UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

FACULTAD DE INFORMÁTICA

TESINA:

# Fundamentos de HSRP (Hot Standby Router Protocol)

Que para obtener el titulo de:
LICENCIADO EN INFORMÁTICA

PRESENTA:
Rosa Aimé Gómez Gómez

DIRIGIDA POR:
ISC. Pablo Gutiérrez Lara

Santiago de Querétaro, Qro., Diciembre de 2004.

# CARTA DE ACEPTACIÓN

Por este medio, se otorga constancia de aceptación de tesina para obtener el título de Licenciado en Informática, que presenta la pasante **ROSA AIME GÓMEZ GÓMEZ** con el tema denominado "FUNDAMENTOS DE PROTOCOLO HSRP (HOT STANDBY ROUTER PROTOCOL)".

Este trabajo fué desarrollado como una investigación derivada del curso de titulación "ADMINISTRACIÓN DE REDES" , dando cumplimiento a uno de los requisitos contemplados en el artículo 34 del reglamento de titulación vigente, en lo referente a la opción de titulación por realización y aprobación de cursos de actualización.

Se extiende la presente para los fines legales a que haya lugar y para su inclusión en todos los ejemplares impresos de la tesina, a los doce días del mes de enero del 2005.

ATENTAMENTE

**I.S.C. PABLO GUTIÉRREZ LARA**
INSTRUCTOR DEL CURSO

**DEDICATORIA**

*Al gran guía de mis pasos…*

*Dios.*

*A los grandes maestros de mi vida…*

*Mis Padres.*

*A mis mejores amigos y cómplices por siempre…*

*Todos mis hermanos.*

*A mis leales seguidores de andanzas…*

*Mis sobrinos.*

*A los sinceros apoyos en las distintas etapas de mi vida…*

*Mis mejores amigos.*

*A quienes creyeron en mí, pese a los tropiezos…*

*Mis profesores.*

*Dedico el esfuerzo de concluir con este documento uno de los sueños de mi vida;*

*Estudiar una profesión.*

*Rosa Aimé Gómez Gómez.*

## INDICE

## INTRODUCCION.

Día con día la tecnología evoluciona, de una manera tan vertiginosa que lo que ahora es parte de un complejo sistema, el día de mañana se trabaja de forma tal fácil que en ocasiones parece como un juego.

Dentro de este auge el paradigma de la red cambia cada unos pocos años, y las nuevas influencias ponen una mayor atención en la disponibilidad y la rapidez de la red de la empresa. La aceptación global del Web mundial crece, IP hacer el protocolo dominante.

Como es bien sabido en el ámbito de las redes, cuando se trabaja en una red interna dentro de la empresa, los problemas no son mayores y no requiere mayor esfuerzo para la comunicación e intercambio de información.

El punto angustioso de las redes ha sido desde que fue posible la comunicación entre redes distantes, el mantener esa comunicación o restablecerla rápidamente cuando sea interrumpida, y es ahí donde el protocolo HSRP, es decir *Hot Standby Router Protocol* (que es el punto central del presente documento); adquiere importancia.

La posible traducción al español del Protocolo HSRP, pudiera ser Protocolo de Ruteo Seguro Activo; pero como no se ha establecido una traducción propia del protocolo, en el presente documento solo se hace mención de las siglas HSRP.

HSRP es un protocolo de ruteo que busca proporcionar al usuario de la red, una comunicación constante, de tal manera que el pueda trabajar interrumpidamente sin que sufra retardo en su labor por fallos de comunicación.

Lo anterior puesto que este protocolo dicho en pocas palabras, proporciona una configuración tolerante a fallos, puesto que partiendo de la idea de que se tienen al menos dos ruteadores configurados de tal manera que el usuario ve solo uno, los ruteadores se monitorean entre ellos.

Para lo cual uno tiene un papel activo y otro espera, uno dirige el ruteo y otro esta esperando por si se necesita cubrir al otro.

De tal manera que al fallar el ruteador activo en unos pocos segundos el otro se activa, dando pie a que el otro sea reparado, revisado o sustituido y la comunicación de los usuarios sufre solo un retrazo de unos segundos.

Esta es una razón muy importante para estudiar este protocolo, para ver los puntos clave, las mejoras posibles y los aspectos que pueden irse mejorando, pero es indudable que este protocolo proporciona un ruteo más efectivo en el trabajo de comunicación entre redes.

# CAPITULO 1. REDES.

## 1. 1. INTRODUCCIÓN A LAS REDES.

En el siglo pasado la tecnología clave fue la obtención, procesamiento y distribución de la información, y todo ello a partir del uso de computadoras. Todos conocen las grandes ventajas del uso de las computadoras, ya sea para el hogar, o el trabajo ademas de la necesidad de que surgió de tener una cantidad importante de computadoras en operación y de que estas se pudieran comunicar. Las redes en general, consisten en compartir recursos.

Parece sencillo concebir la idea de que las computadoras compartan sus recursos, pero para que todo esto sea de forma transparente al usuario, fueron necesarios grandes progresos en la tecnología, como lo fueron el nacimiento y crecimiento sin precedentes de la industria de las computadoras y el lanzamiento de satélites de comunicación.

Es bien conocido que la industria de la computación es relativamente joven, pero las computadoras han logrado progresos espectaculares en muy poco tiempo. El que un gran número de computadoras separadas pero interconectadas, pudiesen hacer un trabajo conjunto, o bien que fuesen capaces de intercambiar información; es lo que se conoce como redes de computadoras.

La conexión de estas computadoras puede ser por varios medios; ya sea por alambre de cobre, fibra óptica, microondas y satélites de comunicación.

Hay dos elementos importantes del funcionamiento de las computadoras, por tanto son puntos clave dentro del sistema redes de computadoras estos son el *hardware* y el *software*. Cada una con infinidad de cuestiones técnicas, que son muy importantes para el uso, funcionamiento y trabajo de las redes de computadoras. El usuario sólo ve la facilidad del uso de las aplicaciones, pero esta lejos de percibir todo lo que la más sencilla aplicación en red, lleva detrás.

Dentro de se trabajo se hará uso de la palabra de redes con el entendido de que se está haciendo referencia a las redes de computadoras.

## 1.2. USO DE LAS REDES.

Antes de examinar algunos de los aspectos técnicos con algunos detalles, es importante que se entienda porque la gente está interesada en las redes y para qué puede usarlas.

Todos lo referente al uso de las redes se dirige en dos líneas fundamentales, las redes para las compañías y las redes para la gente.

Los objetivos de las redes son muchos y se han convertido en fuertes ventajas, que no sólo dan confianza en su utilización, sino que se vuelven bases firmes sobre las que se sustenta el uso de esta tecnología, abren al panorama de tal forma que no es raro verlas en cualquier lugar. Los objetivos de las redes se resumen brevemente en los siguientes:

- Disponibilidad de la información.
- Alta Confiabilidad.
- Ahorro económico.
- Alta escalabilidad.
- Medio de comunicación.
- Antecedentes de las redes.

## 1.3. HARDWARE DE RED.

Como ya se ve, se denomina red a una serie de *host* autónomos y dispositivos especiales intercomunicados entre sí. Ahora bien, este concepto genérico de red incluye multitud de tipos diferentes de redes y posibles configuraciones de estas, por lo que surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

Dejando a un lado las aplicaciones y los aspectos generales de las redes, pues es necesario tomarse un tiempo para enfocarse a los problemas técnicos que implica su diseño.

Las posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, y puesto no existe una forma generalmente aceptada dentro de la cual quepan todas las redes de computadoras siendo las más comunes y aceptadas tres de ellas., pero dos dimensiones sobresalen como importantes: tecnología de transmisión y la escala.; aunque también se hará mención de la del tipo de transferencia.

### 1.3.1. Clasificación de redes por la tecnología de transmisión.

En términos generales, hay dos tipos de tecnología de transmisión:

- Redes de difusión.
- Redes punto a punto.

#### *1.3.1.1. Redes de difusión.*

Las redes de difusión tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes cortos llamados paquetes, que envía una máquina son recibidos por todas las demás. Un campo dirección dentro del paquete, especifica a quien se dirige. Al recibir un paquete una máquina verifica el campo dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a otra máquina, lo ignora. Es decir el mensaje puede ser escuchado por muchos pero solamente a quien vaya dirigido va a contestar.

Los sistemas de difusión generalmente dan la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Al trasmitir un paquete con este código, cada máquina en la red lo recibe y procesa. Este modo de operación se llama difusión o *broadcasting*. Ciertos sistemas de difusión, ven la transmisión a un subconjunto de máquinas, se conoce como multidifusión. Cada máquina puede suscribirse a cualquier grupo o a todos. Al enviar un paquete a cierto grupo, se entrega a todas las máquinas suscritas a ese grupo.

#### *1.3.1.2. Redes punto a punto.*

Retomando lo descrito en las redes de difusión, por el contrario, las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que pasar antes a una o más máquinas intermedias, siendo necesario en tal caso un trazado de rutas mediante ruteadores. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo desempeñan un papel importante para las redes punto a punto. Como regla general aunque claro hay excepciones, las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

### 1.3.2. Clasificación de redes por escala.

Un criterio alterno para clasificar las redes es su escala, o tamaño y extensión. En la figura 1.1. Se da una clasificación de los sistemas de múltiples procesadores de acuerdo su tamaño físico. En la parte superior están las máquinas de flujo de datos, computadoras con alto grado de paralelismo y muchas unidades funcionales, todas trabajando en el mismo programa. Después vienen las computadoras, sistemas que se comunican enviando mensajes por buses muy cortos y rápidos. Más allá de las computadoras están las verdaderas redes, computadoras que se comunican intercambiar mensajes por cables largos. Estas pueden dividirse en redes locales, metropolitanas y amplias. Finalmente, la conexión de dos o más redes es una interred. La red Internet, de alcance mundial es un ejemplo conocido de interred la distancia es importante como medio de clasificación porque se usan diferentes técnicas a diferentes escalas. En ese documento solamente se retoma lo concerniente a redes verdaderas y su interconexión.

| Distancia entre procesadores. | Procesadores ubicados en él (la) mismo(a). | Ejemplo. |
|---|---|---|
| 0.1 m | Tarjeta de circuitos | Máquina de flujo de datos |
| 1 m | Sistema | Una computadora |
| 10 m | Cuarto | Red de área local |
| 100 m | Edificio | |
| 1 km | Campus | |
| 10 km | Ciudad | Red de área metropolitana |
| 100 km | Pais | Red de área amplia |
| 1000 km | Continente | |
| 10000 km | Planeta | La Internet |

Figura 1.1. Clasificación de procesadores interconectados según su escala.

Partiendo del concepto de red, donde se define un conjunto de equipos conectados entre sí con la finalidad de compartir información y recursos, hay varios tipos de redes. Y estas se pueden clasificar según; la extensión, es decir, de acuerdo con la distribución geográfica, se habla de redes:

- Redes de Área Local o LAN.
- Redes de Área Metropolitanas o MAN.
- Redes de Área Extendida o WAN.

### *1.3.2.1. Redes de área local o LAN.*

Las redes de área local, generalmente son llamadas redes LAN. Son redes de propiedad privada dentro de un solo edificio o campus. Redes LAN, son redes de computadoras cuya extensión es de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos e intercambiar información. Las LAN se distinguen de otro tipo de redes por tres características: el tamaño, su tecnología de transmisión y su topología.

Las LAN generalmente usan la tecnología de transmisión o de *broadcast*, es decir, que a un sólo cable se conectan todas las máquinas. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, operan a velocidades de 10 a 100 Mbps (Mega *bits* por segundo). Las LAN a menudo usan una tecnología que consiste en un cable sencillo, y experimentan muy pocos errores. Las LAN de transmisión pueden tener diversas topologías, la figura 1.2, muestra dos de ellas.

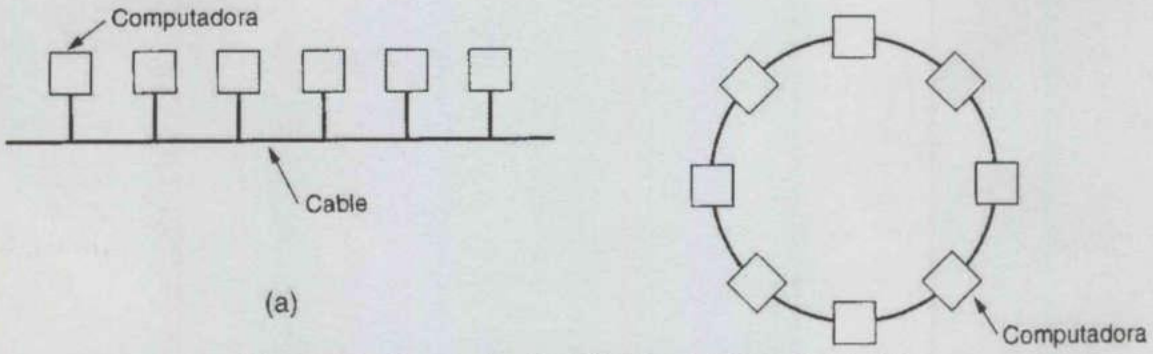



Figura 1.2. Dos redes de difusión. (a) Bus. (b) Anillo.

En una red de bus, es decir, un cable lineal, en cualquier momento una computadora es la máquina maestra y puede trasmitir; se pide a las otras máquinas que no de envíen mensajes. Por ello es necesario un mecanismo arbitraje en los posibles conflictos; cuando dos o más máquinas desean enviar a igual tiempo. El mecanismo puede ser centralizado o distribuido.

El segundo tipo de sistema de difusión es el anillo, donde cada *bit* se propaga por si mismo sin esperar el resto del paquete al cual pertenece. Cada *bit* recorre el anillo entero en el tiempo que toman transmitir unos pocos *bits*, a veces antes de que el paquete completo sea transmitido. Como sistema de difusión se les dan reglas para arremeter el acceso simultáneo del anillo.

Las redes de difusión se pueden dividir también en estáticas y dinámicas dependiendo como se asigna el canal. Una asignación estática típica divide el tiempo en intervalos discretos y ejecutó un algoritmo de asignación estática, permitiendo cada máquina transmitir únicamente cuando llega su turno.

La asignación estática desperdicia la capacidad del canal cuando una máquina no tiene nada que decir durante un segmento asignado, por lo que muchos sistemas intentan asignar el canal dinámicamente, es decir, por la demanda.

Los métodos de asignación dinámica para un canal común son centralizados o descentralizados. En el método de asignación de canal centralizado hay una sola entidad, por ejemplo una unidad de arbitraje del bus, la fase terminal es el siguiente. Esto se puede hacer aceptando peticiones y tomando una decisión de acuerdo con algoritmo interno. En el método de asignación de canal descentralizado no hay una entidad central; cada máquina debe decidir por sí misma si transmite o no. Se puede pensar que esto siempre conduce al caos, pero no es así. Ya que hay muchos algoritmos diseñados para poner orden.

### *1.3.2.2. Redes de área metropolitana o MAN.*

Una Red de Área Metropolitana o MAN. Es básicamente una versión más grande de una LAN, y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas que se encuentren cerca o bien en una ciudad y podría ser privada o pública. Redes MAN, son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en una misma área metropolitana, por lo que, su tamaño máximo comprende un área de mas o menos 10 kilómetros.

Una MAN puede manejar datos y voz, incluso podría estar relacionada con la red de televisión por cable local. Una MAN solo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una o varías líneas de salida; al no tener que conmutar se simplifica el diseño.

La razón principal para distinguir las redes MAN es que han adoptado e implementado un estándar para ellas, este es el Bus Dual de Cola Distribuida o DQDB. El DQDB consiste en dos buses o cables unidireccionales, a los cuales están conectadas todas las computadoras.

Un aspecto clave de las MAN es que hay un medio de difusión al cual se conectan todas las computadoras; tal como se muestra en la figura 1.3, donde cada bus tiene una cabeza terminal o *head-end*, un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior. El tráfico hacia la izquierda usa el bus inferior.


Figura 1.3. Arquitectura de red de área metropolitana DQDB.

### *1.3.2.3. Redes de área amplia o WAN.*

Una red de área amplia, o WAN, se extiende sobre un área geográfica extensa, contiene una colección de máquinas dedicadas a ejecutar programas de usuario, o de aplicación, estas máquinas son llamadas *hosts*. Las *hosts* están conectadas por una subred. El trabajo de la subred es conducir mensajes de una *host* a otra. La separación entre los aspectos de comunicación de la red o subred y los aspectos de aplicación o de las *hosts*, simplifican enormemente el diseño total de la red.

Las redes WAN, son una colección de *host* o de redes LAN conectadas por una subred. La subred está formada por una serie de líneas de transmisión interconectadas por medio de ruteadores, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o *host* adecuado, enviando éstos paquetes de un ruteador a otro. el tamaño de las redes LAN va entre 100 y 1000 kilómetros.

En muchas Redes de Área Amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión también llamadas circuitos, canales o troncales mueven *bits* de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan una o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de

conmutación debe elegir una línea de salida para enviarlos desgraciadamente no hay una terminología estándar para escoger estas computadoras; se denominan nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos, entre otras cosas. Como término general para las computadoras de conmutación, se hace uso de la palabra ruteador. En el modelo de la figura 1.4, cada *host* habitualmente está conectada a una LAN en la cual está presente un ruteador, la colección de líneas de comunicación y ruteadores, pero no las *hosts;* forman la subred.

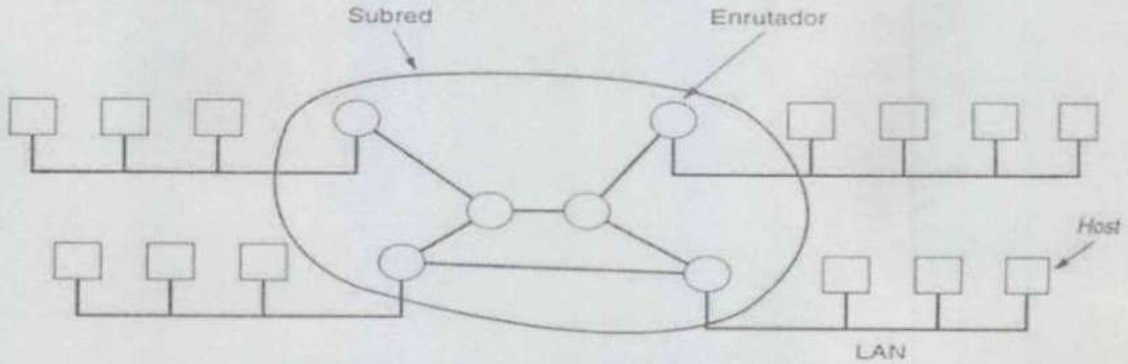



Figura 1.4. Relación entre las *hosts* y la subred.

Es importante retomar algunos aspectos del término subred, que de inicio sólo significo la serie de ruteadores y líneas de comunicación que movían los paquetes de la *host* origen a la *host* destino, sin embargo después surgió otro significado en relación con la identificación de direcciones en la red. Por lo que el término puede ser usado en ambos sentidos.

En casi todas las WAN, la red tiene numerosos cables o líneas telefónicas, cada una conectada a un par de ruteadores. Si dos ruteadores que no comparten un cable desean comunicarse, deberán hacerlo de forma indirecta, por medio de otros ruteadores. Cuando se envía un paquete de un ruteador a otro a través de uno más ruteadores intermedios, el paquete que se recibe completo en cada ruteador intermedio, se almacena hasta que la línea de salida requerida está libre y entonces se reenvía.

Una subred basada en este principio se llama, de punto a punto, de almacenar y reenviar, o de paquete conmutado. Casi todas las redes de área amplia excepto las que usan satélites, tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse celdas.

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión de ruteador. La figura 1.5, muestra algunas posibles topologías. Las redes locales que fueron diseñadas como tales prácticamente tienen una topología simétrica. En contraste, las Redes de Área Amplia tienen topologías irregulares.

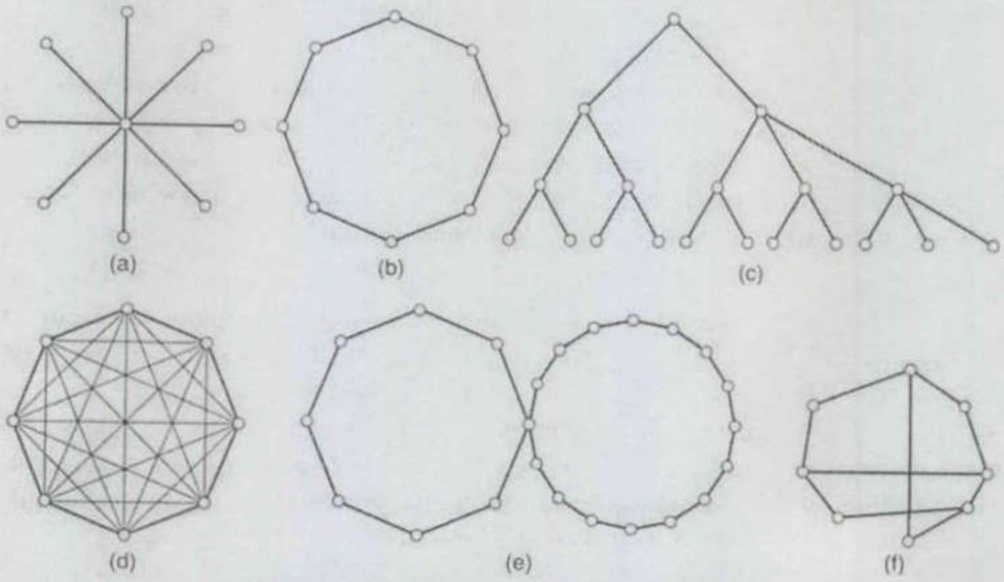



Figura 1.5. Posibles topologías para una subred punto a punto.
(a)Estrella. (b)Anillo. (c)Árbol. (d)Completa. (e)Intersección de anillos. (f) Irregular.

Otra posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada ruteador tiene una antena por medio de la cual puede enviar y recibir. Todos los ruteadores pueden oír las salidas enviadas desde el satélite y en algunos casos pueden también oír la transmisión ascendente de los otros ruteadores hacia el satélite. Por su naturaleza, en redes de satélite son de difusión

### *1.3.2.4. Redes inalámbricas.*

Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo, lo que las diferencia de las redes anteriores. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

Muchos de los usuarios de computadoras portátiles, tiene maquinas de escritorio conectadas a LAN y WAN en la oficina y quieren estar conectados a su base de operaciones aún cuando estén de viaje u en casa. Puesto que desde una conexión por cable es imposible mantener la conexión en autos y aviones, existe mucho interés en las redes inalámbricas.

Las redes inalámbricas tienen muchos usos, son importantes y de gran valor para aquellas personas que necesitan mantenerse en contacto permanente, sin importar el lugar físico donde se encuentren, sin que la distancia sea un obstáculo para la comunicación. Hay para quienes es común tener una oficina portátil. También son importantes para los militares. Las redes inalámbricas y las computadoras portátiles con frecuencia están relacionadas, pero no son iguales, como lo muestra la figura 1.6, las computadoras portátiles en ocasiones se conectan a las redes de cable, podría decirse redes alambradas.

| Inalámbrica | Móvil | Aplicaciones |
|---|---|---|
| No | No | Estaciones de trabajo estacionarias en oficinas |
| No | Si | Uso de una portátil en un hotel, mantenimiento de trenes |
| Si | No | LAN en edificios viejos y sin alambrado |
| Si | Si | Oficina portátil; PDA para inventarios. |

Figura 1.6. Combinación de redes inalámbricas y computación móvil.

Algunas redes inalámbricas nos son portátiles. Aunque estas LAN son fáciles de instalar todavía tienen desventajas, su capacidad es menor, es decir, que es mucho más lento que las LAN de cable, las tasas de error son mucho más altas y las transmisiones desde diferentes computadoras pueden interferirse.

Las redes inalámbricas tienen muchas formas. Un ejemplo es usando el teléfono celular con un módem análogo tradicional. Es posible tener diferentes combinaciones de redes alámbricas e inalámbricas.

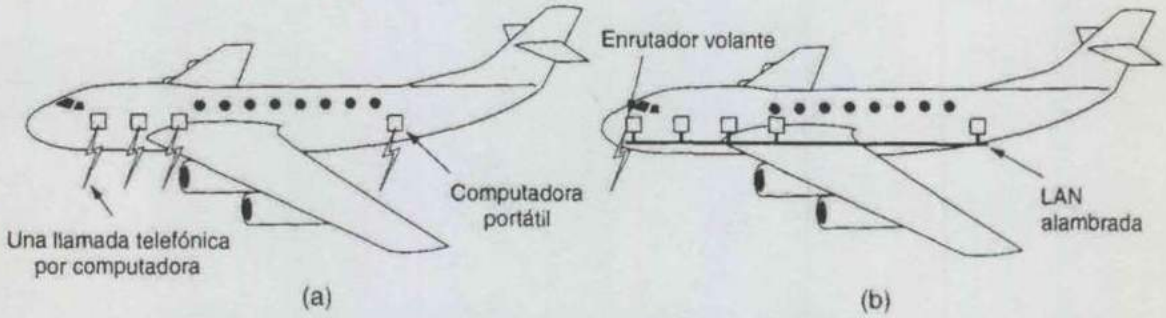



Figura 1.7. (a) Computadoras individuales móviles (b) Una LAN volante.

En la figura1.7 (a), se muestra un avión con varias personas usando módems y teléfonos fijos al asiento para llamar la oficina, donde cada llamada es independiente. Pero una opción mucho más eficiente es la LAN volante de la figura 1.7 (b), donde cada lugar en el avión viene equipado con una conexión a Internet a la cual los pasajeros pueden conectar

sus computadoras. Un ruteador simple en el avión mantiene un enlace de radio con algún ruteador de la tierra, cambiando de ruteador según avanza el vuelo. Esta configuración corresponde a una LAN tradicional, excepto que su conexión al mundo externo es un enlace de radio en lugar de una línea de cable.

### *1.3.2.5. Interredes.*

Existen muchas redes en el mundo, a veces con diferente *hardware* y *software*. Frecuentemente la gente conectada a una red quiere comunicarse con gente conectada a una red distinta. Lo que requiere conectar redes diferentes y frecuentemente incompatibles en puentes para hacer la conexión y realzar la traducción necesaria, ambas en términos de *hardware* y *software* una colección de redes interconectadas se llaman interred, una forma común de interred es una colección de LAN conectadas por una WAN.

Si se reemplaza la etiqueta subred en la figura 1.4, por WAN, nada más tendría que cambiar. La única diferencia real entre una subred y una WAN es si están o no presentes en las *hosts*. Si el sistema dentro de la circunferencia contiene solo ruteadores, es una subred, si tiene tanto ruteadores como *hosts* por sus propios usuarios, es una WAN.

Con frecuencia se confunden las subredes, redes e interredes. La subred tiene sentido en el contexto de una WAN, donde se refiere a las flechas de ruteadores y líneas de comunicación propiedad del operador de la red; como analogía el sistema telefónico consiste en centrales telefónicas conectadas unas a otras por líneas de velocidad, a casas y negocios por líneas de baja velocidad. Estas líneas y equipo propiedad de la compañía y administrado por ella, forman la subred del sistema telefónico, los teléfonos por sí mismos no son parte de la subred. La combinación de una subred y sus nodos forma una red. En el caso de una LAN, el cableado y los nodos forman la red, no hay subred.

La red interred, es una red de redes, vinculadas mediante ruteadores o *gateways*. Un *gateway* o pasarela es un computador especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ser desde 10000 kilómetros en adelante, y su ejemplo más claro es Internet (la red de redes mundial) pero en gran escala. Se forma una interred cuando se conectan distintas redes entre sí. Desde un particular punto de vista al conectar una LAN y una WAN o al conectar dos LAN se forma una interred.

### 1.3.3. Clasificación de las redes según la tecnología de transmisión.

Las redes también pueden ser clasificadas según el tipo de transferencia de datos que soportan:

- *Redes de transmisión simple.* Son aquellas redes en las que los datos sólo pueden viajar en un sentido.
- *Redes Half-Duplex.* Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.
- *Redes Full-Duplex.* Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

### 1.3.4. Topologías de red.

La topología o forma lógica de una red puede ser de distintas maneras, a continuación se hace mención de las topologías de red:

- Anillo.
- Estrella.
- Bus.
- Árbol.
- Trama.
- Combinadas.
    - Anillo en estrella.
    - Bus en estrella.
    - Estrella jerárquica.

#### *1.3.4.1. Anillo.*

Es una de las tres principales topologías de red. Las estaciones están unidas una con otra formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo.

Una variación del anillo que se utiliza principalmente en redes de fibra como FDDI es el doble anillo.

### *1.3.4.2. Estrella.*

Es otra de las tres principales topologías. La red se une en un único punto, normalmente con control centralizado, como un concentrador de cableado.

### *1.3.4.3. Bus.*

Es la tercera de las topologías principales. Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo.

### *1.3.4.4. Árbol.*

Esta estructura de red se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

### *1.3.4.5. Trama.*

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de las LAN. Los nodos están conectados cada uno con todos los demás.

### *1.3.4.6. Combinadas.*

Cuando se estudia la red desde el punto de vista puramente físico aparecen las topologías combinadas.

- *Anillo en estrella.* Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.
- *Bus en estrella.* El fin es igual a la topología anterior. En este caso la red es un bus que se cablea físicamente como una estrella por medio de concentradores.
- *Estrella jerárquica.* Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

### 1.3.5. Equipos de red.

En cuanto al campo de *hardware*, conforme se hacen los diseños de una red es más interesante, y se desarrollan nuevos equipos para su mayor eficiencia, e irán surgiendo equipos que faciliten la implantación y administración de las redes, pero esencialmente los equipos de red partirán de las funciones de los principales equipos de red, que se listan a continuación:

- Tarjeta de red o NIC/MAU.
- Concentradores.
- Repetidores.
- Puentes.
- Ruteadores.
- *Gateways*.
- Servidores de terminales e impresoras.

#### *1.3.5.1. Tarjeta de red o NIC/MAU.*

Tarjeta de interfaz de red o Unidad de Acceso al Medio. Es el dispositivo que conecta la estación (computadora u otro equipo de red) con el medio físico. Se suele hablar de tarjetas en el caso de las computadoras, ya que la presentación suele ser como una tarjeta de ampliación de los mismos, diferente de la placa de CPU, aunque cada vez son más los equipos que disponen de interfaz de red, principalmente *Ethernet*, incorporado.
A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10base5) o porque el medio sea distinto del que utiliza la tarjeta.

#### *1.3.5.2. Concentradores.*

Son equipos que permiten estructurar el cableado de las redes. Hay una gran de la variedad de tipos y características de estos equipos. En inicio eran solo de cableado, pero cada vez disponen de mayores capacidades, como: aislamiento de tramos de red, conmutación de las salidas para aumentar la capacidad de la red, gestión remota, etc. La tendencia es incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.

### *1.3.5.3. Repetidores.*

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

### *1.3.5.4. Puentes.*

También conocidos como *bridges*. Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio.

Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los puentes producen las señales, con lo cual no se transmite ruido a través de ellos.

### *1.3.5.5. Ruteadores.*

Son equipos de interconexión de redes que actúan al nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Funcionan más lento que los *bridges* pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que usa un protocolo distinto.

### *1.3.5.6. Gateways.*

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

### *1.3.5.7. Servidores de terminales e impresoras.*

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos

compartidos. Así un terminal conectado a uno de estos dispositivos puede establecer sesiones contra varios computadora es multiusuario disponibles en la red. Igualmente, cualquier sistema de la red puede imprimir en las impresoras conectadas a un servidor.

### 1.3.6. Equipos de red.

Para poner a disposición de los usuarios los servicios anteriormente comentados, se necesita lógicamente montar el *hardware* adecuado. Antes se describieron componentes tales como tarjetas de red, concentradores, repetidores, puentes, ruteadores, etc. Ahora se refiere a los tipos de computadoras existentes en una red.

#### *1.3.6.1. Servidores.*

Un servidor es una computadora que ejecuta un sistema operativo de red y ofrece servicios de red a las estaciones de trabajo. El servidor debe ser un sistema fiable con un procesador potente, con discos de alta capacidad y con gran cantidad de memoria RAM. Una configuración que se puede encontrar, en el caso de LAN es un equipo con procesador Pentium, disco duro SCSI de más de 4Gb, con 64Mb de RAM y sistema operativo Windows NT.

Es posible montar una red sin servidor, es decir, donde cada equipo se comporta como servidor y cliente al mismo tiempo, por ejemplo a través de Windows 3.11 para trabajo en grupo o Windows 95. En este caso, el sistema operativo se debe instalar en cada estación de trabajo y los recursos se distribuyen entre las estaciones. No obstante, en este tipo de configuración, aspectos como la seguridad y la administración de usuarios se ven seriamente restringidos.

#### *1.3.6.2. Estaciones de trabajo.*

Cuando una computadora se conecta a una red el primero se convierte en un nodo o estación de trabajo de la última. Las estaciones de trabajo pueden ser computadora es personales con el DOS, sistemas Macintosh de Apple, sistemas Windows o estaciones de trabajo sin disco.

## 1.4. SOFTWARE DE RED.

No esta de más decir que las primeras redes de computadoras se diseñaron con el *hardware* como preocupación principal y el *software* como algo después, sin embargo ahora ya no es así y el *software* de la red es altamente estructurado. Es importante ver la técnica de estructuración de *software*.

### 1.4.1. Jerarquía de protocolos.

Para reducir la complejidad de su diseño, muchas redes están organizadas como una serie de capas o niveles, cada una construida sobre la inferior. El numero de capas y el nombre, el contenido y la función son diferentes de red a red. El propósito de cada capa es ofrecer ciertos servicios a las capas superiores de modo que no tengan que ocuparse del detalle de la implementación real de los servicios.

La capa n de una computadora lleva a cabo una conversación con la capa n de otra. Las reglas y convenciones que se siguen en esta conversación se conocen colectivamente como protocolo de la capa n.

Un protocolo es un acuerdo entre las partes que se comunican sobre como va a proceder la comunicación. Si se viola un protocolo, la comunicación se vuelve difícil si no es que imposible.

En la figura 1.8, se ilustra una red de cinco capas. Las entidades que comprenden las capas correspondientes en las diferentes máquinas se dominan pares. Es decir son los pares los que se comunican usando el protocolo.

Los datos no se transfieren directamente de la capa n de una máquina a la capa n de la otra. Lo que ocurre es que cada capa pasa la información de control, a la capa que esta inmediatamente debajo de ella, hasta llegar a la capa más baja. Bajó a la capa uno está el medio físico a través del cual ocurre la comunicación real. En la figura 1.8, se muestran líneas planteadas la comunicación virtual, líneas continuas la comunicación física.

Entre cada par de capas adyacentes hay una interfaz. La interfaz define cuales operaciones y servicios ofrece la capa inferior a la superior.

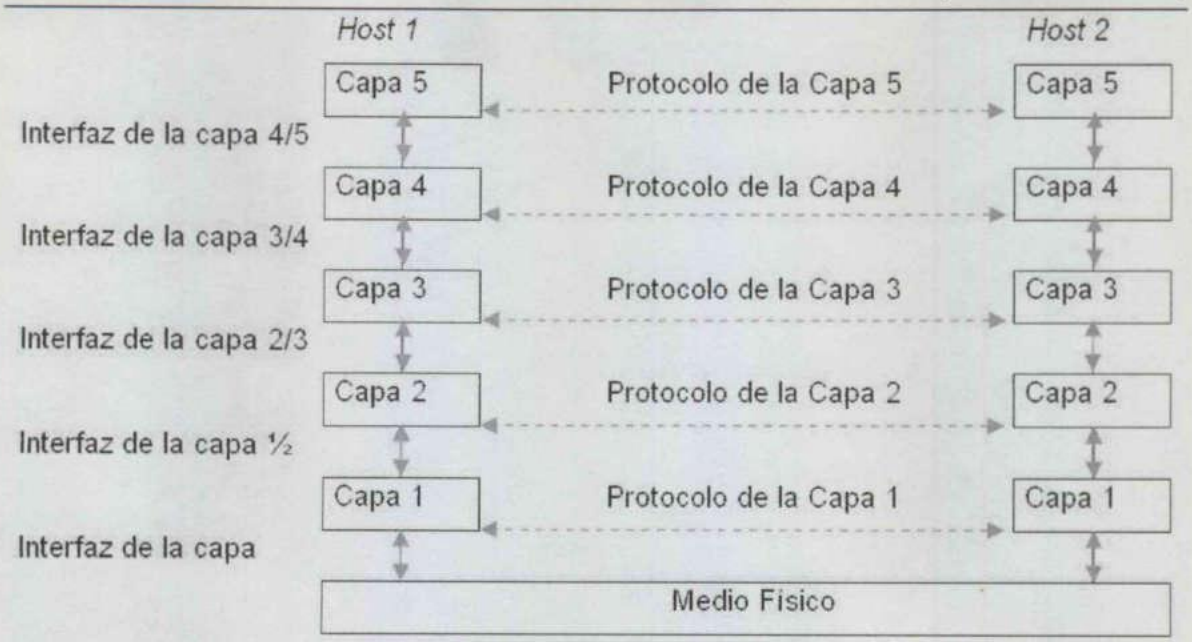



Figura 1.8. Capas, protocolos e interfaces.

El conjunto de capas y protocolos recibe el nombre de arquitectura de red. Una arquitectura debe contener información suficiente para que un implementador pueda escribir el programa y construir el *hardware* para cada capa de manera que cada una obedezca en forma correcta el protocolo apropiado.

No son parte de la arquitectura; los detalles de implementación ni la especificación de interfaces porque se encuentran ocultas dentro de las máquinas. No es necesario que las interfaces en todas las máquinas de una red sean iguales, siempre que cada máquina puedo usar correctamente todos los protocolos. La lista de protocolos empleados por cierto sistema, con un protocolo por capa, se llama pila de protocolos.

Para suministrar la comunicación a la capa superior de la red de cinco capas de la figura 1.9, se produce un mensaje M por un proceso de aplicación que se ejecuta en la capa 5, y se entrega a la capa 4 para su transmisión. La capa 4 coloca un encabezado al principio del mensaje para identificarlo y pasa el resultado a la capa 3. El encabezado incluye información de control, como nombres de secuencia, para que la capa 4 en la máquina de destino pueda entregar los mensajes en el orden correcto si las capas inferiores no mantienen la secuencia. En algunas capas, los encabezados contienen también tamaños, horas y otros campos de control.

En muchas redes no hay límite al tamaño de los mensajes que se transmiten en el protocolo de la capa 4, pero casi siempre existe un límite impuesto por el protocolo de la capa 3, en consecuencia, la capa 3 debe dividir los mensajes que le llegan en unidades más pequeñas, paquetes, anexan un encabezado de la capa 3. Cada paquete, como se puede ver en la figura 1.9, M se divide en dos partes, M1 y M2.

La capa 3 decide cuál de las líneas que salen usar y pasa los paquetes a la capa 2. La capa 2 no solamente añade un encabezado a cada pieza, sino también un apéndice, y entrega la unidad resultante de la capa 1 para su transmisión física. En la máquina receptora el mensaje se mueve hacia arriba, de capa en capa, perdiendo los encabezados conforme avanza. Ninguno de los encabezados para capas inferiores a la n pasa hasta la capa n.

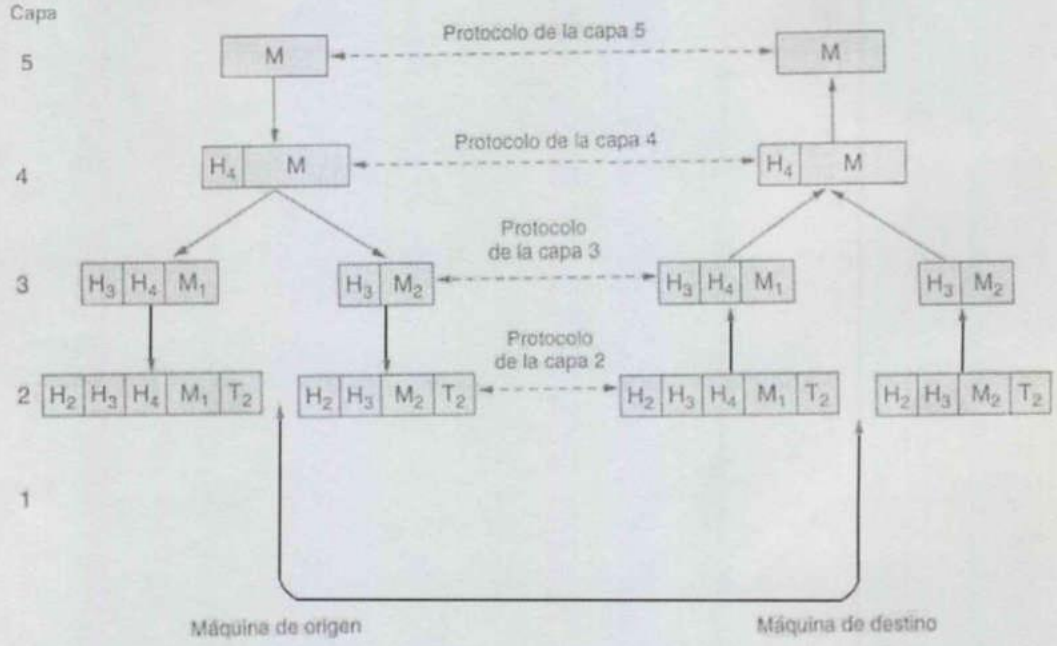



Figura 1.9 Ejemplo del flujo de información que apoya la comunicación virtual en la capa 5.

En la figura 1.9, es importante recordar la relación entre la comunicación virtual y la real y la diferencia entre protocolos e interfaces. Los procesos pares de las capa x piensan que su comunicación es horizontal empleando el protocolo de la capa x, aunque realmente estos procesos se comunican a capas inferiores a través de la interfaz x-1/x+1 no con el otro lado.

La abstracción de los procesos pares es básica para todo diseño de red. Al usarla, la compleja tarea de diseñar la red se puede dividir, en varios problemas de diseño más manejables por ser más pequeños, porque se hace un diseño de capas individuales.

### 1.4.2. Servicios.

La función de capa es proporcionar servicios a la capa que esté encima de ella. Los elementos activos de cada capa generalmente se llaman entidades. Una entidad puede ser de *software* como un proceso, o de *hardware* como un circuito integrado inteligente de entrada/salida. Las entidades de la misma capa en máquinas diferentes se llaman entidades pares. Las entidades de la capa n implementar un servicio que usa la capa n+1 en este caso la capa n se llama proveedor de servicios y la capa n+1 es el usuario del servicio. La capa n puede usar los servicios de la capa n-1 con el fin de proveer su propio servicio; puede proveer varias clases de servicio.

#### *1.4.2.1. Tipos de servicios.*

Las capas pueden ofrecer dos tipos diferentes de servicio las capas que se encuentra sobre ellas, los tipos de servicios son:

- *Servicios orientados a la conexión.* Para usar un servicio de red, el usuario del servicio establece primero una conexión, la usa y después la libera, toma su modeló del sistema telefónico.
- *Servicios sin conexión.* Cada mensaje lleva la dirección completa de destino y se encamina a través del sistema de forma independiente de todos los demás, toma su modelo del sistema postal.

Algunos servicios son confiables porque nunca pierden datos. Un servicio confiable usualmente se implementa haciendo que el receptor acuse el recibo de cada mensaje, de modo que el emisor este seguro de que llegó. El proceso de acuse de recibo introduce una sobrecarga y retardos que con frecuencia valen la pena pero que algunas veces son intolerables.

Los servicios confiables orientados a la conexión tienen dos variantes menores: secuencias de mensajes y corrientes de base. En la primera, se mantienen límites del mensaje, es decir puede haber muchos mensajes pequeños para construir uno solo, y en la segunda, la conexión es solo una corriente de *bytes* sin fronteras entre mensajes.

Una aplicación donde son inoperables los retrasos, es en transmisión de videos y voz. En este caso es preferible recibir la señal con un poco de interferencia en menor tiempo que recibir una frase o movimiento por partes. No todas las aplicaciones requieren conexiones. Es decir, no es esencial que haya una entrega al 100% confiable, más aún si cuesta más.

El servicio sin conexión no confiable es decir sin acuse de recibo, recibe con frecuencia el nombre de servicio de datagramas, en analogía al servicio de telegramas. Hay situaciones en que no se requiere una conexión para enviar un mensaje corto pero es esencial la confiabilidad. Aquí se puede proporcionar el servicio de datagrama con acuse.

En servicio de petición y respuesta, el origen transmite un datagrama sencillo que contiene una petición; la respuesta contiene la contestación. Petición/respuesta se usa mucho para instrumentar la comunicación en el modelo cliente - servidor; el cliente emite una petición y el servidor le responde. La figura 1.10, resume los tipos de servicio mencionados.

| | Servicio | Ejemplo |
|---|---|---|
| Orientado a la conexión | Flujo del mensaje confiable. | Secuencia de páginas |
| | Flujo de *bytes* confiable | Ingreso remoto |
| | Conexión o confiable | Voz digitalizada |
| Sin conexión | Data drama no confiable | Correo electrónico chatarra |
| | Drama con acuse de recibo | Correo registrado |
| | Petición/respuesta | Consulta de base de datos |

Figura 1.10. Seis tipos diferentes de servicio.

### 1.4.3. Primitivas de servicio.

Un servicio se especifica de manera formal con un conjunto de operaciones o primitivas disponibles para que un usuario acceda al servicio. Estas primitivas ordenan al servicio que ejecute una acción o que informe de una acción que haya tomado una entidad par. Un modo de clasificar las primitivas de servicio es partirlas en clases, la figura 1.11, lo muestra.

| Primitiva | Significado |
|---|---|
| *Petición.* | Un usuario quiere que el servicio haga un trabajo. |
| *Indicación.* | Se le informa a un usuario acerca del suceso. |
| *Respuesta.* | Un usuario quiere responder a un suceso. |
| *Confirmación.* | Ha llegado la respuesta a la petición anterior. |

Figura 1.11. Cuatro clases de primitivas de servicio.

Las primitivas pueden tener parámetros, y la mayor parte de ellas los tiene. Los parámetros de una petición de conexión pueden especificar la máquina a la que se va a conectar, el tipo de servicio deseado y el tamaño máximo de mensaje. Si la entidad llamada no está de acuerdo con el máximo propuesto, puede presentar una contrapropuesta en su primitiva de respuesta, que se pone a disposición del origen de la llamada en la confirmación. Los detalles de esta negociación son parte del protocolo.

Los servicios pueden ser confirmados o no confirmados en un ser confirmado, existe una petición, una indicación, una respuesta y una confirmación. En un servicio no confirmado únicamente hay una petición y una indicación. El servicio con conexión siempre es un servicio confirmado porque el par remoto debe estar de acuerdo con establecer una conexión. La transferencia de datos pues ser confirmada o no confirmada, dependiendo de si el emisor necesita acuse de recibo no. En la red se usan ambas clases de servicio.

### 1.4.4. La relación entre servicio y protocolo.

Los conceptos servicio y protocolo son distintos, aunque se confunden muy frecuentemente. Un servicio es un conjunto de operaciones o primitivas que ofrece una capa a la que está por encima de ella. Este define cuáles operaciones está preparada la capa para ejecutar en beneficio de sus usuarios. El servicio se refiere a la interfaz entre dos capas, donde la capa inferior provee el servicio y la capa superior hace uso de él.

Un protocolo es un conjunto de reglas que gobiernan el formato y el significado de los marcos, paquetes o mensajes que se intercambian entre las entidades pares dentro de una capa. Las entidades usan protocolos con el fin de instrumentar sus de servicios; las entidades son libres de cambiar sus protocolos, siempre que no cambien el servicio visible a sus usuarios. Es decir, el servicio y el protocolo están separados.

Es bueno hacer una analogía con lenguajes de programación. Un servicio es como un tipo de datos abstracto o un objeto en un lenguaje de programación orientada a objetos. El servicio define las operaciones que se pueden ejecutar con un objeto pero no especifica como se implementan éstas. El protocolo será la implementación del servicio y como tal no es visible al usuario.

## 1.5. MODELOS DE REFERENCIA.

Antes de analizar la abstracción de las redes basadas en capas, pero se necesita ver algunos ejemplos. Dentro de esto, dos arquitecturas de red importantes. Estas dos arquitecturas de red dominantes son: el modelo de referencia OSI y el modelo de referencia TCP/IP. Las pilas de protocolos se basan ya sea en el modelo OSI o en el TCP/IP.

El primero, basada en el trabajo realizado por la Organización Internacional para la Estandarización o ISO, conocida como Modelo de Referencia de Interconexión de Sistemas Abiertos de ISO, denominada frecuentemente modelo OSI.

El segundo modelo proviene investigaciones realizadas respecto al conjunto de protocolos de TCP/IP. Con un poco de esfuerzo, el modelo ISO puede ampliarse y describir el esquema de estratificación por capas del TCP/IP, pero son suficientemente distintos para distinguirlos como dos diferentes.

### 1.5.1. Modelo de referencia OSI.

Como bien se sabe dentro de cada capa del modelo OSI, se encuentran abstraídas operaciones específicas para la comunicación, dentro de este panorama es importante mencionar que cada capa cumple con una función importante.

### 1.5.2. Capas del modelo OSI.

El modelo OSI trabaja con 7 capas, cada una con una función específica y un nivel de abstracción diferente. La forma en que las capas se comunican se ilustra en la figura 1.12.

Estas capas son:

1) Capa física
2) Capa de enlace de datos
3) Capa de red
4) Capa de transporte
5) Capa de sesión
6) Capa de presentación
7) Capa de aplicación

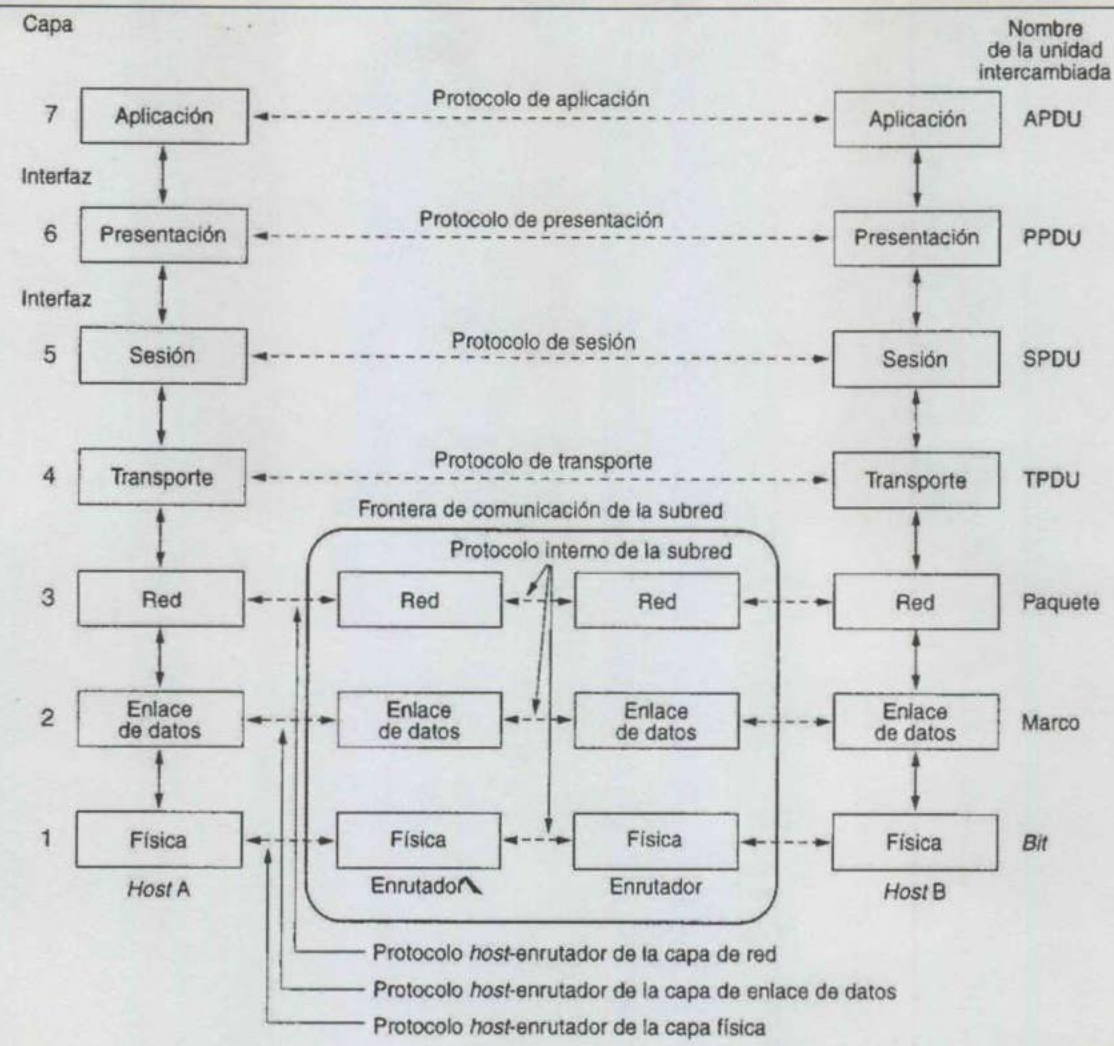



Figura 1.12. Modelo de referencia OSI.

### *1.5.2.1. Capa física.*

La capa física tiene que ver con la transmisión de *bits* por un canal de comunicación. Las consideraciones de diseño tienen que ver con la acción de asegurarse de que cuando un lado envíe un *bit* 1, se recibe en el otro lado como *bit* 1, no como *bit* 0.

La capa física es la base de todas las redes. Impone los límites fundamentales a todos los canales, y esto determina su ancho de banda. Los medios de transmisión pueden ser guiados o no guiados. Los principales medios guiados son el par trenzado, el cable coaxial y la fibra óptica. Los medios no guiados incluyen la radio, las microondas, el infrarrojo y los láseres a través del aire.

### *1.5.2.2. Capa de enlace de datos.*

La tarea principal de la capa de enlace de datos es tomar un medio de transmisión en bruto y trasformarlo en una línea que parezca libre de errores de transmisión no detectados a la capa de red. Corresponde a esta capa de enlace de datos crear y reconocer los límites de los marcos. Una ráfaga de ruido en la línea puede destruir por completo un marco, en cuyo cayo se puede retransmitir el marco, pero la retransmisión ocasiona posibilidades de duplicación. Corresponde a esta capa resolver el problema provocado por los marcos dañados, perdidos y duplicados. Otra consideración es evitar que un transmisor veloz sature a un receptor lento; se emplea un mecanismo que regula el tráfico para que el transmisor sepa cuanto espacio de almacenamiento temporal tiene el receptor en ese momento.

### *1.5.2.3. Capa de red.*

La capa de red se ocupa de controlar el funcionamiento de la subred. Una consideración clave de diseño es determinar cómo se encaminan los paquetes de la fuente a su destino. Si en la subred se encuentran presentes demasiados paquetes a la vez, se estorbarán mutuamente, formando cuellos de botella. El control de tal congestión pertenece también a la capa de red.

### *1.5.2.4. Capa de transporte.*

La función básica de la capa de transporte es aceptar datos de la capa de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de la red y asegurar que todos los pedazos lleguen correctamente al otro extremo. Esta capa se encarga de que si la información fluye lenta por una conexión, puede enviarla por varias conexiones y así aumentar el flujo de la información. Es importante mencionar que la maquina transmisora no tiene por que ser similar con la maquina receptora, puede incluso ser completamente diferentes entre sí, la maquina transmisora es similar en cuanto a sus protocolos con su vecina, esta con su vecina, y así sucesivamente, hasta que al final la que recibe la información es completamente diferente a la que lo envió, por eso se le conoce como Extremo a Extremo.

### *1.5.2.5. Capa de sesión.*

La capa de sesión permite a los usuarios de máquinas establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Es el permiso para acceder a un determinado servicio.

### *1.5.2.6. Capa de presentación.*

La capa de presentación realiza ciertas funciones que se piden con suficiente frecuencia para justificar la búsqueda de una solución general, en lugar de dejar que cada usuario resuelva los problemas. Además se ocupa de la sintaxis y la semántica de la información que se trasmite. Esta capa trabaja la forma en que percibe la información el usuario.

### *1.5.2.7. Capa de aplicación.*

La capa de aplicación contiene varios protocolos que se necesitan con frecuencia. Existen cientos de tipos de terminales incompatibles en el mundo. Una forma de resolver este problema es definir una terminal virtual de red abstracta que los editores y otros programas puedan manejar.

## 1.5.3. Información adicional sobre el modelo de referencia OSI.

Por otra parte el modelo de referencia OSI, se comunica de manera vertical entre las capas, es decir de la capa de Aplicación a la de Presentación, de la de Presentación a la de Sesión, y así sucesivamente. Cuando llega a la capa Física es cuando ya transmite de forma Física la información, hacia la otra capa Física, que se comunica de forma vertical a la de Enlace de Datos, esta a la de Red, y así hasta la de Aplicación.

Parece muy simple, pero ahí no termina todo, aunque las capas del modelo OSI se comunican de forma Horizontal están diseñadas para comunicarse de manera vertical.

Es decir cuando una capa de la maquina emisora por ejemplo la de Transporte (acepta los datos de la de sesión, para dividirlos en unidades más pequeñas si es necesario, pasarlos a la

de red y asegurar que todos los pedazos lleguen correctamente al otro extremo, etc.) además agregan instrucciones referentes a la codificación de la información en esta capa, las cuales van dirigidas a la capa de Transporte de la maquina receptora, con la finalidad de que esta capa pueda decodificar la información y hacer su trabajo correctamente.

Parece muy simple, pero ahí no termina todo, aunque las capas del modelo OSI se comunican de forma Horizontal están diseñadas para comunicarse de manera vertical. La forma en que las capas se comunican se ilustra en la figura 1.13.

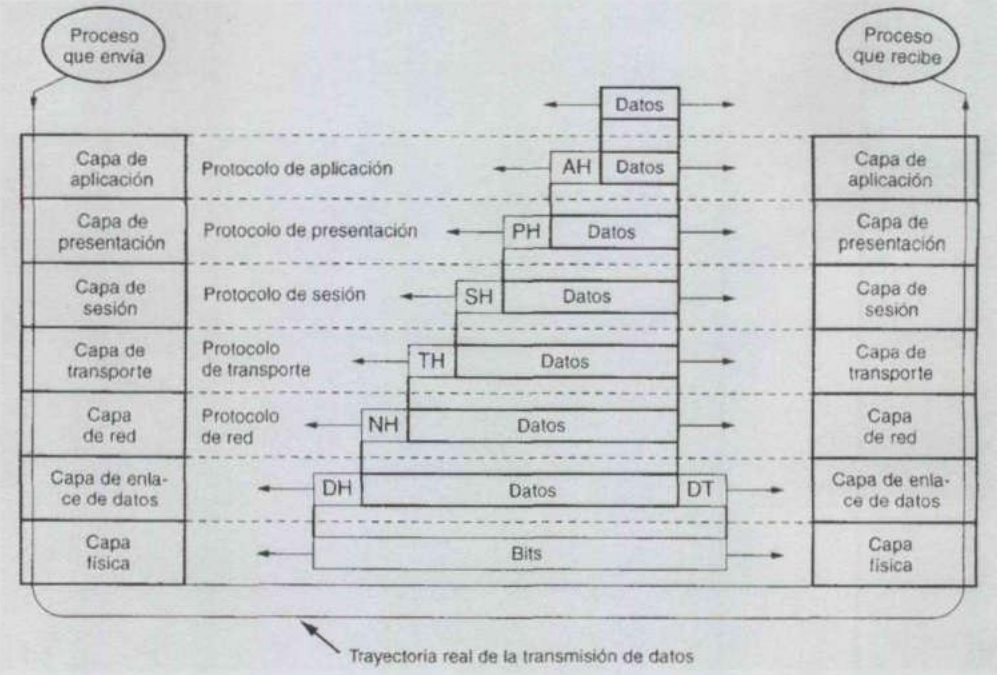



Figura 1.13. Ejemplo de uso del modelo OSI. Algunos encabezados pueden ser nulos.

Por eso decimos que cada capa de la maquina emisora, se comunica de forma horizontal con la capa receptora que lleva a cabo la misma función, debido a esto es por lo que no se puede comunicar directamente maquinas con distintas cantidades de capas.

Cada capa trabaja de forma similar a como se planteo antes, para lo cual agrega un encabezado donde da las instrucciones, si es que las hay, indica si es nula, entre otras cosas.

Cada capa es independiente en el sentido de que la capa que recibe la información no sabe que parte son los datos del usuario y cual es la que agrega la capa, por lo cual no puede invadir el trabajo de otra capa. La información que se envía pasa por todas y cada una de las capas aun cuando no se haga nada en ella.

### 1.5.4. Modelo de referencia TCP/IP.

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas. El más utilizado es conocido como TCP/IP.

Es un protocolo que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP/IP Proviene de dos protocolos importantes, el Protocolo de Control de Transmisión o TCP y Protocolo de Interred o IP.

El TCP/IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo computadoras personales, mini computadoras y computadoras centrales sobre redes de área local y área extensa. TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.

El modelo ISO, elaborado para describir protocolos para una sola red, no contiene un nivel especifico para el ruteo en el enlace de redes, como sucede con el protocolo TCP/IP.

### 1.5.5. Las capas del modelo TCP/IP.

Habrá que pensar que en el *software* de protocolos como en una pila vertical constituida por capas. Cada capa tiene la responsabilidad de manejar una parte del problema.

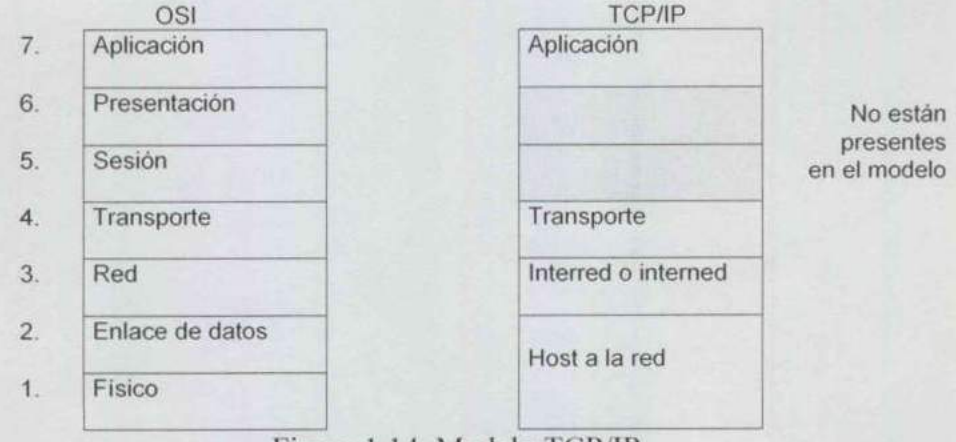



Figura 1.14. Modelo TCP/IP.

En términos generales, el *software* TCP/IP está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de *hardware*. La figura 1.14. Muestra las capas conceptuales así como la forma en que los datos pasan entre ellas.

Estas capas son:

1. Capa de internet.
2. Capa de transporte.
3. Capa de aplicación.
4. Capa de nodo a la red.

### *1.5.5.1. Capa internet.*

La capa internet o interred es el eje que mantiene unida toda la arquitectura y maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia el destino a que debe enviar el paquete. Los paquetes pueden llegar en distinto orden al enviado. La capa Internet envía los mensajes ICMP de error y control necesarios y maneja todos los mensajes ICMP entrantes. Esta capa define el formato de paquete y protocolo oficial llamado Protocolo de Interred o IP. El trabajo de esta capa es entregar paquetes IP a su destino, es claramente el ruteo de los paquetes y evitar la congestión. Es sensato decir que es muy parecida a la de red OSI.

### *1.5.5.2. Capa de transporte.*

Esta sobre la capa de interred. La principal tarea de la capa de transporte es proporcionar la comunicación entre los nodos destino y origen. La capa de transporte regula el flujo de información. Aquí se definieron dos protocolos de extremo a extremo.

El primero es el Protocolo de Control de Transmisión o TCP, es un protocolo confiable orientado a la conexión permite proporcionar un transporte confiable, asegurando que los datos lleguen sin errores. El segundo es el Protocolo de Datagrama de Usuario o UDP, es un protocolo sin conexión, no confiable usado para consultas de petición y respuesta de tipo cliente-servidor, y en aplicaciones donde la entrega rápida es más importante que la precisa.

La capa de transporte debe aceptar datos desde varios programas de usuario y los envía a la capa superior. Para hacer esto, añade información adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así

como una suma de verificación para verificar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

#### *1.5.5.3. Capa de aplicación.*

Es la capa mas alta, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de capa de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continúo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia la capa de transporte para su entrega.

#### *1.5.5.4. Capa de nodo a la red.*

El *software* TCP/IP de capa inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. La capa de nodo a la red puede consistir en un dispositivo controlador, o un complejo subsistema que utiliza un protocolo de enlace de datos propios.

En realidad el modelo no dice mucho de esta capa solo que se ha de conectar a la red haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes de IP.

### 1.5.6. Información adicional sobre el modelo de referencia TCP/IP.

Conceptualmente, enviar un mensaje desde un programa de aplicación en una maquina hacia un programa de aplicaciones en otra, significa transferir el mensaje hacia abajo, por las capas sucesivas del *software* de protocolo en la maquina emisora, transferir un mensaje a través de la red y luego, transferir el mensaje hacia arriba, a través de las capas sucesivas del *software* de protocolo en la maquina receptora.

En la práctica, el *software* es mucho más complejo de lo que se ve en el modelo. Cada capa toma decisiones acerca de lo correcto del mensaje y selecciona una acción apropiada con base en el tipo de mensaje o la dirección de destino. Por ejemplo, una capa en la maquina receptora debe decidir cuándo tomar un mensaje o enviarlo a otra. Otra capa debe decidir

que programa de aplicación debe recibir el mensaje. Sólo cuando se alcanza la maquina destino, IP extrae el mensaje y lo pasa hacia la capa superior del *software* de protocolos.

## 1.6. SERVICIOS DE RED.

La finalidad de una red es que los usuarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la organización. Así las organizaciones obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- Mayor facilidad de comunicación. mayor variedad de programas y mayor facilidad de uso.
- Mejora de la competitividad y mejora de la dinámica de grupo y en los tiempos de respuesta.
- Reducción del presupuesto para proceso de datos y reducción de los costos de proceso por usuario.
- Mejoras en la administración de programas y mejoras en la integridad de los datos.
- Flexibilidad en el proceso de datos.
- Mejor seguridad.

## 1.7. SERVICIOS.

Para que todas las ventajas mencionadas antes sean posibles, la red debe prestar una serie de servicios a sus usuarios.

### 1.7.1. Servicios a usuarios.

La serie de servicios a usuarios que presta la red son:

- Acceso.
- Ficheros.
- Impresión.
- Correo.
- Información.
- Otros.

### *1.7.1.1. Acceso.*

Los servicios de acceso a la red comprenden tanto la verificación de la identidad del usuario para determinar cuales son los recursos de la misma que puede utilizar, como servicios para permitir la conexión de usuarios de la red desde lugares remotos.

### *1.7.1.2. Control de acceso.*

Para el control de acceso, el usuario debe identificarse conectando con un servidor en el cual se autentifica por medio de un nombre de usuario y una clave de acceso. Si ambos son correctos, el usuario puede conectarse a la red.

### *1.7.1.3. Acceso remoto.*

En este caso, la red de la organización está conectada con redes públicas que permiten la conexión de estaciones de trabajo situadas en lugares distantes. Dependiendo del método utilizado para establecer la conexión el usuario podrá acceder a unos u otros recursos.

### *1.7.1.4. Ficheros.*

El servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

### *1.7.1.5. Impresión.*

Permite compartir impresoras de alta calidad, capacidad y coste entre múltiples usuarios, reduciendo así el gasto. Existen equipos servidores con capacidad de almacenamiento propio donde se almacenan los trabajos en espera de impresión, lo cual permite que los clientes se descarguen de esta información con más rapidez. Una variedad de servicio de impresión es la disponibilidad de servidores de fax, los cuales ponen al servicio de la red sistemas de fax para que se puedan enviar éstos desde cualquier estación. En ciertos casos, es incluso posible enviar los faxes recibidos por correo electrónico al destinatario.

#### *1.7.1.6. Correo.*

El correo electrónico es la aplicación de red más utilizada. Permite claras mejoras en la comunicación frente a otros sistemas. Por ejemplo, es más cómodo que el teléfono porque se puede atender al ritmo determinado por el receptor, no al ritmo de los llamantes. Además tiene un costo mucho menor para transmitir iguales cantidades de información. Frente al correo convencional tiene la clara ventaja de la rapidez.

#### *1.7.1.7. Información.*

Los servidores de información pueden bien servir ficheros en función de sus contenidos como pueden ser los documentos hipertexto, como es el caso de esta presentación. O bien, pueden servir información dispuesta para su proceso por las aplicaciones, como es el caso de los servidores de bases de datos.

#### *1.7.1.8. Otros.*

Las redes más modernas, con grandes capacidades de transmisión, permiten transferir contenidos distintos a datos, como son imagen o sonido. Esto permite aplicaciones como:

- Estaciones integradas (voz y datos).
- Telefonía integrada.
- Servidores de imágenes.
- Videoconferencia de sobremesa.

### 1.7.2. Los servidores y servicios de red.

Para la prestación de los servicios de red se requiere que existan sistemas en la red con capacidad para actuar como servidores. Los servidores y servicios de red se basan en los sistemas operativos de red. Un sistema operativo de red es un conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios. Estos programas interceptan las peticiones de servicio de los usuarios y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red, le permite a ésta ofrecer capacidades de multiproceso y multiusuario. Según la forma de interacción de los programas en la red, existen dos formas de arquitectura lógica:

### *1.7.2.1. Cliente-servidor.*

Este es un modelo de proceso en el que las tareas se reparten entre programas que se ejecutan en el servidor y otros en la estación de trabajo del usuario. En una red cualquier equipo puede ser el servidor o el cliente.

El cliente es la entidad que solicita la realización de una tarea, el servidor es quien la realiza en nombre del cliente. Como las aplicaciones de acceso a bases de datos, las estaciones ejecutan las tareas del interfaz de usuario (pantallas de entrada de datos o consultas, listados, etc.) y el servidor realiza la actualización y recupera los datos en la base. En este tipo de redes, las estaciones no se comunican entre sí.

Las ventajas de este modelo incluyen:

- Incremento en la productividad.
- Control o reducción de costos al compartir recursos.
- Facilidad de administración, al concentrarse el trabajo en los servidores.
- Facilidad de adaptación.

### *1.7.2.2. Redes de pares.*

Este modelo permite la comunicación entre usuarios o estaciones de trabajo directamente sin tener que pasar por un equipo central para transferir. Las principales ventajas de este modelo son: Sencillez y facilidad de instalación, administración y uso; y Flexibilidad. Cualquier estación puede ser un servidor y puede cambiar de rol, de proveedor a usuario según los servicios.

# CAPÍTULO 2. PROTOCOLOS.

## 2.1. INTRODUCCIÓN A LOS PROTOCOLOS.

Hasta mediados de los ochenta, la mayoría de las redes LAN estaban aisladas. Una LAN servía a un departamento o a una compañía y escasamente se conectaba a entornos más grandes. Sin embargo, a medida que maduraba la tecnología LAN, la comunicación de los datos necesito la expansión de negocios, las LAN evolucionaron, haciéndose componentes redes de comunicaciones más grandes en las que las LAN podían hablar entre sí.

Pero para que la comunicación se diera, fuere necesario emplear reglas y procedimientos que permitieran esa comunicación de forma transparente al usuario.

Los protocolos son reglas y procedimientos para la comunicación. El término protocolo se utiliza en distintos contextos. Un ejemplo, es que los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma manera se aplican las reglas del protocolo al ambiente informático.

## 2.2. CLASIFICACION DE PROTOCOLOS.

Se podría definir protocolo como el conjunto de normas que regulan la comunicación, es decir, establecimiento, mantenimiento y cancelación; entre los distintos dispositivos de una red. Es como el lenguaje común que deben de usar todos los componentes para entenderse entre ellos.

Los protocolos se clasifican en dos grupos:

- Los protocolos de bajo nivel.
- Los protocolos de red

### 2.2.1.-Protocolos de Bajo Nivel.

Los protocolos de bajo nivel que son los que se encargan de gestionar el tráfico de información por el cable, o sea a nivel físico.

El protocolo de bajo nivel es, en cierto modo, la forma en que las señales se transmiten por el cable, transportando tanto datos como información y los procedimientos de control de uso del medio por los diferentes modos.

Los protocolos de bajo nivel controlan el acceso al medio físico, lo que se conoce como MAC, y, además, parte del nivel de transmisión de datos, ya que se encargan también de las señales de temporización de la transmisión. Sobre todos los protocolos de bajo nivel Control de Acceso al Medio o MAC, se asientan en los protocolos de Control Lógico del Enlace o LLC, definidos en el estándar IEEE 802.2.

Existen bastantes protocolos de bajo nivel como pueden ser *Ethernet*, *Token ring*, etc. Aunque los más utilizados son:

- *Ethernet*.
- *Token ring*.
- *Token bus*.
- FDDI.
- CDDI.
- HDLC.
- *Frame Relay*.
- ATM.

#### *2.2.1.1. Ethernet.*

El protocolo de red *Ethernet* fue diseñado originalmente por *Digital*, *Intel* y *Xerox* por lo que, originalmente se conoce como *Ethernet DIX*. Posteriormente, IEEE definió el estándar *Ethernet* 802.3. La forma de codificación difiere ligeramente en ambas definiciones.

Es el método de conexión más extendido porque permite buen equilibrio entre velocidad, costo y facilidad de instalación. Esto combinado con su buena aceptación en el mercado y la facilidad de soportar prácticamente todos los protocolos de red, convierten a *Ethernet* en la tecnología ideal para la mayoría de las instalaciones de LAN. Consigue velocidad de conexión de 10 Mbps aunque existen especificaciones de velocidades superiores como es el caso de *Fast Ethernet* que llega a conseguir hasta 100 Mbps.

En el caso del protocolo *Ethernet* / IEEE 802.3, el acceso al medio se controla con un sistema conocido como Detección de Portadora con Acceso Múltiple y Detección de Colisiones o CSMA/CD.

Existen cuatro tipos de *Ethernet*:

- *10base5. Ethernet* original. Sobre cable coaxial grueso y transceptores.
- *10base2.* Es la especificación *Ethernet* sobre cable coaxial fino o red barata.
- *10baseT.* Es la especificación *Ethernet* sobre cable telefónico. de par trenzado.
- *10baseF.* Es la especificación *Ethernet* sobre fibra óptica.

En la actualidad han surgido nuevas especificaciones basadas en *Ethernet* que permiten transmitir datos a mayor velocidad como son:

- *Switched Ethernet.* Esta especificación utiliza concentradores de red con canales de comunicación de alta velocidad en su interior, con una arquitectura similar a las centrales de teléfonos, que conmutan el tráfico entre estaciones conectados a ellos.
- *Ethernet de 100* Mbps *(100baseX).*Esta especificación permite velocidades de transferencia de 100 Mbps sobre cables de pares trenzados, directamente desde cada estación.

### *2.2.1.2. Token Ring.*

Es un sistema bastante usado aunque menos que *Ethernet*. Llega a conseguir velocidades de hasta 16 Mbps aunque existen especificaciones para velocidades superiores. La topología lógica que usa es en anillo aunque en la práctica se conecta en una topología física en estrella, a través de concentradores llamados Unidad de Acceso Multiestación o MAU. Es más fácil de detectar errores que en *Ethernet*. Cada nodo reconoce al anterior y al posterior. Se comunican cada cierto tiempo. Si existe un corte, el nodo posterior no recibe información del nodo cortado e informa a los demás de cual es el nodo inactivo.

Las redes basadas en protocolos de pasar el toque o *Token passing* basan el control de acceso al medio en la posesión de un toque. Éste es un paquete con un contenido especial que permite transmitir a la estación que lo tiene. Cuando ninguna estación necesita transmitir, el toque va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el toque a la siguiente.

Las redes de tipo *Token ring* tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbps. Existen redes *Token ring* de 16 Mbps, pero no están definidas en ninguna especificación de IEEE.

#### *2.2.1.3. Token bus.*

Es una especificación de red basada en control de acceso al medio por paso de toque con topología de bus.

#### *2.2.1.4. FDDI.*

Es una especificación de red sobre fibra óptica con topología de doble anillo, control de acceso al medio por paso de testigo y una velocidad de transmisión de 100 Mbps. Esta especificación estaba destinada a sustituir a la *Ethernet* pero el retraso en terminar las especificaciones por parte de los comités y los avances en otras tecnologías, principalmente *Ethernet*, la han relegado a unas pocas aplicaciones como interconexión de edificios.

#### *2.2.1.5. CDDI.*

Es una modificación de la especificación FDDI para permitir el uso de cables de cobre de la llamada categoría cinco, cables de alta calidad específicos para transmisión de datos, en lugar de fibra óptica.

#### *2.2.1.6. HDLC.*

Es la especificación de red utilizada principalmente en las transmisiones por líneas telefónicas para comunicaciones de datos, como pueden ser las líneas punto a punto y las redes públicas de conmutación de paquetes.

#### *2.2.1.7. Frame Relay.*

*Frame Relay* o paso de tramas; puede ser tanto un servicio prestado por una compañía telefónica como una especificación de red privada. Este sistema de transmisión permite velocidades de 56 Kbps, n x 64 Kbps o 2 Mbps. El servicio se puede establecer con líneas punto a punto entre ruteadores o por medio de una conexión con una red pública.

Un parámetro básico del servicio *Frame Relay* es la Tasa de Información Asegurada o CIR, la cual se utiliza para facturar las conexiones a redes públicas. Este valor se basa en la naturaleza aleatoria de la transmisión de datos, ya que no todas las estaciones transmiten al mismo tiempo, con lo cual, la suma de la capacidad, en *bits*/s, de los canales de cada una de ellas, puede ser superior a la capacidad de los canales de interconexión. Cada estación puede transmitir toda la información que permita el canal, pero, en caso de que la red se congestiones, sólo podrá transmitir, en principio, la cantidad permitida por el CIR.

#### *2.2.1.8. ATM.*

Modo de transferencia asíncrono o ATM. Es la especificación más reciente y con mayor futuro. Permite velocidades de a partir de 156 Mbps llegando a superar los 560 Mbps. Se basa en la transmisión de pequeños paquetes de datos de 56 *bytes*, con una mínima cabecera de dirección que son conmutados por equipos de muy alta velocidad. La gran ventaja de esta especificación es la capacidad que tiene para transmitir información sensible a los retardos como pueden ser voz o imágenes digitalizadas combinada con datos, gracias a la capacidad de marcar los paquetes como eliminables, para que los equipos de conmutación puedan decidir que paquetes transmitir en caso de congestión de la red.

### 2.2.2. Protocolos de Red.

Los protocolos de red que se ven después de los de bajo nivel, cuando se necesite configurar la red y que fundamentalmente definen las normas a nivel de software por las que se van a comunicar los distintos dispositivos de la red, y son estos los que nos interesan mas en este documento.

Los protocolos de red organizan la información, es decir, los controles y datos; para su transmisión por el medio físico a través de los protocolos de bajo nivel. Algunos son:

- IPX/SPX
- NetBIOS
- NetBEUI
- AppleTalk
- TCP/IP

### *2.2.2.1. IPX/SPX.*

IPX es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es un protocolo orientado a paquetes y no orientado. Otro protocolo, el SPX actúa sobre IPX para asegurar la entrega de los paquetes.

Intercambio de paquetes entre redes/Intercambio de paquetes en secuencia o IPX/SPX. El Intercambio de paquetes entre redes o IPX define los esquemas de direccionamiento utilizados en una red Netware, e Intercambio de paquetes en secuencia o SPX proporciona la seguridad y fiabilidad al protocolo IPX. IPX es un protocolo a nivel de red basado en datagramas, no orientado a la conexión y no fiable, equivalente a IP. No requiere confirmación por cada paquete enviado. Cualquier control de confirmación o control de conexión tiene que ser proporcionado por los protocolos superiores a IPX. SPX proporciona servicios orientados a la conexión y fiables a nivel de transporte.

### *2.2.2.2. NetBIOS.*

Sistema básico de Entrada/Salida de la red o NetBIOS, es un programa que permite que se comuniquen aplicaciones en diferentes computadoras dentro de una LAN. Se usa en redes con topologías *Ethernet* y *Token ring*. No permite por si mismo un mecanismo de ruteo por lo que no es adecuado para MAN, en las que se deberá usar otro protocolo para el transporte de los datos (por ejemplo, el TCP).

La mayoría de los servicios y aplicaciones que se ejecutan en el sistema operativo Windows utilizan la interfaz NetBIOS o la Comunicación entre procesos o IPC. NetBIOS se desarrolló sobre LAN y se ha convertido en una interfaz estándar para que las aplicaciones puedan acceder a los protocolos de red en la capa de transporte con comunicaciones orientadas o no a la conexión.

NetBIOS puede actuar como protocolo orientado o no a la conexión en sus modos respectivos sesión y datagrama. En el modo sesión dos computadoras establecen una conexión para establecer una conversación entre los mismos, mientras que en el modo datagrama cada mensaje se envía independientemente. Una de las desventajas de NetBIOS es que no proporciona un marco estándar o formato de datos para la transmisión.

Existen interfaces NetBIOS para NetBEUI, NWLink y TCP/IP. Las interfaces NetBIOS necesitan una dirección IP y un nombre NetBIOS para identificar de forma única a un equipo. NetBIOS realiza cuatro funciones importantes:

- *Resolución de nombres NetBIOS.* Cada estación de trabajo de una red tiene uno o más nombres. NetBIOS mantiene una tabla con los nombres y algunos sinónimos. El primer nombre en la tabla es el nombre único de la NIC. Se pueden añadir nombres de usuario opcionales para proporcionar un sistema de identificación expresivo.
- *Servicio de datagramas NetBIOS.* Esta función permite enviar un mensaje a un nombre, a un grupo de nombres, o a todos los usuarios de la red. Sin embargo, debido a que no utiliza conexiones punto a punto, no se garantiza que el mensaje llegue a su destino.
- *Servicio de sesión NetBIOS.* Este servicio abre una conexión punto a punto entre dos estaciones de trabajo de una red. Una estación inicia una llamada a otra y abre la conexión. Debido a que ambas estaciones son iguales, pueden enviar y recibir datos concurrentemente.
- *Estado de la sesión/NIC NetBIOS.* Esta función ofrece información sobre la NIC local, otras NIC y las sesiones activas disponibles a cualquier aplicación que utilice NetBIOS.

#### *2.2.2.3. NetBEUI.*

NetBEUI es el acrónimo de Interfaz de usuario ampliada NetBIOS, es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una transmisión de datos. Originalmente, NetBIOS y NetBEUI estaban casi unidos y se les consideraba como un protocolo. Sin embargo, varios fabricantes separaron NetBIOS, el protocolo a capa de sesión, de forma que pudiera utilizarse con otros protocolos de transporte ruteables.

NetBIOS, es una interfaz para LAN a nivel de sesión de IBM que actúa como una interfaz de aplicación para la red. NetBIOS proporciona a un programa las herramientas para que

establezca en la red una sesión con otro programa, y debido a que muchos programas de aplicación lo soportan, es muy popular. También desarrollado por IBM y adoptado después por Microsoft, es actualmente el protocolo predominante en las redes Windows NT, LAN Manager y Windows para trabajo en grupo.

NetBEUI es un protocolo pequeño, rápido y eficiente a nivel de transporte proporcionado con todos los productos de red de Microsoft. Está disponible desde mediados de los ochenta y se suministró con el primer producto de red de Microsoft: MS-NET.

Entre las ventajas de NetBEUI se incluyen su pequeño tamaño, importante para los equipos que ejecuten MS-DOS, su velocidad de transferencia de datos en el medio y su compatibilidad con todas las redes Microsoft.

El principal inconveniente de NetBEUI es que no soporta el ruteo. También está limitado a redes Microsoft. NetBEUI es una buena solución económica para una red Trabajo en Grupo donde todas las estaciones utilizan sistemas operativos Microsoft.

Aunque NetBEUI es la mejor elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el ruteo de mensajes hacia otras redes, que deberá hacerse a través de otros protocolos; por ejemplo, IPX o TCP/IP. Un método usual es instalar tanto NetBEUI como TCP/IP en cada estación de trabajo y configurar el servidor para usar NetBEUI para la comunicación dentro de la LAN y TCP/IP para la comunicación hacia afuera de la LAN.

#### *2.2.2.4. AppleTalk.*

Es el protocolo de comunicación para computadoras Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo. AppleTalk es una colección de protocolos que se corresponde con el modelo OSI. Existen tres variantes de este protocolo:

- *Local Talk*. La comunicación se realiza a través de puertos serie de las estaciones. La velocidad de transmisión es pequeña pero sirve para compartir impresoras. Describe el cable par trenzado apantallado usado para conectar equipos Macintosh con otros Macintosh o impresoras. Un segmento *Local Talk* permite hasta un máximo de 32 dispositivos y opera a una velocidad de 230 Kbps.

- *Ether Talk.* Es la versión para *Ethernet*. Esto aumenta la velocidad y facilita aplicaciones como por ejemplo la transferencia de archivos. Opera a una velocidad de 10 Mbps. *Fast Ethernet* opera a una velocidad de 100 Mbps.
- *Token Talk.* Es la versión de *Apple Talk* para redes *Token ring*. Dependiendo de su *hardware*, *TokenTalk* opera a 4 o a 16 Mbps.

### *2.2.2.5. TCP/IP.*

El Protocolo de Control de Transmisión/Protocolo Internet o TCP/IP es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo formado por elementos diferentes. TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el ruteo y se suele utilizar como un protocolo de interconexión de redes.

Es realmente un conjunto de protocolos, donde los más conocidos son TCP e IP. Dicho conjunto o familia de protocolos es el que se utiliza en Internet.

- *Protocolo de Control de Transmisión o TCP.* Es el responsable de la transmisión fiable de datos desde un nodo a otro. Es un protocolo orientado a la conexión y establece una conexión, también conocida como una sesión, circuito virtual o enlace; entre dos máquinas antes de transferir algún dato. Para establecer una conexión fiable, TCP utiliza lo conocido como; acuerdo en tres pasos. Establece número de puerto y de secuencia de inicio desde ambos lados de la transmisión.
- *El Protocolo Internet o IP.* Es un protocolo de conmutación de paquetes que realiza direccionamiento y ruteo. Cuando se transmite un paquete, este protocolo añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de ruteo dinámico. IP es un protocolo no orientado a la conexión y envía paquetes sin esperar la señal de confirmación por parte del receptor. Además, IP es el responsable del empaquetado y división de los paquetes requerido por los niveles: físico y de enlace de datos del modelo OSI.

Diseñado para ser ruteable, robusto y funcionalmente eficiente. Actualmente, la responsabilidad del desarrollo de TCP/IP reside en la propia comunidad de Internet. La utilización de TCP/IP ofrece varias ventajas:

- *Es un estándar en la industria.* Como un estándar de la industria, es un protocolo abierto. Es decir, no está controlado por una compañía, y está menos sujeto a cuestiones de compatibilidad. Es el protocolo, de hecho, de Internet.
- *Contiene un conjunto de utilidades para la conexión de sistemas operativos diferentes.* La conectividad entre equipos no depende del SO de red que usen estos.
- *Utiliza una arquitectura escalable, cliente/servidor.* TCP/IP puede ampliarse o reducirse para ajustarse a las necesidades y circunstancias futuras. Utiliza *sockets* para hacer que el sistema operativo sea algo transparente.

Un *socket* es un identificador para un servicio concreto en un nodo concreto de la red. El *socket* consta de una dirección de nodo y de un número de puerto que identifica al servicio.

### 2.2.3. Cuestiones importantes de los protocolos de red.

Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos. Cuando se piense en protocolos de red es importante recordar tres puntos:

- *Existen muchos protocolos.* A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.
- *Algunos protocolos sólo trabajan en ciertos niveles OSI.* El nivel al que trabaja un protocolo describe su función. Un ejemplo, un protocolo que trabaja a nivel físico asegura que los paquetes pasen a la tarjeta de red o NIC y salgan al cable de la red.
- *Los protocolos también puede trabajar juntos en una jerarquía o conjunto de protocolos.* Al igual que una red incorpora funciones a cada uno de las capas del modelo OSI, otros protocolos también trabajan juntos en distintas capas en la jerarquía de protocolos. Las capas de la jerarquía de protocolos se corresponden con

las capas del modelo OSI. Por ejemplo, la capa de aplicación de TCP/IP se corresponde con la de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

### 2.2.4. Funcionamiento de los protocolos.

La operación técnica en que los datos son transmitidos a través de la red se puede dividir en dos pasos discretos, sistemáticos. A cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos, o protocolo.

Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

#### *2.2.4.1. Los protocolos en el equipo origen.*

Los protocolos en el equipo origen constan de una serie de pasos:

- Se dividen en secciones más pequeñas, denominadas paquetes.
- Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.
- Prepara los datos para transmitirlos a través de la NIC y enviarlos a través del cable de la red.

#### *2.2.4.2. Los protocolos en el equipo de destino.*

Los protocolos en el equipo de destino tienen los mismos pasos, pero en sentido inverso:

- Toma los paquetes de datos del cable y los introduce al equipo a través de la NIC.
- Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.
- Copia los datos de paquetes al búfer para reorganizar y enviar estos a la aplicación.

Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura al recibirse que cuando se enviaron.

#### *2.2.4.3. Protocolos ruteables.*

Los datos se envían de una LAN a otra a lo largo de varios caminos disponibles, es decir, se encaminan o rutean, que en términos informáticos y para fines de este documento se empleara el termino rutear en referencia a esto, por ser mas afín a el tema tratado. A los protocolos que permiten la comunicación LAN a LAN se les conoce como protocolos ruteables, es decir ruteables. Debido a que los protocolos ruteables se pueden utilizar para unir varias LAN y crear entornos de red de área extensa, han tomado gran importancia.

## 2.3. PROTOCOLOS EN UNA ARQUITECTURA MULTINIVEL.

En una red, tienen que trabajar juntos varios protocolos. Al trabajar juntos, aseguran que los datos se preparen correctamente, se transfieran al destino adecuado y se reciban de forma apropiada. El trabajo de los distintos protocolos tiene que estar coordinado de forma que no se originen conflictos o se realicen tareas incompletas. Los resultados de esta coordinación se conocen como trabajo en niveles.

### 2.3.1. Jerarquía de protocolos.

Retomando lo visto en el capitulo uno, una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación. Cada nivel o capa tiene su propio conjunto de reglas. Se puede usar los términos indistintamente pero comúnmente se usa más el término capa. Los protocolos definen las reglas para cada capa en el modelo OSI, según se puede observar en la figura 2.1.

Las capas inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los productos de otros fabricantes, por ejemplo, utilizando NIC de varios fabricantes en la misma LAN. Cuando utilicen los mismos protocolos, pueden enviar y recibir datos entre sí.

Las capas superiores especifican las reglas para dirigir la sesión de comunicación, es decir, el tiempo en que dos equipos mantienen una conexión, y la interpretación de aplicaciones.

| | Nivel o Capa | |
|---|---|---|
| 7. | **De aplicación** | Inicia o acepta una petición |
| 6. | **De presentación** | Añade información de formato, presentación y cifrado al paquete de datos |
| 5. | **De sesión** | Añade información del flujo de tráfico para determinar cuándo se envía el paquete |
| 4. | **De transporte** | Añade información para el control de errores |
| 3. | **De red** | Se añade información de dirección y secuencia al paquete |
| 2. | **De enlace de datos** | Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física |
| 1. | **Físico** | El paquete se envía como una secuencia de *bits* |

Figura 2.1. Capas del modelo OSI.

A medida que aumenta el nivel de la jerarquía, aumenta la sofisticación de las tareas asociadas a los protocolos. Se debe recordar que el modelo TCP/IP no se corresponde exactamente con el modelo OSI. En lugar de tener 7 capas, sólo usa 4. Normalmente se conoce como conjunto de protocolos de Internet, TCP/IP se divide las capas: Interfaz de red, Internet, Transporte y Aplicación. Cada uno de estos niveles se corresponde con uno o más niveles del modelo OSI. Según se aprecia en la figura 2.2.

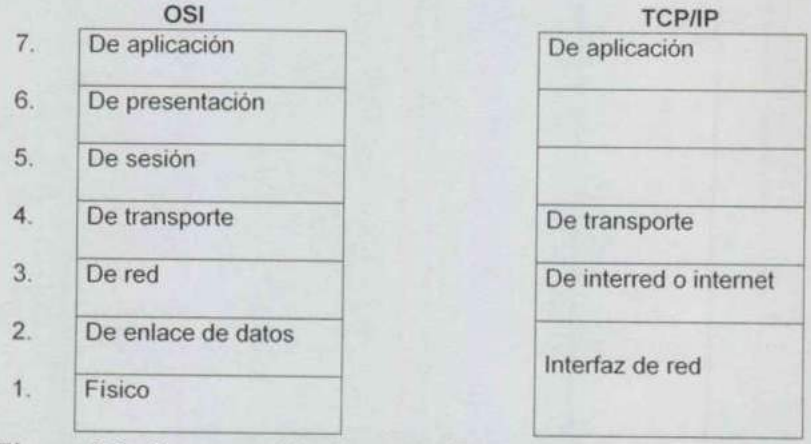



Figura 2.2. Comparación de capa de los modelos de referencia.

### 2.3.2. El proceso de enlace.

El proceso de enlace o *binding process*, es con el que se conectan los protocolos entre sí y con la NIC, permite una gran flexibilidad a la hora de configurar una red. Se pueden mezclar y combinar los protocolos y las NIC según las necesidades. Por ejemplo, se pueden

ligar dos jerarquías de protocolos a una NIC, como IPX/SPX. Si hay más de una NIC en el equipo, cada jerarquía de protocolos puede estar en una NIC o en ambas.

El orden de enlace determina la secuencia en la que el Sistema Operativo o SO ejecuta el protocolo. Cuando se enlazan varios protocolos a una NIC, el orden de enlace es la secuencia en que se utilizarán los protocolos para intentar una comunicación correcta.

Normalmente, el proceso de enlace se inicia cuando se instala o se inicia el SO o el protocolo. Por ejemplo, si el primer protocolo enlazado es TCP/IP, el SO de red intentará la conexión con TCP/IP antes de utilizar otro protocolo. Si falla esta conexión, el equipo tratará de realizar una conexión utilizando el siguiente protocolo en el orden de enlace.

El proceso de enlace consiste en asociar más de una jerarquía de protocolos a la NIC. Las jerarquías de protocolos tienen que estar ligadas o asociadas con los componentes en un orden para que los datos puedan moverse adecuadamente por la jerarquía durante la ejecución. Por ejemplo, se puede enlazar TCP/IP al nivel de sesión del NetBIOS, así como al controlador de la NIC. El controlador de la NIC también está enlazado a la NIC.

## 2.4. JERARQUÍAS DE PROTOCOLOS ESTÁNDAR.

La industria informática ha diseñado varios tipos de protocolos como modelos estándar de protocolo. Los fabricantes de *hardware y software* pueden desarrollar sus productos para ajustarse a cada una de las combinaciones de estos protocolos.

Los modelos más importantes incluyen:

- Conjunto de protocolos OSI.
- DECnet.
- Novell Netware.
- Apple Talk.
- Conjunto de protocolos TCP/IP.

Antes del modelo de referencia OSI se escribieron otros protocolos. Por tanto, no es extraño encontrar jerarquías de protocolos que no correspondan directamente con el modelo OSI.

### 2.4.1. Conjunto de protocolos OSI.

El conjunto de protocolos OSI es una jerarquía completa de protocolos. Cada protocolo se corresponde directamente con una única capa del modelo OSI. El conjunto de protocolos OSI incluye protocolos de ruteo y transporte, la serie de protocolos IEEE 802, un protocolo a capa de sesión, un protocolo a capa de presentación y varios protocolos a capa de aplicación diseñados para proporcionar una funcionalidad de red, incluyendo el acceso a archivos, impresión y emulación de terminal.

### 2.4.2. Protocolos DECnet.

DECnet es una jerarquía de protocolos de DEC. Es un conjunto de productos *hardware* y *software* que implementan la Arquitectura de Red de Digital o DNA. Define redes de comunicación sobre LAN *Ethernet*, redes de área metropolitana con Interfaz de datos distribuida de fibra o FDDI MAN y WAN que utilicen características de transmisión de datos privados o públicos. DECnet también puede utilizar protocolos TCP y OSI, así como sus propios protocolos. Se trata de un protocolo ruteable.

### 2.4.3. Novell NetWare.

Al igual que TCP/IP, Novell proporciona un conjunto de protocolos desarrollados específicamente para NetWare. Debido a que estos protocolos se definieron antes de la finalización del modelo OSI, no se ajustan exactamente al modelo OSI. Actualmente, no existe una correlación directa entre los límites de las capas de las dos arquitecturas. Estos protocolos siguen un patrón de recubrimiento.

#### *2.4.3.1. Protocolos NetWare.*

Los cinco protocolos principales utilizados por NetWare son:

- Protocolo de Acceso al Medio.
- IPX/SPX.
- Protocolo de Información de Ruteo o RIP.
- Protocolo de Notificación de Servicios o SAP.
- Protocolo básico de NetWare o NCP.

Concretamente, los protocolos de capa superior: NCP, SAP y RIP, están recubiertos por IPX/SPX. Luego, una cabecera y un final del Protocolo de Acceso al Medio recubren a IPX/SPX.

*Protocolos de acceso al medio.* Los protocolos de acceso al medio definen el direccionamiento que permite diferenciar a los nodos de una red NetWare. El direccionamiento está implementado en el *hardware* o la NIC. Las implementaciones más conocidas son: 802.5 *Token ring*, 802.3 *Ethernet* y *Ethernet* 2.0.

### 2.4.4. Apple Talk.

*Apple Talk* es la jerarquía de protocolos de *Apple Computer* para permitir que los equipos Apple Macintosh compartan archivos e impresoras en un entorno de red. Se introdujo en 1984 como una tecnología LAN autoconfigurable. *Apple Talk* también está disponible en muchos sistemas UNIX que utilizan paquetes comerciales y de libre distribución. El conjunto de protocolos *AppleTalk* permite compartir archivos a alto nivel utilizando *AppleShare*, los servicios de impresión y gestores de impresión de *LaserWriter*, junto con la secuencia de datos de bajo nivel y la entrega de datagramas básicos.

#### *2.4.4.1. Protocolos AppleTalk.*

*AppleTalk* es una colección de protocolos que se corresponde con el modelo OSI. Soporta *LocalTalk, EtherTalk y TokenTalk.*

### 2.4.5. Conjunto de protocolos TCP/IP.

Históricamente, TCP/IP ha tenido dos grandes inconvenientes: su tamaño y su velocidad. TCP/IP es una jerarquía de protocolos relativamente grandes que puede causar problemas en clientes basados en MS-DOS. En cambio, debido a los requerimientos del sistema; velocidad de procesador y memoria, que imponen los sistemas operativos con Interfaz Gráfica de Usuario GUI, como Windows NT o 95 y 98, el tamaño no es un problema.

TCP/IP proporciona un protocolo de red ruteable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo

que se conoce como interconexión de redes, la intercomunicación en una red que está formada por redes más pequeñas.

TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el ruteo y se suele utilizar como un protocolo de interconexión de redes.

#### *2.4.5.1. Protocolos del conjunto TCP/IP.*

Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

- SMTP o Protocolo Básico de Transferencia de Correo. Correo electrónico.
- FTP o Protocolo de Transferencia de Archivos. Para la interconexión de archivos entre equipos que ejecutan TCP/IP.
- SNMP o Protocolo Básico de Gestión de Red. Para la gestión de redes.

## 2.5. PROTOCOLOS EN LAS CAPAS DE LAS JERARQUÍAS.

El modelo OSI se utiliza para definir los protocolos que se tienen que utilizar en cada capa. Los productos de distintos fabricantes que se ajustan a este modelo se pueden comunicar entre sí.

La ISO, el Instituto de Ingenieros Eléctricos y Electrónicos o IEEE, El Instituto de Estandarización Nacional Americano o ANSI, El Comité Consultivo Internacional de Telegrafía y Telefonía o CCITT, ahora Unión Internacional de Telecomunicaciones o ITU y otros organismos de estandarización desarrollaron protocolos que se correspondan con algunas capas del modelo OSI. Tal es el ejemplo de los protocolos de IEEE de capa física.

Por tratarse de un tema demasiado amplio, y para mayor comprensión del mismo se mencionaran algunos de los protocolos mas usados o de mayor importancia en el usos de las redes, pero no se puede dejar de aclarar que aunque se pretende clarificar lo mas posible, es tan solo una mínima parte del mundo de los protocolos usados para las redes.

Los protocolos existen en cada capa de estas jerarquías, realizando las tareas especificadas por la capa. Sin embargo, las tareas de comunicación que tienen que realizar las redes se

agrupan en un tipo de protocolo pues algunos asocian capas adyacentes. Algunos ejemplos de estos protocolos se mencionan en los grupos siguientes:

- Protocolos de capa física.
- Protocolos de capa acceso de datos.
- Protocolos de capa de red.
- Protocolos de capa de sesión.
- Protocolos de capa de transporte.
- Protocolos de capa de presentación.
- Protocolos de capa de aplicación.

Es importante aclarar que cada protocolo puede incorporarse por uno o más capas del modelo OSI, como en los protocolos TCP/IP.

Las funciones de cada capa se vieron en el capitulo 1, por lo que en algunas capas solo se hace mención de algunos puntos generales, es el tema importante aquí son los protocolos de las capas.

### *2.5.1. Protocolos de capa física.*

Antes de adentrarnos en los estándares de los protocolos de capa física, es pertinente hacer referencia al modelo TCP/IP donde la capa de interfaz de red, se corresponde con las capas física y de enlace de datos del modelo OSI se comunica directamente con la red. Proporciona la interfaz entre la arquitectura de red como *Token Ring, Ethernet* y la capa internet.

*Los protocolos de IEEE de capa física son:*

*802.3 (Ethernet).* Es una red lógica en bus que puede transmitir datos a 10 Mbps. Los datos se transmiten en la red a todos los equipos. Sólo los equipos que tenían que recibir los datos informan de la transmisión. El protocolo CSMA/CD regula el tráfico de la red permitiendo la transmisión sólo cuando la red esté despejada y no haya otro equipo transmitiendo.

*802.4 (Token Bus).* Es una red en bus que utiliza un esquema de paso de toque. Cada equipo recibe todos los datos, pero sólo los equipos en los que coincida la dirección responderán. Un toque viaja por la red determina quién es el equipo que tiene que informar.

*802.5 (Token Ring).* Es un anillo lógico que transmite a 4 ó a 16 Mbps. Aunque se le llama en anillo, está montada como una estrella ya que cada equipo está conectado a un concentrador. Realmente, el anillo está dentro del concentrador. Un toque a través del anillo determina qué equipo puede enviar datos.

### *2.5.2. Capa de enlace de datos.*

Una mención importante, respecto de la capa de enlace de datos del modelo OSI, es que contiene dos subcapas, la subcapa de Control de Acceso al Medio o MAC y la subcapa de Control de Enlace Lógico o LLC según lo muestra la figura 2.3.

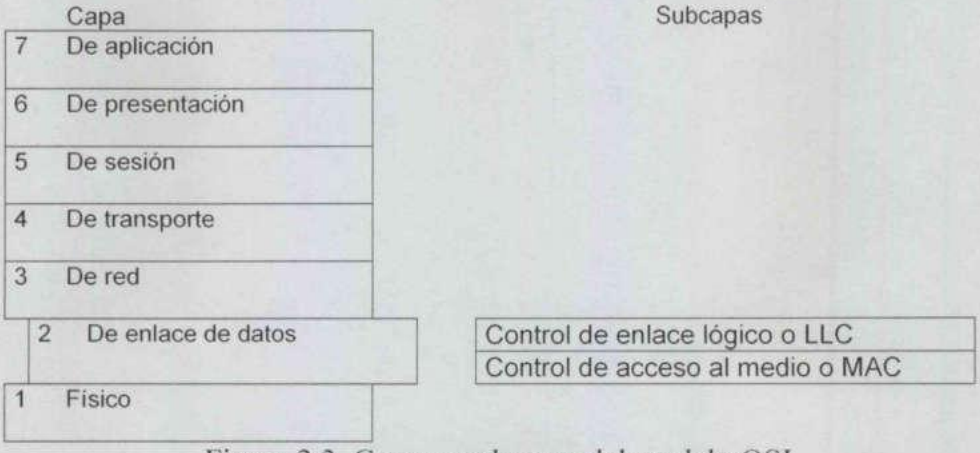



Figura 2.3. Capas y subcapas del modelo OSI.

*El IEEE definió estos protocolos para facilitar la comunicación en la subcapa MAC.*

Un controlador MAC está situado en la subcapa MAC; este controlador de dispositivo se conoce como controlador de la NIC. Provee acceso bajo nivel a los adaptadores de red para suministra soporte en transmisión de datos y funciones básicas de control del adaptador.

Un protocolo MAC determina qué equipo puede utilizar el cable de red cuando varios equipos intenten utilizarlo simultáneamente. CSMA/CD, el protocolo 802.3, permite a los equipos transmitir datos cuando no hay otro equipo transmitiendo. Si dos máquinas transmiten simultáneamente se produce una colisión. El protocolo detecta la colisión y detiene toda transmisión hasta que se libera el cable. Entonces, cada equipo puede volver a tratar de transmitir después de esperar un período de tiempo aleatorio. Las direcciones NIC de hardware también se denominan direcciones de Control de Acceso al Medio o MAC, y es una de las subcapas de la capa de enlace de datos.

### *2.5.3. Protocolos de capa de red.*

Es la capa del modelo OSI que establece y mantiene circuitos de conexión virtuales entre sistemas, es el encargado de la conmutación de paquetes y de transmitir los datos por toda la red. Se encarga de que los paquetes que salen del transmisor lleguen a su destino final aunque el emisor y el receptor no estén adyacentes, es decir permite el ruteo de tramas. Los protocolos de red proporcionan lo que se denominan; servicios de enlace. Estos protocolos gestionan información sobre direccionamiento y ruteo, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es *Ethernet* o *Token Ring*.

La capa internet de TCP/IP, que se corresponde con la capa de red del modelo OSI, utiliza varios protocolos para rutear y entregar los paquetes. Los ruteadores son dependientes del protocolo. Funcionan en esta capa del modelo y se utilizan para enviar paquetes de una red a otra o de un segmento a otro. En la capa de red trabajan varios protocolos. Claros ejemplos de los protocolos de red son: IP, ARP, RARP, ICMP, IPX.

- IP. Protocolo Internet.
- ARP. Protocolo de resolución de direcciones.
- RARP. Protocolo inverso de resolución de direcciones.
- ICMP. Protocolo de mensajes de control de Internet.
- IP. El protocolo de TCP/IP para el ruteo de paquetes.
- IPX. El protocolo de Novell para el ruteo de paquetes.
- NWLink. La implementación de Microsoft del protocolo IPX/SPX.

### *2.5.4. Protocolos de capa de transporte.*

La capa del modelo OSI encargado de la transferencia de los datos entre el emisor y el receptor y de mantener el flujo de la red.

La capa de transporte de TCP/IP, que se corresponde con la capa de transporte del modelo OSI, es el responsable de establecer y mantener una comunicación entre dos *hosts*. La capa de transporte proporciona notificación de la recepción, control de flujo y secuenciación de

paquetes. También gestiona las retransmisiones de paquetes. La capa de transporte puede utilizar los protocolos TCP o el UDP en función de los requerimientos de la transmisión.

- El TCP es el responsable de la transmisión fiable de datos desde un nodo a otro.
- El UDP protocolo no orientado a conexión, y es el responsable de la comunicación de datos extremo a extremo. Contrario a TCP, UDP no establece una conexión.

### *2.5.5. Protocolos de capa de sesión.*

La capa del modelo OSI que se ocupa de las funciones de gestión de red que incluyen contraseñas, monitorización e información de la red.

La capa de sesión tiene la responsabilidad de asegurar la entrega correcta de la información a la siguiente capa; es decir, la capa de presentación. Los protocolos de esta capa generalmente incorporan trabajo de la capa de transporte por lo que en este grupo se encuentran incorporados ejemplos de protocolos de transporte y sesión. Algo no ajeno pues los protocolos de transporte facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

- SPX. Parte de los protocolos IPX/SPX para datos en de paquetes secuenciados.
- NetBEUI. Establece sesiones de comunicación entre equipos NetBIOS y proporciona los servicios de transporte de datos subyacentes NetBEUI.
- ATP. Protocolo de Transacciones *Apple Talk*.
- NBP. Protocolo de Asignación de Nombres. Protocolos de Apple de sesión de comunicación y de transporte de datos.

### *2.5.6. Protocolos de capa de presentación.*

La capa de presentación es el nivel del modelo OSI que se ocupa de las funciones de seguridad de red, transferencias de ficheros y funciones de formato. Ejemplos de protocolos de la capa de presentación del modelo OSI son:

- HTTP. Protocolos de Transferencia de Hipertexto.
- FTP. Protocolo de Transferencia de Archivos.
- HTTPS. Seguridad en el Protocolo de Transferencia de Hipertexto.

Algo importante de mencionar aquí es que la capa de aplicación de TCP/IP, se corresponde con los niveles de sesión, presentación y aplicación del modelo OSI, y conecta las aplicaciones a la red. Dos Interfaces de Programación de Aplicaciones o API proporcionan acceso a los protocolos de transporte TCP/IP, los *sockets* de Windows y NetBIOS

### *2.5.7. Protocolos de aplicación.*

Los protocolos de aplicación trabajan en capa superior o capa 7 del modelo OSI y proporcionan interacción entre aplicaciones e intercambio de datos.

Según el modelo OSI, la capa de aplicación ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros.

Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. Entre sus protocolos más conocidos destacan:

- HTTP. Protocolo de Transferencia de Hipertexto.
- FTP. Protocolo de Transferencia de Archivos. En Internet.
- SMTP. Protocolo Básico para la Transferencia de Correo. En Internet.
- POP. Protocolo de Oficina Postal.
- Telnet. Un protocolo Internet para conexión remota y procesar los datos localmente.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP. Protocolo Básico de gestión de red. En Internet controla redes y componentes.
- DNS. Servidor de Nombres de Dominio.

Casi todas las aplicaciones; proceso de información, desarrolladas para TCP/IP comparten la arquitectura cliente-servidor.

# CAPITULO 3. PROTOCOLOS DE CAPA DE ENLACE Y DE RED.

## 3.1. INTRODUCCIÓN.

La capa de enlace de OSI es la encargada de establecer una línea de comunicación, libre de errores, que pueda ser utilizada por a la capa de red.

La capa física opera con *bits* aislados, que no tienen significado por sí mismos, sin embargo, la capa de enlace opera con bloques fraccionados del mensaje, a lo que se denominan tramas. Estas tramas están constituidas por parte de la información de los usuarios y por información adicional que se añade para el ruteo de las tramas, recuperación de errores y otras funciones.

Para que se pueda establecer comunicación entre dos equipos, es preciso que ambos se entiendan. Para ello se establecen una serie de reglas estandarizadas, establecidas por organismos internacionales u otras organizaciones que ambos equipos han de seguir. A este conjunto de reglas a seguir es ha lo que se denomina protocolo.

## 3.2. CODIGOS DE COMUNICACIONES.

Las computadoras trabajan con información digital. Toda información digital se representa mediante una serie de 0 y 1 agrupados según las reglas previamente establecidas. Esta forma de representación se denomina codificación, que no es otra cosa que representar cada elemento siempre de igual manera y con la misma duración dependiendo del código elegido.

Entre los distintos códigos que han ido surgiendo cabe destacar:

- *Código de Intercambio de Códigos Binario y Decimal Extendido o EBCDIC.* Desarrollado por IBM y inicialmente usado para enlaces entre dispositivos y grandes ordenadores.
- *Estándar Americano para el Intercambio de Información o ASCII.* Definido por el ANSI de EEUU. y por el ISO a escala mundial, adoptado por la mayoría de fabricantes de sistemas. Este código de 7 elementos permite la representación de hasta 128 caracteres, con lo cual se puede utilizar cualquier elemento.

### 3.2.1. El código ASCII.

Todos los ordenadores funcionan con tecnología digital. Cada vez que se pulsa una tecla, el teclado se comunica con el ordenador mandándole 0 y 1.

Dependiendo del número de *bits* que se utilicen para la codificación se podrán representar cierto número de elementos, es decir, si se utilizase una codificación de 5 *bits*, solo podrían representarse 32 elementos, que servirían para el alfabeto, pero sin diferenciar mayúsculas de minúsculas.

Por eso lo mínimo que se ha de mandar son 7 *bits*, que permitirían 128 combinaciones posibles (mayúsculas y minúsculas, acentuadas, números, signos,...) Si se quiere utilizar algún signo mas (@, |, ¬,...) se usan 8 *bits*, que son nada menos que 256 combinaciones y va ha permitir representar todas las letras, números, signos de puntuación, gráficos y alguna letra griega para fórmulas matemáticas, según un código que se llama ASCII.

Con este código, se suele enviar además de los *bits* de información un *bit* adicional denominado *bit* de paridad que sirve para verificar de una manera muy sencilla si se ha producido o no algún error en la transmisión de la información. Pero este método no es muy fiable ya que si se produce un doble error no lo detecta. Así pues, se puede ver también nombrado como código ASCII de 8 *bits* a un código ASCII de 7 *bits* +1 de paridad.

## 3.3. ACERCA DE LAS CAPAS.

Antes de entrar de lleno a la capa de enlace de datos es importante retomar una visión general de las capas adyacentes a ella; es decir la capa física y la capa de red.

### 3.3.1. La capa física.

La capa física es la base de todas las redes. Impone los límites fundamentales a todos los canales, y esto determina su ancho de banda.

Los medios de transmisión pueden ser guiados o no guiados. Los principales medios guiados son el par trenzado, el cable coaxial y la fibra óptica. Los medios no guiados incluyen la radio, las microondas, el infrarrojo y los laceres a través del aire.

Un elemento clave de la mayor parte las redes WAN es el sistema telefónico. Sus componentes principales son los lazos locales, troncales y conmutadores.

- Los lazos locales son circuitos de par trenzado, analógicos que requieren módems para transmitir datos digitales.
- Los troncales son digitales y se pueden multiplicar de varias formas, incluidas FDM, TDM y WDM.
- Los conmutadores incluyen los de matriz, los de división el espacio y los de división en el tiempo. Tanto la conmutación de circuitos como la de paquete son importantes.

En el futuro, no muy lejano el sistema telefónico será digital de un extremo al otro llevará tráfico tanto de voz como de datos por las mismas líneas. Se están presentando dos variantes este nuevo sistema llamado ISDN o Red Digital de Servicios Integrados.

La ISDN de banda estrecha es un sistema digital de conmutación de circuitos que representa una mejora incremental respecto al sistema actual. En contraste, la ISDN de banda ancha representa un cambio de paradigma, de que se basa en la tecnología ATM de conmutación de células. Existen varias clases de conmutadores ATM, incluido el conductor de eliminación. Para aplicaciones móviles, las alternativas de sistema telefónico incluyen la radio celular y los satélites de comunicaciones.

La radio celular ya se usa para teléfonos portátiles, pronto también para el tráfico de datos. La generación actual de sistemas celulares es análoga, pero la generación entrante será completamente digital. Los satélites de comunicación tradicionales son los cinco lados pero ha surgido mucho interés por los satélites de órbita baja.

### 3.3.2. La capa de enlace de datos.

La tarea de la capa de enlace de datos es convertir la corriente de *bits* en bruto ofrecida por la capa física en una corriente de marcos a ser usados por la capa de red. Se emplean varios métodos de enmarcado, incluidos el conteo de caracteres, el relleno de caracteres y el relleno de *bits*. Los protocolos de enlace de datos pueden proporcionar control de errores para retransmitir marcos dañados o perdidos. Para evitar que un transmisor rápido sature a uno lento, el protocolo de enlace de datos también puede proporcionar control del flujo.

El mecanismo de ventana corrediza se usa ampliamente para integrar el control de errores y el control del flujo de una manera conveniente.

Los protocolos de ventana corrediza pueden clasificarse por el tamaño de la ventana del transmisor y por el tamaño de la ventana del receptor. Cuando ambas son iguales, el protocolo de parada y espera. Cuando la ventana del transmisor es mayor que1, por ejemplo para evitar el bloqueo del transmisor en un circuito con retardo de propagación grande, el receptor puede programarse para descartar todos los marcos diferentes al siguiente de la secuencia o almacenar en *buffer* marcos fuera de orden hasta que se necesiten.

Los protocolos pueden modelarse usando varias técnicas para demostrar que son correctos o no. Los modelos de máquina de estado finito de red de Petri se usan frecuentemente para este propósito.

Muchas redes utilizan uno de los protocolos orientados a *bits;* SDLC, HDLC, ADCCP o LAPB, en la capa de enlace de datos. Todos estos protocolos usan *bytes* indicadores para delimitar marcos y relleno de *bits* para evitar que los *bytes* indicadores ocurran en los datos. Todos ellos también los son ventanas corredizas para el control del flujo. Internet emplean SLIP y PPP como protocolos de enlace de datos. Los sistemas ATM tienen su propio protocolo sencillo, que efectúa un mínimo de revisiones error y no tiene control del flujo.

### 3.3.3. La capa de red.

La capa de red proporciona servicios a la de transporte; puede basarse tanto de circuitos virtuales, como en datagramas. En ambos casos, la tarea principal de esta es rutear paquetes del origen al destino. En las subredes de circuitos virtuales se toma una decisión de ruteo al establecerse circuito virtual; en la subred de datagramas, se hace con cada paquete.

Se usan muchos algoritmos de ruteo en las redes de computadoras. Los algoritmos estáticos incluyen el ruteo para la trayectoria más corta, la inundación y el ruteo basado en flujo. Los algoritmos dinámicos incluyen el ruteo por vector de distancia y el ruteo por estado de enlace. La mayoría de las redes usan alguno de estos.

Otros temas importantes relativos al ruteo son el ruteo jerárquico, el ruteo para *host* móviles, el ruteo por división y el ruteo por multitransmisión.

La subredes pueden congestionase, aumentando retardo y reduciendo el rendimiento en los paquetes. Los diseñadores de redes intentan evitar los congestionamientos mediante un diseño adecuado. Las técnicas incluyen conformación de tráfico, especificaciones del flujo y reservación de ancho de banda. Si ocurre un congestionamiento, habrá que encargarse de el. Pueden enviarse paquetes de estrangulamiento de regreso, deshacerse parte la carga y aplicarse otros métodos.

Las redes difieren de varias maneras, por lo que cuando se conectan redes múltiples pueden ocurrir problemas. A veces los problemas pueden superarse enviando los paquetes en túnel a través de una red hostil, pero si las redes de origen y destino son diferentes, este enfoque falla. Cuando las diferentes redes tienen diferentes tamaños máximos de paquete, puede requerirse una fragmentación.

Internet posee una copiosa variedad de protocolos relacionados con la capa de red. Estos incluyen el protocolo de capa de transporte de datos, IP, pero también los protocolos de control ICMP, ARP y RARP, y los protocolos el ruteo OSPF y BGP. Internet está quedando sin direcciones de IP, por lo que se desarrolla una versión nueva IPV6.

A diferencia de Internet basada en datagramas, las redes ATM usan circuitos virtuales. Estos deben establecerse antes de poder trasmitir, liberarse después de la transmisión. La calidad del servicio y el control de congestionamiento son asuntos de gran importancia en las redes ATM.

### 3.4. LA CAPA DE ENLACE DE DATOS.

La capa de enlace de datos. Tiene que ver con los gobiernos para lograr una comunicación confiable y eficiente entre dos máquinas serían adyacentes en la capa de enlace datos. Se podría pensar que este problema es sencillo, pero los circuitos de comunicación cometen errores, además tienen una tasa de datos finita, y un retardo de propagación. Todas estas limitaciones tienen implicaciones importantes para que sea eficiente la transferencia de datos.

Los protocolos usados para con limitación deben conocer todos estos factores. Es importante observar la naturaleza de los errores, sus causas y la forma, como se pueden detectar y corregir.

La capa de enlace de datos tiene que desempeñar varias funciones específicas que incluyen proporcionar una interfaz de servicio bien definida la capa de red, determinar la manera en que los *bits* de la capa física se agrupan en marcos, manejar los errores de transmisión y regular el flujo de marcos, para los receptores lentos no sean agobiados por los transmisores rápidos.

Los protocolos en esta capa realizan una serie de funciones:

1. Establecimiento y finalización de la comunicación.
2. Envío de los mensajes.
3. Detección y corrección de errores.

### 3.4.1. Servicios proporcionados a la capa de red.

La función de la capa de enlace de datos es suministrar servicios a la capa de red. El servicio principal es la transferencia de datos de la capa de red en la máquina origen a la capa de red en la máquina destino. En la máquina origen hay una entidad, llámese proceso, en la capa de red que entrega algunos *bits* en la capa de enlace de datos para su transmisión a la máquina destino.

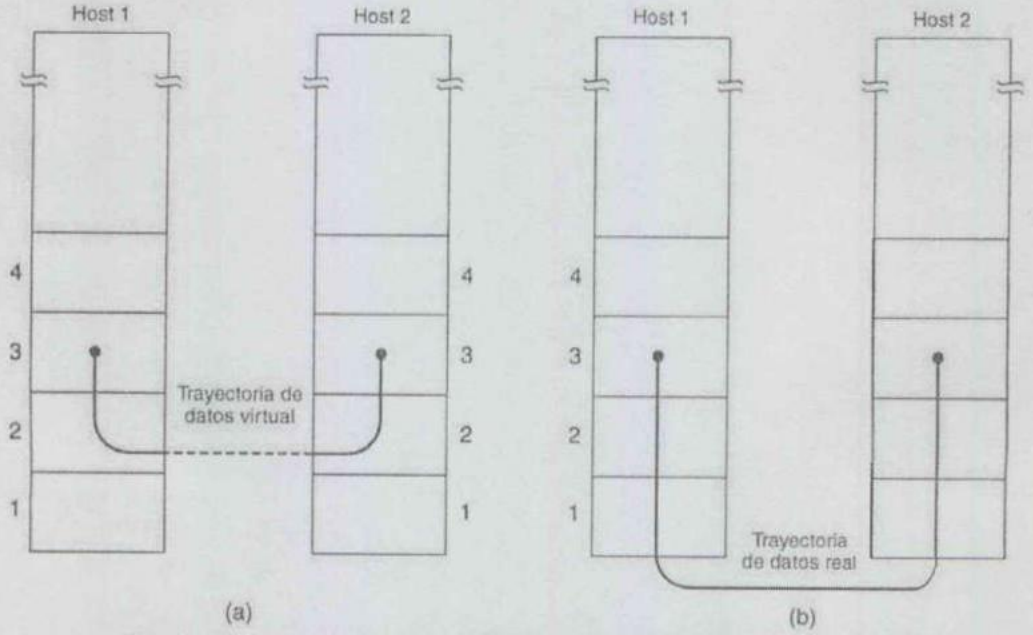



Figura 3.1. (a) comunicación virtual. (b) comunicación real.

El trabajo de la capa de enlace de datos es transmitir los *bits* a la máquina destino, para que puedan ser entregados a su capa de red, como se muestra en la figura 3.1(a). La transmisión

real sigue la trayectoria de la figura 3.1 (b), pero es más fácil pensar en términos de dos procesos de capa de enlace de datos que se comunican usando protocolo de enlace de datos. Por esta razón se usa el modelo de la figura 3.1(a).

La capa de enlace de datos puede diseñarse para ofrecer varios servicios. Los servicios reales ofrecidos pueden variar de sistema en sistema. Tres posibilidades razonables que normalmente se proporciona son:

- Servicio sin acuse sin conexión.
- Servicio con acuse sin conexión.
- Servicio con acuse orientado a la conexión.

El servicio más elaborado que puede proporcionar la capa enlace datos es al acatar el servicio orientado a la conexión. Al usarse un servicio orientado a conexión, las transferencias tienen tres fases distintas.

La primera, la conexión se establece haciendo que ambos lados inicialicen las variables y contadores necesarios para seguir la pista de los marcos que han sido o no recibidos. La segunda, se transmiten uno o más marcos. En la tercera, la final, la conexión se cierra liberando las variables, los *buffers* y otros recursos utilizados para mantener la conexión.

### 3.4.2. Enmarcado.

La capa de enlace proporciona servicios a la capa de red, usa los servicios proporcionados a ella por la capa física. Lo que hace la capa física es aceptar un flujo de *bits* en bruto e intentar entregarlo al destino. No se garantiza que este flujo de *bits* quede libre de errores. El número de *bits* recibidos puede ser menor, igual o mayor del número de *bits* admitidos, y pueden tener diferentes valores.

La responsabilidad de la capa de enlace de datos es detectar y de ser necesario corregir los errores. El enfoque común es que la capa enlace divida el flujo de *bits* en marcos discretos y que calcule la suma de comprobación para cada marco. Cuando el marco llega al destino se calcula la suma de comprobación. Si la suma de comprobación calculada es diferente de la que tiene el marco, la capa enlace datos sabe que ocurre un error y toma medidas para manejarlo.

La división en marcos del flujo de *bits* es más difícil de lo que parece. Una manera de lograr esta división, es introducir intervalos de tiempo entre los marcos, a semejanza de los espacios entre las palabras de texto común. Pero las redes pocas veces ofrecen garantías sobre la temporización, por lo que es posible que estos intervalos se eliminen o puedan introducir otros intervalos durante la transmisión.

Como es muy riesgoso depender de la temporización para marcar el inicio y el fin de cada marco, se diseñaron otros métodos:

- *Conteo de caracteres.*
- *Caracteres de inicio y fin, con relleno de caracteres.*
- *Indicadores de inicio y fin, con relleno de bits.*
- *Violaciones de codificación de la capa física.*

### *3.4.2.1. Conteo de caracteres.*

Este método se vale de un campo del encabezado por específica del número de caracteres en el marco. El problema aquí es que la cuenta pueda quedarse por un error de transmisión. Por ejemplo, si la cuenta de caracteres de 5 en un marco se vuelve un 7, el destino perderá la sincronía y será incapaz de localizar inicio del siguiente marco. Aun si la suma de comprobación es incorrecta, y el destino sabe que marco está mal, no tiene forma de saber dónde empieza el siguiente marco. Por esta razón, el método de conteo de caracteres de casi no se usa.

### *3.4.2.2. Caracteres de inicio y fin, con relleno de caracteres.*

Éste supera el problema de sincronización tras un error al hacer que cada marco contenga al inicio de la secuencia de caracteres ASCII DLE STX y termine con la secuencia DLE ETX. Escape de Enlace de Datos o DLE; Inicio de Texto o STX; Fin de Texto o ETX. De manera que si el destino llega perder la pista de los límites del marco, sólo busca los caracteres DLE STX y DLE STX para determinarlos. De problema aquí es cuando se transmiten datos binarios, como programas objeto o números de punto flotante, ya que puede ocurrir que los caracteres correspondan a DLE STX y DLE STX lo que puede interferir en el enmarcado.

#### *3.4.2.3. Indicadores de inicio y fin, con relleno de bits.*

El marco comienza y termina con un patrón especial de *bits*, llamado *byte* indicador. Desde la capa de enlace de datos del transmisor encuentra cinco unos consecutivos a los datos, automáticamente inserta un *bit* 0 en la cadena de *bits*. Cuando el receptor de cinco *bits* 1 de entrada consecutivos, seguidos de un *bits* 0, automáticamente quita el 0 de relleno. Con el relleno de *bits*, el límite entre dos marcos puede ser reconocido sin ambigüedades mediante un patrón indicador.

#### *3.4.2.4. Violaciones de codificación de la capa física.*

Este método de enmarcado sólo se aplica a las redes en las que la codificación en medio físico contiene cierta redundancia. Una codificación de un *bit* de datos usa dos *bits* físicos. Normalmente un *bit* 1 es un par alto-bajo, y un *bit* 0 bajo-alto. Combinaciones alto-alto y bajo-bajo muchos son para datos. El esquema implica que cada *byte* de datos tiene una transición a medio camino, lo que se facilita al receptor localizar los límites de los *bits*.

Muchos protocolos de enlace de datos buscan por seguridad, una combinación de cuenta de caracteres como de otros métodos.

### 3.4.3. Control de errores.

Cuando se resuelve el problema de marcar el inicio y fin de cada marco, el siguiente problema es asegurar que todos los marcos sean entregados correctamente a la capa de red en el destino, en el orden apropiado. La manera normal de asegurar la entrega correcta de datos es proporcionar al transmisor alimentación sobre lo que está ocurriendo el otro de la línea.

Usualmente, el protocolo exige que el transmisor envíe de regreso marcos de control especiales que contengan acuses positivos o negativos de los marcos de entrada. El transmisor cuando recibe un acuse positivo sabe que el marco llegó correctamente. Si llega negativo significa que algo fallo y el marco debe transmitirse otra vez.

Cuando el transmisor envía un marco, por lo general también arranca un temporizador, y este se ajusta de modo que termine cuando haya transcurrido un intervalo suficiente para

que el marco llegue su destino, se procese ahí y el acuse se propague de regreso al transmisor. Normalmente el marco se recibe correctamente y el acuse llega antes de que el temporizador termine, en cuyo caso se cancela.

Si el marco o el acuse se pierden, el temporizador termina y alerta al transmisor sobre el posible problema. La solución es solo retransmitir el marco. Pero al retransmitirse los marcos, hay peligro de que el receptor acepte el mismo marco dos o más veces, y que lo pase a la capa de red muchas veces. Para evitar esto, es necesario asignar un número de secuencia a los marcos de salida, para que el receptor distinga la retransmisión del original.

### 3.4.4. Control de flujo.

Un importante tema de diseño que se presenta en la capa de enlace de datos y también en las capas superiores, es quehacer común transmisor que sistemáticamente quiere trasmitir marcos a mayor velocidad que aquella con que puede aceptarlos el receptor. Esto ocurre cuando el transmisor opera en una computadora rápida y el receptor opera en una máquina lenta. El transmisor envía los marcos a alta velocidad hasta que satura al receptor. Aún así la transmisión está libre de errores, solo que en algún momento el receptor simplemente no será capaz de manejar los marcos que van llegando y comenzará perder algunos.

La solución es introducir un control de flujo para controlar la velocidad del transmisor de manera que no envíe a mayor velocidad que la que puede manejar el receptor. El control de velocidad generalmente requiere mecanismos de realimentación para que el transmisor pueda enterarse si el receptor es capaz de mantener el ritmo o no.

Se conocen varios esquemas de control de flujo, pero la mayoría se basa en el mismo principio, el protocolo tiene reglas bien definidas sobre el momento en que un transmisor puede enviar el siguiente marco. Estas reglas a veces prohíben el envío de marcos hasta que el receptor no lo haya autorizado, implícita o explícitamente.

### 3.4.5. Subcapas de capa de enlace.

El modo de acceso al medio de transmisión es una gran función de la capa de enlace de datos. La mayoría de las arquitecturas de red con referencia en el modelo OSI descomponen la capa de enlace de datos en una subcapa inferior de acceso al medio o MAC

y otra subcapa superior que se encarga del gobierno de la comunicación. Según se vio en el capitulo 2. Las subcapas de la capa 2 son; la subcapa de Control de Acceso al Medio o MAC y la subcapa de Control de Enlace Lógico o LLC según lo muestra la figura 3.2.

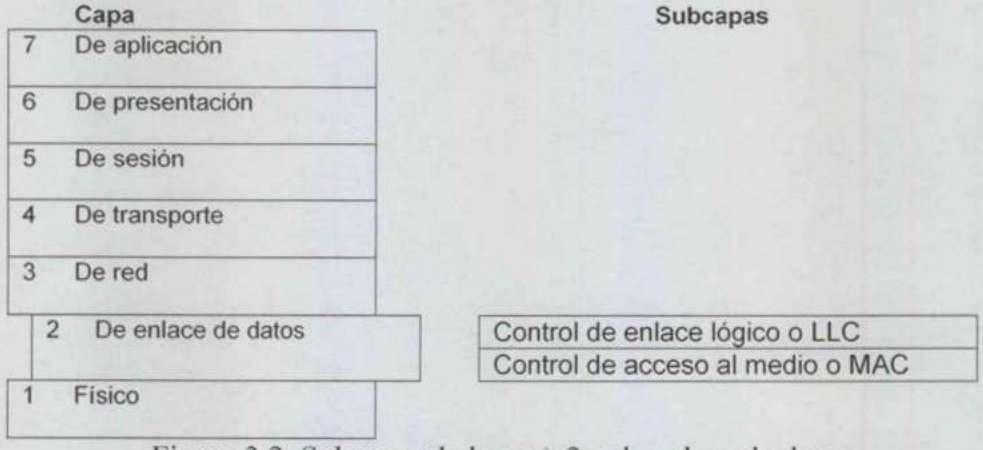



Figura 3.2. Subcapas de la capa 2 o de enlace de datos.

Los principales métodos de acceso al medio que se utilizan en redes LAN son; el CSMA, el paso de toque y la multiplexación en tiempo o en frecuencia.

### *3.4.5.1. La subcapa de control lógico de enlace.*

Antes de continuar es preciso volver atrás y comentar con más detalle algunas especificaciones desarrolladas por el para la capa de enlace de datos del modelo OSI. La especificación divide la capa de enlace de datos en dos capas, LLC y MAC.

La subcapa de Control Lógico de Enlace o LLC 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 también proporciona Puntos de Acceso al Servicio o SAP, que no son más que puntos de referencia a los que otras computadoras que envían información, pueden referirse para comunicarse con las capas superiores del conjunto de protocolos dentro de un determinado nodo receptor.

La subcapa de Control de Acceso al Medio o MAC determina la forma en que las computadoras se comunican dentro de la red, y cómo y donde una computadora puede acceder, de hecho, al entorno físico del que enviaron datos. La especificación 802 divide a su vez la subcapa MAC en una serie de categorías, directamente relacionados con la arquitectura específica de la red, como *Ethernet* y *Token Ring*.

### *3.4.5.2. La subcapa de acceso al medio.*

Algunas redes tienen un solo canal que se usa para todas las comunicaciones. En estas redes, el aspecto clave del diseño es el reparto del canal entre las estaciones competidoras que desean usarlo. Se han desarrollado muchos algoritmos de reparto de canal.

Los métodos de reparto más sencillo son la Multiplexión por División en Frecuencia o FDM y la Multiplexión por División en Tiempo o TDM; son eficientes con un número de estaciones pequeño y tráfico continuo. Ambos se usan ampliamente en circunstancias como dividir el ancho de banda de los enlaces satelitales usados como troncales telefónicas.

Con un número grande y variable de estaciones, o con un tráfico de ráfagas, la FDM y la TDM son soluciones pobres. Se ha propuesto como alternativa del protocolo ALOHA, con y sin ranuras y control. El ALOHA y sus muchas variantes y derivaciones han sido ampliamente estudiados, analizados y usados en sistemas reales.

Cuando puede detectarse el estado del canal, las estaciones pueden evitar el comienzo de una transmisión mientras otra estación esta retransmitiendo. Esta técnica, la detección de portadora, ha producido varios protocolos que pueden usarse en redes LAN y MAN.

Se conoce una clase de protocolos que eliminan por completo la contención, o mínimo la reducen grandemente. El conteo descendiente binario elimina por completo la contención. El protocolo de recorrido de árbol la reduce dividiendo dinámicamente las estaciones en 2 grupos separados, uno que puede transmitir y otro que no. Se intenta hacer la división de tal manera que sólo una estación lista para retransmitir pueda hacerlo.

Las LAN inalámbricas tienen sus propios problemas y soluciones. El problema principal lo causan las estaciones ocultas, por lo que el CSMA no funciona. Una clase de soluciones típicas por el MACA, intenta estimular las trasmisiones en las cercanías del destino, para hacer que CSMA funcione mejor. En lo que toca a computadoras móviles y los teléfonos, la tecnología en ascenso es la radio celular. El GSM, CDPD y CDMA se usan ampliamente.

Las LAN IEEE 802 son: CSMA/CD, *token bus y token ring.* Cada una tiene sus propias ventajas, desventajas, y ha encontrado su propia comunidad de usuarios, así que continuará sirviendo esa comunidad durante varios años más.

La convergencia a un solo estándar LAN es poco probable. Una nueva visión a esa familia es DQDB, que se vende como MAN en muchas ciudades.

Una organización con varias LAN con frecuencia las conecta mediante puentes. Cuando un puente conectado dos o más tipos distintos de LAN, sobre nuevos problemas, algunos ellos sin solución.

Algunas LAN 802 son los caballos de batalla del día, los caballos de carrera son las FDDI, el *Ethernet* rápido, HIPPI y el canal de fibra. Todos estos ofrecen anchos de banda del orden de 100 Mbps con más.

Las redes satelitales también emplean canales de acceso múltiple para el enlace ascendente. Se usan varios métodos de reparto de canal, incluidos ALOHA, FDM, TDM y CDMA.

## 3.5. PROTOCOLOS PARA TRANSMISIÓN DE DATOS.

Las funciones básicas que ha de realizar cualquier protocolo son las siguientes:

- Establecimiento del enlace; punto de origen y destino.
- Transmisión de la información y control de flujos.
- Detección de fallos en la transmisión.
- Corrección de errores.

### 3.5.1. Protocolos elementales de enlace.

La capa de enlace recibe la Unidad de Datos del Servicio o SDU de la capa de red, la fragmenta, le añade Información de Control de Protocolo o PCI y la envía a la capa física; también en el otro sentido, recibe los fragmentos de la capa física y si llegan desordenadas se encarga de reordenarlos, elimina la Información de Control de Protocolo y envía la información a la capa de red.

Los protocolos de esta capa se pueden clasificar en:

- *Por un lado los orientados a carácter*, que tienen su información agrupada en bloques y transmiten caracteres BSC (IBM), BDCMP (ISO).
- *Por otro lado los orientados a bits*, donde la unidad de datos es *bit*, HDLC, SDLC.

### 3.5.2. Control de flujos.

Los protocolos de la capa de enlace se encargan de adecuar las velocidades de intercambios de datos entre emisor y receptor, de manera que se consiga una alta eficiencia en la transferencia, ajustándola a la capacidad de los Buffer de memoria o a otras características de los equipos que se comunican, para que no se pierda la información.

Existen tres grandes familias de protocolos, clasificados en función de cómo realizan esta función de control de flujo son:

- Protocolos *hardware / software HW / SW.*
- Protocolos Reenvió.
- Protocolos de ventana corrediza.

#### *3.5.2.1. Protocolos hardware/software.*

El control de flujos de comunicación entre dispositivos se realiza tanto con protocolos *hardware* como *software*. El ejemplo mas sencillo de protocolo *hardware* es el protocolo DTR/DSR, donde la línea TD y RD solo envían información de usuario cuando el estado de circuitos de control lo permite, siempre de acuerdo con las especificaciones del protocolo.

Otra manera, igual de sencilla es mediante las señales *software* XON y XOFF, dos caracteres de control del código ASCII que se envían por la línea de comunicación TD / RD del Interface. Con XON el receptor indica el emisor que se encuentra en disposición de recibir información y con XOFF que no lo está, este último debe esperar a recibir un XON para proceder de nuevo con la transmisión de nueva información.

Estos dos protocolos, por su sencillez, se usan ampliamente en comunicaciones serie entre PC, utilizando un Modem o un cable eliminador de Modem. Situaciones más complejas se requieren protocolos algo más sofisticados.

#### *3.5.2.2. Protocolos de reenvió.*

Los protocolos de este tipo basan su eficacia en solicitar la retransmisión automática de las tramas cuando detectan que se produjo la pérdida de una de ellas, precisamente por ello se denominan ARQ.

Los métodos de envío y espera o envío continuo no son más que dos modos distintos de las técnicas ARQ. Estos protocolos se usan en comunicación no muy sofisticada, básicamente entre PC's siendo alguno de ellos el X MODEM, Z MODEM, KERMIT, entre otros.

#### *3.5.2.3. Protocolos de ventana deslizante.*

El concepto que utiliza esta familia de protocolos consiste en enumerar las tramas y enviar un grupo de ellos antes de esperar a recibir una confirmación. Tanto el emisor como el receptor tienen un determinado tamaño de ventana que es variable para el emisor pero fijo para el receptor; este tamaño indica el número de tramas que pueden tener en el *Buffer*, y el receptor va confirmando al emisor los números de secuencia de las tramas conforme le llega. Si en un momento dado el receptor no puede aceptar una trama por falta de capacidad la rechaza y como el emisor nunca recibe confirmación de ella, una vez vencidos los tiempos de espera la vuelve a enviar.

En este tipo de protocolos, para ventanas de tamaño mayor a 1 las confirmaciones pueden ser trama a trama o por grupo de ellas, al igual que sucede con las retransmisiones. Este tipo de protocolos se utiliza en transmisiones que llevan una mayor complejidad como las que suceden entre una computadora central y varios terminales distribuidos. Ejemplo típico de protocolo perteneciente a esta familia es el HDLC, que sirve de base para muchos otros.

## 3.6. PROTOCOLOS DE ENLACE DE DATOS.

Los protocolos de enlace de datos son usados generalmente en todas las redes, pero existen distintas orientaciones, los orientados a carácter y los orientados a *bits*.

Respecto de los orientados a carácter es importante recordar que; en inicio la organización ISO empezó a estudiar los protocolos de enlace muy pronto, para garantizar su compatibilidad entre los distintos fabricantes, pero ante su tardanza en lograr resultados, algunos fabricantes se adelantaron, como fue IBM con su BSC.

En los orientados a *bits* se hace mención de varios protocolos enlace de datos de amplio uso. El primero, HDLC, es común en X.25 y muchas otras redes. Después, se mencionaran protocolos de enlace de datos usados en Internet y en las redes de redes ATM tiene respectivamente.

### 3.6.1. Protocolos orientados a carácter.

Su desarrollo comenzó en la década de los 60, cuando se empezaron a utilizar las comunicaciones de datos a través de redes públicas de telecomunicaciones. Estos protocolos aún se siguen utilizando, a pesar de que, en muchos casos, los orientados a *bits* son más potentes.

#### *3.6.1.1. Protocolo BSC.*

Uno de los protocolos mas usados por la industria es el Comunicación Binaria Sincronía o BSC o BISYNC. Es un protocolo orientado a carácter, semiduplex, aunque en muchas ocasiones el medio de transmisión sea duplex. Puede ser usado tanto en circuitos punto a punto como multipunto, bien con enlaces permanentes o en de la red telefónica conmutada.

Es necesario que el emisor y el receptor estén perfectamente sincronizados, para que este último pueda identificar correctamente cada uno de los caracteres. Para ello, inicialmente se envía 1 o más caracteres específicos de sincronización, denominados SINC o SYN que permiten la correcta interpretación de los caracteres sucesivos.

Un caso muy particular en el protocolo es que se quiera enviar información que no represente caracteres, tal es el caso de enviar un programa, en este caso algunas de las combinaciones de ceros y unos pueden coincidir con los caracteres de control y ser mal interpretados. En este caso se contempla el envío en modo transparente, consistente en preceder cada carácter verdadero de control por el carácter DLE.

Los caracteres de control utilizados por este protocolo son algunos de los que contempla el código ASCII, para delimitación de bloques; SYN, SOH, STX, ETX, y ETB, para controlar el diálogo entre las estaciones; EOT, ENQ, ACK, NAK) y para la Transmisión en Modo Transparente o DLE.

Para el control de errores se utilizan los métodos de paridad simple, paridad horizontal - vertical y CRC. Para controlar la posible pérdida de tramas, BSC utiliza los caracteres de confirmación de trama ACK 0 y ACK 1, uno para las tramas pares y el otro para las impares.

El carácter SOH habré la trama, el campo cabecera va encerrado entre un SOH y un STX. Este campo no está definido por el protocolo, depende de la red en la que se esté utilizando. Posteriormente viene el campo de datos del usuario, que acaba con un ETB si es final de bloque pero no el último bloque de la transmisión y ETX si ya se envió el último bloque. La trama termina con un campo de control de errores del tipo CRC.

### 3.6.2. Protocolos orientados a *bits*.

Hay grupos de protocolos íntimamente relacionados que, a pesar de ser viejos, se siguen utilizando en redes de todo el mundo. Todas se derivan del protocolo de enlace de datos usado en la SNA, llamado Protocolo de Control Sincrónico de Enlace de Datos o SDLC. Tras desarrollar SDLC, IBM los sometió a ANSI y a ISO para su recepción como estándar de EEUU e internacional, respectivamente. ANSI lo modifico convirtiendo lo que en Procedimiento Avanzado de Control de Comunicación de Datos o ADCCP, e ISO lo modificó para convertirlo en Control de Enlace de Datos de Alto Nivelo o HDLC. Luego, el CCITT adoptó y modificó HDLC para su Procedimiento de Acceso de Enlace como parte del estándar de interfaz de red, pero después lo modificó nuevamente a LAPB para hacerlo más compatible con la versión posterior de HDLC. Lo agradable de los estándares es que hay tantos donde escoger.

Todos los protocolo se basan el mismo principio todos están orientados a *bits* y usan el relleno de *bits* para lograr la transparencia de los datos; difieren sólo en aspectos menores aunque irritantes. El análisis de protocolos orientados a *bits* que se hace es solo una introducción general. Si desea los detalles específicos de porque protocolo consulte la definición adecuada. La línea toros protocolos orientados a *bits* usan la estructura marco mostrada en la figura 3.3.

| Bits | 8 | 8 | 8 | 0 | 16 | 8 |
|---|---|---|---|---|---|---|
| | 01111110 | Dirección | Control | Datos | Suma de Comprobación | 01111110 |

Figura 3.3. Formato de marco para protocolos orientados a *bits*.

- El campo dirección es de importancia primordial en las líneas con múltiples terminales pues sirve para identificar una de las terminales. Es el líneas punto a punto a veces se usa para distinguir los comandos de las respuestas.

- El campo de control se usa para números de secuencia, cursos y otros propósitos.
- El campo de datos puede contener información arbitraria; puede ser de longitud arbitraria, aunque la exigencia de la suma de comprobación decae al aumentar el tamaño del marco, debido la mayor probabilidad de múltiples errores.
- El campo de suma de comprobación es una variación menor del bien conocido código de preguntarse cíclica. La variación consiste en permitir la detección detalles de indicación perdidos. Hay tres tipos de marcos: información, de supervisión y no numerados.

### *3.6.2.1. Protocolos HDLC / SDLC.*

Conforme se fue ampliando el uso de terminales interactivos y la oferta de enlaces duplex, se presentó la necesidad de desarrollar nuevos protocolos para rentabilizar el uso de los medios disponibles. Básicamente, las necesidades eran las siguientes:

- Poder transmitir en ambos sentidos simultáneamente.
- Protocolo válido tanto para Red Telefónica Conmutada o RTC semi-duplex y multipunto como para líneas punto a punto y duplex.
- Posibilidad de varios mensajes en el mismo canal.
- Un potente y fiable método de detección y corrección de errores.

Esta última necesidad es la más difícil de conseguir, puesto que se puede dar el caso de que un mensaje erróneo aparezca como bueno. Todos los esfuerzos se dedicaron a conseguir la máxima eficiencia en la detección de errores, pues existen aplicaciones tales como las militares o las bancarias en las que es imprescindible conseguir una correcta transmisión y tener la certeza absoluta de que ha sido así.

*HDLC.* En oposición al protocolo BSC, donde el control se desarrolla a capa de caracteres en el Control de Enlace de Datos de Alto Nivel o HDLC, el control se realiza a capa de *bits*, por eso a este tipo de protocolos se le conoce como Protocolo Orientado a *Bit* o BOP.

*SDLC.* El protocolo SDLC, usado dentro del entorno de IBM, es equivalente al HDLC, pero con algunas excepciones: el campo de información debe ser multiplo de 8 *bits*, y contiene comandos adicionales.

Puesto que este protocolo puede dar confirmación a varias tramas simultáneamente, y además, por ser duplex, consigue una alta eficiencia en la utilización de la línea, obtiene lo que el usuario requiere. A esto se debe la gran difusión que tiene, y su aceptación por otros fabricantes de ordenadores y terminales, convirtiéndose en un estándar internacional. El formato de las tramas es similar a las del protocolo HDLC.

# CAPITULO 4. LA CAPA DE RED Y LOS PROTOCOLOS DE RUTEO.

## 4.1. INTRODUCCION A LOS PROTOCOLOS DE RUTEO.

Habrá que recordar que la capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y ruteo de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.

### 4.1.1. Funciones principales.

Sus principales funciones son:

- Dividir los mensajes de la capa de transporte en unidades más complejas, denominadas paquetes, a los que asigna las direcciones lógicas de los *host* que se están comunicando.
- Conocer la topología de la red y manejar el caso en que la máquina origen y la máquina destino estén en redes distintas.
- Rutear la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y ruteo a través de dispositivos intermedios ruteadores.
- Enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas.
- Ensamblar los paquetes en el *host* destino.
- En esta capa es donde trabajan los ruteadores, dispositivos encargados de rutear o dirigir los paquetes de datos desde el *host* origen hasta el *host* destino a través de la mejor ruta posible entre ellos.

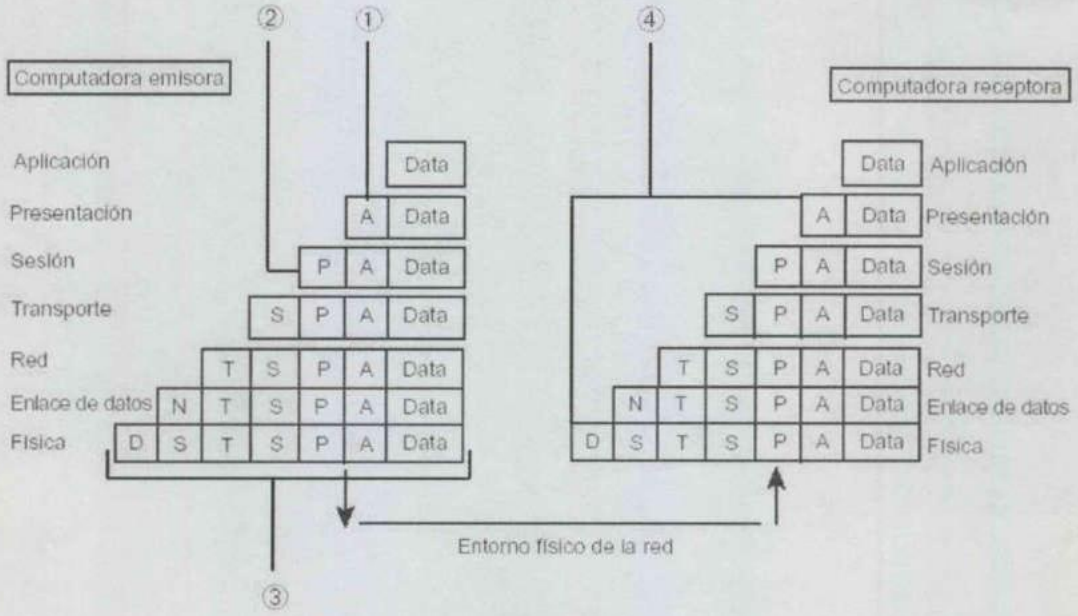
## 4.2. LA CAPA DE RED.

En modelo OSI divide en siete capas el proceso de transmisión de la información entre equipos informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global. Este marco de trabajo estructurado en capas, aun siendo puramente conceptual, puede utilizarse para describir y explicar el conjunto protocolos reales que, como se ve, se utilizan para la conexión de sistemas.

Por ejemplo, TCP/IP y Apple-Talk son dos de las pilas de protocolos que se utilizan en el mundo real para transmitir datos; los protocolos que, de hecho, sirven como capas o niveles dentro de un conjunto de protocolos como pueden, por tanto, explicarse de acuerdo con correlación con el modelo teórico de capas o niveles de redes que conforman.

### 4.2.1. Pila de protocolos.

Las pilas o *suite* o capas de protocolos no son más que una jerarquía de pequeños protocolos que trabajaban juntos para llegar a cabo la transmisión de datos de un nodo a otro de la red, ver la figura 4.1.




1. Encabezado de la capa de aplicación.
2. Encabezado de la capa de presentación.
3. Paquete con todos los encabezados de las capas OSI.
4. Los encabezados se van suprimiendo a medida que los datos suben por la capa OSI.

Figura 4.1. Pila de protocolos.

Las pilas de protocolos se asemejan mucho las carreras de relevos, pero, en vez pararse en un toque, se transmiten paquetes de datos de un protocolo a otro hasta que estos tienen la forma adecuada; una secuencia única de *bits*, para trasmitirse por el entorno físico de la red.

Los datos bajan por la pila OSI de la computadora emisora y suben por la pila OSI de la computadora receptora.

Aunque los administradores de red están familiarizados con pilas de protocolos de red como IPX/SPX o TCP/IP, muchos desconocen la existencia de la pila de protocolos basada en el modelo OSI, denominada pila de protocolos OSI. Por desgracia, los sistemas operativos de red mas utilizados como Novell o Windows NT no la soportan.

### 4.2.2. Protocolos de red del mundo real.

Después de repasar el modelo teórico que determina la forma en que los datos van de una computadora a otra dentro de una red, pasando por las distintas capas que conforman el modelo OSI, se pueden explicar algunos de los conjuntos de protocolos de red mas utilizados hoy en día y cotejar las capas que los integran con las del modelo OSI. De esta forma, se logra una visión clara y sencilla del modo en que operan estas pilas de protocolos reales y la forma en que transportan los datos por la red.

También es importante ver que protocolos de un determinado grupo participan en la capa de red del modelo OSI. Estos protocolos con de suma importancia ya que contribuyen a rutear los paquetes en una conexión entre redes.

#### *4.2.2.1. NetBEUI.*

Es un protocolo de red rápido y sencillo que fue diseñado para ser usado junto con el protocolo NetBIOS desarrollado para redes pequeñas. NetBEUI opera en las capas de transporte y red del modelo OSI. Puesto que NetBEUI solo proporciona los servicios requeridos en las capas de transporte y red de OSI, necesita funcionar con NetBIOS que opera la capa de sesión de OSI, y se encarga de establecer la sesión de comunicación entre las dos computadoras conectadas a la red. Las redes Microsoft además incluyen dos componentes; el redirector y el Boque de Mensajes del Servidor o SMB.

Aunque resulta un excelente protocolo de transporte de bajo costo, NetBEUI no es un protocolo que pueda rutarse por medio de ruteadores o *routers*, por lo que no puede utilizarse en interconexiones de redes. Por tanto, si bien NetBEUI es una opción de protocolo de red para redes pequeñas y sencillas, no resulta valida para redes más amplias que requieren el uso de ruteadores (por lo que dejara de tratarse en este documento).

### *4.2.2.2. TCP/IP.*

TCP/IP se ha convertido en el estándar por *default* para la conexión en red corporativa. Las redes TCP/IP son ampliamente escalables, por que TCP/IP puede usarse tanto para redes pequeñas como grandes.

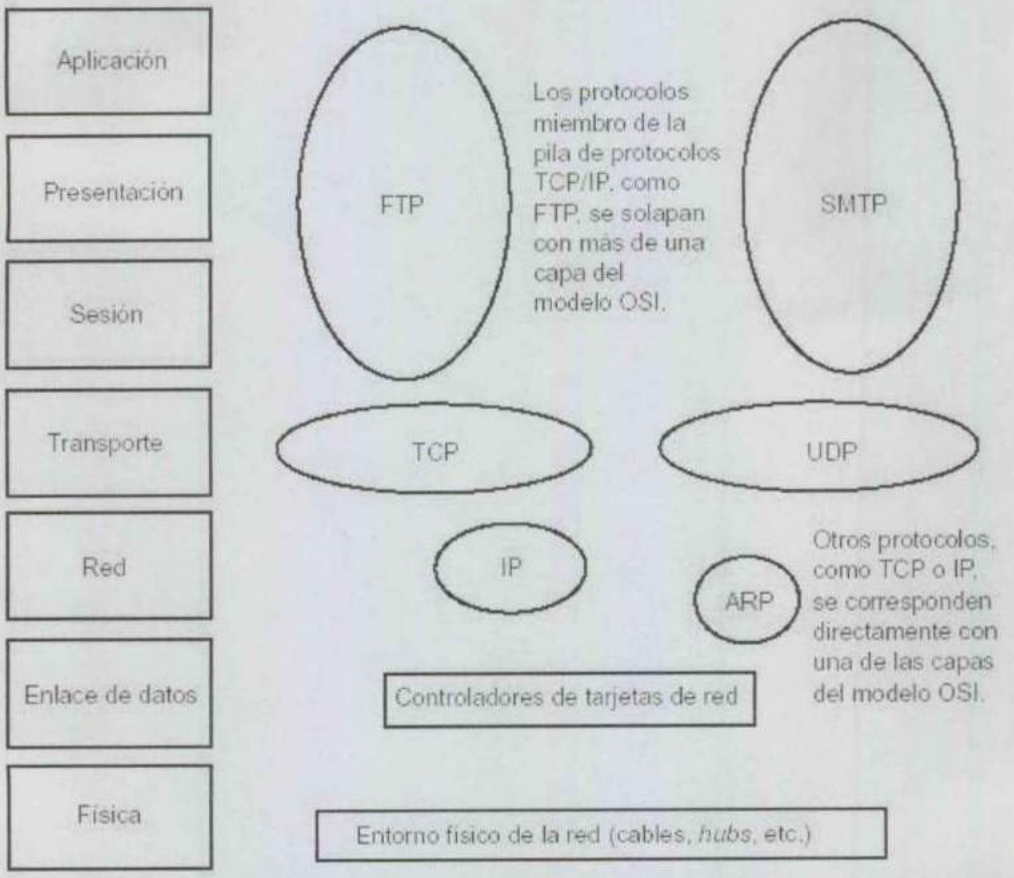



Figura 4.2. TCP/IP es un amplio conjunto de protocolos que utiliza una serie de protocolos miembro en varias de las capas del modelo OSI.

TCP/IP como se ha visto es un conjunto de protocolos encaminados que puede ejecutarse en distintas plataformas de software como son Windows UNIX, por mencionar algunos Casi todos los SO de red lo soportan como protocolo de red predeterminado.

TCP/IP consta de una serie de protocolos que componen la pila TCP/IP. Y puesto que el conjunto de protocolos TCP/IP se desarrollo antes de que terminara de desarrollarse OSI, los protocolos que lo conforman no se corresponden perfectamente con las capas del modelo.

La figura 4.2, muestra la correlación entre el conjunto de protocolos TCP/IP y las capas OSI, la figura 4.2, ofrece una descripción general de TCP/IP y no los protocolos que incluye. Los protocolos que aparecen en la figura 4.2, se describen a en la figura 4.3.

| Protocolo | Función |
|---|---|
| **FTP.** | *Protocolo de Transferencia de Archivos*, proporciona una interfaz y servicios para la transferencia de archivos en la red. |
| **SMTP.** | *Protocolo Simple de Transferencia de Correo*, proporciona servicios se correo electrónico las redes Internet e IP. |
| **TCP.** | *Protocolo de Control de Transporte*, es un protocolo de transporte orientado a la conexión. Gestiona la conexión entre las computadoras emisora receptora de forma parecida al desarrollo de llamadas telefónicas. |
| **UDP.** | *Protocolo de Datagrama de Usuario*, es un protocolo de transporte sin conexión que proporciona servicios en colaboración con TCP. |
| **IP.** | *Protocolo Internet* es la base para todo el direccionamiento que se produce en las redes TCP/IP se proporcionan protocolo orientado la capa de red sin conexión. Funciona de forma semejante a una carta con remite echada al buzón y después entregada su destinatario. |
| **ARP** | *Protocolo de Resolución de Direcciones* hace corresponder las direcciones IP con las direcciones MAC de hardware. |

Figura 4.3. Protocolos miembro de la pila TCP/IP.

TCP/IP proporciona un ancho conjunto de características referidas a la conexión en red, además un sistema de direccionamiento lógico y único. Cualquier usuario conectado a Internet esta familiarizado con las direcciones IP de 32 *bits*. Que se escriben en 4 *bytes* u octetos, 1 octeto vale por 8 *bits* de información. El formato dirección es tipo 129.30.20.4, donde cada valor decimal de los 4 separados por puntos vale 8 *bits* de información binaria.

Dada la importancia de TCP/IP en las conexiones entre redes y la complejidad que implica rutear redes TCP/IP, trataría un documento entero explicar y repasar los aspectos del direccionamiento TCP/IP. Al igual que los comandos referidos al ruteo TCP/IP en redes de campus y corporativas, por tanto la información al respecto solo da un panorama global.

### *4.2.2.3. IPX/SPX.*

Protocolo de red de Novell, agrupa menos protocolos que TCP/IP, por tanto no requiere la carga general que TCP/IP necesita. IPX/SPX se usa tanto en redes pequeñas como grandes y también permite el ruteo de datos.

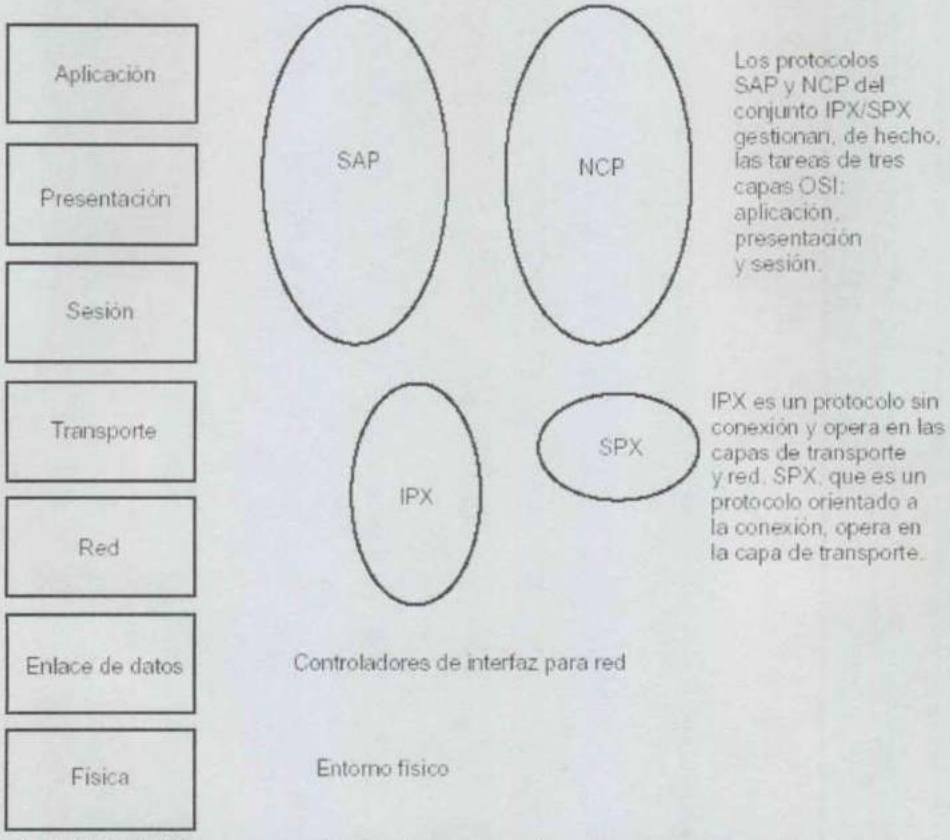



Figura 4.4. IPX/SPX es un conjunto de protocolos eficaz que se utiliza tanto en redes grandes como pequeñas.

| Protocolo | Función |
|---|---|
| **SAP** | *Protocolo de Anuncio de Servicio*, revisa los servidores de archivos y los servidores de impresora de NetWare para anunciar la dirección del servidor. |
| **NCP** | *Protocolo del Núcleo NerWare*, gestiona las funciones de red en las capas de aplicación, presentación y sesión. Gestiona además la creación de paquetes y se encarga de proporcionar servicios de conexión entre los clientes y servidores. |
| **SPX** | *Protocolo de Intercambio Secuenciado de Paquetes* es un protocolo de transporte orientado a la conexión. |
| **IPX.** | *Protocolo de Intercambio de Paquetes entre Redes* es un protocolo de transporte sin conexión que gestiona el de direccionamiento y ruteo de los datos en la red. |

Figura 4.5. Protocolos miembro de la pila IPX/SPX.

La figura 4.4, ofrece una correlación entre la pila IPX/SPX y las capas del modelo OSI. La figura 4.5, describe brevemente cada uno de los protocolos que lo componen. Lo que más nos interesa acerca de IPX/SPX es la forma en que deben rutearse este conjunto protocolos dentro de una conexión entre redes. Se vera el ruteo de IPX/SPX después.

### *4.2.2.4. AppleTalk.*

Aunque muchos administradores de red no consideran *AppleTalk* un protocolo de red corporativo o de interconexión, *AppleTalk* permite el ruteo de datos mediante ruteadores. De hecho, con el tipo apropiado de NIC *AppleTalk* puede soportar arquitecturas *Ethernet, Token Ring y* FDDI. Las computadoras Macintosh suelen utilizarse en los entornos empresariales para la manipulación de gráficos y otras tareas de tipo multimedia, por lo que no resulta ilógico incluir *AppleTalk* como otro protocolo ruteado en la red corporativa.

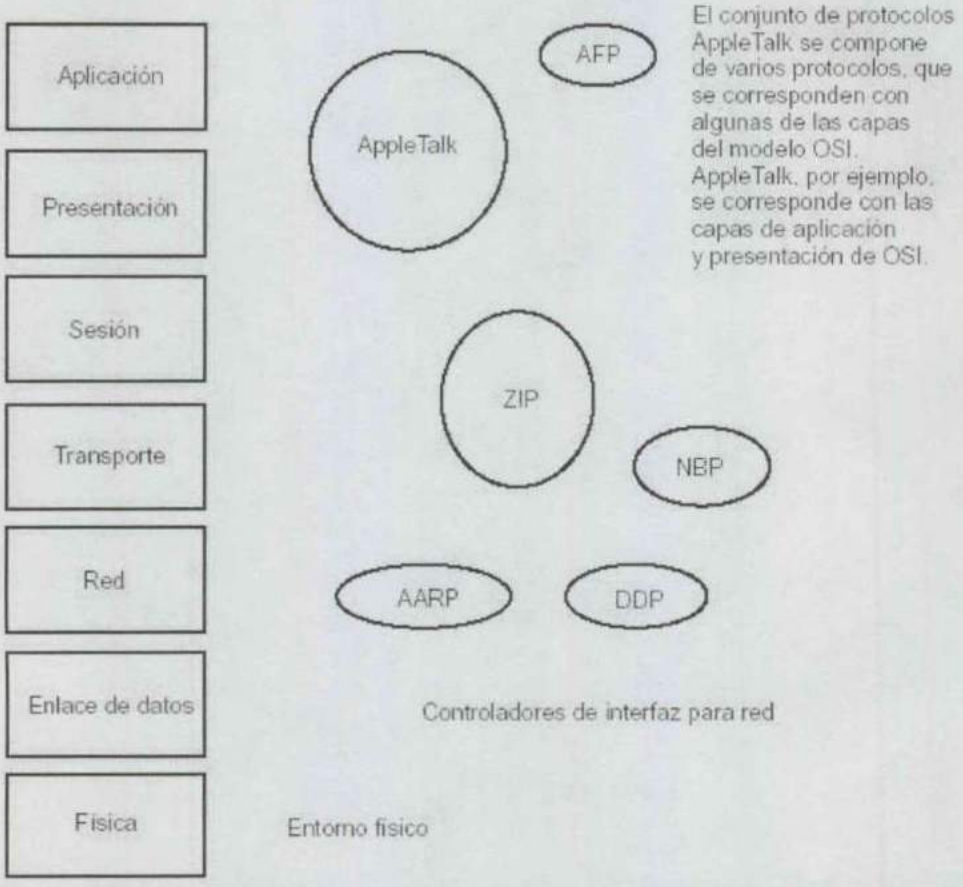



Figura 4.6. AppleTalk es un conjunto de protocolos encaminados para redes Macintosh que pueden comunicarse con redes *Ethernet, Token Ring* y FDDI.

En el capitulo 2 se vio AppleTalk como arquitectura de red, e indudablemente también es un conjunto de protocolos. La figura 4.6, da la correlación entre los protocolos que integra *AppleTalk* y las capas OSI. La figura 4.7, describe en breve cada uno de estos protocolos.

| Protocolo | Función |
|---|---|
| **AppleShare** | Proporciona servicios en la capa de aplicación |
| **AFP** | *Protocolo de Archivo AppleTalk*, proporciona y gestiona la competición de archivos entre modos de una red. |
| **ATP** | *Protocolo de Transacción AppleTalk*, proporciona la conexión de capa de transporte entre computadoras |
| **NBP** | *Protocolo de Enlace de Nombre*, hace corresponder los nombres de servidores de red con las elecciones de la capa de red. |
| **ZIP** | *Protocolo de Información de Zona*, controlar las zonas *AppleTalk* y hace corresponder los nombres de zonas con las direcciones de red. |
| **AARP** | *Protocolo de Resolución de Direcciones AppleTalk*, hace corresponder las direcciones de la capa de red con las direcciones de hardware de enlace de datos. |
| **DDP** | *Protocolo de Entrega de Datagramas*, proporciona el sistema de direccionamiento para la red AppleTalk, así como el transporte sin conexión de los datagramas entre las distintas computadoras. |

Figura 4.7. Protocolos miembro de AppleTalk.

Nuestro interés en el conjunto de protocolos de red AppleTalk se centra en el modo en que *AppleTalk* encamina los datos por medio de ruteadores. La configuración de redes *AppleTalk* y la forma en que este conjunto de protocolos viene encaminado por un ruteador de Cisco se trata después.

Las figuras 4.2, 4.4, y 4.6 presentan correlaciones entre protocolos reales y el modelo OSI. Para entender estas figuras, debe tenerse en cuenta la forma en que las 7 capas de OSI convierten y transmiten datos entre dos computadoras conectadas en red.

Los conjunto de protocolos del mundo real, como TCP/IP, ejecutan también todas las tareas que describe el modelo teórico, pero usando menos protocolos que el modelo OSI. En vez de tener 7 protocolos, incorpora varios protocolos que gestionan a un tiempo las tareas de varias capas OSI. Por ejemplo, FTP gestiona las tareas de las capas de aplicación, presentación y sesión, de ahí que el círculo de FTP en la figura 4.2, englobe las tres capas del modelo OSI.

### 4.2.3. Protocolos de ruteo o encaminamiento.

Seguramente habrá reparado en que muchas de las figuras muestran la correlación entre conjuntos de protocolos y las capas de modelo OSI no incluían protocolos de ruteo. Obviamente, cada conjunto protocolos cuenta con un protocolo de ruteo predeterminado; por ejemplo, RIP es el protocolo predeterminado de TCP/IP y el Protocolo de Mantenimiento de la Tabla es el que utiliza por *default* AppleTalk. Esos protocolos se tratan en el ruteo de datos.

## 4.3. RUTEO.

Una computadora sola, sin conexión con ningún otro, es una isla de información y de recursos que no es rentable, y más cuando para el trabajo diario donde se necesita recurrir a diferentes fuentes de datos.

Cuando se dieron cuenta las empresas, solicitaron a las compañías de desarrollo de *hardware* y *software* un medio compartido de trabajo, en el que diferentes estaciones de trabajo, servidores e impresoras pudieran comunicarse entre ellos y compartir recursos. De este modo surgieron las primeras redes.

### 4.3.1. Ruteadores y la comunicación entre redes.

Una red está formada por una serie de estaciones de trabajo unidas entre sí por medios de transmisión físicos, redes cableadas o basados en ondas, redes inalámbricas; coordinados por unas máquinas especiales, servidores; y por un conjunto variable de dispositivos de trabajo, como impresoras o escáneres. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los ruteadores o *routers*, conmutadores o *switches* y concentradores o *hubs*.

#### *4.3.1.1. Paquetes de datos.*

Cuando un *host* desea enviar una serie de datos a otro, estos son convertidos a un formato de red apropiado, capa de Aplicación; y divididos en una serie de unidades, denominadas segmentos, capa de Transporte; que son numerados para su correcto reensamble en la máquina destino.

Posteriormente, son pasados a la capa de Internet, que les coloca las direcciones IP de la máquina origen y de la máquina destino. Las unidades así obtenidas se conocen con el nombre de paquetes. Entonces son pasados a la capa de Enlace de Datos, que les añade las direcciones MAC de ambas máquinas y un número calculado para la verificación posterior de errores en el envío, pasando entonces a denominarse tramas.

Por último, las tramas son pasadas a la capa Física que las une en trenes de *bits* apropiados para su transformación en impulsos eléctricos o en ondas, que posteriormente son enviados al medio. Cuando los impulsos llegan a la máquina destino el proceso se invierte, obteniendo la aplicación receptora los datos en su formato original.

A pesar de que lo que se transmite por el medio físico son impulsos eléctricos, se suele hablar de paquetes transmitidos, ya que son las unidades de información con entidad propia.

#### *4.3.1.2. Comunicación en una red.*

Imagine que una red formada por varios *host*, como la muestra la figura 4.8. Si el *host* A IP: 210.23.5.14, es el origen; se desea comunicar con el *host* C IP:210.23.5.27, es el destinatario; construye sus paquetes de datos y la capa de Internet les coloca su dirección IP del origen y la de destino, pasándolos a la capa de Enlace de Datos, que no sabe la dirección MAC de C. Para averiguarla, envía un mensaje a todas las máquinas de la red, conocido como petición ARP, preguntando cuál es la dirección MAC correspondiente a la IP 210.23.5.27. Las peticiones ARP son de tipo *broadcast*, es decir, peticiones que son enviadas a todos y cada uno de los equipos en la red

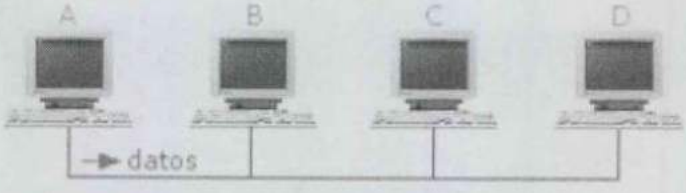



Figura 4.8. Ejemplo de comunicación en una red.

La pregunta llega a todas las máquinas, pero sólo C contesta, enviando una respuesta con su dirección MAC. Entonces, A añade ambas direcciones MAC a los paquetes y los pasa a la capa física, que lo transmite al medio.

### *4.3.1.3. Comunicación entre dos redes.*

Ahora el mismo caso pero el *host* C IP:190.200.23.5; no se encuentra en la misma red que A IP: 210.23.5.14. Cuando éste envíe el *broadcast* preguntando la dirección MAC de C nadie le responderá, por lo que, si no se hace nada al respecto, la comunicación entre ambas máquinas resultará imposible.

Los encargados de solucionar este problema son unos dispositivos de red especiales, llamados ruteadores, que conectan dos o más redes, sirviendo de enlace entre ellas. Los ruteadores trabajan en la capa de Internet, encargándose de encaminar o rutear paquetes de datos entre máquinas de redes diferentes.

Para poder funcionar de esta forma deben pertenecer a cada una de las redes que conectan, como si fueran un *host* más de las mismas. De esta forma, un ruteador que conecte dos redes debe tener una tarjeta de red diferente para cada una de las redes y, consecuentemente, dos direcciones MAC diferentes. También debe tener asignada una dirección IP en cada una de las dos redes, ya que si no sería imposible la comunicación con las máquinas de las mismas. El esquema de dos redes conectadas por un ruteador puede representarse en la figura 4.9.

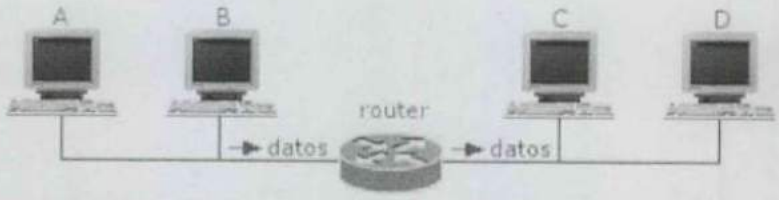



Figura 4.9. Ejemplo de comunicación entre dos redes.

Cuando un *host* envía una petición ARP para averiguar la dirección MAC correspondiente a una IP dada, no responde ningún equipo de su red, envía los paquetes correspondientes a un ruteador que esta configurado para estos envíos, denominado *gateway* por *default*.

Cuando el ruteador recibe los paquetes de datos usa un parámetro especial, denominado máscara de red, que sumado lógicamente a la dirección IP destino, le da la red a la que pertenece el *host* buscado. Pasa entonces los paquetes a la red a la que pertenece C, haciendo una nueva petición de *broadcast* preguntando la MAC de C. Este le responde, y entonces el ruteador le envía los paquetes directamente. Si C desea responder a A, el proceso se invierte.

Este proceso es necesario realizarlo sólo una vez, ya que en esta tanto los *host* A y C como el ruteador anotan las parejas de direcciones MAC-IP en unas tablas especiales, denominadas tablas de ruteo, que usan en envíos de datos posteriores para rutear los paquetes directamente.

Resumiendo, los ruteadores son los principales responsables de la correcta comunicación entre máquinas de diferentes redes, se encargan en este proceso de rutear correctamente los paquetes de datos.

## 4.4. RUTEADORES.

Los ruteadores son dispositivos de red que raramente se encuentran aislados entre sí. Al contrario, suelen estar interconectados, formando una especie de telaraña que hace posible el tráfico de datos entre redes separadas físicamente.

### 4.4.1. Funcionamiento de un ruteador.

Tomando de ejemplo Internet, cuando una máquina envía una serie de paquetes de datos a otra situada en otra ciudad o país, estos son encaminados de ruteador a ruteador a lo largo del camino entre ambas máquinas. Cada paso de un paquete de un ruteador a otro se denomina salto; y el principal objetivo de todos y cada uno de los ruteadores que intervienen en la transferencia del paquete es que éste llegue a su destino en el menor número de saltos posible, por la mejor ruta posible.

Para realizar esta tarea, los ruteadores se comunican constantemente entre sí, informándose de las rutas bloqueadas, de las máquinas intermedias que se encuentran caídas o saturadas de tráfico, aprendiendo así cuál es el ruteador idóneo para enviarle los paquetes recibidos.

Si se considera ahora el caso de un ruteador segmentando una red LAN, aunque ahora no debe enviar los paquetes a otro ruteador, sí que debe saber por qué puerto debe enviar los datos para que lleguen a la máquina local destino. Esta habilidad de saber a dónde tienen que enviar los paquetes de datos que reciben la consiguen almacenando en su interior una tabla especial, conocida como tabla de ruteo, en la que van anotando las direcciones IP de las máquinas que se comunican con él y el puerto por el que está accesible esa máquina.

#### *4.4.1.1. Tabla de ruteo.*

Cuando a un ruteador llega un paquete, mira en su tabla de ruteo. Si está en ella referenciada la dirección IP de la máquina destino, también lo estará el puerto por el que ésta es accesible, con lo que envía por él el paquete. En caso de no estar la IP en la tabla, manda una petición de respuesta por todos los puertos, preguntando en cuál de ellos se encuentra la máquina destino, y una vez obtenido el puerto de acceso, ingresa la nueva pareja IP/PUERTO en su tabla de ruteo, con lo que los próximos paquetes para esa máquina los enviará directamente, un ejemplo de tabla de ruteo se ilustra en la figura 4.10.

Se puede buscar una analogía del funcionamiento de los ruteadores con el de las oficinas de correos. Cuando se envía una carta desde Toluca en México, a Monterrey en Nuevo león, ésta llega en primer lugar a la oficina local de Toluca, que la reenvía a la de México, que a su vez la manda a la de Nuevo león, que la remite a la oficina de Monterrey, que hace la entrega. Si la oficina de correos de Nuevo león está cerrada por obras, la de México la enviará a la de Tamaulipas, que la remitirá a la de Ciudad Victoria, que a su vez se encargará de mandarla a Monterrey, haciendo ésta de nuevo la entrega. Cierre la oficina que cierre, siempre se encontrará un camino para entregar la carta.

| Destino | Métrica | Interfase |
|---|---|---|
| 226.50. 102.21 | 0 | Ethernet0 |
| 226.50.102.3 | 0 | Ethernet0 |
| 158.56.24.54 | 5 | S1 |
| 187.51.26.2 | 8 | S0 |

Figura 4.10. Tabla de ruteo simple.

Para evitar mantener en su tabla direcciones IP que hayan quedado obsoletas, cada cierto tiempo borra aquellas que no tienen actividad y las que, tras enviarles paquetes, no han respondido. Esto lo consiguen manteniendo conversaciones entre ellos, en unos lenguajes especiales denominados Protocolos de Ruteo.

### 4.4.2. Componentes básicos de un ruteador.

Básicamente, se puede considerar un ruteador como una computadora especial que funciona solo en las tres primeras capas de la arquitectura TCP/IP, al que se la han

eliminado una serie de componentes físicos y funcionalidades lógicas que no necesita para su trabajo, mientras que se le han añadido otros componentes de *hardware* y de *software* que le ayudan en su trabajo de ruteo.

Como toda computadora, un ruteador necesita un sistema de arranque *bootstrap*, encargado de realizar un chequeo del resto de los componentes antes de pasar el control a un Sistema Operativo o SO (Cisco IOS, en el caso de los ruteadores Cisco).

El sistema de arranque se almacena en una memoria ROM o Memoria de Solo Lectura, junto con una parte básica del SO, la que toma el control al inicio, mientras que el cuerpo principal de éste se almacena en una memoria especial, de tipo *Flash*, que se puede borrar y reprogramar, permitiendo así las actualizaciones necesarias. El contenido de la memoria *Flash* se conserva en caso de cortes de energía o durante los reinicios del ruteador.

Por otra parte, las funcionalidades operativas de los ruteadores son configurables mediante una serie de instrucciones escritas en un fichero de texto, denominado archivo de configuración, que se almacena en un módulo de memoria de tipo RAM No Volátil o NVRAM, cuyo contenido se conserva durante un corte de energía o si se reinicia el equipo.

Una vez inicializado un ruteador, el fichero de configuración es cargado en una memoria RAM o Memoria de Acceso Aleatorio, desde la que se va ejecutando el conjunto de órdenes contenidas en el. También se almacenan en esta memoria las tablas de ruteo, encargadas de almacenar los puertos del ruteador por los que son accesibles las diferentes máquinas.

Por último, el ruteador posee una serie de puertos o interfaces físicas, puntos de conexión del mismo con las diferentes redes a las que está unido, y a través de los cuales se produce la entrada y salida de datos al equipo. El número de interfaces depende del tipo y funcionalidades del ruteador.

### 4.4.3. Tipos de ruteadores.

Los tipos de ruteadores a usar en una red varían dependiendo del tipo de ésta, del número de usuarios y de la función o funciones que deba desempeñar, pudiendo variar mucho la complejidad y el precio de ellos en función del tipo elegido.

- Para segmentar la red en otras subredes, hace falta un *ruteador de segmentación*, con tantos puertos *Ethernet* como subredes se quiera crear, más los de enlace con otros ruteadores; es útil que sobren puertos, para futuras ampliaciones en la red. Cada subred usa luego un concentrador o un conmutador para dar acceso a sus clientes individuales.

- Se puede querer un ancho de banda dedicado para un gran número de equipos individuales, y prescindir de los concentradores. Se necesita entonces un *ruteador de concentración*, que precisa más puertos Ethernet, aunque no necesariamente sean de alta velocidad de transmisión.

- Para conectar una red corporativa a Internet se necesita un *ruteador de frontera*, que actúa como *gateway* de la red interna, recogiendo todos aquellos paquetes de datos destinados a máquinas externas.

- En caso de tener que conectar dos redes WAN o dos segmentos de red en sucursales o campus diferentes, se necesita un *ruteador de backbone*, que suministra transporte óptimo entre nodos de la red, con interfaces de alta velocidad que proveen un elevado ancho de banda. Generalmente basados en tecnología de fibra óptica.

- Por último, también es posible el acceso inalámbrico a redes mediante *ruteadores con tecnología wireless*, un medio práctico de liberar los equipos de las limitaciones de los cables físicos.

## 4.5. PROTOCOLOS DE RUTEO.

Se ha visto antes que los ruteadores mantienen unas tablas de ruteo, en las que van anotando las direcciones IP de las máquinas destino y los puertos adecuados para darles salida de forma óptima.

Los ruteadores suelen hallarse interconectados entre ellos, pasándose paquetes de datos de uno a otro, hasta la máquina destino. Como cada ruteador es solo responsable de las máquinas directamente conectadas a él incluyendo los ruteadores vecinos, se hace necesario un mecanismo que permita a los ruteadores comunicarse entre sí, para evitar que cada uno tenga en sus tablas registros inválidos.

Esto se consigue por medio de una serie de protocolos de ruteo, responsables de que los diferentes ruteadores mantengan sus tablas de ruteo afines, obteniendo una red convergente. Con ello se consigue, por ejemplo, que si una PC o un servidor se apaga en una red, los ruteadores sepan que ya no está accesible, evitando el envío de datos que no llegarán a su destino, y disminuyendo con ello el tráfico de red.

### 4.5.1. Protocolos de comunicación entre ruteadores.

Depende del protocolo de ruteo con que funcione.

- *Ruteo por vector de distancia.* Para mantener las tablas de ruteo actualizadas, un ruteador puede mandar a los ruteadores vecinos una copia de su tabla cada determinado periodo de tiempo.
- *Ruteo por estado de enlace.* Cuando alguna máquina en su red sufre algún cambio.

Existen diferentes protocolos de comunicación entre ruteadores, cada uno de los cuales utiliza mecanismos propios para conseguir la convergencia en la red y para determinar el mejor camino que puede seguir un paquete de datos en su viaje hasta la máquina destino, y cada uno utiliza un sistema de determinación de mejor ruta, es decir una métrica diferente.

### 4.5.2. Protocolos de ruteo según su misión en una red.

Según su misión en una red se puede distinguir dos tipos principales de protocolos de ruteo:

- *Los Protocolos de Gateway Interior o IGP*, encargados de la comunicación entre ruteadores de una misma red, entre los que destacan RIP e IGRP.
- *Los Protocolos de Gateway Exterior o EGP* o de frontera, encargados de la comunicación entre ruteadores de redes diferentes.

### 4.5.3. Principales protocolos de ruteo.

Entre los más importantes protocolos de ruteo se pueden destacar los siguientes:

- RIP.
- IGRP.
- EIGRP.
- OSPF

#### *4.5.3.1. RIP.*

Protocolo de Información de Ruteo o RIP, es un protocolo de ruteo por vector de distancia que calcula las distancias hacia la máquina destino en función de cuántos ruteadores debe atravesar un paquete para llegar a su destino, saltos; enviando cada paquete de datos por el camino que en cada momento muestre una menor distancia. RIP actualiza las tablas de ruteo a intervalos programables, generalmente cada 30 segundos. Es un buen protocolo de ruteo, pero necesita que constantemente se conecten los ruteadores vecinos, generándose con ello una gran cantidad de tráfico de red.

#### *4.5.3.2. IGRP.*

Protocolo de Ruteo de Gateway Interior o IGRP, desarrollado por Cisco System, es un protocolo de ruteo por vector de distancia que usa una métrica compuesta basada en diferentes variables de red, como ancho de banda, Unidades Máximas de Transmisión o MTU, confiabilidad, etc. Envía actualizaciones de las tablas de ruteo cada 90 segundos.

#### *4.5.3.3. EIGRP.*

EIGRP (Protocolo de Ruteo de Gateway Interior Mejorado), protocolo mixto basado en IGRP, basado en una métrica de vector distancia, pero que manda actualizaciones de las entradas de las tablas que han cambiado por haber sido alterado el estado de alguna máquina de su red.

#### *4.5.3.4. OSPF.*

Protocolo Puro de Estado de Enlace o OSPF, que calcula las rutas más cortas y accesibles mediante la construcción de un mapa de la red y el mantenimiento unas bases de datos con información sobre su sistema local y sobre los vecinos. Cuando una máquina de su sistema cambia, se envía esa entrada de la tabla a los ruteadores vecinos.

El protocolo de ruteo a elegir en cada caso depende del tipo de red: LAN, WAN, etc., de su topología y del uso de la misma, siendo posible en la mayoría de los casos configurar varios protocolos en un mismo ruteador.

# CAPITULO 5. PROTOCOLO DE RUTEO HSRP.

## 5.1. INTRODUCCION AL PROTOCOLO DE RUTEO HSRP.

Desde que las redes se popularizaron y se crearon las estructuras de red, se observo la problemática de que cuando un equipo fallaba se paraba el trabajo de la red, de tal manera que surgió la preocupación de tener las redes funcionando a pesar de los fallos que pudiesen ocurrir.

Como bien se sabe, el campo en el que se aplican la redes es tan amplio, que actualmente se utilizan en casi todos los rubros, por ello en este capitulo se hará un fuerte hincapié en las redes de empresa, a fin de que, se aterrice el tema de forma mas clara, en la medida de lo posible.

## 5.2. CUESTIONES IMPORTANTES.

Una vez limitado en un tanto el campo de estudio, es necesario analizar algunos aspectos para adentrarse en el ambiente, empaparse de los aspectos importantes, de tal forma que se hable el mismo lenguaje.

### 5.2.1. Contexto.

El alcance del establecimiento de una red de empresa abarca todas las localizaciones de una red que un negocio utiliza para llegar 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 MAN y la red del campus, y los arquitectos de la red han sido acertados en el abastecimiento de una infraestructura directa para ambos ambientes.

### 5.2.2. Extender el nivel de redundancia.

Uno de los desafíos más grandes que permanece, es extender este nivel de redundancia entre sitios de trabajo y el equipo de la red en el nivel de sesión. El *Cisco Systems* ha dado soluciones end-to-end dentro de interred de trabajo y, con la disponibilidad del protocolo HSRP puede quitar este último obstáculo de resistencia dentro de la red de empresa.

### 5.2.3. La convergencia de la red.

Una red de la empresa es adquirida por varios departamentos dentro de una organización. El propósito primario de la red es proporcionar a los usuarios de extremo dentro de estos departamentos acceso a sus datos y aplicaciones.

Los usuarios de extremo típicamente no se preocupan de cuidar aspectos sobre los ruteadores, las líneas de telecomunicaciones, los conmutadores de transmisión de marco, o los conmutadores de LAN, o el hecho de que están abajo. Su percepción 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 percibe la red, como sistema total, para mantener conexiones y para converger alrededor de faltas. 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 de extremo; considera la recuperación de todos los dispositivos, acoplamientos, y protocolos que un usuario emplee para tener acceso a datos.

### 5.2.4. Protocolo de redundancia.

Los protocolos de la red transportan datos de aplicación a través de la red de la empresa. Estos protocolos confían en una arquitectura de red para proporcionar la jerarquía para la dirección del sitio de trabajo y la información de la topología de la red.

| Protocolo | Ayuda de la entrada redundante | Tiempo de la recuperación |
|---|---|---|
| IP | Si con el IRDP | Configurable |
| IPX | Si | 10 segundos |
| NetBIOS | No | |
| Banyan | No | |
| DECNet | No | |
| Appletalk | Si | 30 segundos |

Figura 5.1. Resistencia del Protocolo.

Una entrada o un ruteador multiprotocolo provee esta información. Los sitios de trabajo, los ruteadores, y los servidores de archivo deben hablar el uno al otro, y para este propósito, los protocolos han puesto métodos de la búsqueda en ejecución para encontrar y para almacenar la dirección de la entrada.

Algunos protocolos hacen este procedimiento dinámicamente, mientras que otros requieren la dirección de la entrada para ser *hardcode* en la configuración de los sitios de trabajo según lo ilustrado en la figura 5.1.

Después de que se haya encontrado la entrada y las comunicaciones entre el servidor de aplicaciones y el sitio de trabajo se han establecido sobre una entrada específica, se forma la trayectoria. Las trayectorias permanecen por la duración de la sesión, de esta manera hay un solo punto de la falta. Si cualquier cosa en la trayectoria cambia, por ejemplo la entrada, la sesión termina. Incluso si una entrada redundante se agrega a la red para aumentar la disponibilidad de la red, los protocolos medirán el tiempo con eficacia fuera de las sesiones antes de establecer otra trayectoria a través de la segunda entrada.

## 5.3. PROTOCOLO HSRP.

HSRP provee un método para proporcionar la redundancia directa de la trayectoria para el Protocolo de Internet o IP compartiendo protocolo y direcciones del Control de Acceso al Medio o MAC entre las entradas redundantes. HSRP fue introducido en el software IOS de Cisco en la versión 10 a tratarse de esta edición.

HSPR es una manera para que dos ruteadores de Cisco compartan una dirección IP virtual común, mientras que un ruteador está direccionando o ruteando activamente los paquetes, el otro ruteador o ruteadores están esperando si ocurre el caso de que el ruteador activo falle. Es una manera muy buena de proporcionar tolerancia a fallos. De hecho, si lo toma en cuenta, se puede leer RFC 2281 para aprender un poco más sobre este protocolo.

### 5.3.1. El protocolo de ruteo HSRP.

Cisco implemento un protocolo de ruteo de su propiedad, el protocolo HSRP, a través de sus ruteadores para mantener alta confiabilidad con el uso de la redundancia. Los ruteadores redundantes se utilizan como medios de una ruta de reserva a través de la red en caso de que el ruteador activo falle.

Por lo menos 2 ruteadores son requeridos para implementar HSRP, un ruteador activo y un grupo de ruteadores espera, el grupo puede tener solo un ruteador espera. Solo se permite que un ruteador sea ruteador activo a cualquier hora, el ruteador activo es el que tiene la

la prioridad más alta. La prioridad de los ruteadores se puede fijar a través de la línea opción de comando del IOS de Cisco o prioridad *standby.*

Los ruteadores se comunican uno al otro cada par de segundos por medio del uso de los paquetes HSRP. La estructura del encabezado HSRP se puede considerar en la figura 5.2, dentro del tema encabezado de HSRP. La estructura del paquete demuestra que la prioridad es un campo *byte* 1, la prioridad puede extenderse de 0 - 255.

### 5.3.2. Encabezado de HSRP.

Según se explico antes dos o más ruteadores se comunican entre si usando paquetes de HSRP. Los paquetes de HSRP se componen de un encabezado IP, de un encabezado de UDP y también del encabezado de HSRP según se muestra en la figura 5.2.

La comunicación de HSRP se envía a la dirección IP *multicast* 224.0.0.2 con el origen y el puerto destino juntos UDP y coloca 1985. La dirección del *multicast* se fija dentro del encabezado IP; los puertos, el origen y destino se fijan dentro del encabezado UDP.

| 1 byte | 1 byte | 1 byte | 1 byte |
|---|---|---|---|
| Versión | Código de OP. SYS. | Estado | Tiempo Hola o *Hello* |
| Tiempo *Hold* | Prioridad | Grupo | Reservado |
| Datos de la Autentificación | | | |
| Datos De la Autentificación | | | |
| Dirección IP Virtual | | | |

Figura 5.2. Estructura del encabezado de HSRP

*Versión:* El número de versión de HSRP, sistema a 0.

*Código de OP:* Tres diversos códigos de OP.

*1 – Hello (Hola)* - el ruteador está informando a los otros ruteadores con en el grupo de HSRP de su estado actual.

*2 – Coup (Golpe)* - el ruteador desea convertirse en el ruteador activo.

*3 – Resign (Dimita)* - el ruteador ningunos deseos más largos para ser el ruteador activo.

*Estado:* Hay 6 diversos estados que los ruteadores pueden estar adentro, el ataque es solamente interesado al usar los dos pasados, espera y activo.

*0 – Initial (Inicial)*

*1 – Learn (Aprenda)*

*2 – Listen (Escuche)*

*3 – Speak (Hable)*

*4 – Standby (Espera)* es el estado en que un ruteador está cuando en el grupo espera.

*5 – Active (Activo)* - el ruteador en este estado esta envía hacia delante los paquetes.

*Tiempo Hola o Hello time*: el tiempo Hola es el tiempo en segundos entre cada mensaje hola enviado.

*Tiempo de Hold o Hold time*: El tiempo en segundos el mensaje actual hola debe ser válido.

*Prioridad:* El ruteador con la prioridad más alta es el ruteador activo

*Grupo:* Éste es el número de grupo para el grupo de HSRP que contiene el activo y todos los ruteadores espera para ese acoplamiento de la red.

*Reservado:* No utilizado.

*Datos de la autentificación:* Una contraseña clara de texto de 8 ruteadores, que puede ser percibida y replicada fácilmente. La contraseña de la autentificación por *default* es Cisco.

*Dirección IP virtual:* Ésta es la dirección IP virtual usada por el grupo de HSRP, para identificar en cual grupo *multicast* están ellos.

### 5.3.3. Prioridad del ruteador.

El ruteador con la prioridad más alta según lo mencionado antes, es el ruteador activo y es que envía los paquetes. Hay un grupo de ruteadores espera, si el ruteador activo fallara el ruteador espera con la prioridad más alta siguiente se convierte en el ruteador activo, así la red continuaría la función.

## 5.4. DESCRIPCIÓN DE HSRP.

HSRP permite que un ruteador asuma automáticamente la función del segundo ruteador si el segundo ruteador falla. HSRP es particularmente útil cuando los usuarios en una subred requieren el acceso continuo a los recursos en la red.

### 5.4.1. Característica multicast.

El protocolo consiste de una dirección MAC virtual y una dirección del protocolo que se comparte entre dos ruteadores y un proceso que supervise la LAN e interfaces en serie vía un protocolo *multicast*.

La característica se activa con los siguientes comandos:

```
Standby [número de grupo] IP [dirección-ip (secundario) ]
Standby [número de grupo] timers hellotime holdtime
Standby [número de grupo] priority priority number
Standby [número de grupo] preempt
Standby [número de grupo] track type number [interface priority]
Standby [número de grupo] authentification string
```

Los ruteadores que están participando en un grupo de HSRP se comunican el uno al otro vía un Protocolo de Datagrama de Usuario del *multicast* (UDP)-basado paquete hola.

### 5.4.2. Valores de HSRP.

Durante el arranque, o con el uso de la prioridad y los comandos *pre-empt* o derecho de preferencia, uno de los ruteadores se elige para ser el ruteador activo y el segundo ruteador se señala como el de reserva o espera. Si el ruteador de espera no recibe el paquete hola del ruteador activo, o el segmento local de LAN es inestable o el ruteador activo ha tenido una falla. En cualquier caso el ruteador espera asume el control del MAC virtual y de las direcciones del protocolo. Dentro del software IOS de Cisco, el tiempo entre los paquetes de hola HSRP o *hellotime* y la cantidad de tiempo antes de que el ruteador espera se declare ruteador activo o *holdtime*, se configura. Los valores por *default* se ven en la figura 5.3.

| Lanzamiento de IOS de Cisco | Hellotime | Holdtime | Model1 de Ruteador | Protocolos Soportados | Medios Soportados |
|---|---|---|---|---|---|
| 10.3 | 1 segundos | 3 segundos | serie Cisco 7000/7500 | IP | Ethernet, Token Ring y FDDI |
| 11.x | 3 segundos | 9 segundos | serie Cisco 7000/7500 | IP | Ethernet y FastEthernet, Token Ring y FDDI, ATM (11.2) |

1. La serie 4000 de Cisco no soporta direcciones MAC multiples en las interfaces de Ethernet.

Figura 5.3. HSRP Ayuda del IOS

### 5.4.3. Implementación general de HSRP.

Al implementan HSRP en cualquier ambiente, se necesita seguir una regla específica; si no la red no funcionará correctamente. La regla es simple: la conectividad se debe garantizar entre los puertos del ruteador. Si el ambiente de la LAN se rompe, luego ambos ruteadores asumen la dirección IP primaria y anuncian accesibilidad al resto de la red. Si los ruteadores se unen a un grupo de interruptores o conmutadores, la misma regla se aplica; los interruptores se deben considerar como solo segmento del anillo de *Ethernet/Token*.

Si el Modo de Transferencia Asincrónico o ATM se utiliza para interconectar los interruptores y los ruteadores de la LAN, durante la recuperación de HSRP todos los datos trafican, de tal forma que, son destinados para que el ruteador este enviando a través de la difusión y el desconocido servidor o BUS. Esto ocurre porque los VCs o Circuitos Virtuales directos de los datos se van abajo como resultado de la falta del ruteador primario, y el nuevo VCs tiene que ser restablecido al ruteador de reserva.

#### *5.4.3.1. Un ruteador falla.*

Además de compartir una dirección IP, esa dirección IP tiene una dirección MAC común que los ruteadores comparten. Si se tiene un grupo de trabajo o *workgroup*, por ejemplo de 100 computadoras. Cada una de estas máquinas configurada con una entrada por *default*, si estas máquinas han utilizado la entrada o el ruteador por *default*, ellas tienen esta dirección MAC en su cache ARP. Desde entonces los ruteadores en el grupo HSRP comparten una dirección IP con una dirección MAC correspondiente, cuando fallan, las estaciones de trabajo no son conscientes del cambio. Lo qué ven ellos, es un ruteador virtual.

#### *5.4.3.2. Control de los ruteadores.*

Los ruteadores en un grupo HSRP envían y reciben *keep alives* o mantener con vida; usando la dirección *multicast* de 224.0.0.2 y el puerto 1985 del UDP. Por *default* el intervalo hola es de 3 segundos. Una vez que 3 intervalos hola pasen sin oír al ruteador activo, el ruteador espera se convierte en automáticamente en activo. Cada ruteador es configurado con un número de prioridad, el ruteador con el número de la prioridad más alta en un grupo espera es el ruteador activo, en caso contrario cada ruteador espera se relaja.

### *5.4.3.3. Configuración.*

Aunque todo esto parece muy difícil de configurar, no lo es, ya que se necesitan solamente 2 comandos para hacerlo, y 2 comandos adicionales para modificar esto. Lo que es más, esto es configurado en el interfaz que se quiere para participar en el grupo espera. Es tan fácil que, cualquiera podría hacerlo.

### *5.4.3.4. Comandos.*

Antes en configurar primero se apaga el ruteador que se quiere sea el ruteador activo, va al interfaz que se quiere para funcionar en HSRP, luego se piensa en un número de grupo, todos los ruteadores que participan en este diseño deben usar el mismo número de grupo, también se piensa acerca de la dirección IP que quiera el grupo HSRP comparta, y teclea:

```
dingo(config-if)#standby 1 ip address 10.1.1.254
dingo(config-if)#standby 1 priority 100
```

Tal qué lo que se tiene aquí, es un número de grupo espera de **1**, una dirección IP de 10.1.1.254 que los ruteadores van a compartir, ahora se configura el ruteador espera:

```
fosters(config-if)#standby 1 ip address 10.1.1.254
fosters(config-if)#standby 1 priority 90
```

Ahora bien, la única cosa diferente en el ruteador espera es la prioridad. El ruteador con la prioridad más alta se convierte en el ruteador activo.

### *5.4.3.5. Regresar el rol activo a un ruteador.*

Posiblemente si el ruteador activo, con la prioridad de 100 falle y vuelve a estar disponible, puesto que él tiene la prioridad más alta, llega a ser este el ruteador activo otra vez, y aunque seguro es la idea lógica ante este panorama. Pero, si se quiere que el ruteador antes activo lo sea otra vez, se debe agregar la palabra clave *preempt* al comando de la prioridad:

```
dingo(config-if)#standby 1 priority 100 preempt
```

### *5.4.3.6. Acoplamiento WAN.*

Pero que pasa si los ruteadores están conectados con un acoplamiento WAN, y los ruteadores están funcionando muy bien, pero el acoplamiento WAN falla.

Hay otra manera de seguir eso, y el comando es *track*. Si quiere tener falla sobre HSRP si el acoplamiento WAN falla, bien con solo *track* el interfaz del acoplamiento WAN es conectado, como:

```
dingo(config-if)#standby 1 track s0 priority 11
```

#### *5.4.3.7. Prioridad.*

De lo anterior es donde esta de la palabra clave *priority* seguida por un número. Ese número es el número a restar de propio número de prioridad del ruteador para darle un número de prioridad ajustado si el interfaz que está siguiendo va abajo. Si el interfaz Serial 0 va abajo, la prioridad de nuestro ruteador va a partir el 100 a 89 Cual causara que el ruteador espera llegue a ser activo puesto que tiene una prioridad de 90. Se puede necesitar que suceda esto si el ruteador espera es configurado para DDR.

## 5.5. IMPLEMENTAR HSRP EN LA RED DE LA EMPRESA.

El protocolo del ruteo de Cisco HSRP es un protocolo del ruteo usado para rerutear tráfico de la red cuando un ruteador llega a ser inoperable.

### 5.5.1. Implementar HSRP.

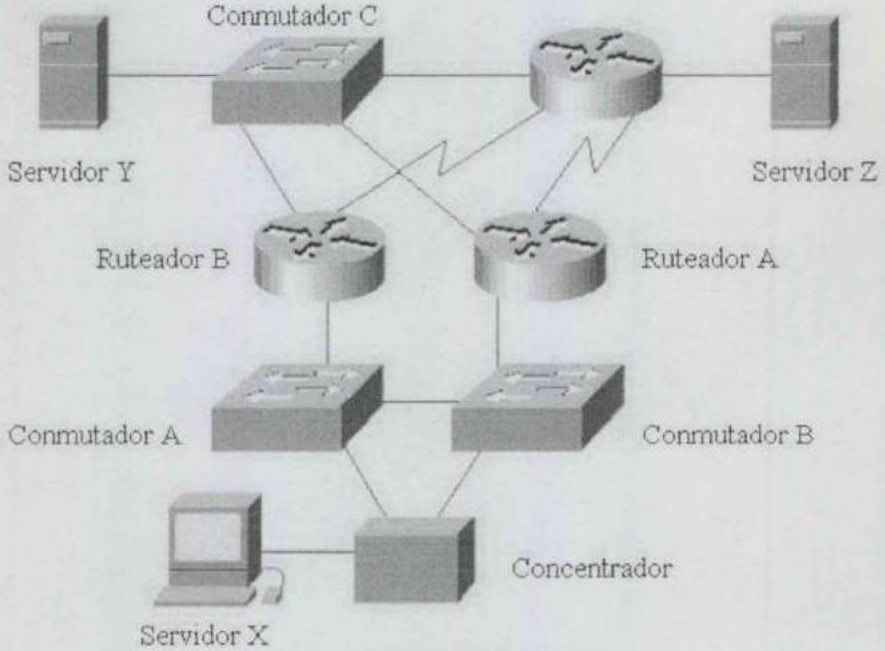



Figura 5.4. Prueba de la Red.

Una implementación típica de HSRP como se aprecia en la figura 5.4, consiste en un sistema de usuarios unidos a un concentrador compartido o a un conmutador, y dos servidores. El servidor Y está conectado con un puerto de alta velocidad del conmutador detrás de los ruteadores, y el servidor Z está localizado en un sitio remoto. Los conmutadores de la LAN están conectados el uno al otro vía puertos del troncal 100BaseT, y cada conmutador de la LAN, alternadamente, está conectado con los ruteadores.

### *5.5.1.1. Posibles fallas.*

Esta implementación de la configuración reduce perceptiblemente el impacto de la falta de cualquier solo componente. Si el conmutador A es el puente de la raíz y el ruteador B es el ruteador activo de HSRP en el peor caso, cuatro faltas posibles pueden ocurrir, fallas que no son de los sitios de trabajo y del servidor:

- El ruteador primario falla.
- El conmutador de la expedición pierde la conexión al concentrador.
- Ambos conmutadores pierden las troncales entre ellos.
- Una de los acoplamientos seriales se rompen.

Cada uno de estas faltas causará una reconfiguración de la red, convergencia, y una serie de cálculos ocurren para ambos HSRP y el Protocolo de Atravesar Árbol o STP.

La falla de la interfaz en serie presentará un *hop* o salto adicional porque el tráfico todavía tiene que atravesar el ruteador primario, porque cuando se permite HSRP, el Protocolo de Control de Mensage de Internet o ICMP vuelve a dirigir los mensajes que son inválidos.

### *5.5.1.2. Contadores de tiempo.*

Todos los protocolos de ruteo; capa 3, tienen un sistema de contadores de tiempo que tienen gran efecto en la convergencia de la red. La capa 2 utiliza el protocolo del STP para determinar la topología de la red, y pues tal tiene un sistema de parámetros básicos que tienen el impacto más grande en el tiempo de convergencia de la red.

Los parámetros de la actual preocupación es el tiempo del STP hola, se pueden ver en la figura 5.5; el tiempo entre las actualizaciones STP; el contador de tiempo del maxage del

STP, un contador de tiempo que indica cuánto tiempo el conmutador mantendrá su base de datos de la información de STP antes de escuchar una actualización; y sigue STP retrasa el contador de tiempo, una tiempo durante la cual los paquetes no se remitan de los puertos.

| **Switch** | **Valor del Parámetro por *Default*** |
|---|---|
| Set SPAN maxage | 20 segundos |
| Set SPAN hello | 2 segundos |
| Set SPAN FWDDELAY | 20 segundos |

Figura 5.5. Parámetros del catalizador STP

Dos áreas en el lado del ruteador necesitan ser consideradas: los contadores de tiempo del protocolo de ruteo IP y los contadores de tiempo *keepalive* del interfaz.

| **Contadores de tiempo del Ruteo** | **Valor por *Default*** |
|---|---|
| **Enhanced IGRP** | |
| — | Hello = 5 segundos |
| — | Holdtime = 15 segundos |
| **IGRP** | |
| — | intervalo de la actualización = 90 segundos |
| — | Ruta invalida = 270 seconds |
| — | holdtime de la ruta = 280 segundos |
| — | Tiempo flush de la ruta= 630 segundos |
| Interface Keepalive | 10 segundos |

Figura 5.6. Contadores de tiempo de Ruteo IOS

El software IOS de Cisco envía un paquete *multicast* fuera de todas los interfaces direccionadas a la dirección MAC de cada interfaz específica, conocido como el *keepalive*. Si el interfaz no recibe este paquete *keepalive* dentro del contador de tiempo especificado, el software IOS de Cisco inhabilita el interfaz.

El protocolo de ruteo tiene virtualmente los mismos contadores de tiempo de STP:

- El tiempo de hola o *hellotime* o intervalo de la actualización, que es el tiempo entre las actualizaciones de la tabla de ruteo; y
- El *holdtime* de la ruta, la cantidad de tiempo el ruteador no actualizara las rutas dentro de su tabla de ruteo. Esto se ilustra en la figura 5.6.

#### *5.5.1.3. Circuitos Virtuales.*

Si el medio del transporte es ATM, debe también ser entendido por el arquitecto de la red que la emulación directa de la LAN de los Circuitos Virtuales de los datos se está utilizando para conectar los conmutadores con el ruteador, que se va abajo durante la conmutación arriba de HRSP. Esto es debido al cambio de los Indicadores Virtuales de la Trayectoria o VPI y de los Indicadores del Circuito virtual o VCI.

Durante la conmutación arriba o *switch over*, los paquetes excesivos son enviados de nuevo al *broadcast* y al servidor desconocido, y una vez que el VC a las direcciones MAC ha sido vuelto a asimilar por el *bus*, los datos del Circuito Virtual directo se establecen de nuevo.

### 5.5.2. Prueba la red.

La meta era probar el tiempo requerido para convergencia de la red. Los componentes individuales de la prueba pueden converger en segundos, pero si no convergen como sistema total, el efecto se pierde. Por lo que la prueba de varias condiciones de interrupción es una prueba de la convergencia de la red.

La red, según se ilustro antes, se instalo en un ambiente controlado. Para vigilar el período de convergencia, un *ping* continuo se inicio entre el sitio de trabajo X y el servidor Y. El *ping* era un valor de tiempo fuera o *time out* de 2000 ms.

Las 6 pruebas eran acumuladas, a menudo un cambio del parámetro rendía un tiempo más corto de convergencia, que el parámetro no fue cambiado para el resto de las pruebas. Cada uno de los siguientes panoramas con falla se realizó durante 6 pruebas:

- Tirar de la conexión del conmutador A a un concentrador.
- Inhabilitar la conexión entre el ruteador B y el conmutador B.
- Inhabilitar la conexión entre los conmutadores A y B.

#### *5.5.2.1. Prueba 1.*

La prueba inicial fue utilizada como prueba patrón o *benchmarck*; el valor del sistema para los contadores de tiempo era por *default*, a excepción de FWDDELAY en los

conmutadores, que fue cambiado por *default* de 20 segundos a 15 segundos. El tiempo de la convergencia de la red fue supervisado según lo demostrado en la figura 5.7:

| Prueba | Tiempo de la Convergencia |
|---|---|
| A | 28 segundos |
| B | 38 segundos |
| C | 28 segundos |

Figura 5.7. Resultados de la Prueba 1.

### *5.5.2.2. Prueba 2.*

La segunda prueba era establecer o no si se rutean actualizaciones del protocolo tenga algún efecto en convergencia de la red. Fue observado que cambiando los contadores de tiempo de la actualización del protocolo del ruteo con el comando: contadores de tiempo básicos 10 20 30 30; no afectan el tiempo de la convergencia de la red. Los resultados de la prueba 2 se demuestran en la figura 5.8:

| Prueba | Tiempo de la Convergencia |
|---|---|
| A | 28 segundos |
| B | 38 segundos |
| C | 28 segundos |

Figura 5.8. Resultados de la Prueba 2.

### *5.5.2.3. Prueba 3.*

Para la tercera prueba, el protocolo de ruteo fue cambiado del Protocolo Interior de Ruteo de la Entrada o IGRP de Cisco; al realzar IGRP para considerar si cambiar el protocolo del ruteo afecta tiempo de la convergencia. Los resultados indicaron que el protocolo del ruteo tiene poco a ningún efecto; ver la figura 5.9:

| Prueba | Tiempo de la Convergencia |
|---|---|
| A | 28 segundos |
| B | 38 segundos |
| C | 28 segundos |

Figura 5.9. Resultados de la Prueba 3.

#### *5.5.2.4. Prueba 4.*

Sin cambios en todos los parámetros, la cuarta prueba debía medir el impacto de los contadores de tiempo de *keepalive* del ruteador. El contador de tiempo se redujo a 3 segundos por *default* de 10. En la prueba B, que simula la falta del acoplamiento entre el ruteador B y el conmutador B, la red se recuperó en el plazo de 10 segundos; un aumento de más el de 50%. Ver la figura 5.10:

| Prueba | Tiempo de la Convergencia |
|---|---|
| A | 28 segundos |
| B | 10 segundos |
| C | 28 segundos |

Figura 5.10. Resultados de la Prueba 4.

#### *5.5.2.5. Prueba 5.*

La prueba 5 redujo el interfaz *keepalive* de los ruteadores un segundo. Una vez más, solamente la prueba B fue afectada por este cambio; ver la figura 5.11:

| Prueba | Tiempo de la Convergencia |
|---|---|
| A | 28 segundos |
| B | 4 segundos |
| C | 28 segundos |

Figura 5.11. Resultados de la Prueba 5.

#### *5.5.2.6. Prueba 6.*

La prueba 6 mantuvo el interfaz *keepalive* en un segundo y cambió el parámetro del *maxage* del STP en los conmutadores Catalyst 5000 a 6 segundos. Ver la figura 5.12:

| Prueba | Tiempo de la Convergencia |
|---|---|
| A | 12 segundos |
| B | 4 segundos |
| C | 12 segundos |

Figura 5.12. Resultados de la Prueba 6.

Para esta configuración, el tiempo de la convergencia de la red en las pruebas A y C eran menos que la mitad del tiempo de la convergencia registró en la prueba 5.

### 5.5.3. Las conclusiones de las pruebas.

Los resultados indican que implementar HSRP proporciona una convergencia confiable de la red, durante la cual el usuario final puede ver un retardo en tiempos de reacción pero que no nota una interrupción.

Fijar valores de la recuperación del STP y contadores de tiempo HSRP a los resultados más bajos de los valores del servicio intermitente.

Otros patrones de falta causados por valores bajos del contador de tiempo incluyen oscilaciones de la topología del STP y ediciones de la CPU dentro de conmutadores de la LAN. Cisco recomienda que los valores indicados en la prueba 6 se consideren los valores mínimos para los contadores de tiempo.

## 5.6. UTILIDAD DE HSRP.

Es tiempo de volver a la configuración de la LAN. Dando una vista en el protocolo de ruteo HSRP. Para entender la utilidad e inteligencia de HSRP, sin embargo, se debe mirar en la figura 5.13, cómo calculan los *hosts* que ruteador usar para alcanzar otras redes o subredes.

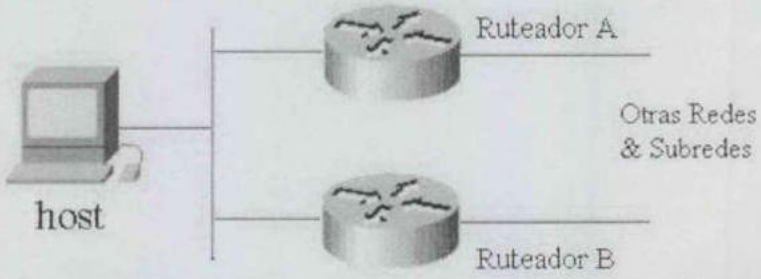



Figura 5.13. Cómo los *hosts* calculan qué ruteador para utilizar fuera.

Hay varias técnicas, cada uno con sus representantes. Son:

- Funcionar un proceso de ruteo en el *host*
- Ruteador estático por *default*
- Proxy ARP
- GDP e IRDP
- HSRP

### 5.6.1. Funcionar un proceso de ruteo en el host.

El primer se parece a menudo deseable a los usuarios de alta potencia del sitio de trabajo. Desean lo mejor de todo; Tan esperanzadamente el ruteo consigue encendido en su estación de trabajo, en modo pasivo, donde la estación de trabajo escucha pero no transmite. La estación de trabajo está ciertamente bien informada.

Pero el CPU se está utilizando para recibir y para procesar actualizaciones de ruteo. Esto puede disminuir algo el funcionamiento computacional de la estación de trabajo. Peor si la estación de trabajo o servidor tiene interfaces múltiples. Los *hosts* de UNIX y OS/2 pueden pensar que son ruteadores, y transmitir actualizaciones de ruteo, y enviar paquetes. Los paquetes del envió interrumpen la CPU, generalmente un golpe efectivo al funcionamiento.

Las actualizaciones del ruteo no son tan grandes, si la estación de trabajo no se configura correctamente. El ruteador y el personal que establece una red piensan usualmente que esto no es bueno, pero es mejor dejar al ruteador hacer su trabajo.

### 5.6.2. Ruteador estático por default.

Las rutas estáticas por *default* son el otro extremo. Las PC se pueden configurar a menudo solamente con de 1 a 3 ruteadores de *default*. El tráfico no local entonces se envía al ruteador por *default*. Esto es simple, bajo impacto en el *host*, pero en caso de que de un ruteador o un acoplamiento inoperable, no pueda permitir que un ruteador o un acoplamiento alternativo se utilicen, dependiendo de la implementación. Los sitios de trabajo de UNIX se pueden *bootear* con las rutas múltiples por *default*, pero pueden no recuperar las rutas si los ruteadores de la entrada es decir *gateway* llegan a ser inaccesibles.

### 5.6.3. Proxy ARP.

El proxy ARP es común en ambientes de la PC. La idea es convencer al PC o *host* de ARP para todas las direcciones IP como si estuvieran en el cable local. Hacer esto depende de la implementación. Un ruteador entonces responde a la petición ARP con su propia dirección MAC, y el *host* entonces envía los paquetes a esa dirección MAC. El ruteador envía el paquete al destino, y el *host* nunca se percata que no tenía la dirección MAC destino.

El único problema con proxy ARP es que la mascara de subred configurada en las PC puede ser algo impar, como 0.0.0.0. Esto dice que no hay parte de la dirección significativa para las decisiones de ruteo, o todas las direcciones están en el cable local. Eso suena ciertamente como impar. También pone tráfico adicional en el acoplamiento local, siempre que el *host* desee enviar los paquetes a una nueva dirección IP.

El *host* envió una *broadcast* del ARP, y todos los ruteadores locales responden. Así para cada destino nuevo hay un *broadcast* y una o más respuestas, todas llevan las mismas direcciones MAC como el tiempo anterior. Las *broadcast* interrumpen cada CPU en el acoplamiento, así que ésta no escala ésa bien, por no mencionar que sea algo innecesariamente habladora.

### 5.6.4. GDP e IRDP.

El Protocolo de Descubrimiento de la Entrada o GDP, de Cisco, es una alternativa. La idea es que los ruteadores difunden periódicamente, cada 15 a 30 minutos generalmente, anunciando que ellas están abiertas para la acción, y que esta información es válida por cierto período del tiempo. Con los ruteadores múltiples, las prioridades se pueden anunciar, dando preferencia a un ruteador sobre otro. Los *hosts* que cargan pueden solicitar la información, solo una vez.

El Protocolo de Descubrimiento de Ruteo de ICMP o IRDP limpia esto para uso *multicast*, y se describe en RFC 1256. Los ruteadores de Cisco apoyan el GDP e IRDP. Para utilizar IRDP o el GDP, se necesita código de funcionamiento en su *host*. El código está disponible en ftp.cisco.com en pub/rdisc. IRDP está también disponible para Suns en algunos de los sitios generalmente, como irdpd.c. Todo lo que se tiene que hacer debe compilar y se tiene un proceso para su Sun se actualice el ruteo por *default* en la tabla de ruteo siempre que sea necesario. Si se tiene otro tipo del SO, se consigue el derecho del código.

### 5.6.5. HSRP.

HSRP es un protocolo de ruteo Cisco, creado con la idea de que pese a posibles fallas en algún ruteador, se siga trabajando sin mayor problema, es decir que permita a la red ser tolerante a fallos; en lo relativo a los ruteadores.

### *5.6.5.1. Ruteador Virtual.*

La idea detrás de HRSP es establecer un ruteador virtual, con su propia dirección IP; como el ruteador por *default* para los *hosts* en una LAN, se puede ver en la figura 5.14, como utiliza HSRP un ruteador virtual.

El ruteador virtual también tiene su propia dirección MAC. Uno o más ruteadores entonces son el grupo espera para este ruteador virtual. Uno de los ruteadores en el grupo es activo en cualquier momento, realmente los paquetes de la expedición son enviados a la dirección MAC del ruteador virtual. Si desaparece ese ruteador activo, posiblemente por una falla, otro ruteador en el grupo espera asume el control.

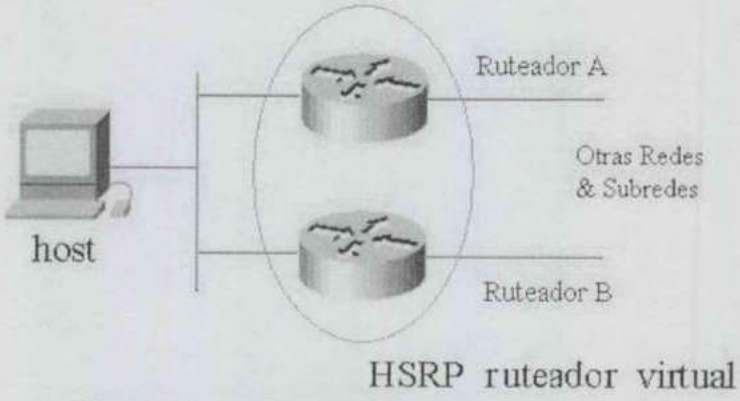



Figura 5.14. HSRP utiliza un ruteador virtual.

La ventaja es que el *host* nunca sabe que diversos ruteadores están implicados, el solo percibe un ruteador. Apenas envía los paquetes al ruteador virtual, obviamente al ruteador actual que envía los paquetes. Y este tiene ARP solo una vez, para conseguir la dirección MAC asociada a la dirección IP del ruteador virtual. Esto ahorra todo el tráfico del ARP que viene con proxy ARP. También acomoda las implementaciones que ignoran cambios de la tabla del ARP, un problema del *host* con el cambio de una dirección MAC a partir de una dirección IP a otra.

### *5.6.5.2. Configuración de HSRP.*

Configuración de HSRP es fácil. Todo lo que se configura es:

```
interface ethernet 0
ip address 131.108.1.1 255.255.255.0
standby 2 ip 131.108.1.3
```

En el segundo ruteador unido a la LAN de *Ethernet*:

```
interface ethernet 0
ip address 131.108.1.2 255.255.255.0
standby 2 ip 131.108.1.3
```

Esto pone ambas interfaces de los ruteadores en la misma subred, con un común grupo espera de 2 en ese acoplamiento. Ambos ruteadores son responsables de actuar juntos como el ruteador virtual 131.108.1.3. Los *hosts* se configuran con una entrada estática por *default*, la dirección IP que del ruteador virtual, 131.108.1.3. Y eso es todo lo que toma.

#### *5.6.5.3. Utilidad de HSRP.*

HSRP puede ser utilizado en interfaces de LAN: FDDI, *Token Ring*, y *Ethernet*. En algunos modelos e interfaces del ruteador se puede utilizar a grupos múltiples de HSRP. Un uso pudo ser crear dos ruteadores virtuales, los grupos que atraviesan dos ruteadores actuales. Se señala la mitad de los *hosts* de la LAN en un ruteador virtual, mitad en la otra. Diversas prioridades del uso, así un ruteador actual es activo como el primer ruteador virtual, el otro como el segundo ruteador virtual. Esta carga balancea, y si cualquier ruteador muere, el otro asume el control para el.

Hay una limitación de en mayoría 3 grupos espera, ruteadores virtuales; por interfaz del *Token Ring*. Las 1000, 2500, 3000 y 4000 ruteadores modelo con los chips de *Ethernet* de lanza pueden apoyar solamente un grupo HSRP por interfaz de *Ethernet*. Asumiendo que esto es sobre todo una limitación del *hardware*: si realmente no desea el CPU del ruteador habrá que mirar cada paquete ruteado, así que el interfaz tiene que proporcionar una cierta selectividad en cuanto a direcciones MAC con que interrumpe el CPU del ruteador.

### 5.6.6. Comandos de HSRP.

El mecanismo subyacente es *multicasts* del UDP: los ruteadores envían periódicamente mensajes hola al grupo para dejar a sus pares saber que todavía están allí. Una vez que se tenga esta idea básica, los otros comandos de HSRP son faciles al diseñador, y puede permitir que otro tome los ajustes. A propósito, los comandos de HSRP son todos los comandos del interfaz.

El comando:

```
Standby 2 timers 1 3
```

Fija el hola y los contadores de tiempo de asimiento para el grupo espera 2. Éstos son los valores prefijados de 1 segundos entre los mensajes hola y 3 segundos antes de que se asuma que un ruteador fallo.

Para controlar qué ruteador es activo, configure:

```
Standby 2 priority 90
```

La prioridad por *default* es 100, gana la prioridad más alta.

Para permitir que un ruteador reasuma el ser el ruteador activa para el grupo 2, se debe agregar:

```
Standby 2 preempt
```

Hay también un comando que permite seguir interfaces y bajar la prioridad si cualquiera de las interfaces fallo (hace al ruteador menos deseable como entrada por *default*).

El incremento de la prioridad por *default* es 10, pero se puede configurar otros incrementos. Los incrementos con excepción de 10 son acumulativos. Tan si varios interfaces están abajo, los incrementos configurados todos se restan del nivel de la prioridad del ruteador. Aquí es lo que parece el comando:

```
Standby 2 track ethernet 0 25
```

Para supervisar la espera, se puede utilizar los comandos que se esperan:

```
Show standby
Debug standby
```

El comando:

```
Standby 2 timers 1 3
```

Fija el hola y los contadores de tiempo de asimiento para el grupo espera 2. Éstos son los valores prefijados de 1 segundos entre los hellos y 3 segundos antes de que se asuma que un ruteador está abajo.

Para controlar qué ruteador es activo, configure:

```
Standby 2 priority 90
```

La prioridad por *default* es 100, gana una prioridad más alta.

Para permitir que un ruteador reasuma el ser el ruteador activa para el grupo 2, agregue:

```
Standby 2 preempt
```

Hay también un comando que le deja seguir interfaces y bajar la prioridad si cualquiera de las interfaces están abajo (haciendo el ruteador menos deseable como entrada por *default*).

El incremento de la prioridad por *default* es 10, pero se puede configurar otros incrementos. Los incrementos con excepción de 10 son acumulativos. Tan si varios interfaces están abajo, los incrementos configurados todos se restan del nivel de la prioridad del ruteador. Aquí es lo que parece el comando:

```
Standby 2 track ethernet 0 25
```

Para supervisar la espera, se puede utilizar los comandos que se esperan:

```
Show standby
Debug standby
```

# CAPITULO 6. CONFIGURACION DE HSRP.

## 6.1. INTRODUCCION AL PROTOCOLO HSRP.

Como más y mas organizaciones buscan los beneficios económicos del campo de red para cuestiones criticas de comunicaciones, la alta confiabilidad llega a ser cada vez más crucial. Dentro del campo de red, la atención ha sido enfocada en el abastecimiento de infraestructura directa. Uno de los desafíos más grandes, sin embargo es extender el nivel de redundancia entre estaciones de trabajo y en el equipo de la red en el nivel de usuario.

Este capitulo se enfoca en como los administradores de la red pueden crear una dirección virtual de entrada por *default* y asignar esta a los ruteadores redundantes en un segmento de la LAN, asegurando la tolerancia a fallos y realzar el funcionamiento del ruteo en la red.

## 6.2. DESCRIPCIÓN DEL PROTOCOLO HSRP.

El protocolo de ruteo HSRP, es un protocolo propiedad de Cisco. HSRP es un protocolo de ruteo que proporciona la reserva a un ruteador cuando ocurre una falla. Usando HSRP, varios ruteadores están conectados con el mismo segmento de una red de *Ethernet*, del FDDI o del simbolo-anillo y trabajan juntas para presentar el aspecto de un solo ruteador virtual en la LAN. Los ruteadores comparten las mismas direcciones IP y MAC, por lo tanto cuando ocurre la falla de un ruteador, los *hosts* en la LAN pueden continuar enviando los paquetes a una constante dirección IP y MAC. El proceso de transferir las responsabilidades de ruteo de un dispositivo a otro es transparente para el usuario.

### 6.2.1. Descripción del Protocolo.

El protocolo de ruteo HSRP proporciona tolerancia a fallos y realza el funcionamiento de ruteo para las redes IP. HSRP permite que los ruteadores IOS de Cisco supervisen cada estado operacional de otro y asuman muy rápidamente la responsabilidad del paquete-enviado en caso que el dispositivo actual de transporte en el grupo HSRP falle o se retire para mantenimiento, el mecanismo espera sigue siendo transparente para los *hosts* unidos y se puede desplegar en cualquier tipo de LAN.

Con los grupos múltiples de espera activos, los ruteadores pueden proveer simultáneamente de la reserva redundante y realizan el compartir de carga a través diversas direcciones IP.

### 6.2.2. Configuración de HSRP para ruteo tolerante a fallos.

El propósito primario de la red del campus es proporcionar a los usuarios finales el acceso de a sus datos y aplicaciones.

Los usuarios finales perciben la red del campus como un sistema total y no cuidan típicamente si los ruteadores y los conmutadores de la LAN son operacionales. Para construir varios niveles de redundancia en la red, el diseñador de la red percibe la red, como sistema total, para mantener conexiones y para converger alrededor de fallas.

## 6.3. PROBLEMAS.

Para poder construir varios niveles de redundancia en la red, el diseñador percibe a la red como un sistema total, con el objeto de mantener las conexiones y al mismo tiempo poder trabajar óptimamente independientemente de los problemas que puedan ocurrir.

- Problema: usando las entradas por *Default*.
- Problema: usando Proxy ARP.
- Problema: usando el RIP
- Problema: usando IRDP.

### 6.3.1. Problema: usando las entradas por *Default*.

Aquí se hace uso del término entrada en lugar del concepto *gateway* para mejorar la comprensión del protocolo.

El modelo jerárquico del campus construye en redundancia el nivel bloque del conmutador. Las trayectorias primarias y secundarias entre la capa del acceso y el conmutador de distribución proporcionan el acceso continuo a pesar de una falla del acoplamiento en la capa del acceso. Las trayectorias primarias y secundarias entre el ruteador de distribución y el corazón o centro de la red proporcionan operaciones continuas si un acoplamiento falla en la capa de la distribución.

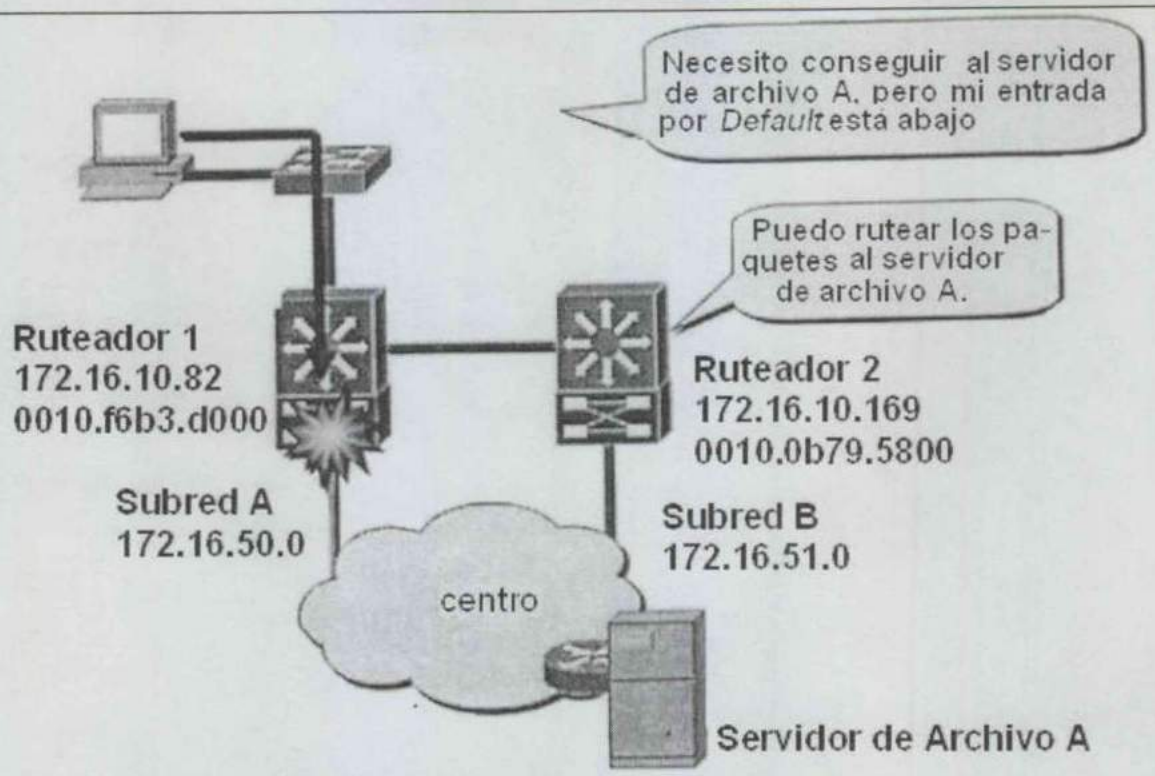



Figura 6.1. Ejemplo usando entradas por default.

En el ejemplo de la figura 6.1, el ruteador 1 es responsable de rutear los paquetes para la subred A y el ruteador 2 es responsable de manejar los paquetes en la subred B. Si el ruteador 1 llega a ser indisponible al usuario final, los protocolos convergentes rápidos de ruteo pueden responder dentro de segundos. Después de la convergencia, el ruteador 2 está preparado para transferir los paquetes que habrían pasado de otra manera a través del ruteador 1.

Sin embargo, no es la responsabilidad del sitio de trabajo, de los servidores, y de las impresoras intercambiar la información de ruteo dinámica, ni es el ruteo por tales dispositivos un buen diseño.

Estos dispositivos se configuran típicamente con una sola dirección IP de entrada por *default*. Si el ruteador que es la entrada por *default* falla, el dispositivo se limita a comunicarse solamente en el segmento local de la red IP y se desconecta efectivamente del resto de la red. Incluso si existe un ruteador redundante que podría servir como entrada por *default*, no hay método dinámico por el cual estos dispositivos pueden cambiar a una nueva dirección IP de la entrada por *default*.

### 6.3.2. Problema: Usar Proxy ARP.

Algunos *hosts* de IP utilizan el Protocolo de Resolución de Dirección o ARP de proxy para seleccionar un ruteador. La estación del usuario final enviaría un pedido del ARP para la dirección IP a la destinación. El ruteador responsable respondería con esta su propia dirección de Control de Acceso al Medio o MAC a la petición del ARP.

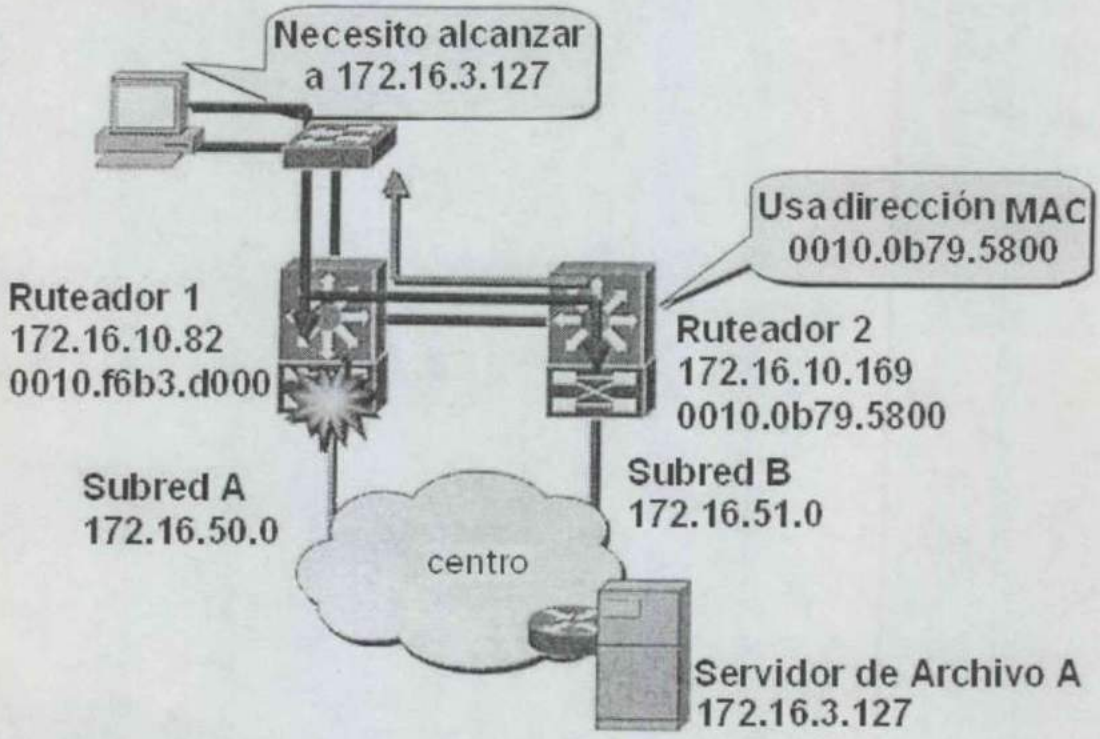



Figura 6.2.Ejemplo usando proxy ARP.

Con ARP proxy, la estación del usuario final se comporta como si el dispositivo de la destinación fuera conectado a el mismo segmento de la red. Si el ruteador responsable falla, la estación de extremo de la fuente continúa enviando los paquetes para la destinación a la dirección MAC de ese ruteador. Esos paquetes se caen posteriormente de la red. Lo antes mencionado se puede apreciar en el ejemplo de la figura 6.2.

Para adquirir la dirección MAC del ruteador que fallo, la fuente de la estación final debe: iniciar cualquier otra petición del ARP o reanudarse. En cualquier caso, la fuente de la estación final no puede comunicarse con la destinación por un período del tiempo significativo aunque regule ha convergido el protocolo de ruteo. El protocolo ARP utiliza la actualización del ARP más la entrada de tiempo sofocante del ARP para calcular el intervalo en el cual la fuente no puede comunicarse con la destinación.

### 6.3.3. Problema: usando el RIP.

Algunos *hosts* IP utilizan el Protocolo de Información de Ruteo o RIP para descubrir los ruteadores.

La estación del usuario final mantiene una tabla de la cual los ruteadores tienen una trayectoria a la destinación. La estación del usuario final utiliza la trayectoria más conveniente.

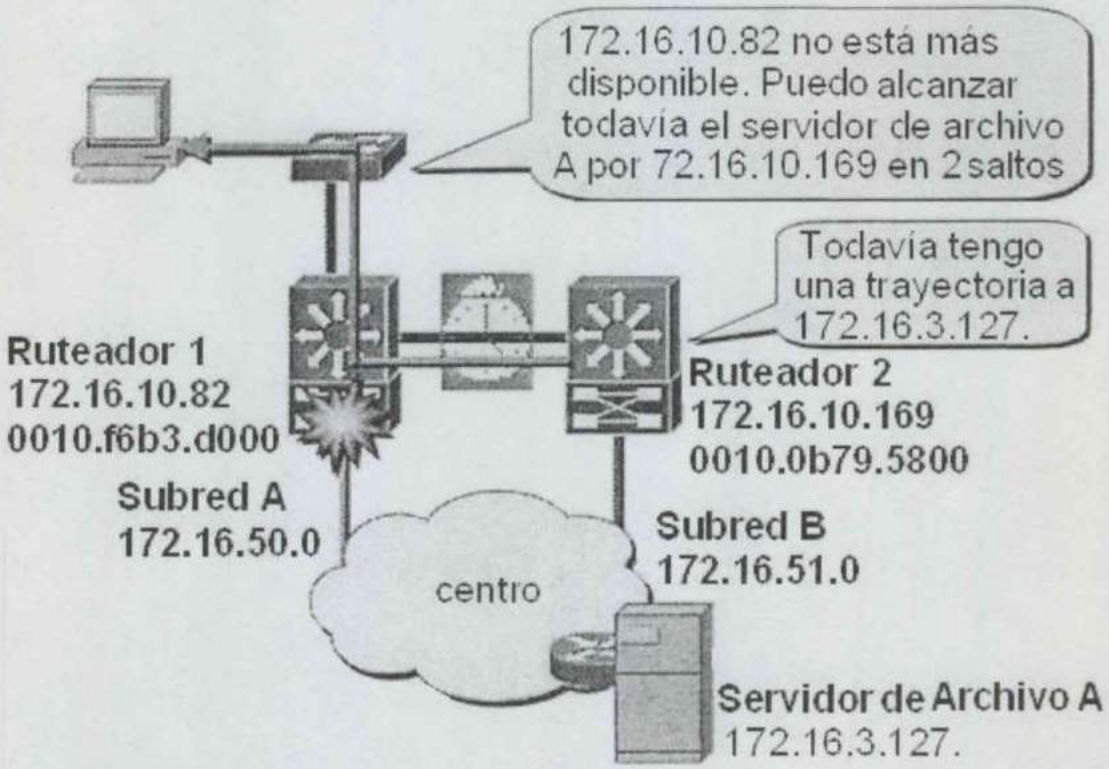



Figura 6.3. Ejemplo usando el RIP.

La desventaja de usar el RIP es que es lento adaptarse a los cambios en la topología. Si la fuente de la estación final se configura para utilizar el RIP, un período de tres veces el intervalo de la actualización pudo transcurrir antes de que el RIP haga otro ruteador disponible. Observar en el ejemplo de la figura 6.3.

### 6.3.4. Problema: Usando IRDP.

Algunos *hosts* IP utilizan el Protocolo de Control de Mensaje de Internet o ICMP, el Protocolo del Descubrimiento del Ruteador o IRDP, para encontrar una trayectoria nueva

cuando el ruteador primario llega a ser indisponible. IRDP no es un protocolo de ruteo como RIP o el Protocolo de Ruteo de la Entrada Interior o IGRP. IRDP es una extensión al ICMP que proporciona un mecanismo para los ruteadores para anunciar las rutas útiles por *default*. IRDP ofrece varias ventajas sobre otros métodos de descubrimiento de direcciones de ruteadores vecinos. IRDP no requiere *hosts* para reconocer protocolos de ruteo, ni IRDP requiere configuración manual de un administrador.

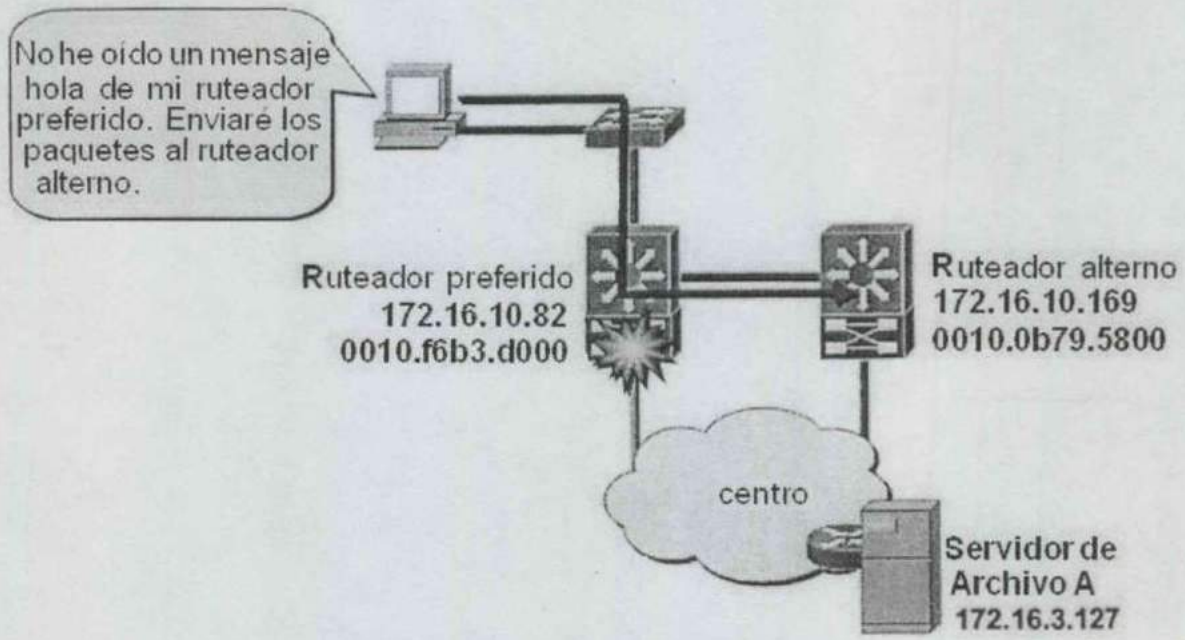



Figura 6.4. Ejemplo usando el IRDP.

Un *host* que utiliza IRDP escucha mensajes *multicast* hola del ruteador preferido por *default*. Los anuncios IRDP-basados se consideran válidos solamente para un valor de tiempo de vida predefinido. Si un anuncio nuevo no se ve durante ese tiempo de vida, la dirección del ruteador se considera inválida y el *host* quita la ruta correspondiente por *default*. el uso del RIP se muestra en la figura 6.4.

El protocolo IRDP permite valores de sincronización que varían. Un valor de tiempo de vida se incluye en el encabezado de cada anuncio IRDP y se aplica a todas las direcciones incluidas en el paquete. Un *host* utilizará la dirección del ruteador solamente para el número de segundos de tiempo de vida después del anuncio más reciente.

Los anuncios se envían cada 7 a 10 minutos; el tiempo de vida por *default* es 30 minutos. Sin embargo, el ruteador tiene control completo sobre el intervalo y valores del tiempo de vida, y puede controlar así el período del tiempo que las direcciones se consideran válidas.

IRDP tiene dos separaciones del intervalo de tiempo: un mínimo y un máximo intervalo de anuncio. Todos los anuncios no solicitados se envían en la ventana de tiempo definida por estos dos valores. IRDP se cubre en mayor detalle en el RFC 1256.

## 6.4. PROTOCOLO DE RUTEO HSRP.

HSRP define un sistema de ruteadores que trabajan juntos para representar un ruteador virtual tolerante a fallos.

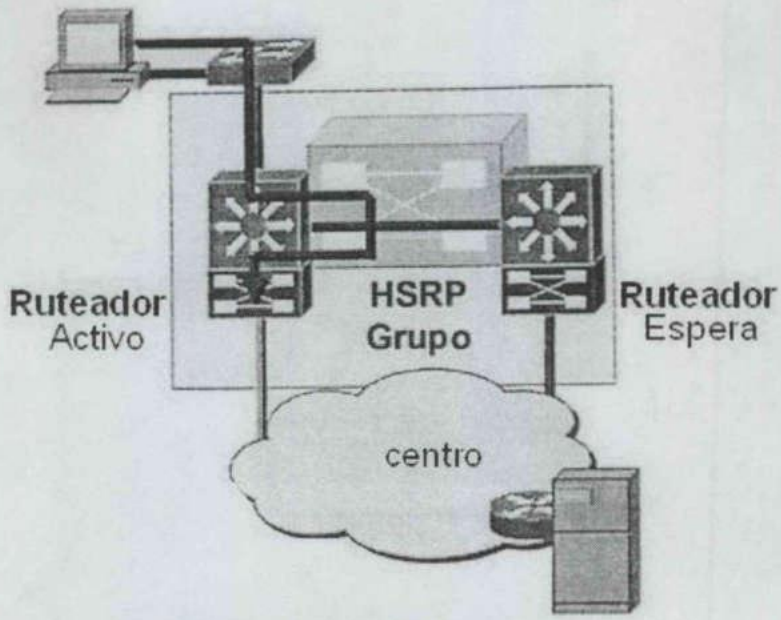



Figura 6.5. Protocolo de ruteo HSRP.

Los ruteadores de Cisco utilizan el HSRP, que permite a estaciones finales continuar comunicándose a través de la red incluso cuando la entrada por *default* llega a ser indisponible.

Con HSRP, un sistema de ruteadores trabajan juntos para representar un solo ruteador virtual espera. El grupo espera funciona como un solo ruteador configurado con un IP y una dirección MAC virtuales. Del punto de vista del sistema final, el ruteador virtual es un solo ruteador meta con su propio IP y dirección MAC, distintos de los ruteadores físicos en la red, se ilustra en la figura 6.5.

Es importante mencionar que, si la conectividad entre los procesadores de la ruta falla, ambos procesadores de la ruta asumen la dirección IP virtual y remiten los paquetes enviados a la dirección virtual. Esta acción da lugar a exceso de paquetes en la red.

### 6.4.1. Solución: protocolo de ruteo HSRP.

Antes se mencionaron algunas opciones de ruteo y los posibles problemas que surgen de sus implementaciones.

Debido a que estos problemas no los sufre HSRP, se plantea como una solución viable, en virtud de que; los paquetes todavía se rutean incluso cuando el ruteador actual que remite falla. Esto se ilustra en la figura 6.6.

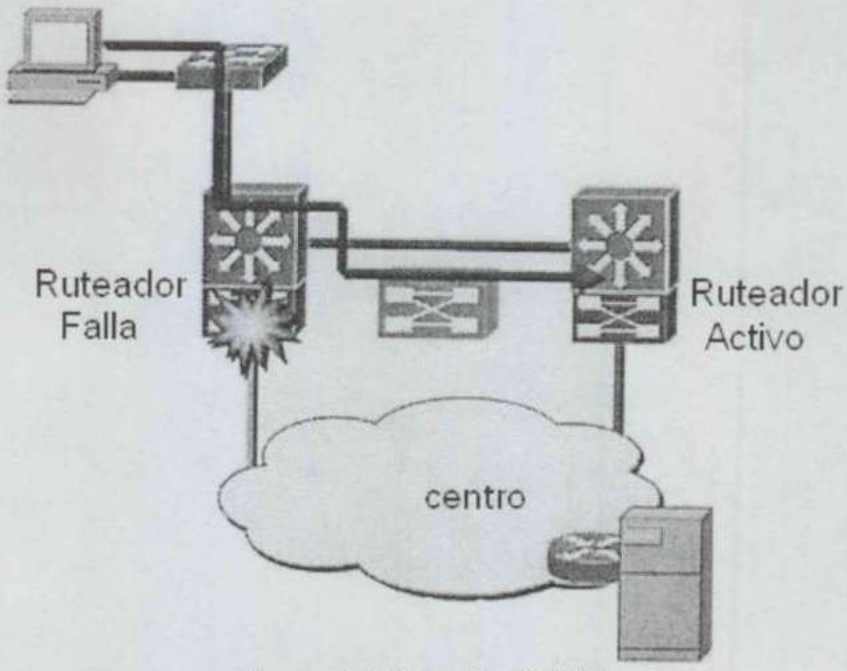



Figura 6.6. Solución HSRP.

Porque los ruteadores en el grupo espera rutean los paquetes enviados a una dirección virtual, los paquetes todavía se rutean a través de la red incluso cuando el ruteador originalmente remite los paquetes fallidos.

HSRP permite que un ruteador asuma automáticamente la función del segundo ruteador si el segundo ruteador falla. HSRP es particularmente útil cuando los usuarios en una subred requieren el acceso continuo a los recursos en la red.

### 6.4.2. Miembros del grupo HSRP.

Los grupos espera de HSRP consisten en ruteadores múltiples que realizan papeles específicos.

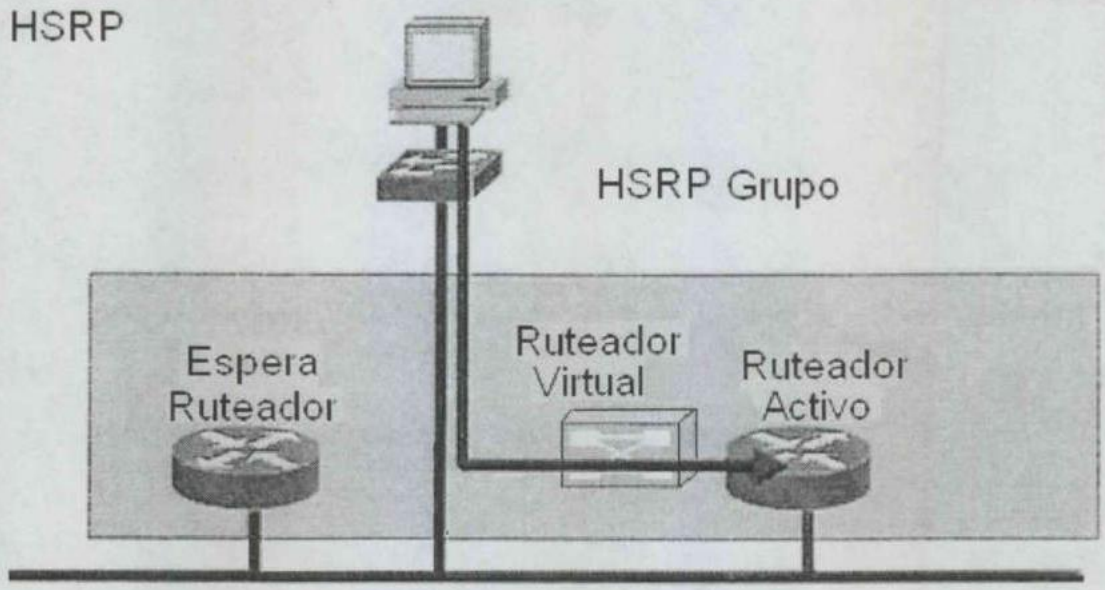



Figura 6.7 Miembros del grupo HSRP.

El grupo espera abarca las siguientes entidades:

- Un ruteador activo.
- Un ruteador espera.
- Un ruteador virtual.
- Otros ruteadores.

Estos diversos roles del ruteador se discuten detalladamente más adelante en este capítulo; y se ilustran en la figura 6.7.

### 6.4.3. Grupos de HSRP.

Los ruteadores pueden pertenecer a grupos múltiples en la misma subred en una VLAN.

Para facilitar compartir de carga, un solo ruteador puede ser un miembro de múltiples grupos espera de HSRP en un solo segmento. Cada grupo espera emula un solo ruteador virtual. Puede haber hasta 255 grupos espera en cualquier LAN.

En el ejemplo de la figura 6.8, el ruteador A y el ruteador B son miembros de los grupos 1 y 2. Sin embargo, el ruteador A es el ruteador activo que remite para el grupo 1 y el ruteador espera para el grupo 2. El ruteador B es el ruteador activo que remite para el grupo 2 y el ruteador espera para el grupo 1.

**Advertencia:** *el aumento del número de los grupos en los cuales un ruteador participa incrementa la carga en el ruteador y puede afectar el funcionamiento del ruteador.*

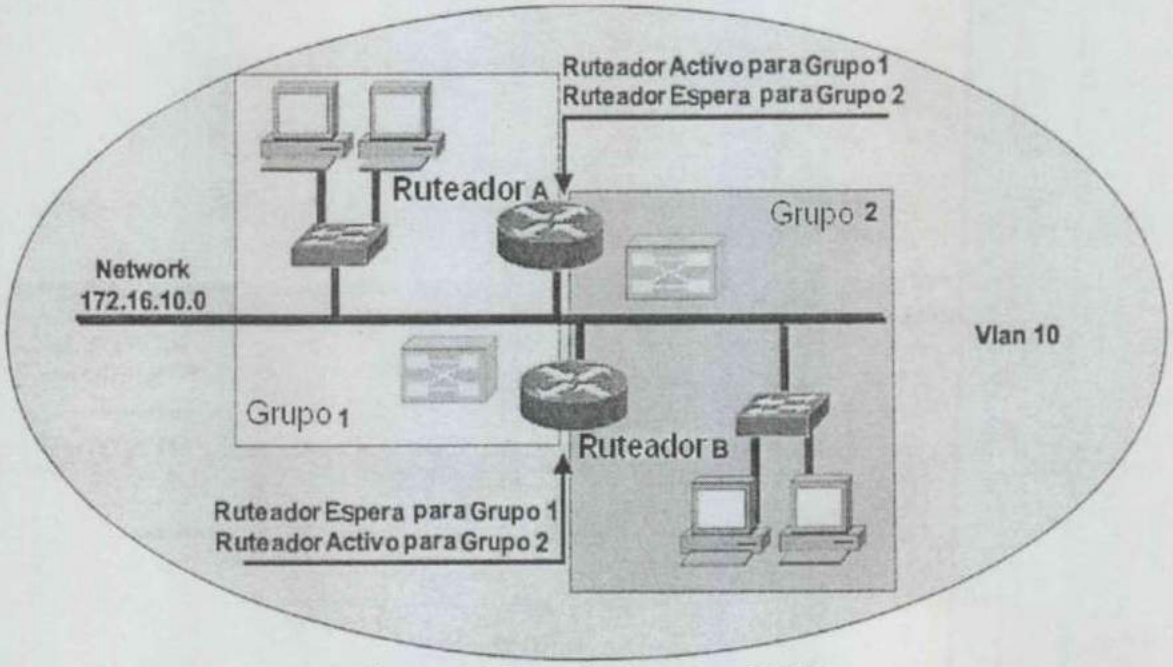



Figura 6.8 Ejemplo de grupos HSRP.

### 6.4.4. Dirigirse a grupos HSRP a través de acoplamientos ISL.

Los ruteadores pueden proporcionar simultáneamente la reserva redundante y realizar el compartir de carga a través de diversas subredes IP.

Para cada grupo espera, una dirección IP y una sola dirección MAC bien conocida con un identificador único de grupo se asigna al grupo.

La dirección IP de un grupo está en el rango de direcciones que pertenecen a la subred en uso en la LAN. Sin embargo, la dirección IP del grupo debe diferenciar de las direcciones asignadas como direcciones del interfaz en todos los ruteadores y *hosts* en la LAN, incluyendo las direcciones IP virtuales asignadas a otros grupos HSRP.

En la figura 6.9, este ejemplo muestra la configuración para dos ruteadores HSRP-permitidos que participan en dos LANs Virtual o VLANs separadas usando el Acoplamiento de Inter - Conmutación o ISL. Funcionando HSRP sobre ISL permite que los usuarios configuren redundancia entre los ruteadores múltiples que son configurados como frentes finales para las subredes IP de VLAN.

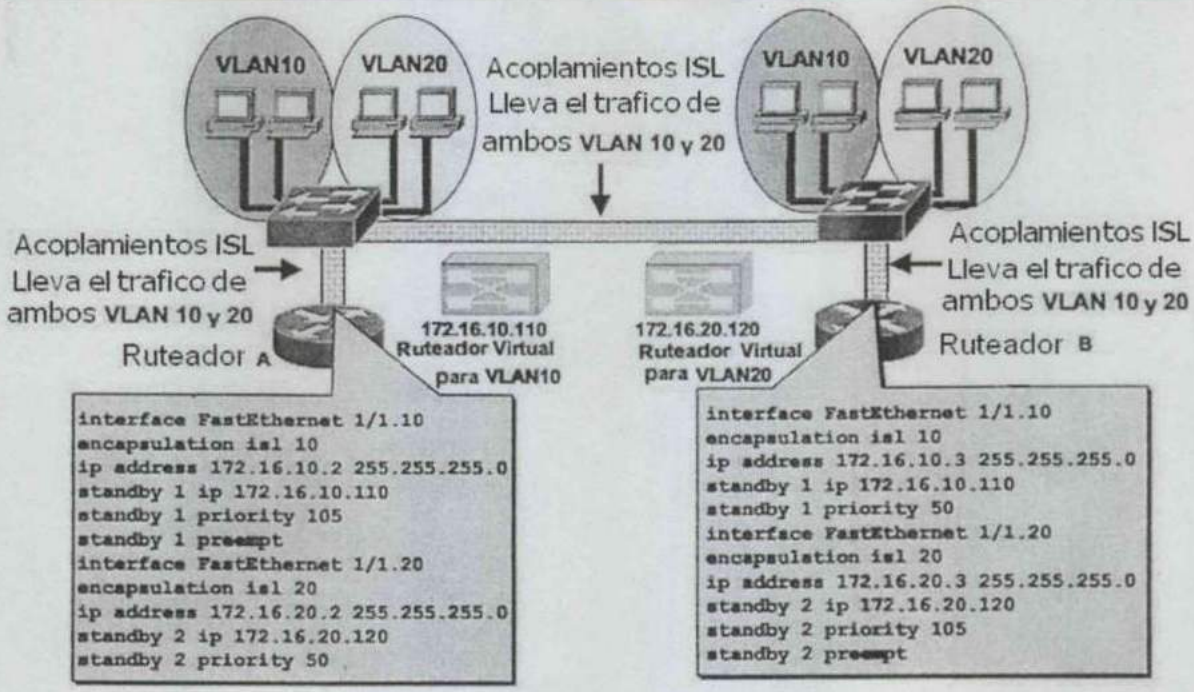



Figura 6.9 Ejemplo de acoplamientos ISL.

Para configurar HSRP sobre ISLs, los usuarios pueden eliminar las situaciones en las cuales un solo punto de falla causa interrupciones del tráfico. Esta característica inherente proporciona una cierta mejora en resistencia total del establecimiento de una red proporcionando capacidades carga-balance y de redundancia entre las subredes y VLANs.

Para configurar HSRP sobre un acoplamiento ISL entre VLANs, realice las tareas siguientes:

- Defina el formato de la encapsulación.
- Defina la dirección IP.
- Permita HSRP.

Los primeros dos pasos fueron vistos antes. Los pasos para permitir HSRP se discuten más adelante en este capítulo. Es importante decir que, un procesador de la ruta puede apoyar teóricamente hasta 32,650 subinterfaces; sin embargo, el número real de interfaces apoyados se limita a la capacidad del procesador de la ruta y al número de VLANs.

### 6.4.5. Múltiples grupos HSRP.

Los ruteadores pueden pertenecer a múltiples grupos en múltiples VLANs.

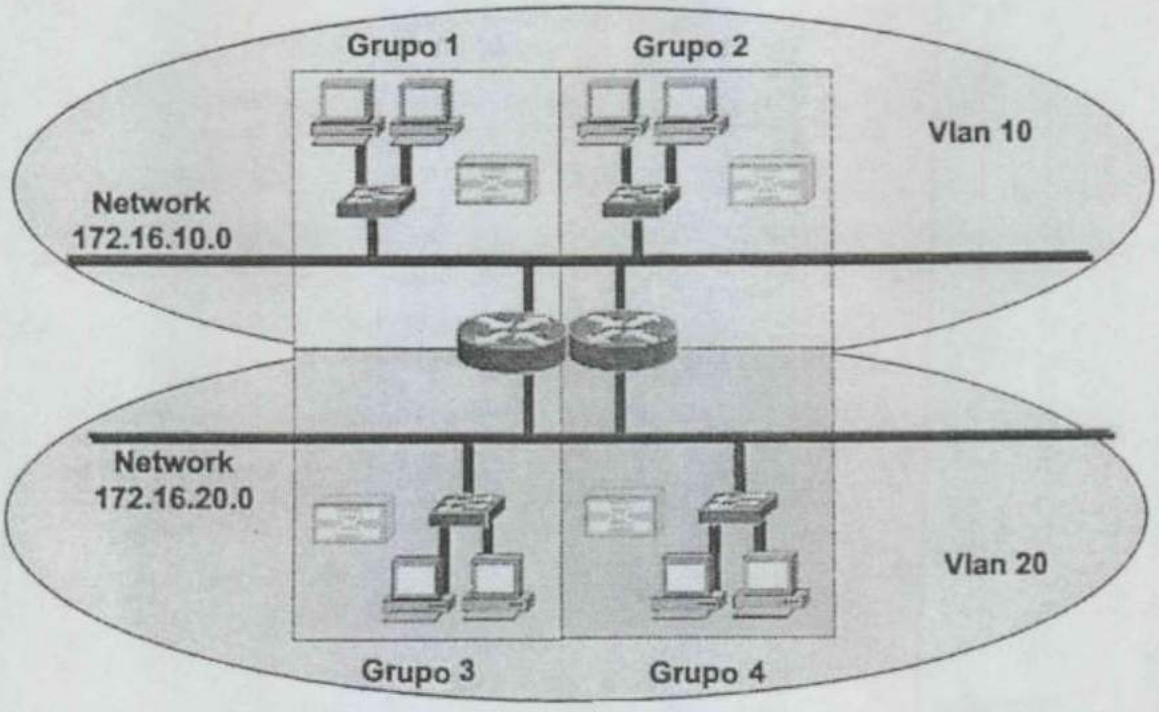



Figura 6.10. Ejemplo de múltiples grupos HSRP.

Los ruteadores pueden pertenecer a múltiples grupos dentro de múltiples VLANs, como se puede apreciar en la figura 6.10. Como miembros de múltiples grupos espera, los ruteadores pueden proporcionar simultáneamente la reserva redundante y realizar compartir de carga a través de diversas subredes IP.

Aunque múltiples ruteadores pueden existir en un grupo HSRP, sólo el ruteador activo remite los paquetes enviados al ruteador virtual.

Algo conveniente es mencionar que un grupo separado HSRP es configurado para cada subred VLAN.

## 6.5. CONFIGURACIÓN DE HSRP PARA RUTEO TOLERANTE POR DEFAULT.

En esta sección se cubren los siguientes aspectos:

- Los miembros de un grupo espera HSRP y los roles que cada miembro desempeña.
- Cómo interactúan los miembros de un grupo espera.
- El proceso que los miembros del grupo usan para delegar los roles y el estado a través del que cada ruteador pasa durante ese proceso.

### 6.5.1. Operaciones HSRP.

Esta sección discute como operan los ruteadores dentro de un grupo espera HSRP.

- Roles activo y espera del ruteador.
- Interacciones entre los ruteadores activo y espera.
- Estados de HSRP

#### *6.5.1.1. Designando un ruteador activo.*

- El ruteador con la prioridad HSRP más alta se convierte en el ruteador activo.
- El ruteador activo responde a las peticiones del ARP con la dirección MAC del ruteador virtual.

Dentro del grupo espera, un ruteador se elige para ser el ruteador activo. El ruteador activo remite los paquetes enviados al ruteador virtual. El ruteador con la prioridad espera más alta del grupo se convierte en el ruteador activo. La prioridad por *default* para un ruteador HSRP es 100; sin embargo, esta opción puede ser cambiada para el usuario final.

El ruteador activo responde al tráfico por el ruteador virtual. Si una estación final envía un paquete a la dirección MAC del ruteador virtual, el ruteador activo recibe y procesa ese paquete. Si una estación final envía una petición del ARP con la dirección IP del ruteador virtual, el ruteador activo contesta con la dirección MAC del ruteador virtual.

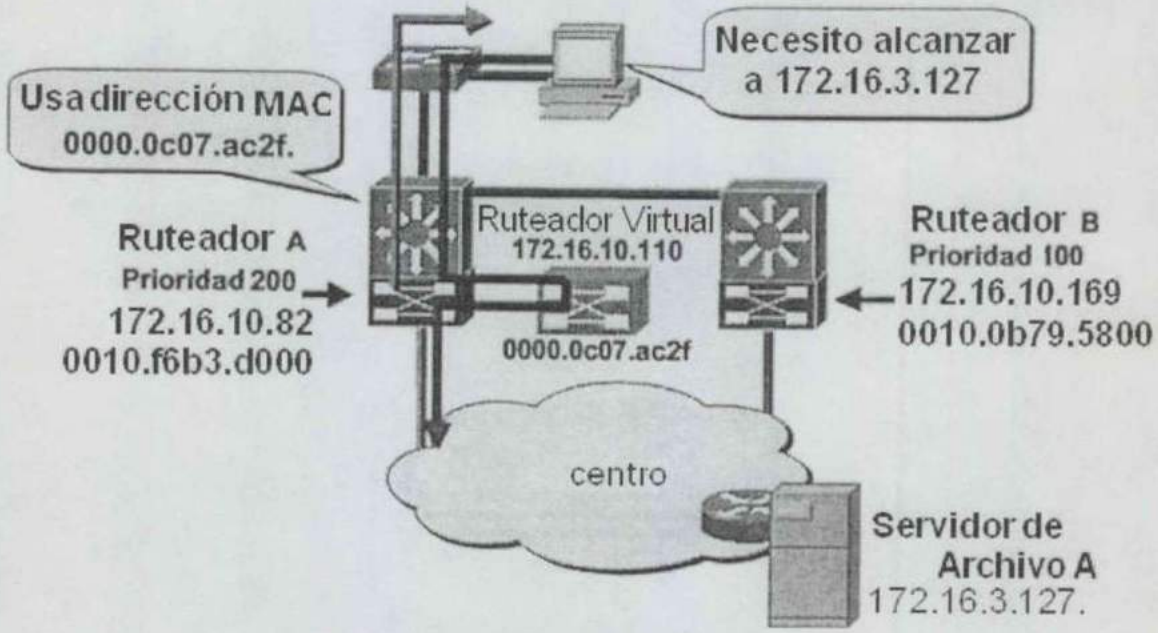



Figura 6.11. Ejemplo de prioridades HSRP.

En el ejemplo de la figura 6.11, el ruteador A tiene una prioridad de 200 y el ruteador B tiene una prioridad por *default* de 100. El ruteador A asume el rol del ruteador activo y remite todos los marcos dirigidos a la dirección MAC bien conocida de 0000.0c07.acxx, donde xx está es el identificador de grupo HSRP.

### *6.5.1.2. Localización de la dirección MAC del ruteador virtual.*

El ARP establece correspondencias entre las direcciones de red, tales como una dirección IP y una dirección del hardware *Ethernet*. Cada ruteador mantiene una tabla de direcciones resueltas.

El ruteador comprueba esta cache del ARP antes de procurar entrar en contacto con un dispositivo para determinarse si la dirección ha sido resuelta ya. La dirección IP y la dirección MAC correspondiente al ruteador virtual se mantiene en la tabla del ARP de cada ruteador en un grupo espera de HSRP.

Para exhibir el cache del ARP en un ruteador, incorpore el comando siguiente en modo privilegiado de EXEC; observe la figura 6.12.

```
Router#show ip arp
```

El funcionamiento de este comando exhibe la información siguiente.

| Campo | Definición |
|---|---|
| Protocolo | Protocolo para la dirección de red en el campo de dirección. |
| Dirección | La dirección de red que corresponde a la dirección del hardware. |
| Edad (min) | Edad, en minutos, de la entrada cache. |
| Dirección Hardware | La dirección MAC que corresponde a la dirección de red. |
| Tipo | Tipo de encapsulación: ARPA (Ethernet), SNAP (RFC 1042), o SAP (IEEE802.3). |
| Interfaz | Interfaz a el cual ha sido asignado el este mapeo de dirección. |

Figura 6.12. Campos del comando.

En el ejemplo mostrado en la figura 6.13, la salida exhibe un cache ARP para un Módulo de Conmutador Remoto o RSM que sea un miembro del grupo espera 47 de HSRP en VLAN10. El ruteador virtual para VLAN10 se identifica como 172.16.10.110. La

dirección MAC bien conocida que corresponde a esta dirección IP es 0000.0c07.ac2f, donde 2f es el identificador del grupo HSRP para el grupo espera 47.

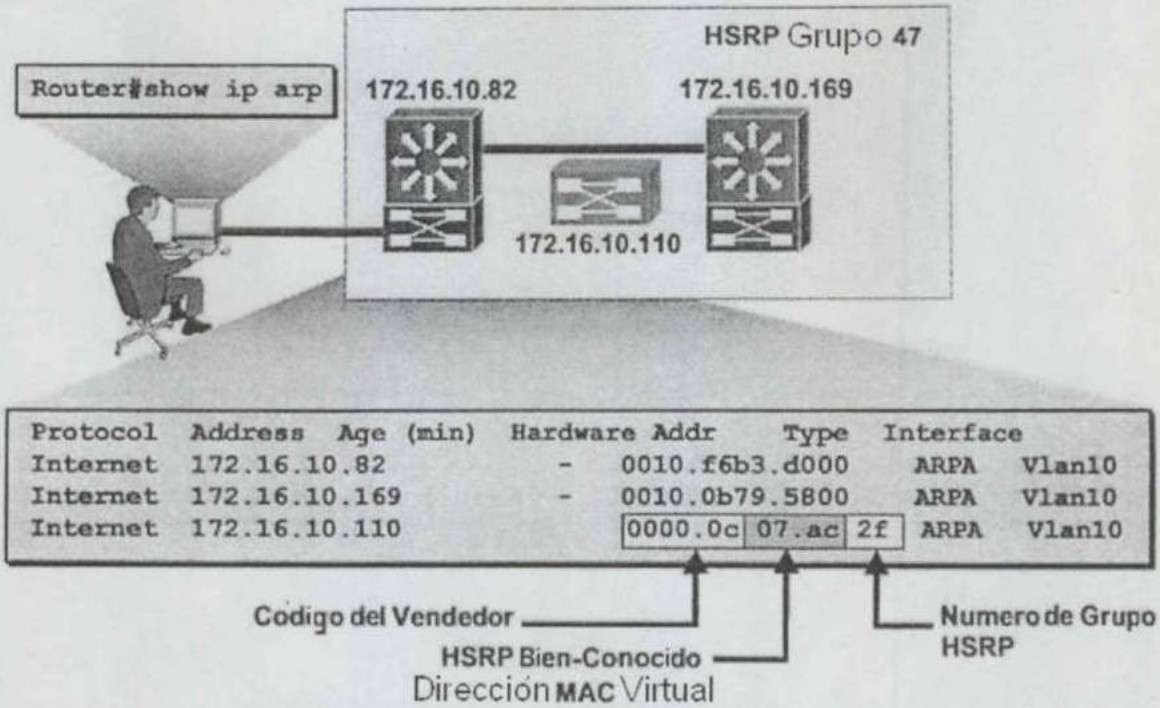



Figura 6.13. Ejemplo de dirección MAC virtual en un grupo HSRP.

Se puede también obtener el IP del ruteador virtual HSRP y la dirección MAC usando el comando del *show standby*. El comando *show standby* se ve más adelante en este capítulo

### *6.5.1.3. Interacción activa y secundaria del ruteador.*

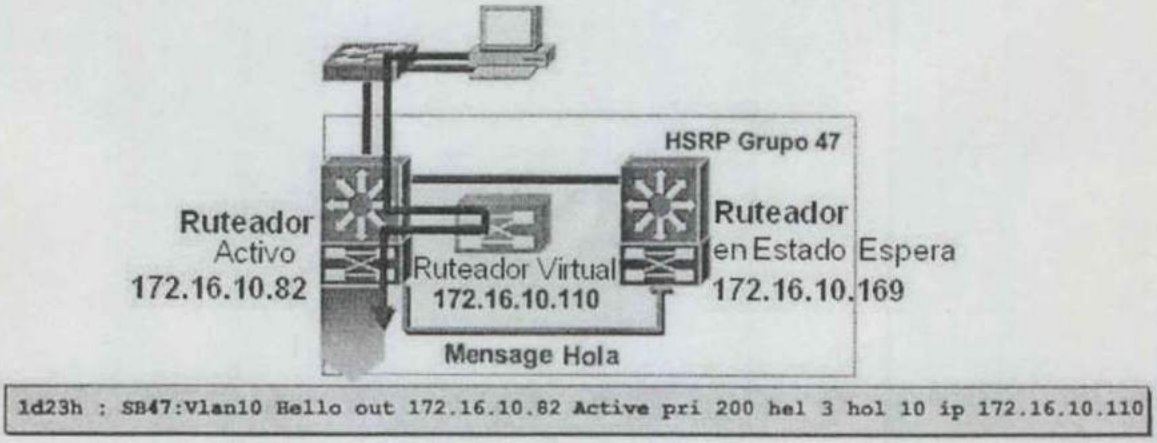



Figura 6.14. Ejemplo de entidades en un grupo HSRP.

Según lo anterior mencionado, cada grupo HSRP contiene las entidades, estas entidades se muestran en la figura 6.14 y son las siguientes:

- Un ruteador activo.
- Un ruteador espera.
- Un ruteador virtual

La función del ruteador activo es remitir los paquetes enviados al ruteador virtual. El ruteador activo asume y mantiene su rol activo a través de la transmisión de mensajes hola.

Otro ruteador en el grupo es elegido como mí ruteador espera. La función del ruteador espera es supervisar el estado operacional del grupo HSRP y asumir rápidamente la responsabilidad del paquete-remitido si el ruteador activo llega a ser inoperable. El ruteador espera también transmite mensajes hola para informar a el resto de los ruteadores en el grupo del rol y estado espera del ruteador.

La función del ruteador virtual es presentar un ruteador disponible constantemente al usuario final. Al ruteador virtual se asigna su propio IP y dirección MAC; sin embargo, el ruteador virtual no remite los paquetes.

Un grupo espera HSRP puede contener otros ruteadores. Estos ruteadores supervisan los mensajes hola pero no responden. Estos ruteadores remiten cualquier paquete tratado a las direcciones del IP de los ruteadores pero no remiten los paquetes paral ruteador virtual.

### *6.5.1.4. Interacción activa y secundaria del ruteador.*


Figura 6.15. Ejemplo de interacciones de ruteadores HSRP.

Cuando el ruteador activo falla, los otros ruteadores HSRP paran al recibir mensajes del hola, y el ruteador espera asume el papel del ruteador activo. Las interacciones de ruteadores se pueden observar en la figura 6.15.

Porque el nuevo ruteador activo asume las direcciones IP y MAC del ruteador virtual, las estaciones finales no consideran ninguna interrupción en servicio. Las estaciones del usuario final continúan enviando los paquetes a la dirección MAC del ruteador virtual y el ruteador activo nuevo entrega los paquetes a la destinación.

En caso que los ruteadores activo y espera fallen, todos los ruteadores en el grupo luchan para los papeles activo y espera del ruteador.

### 6.5.2. Formato de los Mensajes HSRP.

Los mensajes de HSRP utilizan la porción de los datos de un datagrama UDP.

Mientras que los ruteadores activo y espera envían mensajes HSRP, todos los ruteadores en un grupo espera reciben estos mensajes. Los mensajes HSRP se utilizan para determinar y para mantener los roles del ruteador dentro del grupo. Los mensajes HSRP se encapsulan en la porción de los datos de paquetes del Protocolo de Datagrama de Usuario o UDP, y utilizan el número de acceso 1985, el formato de mensajes HSRP se muestra en la figura 6.16. Estos paquetes son direccionados para un todo ruteador de la dirección *multicast* con un valor de Tiempo de Vida o TTL de uno.

| 1 Octeto | 1 Octeto | 1 Octeto | 1 Octeto |
|---|---|---|---|
| Version | Código Op | Estado | Hellotime |
| Holdtime | Prioridad | Grupo | Reservado |
| Datos de Autentificación | | | |
| Datos de Autentificación | | | |
| Dirección IP Virtual | | | |

Figura 6.16. Formato de mensajes HSRP

El mensaje HSRP contiene la información siguiente:

- El campo de la *Versión* indica la versión del HSRP.
- El *Código de Op.* describe el tipo de mensaje contenido en este paquete. Los valores posibles son:
    - Los mensajes Hola se envían para indicar que un ruteador está funcionando y es capaz de convertirse en el ruteador activo o espera.

- Los mensajes Golpe se envían cuando un ruteador desea convertirse en el ruteador activo.
- Los mensajes Dimita se envían cuando un ruteador ya no desea ser mas el ruteador activo.

- Internamente, cada ruteador en el grupo espera implementa un estado de la máquina. El campo de *Estado* describe el estado actual del ruteador que envía el mensaje.
- El campo de *Hellotime* es solamente significativo en mensajes hola. Este campo contiene el período aproximado entre los mensajes hola que son enviados por el ruteador. El tiempo se da en segundos.
- El campo de Holdtime es solo significativo en mensajes hola, el campo contiene la cantidad de tiempo que el mensaje actual hola debe ser válido, se da en segundos.
- El campo de la *Prioridad* se utiliza para elegir los ruteadores activo y espera. Al comparar prioridades de dos diferentes ruteadores, el ruteador con la prioridad numéricamente más alta gana. En el caso de ruteadores con prioridad igual, el ruteador con la dirección IP más alta gana.
- El campo *Grupo* identifica al grupo espera. Los valores 0 y 255, incluso son válidos.
- El campo *Datos de Autentificación* contiene la contraseña clear-text de 8-character.
- El campo *Dirección Virtual* contiene la dirección IP del ruteador virtual que usa este grupo.

Solamente los ruteadores activo y espera envían mensajes HSRP periódicos una vez que el protocolo haya terminado el proceso de la elección.

### 6.5.3. Seleccionar los ruteadores activas y espera.

```
3wld:%STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Init -> Listen
3wld:%STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Listen -> Speak
3wld:SB47:Vlan10 Hello out172.16.10.82 Speak pri150 hel 3 hol 10 ip
172.16.10.110
3wld:%STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Speak -> Standby
3wld:%STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Standby -> Active
3wld:SB47:Vlan10 Adding 0000.0c07.ac2f to address filter
```

HSRP define seis estados en los cuales un ruteador HSRP configurado puede existir. Cuando un ruteador existe en uno de estos estados, el ruteador realiza las acciones necesarias requeridas en ese estado.

Los estados de HSRP son como sigue:

- Estado inicial.
- Estado aprende.
- Estado escucha.
- Estado habla
- Estado espera.
- Estado activo.

No todas los ruteadores HSRP requieren la transición a través de todos los estados. Por ejemplo, un ruteador que no es espera o activo no incorporará los estados espera o activo.

### *6.5.3.1 Estado Inicial de HSRP.*

Ruteador en estado inicial.

- HSRP no está funcionando.

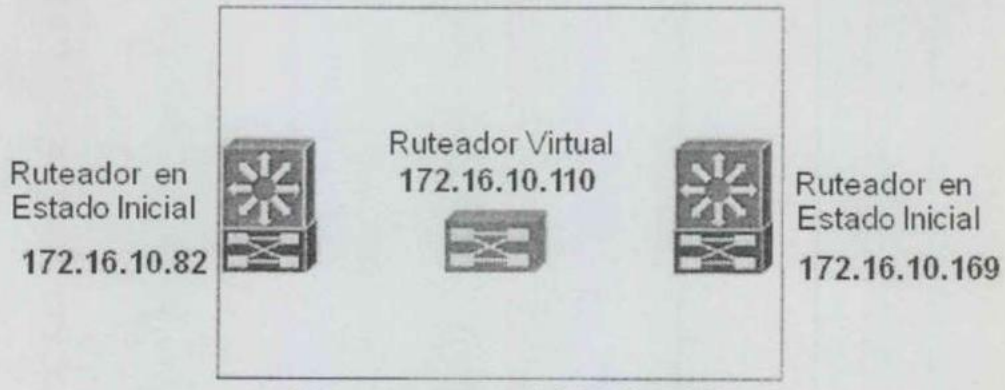



Figura 6.17. Estado inicial de HSRP.

Todos los ruteadores comienzan en el Estado Inicial. Éste es el estado que comienza e indica que HSRP no está funcionando.

Este estado se incorpora vía un cambio de configuración o cuando se inicia un interfaz. El estado inicial se muestra en la figura 6.17.

### *6.5.3.2. Estado Aprende de HSRP.*

Ruteador en estado aprende.

- No ha recibido un mensaje hola de un ruteador activo.
- No sabe la dirección IP del ruteador virtual.


Figura 6.18. Estado aprende de HSRP.

En el Estado Aprende, el ruteador todavía está esperando para oír al ruteador activo. El ruteador todavía no ha visto un mensaje hola del ruteador activo, ni ha aprendido la dirección IP del ruteador virtual. El estado aprende se muestra en la figura 6.18.

### *6.5.3.3. Estado Escucha de HSRP.*

Ruteador en estado escucha.

- Ni el ruteador activo ni espera.
- Recibe el mensaje hola (si cualquiera).
- Sabe la dirección IP del ruteador virtual.

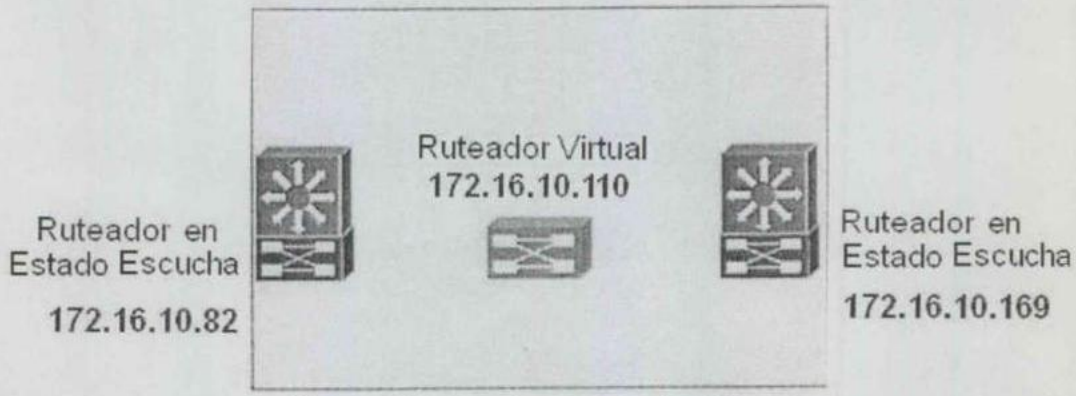



Figura 6.19. Estado escucha de HSRP.

En el Estado Escucha, el ruteador sabe la dirección IP virtual, pero ni es el ruteador activo ni el ruteador espera. El ruteador escucha mensajes hola de esos ruteadores. El estado escucha se muestra en la figura 6.19.

### *6.5.3.4.* Estado Habla de HSRP.

Ruteador en estado habla.

- Envía mensajes periódicos hola.
- Participa en la elección del ruteador activo y espera.
- Sabe la dirección IP del ruteador virtual.

En el Estado Habla, el ruteador envía mensajes periódicos hola y está participando activamente en la elección del ruteador activo y/o espera. Un ruteador no puede incorporar el estado Habla a menos que el ruteador me tenga la dirección IP del ruteador virtual. El estado habla se muestra en la figura 6.20.

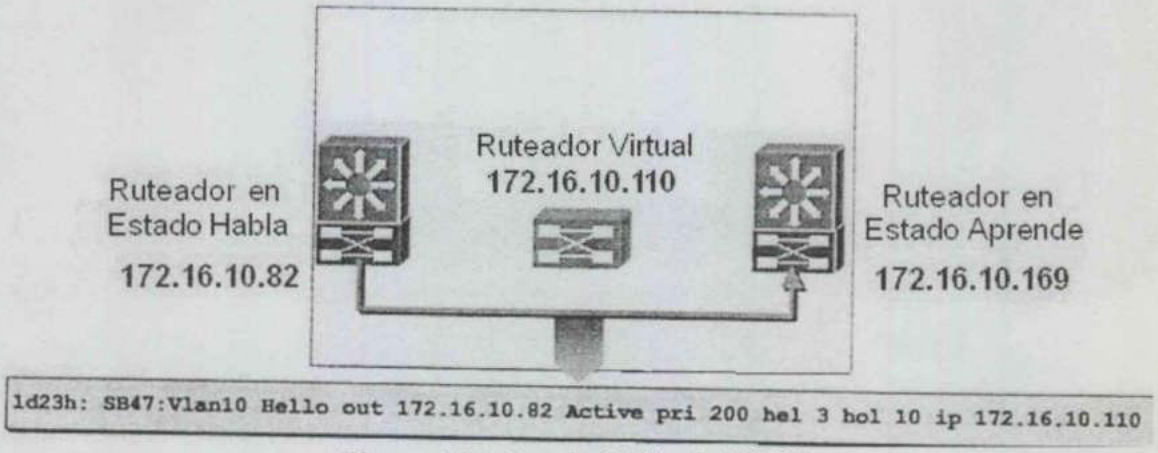



Figura 6.20. Estado Habla de HSRP.

### *6.5.3.5.* Estado Espera de HSRP.

En el Estado Espera, el ruteador es un candidato a convertirse en el siguiente ruteador activo y envía mensajes periódicos hola.

Ruteador en estado espera.

- Candidato a ruteador activo.
- Envía el mensaje hola.
- Sabe la dirección IP del ruteador virtual.

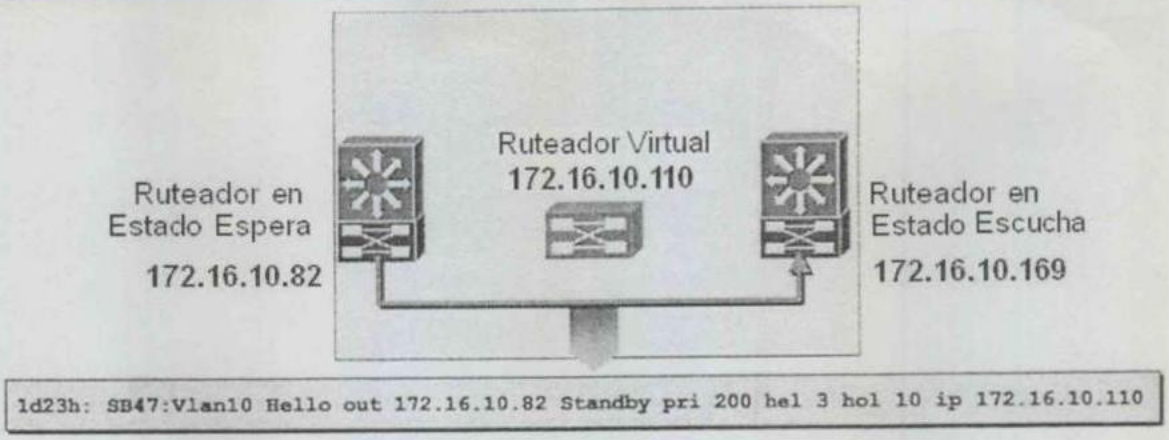



Figura 6.21. Estado Espera de HSRP.

Debe haber un ruteador espera en el grupo HSRP. El estado espera se ilustra en la figura 6.21.

### *6.5.3.6.* Estado Activo de HSRP.

- Asume el envió activo de los paquetes paral ruteador virtual.
- Envía mensaje hola.
- Sabe la dirección IP del ruteador virtual.

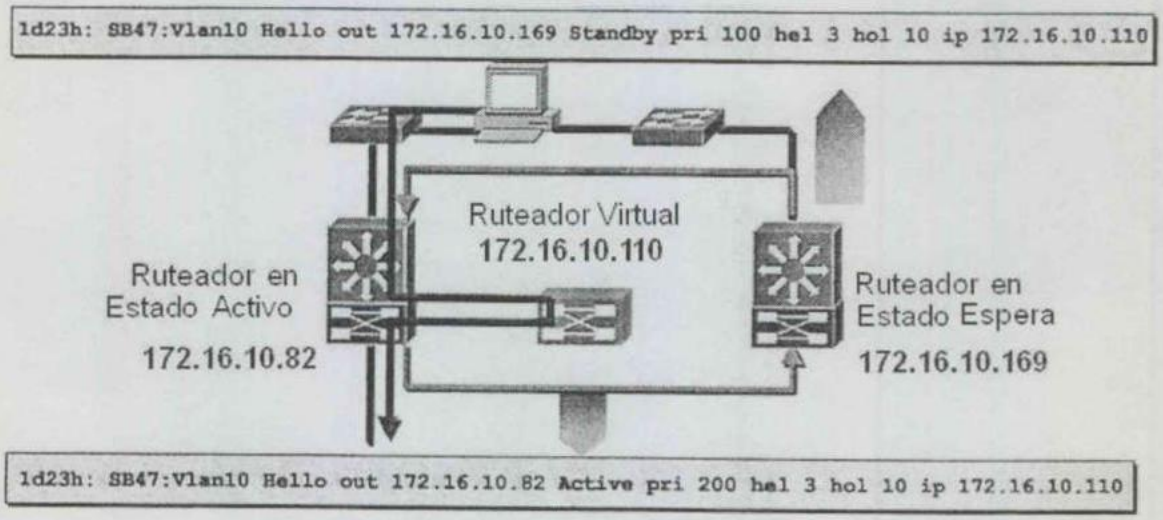



Figura 6.22. Estado Activo de HSRP.

En el Estado Activo, el ruteador esta actualmente remitiendo los paquetes que son enviados a la dirección MAC virtual del grupo. El ruteador activo envía mensajes periódicos hola. Debe haber un ruteador activo en el grupo HSRP. El estado activo se ve en la figura 6.22.

## 6.6. CONFIGURACIÓN DE HSRP.

La siguiente sección describe los pasos básicos requeridos para crear las entradas múltiples por *Default*. Para una lista completa de los comandos de HSRP, refiera a Servicios de configuración IP en la guía de configuración de los protocolos de red autorización 12.0 del IOS de Cisco.

Esta sección cubre los siguientes temas:

- Configuración de un interfaz para participar en un grupo espera HSRP.
- Configuración de la prioridad de un interfaz.
- Configurando la opción derecho preferente de espera en un interfaz.
- Seguir la configuración HSRP en un interfaz.
- Usar el comando *debug standby.*

### 6.6.1. Configuración e interfaz espera de HSRP.

Permitir HSRP en un interfaz del ruteador Cisco inhabilita automáticamente ICMP redireccionado, la configuración e interfaz espera de HSRP se ilustra en la figura 6.23.


Figura 6.23. Ejemplo de configuración e interfaz espera de HSRP.

Para configurar un ruteador como miembro de un grupo espera HSRP, incorpore el comando siguiente en modo configuración del interfaz y observe la figura 6.24.

```
Router (config-if) #standby group-number ip ip-address.
```

| Variable | Definición |
|---|---|
| *group-number* | (Opcional) indica el grupo HSRP a quien pertenece este interfaz. Especificar un número de grupo único en los comandos espera permite la creación de los grupos múltiples HSRP. El grupo por *default* es 0. |
| *Ip-address.* | Indica la dirección IP del ruteador virtual HSRP. |

Figura 6.24. Variables de comando.

Mientras que funciona HSRP, es importante que las estaciones del usuario final no descubran las direcciones reales del MAC de los ruteadores en el grupo espera. Cualquier protocolo que informe a un *host* la dirección real del ruteador debe ser deshabilitado. Asegurarse de que las direcciones reales de los ruteadores HSRP que participan no estén descubiertas, permitiendo HSRP en un interfaz del ruteador Cisco inhabilita automáticamente ICMP redirecionado en ese interfaz.

Una vez que es publicado el comando standby ip, el interfaz cambia al estado apropiado.

Cuando el ruteador ejecuta con éxito el comando, el ruteador publica un mensaje HSRP. Lo que sigue es un ejemplo de un mensaje del estado que pudo ser generado.

```
3w1d: %STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Speak -> Standby
3w1d: %STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Standby -> Active
```

El ejemplo siguiente indica que el interfaz VLAN10 es un miembro del grupo espera de HSRP 47, la dirección IP del ruteador virtual para ese grupo es 172.16.10.110, y que ICMP redireccionado es deshabilitado.

```
Router#show run
Building configuration...

Current configuration:
!
(text deleted)
interface Vlan10
ip address 172.16.10.82 255.255.255.0
no ip redirects
standby 47 ip 172.16.10.110
!
```

Para quitar un interfaz de un grupo HSRP, incorpore el comando **no standby** *grupo* **IP**.

### 6.6.2. Configuración de Prioridad de Espera HSRP.

- El ruteador en un grupo HSRP con la prioridad más alta se convierte en el siguiente ruteador.
- La prioridad por *default* es 100.

Cada grupo espera tiene sus propios ruteadores activo y espera. El administrador de la red puede asignar un valor de la prioridad a cada ruteador en un grupo espera, permitiendo que el administrador controle el orden en la cual los ruteadores activos para ese grupo son seleccionados. Un ejemplo de esta configuración se muestra en la figura 6.26.

Para fijar el valor de la prioridad de un ruteador, incorpore el comando siguiente en modo de la configuración del interfaz, observe la figura 6.25.

```
Router# (config-if) standby group-number priority priority-value
```

| Variable | Definicion |
|---|---|
| Número-grupo | Indica el grupo espera HSRP. Este número puede estar en el rango de 0 a 255. |
| Valor-prioridad | Indica el número que da la prioridad a un ruteador potencial de espera. El rango es 0 a 255; por *default* es 100. |

Figura 6.25. Variables de comando.

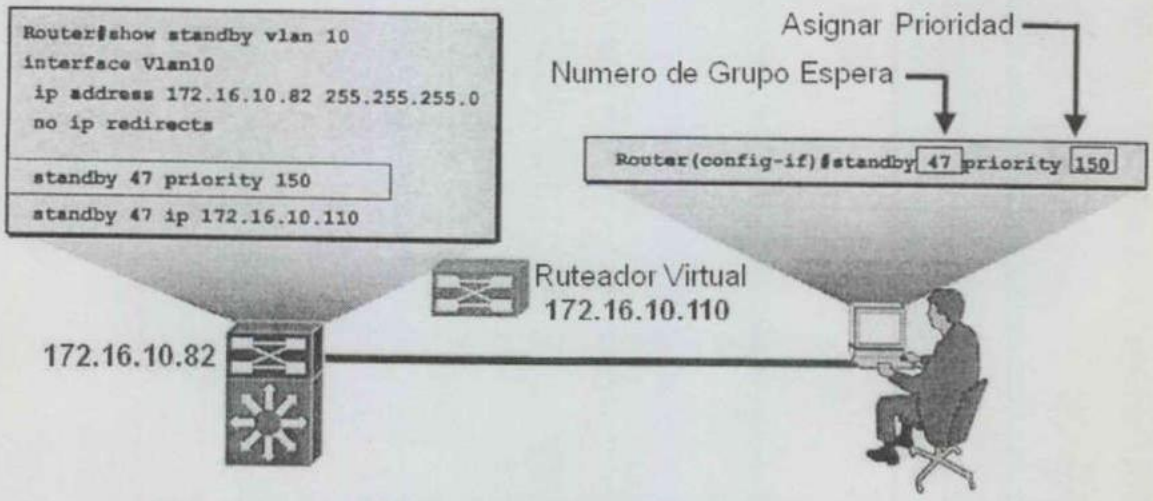



Figura 6.26. Ejemplo de configuración de prioridad de espera de HSRP.

Durante el proceso de la elección, el ruteador en un grupo HSRP con la prioridad más alta se convierte en el ruteador siguiente. El ejemplo siguiente indica que el interfaz VLAN10

tiene un valor de la prioridad de 150 en el grupo espera HSRP 47. Si este valor de la prioridad es el número más alto de eso grupo espera HSRP, entonces el dispositivo de ruteo en el cual este interfaz reside es el ruteador activo para ese grupo.

```
Router#show run
Building configuration...
Current configuration:
!
(text deleted)
interface Vlan10
ip address 172.16.10.32 255.255.255.0
no ip redirects
standby 47 priority 150
standby 47 ip 172.16.10.110
```

Al reinstalar el valor espera de la prioridad por *default*, incorpore el comando espera **no standby priority.**

### 6.6.3. Configuración de espera HSRP con derecho preferente.

El derecho preferente permite a un ruteador reasumir el rol del ruteador que remite.

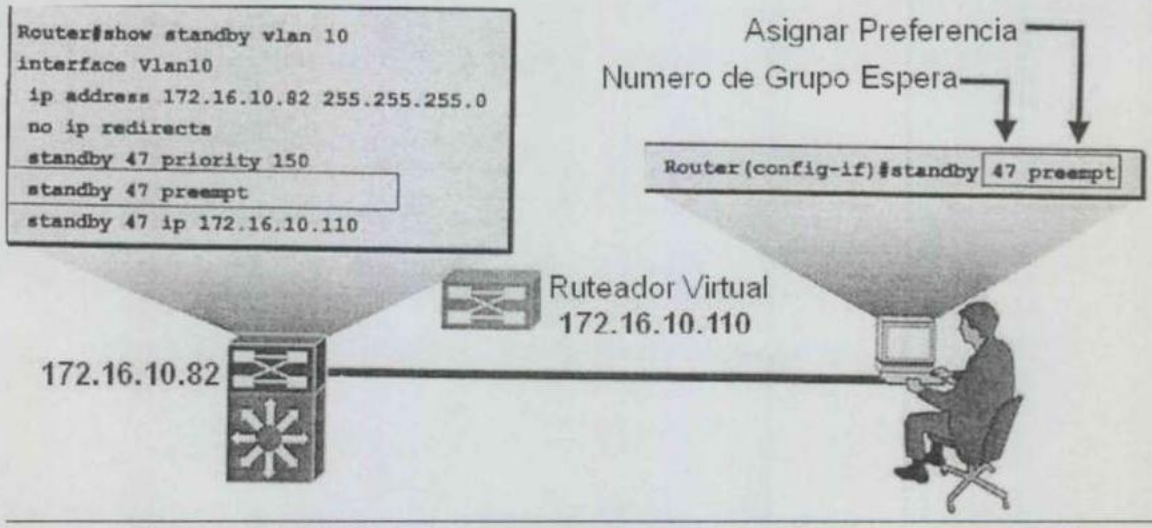



Figura 6.27. Ejemplo de configuración de espera HSRP con preferencia.

El ruteador espera asume automáticamente el rol del ruteador activo cuando el ruteador activo falla o es removido del servicio. Este nuevo ruteador activo sigue siendo el ruteador

que remite incluso cuando el ruteador activo anterior con la prioridad más alta recupera el servicio en la red. El ejemplo de esto se ilustra en la figura 6.27.

El ruteador activo anterior se puede configurar para reasumir el rol del ruteador que remite de un ruteador con una prioridad más baja. Para permitir a un ruteador reasumir el rol del ruteador que remite, incorporar el comando siguiente en modo de configuración del interfaz.

```
Router (config-if) #standby group-number preempt
```

Una vez que el comando espera con derecho preferente es publicado, el interfaz cambia al estado apropiado. Lo siguiente es un ejemplo del estado del mensaje generado. Este mensaje se genera automáticamente tan pronto como el ruteador llega a ser activo en la red.

```
3w1d: %STANDBY-6-STATECHANGE: Standby: 47: Vlan10 state Standby -> Active
```

El ejemplo siguiente indica que el interfaz VLAN10 está configurado para reasumir su rol como el ruteador activo en el grupo HSRP 47, el interfaz asumido VLAN10 en este ruteador tiene la prioridad más alta en ese grupo espera.

```
Router#show run
Building configuration...

Current configuration:
!
(text deleted)
interface Vlan10
ip address 172.16.10.82 255.255.255.0
no ip redirects
standby 47 priority 150
standby 47 preempt
standby 47 ip 172.16.10.110
```

Para quitar el interfaz del estado con derecho preferente, incorporar el comando **no standby** *grupo* **preempt**.

### 6.6.4. Configuración los contadores de mensaje hola.

El *holdtime* debe ser por lo menos tres veces el valor del *hellotime*.

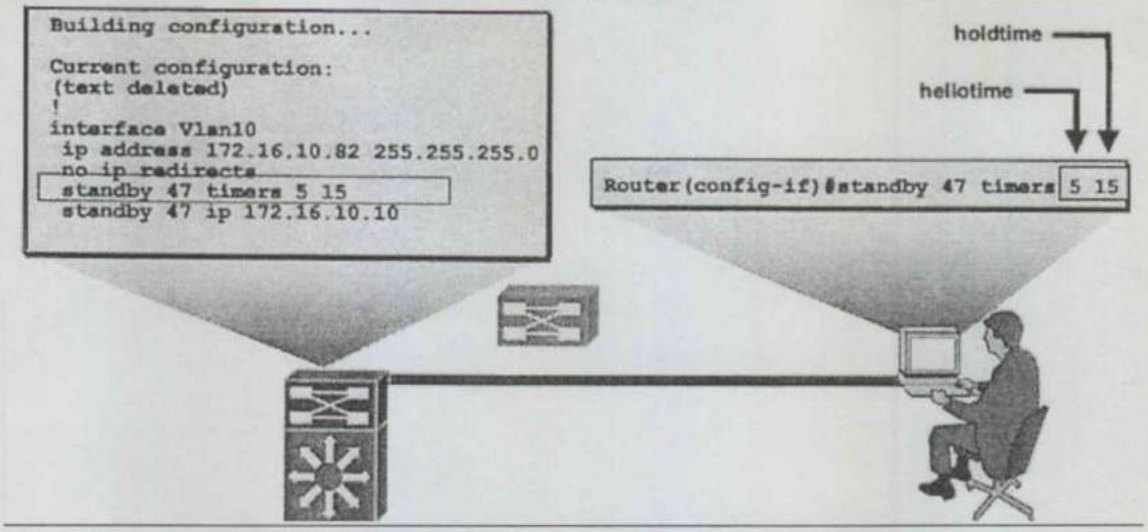



Figura 6.28. Ejemplo de valores *holdtime* y *hellotime*.

Un ruteador permitido HSRP envía mensajes hola para indicar que el ruteador está funcionando y es capaz de convertirse en el ruteador activo o espera. El mensaje Hola contiene la prioridad del ruteador, así como un valor *hellotime* y del *holdtime*. El valor de *hellotime* indica el intervalo entre los mensajes hola que el ruteador envía. El valor del *holdtime* contiene la cantidad de tiempo que el mensaje hola actual se considera válido.

Si un ruteador activo envía un mensaje hola, después de recibir los ruteadores consideran ese mensaje hola es válido para un *holdtime*. Observe el *holdtime* podría ser por lo menos tres veces el valor del *hellotime*, y debe ser mayor que el *hellotime*, ver la figura 6.28.

Ambos parámetros el *hellotime* y el *holdtime* son configurables. Para configurar el tiempo entre los mensajes hola y el tiempo antes de que otro grupo de ruteadores declaren el ruteador activo o espera no esta en funcionamiento, incorpore el comando siguiente en modo de la configuración del interfaz, observe la figura 6.29.

```
Router (config-if)#standby grupo-numero timers hellotime holdtime
```

| Variable | Description |
|---|---|
| *grupo-numero* | (Opcional) El numero de grupo en el interfaz al cual los contadores de tiempo se aplican. El número de grupo por *default* es 0. |
| *hellotime* | Intervalo del hola en segundos. Esto es un número entero a partir la 1 a 255. El número por *default* es 3 segundos. |
| *holdtime* | El tiempo, en segundos, antes de que el ruteador activo o espera sea declarado para ser dados de baja. Este es un número entero a partir la 1 a 255. El número por *default* es 10 segundos. |

Figura 6.29. Variables de comando.

Al reinstalar los valores del contador de tiempo de espera por *default*, incorporar el comando **no standby** *grupo* **timers.**

### 6.6.5. Seguimiento del Interfaz HSRP.

En algunas situaciones, el estado de un interfaz afecta directamente al ruteador que necesite convertirse en el ruteador activo. Esto es particularmente verdad cuando cada uno de las ruteadores en un grupo HSRP tiene una trayectoria distinta a los recursos dentro de la red del campus.

En el ejemplo de la LAN del campus, mostrado en la figura 6.30, el ruteador A y el ruteador B residen en una sucursal. Cada uno de estos dos ruteadores soportan un acoplamiento T1 a las jefaturas. El ruteador A tiene la prioridad más alta y es el ruteador activo que remite para el grupo espera 47. El ruteador B es el ruteador espera para ese grupo. El ruteador A y B están intercambiando mensajes hola a través de sus interfaces E0.

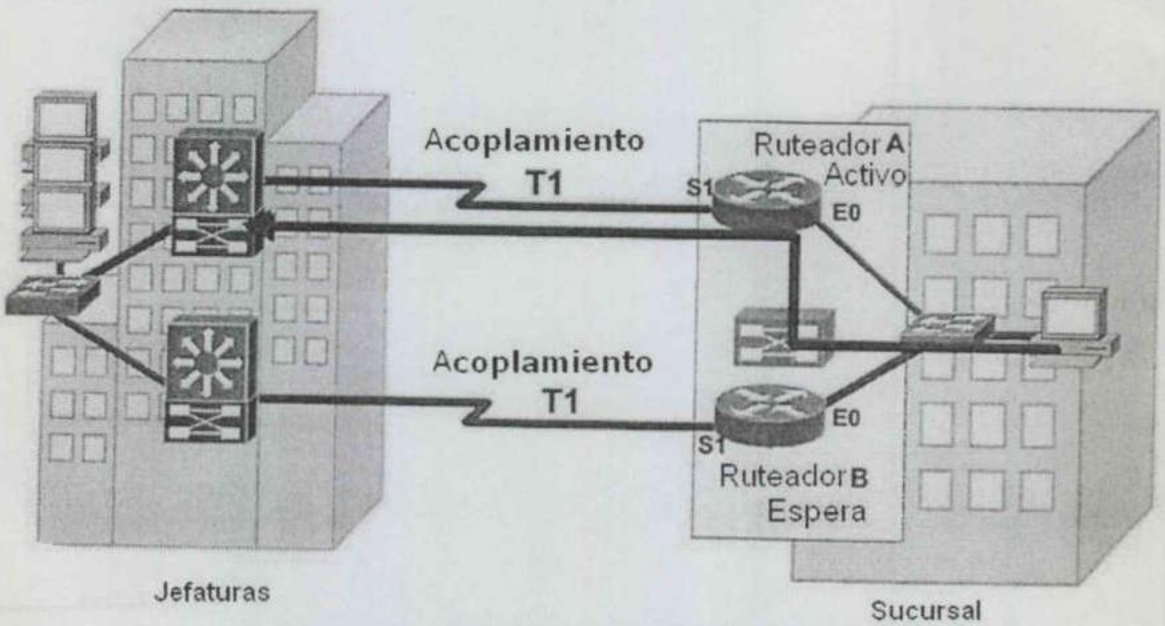



Figura 6.30. Ejemplo de seguimiento del interfaz HSRP.

El acoplamiento T1 entre el ruteador activo que remite para el grupo espera y las jefaturas experimenta una falta. Sin HSRP permitido, el ruteador A detectaría el acoplamiento fallado y envía un ICMP redireccionado al ruteador B. Sin embargo, cuando HSRP es permitido, el ICMP redireccionado esta deshabilitado.

Por lo tanto, ni el ruteador A ni el ruteador virtual envía un ICMP redireccionado y, aunque el interfaz S1 en el ruteador A no es funcional más largo, el ruteador A todavía comunica mensajes hola fuera del interfaz E0 que indicando que el ruteador A sigue siendo el ruteador activo.

Los paquetes enviados al ruteador virtual para el envió a las jefaturas no pueden ser ruteados. El seguimiento del interfaz permite a la prioridad de un ruteador del grupo espera automáticamente sea ajustada basada en la disponibilidad de las interfaces de ese ruteador.

Cuando seguimiento del interfaz llega a ser invalido, la prioridad HSRP del ruteador se disminuye. El seguimiento de la característica HSRP reduce la probabilidad que un ruteador con interfaz dominante invalido seguirá siendo el ruteador activo, ver figura 6.31.

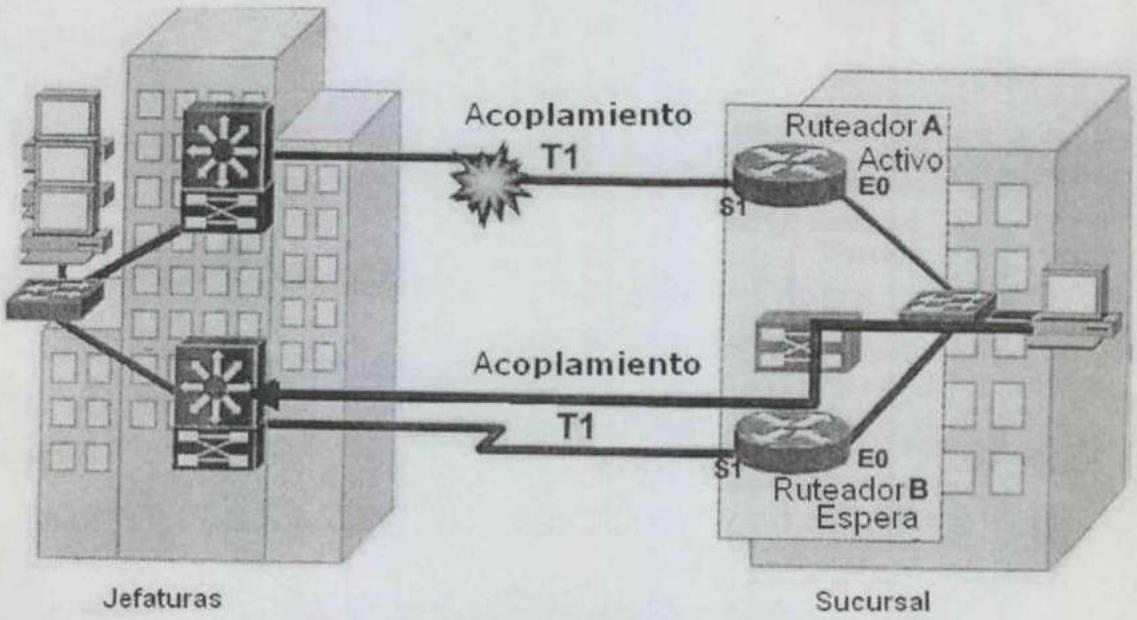



Figura 6.31. Ejemplo de seguimiento del interfaz HSRP.

En este ejemplo de la LAN del campus, el interfaz E0 en el ruteador A sigue al interfaz S1. Si el acoplamiento entre el interfaz S1 y las jefaturas falla, el ruteador automáticamente decrementa su prioridad en ese interfaz y detiene la transmisión de mensajes hola fuera del interfaz E0.

El ruteador B asume el rol del ruteador activo cuando no se detecta mensajes hola para el período específico del *holdtime*.

### 6.6.6. Seguimiento de Configuración HSRP: Ruteador Externo.

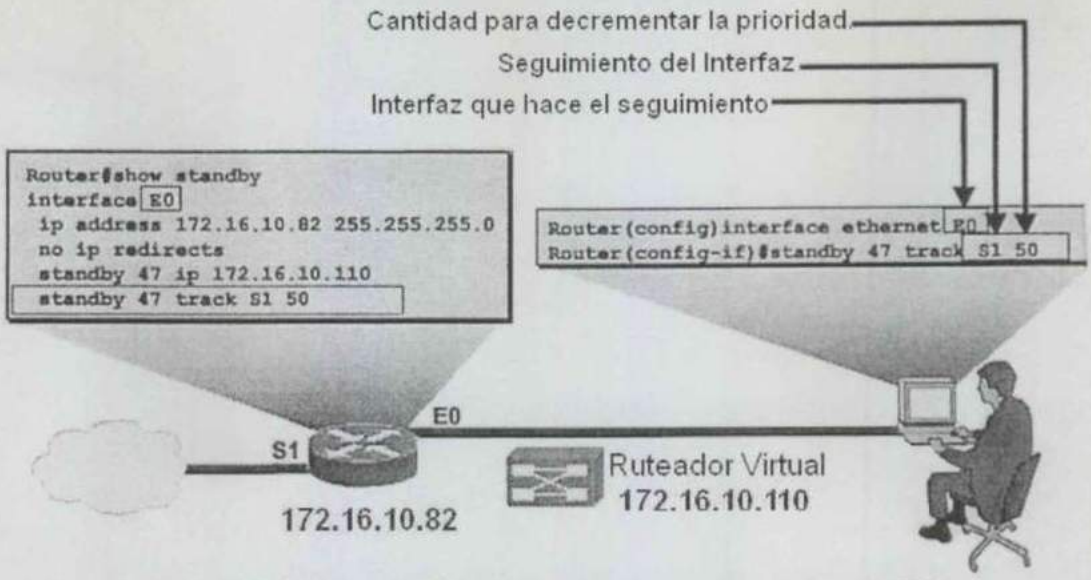



Figura 6.32. Ejemplo de seguimiento de configuración HSRP.

Para el seguimiento de la configuración HSRP, figura 6.32; incorpore el comando siguiente en modo de configuración del interfaz, observe la figura 6.33.

Router (config-if) **#standby** *group-number* **track** *type-number interface-priority*

| Variable. | Descripcion. |
|---|---|
| *grupo-numero.* | (Opcional) indica el número de grupo en el interfaz a el cual el seguimiento se aplica. El número por *default* es 0. |
| *Tipo.* | Indica el tipo del interfaz (combinado con el número del interfaz) que será seguido. |
| *Numero.* | Indica el número del interfaz (combinado con el tipo del interfaz) que será seguido. |
| *Interfaz-prioridad.* | (Opcional) indica la cantidad por la cual la prioridad espera para el ruteador es decrementada cuando el interfaz llega a ser invalido. La prioridad del ruteador es incrementada por esta cantidad cuando el interfaz llega a estar disponible. El valor por *default* es 10. |

Figura 6.33. Variables de comando.

Para inhabilitar el seguimiento del interfaz, incorpore el comando **no standby** *grupo* **track**.

### 6.6.7. Seguimiento de Configuración HSRP: Ruteador Interno.

El comando para el seguimiento de configuración HSRP en un RSM, el mismo que en el ruteador externo excepto el tipo del interfaz es identificado como **vlan** seguido por el *número vlan* asignado a ese interfaz, figura 6.34.

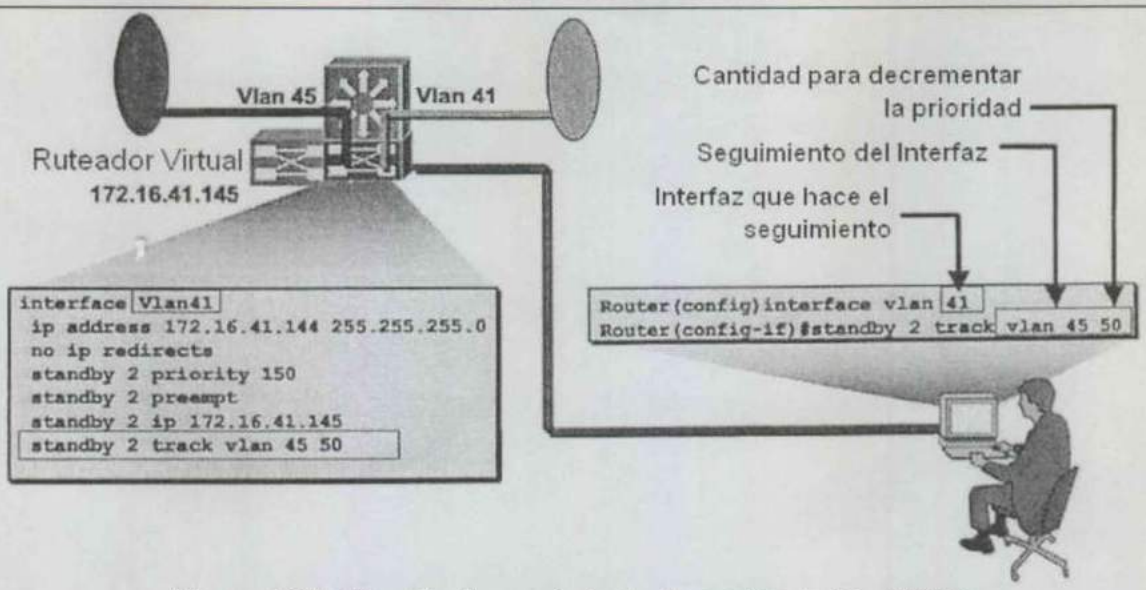



Figura 6.34. Ejemplo de seguimiento de configuración HSRP.

El dispositivo interno de ruteo utiliza el mismo comando que el dispositivo de ruteo externo para inhabilitar el seguimiento del interfaz.

### 6.6.8. Exhibir el breve estado espera.

Para exhibir el estado HSRP del ruteador, incorporar el comando siguiente en modo privilegiado de EXEC. Observe la figura 6.35.

```
Router#show standby tipo-numero grupo brief
```

| Variable. | Descripción. |
|---|---|
| *Tipo-number.* | (Opcional) indica el tipo y el número del interfaz del blanco para el cual se exhibe la salida. |
| *Grupo.* | (Opcional) indica un específico grupo HSRP en el interfaz para el cual se exhibe la salida. |
| **Brief** (escrito) | (Opcional) exhibe una sola línea de la salida que resume cada grupo espera. |

Figura 6.35. Variables de comando.

Si los antedichos parámetros opcionales del interfaz no son indicados, el comando **show standby** exhibe la información HSRP para todos los interfaces. Debajo está un ejemplo de la salida que resulta cuando usted especifica los parámetros del *tipo-numero y grupo.*

```
Router#show standby Vlan10 47
Vlan11 - Group 47
```

```
Local state is Active, priority 150 y may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.944
Hot standby IP address is 172.16.10.110 configured
Active router is local
Standby router is 172.16.10.82 expires in 00:00:08
Standby virtual mac address is 0000.0c07.ac2f
Tracking interface states for 1 interface, 1 up.
   Up Vlan51 Priority decrement: 40
```

El estado local es activo, la prioridad 150 y puede adquirir con derecho preferente

El ruteador activo configurado es local

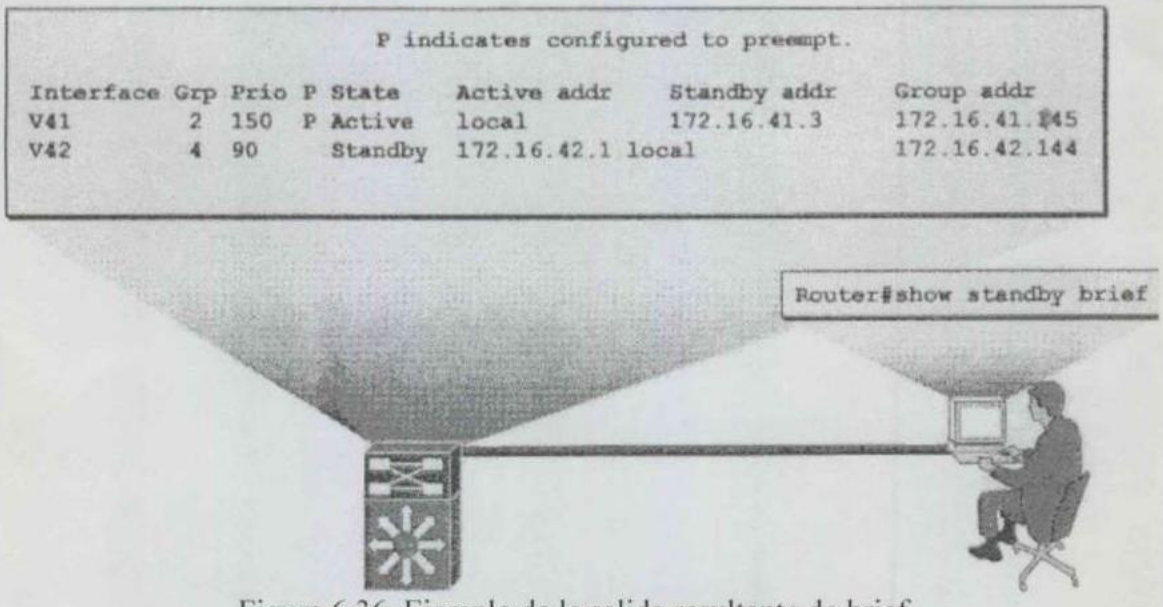



Figura 6.36. Ejemplo de la salida resultante de brief.

En la figura 6.36; está un ejemplo de la salida resultante cuando usted especifica el parámetro **brief**.

```
Router#show standby brief
```

| Interface | Grp | Prio | P | State | Active addr | Standby addr | Group addr |
|---|---|---|---|---|---|---|---|
| V110 | 47 | 150 | P | Active | local | 172.16.10.82 | 172.16.11.10 |
| V112 | 12 | 100 | | Standby | 172.16.102.82 | local | 172.16.12.10 |

No se debe olvidar que cuando especifica un grupo, usted debe señalar un interfaz.

### 6.6.9. Usar el comando de eliminar errores de espera.

```
Router#debug standby
3w1d: %STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Init ->
Listen
3w1d: %STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Listen ->
Speak
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: %STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Speak ->
Standby
3w1d: %STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Standby ->
Active
3w1d: SB47:Vlan10 Adding 000.0c07.ac2f to address filter
3w1d: SB47:Vlan10 Adding 000.0c07.ac2f to address filter
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
```

La puesta en práctica de HSRP del IOS de Cisco apoya el comando **debug**. Permite el eliminar errores con facilidad ya que exhibe los cambios del estado HSRP y elimina errores de información con respecto la transmisión y recepción de los paquetes HSRP. Para permitir que HSRP elimine errores, incorpore el comando siguiente en modo privilegiado de EXEC.

```
Router#debug standby
```

Se debe tener precaución; porque salida el eliminar errores se asigna la alta prioridad en el proceso de la CPU, este comando puede hacer el sistema inutilizable

El siguiente ejemplo exhibe el comando **debug standby** salida como el ruteador con la dirección IP 172.16.10.82 se inicializa y negocia para el rol del ruteador activa.

```
3w1d:%STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Init ->
Listen
3w1d:%STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Listen ->
Speak
3w1d:SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10 ip
172.16.10.110
3w1d:SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10 ip
172.16.10.110
3w1d:SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10 ip
172.16.10.110
3w1d: SB47:Vlan10 Hello out172.16.10.1 Speak pri150 hel 3 hol 10
ip 172.16.10.110
3w1d: %STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Speak ->
Standby
3w1d: %STANDBY-6-STATECHANGE: Standby: 47 Vlan10 state Standby ->
Active
3w1d: SB47:Vlan10 Adding 000.0c07.ac2f to address filter
```

Para inhabilitar la característica que elimina errores, incorpore el comando **no debug standby** or **the no debug all**.

No olvidar que una versión corta de la salida de la eliminación de errores es asignada prioridad alta en el proceso del CPU, este comando puede contribuir a inhabilitar el sistema <cr><cr>u todo.

La figura 6.37, ilustra un ejemplo de bloque de conmutación HSRP, tal que fue un concepto nombrado en varias ocasiones dentro de los últimos capítulos.

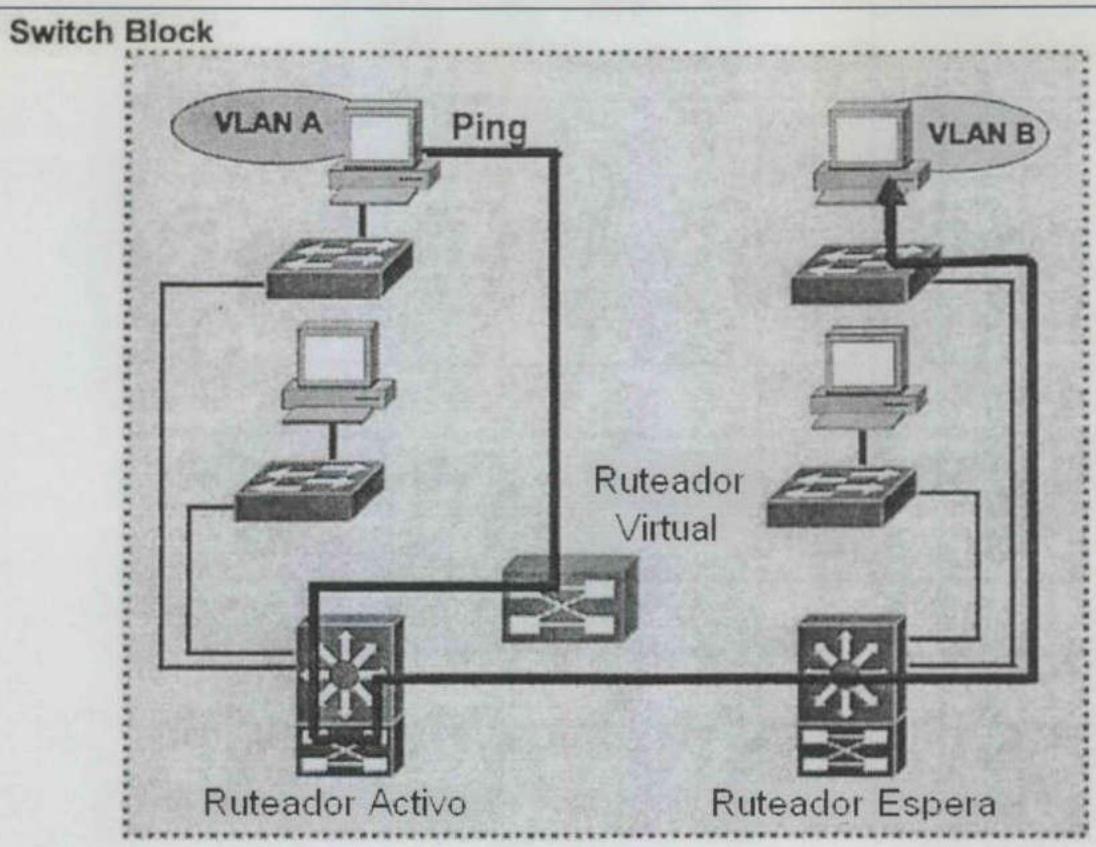



Figura 6.37. Ejemplo de bloque de conmutación HSRP.

## GLOSARIO DE TÉRMINOS.

| | |
|---|---|
| AARP | AppleTalk Address Resolution protocol |
| AFP | AppleTalk Filing Protocol |
| ANSI | American National Standards Institute |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| ARQ | Automatic Request for Repeat |
| ASCII | American Standard Code of Information Interchange |
| ATM | Asynchronous Transfer Mode |
| ATP | AppleTalk Transaction Protocol |
| ADCCP | Advanced Data Communication Control Procedure |
| BDC | Backup Domain Controller |
| BGP | Border Gateway Protocol |
| BOP | Bit Oriented Protocol |
| BSC | Binary Synchronous Comunications |
| CCITT | Consultative Committee for International Telegraph and Telephone |
| CDDI | Interfaz de Datos Distribuidos por Cable |
| CDPD | Celular Digital Packet Data |
| CIR | Tasa de Información Asegurada |
| CPPD | Paquete Celular Digital de Datos |
| CRC | Cyclical Redundancy Checking |
| CSMA | Carrier Sense Multiple Access |
| CSMA/CD | Carrier Sense Multiple Access with Collision |
| DDP | Datagram Delivery Protocol |
| DEC | Digital Equipment Corporation |
| DNA | Digital Network Architecture |
| DNS | Domain Name Server |
| DQDB | Distributed Queue Dual Bus |
| EBCDIC | Código de Intercambio de Código Binario y Decimal Extendido |

| | |
|---|---|
| EIGRP | Enhanced Interior Gateway Routing Protocol |
| FDDI | Interfaz de Datos Distribuidos por Fibra |
| FDM | Frequency Division Multiplexion |
| FTP | File Transfer Protocol |
| FCS | Frame Check Sequence |
| GDP | Gateway Discovery Protocol |
| GUI | Graphical User Interface |
| GSM | Groupe Special Mobile |
| HEC | Header Error Control |
| HDLC | High-level Data Link Control |
| HOSTS | PCs, word stations, servers and otters |
| HTTP | HyperText Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| ICMP-R | Internet Control Message Protocol Redirect |
| IDU | Interface Data Unit |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IGRP | Interior Gateway Routing Protocol |
| IOS | Internet Operative System |
| IP | Internet Protocol |
| IPV6 | Internet Protocol Version 6 |
| IPDC | Internet Protocol Device Control |
| IRDP | Router Discovery Protocol |
| ISDN | Integrated Services Digital Network o RDSI |
| ISL | Inter – Switching Link |
| ISO | International Organization for Standardization |
| ITU | International Telecommunication Union |
| ITU-T | International Telecommunication Union Telecommunication Standardization Sector |
| IPC | Inter-Process Communication |

| | |
|---|---|
| IPS | Internet Protocol Suite |
| IPX | Inter-network Packet eXchange |
| IPX/SPX | Inter-network Packet eXchange / Sequence Packet eXchange |
| LAN | Local Area Network |
| LAP | Link Access Procedure |
| LCP | Link Control Protocol |
| LLC | Logical Link Control |
| MAC | Medium Access Control |
| MAN | Metropolitan Area Network |
| NIC | Number Identification Control |
| NBP | Name Binding Protocol |
| NCP | Network Core Protocol |
| NCP | Network Control Protocol |
| NSF | National Science Foundation |
| NVRAM | No Volatile RAM |
| OAM | Operation And Maintance |
| OSI | Open Systems Interconnection |
| OSPF | Open Shortest Path First |
| PC | Personal Computer |
| PCI | Protocol Control Information |
| PDA | Personal Digital Assistants |
| PDU | Protocol Data Unit |
| POP | Post Office Protocol |
| PPP | Point – to - Point Protocol |
| PRI | Primary Rate Interface |
| RFC | Requests For Comments |
| ROM | Read Only Memory |
| RAM | Random Access Memory |
| RARP | Reverse Address Resolution Protocol |
| RIP | Routing Information Protocol |

| | |
|---|---|
| RSM | Remote Switching Module |
| RTC | Red Telefónica Conmutada |
| SAP | Service Advertising Protocol |
| SAP | Service Access Point |
| SDLC | Synchronous Data Link Control |
| SDU | Service Data Unit |
| SIP | Status Indicator Processor |
| SLIP | Series Line IP |
| SMB | Server Message Block |
| SMTP | Simple Mail Transport Protocol |
| SNMP | Simple Network Management Protocol |
| SPX | Sequence Packet eXchange |
| SSH | Secure SHell |
| STP | Spanning Tree Protocol |
| TCP | Transport Control Protocol |
| TCP/IP | Transport Control Protocol / Internet Protocol |
| TDM | Time Division Multiplexion |
| TELNET | Terminal Virtual |
| TTL | Time to Live |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| VC | Virtual Circuit |
| VCI | Virtual Circuit Indicator |
| VLAN | Virtual LAN |
| VCPI | Virtual Control Program Interface |
| WAN | Wide Area Net |
| WDM | Wavelenght Division Multiplexing |
| ZIP | Zone Information Protocol |

## BIBLIOGRAFIA

**En Libros:**

Cisco Training and Certification -Learning the way you want it. *BSMSN; Building Cisco Multilayer Switched Networks, volume 2, version 1.0. Student Guide.*Copyright 2002; Cisco Systems, Inc.

Cisco Training and Certification -Learning the way you want it. *BSMSN; Building Cisco Multilayer Switched Networks, volume 2, version 2.0, Student Guide.* Copyright 2003; Cisco Systems, Inc.

Tanenbaum, Andrew S., *Redes de Computadoras,* PERSON EDUCACION S.A. Mexico, 1997. Prentice Hall. 3ª. Edición.

Conner, Douglas E., *Redes Globales de Información con Internet y TCP/IP*, Prentice Hall. 1ª Edición.

**Artículos.**

*"Redes de comunicación"*, Enciclopedia Microsoft(R) Encarta(R) 98. (c) 1993-1997 Microsoft Corporation.

**En Internet.**

http://www.cisco.com

http://www.cisco.com/warp/public/459/hsrp_bgp.html

http://www.cisco.com/warp/public/619/hsrpguidetoc.html

http://www.cisco.com/warp/public/619/3.html

http://www.cisco.com/warp/public/619/6.html

http://www.cisco.com/warp/public/619/hsrpmcast.html

http://www.cisco.com/warp/public/619/7.html

http://www.cisco.com/warp/public/619/8.shtml

http://www.cisco.com/warp/public/619/hsrpguidetoc.html

http://www.cisco.com/public/"Cisco - Implementing HSRP Over LANE.htm"

http://www.cisco.com/public/"Cisco - HSRP Support - No_ 768.htm"

http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/1214ea1/3550scg/swhsrp.html

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/redund.html

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_hsrpi.html

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/icdip.htm

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080093f2c.shtml

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_Tech_note09186e0080094e8c.shtml

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_Tech_note09186e0080094a91.shtml

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_Tech_note09186e0080093f93.shtml

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_Tech_note09186e0080094e8c.shtml

http://www.cisco.com/networkers/nw00/pres/2402.pdf

http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Technologies:HSRP

http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:HSRP

http://www.cisco.ohio-state.edu/htbin/rfc/rfc2281.html

http://www.cis.ohio-state.edu/htbin/rfc/rfc2281.html

http://www.faqs.org/rfcs/rfc2281.html

http://www.ITPRC.COM

http://www.isc.org/ml-archives/dhcp-server/2000/09/msg00339.html

http://www.kb.cert.org/vuls/id/228186

http://www.lawebdelprogramador.com/diccionario/

http://www.logilent.com/labs/lab070.html

http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

http://www.networkpenetration.com /sep.html

http://www.netcordia.com/tnm/tnm13/hotnets.htm

http://www.netcraftsmen.net/welcher/papers/hsrp.htm

http://www.osmosislatina.com/conectividad/routers.htmç

http://www.routergod.com/paulhogan

http://www.securityfocus.com/archive/1/182008

http://www.simulationexams.com/SampleQuestions/...witching-q7.htm

http://www.techtip.htm

http://www.vnunet.es/Actualidad/Entrevistas/Inform%C3%A1tica_profesional/Personajes/20040601029/2

http://www.webopedia.com/TERM/cc/td/doc/

http://archives.neohapsis.com/archives/bugtraq/2001-05/0035.html

http://archives.neohapsis.com/archives/bugtraq/2001-05/0037.html

http://directorio.adfound.com/Informatica/Redes/Protocolos/index.html

http://dl.jcc.kctcs.net/rogers/ccnp/semester7/lectures/chapter8/default_files/frame.htm#slide0001.htm

http://es.wikipedia.org/wiki/Wikipedia:Plantilla_para_protocolos_de_red

http://home.t-online.de/home/miko.h/ciscoi~1.htm

http://home.t-online.de/home/miko.h/hsrp~1.htm

http://xforce.iss.net/xforce/xfdb/11909

http://xforce.iss.net/xforce/xfdb/6497

**Otros.**

*"Administración de Redes"*, Apuntes del Curso. Enero – Junio 2003.

*"Tópicos Selectos"*, Notas y Apuntes del Clase. Artículos y Trabajos de los cursos.

## AGRADECIMIENTO

*Dios.*

*Gracias por la vida, por mi familia, amigos y las oportunidades de cada día. De entre ella la simple experiencia de existir.*

*Papá y Mamá.*

*Los amo profundamente, han sido los mejores guías y ejemplos de lucha, trabajo y amor; y serán siempre el mejor regalo de mi vida.*

*Todos mis hermanos.*

*Son y serán el mayor combustible para superarme cada día, el motivo de querer ser mejor y la confianza para seguir adelante. Lazos de amor incondicional.*

*Mis sobrinos.*

*Son la esperanza en el futuro, la recompensa de la lucha de cada día y la fe en el nuevo amanecer. Pequeños destellos de Dios.*

*Mis mejores amigos.*

*Han sido compañeros de mi vida, consejeros, paño de lagrimas de mis tropiezos, y motivos de risa y confort, son ángeles que dios pone en mi camino.*

*Gracias por estar ahí para mí, cuando lo necesite; Por su interés, confianza, apoyo, fe y amor.*

*Rosa Aimé Gómez Gómez*