

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA



PROYECTO DE TRABAJO DE GRADUACIÓN
PARA OPTAR POR EL GRADO DE
INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

"Desarrollo de Propuesta de Alternativas que Permitan Solventar el problema de desconexión de la red y aseguren la Provisión de Acceso Continuo a la Red Corporativa e Internet."



PRESENTADO POR:

LETICIA MERYLUZ LAZO TOBAR

ASESOR:
ING. ANGEL SORIANO

LECTOR:
ING. RAUL MARTÍNEZ

Soyapango, Agosto del 2008

**UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA**



**RECTOR
ING. FEDERICO MIGUEL HUGUET RIVERA**

**SECRETARIO GENERAL
ING. XIOMARA MARTINEZ**

**DECANO FACULTAD DE INGENIERIA
ING. ERNESTO GODOFREDO GIRON**

**AGOSTO 2008
EL SALVADOR - CENTROAMÉRICA**

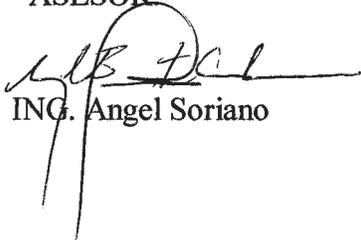
UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA



TRABAJO DE GRADUACIÓN
PARA OPTAR POR EL GRADO DE
INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

"Desarrollo de Propuesta de Alternativas que Permitan Solventar el problema de desconexión de la red y aseguren la Provisión de Acceso Continuo a la Red Corporativa e Internet."

ASESOR:



ING. Angel Soriano

LECTOR:



ING. Raúl Martínez Rivas

Soyapango, Agosto del 2008

INDICE

Dedicatoria	4
Agradecimientos	5
Introducción.	6
Capítulo I	7
Marco Referencial	7
1. Antecedentes.	8
2. Definición del Tema.	9
3. Planteamiento del Problema.	10
4. Objetivos.	11
4.1. Objetivo General.	11
4.2. Objetivos Específicos.	11
5. Justificación Del Tema.	12
6. Marco Teórico y Práctico.	13
6.1. Alcance.	13
6.2. Delimitantes.	13
6.3. Contexto.	14
Capítulo II 15	
Metodología y técnicas de la Investigación	15
2. Metodología y técnicas de la investigación.	16
2.1. Metodología.	16
2.2 Proceso del Plan de la búsqueda de alternativas.	16
2.3 Técnica Para El Plan De Alternativas De Solución A Utilizar.	18
2.3.1. Definición del Problema.	18
2.4. Desarrollo de Búsqueda de Alternativas de Solución.	19
2.5. Solución.	20
Capítulo III	21
Desarrollo del tema	21
3. Importancia del servicio de red.	22
3.1 Red WAN	23
3.2. Breve presentación de la estructuración de una red WAN	24
3.3 WAN	25
3.3.1 Red Privada	26
3.3.2 Red Pública	27
3.3.3 Red Dedicada	28

3.4. Dinámica a utilizar para realizar la búsqueda de solución.....	30
3.4.1. Proceso de búsqueda y selección	31
3.4.1.1 Modelo OSI.....	31
3.4.1.3 Búsqueda de topología WAN	33
3.4.2 Búsqueda de Tecnologías WAN	34
3.4.2.1 Breve descripción de capa física.	34
3.4.2.3 Dispositivos WAN	35
3.4.2.4 Dispositivos WAN	35
3.4.2.5 Estándares de la capa física	36
3.4.2.6 Normas WAN	36
3.4.2.7 Capa Física: WAN	38
3.5 Los protocolos de encapsulamiento WAN	38
3.5.1 Capa de Enlace de Datos: Protocolos WAN	39
3.6. Protocolos WAN	40
3.7 Esquemmatización de prototipo.	45
Propuesta 1.	45
Opción 1.1 conexión punto a punto	45
Opción 2.2 Conexión punto a punto, utilizando Internet como conexión.	46
Propuesta 2. Conexión punto a punto con opción de respaldo alternativo, lo que permite que automáticamente se presente una forma de prevenir una perdida total de conexión.	47
Propuesta 3. Conexión punto a punto conectado con una conexión alterna a partir de Internet.	48
Propuesta 4. Conexión punto a punto con opción de respaldo	49
Propuesta 5. Conexión a partir de red WAN con opción de respaldo.	50
Propuesta 6. Conexión a partir de red WAN con opción de respaldo.	51
3. 7.1 Presentación de los Routers que brinden solución de respaldo.	52
3.7.2 Selección más viable	55
3.8. Respaldo a partir del protocolo OSPF	55
3.8. Protocolos de estado de enlace	56
3.8.1 Descubriendo vecinos OSPF.....	58
3.8.2 Determinación del DR	58
3.8.3. Formando Adyacencias	60
3.8.4. Sincronización de las bases de datos	61
3.8.5. Calculando la tabla de encaminamiento	61
3.8.6. Anunciando los estados de enlace	62

3.9. Respaldo utilizando ISDN	62
3.10 Características de la reserva y de balanceo.	63
3.11. Respaldo a partir del protocolo EIGRP:	64
3.11.1 BGP como respaldo auxiliar	65
Tipos de Respaldo utilizando BGP	65
3.11.2. Respaldo Múltiple	65
3.11.2. Respaldo del tipo Par a par	66
3.11.3 .Niveles De Prevención.....	68
Conclusiones.....	70
Recomendaciones.....	71
4. ANEXOS	72
5. GLOSARIO	82
6. BIBLIOGRAFÍA.	899

Dedicatoria

Dedico toda mi investigación a, Dios todo poderoso, por haberme dado la oportunidad de crecer en un hogar donde puedo contar con la ayuda de mis padres y hermanos que a pesar de los problemas y dificultades que se me presentaron en el transcurso de mi carrera, ellos estuvieron junto a mi para apoyarme cuando más los necesite.

Leticia Meryluz Lazo Tobar (agosto del 2008)

Agradecimientos

A Dios todo poderos, por haberme dado fuerzas para continuar en mi carrera en los momentos más difíciles y por iluminarme en el transcurso de mi trabajo de graduación y finalizarlo con éxito

A mis padres, Víctor René y María Leticia, gracias por creer en mi y apoyarme en determinados momentos de mi vida, la verdad que son mis buenos amigos, puedo decir de cada uno de ellos, llevo el recuerdo de las cosas buenas que compartimos y los buenos consejos que me dieron.

A mis hermanos, son mis amigos, compañeros y consejeros de toda la vida, espero que durante el tiempo que nos resta de vida sigamos siendo así, ya que con su apoyo incondicional he podido finalizar mi trabajo de graduación.

Agradezco a todas las personas, que he conocido en el transcurso de mi carrera, a mis profesores, compañeros, lector, asesor y para aquellas que no he vuelto a ver pero dejaron una huella en mi camino así como aquellas que aun siguen presentes hasta el día de hoy. Sólo espero que las personas que me aprecian y lean esto sepan que los llevo en mi mente y corazón

Leticia Meryluz Lazo Tobar

Introducción.

La dependencia de los servicios de red para la continuidad de los negocios en general, ha planteado un reto para mantener la disponibilidad de esos servicios casi el 100%. Aun cuando nuevas tecnologías surgen con el avance del tiempo y los medios de transmisión se vuelven más confiables, es de mencionar que siempre existe la posibilidad de una falta de conectividad asociada a diversos factores impredecibles, que de una u otra forma aíslan a sitios completos del acceso a la red. Por lo que debe mencionarse que el tipo de red en la que se pretende trabajar será del tipo de red de área amplia y sus respectivas terminales, ya sean sitios centrales¹ o remotos².

La búsqueda de alternativas para mantener una conexión continua en la red, es el objeto del presente trabajo. Aun cuando una cuantiosa cantidad de compañías utilizan ya algunas opciones para solventar el problema, muchas aun no disponen o desconocen la posibilidad de optar por conexiones de respaldo a un costo más bajo, con la facilidad de lograr el objetivo de alcanzar el más alto porcentaje de disponibilidad de acceso a la red.

Al hablar de conexiones de respaldo, significa hablar también de redundancia³, donde el objetivo final es la disponibilidad de acceso a la red de manera continua, asegurando el menor número de fallas de conexión posible; en el cual se utilizarán las tecnologías adecuadas para lo que se pretende realizar; así como la selección de la posible topología que permita una conectividad continua para lograr esa disponibilidad. Este proceso debe ser automático para darse de manera imperceptible al usuario, y por supuesto sin intervención humana, excepto sólo para su configuración e instalación inicial.

¹ Referirse al glosario

² Referirse al glosario

³ Referirse al glosario

Capítulo 1

Marco Referencial

1. Antecedentes.

La oportunidad del uso de conexiones remotas fue posible en un principio gracias a la utilización de las líneas telefónicas, proveyendo conexiones a velocidades bastante bajas, que en su momento eran suficientes para el intercambio de información y el acceso a recursos remotos; en ese momento los MODEM análogos hicieron su aparición presentando opciones de transmisión de hasta 56kbps. A medida que los usuarios, el tipo de aplicación y la cantidad de datos a procesar fue cambiando, estas conexiones comenzaron a volverse lentas y poco efectivas.

A partir de esta evolución tecnológica, surgió la necesidad de contar con una nueva forma de conectividad, la cual proporcionaría una conexión permanente a menor costo, cumpliendo con la función de acoplarse a la nueva tendencia de transmisión de datos. Dando origen a las líneas dedicadas punto a punto, las cuales fueron una alternativa muy efectiva; proveyendo conexiones síncronas, evitando el overhead⁴ pudiendo transmitir a velocidades mucho mayores que las permitidas a través de línea telefónica. Dichas velocidades que oscilaban desde 64kbp hasta 2Mbps, eran entonces una opción viable para los usuarios con necesidad de conectividad local, nacional e internacional.

Así nuevas tecnologías fueron surgiendo, con el transcurso del tiempo y actualmente muchas opciones siguen vigentes y se encuentran disponibles para proporcionar una conectividad de rápido acceso a los recursos de la red, tanto de sitios centrales como remotos.

Resuelto el problema de ancho de banda y el bajo costo del acceso, la disponibilidad de la conexión paso a considerarse un aspecto prioritario. Ahora las conexiones de red de área amplia como Internet es primordial y rotundamente inaceptable no contar con ello.

⁴ Referirse al glosario

2. Definición del Tema.

El trabajo de graduación a realizar consiste en el planteamiento de opciones que nos permitan un acceso continuo e ininterrumpido a la red de las compañías y al servicio de Internet, por tal motivo se ha seleccionado el siguiente tema:

"Desarrollo de Propuesta de Alternativas que Permitan Solventar el problema de desconexión de la red y aseguren la Provisión de Acceso Continuo a la Red Corporativa e Internet."

Viendo los requerimientos actuales de las empresas en cuanto a la necesidad del servicio de red, se generó la idea de buscar alternativas de solución inmediata ante la desconexión de la red de área amplia en alguna de sus terminales⁵. En este caso el principal objetivo será mantener la red activa a pesar de las circunstancias que se presenten.

Se puede dar una pérdida de conexión en la red, pero esta puede ser reestablecida mediante tecnologías ya existentes, donde la idea principal a seguir será buscar la manera que permita solventar la falta de servicio de conexión de red ya sea de una estación central o remota, refiriéndose a las redes de área amplia. Con lo que se pretende la búsqueda de una posible alternativa de solución, conformada a partir de un conjunto de mecanismos, protocolos, hardware y tecnologías que cumplan con lo que se desea realizar; así como la selección de la posible topología que permita una conectividad continua.

Esta selección de tecnologías permitirá poner a prueba el tipo de características y funcionalidad de cada una de las posibles alternativas que se pretende mostrar, dando una idea más clara de lo que se deberá hacer a partir de las diferentes opciones de solución que se tengan. Donde se buscará encontrar una forma de solventar la falta del servicio red a partir de conexiones de respaldo ó redundancia, con el fin de disponibilidad de acceso a la red de manera prolongada ; permitiendo dar una mejor percepción de cómo unificar diferentes tecnologías en un fin común , en este caso reaccionar ante la problemática de desconexión de la red.

⁵ Redes centrales o remotas

3. Planteamiento del Problema.

Actualmente existen diferentes tecnologías de conexión de red, así también van surgiendo nuevos avances los cuales van creando una expansión de requerimientos y necesidades de la funcionalidad en el servicio de acceso a la red de área amplia como hacia Internet es primordial, todo esto genera que las grandes compañías dependan de la conectividad y eficiencia de este servicio para poder realizar la mayor parte de sus procesos laborales; pero es de mencionar que existen diferentes imprevistos que provocan una desconexión en alguna de sus terminales impidiendo así el acceso satisfactorio a la red; por tal motivo a pesar de las consecuencias que conllevan la pérdida de servicio de conexión de red e independientemente de las causas que lo generan, se hará énfasis al hecho de mantener la red activa.

Partiendo de esta problemática de desconexión se buscarán diferentes opciones que den una serie de alternativas que permitan solventar la falta de servicio de red, por lo que ofrecerá la oportunidad de hacer una depuración por medio del estudio de las características y especificaciones de cada una de las tecnologías que la conformen la búsqueda; permitiendo establecer con mejor detalle la diversidad de mecanismos, protocolos, hardware, tecnologías y topologías que cumplan con más cercanía a lo que se pretende realizar; exponiendo así diferentes opciones que permitan una solución ante la pérdida de conexión en una de las terminales de la red de área amplia.

Posteriormente ya mostradas todas las alternativas que ofrezcan una solución viable a lo que se busca; se pretenderá continuar con un siguiente paso el cual será presentar una determinada opción de solución, la que permitirá brindar un servicio de reconexión inmediata ante la pérdida de conexión de red.

4. Objetivos.

4.1. Objetivo General.

Buscar una alternativa de solución que permita dar un respaldo a las terminales de red área amplia cuando esta experimente una desconexión, donde se pretende encontrar la manera de solventar esta falta de conectividad de la red, utilizando diferentes alternativas tecnológicas actuales. Estas opciones permitirán respaldar la conexión hacia la red de forma inmediata, manteniéndola activa ; sin la necesidad de buscar las causas o razones que generaron la desconexión, ya que el punto focal a seguir será mantener la red activa a pesar de imprevistos que se presenten.

4.2. Objetivos Específicos.

- Elaborar una guía para la selección del hardware a utilizar, para proveer soluciones de acceso continuo a la red.
- Seleccionar los diferentes protocolos, medios y tecnología que proporcione una alternativa rápida y segura de conectividad a la red.
- Mostrar algunas de las posibles topologías que permitan una conectividad continua a la red de manera transparente e inmediata.
- Desarrollar un prototipo de lo que se desea; esto se hará buscando un equipo que se adecue a la alternativa de solución , donde cabe mencionar que por el valor adquisitivo de este, se hará solo una pequeña muestra de un prototipo de la alternativa que se busca.

5. Justificación Del Tema.

La evolución tecnológica que se ha generado hoy en día ha hecho que la mayoría de las compañías vivan en constante actualización, haciendo cada vez más grande la dependencia del servicio de red, principalmente las conexiones de las redes de área amplia a nivel global. Esto hace necesario el interés de prevenir situaciones que generen una pérdida de conexión de red.

Dicho motivo de prevenir situaciones emergentes futuras, se enfoca más que todo en el hecho prepararse anticipadamente a las situaciones que generan pérdida de conexión en una compañía ya sea en una estación central o remota; es de mencionar que no se tomará en consideración las causas que la generaron; sino que principalmente se centrará en la idea de poder encontrar alternativas que presenten una solución de reconexión ante el inconveniente de pérdida del servicio de red; tratando de solventar dicha pérdida de conexión de manera inmediata e imperceptible para los usuarios.

Cabe mencionar que anteriormente han existido tecnologías que han servido de respaldo a la red los cuales cumplieron con el fin de mantener la red estable a pesar de la pérdidas de conexión; dicho conocimiento generó la idea de buscar una alternativas de solución a partir de mecanismos, protocolos, hardware y tecnologías que proporcionen una cercana compatibilidad con lo que se pretende realizar; así como de la posible topología que permita una conectividad continua. Presentado una gama de posibles soluciones con tecnologías actuales, las cuales permitirán dar un respaldo de una manera similar a una red real; pero con la diferencia que disminuirán los costos.

6. Marco Teórico y Práctico.

6.1. Alcance.

Lo que se desea es crear una búsqueda de solución sobre una alternativa que sirva como soporte a una red de área amplia y sus respectivas terminales, para una corporación en situaciones que generen una pérdida de conexión ; por lo que se observarán las posibles maneras que permitan realizar la búsqueda de una solución ante una repentina desconexión, por tal motivo generó la necesidad de seccionar el proceso de trabajo en cuatro partes las cuales son:

- El primer paso será realizar una guía que permita la selección del hardware a utilizar para proveer soluciones de acceso continuo a la red.
- Segundo paso será la selección de los diferentes tipos de protocolos, medios y tecnología que permitan una alternativa eficaz y confiable de conectividad a la red
- El tercer paso será presentar algunas de las posibles topologías que permitan generar una conectividad continua a la red de manera eficiente.
- El cuarto paso será generar un prototipo de lo que se pretende; lo cual se conseguirá buscando un equipo que se mejor se adapte a la alternativa de solución , donde por el valor adquisitivo de este, se hará solo una pequeña prueba de un prototipo de lo que se busca.

6.2. Delimitantes.

En este caso cabe mencionar que existe un límite en el momento de materializar la información ya que no se podrá poner a prueba una muestra integra del producto final, en este caso se presentará una pequeña demostración; por la razón de que el valor económico del equipo impide poder adquirirlo por completamente . Lo anterior amerita decir que no se puede poner un nivel tangible aproximado sobre el límite de hasta donde se podrá llegar con la prueba de eficiencia de lo que se va a documentar.

6.3. Contexto.

Existen diferentes tecnologías de acceso, las cuales han sido utilizadas anteriormente como respaldo en situaciones en las que la conexión a la red se pierde, pero cabe mencionar que dichas tecnologías respondían a las necesidades y requerimientos considerados en la actualidad de poco uso. Donde a pesar de esto, dicho conocimiento será la base por medio del cual se desarrollará la idea de cómo generar un respaldo que prevenga una pérdida o desconexión en las terminales de red de área amplia; ya que independientemente que hayan evolucionado las tecnologías y velocidades de transmisión de datos; el fenómeno de pérdida de conexión aún continúa vigente y sigue causando grandes pérdidas hoy en día.

Por tal razón se ve necesario unificar mecanismos, protocolos, hardware, tecnologías y topologías que más se asemejen a los requerimientos de búsqueda de solución ante una desconexión. Donde se estudiarán todas sus características y especificaciones de funcionalidad de manera individual; permitiendo tener una idea más clara de cual conexión de respaldo ó redundancia, será la más viable para poder realizar un respaldo auxiliar el que permitirá dar soporte a la red en situaciones que generen una desconexión; encontrando así una virtud más a las tecnologías actuales, así como una alternativa que solvete un inconveniente en la falta de conexión.

Capítulo 2

Metodología y técnicas de la Investigación

2. Metodología y técnicas de la investigación.

2.1. Metodología.

El hecho de decidir por el tipo de metodología utilizar, generó la inquietud de cómo realizar la búsqueda de solución sobre el tema propuesto; en este caso se partió de la premisa de que dicho método se acople mejor a los requerimientos que se necesitan para el desarrollo de la búsqueda de una solución. En este caso, se realizará una recopilación de las posibles alternativas de solución que permitirán dar a conocer los requerimientos de implementación así como características de la red a partir de conexiones de respaldo ó redundancia; dando la pauta de poder manipular los datos de las diferentes herramientas tecnológicas que permitan la búsqueda de diferentes opciones que permitan brindar alternativas de solución.

Por tal razón se vio de manera aceptable el escoger esta metodología de gestión de proyectos de ingeniería, ya que presenta la fusión entre la teoría y la práctica consolidando así una forma aceptable para el desarrollo de búsqueda del plan de solución.

A continuación se presentará un esquema con los posibles puntos a trabajar:
2.2 Proceso del Plan de la búsqueda de alternativas. 8

- Pasos: 8

La calidad del Plan de búsqueda de alternativas de solución es clave para el éxito de la misma. Este incluye las siguientes actividades:

- Revisión de los documentos de entrada
- Desarrollar el cronograma para completar el plan
- Identificar la herramienta de gestión de documentación adecuada
- Esquematizar cómo se usará el plan y cómo se actualizará

- Preparar la introducción del Plan de búsquedas de alternativas.

Los siguientes aspectos deben quedar definidos y convenidos:

Propósito y objetivo, Alcance, Producto de la búsqueda de alternativas de solución.

- Definir la estructura de la búsqueda de solución

- Desarrollar la estructura del desglosamiento de actividades de estudio para el desarrollo de alternativas del plan de solución, en este caso en cuanto a los mecanismos, protocolos, hardware y tecnologías que cumplan con los requisitos de lo que se pretende realizar; así como la selección de la posible topología que permita una conectividad continua .

- Desarrollar los planes preliminares de la búsqueda de alternativas que permitan dar una solución.
- Revisar los planes de búsqueda de solución.
- Identificar las características y requerimientos específicas a nivel del desarrollo que permitan dar opciones de solución.
- Integrar los planes de desarrollo / guías

Se extraen datos claves de cada plan de la búsqueda de alternativas de una solución, a continuación se dará una pequeña muestra de las partes que la conformarán:

- ✓ Documentos de referencia
 - ✓ Estructura del plan que permita dar opciones de solución.
 - ✓ Cómo se trabajará el plan de solución.
 - ✓ Proceso de control de cambios.
 - ✓ Indagación de características y requerimientos de las posibles alternativas a utilizar.
- Definir recursos y estimar costos.
 - Definir revisiones y aprobaciones.
 - Conducir la planificación de administración de riesgos.

El propósito de la planificación de la administración de riesgos es reducir la ocurrencia del riesgo, para minimizar el impacto si ocurre el riesgo y proponer acciones apropiadas si se requiere.

- Hacer pruebas que permitan descubrir las opciones más factibles, a partir de el estudio de las características y requerimientos de cada uno de ellos.

El fin de este, será poner en práctica y poder aplicar los conocimientos en conjunto para poder encontrar un resultado que pueda solventar perdida de conexión.

□ Optimizar los planes

En esta etapa se analizan los potenciales que aplican al uso de recursos, prioridades del plan de medidas e implementaciones de alternativas. Donde podría verse en la necesidad de analizar distintos escenarios, cada uno basado en premisas distintas que afectan a los recursos, prioridades, asignación de actividades, cronograma y otros factores claves.

□ Completar los borradores finales

Se efectúan los cambios finales a los planes de resolución.

2.3 Técnica Para El Plan De Alternativas De Solución A Utilizar.

2.3.1. Definición del Problema.

En este caso debe de mencionarse que el problema a tratar en sí será mantener la red activa a pesar de la pérdida de conexión. Donde el fin principal será encontrar alternativas de solución a partir tecnologías actuales las cuales permitan ser respaldo a la red, con lo que se podrán solventar la falta de conexión de red en determinados momentos. Viendo esta necesidad de tener un servicio confiable y activo se ve la prioridad de buscar diferentes alternativas de solución a partir de mecanismos, protocolos, hardware y tecnologías que cumplan con mayor cercanía posible con los requisitos de lo que se pretende realizar; así como la selección de la topología que permita una conectividad continua de la red. Los cuales tendrán la facultad de trabajar de manera unificada y así poder reaccionar ante una pérdida de conexión, manteniendo la continuidad en el, servicio generando así estabilidad permanente en la red.

2.4. Desarrollo de Búsqueda de Alternativas de Solución.

Las técnicas de alternativas de solución concretas aplicables para resolver un problema varían según el tipo de situación de que se trate y según la experiencia y conocimientos. Sin embargo, es posible señalar algunos pasos y procedimientos generales que pueden combinarse para ayudar a generar la búsqueda una alternativa de solución, ante la pérdida de conexión, estos pueden ser:

a. Dominar el campo, En este caso se enfocará en el hecho de buscar una alternativa que permita reactivar la red en el momento que se de una repentina pérdida a de conectividad o acceso a la red; donde en este caso se buscarán todos los requerimientos y características de las tecnologías apropiadas para poder encontrar una alternativa de solución.

b. Simplificar el problema, Ya teniendo la idea de las posibles alternativas a trabajar se seleccionarán aquellas que más se adecuen a suplir la necesidad de reactivar la red en el momento en que esta sufra una desconexión.

c. Descomponer y recomponer el problema En este caso que por medio de la selección de alternativas se irá conociendo y depurando la información con la que se trabajará , destacando así lo más importante e indispensable para la búsqueda de alternativas de solución.

D. Establecer analogías, Comparación de las características de funcionalidad entre las alternativas propuestas y sus posibles soluciones de respaldo ante una pérdida de conexión en la red.

e. Generalizar el problema, La pérdida de conectividad no será relevante, más que todo se le dará énfasis a la búsqueda de alternativas de solución que permitan crear un respaldo de conexión en la red.

f. Explorar direcciones plausibles, una vez se identifique el problema de pérdida de conexión se buscará la alternativa más viable, el cual pueda atacar el problema con mayor eficiencia logrando alcanzar el objetivo de reactivar la red .

g. Discutir el problema Tratar de depurar la información de las posibles alternativas de solución, hasta lograr obtener una solución eficiente para solventar el problema de pérdida de conexión.

2.5. Solución.

Anteriormente han existido tecnologías que originalmente fueron creadas para otros fines pero cabe mencionar que a la vez se ha podido sacar provecho de diferentes maneras , un ejemplo a mencionar es el hecho se crearon respaldos para mantener la red activa a pesar de la circunstancias de perdidas de conexión. Dichas implementaciones previas no poseen una basta documentación, por el hecho de ser del tipo de tecnología alternativa; pero es de mencionar que a partir de estos principios se posee una idea contextual, lo que permitirá dar una idea más clara de lo que se desea buscar. En este caso se pretende unificar diferentes conocimientos tecnológicos para poder así establecer un fin común, el cual es la búsqueda de una alternativa que genere una solución ante la perdida de conexión a la red.

Contextualmente se tiene la idea de que para crear una red de respaldo se necesita un protocolo, un medio y una tecnología adecuada donde de una forma unificada permitirá mantener la conexión de la red; todo esto se llevará a cabo a partir de la búsqueda de las tecnologías actuales donde consecutivamente permitirá hacer una depuración y selección de las herramientas más apropiadas que permitan crear un respaldo de conexión manteniendo la red en un estado funcional.

Capítulo 3

Desarrollo del tema

3. Importancia del servicio de red.

Cada vez más, las empresas requieren disponibilidad continua conexión de red ya que el tiempo de actividad del uso del mismo va en aumento y es poco probable obtener un nivel de actividad al cien por ciento, pero por las necesidades actuales de servicio de conexión hace generar la búsqueda que permita alcanzar el tiempo mas cercano a ese nivel de exigencia de servicio. Donde es necesario contar con redes altamente confiables que logren alcanzar este objetivo, ya que la falta de conectividad implica que la sumarización de los períodos de inactividad equivalentes a perdidas económicas sin precedentes; por lo que se buscarán alternativas que logren el objetivo de generar estabilidad en la red.

La confiabilidad de conexión se logra con equipos y diseños de red que sean tolerantes a las fallas. Dichas redes deben estar diseñadas para reconverger rápidamente de modo que la falla se pase por alto.

En la actualidad existen diferentes maneras de interconexión de red, las cuales han sido creadas para poder solventar en gran medida la gran demanda de conectividad entre terminales independientemente de la necesidad ,posición geográfica o tamaño de los requerimientos de las compañías; dichas tecnologías ofrecen el servicio adaptabilidad y escalabilidad permitiendo cumplir con lo que las empresas solicitan.

Por tal razón se ve con beneficio la búsqueda de alternativas de solución ante la perdida de conexión de red, lo que presenta una forma viable de brindar la idea de el tipo tecnologías que existentes en el mercado, así como la manera más detallada de como enfrentar el problema de desconexión y buscar una pronta solución partiendo de las herramientas tecnológicas actuales. Dado que la tecnología ha avanzado notablemente se puede tener una idea concisa de como se desarrolla la interconexión entre terminales, ya que todas estas han sido debidamente clasificadas y seleccionadas de acuerdo a sus características y funcionalidad.

A pesar de todo este desarrollo y organización tecnológica es necesario mencionar que siempre se dan inconvenientes que hacen que este proceso se paralice o sufra algún inconveniente de perdida de conexión, por lo que se hace indispensable aplicar de una manera auxiliar las tecnologías existentes, para poder solventar dicha perdida.

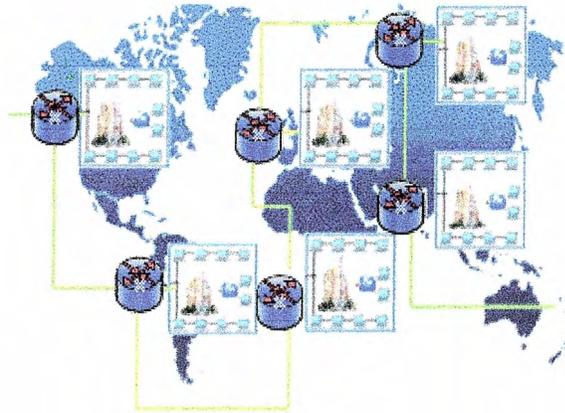


Figura 1. Representa el auge i nivel de importancia de las redes WAN en las empresas a nivel global

En este caso se va a trabajar con la red WAN, por el hecho de que una red de esta naturaleza, se considera actualmente como una intranet ya que independientemente de la ubicación geográfica ; esta pertenecerá a la misma red la que continuará siendo de la misma corporación; por ende sus características aplican con lo que se desea encontrar y a continuación se dará una breve descripción de lo que consiste :

3.1 Red WAN

Es una red que tiene expansión geográfica amplia lo que permite un nivel de conectividad mayor. La manera más eficiente de utilizar la WAN es por medio del INTERNET⁶ ya que es una herramienta libre que presta servicio a nivel mundial, hay que mencionar que una red WAN también puede ser una red privada ,donde una de sus características de conectividad es que no necesariamente la red corporativa tiene estar conectada con otras redes de forma permanente.

Características:

- Cubren una región, país o continente
- Generalmente se dividen en subredes intercomunicadas.
- Conectan múltiples LAN.
- Una subred, donde conectan uno o varios hosts

⁶ Referirse al Glosario

3.2. Breve presentación de la estructuración de una red WAN

Ya teniendo clara la idea de que tipo de red se va utilizar se ve necesario conocer cada una de las partes que la componen, para así poder desglosar e identificar la posible solución ante la perdida e conexión, por lo que a continuación presenta su estructuración:

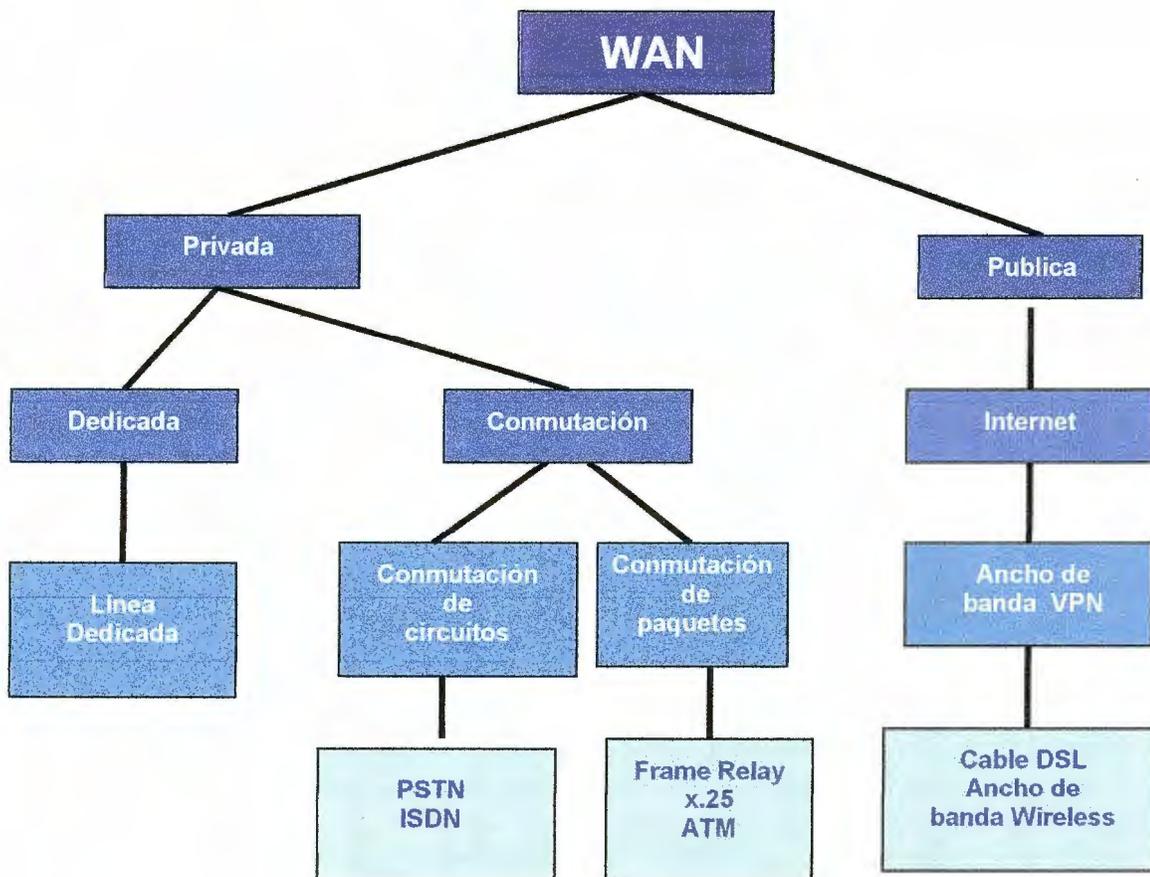


Figura 2. Esquemmatización de la red WAN y los elementos que la componen

3.3 WAN

A continuación se presenta un breve análisis de cómo está organizada la red WAN con sus respectivas características y funciones, con el fin principal de presentar una idea de todos los medios y tecnologías actuales con los que se cuentan para mantener la red activa. El mejor ejemplo de esto es INTERNET el cual es considerado como una red WAN por excelencia, por el hecho de ser una red de gran dimensión y presentar facilidad de acceso; por tal razón es considerada como una red pública.

Por otro lado, se encuentra la red privada que es esencialmente dos o más redes LAN conectadas de un punto a otro, con la diferencia que posee accesos restringidos, presentando limitantes de acceso a cualquier usuario ajeno a la red. Es de mencionar que independientemente de las características mencionadas de ambas redes estas forman en conjunto la red WAN, donde es la agrupación de un todo independientemente de que la red sea Pública o Privada en este caso la red WAN la conforman diferentes conexiones de redes a nivel global.

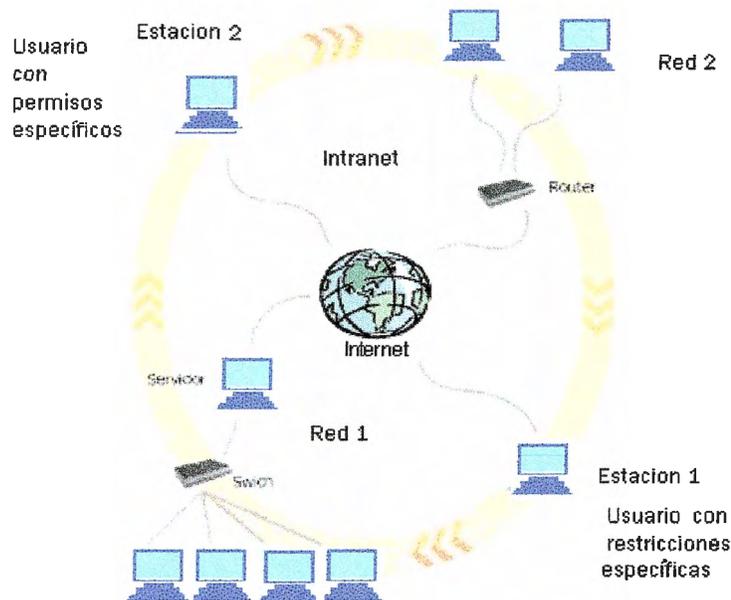


Figura 3. Esquema como están formadas las redes, donde se aplica el término intranet para referirse a una red interna y Internet a una red pública a nivel global.

Por ejemplo una red corporativa, es una red WAN que funciona en una línea dedicada por lo que es considerada una WAN privada, pues no hay tráfico con acceso al público en la línea; pero dicha conexión de la red corporativa permanece activa con la ayuda de Internet, lo que permite que la red se encuentre comunicada con el exterior. Resguardando de manera confidencial información de interés de la compañía, independientemente de la posición geográfica.

En este caso por el amplio nivel de uso de la red WAN se ve de gran interés el hecho de aplicar este tipo de red como alternativa ante la pérdida de conexión, por lo que se ve necesario presentar en lo que consiste la red WAN desde sus diferentes perspectivas para entender de mejor manera como se va resolver el problema de pérdida de conexión.

3.3.1 Red Privada

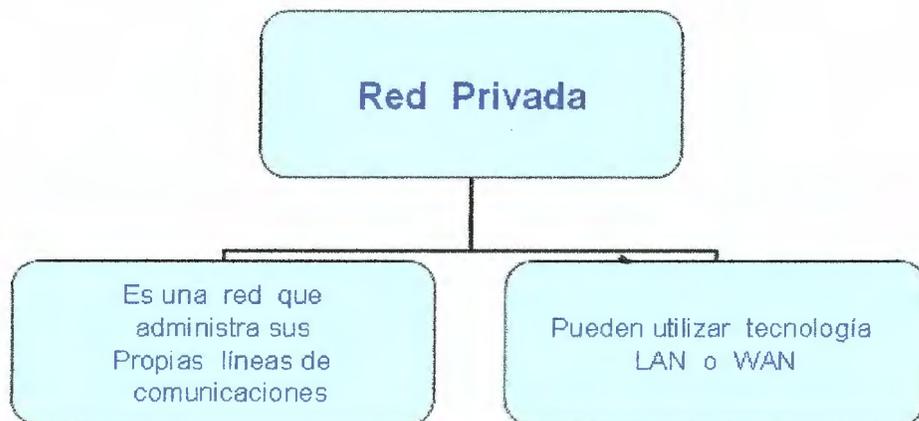


Figura 4. Representación esquemática de lo que consisten las redes privadas

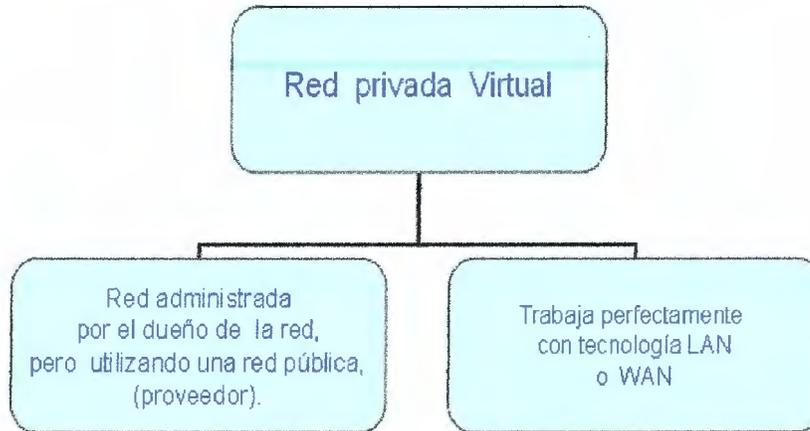


Figura 5. Representación esquemática de lo que consisten las redes privadas virtuales

En este caso se ve la ventaja de usar una red privada virtual ya que esta permite conexión con la red pública, lo que favorece la necesidad que se desea solventar, ya que se hará con ayuda de Internet dicho proceso de respaldo.

3.3.2 Red Pública

Las redes públicas son los recursos de telecomunicación de área extensa pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción. El ejemplo más tangible es el INTERNET el cual ofrece un servicio a nivel global.

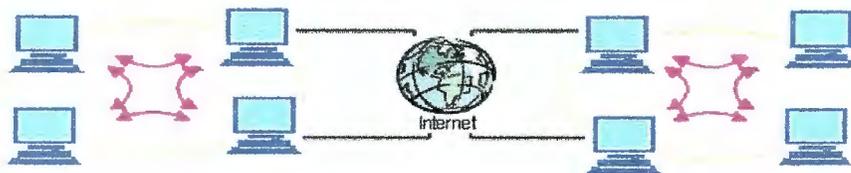


Figura 6. Representación que ejemplifica el hecho de como Internet sirve de medio de conexión entre dos redes distintas

La ventaja de utilizar una red pública para el desarrollo de la solución de conexión en este caso INTERNET, es el hecho de que permite su libre manipulación eventos y protocolos, ya que esta es una red pública .

La cual puede ser empleada desde cualquier parte del mundo sin mayores restricciones que faciliten su uso. Esto ofrece una gran ventaja a la hora de buscar una alternativa de solución, ante la pérdida de conexión, ya que INTERNET presenta facilidad de manipulación. Permitiendo el hecho de poder trabajar y aplicar la tecnología respectiva, para solventar la pérdida de conexión de una red corporativa; en este caso tanto la red privada como la pública trabajaran en conjunto para el mismo fin lo que permitirá mantener la red activa a pesar de los imprevistos.

Ya teniendo una idea de las generalidades de la red WAN, debe de enfatizarse de que existirá un punto de partida el cual será el hecho que existe una pérdida de conexión en la red. Donde el enfoque será buscar alternativas que solventen la falta de conectividad ;por lo que se ve de gran importancia el hecho de conocer componentes específicos de la red WAN, así como sus respectivas de características en el mercado para así poder buscar y depurar la información de tal manera que se pueda solventar la pérdida de conexión.

3.3.3 Red Dedicada

Una red dedicada es una denominación que usualmente se reserva para redes de comunicaciones, en las cuáles existe un único tipo de tráfico, donde poseen objetivos de calidad establecidos explícitamente en el contrato entre el operador y los usuarios. Normalmente se utilizan para garantizar la disponibilidad de un fragmento de información bajo ciertas condiciones, las cuales presenten facilidades de transporte, para los grandes usuarios de comunicaciones.

Las tecnologías que soportan estas redes dedicadas dependen en primer lugar, del tipo de información considerado: voz, vídeo (+ audio) o datos. Donde los routers juegan un papel clave, ya que se utilizan para dirigir comunicaciones entre LANs que a la vez permiten la comunicación en una WAN.

El Router, instalado en la línea dedicada, lee "envuelve" o los encabezados de cada paquete de los datos que pasan a través del WAN, enviándolo a la LAN apropiada. Cuando el paquete llega el LAN, un dispositivo llamado un SWITCH, envía el paquete de los datos activado a la máquina correcta.

Por lo tanto, la WAN actúa como un interfaz entre LAN para la comunicación interurbana, dicha función permite idea de crear respaldos alternativos para poder mantener la red activa.

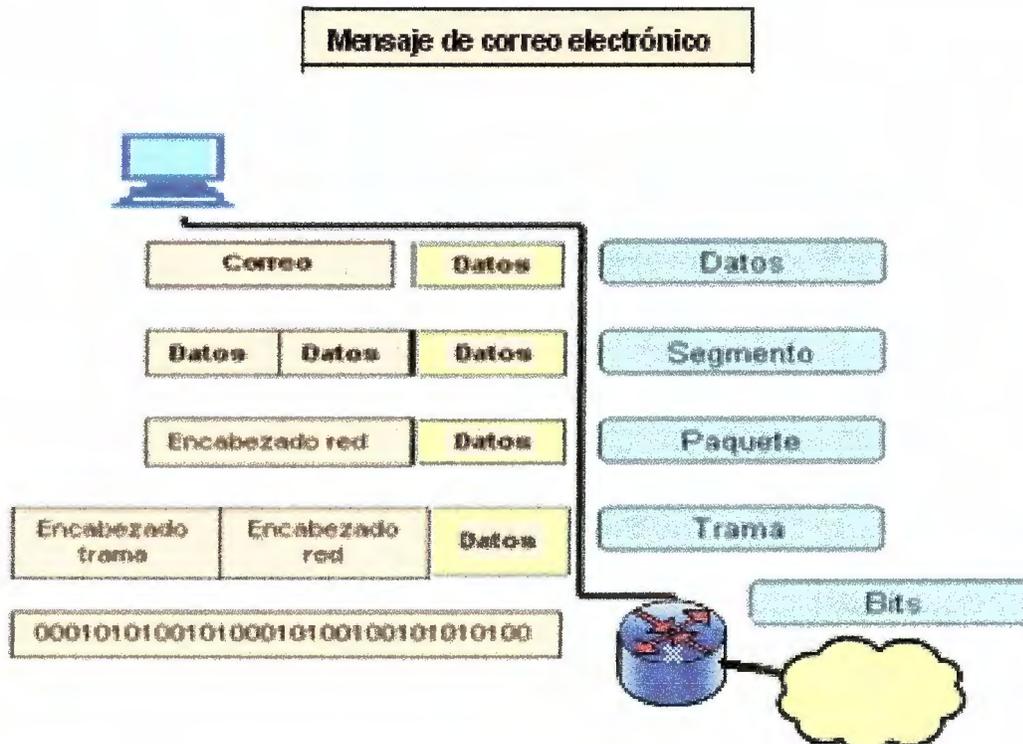


Figura 7. Ejemplificación del proceso de empaquetado de información desde que su inicio como un correo convencional, siguiendo un proceso de segmentación de los datos enviados hasta llegar al punto de entramado de datos, lo cual es un proceso que permite la fácil distribución de la información desde el origen hasta el destino el cual esta etiquetado en el encabezado con la dirección de red a la cual se quiere dirigir la información en toda la red WAN.

Viendo la importancia de las redes dedicadas y su funcionalidad actual se ve necesario mantener el servicio de conectividad en optimas condiciones, por lo que la red dedicada necesita de la búsqueda de una alternativa que brinde respaldo ante la perdida de conexión, tomando en cuenta los factores que componen una WAN.

3.4. Dinámica a utilizar para realizar la búsqueda de solución.

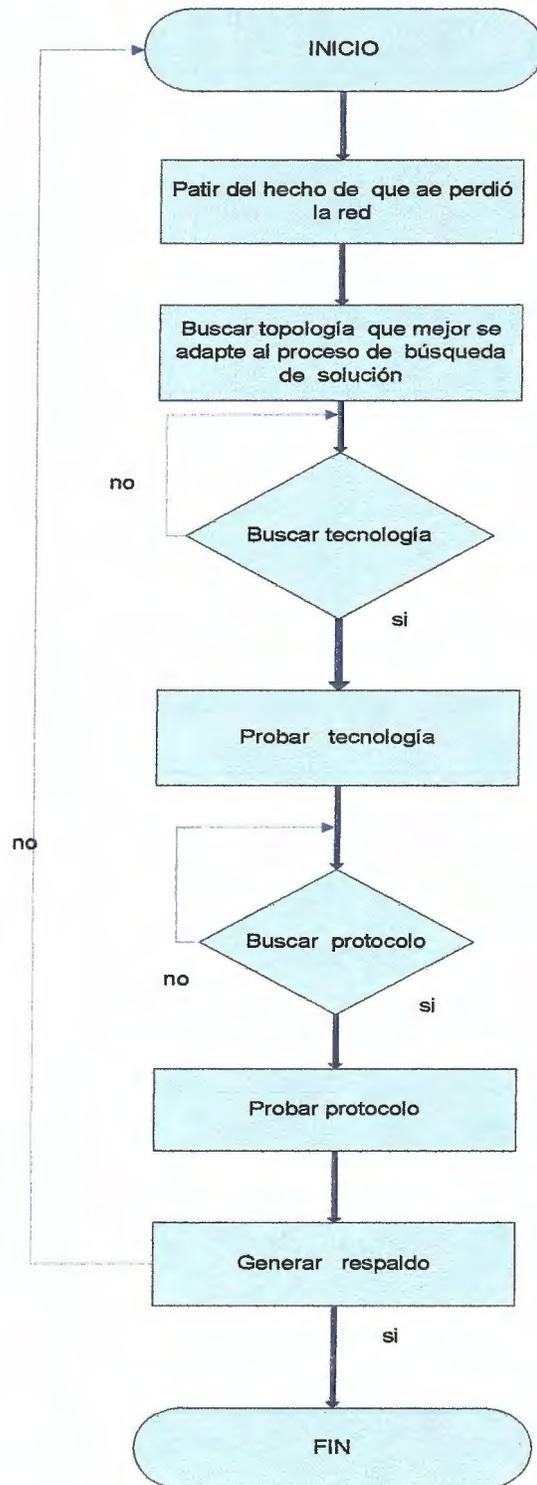


Figura 8 El presente diagrama de flujo representa el proceso de búsqueda, recopilación y selección de elementos y tecnologías existentes para encontrar una solución ante la pérdida de conexión

El anterior diagrama de flujo presenta una idea más clara y ordenada de como se realizará la búsqueda de todos los componentes que conformarán la solución de perdidas de conexión, por lo que a continuación se enunciarán las características y especificaciones de cada componente de la tecnología WAN específicamente lo cual permitirá dar una idea más clara de cual será la opción más viable para lograr el objetivo de búsqueda de conexión.

3.4.1. Proceso de búsqueda y selección

Ya teniendo la idea de cómo será el proceso de búsqueda y selección se presentará cada uno de los posibles elementos que serán necesarios para poder generar un solución factible ante la pedida de conectividad, por lo que a continuación se dará una breve introducción.

3.4.1.1 Modelo OSI

Por como ha avanzado la tecnología y la forma en que se ha implementado, se puede tener una idea de como se desarrolla la interconexión entre terminales; ya que han sido clasificadas de acuerdo a sus características y funcionalidad, lo que permite tener idea más clara y ordenada sobre lo que se desea hacer. Todo esto a partir del modelo OSI (Open Systems Interconexión, Interconexión de sistemas abiertos); el cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red.



Figura 9. Representación de las 7 capas que conforman el modelo OSI.

En el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los servicios son implementados realmente.

Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora. Gracias a esto las redes corporativas actuales pueden permanecer interconectadas, permitiendo la facilidad de comunicación e intercambio de información; lo que da la opción de poseer un control de el flujo de datos en la red , así como el continuo trafico de información en la misma.

Dado el hecho que se quiere buscar una alternativa de solución ante la perdida de conexión se debe mencionar que se hará énfasis a determinadas capas del modelo OSI , las cuales servirán para lo que se pretende realizar, es de enfatizar de que como se trabajará con la red WAN; se hará énfasis a las tres ultimas capas del nivel OSI las cuales serán de gran utilidad para poder desarrollar una solución conveniente ,la cual mencionará a continuación:

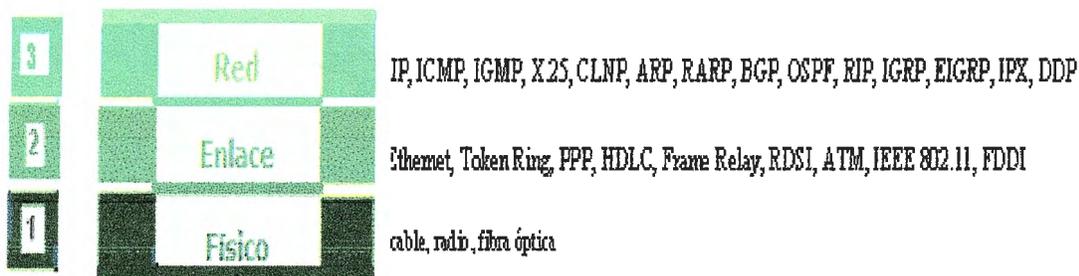


Figura 10. En el esquema anterior se presentan las 3 ultimas capas de el nivel OSI, así como sus respectivos protocolos, las cuales son las más utilizadas a nivel WAN para todo lo concerniente a la comunicación e intercambio de información.

3.4.1.3 Búsqueda de topología WAN

Al igual que la topología LAN, la topología⁷ WAN poseen características similares en cuanto a diseño de las mismas; en este caso es necesario familiarizarse con cada una de ellas para así poder tener una noción mas clara de la topología que mas se adecue a solventar la búsqueda de solución; por lo que continuación se presenta un breve esquema:

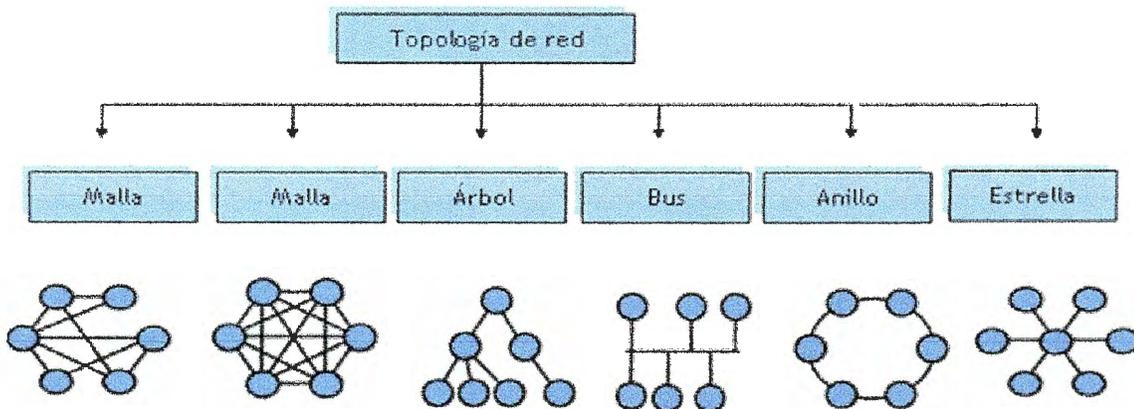


Figura 11. Esquema que representa los diferentes tipos de tecnologías existentes en el mercado

Topología más eficiente para realizar respaldo.

A partir de la información recopilada se ve la ventaja de tener una topología tipo malla completa, ya que si se estropea algún un nodo en este tipo de topología; los demás nodos pueden seguir funcionando. Por este motivo esta topología se apega mejor a la necesidad de solución que se anda buscando.

⁷ Referirse al Anexo

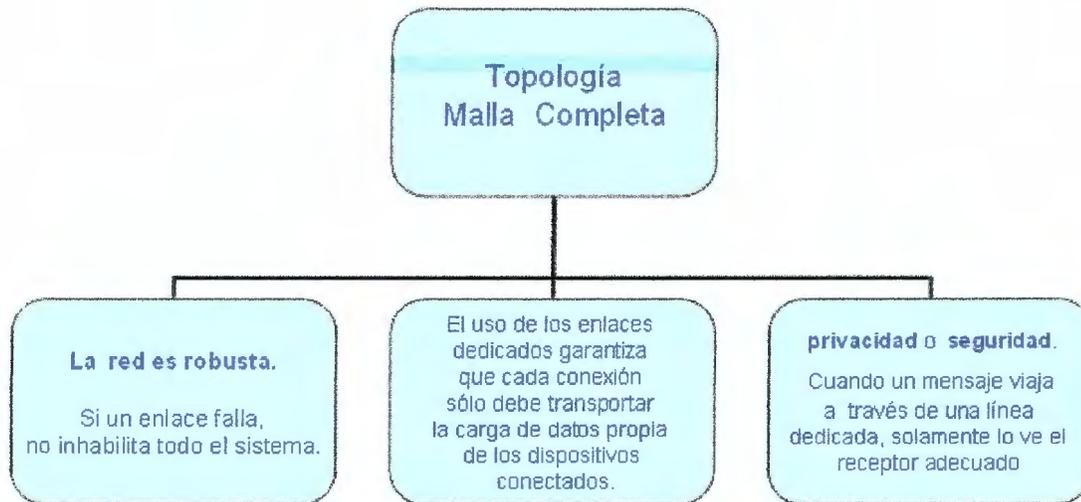


Figura 12. El esquema anterior confirma el hecho que la topología malla cumple con las características requeridas para la búsqueda de respaldo de conexión en una red WAN.

3.4.2 Búsqueda de Tecnologías WAN

Por medio de búsqueda de tecnologías de punta, se pretende respetar los estándares de uso y fabricación de redes WAN; lo que permitirá facilitar el objetivo de búsqueda de equipo que se acerque mas a los requerimientos que se necesitan para encontrar una solución que sirva de respaldo a una red corporativa ante la perdida de conexión.

3.4.2.1 Breve descripción de capa física.

La Capa Física, es la que se encarga de las conexiones de la computadora hacia la red; gracias a estos medios tangibles, existe la comunicación e intercambio de información constante. Por lo que se ve necesario saber las características y especificaciones de cada uno de sus componentes, para entender con que tipo de herramientas tecnológicas se cuentan en la actualidad y así poder tener una idea más conveniente de como implementar los elementos necesarios para generar un respaldo.

3.4.2.3 Dispositivos WAN

A continuación se presentan algunos dispositivos WAN, los cuales permitirán dar una idea de el tipo de tecnología que se podría utilizar, para poder solventar la pérdida de conexión, dichos dispositivos permiten la relación entre la red pública como privada; así como la relación de identificación de un respectivo protocolo de trabajo.

3.4.2.4 Dispositivos WAN

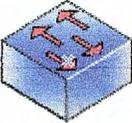
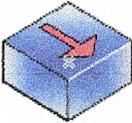
SWITCH	
MODEM	
ROUTER	

Figura 13. Representación de los principales dispositivos que se utilizan para la creación de la red WAN, referirse al glosario para saber en que consiste cada dispositivo.

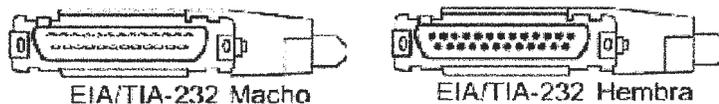
3.4.2.5 Estándares de la capa física

Dichas tecnologías poseen normas o estándares tanto eléctricas (EIA)⁸ como de telecomunicación (TIA)⁹, las cuales permiten dar las especificaciones necesarias para determinar que tipo de equipo cumple de mejor manera con los requerimientos de búsqueda de conexión así como las respectivas restricciones de uso, facilitando la selección de los elementos físicos que generen respaldo.

3.4.2.6 Normas WAN

Dichas normas cumplen con los estándares eléctricos EIA y de telecomunicación TIA correspondientes, donde existe un conector macho y un conector hembra para realizar la conexión, permitiendo ser un medio de transporte y comunicación de datos entre los routers, por los que a continuación se mencionan :

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



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

⁸ Referirse al glosario

⁹ Referirse al glosario



EIA/TIA-449 Hembra

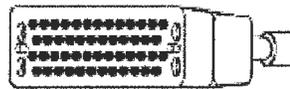


EIA/TIA-449 Macho

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



V.35 Macho



V.35 Hembra

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



X.21 Macho



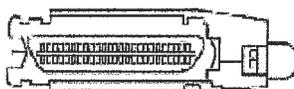
X.21 Hembra

- **EIA-530:** Presenta el mismo conjunto de señales que la EIA-232D.



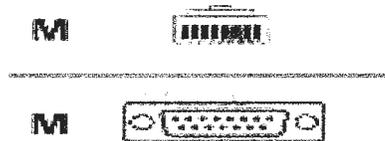
EIA-530 Macho

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



EIA-613 HSSI Macho

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



3.4.2.7 Capa Física: WAN

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio y el DTE es el dispositivo asociado. En este caso el propósito principal del DCE es suministrar una interfaz para el DTE al enlace de comunicación en la nube WAN.

A partir de este conocimiento se conectan los dispositivos físicos antes mencionados para que se de un conexión entre dos routers diferentes.

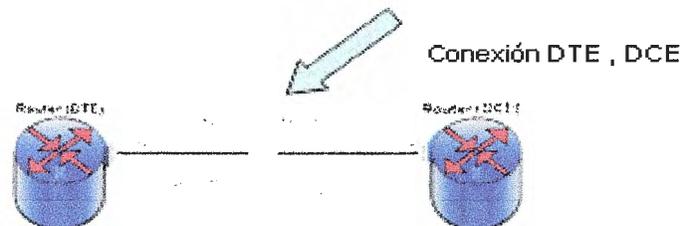


Figura 14. Representación de como se generan las conexiones entre dos terminales a nivel WAN, el símbolo del centro significa conexión DCE , DTE

5 Los protocolos de encapsulamiento WAN

Los protocolos de WAN tienen funcionalidades de los tres primeros niveles, físico, enlace y red según el modelo de referencia OSI.

A continuación se hablará de la capa de enlace a nivel WAN, por el motivo que a este nivel se llevan a cabo diferentes tipos de conexiones y envíos de datos; con ayuda de dispositivos y protocolos específicos, dichos elementos permitirán que se desarrolle el respaldo de la red.

3.5.1 Capa de Enlace de Datos: Protocolos WAN

Los protocolos de enlace de datos WAN, describen cómo se transportan las tramas entre sistemas a través de un solo enlace de datos. Incluyen protocolos diseñados para operar a través de servicios dedicados de conmutación de punto a punto, multipunto y multiacceso, como Frame Relay.

La tarea principal es tomar un segmento de datos y transformarla en una abstracción libre de errores, lo cual generará transmisión de datos para la capa de red; esta función se logra dividiendo los datos de entrada en tramas¹⁰, las cuales se transmiten en forma secuencial y procesa las tramas de estado que envía el nodo destino.

A continuación se presentan los protocolos más comunes en la capa de enlace de datos nivel WAN, en este serán las posibles opciones de envío de tramas asociadas con las líneas seriales síncronas, en la que se escogerá las más indicada para la solución de perdida de conexión:

- **High-Level Data Link Control (HDLC).** Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores por la forma en que cada vendedor ha elegido cómo implementarla. HDLC soporta tanto configuraciones punto a punto como multipunto.
- **Link Access Procedure Balanced (LAPB).** Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de marcos así como también para intercambio, retransmisión, y reconocimiento de marcos.
- **Point-to-Point Protocol (PPP).** Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.

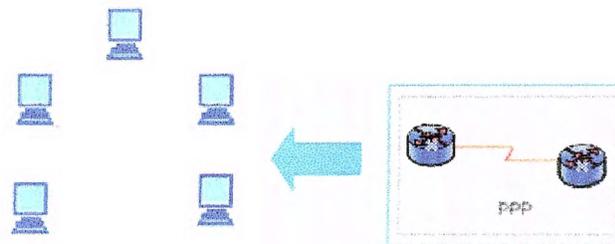


Figura 15. Por la facilidades que presenta el protocolo PPP , se ha escogido dicho protocolo para la creación de conexiones punto a punto en la red WAN .

¹⁰ Referirse al Glosario

Los dos encapsulamientos WAN punto a punto más comunes son HDLC y PPP; en este caso se parte de el hecho de que se ha seleccionado una topología específica la cual es tipo malla, lo que permitirá sacarle mejor provecho al tipo de conexión punto a punto ya que dicha conexión facilita el uso del protocolo PPP.

Algo que vale la pena mencionar es el hecho del porque se usará PPP es por el motivo que puede encapsular varios datagramas de diferentes tipos de protocolos; donde a la vez dicho protocolo posee un mecanismo de detección de errores, permitiendo cumplir con el objetivo de conectividad y a la vez reacción ante la perdida de conexión. Siendo un protocolo amigable, confiable y eficiente entre dos puntos adyacentes de conexión.

3.6. Protocolos WAN

La tecnología WAN, abarca una magnitud considerable de lo que son las redes corporativas, sin tomar en cuenta la ubicación geográfica. Por lo que da la capacidad de aprovechar todas sus virtudes que esta tecnología brinda, donde el fin será crear un respaldo que permita una continuidad en las conexiones de red independientemente de los imprevistos.

El uso de la red WAN, implica que habrá comunicación entre distintas redes, por lo que será necesario utilizar un protocolo que soporte un nivel de red que permita conectividad, por lo que se necesitará la ayuda de el nivel de enlace para que permita el intercambio de información entre redes. Por este motivo se ve de provecho utilizar el protocolo IP¹¹, ya que este protocolo en particular presenta la facilidad de trabajar con las redes de área extensa WAN, así como el hecho de que este protocolo es el más utilizado en Internet.

Ya que IP es un protocolo universal el cual permite que cualquier computadora se pueda comunicar desde cualquier parte del mundo, ya que IP es un estándar TCP/IP necesario que está definido en RFC 791, "Internet Protocol (IP)" (Protocolo de Internet (IP)). IP es tipo un protocolo que se caracteriza por poseer datagramas sin conexión y no confiable, responsable principalmente del direccionamiento y enrutamiento de paquetes entre hosts.

Sin conexión significa que no se establece una sesión antes de intercambiar datos. La confirmación de paquetes entregados y la recuperación de paquetes perdidos es responsabilidad de un protocolo de nivel superior, como TCP. Un paquete IP, también llamado datagrama IP, consta de un encabezado IP y una carga IP, como se muestra en la siguiente ilustración.

¹¹ Referirse al Anexo

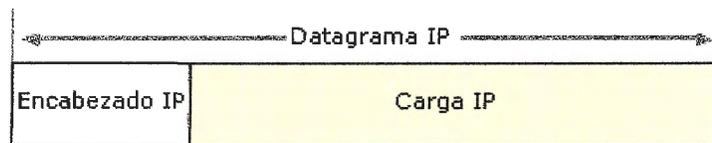


Figura 16. Por la facilidades que presenta el protocolo PPP , se ha escogido dicho protocolo para la creación de conexiones punto a punto en la red WAN

IP representa el corazón de los protocolos de internet. IP tiene dos responsabilidades primarias las cuales son:

- ✓ Proporciona la falta de conexión.
- ✓ la mejor forma de entrega de datagramas por medio del servicio de Internet, lo que proporciona la fragmentación de datagramas¹² así como el nuevo ensamble de los datos de apoyo liga diversos tamaños de conexión a partir de (MTU).

Lo anterior hace la referencia a la búsqueda de respaldo ante la perdida de una red dedicada, ya que cumple con los requisitos de mantener la información activa. Pero es de mencionar que para que esto se lleve a cabo se necesita de un medio para poder transportar los datos al destino ; en este caso con la ayuda de elementos específicos , los cuales poseen la tarea de proporcionar conectividad así como selección de la mejor ruta entre dos sistemas de hosts. En este caso la ubicación geográfica es irrelevante , dado que se va implementar WAN y por ende INTERNET, en este caso se reconocerán sistemas autónomos internos IGP así como externos EGP.

Todo esto mediante el transporte de los paquetes desde la computadora de origen por medio del protocolo IP, hasta su destino mediante el análisis de una tabla de enrutamiento para determinar cuál es el mejor camino o ruta; de esta forma la información puede ser dirigida a la dirección destino esto con la ayuda de los enrutadores ó "Routers" los cuales son dispositivos que a pesar de el alto volumen de tráfico que hay en Internet, se puede tener la seguridad de que el mensaje llegue a su destino.

¹² Referirse al Anexo

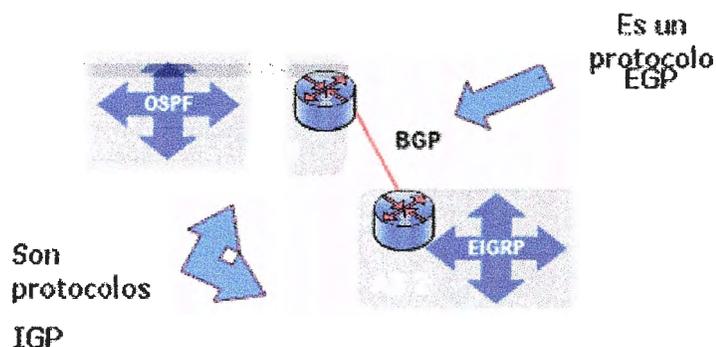


Figura 17. Breve esquematización que presenta la facilidad que posee WAN para interactuar con diferentes tecnologías y protocolos, tanto en redes internas así como externas.

Dado que los routers tienen una cantidad de memoria y una potencia de procesamiento finitas, la tabla de enrutamiento¹³ debe conservarse dentro de un tamaño manejable a fin de mantener la calidad del servicio.

Con lo anterior se busca es el hecho de no perder el enfoque de la búsqueda implementación de respaldo a una conexión de red, donde se parte de la premisa que con el transcurso del tiempo la red primaria podría llegar a experimentar un nivel que genere riesgo en el momento de utilización. Tal es el caso que se buscará encontrar la manera de saldar la falta de conexión, por medio de un respaldo auxiliar que presente características similares de conexión.

Por lo que se observa el beneficio de usar IP, ya que las direcciones que serán usadas por los conmutadores de paquetes para transportar la información. En este caso IP no trabaja por sí solo ya que necesita un medio que le permita conducir la información hacia su destino.

Por lo que se ve la utilidad de implementar los protocolos de red¹⁴ a nivel WAN como soporte ante este tipo de situaciones ya que dicho nivel posee un mayor alcance de control en las redes de gran magnitud así como mayor capacidad reacción, donde los routers juegan un papel clave para que las conexiones entre diferentes puntos de la red sea posible.

¹³ Referirse al Anexo pag 54

¹⁴ Referirse al Anexo pag 55

En este caso es de mencionar que existen determinados protocolos encargados de transportar la información entre routers, donde posteriormente se hará la elección del protocolo que mejor se acople a las necesidades de búsqueda de solución.

Por lo que a continuación se dará una breve idea de lo que es un router y en que consiste para poder continuar y así seguir con la búsqueda de una solución.

El router en vez de mover un mensaje entre todas las redes que componen Internet, solo mueve el mensaje entre las dos redes que están involucradas, la del emisor y la del destinatario. Es decir, un router tiene dos misiones distintas aunque relacionadas, las cuales se mencionarán a continuación:

1. El router se asegura de que la información no va a donde no es necesario.
2. El router se asegura que la información si llegue al destinatario.

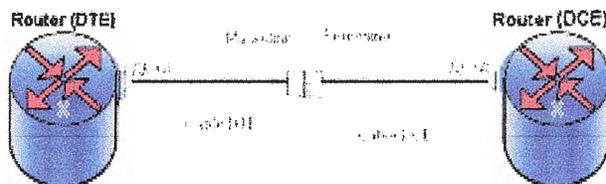


Figura 18. Demostración del uso de router en las conexiones de red WAN

El router unirá las redes del emisor y el destinatario de una información determinada (email, página Web) y además solo transmitirá entre las mismas la información necesaria.

Transmisión de paquetes

El movimiento de información en Internet funciona de forma distinta, primero la información (emails, página web o lo que sea) se divide en pequeñas unidades o "paquetes" (de unos 1.500 bytes por paquete). Cada paquete lleva información del origen, el destinatario y lugar de ese paquete en el total de la información transmitida (para que luego el mensaje pueda ser reconstruido correctamente) e información de como confirmar su llegada al destino.

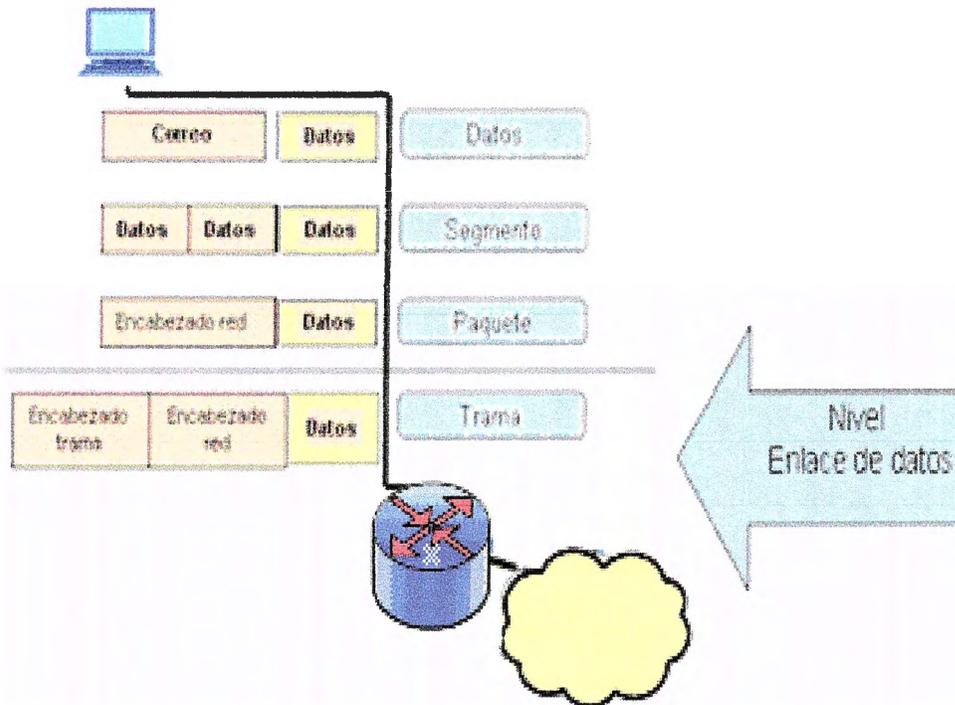


Figura 19. Esquema que representa el proceso de empaquetado de información

La transmisión de una información emitida de un emisor a un receptor se divide en lo que se conoce como paquetes. Cada paquete es de aproximadamente 1500 bytes. Éstos llevan la información al receptor. El router se encarga de examinar todos los paquetes que conforman el mensaje en su totalidad y a partir de esto buscará el camino más corto y rápido para enviar la información a su destino. Este medio de transmisión tiene dos grandes ventajas. En primer lugar, el router es capaz de distinguir aquellas rutas que no son efectivas y por lo tanto puede buscar otra mejor opción. Y en segundo lugar es capaz de seleccionar la ruta más rápida para emitir la información, por ejemplo la que tenga menos tráfico.

3.7 Esquematización de prototipo.

Ya teniendo información de los equipos y los protocolos que se mencionaron anteriormente, se puede aplicar dicho conocimiento para formar las conexiones físicas de lo que será una de las posibles soluciones de respaldo, donde a continuación se presentan cada una de ellas:

Propuesta 1.

Opción 1.1 conexión punto a punto

Estado normal



Experimentando una falla

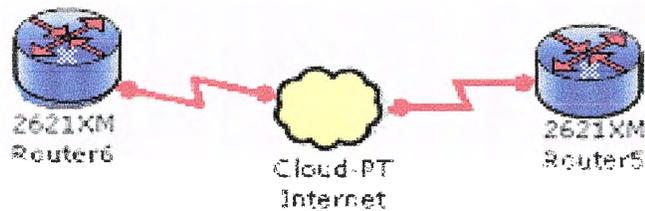


Explicación:

En este caso que existe una conexión punto a punto donde se puede poner de manifiesto, que no existe una manera viable que permita una recuperación de conexión inmediata ante la pérdida de conectividad; por tal motivo es necesario invertir en tiempo y dinero para su recuperación. Lo que implica un mayor gasto para la compañía.

Opción 2.2 Conexión punto a punto, utilizando Internet como conexión.

Estado normal



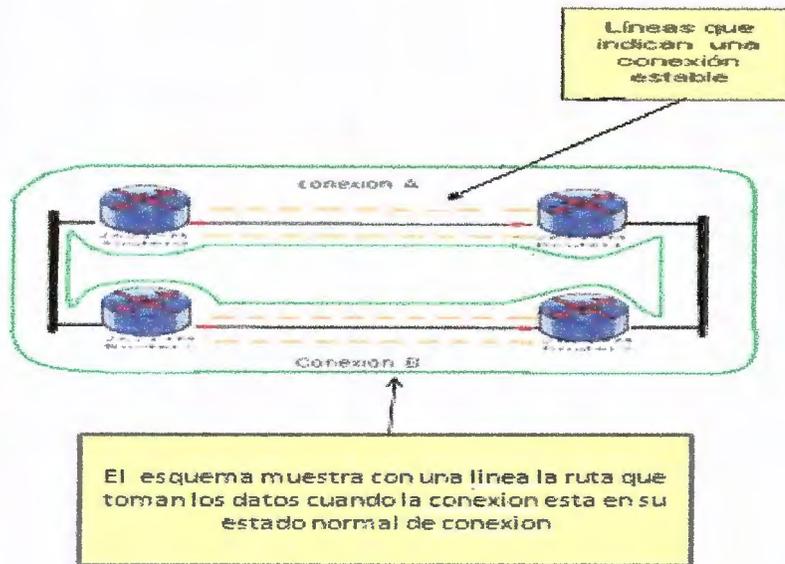
Experimentando una falla



Explicación:

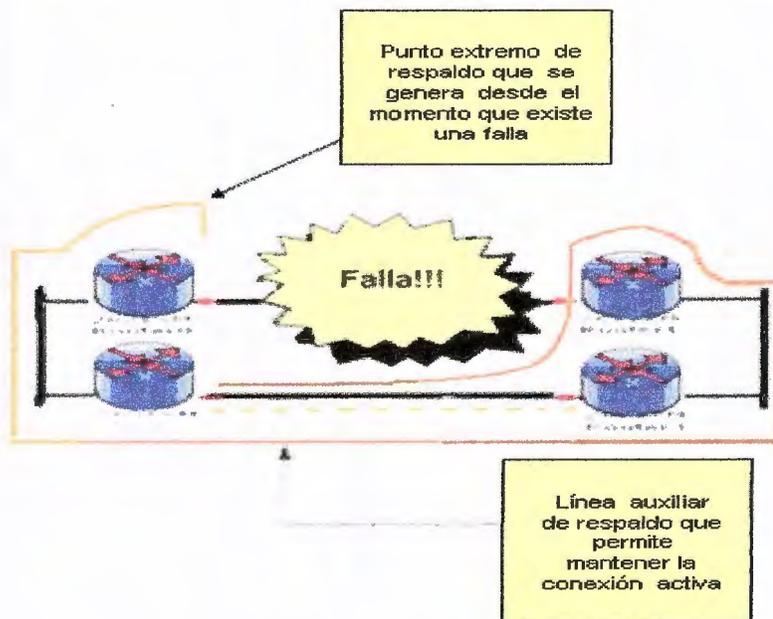
Al igual que la conexión punto a punto, si el servicio de Internet falla no existe manera de recuperar la información de manera inmediata o que brinde un respaldo que permita la continuidad de transporte de información, por tanto no es aceptada como una solución viable.

Propuesta 2. Conexión punto a punto con opción de respaldo alternativo, lo que permite que automáticamente se presente una forma de prevenir una pérdida total de conexión.

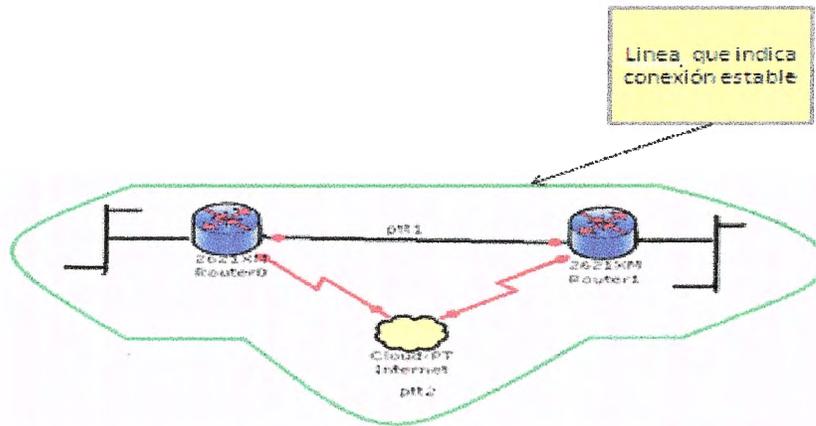


Explicación:

Desde el momento en que se pierda conectividad en la red, automáticamente se generará una conexión de respaldo alterna que permita dar continuidad a la conexión de la red. Por tanto no es aceptada como una solución viable.

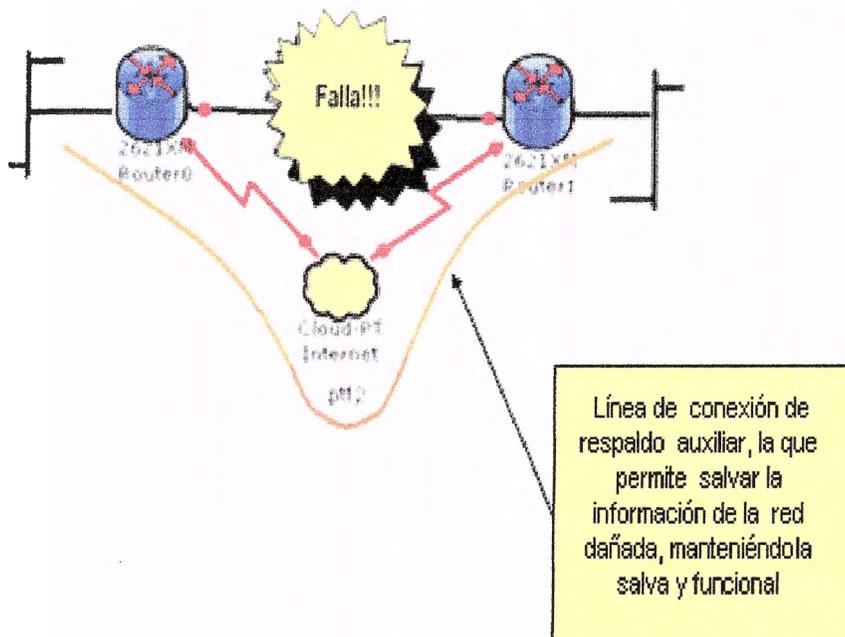


Propuesta 3. Conexión punto a punto conectado con una conexión alterna a partir de Internet.

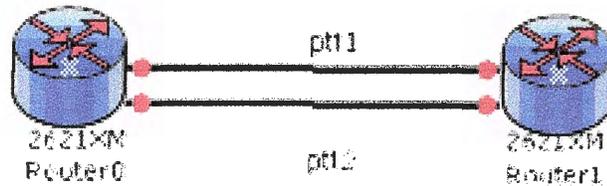


Explicación:

Independientemente del camino que sufra inconveniente toda la información será reprogramada automáticamente, con el objetivo de no perder conectividad en la red.

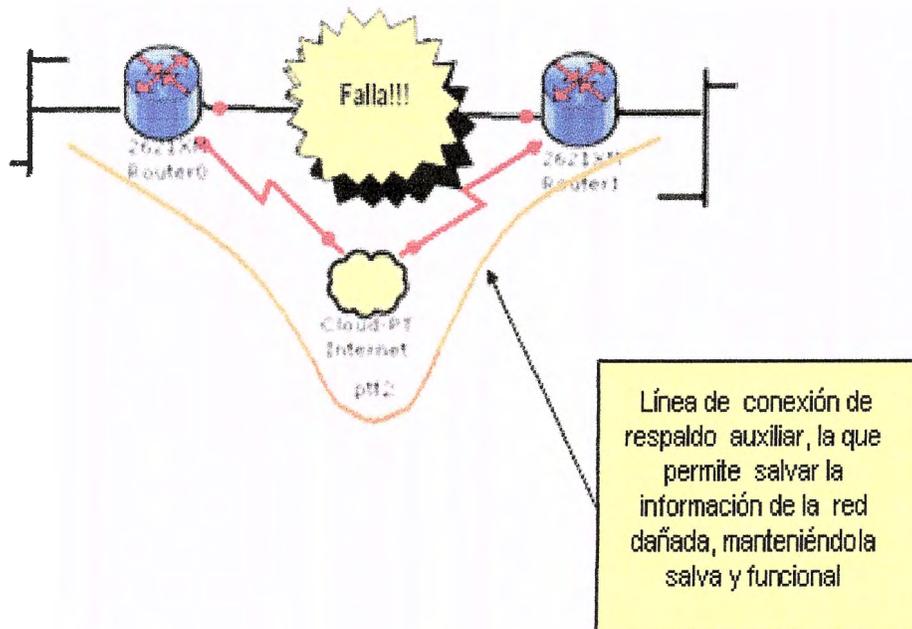


Propuesta 4. Conexión punto a punto con opción de respaldo

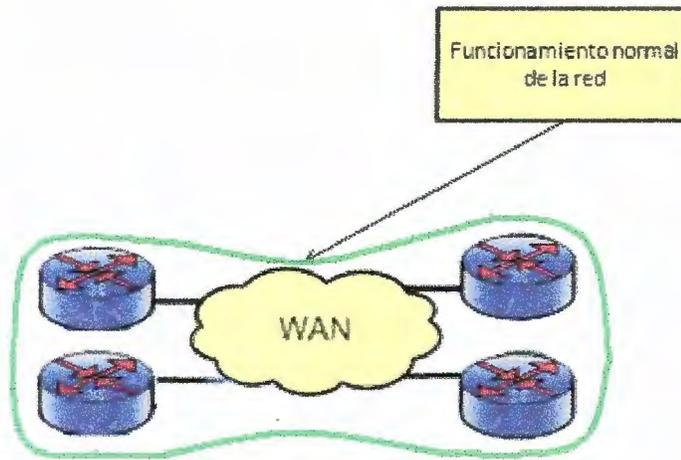


Explicación:

Desde el momento en que se pierda conectividad en la red, automáticamente se generará una conexión de respaldo alterna a partir de Internet, lo que permitirá dar continuidad a la conexión de la red.

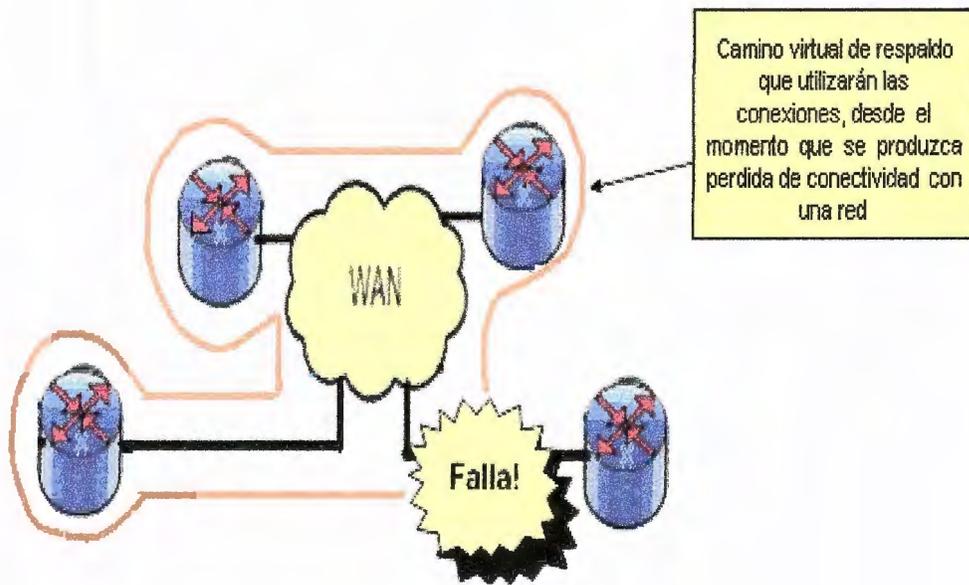


Propuesta 5. Conexión a partir de red WAN con opción de respaldo.

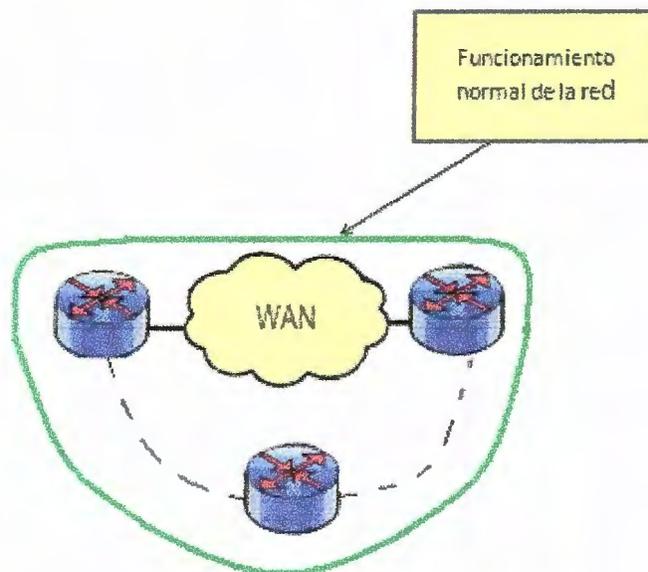


Explicación:

Independientemente del camino que sufra inconveniente toda la información será reprogramada automáticamente, con el objetivo de no perder conectividad en la red.

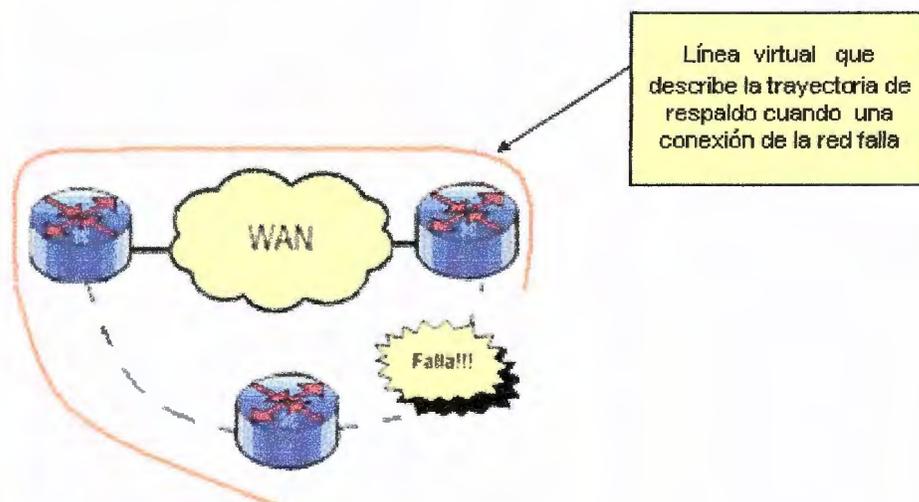


Propuesta 6. Conexión a partir de red WAN con opción de respaldo.



Explicación:

Así como el prototipo anterior en dado caso que la red sufra de algún inconveniente, mencionado respaldo reemplazará automáticamente la conexión de red que ha sido dañada.



3. 7.1 Presentación de los Routers que brinden solución de respaldo.

A continuación se dará la hoja de especificación de los equipos que servirán para enrutar la información en la red y a la vez para crear conexiones de respaldo ante la pérdida de conexión.

Opción 1

Especificación detallada - CISCO 1811 Integrated Services Router

General

Tipo de dispositivo	Encaminador
Factor de forma	Externo - 1U
Anchura	32.3 cm
Profundidad	24.6 cm
Altura	4.5 cm
Peso	2.8 kg

Memoria

Memoria RAM	128 MB (instalados) / 384 MB (máx.)
Memoria Flash	32 MB (instalados) / 128 MB (máx.)

Conexión de redes

Tecnología de conectividad	Cableado
Conmutador integrado	Conmutador de 8 puertos
Velocidad de transferencia de datos	100 Mbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Protocolo de conmutación	Ethernet
Red / Protocolo de transporte	RSVP, IP/IPX, IPSec
Protocolo de direccionamiento	OSPF, RIP-1, RIP-2, BGP, EIGRP
Protocolo de gestión remota	SNMP, HTTP
Rendimiento	Capacidad VPN (3DES IPSec) : 40 Mbps
Capacidad	Túneles VPN IPSec : 50 ; Interfaces virtuales (VLAN) : 8

Características	Protección firewall, cifrado del hardware, asistencia técnica VPN, equilibrio de carga, soporte VLAN, Stateful Packet Inspection (SPI), activable, Sistema de prevención de intrusiones (IPS), filtrado de URL, Low-latency queuing (LLQ), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Fair Queuing (WFQ), Weighted Random Early Detection (WRED), Committed Access Rate (CAR), Link Fragmentation and Interleaving (LFI)
-----------------	---

Opción 2

Especificación detallada - CISCO 1841 Integrated Services Router

General

Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 1U
Cantidad de módulos instalados (máx.)	0 (instalados) / 3 (máx.)
Anchura	34.3 cm
Profundidad	27.4 cm
Altura	4.8 cm
Peso	2.7 kg

Memoria

Memoria RAM	128 MB (instalados) / 384 MB (máx.) - SDRAM
Memoria Flash	32 MB (instalados) / 128 MB (máx.)

Conexión de redes

Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP, HTTP

Características	Protección firewall, compresión del hardware, cifrado del hardware, asistencia técnica VPN, soporte VLAN, Sistema de prevención de intrusiones (IPS), montable en pared, Dynamic Multipoint VPN (DMVPN), Network Admissions Control (NAC)
-----------------	---

Expansión / Conectividad

Total ranuras de expansión (libres) 1 (0) x Tarjeta CompactFlash ; Memoria ; 1 (1) x AIM ; 2 (2) x HWIC

Interfaces 2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ; 1 x USB - 4 PIN USB tipo A ; 1 x gestión - consola ; 1 x gestión - auxiliar

Diverso

Kit de montaje en bastidor Opcional

Opción 3

Especificación detallada - CISCO 2801

General

Tipo de dispositivo Encaminador
Factor de forma Externo - modular - 1U
Anchura 44.5 cm
Profundidad 41.9 cm
Altura 4.37 cm
Peso 6.2 kg

Memoria

Memoria RAM 256 MB (instalados) / 384 MB (máx.) - SDRAM
Memoria Flash 64 MB (instalados) / 128 MB (máx.)

Conexión de redes

Tecnología de conectividad Cableado
Protocolo de interconexión de datos Ethernet, Fast Ethernet
Red / Protocolo de transporte IPSec
Protocolo de gestión remota SNMP 3
Indicadores de estado Actividad de enlace, alimentación
Características Diseño modular, protección firewall, cifrado del hardware, asistencia técnica VPN, soporte de MPLS, filtrado de URL

Expansión / Conectividad

Total ranuras de expansión (libres) 2 (2) x HWIC ; 2 (1) x AIM ; 2 (2) x PVDM ; 1 (1) x WIC ; 1 (1) x VIC ; 1 memoria ; 1 Tarjeta CompactFlash

3.7.2 Selección de solución más viable

En este caso viendo los esquemas de las posibles soluciones de respaldo y las especificaciones de los posibles Routers a utilizar, es de mencionar que dichos dispositivos son de gran importancia para que se genere un respaldo en la red; ya que permite conectividad en las tres primeras capas del modelo OSI las cuales son clave en una conexión WAN, así como la factibilidad de poder utilizar diferentes protocolos de enrutamiento que permita que se tenga una rápida reacción.

Es de mencionar que mientras mayor sea la cantidad de routers que en este caso son marca cisco, mayor será el gasto económico en este caso nos referimos a las propuestas 5 y 6 ; aunque esto represente una mejor calidad de respaldo, pero implica un mayor monto de inversión. Por lo que va a depender de disponibilidad de implementar una nueva solución y de la capacidad adquisitiva de la empresa o corporación para contratar sistema de respaldo.

Posteriormente ya seleccionada una opción de solución, debe procederse al siguiente paso el cual es programar los protocolos de enrutamiento los cuales permitirán generar una reacción inmediata ante la pérdida de conectividad. De esta manera existirá una continuidad de enrutamiento permitiendo la interacción entre las conexiones lógicas y físicas, brindando la oportunidad de trabajar en conjunto ofreciendo una solución óptima. Debe de enfatizarse que el proceso de recuperación de información así como de la conectividad de la red ira actualizando *información; todo esto por medio de protocolos de enrutamiento los cuales tienen la función de recuperar periódicamente toda la información que se vaya recopilando*

Por lo que a continuación se presentarán las características de respaldo de los protocolos de enrutamiento que trabajan a ese nivel WAN:

3.8. Respaldo a partir del protocolo OSPF

OSPF presenta características que permiten que se pueda trabajar a nivel WAN, debido a su eficacia y capacidad de reacción en redes de grandes dimensiones. Es por esto que se ve el potencial de dicho protocolo ya que el *escenario en que la red corporativa se desenvuelva considerablemente amplio* , por lo que su estabilidad juega un papel primordial , ya que en esta situación el protocolo OSPF estará configurado en todos los enrutadores del sitio corporativo, lo que permitirá actualizar la información entre redes de una manera rápida y confiable , facilitando utilizar rutas alternativas en función del tipo de conexión de WAN ;cumpliendo con el requerimiento de respaldo ante la pérdida de conexión.

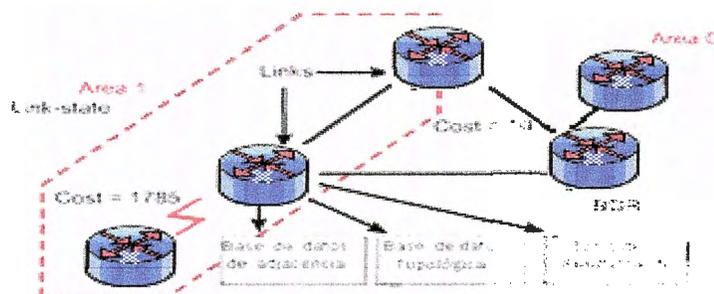


Figura 20. Representación gráfica de una configuración en OSPF.

3.8. Protocolos de estado de enlace

Los protocolos de enrutamiento por estado de enlace recopilan la información necesaria de todos los routers de la red, cada uno de los routers calcula de manera independiente su mejor ruta hacia el destino. De esta manera se producen muy pocos errores al tener una visión independiente de la red de cada router.

Para entender mejor que es un protocolo OSPF es necesario tener una idea de cómo trabajan los protocolos de estado de enlace:

- Los protocolos de estado de enlace¹⁵ utilizan métricas de costo para elegir rutas a través de la red.
- La métrica del costo refleja la capacidad de los enlaces en estas rutas.
- Los protocolos de estado de enlace utilizan actualizaciones generadas por eventos e inundaciones LSA¹⁶ para informar los cambios en la topología de red a todos los routers de la red de forma inmediata. Esto da como resultado tiempos de convergencia más rápidos, lo que permite mantener la red activa y actualizada.

Las actualizaciones de enrutamiento ocurren sólo al producirse cambios en la red, en este caso cuando ocurre una falla se dice que el router vecino se vuelve inalcanzable; los protocolos de estado de enlace inundan el área con LSA mediante una dirección multicast especial. La inundación es un proceso se caracteriza por enviar información a todos los puertos, salvo el puerto donde se recibió la información; por lo que automáticamente la red completa queda informada de los cambios generados manteniendo activa la conexión.

¹⁵ Referirse al Glosario

¹⁶ Referirse al Glosario

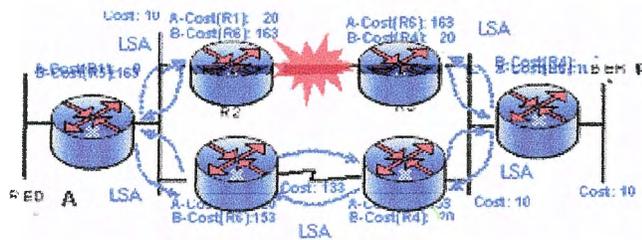


Figura 21. Ejemplificación del proceso de recuperación de conexión a partir del conteo y búsqueda de costos

- Si la ruta preferida a través del Router experimenta dificultades operacionales como por ejemplo congestión o falla en algún componente, el protocolo de enrutamiento del estado de enlace puede detectar este cambio y enrutar los paquetes a través de un router de respaldo opcional estabilizando las posibles fallas que se puedan dar.

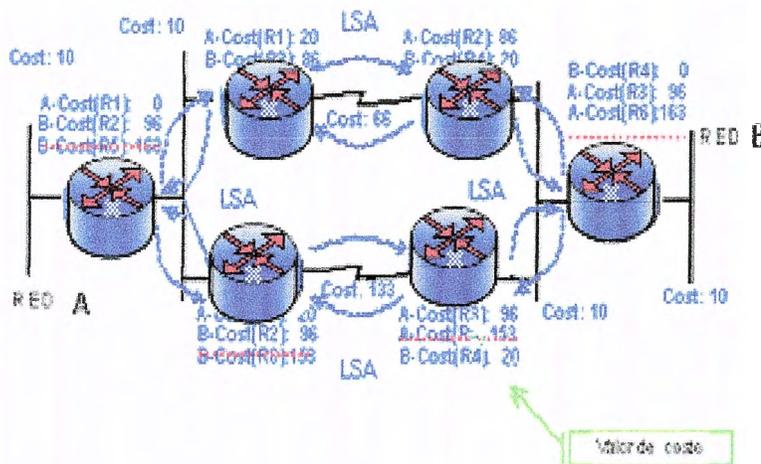


Figura 22. Ejemplificación del proceso de recuperación de conexión a partir del conteo y búsqueda de costos

Todo lo anteriormente mencionado son las características que se buscan para poder encontrar un respaldo que reaccione ante la pérdida de conexión, ya que los protocolos de estado de enlace poseen la peculiaridad de desplegar la información acerca de los cambios dados a todos los rincones de la red. Pudiendo tener un mayor control de las actividades que se presentan, así como una rápida reacción ante las repentinas variantes de falla o congestión de pérdida de conectividad.

A continuación se presentará la secuencia básica de operaciones realizadas por los "routers" **OSPF** los cuales son:

1. Descubrir vecinos OSPF
2. Elegir el DR
3. Formar *adyacencias*
4. Sincronizar bases de datos
5. Calcular la *tabla de encaminamiento*
6. Anunciar los *estados de los enlaces*

Los "routers" efectuarán todos estos pasos durante su activación, y los repetirán en respuesta a eventos de red. Cada "router" debe ejecutar estos pasos para cada red a la que está conectado, excepto para calcular la tabla de encaminamiento. Cada "router" genera y mantiene una sola tabla de encaminamiento para todas las redes, lo que permite mantener la red informada de todos los cambios.

3.8.1 Descubriendo vecinos OSPF

Cuando los "routers" OSPF se activan, inician y mantienen relaciones con sus vecinos usando el *protocolo Hello*. El *protocolo* además asegura que la comunicación entre vecinos sea bidireccional, es decir que si se envía un mensaje a una red determinada también debe recibirse una respuesta. Esto permite mantener un sondeo en la red acerca de cualquier tipo de anomalía que se pueda dar en la red, donde a la vez generará una reacción ante una repentina desconexión.

Los *paquetes Hello*¹⁷ se envían periódicamente al exterior por todas las interfaces de los "routers". La comunicación bidireccional se indica si el propio "enrutador" aparece en el *paquete Hello* del vecino. En una red de *broadcast*¹⁸, los *paquetes Hello* se envían por multicast¹⁹; los vecinos se descubren luego dinámicamente.

En redes no *broadcast*, cada "router" que sea un DR potencial tiene una lista de todos los "routers" conectados a la red y enviará *paquetes Hello* a todos los demás DR potenciales cuando su interfaz a la red sea operativa por primera vez.

3.8.2 Determinación del DR

Esto se hace usando el *protocolo Hello*. Aquí se da una breve descripción del proceso. El "router" examina la lista de sus vecinos, desecha cualquier alternativa que no tenga comunicación bidireccional, en este caso cuando se ha generado una pérdida de conectividad o que tenga un costo adicional y graba el DR, el BDR correspondiente con el costo que se ha declarado para cada uno de ellos.

El "router" se añade él mismo a la lista, usando el valor de costo configurado para la interfaz y cero (desconocido) para el DR y el BDR, en el caso de que esté en proceso de activación.

¹⁷ Referirse al glosario

¹⁸ Referirse al Glosario

¹⁹ Referirse al Glosario

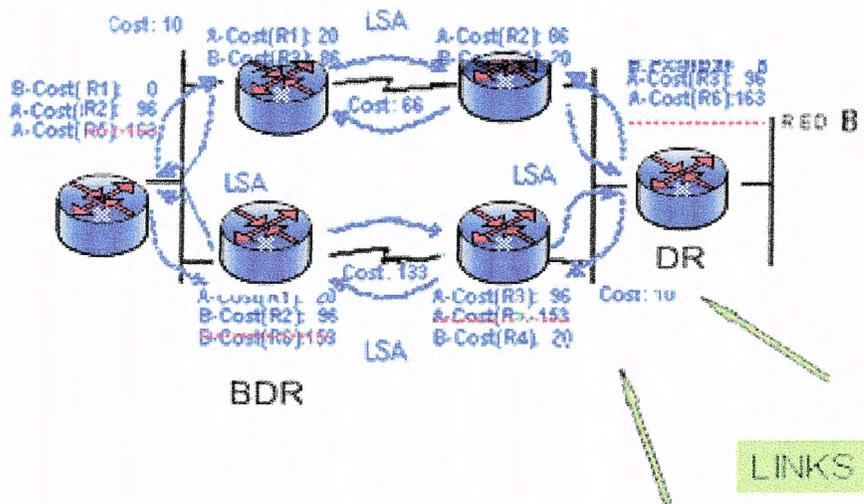


Figura 23. Ejemplificación del proceso del router de mayor costo considerado router DR principal de administración

Se emplean las siguientes reglas para determinar el BDR:

- Si uno o más "routers" declaran ser el BDR²⁰ y no el DR²¹, gana el que tenga un costo superior.
- En caso de empate, gana el que tenga mayor costo.
- Si ningún "router" declara ser el BDR, entonces el se elige el "router" con mayor costo a menos que se haya declarado como DR.
- De nuevo, en caso de empate gana el "router" con mayor costo.

Como el propio "router" que hace los cálculos está en la lista, puede determinar que él mismo es el BDR.

Un proceso similar se sigue para el DR:

- Si uno o más "routers" declaran ser el DR, gana el que tenga un costo superior.
- En caso de empate, gana el que tenga mayor costo.
- Si ningún "router" ha declarado ser el DR entonces el costo se convierte en el DR.

²⁰ Referirse al Glosario

²¹ Referirse al Glosario

El proceso real es mucho más complejo, debido a que los *mensajes Hello* transmitidos incluyen los cambios en los campos grabados en otros "routers", y estos cambios causan eventos en los "routers" que a su vez podrán provocar nuevos cambios u otras acciones.

Por lo que es de suma importancia conocer dicho proceso ya que se necesita saber como funciona mecanismo de actualización de información para poder crear una forma que en que se pueda utilizar OSPF como una fuente de respaldo ante la pérdida de conexión.

3.8.3. Formando Adyacencias

Después de que se ha *descubierto un vecino*, asegurado la comunicación bidireccional, y (en una red multiacceso) elegido un DR, se toma la decisión de si se debería formar una adyacencia con uno de sus vecinos:

- En redes multiacceso, todos los "routers" se hacen adyacentes al DR y al BDR²².
- En enlaces punto a punto (virtuales), cada "router" forma siempre una adyacencia ²³ con el "router" del otro extremo.
- Si se toma la decisión de no formar una adyacencia, el estado de la comunicación con el vecino permanece en el estado "Dos-caminos".
- Las adyacencias se establecen usando paquetes DD("Database Description"), que contienen un resumen de la base de datos de estados de enlaces del emisor. Se pueden usar múltiples paquetes para describir la base de datos: con este fin se emplea un procedimiento de sondeo-respuesta. El "router" con mayor ID se convertirá en maestro, el otro en esclavo. Los paquetes DD enviados por el maestro(sondeos o polls) serán reconocidos por los DDs del esclavo(respuestas). El paquete contiene números de secuencia para asegurar la correspondencia entre sondeos y respuestas. Este proceso se denomina DEP("Database Exchange Process").

²² Referirse al Anexo pag 57

²³ Referirse al glosario

3.8.4. Sincronización de las bases de datos

Después de que terminar el DEP("Database Exchange Process"), cada "router" tiene una lista de aquellos anuncios para los que el vecino tiene más instancias actualizadas, que se solicitan por medio de paquetes LSR("Link State Request"). La respuesta a un LSR es un LSU("Link State Update") que contiene algunos o todos los anuncios solicitados. Si no se recibe respuesta, se repite la solicitud. Cuando se han respondido los paquetes LSR, las bases de datos se sincronizan y los "routers" se describen como totalmente adyacentes. La adyacencia se añade a los anuncios de los dos "routers" correspondiente.

Conexión bajo condiciones normales

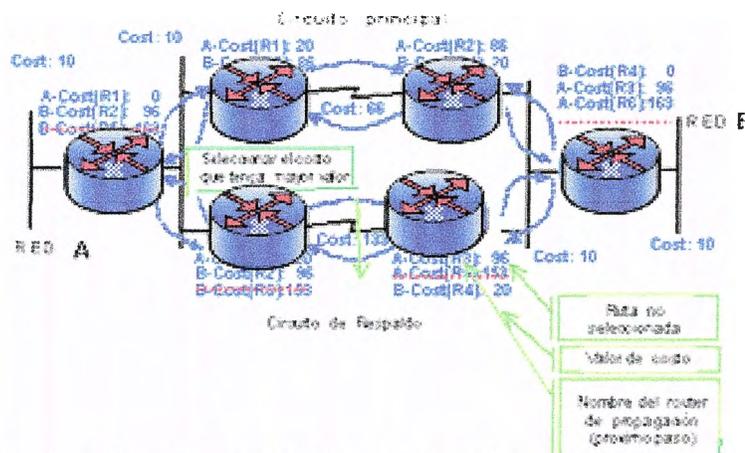


Figura 24. Ejemplificación del proceso de recuperación de conexión a partir del conteo y búsqueda de costos

Usando OSPF, solamente el circuito principal se utiliza bajo condiciones normales. En dado caso ocurra una falta, se buscará generar un circuito secundario el cual será utilizado como respaldo.

3.8.5. Calculando la tabla de encaminamiento

Usando como entrada las bases de datos de estados de enlaces de las áreas con las que está conectado, un "router" ejecuta el algoritmo SPF para construir su tabla de encaminamiento. La tabla de encaminamiento siempre se construye es de cero: nunca se hacen actualizaciones a una tabla ya existente.

Una tabla de encaminamiento vieja no se desecha hasta que se han identificado los cambios entre las dos tablas. Cuando el algoritmo produce rutas de igual coste, OSPF puede balancear uniformemente la carga a través de ellas. El número máximo de rutas iguales admitidas depende de la implementación.

3.8.6. Anunciando los estados de enlace

Un "router" anuncia periódicamente el estado de su enlace, por lo que la ausencia de un anuncio reciente indica a los vecinos del "router" que no está activo. Todos los "routers" que hayan establecido comunicación bidireccional con un vecino ejecutan un contador de inactividad para detectar ese suceso. Si no se resetea el contador, al final se desbordará y el evento asociado sitúa el estado del vecino en "down" o sin conexión.

Pues los paquetes del OSPF Hello fluyen constantemente en el circuito la red se mantendrá actualizándose generando una ruta de respaldo en dado caso exista una falla ,ya que es imposible hacer que el tráfico en la red se paralice. En dado caso que la conexión sufra un problema; se buscará reanudar la conexión desde el momento en que OSPF detecte alguna situación anormal, cumpliendo con la finalidad de generar un aviso y reanudación de un respaldo alternativo de conexión

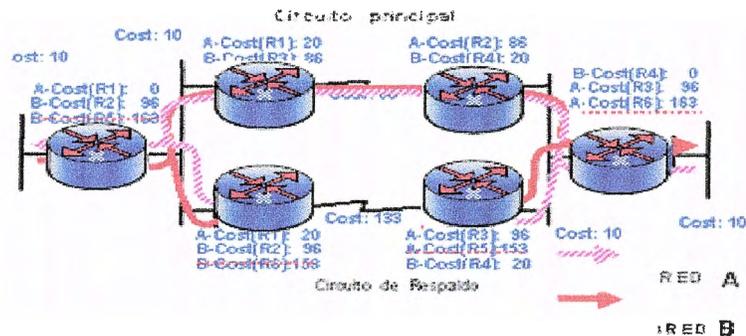


Figura 25. Ejemplificación del proceso de recuperación de conexión a partir del conteo y búsqueda de costos

3.9. Respaldo utilizando ISDN

Otra opción de respaldo usando ISDN en dado caso falle OSPF a nivel WAN. En este caso se puede ver que el encapsulamiento ppp juega un papel importante en las conexiones ISDN, El PPP es mucho más sólido que el HDLC ya que ofrece un mecanismo para la autenticación y negociación de la configuración de protocolos y enlaces compatibles.

En dado caso exista un circuito primario y uno secundario el cual será considerado de respaldo, de donde el secundario se activará en dado caso el circuito primario llegara a sufrir algún inconveniente, ya que este servicio no puede ser cortado, por el hecho que generaría interrupción de tráfico de datos por el motivo que OSPF envía paquetes HELLO a los routers vecinos²⁴.

²⁴ Referirse al Anexo pag 56

En este caso fluirán como copia de seguridad en las líneas de reserva; es decir que necesita de otras medidas en que la configuración del OSPF en este interconectado la reserva con el ISDN. En el siguiente esquema se presenta una opción de respaldo de conexión donde se crea una línea de reserva utilizando un ISDN junto a OSPF.

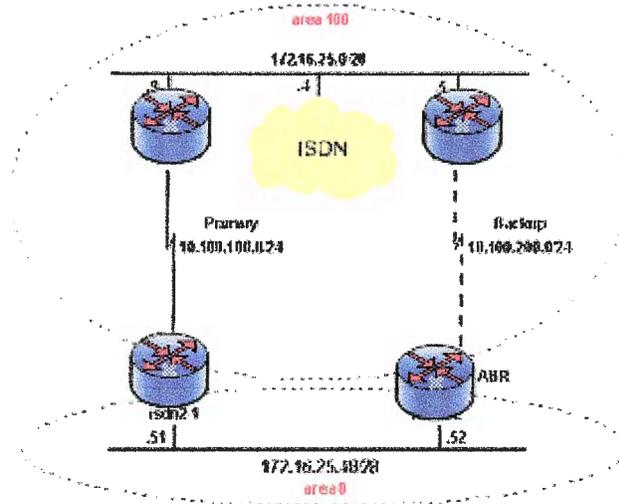


Figura 26. Proceso de respaldo a partir de una línea alquilada o ISDN.

3.10 Características de la reserva y de balanceo.

- El circuito secundario no puede ser cortado porque este sirve como respaldo para que los paquetes del OSPF HELLO²⁵ fluyan en las líneas de reserva también.
- Necesita otras medidas que la configuración del OSPF a la reserva con el ISDN.
- Dos líneas se pueden utilizar para diversos propósitos, y cuando ocurre una falta de conexión en un punto, la línea restante o ISDN se puede utilizar como respaldo ante la pérdida de conexión, cumpliendo con el fin de brindar respaldo a la red ante la pérdida de conexión.

²⁵ Referirse al Anexo pag 56

3.11. Respaldo a partir del protocolo EIGRP:

Una meta de la puesta en práctica de conexión de la red WAN es proporcionar una manera para sostener dicha conexión, si en dado caso esto falla. El ISDN proporciona con frecuencia esta reserva, ya que presenta las estrategias de respaldo adecuadas para alcanzar la misma funcionalidad pero de una manera diferente.

Si la información de enrutamiento se pasa a través del ajuste de información por medio de Frame Relay, donde se generará una ruta estática flotante que puede traer un ajuste de respaldo, en este caso Frame Relay debe permitir el paso de la información ya que servirá como puente alternativo de transporte generando un respaldo a la red que ha sufrido daño.

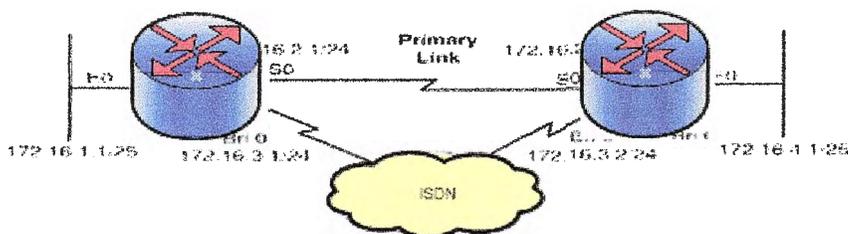


Figura 27. El respaldo del ISDN sirve como conexión auxiliar si la red primario falla.

Dicha ruta será aprendida también para una misma subred a partir del el acoplamiento del Frame Relay vía protocolo interior realizado el encaminamiento de la entrada por medio de (EIGRP), lo cual hace que se acentúa el nivel de redundancia.

EIGRP utiliza la tabla vecina para enumerar los enrutadores adyacentes. La tabla de la topología enumera todas las rutas para cada destino, mientras que la tabla de enrutamiento contiene la mejor ruta a cada destino. La mejor ruta de la tabla de encaminamiento se llama la ruta del sucesor. Una ruta factible del sucesor es una ruta de reserva a una destinación que es uno de los requisitos que se andan buscando para solventar una perdida de conexión, donde EIGRP aprenderá la ruta que será ajustada en la tabla de encaminamiento debido a su distancia administrativa más baja, comparada a una ruta con un costo mayor.

La tabla de la topología es actualizada cuando una ruta directamente conectada o los cambios del interfaz o cuando un enrutador divulga un cambio a una ruta.

En el acontecimiento de la falta de ajuste con frame Relay, la ruta de EIGRP desaparecerá de la tabla de encaminamiento, dicha ruta estática flotante instalará cualquier tráfico interesante que se enviará a través de la conexión del ISDN con la cual esta conectada. Cuando la conectividad se restaura sobre el frame Relay, la ruta es aprendida una vez más por medio de EIGRP.

Sin embargo, una vez que el respaldo este activo los paquetes de EIGRP pueden cruzar el ajuste y los enrutadores pueden intercambiar la información de encaminamiento. Se crea una palabra clave de difusión la cual se incluye en la declaración del mapa del sintonizador para permitir el paso del tráfico del protocolo de encaminamiento sobre ajuste del ISDN. En este caso el programador de la red organiza los datos para poder intercambiar la información de encaminamiento entre rutas, permitiendo proyectar la red con las posibles rutas de respaldo; lo que da la oportunidad desarrollar el objetivo de solución ante la perdida de conectividad en la red generando un respaldo inmediato.

EIGRP ofrece ventajas sobre el OSPF en las redes grandes construidas sobre todo en los routers del Cisco. En redes grandes, el OSPF se despliega en un diseño jerárquico del multi-área, que es administrativo con un alto nivel de complejidad. El descubrimiento vecino y la recuperación de EIGRP permite a los enrutadores aprender dinámicamente sobre otras enrutadores en sus redes directamente unidas; cumpliendo con el objetivo de mantener la continuidad de conexión en la red independientemente de los imprevistos que se presenten.

3.11.1 BGP como respaldo auxiliar

El Internet consiste en una gran cantidad de sistemas autónomos esa información de encaminamiento del intercambio se transporta es usado Routers tipo (BGP²⁶). Cada sistema Autónomo se aplica políticas locales para seleccionar las rutas y propagar las rutas a otras, con las implicaciones importantes para la confiabilidad y la estabilidad del sistema global. Algo que hay que aclarar es que BGP no garantiza convergencia a una ruta estable.

BGP es el protocolo de encaminamiento de opción y es utilizado por todos los abastecedores de servicio de red. Es dinámico y maneja interrupciones y faltas de conexión bastante amplio.

Existen dos clases de respaldo que se utilizan más en la realidad:

Tipos de Respaldo utilizando BGP

3.11.2. Respaldo Múltiple

El Primer tipo, presenta una relación que genera redundancia la cual implica el usar de una conexión secundaria a partir de la conexión cliente-servidor si la conexión de el router primario falla, entonces la información se transfiere a un respaldo o router secundario lo que permitirá mantener la conexión activa.

²⁶ Referirse al anexo pag 59

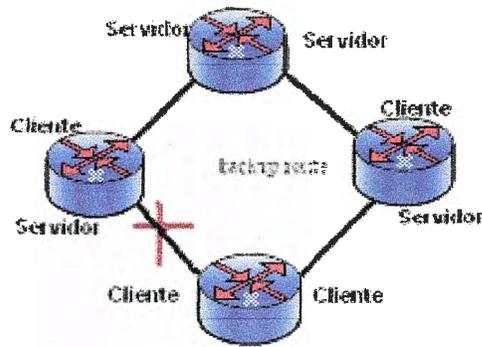


Figura 28. En este caso si una de los nodos de conexión falla se creará un camino o ruta alterna que permitirá dar seguimiento a la conexión de red para no perder la continuidad de el trafico de información.

Características:

- Permita al Sistema Autónomo a que tenga un servicio de proveedor de respaldo.
- Asigne la preferencia más baja para la ruta de respaldo.
- La ruta de respaldo seleccionada se activa cuando la ruta de red de conexión primaria falla.

Niveles De Prevención

- Cada trayectoria tiene un nivel de prevención, del número entero del peso.
- El nivel de prevención, no puede decrementarse una vez haya sido anunciada o se encuentre en proceso de anuncio.

3.11.2. Respaldo del tipo Par a par

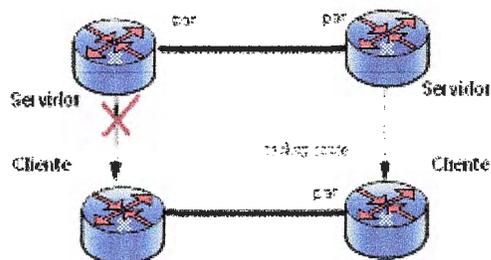


Figura 29. En este caso si una de los nodos de conexión falla se creará un camino o ruta alterna que permitirá la continuidad de el trafico de información.

En este caso el servicio de respaldo actualizará y llevará la información de el router dañado a rutas alternas, en este caso se dará un aviso punto por punto en la red ,permitiendo mantener siempre activa la información a pesar de que se presente una repentina pérdida de conexión en un determinado punto de la red.

Por lo que a continuación se presentan las siguientes características:

- Permite que dos Servicios Autónomos proporcionen servicio de respaldo
- Políticas de exportación de paquetes libres para la relación de respaldo
- Asigna la preferencia con el costo más baja a las rutas de respaldo

Centrándose en relaciones del Cliente-Proveedor y del par-par, el trabajo dentro de la red demuestra que las políticas locales de las rutas que favorecen las rutas del excedente de los clientes vía terminal y routers aseguran que converja el sistema global del BGP.

Sin embargo, las rutas de respaldo introducen dos nuevos desafíos. Primero, bajo relaciones de reserva Múltiple y del respaldo par-par, en este caso un AS puede preferir una trayectoria vía proveedor o punto a punto, más bien se elige una ruta a través del cual se atravesen uno o más conexiones de reserva. En segundo lugar, bajo relación de reserva del par-par, un AS viola las políticas tradicionales de encaminamiento a partir del anuncio de las rutas de su par a otros pares o enrutadores por rutas alternativas.

BGP es un sistema que presenta seguridad ante cualquier combinación de conexiones de las fallas de enrutamiento. AL mismo tiempo, las políticas de enrutamiento son localmente realizables. Es decir, solamente la coordinación entre AS y sus vecinos es requerida; los resultados pueden contabilizarse uno seguido de otro de manera resumida. Demostrando que se puede garantizar la seguridad, si una ruta está marcada como ruta de respaldo, entonces esta información es retenida, para luego ser propagada a AS subsecuentes. Un AS debe preferir siempre una ruta primaria sobre una ruta de reserva a partir del mismo destino. Estos principios indican que BGP esta bastante relacionado con lo que es la propagación de rutas alternas o de respaldo como sistema de seguridad ante futuros inconvenientes lo que encaja de manera aceptable con lo que se anda buscando para solventar la falta de conexión de red.

Así como RIP y OSPF se conectan, los puntos de sección de BGP necesitase explícitamente configurado en ambas terminales. Las conexiones que miran con fijeza del BGP se deben configurar explícitamente en ambos extremos. Para establecer una sesión entre los pares del BGP, se debe especificar manualmente la dirección de la interfaz a la cual se está estableciendo una conexión. Una vez que esta configuración sea completa debe de revisar que ambos terminales realicen un acoplamiento, una negociación del TCP, si esto ocurre se establece una sesión del BGP.

Las Trayectorias De reserva Tienen Significado Global

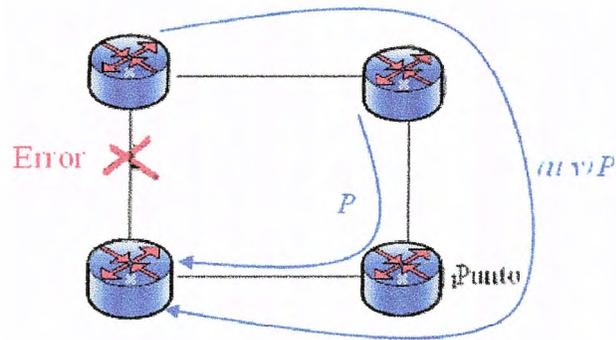


Figura 30. Ejemplificación de una trayectoria global utilizando ospf

- Una vez se crea una trayectoria de respaldo, esta trayectoria de reserva permanecerá activa.
- Si P en El Sistema Autónomo v es una trayectoria de reserva, entonces $(u v)P$ de u en como u

3.11.3 .Niveles De Prevención

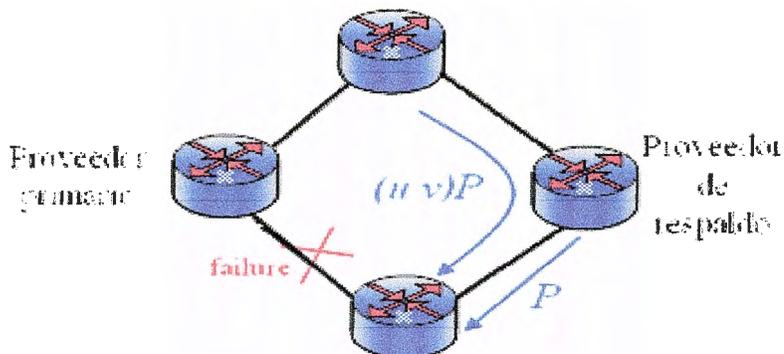


Figura 31. Ejemplificación de una trayectoria donde ha existido una falla.

- Cada trayectoria tiene un nivel de prevención, del número entero del peso.
- El nivel de prevención, no puede decrementarse una vez haya sido anunciada o se encuentre en proceso de anuncio.
- El nivel de prevención $K(P)$ no puede exceder el nivel $K((u v)P)$

Grado comparativo entre tipos de respaldo BGP

Nivel más bajo para las trayectorias de respaldo.

- Prefiere trayectorias primarias sobre las trayectorias de respaldo.
- Prefiere la trayectoria P con un nivel más pequeño $K(P)$ de el cual se desea evitar.

Una graduación más alta para las rutas del cliente

- Permite nivelar las rutas entre las trayectorias con el mismo nivel de rechazo.
- Prefiere la trayectoria vía cliente sobre la trayectoria vía par a partir del proveedor.

Seguridad Inherente

- Garantizado para prevenir la divergencia de la ruta
- El resultado realiza bajo cualquier tipo de falta como cambio político

Características de solución

- Trayectorias de respaldo ante la falta de conexión en una red
- Garantiza seguridad ante la pérdida de conexión de una red determinada
- Configuración local de BGP en cada Sistema Autónomo

Conclusiones

- Se logro presentar, por medio de investigación de la búsqueda de información realizada, un informe detallado de los equipos con los que se cuentan en la actualidad; así también el detalle de sus características.
- Se concluye que OSPF es el protocolo de enrutamiento más adecuado por el hecho de ser confiable y seguro para la realización del respaldo, hay que mencionar que el resto de protocolos son igual de seguros; esto va a depender de el administrador de la red para la selección de protocolos de enrutamiento . En el caso de los equipos y tecnología a utilizar esto tendrá que ver con el nivel de seguridad de respaldo que se desea tener, así como la cantidad monetaria que se desea invertir.
- Se presentaron diferentes opciones de respaldo con los respectivos elementos físicos, que permitan una conectividad continua a pesar de los imprevistos. Hay que enfatizar que va a depender de la necesidad y la capacidad económica del cliente para escoger la alternativa; se debe de mencionar que las propuestas 5 y 6 son las más costosas ya que requieren mayor cantidad de equipo para su funcionamiento.
- Con toda la información recopilada se puede llegar a tener la idea clara de todos los elementos tecnológicos que sean necesarios para desarrollar un prototipo de lo que se desea; en este caso es de mencionar que dicha información servirá como patrón que permita generar respaldo a una red, cuando esta pierda conectividad. En este caso las propuestas 5 y 6 son las que presentan mayor efectividad pero a la vez son las más caras.

Recomendaciones.

- Retomar el tema de investigación para su continuación por otro grupo de trabajo de graduación con el objetivo de estructurar una alternita para la Universidad Don Bosco.
- Es que los estudiantes que retomen el tema deben tener conocimientos sólidos en redes y tipos de protocolos de comunicación a nivel WAN.
- Es de tener en cuenta que existen diferentes alternativas de solución de conexión, por lo que se debe de enfatizar que si se desea mayor seguridad y factibilidad de respaldo como el caso de las propuestas 5 y 6, necesariamente se incrementarían los costos de inversión en cuanto a la cantidad y la calidad de equipo que se requiera.
- Profundizar en el estudio de este tipo de tecnologías en cátedras de redes para que los estudiantes tengan ideas de cómo enfrentar este tipo de situaciones.

4. ANEXOS

Tablas de enrutamiento

Si sabe qué direcciones de red (o identificadores de red) se encuentran disponibles en la interconexión de redes, le resultará más fácil decidir si debe realizar un enrutamiento. Esta información se obtiene a partir de una base de datos denominada tabla de enrutamiento. La tabla de enrutamiento está constituida por una serie de entradas denominadas rutas que contienen información acerca de dónde están situados los identificadores de red de la interconexión de redes. La tabla de enrutamiento no es exclusiva de un solo enrutador. Los hosts (no los enrutadores) también pueden disponer de una tabla de enrutamiento utilizada para determinar la ruta más adecuada.

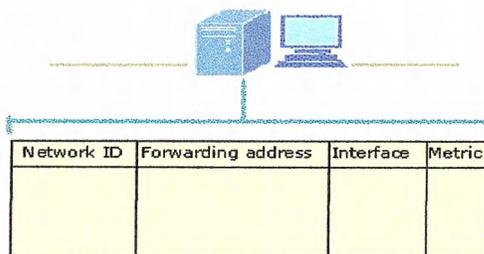
Tipos de entrada de la tabla de enrutamiento

Cada entrada de la tabla de enrutamiento se considera una ruta y pertenece a uno de los tipos siguientes:

- Ruta de red: Una ruta de red proporciona la ruta de un determinado identificador de red de la interconexión de redes.
- Ruta de host: Una ruta de host proporciona la ruta de una dirección de la interconexión de redes (identificadora de red e identificadora del nodo). Las rutas de host se utilizan normalmente para crear rutas personalizadas a hosts específicos a fin de controlar u optimizar el tráfico de la red.
- Ruta predeterminada: Se utiliza cuando no se encuentra ninguna otra ruta en la tabla de enrutamiento. Por ejemplo, si un enrutador o host no puede encontrar una ruta de red o de host para el destino, se utilizará la ruta predeterminada. La ruta predeterminada simplifica la configuración de los hosts. En vez de configurar hosts con rutas para todos los identificadores de red de la interconexión de redes, se utiliza una única ruta predeterminada para reenviar todos los paquetes con una dirección de red o de interconexión de redes de destino que no se encontró en la tabla de enrutamiento.

Estructura de la tabla de enrutamiento

La ilustración siguiente muestra la estructura de la tabla de enrutamiento.



Cada entrada de la tabla de enrutamiento consta de los siguientes campos de información:

- Identificador de red

Identificador de red o dirección de la interconexión de redes correspondiente a una ruta de host. En los enrutadores IP, hay un campo de máscara de subred adicional que determina el identificador de red IP desde una dirección IP de destino.

- Dirección de reenvío

La dirección a la que se reenvía el paquete. La dirección de reenvío es una dirección de hardware o una dirección de interconexión de redes. En el caso de redes a las que se conecta directamente el host o el enrutador, es posible que el campo de la dirección de reenvío sea la dirección de la interfaz que se conecta a la red.

- Interfaz

La interfaz de red que se utiliza cuando se reenvían los paquetes al identificador de red. Se trata de un número de puerto u otro tipo de identificador lógico.

- Métrica

Medida de la preferencia de una ruta. Normalmente, la métrica más baja es la ruta preferida. Si hay varias rutas a una red de destino dada, se utiliza la ruta con la métrica menor. Algunos algoritmos de enrutamiento solamente almacenan una única ruta para cualquier identificador de red en la tabla de enrutamiento, aunque existan varias rutas. En este caso, el enrutador utiliza la métrica para determinar qué ruta debe almacenar en la tabla de enrutamiento.

Técnicas de Conmutación:

Para la utilización de la Conmutación de Paquetes se han definido dos tipos de técnicas: los Datagramas y los Circuitos Virtuales.

Datagramas:

- Considerado el método más sensible.
- No tiene fase de establecimiento de llamada.
- El paso de datos es más seguro.
- No todos los paquetes siguen una misma ruta.
- Los paquetes pueden llegar al destino en desorden debido a que su tratamiento es independiente.
- Un paquete se puede destruir en el camino, cuya recuperación es responsabilidad de la estación de destino. (Esto da a entender que el resto de paquetes están intactos)

Capa Física o de Acceso de Red

También llamada capa Internet ("Internet Layer"). Es la responsable de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información. Los protocolos de transmisión, como el IP están íntimamente asociados a esta capa. Es la responsable del envío de la información sobre el sistema hardware utilizado en cada caso, se utiliza un protocolo distinto según el tipo de red física.

A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta.

Como consecuencia esta capa puede considerarse subdividida en dos:

- Transporte. Encargada de encapsular los datos a transmitir (de usuario). Utiliza los paquetes de datos. En esta categoría se encuentra el protocolo IP.
- Conmutación ("Switching"): Esta parte es la encargada de intercambiar información de conectividad específica de la red (su actividad es raramente percibida por el usuario). Los routers son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. En esta categoría se encuentra el protocolo ICMP ("Internet Control Message Protocol"), responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante PING [3].

Capa de Enlace de Datos: Protocolos WAN

Protocolo OSPF

OSPF (Open Shortest Path First) Uno de los protocolos IGP mas nuevos es el OSPF. Este protocolo ofrece un mayor grado de sofisticación con características como: Rutas basadas en el tipo de servicio, la distancia, nivel de carga, etc. El formato del mensaje OSPF es más complejo que el RIP. Tiene una cabecera fija de 24 octetos, y una parte variable para especificar el tipo del mensaje. Existen cinco tipos de mensaje.

Características del protocolo de estado de enlace

- Mantiene una base de datos compleja.
- Tiene pleno conocimiento de los routers distantes y la forma en que se interconectan.
- Las actualizaciones son desencadenadas por eventos.
- Converge rápidamente.
- No es susceptible a bucles de enrutamiento.

- Características de respaldo en la red a partir de OSPF
- El OSPF permite la generación de respaldos de reserva y balancear cuando tiene rutas múltiples.
- Cuando las rutas tienen diversos costes, la ruta con costes más pequeños se puede utilizar como ruta principal tomando dicho router como prioridad DR y con mayores costes se puede utilizar como reserva BDR.
- Balanceando los costos de las rutas, el tráfico puede ser dispersado.
- Incluso si uno de la ruta para la cual se pone en ejecución el balancear los costos, las rutas restantes puede ser servicio como respaldos auxiliares.

Protocolos de estados de enlace

Los protocolos de estado de enlace construyen tablas de enrutamiento basándose en una base de datos de la topología. Esta base de datos se elabora a partir de paquetes de estado de enlace que se pasan entre todos los routers para describir el estado de una red

Significado de cada paquete.

Tipo	Nombre del Paquete	Significado
1	Hello	(Utilizado para comprobar la accesibilidad)
2	DBD	Descripción de la Base de Datos
3	LSR	Solicitud del estado del enlace
4	LSU	Actualización del estado del enlace
5	LSAck	Reconocimiento del estado del enlace

Figura 32. Explicación de cada uno de los paquetes que se utilizan como protocolos de enrutamiento

Las interfaces OSPF reconocen tres tipos de redes:

- Multiacceso de broadcast como por ejemplo Ethernet
- Redes punto a punto.
- Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay



Figura 33. Ejemplificación de conexión punto a punto

El tipo de red que se utilizará en el desarrollo de esta búsqueda de solución, será la conexión de terminales punto a punto ya que cumple con las características necesarias para poder trabajar y manipular el equipo así como el protocolo Ospf

Manera de selección del DR y BDR

La intención que se esconde tras este mecanismo es doble:

- Que cuando un "router" se active, no debería usurpar la posición del BDR actual aunque tenga un router con un costo superior.
- Que la promoción de un BDR a DR debería ser ordenada y requerir que el BDR acepte sus responsabilidades.
- El algoritmo no siempre da lugar a que el "router" de mayor prioridad sea el DR, ni tampoco que el segundo de mayor prioridad sea el BDR.

El DR tiene las siguientes responsabilidades:

- El DR genera para la red los anuncios de los estados de los enlaces, que inundan el área y describen esta red a todos los "routers" de todas las redes del área.
- El DR se hace adyacente a otros "routers" de la red. Estas adyacencias²⁷ son centrales con respecto al proceso de inundación usado para asegurar que los anuncios alcanzan a todos los "routers" del área y que por tanto la base de datos topológica que usan todos permanece igual.

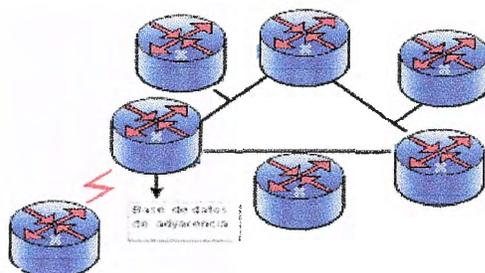


Figura 34. Los routers procesan la información acerca de los estados de enlace y crean una base de datos del estado de enlace. Cada router del área OSPF tendrá la misma base de datos del estado de enlace.

²⁷ Referirse al Anexo

El BDR tiene la siguiente responsabilidad:

- El BDR se hace adyacente a todos los demás "routers" de la red. Esto asegura que cuando ocupe el puesto del DR lo pueda hacer rápidamente.

Esto significa que la comunicación se debe establecer desde cero, incluyendo la re sincronización de las bases de datos. Un "router" también relanza sus anuncios cuando su estado cambia.

Un "router" puede lanzar diversos anuncios para cada área. Estos se propagan a través del área por el procedimiento de inundación. Cada "router" emite un RLA. Si el "router" es además el DR para una o más de las redes del área, originará NLAs para estas.

Los ABR generan una SLA para cada destino inter-area conocido. Los ASBR originan un ASL para cada destino externo conocido. Los destinos se anuncian una cada vez de tal forma que el cambio de una sola ruta puede inundar la red sin tener que enviar el resto de las *rut*as. Durante el proceso de inundación, un sólo LSU puede llevar muchos anuncios.

BGP

Border Gateway Protocol es un protocolo mediante el cual intercambia información de encaminamiento entre Sistemas Autónomos (conjunto de routers dirigidos por la misma autoridad y que usan un mismo protocolo interno de distribución y actualización de información de encaminamiento(IGP). Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos.

Actualmente entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo. Estos routers deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un EGP (*external gateway protocol*)

BGP es un protocolo resistente, seguro que se debe configurar sobre una base punto a punto. Una vez que se haya configurado una sesión que miraba con fijeza, el BGP utiliza una conexión del TCP para establecer una sesión. Después de que se establezca una sesión del BGP, el tráfico se pasa a lo largo del acoplamiento BGP-Habilitado.

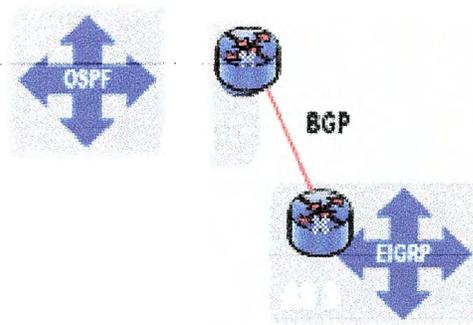


Figura 35. Ejemplificación del uso simultaneo de varios protocolos de enrutamiento

El Internet consiste en una gran cantidad de sistemas autónomos (ASes) que interactúan para coordinar el envío de tráfico IP. Un AS es una colección de routers y conexiones administradas por una sola institución, como una compañía, universidad o un proveedor de servicio de Internet.

Los vecinos del Sistema Autónomo utilizan (BGP) como una vía para intercambiar la información de encaminamiento.

Cada anuncio de la ruta del BGP anuncia a un bloque particular acerca de las direcciones IP la cual incluye una lista de la trayectoria de los AS, junto con un número de atributos.

Cada Sistema Autónomo aplica políticas locales para seleccionar la mejor ruta y opción para decidir entre propagar o no las rutas a los AS vecinos, con el debido nivel de seguridad, en este caso respetando privacidad sin la divulgación de sus políticas y topología interna a otras redes. Prácticamente, las políticas del BGP reflejan las relaciones comerciales entre AS vecinos.

Así como los pares de terminales de conexión donde típicamente se tiene ya sea un cliente y un servidor o una conexión punto a punto interrelacionado, un proveedor abastece la conectividad con el Internet como un servicio al cliente, mientras que una terminal proporcionan simplemente conectividad entre sus respectivos clientes.

La relación entre sistemas autónomos se pueden interpretar como reglas locales para la determinación de si es necesario o no la exportación de información de la mejor ruta que lo dirija al AS vecino.

Estas políticas limitan las trayectorias posibles entre cada par de Host del Internet. Por sí mismo BGP no asegura de que cada par de anfitriones pueda comunicarse, incluso si la topología subyacente está conectada. Además, las redes pueden sufrir diferentes imprevistos los cuales generen perdidas de conectividad, forzando al AS a buscar trayectorias alternativas que permitan dar respaldo a la conexión.

Estos respaldos locales se reservan entre AS los cuales introducen rutas BGP adicionales las cuales anuncian las rutas de reserva. En la superficie, el aviso de rutas de reserva debe ayudar a mejorar la robustez del Internet ante las conexiones y fallas en el router. Sin embargo, las rutas de reserva tienen implicaciones negativas en las propiedades globales del Internet utilizando el sistema de enrutamiento simple.

Las rutas de reserva pueden introducir los problemas globales de la convergencia del BGP que dan como resultado a la divergencia del protocolo, la cual afecta la robustez de la red; incluso si el sistema converge.

En este papel, se centrará en asegurarse de que el sistema converge, más bien haciendo un análisis de cómo las rutas de reserva afectan el tiempo de la convergencia.

Presentación física de los Routers que brinden solución de respaldo

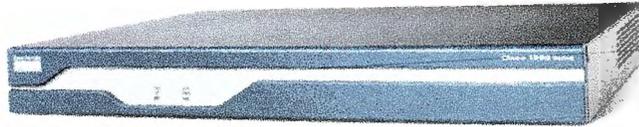
Opción 1

Especificación detallada - CISCO 1811 Integrated Services Router



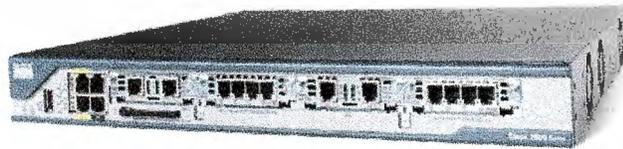
Opción 2

Especificación detallada - CISCO 1841 Integrated Services Router



Opción 3

Especificación detallada - CISCO 2801



5. Glosario

ANSI

Instituto Nacional Americano de Normalización

Adyacencias

Termino OSPF los cuales determinan con qué routers pueden intentar formar adyacencias tomando como base el tipo de red a la cual están conectados. Algunos routers tratarán de tender a la adyacencia con respecto a todos los routers vecinos. Otros routers tratarán de hacerse adyacentes con respecto a sólo uno o dos de los routers vecinos. Una vez que se forma una adyacencia entre vecinos, se intercambia la información del estado de enlace.

Ancho de Banda

En general, la banda ancha refiere a la telecomunicación en la cual una banda de frecuencias está disponible para transmitir la información. Porque una banda ancha de frecuencias está disponible, la información se puede multiplexar y enviar encendido diversas frecuencias o canales dentro de la banda concurrentemente, permitiendo más información sea transmitida en una cantidad de tiempo dada.

Dirección IP

Una es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar.

BIT (bitio, bit)

Unidad mínima de información digital que puede ser tratada por un ordenador. Proviene de la contracción de la expresión binary digit(dígito binario).

Base de datos de adyacencia

Lista de todos los Enrutadores vecinos con los que un enrutador ha establecido comunicación bidireccional. Esto es exclusivo para cada enrutador.

BGP-3 (Border Gateways Protocol)

El problema del protocolo EGP, fue el que impulso a diseñar e implementar el protocolo BGP.

El protocolo BGP es un protocolo interno de sistema autónomo. Un sistema autónomo puede contener múltiples dominios de direccionamiento, cada uno con su propio protocolo interno de sistema autónomo, o IGP.

Dentro de cada sistema autónomo pueden haber varios Gateways que se pueden comunicar con los Gateways de otros sistemas. También se puede elegir un Gateways para lograr un informe de la información de direccionamiento para el sistema autónomo. En cualquier caso, un sistema autónomo aparece ante otro sistema autónomo como un direccionador consistente. Esto elimina la estructura de árbol del protocolo EGP.

Broadcast

Que significa difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Costo

El algoritmo de Dijkstra es el que se encarga de determinar la mejor ruta añadiendo a la información de la ruta, el valor total del costo de todo el camino. El costo o métrica es el resultado de dividir: (100 Mbps/BW en Mbps). También es posible cambiar el valor referencial que es de 100 por default.

CCITT

Comité Consultivo Internacional Telegráfico y Telefónico

La Conmutación de Circuitos

El objetivo de los Nodos de Conmutación es el Intercambio de los Datos entre éstos para que lleguen a su destino, mas no es del interés de los nodos el contenido de los Datos, por lo general la conmutación de circuitos se asocia con la red vía telefónica.

Conmutadores de paquetes

Un Paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, en la que está especificado la ruta a seguir a lo largo de la red hasta el destino del paquete.

Conmutación por División en el tiempo

Se basa en la Multiplexación por división en el Tiempo Síncrona donde las cadenas de bits de baja velocidad pueden compartir una línea de velocidad, los datos que llegan por la línea de entrada se fragmentan pasando una ráfaga de datos por un puesto controlada, que se habilita por un periodo, hacia el bus de alta velocidad que dirige los datos a la línea de salida

DCE

Dispositivos de red intermediarios que reciben y retransmiten las tramas dentro de la red; pueden ser: ruteadores, conmutadores (switch).

DTE

Dispositivos de red que generan o que son el destino de los datos: como los PCs, las estaciones de trabajo, los servidores de archivos, los servidores de impresión; todos son parte del grupo de las estaciones finales.

EIA

Asociación de Industrias Electrónicas

EGP

(Exterior Gateway Protocol) es un protocolo estándar. Su status es recomendado.

EGP es el protocolo utilizado para el intercambio de información de encaminamiento entre pasarelas exteriores (que no pertenezcan al mismo Sistema Autónomo AS).

Protocolo Hello

Hello mide la distancia por el tiempo transcurrido. Este protocolo tiene un problema asociado al vector de distancia. El problema tiene dos etapas.

IEEE

Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica

INTERNET

Es una red informática. No es más que conjunto de ordenadores desplegados por todo el mundo y conectados entre sí intercambiándose información

LSA

El primer LSA se genera siempre inmediatamente sobre un cambio de la topología del OSPF, y el LSA siguiente generado es controlado por el intervalo mínimo del comienzo. El LSAs subsecuente generado para el mismo LSA es tarifa-limitado hasta que se alcanza el intervalo máximo. Se define el "mismo LSA" mientras que un caso de LSA que contenga el mismo número de la identificación de LSA, el tipo de LSA, y la publicidad de la identificación de el enrutador.

MODEM

Un módem, o modulador-demodulador, es un dispositivo que ofrece al computador conectividad a una línea telefónica. El módem convierte (modula) los datos de una señal digital en una señal analógica compatible con una línea telefónica estándar. El módem en el extremo receptor demodula la señal, convirtiéndola nuevamente en una señal digital.

Multicast

La tecnología *multicast* representa un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, se puede enviar simultáneamente a diversos receptores interesados.

Cabe a la infraestructura de red transportar este flujo de datos, replicándolo cuando sea necesario, para todos los receptores que registren interés en recibir estos datos.

Overhead

Desperdicio de ancho de banda, causado por la información adicional (de control, de secuencia, etc.) que debe viajar además de los datos, en los paquetes de un medio de comunicación. El overhead afecta al Throughput de una conexión.

Protocolo

Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos.

Redundancia

Las redes robustas requieren redundancia, si algún elemento falla, la red deberá por sí misma deberá seguir operando. Un sistema tolerante a fallas debe estar diseñado en la red, de tal manera, si un servidor falla, un segundo servidor de respaldo entrará a operar inmediatamente.

La redundancia también se aplica para los enlaces externos de la red. Los enlaces redundantes aseguran que la red siga funcionando en caso de que un equipo de comunicaciones falle o el medio de transmisión en cuestión. Es común que compañías tengan enlaces redundantes, si el enlace terrestre falla (por ejemplo, una línea privada), entra en operación el enlace vía satélite o vía microondas.

Router (encaminador, direccionador, enrutador)

Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Ver también: "gateway". vé's de la red conmutada. Ver también: "dialup".

Sistema Autónomo

En Internet, un Sistema Autónomo (Autonomous System, AS) es un conjunto de redes y dispositivos router IP que se encuentran administrados por una sola entidad (o en algunas ocasiones varias) que cuentan con una política común de definición de trayectorias para Internet. Los Sistemas Autónomos se comunican entre si mediante routers BGP y se intercambian el tráfico de Internet que va de una red a la otra. A su vez cada Sistema Autónomo es como una Internet en pequeño, ya que lo se llevaba a cabo por una sola entidad, típicamente un Proveedor de Servicio de Internet (ISP) o una gran organización con conexiones independientes a múltiples redes, las cuales se apegaban a una sola y clara política de definición de trayectorias definida. Técnicamente un Sistema Autónomo se define como "un grupo de redes IP que poseen una política de rutas propia e independiente".

Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. Aún considerando que el ISP podía soportar múltiples sistemas autónomos, Internet solo considera la política de definición de trayectorias establecida por el ISP. Por lo tanto, el ISP debería contar con un ASN registrado. Un número de AS o ASN se asigna a cada AS para ser utilizado por el esquema de encaminamiento BGP, este número identifica de manera única a cada red dentro del Internet.

Switch

Un switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los puentes, los switches aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los switches utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red.

TIA

Asociación de la Industria de las Telecomunicaciones

UIT

La Unión Internacional de Telecomunicaciones

6. Bibliografía.

6. Bibliografía

- BACA URBINA. EVALUACIÓN DE PROYECTOS, Editorial McGraw Hill. México.
- TODD LAMMLE. CCNA CISCO. CERTIFIED NETWORK ASOCIATE.. Study Guide, Editorial Sybex , 1 ,999.
- PATRICK REGAN WIDE. AREA NETWORKS, Prentice Hall; 1st Edition (July 24, 2003).
- FRANCISCO MIRANDA GUZMAN, ANTONIO AVEDAÑO OSORIO, Trabajo de graduación DISEÑO, INSTALACIÓN Y ADMINISTRACION DE UN PROTOTIPO DE UNA INTRANET, Soyapango El Salvador 1,999.
- TED GREVERS and JOEL CHRISTNER, APPLICATION ACCELERATION AND WAN OPTIMIZATION FUNDAMENTALS (Paperback).
- DAVID MCDYSAN., VPN APPLICATIONS GUIDE: REAL SOLUTIONS FOR ENTERPRISE NETWORKS. (Paperback),Wiley.
- NETWORK MODELING, SIMULATION, AND ANALYSISs, Autor Ricardo F. GARZI, Publicado en 1990, inpublisher:"CRC Press".
- COMPUTER NETWORKING ESSENTIALS, DEBRA LITTLEJOHN SHINDE, (Paperback),Wiley.

6.1. Sitios de Internet.

- <http://www.cisco.com/web/learning/netacad/index.html>
Sitio oficial referente a redes CISCO.
- <http://www.ua.es/es/internet/vpnua/acceso/index.html>
Universidad de alicante.
- http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/conmutacion_paquetes.htm
Conmutación de paquetes.
- <http://www.dednet.net/institucion/itba/cursos/000183/demo/unidad01/conmutaciondecircuitos.htm>
Conmutación de circuitos.
- <http://technet.microsoft.com/es-es/library/bb124606.aspx>
página técnica de Microsoft.
- http://www.raduniversity.com/networks/2004/PacketSwitching/main.htm#_Toc80455261 conmutación de paquetes.
- http://www.ucaribe.edu.mx/archivos/freyes/IT0103/cbxc_wans.pdf Universidad del Caribe de México, Red pública.
- http://www.radioptica.com/Fibra/tipos_fibra_optica.asp
Página referida especialmente a Fibra óptica.
- <http://www.arqhys.com/arquitectura/cable-coaxial.html> Página referida especialmente a cable coaxial.
- <http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/REDES02.htm> Universidad de Argentina
- <http://www.lsi.uvigo.es/lsi/jdacosta/documentos/apuntes%20web/Topologia%20de%20redes.pdf> Universidad de Valladolid España
- <http://www.rhernando.net/modules/tutorials/doc/redes/sist.html> Redes en general
- http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/capa_enlace.htm. Universidad de Ecuador
- http://www.lcc.uma.es/~eat/services/fast_eth/fast_eth.htm# Universidad de Sevilla España