# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

# DISEÑO DE INTERCONEXIÓN DE REDES DE ALTA DISPONIBILIDAD

## INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

## INGENIERO ELECTRÓNICO

## PRESENTADO POR:


## RUDY CÉSAR MEZA BERROSPI


## PROMOCIÓN
## 2000 – II

## LIMA – PERÚ
## 2006

# DISEÑO DE INTERCONEXIÓN DE REDES DE ALTA DISPONIBILIDAD

# DISEÑO DE INTERCONEXIÓN DE REDES DE ALTA DISPONIBILIDAD

*Dedico este trabajo a:*
*Mis padres, hermanos y esposa, que ven reflejado*
*en este informe el resultado de su apoyo*
*incondicional a lo largo*
*de mi carrera.*

## SUMARIO

El trabajo presentado en este informe muestra el marco teórico para la implementación de un enlace de contingencia, el cual será diseñado de acuerdo a las necesidades de cada punto al cual se le va a proveer una alta disponibilidad.

Se describirán los criterios para la construcción de las conexiones de redundancia, siendo la más común la tecnología ISDN, que brinda una solución económica y práctica de redundancia, sin obviar otros tipos de solución.

Se mostrarán también los criterios para la conmutación del tráfico de datos del enlace principal al enlace de contingencia en caso de falla del primero, los cuales pueden ser por enrutamiento, HSRP; asimismo los criterios de seguridad en caso de un enlace ISDN.

Para la preparación de este informe se han tomado muestras y modelos de enlaces que actualmente están en funcionamiento y se ha comprobado su operatividad. Los equipos routers que se usan para las pruebas son de la marca Cisco, pudiendo aplicarse los mismos criterios para otras marcas de equipos, por supuesto adaptando las configuraciones de acuerdo a cada uno de ellos.

Se ha incluido también criterios de para la verificación de la operatividad del enlace de contingencia, mediante la consulta por comandos o por el proceso de un debug (proceso de verificación paso a paso de cada proceso en un router).

# ÍNDICE

# PRÓLOGO

Actualmente las comunicaciones son un punto vital en el quehacer diario de muchas instituciones, tal es el caso de oficinas del gobierno, dependencias militares por seguridad interna o nacional, asimismo instituciones privadas, las cuales necesitan estar interconectadas las 24 horas los 365 días del año, tratando de reducir al mínimo la pérdida de conexión entre sus diferentes dependencias, ya que estar incomunicados implica un costo económico.

La necesidad de información ha hecho que los medios de comunicación evolucionen, desde hace algunas décadas, de una manera exponencial, siendo actualmente posible enviar un "correo" en unos cuantos segundos, lo que anteriormente hubiese demorado algunos días por un servicio de correo postal tradicional. Así, se reduce el tiempo de respuesta en cualquier ámbito: educación, negocios, cultura, etc., acelerando la velocidad con la que se mueven los negocios entre las empresas.

Para una institución, el estar interconectado no solo con sus sedes, sino también con sus socios estratégicos, clientes, proveedores, etc. es una necesidad que cada día se incrementa.

Existen datos que pueden esperar un tiempo razonable para ser conocidos, por ejemplo: el resultado de un partido de fútbol, o el informe de la asistencia mensual de los empleados, sin embargo hay datos que se necesitan conocer en el momento (tiempo real), sin pérdida de tiempo, tal es el caso de una institución bancaria o financiera, entre otras. Si una agencia bancaria se queda desconectada de su sede central, donde se encuentra concentrada la información de todos sus clientes, prácticamente es una agencia inútil, ya que no podría realizar ninguna transacción, ni de salida ni de ingreso de dinero por ende la pérdida de negocios, por lo tanto esta agencia implicaría un costo negativo en personal administrativo, cajeros, gastos logísticos, que no estarían generando ningún beneficio a la institución por

el hecho de estar aislada de las demás. Esto sin contar el malestar de los clientes que se llevaran una mala imagen de la institución.

Debido a la necesidad de mantener el flujo de información constante es que se generan soluciones para mantener al mínimo el tiempo de desconexión entre 2 (o más) puntos. Estas consisten generalmente en mantener una conexión de respaldo entre los puntos, una conexión principal que es la que tendrá el flujo de infamación en condiciones normales, y otra conexión de contingencia la cual entrará a funcionar en caso ocurra una caída del enlace principal por cualquier motivo.

Estas soluciones se pueden dar de diferentes maneras, pero siempre tratando de buscar que a la falla del enlace principal no falle el enlace de contingencia, esto se logrará entre otras cosas que los enlaces no tengan la misma ruta de cableado, que no se conecten a los mismos equipos de la red del proveedor (backbone), o incluso que no vayan por el mismo proveedor entre otros criterios.

Asimismo, se observarán criterios para cuando ocurrida la falla del enlace principal, automáticamente se conmute a la línea de respaldo sin necesidad de la intervención de la mano del hombre.

# CAPÍTULO I
# PROTOCOLOS DE ENRUTAMIENTO

## 1.1. Introducción.

Para la conmutación de la ruta en caso avería en una de las líneas de enlace se requiere hacer uso de tablas de enrutamiento. Uno de los puntos importantes a tener en cuenta en el diseño de una red es el enrutamiento.

Enrutamiento es el proceso que un router usa para enviar paquetes hasta un destino de red especifico. Un router toma decisiones basadas en la dirección IP de destino del paquete. Todos los routers a lo largo del camino usan la dirección IP de destino para enviar el paquete en la dirección correcta para que el paquete llegue eventualmente a su destino. Para tomar las correctas decisiones los routers deben aprender la dirección correcta a la red remota. Cuando el router usa enrutamiento dinámico, esta información es aprendida de otros routers. Cuando usa enrutamiento estático, un administrador de red configura información acerca de las redes remotas manualmente.

Debido a que las rutas estáticas deben ser configuradas manualmente, algunos cambios en la topología de la red requieren que el administrador de red agregue y borre manualmente rutas estáticas de acuerdo a los cambios. En una red grande este mantenimiento manual de tablas de enrutamiento podría requerir una gran cantidad de tiempo del administrador de red. En una red pequeña con algunos posibles

cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requerimientos extra de administración, las rutas estáticas no tienen la escalabilidad de un enrutamiento dinámico. Siempre en una red grande, las rutas estáticas que están comprendidas para acompañar un propósito específico son a menudo configuradas en conjunto con un protocolo de enrutamiento dinámico.
Existen 2 tipos de rutas, Rutas Estáticas y Rutas Dinámicas, las cuales se explican en los siguientes párrafos.

### 1.2. Rutas Estáticas.

Usan una ruta programada por el administrador de red que fue ingresada al router.
Se puede dividir en 3 procesos:

- Administrador de red configura la ruta.
- El router instala la ruta en su tabla de enrutamiento.
- Los paquetes son enrutados usando la ruta estática.

Si el router no puede alcanzar la interfase de salida que esta siendo usada en la ruta, la ruta no será instalada en la tabla de enrutamiento. Esto significa, si la interfase esta caída, la ruta no será colocada en la tabla de enrutamiento.

Algunas rutas estáticas son usadas para propósitos de backup. Una ruta estática puede ser configurada en un router que será usada solo cuando la ruta dinámicamente aprendida ha fallado. Para usar una ruta estática de esta manera, simplemente se configura la distancia administrativa más grande que la que esta siendo usada en el protocolo de enrutamiento dinámico.

### 1.3. Rutas Dinámicas.

Usa una ruta que el protocolo de enrutamiento ajusta automáticamente para cambios de topología o tráfico.

Un protocolo de enrutamiento es diferente de un protocolo ruteado en funcionamiento y tareas.

Un protocolo de enrutamiento es la comunicación usada entre routers. Un protocolo de enrutamiento permite a un router compartir información con otros routers de manera que se puede saber que tan próxima esta una red del router. La información que un router toma de otro router usando un protocolo de enrutamiento, es usada para construir y mantener una tabla de enrutamiento.

Ejemplos de protocolos de enrutamiento son:

- Routing Information Protocol (RIP).
- Interior Gateway Routing Protocol (IGRP).
- Enhanced Interior Gateway Routing Protocol (EIGRP).
- Open Shortest Path First (OSPF).

Un protocolo ruteado es usado para direccionar tráfico del usuario. Un protocolo ruteado provee información en su dirección de capa de red para permitir reenviar un paquete de un host a otro basado en el esquema de direccionamiento.

Ejemplos de protocolos ruteados son:

- Internet Protocol (IP).
- Internetwork Protocol Exchange (IPX).

### 1.4. Sistemas Autónomos (Autonomous Systems AS).

Un sistema autónomo es una colección de redes bajo una administración común compartiendo una estrategia común de enrutamiento. Para el mundo exterior, un AS es vista como una entidad singular. El AS puede correr sobre uno o más operadores mientras presente una visión consistente de enrutamiento hacia el mundo exterior.

El American Registry of Internet Numbers (ARIN) http://www.arin.net/, un proveedor de servicios, o un administrador asignan un número de identificador a cada AS. El número del sistema autónomo es un número de 16 bits, Los protocolos de enrutamiento, tales como IGRP de Cisco, requieren asignarse de un único número de sistema autónomo.

## 1.5. Propósitos del protocolo de enrutamiento y el sistema autónomo.

El objetivo de un protocolo de enrutamiento es construir y mantener la tabla de enrutamiento. Esta tabla contiene las redes aprendidas y los puertos asociados para esas redes. Los routers usan protocolos de enrutamiento para manejar información recibida de otros routers, información aprendida de la configuración de sus propias interfaces.

El protocolo de enrutamiento aprende todas las rutas disponibles, coloca la mejor ruta en la tabla de enrutamiento y borra rutas cuando estas tienen un valor muy grande. El router usa la información de la tabla de enrutamiento para reenviar paquetes de protocolos ruteados.

El algoritmo de enrutamiento es fundamental para enrutamiento dinámico. Siempre que la topología de una red cambie debido a una reconfiguración o falla, la tabla de enrutamiento conocida también debe cambiar. La base de datos de la tabla de enrutamiento necesita reflejar una actualización consistente de la nueva topología.
Cuando todos los routers de una red están operando con las mismas rutas conocidas, se dice que la red ha convergido. La rápida convergencia es decisiva porque esto reduce el periodo de tiempo en el cual los routers podrían estar tomando decisiones incorrectas respecto al enrutamiento de paquetes.

El Sistema Autónomo (AS) provee la división de toda una red en redes más pequeñas, de esta manera estas redes son más manejables. Cada Sistema Autónomo tiene sus propias políticas y reglas de enrutamiento, y un número AS que será distinguido de otros sistemas autónomos a través del mundo.

## 1.6. Clases de Protocolo de Enrutamiento.

La mayoría de los protocolos de enrutamiento se pueden clasificarse en una de las dos siguientes:

- Distance Vector (Vector de Distancia)
- Link-state (Estado del enlace)

El enrutamiento distance vector determina la dirección (vector) y la distancia a algún enlace en la red.
El link-state, también llamado Shortest Path First (SPF), recrea la topología exacta de la red entera.

### 1.6.1. Características del protocolo de enrutamiento Distance-Vector (Vector de Distancia).

El algoritmo de enrutamiento distance-vector periódicamente envía copias de las tablas de enrutamiento de un router a otro. Esas actualizaciones regulares entre routers informan de los cambios en topología de la red. Los algoritmos de enrutamiento de distance-vector son también conocidos como algoritmo de Bellman-Ford.
Cada router recibe una tabla de enrutamiento de su router neighbor (vecino) directamente conectado.

Como se muestra en la figura 1.1, el router B recibe la información del router A, el router B agrega un número distance-vector (tal como un número de saltos), el cual incrementa la Distance-Vector. El router B pasa esta nueva tabla de enrutamiento al otro neighbor, router C. Este mismo proceso se repite paso a paso en todas las direcciones entre routers neighbors.

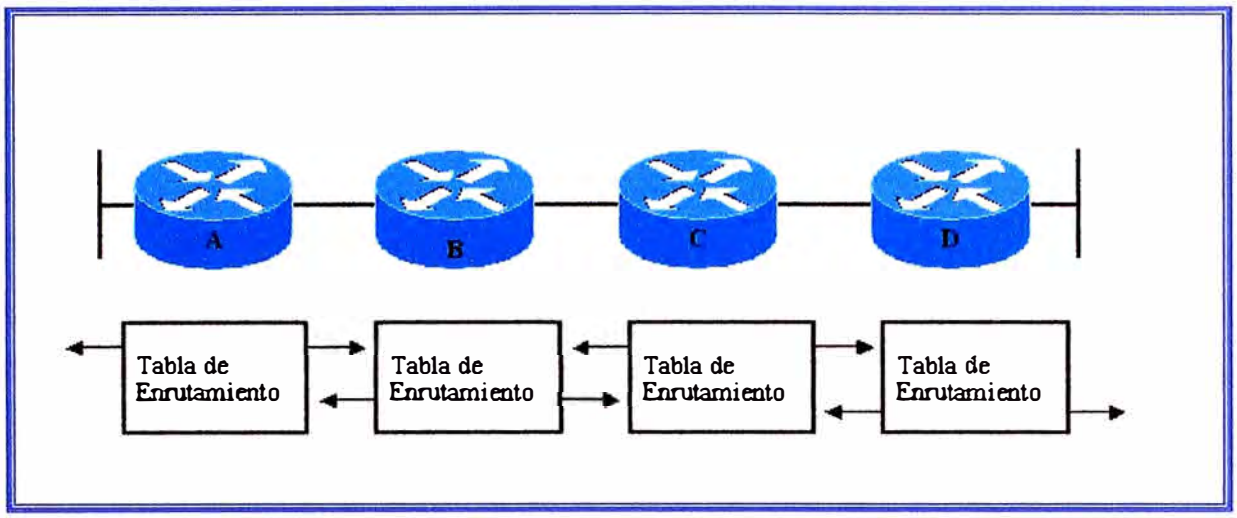


**Fig N° 1.1: Enrutamiento Distance-Vector.**

El algoritmo eventualmente acumula distancias de red hasta que esta pueda mantener una base de datos de la información de la topología de red. Sin embargo, el algoritmo distance-vector no permite a un router conocer la topología exacta de la red ya que cada router solo puede ver su router neighbor.

Cada router que usa enrutamiento distance-vector empieza por identificar su propio neighbor. La interfase que apunta a cada red directamente conectada es mostrada con una distancia de 0. El router descubre la mejor ruta a la red de destino basado en la información que ellos reciben de cada neighbor. El router A aprende acerca de otras redes basándose en la información que recibe del router B. Cada una de las otras entradas de red en la tabla de enrutamiento tiene una distancia acumulada que muestra que tan lejos esta esa red en una dirección dada.

La actualización de la tabla de enrutamiento ocurre cuando la topología cambia. Como con el proceso de descubrir redes, la actualización de los cambios en la topología procede paso a paso de un router a otro.

Los algoritmos de distance-vector invocan al router para enviarle su tabla de enrutamiento a cada uno de sus neighbors adyacentes. La tabla de enrutamiento incluye información acerca del costo total de la ruta, definida por su métrica y dirección lógica del primer router en la ruta a cada red contenida en la tabla.

### 1.6.2 Características del protocolo de enrutamiento Link-state (Estado de Enlace).

El segundo algoritmo básico usado para enrutamiento es el algoritmo link-state. El algoritmo link-state es también conocido como algoritmo Dijkstras o algoritmo SPF (Shorest Path First). El algoritmo de enrutamiento link-state mantiene una base de datos compleja de la información de la topología. El algoritmo distancia vector no específica información acerca de la red distante y no conoce de routers distantes. Un algoritmo de enrutamiento link-state mantiene conocimiento total de routers distantes y como interconectarlos.

El enrutamiento link-state usa:

- Link-state advertisements (LSAs).- Paquetes de anuncio link-state, es un paquete pequeño de información de enrutamiento que es enviado entre routers.
- Base de datos topológica.- Una base de datos topológica es una colección de información tomada de LSAs.
- Algoritmo SPF.- El algoritmo Shortest Path First (SPF) es un cálculo realizado en la base de datos resultando en el árbol SPF.
- Tablas de enrutamiento.- Una lista de rutas e interfaces conocidas.

*Proceso de descubrimiento de redes para enrutamiento link-state.*

LSAs son intercambiados entre routers empezando con las redes directamente conectadas para lo cual ellos tienen información directa. Cada router en paralelo con los otros construye una base de datos topológica consistente de todos los intercambios LSAs.

El algoritmo SPF computa la conectividad a las redes. El router construye su topología lógica como un árbol, con el mismo como raíz, consistente de todas las rutas posibles a cada destino red en la red con protocolo link-state. El router lista la mejor ruta y la interfase por la cual puede llegar a este destino de red en la tabla de enrutamiento. También mantiene otra base de datos de elementos de topología y detalles de estado.

La figura 1.2 muestra el intercambio de LSAs y construcción de las tablas de enrutamiento.

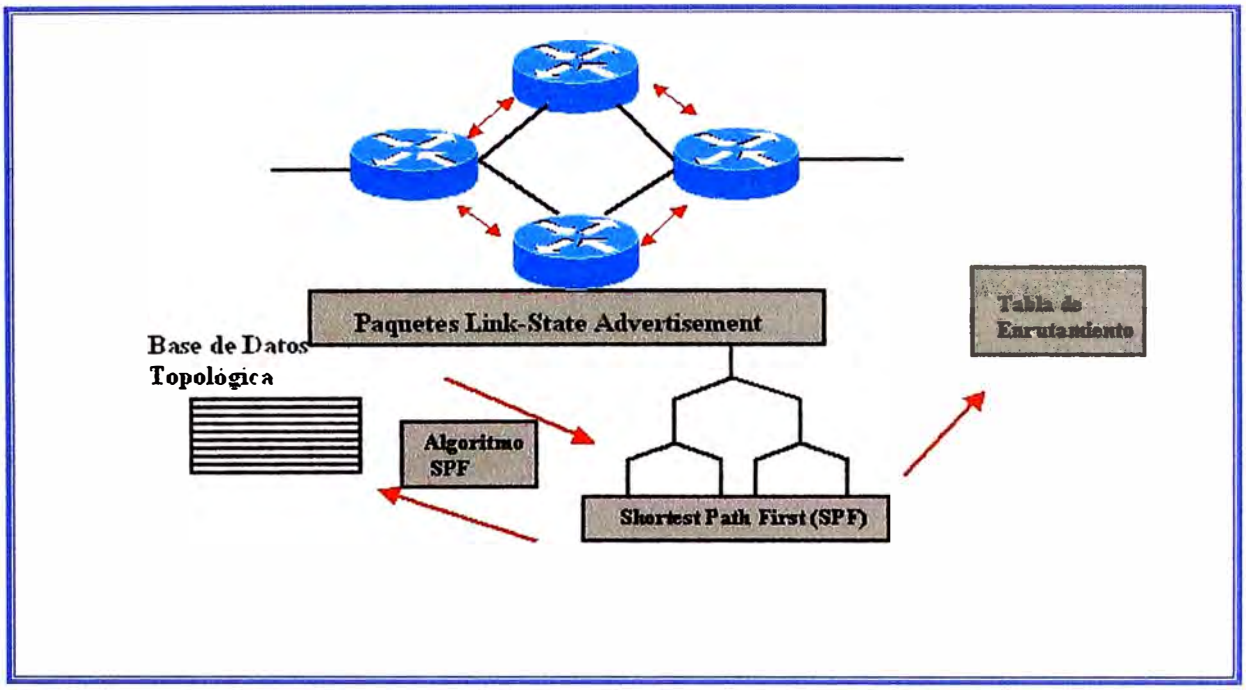


**Fig. Nº 1.2: Enrutamiento Link-State.**

# CAPÍTULO II
# DISEÑO DE LAS TABLAS DE ENRUTAMIENTO

## 2.1. Enhanced Interior Gateway Routing Protocol (EIGRP).

Para el proceso de enrutamiento de redes en este diseño se usara el protocolo Enhanced Interior Gateway Routing Protocol, EIGRP (Protocolo de Enrutamiento de Gateway Interior Mejorado).
EIGRP es un protocolo de enrutamiento propietario de Cisco basado en IGRP, por esto, IGRP y EIGRP son compatibles.

Mientras IGRP, es un classfull routing protocol (protocolo de enrutamiento de clase completa), EIGRP soporta classless interdomain routing (CIDR) (protocolo de enrutamiento de clase incompleta), permitiendo de esta manera a los diseñadores de red maximizar el espacio de direcciones usando CIDR y variable-length subnet mask (VLSM) (mascara de subred de longitud variable). EIGRP converge mas rápidamente que IGRP, escalable y maneja mejor los loops (lazos) de enrutamiento.

EIGRP a menudo es descrito como un protocolo de enrutamiento híbrido, ofreciendo lo mejor de los algoritmos de distance-vector y link-state. EIGRP tiene algunas características de OSPF (link-state), pero EIGRP es más fácil de configurar, usa una métrica con una longitud de 32 bits, mientras IGRP usa una métrica de 24 bits. IGRP tiene un máximo hop-count (contador de saltos) de 255, mientras EIGRP es como máximo 224, esto es mas que suficiente para soportar los diseños de red.

La formula que usa EIGRP para el cálculo de sus métricas es formula 2.1:

$$\text{Metric}=[K1*BW+(K2*BW)/(256-load)+(K3*delay)]*[K5/(reliability+K4)] \quad (2.1)$$

BW: Bandwidth

Los valores por defecto par alas constantes son:

K1 = 1, K2 = 0, K3 =1, K4 = 0, K5 = 0.

De esta manera la formula queda de la siguiente manera:

$$\textbf{Metric} = \textbf{bandwidth} + \textbf{delay} \qquad (2.2)$$

EIGRP actualiza tablas cada 90 segundos.

EIGRP puede compartir la carga.

La información de rutas y topologías que maneja EIGRP se almacena en la memoria RAM (Random Access Memory) de los routers, por tanto pueden ser cambiadas rápidamente.

EIGRP usa 3 tablas:

- Neighbor table (Tabla de vecinos): Esta es la más importante. Cada router mantiene una tabla de neighbor que lista los routers adyacentes.
- Topology table (Tabla de topología)
- Routing table (Tabla de enrutamiento)

Cuando es descubierto un nuevo neighbor, la dirección y la interfase de este neighbor son grabadas. Esta información es almacenada en la estructura de datos de neighbors. Cuando un neighbor envía un paquete hello (hola), este es enviado con un hello-time (tiempo de hola). El hello-time es la cantidad de tiempo que un router comprueba a un neighbor como accesible y operativo. En otras palabras si el paquete hello no es escuchado dentro del hello-time entonces el hello-time expira, cuando esto sucede el Diffusing Update Algorithm (DUAL) (Algoritmo de Difusión de Actualización), el cual es el algoritmo distance-vector de EIGRP es alertado del cambio en la topología y recalcula la nueva topología.

La Tabla de Topología es construida de toda la tabla de rutas de EIGRP en el sistema autónomo. DUAL toma la información proporcionada en la tabla de neighbor y la tabla de topología y calcula las rutas de menor costo para cada destino.

La tabla de topología incluye los siguientes campos:

**Feasible Distance (FD):** Distancia factible, es el menor valor calculado a cada destino.

**Fuente de la ruta:** La fuente de la ruta es el número de identificación del router que originalmente envía la ruta.

**Reported Distance (FD/RD):** Distancia reportada, es la distancia reportada por el neighbor adyacente al destino específico.

**Información de interfase:** La interfase a través de la cual el destino es alcanzable.

**Estado de la ruta:** Las rutas son identificadas como Passive (P) (pasiva), lo cual significa que la ruta es estable y lista para usar, o Active (A) (activa), lo cual significa que la ruta esta en el proceso de empezar a recalcular por DUAL.
La tabla de enrutamiento de EIGRP mantiene la mejor ruta al destino. Esta información es tomada de la tabla de topología. Cada router EIGRP mantiene una tabla de enrutamiento para cada Protocolo de Red.

**Succesor:** Un succesor es una ruta seleccionada como la ruta principal a usar para alcanzar un destino. DUAL identifica esta ruta de la información contenida en las tablas de neighbor y topología y coloca en la tabla de enrutamiento. Puede haber hasta cuatro rutas succesor para cualquier ruta particular. Estas pueden tener igual o diferente costo y están identificadas como las mejores rutas loop-free (libre de lazos) a un destino dado. Una copia de las rutas succesor es colocada en la tabla de topología.

**Feasible Succesor (FS)**: Un feasible succesor es una ruta alterna, estas rutas son identificadas a la vez que es identificado el succesor, pero estos son solo colocados en la tabla de topología. Múltiples feasibles succesors para un destino pueden ser contenidos en la tabla de topología aunque no es obligatorio.
Un router ve a su feasible successor como un neighbors caído. Si la ruta principal cae, el router comienza a buscar al feasible successor, y si esta ultima cae, el router volverá a computar para buscar una nueva ruta, la cual pasara al estado de feasible successor. Un

feasible successor debe tener un menor costo que el succesor existente al destino. Si un feasible successor no es identificado de la información existente, entonces el router coloca en estado Active a una ruta y envía paquetes de QUERY (Pregunta) a todos los neighbors para poder recomputar la actual topología. El router puede identificar alguna nueva ruta succesor o feasible succesor de la nueva data que es recibida a través de los paquetes REPLY (Respuesta) en respuesta a los paquetes QUERY. El router colocara entonces estado Passive a la ruta.

La tabla de topología puede guardar información adicional acerca de cada ruta. EIGRP clasifica las rutas como INTERNA o EXTERNAS. Las rutas internas son generadas dentro del Sistema Autónomo (AS) de EIGRP.
Las rutas externas se originan fuera del AS de EIGRP. Las rutas aprendidas o redistribuidas desde otros protocolos de enrutamiento, tales como Routing Informational Protocol (RIP), OSPF e IGRP son externas. Las rutas estáticas generadas fuera del AS de EIGRP también son externas.

## 2.2. Características de Diseño de EIGRP.

EIGRP es un protocolo de enrutamiento distance-vector avanzado y actúa como un protocolo link-state cuando actualiza neighbors y mantiene la información de enrutamiento. Las ventajas de EIGRP sobre el protocolo simple distance-vector incluye lo siguiente:

- Rápida Convergencia.
- Eficiente uso de ancho de banda.
- Soporta Variable-length subnet mask (VLSM, máscara de subred variable) y Classless Interdomain Routing (CIDR, enrutamiento de clase incompleta). A diferencia de IGRP, EIGRP ofrece soporte completo para classless IP por intercambio de máscaras de subred en la actualización de rutas.
- Soporta múltiples capas de red.
- Independiente del protocolo ruteado

Los routers con EIGRP convergen rápidamente. DUAL garantiza la operación en loop-free en cada instante a través de una ruta permitiendo a todos los routers involucrados en un cambio en la topología sincronizarse todos a la vez.

EIGRP hace eficiente uso del ancho de banda por el envío parcial de paquetes de actualización y su mínimo consumo de ancho de banda cuando la red es estable. Los routers EIGRP hacen envíos parciales, incrementan las actualizaciones más rápido que enviar la tabla completa. Esto es similar a la operación de OSPF, pero a diferencia de routers OSPF, los routers EIGRP envían esas actualizaciones parciales solo a los routers que necesitan esta información, no a todos los routers en el área. Por esta razón, ellos son llamados paquetes de actualización. En vez de usar actualización de rutas temporizadas, los routers EIGRP intercambian con cada otro usando pequeños paquetes hello. Aun con el intercambio regular de estos paquetes hello, no usan una significativa cantidad de ancho de banda.

## 2.3. Tecnologías EIGRP.

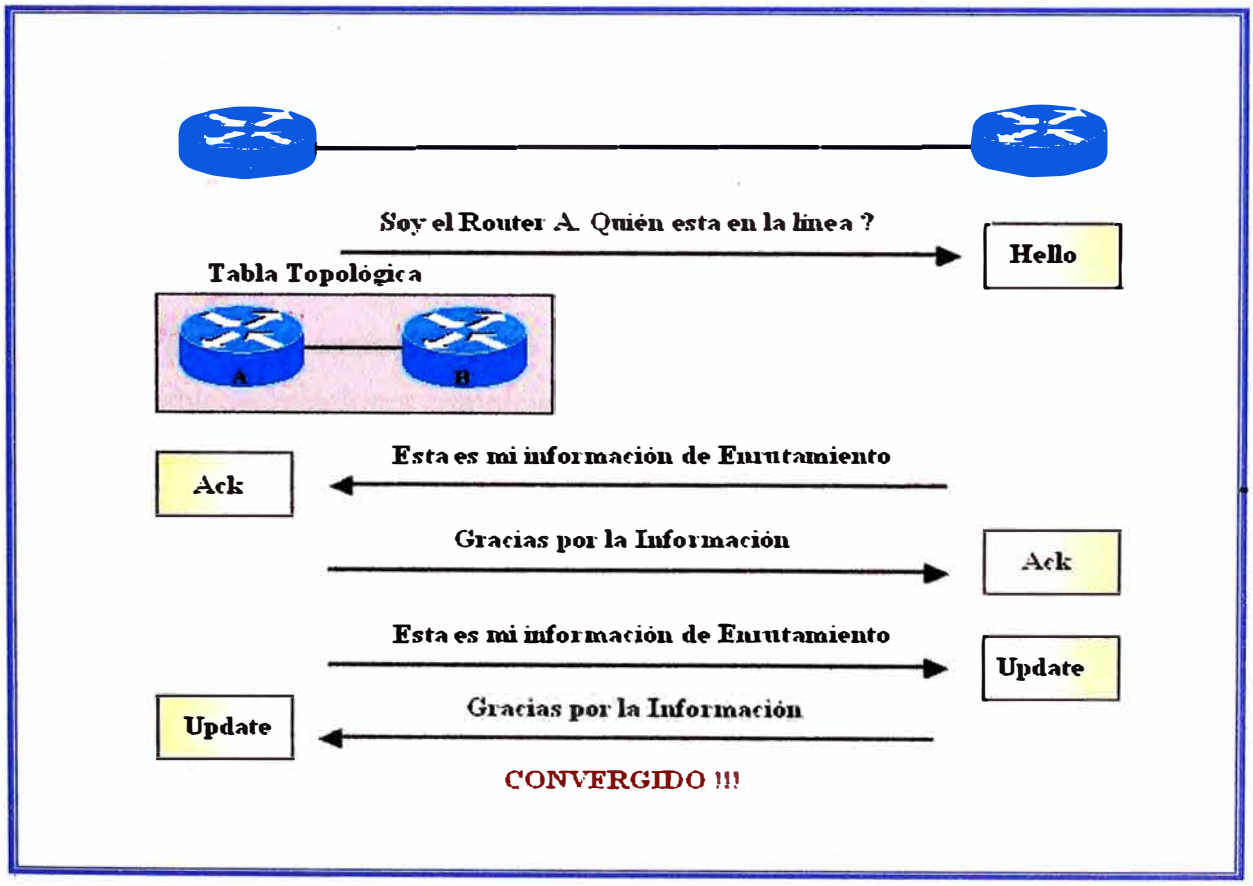


**Fig. Nº 2.1 Actualización de routers EIGRP.**

EIGRP incluye algunas nuevas tecnologías, cada una de las cuales representa una mejoría en la eficiencia de la operación, velocidad de convergencia, o funcionamiento relativo a IGRP y otros protocolos de enrutamiento. Esas tecnologías encajan en una de las siguientes cuatro categorías:

- Descubrimiento y Recuperación de Neighbors.
- Reliable Transport Protocol (RTP) (Protocolo Confiable De transporte).
- DUAL finite-state machine algorithm. (Algoritmo maquina estado finito DUAL).
- Protocol-dependent modules (PDMs), (Módulos Dependientes de Protocolo).

Un router con un simple distance-vector no establece relación alguna con sus neighbors. Los routers RIP e IGRP solo realizan actualizaciones broadcast o multicast en las interfaces configuradas. Por el contrario, los routers EIGRP establecen activamente relación con sus vecinos, muchos de la misma manera que lo hacen los routers OSPF.

Los routers EIGRP se actualizan como se describe en la figura 2.1, lo cual lo hacen usado pequeños paquetes hello. Estos paquetes Hello son enviados cada 5 segundos por defecto.

## 2.4. Estructura de datos de EIGRP.

Como OSPF, EIGRP envía diferentes tipos de paquetes para mantener sus diferentes tablas y establecer relaciones complejas con los routers neighbors.
Los cinco paquetes EIGP son:

- Hello, paquetes Hola
- Acknowledgment, paquetes de confirmación o reconocimiento.
- Update, paquetes de actualización.
- Query, paquetes de pregunta o consulta.
- Reply, paquetes de respuesta a los paquetes Query.

EIGRP envía un paquete hello para descubrir, verificar y redescubrir routers neighbors. El redescubrimiento ocurre si los routers EIGRP no reciben paquetes hello de cualquier otro para un intervalo de tiempo hold-time pero entones restablece la comunicación.

Los routers EIGRP envían paquetes hello en un intervalo fijo pero configurable, llamado el hello-interval. El hello-interval por defecto depende del ancho de banda de la interfase, algunos ejemplos se muestran en la tabla 2.1.

**TABLA 2.1 Intervalos de tiempo en EIGRP.**

| Bandwidth | Example Link | Default Hello Interval | Default Hold Time |
|---|---|---|---|
| 1.544 Mbps o menos | Frame relay multipunto | 60 segundos | 180 segundos |
| Mayor a 1.544 Mbps | T1, Ethernet | 5 segundos | 15 segundos |

En una red IP, los routers EIGRP envían los paquetes hello a la dirección IP Multicast 224.0.0.10.

Un router EIGRP almacena la información acerca de los neighbors en la tabla de neighbors. La tabla de neighbors incluye el campo Sequence Number (Seq No) (numero de secuencia) para grabar el número del último paquete de EIGRP recibido que cada neighbor envió. La tabla de neighbor también incluye un campo Hold-Time (tiempo de espera) el cual guarda el tiempo que el último paquete fue recibido. Los paquetes deben ser recibidos dentro del periodo de tiempo de hold-time para mantener el estado Passive. El estado Passive es un estado de alcanzable y operacional.

Si un neighbor no es escuchado dentro de la duración del hold time, EIGRP considera que el neighbor cayó, y el DUAL debe pasar a re-evaluar la tabla de enrutamiento. Por defecto, el hold-time es tres veces el hello-interval (intervalo hola), pero el administrador puede configurar ambos timers (temporizadores) como lo decida.

OSPF requiere que los routers neighbors tengan el mismo intervalo de hello y dead (expiración) para comunicarse. EIGRP no tiene tal restricción. Los routers neighbors aprenden cada uno del otro los respectivos timers vía el intercambio de paquetes hello. Entonces ellos usan esta información para forjar una relación estable, independiente de timers diferentes. Los paquetes hello son enviados siempre sin confiabilidad. Esto significa que el paquete acknowledgment no es transmitido.

Un router EIGRP usa paquetes acknowledgment para indicar la recepción de algún paquete EIGRP durante un intercambio confiable. Reliable Transport Protocol (RTP) puede proveer comunicación confiable entre hosts EIGRP. Para ser confiable, un mensaje del enviante debe ser reconocido por el receptor.

Los paquetes acknowledgment, los cuales son paquetes hello sin data, son usados para este propósito. A diferencia de los hellos multicast, los paquetes acknowledgment son unicast. Acknowledgments pueden ser hechos para ser adjuntados a otro tipo de paquetes EIGRP, tales como paquetes reply.

Los paquetes Updates (actualización) son utilizados cuando un router descubre un nuevo neighbor. Un router envía un paquete de actualización unicast al nuevo neighbor para que este pueda agregarlo a su tabla de topología. Más que un paquete de actualización tal vez sea necesario para enviar toda la información de la topología al nuevo neighbor descubierto.
Los paquetes update son también usados cuando un router detecta un cambio en la topología. En este caso, el router EIGRP envía un paquete de actualización multicast a todos los neighbors, el cual los alerta del cambio. Todos los paquetes de actualización son enviados con confiabilidad.

Un router EIGRP usa paquetes query siempre y cuando necesite especificar información de uno o todos sus neighbors. Un paquete reply es usado para responder un query.

Si un router EIGRP pierde su succesor (ruta principal) y no puede encontrar un feasible succesor (ruta secundaria) para una ruta, DUAL coloca la ruta en estado ACTIVE. Un paquete query es entonces enviado como multicast a todos los neighbors para lograr ubicar

# CAPÍTULO III
# HOST STANDBY ROUTER PROTOCOL (HSRP)

## 3.1. Características y Operación de HSRP.

Host Standby Router Protocol, HSRP (Protocolo De Estación Router En Espera).
Una forma de lograr que la red llegue a alcanzar cerca al 100% de operación es utilizar HSRP, que proporciona la redundancia de red para las redes IP, asegurándose que el flujo de datos del usuario se recupere transparente e inmediatamente a partir de la una falla en el primer salto en dispositivos del borde de la red o circuitos de acceso.

Compartiendo una dirección IP y una dirección MAC (capa 2), dos o más routers puede actuar como un solo router "virtual". Los miembros del grupo virtual de router intercambian continuamente mensajes del estado. De esta manera, un router puede asumir la responsabilidad de enrutamiento del otro, si sale de servicio por razones imprevistas. Los hosts continúan enviando los paquetes IP a una dirección IP y MAC constantes, y el cambio de los dispositivos hacen que el enrutamiento sea transparente.

### 3.1.1. Mecanismos Dinámicos de Descubrimiento de Router.

A continuación se describen los mecanismos dinámicos de descubrimiento de router que están disponibles para los hosts. Muchos de estos mecanismos no proporcionan la confiabilidad de la red requerida por los administradores de la red. Esto puede ser porque el protocolo no fue pensado inicialmente para proporcionar confiabilidad de la red o porque no es factible para cada host en una red corra el protocolo. Además lo que se menciona abajo, es importante observar que muchos host permiten solamente que usted configure una default-gateway.

**a) Proxy Address Resolution Protocol .**

Protocolo de Resolución de Dirección, algunos hosts IP utilizan el proxy Address Resolution Protocol (ARP) para seleccionar un router. Cuando un router corre proxy ARP, envía un ARP request al Dirección IP del host remoto que desea contactar. Un router, router A, en la red replica al nombre del host remoto y proporciona su propia dirección MAC. Con proxy ARP, el router se comporta como si el router remoto fuera conectado al mismo segmento de la red. Si el router A falla, el host continúa enviando los paquetes destinados al router remoto a la dirección MAC del router A aunque esos paquetes no tienen a donde ir y se pierden. Se puede esperar el ARP para capturar la dirección MAC de otro router, router B, en el segmento local enviando otro ARP request, o reiniciar el host para forzarlo a enviar un ARP request. En cualquier caso, por un período de tiempo significativo, el router no puede comunicarse con el host remoto, aunque el protocolo de enrutamiento ha convergido, y el router B está preparado para transferir los paquetes que pasarían de otra manera a través del router A.

**b) Protocolo de Enrutamiento Dinámico.**

Algunos hosts IP corren un protocolo dinámico de enrutamiento tal como el Routing Information Protocol (RIP) u Open Shortes Path First (OSPF) para descubrir los routers. La desventaja de usar RIP es que es lento para adaptarse a los cambios en la topología. Corriendo un protocolo dinámico de enrutamiento en cada host puede no ser factible por un número de razones, incluyendo overhead (sobrecarga) administrativo, sobrecarga de procesamiento, seguridad, o carencia de un protocolo implementado para algunas plataformas

**c) ICMP Router Discovery Protocol (IRDP) .**

Protocolo de Descubrimiento de Router ICMP, Algunos host IP nuevos utilizan ICMP Router Discovery Protocol (IRDP) para encontrar un nuevo router cuando una ruta llega a ser inalcanzable. Un host que corre IRDP escucha mensajes hello multicast de su router configurado y utiliza un router alterno cuando no recibe esos mensajes hello

por largo tiempo. Los valores de tiempo por defecto de IRDP indican que no es conveniente para la detección de una falla en el primer salto. La velocidad de aviso por defecto esta entre 7 a 10 minutos, y el tiempo de vida por defecto es 30 minutos.

**d) Dynamic Host Configuration Protocol (DHCP).**

Protocolo de Configuración de Host Dinámico, proporciona un mecanismo para pasar la información de la configuración a los hosts en una red de TCP/IP. Un host que corre un cliente de DHCP solicita la información de la configuración de un servidor de DHCP cuando se activa en la red. Esta información de configuración comprende típicamente un Dirección IP y un default-gateway. No hay mecanismo para cambiar a un router alterno sí el default-gateway falla.

### 3.1.2. Operación de HSRP.

Una gran clase de implementación de hosts antiguos que no soportan descubrimiento dinámico son capaces de configurar una ruta por defecto (deafult-router). Correr un mecanismo de descubrimiento dinámico de router en cada host puede no ser factible por muchas razones tales como overhead administrativo, sobrecarga de procesamiento, seguridad, o carencia de un protocolo de implementación para algunas plataformas. HSRP proporciona servicios de respuesta ante fallas (failover) a estos hosts.

Usando HSRP, un sistema de routers trabaja en conjunto para presentar la ilusión de un solo router virtual a los hosts en la LAN. Este grupo de routers es conocido como un grupo HSRP o un grupo standby (grupo en espera). Un solo router seleccionado del grupo es responsable del forwarding (reenvío) de los paquetes que los hosts envían al router virtual. A este router se le conoce como el router Activo. Otro router se escoge como el router Standby. En caso que el router Activo falle, el router Standby asume el trabajo de forwarding de paquetes del router Activo. Aunque un número arbitrario de routers puede correr HSRP, sólo el router Activo reenvía los paquetes enviados al router virtual.

Para reducir el tráfico de la red, solamente los routers Activo y Standby envían mensajes periódicos de HSRP una vez que el protocolo haya terminado el proceso de elección. Si el

router Activo falla, el router Standby asume el control como el router Activo. Si el router Standby falla o se convierte en el router Activo, entonces el otro router se elige como el router Standby.

En una LAN particular, grupos múltiples de host standby pueden coexistir y traslaparse. Cada grupo standby emula un solo router virtual. Los routers individuales pueden participar en grupos múltiples. En este caso, el router mantiene estado y timers separados para cada grupo.
Cada grupo standby tiene una sola dirección MAC, así como una dirección IP.

### 3.2. Direccionamiento HSRP.

En la mayoría de los casos cuando se configura routers para ser parte de un grupo de HSRP, estos escuchan la dirección MAC HSRP para ese grupo así como su propia **burned-in** MAC address (dirección MAC de cada interfase). La excepción son los routers cuyas controllers Ethernet reconocen una sola dirección MAC (por ejemplo, la controller del router Cisco 2500 y del Cisco 4500). Estos routers usan la dirección MAC HSRP cuando son los routers Activos, y su burned-in address cuando no lo son.

HSRP usa la siguiente dirección MAC en todos los medios excepto Token Ring:
**0000.0c07.ac** (donde ** es el numero de grupo HSRP)**
Las interfaces Token Ring usan las direcciones funcionales para la dirección MAC HSRP. Las direcciones funcionales son el único mecanismo general de multicast disponible. Hay un número limitado de direcciones funcionales Token Ring disponibles y muchas de ellas son reservadas para otras funciones. Se pueden usar las tres direcciones siguientes con HSRP:
**c000.0001.0000 (group 0)**
**c000.0002.0000 (group 1)**
**c000.0004.0000 (group 2)**

**Nota:** Cuando HSRP corre en un ambiente Multiple-Ring Source-Route Bridging (SRB) (Puente Ruta-Origen) y el router HSRP reside en diferentes anillos, usar las direcciones funcionales puede causar confusión del Routing Information Field (RIF) (Campo de

Información de Enrutamiento). Por ejemplo, en un ambiente SRB, es posible que un router HSRP standby resida en un anillo diferente que el router Activo. Cuando este router Standby pasa a ser Activo, las estaciones en el mismo anillo como el anterior router Activo necesitan un nuevo RIF para enviar los paquetes al nuevo router Activo. Sin embargo, puesto que el router standby (nuevo Activo) está utilizando la misma dirección funcional que el anterior router Activo las estaciones no está enteradas que deben enviar a exploradores para un nuevo RIF. Por esta razón, fue introducido el comando use-bia (comando de línea de Cisco).

### 3.3. Funcionalidad y Características HSRP en los software Cisco IOS.

En la Tabla 3.1 se muestra las características de HSRP que son soportadas en cada Software Cisco IOS.

**TABLA Nº 3.1: Características soportadas por sistemas operativos de Cisco.**

| Feature | 10 | 10.2 | 10.3 | 11 | 11.1 | 11.2 | 11.3 | 12 | 12.0T | 12.1 | 12.1T |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Preemption | X | X | X | X | X | X | X | X | X | X | X |
| Multiple Groups (MHSRP) | | | X | X | X | X | X | X | X | X | X |
| Ethernet 802.10 SDE | | | | | X | X | X | X | X | X | X |
| Interface Tracking | | | | | X | X | X | X | X | X | X |
| Use BIA | | | | | 8 | X | X | X | X | X | X |
| Preempt Delay | | | | | | X | X | 6 | X | X | X |
| Ethernet LANE | | | | | | X | X | X | X | X | X |
| Tokeng Ring LANE | | | | | | | X | X | X | X | X |
| ISL | | | | | | | X | X | X | X | X |
| Syslog Support | | | | | | | X | X | X | X | X |
| MAC Refresh Interval | | | | | | | | 1 | X | X | X |
| SNMP MIB | | | | | | | | | 3 | X | X |
| MHSRP y Use BIA | | | | | | | | | 3.4 | X | X |
| IP Redundancy | | | | | | | | | 3.4 | X | X |
| BVI | | | | | | | | | 6.2 | X | X |
| 802.1Q | | | | | | | | | 8.1 | X | X |
| Enhanced HSRP Debugging | | | | | | | | | | 0.2 | X |
| HSRP ICMP Redirects | | | | | | | | | | | 3 |
| HSRP MPLS VPNs | | | | | | | | | | | 3 |

A continuación se definen las características de HSRP

### 3.3.1. Preemption.

La característica preemption (Preferencia) de HSRP permite al router con más alta prioridad convertirse inmediatamente en el router Activo. La prioridad es determinada primero por el valor de la prioridad que se configura, y luego por la dirección IP. En cada caso el valor más alto es el de mayor prioridad.

Cuando un router de alta prioridad preempt a un router de más baja prioridad, envía un mensaje coup. Cuando un router Activo de baja prioridad recibe un mensaje coup o Hello de un router Activo de mayor prioridad, cambia al estado speak y envía un mensaje resign (aceptación).

### 3.3.2. Preempt Delay.

La característica de preempt delay (Preferencia retrasada) permite al preemption a ser retrasado por un período de tiempo configurable, permitiendo que el router construya su tabla de enrutamiento antes de convertirse en el router Activo.
Para configurar prioridad y preemption HSRP, se usa el comando:
**[group] [priority number] [preempt [delay [minimum] seconds] [sync seconds]]**

### 3.3.3. Interfase Tracking.

Interfase tracking (Seguimiento de Interfase) permite especificar otra interfase en el router para el proceso HSRP de monitorear para alterar la prioridad de HSRP para un grupo dado.

Si el protocolo de línea de la interfase especificada cae, la prioridad de HSRP de este router se reduce, permitiendo a otro router HSRP con una prioridad mayor pase a ser Activa (sí tiene preemption habilitado). Para configurar HSRP interfase tracking, se usa el comando:
**standby [group] track interface [priority]**

Cuando caen múltiples tracked interfaces, la prioridad es reducida por una cantidad acumulativa. Si se fija explícitamente el valor de disminución, entonces el valor es disminuido por esa cantidad si esa interfase cae, y las disminuciones son acumulativas. Si no se fija un valor explícito de disminución, entonces el valor es disminuido por 10 para cada interfase que caiga, y las disminuciones son acumulativas.

El ejemplo siguiente utiliza la siguiente configuración, con el valor de disminución por defecto de 10.

**Nota:** Cuando no se especifica el numero de grupo HSRP, el número del grupo por defecto es grupo 0.

```
interface ethernet0
    ip address 10.1.1.1 255.255.255.0
    standby ip  10.1.1.3
    standby priority 110
    standby track serial0
    standby track serial1
```

El comportamiento de HSRP con esta configuración es:

- 0 interfaces caídas = no disminuye (prioridad es 110)
- 1 interfase caída = disminuye en 10 (prioridad se convierte en 100)
- 2 interfaces caídas = disminuye en 10 (prioridad se convierte en 90)

El comportamiento antedicho de HSRP es correcto incluso si los valores del decremento se configuran explícitamente como a continuación:

```
interface ethernet0
    ip address 10.1.1.1 255.255.255.0
    standby ip  10.1.1.3
    standby priority 110
    standby track serial0 10
    standby track serial1 10
```

Antes del Cisco IOS release 12.1, si se encendía un router con una interfase caída, HSRP interfase tracking reconocía la interfase como levantada.

### 3.3.4. Usa Burned-In Address

Burned-In Address es la dirección propia de cada interfase, el uso de las características burned-in address (BIA) permite a los grupos HSRP usar su la burned-in MAC address de la interfase en vez de una dirección MAC de HSRP. El uso BIA primero fue implementado en Cisco IOS release 11.1(8). Para configurar HSRP para usar BIA, se usa el comando:
**standby use-bia [scope interface]**

El comando use-bia fue implementado para superar las limitaciones de usar una dirección funcional para la MAC address HSRP en interfaces Token Ring.

**Nota:** Cuando HSRP corre en un ambiente multiple-ring source-routed bridging y los routers HSRP residen en diferentes anillos, usar las direcciones funcionales puede causar la confusión Routing Information Field (RIF). Por esta razón, Fue introducido el comando use-bia.

Las características de use-bia también permiten el uso de DECnet, Xerox Network Systems (XNS), y de HSRP en el mismo router permitiendo que la dirección MAC de DECnet (el BIA) sea utilizado como la dirección MAC HSRP. El comando use-bia también es útil en las situaciones de red donde un dispositivo BIA ha sido configurado en otro dispositivo en la LAN.

Sin embargo, el comando use -bia tiene varias desventajas:

- Cuando un router pasa a ser Activo, la dirección IP virtual es movida a una MAC address diferente. El nuevo router Activo envía una respuesta gratuita ARP, pero no todos los hosts manejan el ARP gratuitos correctamente.
- El Proxy ARP se corta cuando se configura use-bia. Una router standby no puede recobrar la base de datos del proxy ARP perdido del router fallado.
- Antes del Cisco IOS release 12.0(3.4)T, solo un grupo HSRP estaba permitido si estaba configurado use-bia.

Cuando se configura el comando use-bia en una subinterfase, esta es mostrada en la interfase principal y es aplicada a todas las subinterfaces. En Cisco IOS release 12.0(6.2) y

posteriores, el comando use-bia se extiende con otras opciones de la interfase para permitir que sea aplicado a una sola subinterfase.

### 3.3.5. Grupos Múltiples HSRP.

La característica de grupos múltiples de HSRP (Múltiple HSRP: MHSRP) fue agregada en Cisco IOS release 10.3. Esta característica permite redundancia y balanceo de carga dentro de redes, y permite que los routers redundantes sean utilizados más completamente. Mientras un router esta activamente forwardeando tráfico para un grupo de HSRP, puede estar en standby o en el estado listen (escucha) para otro grupo.
Con en el Cisco IOS release 12.0(3.4)T, se puede usar el comando use-bia con múltiples grupos HSRP habilitados.

### 3.3.6. Dirección MAC Configurable.

Normalmente se usa HSRP para ayudar a las estaciones finales a localizar el primer gateway de salto para enrutamiento IP. Las estaciones finales se configuran con un default-gateway. Sin embargo, HSRP puede proporcionar la primera redundancia del salto para otros protocolos. Algunos protocolos, tales como Advanced Peer-to-Peer Networking (APPN), utilizan la dirección MAC para identificar el primer salto para propósitos de enrutamiento.
En este caso, es a menudo necesario poder especificar la dirección MAC virtual usando el comando **standby mac-address**. La dirección IP virtual es poco importante para estos protocolos. La sintaxis actual del comando es:
**standby [group] mac-address mac-address.**

**Nota:** No puede utilizarse este comando en un interfase Token Ring.

### 3.3.7. Autenticación.

La característica de autentificación de HSRP consiste de un clear-text key (llave texto limpio) compartida contenida dentro de los paquetes HSRP. Esta característica evita que

los routers de menor prioridad aprendan la dirección IP standby y los valores standby de los temporizadores del router de mas alta prioridad.

Para configurar la cadena de autentificación de HSRP, se usa el comando **standby authentication string.**

### 3.3.8. Redundancia IP.

HSRP proporciona redundancia stateless para el enrutamiento IP. HSRP por sí mismo se limita a mantener su propio estado. Asume que cada router construye y mantiene sus propias tablas de enrutamiento independientemente de otros routers. La característica de redundancia IP proporciona un mecanismo que permite a HSRP proveer un servicio para aplicaciones cliente de modo que ellos puedan implementar statefull failover.

La redundancia IP no proporciona un mecanismo para aplicaciones pares para el intercambio de información de estado. Esto se deja a aplicaciones propias, y es esencial si las aplicaciones proporcionan el statefull failover.

La redundancia IP es actualmente implementada solo para Agentes Móviles IP Home.

Lo que sigue es una configuración de muestra:

```
configure terminal
 router mobile
 ip mobile home-agent standby hsrp-group1

interface e0/2
 no shutdown
 ip address 20.0.0.1 255.0.0.0
 standby 1 ip 20.0.0.11
 standby 1 name hsrp-group1
```

### 3.3.9. SNMP Management Information Base (MIB).

Esto es la Información Básica de Administración SNMP.

Support SNMP Management Information Base (MIB) fue agregado a Cisco IOS release 12.0(3.0)T. Hay dos MIBs relevantes para HSRP:

- ciscoMgmt 106: El módulo MIB para manejar HSRP.
- ciscoMgmt 107: La extensión del modulo MIB para manejar HSRP.

Antes de Cisco IOS release 12.0(6.1)T, un camino del MIB HSRP extendido cuando una Bridge Group Virtual Interface (BVI) estaba presente causaba un crash en el router.

### 3.3.10. Soporte HSRP para Multiprotocol Label Switching Virtual Private Networks (MPLS/VPN).

HSRP support Multiprotocol Label Switching Virtual Private Networks (MPLS VPNs) fue agregado en Cisco IOS release 12.1(3)T.

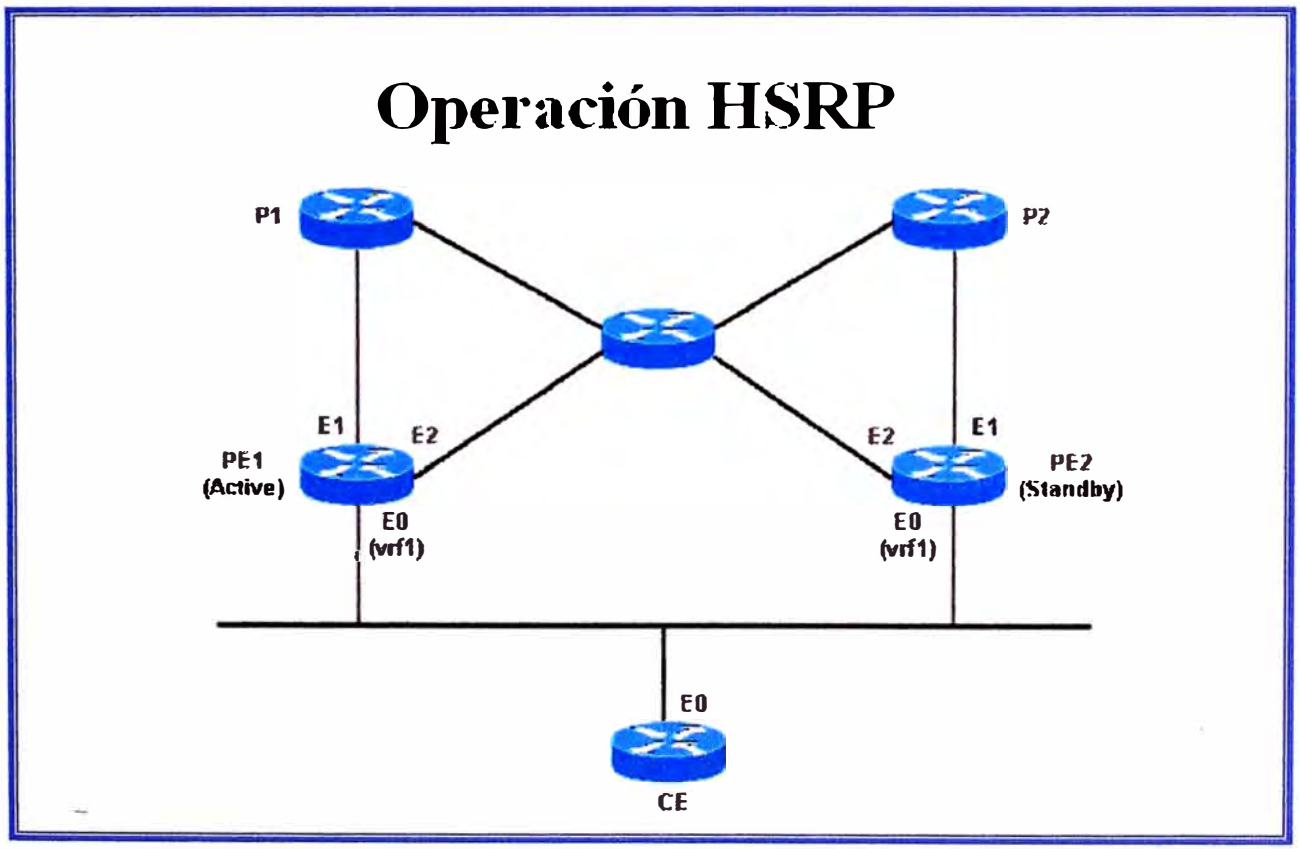


**Fig. Nº 3.1 Ejemplo de diagrama de conexiones VRF.**

HSRP en una interfase MPLS/VPN, es útil cuando se tiene una Ethernet conectada entre dos bordes del proveedor, Provider Edges (PEs) y se tiene cualquiera de lo siguiente:

- Un borde del cliente, Customer Edge (CE) con una ruta default a la Dirección IP virtual HSRP.
- Unos o más hosts con la dirección IP virtual de HSRP configurado como default gateway.

La figura 3.1 muestra 2 PEs con HSRP corriendo entre sus interfaces VPN Routing/Forwarding (VRF). Configuramos el CE con la dirección IP virtual de HSRP como su ruta por defecto. Y configuramos HSRP para seguir las interfaces que conectan el PEs con el resto de la red del proveedor. Por ejemplo, si la interfase E1 de PE1 falla, la prioridad de HSRP será reducida tal que PE2 asume el control de reenvío de los paquetes a la dirección IP/MAC virtual.

Se pueden usar los siguientes comandos para verificar que la dirección IP virtual de HSRP está en las tablas correctas VRF ARP y Cisco Express Forwarding:

**ed1-pe1# show ip arp vrf vrf1**

| Protocol | Address | Age (min) | Hardware Addr | Type | Interface |
|---|---|---|---|---|---|
| Internet | 10.2.0.1 | - | 00d0.bbd3.bc22 | ARPA | Ethernet0/2 |
| Internet | 10.2.0.20 | - | 0000.0c07.ac01 | ARPA | Ethernet0/2 |

**ed1-pe1# show ip cef vrf vrf1**

| Prefix | Next Hop | Interface |
|---|---|---|
| 0.0.0.0/0 | 10.3.0.4 | Ethernet0/3 |
| 0.0.0.0/32 | receive | |
| 10.1.0.0/16 | 10.2.0.1 | Ethernet0/2 |
| 10.2.0.0/16 | attached | Ethernet0/2 |
| 10.2.0.1/32 | receive | |
| 10.2.0.20/32 | receive | |
| 224.0.0.0/24 | receive | |
| 255.255.255.255/32 | receive | |

En la tabla 3.2 se muestra la configuración:

**TABLA 3.2 Configuración del escenario de la figura 3.1.**

| Router PE1 | Router PE2 |
|---|---|
| **Configure terminal** | **configure terminal** |
| ! | ! |
| ip cef | ip cef |
| ! | ! |
| ip vrf vrf1 | ip vrf vrf1 |
| rd 100:1 | rd 100:1 |
| route-target export 100:1 | route-target export 100:1 |
| route-target import 100:1 | route-target import 100:1 |
| ! | ! |
| interface ethernet0 | interface ethernet0 |
| no shutdown | no shutdown |
| ip vrf forwarding vrf1 | ip vrf forwarding vrf1 |
| ip address 10.2.0.1 255.255.0.0 | ip address 10.2.0.2 255.255.0.0 |
| standby 1 ip 10.2.0.20 | standby 1 ip 10.2.0.20 |
| standby 1 priority 105 | standby 1 priority 100 |
| standby 1 preempt delay minimum 10 | standby 1 preempt delay minimum 10 |
| standby 1 timers 3 10 | standby 1 timers 3 10 |
| standby 1 track ethernet1 10 | standby 1 track ethernet1 10 |
| standby 1 track ethernet2 10 | standby 1 track ethernet2 10 |

### 3.3.11. Soporte HSRP para ICMP Redirects.

HSRP se basa en el concepto que los pares de routers HSRP que protegen una subred pueden proporcionar el acceso al resto de las subredes que abarquen la red. Por lo tanto, es irrelevante cual router se convierte en el router HSRP Activo, pues todos los routers tenían rutas a cada subred.

HSRP hace uso de una dirección IP virtual especial y una dirección MAC virtual, que se adjuntan lógicamente al router HSRP Activo. ICMP redirects son deshabilitados automáticamente en una interfase al usar HSRP en esa interfase. Del IOS 12.1(3)T hacia adelante, las características de ICMP Redirects habilitan ICMP redirects en la interfase

configurada con HSRP. Esto se hace para evitar que los hosts vuelvan a dirigir a la dirección IP virtual de HSRP. Es posible que los dos (o más) routers en una subred no tengan conexión idéntica al resto de la red, es decir, para un dirección IP particular de destino, uno u otro de los routers puede tener una mucho mejor ruta a esa dirección, o puede incluso ser el único router adjuntado a esa dirección.

El protocolo del ICMP permite que un router vuelva a redirigir a una estación final a enviar los paquetes a un destino particular a otro router en la misma subred, si el primer router sabe que el otro router tiene una mejor ruta a ese destino particular. Al igual que el caso para default gateways, si el router al cual la estación final ha sido redireccionada para un destino particular falla, entonces los paquetes de la estación final a ese destino no serán entregados. En HSRP estándar, esto es exactamente lo que sucede. Por esta razón, se recomienda deshabilitar ICMP redirects si HSRP esta activado.

Ampliar la relación entre el ICMP redirects y HSRP proporciona una solución a este problema, permitiendo tomar ventajas de los beneficios de ambos ICMP Redirects y HSRP. Dos (o más) grupos HSRP están corriendo en cada subred, con al menos tantos grupos HSRP configurados como routers participantes. Se configuran las prioridades de modo que cada uno de los routers sea master por lo menos de un grupo HSRP. Cuando un router determina redirigir una estación final a un router diferente para un destino especifico, entonces en vez de redireccionar la estación final a la dirección IP de ese otro router, encuentra un grupo HSRP que está siendo dominado por ese router, y redirige la estación final a la dirección IP virtual correspondiente. Si este router falla, HSRP se asegura que otro router asuma el control de su trabajo y, quizás, redireccione la estación final a otro router.

### 3.4. Medios e Interfaces Soportados por HSRP.

Desde Cisco IOS Software release 10.0, la funcionalidad de HSRP ha estado disponible en Ethernet, Token Ring y Fiber Distributed Data Interfase (FDDI). Interfaces Fasth Ethernet y ATM también son soportadas por HSRP.
Virtual LANs (VLANs) permiten que las topologías lógicas de red sobrepongan a la infraestructura física switcheada como tales que cualquier colección arbitraria de puertos

del LAN se puede combinar en un grupo de usuario autónomo o comunidad de interés. Soporte VLAN para HSRP fue agregado en Cisco IOS release 11.1 para IEEE 802.10 Secure Data Exchange (SDE), y Cisco IOS release 11.3 para Cisco Inter-Switch Link (ISL).

### 3.4.1. Ethernet.

Algunos controladores Ethernet (Lance y QUICC) en productos del low-end pueden tener una sola dirección MAC unicast en su filtro de direcciones. En estas plataformas solo un grupo HSRP es permitido, y la dirección de la interfase se cambia a la dirección MAC virtual HSRP cuando el grupo pasa a ser Activo. Si se está utilizando HSRP en routers con interfaces múltiples de este tipo, se debe configurar cada interfase con un número diferente de grupo de HSRP.

**Nota:** El router Cisco 7200 también utiliza el controlador Lance Ethernet, pero soporta MHSRP (Múltiple HSRP) en software.

Cisco recomienda no tener más de veinticuatro HSRP Ethernet Interface Processors (EIPs) debido al tiempo que toma para actualizar los filtros de direcciones para HSRP. Tener más de veinticuatro HSRP EIPs puede causar inestabilidad y carga excesiva del Procesador.

Si se tiene más de veinticuatro EIPs, se debe intentar sustituir el EIPs con Versatile Interface Processors (VIPs) y adaptadores de puerto Ethernet. VIPs han sido aprobados hasta par ochenta grupos HSRP. También se puede reducir el número de grupos HSRP, e incrementar el HSRP hello y hold time.

### 3.4.2. Token Ring.

Una limitación de correr HSRP en un interfase Token Ring es que no se puede reprogramar el filtro de direcciones en el chipset Token Ring de la misma manera que en Ethernet, FDDI o ATM emulation. Token Ring usa direcciones funcionales, de las cuales hay solamente un pequeño número disponible que no tiene conflicto con otras aplicaciones del espacio funcional de direcciones.

Cuando se corre HSRP en un ambiente Source-Route Bridging (SRB), el uso de direcciones funcionales puede causar confusión al RIF.

### 3.4.3. 802.1Q.

Cisco recomienda usar Cisco IOS release 12.0(8.1)T o posterior para HSRP sobre 802.1Q.

### 3.4.4. ISL Inter-Switch Link.

HSRP sobre ISL está disponible en Cisco IOS releases 11.2(6)F, 11.3, 12.X. Se recomienda usar la revisión de 12.0(7) o posterior para evitar los problemas descritos en el Bug ID CSCdm68811.

### 3.4.5. Fiber Distributed Data Interface (FDDI).

Un puerto adaptador FDDI corta frames del anillo si ve una de sus propias direcciones MAC en la MAC origen. Si un evento de la red causa que ambos routers pasen a ser Activos, entonces ambos routers envían paquetes hello HSRP con la misma dirección MAC virtual. Cada router erróneamente corta el paquete hello del otro router de la red, y ambos permanecen activos.
Este defecto tiene Cisco bug ID CSCdj30049 .

La solución a este problema en Cisco IOS release 11.2(11.1) es para routers HSRP en un ambiente FDDI para utilizar su propia única dirección burned-in MAC para intercambiar mensajes y correr el protocolo HSRP. Para asegurar que la caché de bridges y switches aprendan la correcta entrada para la dirección MAC virtual, el router Activo también envía mensajes periódicos de refresco usando la dirección MAC HSRP.

### 3.4.6. Actualizaciones MAC.

Los routers HSRP en un ambiente FDDI utilizan su propia única dirección burned-in MAC para intercambiar mensajes y para correr el protocolo de HSRP. Para asegurar eso, la cache de los bridges y switches aprendan el correcto puerto de entrada para la dirección MAC

virtual el router Activo también envía mensajes periódicos de refresh usando la dirección MAC de HSRP.

Si no se tiene un switch o bridge en la red, se puede deshabilitar el envío de paquetes refresh como se muestra:

```
interface fddi 1/0/0
 ip address 10.1.1.1 255.255.255.0
 standby ip 10.1.1.250
 standby mac-refresh 0
```

### 3.4.7. Bridge Group Virtual Interface (BVI).

El soporte HSRP para Bridge Group Virtual Interfaces (BVIs) fue agregado Cisco IOS release 12.0(6.2)T.

### 3.4.8. Subinterfaces.

Los grupos HSRP en subinterfaces deben tener un número de grupo único entre todos los grupos en todas las subinterfaces en la misma interfase principal. Esto es porque las subinterfaces no reciben un único índice de interfase SNMP. Si se tuviera dos grupos con el número N en diferentes subinterfaces, entonces en el MIB, el grupo N en una sub-interfase 1 y el grupo N en la sub-interfase 2 parecerían ser del mismo grupo.

# CAPÍTULO IV
# DISEÑANDO REDES DIAL-ON-DEMAND ROUTING (DDR)

## 4.1. Introducción a Dial-on-Demand Routing (DDR).

Dial-on-Demand Routing, DDR (Enrutamiento por Llamada bajo Demanda), proporcionan conexiones de red a través de Public Switched Telephone Networks (PSTNs). Las redes dedicadas de gran área son implementadas típicamente sobre líneas arrendadas u opciones más modernas del proveedor de servicio tales como Frame Relay o ATM. Dial-en-Demand Routing proporciona control de sesión para conectividad de redes sobre redes de conmutación de circuito, que alternadamente proporciona servicios en demanda y reduce costes de la red.

DDR puede ser usado sobre interfaces seriales síncronas, interfaces Integrated Services Digital Network (ISDN), o interfaces seriales asincrónicas. V.25bis y DTR dialing son usados para Switched 56 Channel Service Unit/Data Service Unit (CSU/DSUs), ISDN Terminal Adapters (TAs), o módems síncronos. Las líneas seriales asíncronas están disponibles en el puerto auxiliar en los routers Cisco y en los servidores de comunicación Cisco para conexiones a los módems asincrónicos. DDR es soportado sobre ISDN usando interfaces Basic Rate Interface (BRI) y Primary Rate Interface PRI.

El Software de Cisco para Dial-on-Demand Routing (DDR) proporciona varias funciones. Las primeras tablas de enrutamiento spoof (simulación) DDR para proporcionar la imagen de conectividad full-time usan interfaces Dialer. Cuando la tabla de enrutamiento forwardea un paquete a un interfase Dialer, DDR filtra hacia afuera los paquetes interesantes para establecer, mantener, y liberar conexiones conmutadas. Internetworking es lograda sobre la conexión DDR mantenida usando PPP u otras técnicas de encapsulación WAN (tales como HDLC, X.25, SLIP).

### 4.1.1. Diseño Apilado DDR.

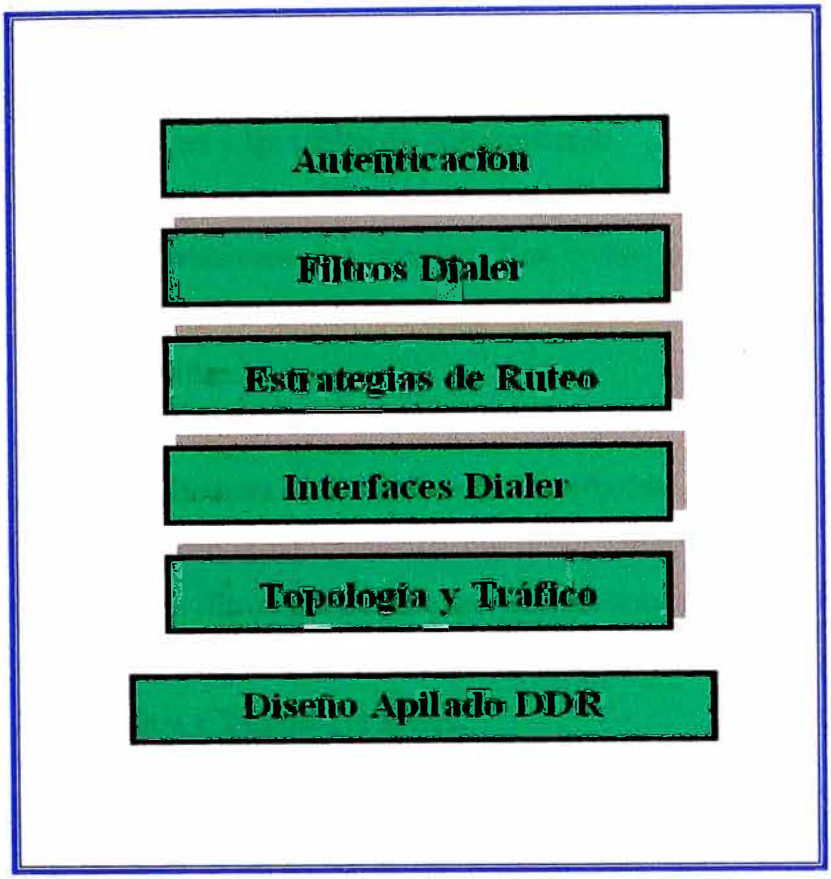


**Fig. Nº 4.1 Diseño apilado DDR.**

Similar al modelo proporcionado por la OSI para entender y diseñar internetworking, una aproximación apilada, mostrada en la figura 4.1, puede ser usada para diseñar redes DDR.

### 4.1.2. Nube Dialer.

La red formada por los dispositivos DDR interconectados puede genéricamente etiquetarse como el medio dialer o nube dialer. El alcance de la nube dialer incluye solamente los dispositivos interconectados previstos y no incluye el medio conmutado enteros (la ISDN entera atraviesa el globo y está más allá del alcance de la nube dialer). La exposición a la ISDN debe ser considerada al diseñar seguridad.

Las características fundamentales de las nubes dialer son las siguientes:

- Las nubes dialer son paquetes colectivos de conexiones potenciales y conexiones activas point-to-point.
- En conexiones activas, las nubes dialer forman un medio NBMA (Non-Broadcast Multiaccess) similar a Frame Relay.

- Para dialing de salida en circuitos conmutados (tales como ISDN) las direcciones del protocolo de red deben estar configuradas a un número de directorio.
- Las conexiones DDR inactivas están spoofed (simulando) para aparecer como activas a las tablas de enrutamiento.
- Broadcast no deseado u otro tráfico que causen conexiones innecesarias puede ser prohibitivamente costoso. Los costes potenciales en medios tarifados (tales como ISDN) se deben analizar y supervisar con mucho cuidado para prevenir tales pérdidas.

Las características de las nubes dialer afectan cada etapa del diseño de la Internetworking DDR. Una sólida comprensión del direccionamiento del protocolo de red, enrutamiento, y estrategia de filtros puede resultar en internetworks muy robustas y rentables.

## 4.2. Tráfico y Topología DDR.

Para determinar la topología óptima, el diseñador DDR debe realizar un análisis de tráfico de las aplicaciones de red que deben ser soportadas. Esto incluye contestar a las preguntas siguientes:

- ¿Qué tan a menudo el tráfico de datos necesita moverse entre los puntos DDR?
- ¿Qué lado de la conexión DDR puede establecer la conexión? ¿Cuántos sitios remotos?
- ¿Es esta una solución punto-punto o una solución multipunto?

### 4.2.1. Topologías.

El factor más importante en seleccionar la topología es el número de sites que serán soportados. Si solo dos puntos están implicados, la topología punto-punto es usada. Si son más de 2 puntos los soportados, entonces la topología hub-and-spoke es típicamente usada. Para una pequeña cantidad de sites con volúmenes de tráfico muy bajos, la topología full-mesh puede ser la solución más apropiada.
Las topologías para DDR que se cubrirán en este estudio son:

- Point-to-point
- Fully meshed

- Hub-and-Spoke

**a) Topología Point-to-Point.**

En una simple topología punto-punto, dos puntos están conectados el uno al otro. Cada punto tiene una interfase dialer y mapea la dirección del otro site a un número telefónico. Si se requiere ancho de banda adicional, se pueden agregar múltiples enlaces usando Multilink PPP. La figura 4.2 muestra este tipo de conexión.

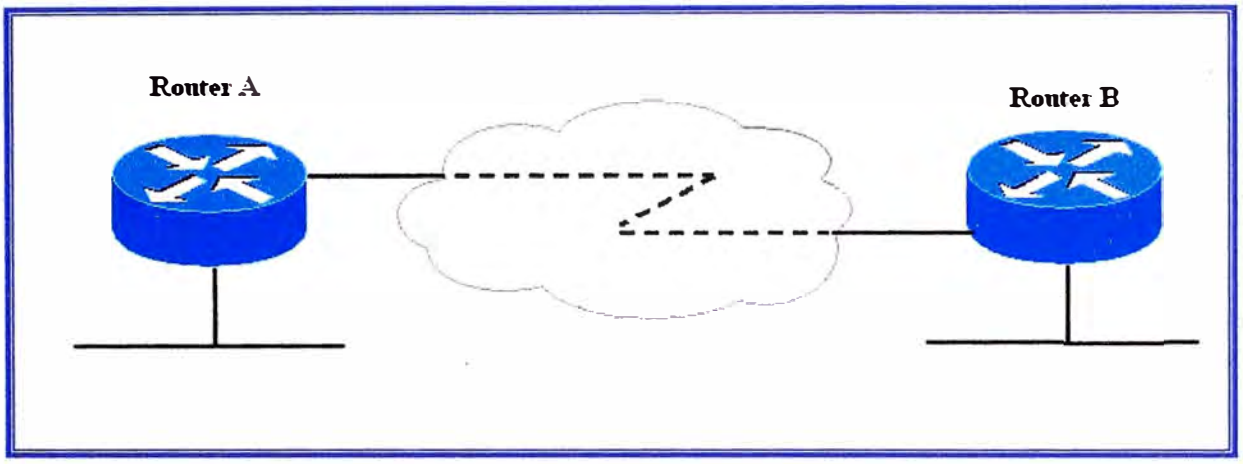


**Fig. N° 4.2 Topología Point-to-Point.**

**b) Topología Fully Meshed.**

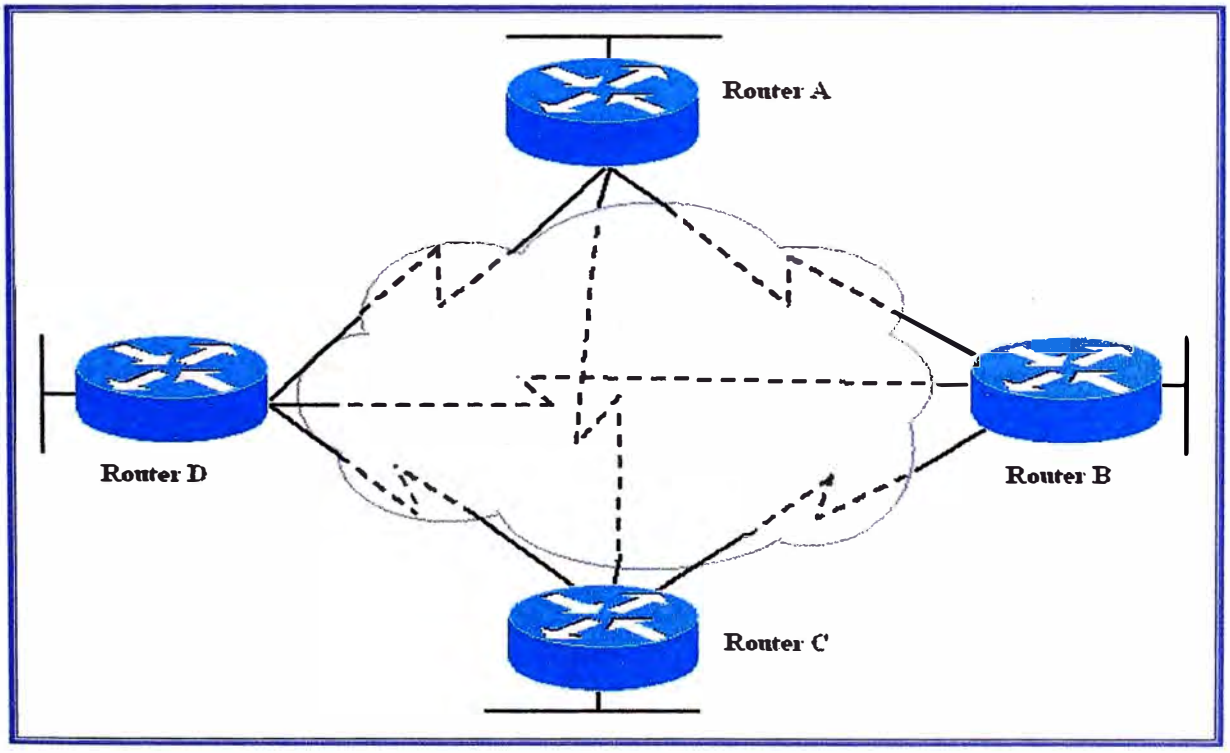


**Fig. N° 4.3 Topología Fully Meshed.**

La configuración fully meshed (conectados todos) es recomendada solo para redes DDR muy pequeñas. La topología fully meshed puede aerodinamizar el proceso dialing para conectividad any-to-any como cada punto puede llamar a cualquier otro directamente, en vez de llamar a través de un punto central, la cual hace otra llamada al punto destino. Sin embargo, la configuración para cada punto es más compleja porque cada uno debe tener la información de mapeo para cada lado remoto.

Si se desea compartir carga, las interfaces pueden configurarse para capacidad de MultiLink PPP. Además de la complejidad de la configuración, debe haber suficientes interfaces en cada dispositivo con la capacidad de llamar o recibir llamadas de todos los demás dispositivos. La figura 4.3 muestra este tipo de conexión.

**c) Soluciones DDR Hub-and-Spoke.**

En una topología hub-and-spoke (central y terminales), un punto central está conectado con varios puntos remotos. Los puntos remotos se comunican directamente con el punto central; no llaman a cualquiera de los otros puntos remotos. Esta topología trabaja muy bien para las soluciones de gran escalamiento. La figura 4.4 muestra este tipo de conexión.

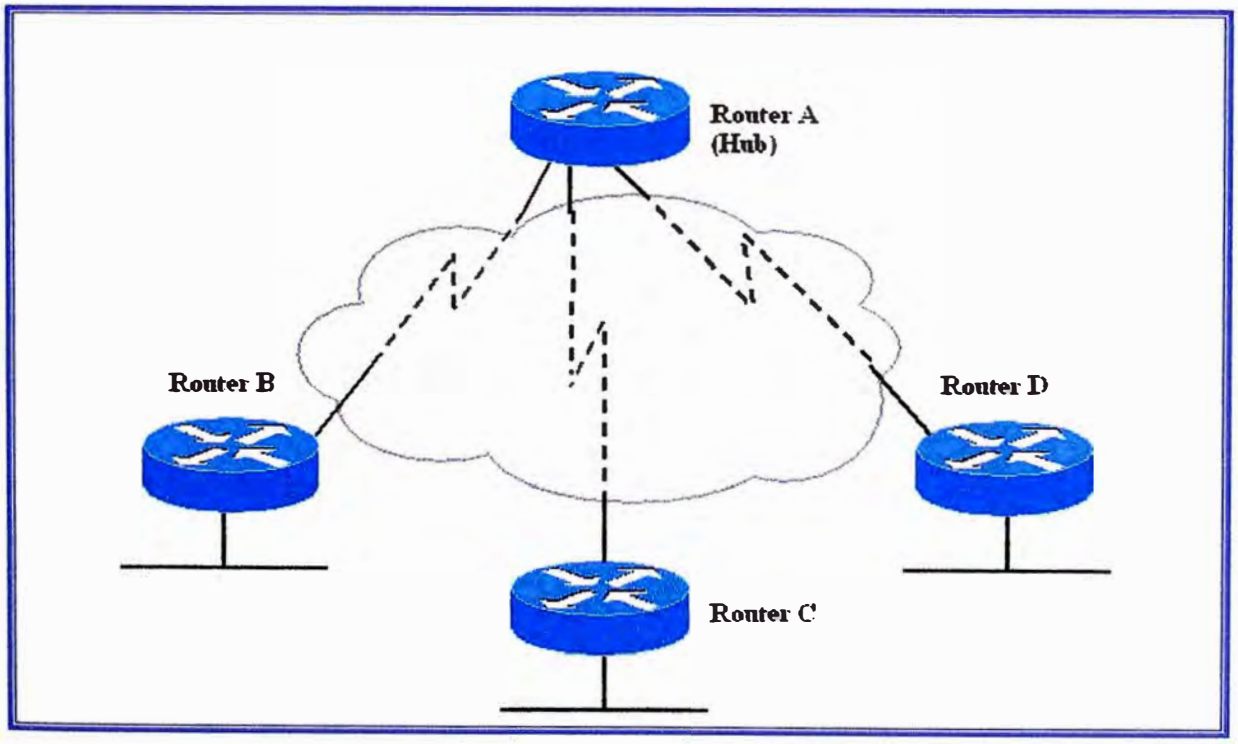


**Fig. N° 4.4 Topología Hub-and-Spoke.**

La topología hub-and-spoke es mas fácil de configurar que la topología fully meshed cuando se requieren topologías multipunto porque las interfaces dialer de los puntos remotos están mapeadas solo al punto central. Esto permite que la mayoría de la complejidad del diseño (tal como dirección, enrutamiento, y autentificación) sea manejada en el Hub DDR (punto central DDR). La configuración de los puntos remotos puede ser grandemente simplificada (similar a un extremo de una topología point-to-point).

Si se requiere el inicio de conectividad any-to-any entre los sites remotos, el comportamiento del enrutamiento puede necesitar ser modificado dependiendo del comportamiento del interfase dialer (es decir, puede ser necesario deshabilitar split-horizon en protocolos de enrutamiento distance-vector).

### 4.2.2. Análisis de Tráfico.

Para el análisis de tráfico, se desarrolla una carta de que protocolos necesitan ser capaces de soportar dialing basado en DDR y de qué dispositivos. Esto será la base del resto del diseño de DDR.
Por ejemplo, la compañía KDT ha seleccionado una topología hub-and-spoke (para proveer escalamiento) y ha desarrollado las necesidades mostradas en la tabla 4.1 para sus requerimientos de la nube de DDR.

El propósito de la tabla 4.1 es identificar qué puntos y protocolos requieren la capacidad para iniciar las conexiones DDR. Una vez que la conexión es establecida, cada protocolo requiere conectividad en 2 sentidos vía las tablas de enrutamiento y el mapeo de direcciones en la nube dialer. Dial-in (llamada entrante) contra dial-out (llamada saliente) es vista desde la perspectiva del punto central.

A menudo la meta fundamental de una red DDR es ofrecer una mejora de coste sobre los cargos WAN asociadas a las conexiones dedicadas. El análisis de tráfico adicional se debe realizar para cada protocolo en este o la etapa de diseño Dialer Filtering (Filtros Dialer). Las aplicaciones de red usan la infraestructura proporcionada por la internetwork en muy diferentes y a menudo inesperadas maneras. Esto es crítico para realizar un análisis cuidadoso del tráfico del mundo real de la red que pasara por los medios dialer para

determinar si una red DDR puede funcionar de una manera confiable. Las herramientas de captura y análisis de paquetes proporcionan la herramienta más valiosa para este análisis.

**TABLA Nº 4.1: Requerimientos de conectividad de Protocolo DDR para KDT.**

| Remote Site | Dial-In Protocols | Dial-Out Protocols | Notes |
|---|---|---|---|
| c700A | IP, IPX | None | |
| c700B | IP | None | |
| c1600A | IP, AppleTalk | IP | |
| c2500A | IP, IPX, AppleTalk | IP, IPX, AppleTalk | |
| c2500B | IP, IPX | IP | |
| NAS3600A | IP, IPX, AppleTalk | IP, IPX, AppleTalk | |

### 4.3 Interfaces Dialer.

El acceso al medio dialer es a través de las interfaces dialer de Cisco. Los canales B ISDN, interfaces seriales síncronas, y las interfaces asíncronas pueden todas convertirse en interfaces dialer usando comandos de configuración de la interfase dialer. Para entender interfaces dialer, se detallan los siguientes conceptos:

- Interfaces físicas soportadas.
- Grupos Rotatorios Dialer.
- Perfiles Dialer.
- Direccionamiento Dialer.
- Mapas Dialer.

Las interfaces dialer también proporcionan la base para el soporte de tabla de enrutamiento spoofing y filtros dialer. Esta sección se centra en características de las capas inferiores de las interfaces dialer.

### 4.3.1 Interfaces Físicas Soportadas.

Varios tipos de interfaces físicas pueden ser habilitadas como interfase dialer.

a) **Interfaces Seriales Síncronas.**

Dialing en líneas seriales síncronas puede ser iniciada usando dialing V.25bis o DTR dialing. V.25bis es el estándar ITU para dialing in-band (llamada en banda). Con dialing in-band, la información dialing se envía sobre la misma conexión que lleva los datos. V.25bis se utiliza en una variedad de dispositivos, incluyendo los módems síncronos, ISDN Terminal Adapters (TAs), y switched 56 DSU/CSUs.

Con DTR dialing, la señal DTR es activada en la interfase física, lo cual hace que algunos dispositivos marquen un número configurado en ése dispositivo. Cuando se usa DTR dialing, la interfase no puede recibir llamadas. Pero usar dialing DTR permite que los dispositivos de bajo-coste sean utilizados en los casos donde solamente un solo número necesita ser marcado. Las líneas seriales síncronas soportan encapsulación de datagrama PPP, HDLC, y X.25.

Para convertir una interfase serial síncrona en una interfase dialer, se usa el comando Cisco IOS **dialer in-band** o **dialer dtr**.

b) **Interfaces Integrated Systems Digital Network (ISDN).**

Todos los dispositivos ISDN se suscriben para proporcionar servicios a través de un proveedor de servicios ISDN, generalmente una compañía telefónica. Las conexiones ISDN DDR se hacen en los canales B a 56 o 64 Kbps dependiendo de las capacidades de portadora del switch ISDN end-to-end. Multilink PPP es muy usado para permitir a los dispositivos BRI agregar ambos canales B para ampliar el ancho de banda y procesamiento.

Las interfaces ISDN BRI y PRI se configuran automáticamente como interfaces dialer in-band. ISDN puede soportar encapsulación PPP, HDLC, X.25, y V.120. Típicamente, PPP será usado para soluciones DDR. Las interfaces ISDN se configuran automáticamente como interfaces dialer in-band.

Por ejemplo, al examinar una interfase BRI en una router Cisco, se puede ver que esta en spoofing (pretendiendo estar up/up así la tabla de enrutamiento puede apuntar a esta interfase), como se muestra en la siguiente línea de comando:

**c1600A#show interface BRI 0**

**BRI0 is up, line protocol is up (spoofing)**

Sin embargo, las interfaces físicas son los canales individuales B (BRI0:1 y BRI0:2) que son manejados por la interfase dialer (BRI0), como se observa a continuación están caídas.

**c1600A#sh int bri 0 1**

**BRI0:1 is down, line protocol is down**

**Hardware is BRI**

**MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255**

**Encapsulation PPP, loopback not set, keepalive set (10 sec)**

**LCP Closed, multilink Closed**

**Closed: IPCP, CDPCP**

**c) Conexiones de Modem Asíncrono.**

Las conexiones asíncronas son utilizadas por los servidores de comunicación o a través del puerto auxiliar en un router. Las conexiones asíncronas DDR se pueden usar para soportar múltiples protocolos capas de red. Cuando consideramos soluciones asíncronas DDR, los diseñadores deben considerar si las aplicaciones de la red pueden tolerar el gran tiempo de disposición de llamada y bajo procesamiento de módems análogos (en comparación con ISDN). Para algunas aplicaciones de diseño, DDR sobre conexiones de modem asíncronos puede proporcionar una opción muy rentable.

### 4.3.2 Grupos Rotatorios Dialer.

Para topologías hub-and-spoke o fully meshed que soportan múltiples conexiones entre puntos, las interfaces físicas pueden ser agrupado en grupos rotatorios con el comando **dialer rotary-group**. Las interfaces físicas asignadas al dialer rotary-group heredan su configuración de la interfase dialer correspondiente.

Si una de las interfaces físicas en un rotary-group está ocupada, la siguiente interfase disponible puede ser usada para hacer o recibir una llamada. No es necesario configurar rotary-groups para interfaces BRI o PRI pues los canales B de ISDN son automáticamente colocados en un rotary-group, no obstante interfaces múltiples BRI o PRI se pueden agrupar usando dialer rotary-group.

### 4.3.3. Perfiles Dialer.

Los perfiles dialer introducidos en el IOS 11.2 de Cisco ofrecen flexibilidad adicional del diseño tal como conexiones multipunto sobre ISDN. Los perfiles dialer proporcionan una metodología alternativa para diseñar redes DDR quitando la definición lógica de los puntos dialer de las interfaces físicas dialer.

### 4.3.4. Métodos de Encapsulación.

Cuando un enlace de datos limpio se establece entre dos puntos DDR, los datagramas de la red deben ser encapsulados y colocados en frames para el transporte a través del medio Dialer. Los métodos de encapsulación disponibles dependen de la interfase física que está siendo usada. Cisco soporta encapsulación data-link Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), Serial Line Interface Protocol (SLIP), y X.25 para DDR:

- PPP es el método de encapsulación recomendado porque soporta protocolos múltiples y es usado por conexiones síncronas, asíncronas o ISDN. Además, PPP realiza la negociación de la dirección y la autentificación y es interoperable con diversos vendedores.
- HDLC es soportado en líneas seriales síncronas y conexiones ISDN solamente. HDLC soporta protocolos múltiples. Sin embargo, HDLC no proporciona autentificación, que puede ser requerida si se usa grupos rotatorios dialer.
- SLIP trabaja solo en interfaces asíncronas y es soportado solo por IP. Las direcciones se deben configurar manualmente. SLIP no proporciona autentificación y es interoperable solo con otros vendedores que usen SLIP.
- X.25 es soportado en líneas seriales síncronas y un solo canal B ISDN.

### 4.3.5. Direccionamiento en la Nube Dialer.

Hay dos maneras de crear direccionamiento en las nubes dialer, como sigue:

- Aplicando una subred a la nube dialer
  Cada sitio conectado a la nube dialer se le entrega una única dirección de nodo en una subred compartida para usar en su interfase dialer. Este método es similar a numerar un LAN o WAN multipunto y simplifica el esquema de direcciones y la creación de rutas estáticas.
- Usar interfaces no numeradas
  Similar a usar direcciones no numeradas en las interfaces de línea dedicada punto-punto, la dirección de otra interfase en el router es prestada para usarla en la interfase dialer. La dirección no numerada toma ventajas del hecho de que hay solo dos dispositivos en el enlace punto a punto. La tabla de enrutamiento apunta a una interfase (la interfase dialer) y a una dirección next-hop (la cual debe estar incluida en una dialer map: estático o dinámico).

La creación de rutas estáticas para interfaces no numeradas puede ser poco más compleja porque el router debe ser configurado con la interfase que encuentra el siguiente salto de salida.

### 4.3.6 Dialer Maps.

Dialer Maps (Mapas Dialer), similar a la función proporcionada por una tabla ARP, dialer map traslada la dirección de protocolo next-hop al numero telefónico. Sin los dialer maps configurados estáticamente, la iniciación de la llamada DDR no puede ocurrir. Cuando la tabla de enrutamiento apunta a una interfase dialer, y la dirección del siguiente salto no se encuentra en un dialer map, el paquete es descartado.

En el ejemplo siguiente, los paquetes recibidos por un host en la red 172.20.0.0 son enrutados a la dirección next-hop de 172.20.1.2, la cual esta estáticamente mapeada al teléfono número 555-1212:

**interface dialer 1**
**ip address 172.20.1.1 255.255.255.0**

**dialer map ip 172.20.1.2 name c700A 5551212**

**!**

**ip route 172.20.0.0 255.255.255.0 172.20.1.2**

Contrastar con los parámetros del **dialer map** para broadcast fallará porque un paquete broadcast se transmite con una dirección next-hop de la dirección broadcast. Si se desea que los paquetes broadcast sean transmitidos al lado remoto definido por un dialer map, se usa el comodín **broadcast** con el comando **dialer map**.

Para configurar que las llamadas sean seteadas a 56 o 64 Kbps para llamadas ISDN, se puede usar la opción de velocidad con el comando **dialer map** cuando se configura la interfase.

**TABLA 4.2: Tabla de mapeo de direcciones DDR para KDT.**

| Remote Site | Dial-In Protocols | Directory# | Notes |
|---|---|---|---|
| c700A | IP: 172.20.1.2<br>IPX: 100.0000.0c00.0002 | 4085551212 | |
| c700B | IP:172.20.1.3 | 4155558888 | 56K |
| c1600A | IP: 172.20.1.4<br>AT: 20.4 | 5305551000 | |
| c2500A | IP: 172.20.1.5<br>IPX: 100.0000.0c00.0005<br>AT: 20.5 | 5125558085 | |
| c2500B | IP: 172.20.1.6<br>IPX: 100.0000.0c00.0006 | 2105552020 | |
| NAS3600A | IP: 172.20.1.1 | 8355558661 | Hub |

Cuando se configura DDR entre más de dos puntos, es necesario utilizar autenticación PPP y usar el comodín **name** con el comando **dialer map**, como el mapa dialer para las llamadas entrantes son mapeadas entre las direcciones de protocolo y nombres autenticados del usuario.

Para facilitar la construcción de los mapas dialer, el diseñador de la red debe construir una tabla de mapeo de direcciones como ayuda para la configuración. En la tabla 4.2, a la nube dialer se le ha asignado la subred IP 172.20.1.0/24, IPX network 100, y cable-range 20-20 de Apple Talk.

### 4.4. Estrategias de Enrutamiento.

La naturaleza de las redes DDR es que rutea y algunas tablas de servicios de directorio se deben mantener sobre conexiones idle (habilitadas y en espera). Los diseñadores DDR pueden usar una combinación de técnicas de enrutamiento estáticas, dinámicas, y snapshot para resolver las necesidades del diseño. Rutas por defecto y técnicas de spoofing del nodo remoto (tales como Cisco 700 series PAT y Cisco IOS EZIP) pueden ser usadas para simplificar grandemente el diseño de ruteo.

A menudo las redes usarán un protocolo de enrutamiento de convergencia rápida tales como OSPF o EIGRP; sin embargo, estos protocolos no funcionan fácilmente en medios dialer debido a su naturaleza broadcast y link-state. Típicamente, el enrutamiento estático y/o los protocolos de enrutamiento vector distancia son seleccionados para las conexiones DDR. La redistribución de rutas puede ser requerida para soportar la propagación de información de enrutamiento entre los diferentes protocolos de enrutamiento.

#### 4.4.1. Enrutamiento Estático.

Con las rutas estáticas, los protocolos de rutas de la red se ingresan manualmente, eliminando la necesidad de un protocolo de enrutamiento para difundir las actualizaciones de enrutamiento a través de la conexión DDR. Las rutas estáticas pueden ser efectivas en redes pequeñas que no cambian a menudo. Los protocolos de enrutamiento pueden generar tráfico que causen que las conexiones se establezcan innecesariamente.

Cuando se diseña en ambientes con IP no numeradas, las versiones antiguas de software de Cisco requerían múltiples rutas estáticas para cada destino: una ruta para definir el Dirección IP next-hop y una segunda para definir la interfase en la cual encontrar el next-hop (y el dialer map), lo cual hace muy complicado el sistema.

Esto es típicamente necesario para configurar redistribución de rutas estáticas en el protocolo de enrutamiento dinámico del backbone para asegurar la conectividad end-to-end. Por ejemplo, para redistribuir la ruta estática a otras redes en el Autonomous System 100 de EIGRP, se usa los comandos siguientes en la configuración:

**router eigrp 100**
**network 172.20.0.0**
**redistribute static**

### 4.4.2 Enrutamiento Dinámico.

El enrutamiento dinámico puede ser usado en el diseño de redes DDR en un número de maneras. El enrutamiento dinámico puede ser usado con snapshot routing (rutas almacenadas) para almacenar las rutas aprendidas por el protocolo de enrutamiento dinámico, así permite la automatización del mantenimiento de rutas estáticas. El enrutamiento dinámico puede ser usado como un trigger (disparador) para la convergencia de enrutamiento en diseños grandes y complejos de DDR.

Cuando el enlace DDR está conectado, la actualización de rutas fluirá entre ambos pares, permitiendo que los diseños redundantes converjan en la conexión física por la redistribución de actualizaciones de enrutamiento.

**a) Seleccionando un Protocolo de Enrutamiento Dinámico.**

El protocolo de enrutamiento seleccionado para el enlace DDR es típico de un protocolo Distance-Vector tal como RIP, RIP II, EIGRP o IGRP. Se recomienda seleccionar el protocolo más simple que resuelva las necesidades del diseño de la red y que es soportado por los routers DDR.

**b) Interfaces Pasivas.**

Las interfaces que son etiquetadas como Passive no enviarán actualizaciones de enrutamiento. Para evitar que las actualizaciones de enrutamiento establezcan conexiones DDR en las interfaces dialer que no envían la información de enrutamiento dinámico, se configura la interfase DDR con el comando **passive-interface** o usar listas de acceso. Usar el comando passive-interface o una lista de acceso evita que las actualizaciones de enrutamiento activen una llamada. Sin embargo, si se quisiera que las actualizaciones de enrutamiento fueran pasadas cuando el enlace esta activo, se usa una lista del acceso en vez del comando **passive-interface**.

**c)Split Horizons.**

Split Horizons (horizonte cortado). Los routers conectados a redes IP tipo broadcast y routers que usan protocolo de enrutamiento distance-vector usan split horizons para reducir la posibilidad de loops de enrutamiento. Cuando es habilitado split horizons, la información sobre las rutas que vienen en una interfase no es enviada hacia fuera en esa misma interfase.

**Nota:** Si el site remoto necesita comunicarse con algún otro, split horizons debe ser deshabilitado para topologías hub-and-spoke. En topologías hub-and-spoke, el punto remoto (spoke) aprenden uno acerca del otro a través del punto central (hub) con el cual están conectadas por una sola interfase. Para que los spoken envíen y reciba información a otro, split horizons puede ser deshabilitado para que las tablas de enrutamiento completas sean construidas en cada site.

**d) Rutas Dinámicas Conectadas.**

Las rutas dinámicas conectadas incluyen las dos siguientes:

- *Rutas instaladas Per-user AAA* - Los servidores AAA pueden instalar rutas asociadas a los usuarios usando la autorización AAA para descargar e instalar rutas mientras que los sites remotos se conectan.
- *Rutas PPP Peer* – Las direcciones IP Control Protocol (IPCP) negocian instalar rutas-host (host-routes) (mascarada de subred /32) para el par remoto. Este host-route puede ser propagado a los routers del backbone para proporcionar una robusta convergencia de enrutamiento. En la mayoría de

aplicaciones, el peer host-routes será beneficioso (o inofensivo) al diseño de redes. Si el peer host-route PPP no interactúa correctamente con las estrategias de enrutamiento existentes, estas pueden ser desactivadas con el comando de configuración de interfase **no peer neighbor-route.**

### 4.4.3 Snapshot Routing.

Con snapshot routing (rutas almacenadas), el router es configurado para enrutamiento dinámico. Snapshot routing controla el intervalo de actualización de protocolos de enrutamiento. Snapshot routing trabaja con los siguientes protocolos vector distancia:

- Routing Information Protocol (RIP) para IP
- Interior Gateway Routing Protocol (IGRP) para IP
- Routing Information Protocol (RIP) y Service Advertisement Protocol (SAP) para Novell Internet Packet Exchange (IPX)
- Routing Table Maintenance Protocol (RTMP) para AppleTalk
- Routing Table Protocol (RTP) para Banyan VINES

Bajo circunstancias normales, estos protocolos de enrutamiento difunden las actualizaciones cada 10 a 60 segundos, así con un enlace ISDN se actualiza cada 10 a 60 segundos simplemente para intercambiar información de enrutamiento. Desde una perspectiva de costos, esta frecuencia es prohibitiva. Snapshot routing soluciona este problema.

**Nota:** Snapshot routing esta disponible en el IOS de Cisco 10.2 o posteriores.

**a) Modelo Snapshot.**

Snapshot routing usa el modelo de diseño cliente-servidor. Cuando se configura snapshot routing, un router es designado como el servidor snapshot y uno o más routers son designados como clientes snapshot. El servidor y los clientes intercambian información de enrutamiento durante un período activo. Al principio del período activo, el router cliente llama al router servidor para intercambiar información de enrutamiento. Al final del período activo, cada router toma un snapshot de las entradas en su tabla de enrutamiento. Estas entradas siguen siendo

congeladas durante un período de silencio. Al final del período de silencio, otro período activo comienza, y el router cliente llama al router servidor para obtener la ultima información de enrutamiento. El router cliente determina la frecuencia a la cual llama al router servidor. El período de silencio puede ser tan grande como 100.000 minutos (aproximadamente 69 días).

Cuando el router cliente pasa del período de silencio al período activo, la línea puede estar caída u ocupada. Si esto sucede, el router tendría que esperar durante otro período completo de silencio antes que pueda actualizar su tabla de enrutamiento, lo cual puede afectar seriamente la conectividad si el período de silencio es muy largo. Para evitar tener que esperar por el período de silencio, snapshot routing soporta un periodo retry (reintentar). Si la línea no está disponible cuando finaliza el período de silencio, el router espera la cantidad de tiempo especificada por el período retry y luego la transición de un período activo empieza otra vez.

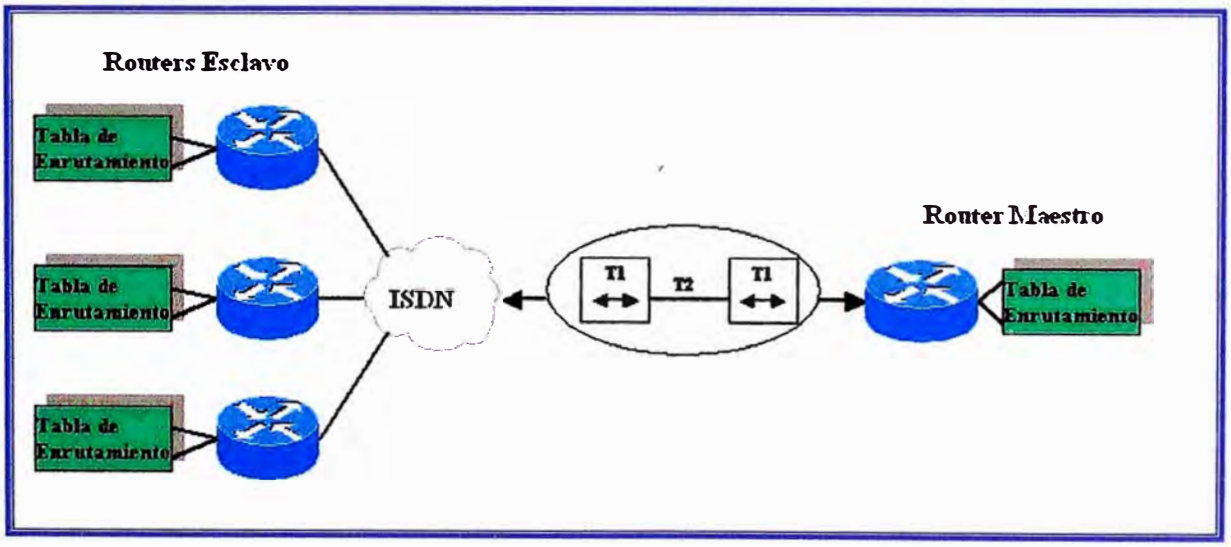


**Fig. N° 4.5: Snapshot routing en acción.**

El período retry es también útil en los ambientes dial-up en los cuales hay mas sitios remotos que líneas de interfase. Por ejemplo, el site central puede tener un PRI (con 30 canales de B disponibles) pero puede marcar más de 30 sites remotos. En esta situación, hay más comandos dialer-map que líneas disponibles. El router usa el comando **dialer map** y usa el tiempo retry para las líneas que no puede tener

acceso inmediatamente. En la figura 4.5 se muestra el modo de operación de snapshot routing.

### 4.4.4 Habilitando Snapshot Routing.

Snapshot routing es habilitado a través de comandos de configuración de interfase. El router central es configurado para snapshot routing aplicando el comando de configuración de interfase **snapshot server** en la interfase ISDN. El comando **snapshot server** especifica la longitud del período activo y si el router está permitido marcar sites remotos para intercambiar actualizaciones de enrutamiento en ausencia de tráfico regular.

Los routers remotos son configurados para snapshot routing aplicando el comando **snapshot client** a cada interfase ISDN. El comando de configuración de interfase **snapshot client** especifica las siguientes variables:

- La longitud del período activo (que debe coincidir con la longitud especificada en el router central)
- La longitud de período de silencio.
- Si el router puede marcar al router central para intercambiar actualizaciones de enrutamiento en ausencia de tráfico regular.
- Si las conexiones que se establecen para intercambiar datos del usuario pueden ser usados para intercambiar actualizaciones de enrutamiento.

Cuando el protocolo de enrutamiento del backbone no es soportado por snapshot routing (por ejemplo, OSPF o EIGRP), las técnicas estándares de redistribución de enrutamiento pueden ser usadas para asegurar que las actualizaciones de enrutamiento sean propagados entre los protocolos de enrutamiento, según lo requerido. Se debe tener mucho cuidado para asegurar la redistribución de subredes si es necesario y para evitar loops de enrutamiento.

En la figura 4.6 se muestra un escenario para la configuración de snapshot routing en Apple Talk.

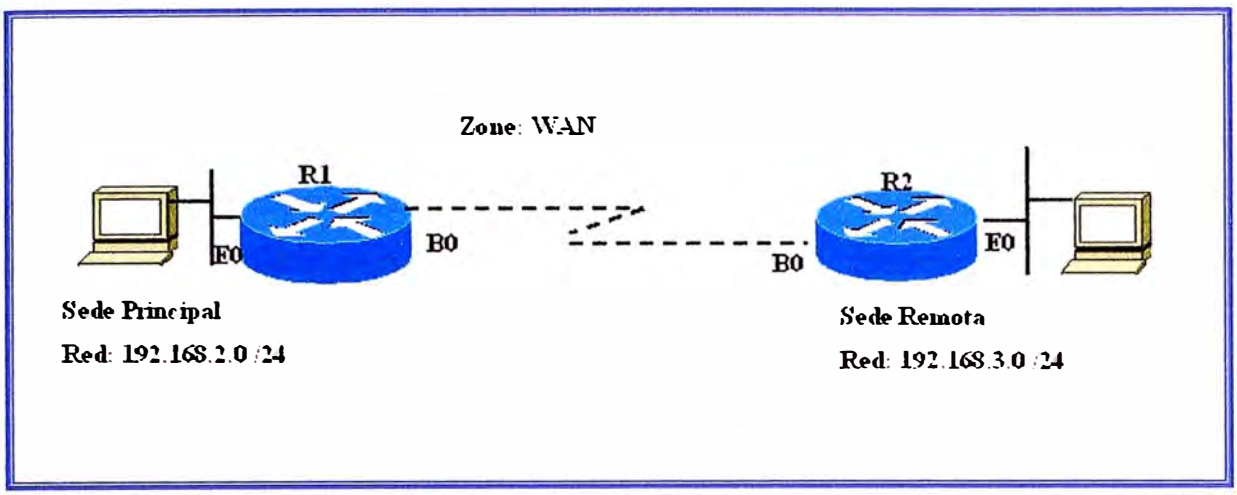


**Fig. N° 4.6 Enrutamiento Snapshot.**

### 4.4.5. Dial de Respaldo para Líneas Dedicadas.

Dial backup protege contra el tiempo de indisponibilidad de una wide-area network (WAN) permitiendo que una conexión dedicada sea respaldada por una conexión de circuito conmutado. Dial backup puede ser usada en varias maneras: cualquiera con rutas estáticas flotantes o con interfaces backup.

Dial backup desafía al diseñador con patrones de tráfico diferente que los sites DDR-soported Small Office – Home Office (SOHO). Cuando se diseñan puertos dial backup, considerar cuántos enlaces pueden fallar frecuentemente en un escenario de falla masiva, así como cuántos puertos serán requeridos en el site central en un escenario de casos extremos. El diseño típico implica seleccionar solo llamada entrante (dial-in) o llamada saliente (dial-out) para evitar la contención cuando ambos lados están intentando reestablecer conectividad.

**a) Interfaces de Respaldo.**

Una línea serial principal / dedicada es configurada para tener una interfase de respaldo ante una falla en el enlace o exceder los umbrales de carga. Si la línea de interfase o el protocolo de línea caen, la interfase de respaldo es usada para establecer la conexión con el router remoto.

Una vez configurado, la interfase dial de respaldo permanece inactiva hasta que se cumplan una de las condiciones siguientes:

1.- La línea de protocolo en el enlace principal cae. La línea de respaldo entonces se activa, reestableciendo la conexión entre los dos puntos.
2.- La carga del tráfico en la línea principal excede un límite definido. La carga de tráfico es monitoreada y cada 5 minutos se computa un promedio. Si el promedio excede el valor definido por el usuario para la línea, se activa la línea de respaldo. Dependiendo de cómo se configura la línea de respaldo, alguno o todo el flujo de trafico sobre ella.

Una interfase IOS de Cisco es colocada en modo backup aplicando el comando **backup interface**:

- El comando de configuración de interface **backup interface** especifica la interfase que actuara como respaldo.
- El comando **backup load** especifica el umbral de tráfico en el cual la interface backup debe ser activada y desactivada.
- El comando **backup delay** especifica la cantidad de tiempo que debe transcurrir antes de que la interfase backup se active o desactive después de una transición en la interfase principal.

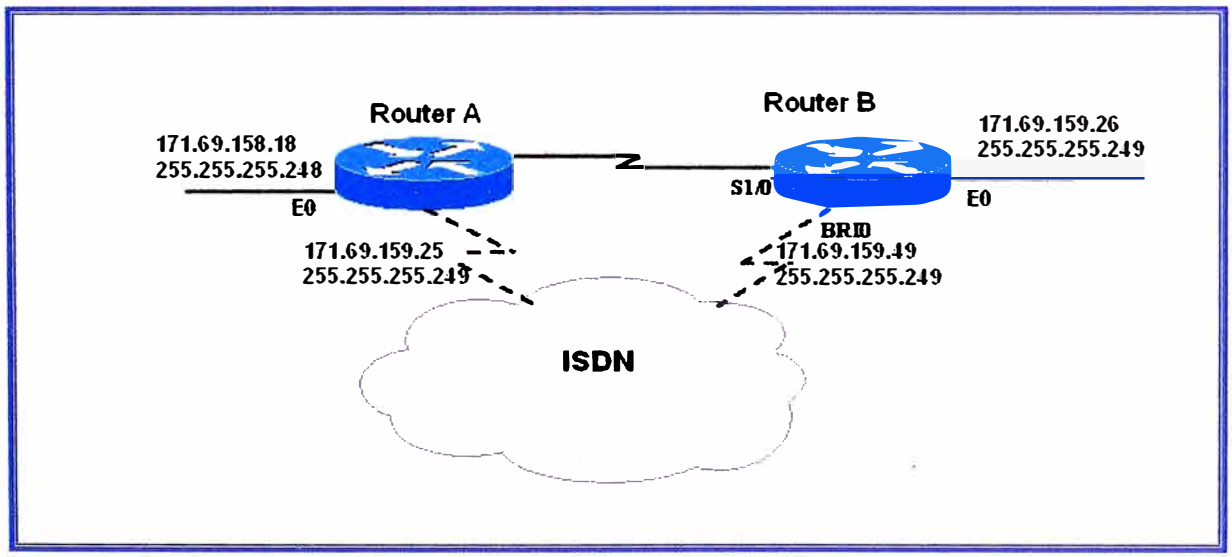


**Fig. Nº 4.7 Dial de respaldo sobre ISDN.**

Las interfaces de respaldo tradicionalmente mantienen la interfase backup en un estado BACKUP así está deshabilitado para otro uso. Los Dialer Profiles eliminan este bloqueo y permiten la interfase física ser usada para múltiples propósitos. El diseño Floating Static Route DDR también elimina este bloqueo en la interfase dialer. La figura 4.7 una línea

dedicada conecta al router A con el router B, la BRI 0 en el router B es usada como línea de respaldo

Usando la configuración que sigue, la BRI 0 solo se activa cuando la interfase serial 1/0 (la línea principal) cae. El comando **backup delay** configura la conexión backup para activar 30 segundos después que la interfase serial 0 cae y seguir activada por 60 segundos después que la interfase serial 1/0 se active:

```
interface serial 1/0
    ip address 172.20.1.4 255.255.255.0
    backup interface bri 0
    backup delay 30 60
```

Usando la configuración que sigue, la BRI 0 solo se activa la carga en la interfase serial 0 (la línea principal) excede el 75 % de su ancho de banda. La línea backup se desactiva cuando la carga agregada entre las líneas primarias y la línea backup está dentro del 5% del ancho de banda de la línea principal:

```
interface serial 1/0
    ip address 172.20.1.4 255.255.255.0
    backup interface bri 0
    backup load 75 5
```

Usando la siguiente configuración, la BRI 0 se activa solo cuando la interfase serial 1/0 cae o cuando el tráfico excede 25 %. Si la interfase serial 1/0 cae, pasaran 10 segundos antes de que la BRI 0 pase a ser activa. Cuando la interfase serial 1/0 levanta, la BRI 0 seguirá siendo activa por 60 segundos. Si la BRI 0 es activada por el umbral de carga en la interfase serial 1/0, la BRI 0 es desactivada cuando la carga agregada de la interfase serial 1/0 y BRI 0 vuelve al 5% del ancho de banda de la interfase serial 1/0:

```
interface serial 1/0
    ip address 172.20.1.4 255.255.255.0
    backup interface bri 0
    backup load 25 5
    backup delay 10 60
```

**b) Rutas Estáticas Flotantes.**

La operación de la interfase de respaldo es determinada por el estado de la línea y el protocolo de línea en el enlace principal. Es posible que la conectividad end-to-end esté perdida, pero la línea protocolo permanece arriba. Por ejemplo, la línea de protocolo en un enlace Frame Relay es determinada por el estado de los mensajes ILMI entre los Frame Relay DCE (switch). La conectividad al Frame Relay DCE no garantiza la conectividad end-to-end.

Diseñar Dial de respaldo con rutas estáticas flotantes utiliza el mantenimiento de tablas de enrutamiento y protocolos de enrutamiento dinámico de Cisco.

## 4.5. Filtros Dialer.

Los Filtros Dialer son usados para clasificar todos los paquetes que atraviesan la conexión de DDR como *interesante* o *no interesante* usando Access Control List (ACLs). Solo los paquetes interesantes pueden activar y mantener las conexiones DDR. Es tarea del diseñador DDR determinar qué tipo de paquetes serán etiquetados como no interesante y desarrollar ACLs para evitar que estos paquetes no interesantes causen conexiones innecesarias DDR.

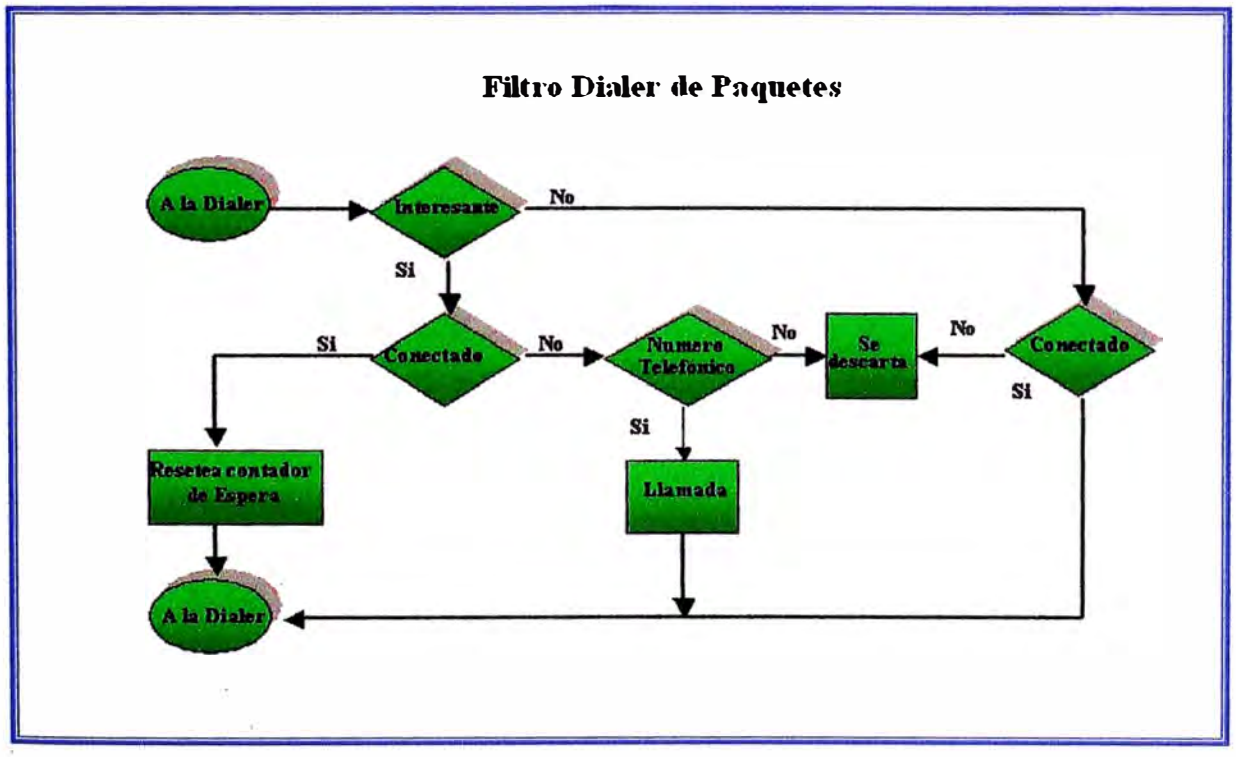


**Fig. N° 4.8 Filtro Dialer.**

Si un paquete es no interesante y no hay conexión establecida, el paquete es descartado. Si el paquete es no interesante, pero una conexión ya esta establecida al destino especificado, el paquete se envía a través de la conexión, pero el contador de tiempo idle (espera) no se resetea. Si el paquete es interesante, y no hay conexión en la interfase disponible, el router procura establecer una conexión. Este proceso se describe en la figura 4.8.

Cada paquete que llega a una interfase dialer se filtra y se determina si es interesante o no interesante basados en la configuración **dialer-group** y **dialer-list**. La siguiente configuración de Cisco en la interfase dialer 1 usa el dialer-group 5 para determinar los paquetes interesantes, según lo definido por el comando **dialer-list** 5. Dialer-group 5 es definido por comandos de la **dialer-list** 5 que en este caso determina todos los paquetes IP, IPX, y AppleTalk para ser interesantes.

**interface Dialer1**
**dialer-group 5**

**dialer-list 5 protocol ip permit**
**dialer-list 5 protocol ipx permit**
**dialer-list 5 protocol appletalk permit**

### 4.5.1. Definiendo Paquetes Interesantes usando Listas de Acceso.

La granularidad del dialer-filtering es proporcionada para cada protocolo por la definición de Cisco IOS Access Control Lists (ACLs). Por ejemplo, la siguiente configuración define el tráfico SNMP como no interesante usando la dialer-list 3 y las ACLs IP extendidas:

**dialer-list protocol ip 3 list 101**

**access-list 101 deny udp any any eq snmp**
**access-list 101 permit ip any any**

Los efectos de las actualizaciones de enrutamiento y de los servicios de directorio en una interfase Dialer pueden ser manejadas por varias técnicas: enrutamiento estático y default, passive-interfaces, o dialer maps non-broadcast. Para las soluciones que requieran

enrutamiento dinámico y no pueden usar SnapShot, el enrutamiento puede aun ser soportado en el enlace ISDN, y después definir no interesante por los filtros dialer.

Por ejemplo, si el diseño de la red requiere actualización de paquetes de enrutamiento EIGRP, los paquetes EIGRP pueden ser filtrados con listas del acceso para prevenir conexiones indeseadas DDR como sigue:

**access-list 101 deny eigrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255**

**access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255**

Se pueden usar las dos listas de acceso siguientes para clasificar tráfico EIGRP como no interesante:

**access-list 101 deny eigrp any any**

**access-list 101 deny ip any 224.0.0.10 0.0.0.0**

La primera lista del acceso deniega todo el tráfico EIGRP y la segunda lista de acceso deniega la dirección multicast (224.0.0.10) que EIGRP usa para sus actualizaciones. Cuando se usan listas de acceso para controlar trafico EIGRP, se necesitan configurar rutas estáticas para crear rutas a través del enlace ISDN. Cuando el enlace DDR está conectado, las actualizaciones de enrutamiento podrán fluir a través de la línea. En el diseño de DDR filtering, es importante entender donde las peticiones de actualización y servicios son útiles y donde estos tipos del paquete pueden ser filtrados con seguridad.

Es importante considerar de cerca los protocolos de servicio de directorio y las aplicaciones de red que necesitan ser soportados en cada punto. Numerosos protocolos y aplicaciones pueden establecer y mantener conexiones DDR, y pueden resultar en cargas WAN extraordinarias si no son monitoreadas y filtradas apropiadamente. No se debe esperar a recibir una sorpresa en la cuenta del teléfono para realizar el análisis cuidadoso del tráfico y de coste para su red. Si se esta avocado a la conexión WAN, implementar herramientas de monitoreo de red para proveer una rápida información sobre la duración y frecuencia de las conexiones.

**a) Simple Network Management Protocol SNMP.**

Aunque SNMP puede proporcionar información útil sobre conexiones ISDN y cómo esta siendo usada, usar SNMP puede resultar en excesivas actualizaciones para los enlaces ISDN. Por ejemplo, HP OpenView recopila la información regularmente por el pooleo (envío de paquetes ping a cada sede remota) a la red por eventos SNMP. Estos pools pueden causar que las conexiones ISDN se activen frecuentemente para comprobar que los routers remotos están allí, lo cual da como resultado un alto uso de la carga ISDN. Para controlar las cargas ISDN, el site central debe filtrar los paquetes SNMP destinados para los sites remotos sobre ISDN. Los paquetes entrantes SNMP de los sites remotos pueden aun ser permitidos, lo cual permite que los traps SNMP fluyan a la plataforma de administración SNMP. De esta manera, si un dispositivo SNMP falla en el site remoto, la alarma alcanzará la plataforma de administración SNMP en el site central.

Para controlar el tráfico SNMP, crear una lista del acceso que deniegue los paquetes SNMP. El siguiente es un ejemplo de filtro SNMP:

**access-list 101 deny tcp any any eq 161**
**access-list 101 deny udp any any eq snmp**
**access-list 101 permit ip any any**

**dialer-list 1 list 101**

## 4.6 Autenticación.

La autenticación en diseño de redes DDR proporciona dos funciones: seguridad y estado del dialer. Pues la mayoría de redes DDR se conectan a la Public Switched Telephone Network (PSTN), es imprescindible que un modelo de seguridad eficaz sea implementado para prevenir el acceso no autorizado a los recursos sensibles. La autenticación también permite que el código DDR no pierda de vista qué sitios están conectados actualmente y proporciona soporte para paquetes MultiLink PPP. Se tratan lo siguiente:

- Autenticación PPP
- Challenge Handshake Authentication Protocol (CHAP)

- Password Authentication Protocol (PAP)
- Seguridad ISDN
- DDR Callback (Llamada de retorno DDR)

### 4.6.1. Autenticación PPP.

La autentificación PPP vía CHAP o PAP se debe usar para proporcionar seguridad en conexiones DDR. La autenticación PPP ocurre después que Link Control Protocol (LCP) es negociado en la conexión DDR, pero antes que cualquier protocolo de red se permita fluir. Autenticación PPP es negociada como una opción de LCP, y es bidireccional, esto significa que cada site puede autenticar al otro. En algunos ambientes, puede ser necesario habilitar la autentificación PPP solo en el lado call-in (esto significa el lado que llama no autentica el lado llamado).

### 4.6.2 Challenge Handshake Authentication Protocol (CHAP).

Con CHAP, un dispositivo remoto que intenta conectarse al router local es presentado con un identificador CHAP que contiene el nombre del host y un identificador recibido. Cuando el router remoto recibe el identificador, mira el hostname recibido en el identificador y responde con el hostname y una respuesta CHAP derivada del identificador recibido y el password para ese hostname. Los passwords deben ser idénticos en el dispositivo remoto y el router local. Los nombres y passwords son configurados usando el comando **username**. En el siguiente ejemplo, el router nas3600A permitirá que el router c1600A llame usando el password "bubble":

Configuración en el router NAS3600A
**hostname nas3600A**
**username c1600A password bubble**

**interface dialer 1**
**ppp authentication chap callin**
Configuración en el router c1600A
**hostname c1600A**

**username nas3600A password bubble**

**interface dialer 1**

**encapsulation ppp**
**dialer in-band**
**dialer-group 5**
**dialer map ip 172.20.1.1 name nas3600A 18355558661**
**ppp authentication chap callin**

Los siguientes pasos ilustran el proceso CHAP:
**Paso 1** c1600A llama a nas3600A y LCP es negociado.
**Paso 2** nas3600A challenges c1600A con: <nas3600A/challenge_string>.
**Paso 3** c1600A ve el password para el username nas3600A y genera response_string.
**Paso 4** c1600A envia una respuesta a c3600A: <nas1600A/response_string>.
**Paso 5** c3600A ve el password para el username c1600A y genera el esperado response_string. Si el response_string recibido concuerda con la cadena respondida esperada, pasa la autenticación PPP, y el PPP puede negociar el control de protocolos de red (tales como IPCP). Si esto falla, el site remoto es desconectado.

### 4.6.3 Password Authentication Protocol (PAP).

Como CHAP, PAP es un protocolo de autenticación usado con PPP. Sin embargo, PAP es menos seguro que CHAP. CHAP pasa una versión encriptada del password en el enlace físico, pero PAP pasa el password en clear text (sin encriptacion), que hace susceptible al ataque sniffer (intruso en la red).

Al ser autenticado con PAP, el router mira el username que coincide con el dialer map usado para iniciar la llamada. Al ser autenticado con PAP en una llamada recibida, PAP mira el username asociado a su hostname (porque no se utilizó dialer map para iniciar la conexión).

En la siguiente configuración, el router nas3600A autenticará el peer con PAP cuando contesta la llamada DDR, y compara el resultado con la base de datos local:

**hostname nas3600A**
**aaa new-model**
**aaa authentication ppp default local**
**username c2500A password freedom**
**username nas3600A password texas**

**interface Dialer1**
**encapsualtion ppp**
**ppp authentication pap**

### 4.6.4 Seguridad ISDN.

ISDN DDR puede usar caller-ID para mejorar la seguridad configurando un caller ISDN en las interfaces entrantes ISDN. Las llamadas entrantes son verificadas para comprobar que el ID de la línea llamante es de un origen previsto. Sin embargo, la investigación caller-ID requiere una conexión end-to-end ISDN que pueda entregar el caller-ID al router.

### 4.6.5 Retorno de Llamada DDR.

Los ambientes DDR pueden ser configurados para operaciones DDR callback (llamada de retorno). Cuando un site remoto marca un site central (o el opuesto), el site central puede ser configurado para desconectar e iniciar una conexión DDR de salida al sitio remoto.
DDR callback proporciona mejora en la seguridad, asegurándose que el sitio remoto puede conectar solo desde una localización según lo definido por el numero callback. DDR callback puede también mejorar la administración centralizando la facturación para las conexiones remotas DDR.

# CAPÍTULO V
# INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

## 5.1. Introducción.

Entre las diferentes tecnologías WAN se encuentra comprendida ISDN (Red Digital de Servicios Integrados), la cual es una alternativa a las líneas dedicadas, que pueden ser usadas para trabajos a distancia y conectar mediante networking oficinas a distancia. Es la mas usada para conexiones de contingencia, y la que usaremos en este informe.

Cuando realiza una llamada de datos con ISDN, el enlace de datos se activa durante la duración de la llamada y se desactiva cuando la llamada finaliza, similar a una llamada telefónica convencional. Esta característica la hace apropiada para un enlace de contingencia, ya que se activará sólo cuando se requiera y permanecerá inactiva cuando no sea requerida, por lo tanto el consumo de la línea se contabilizara solo cuando se realice una llamada, lo que hace la diferencia con una línea dedicada

## 5.2 Descripción de ISDN.

*Integrated Services Digital Network (ISDN)* es el conjunto de estándares que definen una red digital de extremo a extremo.
ISDN es la integración de telefonía digital y servicio de transporte de datos ofrecidos por las compañías telefónicas.

### 5.2.1. Ventajas de ISDN.

Entre las ventajas de ISDN tenemos:

1. Puede transportar una variedad de señales de trafico de usuario. Permite la transmisión de voz, datos, texto, gráficos, música, video y otras fuentes sobre el cable de telefonía existente. Las aplicaciones ISDN incluyen aplicaciones de

imagen de alta velocidad, adicionar las líneas telefónicas domesticas al servicio de la industria de telecomunicación.

2. Las llamadas ISDN son más rápidas que una conexión a través de un MODEM debido al uso de señalización out-of-band (canal D), es así que algunas llamadas ISDN se pueden establecer en menos de 1 segundo.
3. Tiene una velocidad de transferencia mayor que un MODEM, ya que puede usar múltiples canales B de 64 kbps, en el caso de una línea ISDN PRI se pueden usar 30 canales B y un canal D lo cual significa 2.048 Mbps.

### 5.2.2 Desventajas de ISDN.

Sin embargo también se debe tener en cuenta los siguientes puntos:

1. Seguridad, dado que una conexión ISDN pasa a través de una red de telefonía publica conmutada, es vulnerable a una conexión no deseada. Se deben implementar los procesos necesarios para la protección de la red.
2. Costos, se debe hacer un estudio previo del trafico que se va a cursara a través de una línea ISDN, ya que de acuerdo a esto se puede definir la conveniencia o no de usar una línea ISDN o una línea dedicada.

## 5.3 Dispositivos ISDN.

Los dispositivos ISDN incluyen terminales, Terminal Adapters (TAs), dispositivos terminales de red, equipos terminales de línea, y equipos terminales de intercambio.

### 5.3.1 Equipos Terminales.

Los equipos terminales (o terminal adapters TA) ISDN son de 2 tipos.

1. Terminales ISDN especializados son referidos como un Terminal Equipment tipo 1 (TE1). Los TE1 se conectan a la red ISDN a través de un enlace digital de par trenzado de cuatro hilos
2. Terminales no-ISDN, tales como DTE, mas antiguo que los estándares ISDN, se denominan Terminal Equipment tipo 2 (TE2). Los TE2 se conectan a la red RDSI a través de un TA.

El TA ISDN puede ser un dispositivo autónomo o una placa dentro del TE2. Si el TE2 se implementa como un dispositivo autónomo, se conecta al TA a través de una interfase estándar de la capa física. Algunos ejemplos son EIA/TIA-232-C (RS-232-C), V.24, y V.35.

### 5.3.2 Equipos Terminales de Red.

Más allá de los dispositivos TE1 y TE2, el siguiente punto de conexión en la red ISDN es el dispositivo Network Termination:

1. Network Termination tipo 1 (NT1)
2. Network Termination tipo 2 (NT2).

Estos son dispositivos de terminación de red que conectan el cableado de cuatro hilos del abonado con el loop local de dos hilos convencional. En Estados Unidos, NT1 es un dispositivo del equipo terminal del abonado (CPE). En la mayoría de los países del mundo, además de Estados Unidos, NT1 forma parte de la red suministrada por la portadora. NT2 es un dispositivo más complicado que normalmente se encuentra en las centrales telefónicas privadas (PBX) digitales, que ejecutan servicios de protocolo de Capa 2 y Capa 3. También hay un dispositivo NT1/2, que es un dispositivo único que combina las funciones de NT1 y NT2.

## 5.4 Puntos de Referencia ISDN.

ISDN especifica un numero de puntos de referencia que define las interfaces lógicas entre los grupos funcionales, tales como TAs y NT1s. Los puntos de referencia ISDN son:

1. R – Que es el punto de referencia entre un equipo no-ISDN y un TA.
2. S – Que es el punto de referencia entre el terminal (TA) del usuario y el NT2.
3. T – Que es el punto de referencia entre los dispositivos NT1 y NT2.
4. U – Que es el punto de referencia entre el dispositivo NT1 y el equipo terminal de línea en la red del proveedor. Este punto es relevante solo en Norteamérica, donde las funciones de NT1 no son provistas por la red del proveedor.

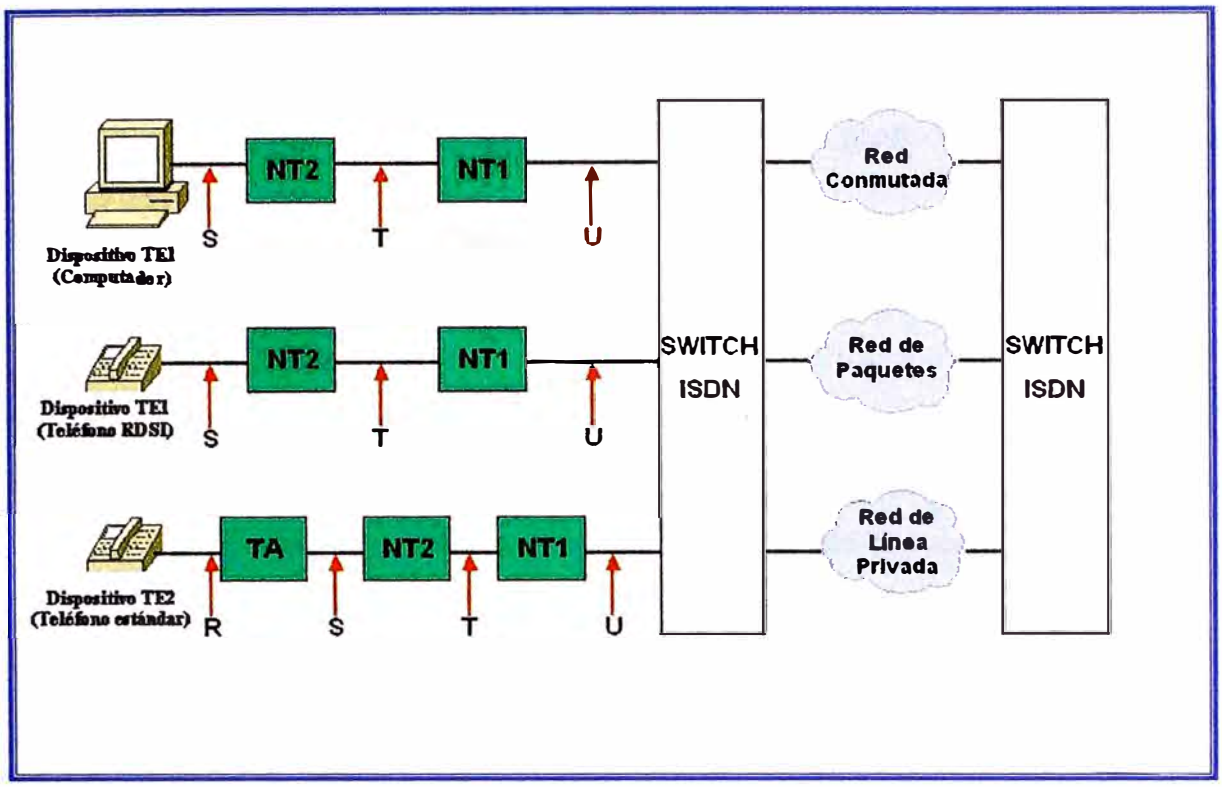


**Fig. N° 5.1 Distribución de dispositivos y puntos de referencia ISDN.**

La figura 5.1 nos muestra una configuración ISDN y nos muestra 3 dispositivos conectados a un switch ISDN en la oficina central. Dos de esos dispositivos son compatibles con ISDN, por lo cual ellos pueden ser conectados a través de un punto de referencia S al dispositivo NT2. El tercer dispositivo (teléfono no-ISDN) se conecta a través del punto de referencia R a un TA. Cualquiera de estos dispositivos también podría ser conectado a un dispositivo NT1/2, el cual puede reemplazar ambos el NT1 y el NT2.

## 5.5. Servicios ISDN.

Hay 2 tipos de servicios asociados con ISDN:

- BRI
- PRI

### 5.5.1. Servicio ISDN BRI.

El servicio ISDN Basic Rate Interface (BRI) ofrece 2 canales B y un canal D (2B+D). El canal de servicio B de una BRI opera a 64 kbps para el envío de data; el canal de servicio

D opera a 16 kbps y es usado para transportar información del canal de control y señalización, en algunos casos puede transmitir la información de datos del usuario a través de este canal. El protocolo del canal de señalización D se produce en las capas 1, 2 y 3 del modelo de referencia OSI.

### 5.5.2 Servicio ISDN PRI.

El servicio ISDN Primary Rate Interface (PRI) ofrece 23 canales B y un canal D en Norteamérica y Japón, sumando un total de 1.544 Mbps (el canal D Pri corre a 64 kbps). ISDN PRI en Europa, Australia y otras partes del mundo proveen 30 canales B mas un canal D de 64 kbps, lo cual resulta en 2.048 Mbps.

## 5.6. Especificaciones ISDN.

A continuación se describen las especificaciones isdn para las capas1, 2 y 3.

### 5.6.1 Capa 1 ISDN.

Los frames de la capa física ISDN (Capa 1) difieren dependiendo de hacia donde es enviado el frame (desde el terminal a la red) o de donde es recibido (de la red al terminal). Ambas interfaces físicas son mostradas en la figura 5.2.

Múltiples dispositivos de usuario ISDN pueden estar conectados físicamente a un circuito. En esta configuración, pueden haber colisiones si 2 terminales transmiten simultáneamente. Por lo tanto, ISDN provee características para determinar la contención del enlace. Cuando un NT recibe un bit D de un TE este responde en la siguiente posición del bit E. El TE espera el siguiente bit E igual a su ultimo bit D transmitido.

Los terminales no pueden transmitir en el canal D a menos que ellos detecten primero un numero determinado de 1s (indicando "no señal") correspondiendo a una prioridad pre-establecida. Si el TE detecta un bit E en un canal diferente de su bit D, esto debe detener la transmisión inmediatamente. Esta técnica simple asegura que solo un terminal pueda transmitir su mensaje D a la vez. Luego que la transmisión del mensaje D es satisfactoria,

el terminal tiene su prioridad reducida a detectar mas 1s continuos antes de transmitir. Los terminales no pueden aumentar su prioridad hasta que todos los demás dispositivos en la misma línea hayan tenido una oportunidad de enviar un mensaje D. Las conexiones telefónicas tienen mayor prioridad que los demás servicios, y la información de señalización tiene una mayor prioridad que la información que no es señalización.

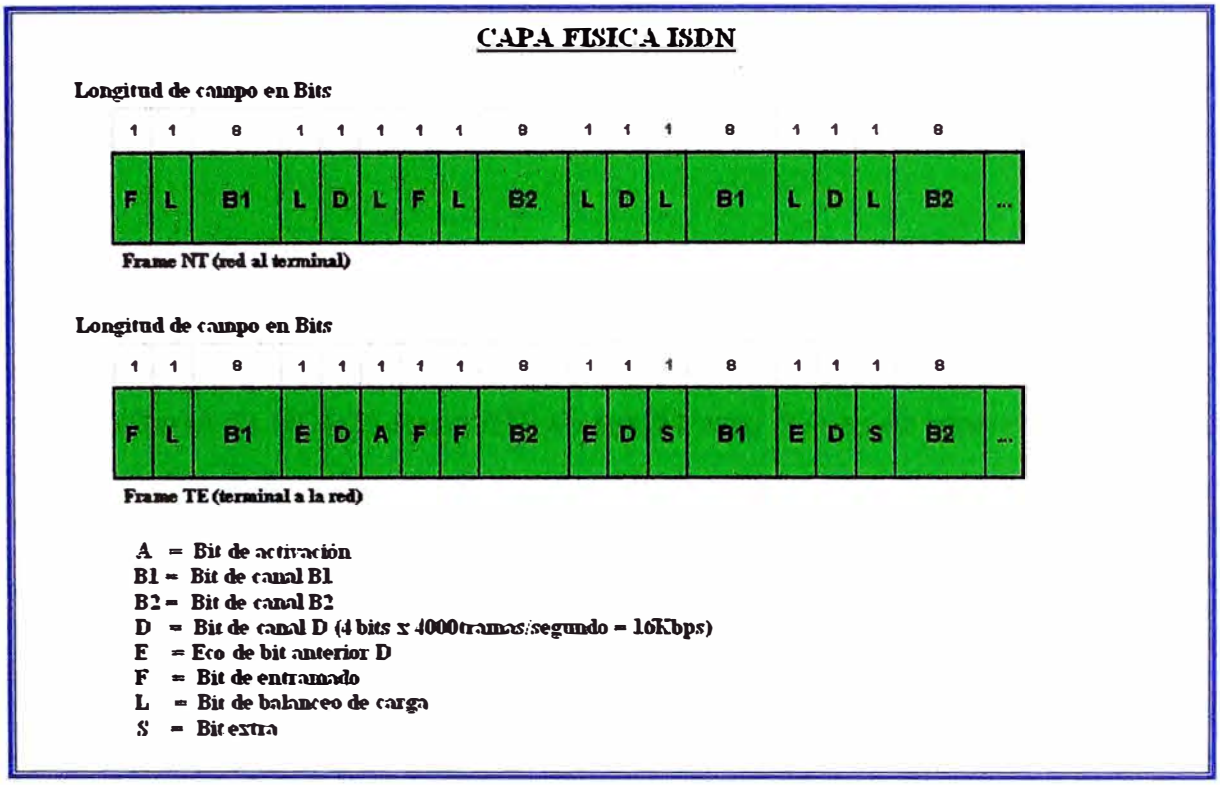


**Fig. Nº 5.2 Formato de frame de la capa 1 ISDN, dependiendo del sentido.**

Los frames son de 48 bits de longitud, de los cuales 36 son de datos. Los bits de un frame de la capa física ISDN son usados como sigue:

F – Provee sincronización.

L – Ajusta el valor promedio del bit.

E – Asegura la resolución de la contención cuando varios terminales de un bus pasivo se disputan un canal.

A – Activa los dispositivos.

S – No asignado

B1, B2 y D – Manejan los datos del usuario.

La especificación de la capa física de la interfase de acceso básico (BRI) RDSI se define en UIT-T I.430. La especificación de la capa física de la interfase de acceso principal (PRI) RDSI se define en UIT-T I.431.

### 5.6.2. Capa 2 ISDN.

La capa 2 del protocolo de señalización ISDN es un Link Access Procedure, D Channel (LAPD). LAPD es similar a High-Level Data Link Control (HDLC) y link Access Procedure, Balanced (LAPB).

Como lo indica LAPD (Procedimiento de Acceso al Enlace por canal D) esta capa es usada a través del canal D para asegurar que la información de señalización y control fluyan y sean recibidas apropiadamente. El formato del frame LAPD (Ver figura 5.3) es muy similar al de HDLC; como HDLC, LAPD usan frames de supervisión, información y no numerados.

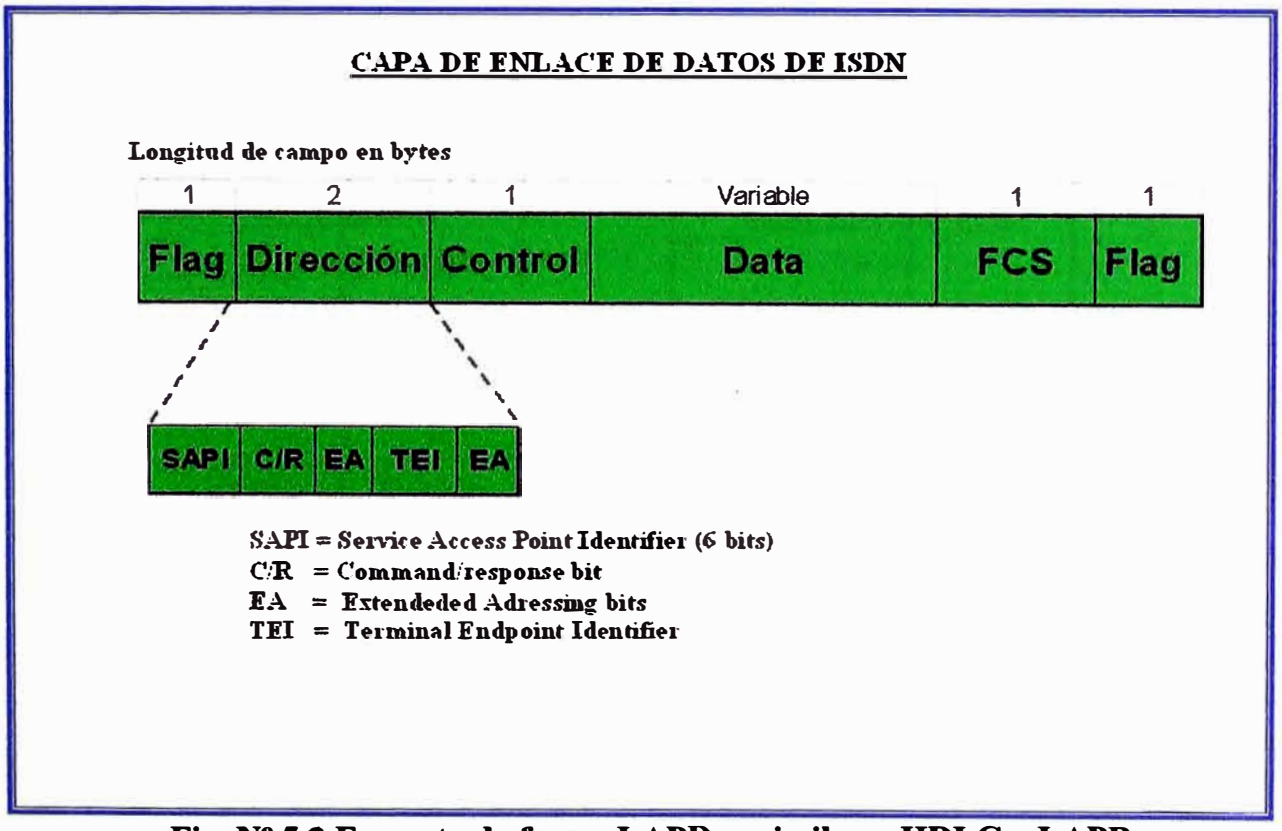


**Fig. Nº 5.3 Formato de frame LAPD es similar a HDLC y LAPB**

Los campos de Control y Flag de LAPD son idénticos a los HDLC, El campo de dirección de LAPD puede tener entre 1 o 2 bytes de longitud. Si el bit de dirección extendida del primer byte es configurado, las direcciones de 1 byte; si no esta configurada, la dirección es de 2 bytes. El primer byte del campo de dirección contiene el Service Access Point Identifier (SAPI), el cual identifica el portal al cual el servicio LAPD esta proporcionando la capa 3. El bit C/R indica donde el frame contiene un comando o una respuesta. El campo Terminal Endpoint Identifier (TEI) identifica si es un terminal simple o múltiples terminales. Un TEI de solo 1s indica un broadcast.

La especificación de la capa de enlace de datos RDSI se basa en LAPD y se especifica formalmente en UIT-T Q.920, UIT-T Q.921, UIT-T Q.922 y UIT-T Q.923.

### 5.6.3. Capa 3 ISDN.

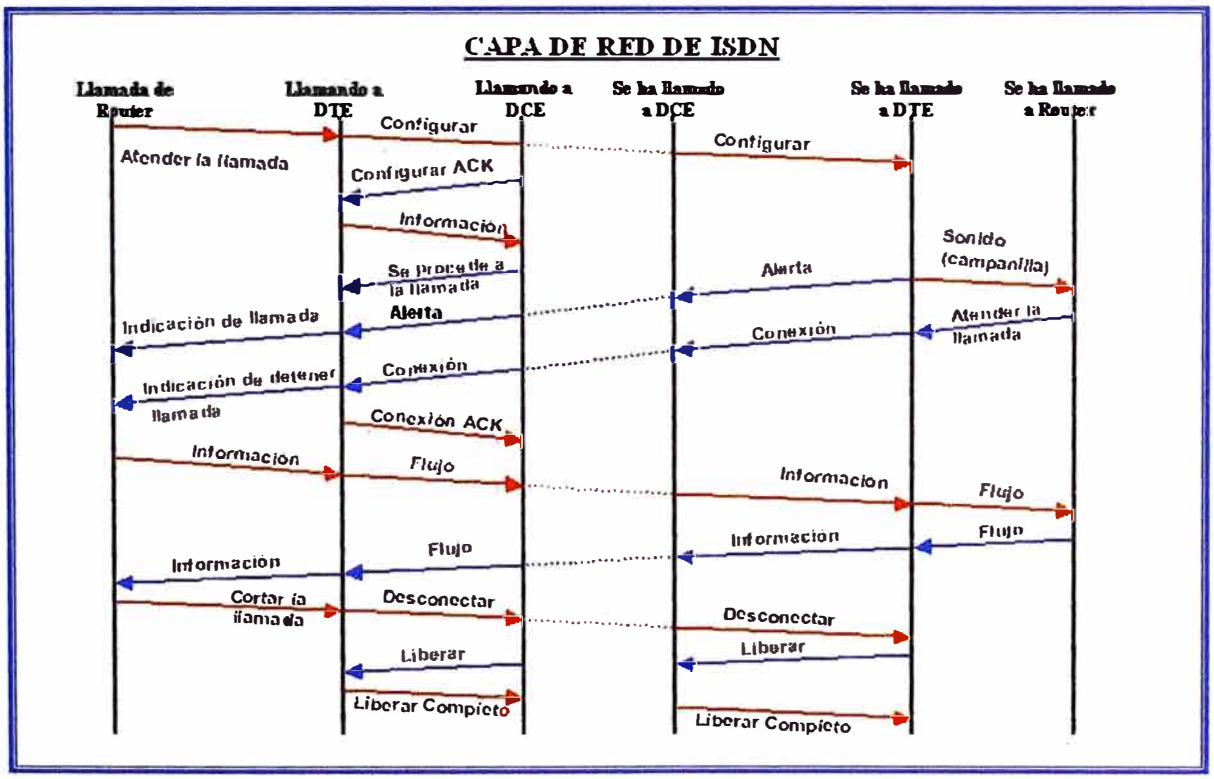


**Fig. N° 5.4 Proceso de una llamada ISDN a través de una red de circuito conmutada.**

Para ISDN son usadas 2 especificaciones de Capa 3: ITU-T (CCITT) I.450 (también conocido como ITU-T Q.930) y ITU-T I.451 (también conocido como ITU-T Q.931). Juntos ambos protocolos soportan user-to-user, circuitos conmutados, y conexiones de paquetes conmutados. Una variedad de establecimiento de llamadas, terminación de

llamadas, información y variedad de mensajes son especificados, incluyendo SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS y Disconnect. Estos mensajes son similares funcionalmente a los que provee el protocolo X.25. La figura 5.4, de ITU-T I.451 nos muestra el proceso típico de una llamada ISDN de circuito conmutado.

# CAPÍTULO VI
# DISEÑO DE REDES CON REDUNDANCIA ISDN

## 6.1. Modelos de conexiones de Redundancia.

De acuerdo a los requerimientos de cada empresa y el tipo de tráfico que cursan estas, se puede escoger entre algunos tipos de distribución para conmutar el tráfico de datos por una línea de respaldo en caso la línea principal presente alguna falla. A continuación se describen algunos de los modelos más comunes de distribución de línea de respaldo.

### 6.1.1. Un router, con línea principal y línea de respaldo ISDN.

Esta solución es la más económica, ya que se tiene un solo router. Este modelo es mas apropiado para una sede remota (agencia, oficina, cajero.)

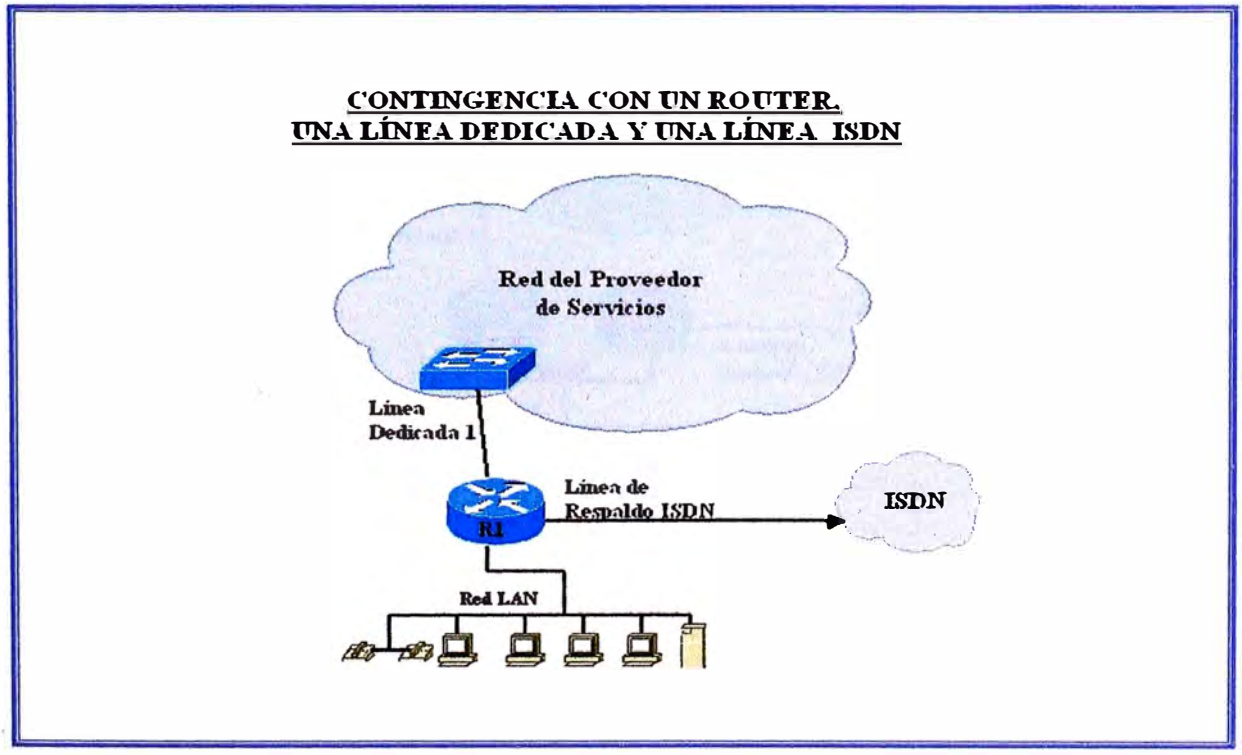


**Fig. Nº 6.1 Contingencia con un router y una línea dedicada**

**Ventaja:** Es más económico que otro tipo de configuración. Si se corta la interconexión de última milla entre la red del proveedor y esta sede o se presenta un problema en la red del proveedor de servicios, la conmutación seria inmediata por la línea de respaldo ISDN.

**Desventaja:** Si el router se avería no habría opción a recuperar el servicio a menos que se reemplace este equipo, lo cual por supuesto tomaría demasiado tiempo. La conexión se vuelve muy vulnerable. El modelo se describe en la figura 6.1.

### 6.1.2. Dos routers, uno con línea principal y el otro con línea de respaldo.

Esta solución es más cara pero brinda mayor seguridad de mantener la comunicación, ya que en caso de corte de enlace principal (ya sea por avería de última milla o el router principal de la sede), la conmutación del tráfico se realiza automáticamente a través de la línea ISDN. En este modelo se requiere usar la configuración HSRP.

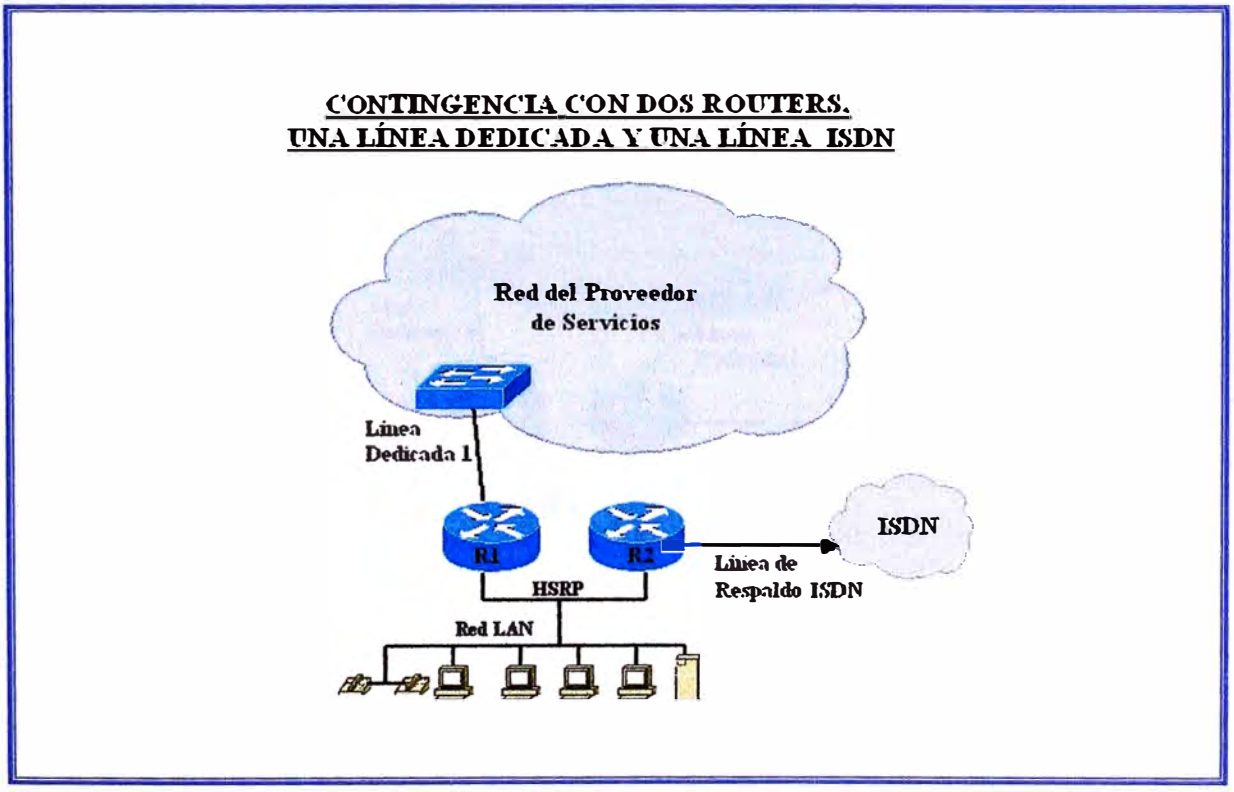


**Fig. Nº 6.2 Contingencia con 2 routers y una línea dedicada**

**Ventaja:** Mayor disponibilidad de conexión en caso se presente algún problema en el enlace de ultima milla o red del proveedor.

**Desventaja:** El costo se incrementa con la introducción de otro router, debido a esto es recomendable usarlo solo en sedes principales, y en sedes que requieran mayor tiempo de conexión disponible. El modelo se grafica en la figura 6.2

### 6.1.3. Dos routers, cada uno con una línea dedicada.

Ambos routers se deben conectar a diferentes puntos de la red del proveedor, ya que de presentarse una avería en alguno de los puntos del proveedor, el otro estará disponible. Como adicional se puede tener una línea de respaldo ISDN. Este modelo es mas recomendado para una sede principal de una institución debido a los cotos y al tiempo de disponibilidad que debe tener.

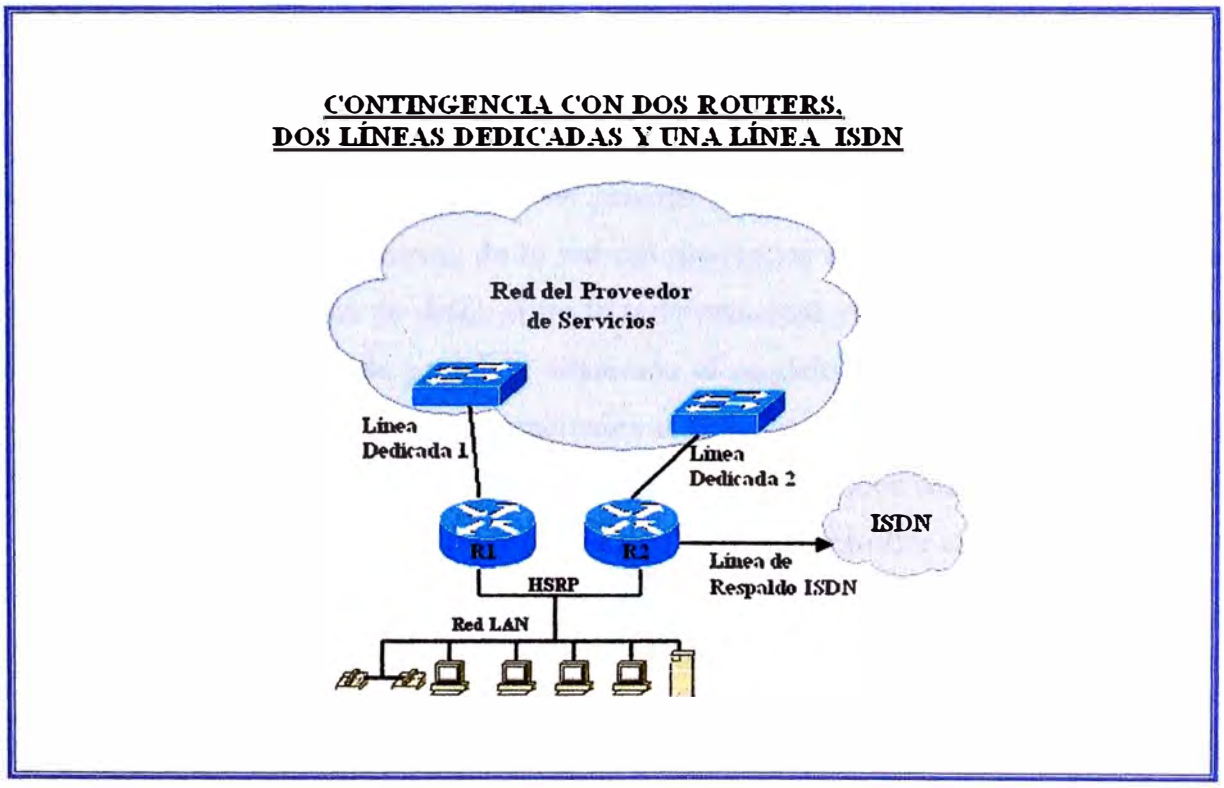


**Fig. Nº 6.3 Contingencia con 2 routers y 2 líneas dedicadas.**

**Ventaja:** La disponibilidad de la interconexión se incrementara mucho mas con referencia a los 2 modelos anteriores. En caso se pierda la conexión a través del primer enlace, la calidad de la comunicación a través de la línea de respaldo (a través del mismo proveedor) no se verá degradada ya que se tiene el mismo medio que la línea principal. Solo en el caso

extremo que ambas líneas a través del proveedor se vean afectadas se verá degradada la comunicación a través de la línea ISDN.

**Desventaja**: Obviamente esta conexión será mucho mas cara que los 2 modelos anteriores, ya que implica tener 2 líneas dedicadas a través del proveedor.
Este modelo se describe en la figura 6.3.

## 6.2. Diseño de una Red Bancaria con redundancia ISDN.

De acuerdo a lo visto en el párrafo 6.1, podemos elegir entre los 3 modelos mostrados para construir una red con líneas de respaldo para una institución.

### 6.2.1. Redundancia de la sede Principal.

Podemos definir la redundancia para la sede principal como la prevención ante un evento que afecte equipos o enlaces con la sede principal, los cuales por supuesto no afectaran solo a una sede remota, sino a todas en general. Existirán primero planes de redundancia para que el tráfico pase a través de la red del proveedor de servicios para no disminuir la calidad de la transmisión de datos entre la sede principal y la remota. Para nuestro diseño de contingencia de la sede principal usaremos el modelo de la figura 6.3 que es la más recomendable para estos puntos principales o sedes con gran importancia. Para nuestro diseño usaremos una variación del modelo mencionado, ambos routers en la sede principal contaran con conexión ISDN a través de una tarjeta E1 Controller cada una.

Para prever estos eventos, se ha diseñado el siguiente plan de contingencia:

a) **Falla del Router Principal (R1).**

En este caso con la ayuda de los protocolos de enrutamiento se procederá automáticamente a la migración del trafico desde las sedes remotas a través del router secundario de la sede principal, es decir ante una falla del equipo Router Principal (R1) el trafico a través de la del proveedor de servicios pasara por el Router Secundario (R2), todo esto a través del mismo medio que el enlace principal, es decir en la red del proveedor de servicios.

**b) Falla en alguna de las líneas en la red del proveedor.**

En el caso que se afecte alguna línea que interconecta a una sede remota con el Router Principal (R1), también se estaría migrando el trafico de la sede afectada a través de la red del proveedor hacia el router Secundario (R2)

En ambos casos la conmutación debe ser automática, la red no puede esperar ninguna acción del administrador de la red para conmutar el tráfico por el enlace de redundancia.

**c) Falla en toda la red del Proveedor.**

Por último si se ve afectada la red del proveedor de servicios, las sedes remotas se conectarán a la sede principal a través de las líneas de respaldo ISDN, primero al router R1 y en segunda instancia con el router R2.

### 6.2.2. Redundancia de las Sedes Remotas.

En nuestro diseño para las sedes remotas usaremos el modelo de la figura 6.1, un router que maneja la línea principal y el enlace de contingencia.

Para este tipo de diseño de contingencia, en caso de eventos con la sede remota se tendrán los siguientes pasos de contingencia.

**a) Corte de Fibra Ultima Milla.**

Sin duda alguna el caso mas frecuente de corte de enlace con una sede remota es el corte del enlace de última milla (fibra, cobre, etc.), en tal situación la línea de respaldo en la sede remota entraría a funcionar, para nuestro caso la línea ISDN, ésta se activa y se comunica primero con el Router Principal (R1), en segunda instancia con el Router Secundario (R2) a través de la línea telefónica.

**b) Problemas en la red del Proveedor.**

Si el problema no se debe a problemas en la última milla entonces el proceso de migración del trafico de la sede remota se hace de la siguiente manera: Primero se migra el trafico a través de la red del proveedor hacia el Router Secundario, por ultimo si falla la comunicación con este último a través del enlace de la red del proveedor

principal, volveríamos al escenario visto en el caso 1 (similar a un corte de fibra en la ultima milla).

Se puede dar el caso también que alguna sede de mayor importancia para la empresa tenga 2 routers en la sede remota, de manera que el segundo router maneje la conexión de respaldo.

Luego de haber escogido los modelos respectivos para cada sede, el diseño de nuestra red quedaría de la siguiente manera como se muestra en la figura 6.4.

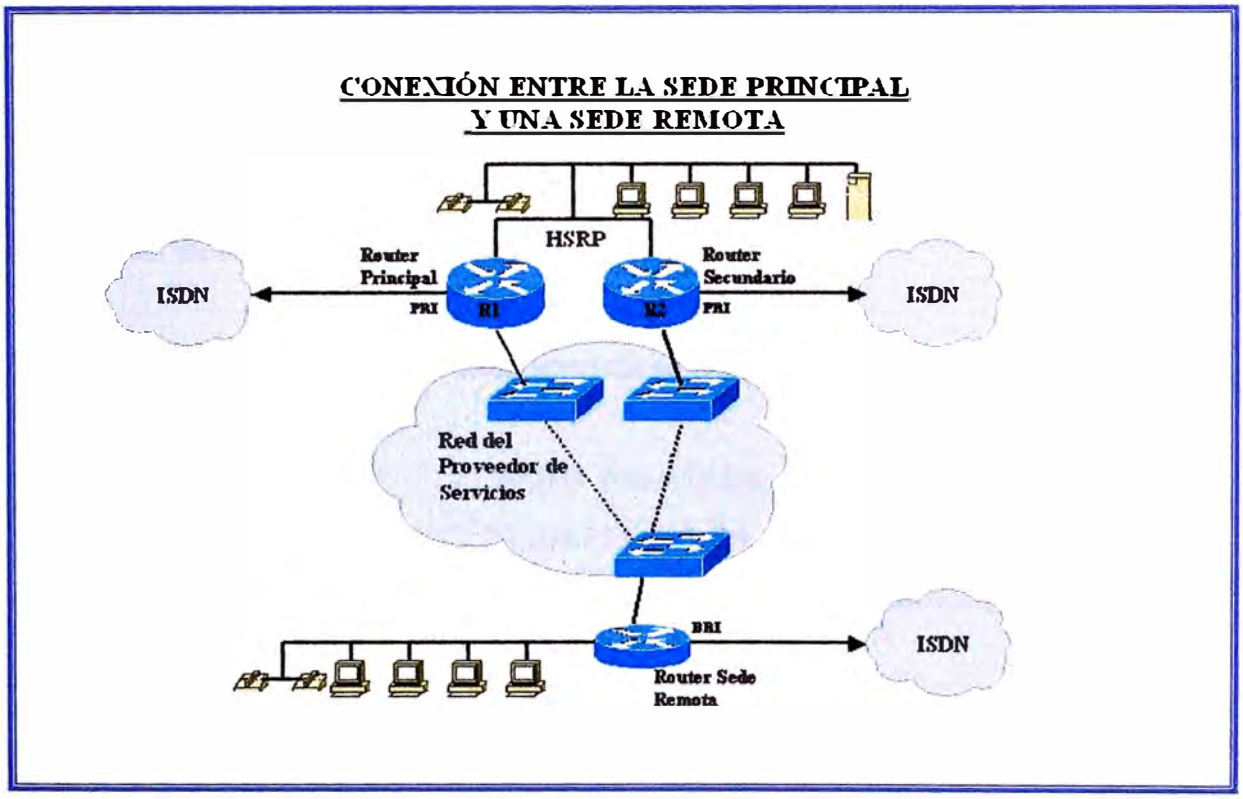


**Fig. N° 6.4 La figura muestra la conexión entre la sede principal y una sede remota.**

## 6.3. Diseño y distribución de las redes WAN, LAN y respaldo.

Para implementar una red de datos se requiere primero realizar un plan de numeración de IPs, tanto para la sede principal como para cada sede remota. Debido a esto se diseña un plan de numeración de tal manera que no se repita ninguna red en ninguna de las sedes, ya que esto implicaría un conflicto en la red pudiendo culminar en un mal funcionamiento de la red, e incluso llegar a ocasionar la caída de la red.

Este plan de numeración debe estar diseñado de tal manera que pueda predecir redes futuras o servicios que se implementaran luego, incluso de aquellos que hasta el momento no se tiene proyectado, dejando IPs disponibles.

Este requerimiento se debe a que si en algún momento se requiere introducir una nueva red o un nuevo servicio, no debe ser necesario variar las redes ya instaladas, puesto que esto implicaría una reestructuración de toda la red, tanto en la sede principal como sedes remotas. Este tipo de reestructuraciones debe ser evitado, ya que al realizarlas se verán afectados los servicios de los usuarios e implicaría un costo adicional a la empresa.

En la Sede Central se tendrán concentrados los servidores de base de datos de clientes, servidores de video, servidores de correo, servidores para cajeros, los cuales lo distribuiremos en diferentes redes LAN para poder distinguirlas:

### 6.3.1. Plan de Numeración para las Redes Lan.

La distribución de las IPs para cada servicio se realizará tomando en cuentas las siguientes redes IP reservadas.
RED LAN Sede Principal: 172.20.0.0 255.255.0.0
RED LAN Sedes Remotas: 172.21.0.0 255.255.0.0
Esta ultima la dividiremos en subredes de mascara /24 para cada sede.

**TABLA Nº 6.1 Plan de numeración redes LAN**

| # Sede | Dirección de Red | Mascara | Dirección de Broadcast | Dirección IP en el router |
|---|---|---|---|---|
| Principal | 172.20.0.0 | 255.255.0.0 | 172.20.0.255 | 172.20.0.1 |
| 1 | 172.21.1.0 | 255.255.255.0 | 172.21.1.255 | 172.21.1.1 |
| 2 | 172.21.2.0 | 255.255.255.0 | 172.21.2.255 | 172.21.2.1 |
| .... | .... | ..... | .... | .... |
| N | 172.21.N.0 | 255.255.255.0 | 172.21.N.255 | 172.21.N.1 |

La primera IP hábil a usarse será asignada a la interfase LAN del router en cada caso. La distribución de las redes LAN para cada sede incluyendo la sede principal se muestra en la Tabla Nº 6.1.

### 6.3.2 Plan de Numeración para las Redes Wan.

Para la interconexión de las sedes remotas con la sede principal se debe tener en cuenta que, cada sede se tiene que comunicar con el router principal (R1) y el router secundario (R2) en la sede principal, teniendo en cuenta esto se observa que se necesita por lo menos 3 direcciones IPs disponibles en cada una de estas redes.

Para las redes WAN usaremos una parte de la red de IPs reservadas 10.0.0.0.

En nuestro caso usaremos la red clase B 10.4.10.0 255.255.255.0 y la dividiremos en sub-redes de 8 IPs cada una, es decir IPs de mascara /29, pues con una mascara /30 tenemos 4 IPs en cada red pero solo 2 de ellas están disponibles descontando la dirección de red y la dirección Broadcast.

La distribución de las IPs para la red Wan se muestra en la Tabla Nº 6.2.

**TABLA Nº 6.2 Plan de numeración redes WAN.**

| Sede | Dirección de Red | Mascara | Dirección de Broadcast | IP Router R1 | IP Router remoto | IP Router R2 |
|---|---|---|---|---|---|---|
| 1 | 10.4.10.8 | 255.255.255.248 | 10.4.10.15 | 10.4.10.9 | 10.4.10.10 | 10.4.10.11 |
| 2 | 10.4.10.16 | 255.255.255.248 | 10.4.10.23 | 10.4.10.17 | 10.4.10.18 | 10.4.10.19 |
| 3 | 10.4.10.24 | 255.255.255.248 | 10.4.10.31 | 10.4.10.25 | 10.4.10.26 | 10.4.10.27 |
| ... | ... | ... | ... | ... | ... | ... |
| N | 10.4.10.8N | 255.255.255.248 | 10.4.10.(8N+7) | 10.4.10.(8N+1) | 10.4.10.(8N+2) | 10.4.10.(8N+3) |

Además se tendrá el siguiente criterio:

La primera IP disponible será adjuntada al router **R1** de la sede principal.

La segunda IP disponible será asignada al router **R2** de la sede principal.

La tercera IP disponible será asignada al router r de la sede remota N (**sedeN**).

### 6.3.3 Plan de Numeración para las Redes de Respaldo.

Para la comunicación de las sedes a través de la línea de respaldo también necesita usar un plan de distribución de IPs para evitar conflictos. Para esta red solo necesitamos 2 IPs útiles por sede, una para el router en la sede remota y otra en el router principal, por lo que será suficiente usar una red con mascara /30.

Usaremos la red clase B 10.4.21.0 255.255.255.0 para la conexión entre las sedes remotas y el router R1 en la sede principal, además de la red clase B 10.4.22.0 255.255.255.0 para la conexión entre las sedes remotas y el router R2 en la sede principal a través de las líneas ISDN. Estas redes serán divididas en subredes de mascar /30, es decir 4 IPs por red, de las cuales solo 2 están disponibles para ser usadas, ya que de las 2 IPs restantes una es la dirección de red y la otra es la dirección de broadcast.

**TABLA Nº 6.3 Plan de numeración líneas ISDN Router 1.**

| # Sede Remota | Dirección de Red | Mascara | Dirección de Broadcast | Dirección IP router R1 | Dirección IP router remoto |
|---|---|---|---|---|---|
| 1 | 10.4.21.4 | 255.255.255.252 | 10.4.21.7 | 10.4.21.5 | 10.4.21.6 |
| 2 | 10.4.21.8 | 255.255.255.252 | 10.4.21.11 | 10.4.21.9 | 10.4.21.10 |
| 3 | 10.4.21.12 | 255.255.255.252 | 10.4.21.15 | 10.4.21.13 | 10.4.21.14 |
| ... | ... | ... | ... | ... | ... |
| N | 10.4.21.(4N) | 255.255.255.252 | 10.4.21.(4N+3) | 10.4.21.(4N+1) | 10.4.21.(4N+2) |

La distribución de IPs para el enlace de respaldo ISDN entre el router R1 y las sedes remotas se muestra en la Tabla Nº 6.3.
La distribución de IPs para el enlace de respaldo ISDN entre el router R2 y las sedes remotas se muestra en la Tabla Nº 6.4.

**TABLA N° 6.4 Plan de numeración líneas ISDN Rrouter 2**

| # Sede Remota | Dirección de Red | Mascara | Dirección de Broadcast | Dirección IP router R2 | Dirección IP router remoto |
|---|---|---|---|---|---|
| 1 | 10.4.22.4 | 255.255.255.252 | 10.4.22.7 | 10.4.22.5 | 10.4.22.6 |
| 2 | 10.4.22.8 | 255.255.255.252 | 10.4.22.11 | 10.4.22.9 | 10.4.22.10 |
| 3 | 10.4.22.12 | 255.255.255.252 | 10.4.22.15 | 10.4.22.13 | 10.4.22.14 |
| ... | ... | ... | ... | ... | ... |
| N | 10.4.22.(4N) | 255.255.255.252 | 10.4.22.(4N+3) | 10.4.22.(4N+1) | 10.4.22.(4N+2) |

Como se menciono anteriormente se tendrán 2 routers de enlace en la sede principal:

Primero: Router1 (R1)

Segundo Router2 (R2)

En las sedes remotas se tendrá un router el cual contara con una interfase para la conexión principal y otra para el enlace de contingencia.

De acuerdo a los requerimientos de cada sede se puede instalara un segundo router en la sede remota, de manera que el segundo router manejara la línea de respaldo.

Los routers en la sede principal tendrán las mismas características de Software y Hardware. Los routers serán de la Serie 7200 de Cisco. Al manejar una sola interfase Controller en cada router de la sede principal estamos asumiendo que se dispondrá de como máximo 30 sedes, las cuales tomaran uno de cada uno de los canales de la línea PRI, se podrían agregar conexiones IDSN de acuerdo a la cantidad de sedes de la empresa o a las proyecciones de expansión de la misma. La pérdida de conexión con todas las sedes es un caso extremo, lo cual es muy poco probable (pero no imposible) ya que la interconexión de ultima milla entre el POP del proveedor de servicios y el cliente debe estar diseñada de tal manera que tenga el mínimo riesgo de sufrir una avería intencional o accidental. Además si ocurriese esto, aun se mantendría la comunicación a través de la red del proveedor del mismo proveedor de servicios al segundo router (R2) en la sede principal, ya que este

como se menciono anteriormente se conecta a otro POP del proveedor y debe llegar por otra ruta de la última milla.

## 6.4. Configuración de los routers de la sede principal y sedes remotas.

A continuación se mostrarán las configuraciones que se realizaran en los routers de la sede principal y de una sede remota.

Se está considerando que para levantar la línea de respaldo ISDN la llamada la realizara la sede remota, esto es porque generalmente son las sedes remotas las que se conectan a un servidor de la sede principal.

Se tomaran como números para la línea ISDN en la sede principal:
Router principal (R1): 555-4444
Router Secundario (R2) : 555-5555

### 6.4.1. Configuración de los equipos en la Sede Principal.

Para el diseño de este trabajo se implementará el enlace principal a través de una red ATM, para esto los routers principales necesitaran una tarjeta ATM en la cual se configurara cada enlace hacia las sedes remotas.
En ambos routers las tarjetas ATM estarán insertadas en el slot 6, y tendrán el siguiente esquema:

**a) Configuración del Router principal (R1).**
Configuracion del nombre del equipo, el cual servira luego para el proceso de autenticacion en las conexiones ISDN

```
hostname Router1
!
```

Asimismos se definiran los usuarios y passwords para que cada sede pueda autenticarse al router principal :

```
!
username sede1 password 7 (sede1)
username sede2 password 7 (sede2)

username sedeN password 7 (sedeN)
!
```

Habilitacion de la interfase ATM en el router, ubicada en el slot 6/0, esta interfase será la encargada de realizar la conexion principal con las sedes remotas a traves de la red del proveedor de servicios:

```
!
interface ATM6/0
description Enlace Principal Router1
no ip address
no atm scrambling sts-stream
 no atm ilmi-keepalive
.
```

Luego se habilita cada subinterfase hacia cada sede remota, se muestra una configuración genérica hacia una sede N:

```
interface ATM6/0.N point-to-point
description Enlace Sede Principal  > Sede N
 ip address 10.4.10.(8N+1) 255.255.255.248
 atm route-bridged ip
 ntp broadcast
 pvc SedeN 0/N
  vbr-nrt BWn  BWn
  encapsulation aal5snap
!
```

**BWn** : Ancho de banda asignado para la sede N.

La Interfase LAN será una FastEthernet insertada en el slot 0, dado que son 2 los routers en la sede principal, uno de ellos será el principal y el otro el de respaldo, solo uno de ellos está activo a la vez, por esto usaremos el protocolo HSRP descrito en el capitulo III.

```
!
interface FastEthernet0/0
description LAN Principal HSRP – Router1
ip address 172.20.0.1 255.255.255.0
no ip redirects
duplex full
standby 1 ip 172.20.0.3
standby 1 priority 110
!
```

En la configuración global se define el tipo de PRI de la red PSTN, para la red de Perú es:

```
!
isdn switch-type primary-net5
```

Se habilita la tarjeta Controller E1 en el slot 4/0, esta se fragmenta en 31 canales, por una de las cuales viajan los paquetes de señalización, quedando habilitados 30 canales para datos.

```
controller E1 4/0
 framing NO-CRC4                        % Tipo de framing
 pri-group timeslots 1-31               % Se definen los 31 canales
 description E1 Backup ISDN – 555-4444  % Descripción
```

Para poder configurar los parámetros para la línea ISDN se habilita la interfase lógica para la interfase Controller E1, dado que la tarjeta E1 controller esta ubicada en el slot 4/0 entonces la interfase serial tendrá como identificador serial4/0:15:

```
!
interface Serial4/0:15
 no ip address
 encapsulation ppp                    % Tipo de encapsulación PPP
 no ip route-cache cef
 no ip route-cache
 dialer pool-member 1                 % Hace referencia a miembros del pool 1
 isdn switch-type primary-net5        % Tipo de PRI en la red PSTN
 no fair-queue
 ppp authentication chap              % Tipo de Autenticación CHAP
 ppp multilink                        % Tipo de protocolo multilink PPP
!
```

Configuración de las interfaces Dialer con cada sede, se muestra la configuración con la sede N:

```
!
interface DialerN                     % Numero de interfase dialer
 description Enlace Backup SedeN
 ip address 10.4.20.(4N+1)255.255.255.252
 encapsulation ppp                    % Tipo de encapsulación PPP
 ip route-cache flow
 no ip mroute-cache
 dialer pool 1                        % Hace referencia a miembros del pool 1
 dialer remote-name SedeN             % Nombre del router de la sede N (hostname)
 dialer-group 1                       % Pertenece al grupo dialer 1
 ppp authentication chap              % Tipo de Autenticación CHAP
 ppp multilink                        % Tipo de protocolo multilink PPP
!
```

Se definen las listas de acceso que se usaran para las líneas ISDN:

```
!
access-list 1 permit 0.0.0.0                    % Permite todo
access-list 11 permit 172.21.1.0  0.0.0.255     % Red LAN sede 1
access-list 11 permit 10.4.10.8  0.0.0.7        % Red WAN sede 1
```

**access-list 11 permit 10.4.21.4 0.0.0.3** % Red ISDN sede 1
**access-list 12 permit 172.21.1.0 0.0.0.255**
**access-list 12 permit 10.4.10.16 0.0.0.7**
**access-list 12 permit 10.4.21.8 0.0.0.3**
**access-list 13 permit 172.21.1.0 0.0.0.255**
**access-list 13 permit 10.4.10.24 0.0.0.7**
**access-list 13 permit 10.4.21.12 0.0.0.3**
**.....**
**access-list 1N permit 172.21.N.0 0.0.0.255** % Red LAN sede N
**access-list 1N permit 10.4.10.8N 0.0.0.7** % Red WAN sede N
**access-list 1N permit 10.4.21.4N 0.0.0.3** % Red ISDN sede N

**access-list 101 deny eigrp any any** % Deniega trafico EIGRP
**access-list 101 permit ip any any** % Permite el resto
**dialer-list 1 protocol ip list 101** % Aplica la lista 101 a la dialer-list 1

También se configurará el protocolo de enrutamiento apropiado, en nuestro caso se ha escogido el protocolo EIGRP, el cual publicara la red de la red LAN de la sede principal en el Sistema Autónomo (AS) 120. Esta lista distribuirá la ruta default a través de las subinterfaces ATM y las interfaces dialer para cada sede remota, configurara en modo pasivo la interfase FastEthernet 0/0.

Deshabilitar el envío de paquetes EIGRP, ya que ante cualquier cambio en la red un broadcast de EIGRP podría activar las líneas ISDN.

**router eigrp 120**
**redistribute static**
**passive-interface FastEthernet0/0** % La interfase F0/0 no publica rutas.
**network 172.20.0.0** % Publica la red 172.20.0.0
**distribute-list 1 out ATM6/0.1**
**distribute-list 1 out ATM6/0.2**
**distribute-list 1 out ATM6/0.3**

.....

**distribute-list 1 out ATM6/0.N** % Publica las rutas a la sede N

**distribute-list 1 out Dialer1**

**distribute-list 11 in Dialer1**

**distribute-list 1 out Dialer2**

**distribute-list 12 in Dialer2**

**distribute-list 1 out Dialer3**

**distribute-list 13 in Dialer3**

**distribute-list 1 out DialerN** % Publica la lista 1 a través de la dialer N

**distribute-list 1N in DialerN** % Permite recibir las rutas de la lista 1N

.....

**no auto-summary** % Las listas no se sumnan

**no eigrp log-neighbor-changes** % No envía los logs de cambios EIGRP

**no eigrp log-neighbor-warnings** %No envia los warnings de cambios EIGRP

Se muestra la configuración de rutas estáticas con un peso de 250, este es mayor al peso que tiene el enrutamiento EIGRP.

***ip* classless**

%Publicación de la red WAN de cada sede por la ISDN

**ip route 10.4.10.8 255.255.255.248 10.4.21.6 250**

**ip route 10.4.10.16 255.255.255.248 10.4.21.10 250**

**ip route 10.4.10.24 255.255.255.248 10.4.21.14 250**

.....

**ip route 10.4.10.8N 255.255.255.248 10.4.21.(4N+2) 250**

%Publicación de la red LAN de cada sede por la ISDN

**ip route 172.21.1.0 255.255.255.248 10.4.21.6 250**

**ip route 172.21.2.0 255.255.255.248 10.4.21.10 250**

**ip route 172.21.3.0 255.255.255.248 10.4.21.14 250**

.....

**ip route 172.21.N.0 255.255.255.248 10.4.21.(4N+2) 250**

**!**

Se define el map-class dialer, el cual tendrá el nombre tesis-uni.

**map-class dialer tesis-uni**
**dialer idle-timeout 60** % Tiempo de espera 60 segundos
**dialer fast-idle 5**
**dialer wait-for-carrier-time 1**
**!**

**b) Configuración del Router Secundario (R2).**

Para el Router Secundario (R2) se sigue la misma secuencia que para el router R1, tomando en cuenta los cambios necesarios por las IPs asignadas según el plan de numeración
Nombre del router:

**hostname Router2**
**!**

Username y passwords de las sedes remotas:
**!**
**username sede1 password 7 (sede1)**
**username sede2 password 7 (sede2)**

**username sedeN password 7 (sedeN)**
**!**

Habilitacion de la interfase ATM

**!**
**interface ATM6/0**
**description Enlace Redundante Router2**

**no ip address**
**no atm scrambling sts-stream**
**no atm ilmi-keepalive**
**!**

Configuración del enlace con la sede remota N:

**!**
**interface ATM6/0.N point-to-point**
**description Enlace Sede Principal > Sede N**
**ip address 10.4.10.(8N+3) 255.255.255.248**
**atm route-bridged ip**
**ntp broadcast**
**pvc SedeN 0/N**
**vbr-nrt BWn BWn**
**encapsulation aal5snap**

La Interfase LAN será una FastEthernet insertada en el slot 0:

**!**
**interface FastEthernet0/0**
**description LAN HSRP**
**ip address 172.20.0.2 255.255.255.0**
**duplex full**
**standby use-bia**
**standby 1 ip 172.20.0.3**
**standby 1 preempt**
**!**

Tipo de línea PRI:

**!**
**isdn switch-type primary-net5**
**!**

Habilitación Controller E1:

```
!
controller E1 4/0
 framing NO-CRC4
 pri-group timeslots 1-31
 description E1 Backup ISDN – 555-5555          % Descripción
!
```

Interfase serial virtual:

```
!
interface Serial4/0:15
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 dialer pool-member 1
 isdn switch-type primary-net5
 no fair-queue
 ppp authentication chap
!
```

Interfase Dialer con la sede N

```
!
interface DialerN
 ip address 10.4.22.(4N+1) 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 dialer remote-name sedeN
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
```

Distribución de rutas a través del protocolo EIGRP

!

**router eigrp 120**

**redistribute static metric 10000 500 255 1 1500**

**passive-interface FastEthernet0/0**

**network 172.20.0.0**

**distribute-list 1 out ATM6/0.1**

**distribute-list 1 out ATM6/0.2**

**distribute-list 1 out ATM6/0.3**

.....

**distribute-list 1 out ATM6/0.N** % Publica las rutas a la sede N

**distribute-list 1 out Dialer1**

**distribute-list 11 in Dialer1**

**distribute-list 1 out Dialer2**

**distribute-list 12 in Dialer2**

**distribute-list 1 out Dialer3**

**distribute-list 13 in Dialer3**

.....

**distribute-list 1 out DialerN** % Publica la lista 1 a través de la dialer N

**distribute-list 1N in DialerN** % Permite recibir las rutas de la lista 1N

.....

**no auto-summary** % Las listas no se suman

**no eigrp log-neighbor-changes** % No envía los logs de cambios EIGRP

**no eigrp log-neighbor-warnings** %No envia los warnings de cambios EIGRP

!

Rutas estáticas hacia las sedes remotas, en este caso se esta apuntando a la interfase DialerN, que es similar a la configuración del Router 1 donde se menciona la IP de la interfase dialer.

!

**ip classless**

%Publicación de la red WAN de cada sede por la ISDN

**ip route 10.4.10.8 255.255.255.248 Dialer1 250**

**ip route 10.4.10.16 255.255.255.248 Dialer2 250**

**ip route 10.4.10.24 255.255.255.248 Dialer3 250**

**.....**

**ip route 10.4.10.8N 255.255.255.248 DialerN 250**

%Publicación de la red LAN de cada sede por la ISDN

**ip route 172.21.1.0 255.255.255.248 Dialer1 250**

**ip route 172.21.2.0 255.255.255.248 Dialer2 250**

**ip route 172.21.3.0 255.255.255.248 Dialer3 250**

**.....**

**ip route 172.21.N.0 255.255.255.248 DialerN 250**

**!**

Se define el map-class dialer, el cual tendrá el nombre tesis-uni, igual al del Router 1

**!**

**map-class dialer tesis-uni**

**dialer idle-timeout 60** % Tiempo de espera 60 segundos

**dialer fast-idle 5**

**dialer wait-for-carrier-time 3**

**!**

### 6.4.2 Configuración de la Sede Remota.

Para cada sede remota se usara un Router Cisco 2611, el cual contara con 2 interfases Ethernet, una de ellas para la red LAN y la otra para la red WAN, esta ultima se conectara a la red del proveedor a través de un enlace de fibra, para esto se requiere de convertidores de medio Ethernet a óptico (Media Converter), la conversión se realizara en los equipos del proveedor. Además contara con una interfase BRI, la cual será usada para la conexión de respaldo ISDN. El ejemplo a continuación es para la sede N.

Primero definiremos el nombre del equipo, el cual debe coincidir con el username para esta sede indicados en los routers Router1 y Router2 de la sede principal:

**!**

**hostname SedeN**

**!**

Se define también el nombre y password de los routers Router1 y Router2, los cuales servirán para el proceso de autenticación.

!

**username Router1 password 7 (Router1)**

**username Router2 password 7(Router2)**

!

Configuración de la Interfase WAN que pasara a través de la red del proveedor de servicios.

!

**Ethernet 0/0**

**description INTERFASE ENLACE WAN Sede N**

**ip address 10.4.10.(8N+2) 255.255.255.248**

**no ip directed-broadcast**

**full-duplex**

**no fair-queue**

!

Configuración de la interfase LAN:

!

**Ethernet 0/1**

**description INTERFASE ENLACE WAN**

**ip address 172.21.N.0 255.255.255.0**

**no ip directed-broadcast**

**full-duplex**

**no fair-queue**

!

Se define el tipo de línea BRI, para Perú es del tipo:

!

**isdn switch-type basic-net3**

La siguiente configuración del Enlace de Backup en la interfase BRI muestra una preferencia mayor hacia el pool-member 1 (dialer1), que es la que apunta a la sede principal Router1. También el parámetro max-link indica que se debe conectar las 2 dialer hacia el router remoto a través de la conexión establecida.

```
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 dialer pool-member 1 priority 200 max-link 2
 dialer pool-member 2 priority 100 max-link 2
 isdn switch-type basic-net3          % Tipo de linea BRI ISDN
 ppp authentication chap              % Tipo de autenticación CHAP
 ppp multilink                        % Tipo de protocolo PPP Multilink
!
```

Se configuran las líneas Dialer para la conexión con la sede principal.

```
!
interface Dialer1
 ip address 10.4.21.(4N+2) 255.255.255.252
 ip nat outside
 encapsulation ppp
 no ip mroute-cache
 dialer pool 1
 dialer remote-name Router1
 dialer string 5554444 class tesis-uni        % # Telefónico Router1
 dialer load-threshold 1 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
!
!
interface Dialer2
```

```
ip address 10.4.22.(4N+2) 255.255.255.252
ip nat outside
encapsulation ppp
no ip mroute-cache
dialer pool 2
dialer remote-name Router2
dialer string 5555555 class tesis-uni          % # Telefónico Router2
dialer load-threshold 1 either
dialer-group 2
ppp authentication chap
ppp multilink
!
```

Definimos las listas de acceso que se aplicaran en las dialer-list1 y dialer-list2, en estas se deniega el envío de paquetes EIGRP.

```
!
access-list 151 deny   eigrp any any
access-list 151 permit ip any any
dialer-list 1 protocol ip list 151
dialer-list 2 protocol ip list 151
!
```

Enrutamiento en la sede Remota, se usa el mismo AS que los routers de la sede principal, en esta caso las interfases dialer se configuran como pasivas, para evitar la activación de la línea de respaldo por el envío de paquetes de enrutamiento, también la interfase Ethernet 0/1 (LAN de la sede).

```
!
router eigrp 120
 passive-interface Dialer1
 passive-interface Dialer2
 redistribute static
 passive-interface Ethernet0/1
 network 172.21.N.0
```

**no auto-summary**

**!**

Definimos las rutas hacia las interfases Dialer con un peso de 200

**!**

**ip classless**

**ip route 0.0.0.0 0.0.0.0 Dialer1 200**

**ip route 0.0.0.0 0.0.0.0 Dialer2 200**

Se configura **map-class**, la cual debe coincidir con las configuradas en los routers de la sede principal.

**!**

**map-class dialer tesis-uni**

**dialer idle-timeout 60**

**dialer fast-idle 5**

**dialer wait-for-carrier-time 20**

**!**

### 6.5 Detección de Fallas (Troubleshooting).

Luego de haber instalado y configurado la conexión ISDN se pueden realizar las siguientes pruebas para verificar el estado del enlace.

#### 6.5.1 Detección de fallas a través de comandos de línea.

**a) Show isdn status**: Muestra el estado de las capas 1, 2 y 3 de todas las interfaces ISDN o de una interfase ISDN especifica. Cuando se realiza el troubleshooting de una ISDN BRI, se debe determinar primero si el router puede comunicarse apropiadamente con el switch ISDN de la red de telefonía pública. Una vez que se ha verificado la comunicación, se puede proceder con el nivel superior, tales como problemas en la interfase dialer, definición de trafico interesante, fallas PPP, etc.

Al aplicar este comando en un router con una tarjeta Controller E1 se tiene:

**Router#show isdn status**

Global ISDN Switchtype = primary-net5

ISDN Serial3/0:15 interface

dsl 0, interface ISDN Switchtype = primary-net5

Layer 1 Status:

ACTIVE

Layer 2 Status:

TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED

Layer 3 Status:

0 Active Layer 3 Call(s)

Active dsl 0 CCBs = 0

The Free Channel Mask: 0xFFFF7FFF

Total Allocated ISDN CCBs = 0

En un router con interface BRI se obtiene:

**Router#show isdn status**

Global ISDN Switchtype = basic-net3

ISDN BRI0/0 interface

dsl 0, interface ISDN Switchtype = basic-net3

Layer 1 Status:

ACTIVE

Layer 2 Status:

TEI = 81, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED

Layer 3 Status:

0 Active Layer 3 Call(s)

Activated dsl 0 CCBs = 0

The Free Channel Mask: 0x80000003

Total Allocated ISDN CCBs = 0

**b) Show dialer:** Despliega el estado de la dialer y el estado individual de los canales ISDN.

Para el caso de un router con interfase BRI, la cual se encuentra con la línea de respaldo activada se tiene:

**Router# show dialer interface dialer1**

Di1 - dialer type = DIALER PROFILE

Load threshold for dialing additional calls is 1

Idle timer (120 secs), Fast idle timer (20 secs)

Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is physical layer up

Number of active calls = 2

| Dial String | Successes | Failures | Last DNIS | Last status | |
|---|---|---|---|---|---|
| 5554444 | 44 | 4517 | 00:01:25 | successful | Default |

**Router# show dialer interface BRI0/0**

BRI0/0 - dialer type = ISDN

| Dial String | Successes | Failures | Last DNIS | Last status |
|---|---|---|---|---|

0 incoming call(s) have been screened.

0 incoming call(s) rejected for callback.

BRI0/0:1 - dialer type = ISDN

Idle timer (60 secs), Fast idle timer (20 secs)

Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is data link layer up

Dial reason: ip (s=10.4.21.6, d=10.4.21.5) % IP Origen y Destino de Llamada

Interface bound to profile Di1

Current call connected 00:01:55

Connected to 5554444 (Router1)

BRI0/0:2 - dialer type = ISDN

Idle timer (60 secs), Fast idle timer (20 secs)

Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is multilink member

Dial reason: Multilink bundle overloaded

Interface bound to profile Di1

Current call connected 00:01:24

Connected to 5554444 (Router1)

**c) Show interface**: Muestra el estado de varias interfaces, tales como las interfases serial y BRI. En el caso de un router con interfase BRI se tiene:

- Cuando la conexión de respaldo no esta activada (está en espera):

**Router#show interfaces BRI 0/0**

BRI0/0 is up, line protocol is up (spoofing) %Line Protocol en spoofing
Hardware is PQUICC BRI

**Router#show interfaces BRI 0/0:1**

BRI0/0:1 is down, line protocol is down % Protocol y Line Protocol en Down
Hardware is PQUICC BRI

**Router#show interfaces BRI 0/0:2**

BRI0/0:2 is down, line protocol is down % Protocol y Line Protocol en Down
Hardware is PQUICC BRI

**Router#show interfaces dialer 1**

Dialer1 is up (spoofing), line protocol is up (spoofing) % Estado spoofing
Hardware is Unknown

**Router#show interfaces dialer 2**

Dialer2 is up (spoofing), line protocol is up (spoofing) % Estado spoofing
Hardware is Unknown

- Cuando la conexión de respaldo esta activa

**Router#show interface BRI0/0**

BRI0/0 is up, line protocol is up (spoofing)
Hardware is PQUICC BRI

**Router#sh interface BRI0/0:1**

BRI0/0:1 is up, line protocol is up % Protocol y Line Protocol en Up
Hardware is PQUICC BRI

**Router#sh interface BRI0/0:2**

BRI0/0:1 is up, line protocol is up % Protocol y Line Protocol en Up

Hardware is PQUICC BRI

**Router# show interface dialer1**

Dialer1 is up, line protocol is up (spoofing) % Solo en Spoofing Line Protocol

Hardware is Unknown

**Router# show interface dialer2**

Dialer1 is up, line protocol is up (spoofing) % Solo en Spoofing Line Protocol

Hardware is Unknown

Como vimos anteriormente, el estado spoofing es una simulación de estado activo, esto para poder conocer las rutas a través de esta interfase, ya que si estuviese caída, las rutas que apuntan a esta interfase no serían almacenadas en la tabla de enrutamiento.

**d) Show controllers E1**: Muestra el estado de la tarjeta controller E1, para nuestro caso en los routers de la sede principal.

**Router# show controllers E1**

E1 4/0 is up.

Applique type is Channelized E1 - unbalanced

Description: *E1 Backup ISDN – 555-5555*

No alarms detected.

Framing is NO-CRC4, Line Code is HDB3, Clock Source is Line.

Data in current interval (650 seconds elapsed):

0 Line Code Violations, 0 Path Code Violations

0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins

0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs

Total Data (last 24 hours)

0 Line Code Violations, 0 Path Code Violations,

0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,

0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs

**e) Show isdn service:** Muestra el estado de los canales en una tarjeta Controller:

**Router#show isdn service**

PRI Channel Statistics:

ISDN Se3/0:15, Channel [1-31]

Configured Isdn Interface (dsl) 0

Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)

Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Service State (0=Inservice 1=Maint 2=Outofservice)

Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

**f) Show isdn active:** Se puede verificar el estado de la conexión de respaldo con el comando: show isdn active.

- No hay conexión activa

Router#show isdn active

ISDN ACTIVE CALLS

---

| Call Type | Calling Number | Called Number | Remote Name | Seconds Used | Seconds Left | Seconds Idle | Charges Units/Currency |
|---|---|---|---|---|---|---|---|

**Router#show isdn history**

---

ISDN CALL HISTORY

Call History contains all active calls, and a maximum of 100 inactive calls.
Inactive call data will be retained for a maximum of 15 minutes.

---

| Call Type | Calling Number | Called Number | Remote Name | Seconds Used | Seconds Left | Seconds Idle | Charges Units/Currency |
|---|---|---|---|---|---|---|---|

---

- Con la línea de respaldo activa:

**Router#show isdn active**

```
-------------------------------------------------------------------------------
                    ISDN ACTIVE CALLS
-------------------------------------------------------------------------------
Call  Calling    Called     Remote  Seconds Seconds Seconds Charges
Type  Number     Number     Name    Used    Left    Idle    Units/Currency
-------------------------------------------------------------------------------
Out  ---N/A---  5554444  +_Router1    59 Unavail  -       0
Out  ---N/A---  5554444  +_Router1    28 Unavail  -       0
-------------------------------------------------------------------------------
```

**Router#show isdn history**

```
-------------------------------------------------------------------------------
                    ISDN CALL HISTORY
-------------------------------------------------------------------------------
Call History contains all active calls, and a maximum of 100 inactive calls.
Inactive call data will be retained for a maximum of 15 minutes.
-------------------------------------------------------------------------------
Call  Calling    Called     Remote  Seconds Seconds Seconds Charges
Type  Number     Number     Name    Used    Left    Idle    Units/Currency
-------------------------------------------------------------------------------
Out  ---N/A---  5554444  +_Router1    120 Unavail  -       0
Out  ---N/A---  5554444  +_Router1    120 Unavail  -       0
-------------------------------------------------------------------------------
```

### 6.5.2 Debugs.

Los debugs son comandos de línea que nos arrojan la información de cada proceso que se ejecuta en el router. Para cada tipo de proceso se habilita un comando diferente en el router.

Cuando una llamada ISDN no es establecida, esta se puede deber a los siguientes factores:

- Dial-on-Demand DDR

Capas 1, 2 y 3 de ISDN.

Poit-to-Point-Protocol (PPP).

Uno de los debugs mas usados para detectar la falla es del Debug de Cisco q931, este se podría activar en ambos extremos de la conexión (sede principal y sede remota)

### 6.2.1 Debug isdn q931.

Este comando nos brindará información de cada proceso al momento de la conexión a nivel de capa 3.

Para realizar las pruebas de ISDN se puede realizar el envío de paquetes ICMP desde el router de la sede remota a la sede principal apuntando a la IP de la interfase Dialer, esto activara una llamada ISDN generando mensajes q931.

Para nuestro caso se ha activado el debug en ambos extremos y se mostrara uno a uno. En cada proceso se describirá lo que se esta ejecutando.

**a) Debug Sede RemotaN (Router llamante).**

**SedeN# debug isdn q931**

**SedeN# terminal monitor**

Sep 17 12:02:43.218: ISDN BR0/0 EVENT: UserIdle: callid 0x8522 received ISDN_CALL (0x0)

Sep 17 07:02:43: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0/0, TEI 64 changed to up

Sep 17 12:02:43.298: ISDN BR0/0 Q931: TX -> SETUP pd = 8 callref = 0x29

*El router llamante transmite (indicado por TX) el mensaje SETUP*

Bearer Capability i = 0x8890

Standard = CCITT

Transer Capability = Unrestricted Digital

Transfer Mode = Circuit

Transfer Rate = 64 kbit/s

Channel ID i = 0x83

Called Party Number i = 0x80, '5554444'

Plan:Unknown, Type:Unknown

**Sep 17 12:02:43.534: ISDN BR0/0 Q931: RX <- CALL_PROC pd = 8 callref = 0xA9**

**Sep 17 12:02:43.542:**

**Channel ID i = 0x89**

*El switch de la red de telefonía publica responde con el mensaje Call Proceeding. Esto indica que la red esta procesando la llamada.*

**Sep 17 12:02:44.179: ISDN BR0/0 Q931: RX <- CONNECT pd = 8 callref = 0xA9**

*Se recibe un mensaje de CONNECT del router remoto. La conexión ISDN ha sido establecida. Cualquier falla de llamada pasada este punto se deben a problemas de nivel superior tales como DDR, PPP, Autenticación, IPCP/IP Addressing.*

**Sep 17 12:02:44.195: ISDN BR0/0 Q931: TX -> CONNECT_ACK pd = 8 callref = 0x29**

*El router responde con un Connect Acknowledgment (CONNECT_ACK) a la red de telefonía.*

**b) Debug Sede Principal Router 1 (Router llamado).**

**Router1# debug isdn q931**

**Router1# terminal monitor**

**Sep 17 07:02:44: ISDN Se4/0:15 Q931: RX <- SETUP pd = 8 callref = 0x0640**

*El router llamado recibe (indicado por RX)un mensaje SETUP del switch.*

**Bearer Capability i = 0x8890**

**Standard = CCITT**

**Transer Capability = Unrestricted Digital**

**Transfer Mode = Circuit**

**Transfer Rate = 64 kbit/s**

*La llamada entrante es digital de 64Khps.*

**Channel ID i = 0xA18381**

**Preferred, Channel 1**

**Calling Party Number i = 0x2183, '15101515'** ← *# origen llamada*

**Plan:ISDN, Type:National**

**Called Party Number i = 0xC1, '5554444'** ← *# destino llamada*

**Plan:ISDN, Type:Subscriber(local)**

**Sending Complete**

*Identifica el número llamante y llamado*

**Sep 17 07:02:44: ISDN Se4/0:15 EVENT: process_rxstate: ces/callid 1/0x114C calltype 1 CALL INCOMING**

**Sep 17 07:02:44: ISDN Se4/0:15 EVENT: UserIdle: callid 0x114C received ACCEPT_CALL (0x13)**

*El router acepta la llamada.*

**Sep 17 07:02:44: ISDN Se4/0:15 EVENT: process_rxstate: ces/callid 1/0x114C calltype 1 CALL INCOMING**

**Sep 17 07:02:44: ISDN Se4/0:15 EVENT: UserIdle: callid 0x114C received ACCEPT_CALL (0x13)**

**Sep 17 07:02:44: %LINK-3-UPDOWN: Interface Serial4/0:0, changed state to up**

**Sep 17 07:02:44: ISDN Se4/0:15 Q931: TX -> CALL_PROC pd = 8 callref = 0x8640**

*El router transmite un Llamada procedente (CALL_PROC)*

**Sep 17 07:02:44: ISDN Se4/0:15 Q931: TX -> CALL_PROC pd = 8 callref = 0x8640**

**Channel ID i = 0xA98381**

**Exclusive, Channel 1**

**Sep 17 07:02:44: ISDN Se4/0:15 Q931: TX -> CONNECT pd = 8 callref = 0x8640**

**Channel ID i = 0xA98381**

**Exclusive, Channel 1**

*La llamada es aceptada y el router envía un mensaje CONNECT al router remoto*

**Sep 17 07:02:44: ISDN Se4/0:15 Q931: RX <- CONNECT_ACK pd = 8 callref = 0x0640**

*El dispositivo llamado recibe un mensaje CONNECT_ACK del switch ISDN.*

**Sep 17 07:02:44: ISDN Se4/0:15 EVENT: process_rxstate: ces/callid 1/0x114C calltype 1 CALL_PROGRESS**

*La llamada ya fue establecida.*

**En este proceso se puede tener la mensajería mostrada en la TABLA Nº 6.5.**

**TABLA 6.5 Mensajería debug Q931.**

| Mensaje | Descripción |
|---|---|
| SETUP | Setup -- Indica que un dispositivo desea establecer una llamada de Capa 3. |
| CALL_PROC | Call_proceeding -- El mensaje SETUP ha sido recibido y esta siendo procesada por la red y o dispositivo remoto. |
| ALERTING | Alerting -- Informa a la red que el router final esta "alertando" al usuario; esto podría normalmente ser el caso para un teléfono y la alerta podría ser un "ring" en el equipo remoto. Este mensaje es normalmente asociado con equipos que usan handset, tal como en el caso de un Teléfono ISDN o TA. |
| CONNECT | Connect -- La llamada es aceptada |
| CONNECT_ACK | Connect_Acknowledge -- Este dispositivo ha recibido el mensaje CONNECT. Los protocolos de capa superior (PPP por ejemplo), deberían estar iniciando la negociación. |
| DISCONNECT | Disconnect -- Router ha iniciado el mensaje desconectar. Este mensaje indica usualmente que el circuito ISDN está funcionando y que la desconexión fue el resultado de algún evento de capa superior (DDR, PPP). Las 3 formas de desconexión estarán acompañadas por un mensaje de RELEASE y RELEASE_COMP.<br>El mensaje DISCONNECT es acompañado también por Disconnect Cause Code. Este código de desconexión puede ser usado para identificar donde fue desconectada la llamada (por ejemplo, router, switch ISDN local, switch ISDN remoto) |
| RELEASE | Release -- Reconoce el mensaje DISCONNECT y la línea caerá. El mensaje RELEASE esta comprendido entre los mensajes DISCONNECT y RELEASE_COMP. El mensaje RELEASE puede estar acompañado por un Disconnect Cause Code |
| RELEASE_COMP | Release-Complete -- La llamada cayo completamente. Este mensaje es comúnmente visto: a)<br>Durante la terminación normal de una llamada iniciada por alguno de los routers.<br>b) En respuesta a un mensaje SETUP del router llamante.<br>El mensaje RELEASE puede estar acompañado por un Disconnect Cause Code |

### 6.2.2 Debug PPP Autenticación.

Este debug nos proporciona la información de la autenticación y negociación entre los routers que están intentando conectarse.

**a) Debug ppp authentication Sede RemotaN (Router llamante).**

**SedeN# debug ppp authenticaction**

**SedeN# terminal monitor**

Sep 17 07:02:44: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up

Sep 17 07:02:44: %DIALER-6-BIND: Interface BR0/0:1 bound to profile Di1

Sep 17 12:02:44.231: BR0/0:1 PPP: Using dialer call direction

Sep 17 12:02:44.231: BR0/0:1 PPP: Treating connection as a callout

Sep 17 12:02:44.231: BR0/0:1 PPP: Phase is ESTABLISHING, Active Open

Sep 17 12:02:44.231: BR0/0:1 PPP: Authorization NOT required

Sep 17 12:02:44.275: BR0/0:1 PPP: Phase is AUTHENTICATING, by both

Sep 17 12:02:44.275: BR0/0:1 CHAP: O CHALLENGE id 17 len 27 from "SedeN"

Sep 17 12:02:44.291: BR0/0:1 CHAP: I CHALLENGE id 178 len 37 from "Router1"

*Se recibió un Challenge CHAP del router remoto (Router1)*

Sep 17 12:02:44.295: BR0/0:1 CHAP: Using hostname from unknown source

Sep 17 12:02:44.295: BR0/0:1 CHAP: Using password from AAA

Sep 17 12:02:44.295: BR0/0:1 CHAP: O RESPONSE id 178 len 27 from "SedeN"

Sep 17 12:02:44.311: BR0/0:1 CHAP: I SUCCESS id 178 len 4

Sep 17 12:02:44.315: BR0/0:1 CHAP: I RESPONSE id 17 len 37 from "Router1"

*Se intercambian los usernames para la autenticación de los equipos.*

Sep 17 12:02:44.319: BR0/0:1 PPP: Phase is FORWARDING, Attempting Forward

Sep 17 12:02:44.323: BR0/0:1 PPP: Phase is AUTHENTICATING, Unauthenticated User

Sep 17 12:02:44.323: BR0/0:1 PPP: Sent CHAP LOGIN Request

Sep 17 12:02:44.327: BR0/0:1 PPP: Received LOGIN Response PASS

Sep 17 12:02:44.327: BR0/0:1 PPP: Phase is FORWARDING, Attempting Forward

Sep 17 12:02:44.327: BR0/0:1 PPP: Phase is AUTHENTICATING, Authenticated User

Sep 17 12:02:44.331: BR0/0:1 CHAP: O SUCCESS id 17 len 4

Sep 17 12:02:44.331: BR0/0:1 PPP: Phase is VIRTUALIZED

Sep 17 12:02:44.339: Di1 PPP: Using dialer call direction

Sep 17 12:02:44.339: Di1 PPP: Treating connection as a callin

Sep 17 12:02:44.339: Di1 PPP: Phase is UP

*Se culmina la autenticación*

**b) Debug ppp authentication Sede Princ. Router1 (Router llamado).**

**Router1# debug ppp authenticaction**

**Router1# terminal monitor**

Sep 17 07:02:44: Se4/0:0 PPP: Using dialer call direction

Sep 17 07:02:44: Se4/0:0 PPP: Treating connection as a callin

Sep 17 07:02:44: Se4/0:0 PPP: Phase is ESTABLISHING, Passive Open

Sep 17 07:02:44: Se4/0:0 PPP: Authorization NOT required

*Se inicia la autenticación*

Sep 17 07:02:44: Se4/0:0 PPP: Phase is AUTHENTICATING, by both

Sep 17 07:02:44: Se4/0:0 CHAP: O CHALLENGE id 178 len 37 from "Router1"

Sep 17 07:02:44: Se4/0:0 CHAP: I CHALLENGE id 17 len 27 from "SedeN"

Sep 17 07:02:44: Se4/0:0 CHAP: Waiting for Peer to authenticate first

Sep 17 07:02:44: Se4/0:0 CHAP: I RESPONSE id 178 len 27 from "SedeN"

*Se intercambian los usernames*

Sep 17 07:02:44: Se4/0:0 PPP: Phase is FORWARDING, Attempting Forward

Sep 17 07:02:44: Se4/0:0 PPP: Phase is AUTHENTICATING, Unauthenticated User

Sep 17 07:02:44: Se4/0:0 PPP: Sent CHAP LOGIN Request

Sep 17 07:02:44: Se4/0:0 PPP: Received LOGIN Response PASS

Sep 17 07:02:44: Se4/0:0 PPP: Phase is FORWARDING, Attempting Forward

Sep 17 07:02:44: Se4/0:0 PPP: Phase is AUTHENTICATING, Authenticated User

Sep 17 07:02:44: %DIALER-6-BIND: Interface Se4/0:0 bound to profile DiN

Sep 17 07:02:44: Se4/0:0 CHAP: O SUCCESS id 178 len 4

Sep 17 07:02:44: Se4/0:0 CHAP: Using hostname from unknown source

Sep 17 07:02:44: Se4/0:0 CHAP: Using password from AAA

Sep 17 07:02:44: Se4/0:0 CHAP: O RESPONSE id 17 len 37 from "Router1"

Sep 17 07:02:44: Se4/0:0 CHAP: I SUCCESS id 17 len 4

Sep 17 07:02:44: Se4/0:0 PPP: Phase is VIRTUALIZED

Sep 17 07:02:44: DiN PPP: Using dialer call direction

Sep 17 07:02:44: DiN PPP: Treating connection as a callin

**Sep 17 07:02:44: DiN PPP: Phase is UP**

Se culmina la autenticación

# CONCLUSIONES

Del trabajo realizado se pueden derivar las siguientes conclusiones:

1- Los enlaces de contingencia juegan un papel muy importante en las telecomunicaciones, independientes del medio o tecnología que se use, las cuales pueden implementarse de acuerdo a las necesidades de cada usuario. Se puede usar un enlace ISDN o un enlace similar al enlace principal. También se pude de tener contingencia no solo en las líneas, sino en los equipos en cada punto del enlace. Esto se debe elegir luego de un minucioso estudio en el cual se verificara el costo beneficio por cada punto, ya que no tendría sentido implementar 2 enlaces de línea dedicada (una principal y una de respaldo), en una sede en la cual solo se realizan transacciones esporádicamente. En cambio, en el caso de una sede central, si se necesitaría 2 líneas dedicadas, además de contingencia de routers.

2- Se deben tener muy claros los criterios de enrutamiento para la conmutación del enlace principal al de contingencia, ya que de no estar bien definidos podría derivar en un mal funcionamiento del enlace de contingencia, como consecuencia la activación del enlace alterno sin haberse afectado el enlace principal. Esto por supuesto implica un costo innecesario, pues la activación del enlace ISDN se está realizando en forma innecesaria. También se puede dar el caso contrario, que se afecte el enlace principal, pero por mala configuración, o no tener los criterios de enrutamiento bien definidos el enlace de contingencia no se active.

3- En el caso de una línea de contingencia ISDN (que es en la que mas se ha profundizado) se debe tener en cuenta la seguridad para el acceso a entre 2 equipos, ya que la línea a través de la cual se enlazan es accesible desde cualquier punto del mundo, esto podría convertir en muy vulnerable la red corporativa. Para evitar este tipo de problemas se definen varios criterios como la autenticación del origen de la

llamada, callback, usuarios y passwords para ingresar, encriptación de estos datos, entre otros.

4- Las líneas de contingencia no solo se pueden usar en caso se presente un problema con el enlace principal, también se puede usar en caso se desborde la carga de tráfico o ancho de banda en el enlace principal, o simplemente no se quiere sobrecargar al enlace principal. Asimismo se pueden usar para conexiones esporádicas desde una oficina remota, la cual se conecta por ejemplo una vez al día por unos minutos.

5- Una empresa que requiere interconectar sus oficinas, puede implementar su propia red para los enlaces principales, o hacer uso de la red ya implementada por un proveedor de telecomunicaciones. Sin embargo, para la implementación de la conexión ISDN se requiere conexión a la red ISDN de un proveedor de telefonía.

## ANEXO A

A continuación, se listan en orden alfabético los acrónimos usados a lo largo de este trabajo.

1.- ACLs : Access Control Lists.
2.- APPN : Advanced Peer-to-Peer Networking.
3.- ARP : Address Resolution Protocol.
4.- AS : Autonomous System.
5.- BIA : Burned-in Address.
6.- BRI : Basic Rate Interface.
7.- BVI : Bridge Group Virtual Interface
8.- CBAC : Context-Based Access Control.
9.- CHAP : Challenge Handshake Authentication Protocol.
10.- CE : Customer Edge.
11.- CIDR : Classless Interdomain Routing.
12.- CSU/DSUs : Channel Service Unit / Data Service Unit.
13.- DCE : Data Circuit-Terminating Equipment.
14.- DDR : Dial-on-Demand Routing.
15.- DHCP : Dynamic Host Configuration Protocol.
16.- DUAL : Diffusing Update Algorithm.
17.- EIGRP : Enhanced Interior Gateway Routing Protocol.
18.- EIPs : Ethernet Interface Processors.
19.- FD : Feasible distance.
20.- FDDI : Fiber Distributed Data Interface.
21.- FD/RD : Reported distance.
22.- GPRS : General Packet Radio Service.
23.- HDLC : High-Level Data Link Control.

24.- HSRP : Host Standby Router Protocol.
25.- ICMP : Internet Control Message Protocol.
26.- IGRP : Interior Gateway Routing Protocol.
27.- ILMI : Interim Local Management Interface.
28.- IPCP : IP Control Protocol.
29.- IOS : Input Output Software.
30.- ISL : Inter-Switch Link.
31.- LCP : Link Control Protocol.
32.- LSAs : Link-state advertisements.
33.- MAC : Media Access Control.
34.- MHSRP : Multiple Host Standby Router Protocol
35.- MIB : Management Information Base.
36.- MPLS/VPN : Multiprotocol Label Switching / Virtual Private Networks.
37.- NAT : Network Address Translation.
38.- NBAR : Network Based Application Recognition.
39.- NBMA : Non-Broadcast Multiaccess.
40.- NCP : Network Control Protocols.
41.- OSI : Open System Internetworking.
42.- OSPF : Open Shortest Path First.
43.- PAP : Password Authentication Protocol.
44.- PE : Provider Edges.
45.- PDM : Protocol-dependent modules.
46.- PPP : Poit-to-Poit Protocol.
47.- PRI : Primary Rate Interface.
48.- PSTN : Public Switched Telephone Networks.
49.- RAM : Random Access Memory.
50.- RIF : Routing Information Field.
51.- RIP : Routing Information Protocol.
52.- RTMP : Routing Table Maintenance Protocol.
53.- RTP : Reliable Transport Protocol.
54.- SAP : Service Advertisement Protocol.

55.- SDE : Secure Data Exchange.

56.- SLIP : Serial Line Interface Protocol.

57.- SMDS : Switched Multimegabit Data Service.

58.- SNMP : Simple Network Management Protocol.

59.- SOHO : Small Office – Home Office.

60.- SRB : Source-Route Bridging.

61.- VIPs : Versatile Interface Processors.

62.- VLSM : Variable-length subset mask.

63.- VPN : Virtual Private Network.

64.- VRF : VPN Routing/Forwarding.

65.- WAN : Wide-Area Network.

# ANEXO B

Como complemento de este documento se mencionan las palabras que, por motivos técnicos no son traducidos en el informe, ya que se perdería el contexto de la frase o párrafo:

1.- Acknowledgment.- Reconocimiento.

2.- Backup.- Respaldo, reserva.

3.- Backbone.- Plataforma principal de la red de transporte.

4.- Bridge Group Virtual Interface (BVI).- Interfaz Virtual de Grupo Puente.

5.- Broadcast.- Difusión.

6.- Burned-in Address.- Dirección original, propia.

7.- Callback.- Devolución de llamada.

8.- Classfull routing protocol.- Protocolo de enrutamiento de clase completa.

9.- Classless interdomain routing (CIDR).- Protocolo de enrutamiento de clase incompleta.

10.- Clear Text.- Texto limpio, sin encriptación.

11.- Debug.- Detector de errores.

12.- Dial-in.- Llamada entrante.

13.- Dial-on-Demand Routing (DDR).- Enrutamiento de llamada por demanda.

14.- Dial-out.- Llamada saliente.

15.- Dialer Filtering.- Filtro de llamadas.

16. - Diffusing Update Algorithm (DUAL).- Algoritmo de Difusión de Actualización.

17.- Dynamic Host Configuration Protocol (DHCP).- Protocolo de Configuración Dinámico de la Estación.

18.- Distance Vector.- Vector Distancia.

19.- Edges.- Borde. Remoto.

20.- Enhanced Interior Gateway Routing Protocol (EIGRP).- Protocolo de Enrutamiento de Gateway Interior Mejorado.

21.- Failover.- Procedimiento a tomarse en caso de fallas del equipo principal.

22.- Feedback.- Retroalimentación.

23.- Fully Meshed.- Completamente enlazado.

24.- Hello Paquet.- Paquete Hola.

25.- Hold Time.- Tiempo de espera.

26.- Host.- Equipo, o dispositivo de paso en la red.

27.- Host Standby Router Protocol (HSRP).- Protocolo de Estación Router en Espera.

28.- Idle.- A la espera.

29.- Integrated Services Digital Network (ISDN).- Red Digital de Servicios Integrados.

30.- Interface Tracking.- Rastreo de interfase.

31.- Interior Gateway Routing Protocol (IGRP).- Protocolo de Enrutamiento de Gateway Interior.

32.- Internet Control Message Protocol (ICMP).- Protocol de mensajes de control de Internet.

33.- Keyword.- Palabra clave.

34.- Link Contro Protocol (LCP).- Protocolo de Control de Enlace.

35.- Link State.- Estado de Enlace.

36.- Link-state Advertisments (LSAs).- Avisos de estado de enlace.

37.- Management Information Base (MIB).- Base de Información de administración.

38.- Multicast.- Difusión hacia varios puntos.

39.- Network Control Protocol (NCP).- Protocolo de Control de Red.

40.- Preemption.- Preferencia.

41.- Preempt delay.- preferencia retrasada.

42.- Pooleo.- Minitoreo punto a punto de los terminales de una red.

43.- Public Switched Telephone Networks (PSTNs).- Red de Telefonía Pública Conmutada.

44.- Release.- Lanzamiento, liberación.

45.- Reliable.- Confiable.

46.- Reliable Transport Protocol (RTP).- Protocolo Confiable de Transporte.

47.- Reply.- Contestación, respuesta.

48.- Request.- Petición.

49.- Resign.- Aceptar, resignar.

50.- Retry.- Reintentar.

51.- Simple Network Management Protocol (SNMP).- Protocolo Simple de Administración de Red.

52.- Sites.- Sitios, terminales.

53.- Sniffer.- Una maquina que acepte todos los paquetes sin importar los que contenga la cabecera, se dice que está en estado promiscuo. Un sniffer es un programa para monitorear y analizar el tráfico en una red de computadoras.

54.- Split Horizons.- Horizonte partido, separado, fracturado.

55.- Spoof.- Simulación.

56.- Tracking.- Seguir, rastrear.

57.- Timers.- Temporizadores.

58.- Trigger.- Disparador, gatillo.

59.- Unicast.- Difusión a un solo punto.

60.- Update.- Actualización.

61.- Variable-length subnet mask (VLSM).- Mascara de subred de longitud variable

# BIBLIOGRAFÍA


1. Catherine Paquet / Diane Teare. "Creación de Redes Cisco". CCNP, CCDP Cisco.
2. Alvaro Retana / Don Slice / Russ White. "Advanced IP Network Design". Cisco Press.
3. Catherine Paquet. "Building Cisco Remote Access Networks". Editado por Cisco Networks.
4. Allan Leinwand. "Configuración de Routers Cisco". Editado por Cisco Networks.
5. Cisco Press. "Academia de Networking Cisco Systems", Guía de primer y segundo año del curso de CCNA.