrona con ayuda de un MODEM. Por lo que a continuación daremos la explicación de las líneas que integran a la configuración Frame Relay y el respaldo en la interfaz Asíncrona.

Observamos que en la Interfaz Ethernet, sólo maneja dos comandos que es la dirección IP que es configurada con el comando "**ip address a.b.c.d 0.0.0.0**", donde a.b.c.d es la dirección IP, y el valor de 0.0.0.0 es la correspondiente mascara. Todo esto se lleva a cabo en el modo de configuración de la interfaz Ethernet.

Cuando configuramos en la interfaz en Frame Relay se vuelve un poco más complejo por que aquí observamos que existe la interfaz física donde se muestra la encapsulación Frame Relay con el comando "**encapsultaion frame-relay**", así como también el tipo de "lmi" configurado, en este caso se realizo el "**ANSI**", realizado con el comando "**frame-relay lmi-type ansi**". Lo que significa que la serial física llevará a cabo la transferencia de datos con el protocolo Frame Relay con la red de su proveedor, sirviéndose para controlar la congestión en la red que en muchos casos es producida por el datos perdidos y reenviados, además también se configura el tiempo de LMI que se utilizara para soportar entre el switch y este extremo de la red.

También observamos como se realizó un subinterfaz, en este caso es punto a punto, realizada con el comando "**interfaz serial0/0.1 point-to-point**", realizado en el modo de configuración de la interfaz, aquí se muestra la línea de la dirección IP utilizada, también esta es configurada con el comando antes mencionado "**ip address a.b.c.d 0.0.0.0**", donde a.b.c.d es la dirección IP, y el valor de 0.0.0.0 es la correspondiente mascara, y se muestra la importancia de la configuración del DLCI para Frame-relay que es el indicador realizar la conmutación e identificarlo en la red, que se expresa con el comando "**frame-relay interface-dlci 27**" para que posteriormente demos la referencia que map class le corresponde. Y el comando que demos en seguida es "**class nombre_del_map_class**".

Es aquí donde nos detenemos para realizar el map class con sus diferentes líneas de configuración, que se define primero por definir el nombre del map class, que esta dado por el comando "**map-class classbw384**", y posteriormente se dan el "cir" y el "mínimo cir" que tomara cuando realice cualquier transferencia, aunque en esta configuración no hay un cambio por que el cliente necesita en todo momento el ancho de banda por ello se expresa con los mismos valores, como sigue el comando "**frame-relay cir 384000**" y el "**frame-relay mincir 384000**" lo que significa que tenemos un ancho de banda de 384 Kbps, y que el cliente lo tomará en todo momento.

Esto se hace con el siguiente los comandos de configuración, ya no nos detendremos mucho en la explicación detallada, ya que en el anterior apartado se definió como se realizaría, por lo que ahora se dará en forma general la explicación de cada modulo, veamos el modulo de Frame Relay:

```
RUT_DDR1#config t
RUT_DDR1(config)#inter ser0
RUT_DDR1(config-if)# encapsulation frame-relay
RUT_DDR1(config-if)# frame-relay lmi-type ansi
```

Y así queda:

```
interface Serial0
 no ip address
 encapsulation frame-relay
 no ip mroute-cache
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
```

Damos aquí mismo la subinterfaz

```
RUT_DDR1(config-if)# interf ser0.1 point-to-point
RUT_DDR1(config-subif)# ip address 10.10.11.62 255.255.255.252
RUT_DDR1(config-if)# frame-relay interface-dlci 27
RUT_DDR1(config-if)# class bw384
```

Y de esta manera queda:

```
interface Serial0.1 point-to-point
  ip address 10.10.11.62 255.255.255.252
 no ip mroute-cache
 frame-relay interface-dlci 27
  class bw384
!
```

A lo cual en este caso se declara el map-class que se define en el modo configuración como sigue:

```
RUT_DDR1#config t
RUT_DDR1(config)# map-clas frame-relay bw384
RUT_DDR1(config-map)# frame-relay cir 384000
RUT_DDR1(config-map)# frame-relay mincir 384000
RUT_DDR1(config-map)# no frame-relay adaptive-shaping
RUT_DDR1(config-map)# frame-relay fair-queue
RUT_DDR1(config-map)# frame-relay fragment 160
```

Este modulo queda de la siguiente manera:

```
map-class frame-relay bw384
 frame-relay cir 384000
 frame-relay mincir 384000
 no frame-relay adaptive-shaping
 frame-relay fair-queue
 frame-relay fragment 160
```

Una vez, realizado todo esto, configuramos la interfaz asíncrona (puerto auxiliar), donde configuramos el protocolo ppp para la comunicación, expresado con el comando “encapsulation ppp”. Así como las líneas siguientes donde muestra la habilitación de DDR

con el comando **“diales in-band”** que específica que los argumentos de charla serán usados en la interfase asíncrona. Con el comando **“diales dile-time out 180”** especifica el tiempo de espera antes de que la línea este desconectada y la configuración se realiza en modo de configuración de interfaz. También tenemos el comando **“dialer enable-timeout 180”** se coloca para configurar la longitud del tiempo en una interfaz que esta caída desde de que una llamada se ha completado ó fallado y antes esta disponible para marcar otra vez, esta también la configuración se realiza en el modo de configuración de interfaz. En este caso se indica que esperara 180 segundos ó 3 minutos antes de que intente marcar otra vez.

La interfaz también tiene configurada un mapeo con el comando expresado como **“dialer map ip 172.18.116.50 AcSer RUT_DDR1 modem-script dialnum broadcast 015557345678”,** donde muestra la dirección IP que tomara, después aparece el nombre del **AcSer** (name) y tambien el de “hostname”, que en este caso es – **RUT_DDR1** – que es el hostname del equipos (es decir, como se configuro es el nombre del Router) para identificar más rápidamente quien se conecta. Definiendo por último el argumento de MODEM que generará el marcado al número -**015557345678**-, ya que la línea de MODEM-script significa que siga la cadena de caracteres a través del MODEM que marcara al número telefónico antes referido, con un palabra clave de **“broadcast”** que significará que se enviara todos los broadcast a la dirección del Access Server como es la IP **172.18.116.50**, que en otras palabras es el próximo salto.

El comando **“chat-script dialnum "" "atdt, 015557345678" TIMEOUT 60 CONNECT \c”** indica que existe un argumento de charla donde el cliente y el servidor hay tendrá una autenticación entre ellos. Donde se esperará un tiempo y después se marcará al número telefónico, siguiendo la siguiente sintaxis. Para crear un argumento que situará una llamada sobre un MODEM, usa el comando **chat-script** (dentro de la configuración global). Después de él, aparece los caracteres **-“”-** que significa que espere una cadena nula y envía un **-“atdt 015557345678”-** y después espera 60 segundos para la próxima cadena esperada **TIMEOUT 60** y espera "connect," pero no envíes nada **(CONNECT \c).**

De esta manera cuando caiga la interfaz serial del circuito Frame Relay entra en una conmutación a través de la interfase asíncrona y marcara al Servidor de acceso al número telefónico configurado e ingresar para realizar el respaldo DDR.

En el comando de **“diales-group 1”** se define un grupo de marcado, este se tendrá que definir, pues si cambiará el arreglo de la red ó realizar otro grupo de marcado se tendrá que definir a que grupo se refiere dependiendo el numero de grupo, en este caso, para toda la red se registra solamente el grupo 1 de marcado. Y por tanto también se agrega el comando **“ppp encapsulation chap”** que indica cual método de encapsulación se llevará a cabo y con que encapsulación.

Por ultimo se define también el comando “**async default routing**” que menciona aquí que se trata de una actualización de tablas de ruteo con otros Ruteadores, y el comando “**async mode dedicated**” que se trata de indicar al puerto auxiliar que se dedicara a una comunicación vía MODEM con encapsulación PPP, como se definió en la líneas anteriores.

Se agrega la configuración del sistema DDR, con las generalidades de su configuración, como sigue:

```
RUT_DDR1#config t
RUT_DDR1(config)# interf asyn1
RUT_DDR1(config-if)#iip unnumbered Ethernet0
RUT_DDR1(config-if)#encapsulation ppp
RUT_DDR1(config-if)#dialer in-band
RUT_DDR1(config-if)#dialer idle-timeout 180
RUT_DDR1(config-if)#dialer enable-timeout 180
RUT_DDR1(config-if)#dialer map ip 172.18.116.50 Ac_Ser RUT_DDR1 modem-script
dialnum broadcast 12345678
RUT_DDR1(config-if)#dialer-group 1
RUT_DDR1(config-if)#ppp authentication chap
RUT_DDR1(config-if)#async default routing
RUT_DDR1(config-if)#async mode dedicated
```

Y quedaría de la siguiente manera:

```
interface Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 180
 dialer enable-timeout 180
 dialer map ip 172.18.116.50 name Access_Server modem-script dialnum broadcast
015557345678
 dialer-group 1
 async default routing
 async mode dedicated
 ppp authentication chap
!
```

En modo de configuración global se configura como sigue:

```
RUT_DDR1#config t
RUT_DDR1(config)#chat-script dialnum "" "atdt, 12345678" TIMEOUT 60 CONNECT \c
!
```

Uno de los puntos que se tienen que definir es el permiso del grupo de marcado como se muestra en la siguiente configuración:

Y así quedaría la configuración:

```
RUT_DDR1#config t
RUT_DDR1(config)# dialer-list 1 protocol ip permit
!
```

Recordemos que nosotros habíamos definido un grupo de marcado con el número 1, para este comando **“dialer-list 1 protocol ip permit”,** indica que dicho grupo de marcado tendrá permitido toda clase de trafico del tipo de protocolo IP, por ello es importante definir tanto el grupo de marcado como el tipo de tráfico que se permitirá o se negará.

Y por último se agrega la línea por donde se configura los parámetros de conexión hacia la línea del MODEM.

```
RUT_DDR1#config t
RUT_DDR1(config)# line aux 0
RUT_DDR1(config-line)# modem InOut
RUT_DDR1(config-line)# transport input all
RUT_DDR1(config-line)# flowcontrol hardware
!
```

Esta configuración que da como sigue, ya que es muy parecido al configurar un MODEM en una PC.

```
line aux 0
 modem InOut
 transport input all
 flowcontrol hardware
```

Como se vió las secciones anteriores, los comandos que albergan en el puerto auxiliar del Ruteador indica el comando **“modem InOut”,** indica la espera cuando el enlace se cae la interfaz serial, por lo que cuando se restablezca este se desconectara automáticamente, y por obvias razones se indica que el puerto auxiliar tendrá tráfico de entrada y salida. Por otro lado el comando **“transport input all”,** el cual define cual protocolo esta permitido para conectarse a este acceso, en este caso como se utilice la palabra “all” significa que cualquier protocolo es permitido. Y por último el comando **“flowcontrol hardware”,** quiere decir que el control del acceso lo tiene el puerto auxiliar cuando se requiere que se desconecte.

Esto indicará que se podrá realizar una redundancia en oficinas centrales y cada nodo de la red será configurado de la misma manera, exceptuando por la dirección IP, tanto de la Interfaz Ethernet como en la Interfaz Serial, y por supuesto dentro del map class se tendrá que verificar que BW se esta configurando. Obviamente el tener que configurar una redundancia es por que es valiosa la información hoy en día y en algunas compañías en el país es más difícil tener accesos sin falla, por lo que se realiza un camino alterno, tal vez un poco más lento, pero que no repercutirá un gran impacto en su negocio.

También se podría decir que es un costo elevado para el cliente con este tipo de redundancia pero, también se tiene que medir la importancia que se tiene en la transferencia de datos y reducir las fallas de circuitos Frame Relay en la red y hacerla mas segura.

VI.12 ESQUEMA FINAL DE LA RED INTERGRADA

En la figura 6.13 se muestra el diagrama integral de toda la red que compone en el acceso de Internet y en la red Frame Relay.

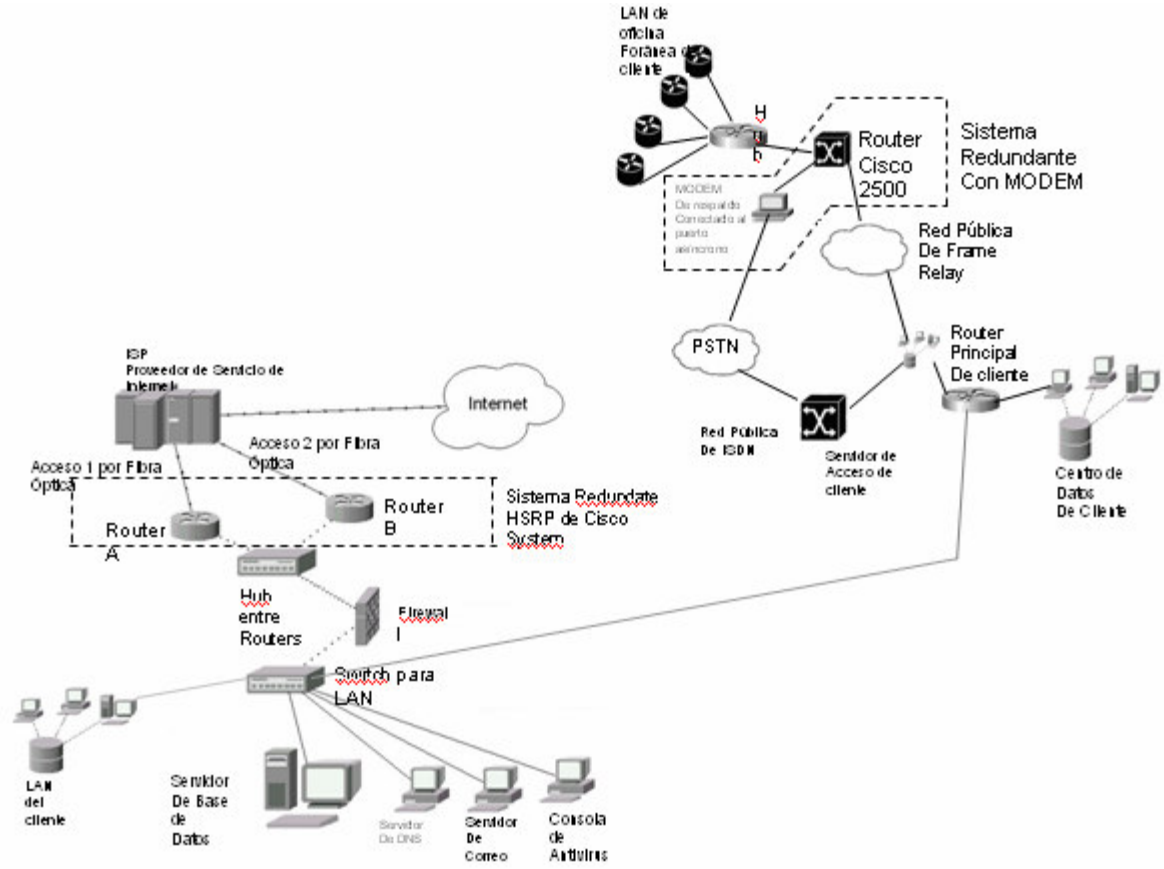


FIGURA 6.13 ESQUEMA INTERGRAL DE SISTEMA REDUNDATES PARA INTERNET Y FRAME RELAY

VI.12.1 EXPLICACION DE LA CONFIGURACION DE REDUNDACIA

Observamos en la figura 6.13; que en el lado de el sistema HSRP para Internet se necesitan de 2 accesos por diferentes backbones, así como dos Ruteador Cisco para que pueda albergar este sistema, dejando un subsistema para que realice el proceso de transferencia de Internet para los usuarios dando un mejor rendimiento en cuanto acceso y procesamiento del Ruteador que se reflejará en el las tareas de los usuarios. Mientras que en otro subsistema de Frame Relay se ve como en la oficinas se tiene una redundancia con DDR para entrar por vía MODEM en caso que se falle el acceso de Frame Relay. Además contribuye que los usuarios no pierdan en buena medida la continuidad de sus procesos en el día de trabajo.

Cabe destacar que el Ruteador del Cliente Principal y el Servidor de Acceso son proporcionado en mucho de las ocasiones por el proveedor de Frame Relay para salvo guardar los parámetros de sus plataforma contra la del usuario, pero las oficinas foráneas o sitios remotos se podrá configurar teniendo estas bases, para que los costos de cómo el cliente puede disminuir en cuanto a servicios y soporte técnico teniendo un mejor rendimiento, previniendo alguna falla en los sitios remotos, así como también al tiempo de

respuesta para su reactivación de circuito, permitirá el traslado hacia la oficina remota ó con la administración remota, sin que se perjudique a las tareas del usuario.

Finalmente, saber que hoy en día la información es muy importante por lo que es necesario salvaguardarla con sistemas de redundancia para estar preparado para cualquier falla de cualquier componente que integre la red, es posible y en muchas de las ocasiones el costo financiero justifica el beneficio de operación.

CONCLUSIONES

Las comunicaciones hoy en día revolucionan con la información requerida por la industria, ya que los servicios que proporcionan cada una de estas industrias a merita el intercambio de información con eficiencia, rapidez y fiabilidad.

Recordando que cada vez el protocolo TCP/IP gana terreno en comparación de otros protocolos define el rumbo del futuro de la telecomunicaciones. Aunque en nuestro país no se cuenta con la alta tecnología al mismo tiempo que los países del primer mundo, aun así se cuenta con tecnología que es vigente y que satisface las necesidades de la industria.

Un ejemplo muy claro es la Tecnología Frame Relay que compañías en México proporcionan este tipo de servicio, dando una gran demanda de usuarios que se conectan a este tipo de redes, a los que nos lleva que los costos de la infraestructura sea alcanzable para industrias medianas y grandes empresas en México. Ya que tecnologías ATM aún en México no se emplean en abundancia ya que se conduce a un alto costo tecnológicamente hablando.

Frame Relay es uno de los protocolos más utilizados en nuestro país, por la alta eficacia de información en múltiples servicios como son Internet, Datos, e incluso Voz, y Videoconferencia, aunque estos últimos dos no fueron parte de la tesis, la infraestructura Frame Relay lo soporta y es la base para esos tipos de información.

En la actualidad Frame Relay ha alcanzado la madurez para proporcionar servicios mas integrados en el país, con la ayuda del protocolo IP que ayuda a la encapsulación de la información y se pueda aprovechar al máximo estas tecnología adaptándola al desarrollo de los servicios que requiere la industria para mejorar su calidad de servicio, como VoIP o VPN, entre otros.

El tomar como referencia al protocolo HDLC en esta tesis es demostrar que un protocolo tan simple como este; es indicado para pequeñas y medianas empresas que solo requieren transmisión de datos que requiere de gran Ancho de Banda, puede utilizar infraestructura más austera y de menor costo.

Teniendo en cuenta que la integridad de datos, son parte esencial de la industria, ya que para la transferencia de cuentas bancarias, intercambio de información de un almacén, o servicios como Internet o como correo electrónico que cada vez son parte de la operación básica de una empresa, y no se puede detener por que tendría un gran impacto en la tarea diaria del usuario, en los ingresos de la industria, en el pago de proveedores, etc., y pueden surgir muchas dudas sobre si se necesita un servicio muy fiable en cuanto a su desempeño y ningún falla en este, por lo creo que los limites de la información, ya no es tan velocidad para grandes transferencia de datos, sino también la fiabilidad de la integridad en cada momento y en línea con los demás departamento, áreas o incluso industrias que se someten día a día en este intercambio, que no debe interrumpirse.

Finalizando el Ruteador, dispositivo que influye de manera importante en la transmisión de datos entre dos oficinas a distancia (redes LAN más sofisticadas), crea el panorama de eficiencia en la información dando seguridad, rapidez, confiabilidad, en la Redes de Área Amplia. Hoy en día una empresa como Cisco es muy fuerte en este ámbito ya que no tan solo ha llegado al limitarse en Ruteadores sino también en otros dispositivos de LAN como switches o como seguridad como Firewalls. Sin embargo el Ruteador es el principio para a dos oficinas separadas geográficamente y dando un mayor rendimiento y mejora en los servicios de redes WAN.

Ya que las industrias de telecomunicaciones se han preocupado por la continuidad de servicio, Cisco nos ha proporcionado hoy en día, sistemas como lo que hemos visto y configurado como es el HSRP y DDR, que cada uno en su campo tanto para integridad del hardware, que en este caso fue el Ruteador por la parte de HSRP, pero la adapte a un sistema de acceso a Internet para el cliente, que como todos sabemos la red Internet esta siendo la herramienta mas importante para la industria y también para nuestra vida diaria. Y sin dejar al un lado, DDR nos ha resuelto la parte de respaldo de una red Frame Relay a través de una simple línea telefónica y un MODEM, conectado al puerto paralelo, lo que implica un sencillo arreglo pero un poderoso respaldo para la industria en cuanto a sus transferencia. Sin duda estos sistemas logran el objetivo de no dejar al cliente sin servicio mientras se restablece y se repara el enlace primario.

BIBLIOGRAFIA

ALTA VELOCIDAD Y CALIDAD DE SERVCIO EN REDES IP
JESUS GARICA TOMAS / JOSE LUIS RAYA CABRERA / VICTOR RODRIGO RAYA
ED. ALFAOMEGA
MEXIC, DF.
OCTUBRE 2002

REDES DE CONMUTACION DE PAQUETES BASADAS EN FRAME RELAY
TESIS INGENIERO EN COMUNICACIONES Y ELECTRONICA
JAVIER VALDEZ MALTOS
MEX. DF 1996
ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA
INSTITUTO POLITECNICO NACIONAL

APRENDIENDO WINDOWS NT SERVER 4
ALLEN WYATT
ED. PRENTICE HALL HISPANOAMERICA, S.A.
MEX. EDO. DE MEXICO
TRADUCCION POR JOSE ALBERTO VELAZQUEZ ARELLANO
1997

CURSO
SOPORTE TECNICO EN COMPUTACION
NIVEL BASICO-HARDWARE
SINTEG EN MEXICO, S.A. DE CV.
ELABORADO POR: GUILLERMO TREJO
REVISION TECNICA: JUAN LOPEZ, RAMON PERALTA, LUCIA RAMIREZ
ENERO 1998

RUTEADORES CISCO
JOE HABRAKEN
TRADUCICION: BEATRIZ PAREDES
EDITORIAL: PRENTICE HALL
MADRID, 2000

DESCUBRE REDES LAN & WAN
FRANK DERFLER
TRADUCIDO: ALEJANDRO RUIZ
EDITORIAL PRENTICE HALL
MADRID, 1998

MANUAL
APREDIENDO WINDOWS NT SERVER 4.0
FEDERICO REINA TORANZO / JUAN ANTONIO RUIZ RIVAS
MEX. DF.

COMUNICACIONES Y REDES DE PROCESAMIENTO DE DATOS.
NESTOR GONZALEZ SAINZ
ED. MCGRAW-HILL
MEX. 1987

REDES DE BANDA ANCHA
JOSE MANUEL CABALLERO
ED. ALFAOMEGA MARCOMBO
MEX. DF.

ACADEMIA DE NETWORKING DE CISCO SYTEMS
GUIA DEL PRIMER AÑO
SEGUNDA EDICION
CISCO SYSTEM INC.
PEARSON EDUCACION S.A. MADRID, ESPAÑA
ED. 2002

CISCO 2500 SERIES RUTEADOR
INSTALLATION AND COFIGURATION GUIDE
CISCO SYSTEM INC.
CALIFORNIA, USA
ED. 1996

“REDES LAN, TOPOLOGÍAS BUS, ESTRELLA Y ÁRBOL”
PACHECO JUÁREZ ONOFRE / PELCASTRE GALVÁN EDUARDO / VARGAS ACEVEDO VICENTE ALBERTO
JIMÉNEZ GONZÁLEZ FRANCISCO JAVIER
POSGRADO EN REDES DE COMPUTADORAS
UNIVERSIDAD TECNOLÓGICA DE MÉXICO
PROF. MC GERARDO VEGA SÁNCHEZ
PERIODO 00-2

REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IP
AUTOR: DOUGLAS E. COMER
EDITORIAL PRENTICE HALL
1996

COMUNICACIONES Y REDES DE COMPUTADORES, QUINTA EDICIÓN.
STALLINGS, WILLIAM:
PRENTICE HALL
1997

TCP/IP
JOHN RAY
PRENTICE HALL
MADRID, 1999
TRADUCIDO POR LUIS DEL PINO GONZÁLEZ / SANTIAGO FRAGUAS

SAMS TEACH YOURSELF TCP/IP IN 24 HOURS
JOE CASAD / BOB WILLSEY
SAMS PUBLISHING
USA, 1998

PAGINA WEB
www.cisco.com