TÉCNICAS PARA ADMINISTRAR Y GESTIONAR REDES

YENEDYS YURYS DÍAZ PÉREZ
HÉCTOR ANDRÉS HOYOS MILLÁN

CORPORACION UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA DE SISTEMAS
CARTAGENA DE INDIAS D.T. y C
2008

TÉCNICAS PARA ADMINISTRAR Y GESTIONAR REDES

YENEDYS YURYS DIAZ PEREZ
HECTOR ANDRES HOYOS MILLAN

Monografía presentada como requisito para optar al título de INGENIERO de SISTEMAS

Director
ISAAC ZUÑIGA SILGADO
Ingeniero de Sistemas.

CORPORACION UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA DE SISTEMA
CARTAGENA DE INDIAS
2008

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena, Enero del 2008.

A Dios padre eterno por ser la luz de mi camino, por darme fuerza cuando me encontraba cansada y regocijarme con su amor en los momentos de desespero. A mis padres Aidee y Jaime por todos los sabios consejos que me dieron y me seguirán dando en mi vida y por enseñarme la dedicación y el amor a mi trabajo; a todos mis amigos, a mi cuñada Sandra y mis hermanos Yamil, Yubisay y Yirley por su apoyo incondicional, a mis sobrinos Shaid y Anderson porque en muchas ocasiones sacaron una sonrisa de mis labios en medio de alguna angustia y a mi novio Ronald por ser tan especial, agradable y amoroso conmigo.

Yenedys Diaz Perez

Dios por iluminarme y acompañarme a lo largo de mi carrera, quien me dio fuerza y salud para superar todos los obstáculos que encontraba en mi camino.

A mis hermanos Leovi Fernando y Leovi José, igualmente a Liliana por darme su apoyo y confianza en todo momento de igual forma
Por darme la inspiración que necesito para salir adelante.

A todos mis amigos y A toda mi familia por que hicieron posible
Cumplir este sueño.

A mi novia Yeismy que muchas veces estaba atenta a cualquier
Dificultad que se me presentaba, por ser tan especial y permitirme llegar a su corazón.

Finalmente a mi madre, quien fue mi apoyo incondicional, por la dedicación y entrega que todo hijo desea tener y sobre todo por el amor infinito día día ella depositaba en mi. Gracia madre, especialmente a ti dedico este logro.

Héctor A. Hoyos Millán

AGRADECIMIENTOS

Deseamos expresar nuestros agradecimientos a todas aquellas personas que han hecho posible la realización de esta monografía en especial a **Dios Padre** por ser el verdadero ingeniero en nuestras vidas, por habernos guiados, iluminarnos y permitir que esta monografía se llevara a cabo.

Queremos agradecerle al director de esta monografía, Ingeniero **Isaac Zuñiga Silgado**, el cual nos aporto su gran experiencia, el tiempo dedicado a esta monografía a pesar de sus múltiples responsabilidades y proyectos y su continuo apoyo en el proceso de esta monografía.

También queremos agradecer a la **CORPORACION UNIVERSITARIA TECNOLOGICA DE BOLIVAR** por habernos permitido gozar de sus instalaciones ofreciéndonos este Minor de Comunicación y Redes, a cada uno de los docentes que estuvieron presente en él por impartir sus ideas, en especial el ingeniero **Giovanni Vasquez**, por su generosidad, apoyo y sus constantes motivaciones para la realización de este minor y hacer todo lo que estaba en su alcance para hacer que todos nos sintiéramos bien en medio de este.

Por ultimo queremos agradecer a todo el cuerpo docente y a la **INSTITUCION UNIVERSITARIA TECNOLOGICO DE COMFENALCO** por estar presente desde los inicios y hasta el final de esta hermosa carrera.

AUTORIZACIÓN

Cartagena de Indias D.T.I.C Febrero 8 del 2008-02-04

Yo YENEDYS YURYS DIAZ PEREZ identificada con la cedula de ciudadanía: 45.558.495 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado "***TÉCNICAS PARA ADMINISTRAR Y GESTIONAR REDES",*** y publicarlo en el catalogo online de la biblioteca.

_____

YENEDYS YURYS DIAZ PEREZ

AUTORIZACIÓN

Cartagena de Indias D.T.I.C Febrero 8 del 2008-02-04

Yo HECTOR ANDRES HOYOS MILLAN identificado con la cedula de ciudadanía: 45.558.495 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado "***TÉCNICAS PARA ADMINISTRAR Y GESTIONAR REDES",*** y publicarlo en el catalogo online de la biblioteca.

_____

HÉCTOR ANDRÉS HOYOS MILLÁN

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Dado el crecimiento de las redes de comunicación y datos, en cuanto a interconexiones lógicos (Protocolos) y físicos (Cableado), surge la necesidad inherente de que las técnicas de administración también hayan ido evolucionando para que los administradores tengan un mejor manejo y análisis de las redes y para de esta manera ofrecer un mejor servicio. El objetivo de esta monografía es la de mostrar cuales son las técnicas que en la actualidad están siendo empleada por los administradores de la red para llevar a cabo el uso eficiente de los recursos como es, el Ancho de Banda. De ahí que se describen técnicas como el encolado, Enlaces agregados – Link aggregation (Trunking), balanceo de carga y enlaces redundantes, las cuales permiten no solo el mejoramiento de ancho de banda sino que traen consigo otros beneficios como: Minimización del tiempo, Reducción de costos, Detección de problemas en la r ed antes de que ocurra sin que éste llegue a materializarse y se tenga que tomar una acción correctiva, Disponibilidad de la red las 24 horas en los 365 días del año, La no saturación del canal.

Con respecto a lo que concierne a la técnica de encolamiento, esta monografía da a conocer que es una técnica de administración que provee prioridad en el trafico en la red, para ello esta técnica de administración utiliza los protocolos de: Encolado por peso justo o encolado inteligente - Weighted Fair Queueing (**WFQ**), El encolamiento equitativo con peso basado en clases - Class-Based Weighted Fair Queueing (**CBWFQ**), Encolado de prioridades - Low Latency Queueing (**LLQ**), en donde cada una de ellas, tiene características y funciones diferentes. A lo que compete al protocolo WFQ, su función radica en detectar los flujos de datos para luego clasificarlos en los más interactivos y menos interactivos, este

protocolo da prioridad a los mas interactivos o de bajo volumen los cuales serán enviados primero que los no interactivo o de alto volumen. Referente al protocolo CBWFQ, su ejecución se basa en la reservación de clases que define el usuario basadas en criterios de coincidencias como los protocolos, Acl´s, entre otros y por último para los protocolos LLQ define cuatro tipo de colas: Alto, Mediano, Normal y Lento, en el cual, el que presenta mayor rango de prioridad es el Alto o high y así sucesivamente hasta llegar al de menor rango de prioridad que es el Lento.

En el mismo orden de ideas, otra de las técnicas que se dará a conocer en esta monografía es la técnica de **Trunking** o mejor conocida como enlaces agregados, esta técnica básicamente lo que busca es aumentar el ancho de banda optimizando los costos, a través de esta técnica el administrador de la red puede tomar ciertos puerto físicos y conectarlos de tal forma que sean un solo enlace lógico, de esta manera se mejoraría es el ancho de banda con que cuenta la red. Anteriormente esta técnica solo podía conectar puertos con la misma velocidad pero gracias a los estudios eficientes, en la actualidad podemos encontrar Trunking con combinaciones de velocidades de 10\100\1000, de ahí que la agregación de enlaces y Gigabit Ethernet son tecnologías complementarias con las cuales se consiguen un ancho de banda, balancear cargas y permitir conexiones redundantes.

Acerca del balanceo de carga, esta es una técnica que el administrador de la red emplea para equilibrar el trabajo de los dispositivos, consiguiendo que todos los elementos que llevan a cabo la misma tarea, estén igualmente cargados con el fin de aumentar la potencia del cálculo, la calidad y disponibilidad del servicio.
Para llevar a cabo la implementación de estas técnicas es necesario cumplir con algunas de las políticas que permitan estandarizar y realizar de forma correcta su uso. Tales políticas fueron combinadas de distintas maneras conllevando a la evolución de nuevas arquitecturas de balanceo de carga.

Otra implementación importante es el manejo de redundancia en la red. La redundancia es una técnica que permite mantener la calidad de servicio en caso que se presente un fallo en cualquiera de los dispositivos que integran la red. Esta redundancia puede ser manejada de distinta maneras y desde distintas perspectivas. Estas pueden ser redundancia en el hardware y redundancia en el software. La redundancia en el hardware abarca todos los dispositivos que integran la red incluyendo el elemento esencial que es el servidor. En el servidor también puede haber redundancia de dispositivos internos tales como los discos duros, tarjetas de red etc. De igual forma se puede hacer redundancia en otros dispositivos como lo son los firewall, routers, switch e igualmente en el proveedor de servicio de internet ISP. El tipo de redundancia implementado en estos dispositivos es el llamado redundancia de caminos que permiten tener un dispositivo como reserva a un eventual fallo en la red.

Es por ello que en la siguiente monografía lleva al lector a alcanzar ciertos logros como el reconocer los protocolos que se utilizan en la técnica de encolamiento, la situación actual de la técnica de administración de trunking, la identificación de las configuraciones de la técnica de balanceo de carga: Round Robin DND y NLB; y la distinción de los diferentes métodos que utiliza la técnica de redundancia para su aplicación, cabe mencionar que el lector tenga en cuenta las siguientes recomendaciones: A medida que el lector entienda e identifique la utilidad de la técnica de administración de Trunking, éste debe ir implementándola para que pueda entender mejor su funcionamiento. Si va a llevar acabo la implementación de encolamiento a través de dispositivos se recomiendan los routers Cisco ya que proveen gran flexibilidad en los protocolos de administración de ancho de banda.

Se recomienda que en el balanceo de carga se utilice la configuración NLB por ser una técnica mas robusta que el Round Robin DNS.

Es importante tener en cuenta que, no vale la pena invertir en redundancia, si la inversión necesaria para tener un sistema redundante cuesta mas de lo que se perdería en dinero, y horas de trabajo si el sistema fallara.

INTRODUCCIÓN

Gracias a la evolución que ha tenido las comunicaciones en el mundo de la informática, el hombre en la actualidad cuenta con una gran herramienta como son las redes de datos. La necesidad que el hombre tenía para comunicarse a larga distancia, permitió que no solo se limitaran a tener ciertos ordenadores interconectados entre sí en una sala, sino que era necesaria la conexión de ellos con otros ordenadores que se encontraran en diferentes salas de una empresa, y con el resto de las sucursales situados en diferentes puntos geográficos. De igual forma con el crecimiento de las redes, el hombre se vio en la tarea de garantizar tanto el funcionamiento como el mantenimiento de la misma, es así como surge la necesidad de la administración de las redes.

Hoy día las empresas han considerado la importancia del manejo de su información así como también de la red que la comunica y la forma en que ésta la trasmita. En consecuencia, son muchas las funciones que se deben llevar a cabo para garantizar el flujo de dicha información, de las cuales las más importantes son de velar por la gestión de la red y garantizar el buen funcionamiento de los dispositivos que la componen.

El tema de "**TÉCNICAS PARA ADMINISTRAR Y GESTIONAR REDES"**, es de suma importancia porque la alta sistematización en las empresas, ha llevado a estas a la necesidad de saber el actual funcionamiento de sus equipos. A grandes rasgos, con la técnicas de Administración de redes se pueden llegar a anticiparse a fallos y detectar el impacto que este causaría en la prestación de servicio a un usuario si este no se detecta a tiempo, además estas técnicas permite que el administrador de redes, pueda conocer los mecanismos óptimos que se pueden emplear en el momento de administrar o controlar la red de tal forma que sean eficiente. Existen en el mercado diversos programas que permiten al administrador de una red gestionarla, alguno son gratuitos y otros son muy costosos. De igual forma, estos, trabajan con técnicas de funcionamiento que hoy en día algunas están obsoletas debido al alto requerimiento de recursos que las empresas manejan las cuales requieren de un elevado o mejoramiento ancho de banda.

Las técnicas de administración de redes no son más que técnicas que tienen la función de organizar, supervisar y controlar cada uno de los elementos de comunicación para garantizar un nivel de servicio optimo a unos costos razonables, de ahí que el objetivo principal de la administración es mejorar la disponibilidad e incrementar la efectividad de la red, todo esto basándose en ciertos componentes administrativos a nivel organizacional, técnico y funcional que permiten que el objetivo de la administración se conciba.

Las técnicas plasmada en este trabajo de monografía, son técnicas que desde tiempos atrás se han venido empleando, pero con poca asiduidad por que muchos administradores las desconocen o por la incompatibilidad que algunas de ellas manejaban lo cual era poco rentable para algunas organizaciones o entidades, pero gracias a la evolución que las redes y a su vez la administración de redes

han tenido, estas técnicas han evolucionado hasta permitir la administración de redes con equipamiento de diferentes fabricantes.

De acuerdo a lo anterior, a través de esta monografía se da a conocer como es el proceso que se lleva a cabo en la administración de las redes, sobre todo las técnicas para administrar y gestionar redes que están implementando hoy en día como son el ***Trunking***, el ***balanceo de carga***, el ***encolado*** y la ***R*****edundancia**. Cada una de ella presenta una función específica las cuales traen infinitas ventajas.

En conclusión, estas técnicas que actualmente se encuentran en fuerte uso, son técnicas que lo que buscas es mejorar el ancho de banda de la red, para que de este modo hacer un buen uso de los recursos con que cuenta la organización o entidad y aumentar el rendimiento de la red.

OBJETIVOS

OBJETIVO GENERAL

Establecer a través de un análisis investigativo acerca de las técnicas para administrar y gestionar redes informáticas y evolución que han tenido estas en la actualidad.

OBJETIVOS ESPECÍFICOS

- Desarrollar un análisis descriptivo de los protocolos de encolamiento que se han venido implementando, detallando las características principales que han permitido mantener su predominio en las aplicaciones administrativas de las redes informáticas.

- Hacer un resumen especifico de los formas y mecanismos utilizados por los administradores de red hoy en día, para llevar a cabo las conexiones troncales (Trunking) y las tecnologías (protocolos) utilizadas para este fin.

- Describir la implementación de la técnica de Balanceo de Carga (load Balancing) en la administración de redes en la actualidad, así como también los métodos utilizados por la misma y las mejoras que ha tenido hoy día.

- Realizar una breve descripción de los métodos utilizados para el manejo de la redundancia actual, teniendo en cuenta la perspectiva en la importancia de su aplicación, los diferentes campos de aplicación beneficios y el impacto que puede éste causar en el sistema.

Capitulo 1.

TÉCNICA DE ADMINISTRACIÓN DE REDES POR ENCOLAMIENTO

1.1 INTRODUCCIÓN.

La administración de la red, de alguna u otra manera su finalidad está muy ligada a la calidad del servicio de la red, porque el administrador de la red debe velar por que los tres pilares de las redes de comunicación se cumplan: Disponibilidad, integridad, confiabilidad, si una red presenta estos tres pilares se dice que es una red con calidad de servicio. Ahora bien para proporcionar una calidad de servicio en una red, es necesario que los elementos que conforman la red lo presenten (QoS). Es ahí en donde las técnicas de administración de red entran en función para poder lograr el objetivo que es la de brindar una red segura y con alto nivel de QoS.

De acuerdo a lo anterior, la alta calidad de servicio hace énfasis a la capacidad que tiene la red de proporcionar un servicio de conexión mejorado a cierto tráfico de la red de comunicaciones, para ello es necesario disponer de:

- Un soporte a la red para que ha un determinado tráfico se le dedique el ancho de banda.

- Conformar el trafico y la gestión en la red y evitar cualquier congestión en el.
- Establecer prioridades al tráfico de la red.

En la actualidad son muchos los factores que han conllevado a que se haga una administración pertinente, sobre todo al ancho de banda de la red con que se cuenta. Factores como el acrecentamiento del uso de tecnologías de Internet, un sin número de servicios que son ofrecidos a través de Internet, el costo de la conexión a Internet sobre todo en entidades que manejan gran cantidad de datos, entre otros, todos estos factores son los que influyen a que este el ancho de banda sea administrado de tal modo que se establezcan prioridades y prevenir el uso de este recurso indebidamente.

1.2. CONCEPTO DE LA TÉCNICA DE ENCOLADO

Casi la totalidad de los métodos que se utilizan para administrar el ancho de banda ya sea a través de software que opera en servidores o en dispositivos, se basan en colas de tráfico, o mejor llamado ***Encolamiento***.

Estas colas de tráfico se configuran dependiendo del nivel de complejidad que requiera el control del tráfico en la red, de tal forma que estas puedan distinguir los flujos de datos que viajan por la red. De ahí que la administración de ancho de

banda a través de la técnica de encolamiento implica decidir que trafico tiene mayor prioridad, como asegurar que este tráfico tenga siempre el ancho de banda que necesita, como manejar el tráfico de menor prioridad y restringir el uso indebido entre otros.

De acuerdo a lo anterior, el encolamiento es entonces, una técnica de administración de red que se utiliza para el control de la congestión. Por defecto cada interfaz de una router tiene una cola de salida la cual se gestiona con una estrategia FIFO (First in First out).

La mayoría de routers en Internet implementan colas de este tipo con descarte ***tail drop***. Esto quiere decir que el paquete colocado en la cola para ser entregado a la red es el primer paquete en alcanzar el router, sin que este realice algún análisis del estado de la red ni de las métricas actuales del flujo al que pertenece el paquete, ahora bien, cuando el router recibe paquetes más rápido de lo que los puede retransmitir, los debe almacenar en la cola, cuando esta cola se llena los paquetes que siguen llegando al router son descartados, en esto consiste este tipo de cola FIFO.

En el mismo orden de ideas, cabe especificar que "CISCO define que un interfaz está congestionado cuando se alcanza un 75% de tiempo de uso"[1]. Es por ello que para el control de la congestión, el router establece en la interfaz varias colas donde se colocarán los paquetes dependiendo de sus prioridades, las cuales según destinos algorítmicos, los router planean como emplear estas colas para evitar la congestión en la red.

[1] Tomado de Internet: www.ua.es/es/**se**rvicios/syf/formacion/cursos_programados/2007/otrasconvocatorias/documentacion/tema_6_1.pdf -

1.3 PROTOCOLOS DE LA TÉCNICA DE ENCOLAMIENTO.

A través de los protocolos, números de puertos interfaces de entrada, direcciones MAC, entre otras, la técnica de encolamiento puede identificar el tipo de tráfico en la red. La operación que realizan los protocolos de encolamiento se llevan cabo en tres etapas, en primera instancia la clasificación del tráfico de entrada, en segunda instancia la asignación de una cola, y por último la entrega del tráfico de salida de acuerdo a las características de dicho tráfico.

Estos protocolos de encolamiento encargados de establecer políticas eficientes para administrar el ancho de banda de tal forma que se reduzca los costos coligados a la adquisición de una mayor cantidad de este recurso, son:

- Encolado por peso justo o encolado inteligente - Weighted Fair Queueing (WFQ).

- El encolamiento equitativo con peso basado en clases - Class-Based Weighted Fair Queueing (CBWFQ).

- Encolado de prioridades - Low Latency Queueing (LLQ).

1.3.1 Encolado por peso Justo o Encolado Inteligente WFQ : WFQ (Weigh Fair Queueing) también conocido con las siglas FQ por **Fair Queueing**, es un algoritmo de encolamiento basado en el flujo que realiza dos cosas simultáneamente, básicamente este tipo de encolamiento lo que hace es asignar

el grado de prioridad equitativamente, clasificando el flujo de datos que detecta en “flujo de datos más interactivos” y “flujo de datos menos interactivos”, de ahí su nombre encolado por peso justo. básicamente lo que este protocolo permite, es que se tenga una justa asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para enlaces de velocidades menores a 2048 Mbps

Este protocolo gracias a que asegura que las colas no mueran de inanición por falta de ancho de banda, se puede implementar cuando se desee proveer un tiempo de respuesta razonable a todos los usuarios de la red sin agregar demasiado ancho de banda.

WFQ utiliza combinación de parámetros par el adecuado ordenamiento del flujo de tráfico, Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto de origen, entre otro. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean llevados al final de la cola, y los volúmenes bajos sean llevados al principio de la cola. De ahí que el “flujo de datos más interactivos” o Los flujos tráfico de bajo volumen, reciben un servicio preferencial, porque son los que comprende la parte más importante del tráfico transmitiendo toda su carga en el momento oportuno. Mientras que Los “flujo de datos menos interactivos” o flujos de tráfico de alto volumen comparten entre ellos la capacidad remanente equitativamente.

Uno de los beneficios que trae la utilización de este protocolo es porque está diseñado para minimizar los esfuerzos de configuración y adaptarse automáticamente a las condiciones de cambio del tráfico en las redes.

1.3.2. El encolamiento equitativo con peso basado en clases o CBWFQ: Este protocolo también maneja encolamiento equitativo con pesos, y además le permite al administrador de la red definir una clase de trafico asignándoles ciertas características. Estas clases se definirán a través de ciertos criterios de coincidencia como las Listas de acceso (ACLs), protocolos e interfaces de entrada, en donde los paquetes que contengan estos criterios de coincidencia, constituirán el tráfico de una clase, la cual se dirigirá hacia la cola reservada correspondiente a dicha clase.

Una vez que se ha definido una clase de acuerdo a los criterios de coincidencia, se le pueden asignar ciertas características como: el peso que es el que se convierte en el peso de cada paquete, límite máximo de paquetes, asignar ancho de banda y el límite de la cola[2], Esto significa que los paquetes con la misma dirección IP de origen y destino, puerto TCP o UDP de origen y destino, son clasificados como pertenecientes al mismo flujo.

A través de este tipo de encolamiento, lo que se pretende es especificar la cantidad en porcentaje de ancho de banda que se le dedica a cada flujo.

En el mismo orden de ideas, del ancho de banda que se le asigno a una clase específica en el momento de su configuración se obtiene el peso para el paquete de dicha clase. Luego de que se le asigna un peso a un paquete, el paquete es puesto en la cola respectiva a la clase. CBWFQ usa los pesos asignados a los paquetes encolados con el fin de asegurar que la cola de la clase es utilizada equitativamente. Por otra parte, el ancho de banda y el límite de la cola, son la base de los paquetes que pertenecen a una clase, ya que estos están sujetos a aquellos. Es decir que cuando una cola, ha llegado o ha alcanzado su límite, se produce un descarte posterior[3] o un descarte de paquetes.

[2] El límite de la cola es el número máximo de paquetes acumulados en la cola.
[3] El descarte posterior entra en función cuando se produce una condición de congestión.

1.3.2.1 Beneficios de la implementación del protocolo CBWFQ:

- ***Asignación de ancho de banda Controlada***: Permite establecer la cantidad precisa de ancho de banda para un tráfico o una clase especifica.

- **Existencia de Escalabilidad**: A través de los criterios de coincidencia, los cuales van más allá de los límites de flujo, se puede definir quienes conforman una clase.

- **Clasificación del tráfico:** A través del uso de los criterios de coincidencia como listas de control de acceso, protocolos o nombres de interfaces de entrada se puede definir como sería clasificado el tráfico, lo cual facilita la gestión de los paquetes.

1.3.2.2 Configuración de Políticas de Clase mediante el protocolo CBWFQ: Esta configuración consta de tres etapas:

- **Definir un mapa de clases**: A través de este proceso se podrán determinar los tráficos de clases para especificar la política de clasificación.

- **Asociación de políticas a cada clase de tráfico**: en esta etapa a través de un mapa de clases, se aplica la configuración de las políticas

para las clases de tráfico, a los paquetes que pertenecen a alguna de las clases definidas previamente.

- **Asociar políticas a las interfaces:** Esta etapa consiste en adjuntarle a la interface un mapa de políticas de servicios existentes para que de esta manera se designe este conjunto de políticas a dicha interface.

1.3.3 Encolado de prioridades o LLQ (Low latency queueing): Este tipo de encolamiento es el que define cuatro tipo de colas: High- Alto, Médium - Mediano, Normal y Low - Lento, esto se realiza con el fin de que cuando haya una información en la cola de más alto rango o prioridad, en este caso el High ó Alto, se enviará primero que la información que se encuentra en una de las colas de menor prioridad (mediano, normal, lento).

Este protocolo garantiza que las clases de tráficos tengan el ancho de banda que necesitan, anexionando encolamiento con prioridad estricta a el protocolo CBWFQ, para que de esta manera se puedan implementar clases de prioridad, y se del desenconamiento y la transmisión de datos sensibles a retardo tales como la voz antes que sea transmitidos antes que los paquetes de otras colas, a diferencia del protocolo CBWFQ, que es altamente intolerable ante retardos, especialmente en aquello que presentan ciertas variaciones como es la voz.

Otra característica que diferencia los protocolo LLQ de los CBWFQ, es el orden de envió de los paquetes, debido a que el CBWFQ, define el peso para un paquete perteneciente a una clase específica por el ancho de banda que se le asignó a dicha clase cuando se configuró, por lo tanto el ancho de banda es quien definirá el orden en que los paquetes serán enviados, es decir que en el CBWFQ, los paquetes son atendidos equitativamente basándose en el peso, por que estas no tienen consigo ninguna prioridad estricta garantizada.

Una de las desventajas que este protocolo tiene es que se recomienda utilizarlas solo para el tráfico de voz más no para el tráfico de videos, porque este último puede incluir ciertas variaciones en el retardo que pueden llegar a afectar la transmisión correcta del tráfico de la voz.

1.3.3.1 Formas de implementación del protocolo LLQ: Existen dos comandos que permiten la implementación del protocolo LLQ

- **Comando Priority:** Para el protocolo CBWFQ, que es un protocolo intolerable ante retardos, principalmente en aquello que presentan variaciones como es en el caso de la voz, la técnica de encolamiento de baja latencia provee una Prioridad estricta a este protocolo para que pueda reducir los Jitter[4] en las conversaciones de voz. Al configurar el comando **priority**, se permite el uso de una cola de prioridad estricta dentro de CBWFQ, para ello se crean clases de prioridad, en donde el tráfico perteneciente a una clase de prioridad [5] es dirigido hacia la única cola de prioridad estricta.

- **Comando Prioridad ip rtp:** permite el uso de colas de prioridad fuera de CBWFQ. A través de este comando los criterios de coincidencia como ACL's, puertos, direcciones ip, entre otros, se aplican al tráfico de prioridad, además con este comando se dan servicios de prioridad estricta dentro de un rango de puertos UDP.

[4] Los jitter son irregularidades de transmisión de tráfico de voz, que se escuchan en medio de la conversación producto de las variaciones en el retardo.

[5] Se le llama clase de prioridad a llas clases a las que se les aplica el comando **priority**

Capitulo 2.

AGREGACIÓN DE ENLACES – TRUNKING

2.1 INTRODUCCIÓN

En este capítulo se presenta una técnica de administración conocida con el nombre de ***agregación de enlaces- trunking*** especificado por el Instituto de ingeniería eléctrica y electrónica **IEEE 802.3 ad** como Link aggregation.

Esta técnica es de vital importancia puesto que a través de ella se puede llegar a garantizar el aumento o mejoramiento del ancho de banda en la red, debido a ello esta técnica es eficaz y eficiente más aun en nuestros días en donde la integración de voz, video y datos en la redes están en pleno auge, y muchas entidades financieras, estudiantiles , corporaciones, entre otras, manipulan redes que manejan un alto trafico de información y necesitan la utilización de un canal grande para poder transmitirla, de esta manera vemos reflejado que esta técnica es sumamente importante en el campo de la administración de redes.

En este capítulo también se especifican las ventajas que esta técnica presenta en el momento de su uso y algunas desventajas que con el paso del tiempo algunas ya no existen por el mejoramiento que esta ha tenido en medio de su proceso evolutivo.

2.2 CONCEPTO DE TRUNKING

Es la técnica que se emplea para aumentar el ancho de banda en una red, a través de dos dispositivos ya sean Switches, routers, servidores, entre otros, conectados paralelamente por dos cables bajo un modo Full – Dúplex. En otras palabras, a través de esta técnica el flujo de datos que será transmitido entres los dos dispositivos, se particionan para que paralelamente sean transmitido por varios puertos del dispositivos que simulan ser un solo enlace lógico, de esta manera se logra el objetivo que es la de obtener un canal de comunicación ampliado. La siguiente figura muestra claramente como es el proceso trunking.

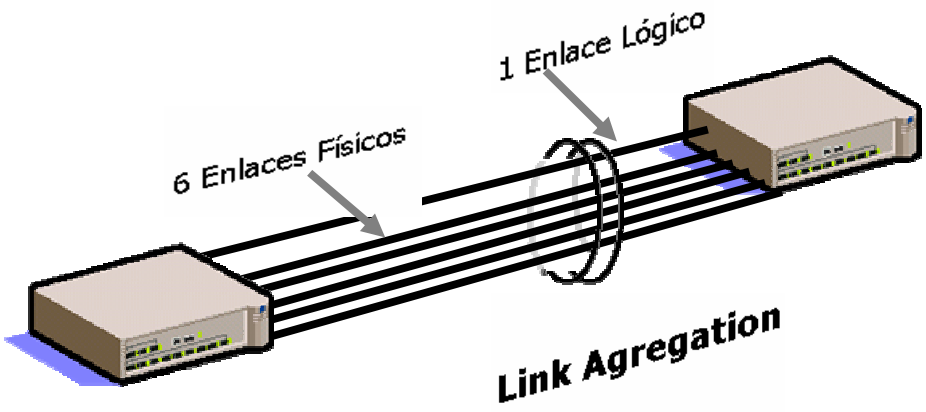


Figura N°1.
Implementación de Trunking

Cabe mencionar que la velocidad de un enlace agregado esta dado por la suma de ancho de banda de cada uno de los enlaces físicos, esto es lo que se conoce con el nombre del Throuput. De acuerdo a la anterior grafica, si cada enlace físico tiene un ancho de banda de 100 Mbps, al aplicar la técnica de trunking con estos 6 enlaces físico, se tiene un mejoramiento de banda de 600Mbps.

2.3. VENTAJAS DEL TRUNKING

- **Reducción de los costos:** Uno de los temas más importantes en el momento de diseñar, construir, actualizar y administrar la red son los costos de inversión que se debe hacer. Utilizando la técnica de trunking no es necesario que para poder aumentar el ancho de banda en la red se deban cambiar los dispositivos existentes o el cableado con que cuenta la red, ni que se compren dispositivos externos a estos.

- **Evita la congestión en la red:** Uno de los problemas más frecuentes que se presentan en la red es la formación de los denominados "***cuello botella***". Este problema en la red es frecuente cuando el administrador no aplica las técnicas correspondientes para evitar la aparición de ellos, a través del trunking la red está libre de que problemas como estos surja por el incremento en el ancho del canal.

2.4 ENLACES AGREGADOS EN LAS VLANS

En las vlan los enlaces agregados se conocen como Trunk – “troncos” o enlaces troncales. Del mismo modo como se ha venido describiendo los enlaces agregados, estos enlaces trunk en las Vlans son enlace punto a punto que designan una conexión de red que transportan múltiplex Vlans identificadas por etiquetas que se le asigna a los paquetes , cuyo propósito es la de conservar los puertos cuando se crea un enlace entre dos dispositivo que implementan las Vlans, permitiendo de esta manera que el trafico de varias Vlans viaje a través de un solo cable entre Switch o entre los switch y los router.

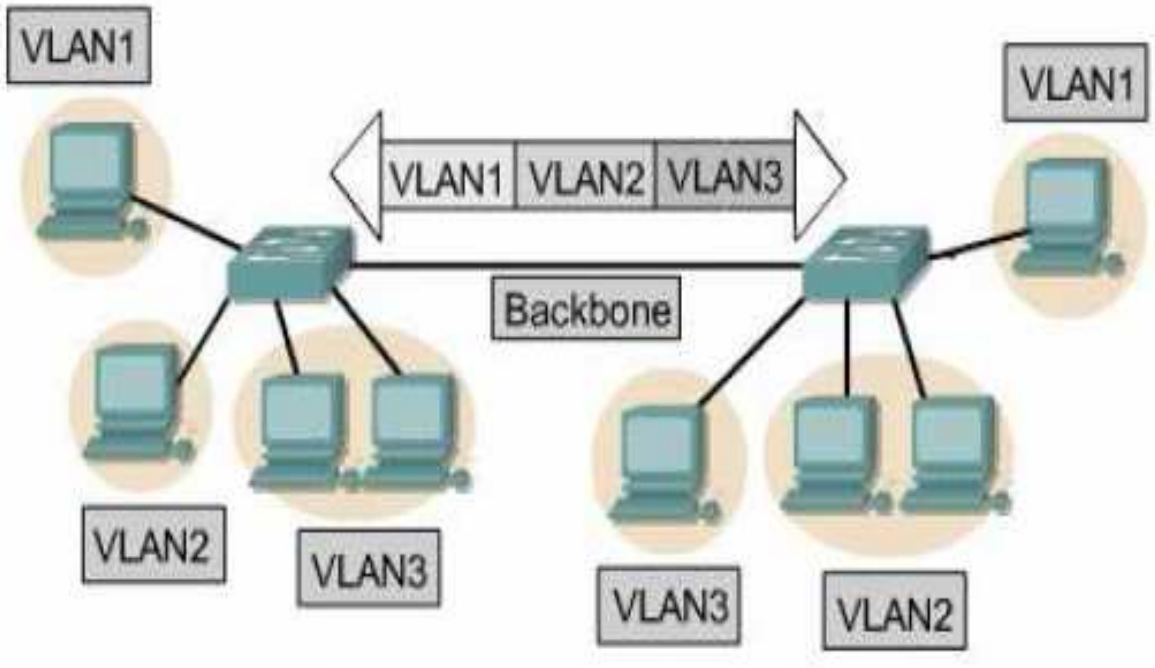


Figura N°2.
Enlaces Agregados

2.4.1 Mecanismos de los enlaces agregados en las Vlans: Existen dos tipos de mecanismos que son esenciales para la agregación de enlaces o enlaces troncales en las Vlan. Estos mecanismos son Filtrado de tramas[6] y etiquetado de tramas, pero con el paso del tiempo, el Instituto de ingeniería eléctrica y electrónica (**IEEE)** prohijó como único mecanismo estándar para los enlaces troncales al etiquetado de tramas, por que a través de este mecanismo se logra una trasmisión de datos más rápida y facilita la administración de los datos. El etiquetado de tramas, que es un mecanismo que trabaja a nivel de capa 2, coloca un identificador[7] que viaja por el backbone de la red, el cual es eliminado antes de que la trama llegue al destino. Existen dos tipos de etiquetados el **Inter Switch Link (ISL)** y el estándar **802.1Q**. El primero es un protocolo que tiene la función de mantener información de VLAN en el trafico entre dispositivos, este protocolo es propietario de Cisco, por ende el proceso de encapsulación solo es soportado entre los dispositivos fabricados por Cisco a través de los enlaces fase y Gigabit-ethernet. El segundo es un estándar diseñado con el fin de permitir realizar la técnica Trunking sin tener ningún tipo de interferencia

Un protocolo de agregación de enlaces en las Vlans es el **VTP** el cual es un protocolo de mensajería propietario de Cisco, fue creado con el fin de solucionar problemas que se presentaban en las Vlans por la forma de configuración de estas. A través del protocolo VTP la coherencia VLAN se mantiene en todo el dominio de administración y se reduce la complejidad de administración y monitorización de las redes VLAN.

[6] Es bloquear o permitir el paso a los paquetes de datos de una forma selectiva. Ellas toman sus decisiones basadas en los protocolos de capa 3 y 4.
[7] Encabezado de cada trama, el cual es único.

2.5 SITUACIÓN ACTUAL DE LA TÉCNICA DE ADMINISTRACIÓN DE RED TRUNKING.

Esta técnica de administración de redes, desde hace muchos años atrás los administradores de red lo implementabas, debido a que era una técnica que ampliaba el canal de transmisión sin necesidad de invertir en elementos externos a los que se tenían para aplicarlo. En ese entonces, los fabricantes soportaban esquemas de trunking propietario para Ethernet 10/100 y FDDI, con el paso de los años se dio la aparición del estándar Giga bit Ethernet, motivo por lo cual muchos fabricantes optaron por lanzar este tipo la técnica de trunking en dispositivos propios que soportaban este nuevo estándar, pero esta técnica de Trunking estaba diseñada para trabajar especialmente con una única marca de equipamiento, esto fue precisamente lo que llevo a la evolución de esta técnica hasta obtener lo que hoy en día tenemos.

Actualmente, según la norma IEEE 802.3ad, esto ya no es motivo de complicación, puesto que esta define cómo dos o más conexiones Giga bit Ethernet pueden ser combinadas para compartir o equilibrar las cargas y proporcionar un mejor soporte a las conexiones de red de grandes anchos de banda.

2.5.1 Características del actual Trunking.

- **Mayores anchos de Banda:** Anteriormente, cuando se decía que una red contaba con 1Gbps el cual no era un ancho de banda suficiente para el trafico de los datos, era imposible de creer , pero en realidad es que, en

nuestros días, muchos proveedores de Internet (IPS) y administradores de red se han dado cuenta de que esta cantidad para un ancho de banda no es lo suficientemente grande para los datos que actualmente organizaciones o entidades utilizan y necesitan ser transportados por la red. Pero si se implementan agregación de enlaces para agrupar en múltiples puertos velocidades de 10/100/1000 Mbps consiguiendo un enlace lógico punto a punto más rápido entre los dispositivos de la red, se obtendría un ancho de banda deseable. Es por ello que esta técnica siempre se tendrá en cuanta, cuando lo que se es de aumentar o mejorar el ancho de banda d una red. Además de mayor ancho de banda, el trunking va muy ligado a otras técnica de administración de redes llamada enlaces redundantes <<ver capitulo 4 >> para que así no solo se llegue a tener una red con aumento de el ancho de banda sino también el aumento de la fiabilidad de ella.

- **Escalabilidad:** Este es un factor importante en torno al Trunking, porque de la misma forma, en que la necesidad de incrementar el ancho de banda fue llevando a la evolución de esta hasta permitir su distribución dinámica, en un futuro, los servidores con la necesidad de utilizar más capacidad de procesamiento llevaran a la agregación de enlaces a permitir ascender a varios gigabits por segundo ya sea en modo half-duplex o full dúplex.

- **Disponibilidad en la red:** A través de esta técnica, el conseguir que la red este en funcionamiento a pesar de alguna falla en algunos de los puertos que pertenece a un enlace lógico, no es complicado, puesto a que esta técnica de agregación de enlaces proporciona una inherente redundancia automática en enlaces punto a punto, es decir que si uno de los múltiples puertos utilizados en un enlace agregado falla, el tráfico de red se redirige

dinámicamente a los puertos de dicho enlace que permanecen activos. De esta manera la red continuaría su operación sin necesidad de interrumpir el servicio de conexión, esto gracia a que el re direccionamiento por parte de switch se realiza de una forma tan rápida, que advirtiendo que la dirección de control de acceso al medio (MAC) de un puerto del enlace agregado se ha reasignado automáticamente a otro puerto del mismo enlace; enviando los datos a la nueva localización del puerto.

- **Asignación dinámica:** Inicialmente, cuando esta técnica está empezando a implementarse por parte de los administradores de red, presentaba un inconveniente que muchas veces impedía el buen uso de ella, era que no permitía la asignación dinámica de velocidades en los puertos, es decir que si se iba a aplicar trunking en la red para formar un canal de 320 Mbps se tenían que utilizar por ejemplo 4 puerto con velocidades de 100 Mbps, dando esto un mal uso de ancho de banda pues quedaba un canal mucho más amplio que lo que realmente se necesitaba, simplemente porque no se podían combinar los puertos con diferentes velocidades.

  Gracias a la evolución que esta técnica de administración a tenido, esto ya es un mito, puesto que en la actualidad una de las ventajas que los enlaces agregados o trunking tiene es la de poder usar combinaciones de estas velocidades (Ethernet 10/100/1000 Mbps) en un único enlace lógico, es decir que actualmente se puede añadir ancho de banda de una manera incremental y asequible.

2.6 PROTOCOLO DE AGREGACIÓN DE ENLACES LAN DINÁMICOS: TRONCAL MULTI-ENLACE / MULTI- LINK TRUNKING (MLT)

Esta tecnología de agregación de enlace denominada ***Troncal Multi-Enlace*** fue especificado por el Instituto de ingeniería eléctrica y electrónica, estándar **IEEE 802.3,** la cual consiste en la agrupación de varios enlaces físicos Ethernet en un único enlace lógico Ethernet para proveer tolerancia a fallos y enlaces de alta velocidad entre routers, switches y servidores.

Actualmente, con esta tecnología se pueden usar varios enlaces combinándolos de tal forma que permitan aumentar el ancho de banda y la disponibilidad en la red a través de los caminos redundantes, cosa que inicialmente no se permitía, por que anteriormente no se utilizaban los enlaces redundantes sino la utilización del protocolo Spanning tree Protocol (STP) que protegía a la red contra los bucles.

Esta tecnología tiene una función esencial y es la de garantizar la tolerancia a fallos. Si uno o más enlaces fallan, la tecnología MLT es la que se encarga de re direccionar automáticamente el tráfico entre los enlaces restantes, esta redistribución automática se produce en menos de medio segundo y es transparente a los usuarios.

2.7 CONFIGURACIÓN TRUNKING

A través de la siguiente grafica se refleja el manejo de trunking en 2 switch:

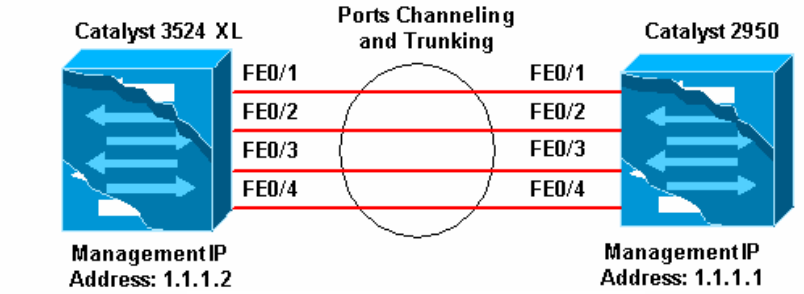


Figura N 3.
Trunking entre dos Switch

Catalyst 3524 XL
Comments between the ouputs are added in *blue* italics for explanation. Switch3524#**sh run** Building configuration... Current configuration: ! version 12.0 no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption

```
!
hostname Flush
!
!
ip subnet-zero
!



!--- Since the 2900XL/3500XL switches do not support
!--- dynamic channel negotiation,verify the
!--- configuration before enabling secondary links.
!--- You may see a loop before the configuration is finished if
!--- both ports are connected while doing changes.
!--- Shut down the ports involved in the channel first. When the
!--- configuration is complete, enable them back.

!--- An example of a brief loop is shown below.
!--- flush#
!--- 6d12h: %LINK-4-ERROR: FastEthernet0/1 is experiencing errors.
!--- 6d12h: %RTD-1-ADDR_FLAP: FastEthernet0/3 relearning five addresses per
minute.
!--- 6d12h: %LINK-4-ERROR: FastEthernet0/1 is experiencing errors.
!--- 6d12h: %RTD-1-ADDR_FLAP: FastEthernet0/24 relearning eight addresses
per minute.
!--- 6d12h: %LINK-4-ERROR: FastEthernet0/1 is experiencing errors.
!
!
interface FastEthernet0/1
port group 1
```

```
!--- Assigned port to port channel 1.
switchport trunk encapsulation dot1q
switchport mode trunk
!--- Configured port to be in trunking mode.
!

interface FastEthernet0/2
port group 1
!--- Assigned port to port channel 1.
switchport trunk encapsulation dot1q
switchport mode trunk
!

interface FastEthernet0/3
port group 1
!--- Assigned port to port channel 1.
switchport trunk encapsulation dot1q
switchport mode trunk
!

interface FastEthernet0/4
port group 1
!--- Assigned port to port channel 1.
switchport trunk encapsulation dot1q
switchport mode trunk
......(output Suppressed)
!
interface VLAN1
ip address 1.1.1.2 255.255.255.0
```

no ip directed-broadcast
no ip route-cache
!
line con 0
transport input none
stopbits 1
line vty 0 4
login
line vty 5 15
login

Catalyst 2950
Comments between the ouputs are added in *blue* italics for explanation. Switch2950>en Switch2950#**sh run** Building configuration... Current configuration : 1298 bytes ! version 12.1 no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption !

```
hostname Hanka
!
!
ip subnet-zero
!
interface Port-channel1
flowcontrol send off
switchport mode trunk
!--- Since the 2900XL/3500XL series switches do not
!--- support dynamic channel negotiation,
!--- please verify the configuration before
!--- enabling secondary links.
!--- You may see a loop before the configuration is
!--- finished if both ports are connected while doing changes.
!--- We suggest shutting down the ports involved in the channel
!--- first, and when the configuration is complete,
!--- enabling them back.
!--- An example of a brief loop is shown below.
!--- flush#
!--- 6d12h: %LINK-4-ERROR: FastEthernet0/1 is experiencing errors.
!--- 6d12h: %RTD-1-ADDR_FLAP: FastEthernet0/3 relearning five addresses per
minute.
!--- 6d12h: %LINK-4-ERROR: FastEthernet0/1 is experiencing errors.
!--- 6d12h: %RTD-1-ADDR_FLAP: FastEthernet0/24 relearning eight addresses
per minute.
!--- 6d12h: %LINK-4-ERROR: FastEthernet0/1 is experiencing errors.
!
interface FastEthernet0/1
 switchport mode trunk
```

```
!--- Configured port to be in trunking mode.
 channel-group 1 mode on
!--- Assigned port to port channel 1.
!--- 2950 switches only support 802.1q encapsulation,
!--- which is the configured automatically
!--- when trunking is enabled on the interface by
!--- issuing the switchport mode trunk command.
!--- Note: The channel-group command is introduced in IOS 12.1. IOS
!--- 12.0 has the port group command
!--- to configure channeling.

!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode on
!--- Assigned port to port channel 1.
!
interface FastEthernet0/3
 switchport mode trunk
 channel-group 1 mode on
!--- Assigned port to port channel 1.
!
interface FastEthernet0/4
 switchport mode trunk
 channel-group 1 mode on
!--- Assigned port to port channel 1.
.....(output Suppressed)
interface Vlan1
 ip address 1.1.1.1 255.255.255.0
```

```
 no ip route-cache
!
ip http server
!
line con 0
 transport input none
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Capitulo 3

EVOLUCIÓN DE LAS TÉCNICAS DE BALANCEO DE CARGA

3.1. INTRODUCCIÓN

El balance o balanceo de carga es un término comúnmente utilizado en informática. Este se refiere a la manera o técnica que utiliza el administrador de un sistema de red, para compartir equitativamente el trabajo de los procesos u otros recursos que están siendo ejecutados por un dispositivo, de manera que se equilibre dicho procesos entre los dispositivos que intervienen en tal balance. Tiene como objetivo conseguir que todos los elementos que llevan a cabo la misma tarea, estén igualmente cargados con el fin de aumentar la potencia del cálculo, la calidad y disponibilidad del servicio (Figura N°4).

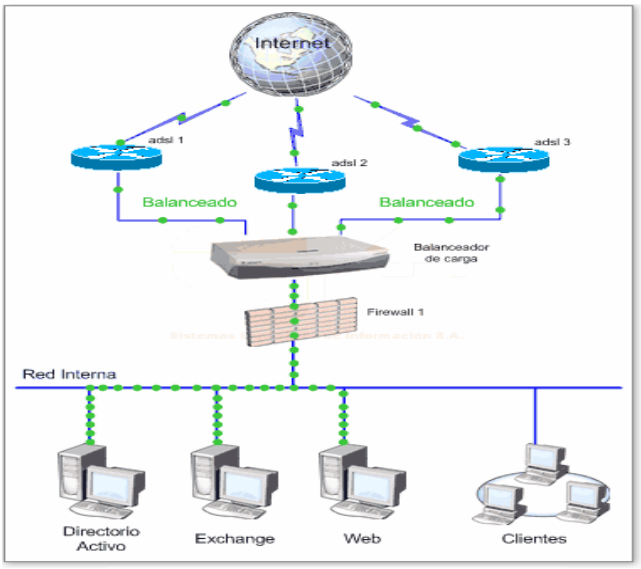


Figura N°4. Balanceo de carga

Está ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.

El *balanceo de carga* se mantiene debido al uso de un algoritmo que divide de la forma más equitativa posible el trabajo, para evitar los denominados *cuellos de botella* que es el objetivo del multiprocesamiento.

Existen técnicas de balanceo de carga que comúnmente se utilizan en el mercado. Los más utilizados son:

- Round Robin
- NLB (Network Load Balancing)

3.2 POLÍTICAS DE BALANCEO

Cuando se diseña un servicio de balanceo de carga es importante seleccionar un algoritmo adecuado que decida que replica procesara el requerimiento que llega. Por ejemplo, aplicaciones donde todos los requerimientos generados de carga son muy semejantes pueden aplicar un algoritmo Round-Robin, mientras que aplicaciones donde la carga generada por cada uno de los requerimientos no puede ser predicha requiera de algoritmos más complejos.

En general las políticas de balanceo pueden ser clasificadas dentro de las categorías siguientes:

- No adaptativa
- Adaptativa

Las políticas anteriormente descritas, fueron combinadas de distintas maneras conllevando a la evolución de nuevas arquitecturas de balanceo de carga como son:

- No adaptativa Por Sesión
- No adaptativa Por Requerimiento
- No adaptativa Sobre Demanda
- Adaptativa Por Sesión
- Adaptativa Por Requerimiento
- Adaptativa Sobre Demanda

3.2.1. No Adaptativa: Un balaceado de carga puede usar unas políticas *No Adaptativas* para el atado de requerimientos y esa política se aplica por toda la vida del cliente. El algoritmo seleccionado puede ser tan simple como el Round-Robin para seleccionar una réplica en donde se procesara el requerimiento.

3.2.2 Adaptativa: Un balanceador de carga puede usar políticas Adaptativas que utilicen información en tiempo de ejecución (replicas disponibles, carga de trabajo en las replicas y requerimientos en espera, etc.) para seleccionar la mejor replica, que posee un requerimiento, o bien, cambiar a otra replica cuando esta proporcione el resultado esperado por el sistema.

3.2.3 No adaptativa Por Sesión: Una manera de diseñar una arquitectura de balanceo de carga es hacer que el balanceador de carga seleccione la réplica destino donde una sesión cliente/servidor quedara establecida, es decir, cuando un cliente obtiene una referencia de objeto a otro objeto (nombre de la réplica) y se conecta a ese objeto. Tal y como se muestra en la Figura N°5.

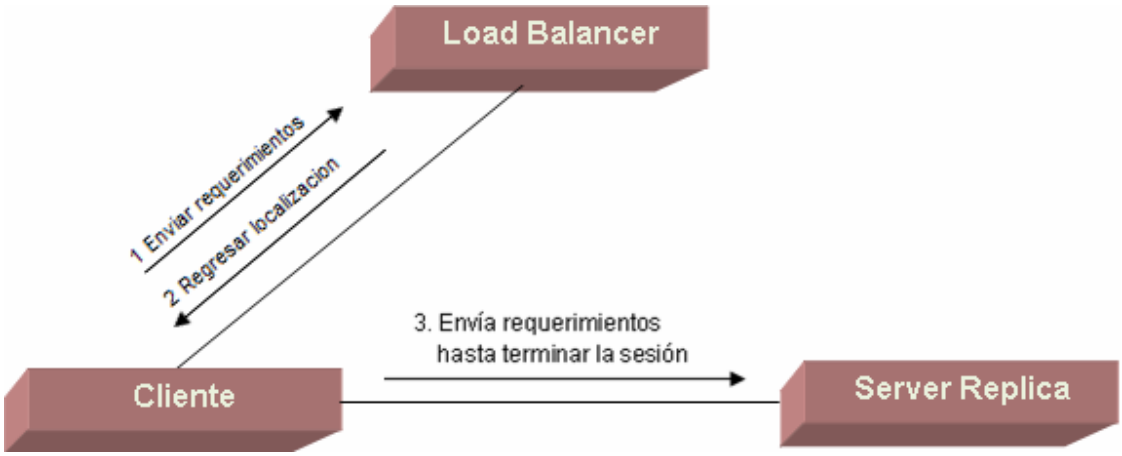


Figura. N°5
. Arquitectura No Adaptativa Por Sesión

Nótese que la política de balanceo en esta arquitectura es *No Adaptativa* ya que el cliente interactúa con el mismo servidor al cual este fue atado originalmente. Esta arquitectura es adecuada para la política de balanceo de carga que implementa algoritmos como el Round-Robin.

3.2.4 No adaptativa Por Requerimiento: Una arquitectura *No Adaptativa* por requerimiento comparte muchas características con la arquitectura No Adaptativa por Sesión. La diferencia es que el cliente es atado a la réplica cada vez que un

requerimiento es invocado. Esta arquitectura tiene la desventaja de degradar el desempeño del sistema debido al incremento de sobrecarga (overead) en la comunicación.

3.2.1 No adaptativa Sobre Demanda: Tiene las mismas características de la arquitectura no Adaptativa *Por Sesión*, Sin embargo, la arquitectura *No adaptativa Sobre Demanda* permite reorganizar los requerimientos del cliente de una manera arbitraria en cualquier tiempo. La información en tiempo de ejecución, como la carga de cada replica, no es usada para decidir cuándo se reorganizan los clientes. En lugar de eso, los clientes se pueden reorganizar en intervalos regulares de tiempo.

3.2.2 Adaptativa por Sesión: Esta arquitectura es similar a la *No Adaptativa Por Sesión*. La primera diferencia es que en la arquitectura Adaptativa Por Sesión puede usar información de la carga en tiempo de ejecución para seleccionar la réplica, por esa razón es menos probable atar un cliente a un servidor con sobre carga. Sin embargo la carga generada por los clientes puede cambiar después de hacer la decisión de atado.

3.2.3 Adaptativa Por Requerimiento: Este diseño introduce un front-end, el cual es un servidor proxy que recibe todos los requerimientos de los clientes. En este caso el servidor “front-end” es el balanceador de carga. El balanceador de carga selecciona una réplica apropiada de acuerdo con las políticas de balanceo de carga y envía el requerimiento a la réplica. El front-end espera la respuesta de las replicas para enviarlas a los clientes.

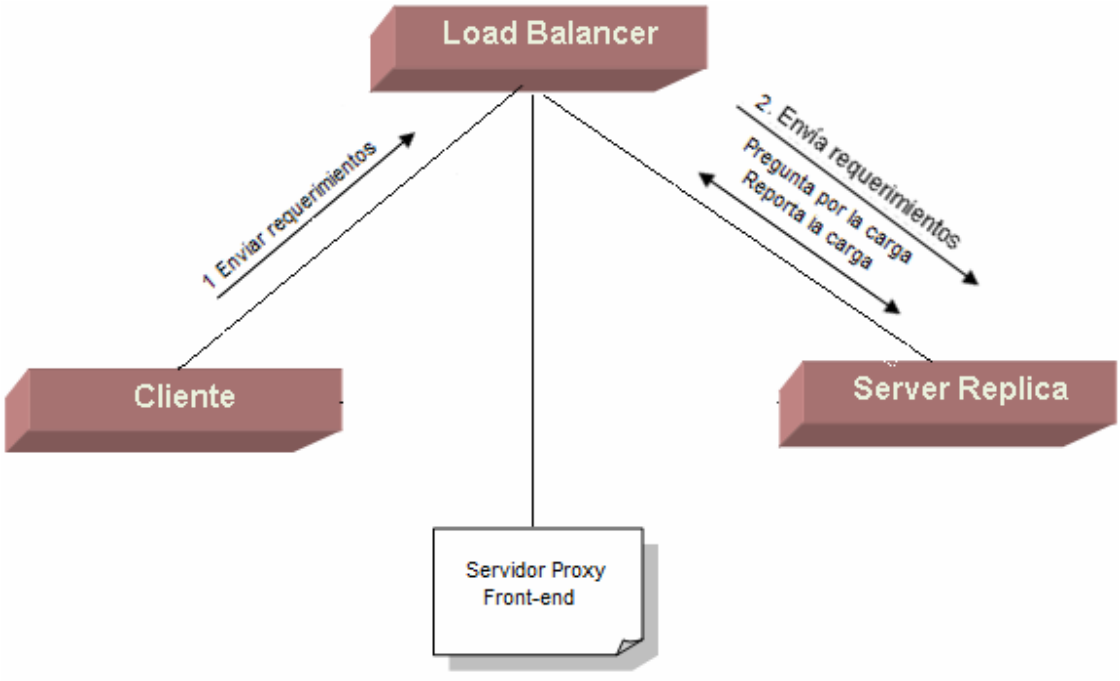


Figura. N°6
. Arquitectura Adaptativa por Requerimiento

3.2.7 Adaptativa Sobre Demanda.: Los clientes reciben un objeto de referencia al balanceador de carga inicial. El balanceador de carga puede redirigir el requerimiento del cliente inicial a la apropiada replica. Los clientes continuaran usando el nuevo objeto de referencia y se comunicaran con las replicas directamente hasta que ellos sean re direccionados otra vez o terminen su sesión.

Después de definir las políticas y estrategias de balanceo de carga, con sus ventajas e inconvenientes, deberían estar soportadas en una arquitectura que idealmente de responder a las siguientes características:

- Trasparencia de servidores
- Balanceo de carga descentralizado
- Conservación del estado de las replicas

- Monitoreo de carga distribuido.
- Activación de replicas Sobre Demanda.
- Balanceo de carga tolerante a fallos
- Soporte a distintos algoritmos de balanceo de carga.

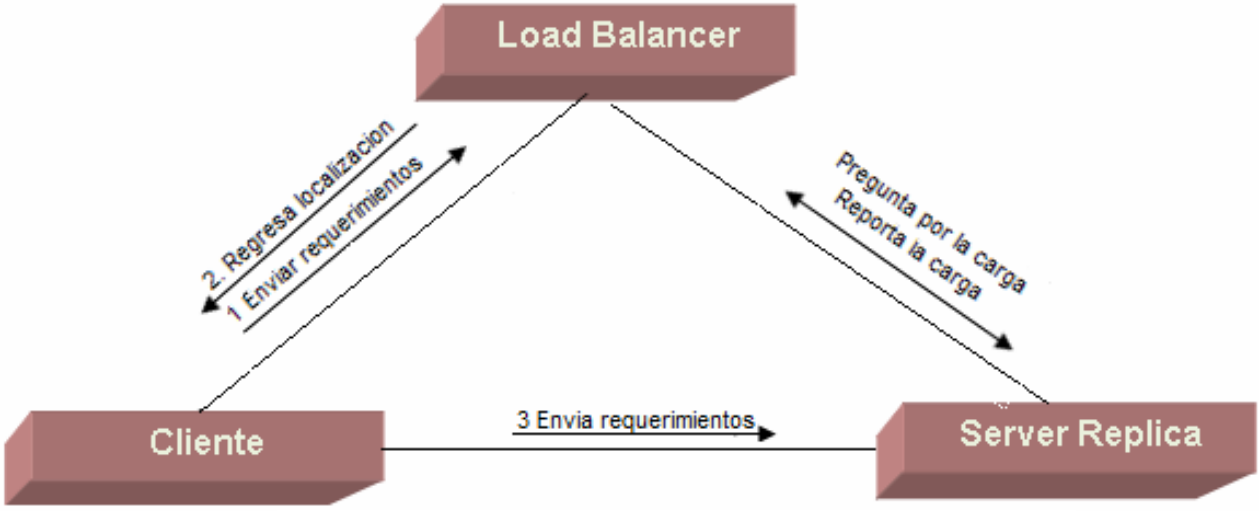


Figura. N°7
. Arquitectura Adaptativa Sobre Demanda

3.3 TÉCNICAS DE BALANCEO DE CARGA ACTUALES

Como habíamos dicho anteriormente, balanceo de carga es la técnica de[8]"distribuir equitativamente el peso del computo entre varios dispositivos. Su objetivo es conseguir que todos los elementos que llevan a cabo la misma tarea, estén igualmente cargados con el fin de aumentar la potencia de cálculo, la disponibilidad y la calidad del servicio".

[8] **Storey, N.** (1996). *Safety-critical Computer Systems.* Massachusetts: Addison-Wesley.

Los elementos que intervienen en el funcionamiento de una red, permiten de alguna manera u otra el balanceo de su carga de trabajo con otros dispositivos semejantes. Las técnicas de balanceo se implementan más que todo en:

- Balance de carga entre servidores
- Balanceo de carga entre Firewall (Cortafuegos)
- Balanceo de carga entre líneas de comunicación
- Balance de carga en el servidor Web

3.3.1 Balance de carga entre servidores: Es un grupo de servidores físicos, en el que cada nodo tiene su propia dirección IP. El servicio que se desea balancear tiene asignada una dirección IP virtual. Uno de los servidores del balanceo actúa como Máster y se encarga de atender las peticiones a la IP virtual y seleccionar el servidor menos cargado para atender la petición. Las formas de selección del servidor menos cargado incluyen carga de CPU, número de conexiones que atiende, selección alternativa, etc.

Para garantizar que el usuario verá sus datos independientemente del servidor que le atienda, existen mecanismos de afinidad que asignan el mismo servidor al mismo usuario entre diferentes conexiones.

3.3.2 Balanceo de Carga entre Firewall: Se utilizan para dar continuidad al servicio de acceso a Internet de la compañía. La tabla de conexiones es compartida entre todos los cortafuegos que atienden selectivamente las conexiones.

3.3.3 Balanceo de Carga entre Líneas de Comunicación: Consiste en agrupar varias líneas de comunicaciones, por ejemplo ADSL, para conseguir una única línea de mayor capacidad. Todas las líneas pueden utilizarse a la vez, la carga es compartida y las conexiones desde el exterior son balanceadas por el dispositivo de balanceo de carga.

3.4 BALANCEO DE CARGA ROUND ROBIN DNS

Round Robin DNS es una técnica de balanceo de carga que se lleva cabo entre distintas maquinas o interfaces de red que funcionan mediante DNS (*Domain Name Server)* de modo que cada vez que se realiza una petición al servidor DNS en cuestión, este contiene varias correspondencias del registro tipo A (host) de manera que va rotando de los resultados que ofrece. Esta técnica suele usarse en grandes redes o redes IRC. Sin embargo, si no se cuenta con grandes redes se posibilita el uso del balanceo de carga sin necesidad de un equipo adicional dedicado a esta tarea.

Round Robin DNS también se usa, generalmente para balancear la carga de servidores Web distribuidos geográficamente, donde cada usuario que accede es enviado a la siguiente dirección IP de manera cíclica. [9]"Round Robin funciona, como se había mencionado anteriormente, **respondiendo a las peticiones DNS** con una lista de direcciones IP en lugar de una sola. El orden con el cual las direcciones IP de la lista son retornadas es la base del Round Robin; actuando en forma de ciclos".

[9] http://bytecoders.homelinux.com/content/balanceo-de-carga-round-robin-dns.html

3.4.1 Desventaja: Hay que tener en cuenta que Round Robin DNS no es la mejor opción para balanceo de carga ya que a pesar de ofrecer un sistema de balanceo sencillo, éste presenta irregularidades e inconsistencia debido a que:

- Nunca repartirá equitativamente las peticiones una vez se extiendan los registros a otros servidores DNS, simplemente alterna el orden de los registro de direcciones cada vez que llega una petición a un DNS.

- No se toma en cuenta el tiempo de transacción, carga del servidor, congestión de la red, etc. Por ello en servidores con recursos homogéneos diríamos que tan solo hace distribución de la carga.

- Otro problema que acarrea es que si una de las direcciones IP a las que se apunta deja de funcionar, no habrá forma de eliminar en un breve periodo las peticiones dirigidas a ella.

A pesar de las desventajas e inconsistencias que la técnica de Round Robin DNS presenta, es de considerar ya que permite trabajar equipos con sistemas operativos heterogéneos como Windows, Linux, Solaris, Unix, etc. para balancear servicios como Web, FTP o correo SMTP entrante y saliente.

3.5 NNETWORK LOAD BALANCING (NLB)

Otra técnica importante es el Network Load Balancing. Se trata de una tecnología de [10]clustering propietaria de Microsoft existente tanto en Windows 2000 como en Windows 2003 Server que crea una red de servidores que mediante distintos mecanismos y algoritmos se intercomunican y deciden quién debe ser el receptor de cada petición. Cuando uno de los servidores deja de funcionar se ejecuta un proceso llamado **failover** quien automáticamente conmuta la carga de trabajo a otro servidor para proporcionar un servicio continuo. También si se produce algún problema en uno de los servidores se detectara y este será retirado automáticamente de la red de servidores en NLB. También es conocido como Network Load Balancing la técnica que usan distintos fabricantes hardware como F5Networks, Radware, NetScaler o Cisco, que mediante dispositivos dedicados (appliances) conocidos como switches L4-L7, dedican uno (varios si están redundados) de estos dispositivos exclusivamente a repartir las peticiones entre los distintos servidores. También suelen integrar en paralelo con el balanceo de carga otras soluciones de seguridad y optimización de los servicios como proxy de SSL.

[11]Esta utilidad (clustering) proporciona un único punto de configuración y administración para los clústeres de NLB permitiendo una mejor gestión en el balanceo de cargar de la red. El Administrador de NLB puede utilizarlo para:

- Crear nuevos clústeres de NLB y propagar automáticamente los parámetros de clúster y las reglas de puerto a todos los hosts del clúster. También propaga los parámetros del host a hosts específicos de un clúster.

[10] Clustering (Agrupamiento): Proceso mediante el cual se unen varios servidores para obtener una mayor tolerancia a fallas o un mayor rendimiento

[11] http://www.microsoft.com/spain/windowsserver2003/evaluation/overview/technologies/clustering.aspx

- Agregar y quitar hosts, a o desde clústeres de NLB.

- Agregar automáticamente direcciones IP de clúster de servidores a TCP/IP.

- Administrar los clústeres existentes conectando con ellos o cargando su información de host a un archivo y guardando esta información para un uso posterior.

- Configurar el NLB para equilibrar la carga de múltiples sitios Web o aplicaciones en el mismo clúster de NLB. Esto incluye agregar todas las direcciones IP de clúster a TCP/IP y controlar el tráfico enviado a aplicaciones específicas en hosts específicos del clúster.

- Diagnóstico de clústeres configurados indebidamente.

Ambas técnicas plantean el problema de que la imposibilidad de dispersar los servidores geográficamente y ser soluciones complejas, en el caso de las soluciones hardware su principal desventaja es el alto precio de este tipo de dispositivos pero a cambio suelen ofrecer pocos problemas de incompatibilidad y un muy buen rendimiento.

En Windows dispone la posibilidad de activar la opción *orden de mascara de red* (subnet mask ordering) en este modo si tuviéramos un mismo registro A (host) que correspondiera a distintas direcciones IP como es el caso de cuando configuramos un Round Robin, en lugar de ir rotando la dirección IP que devuelve en caso de que la IP del peticionario se encuentre en la misma subred que una de las direcciones IP de los resultados siempre devolverá la dirección IP de esa subred. Esto puede ser bastante útil a la hora de ofrecer servicios locales en entornos con

distintas localizaciones. Tanto Round Robin como el orden de mascara de red están habilitadas por defecto, las podemos desactivar en *propiedades avanzadas* del servidor DNS.

Capitulo 4.

NUEVAS TÉCNICAS EN EL MANEJO Y CONTROL DE REDUNDANCIA EN REDES

4.1 INTRODUCCIÓN.

En este capítulo veremos una introducción a las diferentes técnicas que se utilizan actualmente para que los sistemas informáticos estén disponibles y se puedan acceder inclusive cuando alguna parte del funcionamiento del sistema falla.

4.2 CONCEPTO DE REDUNDANCIA.

En muchas empresas es de vital importancia mantener el funcionamiento de sus operaciones. Cuando se cuentan con sistemas críticos en las cuales deben mantener disponibilidad las 24 horas del día los 356 días del año, hay que intentar minimizar los fallos que puedan afectar el funcionamiento normal del sistema.

La redundancia son las diferentes técnicas y configuraciones que ayudan a mantener el funcionamiento de las operaciones con elementos de respaldo en las aéreas más críticas del sistema sin que afecte el funcionamiento del mismo.

Los sistemas informáticos actuales, se encuentran integrados por muchos dispositivos que hacen más susceptibles fallos en el mismo. Cuanto más componentes, mas probabilidad tenemos de que algo falle. Estos problemas pueden ocurrir en el propio servidor, fallos de discos, fuentes de alimentación, tarjetas de red, etc.

Algunas de las técnicas usadas para obtener sistemas redundantes dependen de su importancia y del dinero que perdamos cuando el sistema no está disponible por un fallo.

Es importante tener en cuenta que, no vale la pena invertir en 'redundancia', si la inversión necesaria para tener un sistema redundante cuesta más de lo que perderíamos en dinero, reputación y horas de trabajo, si el sistema fallara.

Actualmente la redundancia se puede aplicar en diferentes técnicas según sean necesarias en la parte que se aplique. Estas son:

- Redundancia en Información
- Redundancia en Tiempo
- Redundancia en Hardware
- Redundancia en Software

En general cualquier tipo de redundancia supone un impacto en el incremento de algunas de las características del sistema donde se deben tener en cuenta para evaluarse.

4.3. REDUNDANCIA EN LA INFORMACIÓN

La redundancia en la información consiste en adicionar información redundante a los datos para permitir el enmascaramiento, detección de posibles fallos que puedan presentarse.

La información es representada mediante un conjunto de reglas bien definidas, entre las cuales, se hace una representación especifica de los errores detectados en códigos generados. Estos a su vez, serán sucesivamente corregidos dichos errores.

4.3.1. Código de Paridad: Es la técnica más sencilla y consiste en añadir 1 bit representando a 1seg en el código original por cada bit de paridad verificando si es par o impar. La distancia de [12]Hamming de este código es 2 ya que permite detectar errores simples. Un ejemplo típico son las memorias de computador en las que antes de escribir un código se anexa y calcula su paridad. Esta se comprueba al leer la memoria.

Estos códigos presentan varios inconvenientes como la imposibilidad de detectar errores en múltiples bits. A pesar de esto, se generaron diversas técnicas para hacerlos como:

[12] Es el número de posiciones en el que difieren dos palabras binarias.

- Paridad Bit-per-Word: Se añade un bit de paridad por palabra. Si fallan todos los bit del bus, puede detectar el error.

- Paridad Bit-per-byte: Se utilizan 2 bits de parida, uno por cada byte de la palabra. Uno de los bit suele detectar la paridad par y otro la impar, cubriendo el caso que de que la palabra completa sea 0 o 1 por error del bus.

- Paridad Bit-per-múltiple chip: En este caso cada paridad se calcula con bits de todos los chips, por ello el fallo de un chip se detectaría al provocar un error simple en todas las paridades. Por el contrario no se puede localizar.

- Paridad bit-per-chip: Cada bit de paridad se asocia con un chip, por lo que no tendríamos el problema del caso anterior. Por otro lado no se detectan los fallos del chip completo.

- Paridad entrelazada: Es una mezcla de los anteriores, pero sin tener en cuenta la estructura interna del chip. Su mayor utilidad se da en la detección de errores en múltiples bits adyacentes.

- Paridad solapada: Los grupos de paridad se forman con dada bit, apareciendo es más de uno de ellos. De esta forma los errores puedes localizarse, además de detectarse. Ese es el concepto básico de alguno de los códigos correctores de Hamming.

4.3.2. Códigos M de N: Consiste en códigos de palabras que tienen n bits de longitud y contienen m 1s. Un error simple supondrá que el código pase a tener m+1 o m-1 1s. El mayor problema de estos es la dificultad para codificar y

decodificar. Una forma sencilla seria los i de 2i códigos, que serian fácilmente codificables mediante una tabla y decodificables despreciándolos.

4.3.3 Códigos Duplicados: Se basan en una duplicación total y completa de la información original para la formación del código. Es bastante simple pero esencialmente redundante. Una variante de este es la duplicación complementada, de gran ventaja cuando la información original y la información duplicada se procesas o fluyen por el mismo medio.

4.3.4. Códigos Aritméticos: Estos códigos son útiles para chequear operaciones aritméticas. El dato se codifica antes de realizar la operación y se chequea después de esta. Un código aritmético debe ser invariante a un conjunto de operaciones aritméticas.

- **Códigos AN:** Se forman multiplicando cada palabra N por una constante A. Es invariante a suma y resta no a multiplicación y división. La constante A determina tanto los bits adicionales como la capacidad de detección de errores siendo su selección un punto crítico en la eficiencia del código.

- **Código Residuo:** Un residuo es el resto generado al dividir un numero N por un entero m. Se trata de añadir este resto a numero original al codificarlo y quitarlo al decodificador. Del entero m o módulo dependen los bits adicionales. Existen versiones de este código en las que se añade el inverso del residuo m-r.

4.3.5. Código Berger: Es un código separable que se crea añadiendo unos bits de chequeo basados en el numero de 1s del dato original. Primero se calcula el número de 1s del dato, se complementa este y se añade al dato. Cuando el número de bits del dato original crece, su porcentaje de redundancia es bastante aceptable.

4.3.6. Código de Hamming: En código de Hamming se forma partiendo de los bits de información en grupos de paridad y especificando la paridad para cada uno de estos grupos. Los bits erróneos se detectan solapando los grupos de bits. La ventaja de los códigos de Hamming es su bajo coste, debido a su baja redundancia, así como su eficacia y rapidez en la corrección. Por ello es muy utilizado en memorias convencionales.

Para elegir un código se deben tener en cuenta ciertas características. Las más importantes a la hora de elegir el código a utilizar son:

- Cantidad de redundancia que introduce
- Facilidad y rapidez para codificar y decodificar
- Efectividad de la detección/corrección.

Los requerimientos que se le suelen pedir son:

- Separabilidad
- Detección /corrección o ambas.
- Cuantos errores han de corregirse.

4.4. REDUNDANCIA EN EL TIEMPO

La redundancia en el tiempo es la repetición de computación de forma que permitan la detección de fallos Debido al alto coste de para la implementación de redundancia en las técnicas mocionadas con anterioridad, surgieron técnicas que sacrificaban tiempo de procesamiento a cambio de una reducción en el hardware adicional. Entre las técnicas que se utilizan actualmente, se encuentran los llamados Detectores de Fallos Transitorios y los Detectores de Fallos Permanentes.

- **Detección de fallos Transitorios:** Solo se pueden basar en el hecho de que si se produce una situación errónea y esta no desaparece pasado un tiempo se podrá catalogar como permanente. Un problema añadido es la integridad de los datos, ya que después de la primera computación se puedes corromper y no ser protegidos.

- **Detección de fallos permanentes:** Durante una primera computación o transmisión los operandos se y usan los resultados se guardan en un registro. Antes de efectuar la segunda computación o trasmisión, los operandos se codifican con una función e. Después de que las operaciones se realizan, se codifican los resultados y se comparan con los de la primera computación. La función e debe permitir la detección de errores hardware.

4.5 REDUNDANCIA EN EL HARDWARE.

La replicación a nivel de hardware y todos las técnicas de redundancia especificas que ésta maneja, es quizás la técnica más utilizada debido al bajo precio de los componentes hardware hoy día. Usualmente se presentan tres técnicas que derivan el método de uso de las técnicas actuales. Estas son: *Pasiva, Activa e Hibrida.*

- **Pasiva:** Usa el concepto de enmascaramiento para evitar que el fallo llegue a producir un error.

- **Activa:** Detecta la presencia del fallo y realiza acciones para eliminarlo.

- **Hibrida:** Se realiza por un lado de la redundancia pasiva para prevenir resultados erróneos, y por otro lado la detección, localización y reconfiguración de los fallos, con elementos añadidos al sistema.

4.5.1. Redundancia de Hardware Pasiva (Técnicas)

Redundancia modular triple (TMR): Esta técnica se basa en triplicar el hardware y utilizar el esquema *majority voting* (salida mayoritaria) para determinar la salida del sistema. Por tanto al parecer un fallo puede enmascararse si los correctos son mayoría. Se aplica en procesadores, memorias etc. El problema que se puede presentar en esta técnica es que un fallo en el módulo de decisión (voter) es crítico para este. A estos componentes se les llama puntos simples de avería. Para

resolver el problema se pueden triplicar los módulos de decisión empleados. Si un modulo de decisión (voter) falla, este ya no sería un punto simple de avería.
Técnica de decisión (volting techniques): La implementación de los dispositivos de decisión hardware (voters) suele ser sencilla. En muchas aplicaciones el tiempo es un parámetro crítico, por lo que los circuitos se muestran poco fiables. Los valores de los sensores se muestrean y acumulan en tres memorias de dos puertos. Estas se pueden implementar con los buses multiplexados entre dos usuarios. Cada procesador puede consultar las memorias para obtener el valor de los sensores. Cada procesador ejecuta su algoritmo para decidir y deja los resultados en otras memorias de dos puertos.

La implementación de técnicas hardware frente a la de software, seria la rapidez, mientras la desventaja radicaría en la potencia consumida, peso y tamaño de la implementación hardware, así como su difícil reconfiguración.

4.5.2 Redundancia de Hardware Activa: Estas técnicas intentan corregir la tolerancia a fallos mediante la detección, localización y recuperación del fallo. En cambio no se enmascaran los fallos, por lo que estas técnicas se aplican a sistemas que pueden tolerar resultado erróneo temporalmente.

- **Duplicación con comparación:** Estos sistemas solo detectan la presencia de fallos, no los corrigen. Debido a esto, se presentan diversos problemas tales como: si la entrada a los módulos se produce un error este no se detecta, el comparador puede no funcionar bien en determinadas aplicaciones. Y si se presenta un fallo en el comparador, ofrecerá resultados erróneos.

- **Preparado para sustituir:** El sistema detecta, localiza y sustituye módulos que aporten resultados erróneos. Un factor importante es la reconfiguración. Existen versiones en las que los sustitutos están

sincronizados con el modulo activo, entrando a funcionar inmediatamente. Si por el contrario los sustitutos no están conectados, el proceso de sustitución es lento y existen un lapsus hasta que entra el repuesto. Esta última técnica es lenta pero ahorra energía por lo que está indicada en sistemas tipo satélite, en los que el consumo es crítico.

- **Temporizadores de Guarda:** El temporizador de guarda es un dispositivo que debe inicializarse por el sistema de forma iterativa. Un daño en el sistema no permitiría realizar esta inicialización y significaría la existencia de un error.

4.5.3. Redundancia Hibrida: Esta técnica intenta aprovechar los beneficios de los enfoques activo y pasivo. Suelen ser muy caras y se restringen a sistemas con necesidad de alta fiabilidad. Esta técnica se subdivide en 2 partes:

- **Redundancia N-modular con sustituto:** Contiene un detector de desacuerdo que determina el fallo de una unidad, momento en el que un sustituto pasaría a funcionar en lugar del modelo erróneo.

- **Redundancia ato-purgante:** Se diferencia de la anterior en que todas las unidades participar activamente, mientras que en la anterior solo lo hacía en caso de sustitución por fallo.
  En este sistema se elemininan los módulos no concordantes con la salida del sistema. Los tres aspectos a considerar son: N módulos, idénticos capaces realizar las funciones del sistema, de quitar su modulo asociado del sistema si se determina que ha fallado y un sistema decisor (voter) que enmascara los fallo.

4.6. REDUNDANCIA DE COMPONENTES EN EL SERVIDOR.

No necesariamente se requiere la implementación de redundancia en todo un dispositivo completo. En ciertos casos, es importante la aplicación de esta técnica en los elementos esenciales que componen el dispositivo mismo. En la mayoría de los casos el dispositivo más importante que compone un sistema de red, es el servidor de información.

Los componentes redundantes más normales en un servidor suelen ser, los discos, las tarjetas de red y las fuentes de alimentación. Existen servidores con múltiples CPUs que incluso siguen trabajando sin problemas con alguna CPU o modulo de memoria estropeado.

4.6.1. Redundancia en Discos: Los discos son los sistemas de almacenamiento que hacen parte de un servidor y este a su vez de un sistema de red. [13]El fallo más común en un servidor es el fallo de un disco duro. Si el servidor tiene solamente un disco y éste falla, fallara el servidor completo y no podremos acceder a los datos contenidos en el mismo.

Por esta razón existen técnicas que nos ayudan a reducir las fallas que se puedan presentar y por consiguiente a que el servidor siga en funcionamiento y no se pierda datos incluso cuando falle algún disco duro.

Lo más normal y comúnmente se utiliza, es que se puedan sustituir los discos que fallan sin necesidad de apagar el servidor mismo. Esta técnica se conoce como HotSwap.

13

Sin embargo, la técnica que más aceptación tiene en su implementación es la llamada RAID (Redundant Array of Independent Disks). Con esta técnica creamos un conjunto de discos redundantes que nos pueden ayudar, tanto a aumentar la velocidad y el rendimiento del sistema de almacenamiento, como a que el sistema siga funcionando aunque algún disco falle. Existen implementaciones por software y hardware y diferentes configuraciones RAID, siendo las más comunes RAID0, RAID1, RAID5 y RAID10.

4.6.1.1 Red Redundant Array of Independent Disks nivel 0 (RAID0): Este es un nivel RAID0 llamado entrelazado de datos. Es un nivel que en la actualidad se encuentra en desuso debido al bajo grado de seguridad que le brinda a la red, esto se debe a que el raid0 no maneja redundancia de datos, por lo que no protege a la red contra la pérdida de datos. A pesar de esta desventaja, este nivel puede mejorar considerablemente el rendimiento porque puede acceder a varias unidades simultáneamente, lo que reduce el tiempo de búsqueda global en archivos grandes. El diseño simple de RAID 0 es fácil de implementar, aunque no se debe utilizar para aplicaciones empresariales críticas.

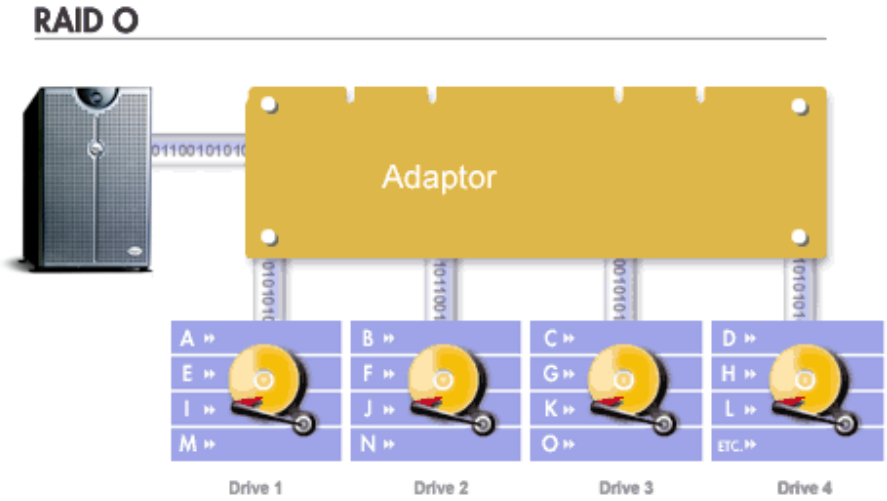


Figura N°8
Red Redundant Array of Independent Disks nivel 1

4.6.1.2 Red Redundant Array of Independent Disks nivel 1 (RAID1): Este nivel es también llamada duplicación de disco o unidades, porque con este nivel se pude hacer una copia exacta de los datos en un segundo disco o unidad de forma simultánea, de esta manera habrá más rendimiento en la red y los datos van a estar más protegidos por esta duplicación. El RAID 1 consiste en dos discos espejo, lo que incrementa la fiabilidad respecto a un solo disco (ver Figura N 9). Dado que los datos están en dos o más discos, con hardware usualmente independientes el uno del otro, el rendimiento se incrementara según el número de copias, es decir, un RAID 1 puede estar leyendo varios datos simultáneamente en discos diferentes por lo que su rendimiento se multiplica. Dentro de esta técnica, se utiliza un método para mejorar su rendimiento, el cual consiste en emplear controladores de discos independientes, una para cada disco (*splitting* o *duplexing).*

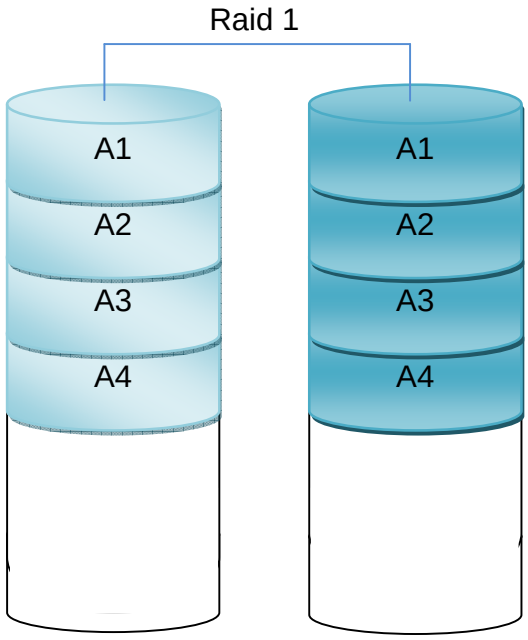


Figura N°9
Red Redundant Array of Independent Disks nivel 2

Adicionalmente, el RAID 1 puede marcar discos como reversa. Pueden ejecutarse en modo *Hot* si desea que se encuentren en funcionamiento o *standby hot spare,* si queremos que se encuentre en modo de espera. En el preciso momento en el que ocurra un fallo en alguno de los discos espejo, los discos de reserva entran a formar parte de los discos espejo, duplicándose la información en él. La desventaja de RAID 1 es su sobrecarga total del disco, lo que provoca un uso ineficaz de la capacidad del mismo.

4.6.1.3 Red Redundant Array of Independent Disks nivel 5 (RAID5): Este es el tipo de RAID más común. RAID5 usa una división de datos a nivel de bloques, de tal forma que distribuye la información de paridad entre los discos que conforman dicho bloque. Su funcionamiento consiste en que, si se ejecuta una petición de lectura del bloque A1 seria servida por el disco 1. Si simultáneamente se ejecuta una petición en el bloque B1, tendría que esperar, pero caso contrario ocurre si luego de estas dos peticiones se realiza una petición de lectura B2, podría atenderse concurrentemente. Cada vez, que en el RAID5, se escribe un bloque de datos, se genera [14]stripe. Si otro bloque, o alguna porción de un bloque, es escrita en esa misma división, el bloque de paridad completo o una porción de él, es recalculada y vuelta a escribir. Sin embargo, los bloques de paridad se leen solo cuando la lectura de un sector de datos provoca un error de Control de Redundancia Cíclica (CRC). En este caso, el sector de datos restantes del bloque en la división así como también dentro de la paridad se utilizan para reconstruir el sector dañado. De esta manera el CRC es ocultado al sistema.

Al distribuir la paridad entre los discos miembro, el nivel 5 elimina el cuello de botella de la escritura del nivel 4. El único cuello de botella sería el proceso para

[14] Un bloque de paridad dentro de la misma división.

calcular la paridad. Con los software RAID y las CPUs modernas no hay problemas. Como con el nivel 4, el resultado es un rendimiento asimétrico haciendo que el de la lectura sea menor del de la escritura. El nivel 5 normalmente se usa para el caché de la escritura en retroceso para reducir la asimetría (Ver Figura N 10). La capacidad de almacenamiento del nivel 5 del hardware RAID es igual a la capacidad de los discos miembro menos la capacidad de cada disco miembro. La capacidad del nivel 5 del software RAID es igual a la capacidad de las particiones miembro menos el tamaño de cada una de las particiones si tienen el mismo tamaño. Para la implementación del RAID5 se necesitan como minino 3 unidades.

[15]"RAID 5 es la solución más económica por megabyte, que ofrece la mejor relación de precio, rendimiento y disponibilidad para la mayoría de los servidores."

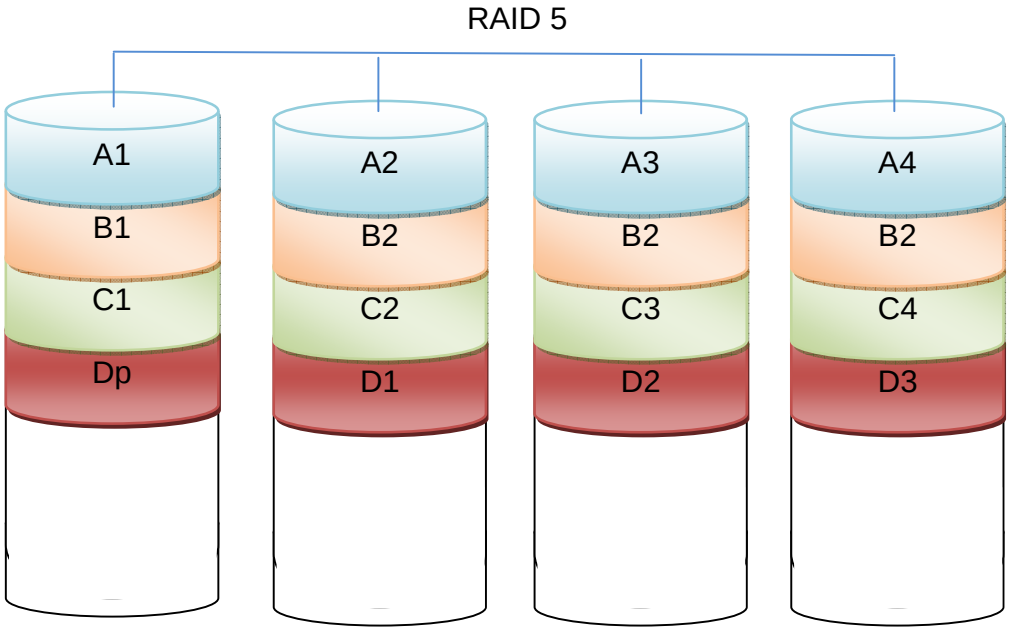


Figura N°10
Red Redundant Array of Independent Disk nivel 5

Las implementaciones RAID 5 presentan un rendimiento malo cuando se someten a cargas de trabajo que incluyen muchas escrituras más pequeñas que el tamaño

[15] Tomado de

de una división (*stripe*). Esto se debe a que la paridad debe ser actualizada para cada escritura, lo que exige realizar secuencias de lectura, modificación y escritura tanto para el bloque de datos como para el de paridad. Implementaciones más complejas incluyen a menudo cachés de escritura no volátiles para reducir este problema de rendimiento.

4.6.1.4. Red Redundant Array of Independent Disks nivel 10 (RAID10): Están bien llamado a veces RAID 1+0, y aunque es parecido a un RAID 0+1 difiere en que los niveles de los RAID que la forman se invierte. RAID10 consiste más que todo en una división de espejos. En el caso de un RAID10 si un disco que falla no se reemplaza entonces un solo error de medio irrecuperable que ocurra en el disco "espejado" resultara una pérdida de datos. Muchos entornos empresariales están empezando a evaluar entornos RAID más tolerantes a fallos. El RAID10 es a menudo la mejor elección para bases de datos de altas prestaciones, debido a que la ausencia de cálculos de paridad proporciona mayor velocidad de escritura. En la siguiente figura, se encuentra una representación de los bloques que conforman el RAID10.

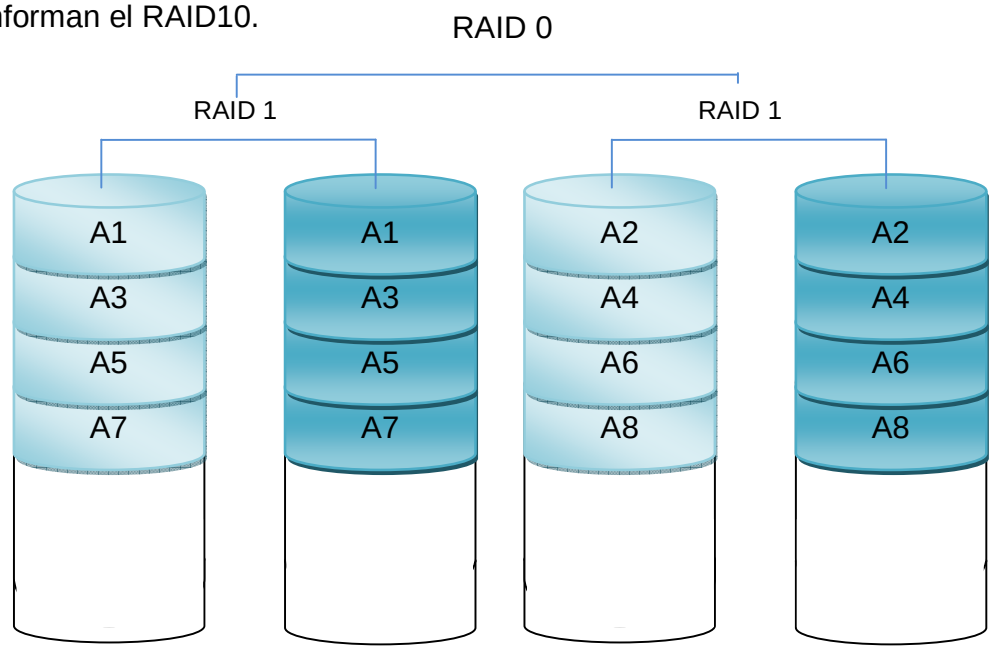


Figura N °11
Red Redundant Array of Independent Disk nivel 5

Aun así, siendo los RAID, métodos para el manejo de redundancia en el Disco de los servidores estos no presentan diferentes inconsistencias o limitaciones.
RAID no impedirá que un virus destruya los datos, así como también modificaciones o borrado total de los mismos por equivocación del usuario.
El RAID, como se ha recalcado en los diferentes métodos de Redundancia en disco, no mejora el rendimiento de las aplicaciones como en las configuraciones típicas del escritorio. Otro aspecto a tener en cuenta es su escalabilidad, es decir, RAID [16]"no facilita el traslado de un sistema nuevo, la BIOS RAID debe ser capaz de leer los metadatos de los miembros del conjunto para reconocerlo adecuadamente y hacerlo disponible al sistema operativo. Dado que los distintos fabricantes de controladoras RAID usan diferentes formatos de metadatos (incluso controladoras de un mismo fabricante son incompatibles si corresponden a series diferentes) es virtualmente imposible mover un conjunto RAID a una controladora diferente, por lo que suele ser necesario mover también la controladora. Esto resulta imposible en aquellos sistemas donde está integrada en la placa base."

4.6.2 Tarjeta de red: La tarjeta de red es el dispositivo que permite al servidor comunicarse con el resto del mundo. Es por ello muy común que los servidores tengan como mínimo 2 tarjetas de red, para garantizar que esta comunicación no se corte en caso de fallo de una de las tarjetas.

En Linux existe además una técnica llamada Bonding, por la cual podemos utilizar 2 o más tarjetas de red como si fueran un único dispositivo, sumando las capacidades de las mismas y teniendo redundancia en el caso que alguna de las tarjetas falle.

[16] **Hegering, H.G.** . *Administración Integrada de Redes Computacionales.* San Francisco: Morgan Kaufmann.

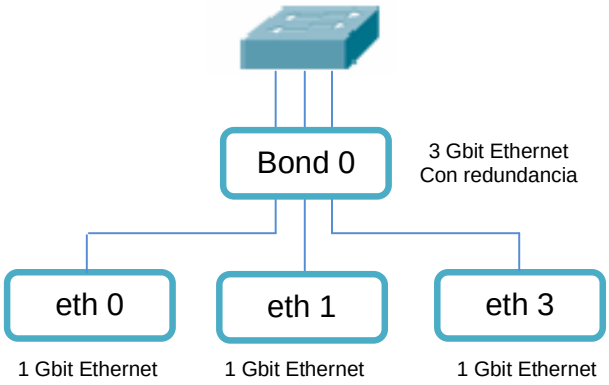


Figura N
Redundancia en Tarjetas de red.

4.6.3 Fuentes de alimentación: La fuente de alimentación es la encargada de proporcionar electricidad al servidor. También es común que los servidores tengan 2 o más fuentes de alimentación conectadas a diferentes sistemas eléctricos, para garantizar el suministro en el caso que una de las fuentes o uno de los sistemas eléctricos fallen. Lo más normal es que se puedan sustituir las fuentes de alimentación que fallan sin necesidad de apagar el servidor (HotSwap).

Otros componentes del sistema como Reuters, Switches, gabinetes de discos, etc. suelen utilizar la misma técnica de redundancia.

4.7 REDUNDANCIA EN EL SUMINISTRO ELÉCTRICO

Siendo el servidor un elemento en el cual necesita un suministro eléctrico constante para su funcionamiento, si éste fallase, aunque fuera por cortos

periodos de tiempo, tendría consecuencias catastróficas para el sistema de red al cual pertenece. No solamente sería necesario un suministro eléctrico constante, también sería indispensable que el flujo de este sea paralelo y no tenga subidas y bajadas bruscas que puedan estropear y/o corromper los componentes electrónicos deteriorando su correcto funcionamiento.

Para conseguir esto se pueden utilizar diferentes componentes según el grado de protección que deseemos.

- **SAI (UPS)**: Son baterías más o menos avanzadas que se conectan entre el servidor y la fuente de suministro eléctrico. Garantizan un suministro constante y estable por un tiempo, dependiendo este de la capacidad de las mismas.

- **Generadores eléctricos**: Funcionan generalmente con diesel y se conectan entre los UPS y la red de suministro eléctrico. Solo entran en funcionamiento cuando el suministro se corta por más de un determinado tiempo. Pueden suministrar electricidad por un tiempo indefinido siempre que tengan carburante en el tanque.

- **Líneas independientes de suministros**: En centros de datos grandes, se suelen tener al menos 2 conexiones diferentes e independientes a la red de suministro eléctrico.

En la siguiente Figura N° se representa la disposición e interacción de los elementos que permiten la redundancia en el suministro eléctrico.

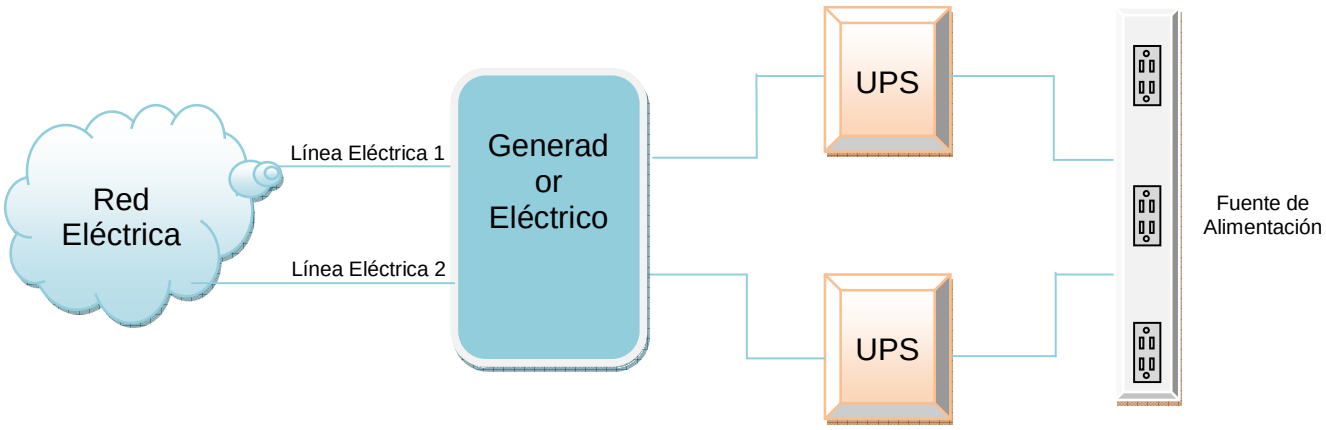


Figura N°13
Redundancia en el Sistema Eléctrico

Cabe anotar que no necesariamente la redundancia deba ser exclusiva, es decir, al componente más importante de la red (servidor). Se puede crear un sistema de redundancia en el suministro eléctrico a nivel general, de manera que hasta el componente menos importante de la cual necesita energía, tenga también la posibilidad de mantener su funcionamiento ante un fallo en el suministro eléctrico. El sistema será tan seguro, estable y redundante como el componente más débil del mismo.

4.4 REDUNDANCIA EN COMPONENTES DE RED

De nada sirve tener servidores con componentes duplicados y redundantes y un suministro eléctrico constante y equilibrado si algunos de los componentes de la red fallan y no podemos acceder al servidor.

Los componentes más normales en una red son:

- **Routers (enrutador)**: Es un dispositivo que interconecta segmentos de red o redes enteras

- **Switch (Conmutador)**: Es un dispositivo que interconecta dos o más segmentos de red

- **Tarjeta de Red o NIC**: Es un dispositivo electrónico que permite a una DTE (Data Terminal Equipment), ordenador o impresora, acceder a una red y compartir recursos

- **Cables de red**: Para interconectar los diferentes componentes, existen muchos y variados tipos, siendo los más comunes el cable de par trenzado y el de fibra óptica.

- **Líneas de conexión**: a la red de área amplia, WAN (por ejemplo Internet).

Cualquiera de estos componentes puede fallar, dejando al sistema incomunicado. Pero existen técnicas para evitar que esto ocurra, lo que se suele hacer es configurar la red, para que al menos existan 2 caminos diferentes entre dos componentes A y B.

En el grafico siguiente se puede ver como configurar una red con redundancia doble desde el servidor hasta Internet. De esta manera se puede estropear un router, un Switche y una tarjeta de red a la vez sin que perdamos conectividad. El

mismo esquema se podría ampliar para tener redundancia triple o cuádruple de los componentes.

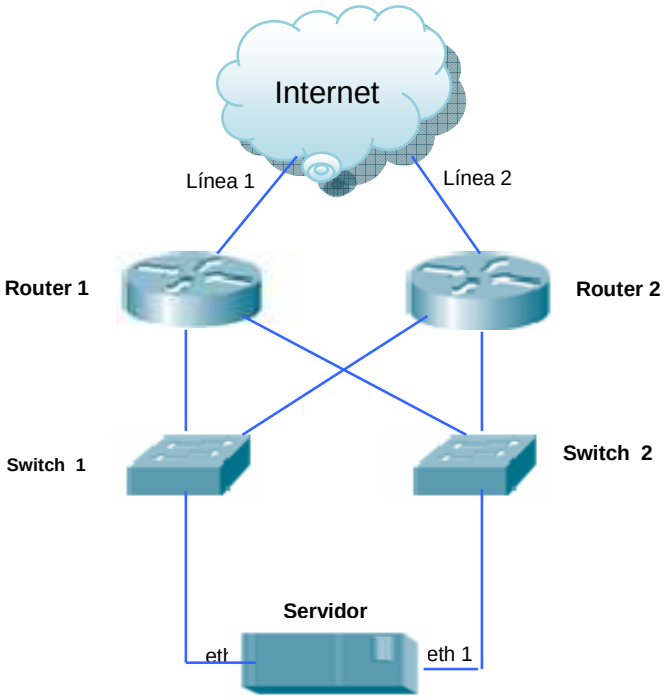


Figura N°14
Redundancia en algunos componentes de la red

CONCLUSIÓN

La presente monografía se enmarca dentro de los ámbitos de las técnicas para administrar y gestionar redes, que son herramientas que permiten tener un manejo de la red de forma más útil debido a que con ellas el administrador de la red puede organizar, supervisar y controlar cada uno de los elementos de comunicación que conforman la red garantizando un nivel de servicio optimo a unos costos razonables, De acuerdo a lo anterior, existen ciertas técnicas de la administración de las redes, en las cuales se destacan; el Trunking o enlaces agregados, el encolado, el balanceo de carga y la redundancia de caminos, cada una de estas técnicas presentan sus propias funciones.

A través de esta monografía se pudo entender y llegar a la conclusión que el encolado es un técnica de administración que permite priorizar el flujo de tráfico en la red y que a través de ciertos protocolos esto se hace más fácil y más sencillo de entender, la técnica de ***Trunking,*** *e*s una técnica que tiene como función principal conectar elementos de la red para mejorar la comunicación entre ellas. Anteriormente esta técnica de administración de redes presentaba algunos obstáculos que hacían difícil la gestión de ella como era la incompatibilidad de equipos o componentes, pero actualmente, esta técnica del Trunking permite la heterogeneidad de las redes, es decir, la red puede estar integrada por

dispositivos hardware y fabricados por diferentes compañías, otro obstáculo que esta técnica presentaba era que no permitía que en un enlace trunking existiera combinaciones de velocidades, gracias a la evolución que esta a tenido, hoy podemos encontrar trunking con enlaces de 10/100/1000 Mbps. Esta técnica del trunking esta muy ligada al ***Balanceo de cargas,*** técnica que se encarga de equilibrar el trabajo de la red entre ya sea varios procesos, dispositivos o recursos. A través de esta técnica lo que se evita es que existan en la red los llamados "**cuellos de botella**" por la sobrecarga de información o de usuarios.

Hoy por hoy muchos fabricantes han optado por implementar esta técnica en sus dispositivos por los beneficios que esta lleva consigo, como es el de garantizar el rendimiento de la red. Por último para lograr que la red siempre este en pleno funcionamiento en todo tiempo, los administradores de red pueden utilizar una técnica llamada ***Redundancia de caminos,*** la cual garantiza uno de los tres pilares de la red: la ***Disponibilidad***.

En conclusión, estas técnicas que actualmente se encuentran en fuerte uso, son técnicas que lo que buscas es mejorar el ancho de banda de la red, para que de este modo hacer un buen uso de los recursos con que cuenta la organización o entidad y aumentar el rendimiento de la red.

GLOSARIO

- **Administración de la red**: Término genérico que se usa para describir sistemas o acciones que ayudan a mantener, describir o solucionar los problemas de una red.

- **ADSL:** Asymmetric Digital Subscriber Line – Linea de Abonado Digital Asimétrica. Consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado. Esta es una tecnología de acceso a Internet de banda ancha, lo que implica capacidad de para transmitir más datos, lo que a su vez se traduce en mayor velocidad.

- **Algoritmo** En networking, los algoritmos se utilizan normalmente para determinar la mejor ruta para el tráfico desde un origen en particular hasta un destino en particular.

- **Ancho de banda**: Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. También se utiliza este término para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

- **Backbone**: Parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de, y se destina a, otras redes.
- **Balanceo de cargas:** Es la técnica de la administración de red que se encarga de equilibrar el trabajo de la red entre ya sea varios procesos, dispositivos o recursos. A través de esta técnica lo que se evita es que existan en la red los llamados "**cuellos de botella**" por la sobrecarga de información o de usuarios. Hoy por hoy muchos fabricantes han optado por implementar esta técnica en sus dispositivos por los beneficios que esta lleva consigo, como es el de garantizar el rendimiento de la red.

- **Clustering:** Es el proceso de dividir un conjunto de datos en grupos mutuamente excluyentes de tal manera que cada miembro de un grupo esté lo "más cercano" posible a otro, y grupos diferentes estén lo "más lejos" posible uno del otro, donde la distancia está medida con respecto a todas las variables disponibles.

- **Cola**: En general, una lista ordenada de elementos a la espera de ser procesados.// En enrutamientos, una reserva de paquetes que esperan ser enviados por una interfaz de router.

- **Cola de prioridad**: Función de enrutamiento en la cual se da prioridad a las tramas de una cola de salida de interfaz según diversas características, por ejemplo, tamaño de paquete y tipo de interfaz.

- **Colisión**: En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de los dos dispositivos chocan y se dañan cuando se encuentran en los medios físicos.

- **Confiabilidad**: Relación entre la cantidad de señales de supervivencia (keepalives) esperada y la recibida de un enlace. Si el porcentaje es alto, la línea es confiable. Se utiliza como una métrica de enrutamiento.

- **Congestión**: Tráfico que supera la capacidad de la red.

- **CRC** : Técnica de verificación de errores en la cual el receptor de la trama calcula un residuo dividiendo el contenido de la trama por un divisor binario primo y compara el residuo calculado con el valor almacenado en la trama por el nodo emisor.

- **DNS** : Sistema de denominación de dominio. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones. Ver también *zona de autoridad*.

- **Encapsulado**: Es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulado consiste pues en ocultar los detalles de implementación de un objeto, pero a la vez se provee una interfaz pública por medio de sus operaciones permitidas. Considerando lo anterior también se define el encapsulado como la propiedad de los objetos de permitir el acceso a su estado únicamente a través de su interfaz o de relaciones preestablecidas con otros objetos.

- **Estándar**: Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

- **FDDI**: Interfaz de datos distribuida por fibra**.** Estándar LAN definido por ANSI X3T9.5, que especifica una red de transmisión de tokens de 100 Mbps con

cableado de fibra óptica y distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble para proporcionar redundancia. Comparar con *CDDI* y *FDDI II*.

- **Flujo** : Corriente de datos que viaja entre dos puntos finales a través de una red (por ejemplo, de una estación LAN a otra). Varios flujos se pueden transmitir a través de un mismo circuito. // En encolamiento se dice que es el tráfico con iguales direcciones IP fuente/destino y puerto fuente/destino.

- **Front-end**: Nodo o programa de software que solicita los servicios de un Back end.

- **FTP** : Protocolo de aplicación, parte de la pila de protocolo TCP/IP utilizado para la transferencia de archivos entre nodos de red. El FTP se define en RFC 959.

- **Full dúplex** : Capacidad de transmisión de datos simultánea entre la estación emisora y la estación receptora.

- **Jitter**: Variación del tiempo de respuesta (delay),

- **IEEE : Instituto de Ingeniería Eléctrica y Electrónica**. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares que predominan en las LAN de la actualidad.

- **Jitter:** Los Jitter son irregularidades de transmisión de tráfico de voz, que se escuchan en medio de la conversación producto de las variaciones en el retardo

- **Latencia:** Es el retardo que se produce entre el tiempo en que una trama comienza a dejar el dispositivo origen y el tiempo en que la primera parte de la trama llega a su destino.

- **MAC**: **Control de acceso al medio**. Capa inferior de las dos subcapas de la capa de enlace de datos, según la define el IEEE. La subcapa MAC maneja el acceso a los medios compartidos.

- **Multiplexión :**Esquema que permite que múltiples señales lógicas se transmitan de forma simultánea a través de un canal físico exclusivo.

- **Nodo:** Cualquier estación de trabajo, Terminal, ordenador personal, impresora o cualquier otro dispositivo conectado a la Internet.

- **Paquete:** Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. El término "paquete" se usa con mayor frecuencia para referirse a las unidades de datos de la capa de red. Los términos *datagrama*, *trama*, *mensaje* y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

- **Protocolo** : Descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información.

- **Proxy:** Entidad que, para aumentar la eficiencia, esencialmente reemplaza a otra entidad// El término **proxy** hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del **servidor proxy**, que sirve para permitir el acceso a Internet a todos los

equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

- **QOS**: Calidad de servicio. Medida de desempeño para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

- **RAID (Matriz redundante de discos Independientes):** conjunto redundante de discos independientes') hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos.

- **Redundancia**: En internetworking, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla.

- **Redundancia:** En internetworking, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla. // Con esta técnica lo que se busca es lograr que la red siempre este en pleno funcionamiento en todo tiempo, es decir que con esta técnica se garantiza uno de los tres pilares de la red: la *Disponibilidad*.

- **Sistema redundante**: Computador, router, switch u otro computador que contiene dos o más de cada uno de los subsistemas más importantes por ejemplo, dos unidades de disco duro, dos CPU o dos líneas de alimentación. Por ejemplo, en un switch ATM LightStream 2020 totalmente redundante, hay

dos tarjetas NP con discos, dos tarjetas de switch y dos sistemas de suministro de alimentación. Un switch LightStream 2020 parcialmente redundante puede tener dos tarjetas NP, una tarjeta de switch y un sistema de suministro de alimentación.

- **SMTP** : Protocolo de transferencia de correo simple. Protocolo Internet que suministra servicios de correo electrónico.

- **STP**: Protocolo de puente que usa el algoritmo de spanning tree (árbol de extensión) y permite que un puente con aprendizaje evite los bucles de forma dinámica en una topología de red con conmutación, creando un árbol de extensión. Los puentes intercambian mensajes BPDU con otros puentes para detectar bucles y luego eliminarlos al desactivar las interfaces de puente seleccionadas. Se refiere al estándar IEEE 802.1 de Protocolo de spanning tree y al Protocolo de spanning tree más antiguo, de Digital Equipment Corporación, en el cual se basa. La versión de IEEE soporta dominios de puente y permite que el puente desarrolle una topología sin bucles a través de una LAN extendida. Generalmente, se prefiere la versión de IEEE en lugar de la versión de Digital. A veces abreviado *STP*

- **SSL**: Es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos **HTTP**, **FTP**, **SMTP**, entre otros.

- **TCP/IP:** So dos protocolos de comunicación de datos: El protocolo TCP(Protocolo de control de transmisión) que se establece a nivel de transporte del modelo OSI y el protocolo IP (Internet Protocolo), que pertenece a nivel de red. Cuando se utiliza el protocolo TCP/IP se hace referencia a una familia muy amplia de protocolos presentada por ambos. Estos protocolos son los que utiliza Internet para la interconexión de nodos.

- **Throuput**: Corresponde a la velocidad de un enlace agregado dada por la suma de ancho de banda de cada uno de los enlaces físicos

- **Trunking**: Es una técnica que tiene como función principal conectar elementos de la red para mejorar la comunicación entre ellas. Anteriormente esta técnica de administración de redes presentaba algunos obstáculos que hacían difícil la gestión de ella como era la incompatibilidad de equipos o componentes, pero actualmente, esta técnica del Trunking permite la heterogeneidad de las redes, es decir, la red puede estar integrada por dispositivos hardware y fabricados por diferentes compañías.

- **VLAN**: LAN virtual**.** Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, de hecho, están ubicados en una serie de segmentos de LAN distintos. Debido a que las VLAN están basadas en conexiones lógicas en lugar de físicas, son sumamente flexibles.

- **VTP :** Protocolo de terminal virtual. Aplicación ISO para el establecimiento de una conexión de terminal virtual a lo largo de la red.

8. LISTA DE ACRÓNIMOS

ADSL: Asymmetric Digital Subscriber Line – Linea de Abonado Digital Asimétrica.

Bw: ancho de banda.

CBWFQ: El encolamiento equitativo con peso basado en clases.

CRC: Verificación por redundancia cíclica**.**

DNS : Sistema de denominación de dominio.

FDDI : Fibre Distributed Data Interface

FTP : Protocolo de transferencia de archivos.

HTTP: Hiper Text Transfer Protocol.

IEEE : Instituto de Ingeniería Eléctrica y Electrónica

IP: Internet Protocolo

LAN: Local Area Network

LLQ: Low Latency Queueing (Encolado de prioridades)

MAC: Control de acceso al medio**.**(Media Access Control)

MAN: Metropolitan Area Network.

Mbps: Mega bit por segundo.

NLB: Network Load Balancing

RAID: Redundancy Array Index Disc

SSL: Secure Socket Layer

SMTP :Protocolo de transferencia de correo simple

TCP/IP: Protocolo de control de transmisión/Protocolo Internet

VLAN: Virtual LAN

VPN: Virutal Private Network

VTP: Virtual Terminal Protocol

QoS: La calidad de servicio.

9. BIBLIOGRAFÍA

SHELDON, Tom. "*Encyclopedia of Networking And Telecomunications*". Estados Unidos: McGraw-Hill, 2004. 1147p.

ORTEGA, J. Eduardo. Ensayo. "*Algoritmos de encolamiento en routers para una distribución justa de la capacidad de un enlace compartido en una red TCP/IP*" Universidad Nacional de Colombia. 2005 187p.

LUNA, Francisco Javier Rosas. "Taxonomía del balanceo de carga". División de De estudios de Postgrado de Ingeniería. Instituto Tecnológico de Aguascalientes (México)

GUNTHER, N.J. "*The Practical Performance Analyst: Performance-by-design for Distributed Systems*." McGraw-Hill (Series on Computer Communications).

CISCO System. Cisco IOS Quality Of Service Solution Configuration Guide. Release12.3 Estados Unidos: Cisco System 2001. Disponible en: www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_r/qosbook.pdf

NxSecurityApliance, "Dispositivos firewall con redundancia integrada."

Disponible en: http://www.n-experts.com/productos/sec_app/tecnicas.php.

Paginas de Internet

www.idg.es/comunicaciones/especial-avether160/Pag07.pdf.

http://www.bujarra.com/ProcedimientoRAID5.html

http://es.wikipedia.org/wiki/MLT.

http://www.s-4.es/mt_BalanceoCarga.aspx

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm.

http://librosnetworking.blogspot.com/2006/04/hsrp-redundancia-en-la-salida-internet.html

http://www.scansource-europe.com/motorola/assets/pdf/5120DS_1205_LA.pdf

ANEXOS

Anexo 1. Dispositivos de Administración

		F5 Network(www.f5.com/espana)
3 DNS Controller ®	Descripción	*Balanceo de carga mundial inteligente y de alta disponibilidad.* La solución 3-DNS Controller le garantiza óptima fiabilidad y rápido rendimiento para todos sus sitios Web, independientemente de su ubicación en el mundo. 3-DNS añade inteligencia al servidor DNS estándar y verifica que los usuarios se dirigen al sitio Web disponible que mejor responde. Su inteligencia única es capaz de explorar el estado de los centros de datos, la red y la situación geográfica de los usuarios y dirigir el tráfico basándose en unas reglas por sector y personalizables.
	Balanceo De carga	Balanceo geográfico de carga, a nivel de país, para dirigir a los usuarios al contenido localizado. El controlador 3-DNS es una solución de balanceo de carga inteligente y disponible para sitios Web y centros de datos distribuidos geográficamente, disponible las 24 horas del día, los siete días de la semana. Gestiona y distribuye las peticiones de Internet a través de numerosos sitios Web con servidores redundantes, independientemente del tipo de plataforma o de su combinación y sin necesidad de instalar software adicional en sus servidores. Para garantizar la mayor disponibilidad posible de su sitio Web, la distribución de las peticiones de los usuarios se realiza en función de las condiciones que presentan tanto el centro de datos como la red, evaluadas a través del tiempo de ida y vuelta, la pérdida de paquetes y otras medidas de QoS.3-DNS integra algoritmos completos de balanceo de carga y cuenta con los métodos de distribución de tráfico más avanzados del mercado, es decir: • Round Robin • Disponibilidad global • Persistencia LDNS • Disponibilidad de aplicaciones • Geografía • Capacidad de servidor virtual • Conexiones mínimas • Paquetes por segundo • Kilobytes por segundo transmitidos • Tiempo de ida y vuelta • Saltos • Índice de paquetes • QoS definida por el usuario • Dynamic Ratio • Round Robin LDNS • Ratio
	Redundancy	Redundancia de los controladores 3-DNS para garantizar la reanudación, en una fracción de segundo, tras un fallo del DNS

	Otras caracteris-ticas importantes	El controlador 3-DNS, combinado con el controlador BIG-IP de F5, garantiza la calidad del contenido Web, tanto estático como dinámico, generado por las aplicaciones de back-end, como las bases de datos. BIG-IP interroga activamente a cada uno de sus servidores a nivel de las aplicaciones. De manera que, cuando sus servidores y aplicaciones funcionan correctamente, pero envían respuestas inadecuadas a sus usuarios finales, el controlador 3-DNS desvía las peticiones a los sitios Web que responden adecuadamente. Una vez corregido el fallo de contenido, el controlador detecta automáticamente que el sitio Web vuelve a responder adecuadamente y le envía peticiones de nuevo.

		UMI S.A.(www.umi.com.co)
FSH2402 GT®	**Descripción**	El Ether-FSH2402GT es un switch Gigabits Ethernet de 24 puertos (10/100 Mbps) + 2 puertos (Gigabits) de muy altas prestaciones, con la capacidad de poder ser Administrado de forma remota. Estas características de alto desempeño en el que la máquina switchea con 8.8 Gpbs throughput y función de auto MDI/MDI-X en todos sus puertos. Pero lo más imortante ofrece una serie impresionante de funciones de dirección al mismo nivel precio como un switche no administrable.
	Caracteristicas de Direccionamiento más significativas	El Ether-FSH2402GT es un equipo con muchas funcioness prácticas de Direccionamiento: • Por puerto puede controlar y limitar el bandwidth entrante y saliente por cada puerto. • Direccionamiento del Switche Central: Configura varios Switches al mismo tiempo. • 802.1Q tag VLAN enables VLAN assignment across different switches. El switch incluso provee los controles para asignar un tráfico single-cast, multi-cast, or broadcast para pasar entrre las VLANs. • Auto configuración Protección por autenticación de password.
		• **10/100Mbps:** 7 Trunk groups in 2 or 4 ports

	Aggregation	• **Gigabit:** 2-port Trunk Group
	Otras caracteristicas importantes	**Ventana del software de Direccionamiento remoto:** Convencionalmente, configurando la dirección inteligente requiere que el usuario conecte el PC (puerto serial o paralelo) directamente al puerto de control del switch. Con el Ether-FSH2402GT la capacidad de direccionaiento In-Band el usuario puede configurar el switche remotamente a través de la red Ethernet. El software de direccionamiento provee un a muy fácil interfase "point-and-click" para alistar todas las funciones. Los usuarios pueden. Lo mejor de todo es que la utilidad de direccionamiento puede Configurar varios Switches al mismo tiempo.

	3Com **(www.f5.com/espana)**	
SuperStack ® 3 Switch 3300	**Descripción**	La familia de conmutadores modulares y apilables de 3Com ha sido diseñada para ayudar a las empresas en rápido desarrollo, a aumentar la potencia y rendimiento de sus redes, de una forma sencilla y económica y con las mínimas molestias. Y además todos los conmutadores tienen capacidad de expansión, por lo que estará preparado para seguir creciendo cuando lo necesite. Presenta una f acil administración porque en cada modulo se incluye Transcend® Network Supervisor de 3Com®. Esta potente aplicación le permitirá conocer, mapear y monitorizar su red con la máxima sencillez
	802.3ad Link Aggregation	Soporte de "trunking" para agregar enlaces en una sola conexión de alta velocidad con otros conmutadores o redes backbone: Permite elegir entre dos modelos, pudiéndose crear así la configuración óptima de conmutación 10/100/1000.
	Opciones de modulo	**1000 Gigabit Ethernet** Estos módulos Gigabit Ethernet ofrecen un soporte de alto rendimiento y tolerancia a los fallos, para grupos de trabajo internos y para las conexiones de grupos de trabajo con el backbone. Además, estos módulos de fácil instalación proporcionan una conectividad Gigabit Ethernet dúplex total, con una velocidad de hasta 2 Gbps, eliminando así los cuellos de botella. Ofrece soporte para enlaces redundantes.

		• El módulo 1000BASE-T con un alcance de hasta 100 metros, a través de cable de cobre de Categoría 5. • El módulo 1000BASE-SX con interface de fibra multimodo y conalcance de hasta 550 metros en el caso de fibra 50/125. • El módulo 1000BASE-LX con soporte para fibra multimodo y monomodo con un alcance, certificado por 3Com, de hasta 10 kilómetros en esta última. **Fast Ethernet 100** Estos módulos añaden un enlace con el backbone Fast Ethernet de fibra, para los grupos de trabajo. Además, estos módulos de fácil instalación proporcionan una conectividad a 200 Mbps dúplex total, a través de fibra, con un alcance de hasta 2 kilómetros. Soporte total de enlaces redundantes para una mayor protección ante fallos de líneas y bucles
	Otras caracteristicas importantes	VLAN basadas en los estándares IEEE 802.1Q; Colas dobles para ayudar a dar prioridad al tráfico multimedia; Control de flujo según los estándares, para optimizar el rendimiento y minimizar la pérdida de paquetes, en condiciones de gran volumen de trabajo en la red.

		D Link Iberia/España
Smart Switch DES-1250G®	**Descripción**	El smart switch DES-1250G es una solución rentable para las pequeñas y medianas empresas que deseen implementar la conmutación de paquetes Ethernet con un fácil ajuste del rendimiento y la seguridad de la red. Este switch dispone de alta densidad de puerto de 48 puertos Ethernet 10/100BASE-TX y 2 combo 1000BASE-T/SFP, lo que da flexibilidad a la conexión Gigabit por cobre/fibra. Los troncales de puerto permiten la utilización del servidor y la conexión al troncal de la red, mientras que las funciones importantes para las aplicaciones intensivas de ancho de banda, como colas de prioridad y VLAN, posibilitan implementar la calidad de servicio (QoS, Quality of Service) y la seguridad, sin tener que pasar por la compleja gestión de red que suelen presentar otros switches gestionados.

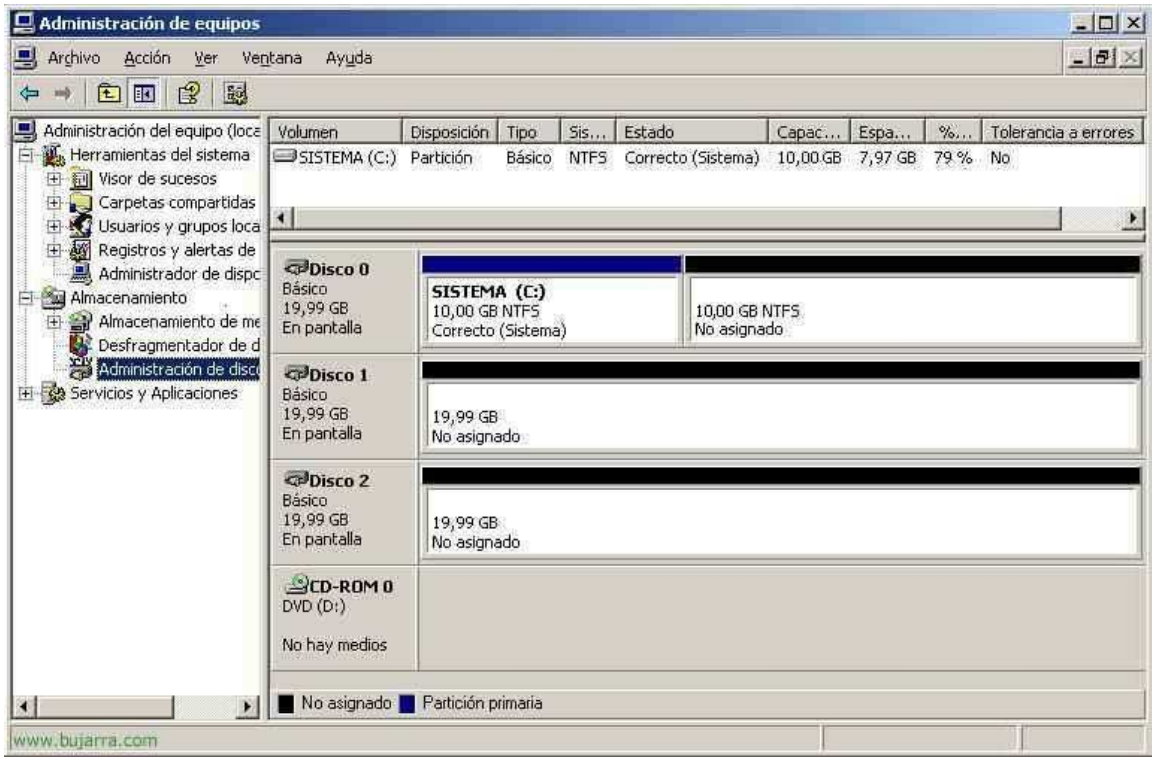
	802.3ad Link Aggregation	Los puertos pueden combinarse para crear anchos de banda agregados de multienlace con balance de carga a un servidor o a un troncal de red. Para expandir la red, también puede usar los troncales de puerto con el fin de eliminar las congestiones entre los switch es en cascada. El switch le permite combinar múltiples puertos en un troncal, y crear múltiples troncales por switch.
	Soporte de calidad de servicio - Encolamiento	El conmutador soporta control de cola de prioridad Layer 2 802.1p para priorizar los paquetes de red. La clasificación de las prioridades de datos de usuario se pueden basar en una cola de prioridad de paquete de datos. Esta función QoS le permite ejecutar aplicaciones intensivas de ancho de banda y sensibles a retardo, así como conectarle al conmutador servidores de vídeo para videoconferencia.
	Otras caracteris-ticas importantes	**Seguridad:** El switch soporta port mirroring como ayuda a la comprobación del tráfico de la red. El administrador de red puede usar esta función como una herramienta de diagnóstico o de depuración, en especial para rechazar un ataque. Le permite mantener un detallado control del rendimiento del smart y modificarlo si es necesario. **Gestión/comprobación de la red:** Tanto la fácil configuración basada en web del smart como la comprobación/gestión de la red puede realizarse desde cualquier estación que esté en red, con lo que no son necesarias ni consolas ni cables de consola. Los dispositivos de red se autodescubren y se muestran en una topología de red, y usted puede recibir avisos de los eventos del sistema y de los errores de puerto mientras comprueba el estado y las estadísticas de la red desde cualquier estación de trabajo

Anexo 2. Configuracion RAID5 en Windows 2003 Server

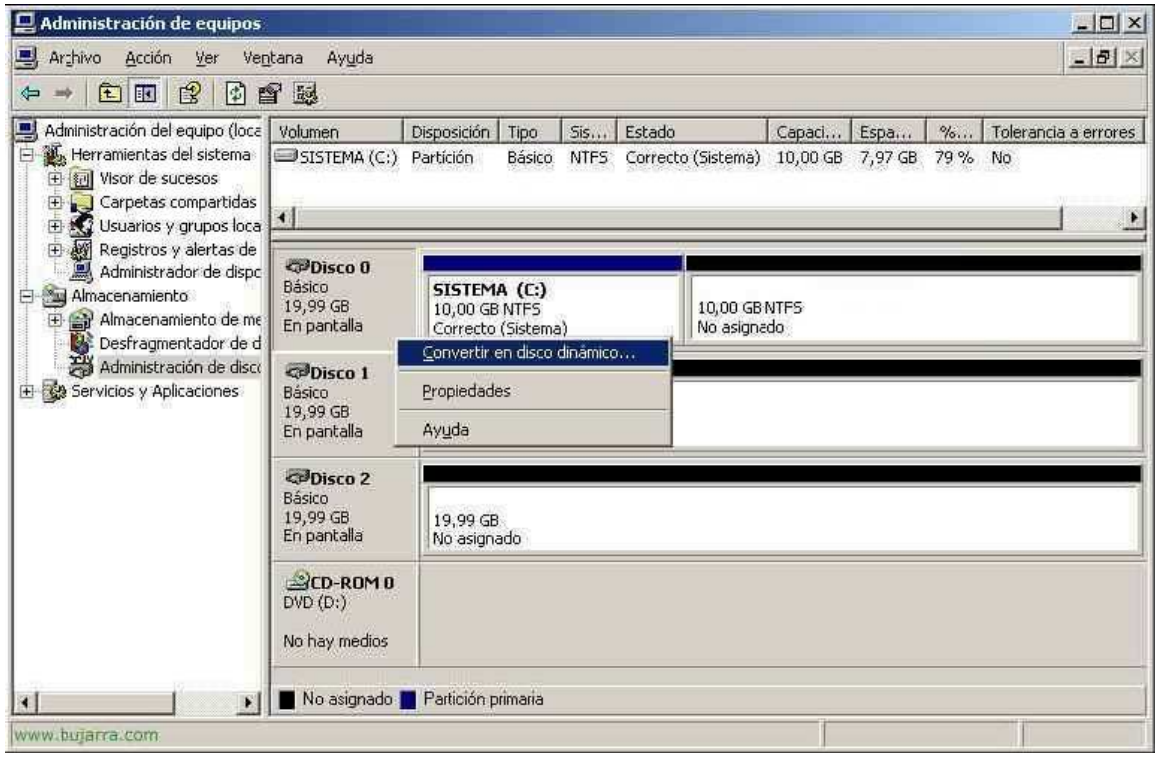
CONFIGURACIÓN DE RAID 5 EN WINDOWS 2003 SERVER

Este tipo de arreglos requiere un mínimo de 3 discos, estos se dividen en stripes (cómo el RAID0) la diferencia es que de los 3 stripes uno se usa para paridad y sólo los otros dos se usan para almacenar datos. Con esto se consigue el incremento de velocidad del RAID-0, pero con la redundancia que permite el disponer de paridad en la práctica el arreglo queda inmune a fallas de un solo disco pero no se desperdicia tanto espacio como en el caso de un RAID 10.

Por ejemplo, un arreglo RAID-5 de 3 discos de 120 GB tiene una capacidad total de (3-1)*120=240 GB, es alrededor de 4 veces más veloz que un disco individual. Sólo se pierde el espacio equivalente a uno de los discos, que en esencia corresponde a la información de paridad.



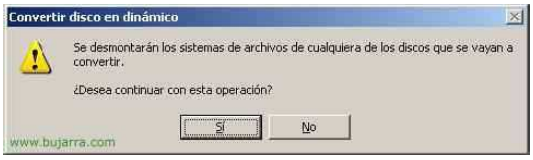
Mínimo se necesitan 3 discos y lo malo es que de la partición del sistema no se puede hacer un RAID5. Para empezar, vamos a "Administración de equipos", (para ello, "Mi PC" > botón derecho > Administrar"). Esto es una vista normal de mi servidor, se supone que tengo 3 discos duros (físicos), una partición donde tengo el sistema de Windows instalado (C:), y un espacio libre donde se creará la partición para que los usuarios guarden sus datos, sobre esta partición se creará el RAID5 y aunque se caiga un disco nadie se da cuenta y sigue todo funcionando sin problemas. Nos fijamos que Windows les llama discos "Básicos" y "particiones", lo que hay que hacer es convertir estos discos Básicos a "Dinámicos" y las Particiones a "Volúmenes". Una vez hecho eso ya podremos jugar con los RAID.



Seleccionamos los tres discos donde haremos el RAID5 y "Aceptar"

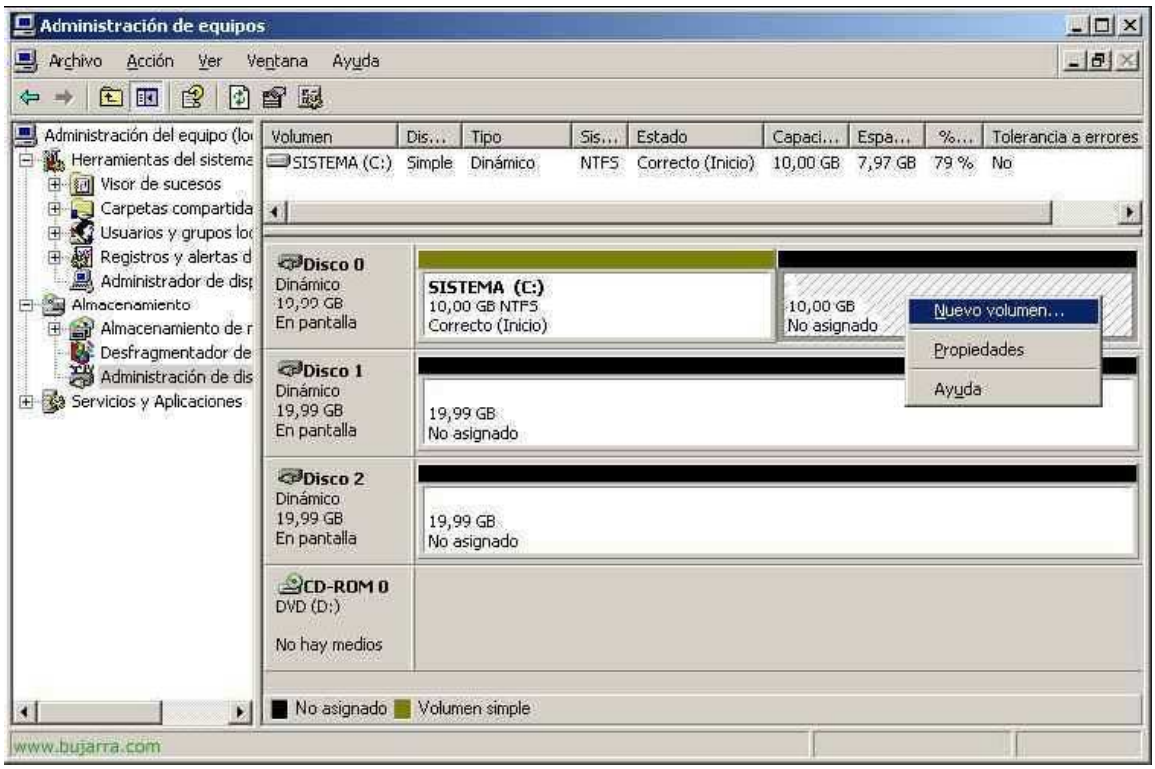
"Convertir"

Si



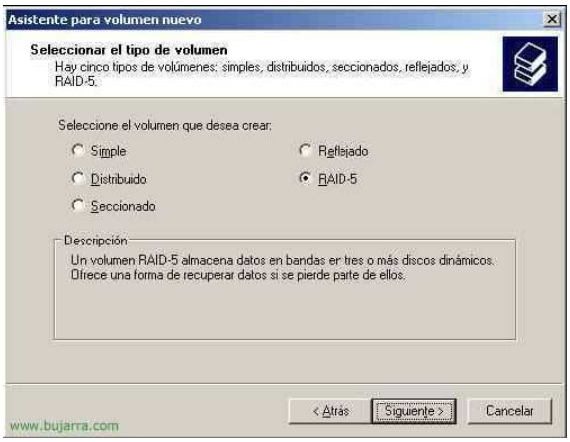
Si

En cuanto pulsemos "Aceptar" se reiniciará el server, así que atentos si se tiene alguna cosa abierta y sin guardar o que podría dañar a algún usuario que esté trabajando en el server.



Una vez reiniciado el servidor vemos que ahora son discos Dinámicos y ya no son particiones, sino Volúmenes (en este caso simples). Ahora, crearemos la nueva partición/volumen, sobre el espacio libre (No asignado), botón derecho > "Nuevo volumen..."

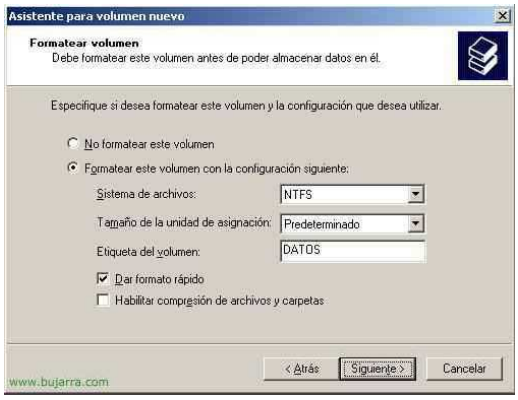
Siguiente"



Seleccionamos el tipo RAID-5 y damos a Siguiente

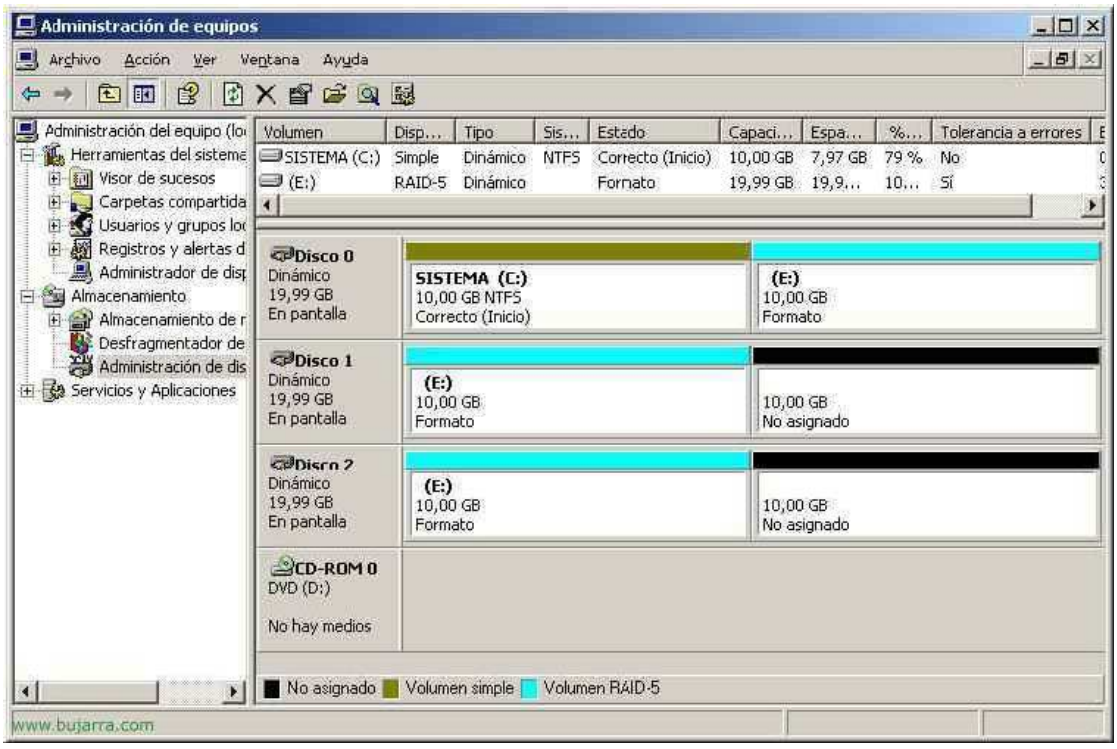
Seleccionamos todos los discos donde crearemos la réplica de todos los datos, y el espacio que queremos crear el volumen RAID5, yo usaré el máximo que me dejen mis HD. y Siguiente

Le pondré la letra E: y "Siguiente"



Formateamos el volumen como NTFS, le ponemos una etiqueta que lo distinga, en plan "DATOS" y quesea un formato rápido para que no tarde, le damos a "Siguiente".

"Finalizar"



Como se puede ver ya se tiene la partición "E:" reflejada en tres discos, así que en caso de caída de cualquier disco no pasará nada.