UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA DE DATOS DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

TOBÍAS DÍAZ CHACÓN

PROMOCIÓN

2005 - I

LIMA – PERÚ

2011

DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA DE DATOS DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS

Dedicatoria: A mi padre y mi madre por todo su cariño y apoyo cuando me observaban estudiando. A mi esposa y mi hija por darme las fuerzas para acabar este informe.

SUMARIO

El presente trabajo nos introduce en la implementación de una red de alta disponibilidad para una entidad con servicios centralizados, analizando los antecedentes cercanos para encontrar sus deficiencias y así llegar a las actuales redes de alta disponibilidad en las cuales los tiempos de corte de servicio son de pocos minutos al año. También conoceremos la importancia que actualmente tienen las redes de comunicaciones para cierto tipo de negocios, donde la pérdida de comunicaciones por periodos de minutos puede provocar grandes pérdidas de dinero que usualmente deben ser asumidas por el operador de telecomunicaciones, basándose en acuerdos de niveles de servicio (SLA) anuales que deben cumplir.

A lo largo de los capítulos de este informe conoceremos los conceptos teóricos necesarios que debemos manejar en una red de alta disponibilidad, incluyendo las definiciones y cálculo de los valores de disponibilidad. También delinearemos las pautas necesarias para diseñar una red de alta disponibilidad incluyendo el equipamiento y las topologías físicas y lógicas. Posteriormente pasaremos a la etapa de implementación en la cual se detallará en mayor medida el equipamiento necesario y se mostrara las configuraciones tipo a ejecutar. Se culmina el presente informe con un listado de conclusiones de acuerdo al desarrollo de cada capítulo.

INDICE

INTRODUCCION 1

CAPITULO I
RED PRIVADA DE DATOS DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS 2

1.1 Descripción 2

1.2 Objetivos y Alcances 2

CAPITULO II
FUNDAMENTOS TEORICOS 4

2.1 Antecedentes de las Redes Privadas de Datos con Alta Disponibilidad para entidades con servicios centralizados. 4

2.2 Actuales esquemas de funcionamiento de las redes de alta disponibilidad 8

2.3 Protocolos de enrutamiento 9

2.4 AS (Autonomous System) 10

2.5 BGP (Border Gateway Protocol) 10

2.5.1 BGP Interno y Externo 11

2.5.2 Descripción del funcionamiento del protocolo BGP 12

2.5.3 Configuración BGP 13

2.6 LOCAL PREFERENCE 15

2.6.1 Configuración LOCAL_PREF 15

2.7 COMMUNITY: 17

2.8 HSRP 18

2.8.1 Configuración HSRP 19

2.9 Cuantificación de la disponibilidad de una red de comunicaciones. 21

2.9.1 Función de disponibilidad para servicios con conexión 24

2.9.2 Porcentaje de indisponibilidad del servicio MPLS (PIU, percent MPLS service unavailability) 25

2.9.3 Porcentaje de disponibilidad del servicio MPLS (PIA, percent MPLS service availability) 26

2.9.4 Definición del estado de disponibilidad/indisponibilidad 26

2.9.5 Tiempo medio entre interrupciones del servicio 27
2.9.6 Tiempo medio hasta el restablecimiento del servicio 27
2.9.7 Modelo básico de disponibilidad y relación de parámetros. 27
2.9.8 Determinación de la disponibilidad de un NSE (Ensamblado de Secciones de Red) en base a la disponibilidad de Secciones Básicas que lo componen 28
2.9.9 Valores de disponibilidad mínimos de acuerdo a la UIT 29
CAPITULO III
DISEÑO DE UNA RED DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS 30
3.1 Entidades con servicios centralizados 30
3.2 Características de diseño para lograr una red de alta disponibilidad 31
3.2.1 Redes redundantes de acceso 31
3.2.2 Hardware redundante 34
3.2.2.1 Convertidor de medio administrado 35
3.2.2.2 Router de acceso 37
3.2.2.3 Switch de interconexión 37
3.2.3 Redes redundantes de energía 38
3.2.4 Sede de contingencia 39
3.2.4.1 Conexión de fibra oscura 40
3.3 Diseño de las sedes Principal, Respaldo y Remotas de una red de alta disponibilidad 41
3.3.1 Cuantificación de la disponibilidad 42
3.3.2 Ancho de Banda 45
3.3.3 Hardware Sede Principal, Contingencia y Remotas 47
3.3.4 Topología final de la red de alta disponibilidad 49
3.3.5 Direccionamiento de la red de alta disponibilidad 50
CAPITULO IV
IMPLEMENTACIÓN DE UNA RED DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS 53
4.1 Equipamiento 53
4.1.1 Equipamiento de la Sede Principal y Contingencia 53
4.1.2 Equipamiento de las Sedes Remotas 54
4.2 Configuración de routers principal, backup y contingencia 54
4.2.1 Configuración de Router Principal 54

4.2.2 Configuración de Router Backup 56
4.2.3 Configuración de Router Contingencia 58
4.2.4 Configuración de Routers Remotos 60
4.3 Análisis del costo del proyecto 63
CONCLUSIONES Y RECOMENDACIONES 66
ANEXO A
DATASHEET ROUTER CISCO 7604 68
ANEXO B
DATASHEET ROUTER CISCO 2800 SERIES 73
ANEXO C
DATASHEET SWITCH CATALYST 3750-X Y 3560-X 78
ANEXO D
GLOSARIO 82
BIBLIOGRAFIA 92

INTRODUCCION

El presente trabajo busca demostrar los niveles de disponibilidad que son necesarios para poder indicar que una red de servicios centralizados tiene una alta disponibilidad, basándonos en ello desarrollamos todos los conceptos necesarios para lograr nuestro objetivo, así como también realizaremos el diseño y la implementación de una red de alta disponibilidad. El diseño e implementación de la red de alta disponibilidad para entidades con servicios centralizados no abarca los componentes propios de una LAN tales como firewall o switches de core, así como tampoco los temas relacionados a la infraestructura de los datacenters como la energía o interconexiones directas de datacenters (fibras oscuras), no obstante se mencionan recomendaciones para que los componentes propios de la LAN y la infraestructura de los datacenters vayan acorde a los niveles de disponibilidad de la red.

En el Capítulo I describimos brevemente que es una red de alta disponibilidad para una entidad con servicios centralizados, también indicamos los objetivos y alcances del presente trabajo.

En el Capítulo II damos el marco teórico necesario para poder desarrollar el diseño y la implementación de la red de alta disponibilidad para entidades con servicios centralizados.

En el Capítulo III diseñamos la red de alta disponibilidad para una entidad con servicios centralizados.

En el Capítulo IV concluimos con la implementación de la red de alta disponibilidad para una entidad con servicios centralizados.

CAPITULO I
RED PRIVADA DE DATOS DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS

1.1 Descripción

Las entidades con servicios centralizados tienen la característica de tener múltiples sedes a nivel local y nacional, las cuales requieren realizar consultas, transacciones e intercambio de información con un punto central que comúnmente es la Sede Principal de la entidad. El concepto de Red Privada de Datos de Alta Disponibilidad consiste en asegurar un alto grado de conectividad entre cualquier Sede Remota y la Sede Principal y se consigue con la implementación de enlaces de respaldo para la Sede Principal, así como redundancias de enlace y equipos en las Sedes Remotas. Este concepto se ha ido masificando en el sector empresarial desde el año 2004, debido a la multiplicación de los requerimientos de mayor ancho de banda, con lo cual se buscaron diversas soluciones para asegurar la continuidad de las operaciones entre una sede remota y la sede principal con la condición de seguir manteniendo el mismo ancho de banda.

En la actualidad es una realidad que diversas empresas, del sector financiero en su mayoría, exijan conexiones de red con disponibilidades mayores al 99,999%, lo cual significa que al año no debemos tener más de 5 minutos de corte de servicio por fallas de la red (1). Este tipo de redes son llamadas redes de alta disponibilidad y su importancia radica en la relación exponencial que se puede tener entre el tiempo de falla con la perdida de dinero que esto ocasiona (2).

Para los ingenieros de redes, el concepto de alta disponibilidad está estrechamente relacionado a esquemas activo – standby o activo – activo, lo cual no es más que colocar segundos enlaces, activos o en espera, que harán subir los valores de disponibilidad de la red.

1.2 Objetivos y Alcances

Los objetivos del presente documento son:

- Familiarizarse con los conceptos de networking orientados a las redes de alta disponibilidad, así como los comandos de configuración orientados a equipamiento de la marca Cisco System.
- Comprender el concepto de disponibilidad y los valores que se manejan en la industria de telecomunicaciones.
- Diseñar una Red Privada de Datos de Alta Disponibilidad orientado a empresas con servicios centralizados tales como Bancos, Financieras y Organismos Gubernamentales.
- Lograr y comprobar una disponibilidad mayor a 99,999%.
- Mostrar los diferentes esquemas de respaldo de conexión y conmutación automática en un entorno empresarial con servicios centralizados.
- Indicar los lineamientos para la implementación de una Red Privada de Datos de Alta Disponibilidad para una entidad con servicios centralizados.
- Elaborar los costos de implementación de una red con servicios centralizados para una entidad con 20 sedes remotas.

Los alcances del documento no abarcan:

- Componentes internos LAN de las empresas, tales como Firewalls, Switches de Core, Servidores Públicos, Servidores de correo o Servidores de aplicaciones propias de la empresa, los cuales se asume que posee sus propios mecanismos de corrección en caso de fallas.
- Componentes eléctricos, los cuales forman parte de la red eléctrica de la empresa, los cuales también debe tener sus propios mecanismos de corrección en caso de falla.
- Interconexiones entre datacenters tales como fibras oscuras.

CAPITULO II
FUNDAMENTOS TEORICOS

2.1 Antecedentes de las Redes Privadas de Datos con Alta Disponibilidad para entidades con servicios centralizados.

Las redes de datos centralizadas hasta el año 2004 se implementaban bajo la plataforma ATM, en la cual los requisitos de ancho de banda, en comparación con la actualidad, eran bastante bajos debido a que las aplicaciones existentes consumían poco ancho de banda y el uso de aplicaciones a través de internet no se había masificado.

No existen estadísticas de uso de ancho de banda empresarial (redes privadas), sin embargo podemos hacer un paralelo con las estadísticas de la OSILAC (Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe) el cual realiza distintas encuestas de uso de tecnologías de la información (3).

En la Figura 2.1 podemos apreciar el comportamiento anual de la penetración de banda ancha en América del Sur. En dicha grafica podemos apreciar que la penetración existente en el 2005 es el doble a la existente en el 2004, lo cual nos da una idea del ritmo de crecimiento en el uso del Internet y, por consiguiente, el desarrollo de aplicativos que requieren mayor ancho de banda así como la explotación de aplicativos cliente – empresa por parte del sector empresarial para aprovechar la penetración del ancho de banda en lo usuarios cliente.

En la Figura 2.2 apreciamos el crecimiento anual del uso de internet para operaciones de banca electrónica. El crecimiento en el uso de este aplicativo bancario requiere también el crecimiento del ancho de banda en las líneas de internet de las empresas del sector bancario y así asegurarnos que no colapse el servicio. Este crecimiento va de la mano con el crecimiento de las líneas privadas de datos de las empresas bancarias ya que el indicador de crecimiento en operaciones bancarias por internet también es un buen indicador de crecimiento de las operaciones bancarias en general.

En el 2004 existían empresas cuyo ancho de banda en su sede principal era de 2 Mbps y en las sedes remotas de 128 Kbps. En estos casos se disponía de contingencias

basadas en enlaces RDSI, cuyo ancho de banda de 64 Kbps era suficiente para las aplicaciones de entonces. El ancho de banda para esa misma empresa en la actualidad fácilmente puede llegar a ser 5 veces el ancho de banda del año 2004. En la Fig. 2.3 se muestra la topología de una empresa comercializadora de electrodomésticos en el año 2004.

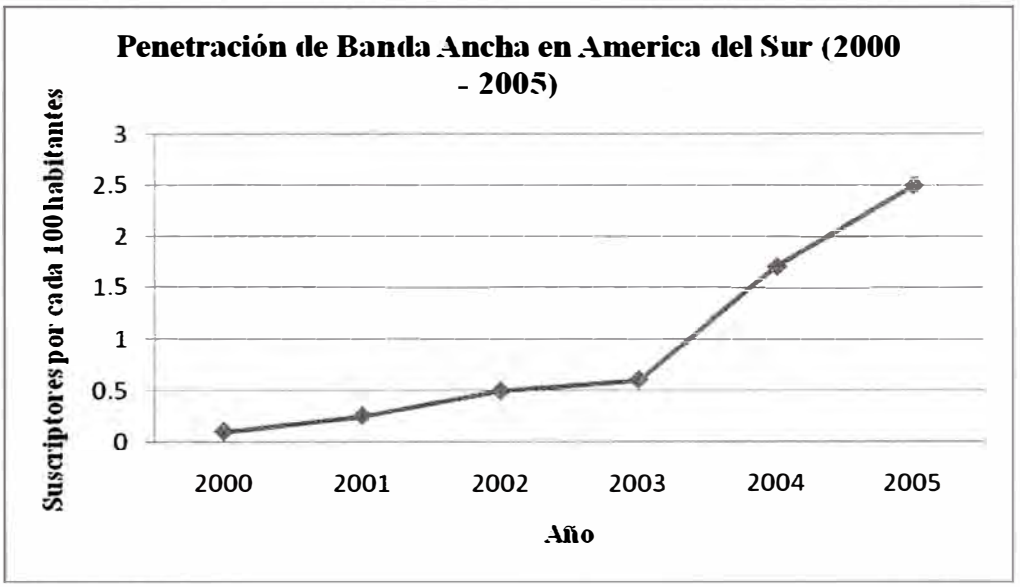


Fig. 2.1 Penetración de Banda Ancha en América del Sur del año 2000 hasta el 2005

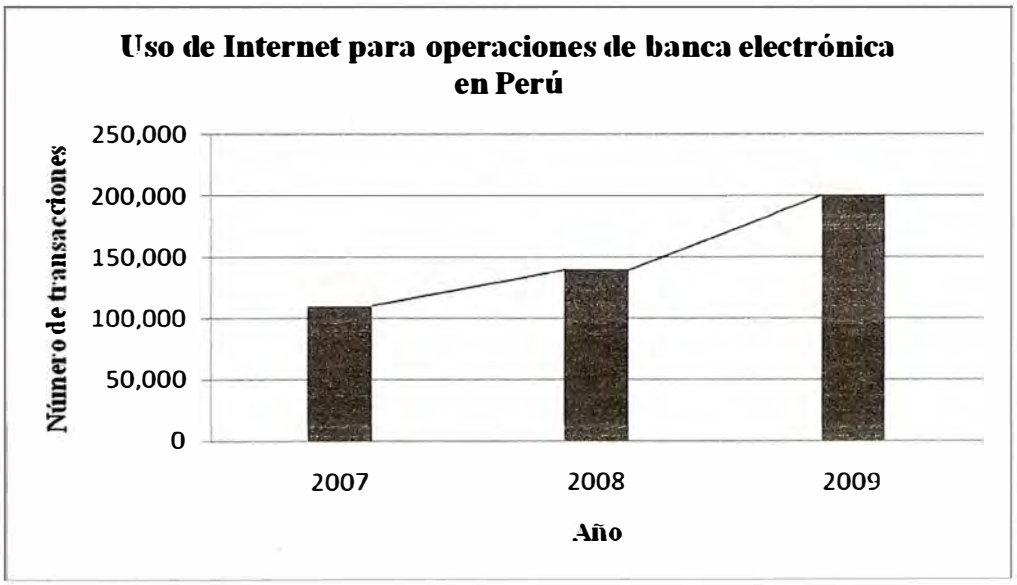


Fig. 2.2 Uso de Internet para operaciones de banca electrónica en el Perú

En ella se observa que cada sede posee una conexión en fibra óptica de 128 Kbps hacia la sede principal con otro enlace BRI de respaldo, el cual aseguraba la continuidad

solo de algunas aplicaciones debido a que el ancho de banda de la línea RDSI (BRI) normalmente es de 64 Kbps. En la Sede Principal se observa un enlace de 2Mbps sobre ATM y otro enlace PRI para todos los enlaces RDSI, el cual funciona de respaldo en caso falle el enlace de fibra óptica.

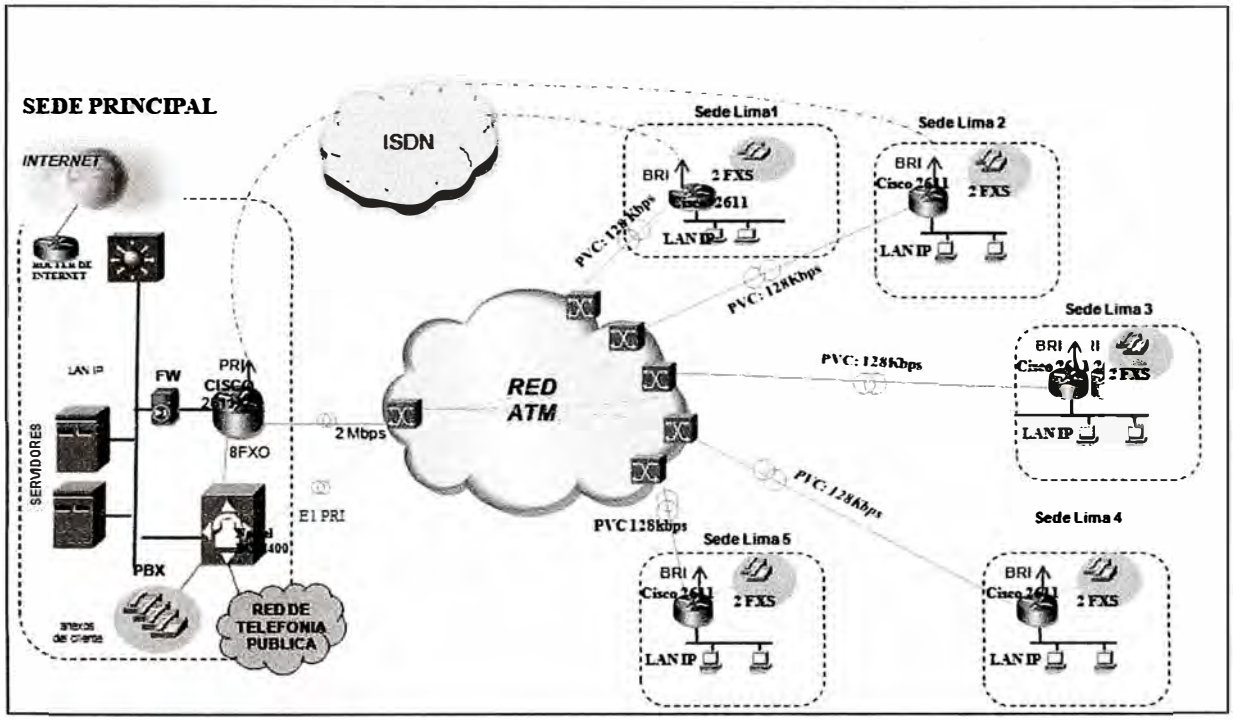


Fig. 2.3 Topología de una red empresarial a mediados del año 2004

Este tipo de esquemas estaba diseñado para los siguientes casos de falla:

Caso I: En caso ocurra algún corte en la fibra óptica de cualquier sede remota o avería en el respectivo POP de atención, el router de dicha sede automáticamente conmutará el trafico crítico hacia el enlace RDSI (BRI), dejando a la sede remota con una comunicación muy básica hacia la sede principal.

Lo indicado anteriormente se explica en la Fig. 2.4 en la cual, después de la rotura de la fibra óptica en la Sede Remota, esta se queda sin conexión a Internet y con limitada comunicación hacia los anexos telefónicos en la sede principal. Estas restricciones se daban para asegurar la fluidez del tráfico más importante (tráfico con los servidores, tráfico con la central telefónica, etc.).

En caso el punto de falla sea el POP de acceso de la Sede Lima 3, el comportamiento de la red es igual al comportamiento explicado anteriormente.

Caso II: En caso ocurra algún corte en la fibra óptica de la Sede Principal o avería en el respectivo POP de atención, el router conmuta automáticamente hacia su puerto PRI todas las conexiones con las sedes remotas. Esto hace que todas las sedes remotas tengan comunicaciones restringidas con la sede principal, comportándose cada una de manera similar al caso I.

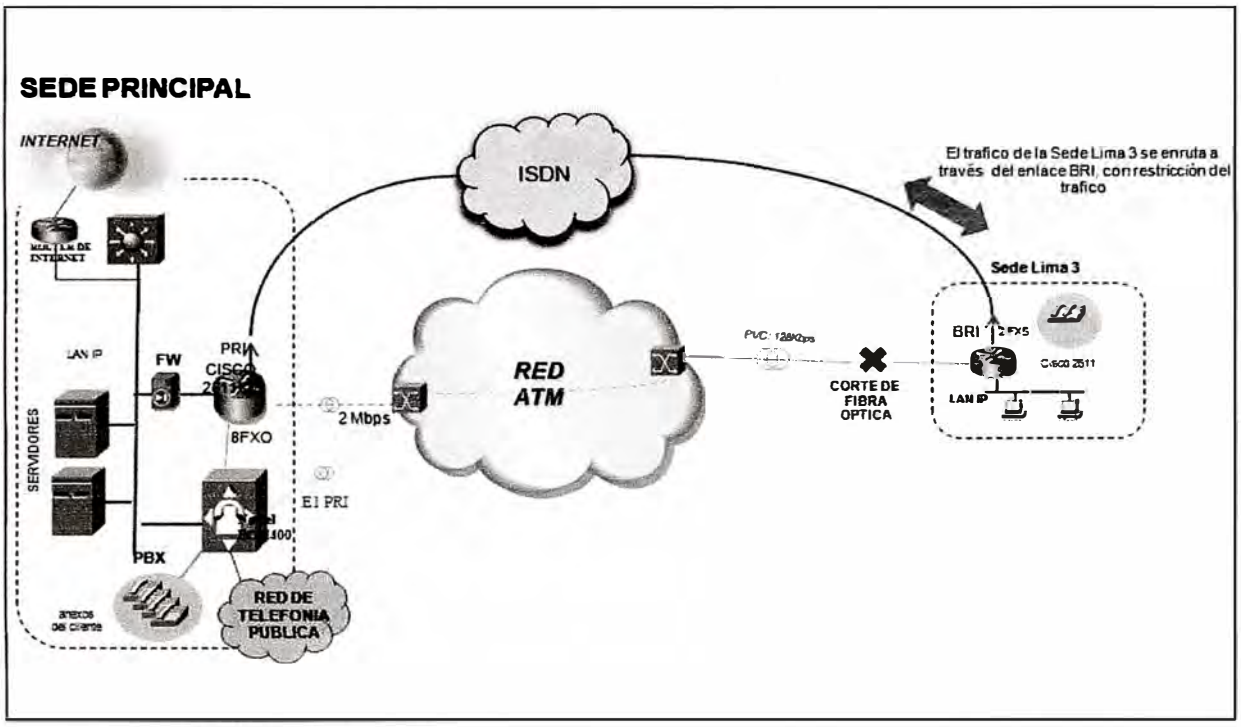


Fig. 2.4 Caso I: Caída de fibra y/o caída del POP de atención

Lo indicado anteriormente se puede apreciar en la Fig. 2.5, en donde el POP de atención ha sufrido un corte de energía, con lo cual el router de la sede principal restringe las comunicaciones con las sedes remotas hacia las conexiones RDSI, con las implicancias que se indicaron en el caso I.

Los siguientes puntos de falla no estaban cubiertos en el esquema de funcionamiento descrito en la Fig. 2.5:

- Avería del router en cualquier sede remota. En este caso, debido a que el enlace de fibra y el enlace RDSI llegan al mismo equipo final, la sede remota quedaría totalmente fuera de red.
- Avería en el router principal. En este caso, debido a que el enlace principal de fibra y el enlace RDSI (PRI) llegan al mismo equipo, la sede principal quedaría fuera de red, con la consiguiente caída de toda la red de la empresa.

- Siniestro en la sede principal. En el caso que ocurriera un desastre natural y/o accidente que cause el corte de todos los servicios en la sede principal, toda la red de la empresa quedaría fuera de servicio.

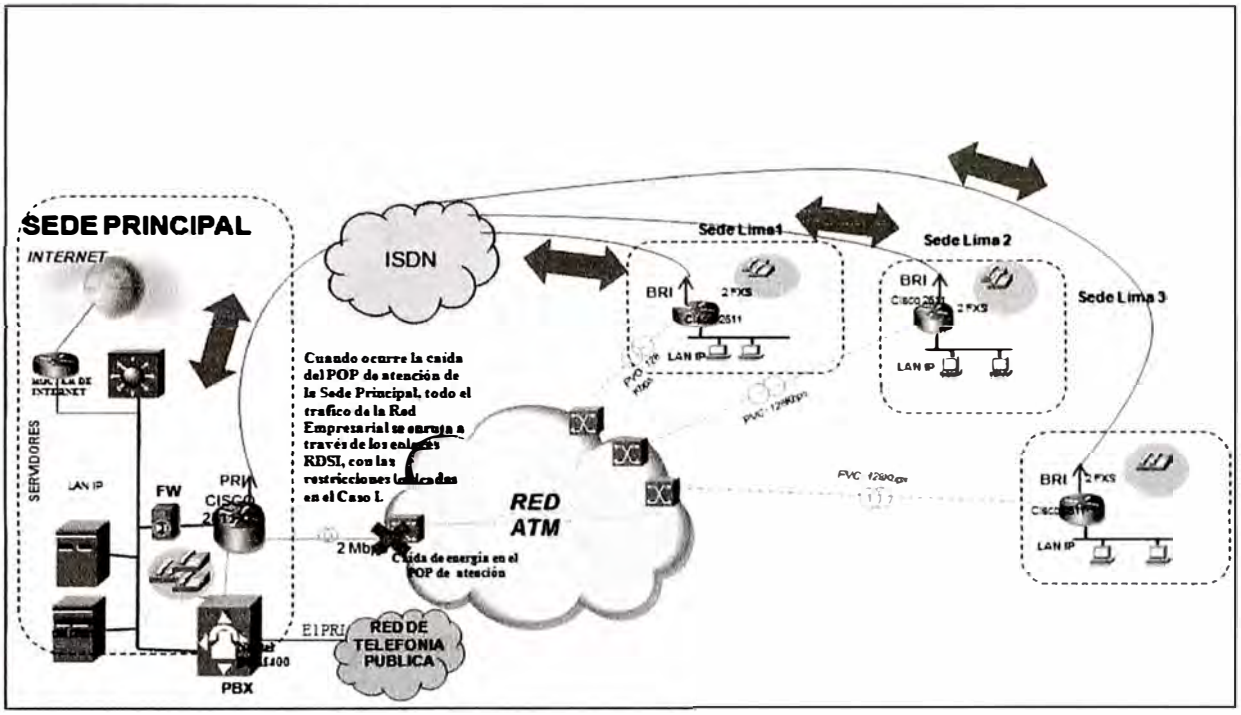


Fig. 2.5 Caso II: Caída de la fibra óptica y/o POP de atención de la Sede Principal

En la actualidad, los requerimientos de ancho de banda son mucho mayores a las indicadas en los ejemplos antes mostrados y, adicionalmente, el mercado exige poseer esquemas de contingencia capaces de mantener el mismo ancho de banda para asegurar la continuidad de todas sus aplicaciones.

2.2 Actuales esquemas de funcionamiento de las redes de alta disponibilidad

Actualmente las redes de comunicaciones de alta disponibilidad son implementadas sobre la plataforma MPLS debido a que es compatible con tecnologías que permiten tener un ancho de banda muy elevado (en el orden de los Tbps) además de introducir el concepto de Ingeniería de Trafico, el cual además de gestionar el ancho de banda, nos permite la recuperación automática ante fallas sobre una ruta.

En la Fig. 2.6 se muestra una red privada de datos de alta disponibilidad para una entidad con servicios centralizados. En dicha red se muestra algunos parámetros de configuración de dicha red, tales como BGP, AS y HSRP.

Estos conceptos serán explicados en detalle en el siguiente punto, considerando que son parámetros de configuración de una red de alta disponibilidad y, dependiendo de un correcto análisis y decisión sobre sus valores, la red será robusta y fiable ante fallas.

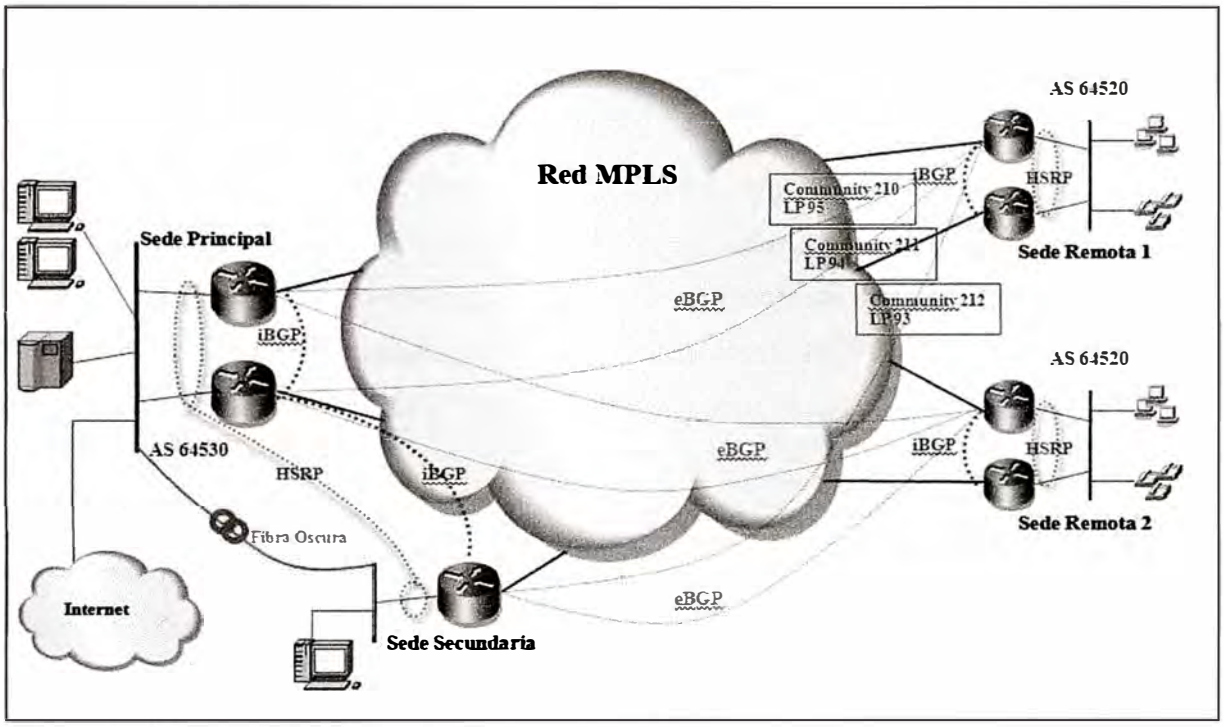


Fig. 2.6 Topología de Red Privada con Alta Disponibilidad

2.3 Protocolos de enrutamiento

Los protocolos de enrutamiento son las reglas utilizadas por un router para intercambiar información con otro router a fin de construir y mantener las tablas de enrutamiento actualizadas. El enrutamiento se puede realizar de manera estática o de manera dinámica, dependiendo de la topología del sistema autónomo.

El enrutamiento estático se utiliza en los casos donde la red está compuesta por pocos routers, la red tiene una sola salida hacia otra red o la red tiene una topología hub-and-spoke (centralizado).

El enrutamiento dinámico se utiliza cuando la topología de la red tiene cierta complejidad, haciendo necesario que los routers cooperen "dinámicamente" entre sí para mantener actualizadas sus tablas ante cualquier cambio topológico. En una red que utiliza protocolos de enrutamiento dinámico, las decisiones de enrutamiento pueden variar de acuerdo a las variaciones de la topología y del tráfico.

Los protocolos de enrutamiento dinámico más conocidos son:

Protocolo de Enrutamiento Dinámico Interior (IGP): Utilizados dentro de un Sistema Autónomo, como el protocolo RIP, IGRP, EIGRP y OSPF.

Protocolo de Enrutamiento Dinámico Exterior (EGP): Utilizado entre Sistemas Autónomos, como el protocolo BGP.

Es común que cualquier red medianamente grande posea tanto enrutamiento estático como enrutamiento dinámico.

2.4 AS (Autonomous System)

Un Sistema Autónomo es un grupo de routers bajo una única administración técnica usando un IGP (Interior Gateway Protocol) con métricas comunes para determinar como enrutar los paquetes dentro del AS y usando un protocolo de enrutamiento inter-AS para determinar la ruta de los paquetes a otros ASs (usualmente BGP). Es común que un AS use muchos IGPs (RIP, OSPF, IGRP, etc) y, algunas veces, tiene muchos grupos de métricas dentro del AS.

El uso del término Sistema Autónomo recalca que, aún cuando se use múltiples IGPs y métricas, la administración de esta AS aparenta para otros ASs tener un único y coherente plan de enrutamiento interior, siendo confiable el envío de tráfico a través de este. Cada Sistema Autónomo tiene un identificador de 16 bits, los cuales van del 1 al 65535, con la consideración que del 64512 al 65535 es de uso privado. En la RFC 1930 se detalla el uso de los números ASs. En el Fig. 2.7 se muestra la interconexión de 3 sistemas autónomos, en el cual cada uno de ellos tiene distinto IGP para el enrutamiento dentro del sistema autónomo y BGP para el enrutamiento entre sistemas autónomos.

2.5 BGP (Border Gateway Protocol)

El protocolo BGP se empezó a documentar en el año 1987 en la RFC 1267 del IETF, actualmente está en su versión 4 (BGP-4) la cual esta descrita en la RFC 1771 y actualizada en la RFC 4271. Adicionalmente se le ha agregado muchas extensiones como el soporte multiprotocolo en la RFC 2858. Es el protocolo de enrutamiento EGP usado por excelencia en todo Internet.

El protocolo BGP interactúa entre Sistemas Autónomos (ASs) intercambiando información de enrutamiento para llegar a otras redes. La información intercambiada incluye la ruta completa para el Sistema Autónomo, así como el trafico que la red destino espera recibir. Esta información es suficiente para construir una grafica de conectividad del AS incluyendo las políticas tomadas para evitar los loops. Las políticas de enrutamiento

que el protocolo BGP utiliza están enfocadas en la siguiente regla: Un Sistema Autónomo publica a otro Sistema Autónomo vecino solo las rutas que el mismo usa.

Esta regla refleja el paradigma de enrutamiento "hop-by-hop", el cual actualmente es utilizado en todo Internet. Se debe considerar que algunas políticas de enrutamiento BGP no se basan en el paradigma de enrutamiento "hop-by-hop" y en estos casos se hace uso de técnicas adicionales como source routing. Por ejemplo, BGP no permite que un AS envíe el tráfico a un AS vecino tomando una ruta distinta al tomado por el tráfico que se origino en el AS vecino. BGP corre sobre el protocolo de transporte TCP, estableciendo las conexiones a través del puerto 179.

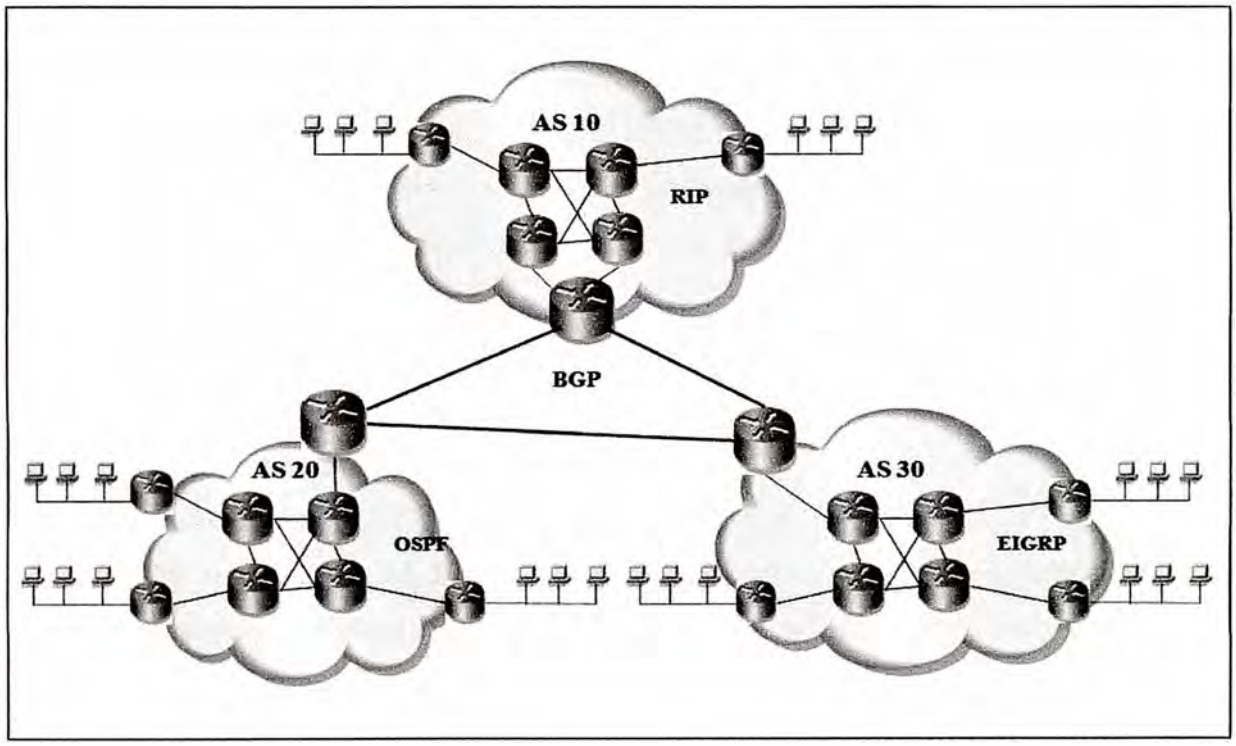


Fig. 2.7 - Interconexión de Sistemas Autónomos

2.5.1 BGP Interno y Externo

El protocolo BGP puede ser usado entre routers que pertenecen a un mismo Sistema Autónomo, llamándolo iBGP (BGP interno). Por exclusión, cuando el protocolo BGP se utiliza entre distintos Sistemas Autónomos es llamado eBGP (BGP externo).

Un router iBGP permite compartir con otros routers iBGP, de su propio AS, las rutas que aprenda de otros ASs a través de eBGP, sin embargo no puede compartir, a otros routers iBGP, las rutas que aprenda a través de otros routers iBGP. Esta restricción asegura que no se formen bucles de notificaciones de rutas, sin embargo obliga a que la red iBGP

sea completamente mallada, es decir que se formen sesiones entre cada router iBGP con todos los routers de un AS. En una red eBGP usualmente los router están directamente conectados y por lo tanto poseen direcciones IP pertenecientes al mismo segmento de red.

En una red iBGP los routers iBGP no necesitan estar directamente conectados por lo que sus direcciones IP pueden pertenecer a distintos segmentos de red.

2.5.2 Descripción del funcionamiento del protocolo BGP

El funcionamiento del protocolo BGP se da de la siguiente manera:

- Establecimiento de sesiones entre routers BGP (vecinos o peers) a través del puerto TCP 179.
- Se envían mensajes OPEN para que los routers BGP vecinos se conozcan.
- Envío de mensajes UPDATE, en la cual se intercambia inicialmente las tablas completas de enrutamiento, previamente filtradas por cada router de origen (en las tablas de enrutamiento solo están las mejores rutas hacia un destino, sin embargo existe la tabla de implementación, en donde están todas las rutas hacia un destino).
- En caso se detecte alguna condición de error, se envía el mensaje NOTIFICATION y se cierra automáticamente la sesión.
- Cada 60 segundos se envían mensajes KEEP-ALIVE, en ambos sentidos, para comprobar que la sesión sigue activa.

Existen 3 tipos de mensajes UPDATE, los cuales son:

WITHDRAWN ROUTES: En caso no se reciban mensajes KEEP-ALIVE en el lapso de 180 segundos (hold down) o se cierre la conexión TCP de la sesión BGP, se abandona la sesión BGP y se elimina todas las rutas anunciadas por el router involucrado. Adicionalmente, se envían mensajes UPDATE informando de las rutas eliminadas (withdrawn routes) a los vecinos BGP.

MENSAJES DE ACTUALIZACIÓN: En caso existan nuevos destinos o mejores rutas hacia destinos conocidos, se debe enviar mensajes de actualización, en las cuales se pueden colocar distintos atributos como AS-PATH, NEXT-HOP, LOCAL_PREF, COMMUNITY, etc. Para nuestro objetivo, que es lograr una red privada de alta disponibilidad, analizaremos en mayor detalle algunos de estos atributos en los siguientes puntos.

NLRI (Network Layer Reachability Information): En caso existan dos rutas para llegar a un mismo destino, localmente (dentro del AS) se indican atributos de preferencia para una de ellas (4).

2.5.3 Configuración BGP

En la Figura 2.8 se muestra la topología de red que nos servirá para mostrar los distintos comandos para configurar el protocolo BGP.

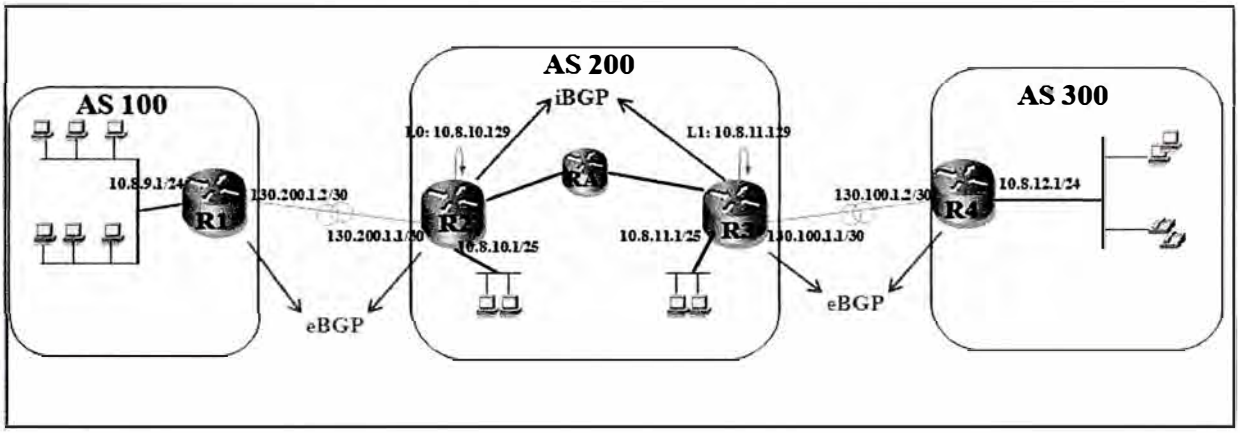


Fig. 2.8 Configuración BGP

Para configurar el protocolo BGP en un router, primeramente debemos definir el proceso BGP y el número de AS asociado al router a configurar, lo cual se realiza con el siguiente comando:

router bgp *AS*

En donde el AS es el Sistema Autónomo asociado al router a configurar.

Una vez definido el proceso BGP, se debe establecer la sesión BGP entre routers vecinos (peers). La sesión BGP se establece a través de una conexión TCP (port 179), en el cual ambos routers envían mensajes OPEN para intercambiar parámetros como su AS, la versión BGP usado y el tiempo de espera para el envío de mensajes KEEPALIVE. El comando a usar es:

neighbor *dirección_IP* remote-AS *AS_remoto*

En donde la dirección_IP es la IP del siguiente salto para poder llegar al AS_remoto en el caso de eBGP.

En el caso de iBGP, la dirección_IP es cualquier IP asociada al otro router iBGP (que no tiene que estar, necesariamente, conectado directamente al router de origen) y el AS_remoto es el mismo número de AS al cual pertenece el router a configurar.

Debemos tener en cuenta que, en dos router configurados como vecinos BGP, las IPs configuradas con el comando neighbor deben verse entre sí. Una manera de comprobar esto es con el comando ping.

Para el caso de la Fig. 2.8, la configuración del protocolo BGP para los routers es:

```
R1#
router bgp 100
neighbor 130.200.1.1  remote-as 200
R2#
router bgp 200
neighbor 130.200.1.2 remote-as 100
neighbor 10.8.11.1 remote-as 200
R3#
router bgp 200
neighbor 10.8.10.1 remote-as 200
neighbor 130.100.1.2 remote-as 300
R4#
router bgp 300
neighbor 130.100.1.1 remote-as 200
```

Usualmente, para el caso de iBGP, la dirección_IP es la IP de loopback asociada al router, esto para asegurar la independencia de la sesión BGP con el estado de cualquier interfaz física del router ya que, al ser la IP de loopbak una IP virtual, la sesión BGP puede establecerse por una u otra interfaz física del router. Cuando se haga uso de la IP de loopback en un proceso BGP, debemos indicarlo expresamente en el router asociado a la IP de loopback mediante el siguiente comando:

neighbor *dirección_IP* update-source *interfaz*

Esto es para forzar a que el router utilice la IP de loopback como IP de origen cuando se comunique con su vecino iBGP.

En la configuración anterior no se utilizo la IP de loopback, sino las IPs asociadas a las interfaces físicas. Si queremos configurar el iBGP en al AS 200, de tal manera que no asociemos interfaces físicas al proceso BGP, la configuración seria de la siguiente manera:

```
R1#
router bgp 100
neighbor 130.200.1.  remote-as 200
R2#
router bgp 200
neighbor 130.200.1.2 remote-as 100
neighbor 10.8.11.129 remote-as 200
neighbor 10.8.11.129 update-source loopback 0
R3#
router bgp 200
```

```
neighbor 10.8.10.129 remote-as 200
neighbor 10.8.10.129 update-source loopback 1
neighbor 130.100.1.2 remote-as 300
R4#
router bgp 300
neighbor 130.100.1.1 remote-as 200
```

Para que los cambios en la configuración de conexión BGP con un vecino empiecen a funcionar es necesario aplicar el comando reset de la siguiente manera:

clear ip bgp *dirección_ip*

Donde dirección_ip es la dirección IP del vecino. También podemos usar:

clear ip bgp *

Para resetear todas conexiones con los vecinos.

2.6 LOCAL PREFERENCE

El LOCAL_PREF (LP) es un atributo del mensaje UPDATE del protocolo iBGP. Este atributo se utiliza solo en los casos que se tenga más de una ruta de acceso desde un mismo AS exterior, asignando a cada una de las rutas un valor de preferencia, el cual se anuncia a todos los routers internos del AS.

Para que un router interno decida su siguiente salto para enviar el tráfico hacia fuera del AS, considerando que existen dos routers de conexión inter-AS y que los dos routers poseen rutas hacia el destino requerido, la ruta preferida será aquella que posee mayor valor de LOCAL_PREF.

2.6.1 Configuración LOCAL_PREF

En la Fig. 2.9 se muestra una topología en la cual el AS 100 dispone de dos caminos para llegar al AS 400. En este tipo de casos, se asigna un valor de preferencia para cada camino, el cual es llamado el LOCAL_PREF (LP), siendo el camino con mayor LP el preferido.

Para configurar el LP en un router, previamente debemos saber cómo controlar y modificar la información de encaminamiento. Esto se logra definiendo condiciones que se aplican a las rutas recibidas, anunciadas y redistribuidas de un protocolo de encaminamiento a otro.

El comando para lograr el control y manipulación de la información de encaminamiento es:

route-map *map-tag* [permit | deny] [sequence-number]

El valor de map-tag es el nombre del route map, esto permite tener múltiples instancias del mismo route map diferenciándolos por el nombre. De manera similar, el valor de sequence-number nos permite indicar la posición de un nuevo route map en una lista de route maps configurados con el mismo nombre.

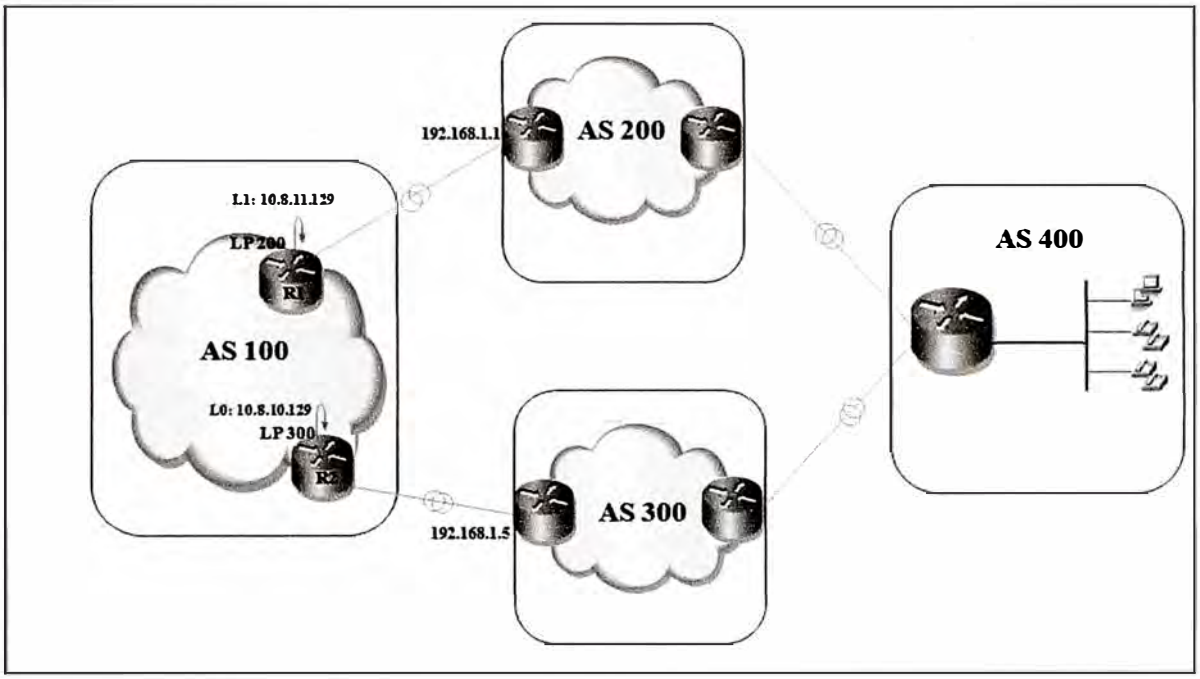


Fig. 2.9 Topología de red – Local Preference

Cada posición o instancia de un route-map contiene una lista de comandos match y set cuyas funciones son, respectivamente, aplicar condiciones a las rutas y modificar sus atributos.

Cuando la opción elegida en el route-map es permit, se evalúa la condición indicada con el comando match de la primera instancia y la ruta se redistribuye o se le aplica la acción especificada con el comando set, terminando de analizar el route-map. En el caso que no se cumpla ninguna condición para la ruta, se pasa a la siguiente instancia del route-map (el siguiente número de secuencia) así hasta que se cumpla algún match o no queden instancias en el route-map. En este último caso, si no se cumple ningún match la ruta no será aceptada ni reenviada.

Cuando la opción elegida en el route-map es deny, la ruta no es redistribuida o controlada, culminando el análisis del route-map sin comprobar el resto de instancias.

En el siguiente ejemplo se muestran dos instancias (10 y 20), una condición (match) y dos acciones para modificar la métrica de las rutas (set).

```
route-map SETMETRIC permit 10
match ip-address 1
set metric 3
route-map SETMETRIC permit 20
set metric 5
access-list 1 permit 170.10.0.0 0.0.255.255
```

En la Figura 2.9, si se quiere configurar el LP en el AS 100, debemos primeramente elegir la mejor ruta de salida y asignarle un valor de LP mayor que cualquier ruta de salida.

En este caso, la ruta que va por el AS 200 se le asignara el LP 200 y la ruta que va por el AS 300 se le asignara el LP 300, de esta manera la mejor ruta es aquella que pasa por el AS 300.

Entonces, considerando lo anteriormente indicado, la configuración relacionado a la topología indicada en la Fig. 2.9 seria:

```
R1(config)#route-map SECONDARY_T1_IN permit 10
R1(config-route-map)#set local-preference 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 192.168.1.1 route-map SECONDARY_T1_IN in

R2(config)#route-map PRIMARY_T1_IN permit 10
R2(config-route-map)#set local-preference 300
R2(config-route-map)#exit

R2(config-route-map)#router bgp 100
R2(config-router)#neighbor 192.168.1.5 route-map PRIMARY_T1_IN in
```

2.7 COMMUNITY:

El funcionamiento de las comunidades BGP esta descrito en la RFC 1997. El atributo COMMUNITY sirve para agrupar destinos (llamados comunidades), y así los routers BGP puedan después utilizar para controlar la información de enrutamiento que acepta, prefiere o distribuye a los routers vecinos. Es muy importante ya que ofrece mayores ventajas con respecto a las redes con la configuración basada solamente en AS, tales como:

Mayor granulidad con respecto a las políticas de enrutamiento.

Mayor simpleza en la configuración y mantenimiento de la red al eliminar la necesidad de manipular las rutas tomadas por los AS.

Eliminación de las configuraciones personalizadas para los clientes que tengan más de una salida hacia internet, en los casos de los ISP.

Los routers BGP pueden incluir la etiqueta COMMUNITY a las rutas que no están etiquetadas, de la misma manera que puede variar los atributos de una ruta con la etiqueta COMMUNITY de acuerdo a las políticas que maneje. Por ejemplo en una red se puede dar un valor de COMMUNITY a las rutas que tienen acceso a Internet y otro valor de COMMUNITY a las rutas que no tienen acceso a Internet.

Los valores de COMMUNITY que van desde 0X00000000 a 0X0000FFFF y de 0XFFFF0000 a 0XFFFFFFFF son reservados, el resto está codificado de manera que los dos primeros octetos indican el AS y los dos últimos contienen el identificador de la comunidad. Por ejemplo el valor de COMMUNITY 0X0032001e indica que el valor del AS es de 50 (0X0032) y el identificador de la comunidad es de 30 (0X001e).

2.8 HSRP

El protocolo HSRP está desarrollado en la RFC 2281. El Hot Standby Router Protocol (HSRP) es un protocolo propietario de Cisco que proporciona un mecanismo diseñado para admitir la conmutación por error y sin interrupciones del tráfico IP en determinadas circunstancias.

Con el protocolo HSRP, un grupo de routers trabaja en conjunto para dar la impresión de ser un solo router virtual ante los host de la LAN. Se elige un solo router del grupo para enrutar el tráfico enviado por los host hacia el router virtual, conociéndose a dicho router como el router maestro. Adicionalmente, también se elige a un segundo router llamado router standby. En el caso que el router maestro fallase, el router standby asume todos los derechos del router maestro para enrutar el tráfico. El grupo de routers que trabaja bajo el protocolo HSRP puede ser de dos a mas, sin embargo el router maestro será el que enrute el trafico enviado al router virtual. Al configurarse el protocolo HSRP en un grupo de más de 2 routers, se envían mensajes periódicos hello entre el router maestro y el router standby. En el caso que el rouer standby asuma la función de maestro o en el caso que falle, un tercer router del grupo HSRP asume la función de router standby.

Los routers que ejecutan HSRP envían mensajes anunciándose mediante UDP por el puerto 1985 a la dirección multicast 224.0.0.2 (todos los routers). La dirección IP virtual

se asocia con una dirección MAC bien conocida con el formato 00:00:0C:07:AC:XX donde XX es el número de grupo que identifica a la IP virtual.

El protocolo HSRP actúa sobre la capa 3 del modelo OSI y administra las direcciones virtuales que identifican al router maestro.

El protocolo HSRP es muy similar al VRRP (Virtual Router Redundancy Protocol), el cual es un protocolo no propietario definido en la RFC 3168 y que fue creado posteriormente al protocolo HSRP de Cisco (5).

2.8.1 Configuración HSRP

Para entender la configuración del protocolo HSRP, primero revisemos como se configurarían los terminales IP en el caso de no utilizar el protocolo HSRP cuando la LAN tiene dos salidas para llegar a otras redes.

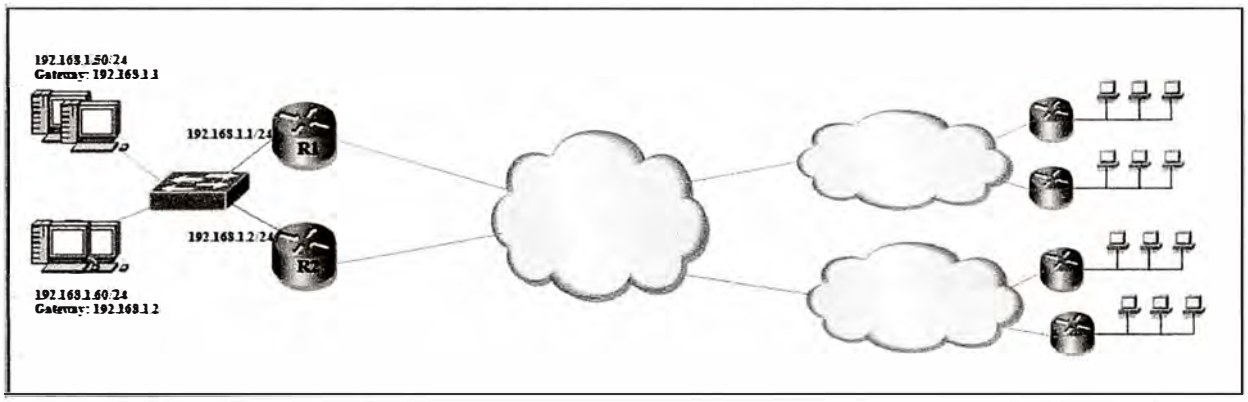


Fig.2.10 Topología sin uso de HSRP

En la Fig. 2.10 notamos que, si queremos configurar las PCs cuando existen dos Gateways, tendríamos que dividir las PCs en dos grupos y asignar un Gateway diferente a cada grupo. Este tipo de configuración, sin lugar a dudas funcionara, sin embargo presenta las siguientes debilidades:

- En el caso que cualquiera de los routers R1 o R2 fallase, todo el grupo de PCs que apunta hacia el router fallado se quedaría fuera de red, es decir no es tolerante a fallas.
- La carga administrativa es muy elevada debido a que se debe tener un registro exacto del número de PCs conectado a cada router.

Para solucionar las debilidades antes mencionadas, se presenta el protocolo HSRP. En la Fig. 2.11 se ha configurado el protocolo HSRP en los routers R1 y R2, de tal manera que cualquier PC de la LAN apuntara a la dirección IP virtual asociado al protocolo HSRP.

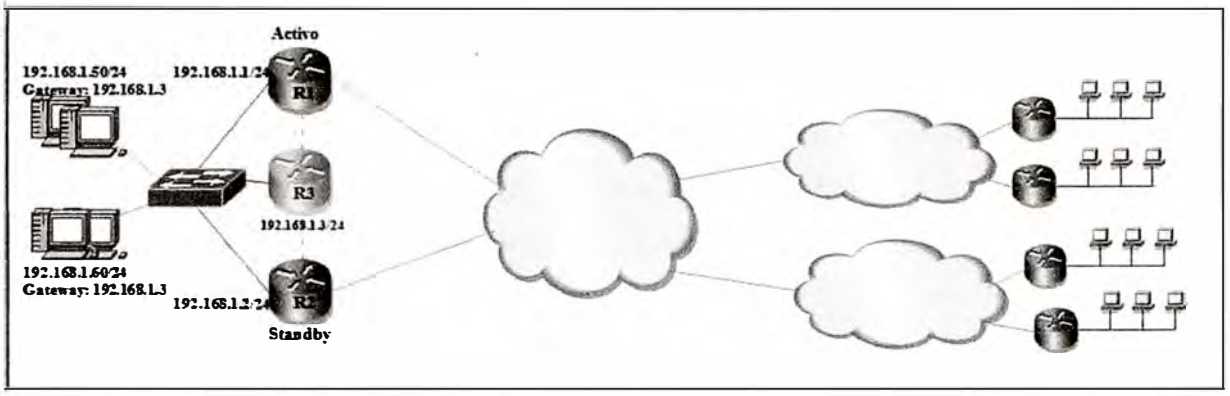


Fig. 2.11 Topología usando el protocolo HSRP

El comando a configurar en la interface para que el protocolo HSRP funcione es:

standby *numero_de_grupo* ip *direccion_ip_virtual*

Si solo el comando anterior está configurado, el router activo será aquel router que se configure primero, sin embargo existe un atributo en el protocolo HSRP que se llama prioridad. Con el atributo prioridad definimos el router activo y el router standby. La prioridad por defecto en los routers al momento de configurar el HSRP es 100. El comando a configurar para definir la prioridad es:

standby *numero_de_grupo* priority *numero_de_prioridad*

Si el protocolo HSRP está funcionando con el atributo de prioridad por defecto y se configura una prioridad mayor en el router standby, no habrá ningún cambio en la red debido a que el protocolo HSRP no está configurado para reemplazar el router activo a menos que este falle. Para lograr reemplazar el router activo, debemos configurar el comando preempt de la siguiente manera:

standby *numero_de_grupo* preempt

En el caso que los routers del grupo HSRP tengan la misma prioridad, el router activo será aquel que tenga la IP más alta del grupo.

La configuración de los routers R1 y R2 de la Fig. 2.11 es:

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#standby 1 ip 192.168.1.3
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#standby 1 ip 192.168.1.3
R1(config-if)#standby 1 priority 101
R1(config-if)#standby 1 preempt
```

2.9 Cuantificación de la disponibilidad de una red de comunicaciones.

La cuantificación de una red de comunicaciones ha sido revisada en múltiples recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), de las cuales nos basamos para lograr cuantificar el nivel de disponibilidad en una Red de Alta Disponibilidad. Las recomendaciones de la UIT referentes a la disponibilidad de redes son:

G.827 (09/03) Parámetros y objetivos de disponibilidad para trayectos digitales internacionales de extremo a extremo de velocidad binaria constante.

G.911 (04/97) Parámetros y metodología de cálculo de la fiabilidad y la disponibilidad de los sistemas de fibra óptica.

Y.1540 (12/02) Servicio de comunicación de datos con protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes de protocolo Internet.

Y.1540 Enmienda 1 (08/03) Nuevo apéndice VIII: Fundamentos de la disponibilidad de servicio IP.

X.137 (08/97) Valores de disponibilidad para redes públicas de datos que prestan servicios internacionales de conmutación de paquetes.

X.147 (10/03) Disponibilidad de las redes con retransmisión de trama

X.147 Enmienda 1 (04/04) Especificación de las valores de los objetivos de disponibilidad.

Y.1561 (05/04) Parámetros de calidad de funcionamiento y disponibilidad para redes con conmutación por etiquetas multiprotocolo.

Para definir donde podemos cuantificar la disponibilidad, nos basaremos en un modelo genérico de transporte MPLS compuesto de secciones de red y enlaces de central que interconectan secciones de red. Bajo este modelo, podremos identificar las secciones en las cuales es aplicable el concepto de disponibilidad.

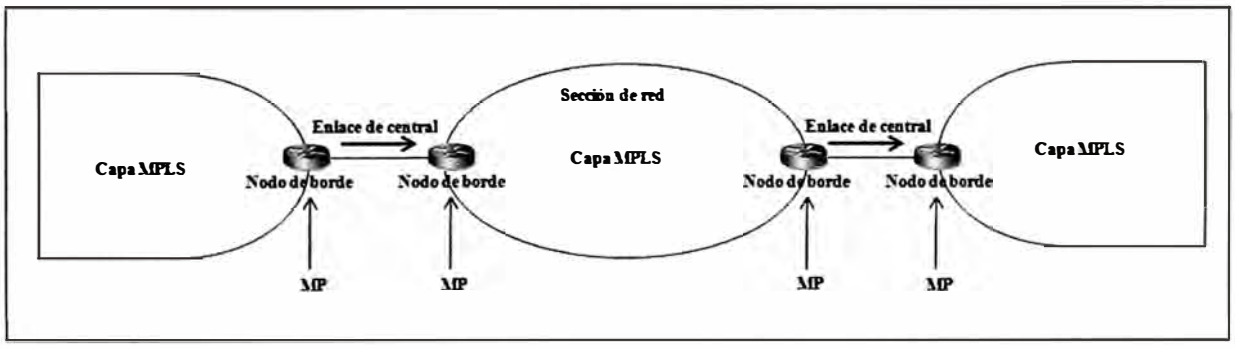


Fig. 2.12 Modelo genérico de transporte MPLS

En la Figura 2.12 se muestra el diagrama de funcionamiento del modelo genérico de transporte MPLS. En dicha figura podemos encontrar los MPs que son los Puntos de Medición donde podemos cuantificar la disponibilidad. Adicionalmente a estos Puntos de Medición, definiremos los demás elementos de acuerdo a la recomendación UIT-T Y.1561:

Enlace de central (EL, exchange link): Enlace que conecta el router de origen o destino con su router adyacente, que puede estar en otra jurisdicción, al que a veces se alude como un enlace de acceso, enlace de ingreso o enlace de egreso. También es el enlace que conecta el router en una sección de red con un router en otra sección de red. Se observa que la responsabilidad del enlace de red, su capacidad, y su calidad de funcionamiento suelen estar compartidas entre las partes componentes.

Sección de red (NS, network section): Conjunto de nodos MPLS con todos sus enlaces que los interconectan formando la totalidad o parte de la red MPLS entre un nodo de ingreso y un nodo de egreso, estando bajo una sola responsabilidad jurisdiccional. Algunas secciones de red consisten en un solo anfitrión sin ningún enlace de interconexión. La NS de origen y la NS de destino son casos particulares de secciones de red. Los pares de secciones de red son interconectadas por enlaces de central.

Punto de medición (MP): Demarcación entre un router o nodo de borde MPLS y un enlace adyacente en la que pueden observarse y medirse eventos de referencia de calidad de funcionamiento. Una sección o una combinación de secciones es mensurable si está limitada por un conjunto de MP.

Sección básica: Las secciones básicas están delimitadas por MP. La calidad de funcionamiento de cualquier EL o NS es mensurable con relación a cualquier red MPLS unidireccional de extremo a extremo. Los MP de ingreso son el conjunto de MP atravesados por paquetes de una FEC cuando entran en una sección básica. Los MP de egreso son el conjunto de MP atravesados por paquetes de esa FEC cuando salen de una sección básica.

Transporte MPLS de extremo a extremo en un trayecto conmutado por etiqueta: Conjunto de EL y NS que proporcionan el transporte de paquetes transmitidos de nodo de borde MPLS a nodo de borde MPLS en una red MPLS. Los MP que delimitan la red MPLS de extremo a extremo son los MP en el nodo de ingreso del primer dominio MPLS y el nodo de egreso del último dominio MPLS que forman el trayecto conmutado por etiqueta (LSP).

La calidad de funcionamiento de la red MPLS de extremo a extremo es mensurable con relación a cualquier trayecto unidireccional conmutado por etiqueta. Los MP de ingreso son los MP atravesados por paquetes de una FEC (*forwarding equivalence class*) cuando entran en el LSP. Los MP de egreso son los MP atravesados por paquetes de esa FEC cuando salen de ese LSP.

Ensamblado de secciones de red (NSE, network section ensemble): Por un NSE ha de entenderse a cualquier subconjunto de NS conectadas conjuntamente, con todos los EL que las conectan. El término NSE puede utilizarse para hacer referencia a una sola NS, dos NS, o cualquier número de NS y los EL que las conectan. Pares de NSE distintos se conectan por enlaces de central. El término NSE puede utilizarse también para representar el transporte MPLS completo de extremo a extremo. Los NSE están delimitados por MP. La calidad de funcionamiento de cualquier NSE es mensurable con relación a cualquier trayecto unidireccional conmutado por etiqueta proporcionado por el NSE. Los MP de ingreso son el conjunto de MP atravesados por paquetes de un servicio cuando entran en un NSE. Los MP de egreso son el conjunto de MP atravesados por paquetes de ese servicio cuando salen de ese NSE. Los MPs no solo sirven para medir la disponibilidad, sin embargo este parámetro es el producto más relevante del estudio de los eventos que acontecen en los MPs. En la Fig. 2.13 podemos ver la correlación de los eventos y recomendaciones dadas en los MPs, los cuales finalizan en la disponibilidad o no del NSE.

La disponibilidad del servicio MPLS es aplicable al servicio de extremo a extremo, secciones básicas y NSE. La función de disponibilidad sirve para clasificar el tiempo total de servicio calendarizado para un servicio MPLS en periodos disponibles y no disponibles (o indisponibles). Sobre la base de esta clasificación se definen la disponibilidad porcentual de la MPLS y la indisponibilidad porcentual de la MPLS. Por último, sobre la base de un modelo de servicio MPLS con dos estados, se definen parámetros de disponibilidad conexos.

NOTA – A menos que el proveedor de servicio indique otra cosa, se supone que el tiempo de servicio calendarizado para el servicio MPLS es 24 horas al día, siete días a la semana.

La disponibilidad puede medirse en la utilización de los siguientes servicios:

Servicios interactivos de gran volumen basados en paquetes, en los que una suspensión de la transferencia de paquetes puede hacer que el equipo del cliente intente el restablecimiento utilizando redes alternas.

- Servicios de transferencia de paquetes con conexión.
- Aplicaciones en tiempo real basadas en flujo continuo, como voz y vídeo.

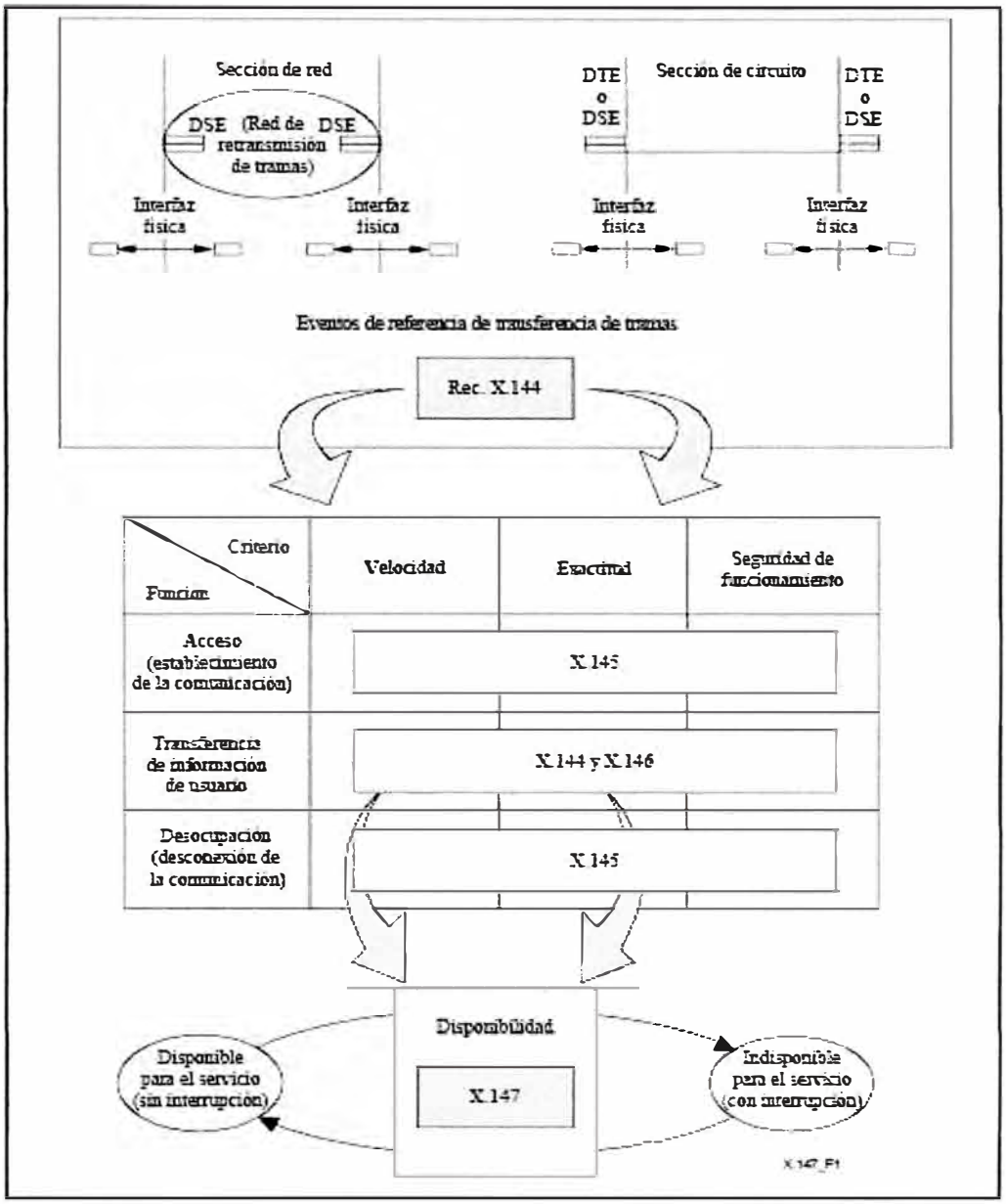


Fig. 2.13 – Correlación de eventos para definir la disponibilidad

Se ha observado que, incluso en las redes de transferencia de paquetes sin conexión, una fracción del tráfico total puede ser tráfico con conexión. Por tanto, se ha definido una sola función de disponibilidad.

2.9.1 Función de disponibilidad para servicios con conexión

Los servicios con conexión requieren una mayor continuidad de la transferencia de paquetes que otros servicios de paquetes. Se produce un resultado de graves pérdidas de

bloques de paquetes (SLB, severe loss block) con respecto a un bloque de paquetes observados durante un intervalo de tiempo Tlb = s en un MP0 de ingreso cuando la razón de los paquetes perdidos en MPi de egreso al número total de paquetes en el bloque es superior a s1 = 0.15 (valor del umbral de pérdida). En la evaluación de bloques (intervalos de tiempo) sucesivos no debe haber superposiciones.

Con relación a un determinado par de nodos de ingreso y egreso MPLS, la disponibilidad de una sección básica o un NSE en el caso de ingreso específico, se evalúa de la manera siguiente:

La indisponibilidad comienza cuando se producen diez SLB consecutivos. Estos diez segundos forman parte del tiempo indisponible. Un periodo de indisponibilidad termina cuando transcurren diez segundos consecutivos, ninguno de los cuales es SLB. Estos diez segundos forman parte del tiempo disponible. Los criterios de diez segundos son soportados mediante una ventana deslizante con una granularidad de un segundo. Cuando determinamos el intervalo de tiempo Tlb = 1seg, el SLB se convierte en un evento de segundo con muchos errores (SES, *severely errored second).* En la Figura 2.14 podemos observar mejor como se determina la disponibilidad o indisponibilidad.

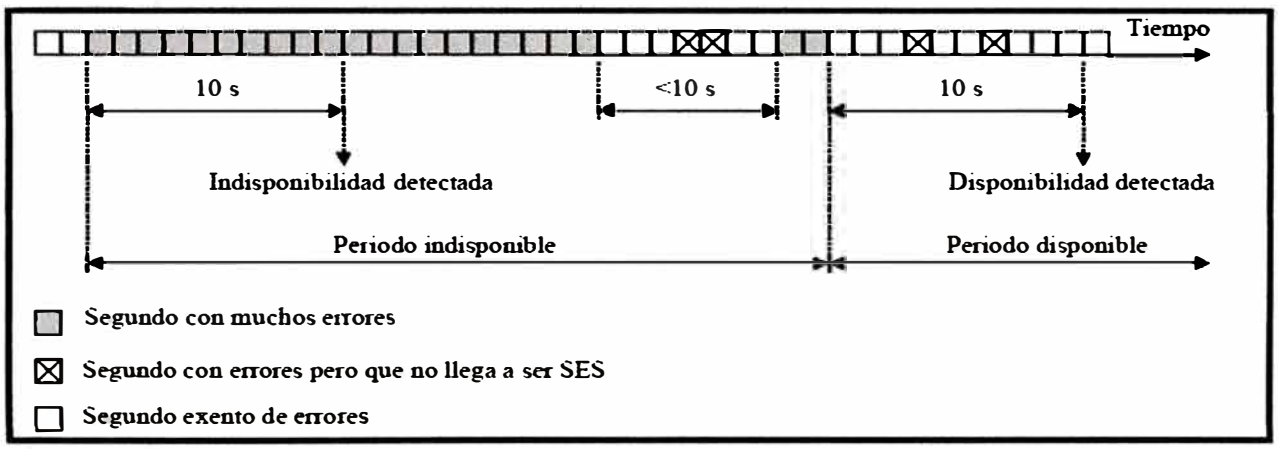


Fig. 2.14 Determinación de periodos disponibles e indisponibles.

2.9.2 Porcentaje de indisponibilidad del servicio MPLS (PIU, percent MPLS service unavailability)

Porcentaje del total de tiempo de servicio calendarizado que se caracteriza como indisponible mediante la función de disponibilidad de la MPLS. Los porcentajes de indisponibilidad se suelen medir anualmente para dimensionar el tiempo de servicio mínimo que espera el usuario.

2.9.3 Porcentaje de disponibilidad del servicio MPLS (PIA, percent MPLS service availability)

Porcentaje del total de tiempo de servicio calendarizado que se caracteriza como disponible mediante la función de disponibilidad de la MPLS.

$$\mathbf{PIU = 100 - PIA} \qquad \mathbf{(2.1)}$$

NOTA – Dado que, típicamente, la tasa de pérdida de paquetes (packet loss ratio – PLR) aumenta cuando aumenta la carga ofrecida de la fuente al destino, la probabilidad de que se rebase el umbral s1 aumenta cuando aumenta la carga ofrecida. Por tanto, es probable que los valores PIA sean menores cuando aumente la demanda de capacidad entre la fuente y el destino.

2.9.4 Definición del estado de disponibilidad/indisponibilidad

En este punto definiremos las causas para determinar si el enlace está disponible o no, de acuerdo a los siguientes hechos:

A La sección de conexión virtual (o conjunto de secciones contiguas) podrá considerarse indisponible si la capa física subyacente en cualquier frontera de sección está indisponible (no hay señal, condición de alarma, etc.) debido a causas propias de la(s) sección(es) de conexión. Es decir, si la conexión virtual con retransmisión de tramas no puede transferir tramas debido a una capa física indisponible, la conexión se considera indisponible. Ese fallo de capa física evitará la transmisión de tramas en la porción de conexión durante el periodo de tiempo considerado, si el usuario trata de transmitir tramas. Una interrupción corresponde a un fallo que se produce dentro de la porción de conexión, ya sea de la capa física o de la capa de retransmisión de tramas.

B Desde el punto de vista de la calidad de transmisión, la sección de conexión (o conjunto de secciones) puede considerarse indisponible si cualquiera de los parámetros de calidad de funcionamiento como tasa de pérdida de tramas, tasa de errores de trama residuales o tasa de tramas extra rebasan un umbral predeterminado. En la Tabla 2.1 se muestra los parámetros de calidad de funcionamiento.

C Desde el punto de vista de la precisión/fiabilidad, la sección de conexión (o conjunto de secciones) puede considerarse indisponible si cualquiera de los siguientes parámetros: probabilidad de error en el establecimiento de la comunicación (CEP, *connection set-up error probability*), probabilidad de fallo en el establecimiento de la comunicación (CFP, *connection set-up failure probability*), probabilidad de desconexión prematura (PDP, *premature disconnect probability*) y probabilidad de estímulo de

desconexión prematura (PDSP, *premature disconnect stimulus probability*) rebasan un umbral predeterminado. En la Tabla 2.1 se muestra los valores umbrales de los parámetros probabilísticos indicados anteriormente.

Tabla 2.1 – Parámetros de calidad de funcionamiento y valores umbrales

Parámetros de decisión de disponibilidad	Criterios de interrupción
Probabilidad de fallo en el establecimiento de la comunicación (cfp) Probabilidad de error en el establecimiento de la comunicación (cep)	(cfp + cep) > 0.9
Capacidad de caudal (tc)	tc < 80 bit/s
Tasa de errores residuales (rer)	rer > 10^{-3}
Probabilidad de reiniciación (rp) Probabilidad de estímulo de reiniciación (rsp_1, rsp_2)	(rsp_1 + rp + rsp_2) > 0.015
Probabilidad de desconexión prematura (pdp) Probabilidad de estímulo de desconexión prematura ($pdsp_1$, $pdsp_2$)	($pdsp_1$ + pdp + $pdsp_2$) > 0.01

2.9.5 Tiempo medio entre interrupciones del servicio

El tiempo medio entre interrupciones del servicio (MTBSO) es la duración promedio de cualquier intervalo continuo durante el cual está disponible la sección de conexión virtual o el conjunto de secciones concatenadas. El MTBSO se define como la duración promedio de los periodos continuos de tiempo de disponibilidad. El MTBSO también puede llamarse MTBF (tiempo medio entre fallas).

2.9.6 Tiempo medio hasta el restablecimiento del servicio

El tiempo medio hasta el restablecimiento del servicio (MTTSR) es la duración promedio de los intervalos de tiempo de servicio de indisponibilidad. El MTTSR también puede llamarse MTTR (Tiempo medio para reparar).

2.9.7 Modelo básico de disponibilidad y relación de parámetros.

Usualmente se utiliza los parámetros MTTR y MTBF para definir la disponibilidad o indisponibilidad, en la Fig. 2.15 se complementa estos conceptos con sus valores reales en el diagrama de estados disponible/indisponible. Adicionalmente, se aclaran los siguientes conceptos que se están usando:

Tasa de fallos (λ) es el número promedio de transiciones del estado de disponibilidad al estado de indisponibilidad por unidad de tiempo disponible;

Tasa de restablecimiento (μ) es el número promedio de transiciones del estado de indisponibilidad al estado de disponibilidad por unidad de tiempo de indisponibilidad;

Indisponibilidad (U) es la relación del tiempo de servicio de indisponibilidad de largo plazo al tiempo de servicio programado, expresada como un porcentaje. Este concepto también es conocido como PIU (porcentaje de indisponibilidad del servicio).

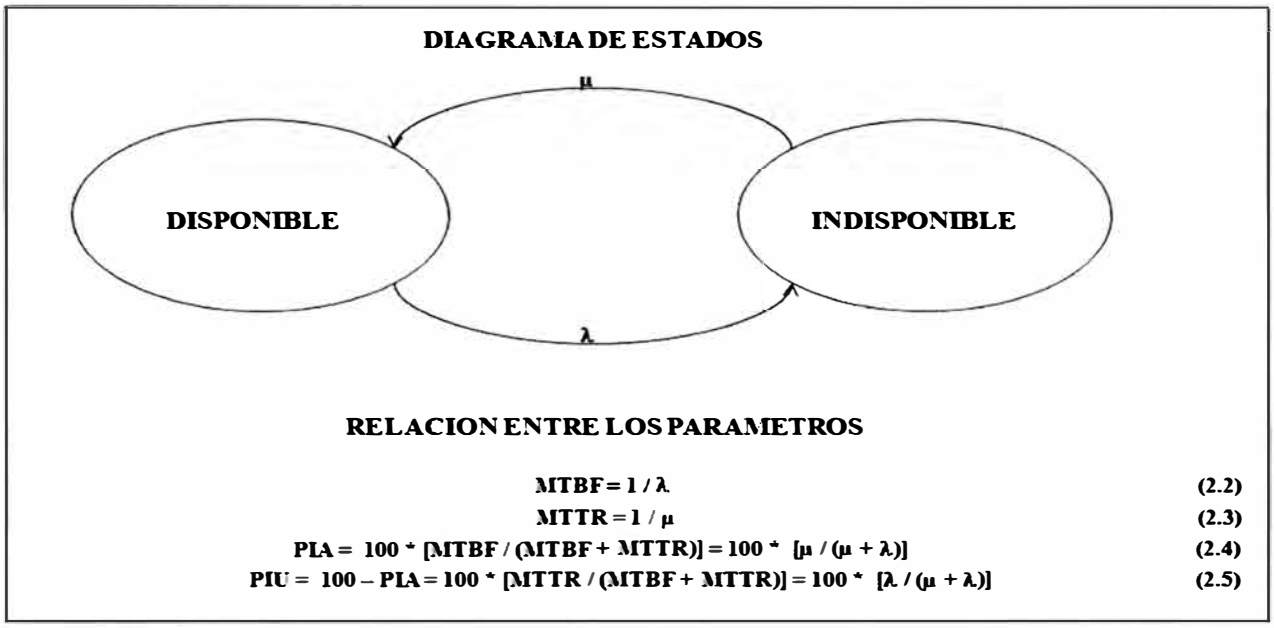


Fig. 2.15 – Modelo básico de disponibilidad y relaciones entre los parámetros

2.9.8 Determinación de la disponibilidad de un NSE (Ensamblado de Secciones de Red) en base a la disponibilidad de Secciones Básicas que lo componen

Nos basaremos en dos topologías básicas para determinar la disponibilidad total de una red cuando se conoce la disponibilidad por tramos de dicha red. En base a estas topologías podemos encontrar la disponibilidad de topologías mixtas o más complejas.

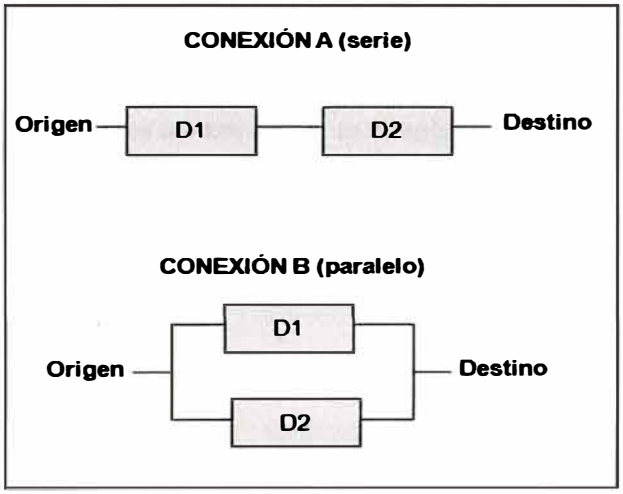


Fig. 2.16 – Topologías básicas para encontrar la disponibilidad resultante

En la Fig. 2.16 se muestra las topologías básicas en donde debemos encontrar la disponibilidad resultante.

La disponibilidad resultante en la conexión A (serie) es:

$$D = D1 \times D2 \quad (2.5)$$

La disponibilidad resultante en la conexión B (paralelo) es:

$$D = 1 - (1 - D1) \times (1 - D2) \quad (2.6)$$

2.9.9 Valores de disponibilidad mínimos de acuerdo a la UIT

De acuerdo a la recomendación UIT-T X.147 (2003) – Enmienda 1, las disponibilidades para tramos nacionales e internacionales tienen un límite inferior, el cual siempre debe ser cumplido por los operadores de telecomunicaciones. En la Fig. 2.16 se muestra estos valores mínimos de disponibilidad.

Estos valores de disponibilidad rigen para la nube de los operadores, es decir para su red troncal hasta los POPs de acceso, no se incluye la red de acceso ni el equipamiento de ultima milla de la sede remota, sin embargo debido a la competencia existente, muchos operadores ofrecen disponibilidades mayores a las indicadas en la Tabla 2.2.

Tabla 2.2 – Objetivos de disponibilidad

Sección o porción de conexión	Objetivo de la tasa de disponibilidad
Sección de circuito de acceso	(con arreglo a la Rec. UIT-T G.827)
Porción de conmutación de red nacional	99,98%
Porción de red de tránsito internacional	99,98%
Porción entre operadores internacionales	(con arreglo a la Rec. UIT-T G.827)
NOTA – Todos los objetivos de disponibilidad de la sección o porción de red son provisionales y no es necesario que las redes los cumplan hasta que se corrija (aumentándolos o disminuyéndolos) basándose en la experiencia de funcionamiento real. NOTA – Se sabe que una determinada conexión virtual individual puede no satisfacer los objetivos de calidad de funcionamiento cuando se evalúa durante periodos cortos, por ejemplo un mes. Ahora bien, los operadores de red tratarán por todos los medios de que se cumpla el objetivo de disponibilidad a largo plazo de una conexión virtual particular.	

CAPITULO III
DISEÑO DE UNA RED DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS

3.1 Entidades con servicios centralizados

En la actualidad existen múltiples empresas que disponen de servicios centralizados, lo cual implica disponer de una sede principal que centralice todos los servicios para todas las sedes remotas. Dependiendo del servicio que presten, podemos definir distintos tipos de entidades, tales como entidades bancarias, de servicios o industria. Es importante saber el negocio al cual está dedicado la empresa a la cual se le implementara la red de alta disponibilidad, debido a que la Alta Disponibilidad es la capacidad de definir, alcanzar y mantener los objetivos de disponibilidad del destino a través de los servicios y/o tecnologías de apoyo en la red que se alinean con los objetivos de la empresa. En los siguientes dos ejemplos revisaremos que los parámetros de Alta Disponibilidad varían de acuerdo al tipo de negocio de la empresa:

Caso 1: Para una entidad bancaria son muy críticas sus comunicaciones con su base de datos de tarjetas de crédito ya que en 1 minuto de caída de dicho servidor puede representar miles de soles en pérdidas para la empresa por la alta demanda en el uso de dicho servidor las 24 horas del día.

Caso 2: Para una entidad industrial (como una empresa minera) puede no ser tan crítica la caída en una base de datos de sus clientes ya que las transacciones con dicha base de datos pueden ejecutarse cada cierto periodo de tiempo y no en forma continua las 24 horas del día.

En la Tabla 3.1 podemos ver los distintos porcentajes de disponibilidad anuales y el tiempo de baja del servicio que estos representan. Para el Caso 1, un nivel de disponibilidad adecuado es 99.999% mientras que para el Caso 2 un nivel de disponibilidad de 99.950% será suficiente.

En el presente documento se trabajará en alcanzar un nivel de disponibilidad de 99.999% anual, con lo cual podremos indicar que tenemos una red de Alta Disponibilidad. Para comprobar esta disponibilidad nos basaremos en datos reales de disponibilidad de los

Proveedores de Servicios de Telecomunicaciones presentes en el Perú. En este capítulo diseñaremos una red de Alta Disponibilidad, empezando con una sola sede remota, la cual se replicará en las demás sedes remotas siguiendo un ordenamiento de acuerdo al direccionamiento IP asignado estas sedes, por lo tanto este diseño es válido para cualquier empresa que disponga de una o de muchas sedes remotas.

Tabla 3.1 Disponibilidad vs Tiempo de caída del servicio al año

Disponibilidad	Corte de Servicio por Año		
99.0000%	3 Días	15 Horas	36 Minutos
99.5000%	1 Día	19 Horas	48 Minutos
99.9000%		8 Horas	46 Minutos
99.9500%		4 Horas	23 Minutos
99.9900%			53 Minutos
99.9990%			5 Minutos
99.9999%			30 segundos

3.2 Características de diseño para lograr una red de alta disponibilidad

Para elaborar el diseño de la red de alta disponibilidad debemos definir los conceptos que nos permiten conseguir ello. Estos conceptos deben cumplirse para poder conseguir una disponibilidad mayor a los "5 nueves", es decir 99,999%.

3.2.1 Redes redundantes de acceso

El acceso de red se refiere al acceso físico con la cual se accede a cualquier red de datos. El acceso físico es la ruta de la fibra óptica desde el punto de acceso a la nube MPLS (POP de acceso) hasta el local donde se ubica la sede (remota o principal). Esta ruta es diseñada de acuerdo a los planos existentes de la ciudad y su ejecución esta normada por los reglamentos propios de dicha ciudad. En el caso de Lima, la ejecución de los trabajos para el acceso de red debe ser aprobada tanto por la Municipalidad Local como la Municipalidad Central (Lima Metropolitana).

En la Fig. 3.1 y 3.2 se muestran 2 planos de acceso interno y externo, el cual nos muestra la ruta física que sigue la fibra óptica desde el POP de acceso hasta nuestro CPE de acceso. Para obtener una alta disponibilidad, debemos asegurarnos que existan 2 rutas distintas tanto externa como interna para reducir las posibilidades de corte de servicio por rotura de la fibra en algún punto de la ruta. En una red de Alta Disponibilidad debemos manejar el concepto activo/standby, el cual se logra tendiendo redes de acceso redundantes

durante todo el trayecto desde el POP de acceso hasta el CPE de acceso ubicado en la Sede Principal (o sede remota).

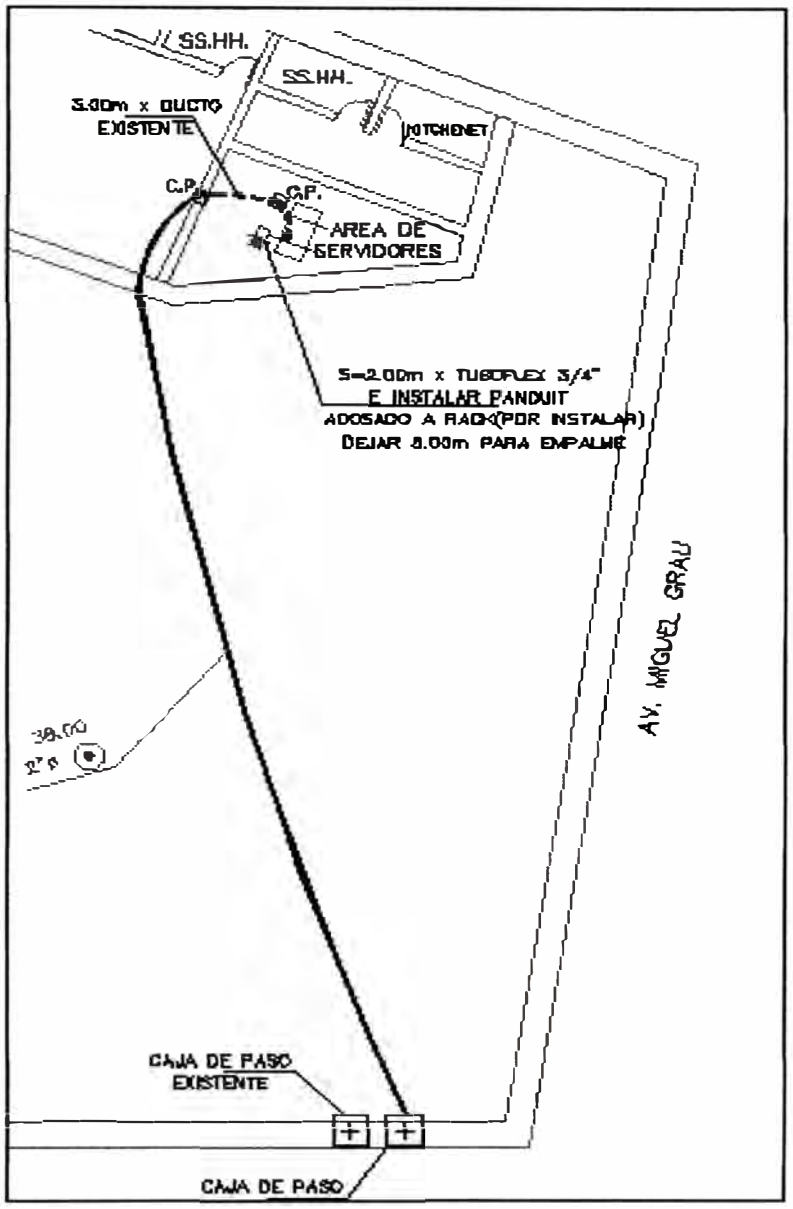


Fig. 3.1 Plano de acceso interno

Las redes de acceso redundantes se refieren a dos redes de fibra óptica con trayectos distintos en todos sus puntos, como la mostrada en la Fig. 3.3, con lo cual se logra asegurar que en caso ocurra un desastre en algún punto de una de sus rutas, el otro enlace tomara la posta del servicio manteniéndolo activo. Dentro de la sede (remota o principal) también se debe asegurar una ruta de fibra distinta y así evitar puntos de falla comunes a los dos accesos.

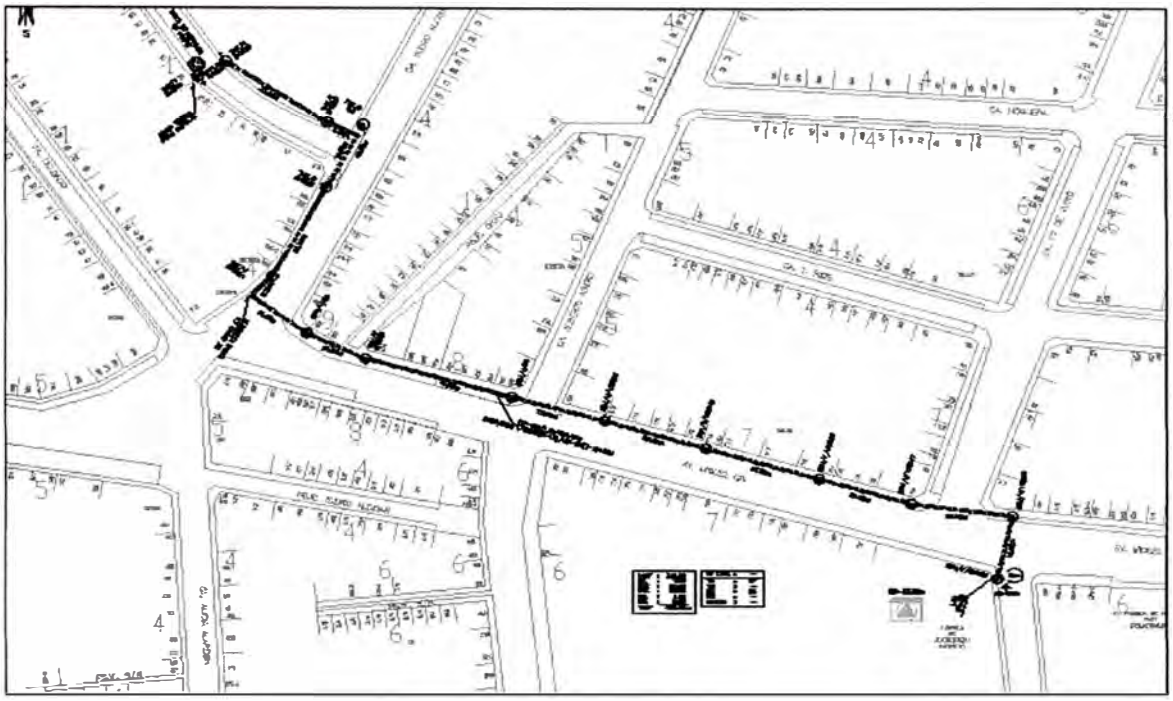


Fig. 3.2 Plano de acceso externo

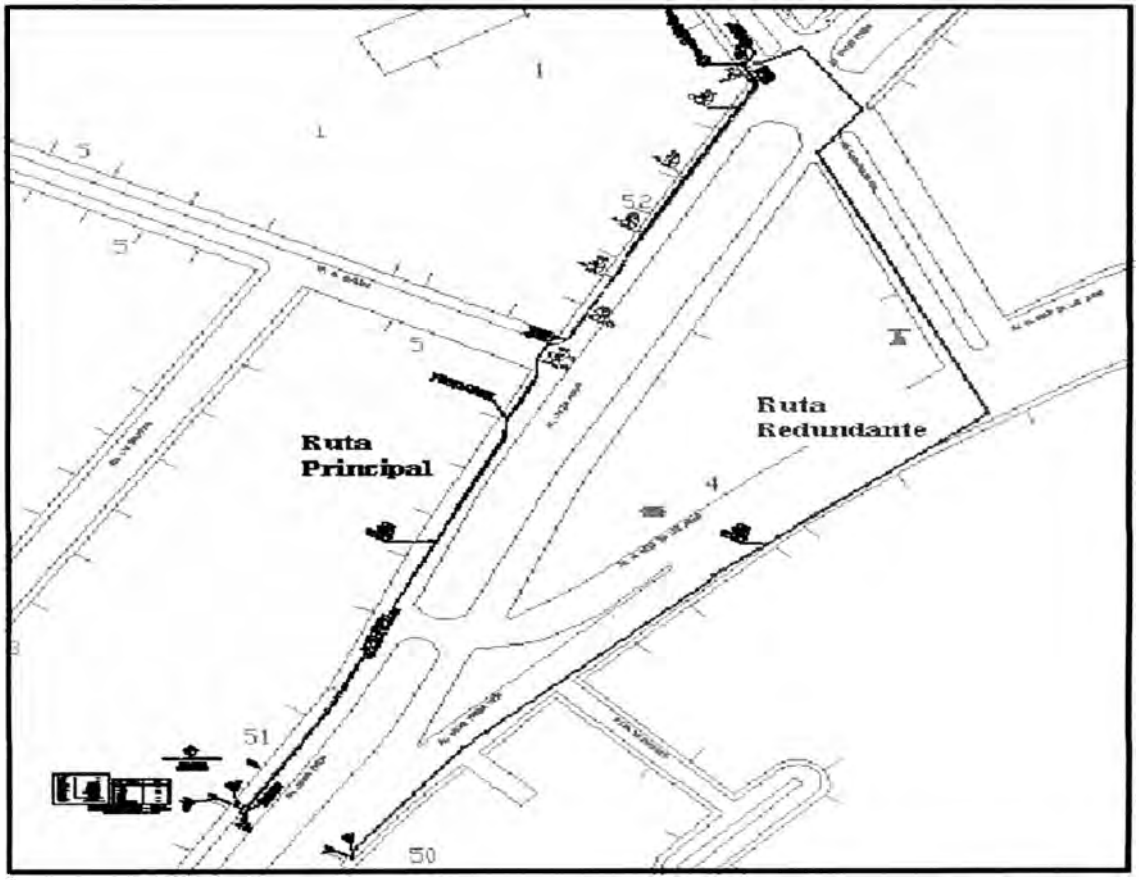


Fig. 3.3 – Planos de acceso externo principal y redundante

3.2.2 Hardware redundante

El hardware utilizado en la implementación de una red de alta disponibilidad debe cumplir con los siguientes lineamientos para conseguir y mantener una alta disponibilidad:

- Redundancia activo/standby para conmutar la carga en caso ocurra fallas.
- Redundancia de fuente de poder para soportar distintas líneas de alimentación eléctrica.
- Soporte de cambios o mejoras "en caliente".

El hardware a implementar en las sedes remotas y en la sede principal son:

- Convertidor de medio administrado
- Router de acceso
- Switches de interconexión (sede principal solamente)

El diseño topológico que debemos seguir en la sede principal es la que se muestra en la Fig. 3.3, en donde se ve la redundancia de la red de acceso, el router de acceso y los switches de interconexión.

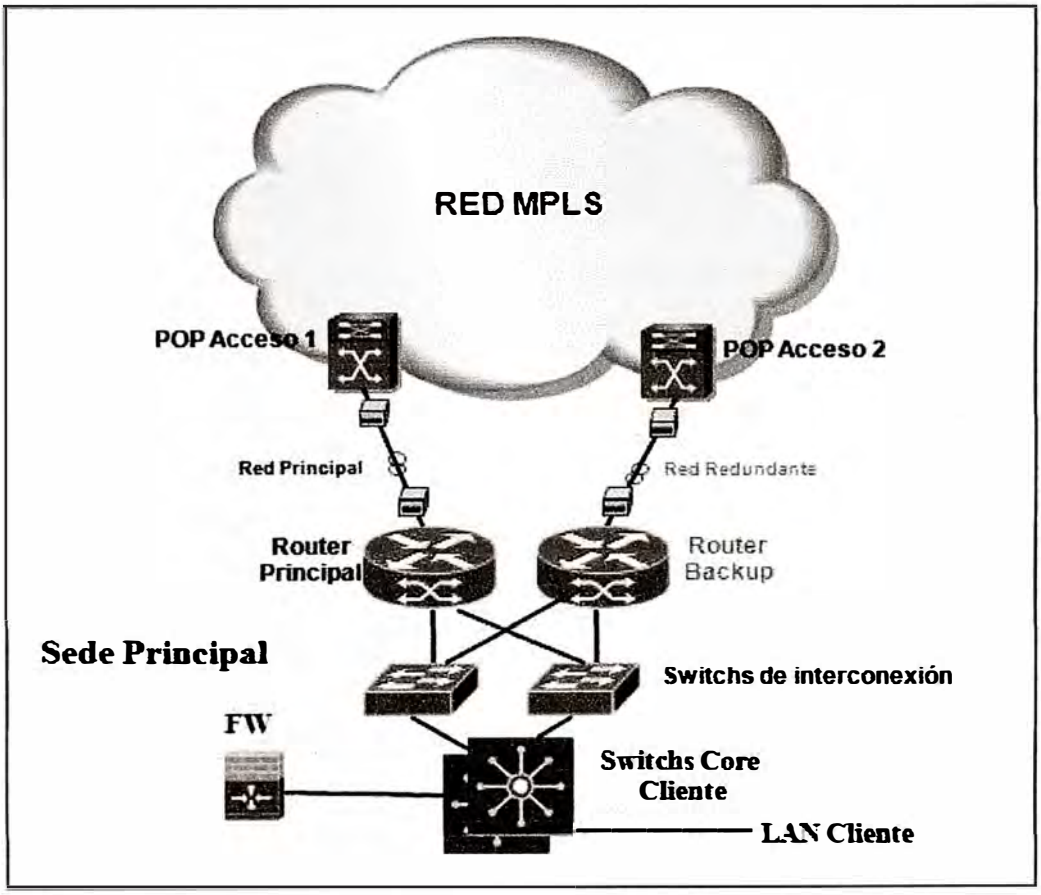


Fig. 3.4 – Topología de la Sede Principal

En las sedes remotas, dependiendo de su envergadura e importancia para el negocio de la empresa, podemos seguir un diseño topológico parecido al de la Fig. 3.4, sin embargo en nuestro caso consideramos que la topología de una sede remota es la indicada en la Fig. 3.5, cuya única diferencia con la Fig. 3.4 es la existencia de un solo switch de interconexión que usualmente es el switch LAN de la sede remota. Para el cálculo de la disponibilidad de la red no se considera el switch LAN ya que cumple funciones propias de un switch LAN de distribución, tal como la conexión de PCs.

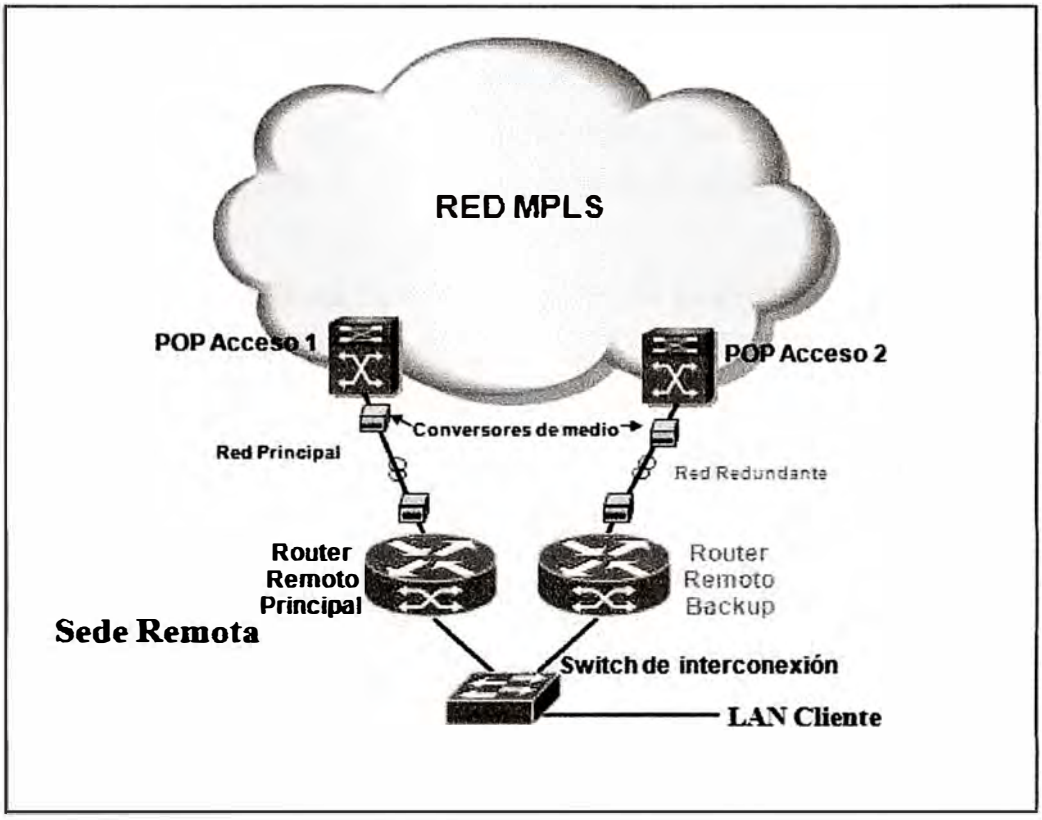


Fig. 3.5 – Topología de la Sede Remota

En las siguientes líneas entraremos en los detalles de cada uno de los componentes indicados anteriormente, manteniendo el objetivo de conseguir una red de alta disponibilidad.

3.2.2.1 Convertidor de medio administrado

El convertidor de medio administrado es el encargado de transformar la señal de un tipo de medio óptico a otro eléctrico y ser monitoreado remotamente. Para definir el tipo de convertidor a utilizar debemos conocer las características de la fibra óptica y la longitud de esta. En el mercado podemos encontrar distintas marcas para la elección del convertidor de

medio, de los cuales debemos tener especial cuidado en el tipo de conector para el lado de la fibra óptica (LC, SC, ST), ya que debemos adecuar la fibra óptica con el tipo de conector que soporte el convertidor de medio.

Debido a que este tipo de equipos no posee un sistema de redundancia, la única manera de conseguir un nivel básico de redundancia es poseer un stock mínimo de repuesto, los cuales deben ser configurados, probados y almacenados adecuadamente para reponerlos manualmente en caso de falla.

En la Tabla 3.2 se muestra algunos modelos de conversores de medio del fabricante americano Transitions Networks, los cuales pueden ser comparados con la Tabla 3.3 en donde se ven algunos modelos de conversores de medio del fabricante chino Raisecom. La elección de la marca adecuada, en caso tengamos las mismas prestaciones, deberá depender del tipo de soporte y reposición en caso de falla, así como el monto de la inversión.

Tabla 3.2 - Modelos de media converters Transitions Networks

Modelo	Descripción	Precio
CETTF1027-105	10Base-T to 10Base-FL Multimode 0-5 Kms RJ45/ST – Module	$300 + Costo Chasis ($450)
E-TBT-FRL-05(L)	MODEM, 10 Base T To 10 Base Fl Long Range Multimode Standalone 220 Vac 0-5 Kms	$350
E-TBT-FRL-05(SM)	Convertor, Ethernet 10 BTX to 10BFL standalone –Single mode 0-20 Kms	$380
E-100BTX-FX-05	100Base-TX to 100Base-FX Multimode 0-2kms (RJ45/ST) Standalone	$250
E-100BTX-FX-05(SM)	100Base-TX (RJ-45) to 100Base-FX 1300nm single mode (SC) (20 Kms)	$390

Tabla 3.3 – Modelos de media converters Raisecom

Modelo	Descripción	Precio
Conversor RC512-FE-M 1FE, MM2K	Media Converter FastEthernet Multimodo hasta 2 Kms	$100
Conversor RC512-FE-SS15/1FE,SM	Media Converter FastEthernet Monofibra 1550, hasta 25 Km	$180

3.2.2.2 Router de acceso

El router de acceso es el equipo principal en la red (remota o principal) ya que es donde se aplican las principales políticas de redundancia para acceder a la nube MPLS y conseguir la comunicación con otras sedes o la sede principal. Para definir el router que debemos usar es necesario conocer las siguientes características:

- Fuente de poder redundante (en la sede principal)
- Tipo de protocolos que soporta, por ejemplo: HSRP, VRRP, MPLS, IP QoS, BGP los cuales son los protocolos necesarios para implementar una red de alta disponibilidad.
- El ancho de banda, soportado bajo un escenario de configuración de todas las prestaciones indicadas en el punto 2.
- Soporta el cambio de tarjetas de expansión en caliente.
- Tipo de monitoreo y gestión del router.

En la actualidad existen básicamente 2 marcas de routers, cuyos modelos abarcan la totalidad del mercado empresarial (y sus distintas prestaciones y requerimientos) y estas son Cisco Systems y Juniper Networks, ambas empresas americanas.En la Tabla 3.4 se muestra las características de procesamiento, ancho de banda y conectividad de algunos modelos de routers de las marcas antes mencionadas.

Tabla 3.4 – Características del CPE para una red de datos

Equipo CPE	BW Soportado	DRAM	Flash	LAN integradas	Slots para tarjetas de expansión	Fuente de Poder Redundante	Soporta Terminación Voz
Cisco 871	5.0 Mbps	128 MB	28 MB	4-port 10/100 Mbps managed switch	No	No	No
Cisco 1841	8.0 Mbps	128 MB	32 MB	2-port 10/100 Mbps managed switch	Si	No	No
Cisco 2801	8.0 Mbps	128 MB	64 MB	2-port 10/100 Mbps managed switch	Si	No	Si
Cisco 2811	9.0 Mbps	256 MB	64 MB	No	Si	Externa	Si
Cisco 7600	132.0 Mbps	1G	512 MB	4-port 10/100/1000 Mbps managed switch	Si	Externa e Interna	Si
Juniper SRX-210B	50.0 Mbps	512 MB	1G	2-port 10/100/1000 Mbps and 8-port 10/100 Mbps	No	Externa	Si
Juniper SRX-210H	50.0 Mbps	1G	1G	2-port 10/100/1000 Mbps and 6-port 10/100 Mbps	No	Externa	Si
Juniper SRX-100B	47.0 Mbps	512 MB	1G	8-port 10/100 Mbps managed switch	No	No	No

3.2.2.3 Switch de interconexión

Los switches de interconexión en la sede principal sirven para darle mayor redundancia al enlace de datos, ya que anula la existencia de un solo punto de falla.

Implementar redundancia a nivel de switches en todas las sedes remotas incrementaría considerablemente el costo del proyecto y, teniendo en cuenta que cada sede remota depende solo de la sede principal, resulta innecesario desplegar redundancias en las sedes remotas, sin embargo podrían existir sedes remotas que si sea necesario implementar un nivel de redundancia similar a la sede principal. Por la razón antes indicada es que no se considera el switch de la sede remota en el cálculo da la disponibilidad de toda la red.

En la Fig. 3.4 observamos que es posible que se formen bucles entre cualquier router de acceso, los dos switches de distribución y el switch de core, por lo que es importante considerar que los switches de distribución que elijamos debe tener algún mecanismo de control que permita controlar la formación de bucles. El protocolo estándar para evitar la formación de bucles es 802.1d - Spanning Tree Protocol (STP), el cual permite activar o desactivar los puertos de los switches para evitar la formación de bucles. Existen variantes de este protocolo como el 802.1w - Rapid Spanning Tree Protocol (RSTP) o el 802.1s - Multiple-instance Spanning Tree (MST). También existen protocolos propietarios que también cumplen la misma función de evitar bucles, tales como:

Per-VLAN Spanning Tree Plus (PVST+): Protocolo propietario de Cisco, es la versión mejorada de Per-VLAN Spanning Tree (PVST). Este protocolo, además de mantener una instancia Spanning Tree por cada VLAN configurada en la red al igual que el PVST, es compatible con el protocolo libre 802.1q y con su similar propietario de Cisco (ISL) los cuales permiten compartir el mismo medio físico de manera transparente para múltiples redes.

Redundant Trunk Group (RTG): Protocolo propietario de Juniper, cuyo funcionamiento es parecido al RSTP pero sin la necesidad de configurarlo, lo cual es una de sus fortalezas (elimina la necesidad de configuraciones complejas del STP). (6)

3.2.3 Redes redundantes de energía

En el punto 3.2.2.2 se indica como la primera característica a considerar en la elección de un router que tenga fuente de poder redundante. Para que esta característica aporte efectivamente a la alta disponibilidad de la red es necesario que el datacenter en donde se encuentren los equipos posea más de una fuente de alimentación eléctrica.

En la Fig. 3.6 se muestra el diagrama de energía en el gabinete de la sede principal, debemos asegurarnos de cumplir ello para evitar puntos críticos de falla. De acuerdo a estudios realizados por empresas dedicadas a la comercialización de equipos eléctricos, el

arreglo mostrado en la Fig. 3.6 nos da una disponibilidad de energía de 99,999% siempre que estemos dentro del periodo de vida útil de los equipos de energía.

La energía es parte de la infraestructura inherente a la empresa, por lo que este documento solo ha delineado los requerimientos mínimos que debe cumplir para asegurar la alta disponibilidad de la red de datos, más no se estudiara su implementación por no se parte de la red de datos de alta disponibilidad. (7)

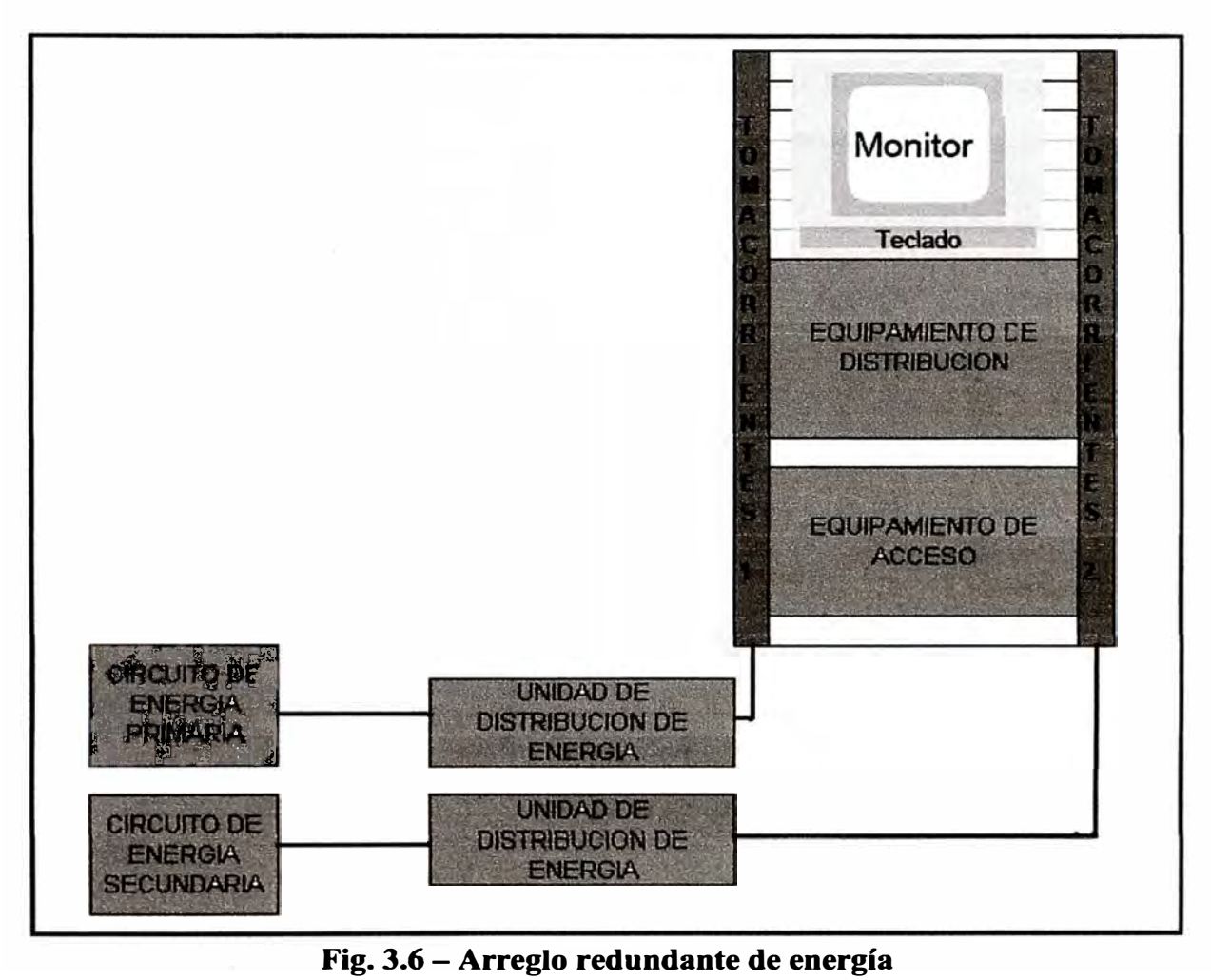


Fig. 3.6 – Arreglo redundante de energía

3.2.4 Sede de contingencia

En una red de datos de alta disponibilidad es importante contar con una sede de contingencia, la cual albergara equipamiento reflejo de la sede principal (servidores, routers, switches, etc). La naturaleza de muchos negocios obliga a implementar una sede de contingencia y, en caso ocurra algún siniestro con el local principal, todas las comunicaciones con las sedes remotas se mantendrán desde los equipos reflejados en la sede de contingencia.

Muchas empresas relacionadas al mundo de las telecomunicaciones se encargan de arrendar espacios en grandes centros de datos para albergar el equipamiento reflejo de los datacenters de sus clientes, por lo que implementar una sede de contingencia no necesariamente implica gastar dinero en construir un nuevo datacenter. Comercialmente se conoce como Housing el arrendar espacios de rack (en unidades de rack) con sus respectivos niveles de energía, aire acondicionado, temperatura y seguridad.

3.2.4.1 Conexión de fibra oscura

Para lograr un reflejo de todos los servidores de la Sede Principal se necesita un enlace de datos de alta capacidad entre la Sede Principal y la Sede Contingencia, el cual se logra a través de una conexión de fibra oscura entre las dos sedes.

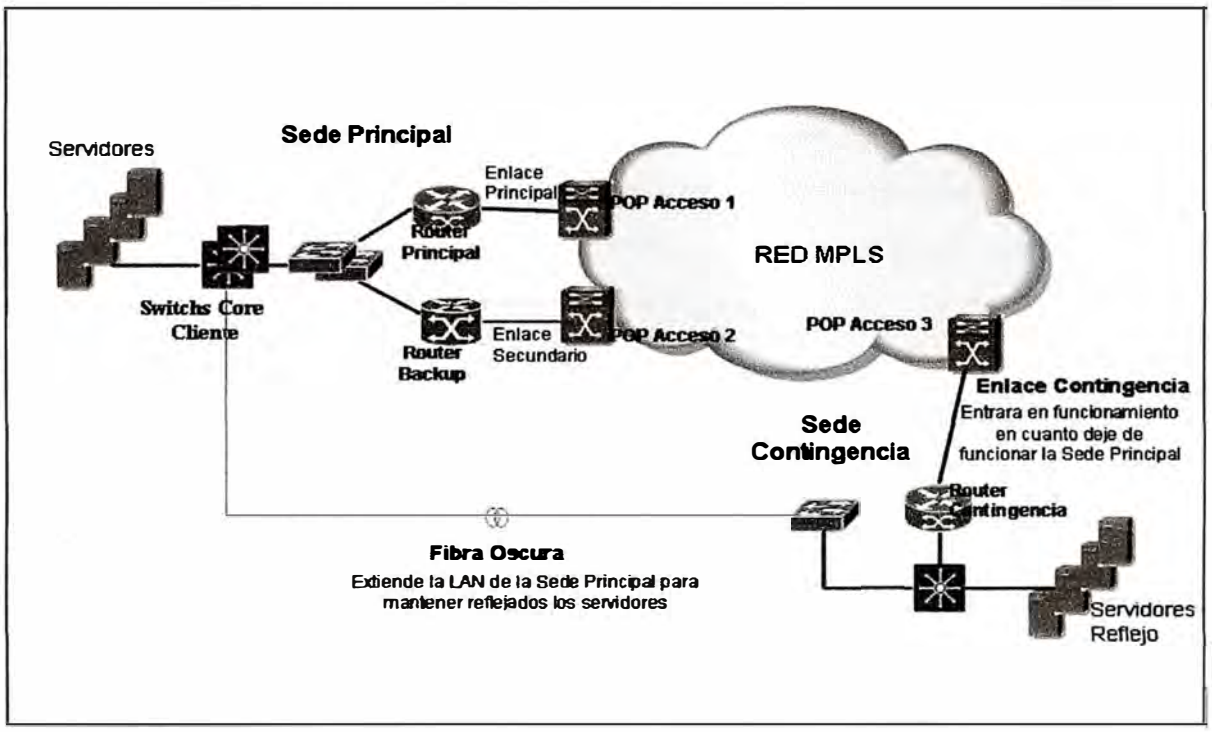


Fig. 3.7- Interconexión de la Sede Contingencia y la Sede Principal

El termino fibra oscura se origina de los hilos de fibra óptica que los operadores de telecomunicaciones no usaban por lo que podían alquilarlos a una empresa que lo solicite, sin embargo en la actualidad es parte del portafolio de servicios que brindan las empresas de telecomunicaciones pudiendo ejecutar trabajos exclusivos para habilitar un enlace de fibra oscura para un determinado cliente, con la restricción de darlo solo en los casos de interconexión de datacenters. La fibra oscura no es más que un enlace de fibra óptica entre 2 puntos, por lo que a los extremos podemos colocar 02 Switches con puertos de fibra y

habremos logrado extender la LAN de la Sede Principal hasta la Sede Contingencia para que los servidores de la Sede Contingencia estén actualizándose constantemente y sean siempre un reflejo de los servidores de la Sede Principal.

En la Fig. 3.7 se muestra la interconexión de la Sede Contingencia y la Sede Principal, en la cual se muestra que la fibra oscura sirve para actualizar la data de los servidores y el enlace de datos en la Sede Contingencia sirve para la operatividad de esta sede en caso falle todas las comunicaciones con la Sede Principal. La fibra oscura y el equipamiento que va conectado en los extremos forma parte de la LAN de la empresa, por lo que no es parte de la implementación que se describirá en el presente documento, sin embargo estamos delineando su necesidad para mantener los niveles de alta disponibilidad.

3.3 Diseño de las sedes Principal, Respaldo y Remotas de una red de alta disponibilidad

En una red de alta disponibilidad, es importante asegurarnos que la sede principal tenga una alta disponibilidad, lo cual se consigue con un arreglo de equipos y configuraciones que nos permitan mantener la continuidad de las operaciones en caso falle algún elemento de la red de acceso, así como la implementación de una sede de contingencia que albergue los espejos de todos los servidores de la empresa, tal cual se ha descrito anteriormente (8).

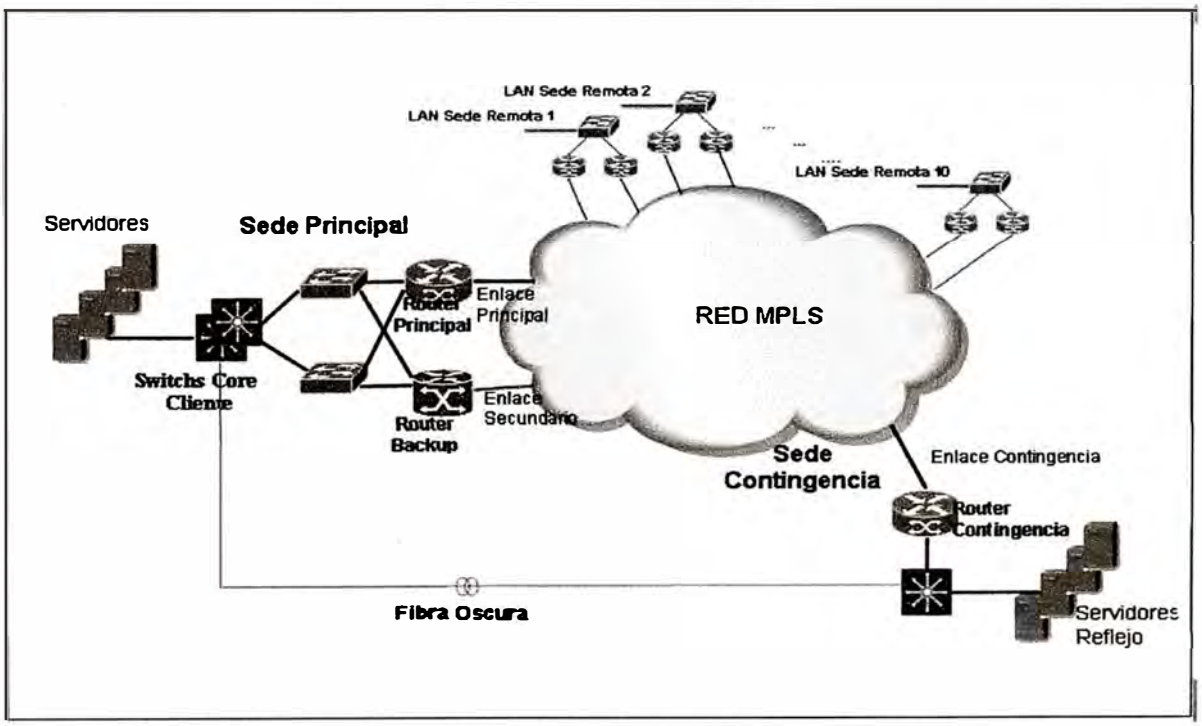


Fig. 3.8 Topología de la Sede Principal, respaldo y remotas.

En la Fig. 3.8 se muestra la topología a utilizar en la sede principal, respaldo y remotas de la red de alta disponibilidad.

En este punto empezaremos comprobando la disponibilidad de nuestra topología, definiremos el ancho de banda para cada una de las sedes, el tipo de router y switch que se implementara en las sedes principal, contingencia y remotas, así como los protocolos que debemos configurar.

3.3.1 Cuantificación de la disponibilidad

La disponibilidad de nuestra topología es la disponibilidad de conexión de cualquier sede remota con la sede principal y, partiendo de ello nuestro análisis será bajo las siguientes consideraciones:

- La conexión entre cualquier router de la sede principal, contingencia o remoto con su respectivo POP de acceso tendrá una disponibilidad D1.
- La nube MPLS tendrá una disponibilidad R, la cual será la disponibilidad promedio que ofrecen los operadores de telecomunicaciones en el Perú en su red backbone.
- Como se indico en el punto 3.2.1, los dos trayectos de fibra proyectados entre cualquier sede remota, principal y contingencia hacia su respectivo POP de acceso será distinto.
- Los switches de la sede principal serán de las mismas características, por lo que su disponibilidad será D2.
- El switch de las sedes remotas no se considera en el análisis de disponibilidad debido a que forman parte de cada Lan remota.

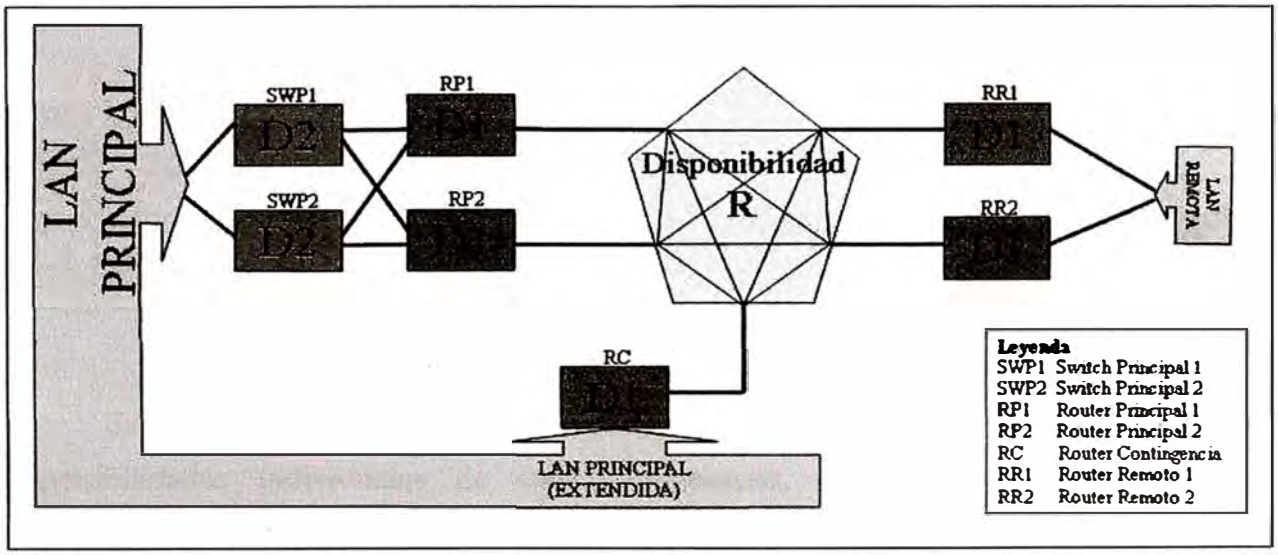


Fig. 3.9 – Diagrama de Bloques resultante de la Topología de Alta Disponibilidad

Convertiremos nuestra topología mostrada en la Fig. 3.8 en un diagrama de bloques con su respectiva disponibilidad, quedando la topología mostrada en la Fig. 3.9 en la cual hallaremos la disponibilidad resultante para conectar la Lan Principal con la Lan Remota.

Para poder determinar la disponibilidad resultante del arreglo mostrado en la Fig. 3.9 debemos determinar todas las rutas disponibles para interconectar la LAN PRINCIPAL con la LAN REMOTA, recordando que debemos determinar que rutas son paralelas y que rutas están en serie para aplicar lo indicado la parte de Cálculo de Disponibilidad en Dispositivos del Capítulo 2.

En la Fig. 3.10 se muestra el desglosamiento de las distintas rutas, así como la disponibilidad por bloques que se repiten, siendo en este caso P1 la disponibilidad del segmento de red entre RP1 y la LAN REMOTO. .

$$P1 = D1 * [1 - (1 - R * D1) * (1 - R * D1)] \quad (3.1)$$

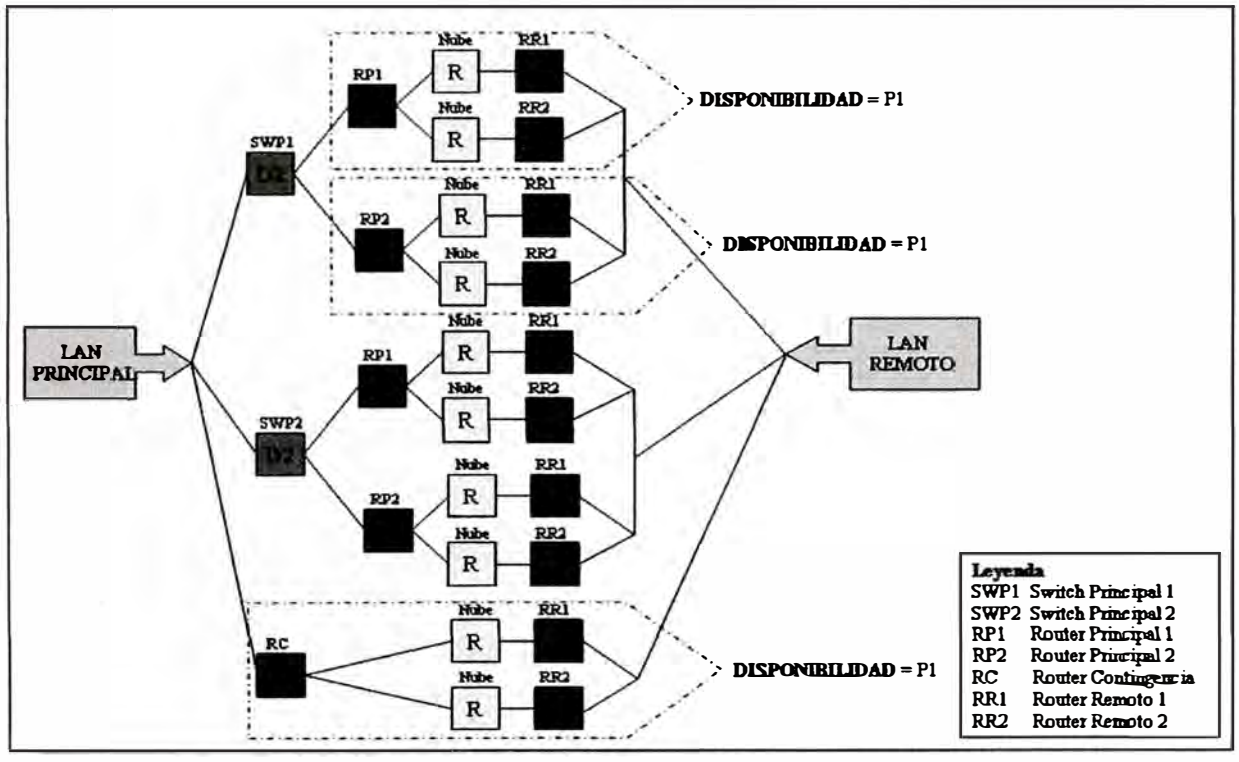


Fig. 3.10 – Rutas disponibles entre Lan Principal y Lan Remoto

En la Fig. 3.11 se muestra la Disponibilidad resultante en función de las disponibilidades individuales de cada componente, definiendo en este caso las disponibilidades P2 y DT, las cuales son:

$$P2 = D2 * [1 - (1 - P1) * (1 - P1)] \quad (3.2)$$

$$DT = P2 // P2 // P1 \quad (3.3)$$

$$DT = 1 - (1 - P2) * (1 - P2) * (1 - P1) \quad (3.4)$$

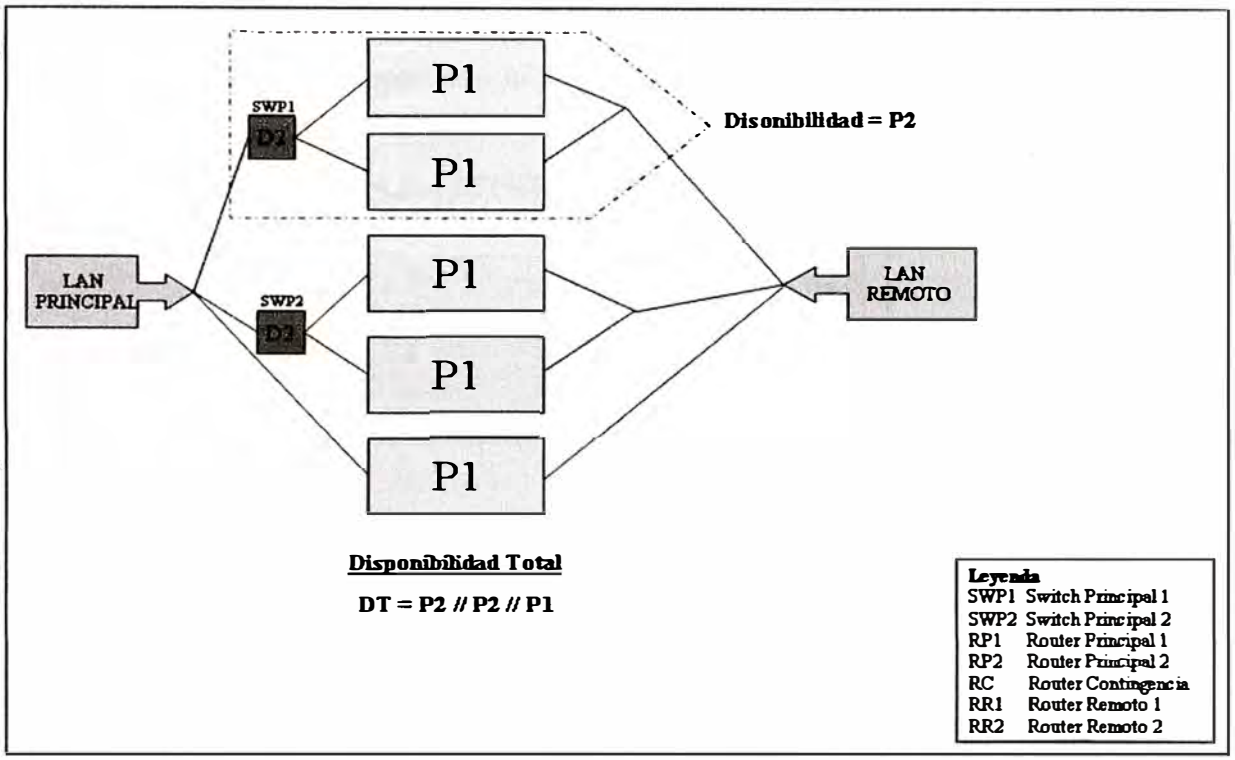


Fig. 3.11 – Calculo de disponibilidad total

En el Perú, los operadores de servicios de telecomunicaciones brindan una disponibilidad mínima de su backbone alrededor de 99.99 %, por lo que podemos considerar:

$$R = 0.9999 \quad (3.5)$$

Los equipos de datos tales como los routers y switches de las marcas indicadas en este capítulo (capitulo 3.2.2.2) tienen una disponibilidad siempre mayor a 99.5% ya que son equipos fabricados para uso empresarial teniendo un alto valor de MTBF. Este dato podemos comprobarlo revisando la tabla 3.5, considerando el MTTR como 24 horas, lo cual en la práctica resulta el peor caso para levantar una falla, por lo tanto podemos considerar:

$$D1 = D2 = 99.5\% = 0.995 \quad (3.6)$$

Reemplazando (3.5) y (3.6) en (3.1), (3.2) y (3.4), tenemos:

$$P1 = 0.994974 \quad (3.7)$$

$$P2 = 0.994975 \quad (3.8)$$

$$DT = 0.99999987 = 99.999987\% \quad (3.9)$$

Con lo cual comprobamos que la disponibilidad de nuestra topología, en el peor de los casos, siempre va a cumplir con la meta de "5 nueves" que se indico al inicio de este capítulo.

Tabla 3.5 – MTBF en Routers Juniper y Cisco

CISCO - JUNIPER Integrated Services Routers	
Mean Time Between Failure (MTBF) Hours	
Modelo	MTBF
Cisco 7206	448000.00
Cisco 2600 Series	239976.00
Familia SRX 200 y 100	35040.00

MTBF mas bajo:
Marca Juniper
MTBF = 35040
MTTR = 24
Disponibilidad = (35040) / (35040 + 24)
Disponibilidad = 99.93155 %

3.3.2 Ancho de Banda

Una de las características más importantes para tener en consideración en el diseño de una red es el ancho de banda de las sedes remotas, en la sede principal y en la sede contingencia.

Ancho de Banda en la Sede Remota: El método más optimo para determinar el ancho de banda que se requiere en una determinada sede remota es realizando un análisis de red. Un análisis de red muestra el tipo de tráfico generado y el ancho de banda consumido entre otras características más complejas, con lo cual se determina el ancho de banda necesario en dicha sede. Los costos de realizar un análisis de red varían de $1500 a $4500 dependiendo del tipo de equipos a utilizar, impacto en la red durante el análisis y el grado de granulidad de los datos recabados para el informe respectivo. Un análisis de red es posible cuando la implementación de la Alta Disponibilidad se da sobre una red ya existente, sin embargo en muchos casos no es posible realizar un análisis de red debido a cualquiera de los siguientes factores:

- Confidencialidad del tráfico generado y recibido.

- Corte de servicio para poder ingresar en la red existente un elemento (sniffer) que capture todo el tráfico.
- Alto costo para ejecutar un análisis de red por cada sede remota.

Cuando se tiene los inconvenientes antes mencionados, podemos utilizar datos estadísticos del consumo de ancho de banda de acuerdo a los aplicativos que se utilicen, por ejemplo al cargar una página Web podemos llegar a consumir hasta 50 Kbps dependiendo si la pagina llega consigo imágenes pesadas, una transacción con un servidor de datos puede consumir 32 Kbps y una llamada telefónica puede consumir 64 Kbps. Si consideramos en peor caso, estaríamos indicando que una persona realiza estas tres tareas al mismo tiempo consumiendo 146 Kbps. Una buena aproximación es considerar que cada máquina puede llegar a utilizar entre 128 Kbps y 192 Kbps en el peor caso, con lo cual estaríamos creando una regla básica para dimensionar el ancho de banda que se necesita en cada sede remota. En este punto debemos considerar un factor de ajuste del 80% debido la poca probabilidad que todas las maquinas consuman todo su ancho de banda dimensionado a la vez.

$$\mathbf{BW_{SEDE\ REMOTA} = (Número\ de\ PCs) * (192\ Kbps) * (80\%)} \quad \mathbf{(3.10)}$$

En nuestro caso, podemos considerar que una sede remota estándar puede llegar a tener hasta 25 PCs, con lo cual:

$$\mathbf{BW = (25)*(192\ Kbps)*(0.8)} \quad \mathbf{(3.11)}$$

$$\mathbf{BW = 3840Kbps} \quad \mathbf{(3.12)}$$

Con lo cual podemos aproximar:

$$\mathbf{BW_{SEDE\ REMOTA} = 4\ Mbps} \quad \mathbf{(3.13)}$$

Ancho de Banda en la Sede Principal: En la Sede Principal se tienen todos los servidores a las cuales se conectan todas las sedes remotas para realizar sus distintas transacciones y, adicionalmente también se encuentra la conexión hacia Internet que normalmente está protegido por un firewall. El ancho de banda dimensionado para una sede principal debe tener un mínimo igual a la suma de todos los anchos de banda de las sedes remotas y así asegurar una comunicación constante con todas las sedes a la vez.

$$BW_{SEDE\ PRINCIPAL} = \sum_{i=1} (BW_{SEDE\ REMOTA\ i}) \quad (3.14)$$

En nuestro caso, considerando un total de 20 sedes remotas y un ancho de banda de cada sede remota de 4 Mbps, entonces el ancho de banda total de la Sede Principal es:

$$BW_{SEDE\ PRINCIPAL} = 80\ Mbps \quad (3.15)$$

En este punto también debemos considerar que el CPE Backup posee un enlace de fibra independiente, es decir es un enlace de datos totalmente distinto por lo que su ancho de banda debe ser igual al Enlace Principal.

Ancho de Banda en la Sede Contingencia: La función de la Sede Contingencia es cumplir con todas las funcionalidades de la Sede Principal cuando ocurra algún corte de servicio, ya sea por desastres naturales o provocados por el hombre. Debido a esto, las características del ancho de banda, entre otras más, debe ser igual a las características de la Sede Principal.

$$BW_{SEDE\ CONTINGENCIA} = BW_{SEDE\ PRINCIPAL} \quad (3.16)$$

Entonces, en nuestro caso el ancho de banda de la Sede Contingencia es:

$$BW_{SEDE\ CONTINGENCIA} = 80\ Mbps \quad (3.17)$$

3.3.3 Hardware Sede Principal, Contingencia y Remotas

En los siguientes puntos definiremos los modelos de los routers y los switches a utilizar en nuestra topología.

Elección del router: Para la elección de los routers en las sedes principal, contingencia y remotas debemos asegurarnos que cumplan las siguientes características:

- Soporten los protocolos indicados en la Tabla 3.8
- Adicionalmente deben asegurar un manejo adecuado de los anchos de banda, definidos en el ítem 3.3.2 (80 Mbps para las sede principal y 4 Mbps para las sedes remotas)

Tabla 3.8 – Herramientas requeridas para la Alta Disponibilidad

Nivel de Aplicación	NAT
	IPSec
	DHCP
	DNS
	IPQoS
Nivel de Protocolo	HSRP
	VRRP
	BGP
	IPQoS
Nivel de Enlace	Spanning Tree Protocol
	L2 QoS
Nivel de Dispositivos	Procesadores redundantes
	Switches
	Tarjetas de Linea
	Fuentes de Poder redundantes

De acuerdo a la Tabla 3.4 y los 2 puntos del presente ítem (considerando que nuestra topología estará basada en equipamiento Cisco) podemos indicar que los router a utilizar serán:

Sede Principal y Contingencia: En la Sede Principal se habilitará 02 router, principal y backup, mientras que en la Sede Contingencia se habilitara un router. Estos 03 routers deberán ser del mismo modelo y marca para asegurar un funcionamiento continuo cuando ocurra la conmutación del tráfico en el caso de fallas. El router que cumple con las características A y B indicadas en el presente ítem es el **Cisco 7604**. En el anexo A se muestra el Data Sheet del router Cisco 7604.

Sedes Remotas: En las sedes remotas no es necesario contar con fuente de poder redundante ya que ello implicaría un alto costo en habilitar líneas eléctricas independientes. Una buena práctica para mantener un respaldo temporal en caso de fallas es identificar las sedes con mayor importancia para los objetivos de la empresa y habilitar sistemas autónomos de energía en caso de fallas (UPS, grupos electrógenos, etc.), los cuales no forman parte del análisis de este informe debido a que no son considerados parte de la infraestructura de telecomunicaciones. Con la salvedad antes mencionada, una buena elección para las sedes remotas es el router **Cisco 2801** considerando además que soporta tarjetas de voz, lo cual en la actualidad es un requerimiento básico de toda empresa con servicios centralizados. En el anexo B se muestra el Data Sheet del router Cisco 2801.

Elección del switch: En la sede principal se debe tener un arreglo de 2 switches para asegurar la alta disponibilidad comprobada en el punto 3.3.1. Estos 02 switches deben manejar las características indicadas en la tabla 3.9.

Tabla 3.9 – Herramientas requeridas para la Alta Disponibilidad en Switches

Nivel de Enlace	Spanning Tree Protocol
	L2 QoS
Nivel de Dispositivos	Procesadores redundantes
	Tarjetas de Linea
	Fuentes de Poder redundantes

Adicionalmente, su disponibilidad debe ser mayor a 99,5% ya que con dicho valor se demostró que nuestra topología cumple con ser una red de alta disponibilidad. En nuestro caso utilizaremos el switch WS-C3750X-24T-L, cuyo data sheet se encuentra en el anexo C.

3.3.4 Topología final de la red de alta disponibilidad

En la Fig. 3.12 podemos ver la topología física final de nuestra red, en la cual vemos los modelos del equipamiento que implementaremos.

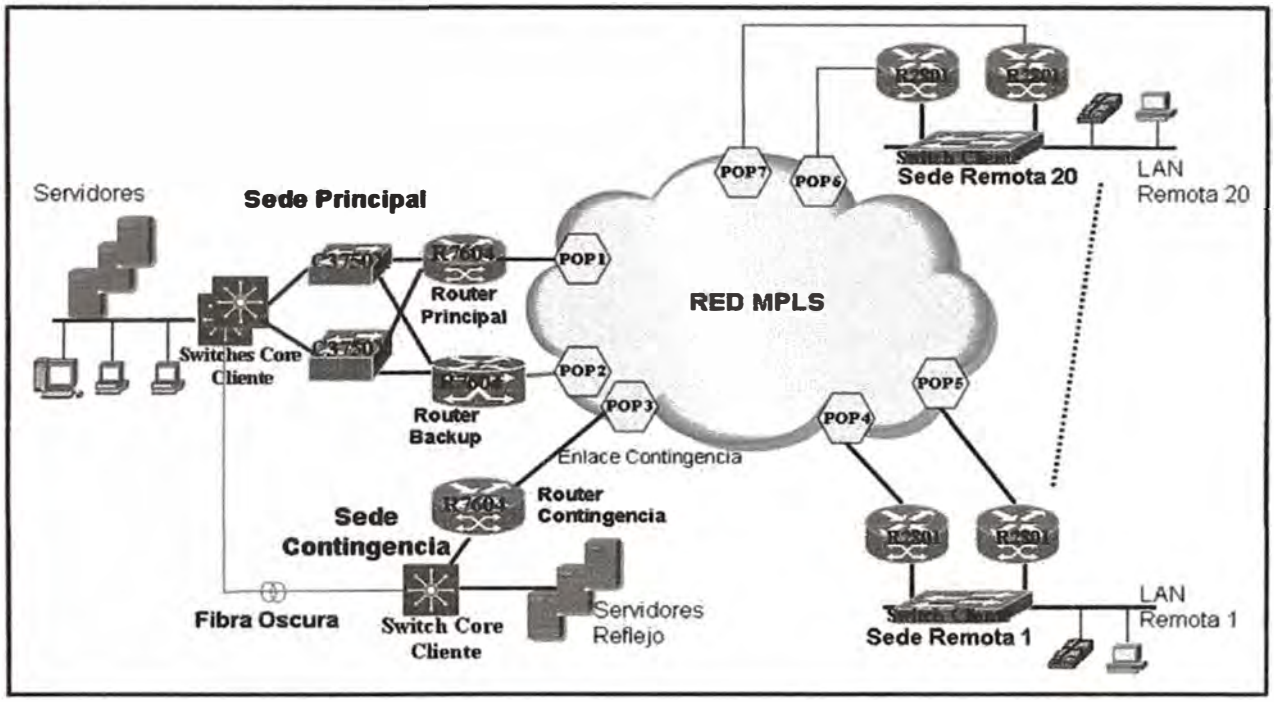


Fig. 3.12 Topología Física – Red de Alta Disponibilidad

En la Fig. 3.13 podemos ver la Topología Lógica de nuestra red, en dicho grafico podemos ver los protocolos que debemos configurar en nuestros routers para asegurar la alta disponibilidad.

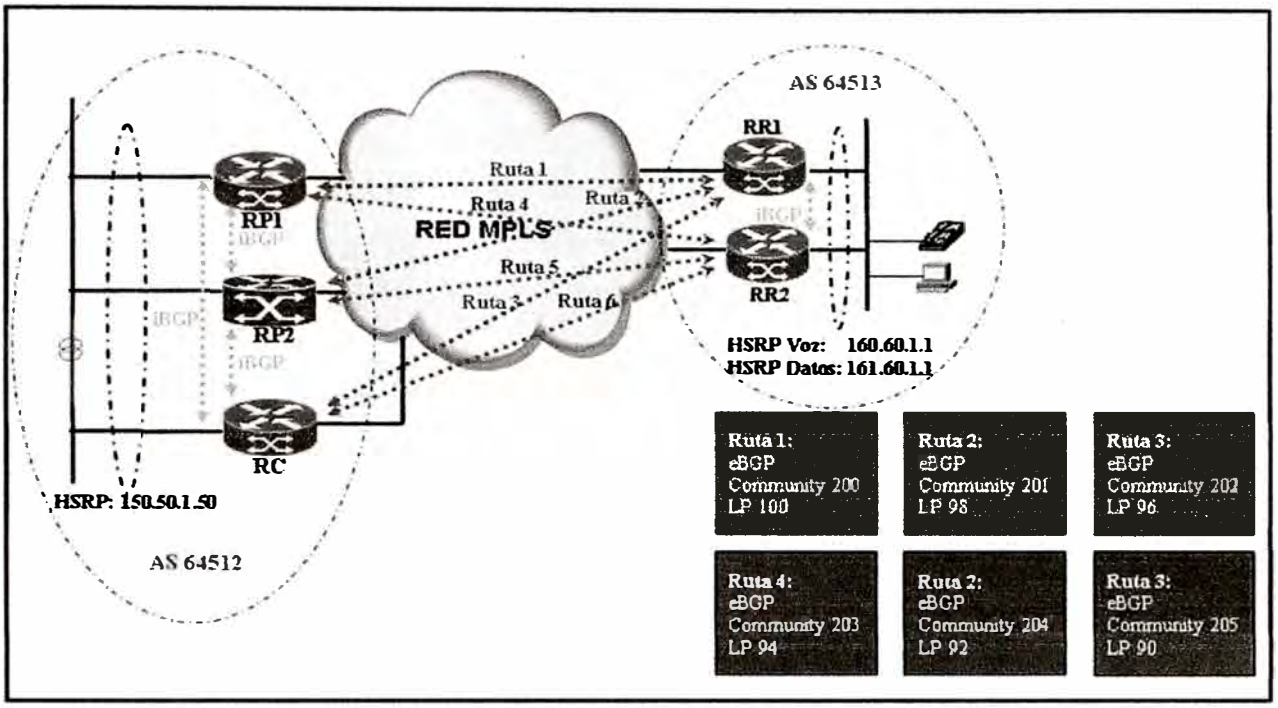


Fig. 3.13 Topología Lógica – Red de Alta Disponibilidad

3.3.5 Direccionamiento de la red de alta disponibilidad

Para el direccionamiento IP debemos tener en cuenta las siguientes características de acuerdo a nuestra topología previamente definida:

- 3 cabeceras (principal, backup y contingencia).
- 20 sedes remotas.
- Cada sede remota dispone de 25 PCs con sus respectivos teléfonos IP.
- Las direcciones IPs asignadas no saldrán a Internet, es decir podemos tomar cualquier rango IP ya que nuestra solución está dada en un ámbito de red privada virtual.

Con las consideraciones antes indicadas, en la tabla 3.11 se muestra el direccionamiento IP para nuestra topología mostrada en la Fig. 3.13. De la tabla 3.11 podemos sacar las siguientes conclusiones:

- La Sede Principal y Contingencia comparten una misma LAN que tiene el rango de IPs 150.46.0.0/16 para la red de datos y el rango de IPs 151.46.0.0/16 para la red de voz.
- La Sedes Remotas tienen un direccionamiento IP del tipo 160.XX.0.0/16 para la red de datos y 161.XX.0.0/16 para la red de voz.
- Se ha elegido distintos rangos de IPs para las cabeceras y las sedes remotas debido a que se les ha considerado como distintos Sistemas Autónomos para dejar libre la

posibilidad de manejar cada enlace, en una sede remota o principal, con distinto operador de telecomunicaciones, tal cual se muestra en la Fig. 3.14.

Tabla 3.11 Direccionamiento IP para la red de alta disponibilidad

		IP Lan Datos	HSRP Datos	IP Lan Voz	HSRP Voz	Mascara
Sede Principal	Router Principal	150.46.1.115	150.46.1.114	151.46.1.115	151.46.1.114	255.255.0.0
	Router Secundario	150.46.1.116	150.46.1.114	151.46.1.116	151.46.1.114	255.255.0.0
Sede Contingencia	Router Contingencia	150.46.1.117	150.46.1.114	151.46.1.117	151.46.1.114	255.255.0.0
Sede Remota 1	Router Principal	160.41.1.2	160.41.1.1	161.41.1.2	161.41.1.1	255.255.0.0
	Router Secundario	160.41.1.3	160.41.1.1	161.41.1.3	161.41.1.1	255.255.0.0
Sede Remota 2	Router Principal	160.42.1.2	160.42.1.1	161.42.1.2	161.42.1.1	255.255.0.0
	Router Secundario	160.42.1.3	160.42.1.1	161.42.1.3	161.42.1.1	255.255.0.0
Sede Remota 3	Router Principal	160.43.1.2	160.43.1.1	161.43.1.2	161.43.1.1	255.255.0.0
	Router Secundario	160.43.1.3	160.43.1.1	161.43.1.3	161.43.1.1	255.255.0.0
Sede Remota 4	Router Principal	160.44.1.2	160.44.1.1	161.44.1.2	161.44.1.1	255.255.0.0
	Router Secundario	160.44.1.3	160.44.1.1	161.44.1.3	161.44.1.1	255.255.0.0
Sede Remota 5	Router Principal	160.45.1.2	160.45.1.1	161.45.1.2	161.45.1.1	255.255.0.0
	Router Secundario	160.45.1.3	160.45.1.1	161.45.1.3	161.45.1.1	255.255.0.0
Sede Remota 6	Router Principal	160.46.1.2	160.46.1.1	161.46.1.2	161.46.1.1	255.255.0.0
	Router Secundario	160.46.1.3	160.46.1.1	161.46.1.3	161.46.1.1	255.255.0.0
Sede Remota 7	Router Principal	160.47.1.2	160.47.1.1	161.47.1.2	161.47.1.1	255.255.0.0
	Router Secundario	160.47.1.3	160.47.1.1	161.47.1.3	161.47.1.1	255.255.0.0
Sede Remota 8	Router Principal	160.48.1.2	160.48.1.1	161.48.1.2	161.48.1.1	255.255.0.0
	Router Secundario	160.48.1.3	160.48.1.1	161.48.1.3	161.48.1.1	255.255.0.0
Sede Remota 9	Router Principal	160.49.1.2	160.49.1.1	161.49.1.2	161.49.1.1	255.255.0.0
	Router Secundario	160.49.1.3	160.49.1.1	161.49.1.3	161.49.1.1	255.255.0.0
Sede Remota 10	Router Principal	160.50.1.2	160.50.1.1	161.50.1.2	161.50.1.1	255.255.0.0
	Router Secundario	160.50.1.3	160.50.1.1	161.50.1.3	161.50.1.1	255.255.0.0
Sede Remota 11	Router Principal	160.51.1.2	160.51.1.1	161.51.1.2	161.51.1.1	255.255.0.0
	Router Secundario	160.51.1.3	160.51.1.1	161.51.1.3	161.51.1.1	255.255.0.0
Sede Remota 12	Router Principal	160.52.1.2	160.52.1.1	161.52.1.2	161.52.1.1	255.255.0.0
	Router Secundario	160.52.1.3	160.52.1.1	161.52.1.3	161.52.1.1	255.255.0.0
Sede Remota 13	Router Principal	160.53.1.2	160.53.1.1	161.53.1.2	161.53.1.1	255.255.0.0
	Router Secundario	160.53.1.3	160.53.1.1	161.53.1.3	161.53.1.1	255.255.0.0
Sede Remota 14	Router Principal	160.54.1.2	160.54.1.1	161.54.1.2	161.54.1.1	255.255.0.0
	Router Secundario	160.54.1.3	160.54.1.1	161.54.1.3	161.54.1.1	255.255.0.0
Sede Remota 15	Router Principal	160.55.1.2	160.55.1.1	161.55.1.2	161.55.1.1	255.255.0.0
	Router Secundario	160.55.1.3	160.55.1.1	161.55.1.3	161.55.1.1	255.255.0.0
Sede Remota 16	Router Principal	160.56.1.2	160.56.1.1	161.56.1.2	161.56.1.1	255.255.0.0
	Router Secundario	160.56.1.3	160.56.1.1	161.56.1.3	161.56.1.1	255.255.0.0
Sede Remota 17	Router Principal	160.57.1.2	160.57.1.1	161.57.1.2	161.57.1.1	255.255.0.0
	Router Secundario	160.57.1.3	160.57.1.1	161.57.1.3	161.57.1.1	255.255.0.0
Sede Remota 18	Router Principal	160.58.1.2	160.58.1.1	161.58.1.2	161.58.1.1	255.255.0.0
	Router Secundario	160.58.1.3	160.58.1.1	161.58.1.3	161.58.1.1	255.255.0.0
Sede Remota 19	Router Principal	160.59.1.2	160.59.1.1	161.59.1.2	161.59.1.1	255.255.0.0
	Router Secundario	160.59.1.3	160.59.1.1	161.59.1.3	161.59.1.1	255.255.0.0
Sede Remota 20	Router Principal	160.60.1.2	160.60.1.1	161.60.1.2	161.60.1.1	255.255.0.0
	Router Secundario	160.60.1.3	160.60.1.1	161.60.1.3	161.60.1.1	255.255.0.0

En la Fig. 3.14 se muestra nuestra misma topología previamente definida, sin embargo se indica explícitamente que los enlaces redundantes y principales deben ser de distinto operador de telecomunicaciones. En la práctica, ello queda a consideración de la empresa dueña de la red.

Este tipo de soluciones se da mayormente para asegurar que las rutas de la fibra óptica principales y redundantes no tienen caminos en común, lo cual por ser en la vía pública y muchas veces de manera subterránea, es difícil de comprobar cuando se contrata

a una sola empresa de telecomunicaciones tanto para los enlaces principales como para los enlaces redundantes.

Por regla general, mientras mayores operadores de telecomunicaciones tengamos en nuestra red estaremos ganando disponibilidad, sin embargo se necesitara que exista un equipo administrado por un agente externo a los operadores de red o por el mismo dueño de la red centralizada que haga el trabajo de convergencia entre los dos o más operadores y, de esta manera, cuando exista alguna falla pueda determinar que operador de telecomunicaciones fue el responsable.

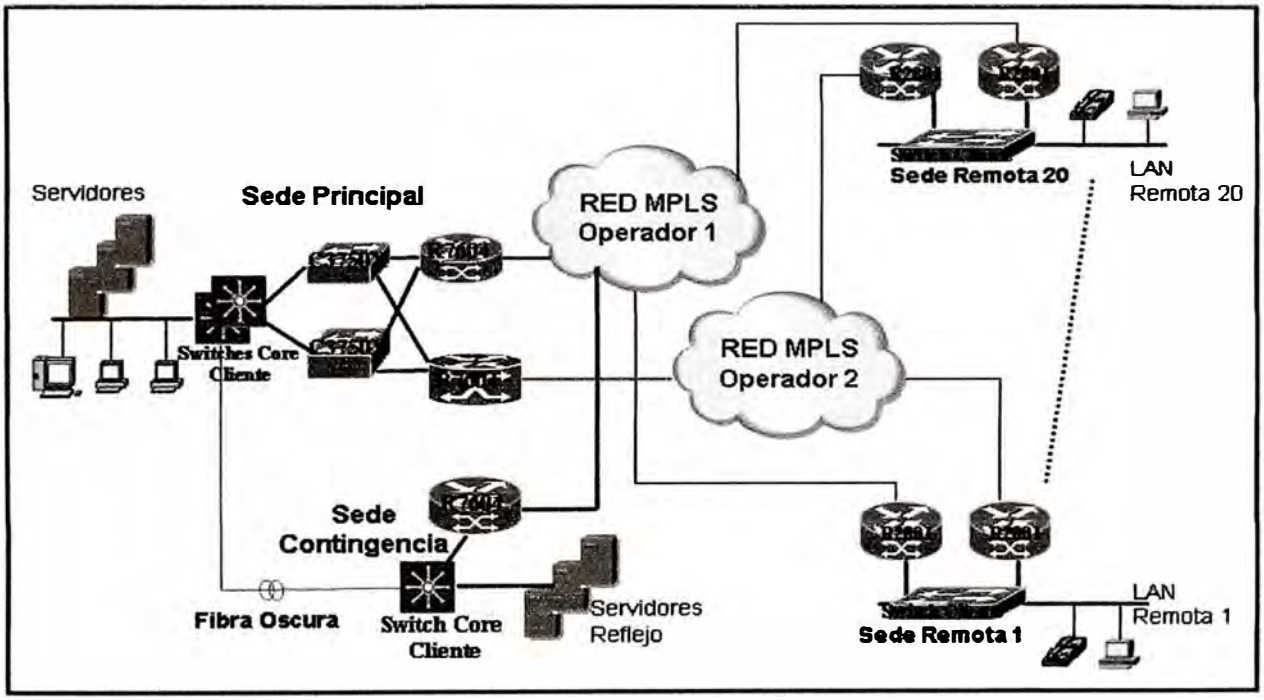


Fig. 3.14 Topologia de Alta Disponibilidad con 2 operadores de telecomunicaciones

CAPITULO 4
IMPLEMENTACIÓN DE UNA RED DE ALTA DISPONIBILIDAD PARA UNA ENTIDAD CON SERVICIOS CENTRALIZADOS

4.1 Equipamiento

En el Capitulo 3 se ha definido los equipos a utilizar por lo que en este ítem se agrupara el equipamiento definido.

4.1.1 Equipamiento de la Sede Principal y Contingencia

En la Sede Principal se tiene dos cabeceras las cuales fueron nombradas como principal y backup. En la Sede contingencia debe haber un router de iguales características que el router de la Sede Principal para que soporte todo el tráfico en caso sea necesario.

En la tabla 4.1 se muestra los routers a utilizar tanto en la Sede Principal como en la Sede Contingencia.

Tabla 4.1 Routers a utilizar en la Sede Principal y Sede Contingencia.

Producto	Descripcion	Cantidad
7600-SIP-400=	Cisco 7600 Series SPA Interface Processor-400	3
SPA-2X1GE-V2	Cisco 2-Port Gigabit Ethernet Shared Port Adapter	9
WS-G5487	1000Base-ZX extended reach GBIC(singlemode)	3
SFP-GE-Z	1000BASE-ZX Gigabit Ethernet SFP (DOM)	3
WS-X4306-GB	Catalyst 4500 Gigabit Ethernet Module, 6-Ports (GBIC)	3

En este equipamiento se está considerando tarjetas ópticas, con lo cual ya no es necesario media converters, es decir la fibra óptica se conectara directamente al router. Adicionalmente, en la Sede Principal es necesario proveer 02 Switches para mantener la alta disponibilidad. En la tabla 4.2 se muestra los switches que se instalará en la sede principal.

Tabla 4.2 Switches a utilizar en la Sede Principal.

Producto	Descripción	Cantidad
WS-C3750X-24T-S	WS-C3750X-24T-S, Catalyst 3750X 48 Port Data IP Base	2

4.1.2 Equipamiento de las Sedes Remotas

En las sedes remotas se utilizarán dos routers por cada sede, el cual se muestra en la tabla 4.3.

Tabla 4.3 Routers a utilizar en las Sedes Remotas

Producto	Descripción	Cantidad
CISCO2801-V/K9	CISCO2801-V/K9,2801 Voice Bundle,PVDM2-8,SP S	2
VIC2-2FXS	VIC2-2FXS,Two-port Voice Interface Card	2
PVDM2-8	PVDM2-8,8-Channel Packet Voice/Fax DSP	2

En las sedes remotas es necesario instalar media converters para hacer el cambio de medio óptico a eléctrico. El tipo de media converter depende de la longitud y tipo de fibra que llega a cada sede remota por lo que se puede solicitar a la empresa encargada de instalar la fibra óptica (o a la empresa arrendadora del circuito de datos) que incluya el conversor de medio adecuado para cada caso, de esta manera se nos entregará cada enlace en cobre (UTP).

Es importante revisar siempre las dimensiones, tipo de conector de energía, voltaje y corriente soportado del equipamiento que se instalará en las sedes para poder dimensionar el espacio y recursos necesarios en el lugar donde quedara instalado.

4.2 Configuración de routers principal, backup y contingencia

En las siguientes líneas se mostrara las configuraciones de los routers principales y de de una sede remota. Se aclara que estas configuraciones son lineamientos de acuerdo a los parámetros colocados en este documento, tanto en las topologías como en el direccionamiento IP indicado en la etapa de diseño del capítulo III.

4.2.1 Configuración de Router Principal

En las siguientes líneas se muestra la configuración de las interfaces del router principal.

```
interface Loopback 0
description Interfase Loopback de Gestión
ip address [IP a ser asignada por el administrador del router]
!
interface GigabitEthernet 1/1
 description Red LAN DATOS SEDE PRINCIPAL
 ip address 150.46.1.115 255.255.0.0
service-policy input SetDscpLan
 load-interval 30
 standby 1 ip 150.46.1.114
 standby 1 priority 150
 standby 1 preempt
 standby 10 track GigabitEthernet2/0/0 100
```

```
!
interface GigabitEthernet 1/2
 description Red LAN VOZ SEDE PRINCIPAL
 ip address 151.46.1.115 255.255.0.0
service-policy input SetDscpLan
 load-interval 30
 standby 1 ip 151.46.1.114
 standby 1 priority 150
 standby 1 preempt
 standby 10 track GigabitEthernet2/0/0 100
!
interface GigabitEthernet 0/0
 description Red WAN
 no ip address
 full-duplex
 speed 1000
!
interface GigabitEthernet 0/0.10
 description Enlace WAN hacia sedes remotas
 encapsulation dot1q [VLAN a ser asignada por el operador de
telecomunicaciones]
 ip address [IP asignada por el operador de telecomunicaciones] [Mask
asignada por el operador de telecomunicaciones]
!
```

En las siguientes líneas se muestra la configuración del protocolo BGP en el router principal.

```
router bgp 64512
 bgp router-id [IP loopback 0]
 bgp log-neighbor-changes
 neighbor LAN peer-group
 neighbor LAN remote-as 64512
 neighbor LAN password (a ser asignado por el Operador de
Telecomunicaciones)
 neighbor LAN timers 10 30
 neighbor WAN peer-group
 neighbor WAN remote-as 64516
 neighbor WAN password (a ser asignado por el operador de
telecomunicaciones)
 neighbor WAN timers 10 30
 neighbor WAN as-override
 neighbor 150.46.1.116 peer-group LAN
 neighbor 150.46.1.116 description Enlace con CPE de Backup
 neighbor 150.46.1.117 peer-group LAN
 neighbor 150.46.1.117 description Enlace con CPE de Contingencia
!
 address-family ipv4
 neighbor LAN send-community both
 neighbor LAN next-hop-self
 neighbor LAN soft-configuration inbound
 neighbor WAN send-community both
 neighbor WAN soft-reconfiguration inbound
 neighbor WAN route-map From_VPN_Telmex in
 neighbor WAN route-map dualhome in
 neighbor 150.46.1.116 activate
 neighbor 150.46.1.117 activate
 no auto-summary
 no synchronization
 network 150.46.0.0 mask 255.255.0.0
```

```
  exit-address-family
!
ip bgp-community new-format
!
ip community-list 1 permit 64512:200
ip community-list 2 permit 64512:201
ip community-list 3 permit 64512:202
ip community-list 4 permit 64512:203
ip community-list 5 permit 64512:204
!
ip prefix-list Red_LAN seq 10 permit 150.46.0.0/16
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
route-map From_VPN_OPERADOR deny 10
 description denegacion de Red 150.46.0.0/16
 match ip address prefix-list Red_LAN
!
route-map From_VPN_OPERADOR permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
route-map dualhome permit 10
 match community 1
 set local-preference 100
!
route-map dualhome permit 20
 match community 2
 set local-preference 98
!
route-map dualhome permit 30
 match community 3
 set local-preference 96
!
route-map dualhome permit 40
 match community 4
 set local-preference 94
!
route-map dualhome permit 50
 match community 5
set local-preference 92
```

4.2.2 Configuración de Router Backup

En las siguientes líneas se muestra la configuración de las interfaces del router Backup.

```
interface Loopback 0
description Interfase Loopback de Gestión
ip address [IP a ser asignada por el administrador de la red]
!
interface GigabitEthernet 1/1
 description Red LAN DATOS
 ip address 150.46.1.116 255.255.0.0
 service-policy input SetDscpLan
 load-interval 30
 standby 1 ip 150.46.1.114
 standby 1 priority 140
 standby 1 preempt
```

```
 standby 1 track GigabitEthernet0/0.10 100
!
!
interface GigabitEthernet 1/2
 description Red LAN VOZ
 ip address 151.46.1.116 255.255.0.0
 service-policy input SetDscpLan
 load-interval 30
 standby 1 ip 151.46.1.114
 standby 1 priority 140
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.10 100

interface GigabitEthernet 0/0
 description Red WAN
 no ip address
 full-duplex
 speed 1000
!
interface GigabitEthernet 0/0.10
 description Enlace WAN hacia sedes remotas
 encapsulation dot1q [VLAN a ser asignada por el operador de
telecomunicaciones]
 ip address [IP a ser asignada por el operadoros de telecomunicaciones]
[mascara]
!
```

En las siguientes líneas se muestra la configuración del protocolo BGP en el router Backup.

```
router bgp 64512
 bgp router-id [IP Loopback]
 bgp log-neighbor-changes
 neighbor LAN peer-group
 neighbor LAN remote-as 64512
 neighbor LAN password (a ser asignado por el Operador de
Telecomunicaciones)
 neighbor LAN timers 10 30
 neighbor WAN peer-group
 neighbor WAN remote-as 64516
 neighbor WAN password (a ser asignado por el Operador de
Telecomunicaciones)
 neighbor WAN timers 10 30
 neighbor WAN as-override
 neighbor 150.46.1.115 peer-group LAN
 neighbor 150.46.1.115 description Enlace con Router Principal
 neighbor 150.46.1.117 peer-group LAN
 neighbor 150.46.1.117 description Enlace con Router Contingencia
!
 address-family ipv4
 neighbor LAN send-community both
 neighbor LAN next-hop-self
 neighbor LAN soft-configuration inbound
 neighbor WAN send-community both
 neighbor WAN soft-reconfiguration inbound
 neighbor WAN default-originate
 neighbor WAN route-map From_VPN_OP in
 neighbor WAN route-map dualhome in
 neighbor 150.46.1.115 activate
 neighbor 150.46.1.117 activate
```

```
 no auto-summary
 no synchronization
 network 150.46.0.0 mask 255.255.0.0
  exit-address-family
!
ip bgp-community new-format
!
ip community-list 1 permit 64512:200
ip community-list 2 permit 64512:201
ip community-list 3 permit 64512:202
ip community-list 4 permit 64512:203
ip community-list 5 permit 64512:204

ip prefix-list Red_LAN seq 10 permit 150.46.0.0/16
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
route-map From_VPN_OP deny 10
 description denegacion de Red 150.46.0.0/16
 match ip address prefix-list Red_LAN
!
route-map From_VPN_OP permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
route-map dualhome permit 10
 match community 1
 set local-preference 100
!
route-map dualhome permit 20
 match community 2
 set local-preference 98
!
route-map dualhome permit 30
 match community 3
 set local-preference 96
!
route-map dualhome permit 40
 match community 4
 set local-preference 94
!
route-map dualhome permit 50
 match community 5
set local-preference 92
```

4.2.3 Configuración de Router Contingencia

En las siguientes líneas se muestra la configuración de las interfaces del router de contingencia.

```
interface Loopback 0
description Interfase Loopback de Gestión
ip address [IP a ser asignada por el administrador de red]
!
interface GigabitEthernet 1/1
 description Red LAN DATOS
 ip address 150.46.1.117 255.255.0.0
 service-policy input SetDscpLan
 load-interval 30
```

```
 standby 1 ip 150.46.1.114
 standby 1 priority 130
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.10 100
!
interface GigabitEthernet 1/2
 description Red LAN VOZ
 ip address 151.46.1.117 255.255.0.0
 service-policy input SetDscpLan
 load-interval 30
 standby 1 ip 151.46.1.114
 standby 1 priority 130
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.10 100
!
interface GigabitEthernet 0/0
 description Red WAN
 no ip address
 full-duplex
 speed 1000
!
interface GigabitEthernet 0/0.10
 description Enlace WAN hacia sedes remotas
 encapsulation dot1q [VLAN a ser asignada por el operador de
telecomunicaciones]
 ip address [IP a ser asignada por el operador de telecomunicaciones]
[mascara]
!
```

En las siguientes líneas se muestra la configuración del protocolo BGP en el router de contingencia.

```
router bgp 64512
 bgp router-id [IP Loppback]
 bgp log-neighbor-changes
 neighbor LAN peer-group
 neighbor LAN remote-as 64512
 neighbor LAN password (a ser asignado por el Operador de
Telecomunicaciones)
 neighbor LAN timers 10 30
 neighbor WAN peer-group
 neighbor WAN remote-as 64516
 neighbor WAN password (a ser asignado por el operador de
telecomunicaciones)
 neighbor WAN timers 10 30
 neighbor WAN as-override
 neighbor 150.46.1.115 peer-group LAN
 neighbor 150.46.1.115 description Enlace con Router Principal
 neighbor 150.46.1.116 peer-group LAN
 neighbor 150.46.1.116 description Enlace con Router Backup
 !
 address-family ipv4
 neighbor LAN send-community both
 neighbor LAN next-hop-self
 neighbor LAN soft-configuration inbound
 neighbor WAN send-community both
 neighbor WAN soft-reconfiguration inbound
 neighbor WAN route-map From_VPN_OP in
 neighbor WAN route-map dualhome in
```

```
 neighbor 150.46.1.115 activate
 neighbor 150.46.1.116 activate
 no auto-summary
 no synchronization
 network 150.46.0.0 mask 255.255.0.0
  exit-address-family
!
ip bgp-community new-format
!
ip community-list 1 permit 64512:200
ip community-list 2 permit 64512:201
ip community-list 3 permit 64512:202
ip community-list 4 permit 64512:203
ip community-list 5 permit 64512:204
!
ip prefix-list Red_LAN seq 10 permit 130.30.0.0/16
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
route-map From_VPN_OP deny 10
 description denegacion de Red 150.46.0.0/16
 match ip address prefix-list Red_LAN
!
route-map From_VPN_OP permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
route-map dualhome permit 10
 match community 1
 set local-preference 100
!
route-map dualhome permit 20
 match community 2
 set local-preference 98
!
route-map dualhome permit 30
 match community 3
 set local-preference 96
!
route-map dualhome permit 40
 match community 4
 set local-preference 94
!
route-map dualhome permit 50
 match community 5
set local-preference 92
```

4.2.4 Configuración de Routers Remotos

En este punto se mostrara la configuración tipo de la Sede Remota 1, la configuración se replicará en las demás sedes. Se empezara con la configuración de las interfaces de uno de los routers remotos.

```
interface Loopback 0
description Interfase Loopback de Gestión
ip address [A ser asignado por el administrador de red]
!
interface FastEthernet 0/1
 description Red LAN
```

```
 ip address 160.41.1.2 255.255.0.0
 ip address 161.41.1.2 255.255.0.0 secondary
 service-policy input SetDscpLan
 load-interval 30
 standby 1 ip 160.41.1.2
 standby 1 priority 150
 standby 1 preempt
 standby 1 track FastEthernet0/0.10 100
 standby 2 ip 161.41.1.2
 standby 2 priority 150
 standby 2 preempt
 standby 2 track FastEthernet0/0.10 100
!
interface FastEthernet 0/0
 description Red WAN
 no ip address
 full-duplex
 speed 100
!
interface FastEthernet 0/0.10
 description Enlace WAN hacia Router Principal
 encapsulation dot1q [VLAN a ser asignada por el OP]
 ip address [IP a ser asignada por el OP] [Mascara]
!
interface FastEthernet 0/0.20
 description Enlace WAN hacia Router Backup
 encapsulation dot1q [VLAN a ser asignada por el OP]
 ip address [IP a ser asignada por el OP] [Mascara]
!
interface FastEthernet 0/0.30
 description Enlace WAN hacia Router Contingencia
 encapsulation dot1q [VLAN a ser asignada por el OP]
 ip address [IP a ser asignada por el OP] [Mascara]
!
ip classless
!
```

En las siguientes líneas se muestra la configuración del protocolo BGP en el router remoto.

```
router bgp 64516
 bgp router-id (A ser asignado por el Operador de Telecomuicaciones)
 bgp log-neighbor-changes
 neighbor LAN_SEDE_REMOTA peer-group
 neighbor LAN_SEDE_REMOTA remote-as 64512
 neighbor LAN_SEDE_REMOTA password (a ser asignado por el Operador de
Telecomunicaciones)
 neighbor LAN_SEDE_REMOTA timers 10 30
 neighbor WAN_ROUTER_PRINCIPAL peer-group
 neighbor WAN_ROUTER_PRINCIPAL remote-as 64512
 neighbor WAN_ROUTER_PRINCIPAL password (a ser asignado por el Operador
de Telecomunicaciones)
 neighbor WAN_ROUTER_PRINCIPAL timers 10 30
neighbor WAN_ROUTER_BACKUP peer-group
 neighbor WAN_ROUTER_BACKUP remote-as 64512
 neighbor WAN_ROUTER_BACKUP password (a ser asignado por el Operador de
Telecomunicaciones)
 neighbor WAN_ROUTER_BACKUP timers 10 30
neighbor WAN_ROUTER_CONTINGENCIA peer-group
 neighbor WAN_ROUTER_CONTINGENCIA remote-as 64512
```

```
 neighbor WAN_ROUTER_CONTINGENCIA password (a ser asignado por el
Operador de Telecomunicaciones)
 neighbor WAN_ROUTER_CONTINGENCIA timers 10 30
 neighbor 160.41.1.1 peer-group LAN_SEDE_REMOTA
 neighbor 160.41.1.1 description Enlace con Router Remoto de Respaldo
 neighbor [IP WAN Router Principal] peer-group WAN_ROUTER_PRINCIPAL
 neighbor [IP WAN Router Principal] description Enlace WAN ROUTER
PRINCIPAL
 neighbor [IP WAN Router Backup] peer-group WAN_ROUTER_BACKUP
 neighbor [IP WAN Router Backup] description Enlace WAN ROUTER BACKUP
 neighbor [IP WAN Router Contingencia] peer-group WAN_ROUTER_CONTINGENCIA
 neighbor [IP WAN Router Contingencia] description Enlace WAN  ROUTER
CONTINGENCIA
!
 address-family ipv4
 neighbor LAN_SEDE_REMOTA send-community both
 neighbor LAN_SEDE_REMOTA next-hop-self
 neighbor LAN_SEDE_REMOTA soft-configuration inbound
 neighbor WAN_ROUTER_PRINCIPAL send-community both
 neighbor WAN_ROUTER_PRINCIPAL soft-reconfiguration inbound
 neighbor WAN_ROUTER_PRINCIPAL route-map From_VPN_OP in
 neighbor WAN_ROUTER_PRINCIPAL route-map SET_OP_COMM1 out
 neighbor WAN_ROUTER_PRINCIPAL route-map ROUTER_PRINCIPAL in
 neighbor WAN_ROUTER_BACKUP send-community both
 neighbor WAN_ROUTER_BACKUP soft-reconfiguration inbound
 neighbor WAN_ROUTER_BACKUP route-map From_VPN_OP in
 neighbor WAN_ROUTER_BACKUP route-map SET_OP_COMM2 out
 neighbor WAN_ROUTER_BACKUP route-map ROUTER_BACKUP in
 neighbor WAN_ROUTER_CONTINGENCIA send-community both
 neighbor WAN_ROUTER_CONTINGENCIA soft-reconfiguration inbound
 neighbor WAN_ROUTER_CONTINGENCIA route-map From_VPN_OP in
 neighbor WAN_ROUTER_CONTINGENCIA route-map SET_OP_COMM3 out
 neighbor WAN_ROUTER_CONTINGENCIA route-map ROUTER_CONTINGENCIA in
 neighbor [IP WAN Router Principal] activate
 neighbor [IP WAN Router Backup] activate
 neighbor [IP WAN Router Contingencia] activate
 neighbor 160.41.1.1 activate
 no auto-summary
 no synchronization
 network 160.41.0.0 mask 255.255.0.0
 network 161.41.0.0 mask 255.255.0.0
 exit-address-family
!
ip bgp-community new-format
!
ip prefix-list Red_LAN_SEDE_REMOTA seq 10 permit 160.41.0.0/16
ip prefix-list Red_LAN_SEDE_REMOTA seq 15 permit 161.41.0.0/16
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
route-map SET_OP_COMM1 permit 10
 description Setear Comunidad200 a todas nuetras redes
 match ip address prefix-list Red_LAN_SEDE_REMOTA
 set community 64512:200
!
route-map SET_OP_COMM2 permit 10
 description Setear Comunidad201 a todas nuetras redes
 match ip address prefix-list Red_LAN_SEDE_REMOTA
 set community 64512:201
!
```

```
route-map SET_OP_COMM3 permit 10
 description Setear Comunidad202 a todas nuetras redes
 match ip address prefix-list Red_LAN_SEDE_REMOTA
 set community 64512:202
!
route-map From_VPN_OP deny 10
 description denegacion de Red 150.46.0.0/16
 match ip address prefix-list Red_LAN_SEDE_REMOTA
!
route-map From_VPN_OP permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
route-map ROUTER_PRINCIPAL permit 10
 description Rutas Principal de ROUTER PRINCIPAL
 set local-preference 100
!
route-map ROUTER_BACKUP permit 10
 description Rutas Secundaria ROUTER BACKUP
 set local-preference 98
!
route-map ROUTER_CONTINGENCIA permit 10
 description Rutas Terciaria ROUTER CONTINGENCIA
 set local-preference 96
```

4.3 Análisis del costo del proyecto

En este punto detallaremos los costos de implementación de la red en nuestro caso. Para implementar nuestra red es necesario apoyarnos en una red MPLS existente, la cual es arrendada por los distintos operadores existentes, quienes también ofrecen el alquiler del equipamiento. En la tabla 4.4 se muestra los costos promedio de los enlaces en Lima.

Tabla 4.4 - Costos referenciales de los enlaces de datos

Costos referenciales y sujetos a disponibilidad				
Acceso Simple Lima	**US$ (mensual)**			
BW (Kbps)	**1 año**	**2 años**	**3 años**	**4 años**
1280	645.47	597.42	549.37	504.53
1536	747.26	691.63	636.00	584.09
2048	874.67	809.56	744.45	683.69
2560	948.49	877.88	807.27	741.39
3072	1037.27	960.05	882.84	810.78
4096	1177.35	1089.71	1002.06	920.28
81920	4601.51	4258.96	3916.41	3596.78
Acceso Backup Lima	**US$ (mensual)**			
BW (Kbps)	**1 año**	**2 años**	**3 años**	**4 años**
1280	480.51	444.47	420.44	396.42
1536	556.28	514.56	486.75	458.93
2048	651.13	602.30	569.74	537.18
2560	706.09	653.13	617.83	582.52
3072	772.18	714.26	675.65	637.05
4096	876.46	810.72	766.90	723.08
81920	3425.51	3168.59	2997.32	2826.04

Los costos mostrados en la Tabla 4.4 incluyen los media converters. Se han colocado distintos anchos de banda para tener un espectro amplio del costo por el alquiler de un enlace de datos.

Para nuestro caso, en la Tabla 4.5 se muestra los costos de arrendar los enlaces que necesitamos. El tiempo de arrendamiento será de 3 años, tiempo usual en que se debe renegociar los costos y características de los enlaces e implementar mejoras por nuevas tecnologías.

Tabla 4.5 – Costos de los enlaces necesarios para la implementación de la red de alta disponibilidad

		Costo mensual (US$)		
	BW (Kbps)	Enlace Principal	Enlace Backup	Total
Sede Principal	81920	3916.41	2997.32	6913.73
Sede Contingencia	81920	3916.41	0	3916.41
Sede Remota 1	4096	1002.06	766.9	1768.96
Sede Remota 2	4096	1002.06	766.9	1768.96
Sede Remota 3	4096	1002.06	766.9	1768.96
Sede Remota 4	4096	1002.06	766.9	1768.96
Sede Remota 5	4096	1002.06	766.9	1768.96
Sede Remota 6	4096	1002.06	766.9	1768.96
Sede Remota 7	4096	1002.06	766.9	1768.96
Sede Remota 8	4096	1002.06	766.9	1768.96
Sede Remota 9	4096	1002.06	766.9	1768.96
Sede Remota 10	4096	1002.06	766.9	1768.96
Sede Remota 11	4096	1002.06	766.9	1768.96
Sede Remota 12	4096	1002.06	766.9	1768.96
Sede Remota 13	4096	1002.06	766.9	1768.96
Sede Remota 14	4096	1002.06	766.9	1768.96
Sede Remota 15	4096	1002.06	766.9	1768.96
Sede Remota 16	4096	1002.06	766.9	1768.96
Sede Remota 17	4096	1002.06	766.9	1768.96
Sede Remota 18	4096	1002.06	766.9	1768.96
Sede Remota 19	4096	1002.06	766.9	1768.96
Sede Remota 20	4096	1002.06	766.9	1768.96
Total de costo (enlaces)				46209.34

El costo mensual por los enlaces será de US$ 46,209.34. En seguida calcularemos el costo mensual del alquiler del equipamiento definido en los capítulos anteriores. Optar por el alquiler del equipamiento para la red de alta disponibilidad trae ventajas tales como:

- Asegurar la actualización del software.

- Asegurar el cambio del equipo ante fallas imprevistas.
- Soporte ante cambios de topología

Estas ventajas se deben a que el equipo (router o switch) pertenece a un tercero y, como tal, se debe hacer responsable ante cualquier actualización o falla del equipo. En la tabla 4.6 se muestra el costo mensual por el alquiler del equipamiento necesario.

Tabla 4.6 – Costo por alquiler del equipamiento

ALQUILER MENSUAL			
	Cant	P. Unitario (US$)	P. Total (US$)
Cisco 7604	3	850	2550
Catalyst 3750	2	70	140
Cisco 2801 w/k9	40	100	4000
Total Mensual			6690

En la Tabla 4.7 se resume el costo total para implementar una Red de Alta Disponibilidad para una entidad con servicios centralizados con 20 sedes remotas.

Tabla 4.7 – Costo Total de Implementación

Costo Total Enlaces	Costo Total Equipamiento	Costo total Mensual
US$ 46,209	US$ 6,690	US$ 52,899

CONCLUSIONES Y RECOMENDACIONES

1. Hasta el año 2004 las redes de comunicaciones se protegían de posibles cortes de servicio en base a contingencias con enlaces RDSI cuyo ancho de banda es de 128 Kbps como máximo, lo cual significaba priorizar el tipo de tráfico para poder darle contingencia.
2. A partir del año 2004 las redes de comunicaciones empezaron a evolucionar debido a la aparición de aplicaciones que requieren mayor ancho de banda, así como el gran aumento del tráfico en internet.
3. Diferentes tipos de empresas empezaron a depender de las comunicaciones para poder aumentar sus ingresos, lo cual significo exigir niveles altísimos de disponibilidad por año.
4. Actualmente un nivel de servicio de alta disponibilidad debe ser mayor o igual a 99.999%.
5. Para poder implementar una red de alta disponibilidad debemos manejar conceptos teóricos de networking tales BGP y sus características, Sistemas Autónomos y HSRP.
6. La cuantificación de la disponibilidad se da a través de modelos genéricos los cuales son planteados y diseñados en diversas recomendaciones de UIT, utilizando diversos parámetros probabilísticos o estadísticos.
7. La UIT también brinda valores mínimos de disponibilidad para secciones de conexión nacional (99.98%), el cual es válida para los operadores de telecomunicaciones.
8. Al diseñar una red de alta disponibilidad debemos alcanzar un 99.999% de disponibilidad anual como mínimo. Esto es equivalente a exigir que el tiempo total de corte al año sea menor o igual a 5 minutos.
9. Para aumentar la disponibilidad de una sede dada debemos implementar doble ruta de acceso, considerando diferente trayectoria.

10. Diseñar la red con hardware redundante en modo activo/stand by también ayuda a aumentar la disponibilidad.
11. Para la elección del hardware debemos validar que soporten los protocolos necesarios para una alta disponibilidad y que la marca tenga una experiencia y soporte reconocido en el mercado local, ya que la realidad de los operadores en cada país es diferente.
12. Siempre se debe exigir al área de infraestructura que habilite líneas de energía dobles (redundantes) en los datacenters donde estén los equipos de red
13. Se recomienda tener una sede de contingencia en la cual albergue espejos de todos los servidores y así ante la caída de la sede principal, por cualquier motivo, la red centralizada seguirá funcionando apuntando a la sede de contingencia.
14. La sede principal y contingencia debe estar interconectadas por un medio directo (usualmente fibras oscuras) para que puedan interactuar y actualizar los servidores espejos constantemente.
15. La cuantificación de una red se calcula en base a las disponibilidades de cada componente.
16. El cálculo del ancho de banda para una sede es necesario conocer las aplicaciones a utilizar y el numero de computadoras que estarán conectadas.
17. El ancho de banda de la sede principal debe ser igual a la suma de todos los anchos de banda de las sedes remotas.
18. El ancho de banda de la sede principal debe ser igual al ancho de banda de la sede contingencia.

ANEXO A
DATASHEET ROUTER CISCO 7604

Cisco 7604 Chassis

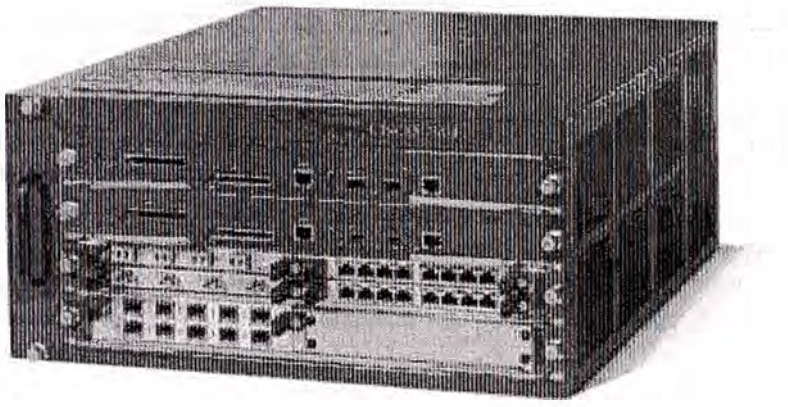
Extending Performance, Versatility, and Reliability at the Provider Edge

Cisco 7604 Router

The Cisco® 7604 Router is a compact, high-performance router designed in a 4-slot form factor for deployment at the network edge, where robust performance and IP/Multiprotocol Label Switching (MPLS) services are necessary to meet the requirements of both enterprises and service providers. It enables Carrier Ethernet service providers to deploy an advanced network infrastructure that supports a range of IP video and triple-play (voice, video, and data) system applications in both the residential and business services markets. The Cisco 7604 also delivers WAN and metropolitan-area network (MAN) networking solutions at the enterprise edge.

With a powerful combination of speed and services in a compact form factor, the Cisco 7604 is an outstanding choice for multiple applications. Whether deployed as a mobile Radio Access Network (RAN) preaggregation device, as a device for peering, as a residential broadband services aggregator, or as a device for Metro Ethernet aggregation and uplink, the Cisco 7604 meets requirements for redundancy, high availability, and rack density. In the point-of-presence (POP) enterprise edge or the metropolitan network edge, the Cisco 7604 sets new standards as part of the industry-leading Cisco 7600 Series Routers (Figure 1).

Figure 1. Cisco 7604 Router



With a forwarding rate of up to 144-Mpps distributed and 320-Gbps total throughput, the Cisco 7604 provides performance and reliability with options for redundant route processors and power supplies. The inclusion of two Gigabit Ethernet ports on the Cisco Catalyst® 6500 Series Supervisor Engine 720 with the Multilayer Switch Feature Card 3 (MSFC-3) or the new Cisco Route Switch Processor 720 (RSP 720) with the MSFC-4 used in the Cisco 7604 eliminates the need for a line-card slot for uplink ports. The result of this design is more efficient use of available line-card slots and increased deployment flexibility. Four Gigabit Ethernet ports are available for use in dual-route processor configurations.

Shared port adaptors (SPAa) on the SPA interface processors (SIPs) are available on the Cisco 7600 Series with interface speeds ranging from OC-3 to OC-192 and from Fast Ethernet to 10

Gigabit Ethernet. The Cisco 7600 Series can also use the Cisco 7600 Series/Catalyst 6500 Series Enhanced FlexWAN Module to take advantage of most Cisco 7200 and 7500 Port Adapters for terminating DS-0 to OC-3 speeds. By using the Cisco Catalyst 6000 Series of Ethernet line cards in conjunction with the SIP-based SPAs and the enhanced FlexWAN module, the Cisco 7600 provides a multitude of options to scale WAN connectivity from DS-0 to OC-192 and LAN connectivity from 10-Mbps Ethernet through 10 Gigabit Ethernet.

The Cisco 7604 chassis accommodates a broad selection of line cards supporting numerous applications, including:

- SPAs and SIPs (Cisco 7600 Series SPA Interface Processor-200 [SIP-200], SIP-400, and SIP-600):
  - Channelized T1/E1, Channelized T3, and Channelized OC-3/STM-1
  - OC-3/STM-1, OC-12/STM-4, OC-48/STM-16 Packet over SONET/SDH (PoS), and OC-192/STM-64 PoS
  - OC-3/STM-1 ATM, OC-12/STM-4 ATM, and OC-48/STM-16 ATM
  - Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet
- Enhanced FlexWAN module: Supporting Cisco 7200 and 7500 WAN Port Adapters from DS-0 to OC-3 for channelized and ATM interfaces and also Fast Ethernet port adapters
- High-density Ethernet services modules: 10/100 Mbps, Gigabit Ethernet, and 10 Gigabit Ethernet
- Services modules: IP Security (IPsec), firewall, distributed denial of service, intrusion detection, network analysis, and content switching commonly used, for example, in the Cisco Mobile Exchange solution
- Supervisor support: Cisco Catalyst 6500 Supervisor Engine 32 (WS-SUP32-GE-3B and WS-SUP32-10GE-3B), Cisco Catalyst 6500 Supervisor Engine 720 (WS-SUP720-3B and WS-SUP720-3BXL), and the new Cisco Route Switch Processor 720 (RSP720-3C and RSP720-3CXL)

The Cisco 7604 can be configured two ways: with a single supervisor engine and up to three line cards, or with dual supervisor engines and up to two line cards for high availability and redundancy. The Cisco 7604 also supports redundant 2700W (AC/DC) power supplies for increased availability. Understanding the need to use rack space efficiently, Cisco designed this router to be 8.75 inches tall (5 rack units [RUs]), with single-side connection management for both interface and power terminations. This setup allows placement of up to nine Cisco 7604 units per standard 7-foot rack.

Applications

The flexible Cisco 7604 Router is ideal for addressing high-performance applications such as:

- IP/MPLS provider edge
- Metro Ethernet access
- Enterprise WAN aggregation
- Mobile RAN preaggregation
- Residential subscriber aggregation
- Customer premises equipment (CPE)
- Leased line

Feature Summary

Cisco 7604 Chassis Features

- 5RU (8.75-in.) compact chassis, up to nine chassis per 7-foot rack
- Four slots (2 supervisor slots and 2 interface slots or 1 supervisor slot with 3 interface slots)
- Route processor protection capability: 1 + 1
- Power supply protection option, AC or DC: 1 + 1
- Network Equipment Building Standards (NEBS) Level 3 compliance (post-first customer shipment [FCS])
- Single-side connection management for interface and power terminations
- Side-to-side airflow

Cisco 7604 System Features

- Total throughput: 320 Gbps
- Up to 144-Mpps forwarding rate distributed

Technical Specifications

Table 1 gives specifications of the Cisco 7604.

Table 1. Product Specifications

Features	Descriptions
Physical specifications	5RU (8.75-in.) chassis 4-slot chassis Dimensions (H x W x D): 8.75 x 17.5 x 21.75 in. (22.225 x 44.45 x 55.245 cm) Weight: 40 lb Power requirements: 110 to 240 VAC, –48 to –60 VDC Mean time between failure (MTBF): 7 years for system configuration
Environmental conditions	Operating temperature: 32 to 104°F (0 to 40°C) Storage temperature: –4 to 149°F (–20 to 65°C) Relative humidity, operating: 10 to 85% noncondensing Relative humidity, storage: 5 to 95% noncondensing Operating altitude: –500 to 6500 ft
Regulatory compliance	EMC • FCC Part 15 (CFR 47) Class A • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI Class A • EN55024 • ETS300 386 • EN50082-1 • EN61000-3-2 • EN61000-3-3 Regulatory Compliance • UL 60950 • IEC 60825-1, -2 • IEC 60950 • EN 60950, EN 60825-1, -2 • CAN/CSA-C22.2 No. 60950-00 • AS/NZS 3260-1993 • 21CFR1040

Features	Descriptions
Safety and environmental standards compliance	• GR-63-Core NEBS Level 3 (post-FCS) • GR-1089-Core NEBS Level 3 (post-FCS) • ETSI 300 019 Storage Class 1.1 • ETSI 300 019 Transportation Class 2.3 • ETSI 300 019 Stationary Use Class 3.1
Minimum software release	Cisco IOS® Software Release 12.2.18SXE

Ordering Information

To place an order, visit the Cisco Ordering Home Page or refer to Table 2.

Table 2. Ordering Information

Chassis Bundles	Description
Spare Units	Note that "=" denotes a spare order
CISCO7604=	Cisco 7604 Router, mounting kit, and cable guide
PWR-2700-AC/4=	2700-WAC power supply for Cisco 7604
PWR-2700-AC/4=	2700-WDC power supply for Cisco 7604
CAB-7513ACU CAB-7513ACR CAB-7513ACSA CAB-ACS-10 CAB-AC-2500W-US1 CAB-AC-C6K-TWLK CAB-AC-2500W-EU CAB-AC-2500W-INT CAB-ACS-16 CAB-AC-16A-AUS CAB-AC-2500W-ISRL CAB-7513AC CAB-C19-CBN	AC power cord (U.K.) AC power cord (Argentina) AC power cord (South Africa) AC power cord (Swiss) Power cord, 250 VAC 16A, straight blade NEMA 6-20 plug, United States Power cord, 250 VAC 16A, twist lock NEMA L6-20 plug, United States Power cord, 250 VAC 16A, Europe Power cord, 250 VAC 16A, International AC power cord (Swiss) 16A Power Cord, 250VAC, 16A, Australia C19 Power Cord, 250VAC, 16A, Israel AC Power Cord North America (110V) Cabinet Jumper Power Cord, 250 VAC 16A, C20-C19 Connectors
FAN-MOD-4HS=	High-speed fan module for Cisco 7604 Chassis
KIT-MNTG-CG-4=	Mounting kit and cable guide for Cisco 7604
CLK-7600=	Spare clock card for Cisco 7603, Cisco 7604, Cisco 7606, or Cisco 7609

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, refer to Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco 7604 Router, visit http://www.cisco.com/go/7600 or contact your local Cisco account representative.

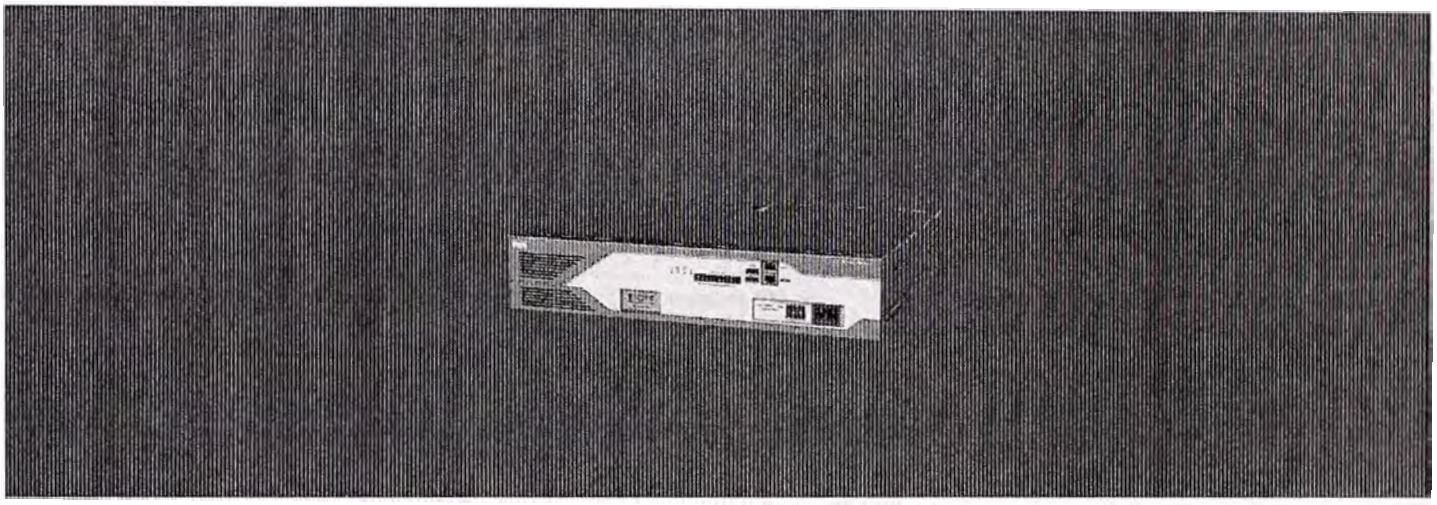
ANEXO B
DATASHEET ROUTER CISCO 2800 SERIES

Data Sheet

Cisco 2800 Series Integrated Services Routers

Cisco Systems®, Inc. is redefining best-in-class enterprise and small- to- midsize business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, video, and wireless services. Founded on 20 years of leadership and innovation, the Cisco® 2800 Series of integrated services routers (refer to Figure 1) intelligently embed data, security, voice, and wireless services into a single, resilient system for fast, scalable delivery of mission-critical business applications. The unique integrated systems architecture of the Cisco 2800 Series delivers maximum business agility and investment protection.

Figure 1. Cisco 2800 Series



PRODUCT OVERVIEW

The Cisco 2800 Series comprises four platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series.

The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

PRODUCT SPECIFICATIONS

Table 7. Chassis Specifications

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Product Architecture				
DRAM	• Default: 128 MB • Maximum: 384 MB	• Default: 256 MB • Maximum: 768 MB	• Default: 256 MB • Maximum: 1 GB	
Compact Flash	• Default: 64 MB • Maximum: 128MB	• Default: 64 MB • Maximum: 256 MB		
Fixed USB 1.1 Ports	1	2		
Onboard LAN Ports	2-10/100		2-10/100/1000	
Onboard AIM (Internal) Slot	2			
Interface Card Slots	• 4 slots; 2 slots support HWIC, WIC, VIC, or VWIC type modules • 1 slot supports WIC, VIC, or VWIC type modules • 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules		
Network-Module Slot	No	1 slot, supports NM and NME type modules	1 slot, supports NM, NME and NME-X type modules	1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules
Extension Voice Module Slot	0		1	
PVDM (DSP) Slots on Motherboard	2		3	
Integrated Hardware-Based Encryption	Yes			
VPN Hardware Acceleration (on Motherboard)	DES, 3DES, AES 128, AES 192, and AES 256			
Optional Integrated In-Line Power (PoE)	Yes, requires AC-IP power supply			
Console Port (up to 115.2 kbps)	1			
Auxiliary Port (up to 115.2 kbps)	1			
Minimum Cisco IOS Software Release	12.3(8)T			
Rack Mounting	Yes, 19-inch	Yes, 19- and 23-in. options		
Wall Mounting	No	Yes	No	No

Network Module		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
INTERFACE-CARD SUPPORT					
Ethernet Switching HWICs					
HWIC-4ESW	4-port single-wide 10/100BaseT Ethernet switch HWIC	X	X	X	X
HWIC-D-9ESW	9-port double-wide 10/100BaseT Ethernet switch HWIC	X	X	X	X
HWIC-4ESW-POE	4-port Ethernet switch HWIC, Power over Ethernet capable	X	X	X	X
HWIC-D-9-ESW-POE	9-port Ethernet switch HWIC, Power over Ethernet capable	X	X	X	X
Gigabit Ethernet HWICs					
HWIC-1GE-SFP	No	X	X	X	
Wireless HWICs					
HWIC-AP-G-A **HWIC-AP-G-E** **HWIC-AP-G-J**	802.11b/g HWIC access point interface card (A-Americas; E-Europe; J-Japan)	X	X	X	X
HWIC-AP-AG-A **HWIC-AP-AG-E** **HWIC-AP-AG-J**	802.11a/b/g HWIC access point interface card (A-Americas; E-Europe; J-Japan)	X	X	X	X
Serial HWIC/WICs					
WIC-1T	1-port high-speed serial WIC	X	X	X	X
WIC-2T	2-port high-speed serial WIC	X	X	X	X
HWIC-4T	4-port Serial HWIC	X	X	X	X
WIC-2A/S	2-port Asynch/Synch serial WIC	X	X	X	X
HWIC-4A/S	4-port Async/Sync serial HWIC	X	X	X	X
HWIC-8A/S-232	8-port Async/Sync serial HWIC, EIA-232	X	X	X	X
HWIC-8A	8-port Async HWIC	X	X	X	X
HWIC-16A	16-port Async HWIC	X	X	X	X
CSU/DSU WICs					
WIC-1DSU-T1-V2	1-port T1/Fractional-T1 DSU/CSU WIC	X	X	X	X
WIC-1DSU-56K4	1-port 4-wire 56-/64-kbps CSU/DSU WIC	X	X	X	X
ISDN BRI WICs					
WIC-1B-U-V2	1-port ISDN BRI with integrated NT1 (U interface)	X	X	X	X
WIC-1B-S/T-V3	1-port ISDN BRI with S/T interface	X	X	X	X

Network Module		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
DSL WAN Interface Cards					
WIC-1ADSL	1-port asymmetric DSL (ADSL) over POTS service WIC	X	X	X	X
WIC-1ADSL-DG	1-port ADSL over basic telephone service with dying-gasp WIC	X	X	X	X
WIC-1ADSL-I-DG	1-port ADSL over ISDN with dying-gasp WIC	X	X	X	X
WIC-1SHDSL	1-port G.shdsl WIC (two wire only)	X	X	X	X
WIC-1SHDSL-V2	1-port G.shdsl WIC (two or four wire)	X	X	X	X
WIC-1SHDSL-V3	One port G.shdsl WIC with 4-wire support	X	X	X	X
HWIC-1ADSL	1-port ADSLoPOTS HWIC	X	X	X	X
HWIC-1ADSLI	1-port ADSLolSDN HWIC	X	X	X	X
Analog Modem WICs					
WIC-1AM	1-port analog modem WIC	X	X	X	X
WIC-2AM	2-port analog modem WIC	X	X	X	X
T1, E1, and G.703 Multiflex Trunk Voice Cards and WICs					
VWIC2-1MFT-T1/E1	1-Port T1/E1 Voice/WAN with Drop & Insert	X	X	X	X
VWIC2-2MFT-T1/E1	2-Port T1/E1 Voice/WAN with Drop & Insert	X	X	X	X
VWIC2-1MFT-G703	1-Port T1/E1 Voice/WAN with D&I & unstructured E1 (G703)	X	X	X	X
VWIC2-2MFT-G703	2-Port T1/E1 Voice/WAN with D&I & unstructured E1 (G703)	X	X	X	X
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk-T1 with drop and insert	X	X	X	X
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk-T1	X	X	X	X
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk-T1	X	X	X	X
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk-E1	X	X	X	X
VWIC-1MFT-G703	1-port RJ-48 multiflex trunk-G.703	X	X	X	X
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk-E1	X	X	X	X
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk-E1 with drop and insert	X	X	X	X
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk-G.703	X	X	X	X
VICs					
VIC2-2FXS	2-port VIC-FXS	X	X	X	X
VIC2-2FXO	2-port VIC-FXO (universal)	X	X	X	X
VIC2-4FXO	4-port VIC-FXO (universal)	X	X	X	X
VIC2-2E/M	2-port VIC-E&M	X	X	X	X
VIC2-2BRI-NT/TE	2-port VIC card-BRI (NT and TE)	X	X	X	X
VIC-2DID	2-port DID voice and fax interface card	X	X	X	X
VIC-1J1	1-port digital VIC (J1) for Japan	No	X	X	X
VIC-4FXS/DID	4-port FXS or DID VIC	X	X	X	X

ANEXO C
DATASHEET SWITCH CATALYST 3750-X Y 3560-X.

Cisco Catalyst 3750-X and 3560-X Series Switches

The Cisco® Catalyst® 3750-X and 3560-X Series Switches are an enterprise-class lines of stackable and standalone switches, respectively. These switches provide high availability, scalability, security, energy efficiency, and ease of operation with innovative features such as Cisco StackPower, IEEE 802.3at Power over Ethernet Plus (PoE+) configurations, optional network modules, redundant power supplies, and Media Access Control Security (MACsec) features. The Cisco Catalyst 3750-X Series with StackWise® Plus technology provides scalability, ease of management and investment protection for the evolving business needs. The Cisco Catalyst 3750-X and 3560-X enhance productivity by enabling applications such as IP telephony, wireless, and video for borderless network experience.

Cisco Catalyst 3750-X and 3560-X Series primary features:

- 24 and 48 10/100/1000 PoE+ and non-PoE models
- Optional four Gigabit Ethernet (GbE) SFP or two 10GbE SFP+ uplink network modules
- Industry first PoE+ with 30W power on all ports in 1 rack unit (RU) form factor
- Dual redundant, modular power supplies and fans
- Media Access Control Security (MACsec) hardware-based encryption
- Open Shortest Path First (OSPF) in IP Base image
- IPv4 and IPv6 routing, Multicast routing, advanced quality of service (QoS), and security features in hardware
- Enhanced limited lifetime warranty (LLW) with next business day (NBD) advance hardware replacement and 90 day access to Cisco Technical Assistance Center (TAC) support
- Enhanced Cisco EnergyWise for operational cost optimization by measuring actual power consumption of the PoE devices, reporting, and reducing energy consumption across the network
- USB Type-A and Type-B ports for storage and console respectively and an out-of-band Ethernet management port

In addition to the above features, the Cisco Catalyst 3750-X switches also offer:

- Cisco StackPower™ technology: An innovative feature and industry first for sharing power among stack members
- Cisco StackWise Plus technology for ease of use and resiliency with 64 Gbps of throughput
- Investment protection with backward compatibility with all other models of Cisco Catalyst 3750 Series Switches

Switch Configurations

All switch models can be configured with the optional four GbE or two 10 GbE network module. The switch models are available with either the LAN Base or IP Base feature set. IP Services feature set is available as an upgrade option at the time of ordering or through a license at a later time.

Stackable Switches

Figure 1 shows the Cisco Catalyst 3750-X Series Switches (front and back).

Figure 1. Cisco Catalyst 3750-X Series Switches (Front and Back)

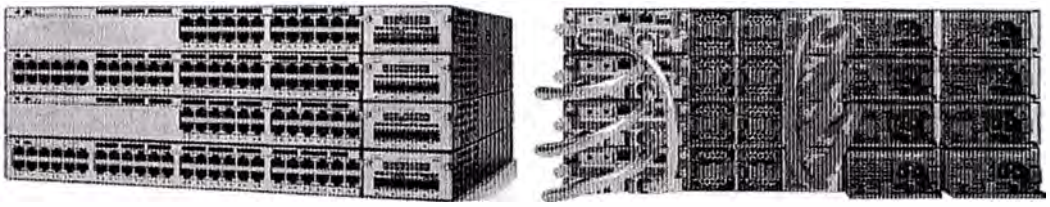


Table 1 shows the Cisco Catalyst 3750-X Series configurations.

Table 1. Cisco Catalyst 3750-X Series Configurations

Feature Set	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power	StackPower
LAN Base	WS-C3750X-24T-L	24	350W	-	Available with upgrade to IP Base
	WS-C3750X-48T-L	48			
	WS-C3750X-24P-L	24 PoE+	715W	435W	
	WS-C3750X-48P-L	48 PoE+			
	WS-C3750X-48PF-L	48 PoE+	1100W	800W	
IP Base	WS-C3750X-24T-S	24	350W	-	Yes
	WS-C3750X-48T-S	48			
	WS-C3750X-24P-S	24 PoE+	715W	435W	
	WS-C3750X-48P-S	48 PoE+			
	WS-C3750X-48PF-S	48 PoE+	1100W	800W	

Standalone Switches

Figure 2 shows Cisco Catalyst 3560-X Series Switches.

Figure 2. Cisco Catalyst 3560-X Series Switches

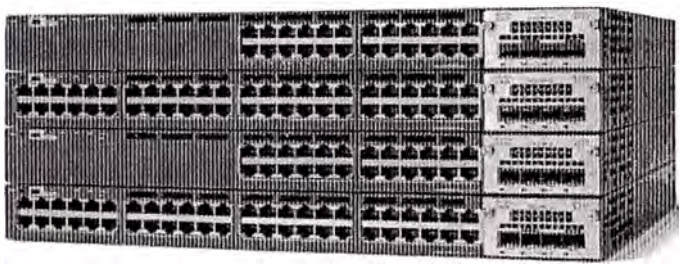


Table 2 shows the Cisco Catalyst 3560-X Series configurations.

Table 2. Cisco Catalyst 3560-X Series Configurations

Feature Set	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
LAN Base	WS-C3560X-24T-L	24	350W	-
	WS-C3560X-48T-L	48		
	WS-C3560X-24P-L	24 PoE+	715W	435W
	WS-C3560X-48P-L	48 PoE+		
	WS-C3560X-48PF-L	48 PoE+	1100W	800W
IP Base	WS-C3560X-24T-S	24	350W	-
	WS-C3560X-48T-S	48		
	WS-C3560X-24P-S	24 PoE+	715W	435W
	WS-C3560X-48P-S	48 PoE+		
	WS-C3560X-48PF-S	48 PoE+	1100W	800W

Cisco Catalyst 3750-X and 3560-X Series Software

In addition to IP Base and IP Services feature sets, the Cisco Catalyst 3750-X and 3560-X Series come with a new LAN Base feature set. The three feature sets available with all Cisco Catalyst 3750-X and 3560-X Series Switches are:

- LAN Base: Enhanced Intelligent Services
- IP Base: Baseline Enterprise Services
- IP Services: Enterprise Services

The LAN Base feature set offers enhanced intelligent services that includes comprehensive Layer 2 features, with up-to 255 VLANs. The IP Base feature set provides baseline enterprise services in addition to all LAN Base features, with 1K VLANs. IP Base also includes the support for routed access, StackPower, and MACsec. The IP Services feature set provides full enterprise services that includes advanced Layer 3 features such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Protocol Independent Multicast (PIM), and IPv6 routing such as OSPFv3 and EIGRPv6. IP Services feature set also includes the Embedded Event Manager (EEM) and IP service-level agreements (SLAs) initiator functionalities. All software feature sets support advanced security, QoS, and management features. The IP Services feature set is only available as an upgrade option at the time of ordering or through a license at a later time; there is no dedicated IP Services switch model.

The Cisco Catalyst 3750-X Series Switches with LAN Base feature set can only stack with other Cisco Catalyst 3750-X Series LAN Base switches. A mixed stack of LAN Base switch with IP Base or IP Services features set is not supported.

Customers can transparently upgrade the software feature set in the Cisco Catalyst 3750-X and 3560-X Series Switches through Cisco IOS® Software activation. Software activation authorizes and enables the Cisco IOS Software feature sets. A special file contained in the switch, called a license file, is examined by Cisco IOS Software when the switch is powered on. Based on the license's type, Cisco IOS Software activates the appropriate feature set. License types can be changed, or upgraded, to activate a different feature set. For detailed information about Software Activation, visit http://www.cisco.com/go/sa.

ANEXO D
GLOSARIO

GLOSARIO

Acuerdo de Niveles de Servicio: Comúnmente conocido por sus siglas en ingles SLA (Service Level Agreement), es un contrato escrito entre un proveedor de servicio y su cliente en el cual acuerdan los niveles para la calidad del servicio brindado.

Esquema activo - activo: Es un arreglo de 02 dispositivos funcionando a la vez, los cuales ante la red de comunicaciones funciona como uno solo.

Esquema activo- standby: Es un arreglo de 02 dispositivos con las mismas capacidades en el cual solo funciona uno de ellos manteniendo al segundo en standby para que entre en funcionamiento cuando falle el primero. Ante la red de comunicaciones funciona como un solo dispositivo.

Ancho de banda: Cantidad de información o datos que se puede enviar por una conexión de red por un periodo de tiempo dado.

AS (Autonomous System): Un sistema autónomo es el conjunto de redes y dispositivos que se encuentran administrados por una sola entidad.

AS - PATH: Es un atributo del protocolo BGP que forma un vector asociado a cada prefijo anunciado, el cual lista los identificadores de los AS que ha recorrido el anuncio. Siempre se prefiere el AS - PATH mas corto.

ATM: La tecnología ATM (Asyncronous Transfer Mode) es una tecnología de conmutación de celdas que utiliza la multiplexación por división en el tiempo asíncrona, permitiendo una ganancia estadística en la agregación de tráfico de múltiples aplicaciones. Las celdas son las unidades de transferencia de información en ATM. Estas celdas se caracterizan por tener una longitud fija de 53 octetos. La longitud fija de las celdas permite que la conmutación sea realizada por el hardware, consiguiendo con ello alcanzar altas velocidades (2, 34, 155 y 622 Mbps) de forma fácilmente escalable.

Banca Electrónica: Banca virtual, banca en línea, e-banking o genéricamente banca electrónica, es la banca a la que se puede acceder mediante Internet. Pueden ser entidades con sucursales físicas o que sólo operan por Internet o por teléfono.

Banda Ancha: El término banda ancha comúnmente se refiere al acceso de alta velocidad a Internet. Este término puede definirse simplemente como la conexión rápida a Internet que siempre está activa. Permite a un usuario enviar correos electrónicos, navegar en la web, bajar imágenes y música, ver videos, unirse a una conferencia vía web y mucho más.

BGP: El BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP

registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

BRI: BRI es un método de acceso ISDN, usado típicamente en oficinas pequeñas y hogares. Consiste de dos canales digitales de 64Kps y un canal de señalización digital y control de 16Kbps. Se lo representa a menudo como 2B+D

CEP (connection set-up error probability): Probabilidad de error en el establecimiento de la comunicación.

CFP (call set-up failure probability): Probabilidad de fallo en el establecimiento de la comunicación.

Cisco System: Cisco Systems es una empresa multinacional con sede en San Jose (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

Conector de fibra LC: Conectores LC de fibra óptica con factor de forma pequeña (SFF, Small form factor) con cierre trasero compatible con TIA FOCIS-10. Cada conector LC simplex o duplex debe ser instalable en el lugar de la instalación dentro de un espacio en módulo. Las fibras deben terminar en manguitos de acoplamiento cerámico de 1,25 mm con función de desconexión no óptica y una pérdida típica por inserción inferior a 0,10dB por par acoplado (monomodo y multimodo).

Conector de fibra ST: Conector ST significa "Straight Consejo". Fue desarrollada por AT&T y es una marca registrada de AT & T. El nombre formal tal como se define en la norma ISO / IEC es BFOC/2.5. El conector ST fue el más popular y por lo tanto primer conector estándar en la industria de la comunicación de fibra óptica.

Convertidor de medio: Los convertidores de medios permiten convertir las señales que corren en cobre a señales que corren en fibra.

CPE (Customer Premises Equipment): Son unidades terminales asociadas a equipamientos de telecomunicaciones, localizadas en el lado del suscriptor y que se encuentran conectadas con el canal de comunicaciones del proveedor o portador de información.

Datacenters: El Datacenter o Centro de Datos es aquella ubicación donde se concentran todos los recursos para el procesamiento de la información de una organización.

DHCP (Dynamic Host Configuration Protocol): es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor.

Dirección IP: Dirección lógica que identifica a un dispositivo perteneciente a una red que utiliza el protocolo IP.

Dirección MAC (Media Access Control o control de acceso al medio): Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red. Se conoce también como la dirección física en cuanto a identificar dispositivos de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits).

Dirección multicast: IP Multicast es un método para transmitir datagramas IP a un grupo de receptores interesados.

DNS (Domain Name System): El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

eBGP (External Border Gateway Protocol): Hace referencia al intercambio de información entre sistemas autónomos.

EIGRP (Enhanced Interior Gateway Routing Protocol): Protocolo de enrutamiento de gateway interior mejorado, es un protocolo de encaminamiento híbrido, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace.

Esquema activo - activo: Es un arreglo de 02 dispositivos funcionando a la vez, los cuales ante la red de comunicaciones funciona como uno solo.

Esquema activo- standby: Es un arreglo de 02 dispositivos con las mismas capacidades en el cual solo funciona uno de ellos manteniendo al segundo en standby para que entre en funcionamiento cuando falle el primero. Ante la red de comunicaciones funciona como un solo dispositivo.

Fibras Oscuras: Es la denominación popular que se atribuye a los circuitos de fibra óptica que han sido desplegados por algún operador de telecomunicaciones, pero no están siendo utilizados. Es el cliente quien brinda la tecnología apropiada que se conectara en los extremos de la fibra oscura.

Firewall: Es un dispositivo de seguridad que forma parte de un sistema o una red, diseñada para bloquear accesos no autorizados y autorizar comunicaciones.

Fuentes de poder redundantes: En esencia, se trata de una fuente de poder que en realidad incluye dos (o más) unidades dentro de él, cada uno de ellos es capaz de hacer

funcionar todo el sistema por sí mismo. Si por alguna razón hay un fallo en una de las unidades, el otro a la perfección se hará cargo para evitar la pérdida de poder del sistema.

Gateway: Gateway o la «puerta de enlace» es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation).

Host: El termino host se refiere a los dispositivos conectados a una red y que necesariamente necesitan una asignación IP.

Housing: Se refiere a alquilar espacio y energía de un datacenter para que el cliente aloje sus servidores o PCs. También es conocido con Colocation.

HSRP (Hot Standby Router Protocol): Es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

iBGP (Internal Border Gateway Protocol): Hace referencia al intercambio de información dentro de un sistema autónomo.

IETF (Internet Engineering Task Force): El Grupo Especial sobre Ingeniería de Internet es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

IGRP (Interior Gateway Routing Protocol): El Protocolo de enrutamiento de gateway interior es un protocolo propietario patentado y desarrollado por Cisco que se emplea con el protocolo TCP/IP según el modelo (OSI) Internet. La versión original del IP fue diseñada y desplegada con éxito en 1986. Se utiliza comúnmente como IGP para intercambiar datos dentro de un Sistema Autónomo, pero también se ha utilizado extensivamente como Exterior Gateway Protocol (EGP) para el enrutamiento inter-dominio.

Indisponibilidad (U): Es el tiempo que la red no se encuentra disponible para hacer uso de él.

Ingeniería de Trafico: Se denomina ingeniería de tráfico a las diferentes funciones necesarias para planificar, diseñar, proyectar, dimensionar, desarrollar y supervisar redes de telecomunicaciones.

IP de loopback: Dirección virtual que se configura en un dispositivo de red y que se utiliza mayoritariamente para diagnósticos de red.

IP QoS: Calidad de servicio en redes IP.

IP virtual: Es una dirección lógica que no tiene asignado una interfaz física.

IPSec (Internet Protocol security): Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ISDN (Integrated Services Digital Network): Red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

Juniper Networks: Multinacional dedicada a sistemas de redes y seguridad fundada en 1996. Su sede principal está Sunnyvale, California. Es actualmente junto con Enterasys, la competencia más directa de Cisco, sobre todo en Europa.

L2 QoS: Calidad de servicio a nivel de la capa 2 del modelo OSI.

LOCAL_PREF: Es un atributo del protocolo BGP que sirve para indicar preferencias en caso de tener 2 o más rutas para un mismo destino. El local_pref es válido para los router de un mismo AS.

Loops: Bucles que se forman en enlaces redundantes degradando la capacidad de la red con trafico innecesario. Los switches deben evitar la formación de loops mediante técnicas como STP, PSTV, etc.

Modelo OSI: El modelo de interconexión de sistemas abiertos, también llamado OSI (open system interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

MPLS (Multiprotocol Label Switching): Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MTTSR: Tiempo medio hasta el restablecimiento del servicio.

Multiple-instance Spanning Tree (MST): La principal ventaja de MST es que crea una instancia de spanning-tree para un grupo de vlans que nosotros definamos.

NAT (Network Address Translation): Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet.

Networking: Término utilizado para referirse a las redes de telecomunicaciones en general.

OSILAC: Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe.

OSPF (Open Shortest Path First): es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

Paradigma de ruteo hop-by-hop: Este paradigma tiene la capacidad de influir en como el router elige el siguiente salto.

PDP (premature disconnect probabilit): Probabilidad de desconexión prematura.

PDSP (premature disconnect stimulus probability): Probabilidad de estímulo de desconexión prematura.

Per-VLAN Spanning Tree Plus (PVST+): Proporciona la misma funcionalidad que PVST (Protocolo spanning tree por VLAN), incluidas las extensiones de STP propiedad de Cisco.

PIA: Porcentaje de disponibilidad del servicio MPLS.

PIU: Porcentaje de indisponibilidad del servicio MPLS.

PLR (packet loss ratio): Tasa de pérdida de paquetes.

PRI: Es el estándar para conexiones a las oficinas. Se basa en una línea T1 en los E.E.U.U., y una línea E1 en Europa. El T1 PRI consiste de 24 canales, y el E1 PRI de 32.

Procesadores Redundantes: Físicamente son 2 procesadores que trabajan en paralelo, al fallar cualquier de ellos, el sistema sigue funcionando con un solo procesador.

Puerto TCP/IP: El número de puerto define el servicio al cual hace referencia un conjunto de datos que son enviados a una dirección IP. Gracias a los puertos podemos tener distintos servicios corriendo bajo un mismo dispositivo con una sola dirección IP.

Rapid Spanning Tree Protocol (RSTP): Protocolo evolucionado a partir del Spanning Tree Protocol (STP). Brinda mayor velocidad para determinar la ruta y evitar la formación de bucles.

RDSI (Red Digital de Servicios Administrados): Red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

Red de Backbone: Red principal de datos, voz y video que tiene ramificaciones para atender a terceros.

Redes de comunicaciones: Las redes de comunicaciones o telecomunicaciones son redes que proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o comunicación en forma de datos, voz, video o cualquier mezcla de los anteriores.

Redundant Trunk Group (RTG): Protocolo propietario Juniper con funciones parecidas al protocolo STP.

RFC (Request for Comments): Son una serie de notas sobre Internet que comenzaron a publicarse en 1969.1 Se abrevian como RFC. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

RIP (Routing Information Protocol): Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

Router Maestro: Router principal que asume toda la carga en cuanto se inicia la operación de una red de datos.

Router Standby: router que se encuentra en estado de espera para asumir toda la carga del router maestro en caso de fallas.

Segmento de red: Parte de una red que dispone de un direccionamiento IP particular.

Servicios centralizados: Son el conjunto de prestaciones que se brinda a una red de agencias desde un solo punto central.

Sistema de Redundancia: Los sistemas redundantes son aquellos en los que se repiten los hardwares de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.

SLA (Service Level Agreement): Es un acuerdo de niveles de servicio, el cual se da bajo el amparo de un contrato escrito entre un proveedor de servicio y su cliente, en el cual acuerdan los niveles para la calidad del servicio brindado.

Source Routing: Método para introducir datos en una tabla de enrutamiento. Este método emplea el encaminamiento fijado en el origen, es decir la ruta óptima es determinada por el sistema final.

Spanning Tree Protocol (STP): Protocolo de capa 2, encargado de evitar la formación de bucles durante el enrutamiento de los paquetes IP en redes con redundancia.

Switch LAN: Switch encargado de interconectar los dispositivos que son administrados por el cliente.

Switch: El switch o conmutador es un dispositivo de red que opera en el nivel de enlace de datos y cuya función es interconectar dos o más segmentos de red basándose en la dirección MAC de destino de las tramas en la red.

Tablas de enrutamiento: Tablas construidas en cada router en la cual guardan información sobre las rutas a seguir para alcanzar diversos destinos. Está basado en direccionamiento IP.

Tasa de fallos (l): Porcentaje de fallas de una conexión durante un periodo de tiempo.

Tasa de pérdida de tramas: Porcentaje de tramas perdidas durante la transmisión de datos en una red de comunicaciones.

TCP (Transmission Control Protocol): TCP es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte, actualmente documentado por IETF en el RFC 793. Es un protocolo de capa 4 según el modelo OSI.

Topología hub-and-spoke: Topología en forma de estrella (centralizada).

UDP (User Datagram Protocol): Protocolo del nivel de transporte basado en el intercambio de datagramas (Paquete de datos). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión.

UIT: Unión Internacional de las Telecomunicaciones.

UIT-T: Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones.

UPS (Uninterrupted Power System): Sistema de Alimentación Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

VRRP (Virtual Router Redundancy Protocol): Es un protocolo de redundancia no propietario definido en el RFC 3768 diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Dos o más routers físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento.

BIBLIOGRAFIA

[1] Keith Hutton; Amir Ranjbar, "CCDP Self-Study: Designing Cisco Network Architectures", Cisco Press, 2004.

[2] Rob Dearborn; Rick Napolitan; Laura Whitcomb; Jeff Wilson, "The Costs of Downtime: North American Medium Businesses 2006", Infonetics Research, Inc., 2006

[3] OSILAC, "Estadísticas de América Latina y El Caribe", http://www.eclac.org/socinfo/osilac/, 2010

[4] Ivan Pepenjakl, "MPLS and VPN Archite4ctures", Cisco in Indianapolis, 2002

[5] Scott Empson, "CCNP BCMSN Portable Command Guide", Cisco Press, 2007

[6] Juniper Networks, "Juniper Networks EX Series/ Cisco Catalyst Interoperability Test Results", 2009

[7] Schneider Electric, "Comparación de la disponibilidad de diversas configuraciones de alimentación de energía redundante al rack", 2008

[8] Chris Oggerino, "High availability network fundamentals", Cisco in Indianapolis, 2001