UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENÍERÍA ELÉCTRICA Y ELECTRÓNICA

VLANS SOBRE REDES LANS GIGABIT ETHERNET

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JORGE LUIS SUENG NAVARRETE

PROMOCIÓN
1985 - II

LIMA – PERÚ

2003

A mis Padres quienes con gran amor y sacrificio,
me apoyan incondicionalmente en todos los retos
que me presenta la vida y merecen esta muestra
de la culminación de su esfuerzo en mi.

VLANS SOBRE REDES LANS GIGABIT ETHERNET

SUMARIO

El presente informe de suficiencia trata sobre el diseño e implementación de las Redes de Area Local (LANs) para una empresa de Telecomunicaciones en sus sedes principales (Tecnológica y Administrativa), basadas en tecnología Gigabit Ethernet y empleando aspectos tecnológicos relacionados con ellas como VLANS para dar flexibilidad y optimizar el tráfico de las redes, el enrutamiento de las VLANS mediante el protocolo OSPF, la implementación del estándar 802.1q para extender las VLANS entre los Switches, la aplicación del protocolo de redundancia de nivel 3 como el VRRP, la implementación de enlaces redundantes entre los switches para obtener un Backbone redundante, bajo un esquema de redes de alto desempeño, disponibilidad y escalabilidad.

Estas redes LAN son parte de la red Corporativa (LAN/WAN) de la Empresa de Telecomunicaciones, por lo cual requería su integración a los equipos existente. Siendo la red LAN de la Sede Tecnológica con su Backbone Gigabit Ethernet el núcleo de la red Corporativa.

Describiremos los conceptos principales empleados para la implementación de las Redes LANs mediante una visión general, no extensiva ni profunda; esto es así por dos motivos: primero, por brevedad y segundo, por ser una temática <<VIVA>>, en evolución, con muchos trabajos en marcha.

ÍNDICE

PRÓLOGO

Desde la aparición de las computadoras personales a principios de los setenta, en el mundo de los negocios han ido emergiendo cada vez más aplicaciones para este tipo de tecnología. Con la introducción de las redes de área local y los archivos y la impresión compartida en los ochenta, quedó patente que la computación distribuida había dejado de ser una moda pasajera. En los años noventa, las computadoras se hicieron más asequibles, e innovaciones como Internet permitieron a todos beneficiarse de los servicios de computación en forma global. El trabajo con las computadoras se ha ido ampliando y haciéndose cada vez más distribuido. Por lo tanto, un interés principal de este informe es describir el rol y la función que desempeñan las redes de área local en un entorno distribuido.

Por otra parte, en el actual mundo de los negocios, el acceso fiable y a tiempo a la información es una de las claves para seguir siendo competitivos. Las redes actuales han de soportar la explosión de servicios de información que se está produciendo y la imparable tendencia hacia la convergencia de voz, video y datos. Y han de hacerlo de una manera efectiva en costos. Por eso a las redes actuales, cada día más críticas se le exigen muy altos niveles de disponibilidad y rendimiento. Estos requerimientos se traducen en la necesidad de contar con mecanismos que garanticen tanto la optimización del ancho de banda como la tolerancia a fallas, la gestión proactiva de la red y un excelente soporte y mantenimiento. Afortunadamente, la conmutación proporciona a las redes de hoy las prestaciones de control escalable requeridas para satisfacer estas demandas, como mallas de conmutadores que permite

formar enlaces activos simultáneos y redundantes de red, y la agrupación de puertos "port trunking" para establecer conexiones punto a punto, tolerante a fallas y de alto ancho de banda (por ejemplo entre conmutadores o entre un conmutador y un servidor). Asimismo, mantener altos niveles de disponibilidad y rendimiento exige disponer de módulos y fuentes de alimentación redundantes y sistemas de resolución automática de problemas, que mantengan en perfecto estado la red con una intervención mínima por parte del administrador.

Además los tradicionales Ethernet e IP se están convirtiendo en las bases tecnológicas sobre la que se evolucionará hacia la nueva generación de redes. IP sobre Ethernet, en cualquiera de sus variantes, será la base fundamental sobre la que se construyan las redes de nueva generación. La implementación , de técnicas que permiten un mayor rendimiento y disponibilidad en la LAN, como "port trunking " y malla de conmutadores "switch meshing" hacen del protocolo IP y de la topología Ethernet la opción preferida de las empresas. Asimismo, la implementación de los nuevos estándares de calidad de servicios (QoS) , que aseguran el ancho de banda necesario para el tráfico crítico y sensible a los retardos como la voz y video, y la aparición de nuevas tecnologías de gestión y administración – como la gestión basada en políticas-, aumentan aún más su poder.

El gran atractivo de IP, ya ampliamente aceptado como el protocolo por excelencia, y Ethernet - a 10, 100 o 1000 Mbps- es que permite cubrir los requisitos presentes y futuros de las empresas con una tecnología estandarizada y ampliamente consolidada, que además reduce el costo de propiedad gracias a sus precios cada vez más bajos y a la gran experiencia de los profesionales en ambos campos.

CAPÍTULO I

ANTECEDENTES

1.1 INTRODUCCIÓN

La Empresa a la cual se diseño e implementó las redes LAN es un operador de telefonía celular de origen italiano.

La empresa de Telecomunicaciones llegó al Perú con una nueva propuesta en telefonía celular y comenzó a operar por Enero del 2001.

Debido al rápido crecimiento de su personal administrativo la empresa de Telecomunicaciones tubo que mudarse de local donde realizaba sus tareas administrativas

Entre Julio y Setiembre del año 2001 la Empresa de Telecomunicaciones comenzó un proyecto de implementación de su red LAN para su nueva sede Administrativa, ubicada en un Edificio y que comprendía los Pisos 6 al 11. Ello supuso la instalación de un cableado estructurado el cual comprendía el cableado Horizontal con cable UTP CAT 6 , el cableado de Fibra Optica en su red troncal y la instalación de Equipos de comunicaciones Gigabit Ethernet de Nortel Networks que fue la solución planteada e instalada

Con casi 500 usuarios, esta red LAN para la Sede Administrativa debería asegurar la continuidad de servicios a todos los usuarios y estar preparada para comenzar con la transmisión de voz video y datos entre computadoras y servidores.

Casi simultáneamente se inicio el proyecto de renovación de la red LAN de su sede Tecnológica. Esta red estaba funcionando pero con caídas periódicas. Al ser la red LAN de la Sede Tecnológica con su Backbone Gigabit Ethernet el núcleo de la red Corporativa era crítico su funcionamiento. Con los equipos Alcatel que estaban instalado esta red Ethernet (ver diagrama 1.1) no podía proveer una disponibilidad garantizada para sus aplicaciones de misión critica, tales como los Servidores de Tarificación, etc . La configuración solicitada por la Empresa de Telecomunicaciones a la empresa integradora fue: Enlaces redundantes desde los switches de Core hacia los Switches de borde, Creación y configuración de 6 VLANs y el enrutamiento entre ellas, Implementación de protocolos de alta disponibilidad entre los switches de Core y Routers respectivamente (VRRP y HSRP) y la implementación del protocolo de enrutamiento OSPF, para integrar esta red LAN a la red Corporativa de la Empresa de Telecomunicaciones. Estas actividades no fueron cumplidas por la empresa proveedora , tras varios intentos fallidos de implementar lo solicitado.

Este fue unos de los motivos por la que la empresa de Telecomunicaciones replanteó su estrategia y evaluó diversas alternativas para sustituir la red LAN corporativa de su sede Tecnológica

Con este proyecto en mente, en el año 2001 y después de un análisis detallado se eligió la oferta de Nortel Networks.

La solución que se instaló fue una red Gigabit Ethernet de Nortel Networks, bajo un esquema de alta disponibilidad la misma que reemplazó a la red que estaba basada en los switches Alcatel. (Ver Capitulo 5, Fig. 5.1.2 con la solución planteada.)

Para minimizar el impacto del diseño de la nueva troncal se trató de mantener el diseño de red IP lógico existente en la compañía basado en LAN virtuales (VLAN) y conmutación de nivel 3.

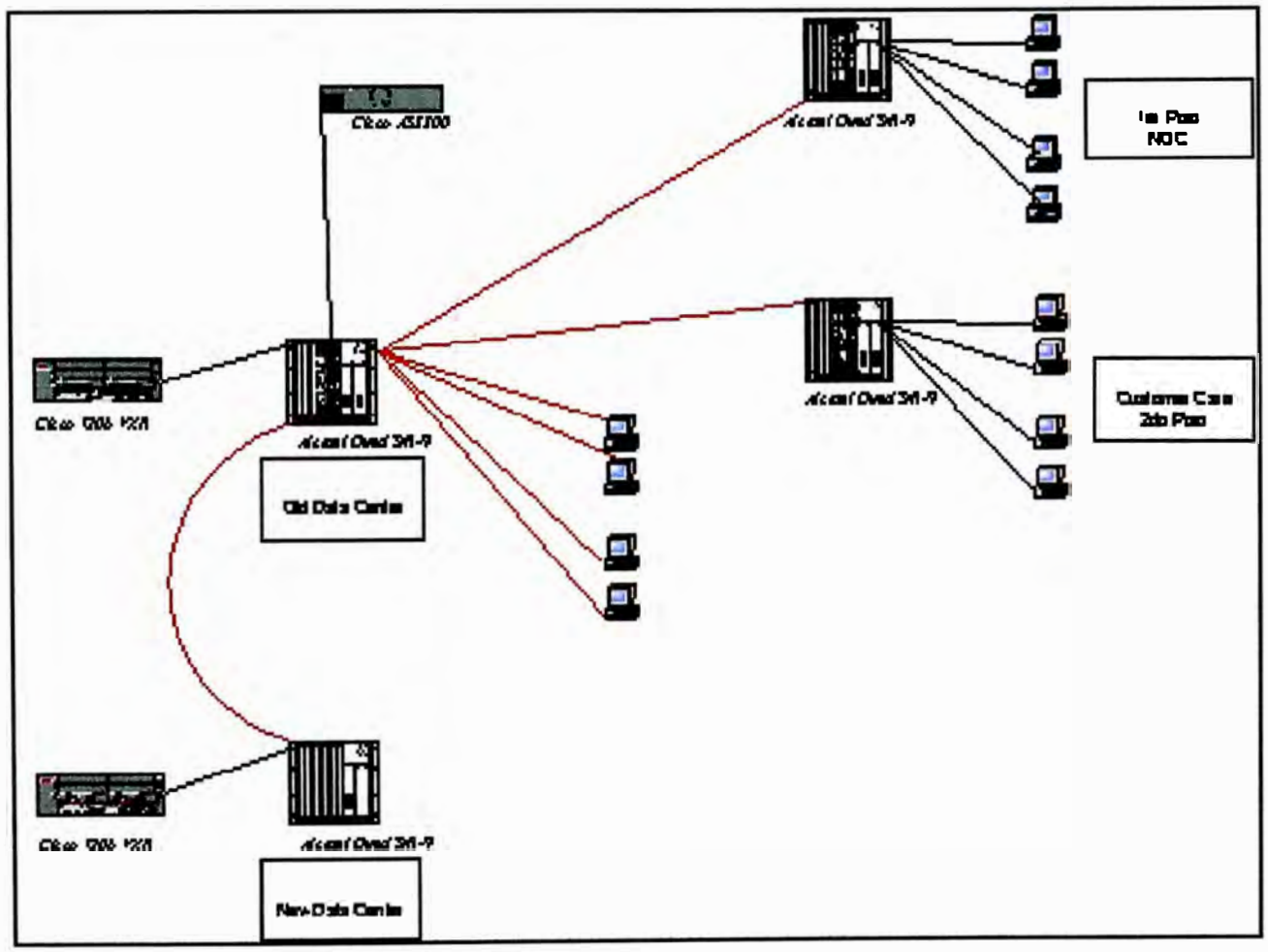


Figura 1.1 Red LAN de la Sede Tecnológica antes del nuevo diseño

CAPÍTULO II

TECNOLOGÍA GIGABIT ETHERNET

2.1 INTRODUCCIÓN

Desde sus comienzos en la Corporación Xerox en los tempranos años 1970s, Ethernet ha sido el protocolo de red dominante. De todos los protocolos actuales de red, Ethernet tiene de lejos el número más alto de puertos instalados y proporciona el mejor costo de performance en comparación a las redes en Anillo Token Ring, FDDI (Fiber Data Interface) y ATM para conectividad al escritorio. Fast Ethernet el cual incrementó la velocidad Ethernet de 10 a 100 Mbps proporcionó una opción simple y rentable para conectividad de la troncal (backbone) y de los servidores.

Gigabit Ethernet construido encima o basado en el protocolo Ethernet incrementó la velocidad diez veces con respecto al Fast Ethernet , es decir 1000 Mbps o 1 Gigabit por segundo (Gbps). Este protocolo que se estandarizó en Junio de 1988, es un jugador dominante en la conectividad de los backbones de gran velocidad de las redes de Area local y los servidores. Desde que Gigabit Ethernet esta significativamente basado en Ethernet , los clientes serán capaces de acomodar su base de conocimiento existente para manejar y mantener redes Gigabit.

2.2 EL ESTÁNDAR GIGABIT ETHERNET

En los últimos años la demanda sobre la red se ha incrementado drásticamente. Las antiguas redes Ethernet 10BASE5 y 10BASE2 fueron reemplazadas por hubs 10BASET, (en 1990 IEEE estandariza 10BASE-T) permitiendo mayor administrabilidad de la red y la planta de cables. Cuando las aplicaciones incrementaron la demanda sobre la red, nuevos protocolos de alta velocidad tales como FDDI y ATM se pusieron disponibles. Sin embargo entre los años 1995 y 1999 (en Junio 1995, IEEE estandariza Fast Ethernet 100BASE-FX,100BASE-TX y 100BASE-T4), Fast Ethernet ha sido el backbone escogido por excelencia debido a su simplicidad y su confianza en Ethernet. La principal meta del Gigabit Ethernet era ser construido en base de esa topología y conocimiento para construir un protocolo de superior velocidad sin forzar a los clientes de dejar de utilizar el equipamiento de redes existente.

El Comité del estándar que trabajò sobre Gigabit Ethernet fue el IEEE 803.2z Task Force, el cual estableció una agresiva timetable (horario) para el desarrollo del estándar Gigabit Ethernet. La posibilidad de un estándar Gigabit Ethernet fue elevada en 1995 después de la ratificación final del estándar Fast Ethernet. Por Noviembre de 1995 había bastante interés para formar un grupo de estudio de gran velocidad. Este grupo se reunió a finales de 1995 y varias veces durantes los primeros meses de 1996 para estudiar la viabilidad de Gigabit Ethernet. Las reuniones crecieron en asistencia alcanzando a 150 a 200 individuos. Numerosas contribuciones técnicas fueron ofrecidas y evaluadas.

En Julio de 1996, el 802.3z Task Force fue establecido con la carta constitucional para desarrollar un estándar para Gigabit Ethernet. El acuerdo de los conceptos básicos en las contribuciones técnicas para el estándar se logró en la reunión de la IEEE en Noviembre de 1996. El primer borrador del estándar fue producido y revisado en Enero de 1997; El Estándar final fue aprobado en Junio de 1998. (IEEE estandarizo Gigabit Ethernet 802.3z, que comprende los medios físicos 1000BASE—SX, 1000BASE-LX y 1000BASE—CX). Previamente en Marzo de 1997, se escinde del grupo de trabajo 802.3z el 802.3ab para la estandarización de 1000BASE-T (Gigabit Ethernet sobre cable UTP CAT 5). En Marzo de 1999 se estandariza 1000BASE-TX.

Una de las causas del retrazo de la estandarización del 802.3z fue resolver el problema del retardo del modo diferencial (differential mode delay DMD) . El DMD afecta solo a las fibras Multimodo cuando usamos lasers LX/LH. El problema es cuando un modo de luz experimenta jitters (saltos) (distorsión de línea), esto podría en los casos extremos, causar que un solo modo de luz sea dividido en dos o más modos de luz (ver Fig 2.2.1). En otras palabras los datos podrían ser perdidos.

La Fibra Multimodo fue diseñada para LEDs (Light Emitting Diodes) de corto alcance, no para láser.

La solución a esto fue referida como un "lanzamiento condicionado" (ver Fig 2.2.2) . En otras palabras, si la luz que viaja a través del centro del core en una línea directa es direccionada con un ligero ángulo (o simplemente dirigida fuera del centro del core) , entonces el retardo modal es corregido. Para lograr un lanzamiento condicionado, un patch Cord de acondicionamiento Modal especial debe ser instalado.

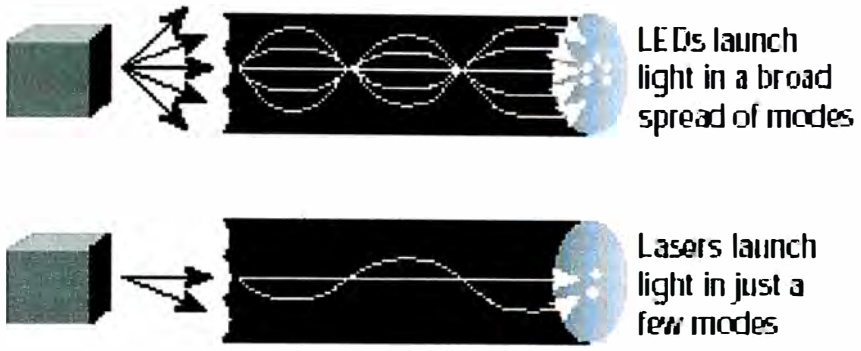
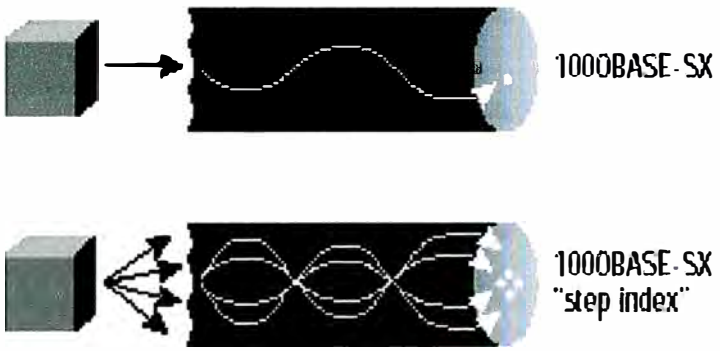


Figura 2.2.1 Descripción del retardo de modo diferencial



- Prohíbe que los transmisores basados en laser concentren su luz en el centro de la Fibra.
- Esto es referido como "Lanzamiento condicionado".

Figura 2.2.2 Descripción del lanzamiento condicionado

2.3 ARQUITECTURA DEL PROTOCOLO GIGABIT ETHERNET

Para acelerar la velocidad desde 100 Mbps Fast Ethernet a 1Gbps, varios cambios se necesitan haber hecho en la interfase física. Se ha decidido que Gigabit Ethernet parezca idéntico a Ethernet desde la capa de enlace de datos hacia las capas superiores. El Desafío involucrado en la aceleración a 1 Gbps ha sido desarrollado por la unión de dos tecnologías juntas: El Ethernet IEEE 802.3 y el ANSI X3T11FiberChannel. La Figura 2.3.1 muestra como los componentes claves de cada tecnología han influido para formar Gigabit Ethernet.

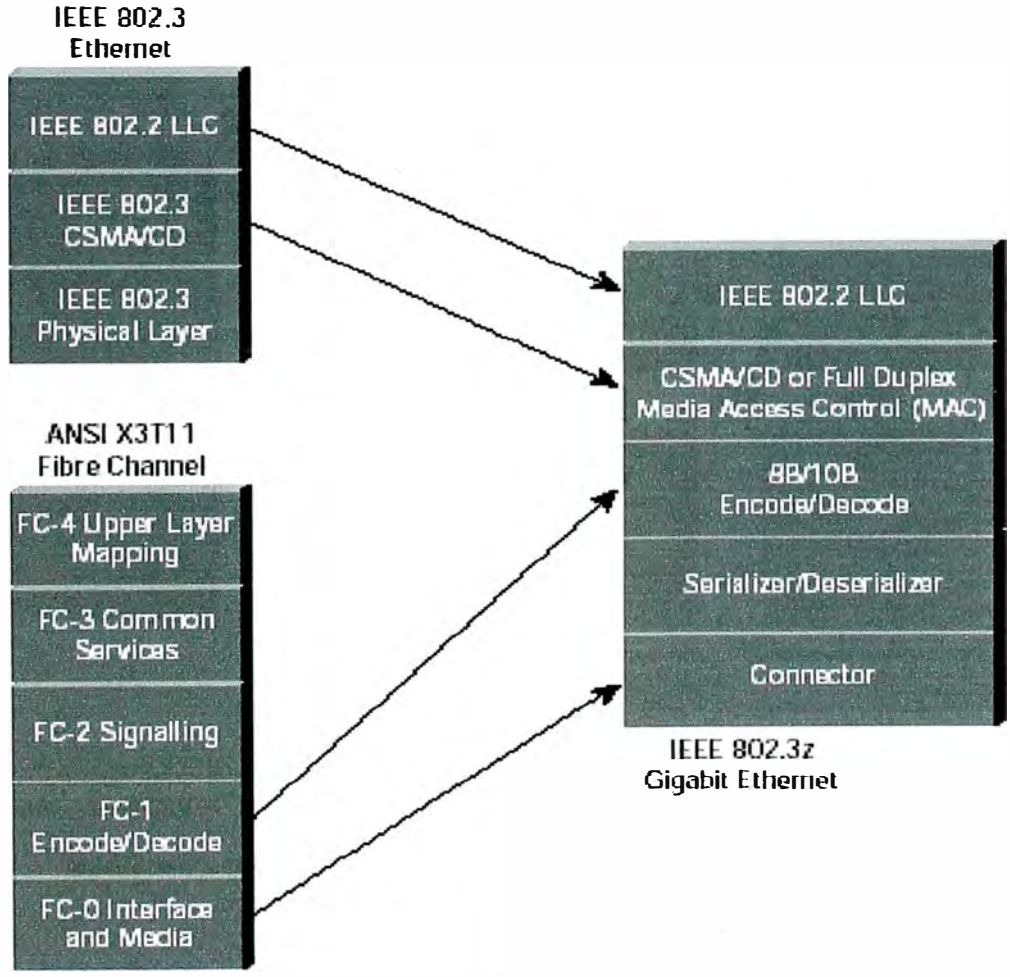
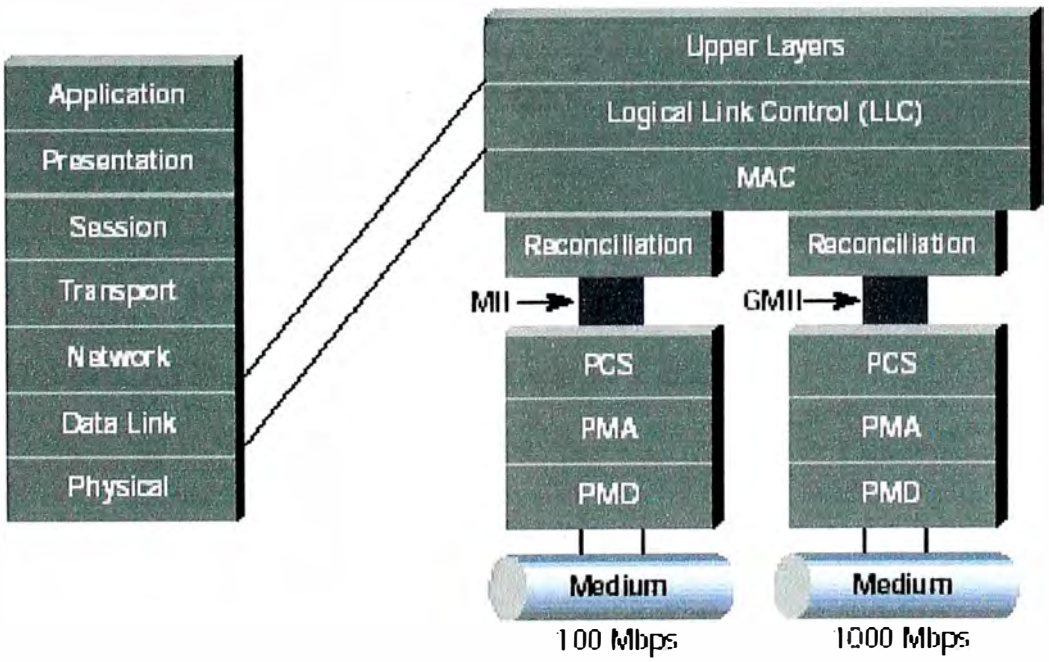


Figura 2.3.1 El Stack de protocolos Gigabit Ethernet

La influencia de estas dos tecnologías significa que el estándar puede sacar ventaja de la tecnología de FibreChannel con la existente interfase física de alta velocidad mientras mantiene el formato del frame Ethernet IEEE802.3, compatibilidad hacia atrás para el medio instalado y uso del acceso múltiple con censado de portadora y detección de portadora (CSMA/CD) en full o half duplex . Este escenario ayuda a minimizar la complejidad de la tecnología, resultando en una tecnología estable que puede ser rápidamente desarrollada.

El modelo actual de Gigabit Ethernet es mostrada en la Figura 2.3.2



Fuente: Parámetros de control de acceso al medio de la IEEE, parámetros de repetidores y administración para operación de 1000 Mbps

Figura 2.3.2 Modelo de Arquitectura del Gigabit Ethernet IEEE 802.3z.

- **Interfase Física**

  En la Figura 2.3.3 se muestra el diagrama físico del 802.3z y 802.3ab.

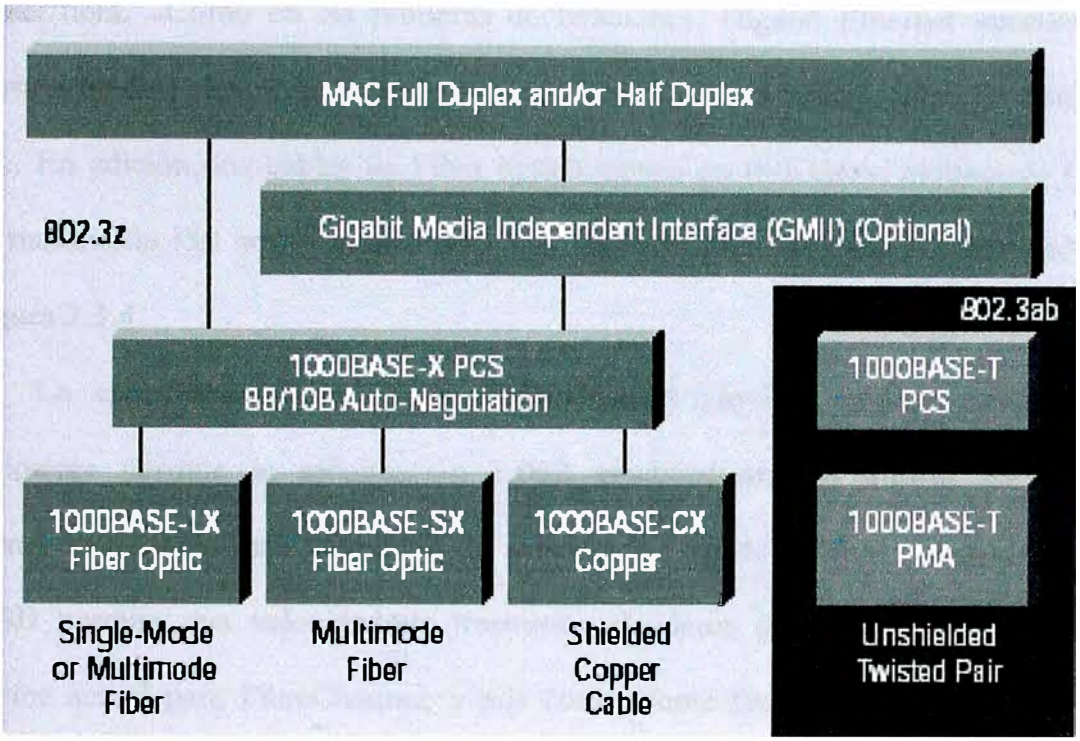


Figura 2.3.3 Diagramas Físicos del 802.3z y 802.3ab.

❑ LA INTERFASE PORTADORA DE GIGABIT ETHERNET

El convertidor de interfase Gigabit (GBIC, "Gigabit interfase converter") permite a los administradores configurar cada puerto Gigabit en un puerto por puerto básico para interfases SX ("short-wave"), LX ("long-wave"), LH ("long-haul") e interfases físicas de cobre (CX). Los GBICs LH extienden la distancia para fibra

monomodo desde el estándar de 5 Km a 10 Km. Los fabricantes tales como Cisco, Nortel Networks ven al LH como un valor añadido, sin embargo este no es parte del estándar 802.3z, permitiendo a los fabricantes de switches construir un único switch físico o modulo de switch que el cliente puede configurar para la topología requerida de láser/fibra. Como en las primeras declaraciones, Gigabit Ethernet inicialmente soporta 3 medios claves: láser de onda corta, láser de onda larga y cobre en distancia corta.. En adición, los cables de Fibra óptica vienen en tres tipos: multimodo (62.5 um), multimodo (50 um) y monomodo. Un diagrama para los GBIC es mostrado en la Figura 2.3.4.

La especificación de PMD ("FiberChannel physical médium dependent") actualmente permite la señalización 1.062 gigabaud en full duplex. El gigabit Ethernet incrementa esta velocidad de señalización en 1.25 Gbps. La codificación 8B/10B permite una velocidad de trasmisión de datos de 1000Mbps. El tipo de conector actual para FibreChannel, y por consiguiente para Gigabit Ethernet, es el conector SC tanto para fibra multimodo y fibra monomodo. La especificación Gigabit Ethernet llama soporte al medio a los cables de fibra óptica multimodo, cable de fibra óptica monomodo y un cable especial de cobre balanceado blindado de 150 ohmios.

En contraste, los switches Gigabit Ethernet sin GBIC no pueden soportar otros tipos de láser o necesitan ser ordenadas customizados a los tipos requeridos de láser.

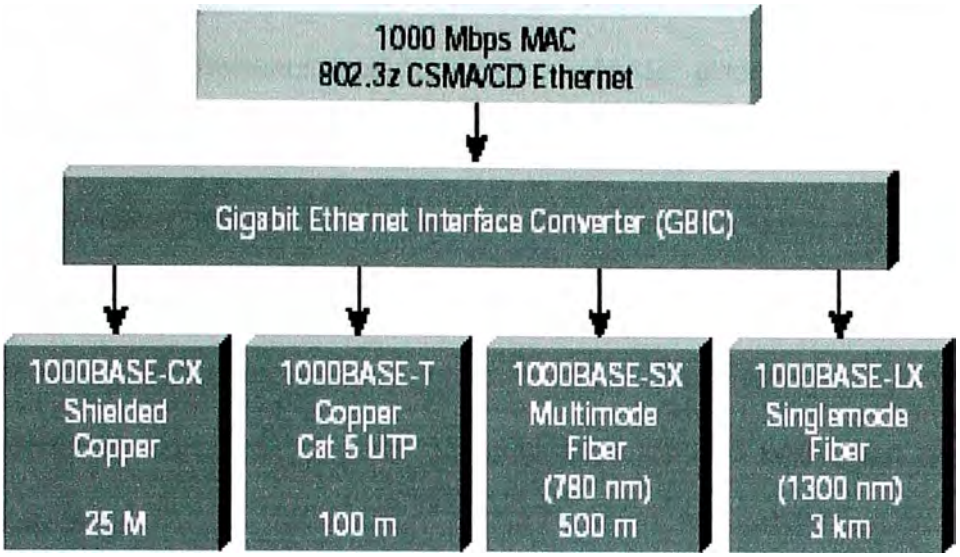


Figura 2.3.4 Función de la Interfase GBIC.

- **Láser de onda larga y de onda corta sobre medio de Fibra Óptica**

Dos tipos de láser estándar son soportados sobre fibra: 1000BASE-SX (láser de onda corta) y 1000BASE-LX (láser de onda larga) los cuales son soportados sobre Fibra Multimodo. Dos tipos de fibra son disponibles: fibras de 62.5 y 50 micras de diámetro. El láser de onda larga es usado para fibra monomodo, debido a que esta fibra es optimizada para trasmisiones láser de onda larga. No hay soporte para láser de onda corta sobre fibra monomodo.

Las diferencias claves entre el uso de las tecnologías de onda larga y onda corta son el costo y la distancia. Los tipos de láser sobre cable de fibra óptica toman ventaja de las variaciones en atenuación en un cable. En diferentes longitudes de onda, declives "dips" en atenuación son encontrados sobre el cable.

El láser de onda corta y de onda larga toman ventaja de estos "dips" e iluminan el cable en diferentes longitudes de onda. El láser de onda corta esta disponible sin esfuerzo debido a que las variaciones de este tipo de láser son usadas en tecnología de disco compacto. El láser de onda larga toma ventaja de los declives "dips" de atenuación en longitudes de onda más grandes en el cable. El resultado neto es por consiguiente que el láser de onda corta cuesta menos, él recorre una distancia corta. En contraste, el láser de onda larga es más caro pero él recorre distancias más larga.

Las fibras monomodo han sido tradicionalmente usados en plantas de cableado de redes para alcanzar distancias grandes. En Ethernet, por ejemplo, el rango del cable monomodo llega hasta 10 Km. Con fibra monomodo, usando un núcleo de 9 micrones y láser de 1300 nanómetro, demuestra la distancia grande con que se llega con esta tecnología. El pequeño núcleo y láser de energía baja con la longitud de onda alargada del láser le permite viajar grandes distancias. Esta configuración habilita a la fibra monomodo alcanzar grandes distancias, de todos los medios con el menos reducción en ruido.

Gigabit Ethernet es soportada sobre dos tipos de fibra multimodo: fibras de 62.5. y 50 micrones de diámetro. La fibra de 62.5 micrones es típicamente aplicado en el cableado vertical de los edificios y en el campus, y ha sido usado para tráfico backbone de Ethernet, Fast Ethernet y FDDI. Este tipo de fibra, sin embargo, tiene un ancho de banda modal bajo (la habilidad del cable de transmitir luz), especialmente con láser de onda corta. En otras palabras, el láser de onda corta sobre fibra de 62.5 micrones, es hábil para viajar distancias cortas en lugar del láser de onda larga. Relativo a la fibra de 62.5 micrones, la fibra de 50 micrones tiene

significativamente mejor característica de ancho de banda modal y es hábil de viajar distancias más grandes con láser de onda corta.

- **Cable de cobre blindado balanceado de 150 ohmios (1000BASE-CX)**

Para cables más corto (de 25 metros o menos), Gigabit Ethernet permite transmisión sobre un cable especial balanceado de 150 ohmios. Este es un nuevo tipo de cable blindado. Este no es un cable UTP o cable tipo I o II de IBM. Para minimizar la seguridad e interferencia concernida, causada por diferencias de voltaje, ambos trasmisores y receptores comparten una tierra común. La perdida de retorno para cada conector es limitada a 20 dB para minimizar las distorsiones de transmisión. El tipo de conector para 1000BASE-CX es un conector DB-9. Un nuevo conector ha sido desarrollado por AMP llamado HHSCD, el cual se incluyo en la revisión final del estándar.

La aplicación para este tipo de cableado es para interconexión en el centro de datos en distancia corta y conexiones inter. o intra racks.

Debido a la limitación en distancia de 25 metros, este cable no trabaja en interconexión de centros de datos o armarios de subidas.

Las distancias para el medio soportado bajo el estándar IEEE 802.3z son mostradas en la Figura 2.3.5.

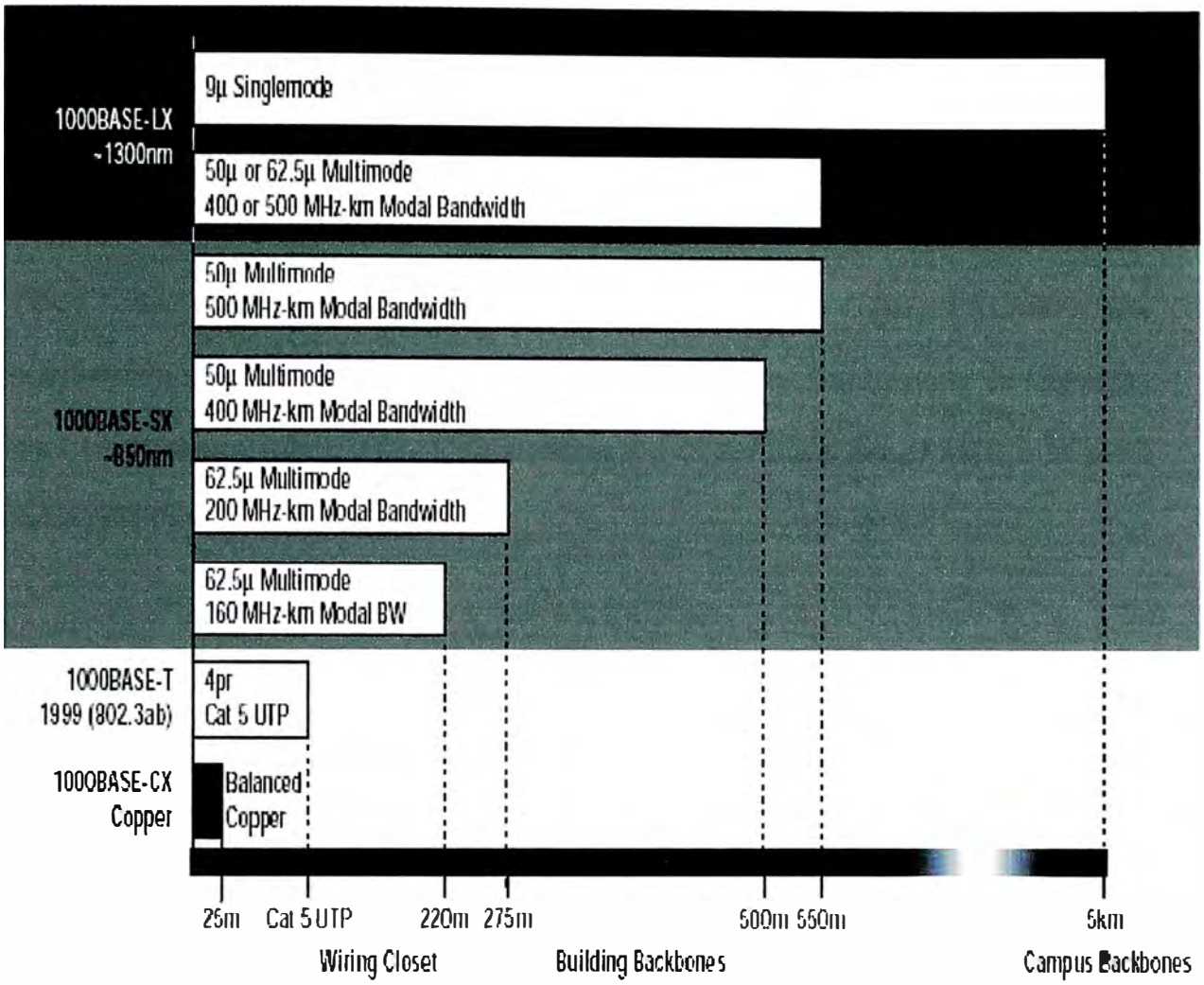


Figura 2.3.5 Cartilla de distancia para el 802.3z y 802.3ab

- **Serializador/Deserializador**

La subcapa de fijación del medio físico (PMA "phisical media attachment") para Gigabit Ethernet es idéntica al PMA para FibreChannel. El serializador / deserializador es el responsable para soportar múltiples esquemas de codificación y permitir la presentación de estos esquemas de codificación a las capas superiores. La data ingresando a la subcapa física (PHY) ingresará a través del PMD y necesitará

soportar el esquema de codificación apropiado a ese medio. El esquema de codificación para FibreChannel es 8B/10B, diseñado especialmente para trasmisiones sobre cable de fibra óptica. Gigabit Ethernet usa un esquema de codificación similar. La diferencia entre FiberChannel y Gigabit Ethernet , sin embargo, es que FiberChannel utiliza señalización a 1.062 gigabaudios donde Gigabit Ethernet utiliza señalización a 1.25 gigabaudios. Un esquema de codificación diferente es requerido para trasmisiones sobre UTP. Esta codificación es realizada por el UTP o la parte física (PHY) del 1000BASE-T.

- **Codificación 8B/10B**

La capa FC-1 de FiberChannel describe la sincronización y el esquema de codificación 8B/10B. El FC-1 define el protocolo de trasmisión, incluyendo la codificación y decodificación serial a y desde la capa física , caracteres especiales y control de errores. Gigabit Ethernet utiliza la misma codificación/decodificación especificada en la capa FC-1 de Fiberchannel. El esquema utilizado es la codificación 8B/10B. Este esquema es similar a la codificación 4B/5B usada en FDDI. Sin embargo, la codificación 4B/5B fue rechazada por FiberChannel debido a su falta de balance DC. La falta de balance DC, puede resultar potencialmente en un calentamiento dependiente de la data de los laseres debido a que un trasmisor envía más en 1 s. que en 0 s. , resultando en razones de errores más alto.

La codificación de la data trasmitida a alta velocidad provee algunas ventajas:

- La codificación limita las características de trasmisión efectiva, tales como razones de 1 s. a 0 s. sobre la razón de error.

- Recuperación del reloj a nivel de bit del receptor puede ser grandemente mejorada usando codificación de la data.
- La codificación incrementa la posibilidad que las estaciones receptoras puedan detectar y corregir trasmisiones o errores de recepción.
- La codificación puede ayudar a distinguir los bits de data de los bits de control.

Todas estas características han sido incorporadas dentro de la especificación de FibreChannel FC-1.

En Gigabit Ethernet, la capa FC-1 toma la data decodificada desde la capa FC-2 de 8 bits a la vez desde la subcapa de reconciliación (RS), el cual conmuta "bridges" la interfase física FibreChannel a las capas superiores del Ethernet IEEE 802.3. La codificación toma vía un mapeo de 8 a 10 caracteres. La data codificada comprime 8 bits con una variable de control. Esta información es, en cambio, codificada dentro un carácter de trasmisión de 10 bits.

La codificación es cumplida dándole a cada carácter de trasmisión un nombre, denotado como Zxx.y. Donde Z es la variable de control que puede tener dos valores: D para Data y K para carácter especial. La designación xx es el valor decimal del numero binario compuesto de un subconjunto de los bits decodificados. La designación y es el valor decimal del numero binario del resto de bits decodificados.

Este escenario implica que hay 256 posibilidades para Data (designación D) y 256 posibilidades para caracteres especiales (designación K) . Sin embargo solo 12 Kxx.y valores son caracteres validos de trasmisión en FibreChannel. Cuando la data

es recibida el carácter de trasmisión es decodificada dentro de uno de las 256 combinaciones de 8 bits.

- **CAPA DE CONTROL DE ACCESO AL MEDIO**
  - **La Capa de enlace lógico**

Gigabit Ethernet ha sido diseñado para adherirse al formato de frame Ethernet estándar. Esta configuración mantiene compatibilidad con la base instalada de productos Ethernet y Fast Ethernet , no requiriendo translación de frame. La figura 2.3.6 describe el formato del frame IEEE 802.3/Ethernet.

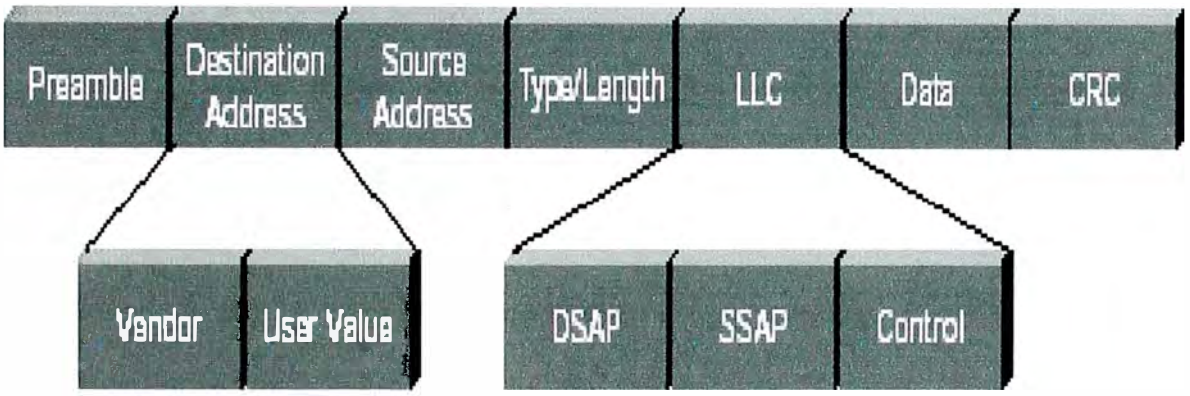


Figura 2.3.6 Formato del Frame Ethernet

La especificación original Xerox identifica un campo *tipo*, el cual fue utilizado para identificación de protocolo. La especificación IEEE 802.3 elimina el campo tipo, reemplazándolo con el campo *longitud*. El campo *longitud* es usado para identificar la longitud en bytes del campo de data. El tipo de protocolo en los frames 802.3 es dejado en la porción de data del paquete. El control de enlace lógico (LLC, "Logical Link Control") es responsable de proveer servicios a la capa de red

independiente del tipo de medio, tales como FDDI, Ethernet, Token Ring, etc. La capa LLC hace uso de los PDUs ("protocol data units") de LLC para comunicarse entre la capa MAC ("Media Access Control") y las capas superiores de la pila de protocolo. La capa LLC usa tres variables para determinar el acceso dentro de las capas superiores vía el LLC-PDU. Estas direcciones son el punto de acceso de servicio destino (DSAP "destination service access point"), el punto de acceso de servicio fuente (SSAP "source service access point") y la variable de control. La dirección DSAP especifica un identificador único dentro de la estación dando la información del protocolo para las capas superiores; el SSAP provee la misma información para la dirección fuente.

El LLC define acceso de servicio para los protocolos que conforman el modelo OSI para los protocolos de red. Desgraciadamente, muchos protocolos no obedecen las reglas para estas capas. Por consiguiente, información adicional debe ser adicionada a el LLC para proveer información con respecto a estos protocolos. Los protocolos que caen dentro de esta categoría incluyen IP e IPX. El método usado para proveer esta información de protocolo adicional es llamado un frame de protocolo de acceso subnetwork (SNAP " subnetwork Access Protocol"). Una encapsulación SNAP es indicada por las direcciones SSAP y DSAP siendo colocado en "0xAA". Cuando esa dirección es vista, nosotros sabemos que una cabecera SNAP sigue. La cabecera SNAP es de 5 bytes de longitud: los primeros 3 bytes consisten del código de la organización, el cual es asignado por el IEEE; Los segundos 2 bytes usan el valor *tipo* colocado desde las especificaciones original del Ethernet.

CAPÍTULO III

DISEÑANDO REDES LANS REDUNDANTES

3.1 CONSIDERACIONES GENERALES

Este capítulo incluye un número de guías y conceptos de red básicos que nos ayudarán a organizar la estructura de nuestra red y en el diseño de redes redundante.

Un número de factores generales necesitan ser considerados cuando diseñamos redes redundantes, incluyendo:

- La confiabilidad y disponibilidad
- Redundancia de plataforma
- El nivel deseado de redundancia.

3.1.1 DEFINICIÓN DE CONCEPTO DE RED

El objetivo de una red de datos consiste en facilitar la consecución de un incremento de la productividad vinculando todas las computadoras y redes de computadoras de manera que los usuarios pueden tener acceso a la información con independencia del tiempo,ubicación y tipo de equipo informático.

Las redes de datos han cambiado nuestra forma de ver nuestras empresas y empleados. Ya no es necesario mantener una ubicación común para todos los empleados si se quiere acceder a la información que éstos necesitan para desarrollar su trabajo. Debido a esto hay muchas organizaciones que han cambiado sus

estrategias comerciales para utilizar estas redes de la forma en que llevan a cabo su actividad empresarial. Hoy día es frecuente que una empresa organice el *internetworking* corporativo de tal forma que permita optimizar sus recursos. La Figura 3.1.1.1 muestra que la red está definida en función de agrupaciones de empleados (usuarios), siguiendo los siguientes criterios:

- La oficina principal es aquella donde todos están conectados a una LAN y donde está ubicada la mayoría de la información corporativa. Una oficina principal podría contar con cientos o miles de usuarios que dependen de la red para desarrollar su trabajo. La oficina principal podría consistir en un edificio con muchas redes de área local (LAN), o bien en un campus de edificaciones de ese estilo. Dado que todos los usuarios necesitan acceder a recursos e información centralizados, es habitual encontrarse con una LAN *backbone* de alta velocidad, así como un centro de datos general con computadoras mainframe y servidores de aplicaciones.
- Las demás conexiones consisten en una diversidad de ubicaciones de acceso remoto que necesitan conectarse a los recursos de las oficinas principales y/o entre ellas incluidas las siguientes:
- **Sucursales**. Se trata de ubicaciones remotas donde trabajan grupos más reducidos de individuos. Estos usuarios se conectan entre sí por medio de una LAN. Para acceder a la oficina principal, los usuarios utilizan servicios de redes de área amplia (WAN). Aunque parte de la información podría estar almacenada en la sucursal, lo más probable es que los usuarios tengan que acceder a la mayoría de los datos desde

la oficina principal. La frecuencia con la que se accede a la red de la oficina principal determina si las conexiones WAN deben ser permanentes, o bien mediante acceso telefónico.

- **Teletrabajadores**. Se trata de empleados que trabajan desde sus domicilios.Estos usuarios requieren, generalmente, conexiones puntuales (bajo demanda) con la oficina principal y/o la sucursal para acceder a los recursos de red.
- **Usuarios móviles**. Se trata de individuos que trabajan desde distintas ubicaciones y dependen de distintos servicios para poder conectarse a la red. Cuando están en las oficinas principales o sucursales, estos usuarios se conectan a la LAN. Cuando se encuentran fuera de la oficina, normalmente dependen de servicios de acceso telefónico para conectarse a la red corporativa.

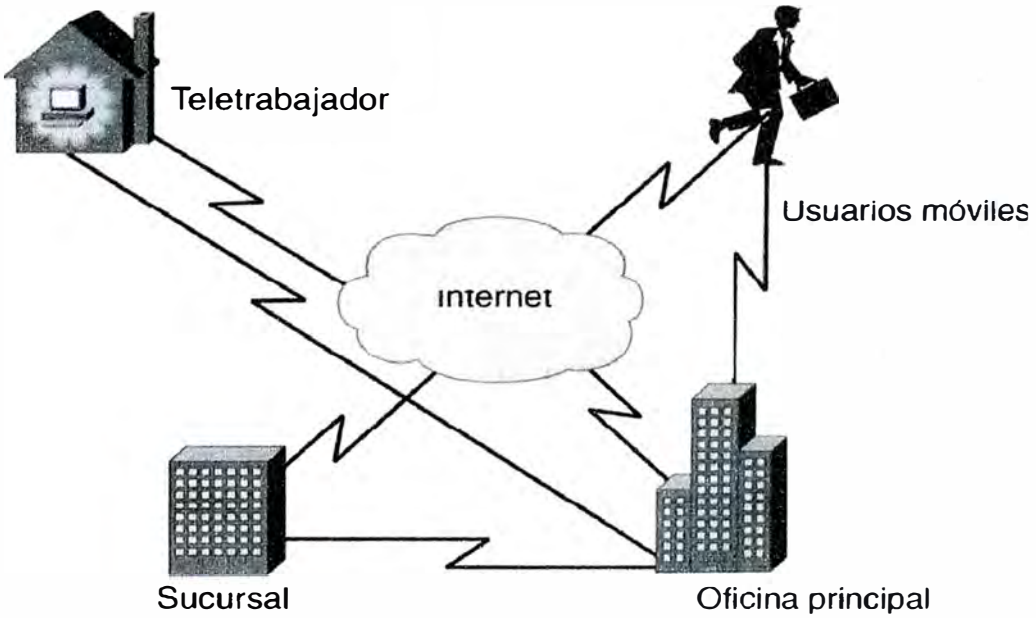


Figura 3.1.1.1 Estrategia de redes corporativas.

Para conocer los tipos de equipos y servicios que es necesario implementar en una red y cuándo deben utilizarse, es importante tener en cuenta las necesidades comerciales y de los usuarios.Esto permite subdividir la red en un modelo jerárquico que se expande desde el equipo de un usuario final hasta el núcleo (Backbone) de la red. La Figura 3.1.1.2 ilustra la interconexión entre diferentes grupos de empleados.

Para subdividir un internetworking de redes en componentes más pequeños, fabricantes como Cisco y Nortel Networks utilizan un modelo jerárquico de tres niveles (capas), como describiremos a continuación.

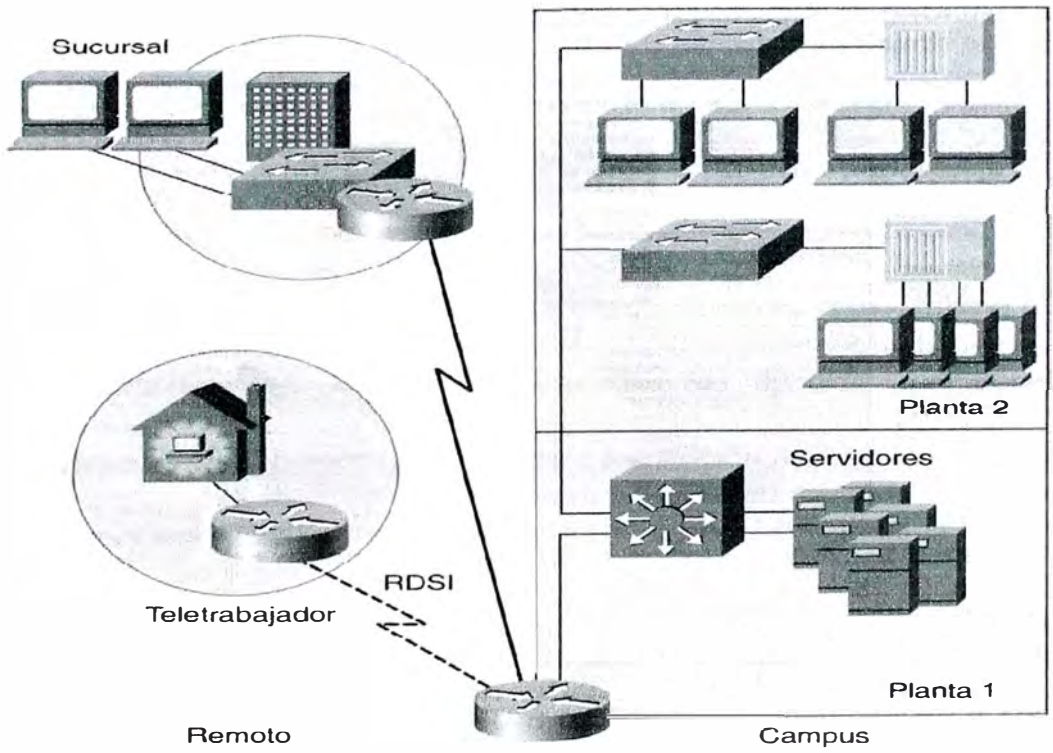


Figura 3.1.1.2 Interconexión de grupos.

3.1.2 ADAPTACIÓN DE LAS NECESIDADES DE EMPRESA A UN MODELO JERÁRQUICO

Con el fin de simplificar el diseño, implementación y administración de las redes, fabricantes como Cisco y Nortel Networks utilizan un modelo jerárquico para describir la red. Aunque la práctica de este método suele estar asociado con el proceso de diseño de la red, es importante comprender el modelo para poder determinar el equipo y características que se van a necesitar en la red.

Tradicionalmente, las redes de campus han colocado la logística y servicios básicos a nivel de red en el centro de la red, compartiendo el ancho de banda a nivel de usuario. Sin embargo, conforme el desarrollo comercial se va apoyando cada vez más en la red como herramienta de productividad, los servicios de red distribuidos y la conmutación van migrando hasta el nivel de puesto de trabajo.

Las demandas del usuario y las aplicaciones de red han obligado a los profesionales de las redes a utilizar patrones de tráfico en la red como criterio para construir un *internetworking*. Las redes no pueden ser divididas en subredes basándose únicamente en el número de usuarios. La aparición de servidores capaces de ejecutar aplicaciones globales tiene también una incidencia directa en la carga de la red. Un tráfico elevado en la red global supone tener que emplear técnicas de enrutamiento y conmutación más eficaces.

Los patrones de tráfico son hoy día los que dictan el tipo de servicios necesarios para los usuarios finales de la red. Para construir correctamente un internetworking de redes que pueda dar una respuesta eficaz a las necesidades de uniusuario, se utiliza un modelo jerárquico de tres capas para organizar el flujo del tráfico (Ver Figura 3.1.1.3).

El modelo consta de tres capas:

- Acceso.
- Distribución
- Núcleo principal

Cada una de estas capas tiene una función en el suministro de servicios de red, como se describe a continuación.

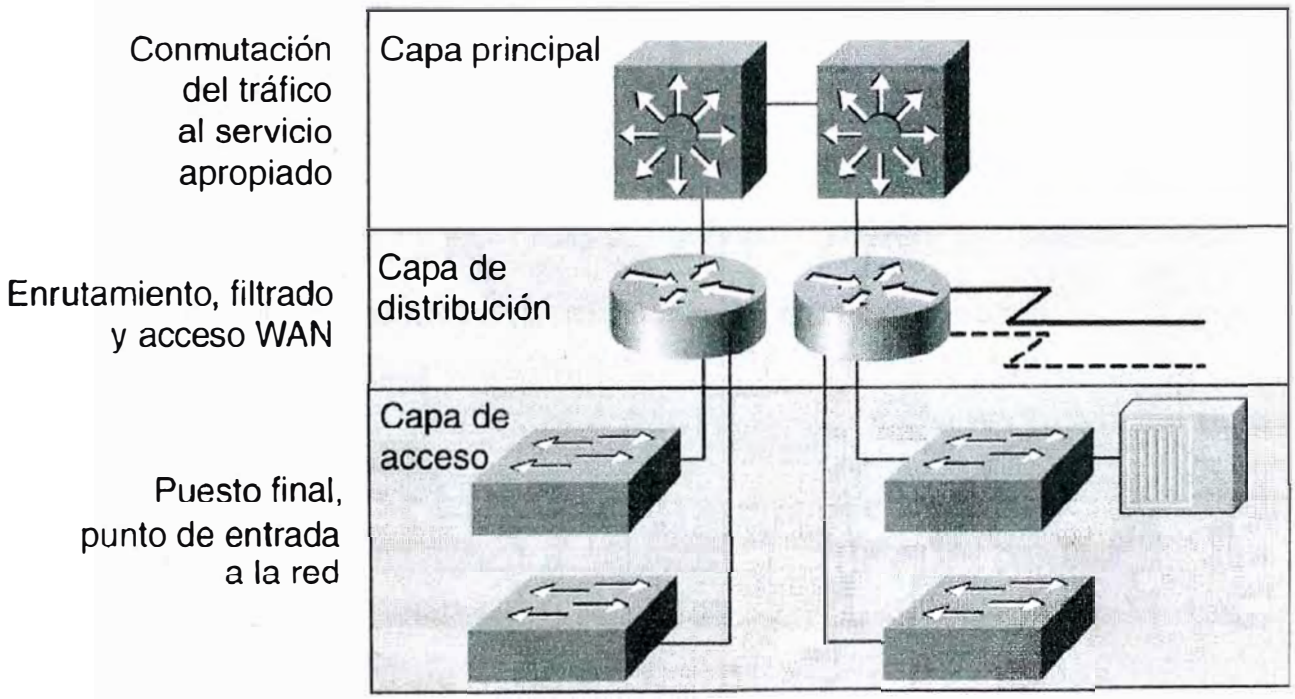


Figura 3.1.1.3 Modelo jerárquico de red basado en tres capas

- **Capa de Acceso**

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Esta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo. Los usuarios, así como los recursos a los que éstos necesitan acceder con más frecuencia,están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales.En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos.

En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de base de datos, almacenamiento centralizado o acceso telefónico al web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

- **Capa de distribución**

La capa de distribución de la red (denominada a veces capa de grupo de trabajo) marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN. En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

  - Servir como punto de acumulación para acceder a los dispositivos de capa.
  - Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.

- Segmentar la red en múltiples dominios de difusión/multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquetes pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa del núcleo principal. La capa principal podrá entonces traspasar rápidamente la petición al servicio apropiado.

- **Capa del núcleo principal ("Core")**

La capa del núcleo principal (también llamado capa *backbone*), se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos ejemplos de tales servicios pueden ser el e-mail, el acceso a Internet o la videoconferencia.

Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte

rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado al núcleo.

Para construir una red de forma eficaz, es necesario entender en primer lugar cómo se utiliza el *internetworking* de redes, las necesidades corporativas y las demandas de los usuarios. Estas necesidades pueden ser adaptadas a un modelo que pueda usarse para construir el *internetworking* de redes.

Una de las mejores formas de comprender cómo construir un *internetworking* de redes pasa por asimilar la forma en que el tráfico circula a través de la red. Esto se consigue por medio de un marco de trabajo de red conceptual, el más popular de los cuales es el modelo de referncia OSI.

3.1.3 EL MODELO DE REFERENCIA OSI

El modelo de referencia OSI ofrece varias funciones a la comunidad que participa del *internetworking*:

- Proporciona una forma de entender cómo opera un *internetworking* de redes.
- Sirve de guía o marco de trabajo para crear e implementar estándares de red, dispositivos y esquemas de *internetworking*.

Estas son algunas de las ventajas de utilizar un modelo estructurado en capas:

- Separa la compleja operación del *internetworking* en elementos más simples.

- Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares.
- Proporciona la posibilidad de definir interfaces estándar para compatibilidad "plug and –play" e integración multifabricante.

Como ilustra la Figura 3.1.1.4, el modelo de referencia OSI consta de siete capas. Las cuatro capas de nivel inferior definen rutas para que los puestos finales puedan conectarse unos con otros y poder intercambiar datos. Las tres capas superiores definen cómo han de comunicarse las aplicaciones de los puestos de trabajo finales entre ellas y con los usuarios.

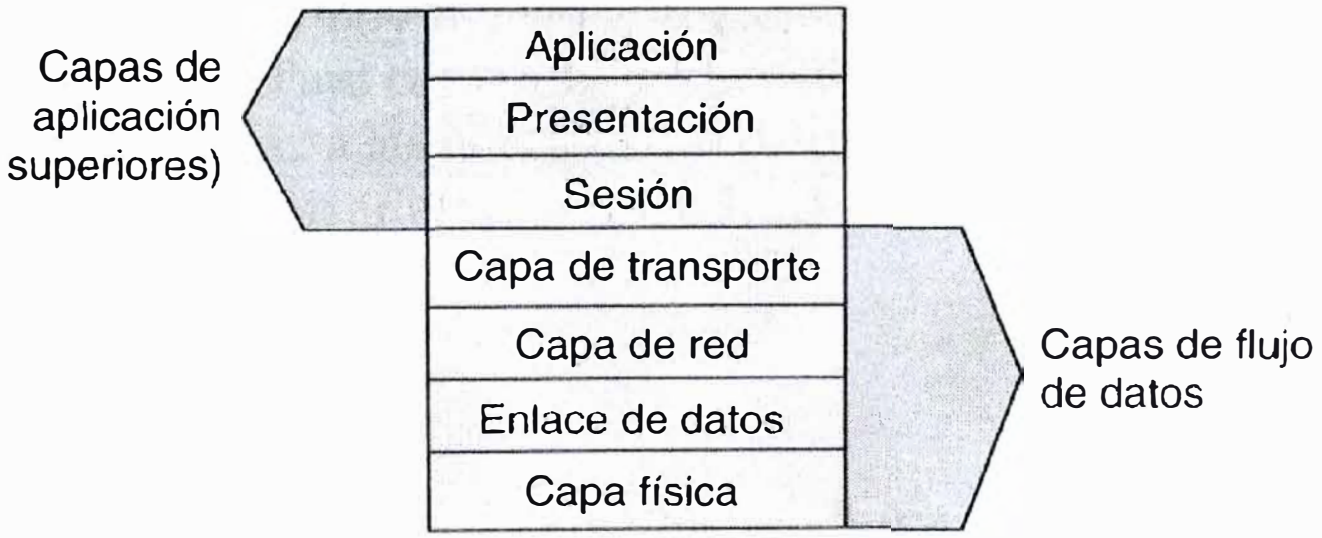


Figura 3.1.1.4 Modelo de referencia OSI.

- **Capas Superiores**

Las tres capas superiores del modelo de referencia OSI se denominan habitualmente capas de **aplicación**. Estas capas están relacionadas con la interfaz de usuario, formato de datos y acceso a las aplicaciones. La Figura 3.1.1.5 ilustra las capas superiores y proporciona información acerca de su funcionalidad con algunos ejemplos.

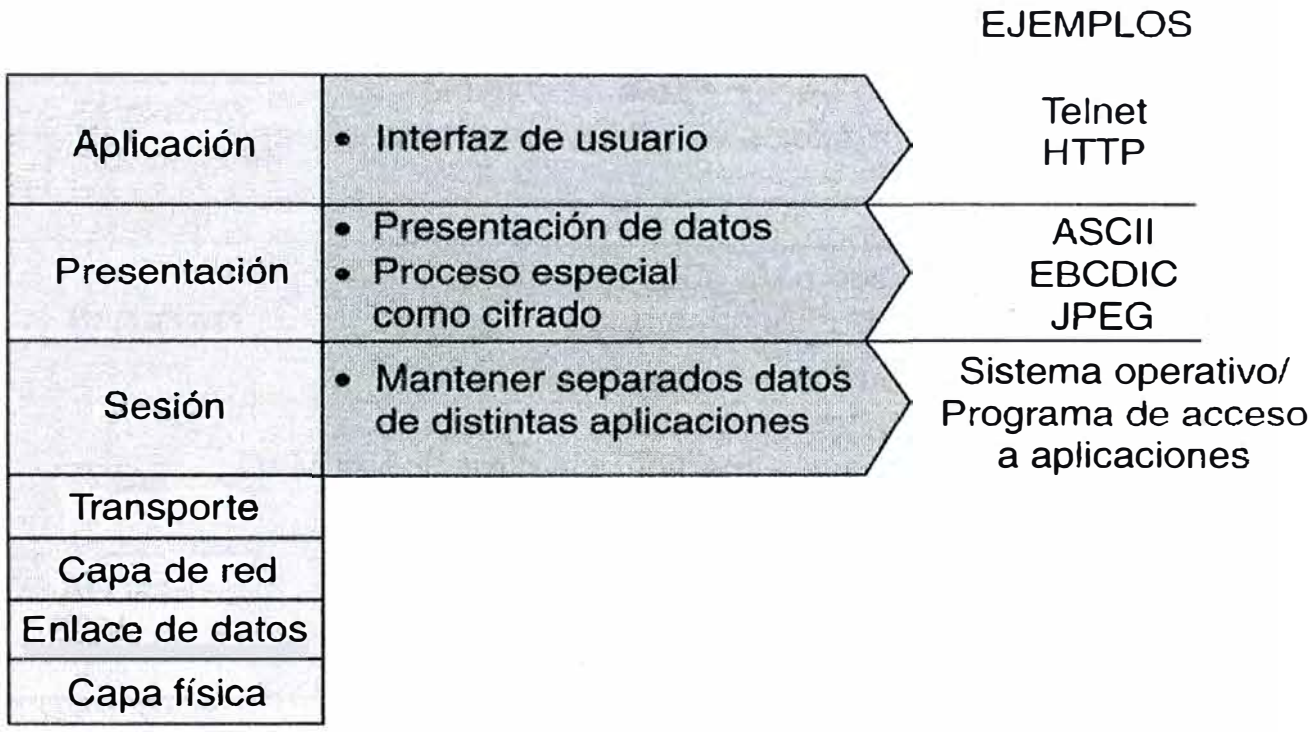


Figura 3.1.1.5 Capas superiores

- **Capas Inferiores**

Las cuatro capas inferiores del modelo de referencia OSI son las responsables de definir cómo han de transferirse los datos a través de un cable físico, por medio de dispositivos de internetworking, hasta el puesto de trabajo de destino y finalmente, hasta la aplicación que está al otro lado. La Figura 3.1.1.6 resume las funciones básicas de estas cuatro capas.

		Ejemplos
Aplicación Presentación Sesión		
Transporte	• Distribución fiable o no fiable • Corrección de errores antes de enviar	TCP UDP SPX
Red	• Proporcionar direccionamiento lógico para que los routers determinen las rutas	IP IPX
Enlace de datos	• Combinar bits en bytes y bytes en tramas • Acceso a medios con direcciones MAC Detectar (no corregir) errores	802.3 / 802.2 HDLC
Física	• Trasladar bits entre dispositivos • Especificar voltaje, velocidad y patillaje del cable	EIA/TIA-232 V.35

Figura 3.1.1.6 Capas inferiores.

3.2 CONFIABILIDAD Y DISPONIBILIDAD DE LAS REDES

Un sistema de red de datos robusto depende de los sistemas de hardware y software interactuando juntos. En el caso del software podemos dividirlo en tres niveles como muestra la Figura 3.2.1

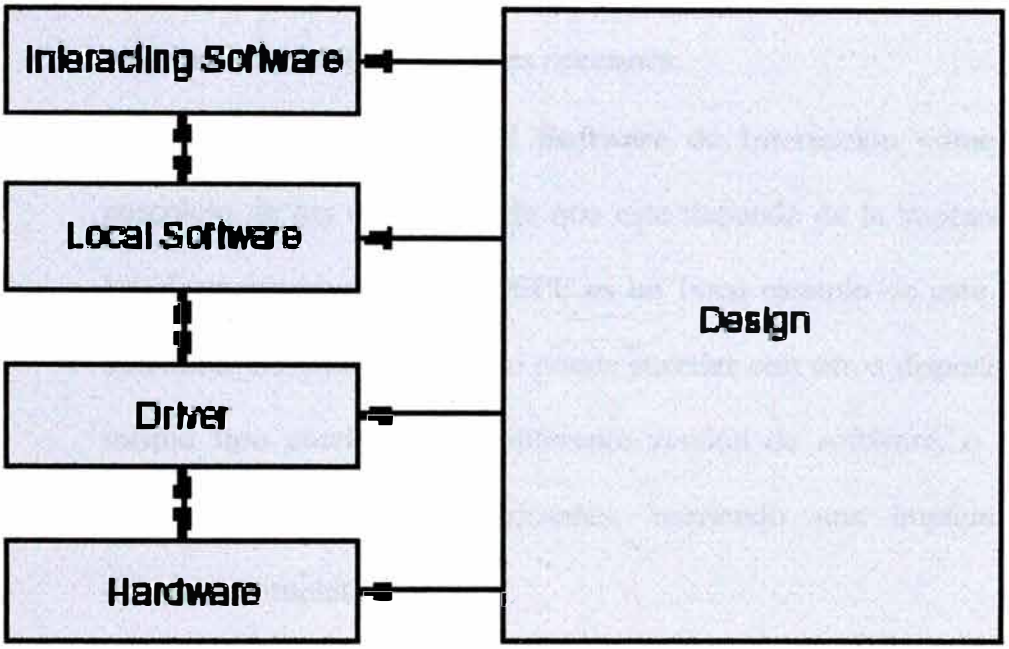


Figura 3.2.1 Confiabilidad del Hardware y Software

Estos niveles están basados sobre las funciones actuales del software. Por ejemplo:

- Podemos ver a los "**Drivers**" como el nivel más bajo del software que realmente realiza cualquier función. Los Drivers residen en un único

módulo sin interactuar con otros módulos, o incluso dispositivos externos. Por consiguiente, podemos considerarlos que están siendo muy estable.

- Podemos ver un MultiLink Trunk (MLT) como un primer ejemplo de **Software Local** desde que funcionalmente este debe tener que interactuar con varios módulos, pero aun en el mismo dispositivo. Podemos probar sus funciones en un modo más fácil desde que ninguna interacción externa es necesaria.
- Finalmente podemos ver el Software de Interacción como el más complejo de los niveles desde que este depende de la interacción con los dispositivos externos. OSPF es un buen ejemplo de este nivel de software. La interacción aquí puede suceder con otros dispositivos del mismo tipo corriendo una diferente versión de software, o aún con dispositivos de otros fabricantes, corriendo una implementación diferente completamente.

Basado en las estadísticas de los seguimientos de los problemas de red, el siguiente modelo de estimación de estabilidad aproximada de estos componentes ha sido desarrollado:

- El Hardware y los drivers representan una porción pequeña de los problemas.
- El Software Local representa una mayor compartición significante.
- El Software de interacción representa la inmensa mayoría de los problemas reportados.

Basado en este modelo, podemos debidamente concluir que esto tenga sentido para el diseño de la red para que el Software de interacción actúe fuera de carga colocándolo como sea posible en otros componentes, especialmente a nivel de hardware. Dado esa realidad, es recomendado que sigamos las siguientes reglas genéricas cuando diseñamos redes:

- El diseño de las redes debe ser tan simple como sea posible.
- Proveer redundancia, pero no sobre diseñar o hacer complejo su red.
- Usar herramientas de diseño para diseñar su red.
- Diseñar de acuerdo a las capacidades del producto, descrita en las notas con que viene cada producto. En este proyecto, que se implementó utilizando los switches de la serie Passport hemos usado por ejemplo el "*Release Notes for the Passport 8000 Series Switch*"
- Seguir las reglas de diseño proveídas con la documentación del producto y aplicando los conceptos de redes. En este caso siempre enfocando a los switches de la serie Passport con que se implementó este proyecto, hemos usado documentos como "*Passport 8000 Series Design Guidelines Release 3.2 Implementation Notes*" y "*Networking Concepts for the Passport 8000 Series Switch*".

- **La Capa Física**

La capa física incluye:

- Distancias de cables Ethernet
- Autonegociación
- Gigabit e Indicación de fallas remotas.

- **Distancias de cables Ethernet**

La tabla 3.2.1 y tabla 3.2.2 listan las distancias de cables para Ethernet 10/100 y Gigabit Ethernet 1000BASE-TX. La tabla 3.2.3 presenta la distancia de cables mínima estándar para Gigabit Ethernet 1000BASE-SX,LX,XD y ZX. Note que la Tabla 3.2.3 representa la mínima distancia asequible sobre fibra de buena calidad.

	Ethernet 10BASE-T	Fast Ethernet 100BASE-TX	Fast Ethernet 100BASE-FX
Estándar IEEE	802.3 Cláusula 14	802.3 Cláusula 21	802.3 Cláusula 26
Date rate	10 Mbps	100 Mbps	100 Mbps
Distancia con Fibra Multimodo	N/A	N/A	412 m (Half-Duplex) 2 Km (Full-Duplex)
Distancia con cable UTP CAT 5	100 m.	100 m.	N/A
Distancia con cable STP/Coax.	500 m	100 m.	N/A

Tabla 3.2.1 : Distancia de cables para Ethernet 10/100

	1000BASE-T
Estándar IEEE	802.3ab Cláusula 40
Date rate	1000 Mbps
Distancia con cable UTP CAT 5 de 100 ohmios	100 m.
Distancia con cable STP de 150 ohmios	N/A
Numero de pares de hilos	4 pares
Tipo de conector	RJ-45

Tabla 3.2.2 : Distancia de cables para Gigabit Ethernet 1000BASE-TX

Transcv	Tipo de Fibra	Diam. (Mcrs)	Longitud de Onda	Ancho de Banda Modal (Km)	Rango Mínimo (metros)
1000BASE-SX	MMF	62.5	850 nm	160	2 a 220
1000BASE-SX	MMF	62.5	850 nm	200	2 a 275
1000BASE-SX	MMF	50	850 nm	400	2 a 500
1000BASE-SX	MMF	50	850 nm	500	2 a 550
1000BASE-LX	MMF	62.5	1300 nm	500	2 a 550
1000BASE-LX	MMF	50	1300 nm	400	2 a 550
1000BASE-LX	MMF	50	1300 nm	500	2 a 550
1000BASE-LX	SMF	9	1300 nm	N/A	2 a 10000
1000BASE-XD	SMF	9	1300 nm	N/A	2 a 50 Km
1000BASE-ZX	SMF	9	1300 nm	N/A	2 a 70 Km

Notas :

- MMF = Fibra Multimodo "Multimode Fiber"
- SMF = Fibra Monomodo "single-mode Fiber"
- El 802.3z especifica tres requerimientos de capa fisica:

  1000BASE-SX (SX = "Short Wavelength Laser o Short Wavelength Optical"),

  1000BASE-LX (LX= "Long Wavelength Laser o Long Wavelength Optical") y el

  1000BASE-CX (CX= "Short Haul Copper") que usa cable STP tipo 2.
- El estándar IEEE para 1000BASE-SX es 802.3 cláusula 38.3
- El estándar IEEE para 1000BASE-LX es 802.3 cláusula 38.4 .Notar que 1000BASE-XD Y 1000BASE-ZX no son estándar de la IEEE.

Tabla 3.2.3 : Rangos de distancias mínimo para el estándar Gigabit Ethernet

- **Autonegociación**

Autonegociación es una técnica, especificada como parte del estándar IEEE802.3u para Fast Ethernet, que habilita dos dispositivos que comparten un enlace común a anunciar sus velocidades y capacidades de modo duplex, reconozcan al receptor y entiendan los modos compartidos de operación y rechacen los modos de operación que no son compartidos.

La autonegociación esta diseñada para proveer tanto configuración automática y manual. Este permite configuración automática de ambos extremos de un enlace punto a punto sin la ruptura de la red. El principal beneficio de la característica de la autonegociación es la habilidad de acomodarse a los máximos recursos de cada nodo. El protocolo de autonegociación permite que los nodos descubran y reconozcan sus capacidades de operación mutua para establecer una conexión con el más alto denominador común de funcionalidades.

Los productos que soportan esta característica negocian las velocidades y modos duplex de acuerdo al estándar de autonegociación IEEE802.3u. Un hub o modulo host usa la información de modo de operación anunciada por el enlace remoto y ajusta (autonegocia) su velocidad de puerto para que concuerde con el mejor servicio proveído por la estación conectada, hasta 100 Mbps full-duplex. Es importante que para realizar esto que no es esencial que ambos extremos del enlace soporten autonegociación para que el enlace trabaje.

La autonegociación permiten que los dispositivos conmuten entre modos operacionales de una forma ordenada, permite la administración para deshabilitar o habilitar la función de autonegociación y permite la administración para seleccionar un modo operacional especifico. La función de autonegociación también provee una

detección paralela (por lo que es llamado "auto sensing") para permitir que dispositivos compatibles 10BASE-T, 100BASE-TX y 100BASE-T4 sean reconocidos, aunque ellos no provean autonegociación. En este caso solo la velocidad puede ser censada pero no el modo duplex. La tabla 3.2.4 muestra la configuración de autonegociación recomendada sobre puertos 10/100BASE-TX, con respecto a la <Figura 3.2.2

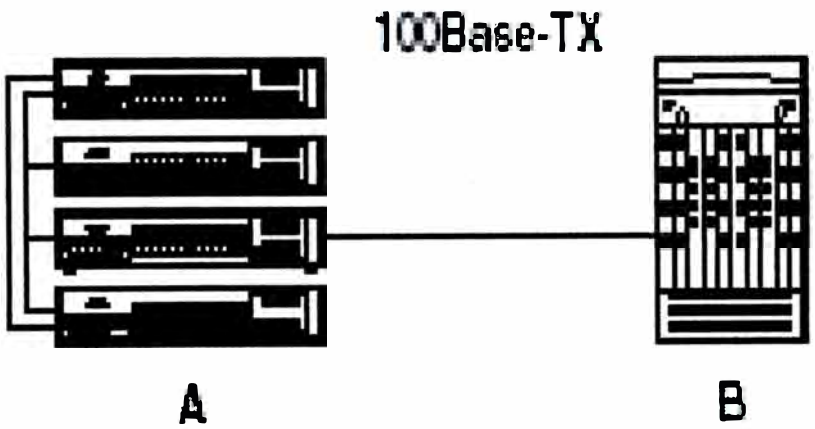


Figura 3.2.2 Proceso de Autonegociación

Puerto en A (Figura 3.2.2)	Puerto en B (Figura 3.2.2)	Comentario	Recomendaciones
Autonegociación	Autonegociación	Los puertos se anulan sobre el modo soportado más alto en ambos lados	Configuración recomendada si ambos puertos soportan el modo de autonegociación
Configuración Fija: Full Duplex	Configuración Fija: Full Duplex	Ambos lados requieren el mismo modo	Configuración recomendada si full duplex es requerido, pero la autonegociación no es soportada.
Configuración Fija: Half Duplex	Autonegociación	El modo debe ser configurado en half-duplex desde que la autonegociación en el puerto no puede detectar el modo duplex.La velocidad puede ser sensada.La autonegociación en los puertos por default es half.	10 half duplex recomendado sobre el lado fijo

Tabla 3.2.4 : Configuración de autonegociación recomendada sobre puertos 10/100BASE-TX

- **Gigabit e Indicación remota de falla**

El estándar 802.3z (Gigabit Ethernet) incorpora la capacidad de falla remota, permitiendo así que un puerto descubra una falla (por ejemplo recibir par desconectado → enlace caído en un lado) para transferir esta información de regreso a través del enlace. El algoritmo de autonegociación incluye capacidades de

indicación de falla remota. Por consiguiente, es recomendado, si es posible, que habilitemos la autonegociación sobre enlaces Gigabit en todos los casos.

3.3 PLATAFORMA REDUNDANTE

Es recomendado que usemos los siguientes mecanismo para llevar redundancia a nivel de dispositivos.:

- **Fuente de alimentación redundante**

  Debemos emplear redundancia de fuentes de alimentación en configuración N + 1. (N es el número de fuentes de alimentación requerida para dar energía al chasis y sus tarjetas). Debemos también conectar la s fuentes de alimentación a una línea adicional de energía para protegerse contra problemas de energía.

  Los switches de la serie Passport de Nortel Networks con que se implementó este proyecto soportan hasta 3 fuentes de alimentación redundantes con compartición de carga, además tienen dos bandejas de ventiladores cada una con 8 ventiladores individuales. Sensores son usados para monitorear la salud de la tarjeta.

- **Redundancia de puertos de entrada/salida (I/O)**

  Podemos proteger los puertos I/O usando mecanismo de agregación de enlaces. MLT (Multilink Trunk), propietario de Nortel Networks pero compatible con el estándar 802.3ad estático (LACP deshabilitado), nos provee compartición de carga y mecanismo de

failover para protegernos contra fallas de modulo, puerto, fibra o enlaces completos.

MLT entonces, es un método de agregación de enlaces que permite múltiples troncales ethernet sean agregados juntos para proveer un único troncal lógico. Un MLT provee el ancho de banda combinado de los múltiples enlaces, así como también la protección de la capa física contra falla de cualquier enlace único.

En redes conmutadas, los switches pueden tener redundancia de enlaces unos con otros. Debido a que los switches implementan el algoritmo de spanning tree IEEE 8021d, los lazos pueden ser evitados.El algoritmo de spanning tree garantiza que haya uno y solo una ruta activa entre dos estaciones de red. El algoritmo permite rutas redundantes que son automáticamente activadas cuando la ruta activa experimenta problemas.

Cuando combinamos MLTs y STGs, notar que el protocolo spanning tree trata a los MLTs como otro enlace que puede ser bloqueado. Si dos grupos de MLT conectan dos dispositivos y pertenecen al mismo grupo de spanning tree (STG), el protocolo spanning tree bloquea uno de los grupos MLT para prevenir lazos.

- **Redundancia de "switch fabric"**

  Es recomendable que usemos dos "switch fabric" (SFs) para protegerse contra fallas de "switch fabric". Los dos SFs comparten carga y también proveen respaldo una para el otro. En caso de una falla de un SF, el ancho total por slot es cortada a la mitad. Todos los

puertos sin embargo mantendrán el envío ("forwarding").

Si instalamos solo un SF, hay un total de ancho de banda de 4 Gbps full duplex por slot disponible. Con dos SFs, instalados, entonces 8 Gbps full duplex es disponible.

Los switches de la serie Passport de 10 slot de Nortel Networks con que se implementó este proyecto tienen dos slots para los módulos CPU/Switch Fabric (SF). Los slots 5 y 6 son reservados solo para los módulos SF. Un modulo CPU/Switch Fabric 8690SF es requerido para operación. Este modulo está optimizado para entregar una alta perfomance en el switching de tráfico en capa 2 y capa 3. Si un segundo modulo CPU/Switch Fabric es instalado, este provee redundancia de fail-over al primer modulo CPU/Switch Fabric. Además, los SSFs sobre ambos módulos CPU/Switch Fabric estan simultáneamente activo y por consiguiente comparten la conmutación de la carga de todos los puertos de los módulos de I/O, incrementando la capacidad de conmutación y throughput del core para proveer capacidades de "non-blocking" aun con 64 puertos Gigabit Ethernet instalados.

- **Redundancia de CPU**

  El CPU es el cerebro del switch. Este controla todo el aprendizaje, calcula los protocolos de enrutamiento y mantiene todos los estados de los puertos. Si el último CPU en un sistema falla, el estado de los puertos de I/O no cambian. En vez de eso, la información que ha sido programada dentro de los ASICs de envío "forwarding" es usada para

realizar decisiones de envío. No hay calculación de las actualizaciones del protocolo de enrutamiento activo, por lo que la convergencia de la red depende del tiempo de caducidad del protocolo de enrutamiento. Para protegerse contra falla de CPU, Nortel Networks fabricante de los equipos Passport con que se implemento este proyecto, ha desarrollado dos tipos diferentes de control de planes de control de protección de CPU:

-Modo estado de espera en caliente ("Warm standby")

En este modo, el CPU secundario esta esperando con la imagen del sistema cargado. Sin embargo, el archivo de configuración es cargado desde el sistema de archivos tan pronto como el CPU principal falle sobre el secundario.

-Modo estado de espera en caliente de alta disponibilidad (HA "Hot Standby high availability")

Este modo asegura que los CPU principal y secundario sincronicen sus configuraciones y tablas de protocolo. Este permite una toma de poder en caso de que un CPU falle, previniendo así la interrupción del tráfico de datos.

- **Redundancia de configuración e imagen**

  Los switches de la serie Passport 8000 con que se implemento este proyecto, nos permiten definir una configuración principal , secundaria y terciaria y rutas al archivo imagen del sistema. Esto protege contra fallas del sistema de flash. Por ejemplo, la ruta principal apunta a la /flash, el secundario apunta a la /pcmcia y la

terciaria a una ruta de red.

Ambas tarjetas CPU/SF son idénticas y soportan flash y almacenamiento PCMCIA. Si habitamos el comando para flag del sistema (**"save to standby").** aseguramos que los cambios de configuración sean siempre almacenado en ambos CPUs**.**

3.4 ESTRUCTURA FÍSICA PARA REDES REDUNDANTES

Cuando diseñamos redes, es recomendable que tomemos un acercamiento modular. Esto significa que debemos partir el diseño en diferentes secciones, las cuales pueden ser replicadas cuando sean necesarios, usando un modelo recursivo.

Necesitamos considerar varias entidades funcionales aquí, incluyendo acceso al usuario, agregación, core y acceso a los servidores.

- **Capa de acceso de usuario** – Puerto conmutado de acceso al usuario. Normalmente esta capa cubre el armario del cableado "wiring closet".
- **Capa de agregación** – La agregación de muchos switches de accesos al usuario o switches de "wiring closet" (W/C), esta capa es frecuentemente llamada capa de distribución, desde que este envuelve la distribución a los closets de cableado de los pisos.
- **Core "Núcleo"** – Interconexión entre diferentes puntos de agregación y granja de servidores.
- **Capa de acceso a los Servidores** – Conectividad a la granja de servidores, capa de recursos.

Notar que el diseño de nuestra red normalmente depende del diagrama físico de nuestro campus y del diagrama de los cables de fibra y cobre.

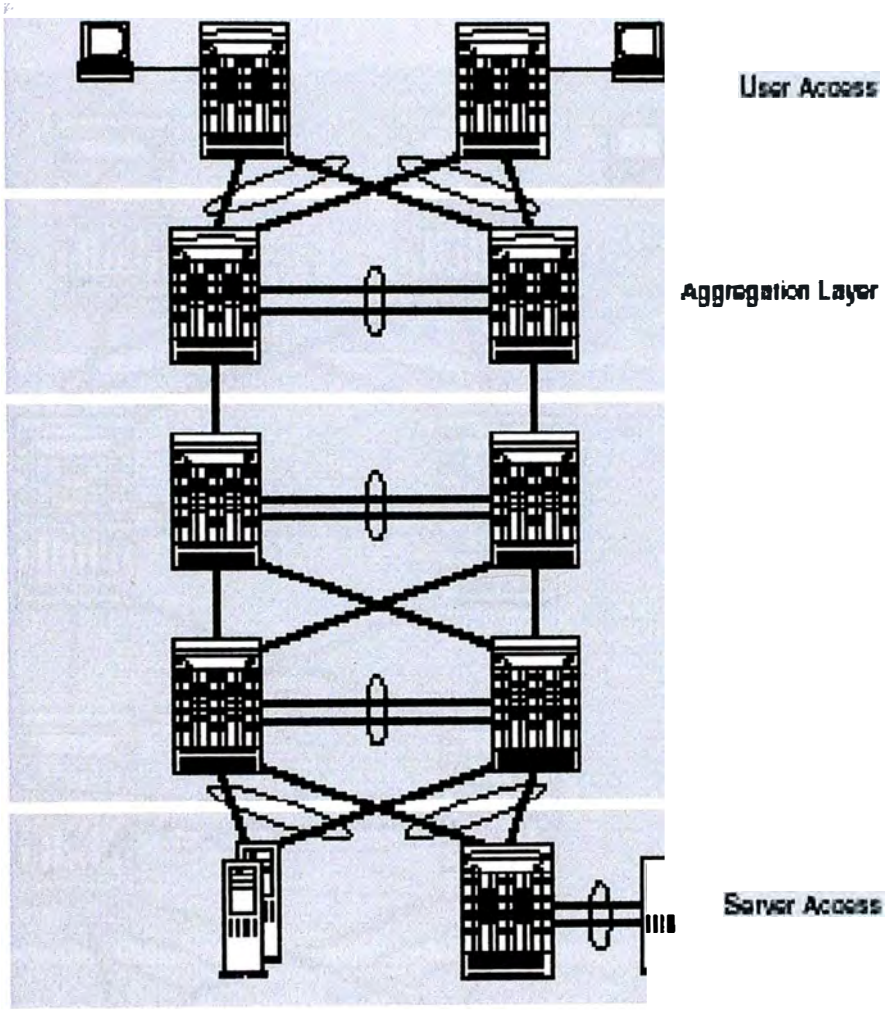


Figura 3.4.1 Diagrama de red de cuatro niveles

En muchos casos, podemos unificar las diferentes capas en un switch manteniendo la funcionalidad, pero decrementando el costo, complejidad y la latencia de la red. (ver figura 3.4.2)

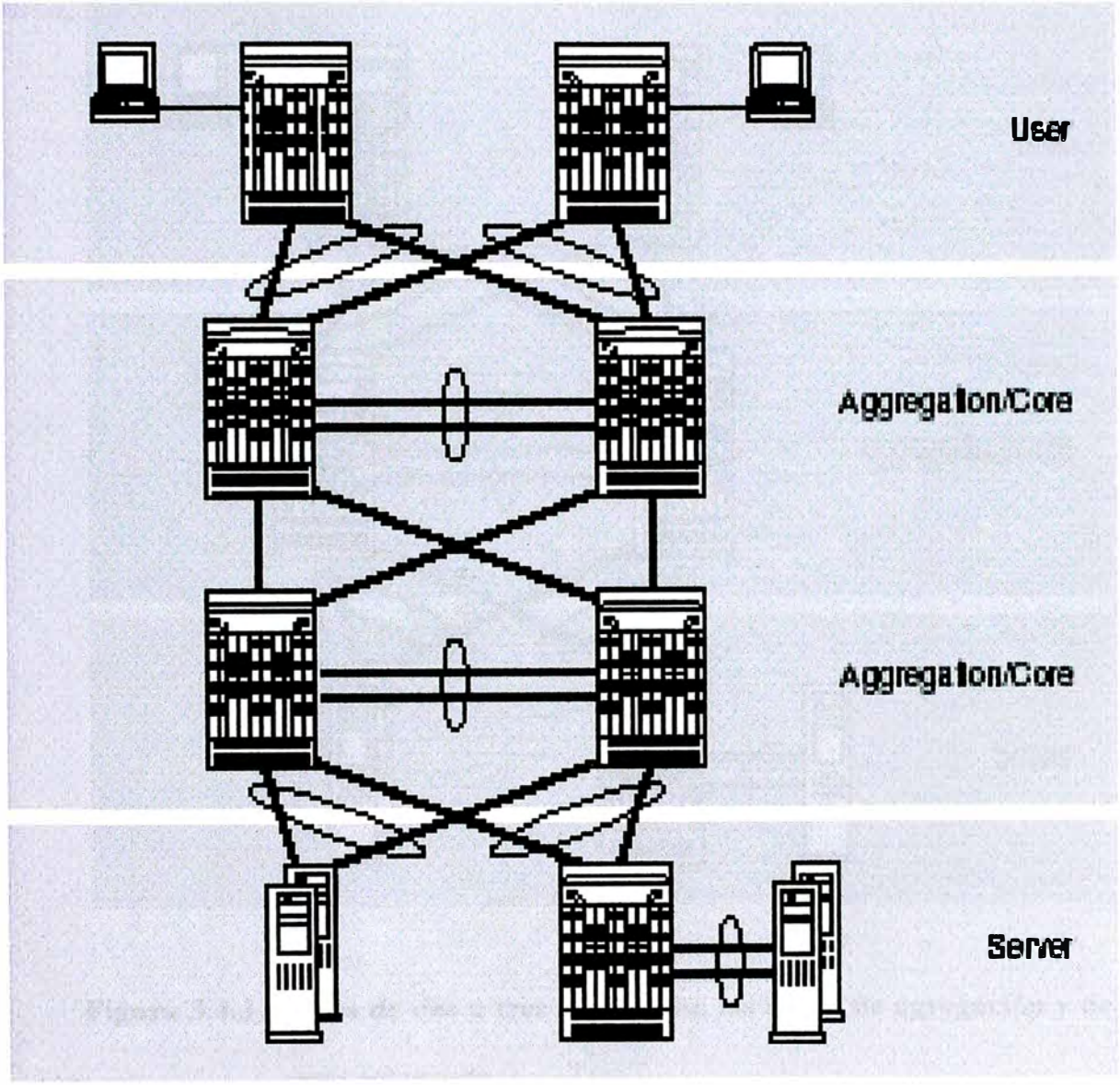


Figura 3.4.2 Diagrama de red de tres niveles.

Dependiendo del diagrama físico del cableado de Fibra y de los requerimientos de la densidad de puertos, las capas de acceso de los servidores y la de Core pueden ser implementadas en el mismo switch. (Figura 3.4.3)

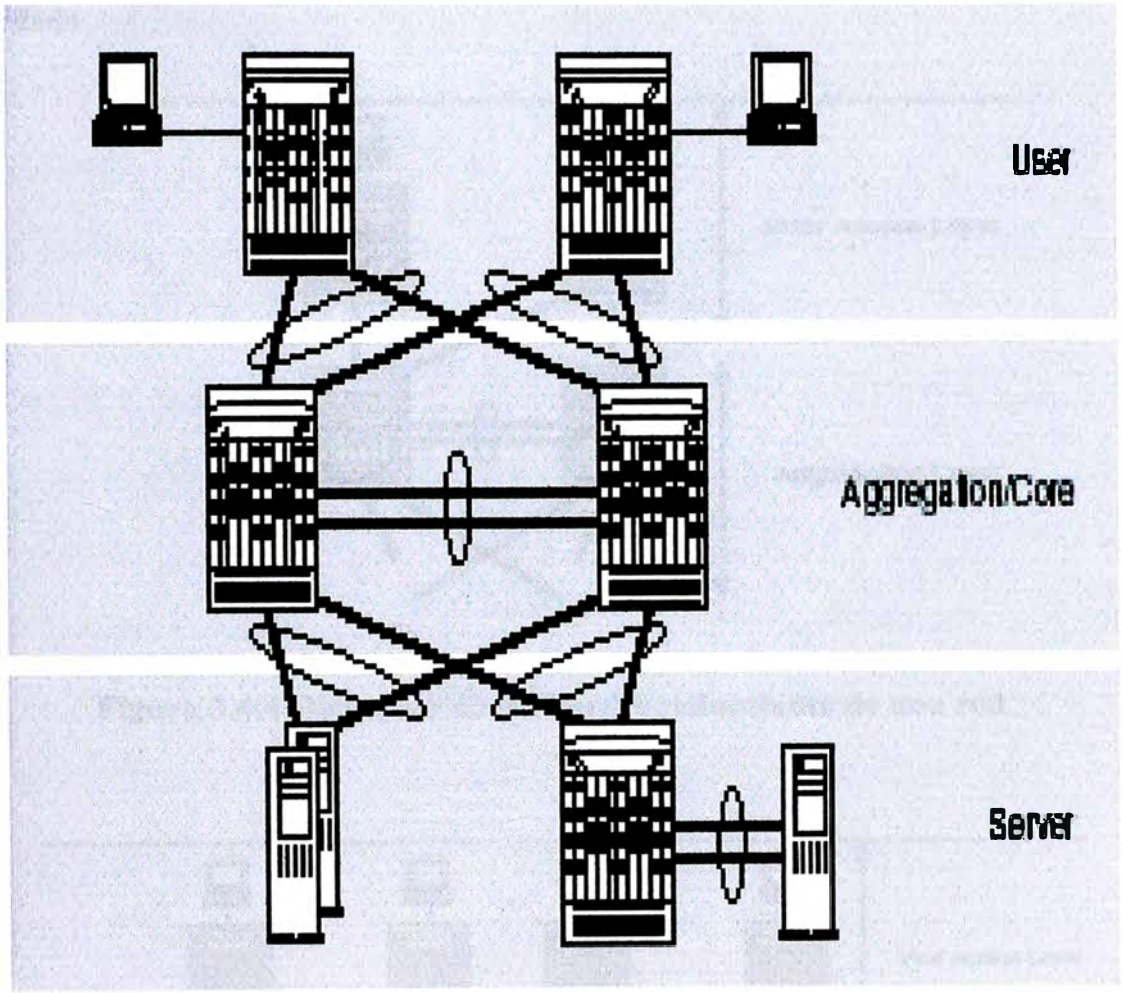


Figura 3.4.3 Redes de dos o tres niveles con las capas de agregación y de core colapsada

- **Redundancia de los bordes de la red**

La Figura 3.4.4 muestra un par de switches de agregación distribuyendo enlaces de subida "riser" a los armarios de cableado.

La figura 3.4.5 muestra una configuración de los bordes de una red recomendada.

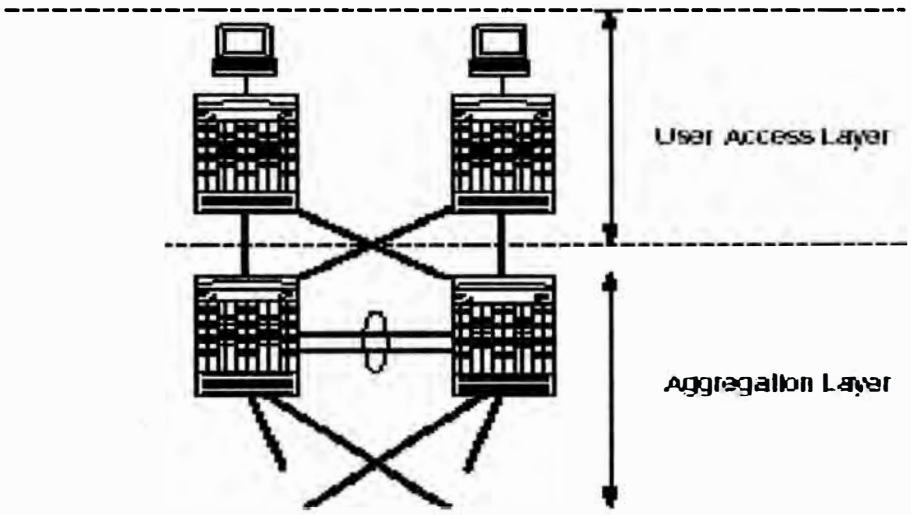


Figura 3.4.4 Diagrama de los bordes redundante de una red .

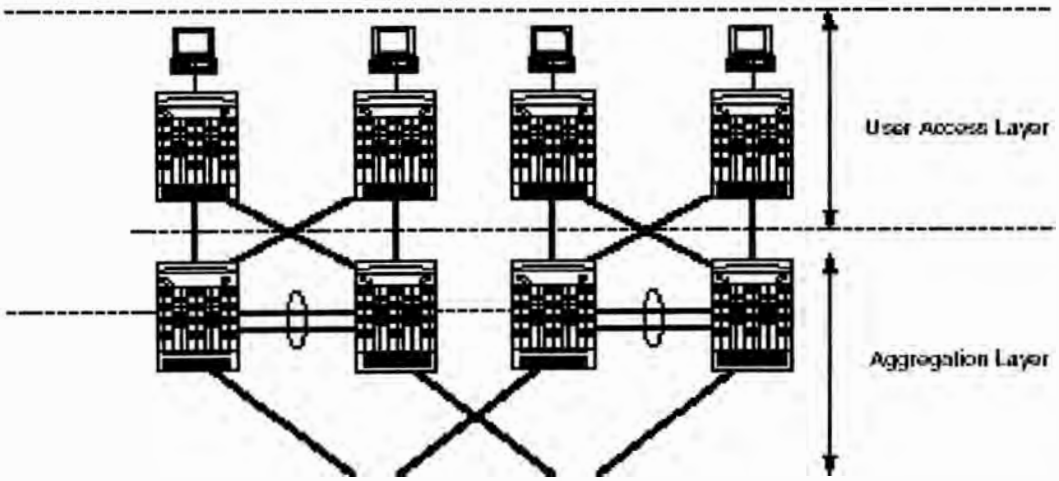


Figura 3.4.5 Diseño recomendado de los bordes de una red.

- **SMLT (Troncales multienlaces divididas, "Split Multilink Trunking")**

Aunque no se uso para el diseño de las redes de este proyecto, debido a que esta función recién salió con las recientes versiones de software de los switches Passport (versión 3.2 y posteriores) trataremos brevemente esta característica y sus ventajas para la implementación de redes redundantes en forma optima.

SMLT es definida como un MLT ("Multilink Trunking"), un extremo de los cuales es dividido entre dos switches de agregación.

Definiendo algunos términos básicos relacionados con el SMLT para comprender su funcionamiento, tenemos:

Switch de agregación SMLT – Un switch que conecta a múltiples switches del closet de cableado, switches de borde o dispositivos CPE, típicamente dentro de un único edificio.

IST ("Inter. Switch Trunk") - Uno o más enlaces paralelo que conectan juntos dos switches de agregación. Los dos switches de agregación utilizan este canal para compartir la información por lo que ellos pueden operar como un switch lógico único. Puede haber solo un IST por switch de agregación SMLT.

MLT ("Multilink Trunking")- Un método de agregación de enlaces que permite que múltiples troncales ethernet puedan ser agregados juntos para proveer una única troncal lógica.

Cliente SMLT – Un switch localizado en el borde de la red, tal como en un closet de cableado o CPE. Un switch cliente SMLT debe ser hábil para realizar agregación de enlaces (tal como MLT o algún otro método compatible) pero no requiere ninguna inteligencia SMLT.

La figura 3.4.6 muestra una configuración que incluye un par de switches Passport 8600, E y F como switches de agregación. Cuatro separados switches de closets de cableado son etiquetados como A,B,C y D (por ejemplo switches Passport 8100, switches Baystack450, switches BPS 2000 o cualquier otro dispositivo compatible con MLT).

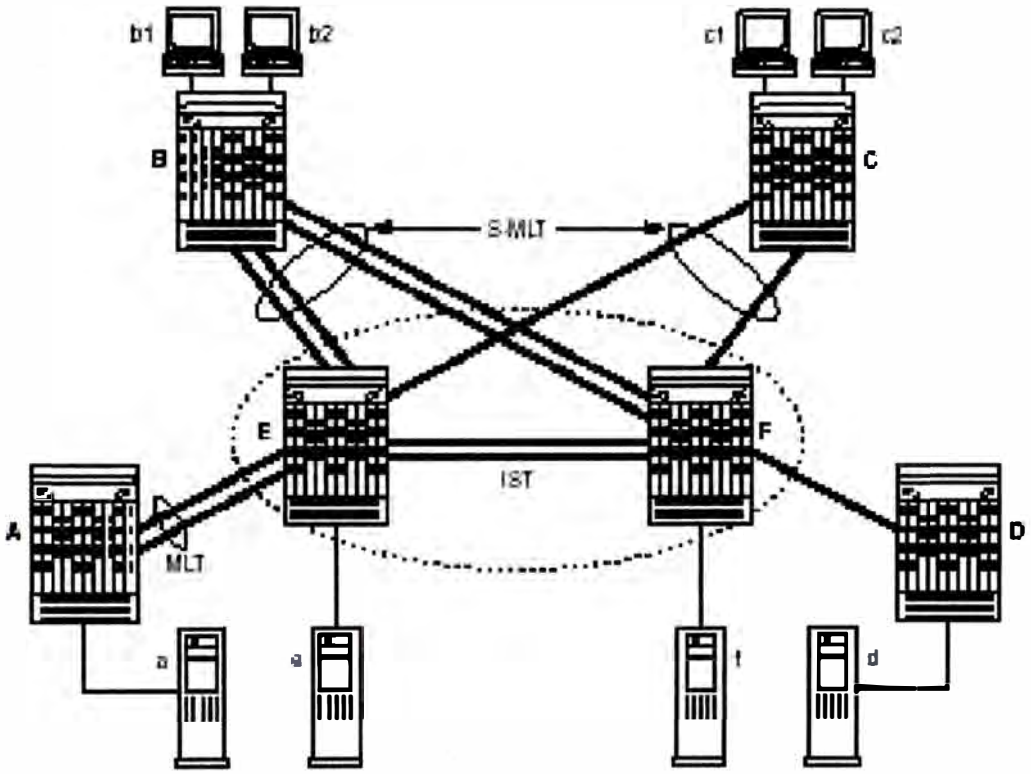


Figura 3.4.6 Configuración SMLT con switches Passport 8600 como switches de agregación

Los switches del armario de cableado B y C son conectados a los switches de agregación vía troncales multienlaces que son divididas entre los dos switches de agregación. Por ejemplo el switch cliente SMLT B puede usar dos enlaces paralelo para su conexión a E y dos enlaces paralelos adicionales para su conexión a F. El switch cliente SMLT C puede tener solo un único enlace tanto a E y F. Como muestra en la Figura 3.4.6, switch A también esta configurado con MLT, pero el MLT termina en solo un switch en el core de la red. El switch D tiene una única conexión al core. Aunque podemos configurar tanto el switch A como el switch D para que terminen a través de ambos switches de agregación usando SMLT, ningún switch podría beneficiarse del SMLT en la configuración displayada.

Enlace SMLT-IST – Como muestra la Figura 3.4.6, nuestra implementación de SMLT solo requiere dos switches de agregación con capacidad de SMLT. Podemos conectar estos switches vía un IST ("Inter Switch Trunk"). Los switches de agregación usan este canal de comunicación para dos procesos.

1. Confirmar que cada switch esta vivo así como también intercambiar información de direcciones MAC. Así el enlace debe ser confiable y no exhibir ningún punto de falla.
2. Para enviar fluido de paquetes o paquetes destinados a switches conectados no SMLT o servidores físicamente conectados a otros switches de agregación.

La cantidad de tráfico desde un closet de cableado SMLT el cual requiere envío a través del IST es probablemente pequeña. Sin embargo, si los switches de agregación son conexiones de terminación para dispositivos "single –home" o en el caso de fallas de enlaces de subida SMLT, el volumen del tráfico SMLT puede ser

significativo. Debido a esto es recomendable que el IST debe ser un MLT multi-gigabit con conexiones a través de diferentes tarjetas de línea sobre ambos switches de agregación para asegurar que no exista ningún punto de falla en el IST.

Enlace SMLT-SMLT- Los switches cliente SMLT son "dual-homed" para los dos switches de agregación, aún ellos no requieran el conocimiento de si ellos están conectados a un único switch o a dos switches. La inteligencia SMLT es requerida solo en los switches de agregación. Lógicamente, ellos aparecen como un único switch para los switches de borde. Por consiguiente, los switches cliente SMLT solo requieren una configuración MLT. La conexión entre los switches de agregación SMLT y los switches clientes SMLT es llamada enlaces SMLT.

La Figura 3.4.6 también incluye estaciones finales conectadas a cada uno de los switches a,b1,b2,c1,c2 y d que son típicamente hosts, mientras que e y f deben ser hosts, servidores o routers. Los switches cliente SMLT B y C pueden usar cualquier método para determinar cual enlace de sus conexiones troncales multienlaces usar para enviar un paquete. Esto es verdad todo el tiempo que el mismo enlace sea usado para un par Fuente /Destino (SA/DA), independiente de si o no el DA sea conocido por B o C.

Este requerimiento asegura que no habrá paquetes fuera de secuencia entre cualquier par de dispositivos de comunicaciones. Los switches de agregación siempre envían tráfico directamente a un switch cliente y solo usan el IST para tráfico que ellos no pueden enviar a otro por un camino más directo.

❑ EJEMPLOS DE DISEÑOS DE RED

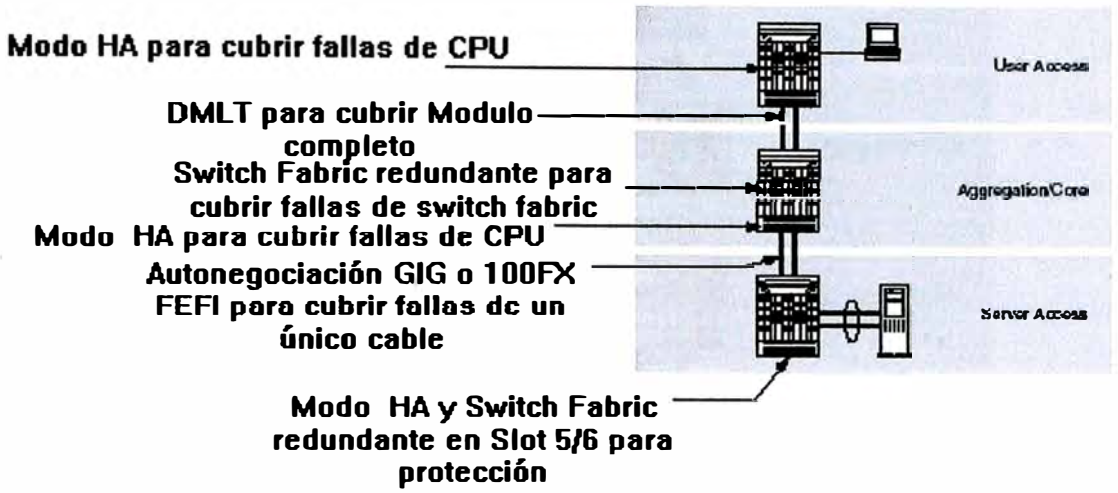
Presentamos a continuación una serie de ejemplos que nos ayudarán en el diseño de las capas relevantes de nuestra red:

- Ejemplos de Capa 1 nos conducen con diagramas de red físicos.
- Ejemplos de capa 2 mapean VLANs sobre los diagramas de red físicos.
- Ejemplos de capa 3 muestran casos de enrutamiento recomendado para optimizar redundancia de redes IP e IPX.

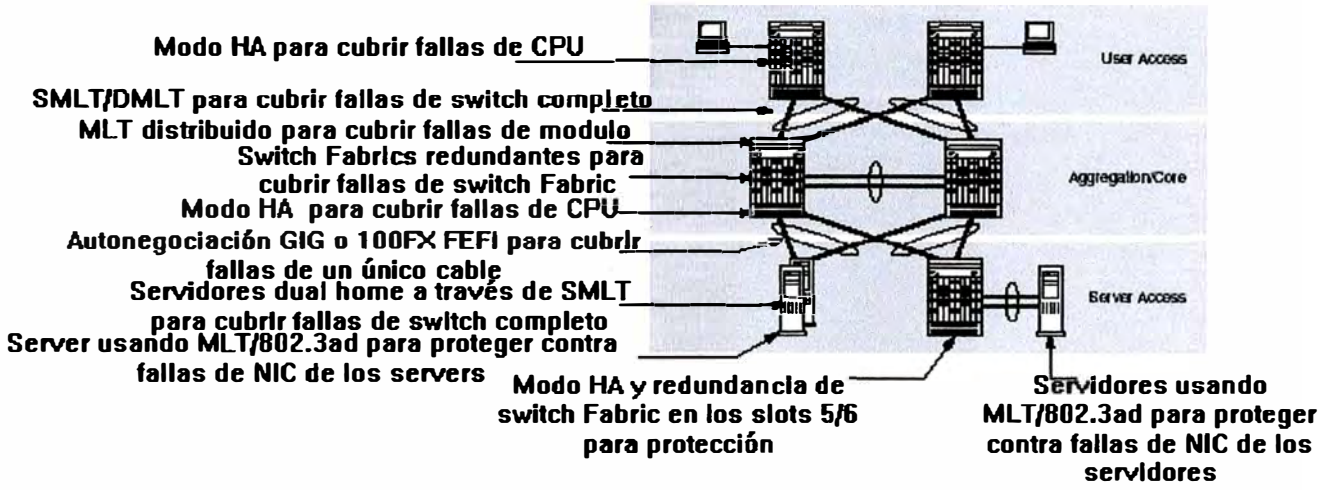
▪ Ejemplos de Capa 1

Las Figuras 3.4.7.1 y 3.4.7.2 contienen una serie de ejemplos de diseño capa 1 que ilustran el diagrama de red físico.

Basado en el ejemplo 2, todos los mecanismos de la redundancia en capa 1 son descrita.

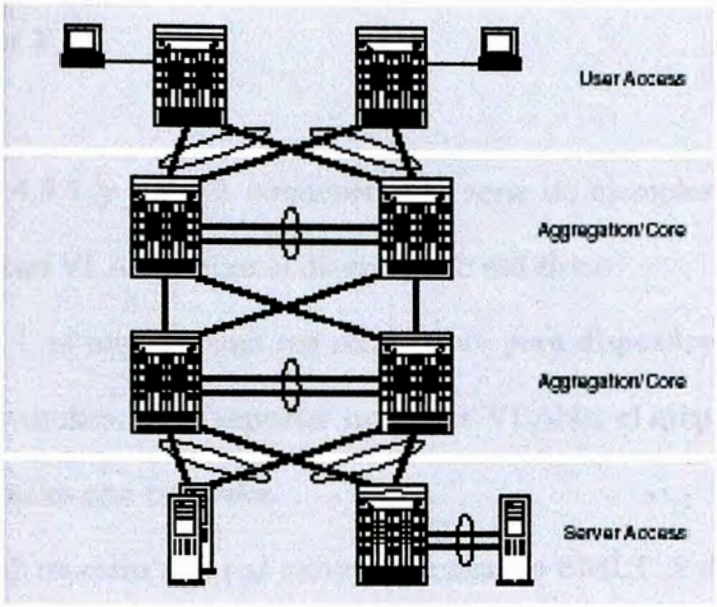


Ejemplo 1

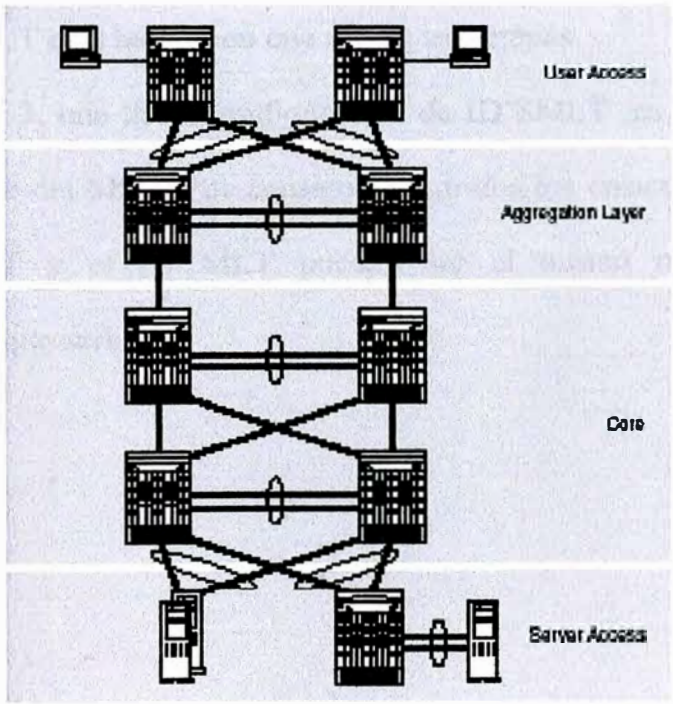


Ejemplo 2

Figura 3.4.7.1 Ejemplos de diseño capa 1.



Ejemplo 3



Ejemplo 4

Figura 3.4.7.2 Ejemplos de diseño capa 1.

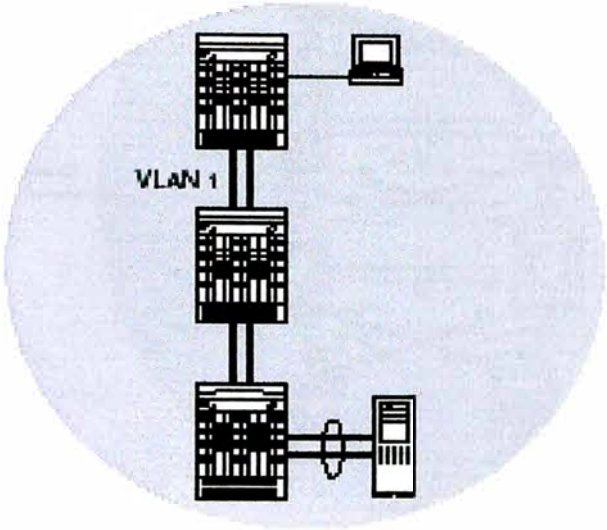
- **Ejemplos capa 2**

Las Figuras 3.4.8.1 y 3.4.8.2 contienen una serie de ejemplos de diseño de redes capa 2 que mapean VLANs sobre el diagrama de red físico.

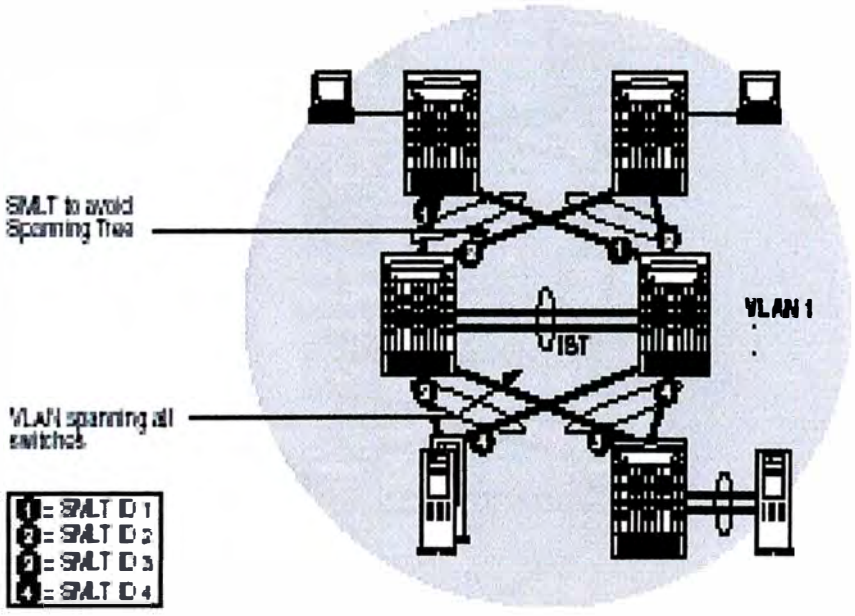
En el ejemplo 1 se muestra una red redundante para dispositivos usando una VLAN en todos los switches. Para soportar múltiples VLANs, el etiquetado 802.1Q es requerido en los enlaces con troncales.

En el ejemplo 2 muestra una red redundante usando SMLT. Este diagrama no requiere el protocolo Spanning Tree (STP). El SMLT remueve los lazos, pero aún asegura que todas las rutas son activamente usadas.Cada closet de cableado (Wc) puede tener hasta 8 Gigabytes de ancho de banda hacia el core. Notar que el ejemplo de configuración SMLT esta basado en una red de tres etapas.

En el ejemplo 3, una típica configuración de ID SMLT es mostrada. (Notar que el SMLT es parte del MLT. Por consiguiente, todos los enlaces SMLT tiene un ID MLT. El SMLT y el ID MLT pueden ser el mismo número, pero no necesariamente tiene que serlo) .

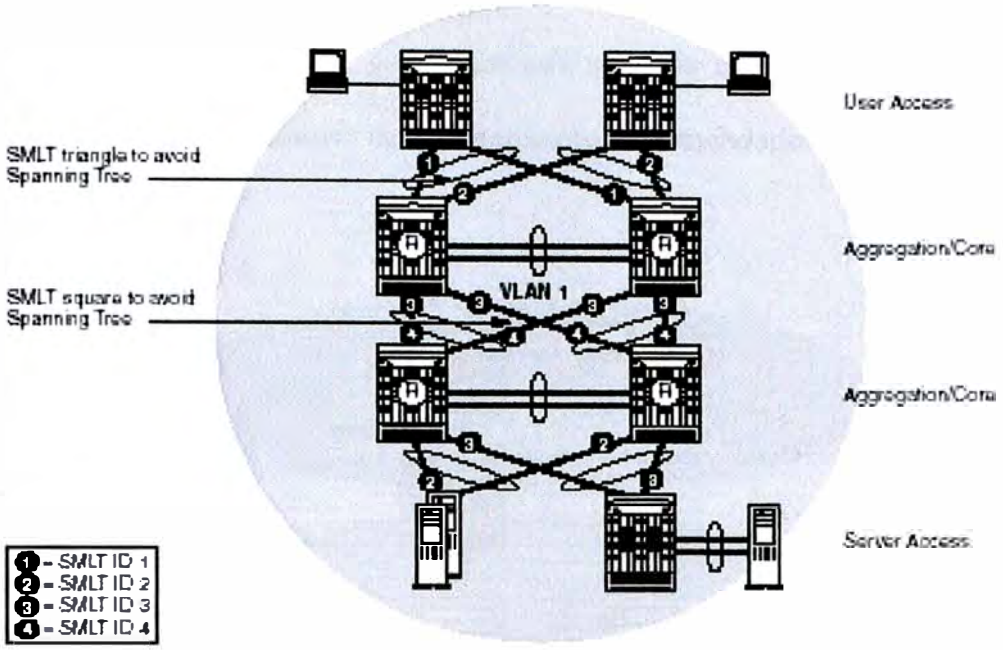


Ejemplo 1

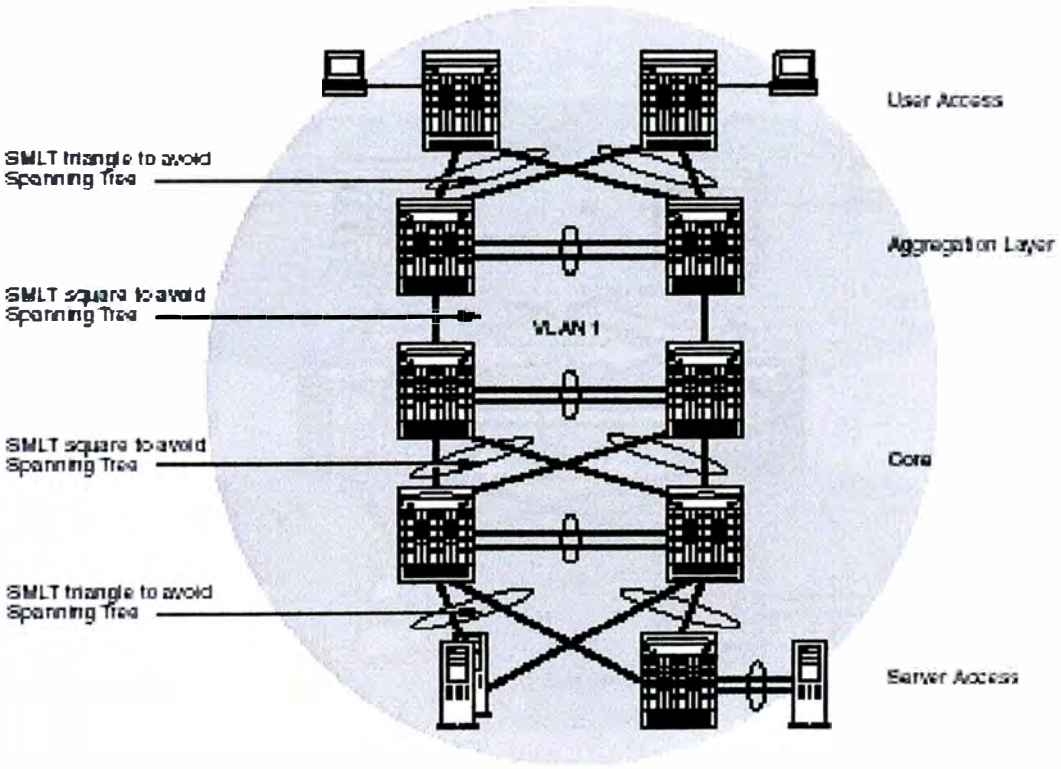


Ejemplo2 Usando SMLT

Figura 3.4.8.1 Ejemplos de diseño capa 2



Ejemplo 3

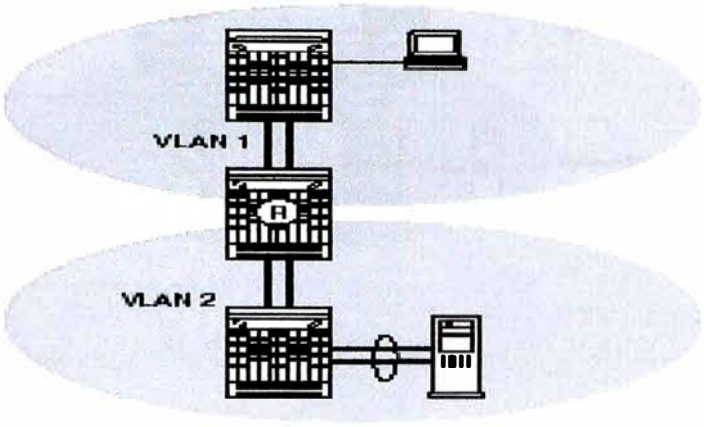


Ejemplo 4

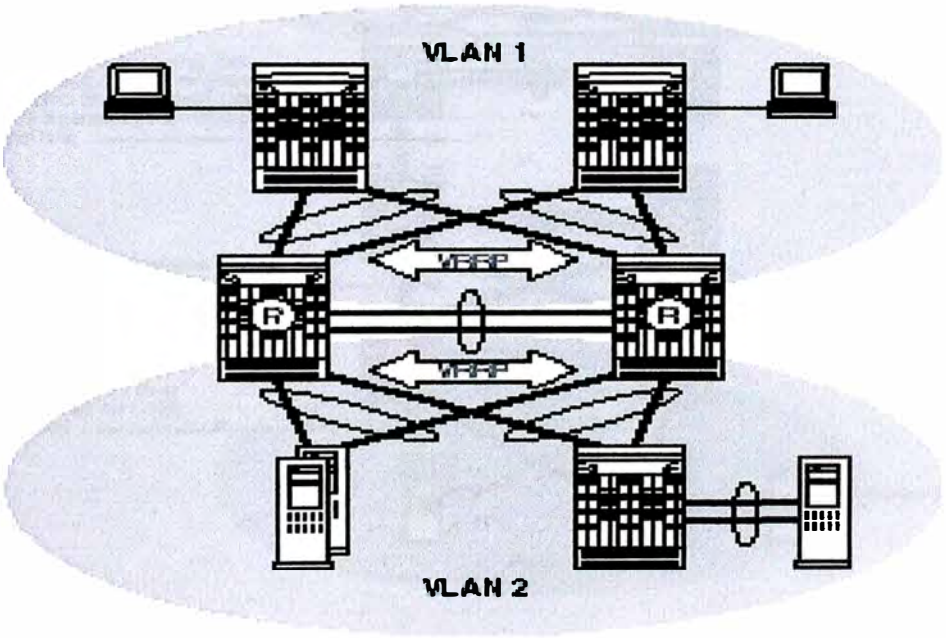
Figura 3.4.8.2 Ejemplos de diseño capa 2

- **Ejemplos capa 3**

Las Figuras 3.4.9.1 y 3.4.9.2 contienen una serie de ejemplos de diseño de redes capa 3 que muestran los casos de enrutamiento recomendados para optimizar redes redundantes IP e IPX.

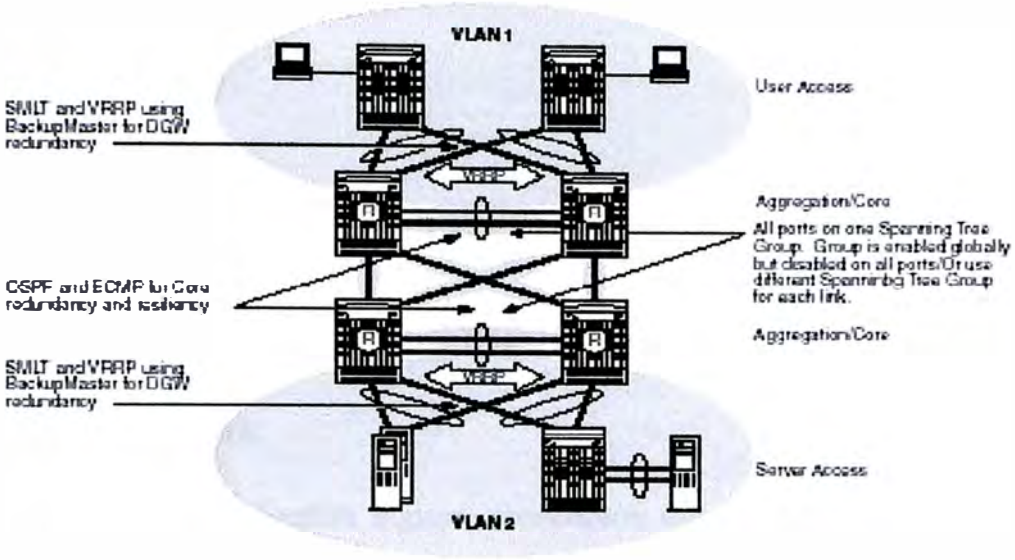


Ejemplo 1

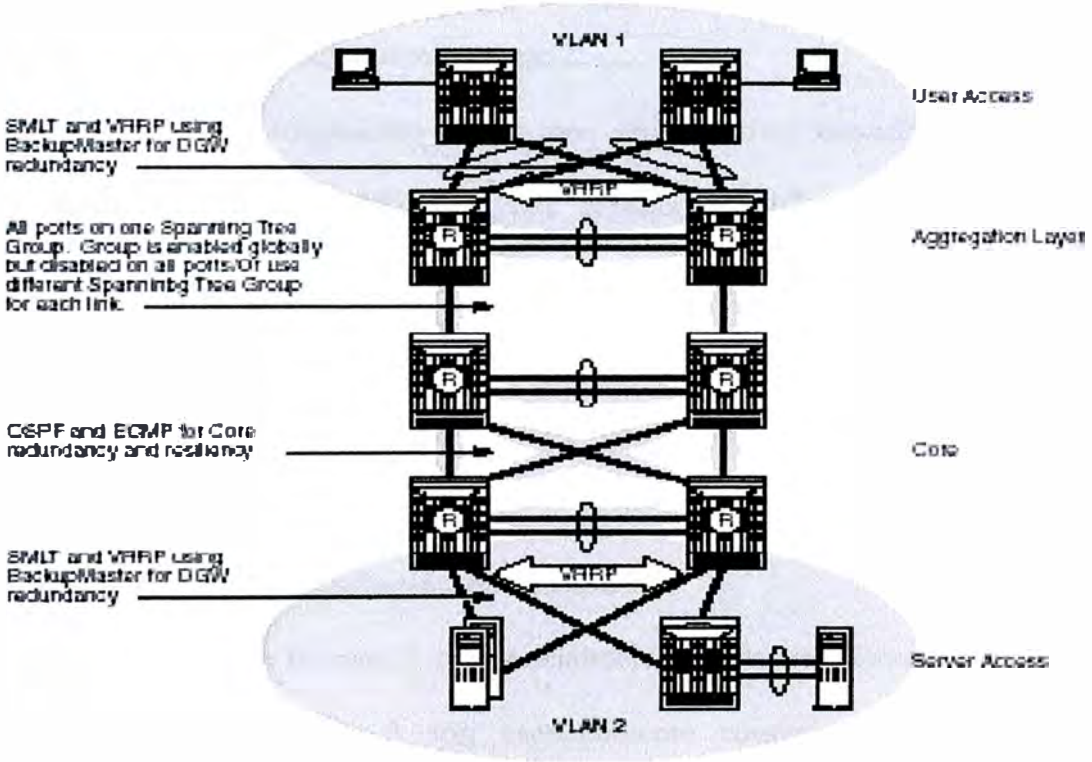


Ejemplo 2

Figura 3.4.9.1 Ejemplos de diseño capa 3



Ejemplo 3



Ejemplo 4

Figura 3.4.9.2 Ejemplos de diseño capa 3

CAPÍTULO IV

DISEÑANDO REDES CONMUTADAS CAPA 3

4.1 INTRODUCCIÓN

En este capítulo se analiza algunos conceptos empleados para el diseño e implementación de las redes LAN de este proyecto.

Se definen algunos términos y conceptos básicos de VLANs, que gracias a su versatilidad y a los ahorros que proporcionan se considera como una de las mejoras más útiles conseguidas en la conmutación capa 2.

Trataremos del enrutamiento IP, y nos enfocaremos especialmente en el protocolo de enrutamiento OSPF, y del protocolo VRRP ("Virtual Router Redundancy Protocol") que fueron utilizados para la implementación de las redes LAN de la entidad corporativa de este proyecto.

En general describiremos consideraciones de diseños que necesitamos cuando diseñamos redes switched capa 3.

- **Perspectiva de la conmutación de la capa 3**

La conmutación de la capa 3 es esencialmente un enrutamiento muy rápido. Los conmutadores de la capa 3 son esencialmente routers que efectúan sus aplicaciones sobre circuito integrados específicos de la aplicación (ASIC, "Aplication Specified Integrated Circuits) en lugar de utilizar software específico. El resultado es que se pierde un poco de flexibilidad (ya que con este método los

procesos de actualización de enrutamiento son un tema de hardware y no de software). Pero la velocidad de los dispositivos aumentan hasta la velocidad máxima del cable.

En la mayoría de los entornos, la diferencia real entre un router y un conmutador de la capa 3 (excluyendo los PSI y algunos entornos empresariales) radica en el papel del dispositivo en la red. Los conmutadores de la capa 3 se utilizan , propiamente , en LAN o MAN para proporcionar transferencia de datos de alta velocidad para clientes locales, donde los routers se emplean para conseguir un acceso WAN de baja velocidad. (Ver Figura 4.1.1).

Como los routers tienen más flexibilidad en sus interfases y en sus conjuntos de características, los procesos basados en software funcionan bastante bien. Además, la mayoría de las conexiones WAN se ejecutan para enlazar oficinas y tienden a ser más lentas de 100 Mbps, de manera que la reducción de las prestaciones inherente a los routers no es un asunto de importancia.

Sin embargo, los conmutadores de la capa 3 siguen siendo dispositivos muy útiles y potentes que pueden aumentar las prestaciones de la red dividiendo el entorno en dominios de difusión, igual que los routers. Además, utilizando VLAN se puede disminuir considerablemente quebraderos de cabeza en la configuración (y a veces también gastos), permitiendo utilizar conmutadores para enrutar las señales entre las diferentes VLAN.

Desde este punto de vista, los conmutadores de la capa 3 utilizan las VLANs igual que los conmutadores de la capa 2: se asigna su pertenencia a la VLAN para dividir los puertos en redes lógicas. Sin embargo los conmutadores de la capa 3 pueden efectuar el enrutamiento entre esas redes por sí mismos y, generalmente, a la

velocidad máxima del cable, lo que significa que no es necesario configurar rígidamente el router ni tampoco preocuparse sobre la compartición entre el conmutador y el router (reduciendo las necesidades de puertos que tiene el proceso).

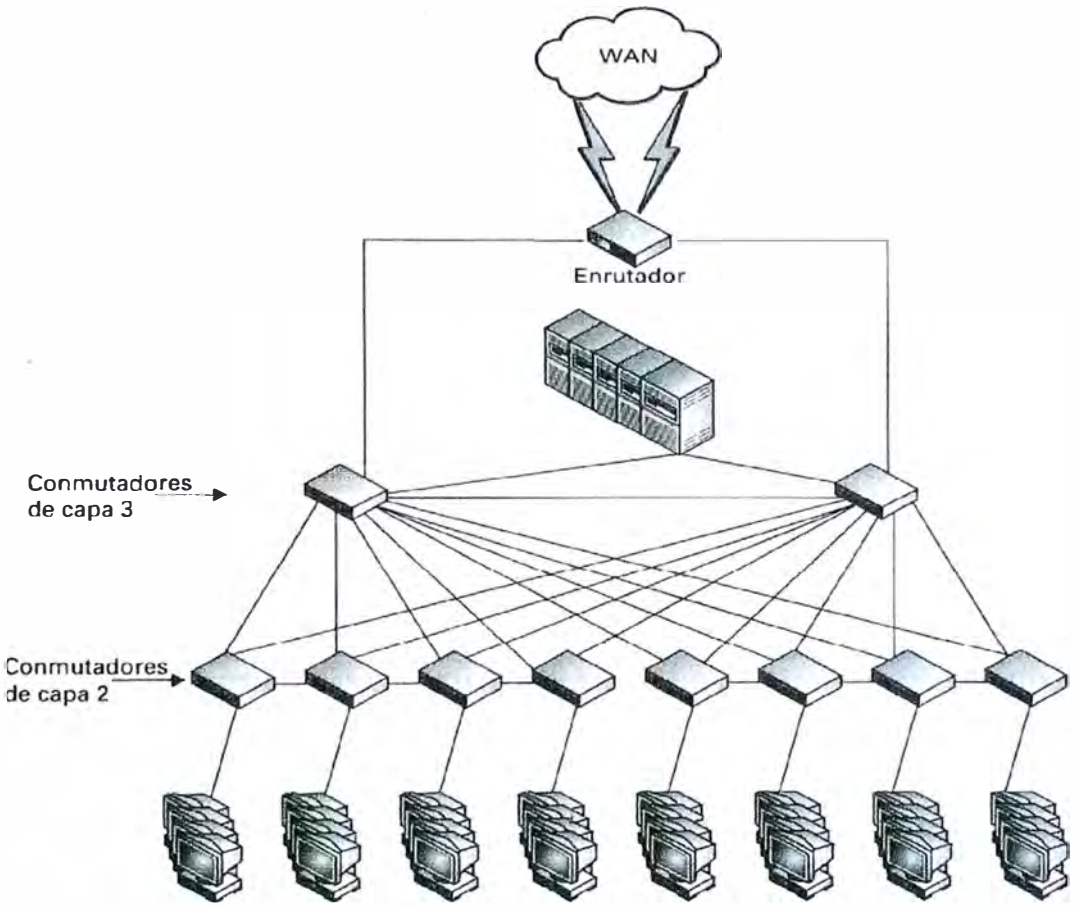


Figura 4.1.1 Función de los routers y los conmutadores de la capa 3.

- **Flexibilidad de configuración de los switches Passport capa 3**

Los switches passport 8600 utilizado para la implementación de este proyecto es un switch capa3, extremadamente flexible y puede ser configurado en una

variedad de modo tal como se muestra en la Figura 4.1.2. y la cual describiremos brevemente:

Como Switch L2 – La configuración por default de los switches Passport 8600 es la de un rápido switch L2 con todo los puertos en el mismo dominio de difusión "broadcast".

Como Router IP/IPX L3 - Todos los puertos pueden ser configurados como puertos de router individuales con enrutamiento L3 y filtraje a la velocidad del cable. En esta configuración el Switch Passport 8600 se comporta como un router IP y/o IPX.

Como Router IP/IPX y Switch L2 – El switch Passport 8600 simultáneamente conmuta entre puertos L2 y enruta entre subredes o VLANs en L3.

Vlans por puertos y por política – Si varios protocolos necesitan ser manejados de diferentes maneras, el Switch Passport 8600 puede crear VLANs para frames de diferente protocolos, políticas y puertos.

Enrutamiento IP/IPX de VLAN a VLAN – El enrutamiento puede ser configurado para enviar tráfico IP/IPX en L3 entre VLANs basados en puertos, VLANs basados en el protocolo y en VLANs basado en la "IP Subnet" a la velocidad del cable.

Cualquier configuración requerida – El switch Passport puede ser configurada para soportar algunos puertos como router, algunos puertos con múltiples VLANs, algunas VLANs enrutadas mientras que otra no – cualquier cosa que sea requerida para soportar las redes empresariales. Todo el tráfico L2 y L3 es manejado a la velocidad de la línea.

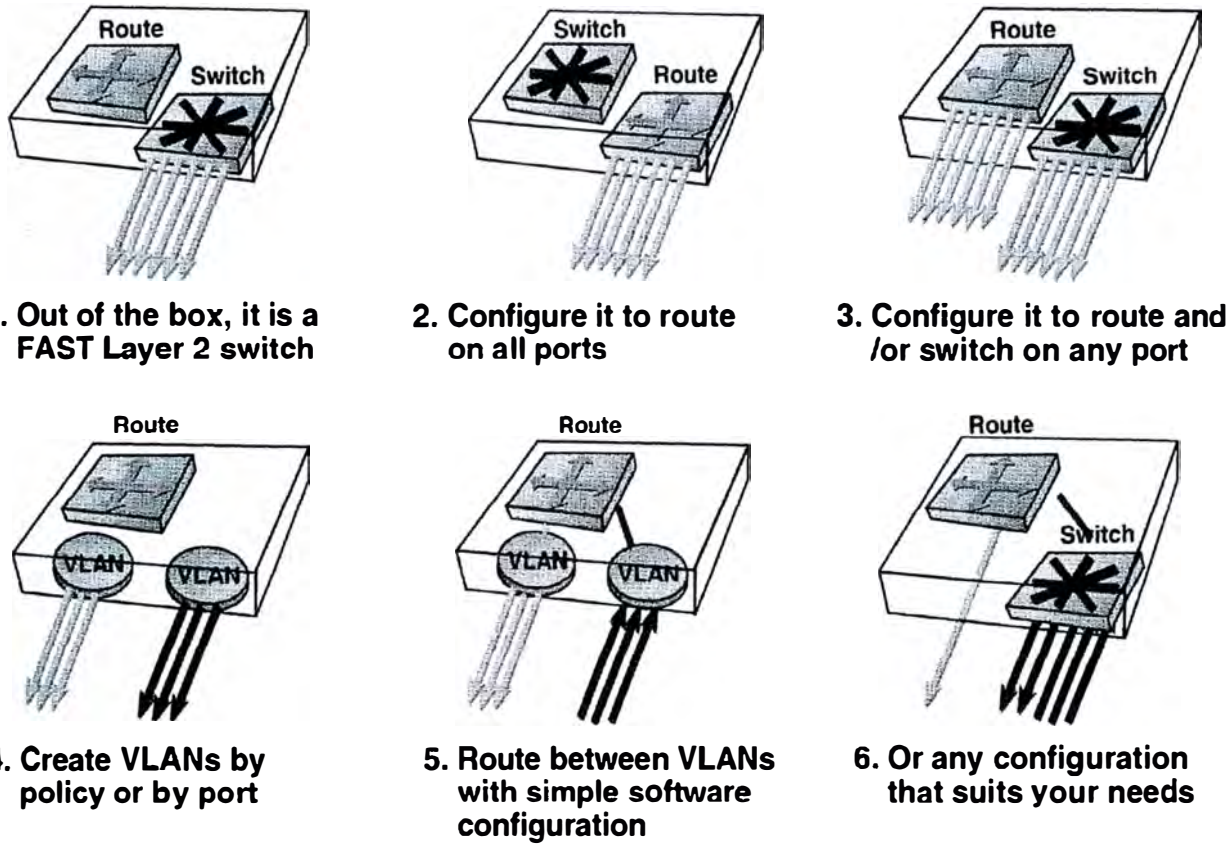


Figura 4.1.2 Flexibilidad de configuración de los switches Passport 8600

4.2 VLANS

4.2.1 SOBREVISTA DE LAS VLANs

Las redes virtuales (VLAN) suponen la mayor ventaja de la conmutación de la capa 2. Los requerimientos para controlar los tamaños y extensiones de los dominios de difusión (broadcast) nos lleva al concepto de LAN virtuales (VLAN). Una VLAN es una colección de puertos de redes que comparten un dominio de broadcast. Las VLANs pueden ser extendidas a través de varios dispositivos capa 2 , creando comunidades de usuarios que pueden estar esparcidos en localizaciones separadas físicamente.

Por definición, las VLANs son dominios de broadcast únicos. Cada VLAN puede ser pensado como si fuese su propia red. El flujo de broadcast solo ocurre entre las estaciones configuradas en la misma VLAN. Las VLANs pueden ser asociadas directamente a subredes IP, números de red IPX y zonas de AppleTalk, permitiendo que las estaciones corriendo estos protocolos interactúen sin impactar en los otros usuarios. Para la comunicación entre las VLANs se requiere el uso de un Router que es un dispositivo capa 3, para enrutar los paquetes entre las VLANs.

Una VLAN :

- Es un flexible grupo de dispositivos definidos por software con fronteras independiente del medio físico.
- Confina trafico broadcast dentro de las fronteras definidas por software.
- Provee baja latencia, comunicación a la velocidad del cableado entre los miembros de la VLAN.
- Soporta segmentación de la red o micro-segmentación.

- Puede contener uno o varias estaciones en un único segmento VLAN.

Una VLAN nos habilita a dividir nuestra LAN en pequeños grupos lógicos sin interferir con la red física . Las VLANs tienen un rango de aplicaciones prácticas, tales como las siguientes:

- Podemos crear VLANs o grupos de trabajo, para grupos de interés común.
- Podemos crear VLANs o grupo de trabajo, para tipos específicos de tráfico de red.
- Podemos adicionar, mover o borrar miembros de estos grupos de trabajo sin hacer ningún cambio físico en la red.

Dividiendo la red en VLANs separadas, podemos crear dominios de broadcast separadas. Este arreglo conserva el ancho de banda , especialmente en redes soportando broadcast y aplicaciones multicast que inundan la red con tráfico.

Un grupo de trabajo definido como VLAN, puede incluir miembros de un número de segmentos físicos disperso sobre la red, mejorando el tráfico que fluye entre ellos.

El switch de la serie Passport 8600 empleado para la implementación de las redes LAN para la entidad corporativa, realiza funciones de switcheo en capa 2 necesario para transmitir información dentro de las VLANs así como también funciones de enrutamiento en capa 3 necesario para que las VLANs se comuniquen

unas con otras. Una VLAN puede ser definida por un único switch o puede expandirse por varios switches. Un puerto puede ser miembro de varias VLANs.

En la figura 4.2.1 cada dominio de broadcast es también una VLAN. El dominio de broadcast AZUL esta extendida entre los dispositivos.

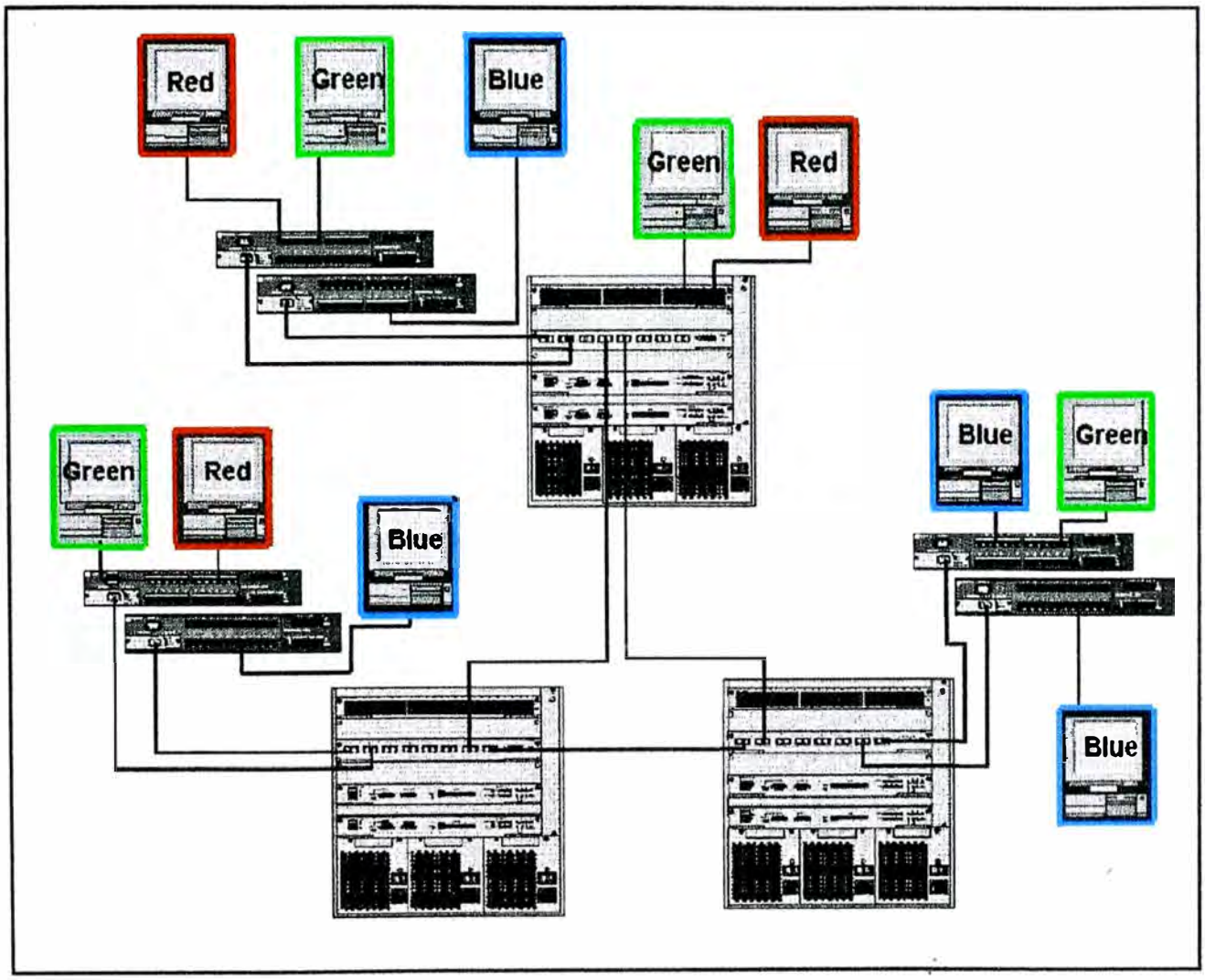


FIGURA 4.2.1 LANs,VLANs y dominios de broadcast

4.2.2 ¿COMO TRABAJAN LAS VLANs?

- **DOMINIO DE BROADCAST**

Cada VLAN es un dominio de broadcast separado. Un bridge interno virtual es creado para conectar juntos a un número de segmentos de red físicos en cada VLAN. En la figura 4.2.2 los usuarios en la VLAN Naranja solo ven el tráfico, incluyendo los broadcast y multicast, destinado para la VLAN naranja. Igualmente, los usuarios en la VLAN azul solo verán el trafico originado en su propia VLAN. Con esta consideración, las VLANs se comportan exactamente de la misma manera que una LAN tradicional.

- **IDENTIFICADOR DE LA VLAN**

La mayoría de switches identifican la VLAN por medio de un identificador numérico. Esta VLAN ID es generalmente incluida en la tabla de envío (forwarding) que el switch mantiene para cada VLAN. Este ID puede ser colocado en una cabecera especial del paquete para asegurar para asegurar funcionamiento de envíos (forwarding) apropiados por los switches mas remotos.

- **CONECTANDO DOS VLANS**

A igual que las LANs tradicionales, un router es requerido para enviar (forwarding) tráfico entre las VLANs.

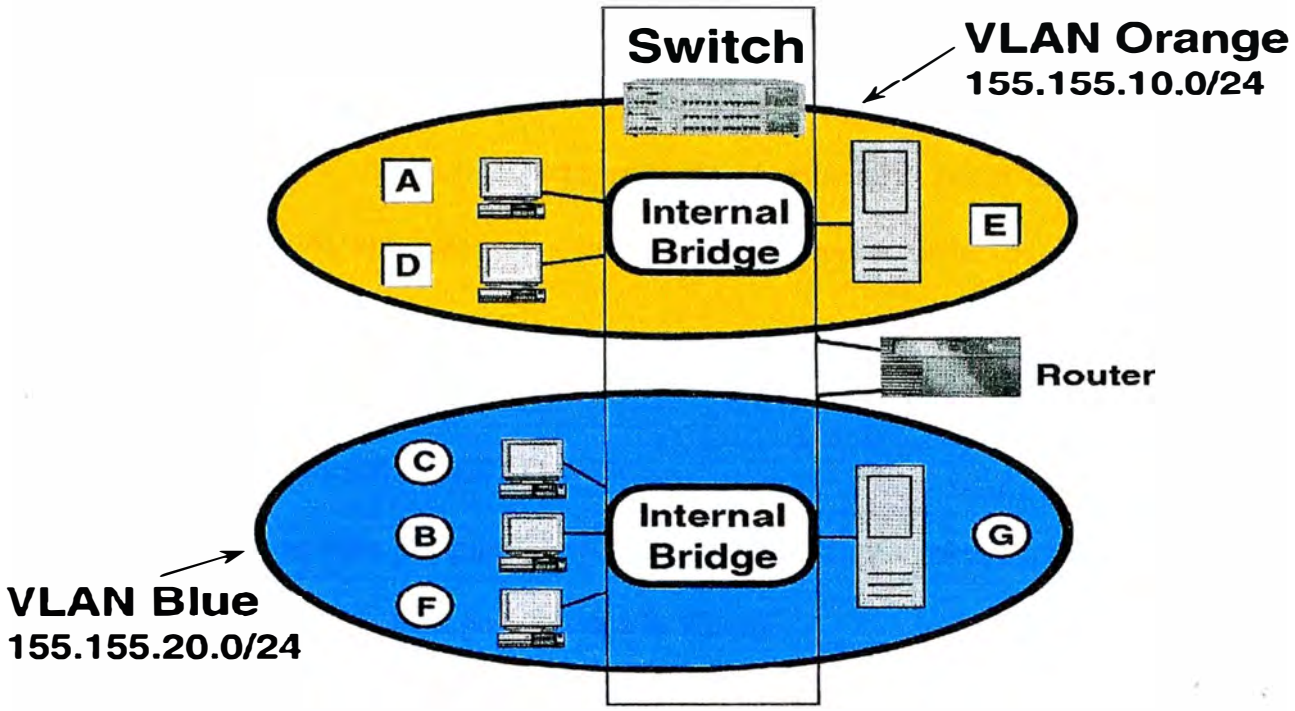


Figura 4.2.2 Como trabajan las VLANs

4.2.3 TIPOS DE VLANS

- **TIPOS DE VLANS**

Hay dos principales tipos de VLANs :

- Basadas en puertos
- Basadas en políticas

Hay tres sub-tipos de VLANs basadas en políticas:

-Basadas en la dirección IP de la subred

-Basadas en el tipo de protocolo

-Basadas en la dirección MAC

- **CRITERIO DE MEMBRESÍA O PERTENENCIA A UNA VLAN**

Varios criterios son usados para determinar que dispositivos son miembros de una VLAN, y a que VLAN un paquete entrante es asignado. Estos criterios son dejados a discreción de los fabricantes de equipos y pueden variar de un tipo de switch a otro.

- **VLANS BASADAS EN PUERTOS**

Una VLAN basada en puerto es una VLAN en el cual los puertos son explícitamente configurados para pertenecer a la VLAN.

Es el método más sencillo para configurar la pertenencia a una VLAN. La VLAN es configurada simplemente asociando un puerto o un grupo de puertos con una VLAN específica. El tráfico recibido sobre un puerto perteneciente a una VLAN dada puede ser solo enviada sobre otros puertos, que también están dentro de esa VLAN.

Generalmente, un puerto puede pertenecer a solo una VLAN basada en puerto. Las VLANs basadas en puertos soportan todos los tipos de frames Ethernet.

En la figura 4.2.3.1 los puertos 2,5,6,8 y 9 están en la VLAN Azul. Los otros puertos están en la VLAN naranja . Las estaciones en la VLAN naranja no pueden comunicarse con las estaciones que están en la VLAN azul al menos que se comuniquen a través de un dispositivo capa 3. Es importante notar que la figura 4.2.3.1 es ligeramente engañoso debido a que las estaciones no están en realidad en la VLAN, sino que los puertos a las cuales las estaciones se conectan participan en la VLAN. Las estaciones como así misma no tienen el concepto de una VLAN, así se retiene el concepto de transparencia.

Cuando creamos una VLAN basada en puerto sobre un switch , asignamos un número de identificación de la VLAN (VLAN ID) y especificamos que puertos pertenecen a la VLAN. La VLAN ID es usada para coordinar las VLANs a través de varios switches.

El ejemplo de la figura 4.2.3.2 muestra 2 VLANs basadas en puertos creadas en los switches Passport que son con lo que se implemento este proyecto: Una VLAN para el departamento de Marketing y otra para el departamento de ventas. Los puertos son asignados a cada VLAN basada en puertos. Un cambio en el área de venta puede mover al representante de venta que esta en el puerto 3/1 (el primer puerto en el módulo que esta en el slot 3 del chasis) al departamento de Marketing sin mover cables. Con una VLAN basada en puertos, solo necesitamos indicar mediante un comando de línea (CLI) o en el Device Manager (interfase grafica para configurar los switches Passport) que el puerto 3/1 que esta en la VLAN de ventas ahora sea un miembro de la VLAN de Marketing.

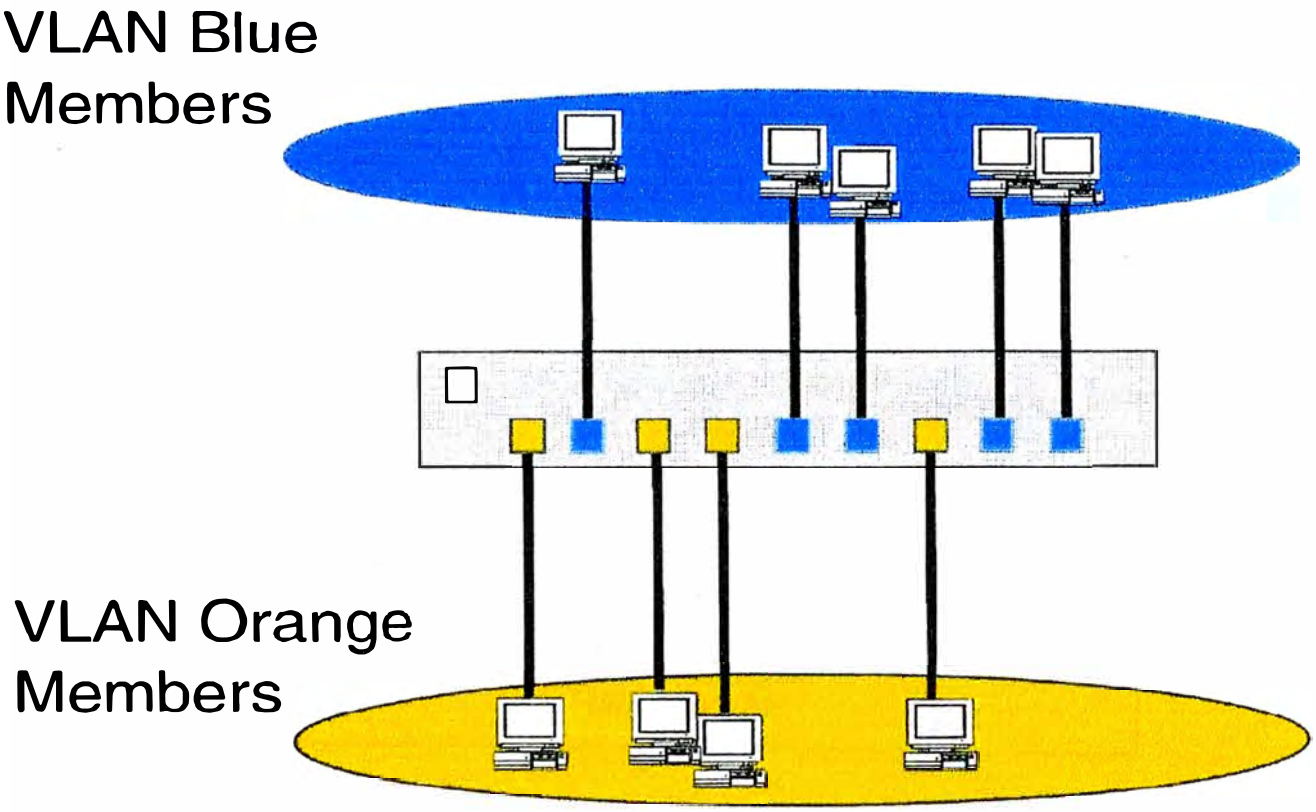


Figura 4.2.3.1 VLANs basadas en puertos

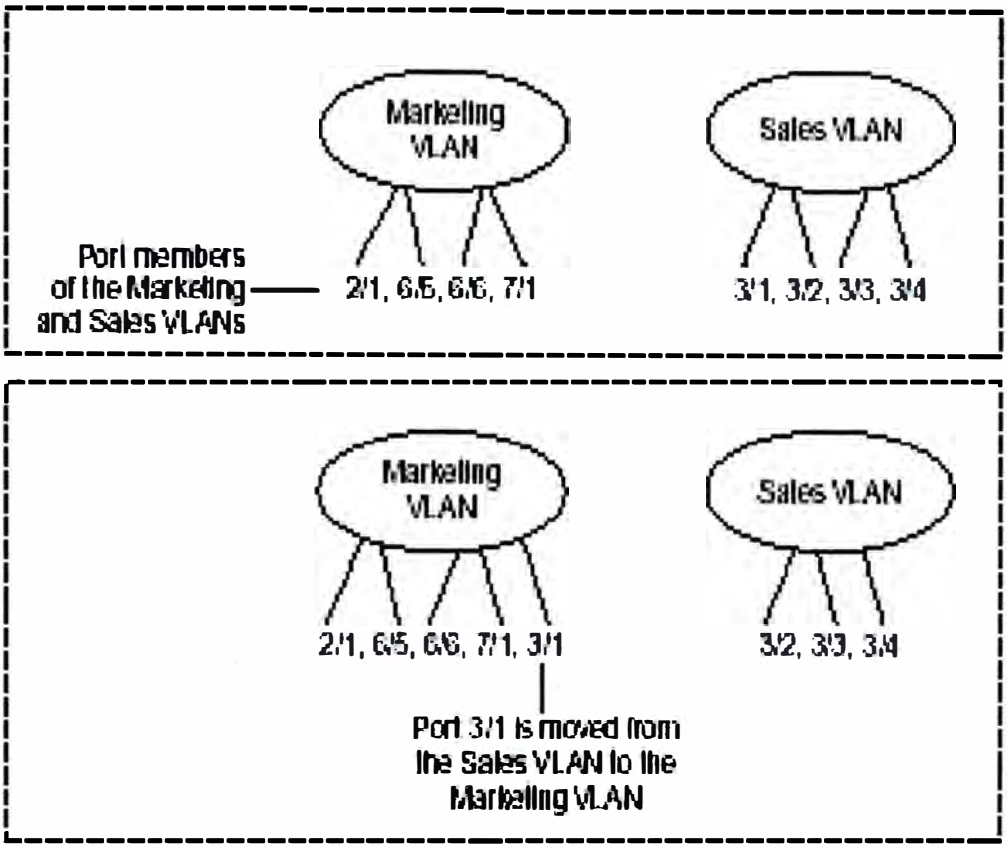


Fig 4.2.3.2 Otro ejemplo de VLANs basadas en puertos

- **VLANS BASADAS EN POLÍTICAS**

Una VLAN basada en políticas es una VLAN en el cual los puertos son dinámicamente adicionados a la VLAN basados en el tráfico entrante dentro del puerto.

Las VLANs basadas en políticas usan algunos atributos del dataframe para determinar la pertenencia a una VLAN. Entre los atributos comunes usados para determinar la membresía de una VLAN cuando usamos VLANs basadas en políticas son el tipo de protocolo, la dirección IP-subnet fuente y la dirección MAC fuente.

En las VLANs basadas en políticas sobre un switch Passport 8600 capa 3 o sobre un switch Passport 8100 de borde capa 2, que son los switches utilizados para la implementación de este proyecto, los puertos son designados como un miembro permanente (always) o un miembro no permanente (never) de la VLAN. En adición podemos designar un puerto como un miembro potencial de la VLAN sobre el switch Passport 8600 con ruteo. Cuando un puerto es designado como un miembro potencial de la VLAN y el tráfico entrante concuerda con la política, el puerto es dinámicamente adicionado a la VLAN. Los puertos miembros tipo potencial que se han juntado a la VLAN son removidos por edad "aged out" de la VLAN cuando el periodo de tiempo de expiración (aging time o tiempo por vejez) se cumple.

La pertenencia a una VLAN de un puerto es determinada por el tráfico entrante dentro del puerto. Por consiguiente Nortel Networks recomienda que al menos algunos puertos sean designados como miembros permanentes (always) de la VLAN. Una situación en el cual un puerto debe ser designado como miembro permanente (always) de una VLAN es si un servidor o un router se conectan al puerto. Si un servidor es conectado a un puerto que esta designado como un miembro potencial y el servidor envía tráfico muy pequeño, un cliente fallará para alcanzar al servidor si el puerto donde esta el servidor tiene un time out de la VLAN

Un puerto puede pertenecer a una VLAN basada en puertos y a muchas VLANs basadas en políticas.

Los módulos del Switch Passport 8600 capa 3, soportan VLANs basadas en políticas, basadas en el protocolo de red, la dirección MAC fuente, o en la IP subnet fuente.

Los módulos del Switch Passport 8100 capa 2 utilizado como switch de borde soportan VLANs basadas en políticas , basadas solo en el protocolo de red.

- **VLANS BASADAS EN EL PROTOCOLO**

Una VLAN basada en el protocolo es una VLAN en el cual los puertos son dinámicamente adicionados a la VLAN, basados en el campo tipo de protocolo del dataframe entrante al puerto. Es decir para determinar si el frame entrante pertenece a una VLAN basada en el protocolo, el switch mira en el campo tipo de protocolo en la cabecera del paquete. Si el campo tipo de protocolo del frame concuerda con una VLAN basada en el protocolo definida sobre el puerto de ingreso, entonces su pertenencia a la VLAN es establecida.

En la figura 4.2.3.3 se ilustra una VLAN basada en el protocolo que usa el campo tipo de protocolo del dataframe. El switch examina cada frame y lo asigna a la VLAN apropiada para ese protocolo. Los dataframes IPX son asignados a la VLAN basada en el protocolo IPX y los dataframes AppleTalk son asignados a la VLAN basada en el protocolo AppleTalk.

Esto no constituye una función de enrutamiento. Esto significa que la información del campo Ethertype es usada para determinar la VLAN en la cual un puerto del switch será un miembro y en el cual el paquete entrante será asignado.

Como un ejemplo del uso de una VLAN basada en el protocolo en los switches Passport , podemos crear una VLAN para el protocolo IPX y colocar puertos llevando tráfico IPX sustanciales dentro de esta nueva VLAN. En la figura 4.2.3.4 el administrador de red ha colocado los puertos 7/1, 3/1 y 3/2 en una VLAN IPX. Estos puertos aun pertenecen a sus respectivas VLANs basadas en puertos

Marketing y Ventas (ver fig 4.2.3.2), pero ellos son también nuevos miembros de la VLAN IPX. Este arreglo localiza el tráfico y asegura que solo los 3 puertos sean inundados con paquetes broadcast IPX.

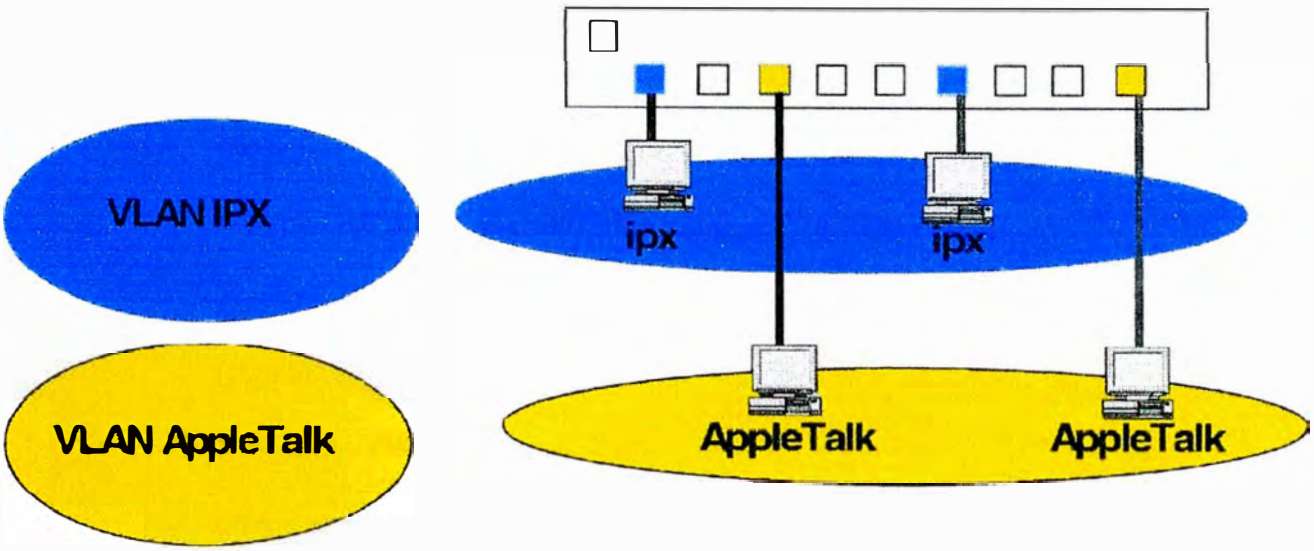


Fig 4.2.3.3 VLANs basadas en el protocolo

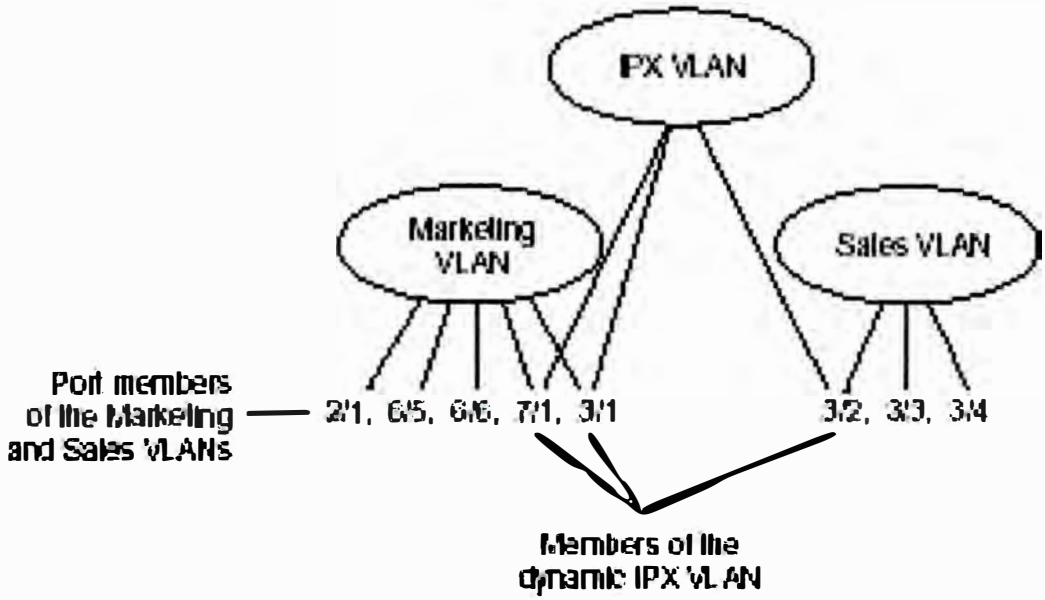


Fig 4.2.3.4 Otro ejemplo de VLAN dinámica basado en el protocolo

El switch de la serie Passport 8000 soporta las siguientes VLANs basadas en protocolos estándares :

- IP versión 4 (ip).
- Novell IPX sobre frames Ethernet 802.3 (ipx802dot3)
- Novell IPX sobre frames IEE802.2 (ipx802dot2)
- Novell IPX sobre framesEthernet SNAP (ipxSnap)
- Novell IPX sobre frames Ethernet tipo 2 (ipxEthernet2)
- AppleTalk sobre Ethernet tipo 2 y sobre Frames Ethernet SNAP (AppleTalk).
- Protocolo DEC LAT (decLat)
- Otros protocolos DEC (decOther)
- IBM SNA sobre frames IEEE 802.2 (sna 802dot2)
- IBM SNA sobre frames Ethernet tipo 2 (snaEthernet2)
- Protocolo NetBIOS (netBIOS)
- Xerox XNS (xns)
- Bayan VINES (vines)
- IP versión 6 (ipv6)
- Protocolo de Resolución de direcciones reversa (RARP Reverse Address Resolution Protocol).

- **VLANS BASADAS EN LA DIRECCIÓN MAC FUENTE**

Una VLAN basada en la dirección MAC fuente es una VLAN en el cual los puertos son dinámicamente adicionados a la VLAN, basados en el campo de la dirección MAC fuente del dataframe entrante al puerto, es decir el data-frame será un miembro de una VLAN basada en la dirección MAC fuente si la dirección fuente concuerda con una dirección MAC configurada, asignada por el usuario a una VLAN particular.

En este caso la pertenencia a una VLAN definida dinámicamente se basa en las direcciones MAC del dispositivo. Esta configuración es un poco más complicada, pero permite desplazar los servidores según se desee y que la pertenencia "les siga" , lo que puede resultar muy útil para empresas que suelen desplazar a sus empleados a menudo o que tienen muchos usuarios conectados a la red mediante portátiles.

Una de los subtipos de las VLANs basadas en políticas es la que se basa en la dirección MAC fuente, que nos permite que los módulos del switch Passport 8600 capa 3 , asocien frames a una VLAN basada en el contenido del frame. Con VLANs basadas en la dirección MAC fuente, un frame es asociado a una VLAN si la dirección MAC fuente es una de las direcciones MAC explícitamente asociada con la VLAN. Para crear una VLAN basada en la dirección MAC fuente, debemos adicionar la dirección MAC a una lista de direcciones MAC que constituyen la VLAN. Sin embargo, debido a que es necesario, que explícitamente se asocien las direcciones MAC con una VLAN basada en la dirección MAC fuente, la sobrecarga administrativa es bastante alto.

Cuando un puerto es asignado a una VLAN basada en la dirección MAC, el usuario debe configurar una tabla de direcciones MAC y las VLANs a los cuales

ellos pertenecen. Esta tabla puede permitir que las direcciones MAC puedan estar sobre cualquier puerto dentro de la VLAN o restringir a solo un único puerto en la VLAN.

Si configuramos para permitir que la dirección MAC pueda existir sobre varios puertos, una VLAN basada en la dirección MAC fuente permite que los trabajadores, no importándole donde ellos estén conectados, sean miembro de la misma red. Esto es particularmente útil para el personal de servicio de red móvil quienes necesitan acceder a los mismos recursos de la red donde ellos se conecten, mientras denieguen estos servicios a cualquier otro dispositivo que pueda estar conectado en el mismo puerto.

Las VLANs basadas en la dirección MAC fuente son generalmente pequeñas debido a los engorrosos requerimientos de configuración.

Las VLANs basadas en la dirección MAC fuente proveen una red más segura debido a que ellas permiten que solo los usuarios conocidos tengan acceso a los recursos de la red.

Por consiguiente podemos usar VLANs basadas en la dirección MAC fuente cuando queramos reforzar un esquema de seguridad a nivel de las direcciones MAC, diferenciando los grupos de usuarios. Por ejemplo, en un ambiente universitario, los estudiantes serán parte de una VLAN de estudiante con ciertos servicios y privilegios de acceso, y el cuerpo docente será parte de otra VLAN basada en la dirección MAC fuente, con servicios y privilegios de acceso propio del cuerpo docente. Así un estudiante y un miembro del cuerpo docente podrían conectarse al mismo puerto pero tener acceso a un diferente rango de servicios. Para proveer el correcto servicio por todo el campus, la VLAN basada en la dirección MAC fuente podría necesitar

ser definida sobre los switches Passport 8600 capa 3 que están por todo el campus, lo cual ocasiona sobrecarga administrativa.

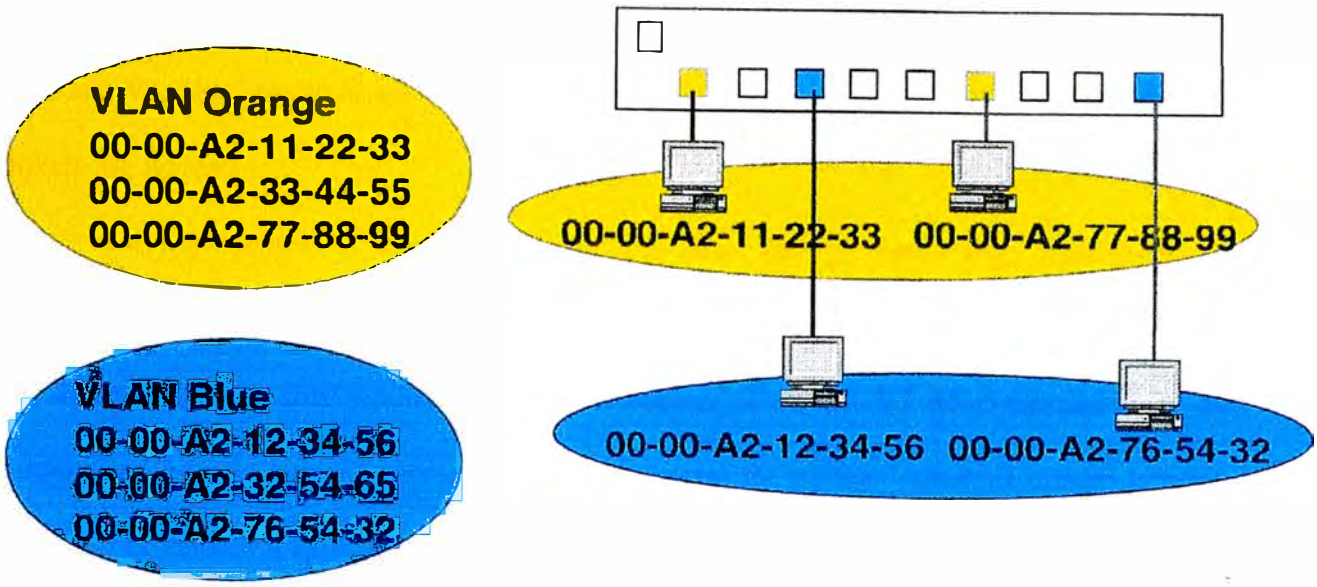


Fig 4.2.3.5 VLANs basadas en la dirección MAC fuente

- **VLANS BASADAS EN LA DIRECCIÓN IP DE LA SUBRED FUENTE**

Una VLAN basada en la dirección IP de la subred fuente es una VLAN en el cual los puertos son dinámicamente adicionados a la VLAN, basados en el campo de la dirección IP de la subred fuente del dataframe entrante al puerto, es decir si una VLAN basada en la dirección de subred fuente es definida sobre el puerto y la dirección de red fuente concuerda con las direcciones configuradas para la VLAN, entonces el data-frame será un miembro de esa VLAN.

Los módulos del switch Passport 8600 capa 3 soportan las VLANs basadas en la dirección IP de la subred fuente. Los puertos de acceso pueden ser asignados a varias VLANs basadas en la dirección IP de la subred fuente , es decir puede haber muchas VLANs basadas en la dirección IP de la subred fuente definida sobre un puerto de acceso.

La pertenencia a una VLAN de este tipo, de un frame esta basada en la dirección IP fuente asociada con una máscara. VLANs basadas en la dirección IP de la subred fuente son opcionalmente ruteables. Usando VLANs basadas en la dirección IP de la subred fuente, varias estaciones de trabajo sobre el mismo puerto pueden pertenecer a diferentes subredes, similar al "multinetting" sobre un router.

En la figura 4.2.3.6 se muestra un ejemplo del uso de VLANs basadas en la dirección IP de la subred fuente.

En la figura 4.2.3.7 se muestra el uso incorrecto de las VLANs basadas en la dirección IP de la subred fuente, dando como resultado la perdida de tráfico.

En el ejemplo de ruteo IP unicast, el host que tiene la dirección IP 172.100.10.2 envía tráfico al switch 2 (que tiene la dirección 172.100.10.1) destinada al ruteador que esta en el switch 1 (que tiene la dirección 172.168.1.1). El switch 2 intenta enrutar el tráfico IP pero ese tráfico no llegará al ruteador en el switch 1 . El switch 1 no asignará este frame a una VLAN 2 que está basada en la dirección IP fuente, debido a que la dirección IP fuente del tráfico no concuerda con la subred IP asignada a la VLAN 2. Si el enlace de acceso en la VLAN 2 , que esta conectando el switch 1 con el switch 2 fuese un enlace etiquetado (tagged), el tráfico podría ser asociado con la etiqueta de la VLAN (VLAN tag) y no con la dirección IP, y así podría ser envido correctamente al switch 1 .

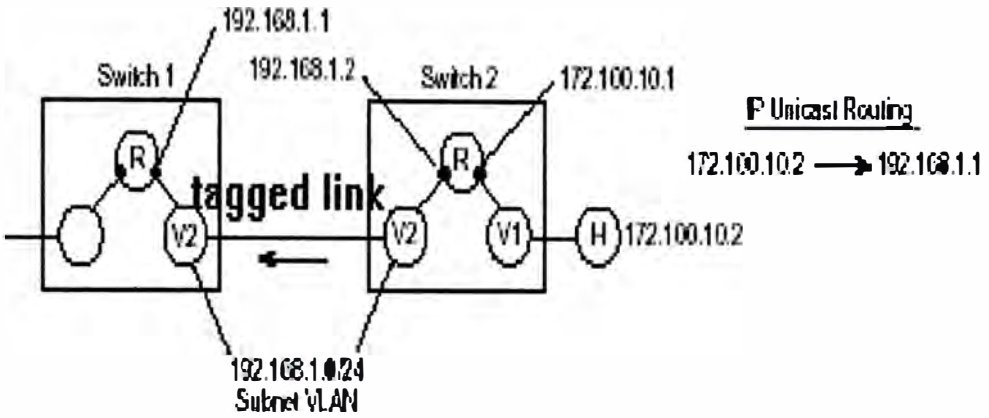


Fig 4.2.3.6 VLANs basadas en la dirección IP de la subred fuente

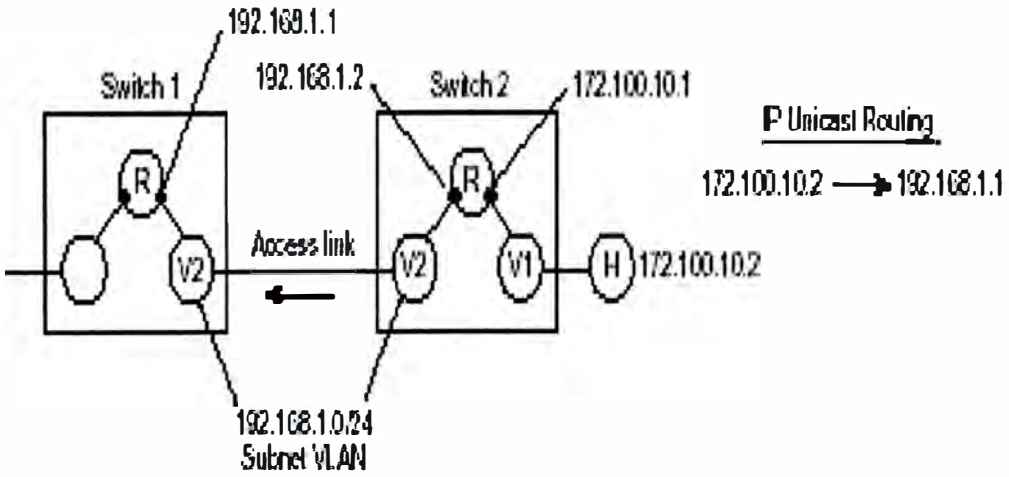


Fig 4.2.3.7 Incorrecto uso de una VLAN basada en la IP subnet

4.2.4 EXTENDIENDO LA VLAN

- **ESPARCIENDO LAS VLANS A TRAVÉS DE VARIOS SWITCHES**

Algunas veces es necesario crear VLANs que estén geográficamente dispersada y extendida a través de varios switches. En este tipo de ambiente, el switch destino debe ser hábil de identificar desde que VLAN cada frame es originado. Una vez que cada switch destino tenga esta información, este podrá fácilmente enviar "forward" los frames a los puertos apropiados.

Un enlace de switch a switch puede llevar tráfico de varias VLANs simultáneamente. El switch receptor necesita algún método para determinar a que VLAN pertenece el paquete.

Hay 2 métodos generales para determinar la membresía de la VLAN para un dataframe recibido.

-**Etiqueta implícita**: Este tipo de determinación de la membresía de la VLAN esta basada en algunos atributos del frame original tales como el puerto receptor o el protocolo del frame.

-**Etiqueta Explicita**: Con la etiqueta explicita, el propio frame lleva un identificador explicito que determina la membresía de la VLAN. Ejemplos incluyen métodos basadas en estándares tales como el 802.1Q, el LANE del Forum de ATM y protocolos propietarios tal como el LattisSpan de Nortel Networks.

En la figura 4.2.4.1 se muestra una VLAN esparcida a través de 2 switches.

- **ETIQUETADO DEL FRAME**

El modo más común para cumplir esto es adicionar información a la cabecera del Ethernet. Esta información adicional es comúnmente referida como una etiqueta

"tag", identifica a la VLAN desde el cual el paquete fue originado. El switch destino usa esta información para determinar con que VLAN el paquete esta asociado. Una vez que el switch destino determina la VLAN apropiada este remueve la información extra y envía así el paquete.

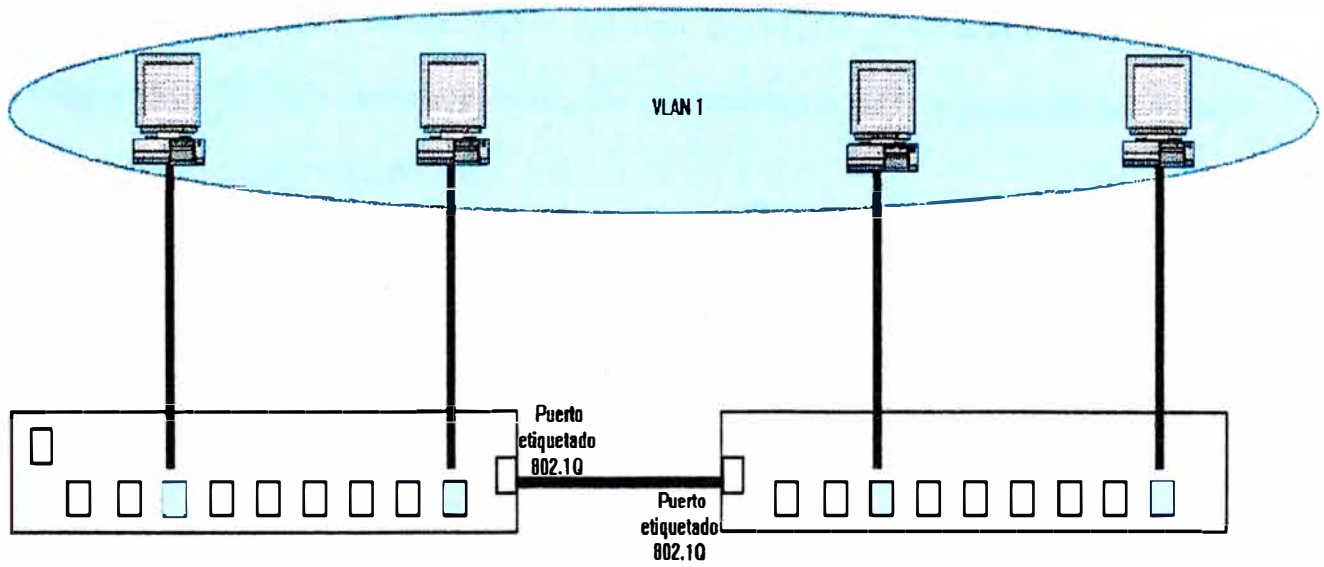


Figura 4.2.4.1 Extendiendo la VLAN

❑ 802.1Q : EL ESTÁNDAR DEL FRAME ETIQUETADO

- **Definición**

La estandarización de las VLANs extendidas a través de los puertos etiquetados "tagged" es soportada por una encapsulación o etiquetado "tagging", método que es especificado en el estándar de la IEEE802.1Q-1988, ***Virtual Bridged Local Area Networks***.

- **Tipo de VLAN**

El 802.1Q es independiente del tipo de VLAN. Este define las reglas del etiquetado y también soporta priorización del tráfico vía bits de prioridad adicionales dentro de la cabecera del 802.1Q.

- **El 802.1Q y el 802.1d**

El 802.1Q especifica un único Spanning Tree para todos los puertos dentro de una VLAN.

Resumiendo el 802.1Q

-Define las reglas del etiquetado basado en los puertos.

-Provee un acercamiento o planteo estandarizado para extender las VLANs.

-Es independiente del tipo de VLAN.

-Soporta priorización del frame.

-Extiende las VLANs para las estaciones finales.

-Especifica un único spanning tree para todos los dispositivos conectados.

-Especifica que múltiples VLANs pueden ser configuradas dentro del dominio de Spanning Tree.

- **ESTRUCTURA DEL IEEE 802.1Q : ETIQUETADO DEL FRAME**

  - **Introducción**

El IEEE 802.1Q especifica la adición de 2 campos de 2 byte dentro de la cabecera del Ethenet estándar. Los 2 campos son:

TPID (Tag Protocol Identifier)

TCI (Tag Control Information)

Los switches de la serie Passport 8000 soportan la especificación IEEE 802.1Q para frames etiquetados, el cual define un método para la coordinación de las VLANs a través de varios switches.

En esta especificación 4 octetos adicionales son insertados en la cabecera de un frame, después del campo con la dirección fuente y antes del campo tipo de frame. Como es mostrado en la figura 4.2.4.2.

La etiqueta "tag" contiene la Identificación de la VLAN (VLAN ID), con el cual el frame es asociado. Por la coordinación de las VLAN IDs a través de varios switches, podemos extender las VLANs a través de múltiples switches.

  - **El campo TPID**

El IEEE tiene especificado un valor para el campo Etiqueta identificadora del protocolo "TPID Tag Protocol Identifier" de 81-00 (hex).

  - **El campo TCI**

El campo Etiqueta de información de control "TCI Tag control information" contiene un único valor global, usando los últimos 12 bits del TCI, el cual identifica

a la VLAN en todo el dominio switchado o conmutado. Podemos asignar este valor durante el proceso de configuración de la VLAN. El campo prioridad usa los 3 primeros bits para dar prioridades desde 0 hasta 7. El campo CFI "canonical field indicator" indica si la dirección esta en formato canónico o no canónico.

- **Máximo tamaño del paquete.**

La adición de los 4 bytes requeridos por los campos TPID y TCI sube la posibilidad de generación de frames más grandes que 1518 octetos de longitud, que es el máximo tamaño de paquete permitido por ethernet. Equipamientos antiguos que no reconocen frames grandes desecharán los paquetes etiquetados por ser paquetes demasiado grandes. En otras palabras el Etiquetado de un frame adiciona cuatro octetos a un frame, haciéndolo más grande que el máximo tamaño del frame tradicional. Estos frames son a veces referidos como frames "baby giant". Si un dispositivo no soporta el etiquetado IEEE 802.1Q, este puede tener problemas para la interpretación de los frames etiquetado y para recibir los frames "baby giant".

En el switch de la serie Passport 8000 para que los frames etiquetados o los frames no etiquetados sean enviados o recibidos, depende de que lo configuremos a nivel del puerto. El etiquetado es configurado como verdadero "True" o falso "False" en el puerto y es aplicado a todas las VLANs sobre ese puerto.

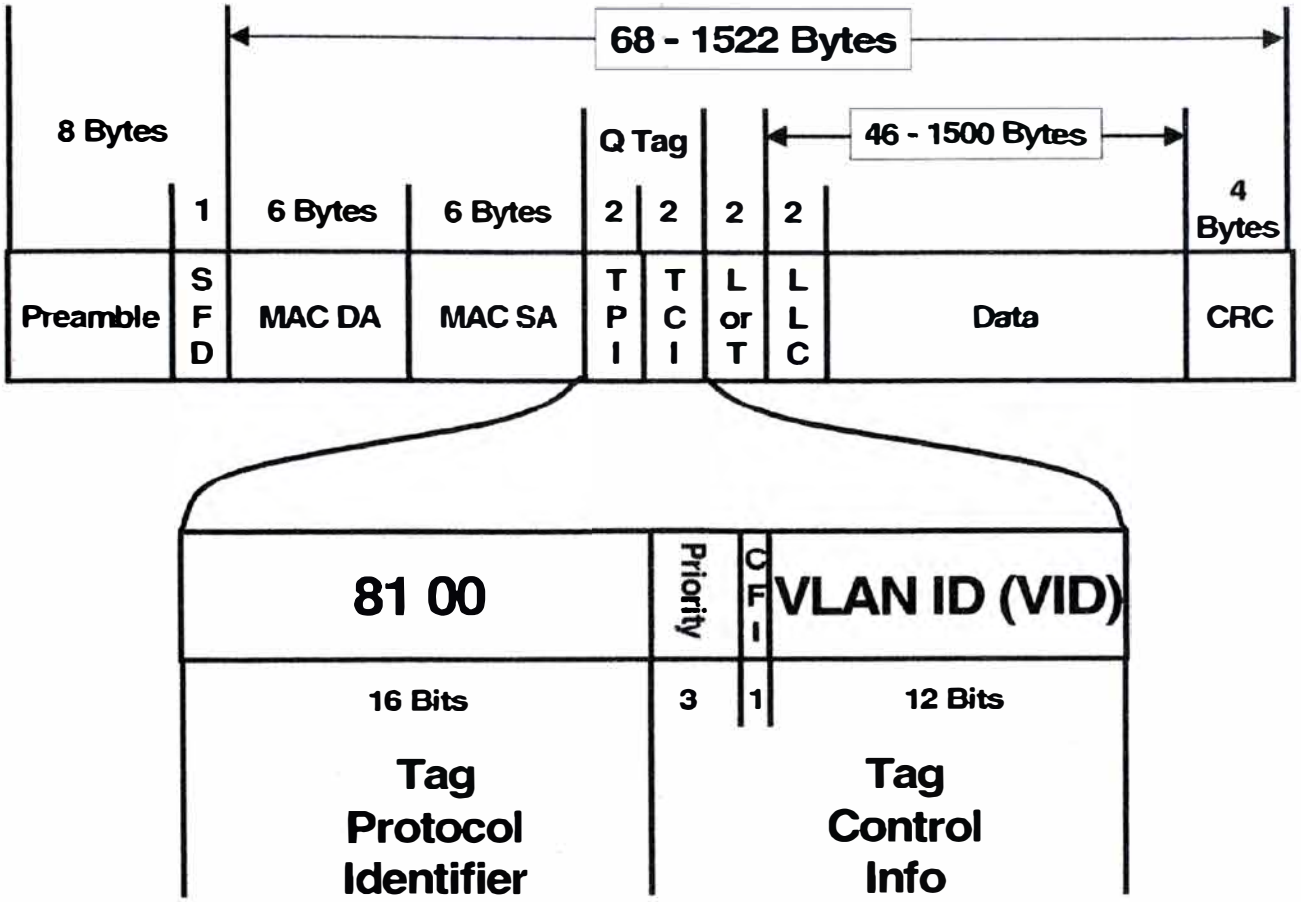


Figura 4.2.4.2 Estructura del IEEE 802.1Q Etiquetado del frame

Hay que resaltar que cuando habilitamos el etiquetado sobre un puerto no etiquetado, las configuraciones previas de las VLANs, como el STGs y MLTs del puerto son perdidas. Además el puerto se resetea y ejecuta el protocolo Spanning Tree, quebrando así la conectividad mientras el protocolo vaya desde los estados de bloqueo y aprendizaje al estado de envío.

Un puerto del switch de la serie Passport 8000 con el etiquetado habilitado envía frames etiquetado. Debido a que todos los frames son explícitamente

etiquetados con una VLAN ID, los puertos etiquetados son típicamente usados para multiplexar tráfico perteneciente a múltiples VLANs hacia otros dispositivos compatibles con el IEEE-802.1Q.

Un puerto del switch de la serie Passport 8000 con el etiquetado deshabilitado no envía frames etiquetado. Un puerto no etiquetado es usado para conectar switches de la serie Passport 8000 a dispositivos que no soporten el Etiquetado IEEE802.1Q. Si un frame etiquetado es enviado hacia un puerto externo que esta configurado con el etiquetado colocado en falso"False", el switch Passport remueve la etiqueta "tag" del frame antes de enviarlo fuera del puerto.

- **VLANS EN EL SWITCH PASSPORT**
  - **Reglas para las VLANs**

Las siguientes reglas gobiernan la configuración de las VLANs sobre el switch Passport 8600 capa 3:

- Soporte de VLANs por Switch Passport capa 3:

  -**Passport 8600**: VLAN por default + 2013 VLANs definidas por el usuario.

  - **Passport 1000**: VLAN por default + 123 VLANs definidas por el usuario.

- Cada adicional Spanning Tree Group (STG) creado reduce el máximo numero de VLANs en uno.
- VLANs y troncales Multi-enlaces "MLT Multi-Link Trunk"

  -**Passport 8600**: Cada VLAN con un puerto MLT reduce el número

máximo de VLANs en ocho.

- Passport 1000: Cada VLAN con un puerto MLT reduce el número máximo de VLANs en cuatro.

- Una VLAN debe estar en solo un grupo de Spaninng Tree (STG).
- Los grupos de Spaninng Tree (STGs) no conocen acerca de VLANs.
- La VLAN por default (VID=1) y la VLAN no designada "unassigned" no pueden ser deleteada.

- **TIPOS DE PUERTOS**
  - **Tipo de puerto**

    Los puertos L2 en el switch Passport 8600 capa 3 son de 2 tipos :

    -De acceso

    -Etiquetado "Tagged" (Tambien conocido como Trunk ó puerto 802.1Q)

  - **Puertos de Acceso**

Un puerto de acceso puede ser un miembro de una y sola una VLAN del mismo tipo "like-type VLAN".

Estos puertos pueden ser usados para conexiones de estaciones finales o segmentos de LAN compartida.

Las reglas que rigen para los puertos de acceso son :

-Puede haber un y solo un grupo de spaninng tree (STG) por puerto de acceso.

-No más de una VLAN del mismo tipo de cualquiera de los tipos de VLANs.

-Los BPDUs en los grupos de STG son "estándar"

-Los data-frame no son etiquetados "tagged".

-Los data-frames etiquetados que son recibidos pueden ser colocados en una VLAN definida por el usuario basadas en puertos (Default VID = 1).

- **Puertos Etiquetados**

Un puerto etiquetado "tagged" puede ser miembro de cualquiera y de todas las VLANs y de todos los grupos de STGs.

Los puertos etiquetados son usados mayormente para extender las VLANs entre los switches.

Las reglas que rigen para los puertos etiquetados son

-Cualquiera o todas las VLANs definidas sobre un switch puede ser definida sobre un puerto etiquetado.

-Cualquiera o todos los grupos de STGs definida sobre un switch puede ser definido sobre un puerto etiquetado.

-Los BPDUs desde el grupo STG1 son trasmitida como "estándar"

-Los BPDUs desde el grupo STG2 y superiores tienen una etiqueta "tag" no estándar insertado.

-Los data frames transmitidos son todos etiquetados.

-Los data frames no etiquetados recibidos pueden ser colocados en una VLAN definida por el usuario basada en puertos (Default VID=1)

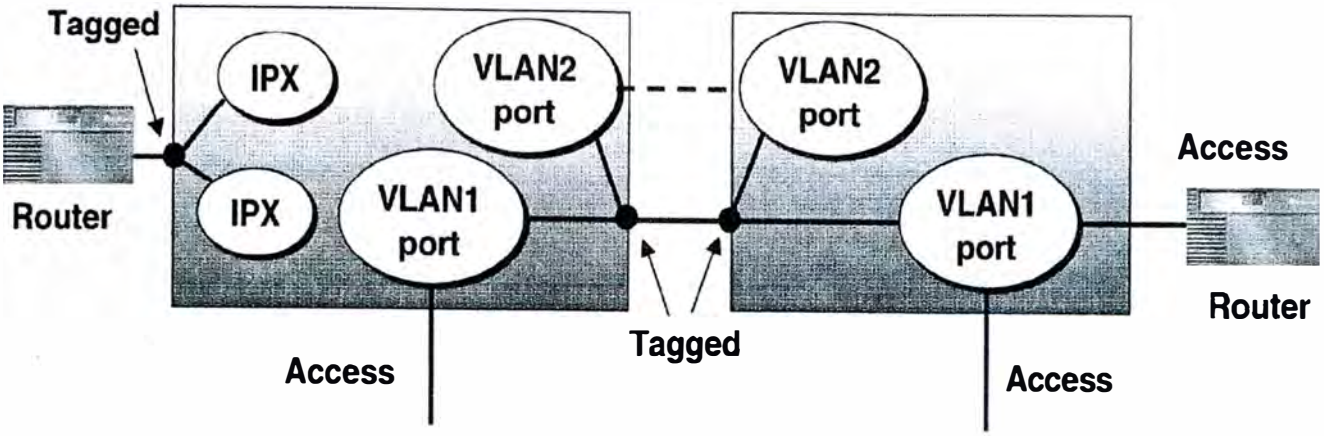


Figura 4.2.4.3 Tipos de puertos

4.2.5 COMO LOS SWITCHES DETERMINAN LA MEMBRESÍA DE LA VLAN

- **MEMBRESÍA DE LA VLAN**

La membresía de la VLAN o la pertenencia a una VLAN de un data frame entrante es determinado examinando la configuración del switch y también examinando el contenido de la cabecera del paquete. Una vez que la membresía de la VLAN es determinada, el frame puede ser enviado hacia su destino.

En la figura 4.2.5.1 se muestra el proceso de decisión que hace el switch Passport para decidir la pertenencia de un data frame a una VLAN.

Los switches Passport intentan asociar los frames con una VLAN en el siguiente orden:

- **¿EL TIPO DE FRAME ES ERRADO?**

Podemos hacer que los puertos de los switches Passport sean configurados tanto como puertos etiquetado o como puertos de acceso. Si un data frame etiquetado es visto sobre un puerto de acceso o si un data frame no etiquetado es visto sobre un puerto etiquetado, la membresía de la VLAN es determinada considerando los parámetros de configuración a nivel de puertos **Discard Tagged Frames** en los puertos de acceso ó **Discard untagged Frames** en los puertos etiquetados Si están configurados en **Falso** , el tipo de frame "erróneo" será colocado en una VLAN definida por la variable a nivel de puerto **DefaultVlanID**. Esta VLAN ID (VID) debe referenciar a una VLAN basada en puertos. Los valores por default de este parámetro son configurados para colocar los frames "erróneos" en la VLAN 1 (VID=1).

Remarcando el tratamiento de los frames etiquetados o no etiquetados por parte del Switch Passport, diremos que este asocia un frame con una VLAN basada en la data contenida del frame y la configuración del puerto destino. Si el frame es etiquetado o no-etiquetado dictamina como ese frame es tratado.

Si un frame etiquetado es recibido sobre un puerto etiquetado con una VLAN ID especificado en la etiqueta "tag", el switch Passport 8000 lo direcciona hacia esa VLAN, si esta presente. Para un frame etiquetado que es recibido sobre un puerto no etiquetado, podemos configurar ese puerto tanto para desechar el frame o para aceptarlo. Si escogemos, No desechar el frame, el switch envía el frame a la VLAN identificada en la etiqueta "tag" del frame.

Para frames no etiquetados, la membresía de la VLAN esta implicada en el contenido propio del frame. Para frames no etiquetados recibidos sobre un puerto etiquetado podemos configurar el puerto tanto para desechar o aceptar el frame. Si configuramos un puerto etiquetado para aceptar frames no etiquetados, el puerto debe ser asignado a una VLAN basada en el puerto en el grupo Spanning tree 1 "STG1".

Como el frame es enviado , esta basado en la VLAN sobre el cual el frame es recibido y sobre las opciones de envío disponibles para esa VLAN.

- **¿EL FRAME ESTA ETIQUETADO?**

Cuando un paquete arriba sobre un puerto etiquetado, podemos decir inmediatamente a que VLAN pertenece simplemente mirando o examinando la etiqueta del 802.1Q.

- **¿EL FRAME PERTENECE A UNA VLAN BASADA EN LA MAC FUENTE?**

El data frame será un miembro de una VLAN basada en la MAC si la dirección fuente concuerda con una dirección MAC configurada y asignada por el usuario a una VLAN particular.

- **¿EL FRAME PERTENECE A UNA VLAN BASADA EN LA DIRECCIÓN IP DE LA SUBRED FUENTE?**

Si una VLAN basada en la dirección IP de la subred fuente es definida sobre el puerto y la dirección de la subred fuente concuerda con la dirección configurada

para la VLAN, entonces el data frame será un miembro de la VLAN. Puede haber muchas VLANs basadas en la dirección IP de la subred fuente definidas sobre un puerto de acceso. Esto es similar al multinetting sobre un ruteador.

- **¿El FRAME PERTENECE A UNA VLAN BASADA EN EL PROTOCOLO?**

Para determinar si el frame entrante pertenece a una VLAN basada en el protocolo, el switch examinará el campo Tipo de protocolo en la cabecera del paquete. Si el campo Tipo de protocolo del frame concuerda con una VLAN basada en el protocolo definida sobre el puerto de ingreso, entonces la membresía de la VLAN es establecida.

- **¿El FRAME PERTENECE A UNA VLAN BASADA EN EL PUERTO?**

Si el campo Tipo del paquete no concuerda con una VLAN basada en política definida y configurada sobre el puerto de ingreso ó ninguna VLAN basada en política está configurada sobre el puerto, entonces el paquete es hecho un miembro de la VLAN basada en el puerto asignada al puerto de ingreso.

Si el frame no reúne ninguno de los requisitos listados arriba, es entonces desechado.

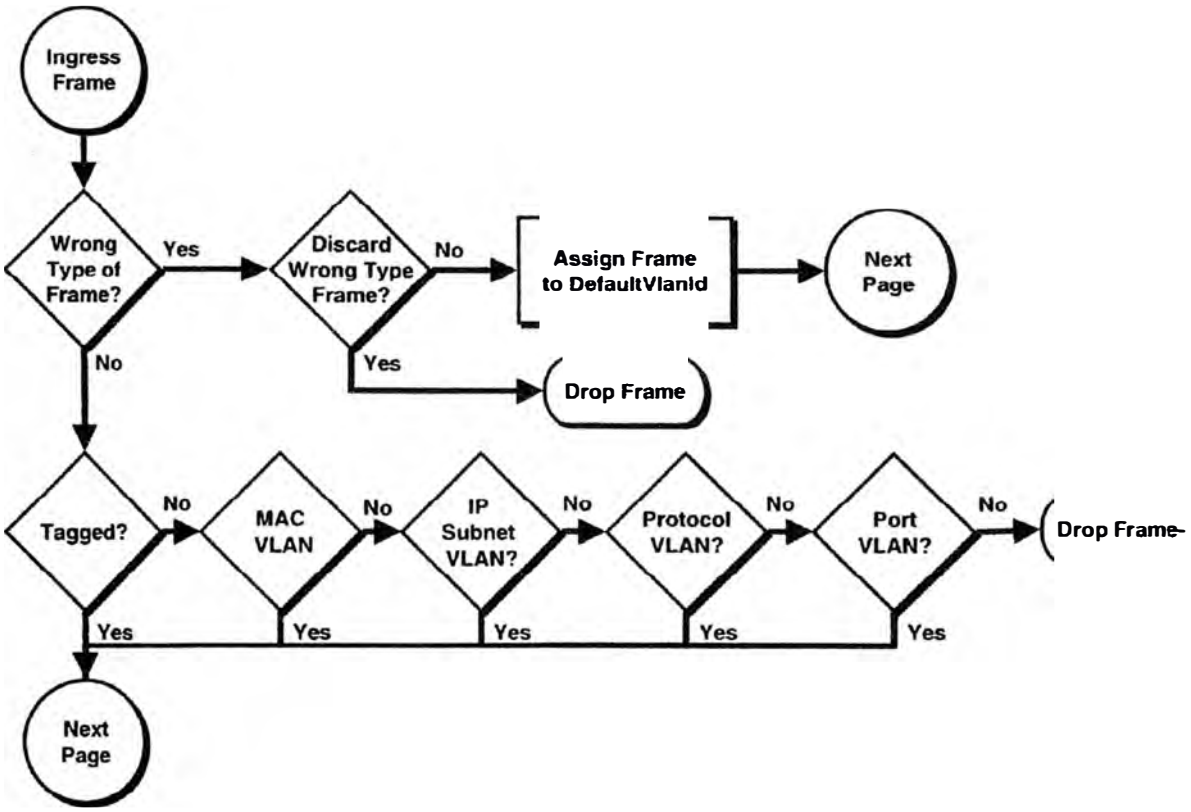


Figura 4.2.5.1 Proceso de decisión de membresía

4.2.6 ENVÍO (FORWARDING) EN L2 O L3?

- **DECISIÓN DE ENRUTAMIENTO**

Una vez que el frame entrante ha sido identificado como perteneciente a una VLAN con el enrutamiento IP habilitado, el ARU ejecuta una decisión de enrutamiento, decidiendo si el paquete necesita ser enrutado y por lo tanto por cual capa L2 o L3.

- **¿ES MIO EL MAC DESTINO?**

Si la dirección MAC destino es la dirección de la misma interfase del router, existen dos posibilidades:

- Que este sea un paquete de administración para el switch L3.
- Que este sea un paquete a ser enrutado usando L3.

Si la dirección MAC destino no es la dirección de la entidad de ruteo, el paquete será manejado en capa L2.

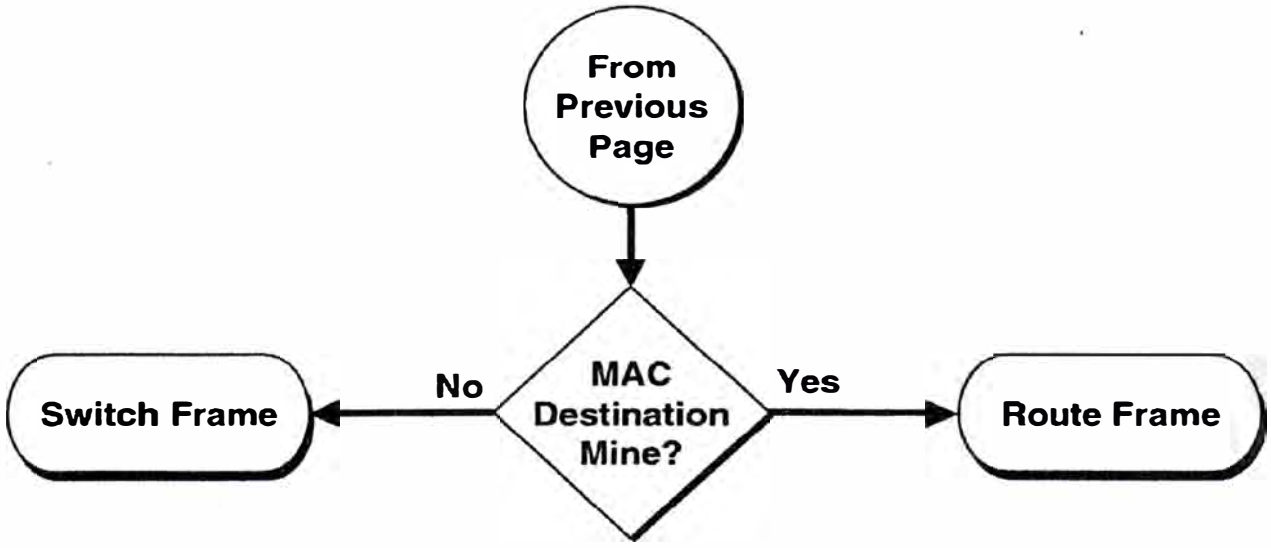


Figura 4.2.6.1 ¿Envío (Forwarding) en L2 o L3 ?

4.2.7 ENRUTAMIENTO IP E IPX

Los switches Passport 8600 capa 3 ,que son los switches con que se implementó este proyecto, soportan tanto enrutamiento IP como enrutamiento IPX.

- **ENRUTAMIENTO IP Y LAS VLANS**

Los módulos del switch Passport 8600 capa 3, soportan enrutamiento IP solo en los siguientes tipos de VLANs:

- VLANs basadas en el puerto.
- VLANs basadas en la dirección IP de la subred fuente.
- VLANs basadas en el protocolo IP.
- VLANs basadas en la dirección MAC fuente.

El enrutamiento IP no es soportada sobre VLANs basadas en otros protocolos, incluyendo el IP versión 6 y en las VLANs basadas en el protocolo definida por el usuario.

- **ENRUTAMIENTO IPX Y LAS VLANS**

Los módulos del switch Passport 8600 capa 3, soportan enrutamiento IPX sobre VLANs basadas en el protocolo IPX y sobre VLANs basadas en el puerto.

El número de red IPX es asociado con una VLAN, y esta puede consistir de uno o mas puertos con uno de los cuatro formatos de frames soportados: Ethernet II, 802.3-SNAP, 802.2-RAW y 802.3-LLC.

Podemos configurar hasta cuatro VLANs basadas en el protocolo IPX sobre un puerto así como también configurar que cada una de estas VLANs usen un

encapsulamiento IPX diferente. Con VLANs basadas en el puerto, podemos asociar la misma VID con cualquier de los cuatro o todos los formatos de encapsulación IPX

Podemos configurar VLANs basada en el protocolo IPX y VLANs basada en el puerto, sobre el mismo puerto, pero el trafico enrutará hacia la VLAN basada en el protocolo y no a la VLAN basada en el puerto, dado que la VLAN basada en el protocolo tiene precedencia sobre la VLAN basada en el puerto.

4.2.8 EL PROTOCOLO SPANNING TREE (STP)

- **SOBREVISTA**

Podemos controlar las redundancias de rutas para las VLANs implementando el Protocolo Spanning Tree (STP), y una red puede incluir múltiples instancias de STP. La colección de puertos en una instancia de spanning tree es llamada un grupo de Spanning Tree (STP).

Los switches Passport 8600 capa 3 ,que son los switches con que se implementó este proyecto, soportan el protocolo STP y hasta 25 grupos de Spanning Tree.

Los switches Passport 8100 capa 2 , soportan el protocolo STP y solo un grupo de Spanning Tree.

Como es definido en el estándar IEEE 802.1d el protocolo Spanning Tree detecta y elimina lazos lógicos en una red bridged o conmutada (switched). Cuando múltiples rutas existen, el algoritmo spanning tree configura la red para que un bridge o un switch use solo la ruta más eficiente. Si esa ruta falla, el protocolo

automáticamente reconfigura la red haciendo que otra ruta sea activada, manteniendo así las operaciones de red.

El algoritmo Spanning Tree crea una topología lógicamente libre de lazos habilitando una ruta única a través de la red extendida y deshabilitando las rutas paralela(s) que crean el lazo. El algoritmo produce una topología de árbol lógico fuera de cualquier arreglo físico de bridges y LANs.

El algoritmo Spanning Tree provee un alto grado de tolerancia a fallas permitiendo la reconfiguración automática de la topología del Spanning Tree alrededor de un bridge fallado o ruta de datos, o en respuesta a una nueva y posible mejor ruta que esta siendo disponible. Este proceso es conocido como reconvergencia.

Una vez que la topología del Spanning Tree ha reconvergido, todos los dispositivos en la red extendida otra vez serán hábiles de comunicarse unas con otras. Sin embargo el envío de paquetes es detenido durante la reconvergencia para prevenir que la red se caiga debido a los lazos de brigde.

El algoritmo del Spanning Tree es inicializado automáticamente cuando los bridges son encendidos o cuando hay un cambio en la topología que afecta al árbol.

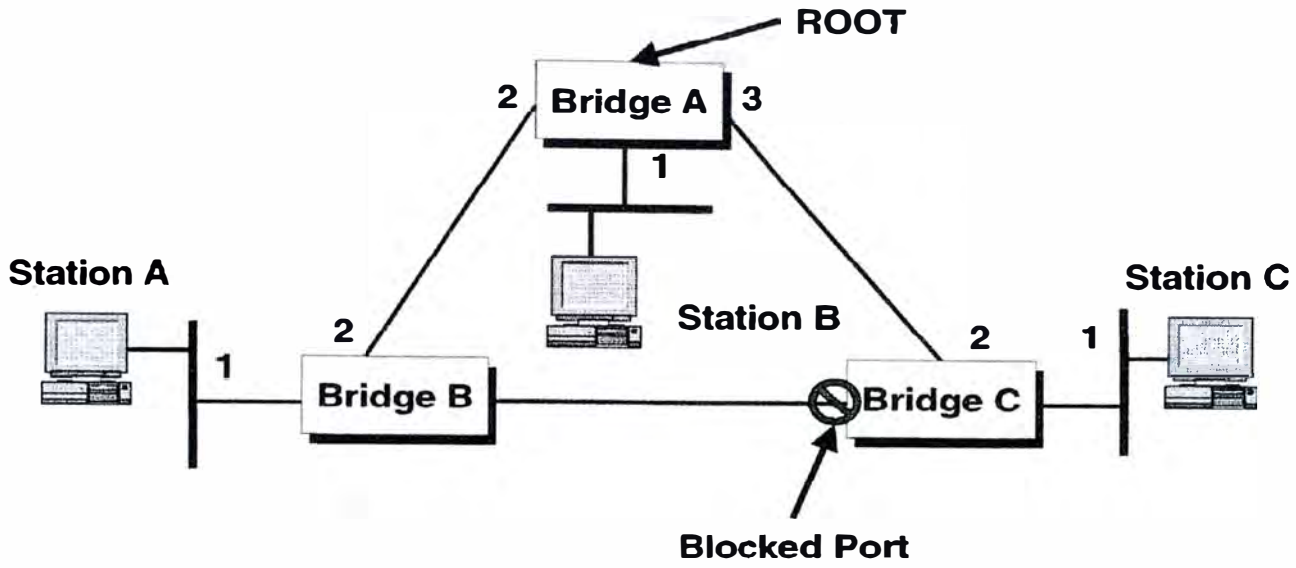


Figura 4.2.8.1 El algoritmo de Spanning tree

- **GRUPOS DE SPANNING TREE**

Los switches Passport 8000, que son los switches con que se implementó este proyecto, soportan el protocolo STP tal como es definido en IEEE 802.1d. Además un switch Passport 8000 puede soportar un grupo de de Spanning Tree (STG), el cual es una colección de puertos que pertenecen a la misma instancia de un STP.

Con los módulos del switch Passport 8600, múltiples STGs son posibles dentro del mismo switch; esto es, Switch capa 3 puede participar en la negociación para multiples spanning trees. En la figura 4.2.8.2 se muestra múltiples grupos de spanning tree.

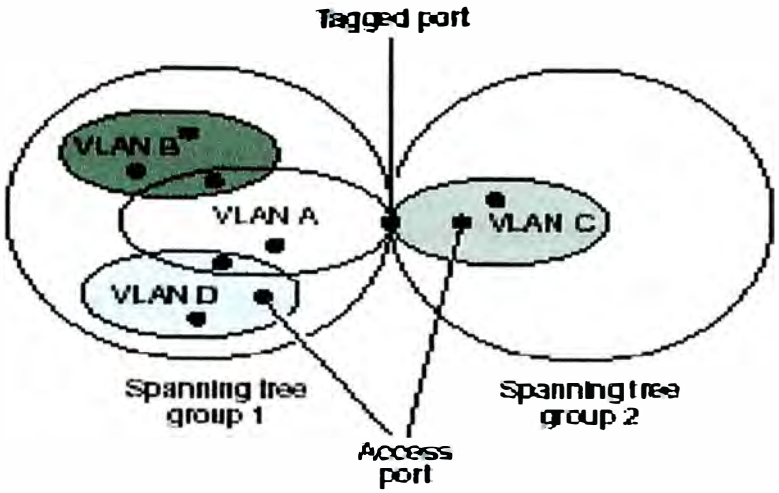


Figura 4.2.8.2 Múltiples grupos de Spanning Tree

- **VLANS Y EL PROTOCOLO SPANNING TREE**

Los puertos asociados con una VLAN y las VLANs mismas deben estar contenidos dentro de un único grupo de Spanning Tree. Al no permitir que una VLAN se esparza a través de múltiples STGs evita los problemas de los puertos bloqueados por el Spanning Tree que puedan causar una perdida de conectividad dentro de la VLAN.

Cada puerto no etiquetado puede pertenecer a uno y solo un STG, mientras que los puertos etiquetados pueden pertenecer a mas de un STG. Cuando un puerto etiquetado pertenece a mas de un STG, los BPDUs ("Bridge Protocol Data Units" mensajes de configuración usados por los bridges para calcular un Spanning Tree) son etiquetados para distinguir los BPDUs de un STG con respecto a los otros STGs.

Los BPDUs del STG 1 no son etiquetados. Los BPDUs etiquetados son transmitidos usando una dirección MAC multicast como los frames etiquetados con una VLAN ID, y podemos especificar la dirección MAC multicast y la VLAN ID. Debido a que los BPDUs etiquetados no son parte del estándar IEEE 802.1D, no todos los dispositivos pueden interpretar los BPDUs etiquetados.

Podemos habilitar o deshabilitar el protocolo Spanning Tree en el puerto o al nivel de grupo de spanning tree. Si deshabilitamos el protocolo al nivel de grupo, los BPDUs recibidos sobre un puerto que esta en un STG fluyen a los otros puertos en ese STG como frames multicast regular. Cuando deshabilitamos el protocolo al nivel de puerto , los BPDUs recibidos sobre ese puerto son descartados.

Para determinar el flujo de la data entre los dispositivos, el protocolo Spanning Tree (STP) debe primero determinar el switch root así como también los puertos root de todos los dispositivos participante. Todos los puertos L2 , por default, están en el mismo grupo de Spanning Tree (STGID = 1) independientes de su membresía en las VLANs.

Esto puede tener el resultado ilustrado en la figura 4.2.8.3 . En este ejemplo, tres switches Passport L3 , cada uno con dos VLANs, están interconectados. Debido a que los puertos usados son miembros de las VLANs por las conexiones, el protocolo Spanning Tree corriendo sobre cada switch ve los otros dispositivos 802.1d; por lo tanto un root es elegido y cada bridge escoge un puerto root.

En el ejemplo de la figura 4.2.8.3 los miembros de la VLAN3 no se comunican entre los switches debido al puerto bloqueado.

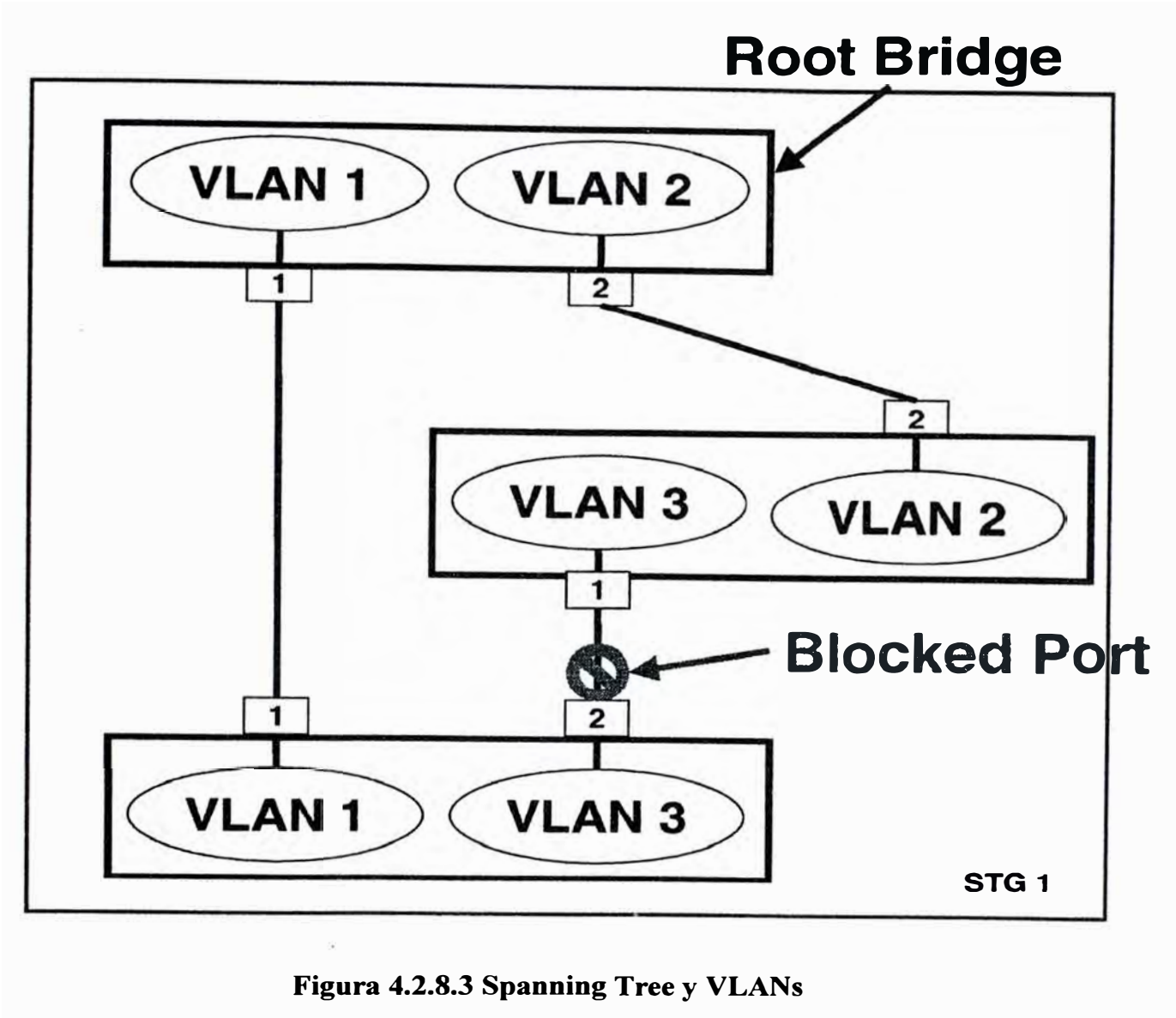


Figura 4.2.8.3 Spanning Tree y VLANs

- **SOLUCIONES AL PROBLEMA DE SPANNING TREE**

Podemos resolver el problema del Spanning Tree en al menos 4 maneras, dependiendo de los requerimientos del diseño de la red.

- **Crear un Grupo de Spanning Tree por cada VLAN**

Al crear un grupo de Spanning Tree por cada VLAN, los puertos bloqueados son evitados debido a que cada STG trabaja solo dentro de si mismo. Desde el punto de vista del STG, ningún lazo es detectado. La figura 4.2.8.4 muestra un ejemplo.

Podemos usar múltiples STGs junto con el el 802.1Q "tagging" para proveer un método de bridging de protocolos no ruteables entre dispositivos.

- **Deshabilitar el Spanning Tree en cada Switch**

Si el diseño de la red es tal que no hay necesidad del STP en la red, entonces podemos deshabilitar el STP sobre todos los switches. Este método trabaja, pero con el STP deshabilitado sobre el switch , la detección y prevención de los lazos no ocurren y la red puede estar sujeto a problemas en el futuro.

- **Crear Puertos de Router aislado o puertos Brouter para la interconexión de los switches**

Si IP es el único protocolo a ser usado entre los switches Passport capa 3, podemos usar puertos de router aislado (o puertos brouter discutido posteriormente) para vencer al Spanning Tree . Por el apropiado uso de los protocolos de ruteo tales como RIP y OSPF, rutas redundantes pueden ser mantenidas sin contar con el STP.

- **Deshabilitar el protocolo Spanning Tree sobre los puertos de interconexión.**

Cuando el STP es deshabilitado sobre los puertos de interconexión, los BPDUs no son trasmitidos sobre esos puertos. Esto tiene el efecto de prevenir que el Spanning Tree detecte lazos.

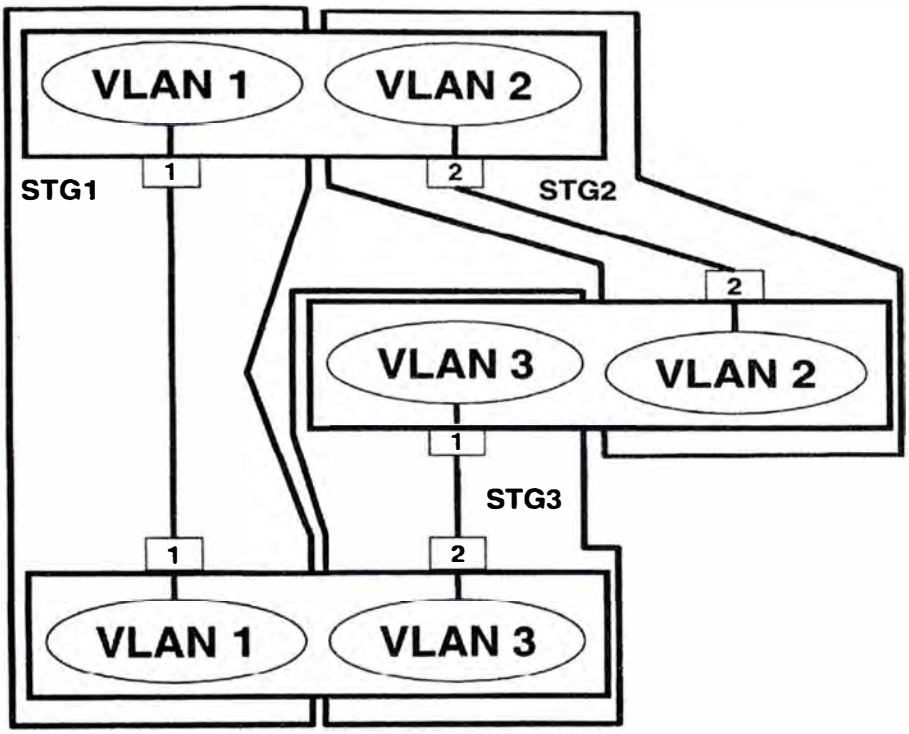


Figura 4.2.8.4 Usando Grupos de Spanning Tree.

- **CARACTERÍSTICA DEL SPANNING TREE FASTSTART**

El Spanning Tree FastStart es un modo de puerto mejorado propietario de los switches Passport capa 3 de Nortel Networks . Si el Spanning Tree FastStart es habilitado sobre un puerto, el puerto es puesto en el estado de envío mas rápidamente siguiendo la inicialización del switch capa 3 o una reconvergencia del Spanning Tree. El puerto va a través de los estados normales de bloqueo y aprendizaje antes del estado de envío , pero los tiempos de mantenimiento para estos estados es el bridge hello timer (2 segundos por defecto) en vez del bridge forward delay timer (15 segundos por defecto). Habilitando FastStart permite convergencia más rápida sobre cambios de topología. FastStart es útil sobre puertos de acceso donde solo un

dispositivo es conectado al switch (como en estaciones sin ningún otro dispositivo con Spanning Tree) y donde no se desea esperar los 30 a 35 segundos usuales para la inicialización del Spanning Tree y aprendizajes de los bridges.

Un puerto que tiene la característica de FastStart envía BPDUs en intervalos estándar.

El puerto se activa así mismo en el estado de envío, permitiendo que el trafico normal de los datos pase.

Si el puerto detecta un BPDU entrante, este inmediatamente revierte al estándar Spanning Tree 802.1d, y va a través de los estados de escucha y aprendizaje del estándar antes de decidir de colocar el puerto en estado de envío o de bloqueo.

- **VLANS ESPECIALES EN LOS SWITCHES DE LA SERIE PASSPORT 8000**

Los switches de la Serie Passport 8000 tienen tres VLANs predefinidas que se comportan diferentemente de las VLANs definidas por el usuario. Estas VLANs son la VLAN por defecto "default", la VLAN sin asignar "unassigned" y los puertos brouters. Los puertos brouters son solo disponibles en los módulos de los Passport 8600 capa 3.

- **VLAN por Defecto "Default"**

Los switches Passport 8000 son configurados de fabrica con todos los puertos en una VLAN basadas en puertos llamada la VLAN por defecto. Con todos los puertos en la VLAN por defecto, el switch se comporta semejante a un switch capa 2.

La VLAN ID de la VLAN por defecto es siempre 1 y es siempre una VLAN basada en los puertos. La VLAN por defecto no puede ser borrada.

- **VLAN sin asignar "Unassigned"**

Internamente, un switch de la serie Passport 8000 soporta un placeholder para puertos que es llamado una VLAN basadas en los puertos sin asignar. Este concepto de unassigned es usado para puertos que son removidos de todas las VLANs basadas en los puertos. Los puertos pueden pertenecer a VLANs basadas en políticas así como también a VLAN unassigned. Si un frame no reúne ningún criterio de las políticas y no hay VLAN fundamental basada en los puertos , el puerto pertenece a la VLAN unassigned y el frame es desechado. Solo puertos en la VLAN unassigned no tienen asociación con grupos de spanning tree, así estos puertos no participan en la negociación del protocolo de Spanning Tree; esto es, ningún BPDUs son enviados fuera delos puertos en la VLAN unassigned.

Debido a que la VLAN unassigned es una estructura interna, este no puede ser borrada. Si un grupo de Spanning Tree definida por el usuario es borrado, los puertos son removidos a la VLAN unassigned y puede ser posteriormente asignada a otro grupo de spanning tree. Moviendo los puertos a la VLAN unassigned evita la creación de lazos no deseados y conexiones duplicadas. Si el enrutamiento es deshabilitado en estos puertos, el puerto es completamente aislado y ninguna funcionalidad de capa 2 y capa 3 es proveída.

El concepto de la VLAN unassigned es útil para consideraciones de seguridad o cuando usamos un puerto para monitorear un puerto mirrored.

- **Puerto Brouter**

Otra VLAN especial soportada por los switches de la serie Passport 8000 es un puerto brouter el cual realmente es una VLAN de un puerto. La diferencia entre un puerto brouter y una VLAN basada en el protocolo IP estándar configurado para realizar ruteo es que la interfase de ruteo del puerto brouter no esta sujeto al estado de spanning tree del puerto.

En otras palabras, un puerto brouter es una VLAN de un solo puerto, el cual puede rutear paquetes IP independiente del estado de Spanning Tree del puerto. Un puerto brouter puede estar en estado de bloqueo para trafico bridged mientras continua enviando trafico IP. Esta característica previene de cualquier impacto sobre el enrutamiento IP así los puertos estén en estado de bloqueo con respecto al STP.

Un puerto brouter tiene las siguientes características:

- VLAN basada en el protocolo IP.
- Miembro del grupo de Spanning Tree cero STG0.
- Solo un puerto en la VLAN.
- La data IP no es afectada por el estado STP del puerto.
- El puerto puede ser un miembro de otras VLANs (Se le aplican las reglas normales).

REGLAS DE LAS VLANS

Todas las VLANs en los switches de la serie Passport 8000 operan bajo el siguiente conjunto de reglas básicas:

- En adición a la VLAN por default, los switches de la serie Passport 8000 soportan 2000 VLANs. El rango de las VLAN IDs van desde 1 hasta 4094.
- Si habilitamos etiquetado "tagging" sobre un puerto que esta en una VLAN, la configuración del grupo de Spanning Tree para ese puerto es perdida. Para preservar el asignamiento de los puertos a las VLANs , habilitar etiquetado "tagging" sobre los puertos antes de que asignemos los puertos a las VLANs.
- Un puerto etiquetado "tagged" puede pertenecer a múltiples VLANs y a múltiples grupos de Spanning Tree. Cuando un puerto etiquetado "tagged" pertenece a múltiples grupos de Spanning Tree, los BPDUs son etiquetado "tagged" para todos los grupos de Spanning Tree excepto para el grupo 1 de Spanning Tree. Bajo la configuración por default el grupo de Spanning Tree por default es el numero 1.
- Un puerto no etiquetado "untagged" puede pertenecer a una y sola una VLAN basada en los puertos. Un puerto en una VLAN basada en los puertos puede pertenecer a otras VLANs basadas en políticas.
- Un puerto no etiquetado "untagged" puede pertenecer a una y sola una VLAN basada en política para un protocolo dado. Por ejemplo, un puerto puede pertenecer a sola una VLAN basada en política donde la política es el protocolo IPX802dot2.

En adición a las reglas generales para las VLANs en los switches Passport , las reglas especificas para las VLANs en los módulos de los switches Passport 8600 son las siguientes:

- Por cada VLAN con MultiLink Trunking que creamos, reducimos en ocho el numero de VLANs disponibles.
- Una VLAN no puede esparcirse en múltiples grupos de Spanning Tree. Esto es, los puertos en la VLAN deben estar dentro de un grupo de spanning tree. Los IDs de los grupos de Spanning Tree pueden estar en el rango de valores de 1 hasta 25.
- Una membresía de un frame en una VLAN es determinada en el siguiente orden de precedencia: la ID de la VLAN, luego VLAN basada en la dirección MAC fuente, luego VLAN basada en la IP subnet, luego VLAN basada en el protocolo y luego VLAN basada en los puertos.
- La VLAN basada en la IP subnet no debe ser asignada a una red de transito, una red enrutando a una subred bridged.

En adición a las reglas generales para las VLANs en los switches Passport , las reglas especificas para las VLANs en los módulos de los switches Passport 8100 son las siguientes:

- Una membresía de un frame en una VLAN es determinada en el siguiente orden de precedencia: la ID de la VLAN, luego VLAN basada en el protocolo y luego VLAN basada en los puertos.

4.3 TRONCALES MULTIENLACES "MULTILINK TRUNKINK"

4.3.1 INTRODUCCIÓN AL MULTILINK TRUNKING (MLT)

Multilink Trunking (MLT) es una conexión punto a punto que agrega múltiples puertos para que ellos actúen lógicamente semejante a un único puerto con el ancho de banda agregado. La agrupación de múltiples puertos dentro de un enlace lógico provee un throughput agregado mas alto sobre aplicaciones de switch a switch o de switch a server.

MultiLink Trunking o MLT es un método para utilizar múltiples conexiones físicas entre un par de switches dados o entre un switch y un server con múltiples tarjetas de red (NICs), como un enlace lógico único. Por ejemplo, el MLT puede hacer que 4 enlaces separados de 100 Mbps aparezcan como una única troncal de 400 Mbps. Si uno de los enlaces falla, el ancho de banda agregado es reducido a 300 Mbps, pero la troncal asimismo permanecerá levantada y continuará enviando tráfico tan largo como al menos una conexión física este disponible.

Los protocolos de las capas superiores ven a todo el conjunto del MLT como una única interfase lógica. Por ejemplo si el protocolo de ruteo RIP aprende una nueva ruta sobre uno de los puertos en la troncal, la siguiente interfase de salto es la misma troncal. El puerto real escogido para el envío es transparente al protocolo IP y RIP.

Cuando se viene el tiempo para enviar un paquete sobre una troncal, MLT selecciona el puerto físico realizando un calculo sobre las direcciones en los paquetes. Desde que muchas aplicaciones requieren que los paquetes en una sesión dada arriben en secuencia, MLT consistentemente usan la misma ruta para cualquier

par de direcciones fuente/destino dadas. Sin embargo MLT no conserva las pistas de las sesiones. Este simplemente aplica el mismo algoritmo de selección de ruta a cada paquete, y la misma direcciones siempre es sometida a la misma ruta. Para trafico bridged, el algoritmo usa las direcciones MAC. Para trafico IP o IPX ruteado, las direcciones de capa de red son usadas.

MultiLink Trunking provee los siguientes beneficios:

- El ancho de banda puede ser desplegado en incrementos finos.
- Las troncales agregadas pueden llegar a velocidades de hasta 8 Gigabits (En los Passport 8600) o 4 Gigabits (En los Passport 1000).
- Redundancia en puertos y Módulos.
- Tiempo de convergencia pequeño o no hay tiempo de convergencia cuando adicionamos o removemos enlaces.
- El trafico de los protocolos (STP, RIP, OSPF,etc) es por troncal en lugar de por enlaces reduciendo el overhead.

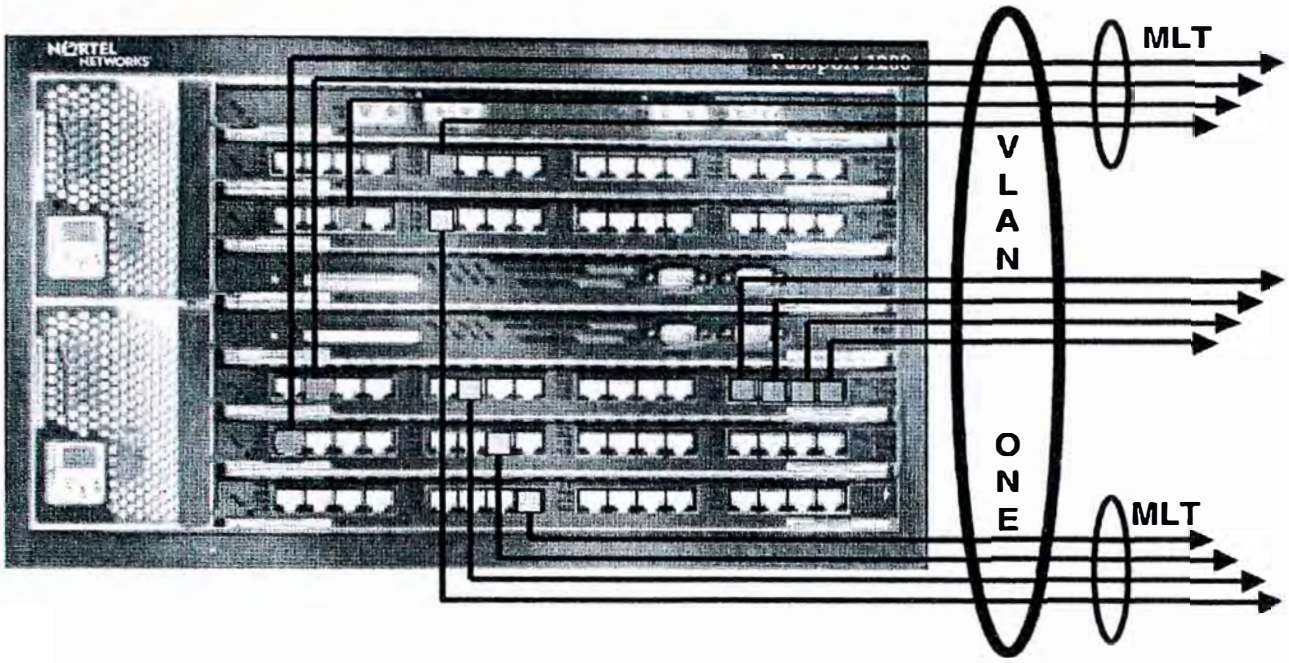


Figura 4.3.1 Passport y MLT

4.3.2 *¿COMO TRABAJA EL MLT?*

- **DIRECCIONES DE APRENDIZAJE Y ENVIO**

Cuando una nueva dirección MAC es aprendida sobre un puerto MLT, esta es ingresada dentro de la base de datos de envío y marcada como aprendida sobre un puerto MLT.

- **Envío en L2**

Cuando un data-frame es enviada en L2, el puerto que será usado en el grupo MLT es determinada por una combinación de las direcciones MAC fuente y destino del data-frame.

- **Envío en L3**

Para el envío en L3, las direcciones IP/IPX fuente y destino son usadas.Todo el trafico para una sesión usa la misma ruta en cualquier dirección dada, asegurando la entrega en secuencia. Sin embargo, múltiples sesiones outbound en el mismo servidor serán distribuidas entre los enlaces.

❑ SPANNING TREE Y MLT

Los puertos dentro de un MultiLink Trunk se comportan como sigue:

- Todos los puertos en el MLT deben pertenecer al mismo grupo de Spanning Tree (Si el Spanning Tree es habilitado).
- Idénticos BPDUs (Bridge Protocol Data Units) salientes son enviados por cada puerto.
- Si BPDUs idénticos son recibidos sobre todos los puertos, el modo MLT es enviado.
- Si ningún BPDU es recibido sobre un puerto o si BPDU etiquetado "tagging" y puertos etiquetados no concuerdan, el puerto individual es tomado fuera de línea.
- El costo de la ruta es inversamente proporcional al ancho de banda del MLT activo. (Por default o configurado por el usuario).

Cuando conectamos los Passport a Servidores o estaciones multi-NIC con MLT, el Spanning Tree debe estar deshabilitado, debido a que diferentes BPDUs son usados para determinar si habilita un puerto.

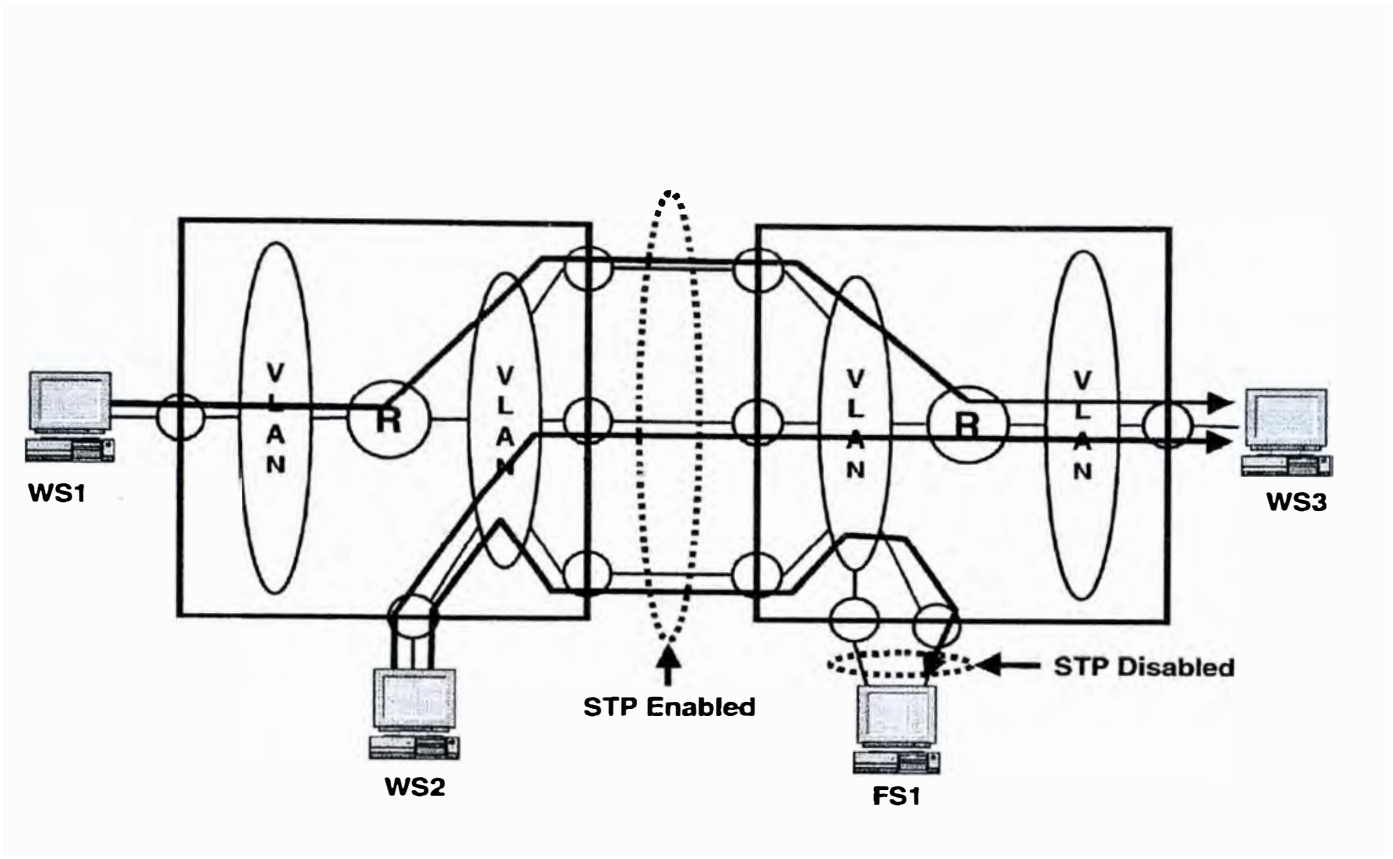


Figura 4.3.2 Selección Mutli-Link

4.3.3 REGLAS DEL MULTILINK TRUNKING

Todos los MLT de los switches de la Serie Passport 8000 operan bajo los siguientes conjuntos de reglas básicas:

- El MLT es soportado sobre puertos 10BASE-T, 100BASE-TX, 100BASE-FX y Gigabit Ethernet.
- Todos los puertos en un MLT deben ser del mismo tipo de medio (cobre o fibra) y tener la misma velocidad y configuración de duplex.
- El MLT es compatible con el protocolo Spanning Tree.
- El IEEE 802.1Q tagging es soportado sobre un MLT.

Para los módulos del SwitchPassport 8600, el MLT tiene las siguientes características y requerimientos generales:

- Hasta 32 grupos de MLT son soportadas con un máximo de 8 puertos del mismo tipo perteneciente a un único MLT.
- Los puertos en un MLT pueden esparcirse a través de los módulos, dando redundancia de módulos.
- Todos los puertos en un MLT deben estar en el mismo grupo de spanning tree, al menos que ellos estén etiquetados "tagged"; entonces ellos pueden pertenecer a múltiples grupos de Spanning Tree (STGs).
- Para tráfico bridged , el algoritmo que distribuye el tráfico a través de un MLT esta basado en las direcciones MAC fuente y destino.
- Para tráfico IP ruteado, el algoritmo que distribuye el tráfico a través de un MLT esta basado en las direcciones IP fuente y destino.

Configurando MLTs reduce el numero de VLANs disponible en el switch. Un switch de la Serie Passport 8000 empieza con 2000 VLANs disponible. Cada MLT reduce el numero total de VLANs disponible en ocho.

Para los módulos del SwitchPassport 8100, el MLT tiene las siguientes características y requerimientos generales:

- Hasta 6 grupos de MLT son soportados con un máximo de 4 puertos del mismo tipo perteneciente a un único MLT.

- Todos los puertos en un MLT deben estar en un grupo de Spanning Tree.
- Para optimizar la performance, el switch distribuirá el tráfico a un MLT sobre el mismo módulo. Si no hay un MLT sobre el módulo, un algoritmo de round robin determina cual MLT debe recibir el tráfico. Este algoritmo esta basado en la dirección MAC fuente y el puerto sobre el cual esa dirección MAC fue aprendida.

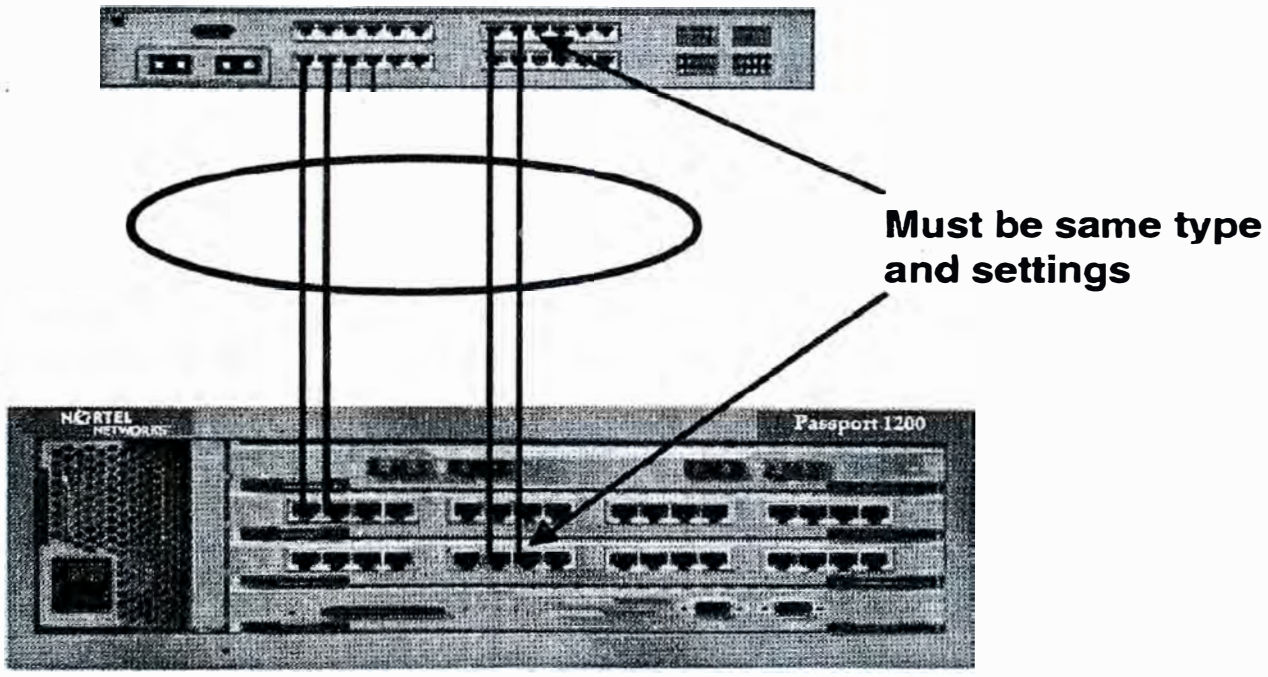


Figura 4.3.3 Interoperabilidad del MLT

4.3.4 *EJEMPLOS DE MULTILINK TRUNKING*

Multilik Trunks nos permite agrupar juntos puertos del switch para formar un enlace a otro switch o servidor , incrementando así el throughput agregado de la interconexión entre los dispositivos. Cuando el protocolo Spanning Tree esta habilitado, el software Multilink Trunking detecta enlaces mal configurados o rotos y remueve el puerto del grupo MLT.

- **Configuración de MLT switch a switch**

Troncales en el Switch Passport 8600 pueden ser configurados con hasta 8 puertos del switch para incrementar el ancho de banda agregado. Las troncales en los switches Passport 8100 pueden soportar hasta 4 puertos del switch.

En la Figura 4.3.4.1 se muestra dos troncales (T1 y T2) conectando el switch S1 a los switches S2 y S3. Cada una de las troncales mostrada en la figura 4.3.4.1 puede ser configurada con múltiples puertos de los switches para incrementar el ancho de banda y la redundancia.

Cuando el tráfico entre la conexión switch a switch aborda o se aproxima a las limitaciones de ancho de banda de un único puerto, creando un multiLink Trunk puede dar el adicional ancho de banda requerido para mejorar la performance.

En conexiones extremadamente ocupadas, podemos instalar más ancho de banda utilizando MLT. Dependiendo del modelo del switch Passport podemos crear troncales capaces de manejar hasta 8 gigabit por segundo entre pares de switches.

Note también el beneficio de la redundacia que entrega el MLT. Sin el MLT, perdida de un solo enlace puede significar reconvergencia de la red como los

protocolos determinen la siguiente mejor ruta de envío. Con MLT, el envío continua y los protocolos de la capa superiores no están consciente de ninguna falla de enlace. Una decisión más sabia es instalar un pedazo de ancho de banda más grande del que necesitamos, para que así la performance no sufra en el caso de una falla del enlace.

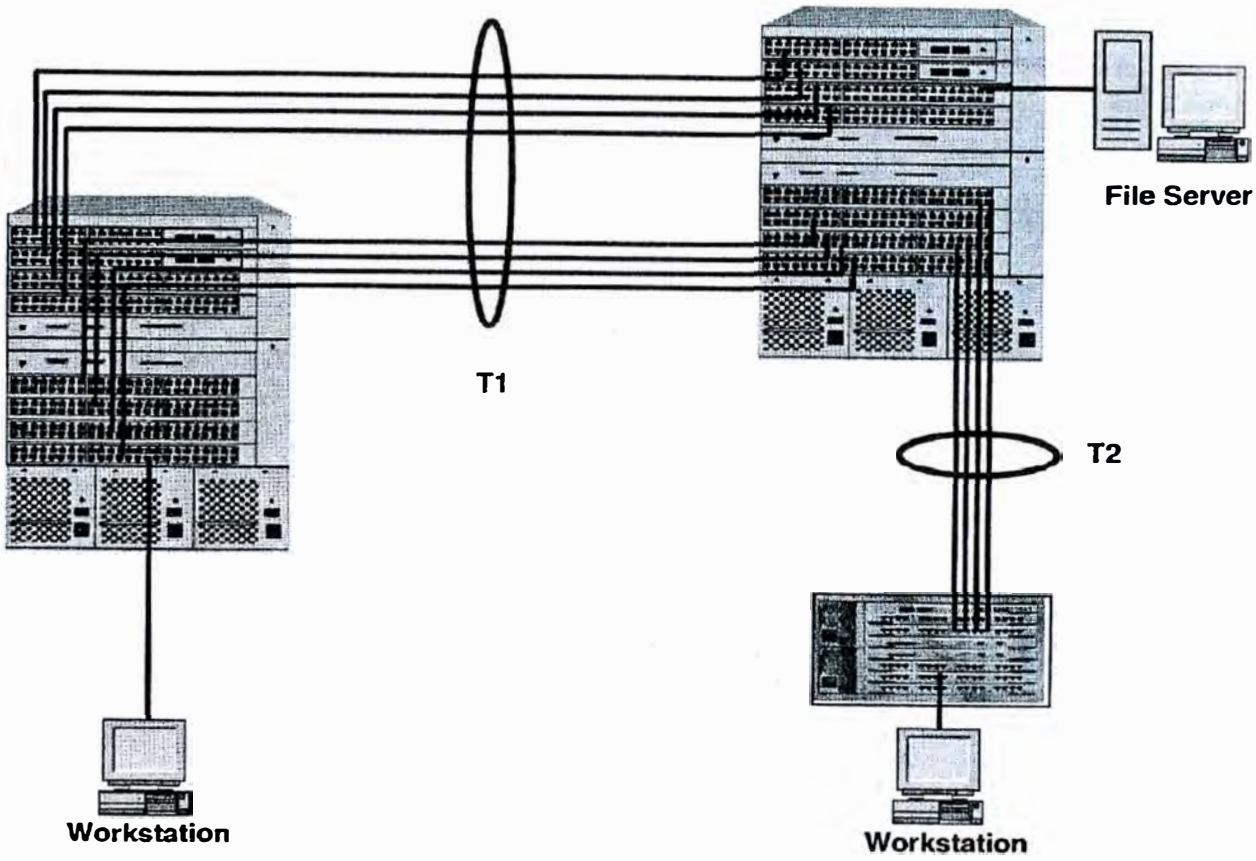


Figura 4.3.4.1 Configuración de MLT switch a switch

- **Configuración de MLT switch a servidor**

La figura 4.3.4.2 muestra una típica configuración de una troncal switch a servidor. En este ejemplo, el File Server FS1 usa direcciones MAC duales, usando una dirección MAC por cada switch. (Este ejemplo es también posible cuando instalamos IP usando direcciones IP duales). MLT no es recomendado en este caso, es decir ningún MLT es configurado en el FS1; Desde que el servidor ve a sus NICs como interfase lógicas separadas el switch Passport debe tratar con ellas separadamente.

El FS2 es un servidor con una única MAC (con una NIC de 4 puertos) y es configurada como una troncal T1. La única MAC significa que los 4 puertos son una entidad lógica, del mismo modo que un switch Passport ve a una troncal. El MLT es ideal para compartir cargas en tales ambientes. Desde que el algoritmo del MLT usa tanto las direcciones fuente y destino, los paquetes desde cualquier cliente dado serán enviados al servidor en secuencia. Sin embargo, múltiples sesiones al mismo servidor viajarán sobre diferentes enlaces, desde que la dirección fuente será diferente.

Note que si solo tres sesiones son activas, no más de tres de los cuatro enlaces estarán llevando tráfico hacia el servidor (el servidor puede escoger cualquier enlace cuando enviamos hacia el switch Passport). Dependiendo de las direcciones especificas en los paquetes, este es aun posible que todos compartirán el mismo enlace; referirse al algoritmo de selección de ruta del MLT si deseamos asignar direcciones en un hecho que evite esta congestión. También , una única sesión con un "big talker" puede potencialmente saturar un enlace dado, mientras los otros

enlaces en la troncal son subutilizados. Esta es una función de usar la selección de rutas basadas en direcciones, en lugar del round robin. Sin embargo, en una red corporativa típica con un servidor manejando muchos clientes, la ley de probabilidad tiende a la distribución del tráfico entre los enlaces disponibles.

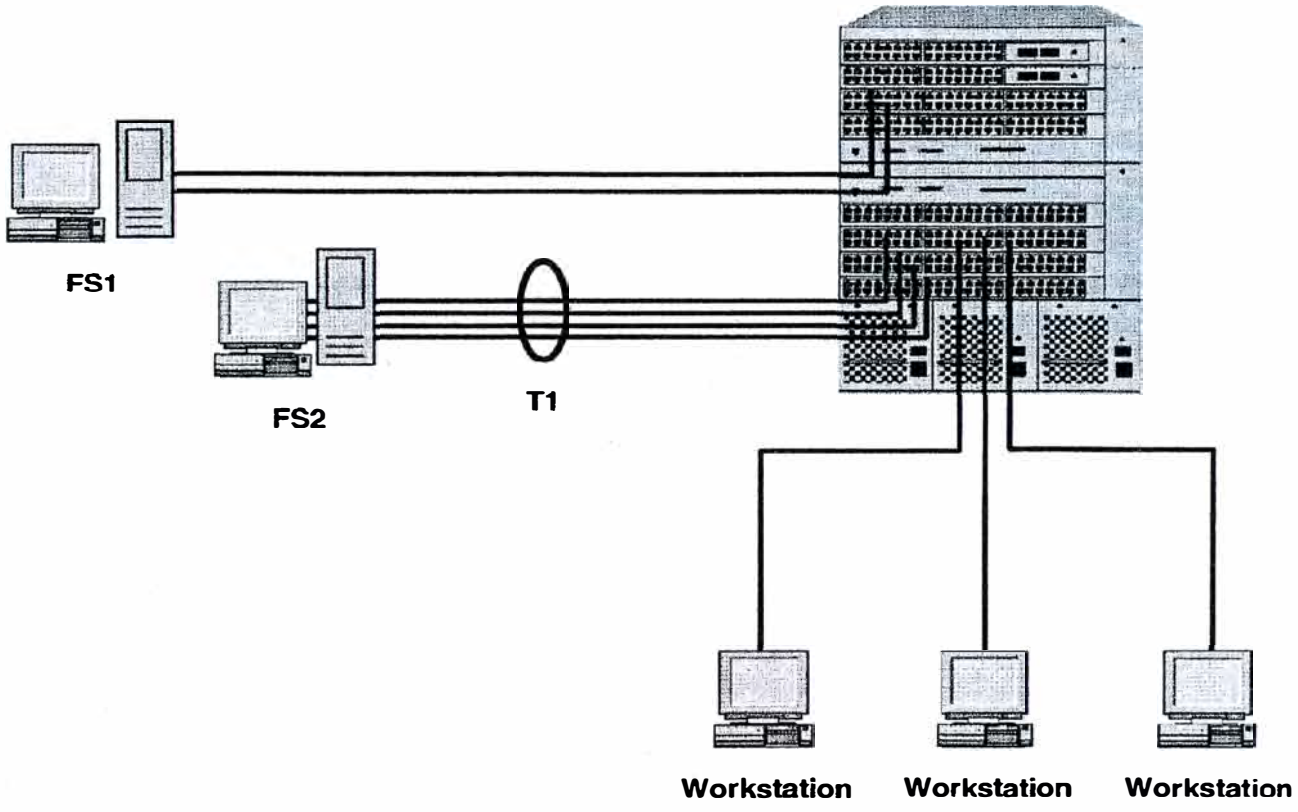


figura 4.3.4.2 Configuración de MLT switch a Server

4.4 ENRUTAMIENTO IP

4.4.1 LA FUNCION DE ENRUTAMIENTO

- **CREANDO LA INTERRED CORPORATIVA**

Como ya hemos visto, dispositivos tales como los switches capa 2 (L2) y bridges pueden ser usados para crear una red de área local virtual (VLAN) que se esparce en múltiples segmentos físicos. Este resuelve el problema de conectividad pero tiene ciertas limitaciones inherentes. Por ejemplo una red plana L2 es un único dominio de broadcast; un broadcast desde cualquier estación debe ser fluida a lo largo de la VLAN, consumiendo recursos de la red y de las estaciones finales. También cada switch y bridge deben mantener una base de datos de envío (FDB) conteniendo la dirección MAC de cada dispositivo en la red. Desde que las redes corporativas de hoy pueden contener miles de dispositivos, esto coloca una tensión sobre los recursos de la red y puede impactar en la performance. Finalmente, el formato propio de las direcciones de red restringe el máximo numero de host, por ejemplo una red clase C solo provee 254 direcciones de host únicas. Para resumir, las redes planas L2 simplemente no escalan lo suficiente en redes corporativas medianas y grandes.

- **Envío en L3: Enrutamiento**

La solución es implementar el envío "forwarding" en L3, también conocido como enrutamiento "routing".

Considerando que los dispositivos L2 envían "forward" dentro de una red dada (o en una VLAN) usando la dirección MAC destino, los routers envían

"forward" entre diferentes redes. Ellos hacen esto examinando el numero de red destino en la cabecera del paquete L3 y buscando el siguiente salto "hop" apropiado en una tabla con las redes conocidas. Los routers no necesitan conocer acerca de todos los host, sino las redes donde ellos residen (la dirección Mac del host es conocida solo por el ultimo router, para entregar el paquete a su tarjeta de red [NIC]). Este sistema de VLANs interconectadas es llamado una interred.

- **IP y otros protocolos L3**

Las Inter-redes usando IP son las predominantes en las redes corporativas de hoy. La Internet global sobre el cual el Worl Wide Web (WWW) es construida es simplemente un ejemplo grande de una interred.

Además de IP, hay un numero de otros protocolos L3 para la creación de Inter.-redes basadas en diferentes estandares.Algunos de estos son IPX de Novell Netware, ApleTalk, para el enrutamiento propietario de las computadoras Apple y DECNet de Digital Equipment Corporation. Aunque estos protocolos legados esta aun en uso, el despliegue extendido de IP ha hecho de este la selección preferida por la vasta mayoría de usuarios de hoy. Por consiguiente nos enfocaremos sobre IP en el resto de esta unidad.

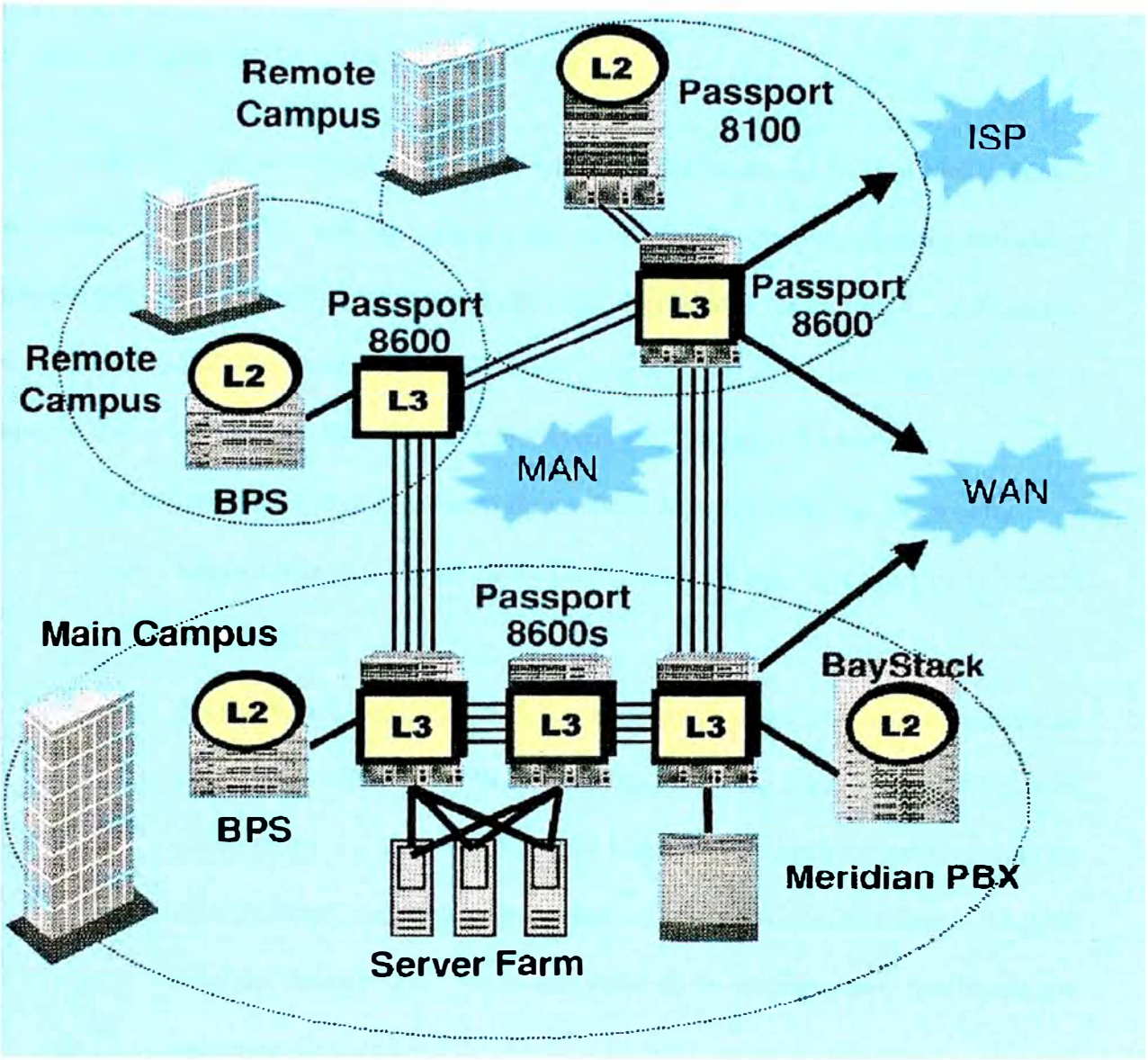


Figura 4.4.1 Redes capa 2 Vs Interredes capa 3

4.4.2 ¿PORQUE ENRUTAR EN VEZ DE BRIDGE?

- **ESCALABILIDAD Y FLEXIBILIDAD**

Las VLANs son construidas para limitar la extensión de los broadcast dentro de la red. Las VLANs son un método de construcción de dominios de broadcast customizado. Las VLANs funcionan en la capa de Enlaces de Datos, L2 del modelo de referencia OSI. Para conectar una VLAN con otra, un dispositivo de envío de la capa de red o L3 es requerido. Estos dispositivos son llamados routers.

El enrutamiento tiene un numero de ventajas sobre el bridging, tales como:

- **Limitación del Broadcast**- Los Broadcast son limitados en la VLAN originante.
- **Flexibilidad del Medio**- Los Routers pueden proveer conectividad entre host sobre diferentes tipos de redes de área local (LAN) tales como Ethernet, Token Ring, FDI y ATM. Los bridges transparente, de otra manera , requieren que todos los hosts residentes sobre la s LANs sean del mismo tipo, desde que ellos no re-encapsulan o modifican los paquetes de datos.
- **Escalabilidad**- Los routers necesitan solo conocer acerca de las direcciones de red y de los host que están directamente conectados a los segmentos o VLANs. Ellos no tienen que conocer acerca de todos los host en la corporación.

Sin embargo, hay también algunas desventajas:

- **Complejidad-** Los routers requieren protocolo de software para aprender direcciones de red desde otro router.
- **Costo-** Los Router y Switches capa 3 son tipicamente mas caro que sus colegas L2.
- **Planificación del diseño-** Los administradores de red deben asignar números de red y de subred en un modo lógico para asegurar la conectividad y performance optima.

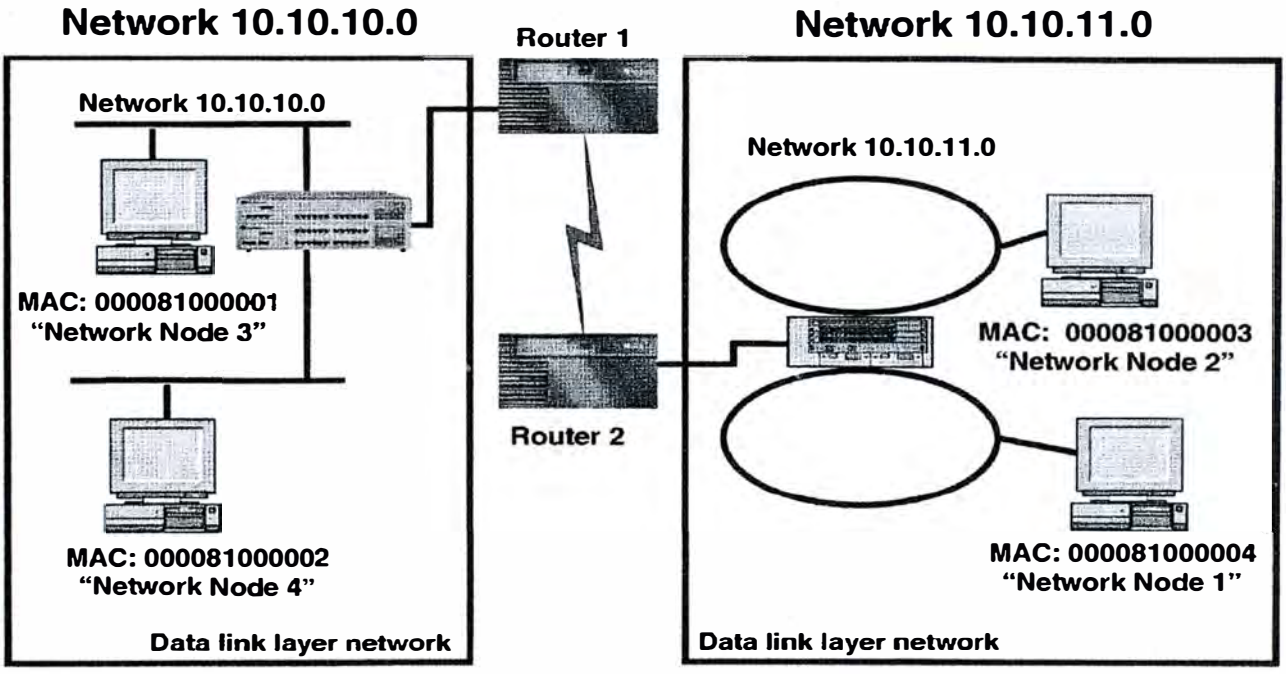


Figura 4.4.2 Conectando dominios de broadcast.

4.4.3 DIRECCIONAMIENTO EN LA INTERNETWORK

- **DIRECCIONES DE LA CAPA DE RED**

Una dirección de la capa de red identifica tanto la red donde el host reside y el host propiamente. En la mayoría de los casos este no es derivado de la dirección MAC de hardware en ningún modo. Los routers usan solo la dirección de red (hasta el ultimo salto "hop"), entonces ellos enmascaran fuera la porción de host, dejando solo el identificador de red.

Una vez que el paquete alcanza la red destino, algunas formas de resolución de direcciones son requeridas para derivar la dirección MAC del host para que el paquete pueda ser enviado a la NIC apropiada.

La primera parte de una dirección de red típica identifica la red en el cual el host reside. Esta parte es el numero de red. La segunda parte identifica al dispositivo o host. Esta parte es el numero de nodo. La Figura 4.4.3.1 ilustra el formato usado por IP.

Cada paquete contiene una dirección de la capa de red tanto de la fuente como el del destino. Los routers usan solo la dirección destino. El host destino usa la dirección de la fuente para enviar una respuesta y establecer una conexión o sesión entre las estaciones finales. Los routers no tienen un papel en la creación de la conexión; Ellos simplemente envían datagramas entre los hosts. Las conexiones, de otra manera, son creadas por los protocolos de la capa 4 (L4) corriendo dentro de los hosts.

Figura 4.4.3.1 Formato típico de la dirección de red

- **RESOLUCIÓN DE DIRECCIONES**

Recordando que L2 confía en la dirección MAC de hardware para entregar la data a una estación final. Cada tarjeta NIC esta programada para aceptar data enviada a su dirección, así como broadcast. Sin embargo , el router del ultimo salto no necesariamente conoce las direcciones MAC de los host directamente conectados. El solo conoce la dirección de la capa de red. Los protocolos ARP "Address Resolution Protocols" son necesarios para trasladar una dirección de la capa de red de un host a la correspondiente dirección MAC en el ultimo salto. Los mismos protocolos permiten que las estaciones en una red plana se comuniquen , aun si ellos inicialmente solo conocen la dirección de la capa de red de cada otra estación.

Por ejemplo en la figura 4.4.3.2, la estación 10.10.10.3 difunde "broadcast" una solicitud por la dirección MAC de la estación 10.10.10.4 el cual es una dirección de la capa de red destino de la estación final. Si el nodo destino usa el mismo protocolo de la capa de red y esta en el mismo dominio de broadcast, este monitoreará el broadcast, reconocerá su dirección de la capa de red en la solicitud, y responderá con su dirección MAC. El enviador puede ahora direccionar un frame

directamente a la tarjeta NIC destino. Generalmente, los enviadores mantienen una tabla de translación o cache de direcciones MAC resultas para evitar el envío repetido de la misma solicitud cada vez que este tenga otro paquete.

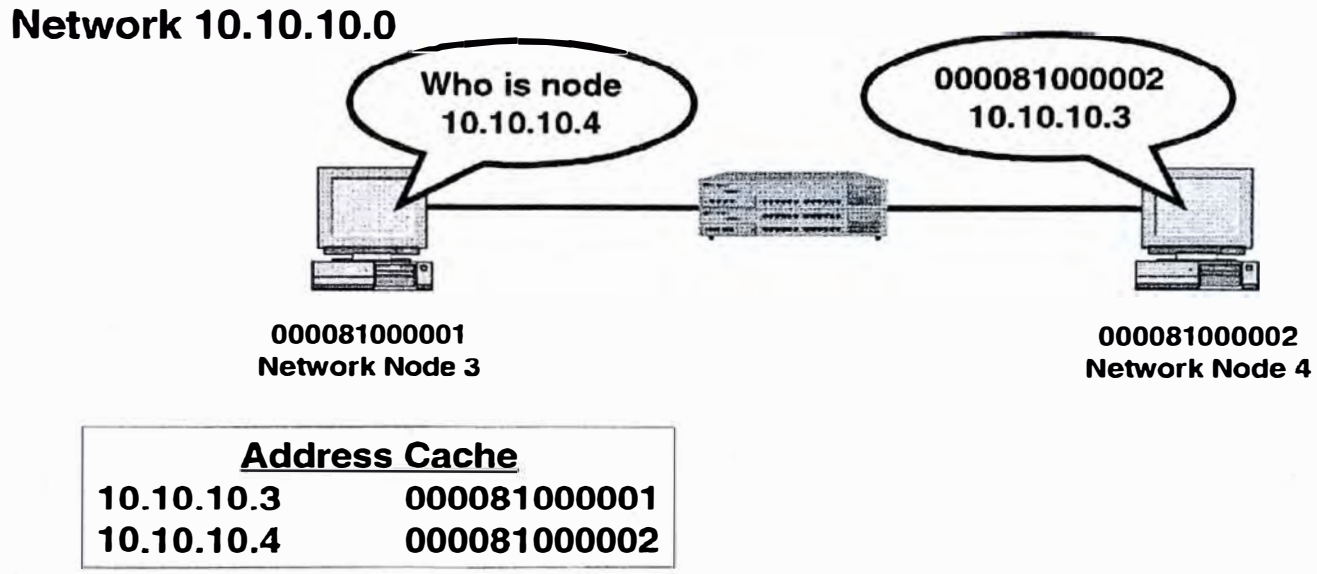


Figura 4.4.3.2 Resolución de direcciones -ARP

4.4.4 COMO TRABAJAN LOS ROUTERS

- **CREACION DE UNA TABLA DE ENRUTAMIENTO**

Como muestra la figura 4.4.4.1, un router conecta dos o más redes a través de sus puertos físicos. Cada uno de los puertos sobre el router tiene una dirección de red correspondiente a la red conectada a él. El router automáticamente aprende las direcciones de estas redes conectadas directamente y rutea los paquetes entre ellos. Para redes remotas (esas que no están directamente conectadas), el router debe

aprender los números de red tanto a través de una configuración estática o desde otro router vía un protocolo de ruteo dinámico tales como RIP o OSPF.

- **Decisiones de envío "Forwarding"**

Los routers basan sus decisiones de envío "forwarding" en la porción de red de una dirección destino de la capa de red del paquete. Ellos generalmente ignoran la porción de host hasta el ultimo salto, desde que todos los host en una red dada tiene usualmente la misma dirección de red relativa al router. Los routers solo mantienen las pistas de las redes en el internetwork, considerando que los bridges y los switches L2 mantienen la pista de los host dentro de una única red. Esto substancialmente reduce el tamaño de la tabla de ruteo.

- **Redes destino**

Una tabla de enrutamiento generalmente provee alguna información acerca de cada red destino, Tal como cual puerto del router es más conveniente para enviar paquetes a esa red, o el numero de saltos de router requerido para alcanzarlo. Esto permite que los routers seleccionen la mejor ruta para una red particular., basados en varios criterios tales como la cuenta de salto, el costo configurado o el ancho de banda. Si una ruta se pone no disponible por alguna razón, un router dirigirá el trafico por la ruta más eficiente que permanezca disponible.

Si un puerto provee una conexión directamente a la red destino, el paquete es enviado al host destino y el enrutamiento es completado. De otra manera , este es enviado a otro router, el cual hace su propia búsqueda y repite el proceso de enrutamiento. Cada router trasmite el paquete hacia su destino por la ruta más eficiente que este conoce. El paquete sigue, salto por salto, hasta que alcanza su red destino.

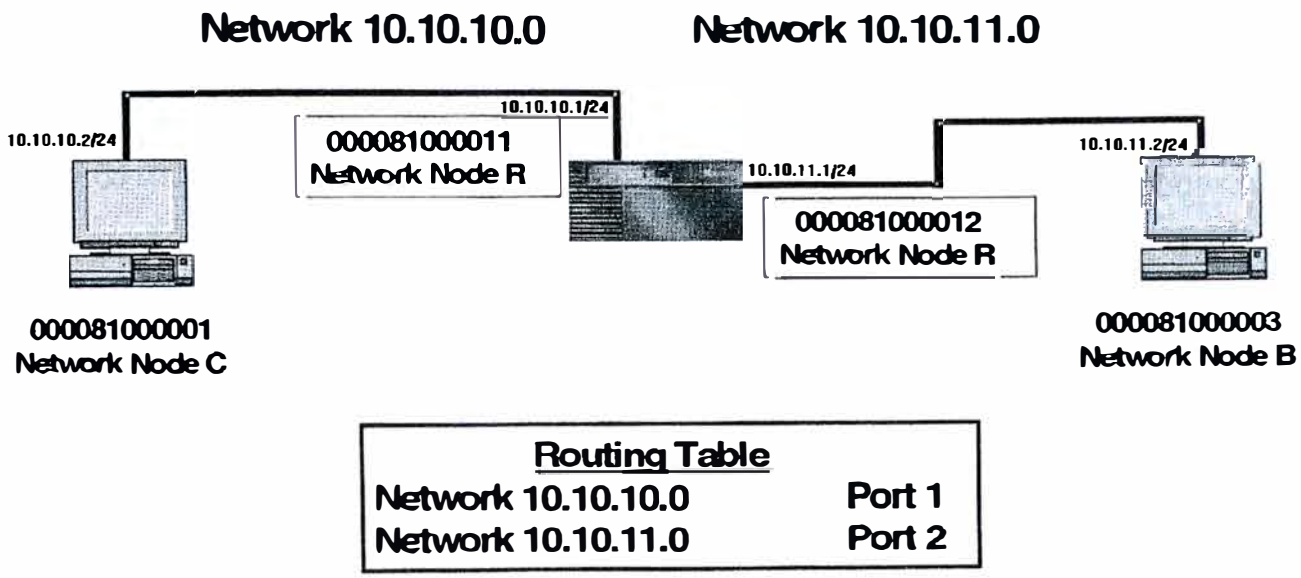


figura 4.4.4.1 Creación de una tabla de ruteo.

- **Contador de saltos "Hop Counter"**

Cada vez que un router envía un paquete, este incrementa el contador de salto en la cabecera de la capa de red. Muchos routers (tales como routers IP) descantar un paquete cuando la cuenta de saltos alcanza su máximo valor. Esto previene que los paquetes estén eternamente circulando a través del internetwork.

Los Routers no escuchan por cada paquete en la red; solo los paquetes explícitamente direccionado al router en la capa de enlace de datos serán monitoreados. Por esta razón, las estaciones finales deben estar conscientes del router. Los host están usualmente configurados con un gateway por default identificando la dirección del puerto del router sobre su red local. Cuando un host quiere enviar un paquete a una red remota, este sabe como enviarlo a su gateway por default en lugar de intentar alcanzar un host remoto por sí mismo.

4.4.5 DIRECCIONAMIENTO IP

- **FORMATO DE LA DIRECCIÓN IP**

Las direcciones IP versión 4 consiste de 32 bits, generalmente escrita como un grupo de 4 octetos separados por punto, en un formato llamado notación punto-decimal (x.x.x.x). El máximo valor de cualquier octeto es 255 (todos los bits colocado en 1) , y ciertos valores (tales como 255) son reservados. Para asignar direcciones IP es frecuentemente necesario entender el valor binario de cada octeto. Esto puede ser hecho convirtiendo el valor de cada octeto en su equivalente binario, como se muestra a continuación:

187.124.255.188 = 10111011. 01111100.11100001.10111100

- **USANDO UNA MÁSCARA DE RED**

Hemos visto que la dirección IP consiste de una porción de red y una porción de host, y que los routers usan la porción de red para realizar decisiones de envío. IP tiene diferentes "clases" de direcciones de red, con variación del número de bits usado para la porción de red y host respectivamente. Esto presenta un problema: ¿ Cómo el router, o el host para este asunto, interpreta una dirección dada? ¿Cuales son los bits de red y cuales son los bits de host?

La solución es una máscara de red, también conocida como una máscara subred "subnet mask". Semejante a la dirección IP , la máscara subred es un número de 32 bits. El número es dividido en cuatro octetos y representado en notación punto-decimal. Las reglas para aplicar una máscara subred son como sigue:

- Si el valor del bit es 1, esa posición del bit es parte de la dirección de red.

- Si el valor del bit es 0, esa posición del bit es parte de la dirección de host.

Por ejemplo, la máscara subred 11111111 11111111 00000000 00000000 reserva los primeros 16 bits para un numero de red (los 1s) y los restantes 16 bits para direcciones de host. La notación punto-decimal para esta máscara subred es 255.255.0.0.

Si extendemos la porción de red en un bit, podemos efectivamente doblar el número de posibles direcciones de red y cortar en la mitad el numero de IDs únicos de host. Cada dispositivo IP debe ser configurado con la máscara que ha sido escogido para su red. Las variadas implementaciones de TCP/IP aceptarán la máscara subred en diferentes modos. Las más comunes son:

- 192.168.10.24/255.255.255.0 o
- 192.168.10.24/24

Ambas direcciones IP representan a un host con una dirección IP de 192.168.10.24 y una máscara de 24 bits de 255.255.0.0.

❑ CLASES DE DIRECCIONES IP

El estándar IP define varias clases de direcciones IP con diferentes valores de máscara por default. Las organizaciones que desean conectarse a la Internet global, solicitan una o más direcciones de red para su compañía. Estas direcciones son administradas por una autoridad central para evitar duplicación:

Las más comunes clases de direcciones IP son:

- **Clase A** – Usadas para grandes redes.

  - Máscara por default de 8 bits

  - Rango de direcciones de red desde 1.0.0.0/8 hasta 126.0.0.0/8

  -2^{24} - 2 Hosts (16,777,214)

  - El bit más significativo (MSB) es colocado en cero.

- **Clase B** – Usadas para medianas y grandes redes.

  - Máscara por default de 16 bits

  - Rango de direcciones de red desde 129.0.0.0/16 hasta 191.255.0.0/16

  -2^{16} - 2 Hosts (65,534)

  - Los primeros dos bits más significativo (MSB) son iguales a 10.

- **Clase C** – Usadas para redes pequeñas.

  - Máscara por default de 24 bits

  - Rango de direcciones de red desde 192.0.0.0/24 hasta 223.255.255.0/24

  -2^{8} - 2 Hosts (254)

  - Los primeros tres bits más significativo (MSB) son iguales a 110.

- **Clase D** – Es reservada para direccionamiento multicast. Rango de direcciones de red desde 224.0.0.0 hasta 239.0.0.0

La tabla 4.4.5.1 lista las clases de direcciones IP con su respectivo rango de direcciones y mascara y la Figura 4.4.5.1 muestra las fronteras entre las porciones de red y host en las clases de direcciones IP.

Clase de dirección IP	Clase A	Clase B	Clase C
Longitud de la Máscara	8 bits (255.0.0.0)	16 bits (255.255.0.0)	24 bits (255.255.255.0)
Numero de redes	126	16,384	2,097,150
Rango de redes	1.0.0.0 / 8 – 126.0.0.0 /8	128.0.0.0 / 16 – 191.255.0.0 /16	192.0.0.0 / 24 – 223.255.255.0 /24
Numero de Host	16,777,214	65,534	254

Tabla 4.4.5.1 : Clases de direcciones IP

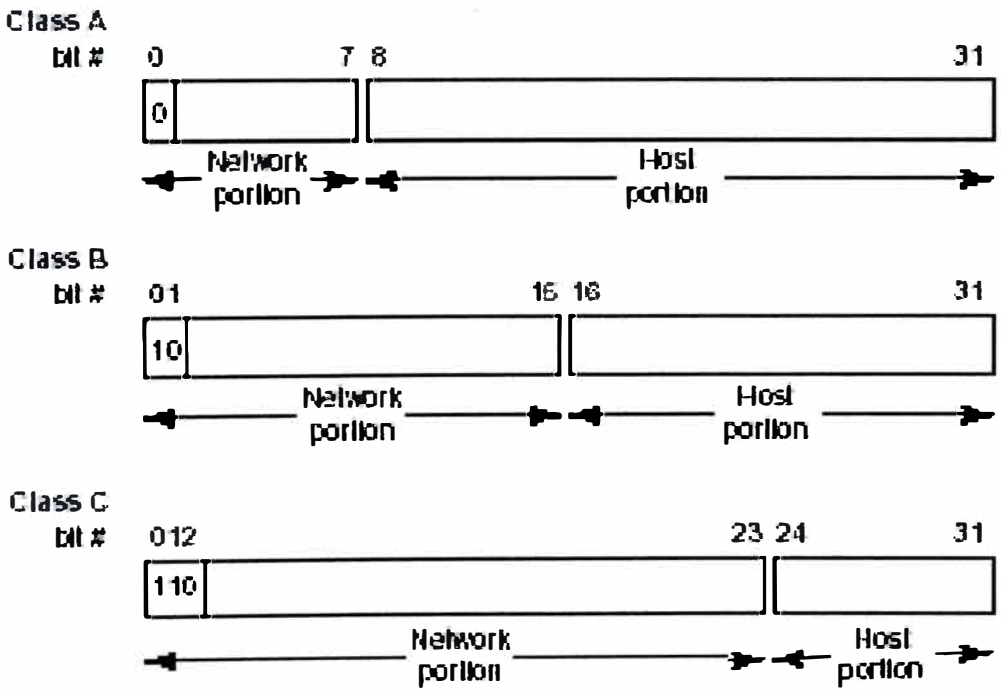


Figura 4.4.5.1 Fronteras entre las porciones de red y host en las clases de direcciones IP.

❑ DIRECCIONAMIENTO SUBRED "SUBNET"

El concepto de subredes "subnetworks" (o subnets) extiende el esquema de direccionamiento IP permitiendo que una organización use un rango de direcciones IP para múltiples redes.

Las subredes son dos o más redes físicas que comparten un campo de identificación de red común (la porción de red de la dirección IP de 32 bits).

Podemos crear una dirección subnet incrementando la porción de red para incluir una dirección subnet, así decrementamos la porción de host de la dirección IP. Por ejemplo, en la dirección 128.32.10.0 la porción de red es 128.32, mientras la subnet es encontrada en el primer octeto de la porción de host (10). Una máscara subnet es aplicada a la dirección IP e identifica las porciones de red y de host de la dirección.

La Tabla 4.4.5.2 ilustra como las máscaras subnets usadas con direcciones clase B y clase C pueden crear diferentes números de subnets y hosts. Este ejemplo incluye la subnet cero , el cual es permitido en los módulos del switch Passport 8600.

Máscaras de subred de longitud variable (VLSM) "Variable-length subnet masking" es la habilidad de dividir su Intranet en piezas que concuerden con sus requerimientos. El enrutamiento será basado en la máscara subnet / red más grande que concuerde. RIPv2 y OSPF son protocolos de enrutamiento que soportan VLSM.

Número de bits	Máscara Subnet	Número de subnets (recomendados)	Número de host por subnet
Clase B			
1	255.255.128.0	1	32,766
2	255.255.192.0	2	16,382
3	255.255.224.0	6+2	8,190
4	255.255.240.0	14+2	4,094
5	255.255.248.0	30+2	2,046
6	255.255.252.0	62+2	1,022
7	255.255.254.0	126+2	510
8	255.255.255.0	254+2	254
9	255.255.255.128	510+2	126
10	255.255.255.192	1,022+2	62
11	255.255.255.224	2,046+2	30
12	255.255.255.240	4,094+2	14
13	255.255.255.248	8,190+2	6
14	255.255.255.252	16,382+2	2
Clase C			
1	255.255.255.128	0+2	126
2	255.255.255.192	2+2	62
3	255.255.255.224	6+2	30
4	255.255.255.240	14+2	14
5	255.255.255.248	30+2	6
6	255.255.255.252	62+2	2

Tabla 4.4.5.2 : Máscara Subnet para direcciones IP clase B y Clase C

- **DIRECCIONAMIENTO SUPERNET Y CIDR (ENRUTAMIENTO INTERDOMINIOS SIN CLASES "CLASSLESS INTER-DOMAIN ROUTING")**

Una supernet es un grupo de redes identificadas por direcciones de redes contiguas. Los proveedores de servicio IP pueden asignar bloques de clientes con direcciones contiguas para definir supernets cuando sea necesario. El supernetting

nos permite direccionar todo un bloque de direcciones clase C y evitar usar tablas de enrutamiento grandes para seguir a las direcciones.

Cada supernet tiene una única dirección supernet que consiste de los bit superiores compartidos por todas las direcciones en el bloque contiguo. Por ejemplo, considerar las direcciones clase C mostrada en la Figura 4.4.5.2. Adicionando la máscara 255.255.128.0 a la dirección IP 192.32.128.0, podemos agregar las direcciones desde 192.32.128.0 hasta 192.32.255.255 y 128 direcciones clase C usan un único aviso de enrutamiento. En la mitad inferior de la figura 4.4.5.2, usamos 192.32.0.0/17 para agregar las 128 direcciones (desde 192.32.0.0/24 hasta 192.32.127.0/24).

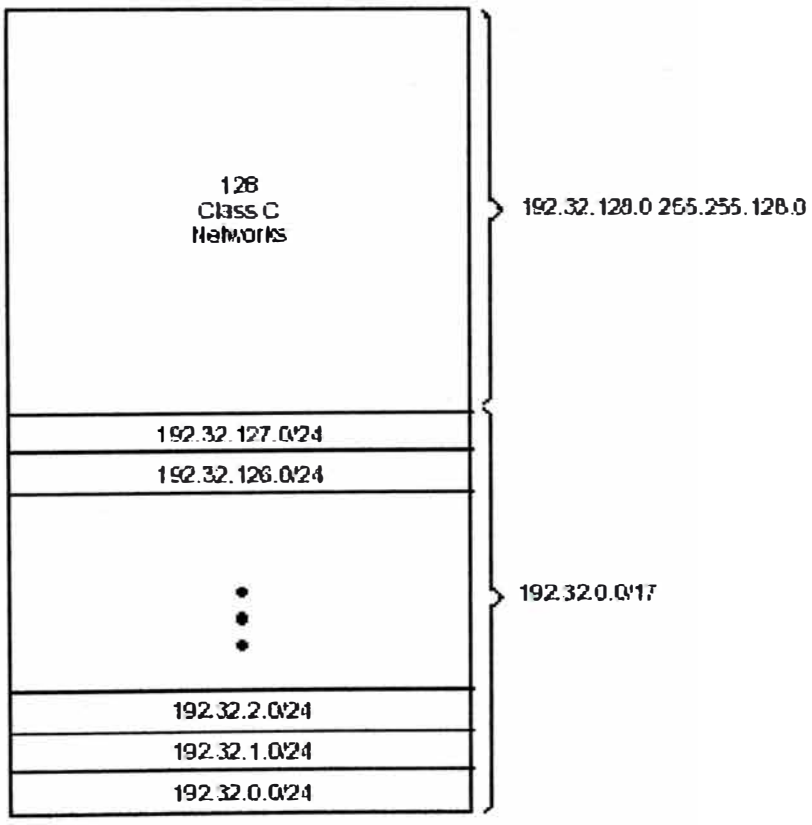


Figura 4.4.5.2 Dirección Supernet Clase C

Otro ejemplo es el bloque de direcciones 192.32.0.0 al 192.32.7.0. La dirección supernet para este bloque es 11000000 00100000 00000, con los 21 bits superiores compartidos por las direcciones de 32 bits.

Una dirección supernet completa consiste del par dirección/máscara :

- La *dirección* es la primera dirección IP de 32 bits en el bloque contiguo. En este ejemplo , la dirección es 11000000 00100000 00000000 00000000 (192.32.0.0 en notación punto-decimal).
- La *máscara* es una cadena de 32 bits conteniendo un bit en set por cada posición de bit en la parte de supernet de la dirección. La máscara para dirección supernet en este ejemplo es 11111111 11111111 11111000 00000000 (255.255.248.0 en notación punto-decimal).

La dirección supernet completa en este ejemplo es 192.32.0.0/21.

La dirección supernet es también referida como la dirección CIDR (enrutamiento interdominio sin clases "Classless interdomain routing") . Si embargo "classful" prohíbe usar máscara direccionada con la dirección IP, CIDR nos permite crear redes de varios tamaños usando la máscara direccionada. Sin embargo VLSM (máscaras de subred de longitud variable "Variable Length Subred Masking") también nos permite dividir el espacio de direcciones, pero la división no es vista exterior a nuestra red. Con CIDR, nuestras direcciones son usadas por routers externo a nuestra red.

❑ EL PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES (ARP "ADDRESS RESOLUTION PROTOCOL")

Para que los hosts IP dentro de la misma red se comuniquen , ellos deben conocer cada dirección MAC de los otros hosts para direccionar correctamente los paquetes hacia la NIC apropiada. La dirección MAC destino es usada por la NIC para determinar si el paquete actual es destinado para ese host.

La resolución de dirección es el proceso de mapear una dirección de la capa de red hacia una dirección de la capa de enlace, tal como una dirección MAC. Las direcciones IP son asignadas a los hosts y son lógicamente independientes de sus direcciones físicas. El software de la capa superior debe depender de la capa de enlace para entregar la data a un host sobre la misma LAN o VLAN. Por consiguiente, la dirección IP debe ser mapeada a la dirección física del host.

El protocolo de resolución de direcciones (ARP) es el protocolo usado para asociar una dirección Internet a una dirección de hardware físico o MAC.

Un nodo hace ARPs a otro nodo cuando este determina que la dirección destino esta en la misma red del enviador. Este realiza esto comparando la porción de red de su propia dirección con la dirección destino. Si ellos concuerdan , el host puede hacer ARP con cada otro host y comunicarse directamente. Si ellos son diferentes, los paquetes deben irse a través de un router. En este caso, el host hace ARP con su gateway por default y envía los paquetes allí para el enrutamiento. Recordar que los puertos del router también tienen direcciones MAC.

En otras palabras una estación de red puede usar ARP solamente a través de una única red, y el hardware de la red debe soportar broadcast físicos. Si una estación

quiere enviar un paquete a un host pero conoce solamente la dirección IP del host, la estación de red usa ARP para determinar la dirección física del host como sigue:

1. La estación de red difunde "broadcasts" un paquete especial , llamado una solicitud ARP, que pide al host con la dirección IP especificada que responda con su dirección física.
2. Todos los host en la red reciben la solicitud broadcast.
3. Solo el host especificado responde con su dirección de hardware.
4. La estación de red entonces mapea la dirección IP del host a su dirección física y graba el resultado en un cache de resolución de direcciones para uso futuro.
5. La tabla ARP de la estación de red displaya las asociaciones de las direcciones MAC conocidas a direcciones IP.

Entradas ARP estática pueden ser creadas, y entradas ARP individuales pueden ser borradas.

La Figura 4.4.5.3 ilustra este proceso. Cuando el Host B ,140.250.200.2/24, desea comunicarse con el Host D, 140.250.200.4/24, este debe primero determinar la dirección MAC del Host D. Para hacer esto, el Host B publica un ARP. El paquete ARP es un broadcast a nivel de MAC. Todas las estaciones en la red local mirarán en el paquete para ver si su información es requerida por esa estación.

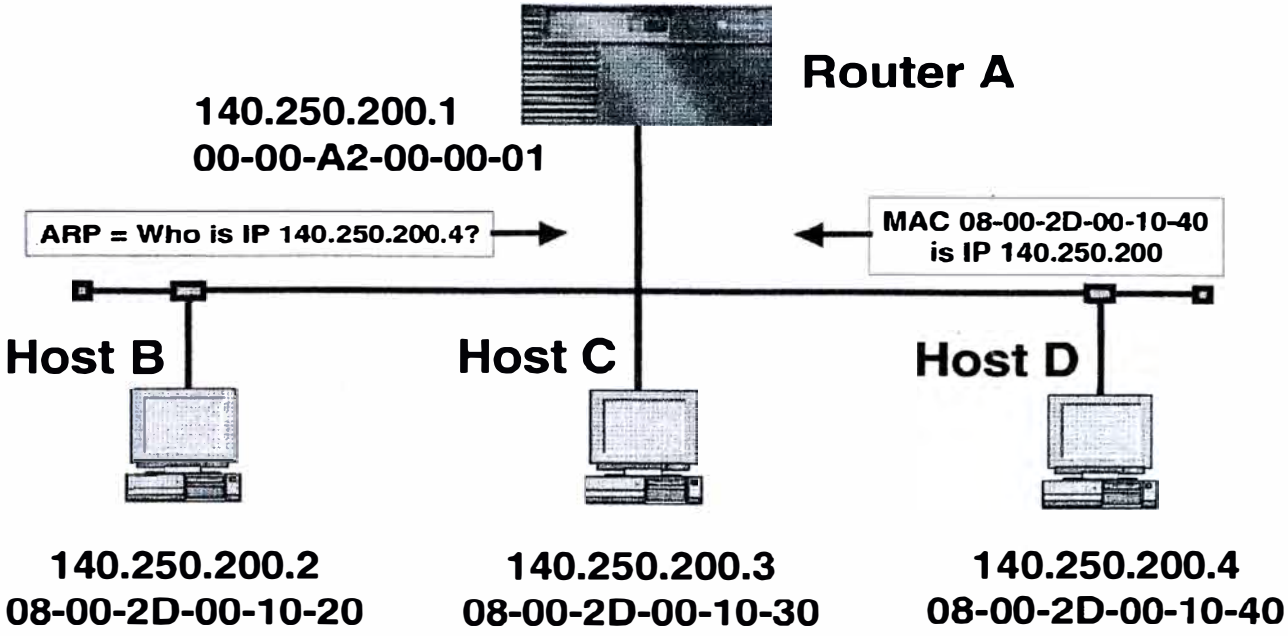


Figura 4.4.5.3 ARP

- **LA COMUNICACIÓN ENTRE SUBREDES**

Si las subredes fuente y destino son diferentes, la estación fuente debe enviar el paquete a su destino vía un router IP. La estación fuente creará una cabecera L2 con su dirección MAC como la MAC fuente y la MAC del router IP como la MAC destino. La cabecera IP contendrá las direcciones IP fuente y destino.

El router IP removerá la cabecera MAC y el CRC "Cyclic Redundancy Checking", examina la cabecera IP por la dirección destino y compara esta dirección en la tabla de enrutamiento del router IP. Si la red destino es localizada o una ruta

por default es descubierta, el router IP enviará el paquete fuera de la interfase hacia el destino IP final. El router colocará una nueva cabecera MAC cuyo MAC destino puede ser tanto el siguiente router bajo la línea o el MAC del destino final.

La Figura 4.4.5.4 ilustra este proceso.

1. La capa IP del host A acepta un paquete UDP destinado para el host B y encapsula el paquete en un datagrama IP que incluye una dirección fuente de 192.30.10.20 y una dirección destino de 192.40.10.20.
2. La capa de enlace de datos en el host A encapsula el datagrama IP en un frame token ring y trasmite el frame al router A.
3. Al recibir el frame token ring, el router A remueve el datagrama IP desde el frame token ring, lo encapsula en un frame ethernet y trasmite el frame al router B.
4. Al recibir el frame ethernet, el router B trasmite el datagrama IP en un frame Ethernet al host B.

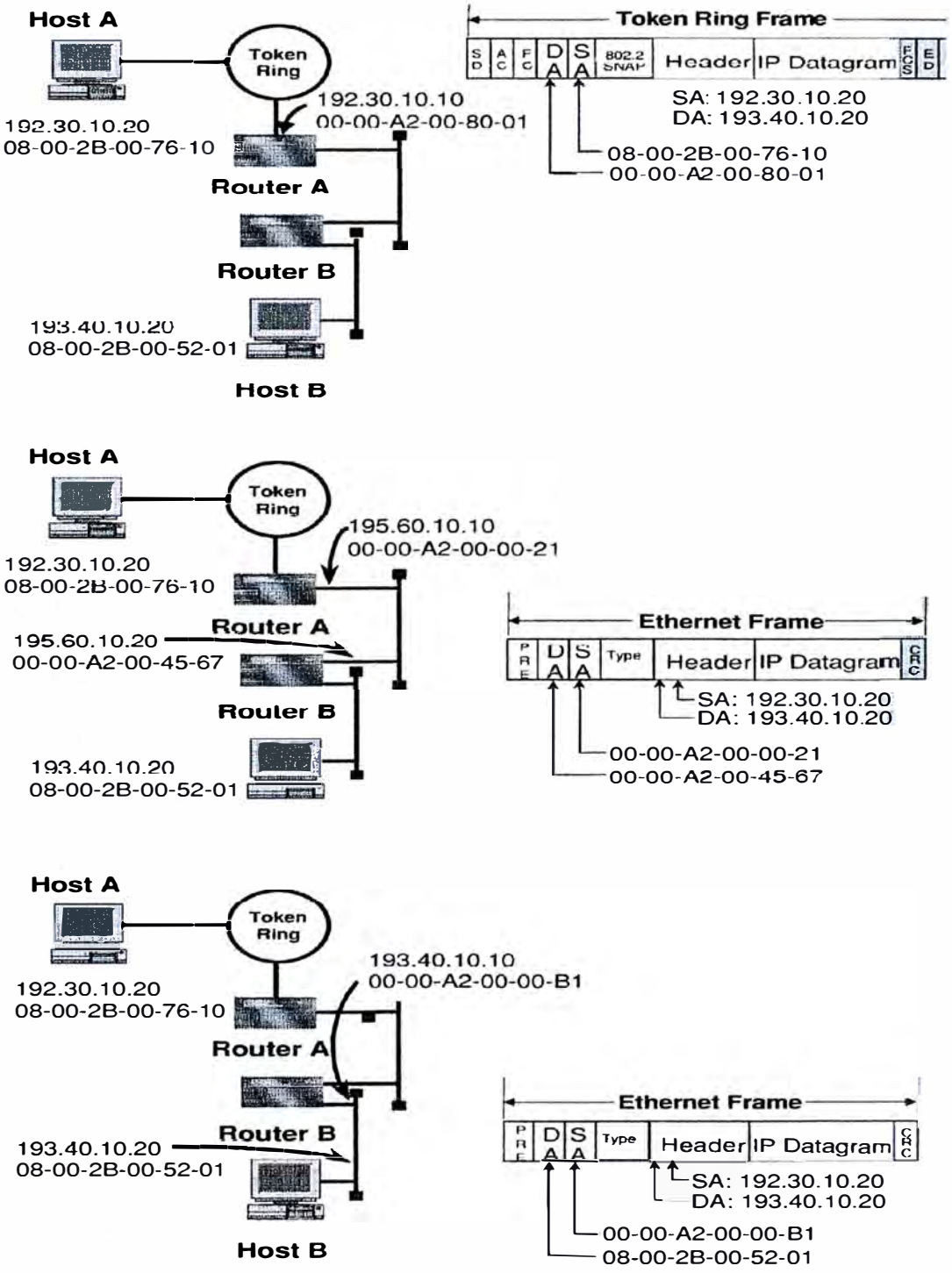


Figura 4.4.5.4 Enrutamiento IP

4.4.6 TIPOS DE ENRUTAMIENTOS IP

Hay dos tipos de interfases de router: Interfases virtuales del router (enrutamiento entre VLANs) y puertos brouters (enrutamiento y conmutación "bridging" sobre el mismo puerto). Cuando ruteamos sobre una VLAN, una dirección IP es asignada a la VLAN y esta dirección IP no es asociada con ningún puerto fisico particular. Los puertos Brouters son VLANs que rutean paquetes IP y conmutan "bridge" tráfico no ruteable en una VLAN de un único puerto.

- **ENRUTAMIENTO VIRTUAL ENTRE VLANS**

Los switches Passport 8600 capa 3 soportan enrutamiento IP a la velocidad del cableado entre VLANs como se muestra en la Figura 4.4.6.1. En esta figura , si bien la VLAN 1 (V1) y la VLAN 2 (V2) están sobre el mismo switch , para que el tráfico fluya desde la V1 a la V2, este debe ser ruteado. Cuando el enrutamiento es configurado sobre una VLAN, una dirección IP es asignada a la VLAN que actúa semejante a una dirección para la VLAN "interfase virtual del router".

Esta es una interfase virtual del router que no tiene ninguna asociación con ningún puerto particular. La dirección IP puede ser alcanzada a través de cualquiera de los puertos en la VLAN y es la dirección IP que sirve como gateway a través del cual un frame es ruteado fuera de la VLAN. El tráfico ruteado puede ser enviado a otra VLAN dentro del switch.

Cuando el protocolo Spanning Tree es habilitado en una VLAN, la convergencia del Spanning Tree debe estar estabilizado antes que el protocolo del router pueda empezar. Este requerimiento puede conducir a un retardo adicional en el envío "forwarding" del tráfico IP.

Debido a que un puerto dado puede pertenecer a múltiples VLANs (algunos de los cuales son configurados para ruteo sobre el switch y otros no), no hay una gran correspondencia de uno a uno entre el puerto físico y la interfase del router.

Como con cualquier dirección IP, las direcciones de las interfaces virtuales del router son también usadas para administración de dispositivos. Para administración SNMP o Telnet, podemos usar cualquier dirección de las interfases virtuales del router para acceder al switch todo el tiempo que el ruteo este habilitado sobre la VLAN.

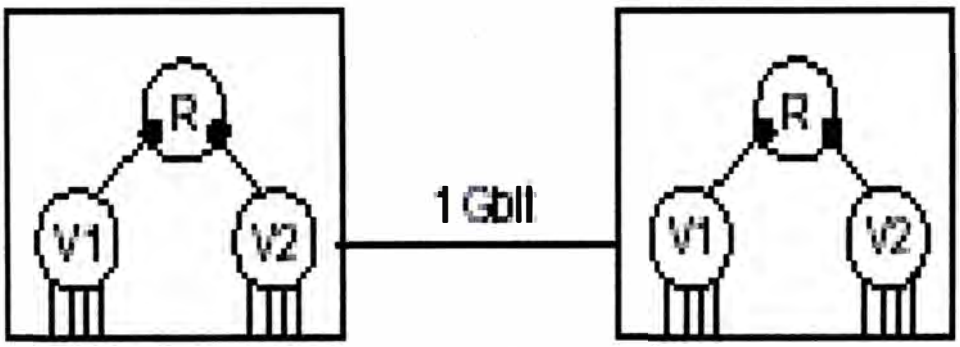


Figura 4.4.6.1 Enrutamiento IP entre VLANs

- **PUERTOS BROUTER**

El switch Passport también soporta el concepto de puertos brouter. Un puerto brouter es una VLAN con un único puerto que puede rutear paquetes IP así como también conmutar "bridge" todo el tráfico no ruteable.

La diferencia entre un puerto brouter y una VLAN estándar basada en el protocolo IP configurada para realizar enrutamiento es que la interfase de enrutamiento del puerto brouter no esta sujeto al estado de Spanning Tree del puerto. Un puerto brouter puede estar en el estado de bloqueo para tráfico no ruteable y aún ser habil de rutear tráfico IP. Esta característica remueve cualquier interrupción causada por la recalculación del protocolo Spanning Tree en el tráfico ruteado.

Un puerto brouter es realmente una VLAN de un puerto; Por consiguiente, cada puerto brouter decrementa el numero de VLANs disponibles en uno y usa una VLAN ID.

4.4.7 RUTAS ESTATICAS Y POR DEFAULT

- **CONFIGURACIÓN MANUAL DE RUTAS**

Las rutas estáticas nos permite crear rutas manualmente hacia una dirección IP destino.

Ocasionalmente podemos crear una ruta manualmente vía configuración estática preferentemente en lugar de depender de un protocolo de enrutamiento semejante al RIP. Algunas razones para usar rutas estáticas son:

- **Enlaces o routers lentos** – RIP anuncia toda la tabla de ruteo cada 30 segundos por default. En una red grande esto podría causar que los enlaces lentos o los routers lentos usen todos sus recursos sirviendo a las actualizaciones de RIP.
- **Sumarización de redes IP** – Si la red esta bien construida, un rango de direcciones de red podría ser alcanzada usando un pequeño conjunto de enlaces. Esto podría tener poco sentido, para anunciar números grandes de redes remotas que fueron todas alcanzable por solo unos cuantos enlaces.
- **Acceso a Internet** – La internet consiste de cientos de miles de redes. Para las mayorías redes corporativas, no hay necesidad de importar todas estas redes dentro de la red. En vez de eso, una única ruta por default es usada por cualquier paquete cuya red destino es desconocida para el router

En cada uno de estos casos, el uso de rutas estáticas y/o rutas por default pueden mejorar la performance de la red.

Las rutas estáticas pueden ser usadas para anunciar rangos de redes alcanzables en enlaces WAN. En este caso las rutas representadas por la ruta estática podrían ser un resumen de las redes alcanzables por el enlace WAN. Esto podría tener el beneficio de reducir el tamaño de la tabla de ruteo local, reduciendo el tamaño de los anuncios RIP locales, así como también removiendo la necesidad de correr RIP sobre una interfase WAN lenta.

Podemos usar una ruta estática por default para especificar una ruta a todas las redes para el cual no hay ninguna ruta explicita en la tabla de enrutamiento. Esta ruta es por definición una ruta con la longitud de prefijo de cero (RFC 1812). El switch Passport 8600 puede ser configurado con cualquier ruta vía la tabla de enrutamiento estático IP.

Las rutas por default pueden ser usadas para soportar acceso a Internet desde dentro de la red corporativa. La ruta por default en efecto dice, "Si este no esta dentro de esta red corporativa, debe estar en algún lugar de Internet". Por consiguiente, el siguiente salto de la ruta por default podría apuntar al router de la compañía proveedora de servicios de Internet (ISP).

Para crear una ruta estática por default, la dirección destino y la máscara subnet deben estar colocado en 0.0.0.0.

Las rutas estáticas pueden también ser configuradas con un siguiente salto que no este directamente conectado, pero que el salto pueda ser alcanzable. De otra manera, la ruta estatica no podria ser habilitada.

Después que una ruta estática o por default es configurada en un router, este podría ser anunciada al resto de la red usando RIP, semejante a cualquier otra ruta.

4.4.8 PROTOCOLOS DE ENRUTAMIENTO IP DINAMICOS

- **COMO LOS ROUTERS APRENDEN REDES REMOTAS**

A diferencia del enrutamiento IP estático, donde una entrada manual debe ser hecha en la tabla de enrutamiento para especificar una ruta, el enrutamiento IP dinámico usa un enfoque de "aprendizaje" para determinar las rutas hacia otros routers.

La mayoría de internetworks consisten de múltiples routers, frecuentemente conectados a una gran distancia usando redes de área amplia o WANs. Los routers pueden solo enviar "forward" hacia las redes que ellos conocen, así un método es necesario para los routers para que aprendan acerca de otras redes. Este intercambio de información de redes destino es realizado por los protocolos de enrutamiento.

- **TIPOS DE PROTOCOLOS DE ENRUTAMIENTO**

Los protocolos de enrutamiento intercambian dinámicamente información acerca de las internetworks. Cuando una nueva red es conectada, el protocolo anuncia su existencia y localización a los routers adyacentes, los cuales re-anuncian acerca de esta red a sus vecinos, hasta que cada router tenga una correspondiente entrada en la tabla de enrutamiento para el nuevo destino. En redes complejas, habría muchas diferentes rutas hacia una red dada. El protocolo es responsable de escoger la ruta optima para cada destino (generalmente la más corta).

Hay dos tipos básicos de protocolos de enrutamiento comunes usados hoy dentro de un AS:

- Protocolo de vectores de distancia "Distance vector protocols"

  - Para IP – RIP

  - Para IPX – RIP

  - Para AppleTalk – RTMP " Routing Table Maintenance Protocol"

- Protocolo de estado del enlace "Link state protocols"

  - Para OSI – IS-IS "Intermediate System-Intermediate System"

  -Para IP – OSPF

  -Para IPX – NLSP "Netware Link State Protocol"

Los protocolos de enrutamiento vectores de distancia cuentan la distancia, normalmente en saltos, para llegar a redes remotas. Esta clase de protocolo no distinguen usualmente entre las conexiones de red de alta velocidad y de baja velocidad. Un protocolo de vector de distancia usualmente requiere que los routers vecinos intercambien la mayoría o todas sus tablas de enrutamiento en intervalos regulares. Cuando aprende, el router simplemente incrementa cada costo de la ruta y lo almacena. En contraste, los protocolos de estado del enlace intercambian información acerca de la topología de la red y cada router luego calcula las rutas optimas. Cada protocolo consume menos ancho de banda debido a que ellos solo re-anuncian cuando las condiciones de red cambian.

- **SOPORTE DE LOS PROTOCOLOS DE ENRUTAMIENTO EN LOS SWITCHES PASSPORT 8600**

Los switches Passport 8600 empleados para la implementación de este proyecto soportan los siguientes protocolos de enrutamiento:

- **RIP (RIP1 RFC1058, RIP2 RFC1723)**

  El Protocolo de enrutamiento de información (RIP, Routing Information Protocol) es conocido como un protocolo vector de distancia. El vector es el numero de red y el siguiente salto, y la distancia es el costo asociado con el numero de red. RIP identifica la alcanzabilidad de la red basada en el costo, y el costo es definido como cuentas de saltos. Un salto es considerado como la distancia desde un router al siguiente. Este costo o salto es conocido como la *métrica.*

- **OSPF (RFC2178)**

  El protocolo llamado Abrir primero el camino más corto (OSPF Open Shortest Path First) es un protocolo IGP "Interior Gateway Protocol" que distribuye información de enrutamiento entre routers perteneciente a un único sistema autónomo (AS). Pensado para usarlo en grandes redes, OSPF es un protocolo de estado del enlace el cual soporta subnetting de IP, enrutamiento basado en TOS y el etiquetado "tagging" de información de enrutamiento derivada externamente.

- **BGP**

  El protocolo BGP (Border Gateway Protocol) es un protocolo de enrutamiento inter-dominio que provee enrutamiento inter-dominio libre de lazos entre sistemas autónomos ASs o dentro de un AS.

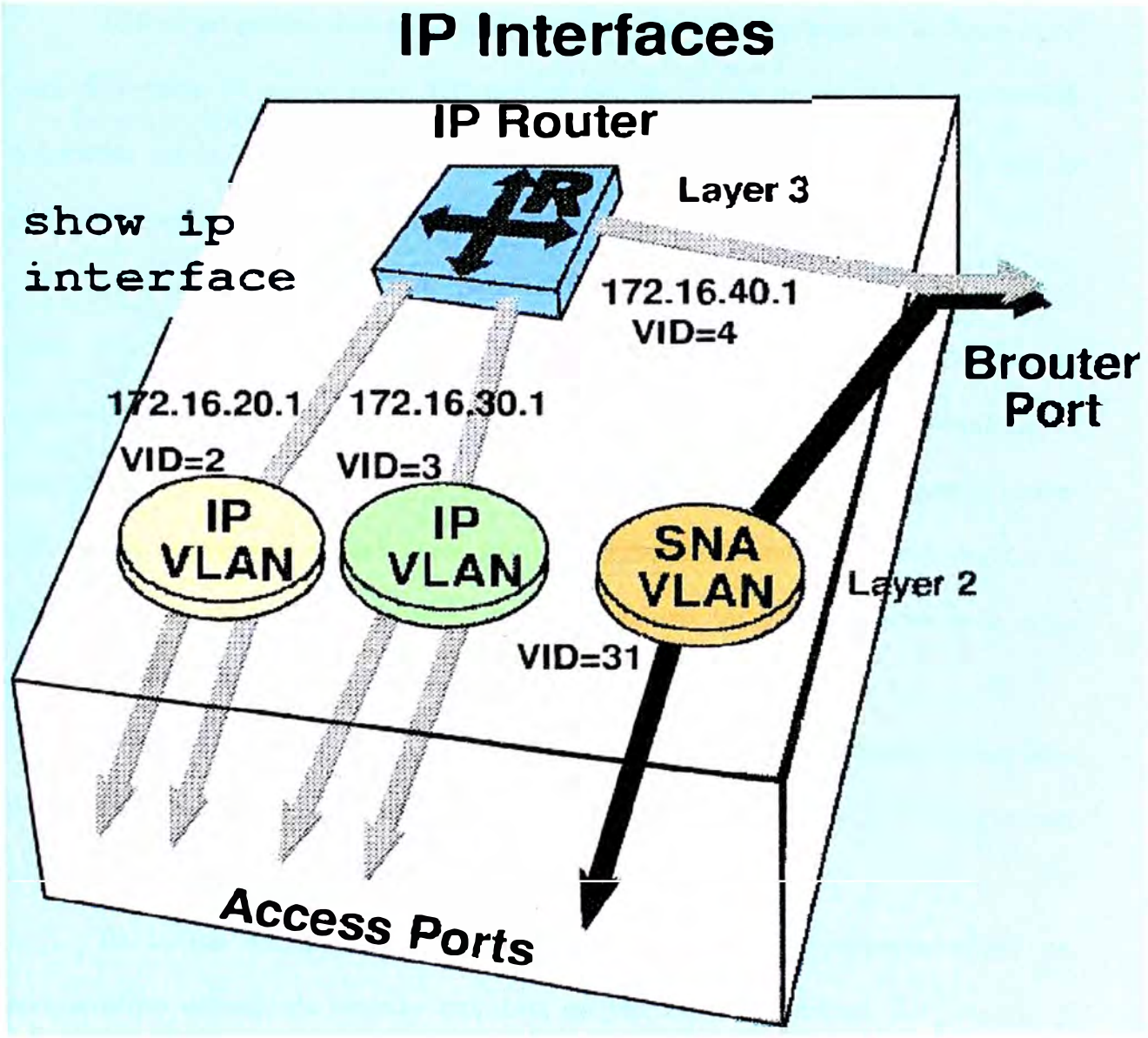


Figura 4.4.8.1 Soporte de enrutamiento en los Switches Passport 8600

4.4.9 CARACTERÍSTICAS DE LOS PROTOCOLOS DE ENRUTAMIENTO

- **CARACTERÍSTICAS DE RIP**

RIP es un protocolo vector de distancia que usa el algoritmo de Bellman-Ford para determinar la mejor ruta. RIP realiza sus decisiones de enrutamiento basado solamente en la distancia (saltos).RIP no toma en consideración cosas como la congestión, velocidad de línea y costo. Ver la Figura 4.4.9.1.

RIP usa broadcasts UDP para intercambiar información de enrutamiento. Cada router anuncia información de enrutamiento enviando información de enrutamiento actualizada cada 30 segundos. Si un router no recibe una actualización desde otro router dentro de los 90 segundos, este marca la ruta servida por el router que no ha enviado su actualización como inutilizable. Si ninguna actualización es recibida dentro de los 240 segundos, el router remueve todas las entradas de la tabla de enrutamiento del router no actualizable.

RIP versión 1 fue distribuido en los años de inicio de Internet y anunciaba direcciones con clase por default sin máscara de subred. RIP versión 2 anuncia más explícitamente, basada en la máscara subred.

El switch Passport soporta RIP versión 2, el cual anuncia tablas de enrutamiento actualizada usando multicast en vez de broadcasting. RIP versión 2 soporta máscara subred de longitud variable (VLSM) y activación de updates de routers.

Una red directamente conectado tiene una métrica de cero. Una red inalcanzable tiene una métrica de 16. La métrica más alta entre dos redes puede ser de 15 saltos o routers. Es decir, RIP permite un máximo de 15 saltos de router entre

redes debido al tiempo que le toma para convergir todos los routers (estabilizar sus tablas de enrutamiento).

En la tabla 4.4.9.1 se muestra las características de RIP.

RIPv1 – RIP, RFC 1058	RIPRv2 – Multicasting RIP-2 updates, RFC 2453
El MAC destino es un broadcast, ff-ff-ff-ff-ff-ff	El MAC destino es un multicast, 01-00-5E-00-00-09
El IP destino es un broadcast para la red, 192.168.10.255/24	El IP destino es la dirección multicast RIP2, 224.0.0.9
La actualización RIP es formada como una actualización RIP1, no incluye la máscara de red.	La actualización RIP es formada como una actualización RIP2, incluye la máscara de red.
Versión de RIP = 1	Versión de RIP = 2

Tabla 4.4.9.1 : Características de RIP

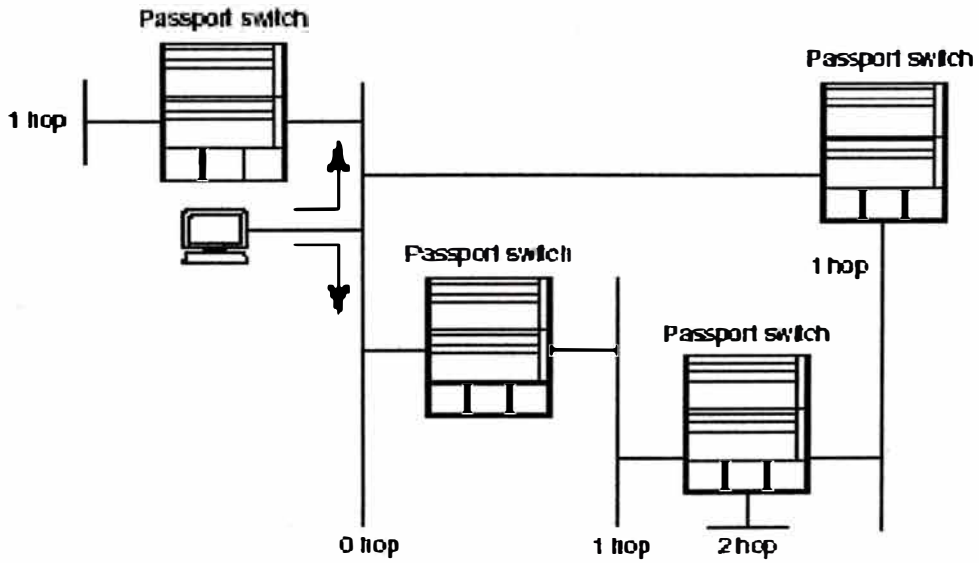


Figura 4.4.9.1 Cuenta de salto o Métrica en RIP

❑ CARACTERÍSTICAS DE OSPF

El protocolo OSPF (Abrir primero el camino más corto "Open Shortest Path First") fue creado para usarlo en grandes internetworks IP. Fue definida por el RFC 1583 y actualizada por el RFC 2178. Este es un protocolo de estado del enlace operando en un modo rápido, confiable y eficiente para que los routers intercambien información de la topología de la red. OSPF es un IGP "Interior Gateway Protocol" que es usado solo para enrutamiento IP. Este usa una ID del protocolo IP de 89 (referirse al RFC 1700). OSPF usa el algoritmo de Dijkstra (SPF "Shortest Path First" primero el camino más corto) para calcular las rutas.

OSPF resuelve problemas con:

- La convergencia, asegurando que todos los routers mantengan una base de datos idéntica con la topología.
- El overhead, solo anuncia los cambios en la red.

▪ Características funcionales de OSPF

Debido a las características funcionales de OSPF se trata de un sistema que tiene varias ventajas frente a los protocolos de vector de distancia. Entre las características se incluyen las siguientes:

- Rápida convergencia
- Jerarquía de Areas para control de la información de enrutamiento
- Soporte para VLSM "Variable Length Subnet Mask"
- Métricas de enrutamiento configurable
- Soporte para multiruta de igual costo.

- Autentificación.
- IP multicast
- Soporte para rutas externas etiquetadas.

4.4.10 El PROTOCOLO OSPF

- **EL VERDADERO COSTO DE LOS ENLACES DE RED**

Los protocolos de enrutamiento vectores de distancia, tales como el RIP, determinan la mejor ruta a redes remotas contando el numero de saltos. El numero más pequeño de saltos es designado como la mejor ruta. Mientras este tipo de métrica trabaja cuando todos los enlaces de red tienen el mismo throughput , los protocolos vectores de distancia tienen dificultad para determinar la "mejor " ruta si los enlaces en la red varían en capacidad. Los protocolos semejantes al RIP realizan cálculos distribuidos. Cada router aprende el costo de todas las redes desde sus vecinos. El router luego selecciona la ruta desde esta lista , adiciona su propio costo a esta lista y envía esta información a todos sus vecinos.

Como un ejemplo , una interfase RIP de 900 baudios tiene la misma métrica que una interfase Gigabit. RIP no tiene modo de distinguir entre los dos, al menos que el administrador asigne una cuenta de salto alta artificialmente en la interfase lenta, una practica que no todos los fabricantes soportan.

Los protocolos de enrutamiento de estado del enlace superan a estas limitaciones. Estas clases de protocolos de enrutamiento usan una base de datos distribuida replicada para calcular las rutas a todas las redes. Cada router anuncia el

costo a cada uno de sus vecinos. Este costo es luego fluido a todos los routers en la red. Estos anuncios forman la la base de datos que cada router mantiene. Para calcular la tabla de enrutamiento, cada router independientemente determina el mejor costo de todas las redes usando esta base de datos. Los protocolos de estado del enlace , semejante al OSPF, anuncian solo los costos de los enlaces asociados con un router. La métrica puede reflejar la velocidad de la interfase. Luego usando estos costos anunciados, cada router puede calcular la mejor ruta a través de la red.

Usando el ejemplo anterior, una interfase de 9600 baudios puede tener una métrica de 10,000 y una interfase Gigabit puede tener una métrica de 1. Estas métricas reflejan las diferencias en la velocidad de las interfases.

- **CUAL PROTOCOLO DE ENRUTAMIENTO USAR RIP (VECTOR DE DISTANCIA) O OSPF (ESTADO DEL ENLACE) ?**

¿Cómo decidir sobre un protocolo de enrutamiento para una red IP?. La selección de un protocolo basado en estándar es entre RIP y OSPF. Cada uno de estos protocolos tiene un lugar en el mundo de enrutamiento IP, el secreto es usar uno de ellos que mejor llene los requerimientos de su red.

- **RIP**

La tabla 4.4.10.1 resume los atributos de RIP versión 2.

En general , RIP es un protocolo fácil de usar en redes pequeñas que tengan enlaces estables. Este requiere especialización en el protocolo mínima o esfuerzo de diseño inicial para funcionar bien. Si embargo, desde que RIP difunde todas las tablas de enrutamiento, este overhead puede ser inaceptable en grandes redes

corporativas. También, este no se adapta rápidamente en caso de enlaces de red fallada en ambientes de misión critica.

Ventajas de RIPv2	Desventajas de RIPRv2
Simple de configurar	Tiempo de convergencia lento.
Requerimientos bajos de CPU.	Pobre detección de lazos de enrutamiento
Soportado por un amplio arreglo de hardware y software por parte de los fabricantes.	Alta utilización del ancho de banda en redes grandes y/o enlaces pequeños.
Soportado por muchos dispositivos legacy.	La métrica no refleja la velocidad del enlace.
Versión de RIP = 1	El diámetro de la red es limitado a 15 saltos (infinito)

Tabla 4.4.10.1 : Ventajas y desventajas de RIP versión 2

- **OSPF**

La tabla 4.4.10.2 resume los atributos de OSPF.

En general , OSPF esta mejor indicado para redes corporativas grandes. Las habilidades de OSPF para restringir el efecto de cambios de topología a una única área, su uso de la métrica reflejando la verdadera velocidad del enlace y su gran control sobre la sumarización, importación de rutas, etc lo hacen un claro ganador en redes grandes.

OSPF requiere más planeamiento, alta performance de las unidades de procesamiento central (CPUs) de los routers y equipos de administración de red

experimentados para monitorear su performance. Estos requerimientos pueden conducir a costos de implementación más alto.

Ventajas de OSPF	Desventajas de OSPF
Convergencia más rápida.	Más difícil de configurar y mantener.
Cambios de la topología limitado al área local.	En redes mal diseñadas, el flujo de LSA puede causar congestión.
La métrica usada refleja la velocidad del enlace.	Requiere una alta performance de los CPU en los router.
Soporta redes grandes.	Configuración y optimización (afinamiento) requiere alta competencia.
Excelente soporte para sumarización entre áreas y desde redes externas.	Más complejo de configurar y para resolver problemas "troubleshoot"
Soporta redes punto a punto y redes broadcast.	Consideraciones cuidadosas deben ser dadas para la numeración de la red para tomar ventaja de la sumarización de rutas.

Tabla 4.4.10.2 : Ventajas y desventajas de OSPF

- **OBJETIVOS DEL PROTOCOLO DE ENRUTAMIENTO OSPF**

OSPF es clasificado como un protocolo IGP "Interior Gateway Protocol". Esto significa que distribuye la información de enrutamiento entre routers perteneciente a un único Sistema Autónomo (AS). El protocolo OSPF esta basado en el estado del enlace o en la tecnología SPF ("Shortest Path First" primero el camino

más corto). Esta es una innovación del Bellman-Ford básico usado por el tradicional protocolo de enrutamiento RIP de TCP/IP.

El protocolo OSPF fue desarrollado por el grupo de trabajo OSPF del"Internet Engineering Task Force" . Este ha sido diseñado expresamente para el ambiente de Internet TCP/IP, incluyendo soporte explicito para CIDR "Classless Inter.-Domain Routing" y el etiquetado "tagging" de información de enrutamiento derivado externamente. OSPF también provee la autentificación de las actualizaciones de enrutamiento y utiliza IP multicast cuando envia/recibe las actualizaciones.

OSPF responde rápidamente a cambios de la topología, involucrando pequeñas cantidades de tráfico del protocolo de enrutamiento.

- **CARACTERÍSTICAS GENERALES DEL PROTOCOLO DE ENRUTAMIENTO OSPF**

  - Creado específicamente para usarlo en grandes internetworks IP, es uno de un numero de protocolos de estado del enlace. NLSP y IS-IS son ejemplos de otros protocolos de estado del enlace.
  - La métrica esta basada en el costo. No hay métrica inalcanzable.
  - Diseñado para soportar CIDR "Classless Inter-domain Routing".
  - Soporta redes punto a punto numeradas y no numeradas.
  - Habilita enrutamiento de tipo de servicio (TOS) y multiruta de igual costo.
  - Converge más rápidamente que RIP. En un ambiente OSPF, LSAs y no redes son intercambiadas. Estos anuncios reflejan la información

de topología actual de la red. La distribución de los LSAs es activada por cualquier cambio en la red y fluida a todos los routers.

- Puede hacer uso intensivo de CPU, particularmente cuando OSPF esta recalculando nuevas rutas. La base de datos de estado del enlace y el árbol SPF consume memoria adicional.
- Requiere más planeamiento y cuidadoso uso de los asignamientos de direcciones de red para usar mejor sus características. Rip es un plug – and-play.
- Usa el algoritmo SPF de Dijkstra.
- El RFC "Request for Comment" 1583/2178/2328 (OSPF versión 2) representa el presente estándar.

❑ TÉRMINOS FUNDAMENTALES RELACIONADOS CON OSPF

Entre los diversos términos operativos básicos relacionados con el protocolo OSPF, que nos sirven para comprender el funcionamiento de OSPF, podemos mencionar:

- **Enlace** – Conexión directa a una red (la interfaz a una red dada).
- **Estado de enlace** – Es la situación en que se encuentra un enlace (activado, desactivado, etc)

- **Coste** – Se trata de la métrica asociada a un enlace. Los costes OSPF se basan en el ancho de banda del enlace (por omisión, 10 /ancho de banda).
- **Área** – Constituye una frontera para el cálculo en la base de datos del estado del enlace. Los routers que están en la misma área contienen la misma base de datos topológica. Las áreas son definidas por los *identificadores de área*. Un área no equivale a un AS. En OSPF, un *área* es una subdivisión de un AS. Cada enlace puede asignarse a un área distinta. Si un router contiene un enlace a un área determinada, se considera un router interno (IR, *Internal Router*) de dicha área. Si un router contiene enlaces a varias áreas dentro del mismo AS, se considera un router de borde de área (ABR *Area Border Router*). Finalmente, si un router contiene enlaces a distintos AS, se considera un router de borde de sistema autónomo (ASBR, *Autonomous System Border Router*).
- **Saludo** – Es un paquete que se utiliza para establecer relaciones de vecindad con routers conectados directamente. Los paquetes de saludo se envían a intervalos periódicos de tiempo, conocidos como *intervalo de saludo*, para mantener relaciones de vecindad. Asimismo, los saludos se utilizan para verificar comunicaciones bidireccionales, anunciar requerimientos de vecindad y elegir router designados (DR, *Designated Routers*), así como routers designados de seguridad (BDR, *Backup Designated Routers*).

- **Intervalo de vecino no operativo –** Se trata de un intervalo utilizado para determinar cuándo hay que considerar que un vecino no ésta operativo (similar al tiempo de espera en el protocolo EIGRP).
- **Vecino –** Router conectado directamente que cumple los parámetros contenidos en el saludo y puede establecer una comunicación bidireccional. Para que dos routers se conviertan en vecinos deben tener los mismos saludos e intervalos de ausencia de vecino, identificador de área, contraseña y máscara de red para el enlace en el que se escuchó el saludo, así como el mismo indicador de área modular. No todos los vecinos se convertirán en elementos adyacentes.
- **Adyacencia –** Conexión virtual a un vecino a través de la que se pueden transferir los anuncios de estado del enlace (LSA, *Link State Advertisements*). Los vecinos se convierten en elementos adyacentes con respecto a los BDR y DR de las redes basadas en difusión y con los puntos extremos remotos en las redes NBMA punto a punto.
- **Anuncio de estado del enlace (LSA) –** Se trata de un anuncio de enlace topológico. Los LSA se incluyen en los paquetes de actualización de estado del enlace (paquete tipo 4). Los LSA parciales, se incluyen en los paquetes de descripción de base de datos (paquete tipo 2), en los paquetes de petición de estado del enlace (paquete tipo 3) y en los paquetes de acuse de recibo del enlace (paquete tipo 5).

- **Listado de petición de estado del enlace** – Esta lista se utiliza para llevar un registro de los LSA que deben solicitarse. Cuando un router se da cuenta de que no tiene la versión más actualizada de un LSA anunciado (o simplemente no tiene el LSA) en un paquete de descripción de base de datos (paquete tipo 2) o en un paquete de petición de estado del enlace (paquete tipo 3), agrega el LSA a esta lista.
- **Listado de retrasmisión de estado del enlace** – Es la lista que contiene los LSA que no se han reconocido. Cuando un router envía uno o más LSA a un vecino en un paquete de actualización de estado del enlace (tipo 4), espera recibir un acuse de recibo de paquete. Si no aparece dicho acuse de recibo antes de que caduque el tiempo límite de la retrasmisión , el router retransmitirá el LSA. Una vez que se oye un acuse de recibo implícito o explícito, el router elimina el LSA de la lista.
- **Acuse de recibo implícito** – Se trata de un acuse de recibo que se produce si un router detecta un paquete de actualización de estado del enlace (tipo 4) procedente de un vecino adyacente que incluya un LSA contenido en la lista de retransmisión de estado del enlace correspondiente a dicho vecino adyacente.
- **Acuse de recibo explícito** – Se trata de un acuse de recibo que se produce si un router recibe un paquete de acuse de recibo de estado del enlace (tipo 5), procedente de un vecino adyacente que incluya

uno o más LSA contenidos en la lista de retransmisión de estado del enlace correspondiente a este vecino adyacente.

- **Inundación** – Es el proceso que consiste en enviar LSA a todas las interfases aplicables (estas interfases dependen del tipo de LSA).
- **Identificación de router** – Es el sistema que permite identificar el router. Puede tratarse de una dirección IP de interfaz (la configuración por omisión) o bien de un número definido estadísticamente. Cada router presente en un AS debe tener un identificador único.
- **Número de secuencia de LSA** – Es el número que se asigna a cada LSA para identificar su versión. En términos generales, los números de secuencia se incrementan con cada cambio producido en un LSA. De esta manera, los números elevados suelen asociarse con LSA más actualizados
- **Prioridad** – Es la capacidad de un router de convertirse en el DR o en el BDR, en el proceso de elección. En términos generales, el router con la prioridad más alta sobre un segmento se convierte en Dr. Los rangos de prioridad van de 0 a 255 y el valor por omisión (para routers Cisco) es 1. Los routers que tengan una prioridad 1 no pueden elegirse para convertirse en DR o BDR.

COMPONENTES BÁSICOS DE OSPF

La Base de datos de estado del enlace y el árbol SPF

La Figura 4.4.10.1 ilustra los componentes básicos de OSPF.

Los routers usando protocolos de estado del enlace, tales como OSPF, no intercambian información de enrutamiento. Ellos intercambian información de estado del enlace, el cual es mantenido por cada router en una base de datos describiendo la topología del dominio. Esta base de datos es llamada es llamada la base de datos de estado del enlace (LSDB "Link State Database") y tiene la siguiente característica:

- La base de datos es frecuentemente displayada en literaturas técnicas como un diagrama con gráficos compuestos de nodos y bordes.
- El LSDB es una estructura de datos conteniendo LSAs. Cada router participante tiene una base de datos idéntica. Cada anuncio "advertisement" en el LSDB fue construido por uno de los routers en el dominio OSPF y enviado a cada otro router OSPF (inundación "flooding").
- Usando el algoritmo SPF de Dijkstra y trabajando desde el LSDB, cada router construye un árbol de caminos más corto considerándose así mismo como la raíz "root" (llamado el árbol SPF). Todos los routers ejecutan este algoritmo en paralelo. El árbol SPF da la ruta a cada destino en el sistema autónomo. Una mejor ruta OSPF puede ser derivada desde el árbol SPF.
- El LSDB no contiene las mejores rutas. El árbol SPF derivado desde este LSDB contiene la mejor ruta OSPF y en el Passport 8600 la

mejor ruta OSPF es pasada al administrador de tabla de enrutamiento (RTM "Routing Table Manager").

- Usando las preferencias de las rutas, el RTM compara las mejores rutas OSPF con las otras rutas de los protocolos para un destino dado y luego lo puebla en la tabla de enrutamiento. El router envía un datagrama al siguiente salto de router basado en la tabla de enrutamiento.

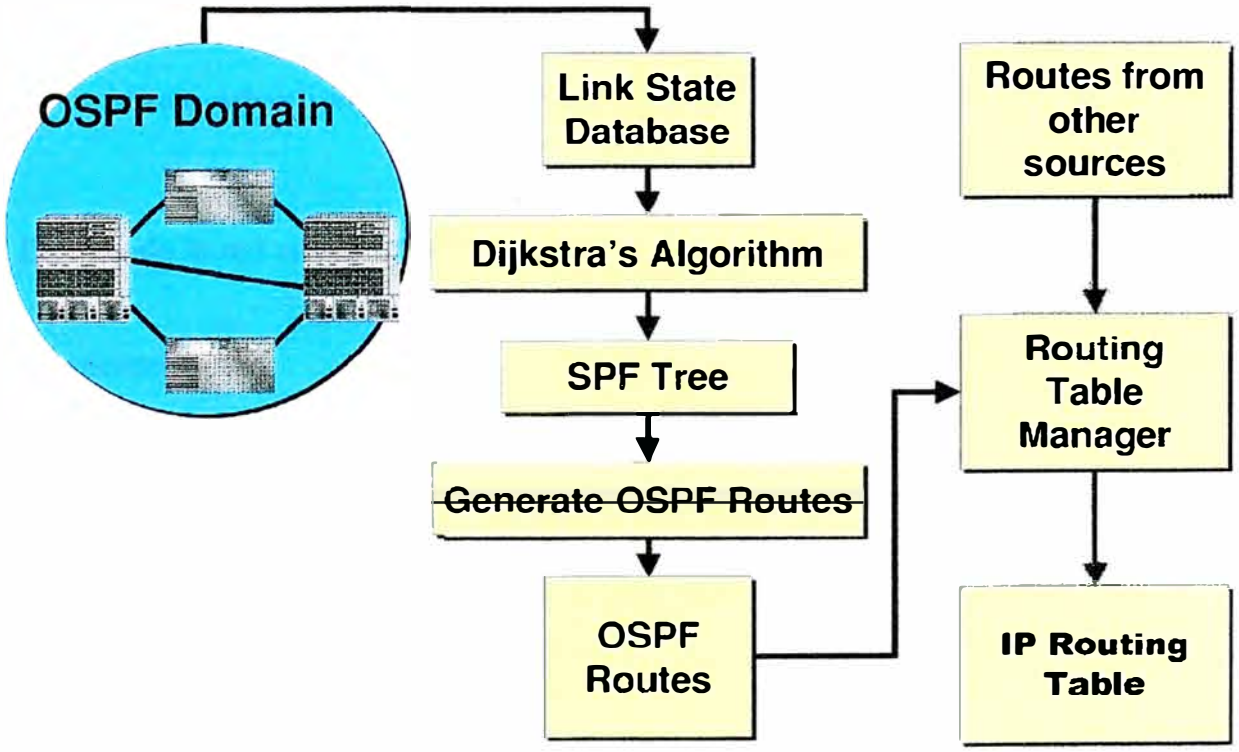


Figura 4.4.10.1 Componentes básicos de OSPF.

- **ÁREAS OSPF**
  - **¿Porque Áreas?**

En corporaciones grandes, con muchos routers y redes, el LSDB "Link State Database" y las tablas de enrutamiento serán grandes. Esto no es una ventaja debido a que:

- Las tablas de enrutamiento grandes consumen memoria y resultan en más ciclos de unidad de procesamiento central (CPU) siendo necesario para realizar una decisión de envío.
- Grandes LSDBs consumen memoria.
- El procesamiento de los anuncios de estado del enlace (LSAs "Link State Advertisements") es intensivo en el CPU.

Dividiendo la red en áreas OSPF se puede reducir estos efectos indeseables.

- **Características**

Cuando una red es dividida en áreas :

- Una separada LSDB es mantenida para cada área.
- Routers internos del área mantienen solo una LSDB del área al cual ellos pertenecen.
- Routers de borde de área (ABRs, Area border routers) deben mantener un LSDB por cada área al cual ellos pertenecen.
- Redes exteriores a un área son anunciadas dentro del área.

- **Ventajas**

  Algunas ventajas de la implementación de áreas OSPF son como sigue

  - Routers interno en el área incurren en menos overhead.
  - El impacto de un cambio de topología es localizado en el área en el cual esto ocurre. Aunque el cambio es anunciado exteriormente al área, el procesamiento de LSA y la consecuente modificación del árbol SPF, requiere menos overhead de CPU.
  - Con un cuidadoso planeamiento de las direcciones de red, las redes dentro del área pueden ser anunciadas en la forma de un resume. Esto reduce la cantidad de procesamiento de todos los routers externo al área y el tamaño de la tabla de enrutamiento.

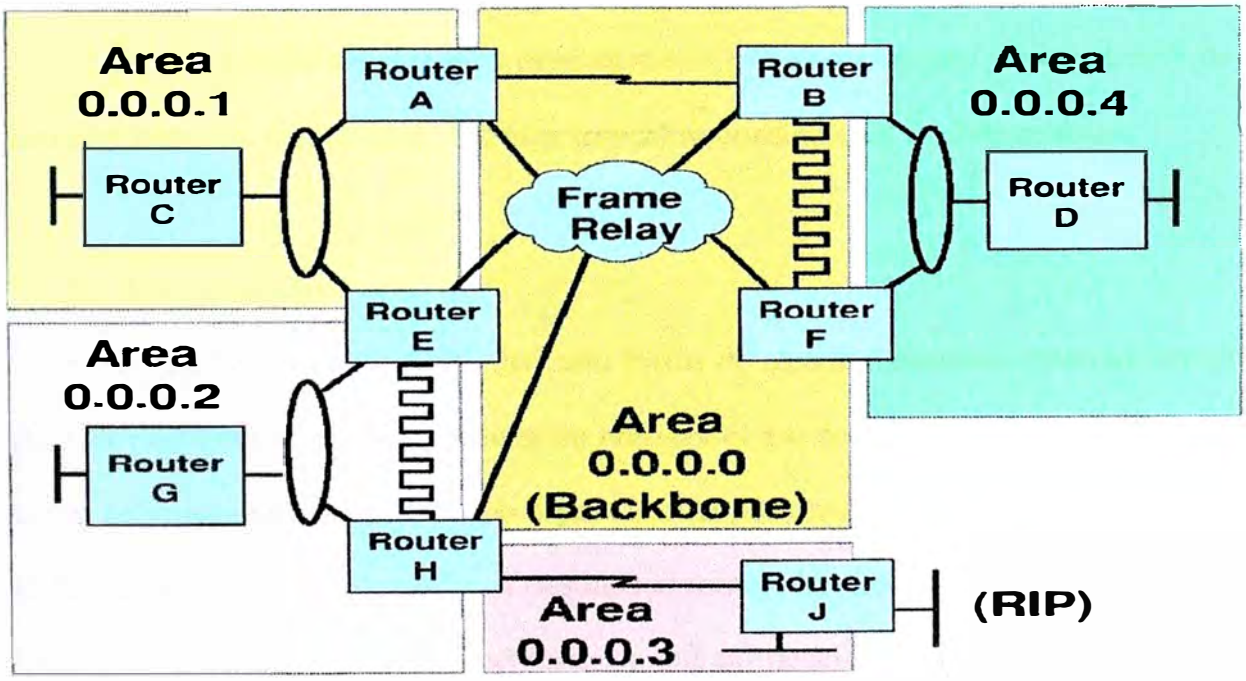


Figura 4.4.10.2 ¿Por qué Areas?.

- **TIPOS DE ÁREAS OSPF**

Entre los tipos de áreas OSPF tenemos:

- **Área estándar**

Es el tipo de área más común. Todas aquellas áreas que no sean troncales "Backbone" o alguna clase de área modular son áreas estándar. Dichas áreas admiten LSA que van del tipo 1 al tipo 5.

- **Área troncal "backbone" (Area 0)**

Es el concentrador presente en AS OSPF. El área troncal "Backbone" tiene la responsabilidad de garantizar el tráfico entre distintas áreas. Todas las áreas situadas en una solución OSPF multiárea deben tener una conexión con el área troncal.

- **Área de tránsito**

Es un área donde el tráfico procedente de otras áreas puede viajar a través de una ruta hasta su destino final. Un área troncal se considera un área de tránsito.

- **Área modular**

Es un área en la que sólo hay una forma de alcanzar destinos externos (otros AS). Por esta razón, un área modular no requiere el uso de LSA tipo 4 o tipo 5. En su lugar, se inserta un único LSA tipo 3 para la ruta por omisión en el área modular con el fin de proporcionar el camino a destinos externos. Las áreas modulares requieren menos recursos de red, CPU y memoria, ya que no tienen necesidad de mantener los LSA externos en la tabla topológica. Las áreas modulares sólo permiten el uso de LSA de tipo 1 a tipo 3.

- **Área totalmente modular**

Es un área en la que sólo hay una forma de alcanzar destinos externos (otros AS) y destinos entre áreas. En otras palabras, en un área totalmente modular hay una única forma de alcanzar destinos externos que conducen al área. Por esta razón , esta clase de área no requiere el uso de LSA tipo3, tipo 4 ni tipo 5. Dentro del área modular se inserta una única ruta por omisión para obtener un camino que lleve a todos los destinos que no formen parte del área totalmente modular. Por ello requiere menos recursos que las áreas modulares. En el caso de las áreas totalmente modulares sólo se permite el uso de LSA tipo 1 y tipo 2 (salvo el caso de los LSA tipo 3 que se utilizan para la ruta por omisión). Las áreas totalmente modulares constituyen una mejora no definida en RFC (definida por cisco).

- **Área no tan modular (NSSA, "Not So Stubby Area")**

Es un área que requiere la transmisión de LSA externos desde un ASBR dentro del área, pero que sólo tiene un camino que conduce a los ASBR presentes en otras áreas. Puesto que el área NSSA sólo dispone de un camino que conduce a destinos externos a los que acceden los ASBR de otras áreas, el área NSSA puede ser un área modular. Sin embargo, como estas últimas no admiten el uso de LSA tipo 5 y la NSSA contiene un ASBR (que genera LSA tipo 5), es preciso que la NSSA sea un área de tránsito estándar (lo que incrementa los recursos necesarios para albergar dicha área). En este caso, cabe configurar el área como una NSSA. Los ASBR en una NSSA generan LSA tipo 7 (en lugar de los LSA tipo 5) para anunciar destinos externos, al tiempo que los ABR correspondientes a dichas NSSA convierten los LSA tipo 7 en LSA tipo 5 para el resto del AS. No obstante, las NSSA no admiten el

uso de LSA tipo 4 o tipo 5 y deben emplear una única ruta por omisión para alcanzar los destinos externos anunciados por los ASBR presentes en otras áreas. Las NSSA tienen definición RFC y se describen en el RFC 1578.

- **TIPOS DE ROUTERS OSPF**

Hay cuatro tipos de routers OSPF:

- Router Interno.
- Router de borde de área (ABR, "Area Border Router")
- Router de Backbone o troncal
- Router de borde de sistema autónomo (ASBR, "Autonomous System Border Router")

- **Routers internos**

Un router interno es un router interno con todas las redes conectadas directamente pertenecientes a la misma área. Los routers con solo interfaces backbone también pertenecen a esta categoría. Estos router ejecutan una única copia del algoritmo de enrutamiento básico y mantienen un SPF para esa área.

En otras palabras, un router interno es cualquier router que tenga todas las interfaces en la misma área. Todos los routers internos para un área dada tiene una única base de datos topológica idéntica.

- **Routers de borde de área (ABRs, "Area Border Routers")**

Un ABR es un router con interfases en múltiples áreas. Los ABRs mantienen múltiples LSDBs, una copia por cada área conectada, incluyendo el área backbone o troncal. Los ABRs deben estar conectadas al área backbone.

En otras palabras, un router ABR es cualquier router que tenga una o más interfases en distintas áreas. Los ABR se usan para resumir y enviar paquetes a través de los caminos situados en distintas áreas.

- **Routers de Backbone o troncal**

Un router de backbone es un router con una interfase al área Backbone. Este router puede también ser un ABR o un router interno. Los ABRs, por definición, también son routers de backbone.

En otras palabras, un router de backbone o troncal es cualquier router que tenga al menos una interfaz en el área 0 (el área backbone o troncal)

- **Routers de borde de sistema autónomo (ASBRs, "Autonomous System Border Routers")**

OSPF ve a las redes no OSPF como externa a su sistema autónomo (AS) y por consiguiente externa a él.. Un router OSPF conectado a tales redes como redes RIP o BGP es un router de borde de sistema autónomo (ASBR). Este router tiene rutas externas al AS que son anunciadas a lo largo del dominio OSPF. Cada router en el dominio OSPF conoce la ruta a cada router ASBR.

En otras palabras un ASBR es cualquier router que redistribuye rutas desde un protocolo de enrutamiento distinto o desde un AS OSPF en el AS OSPF de destino.

En la figura 4.4.10.3 se ilustra los tipos de routers OSPF.

Además de estos cuatro tipos de routers OSPF, también podemos mencionar a los siguientes tipos de router:

- **Router designado (DR, "Designated Router")**

Es el router elegido para ser el <<anunciante>> principal para una red lógica individual y todos los routers asignados a dicha red. Habitualmente, el DR es el router que tiene la prioridad más alta. Los DR sólo existen en redes multiacceso con más de un router que <<hablen>> el protocolo OSPF. Los DR establecen una adyacencia con todos los routers presente en la red.

- **Router designado de seguridad(BDR, "Backup Designated Router")**

Es el router elegido como el <<anunciante>> secundario para una red lógica individual y todos los routers asignados a dicha red. Habitualmente, el BDR es el router que tiene un índice de prioridad secundario. Los BDR sólo existen en redes multiacceso con más de un router que hablen el protocolo OSPF. Los BDR establecen una adyacencia con todos los routers presente en la red.

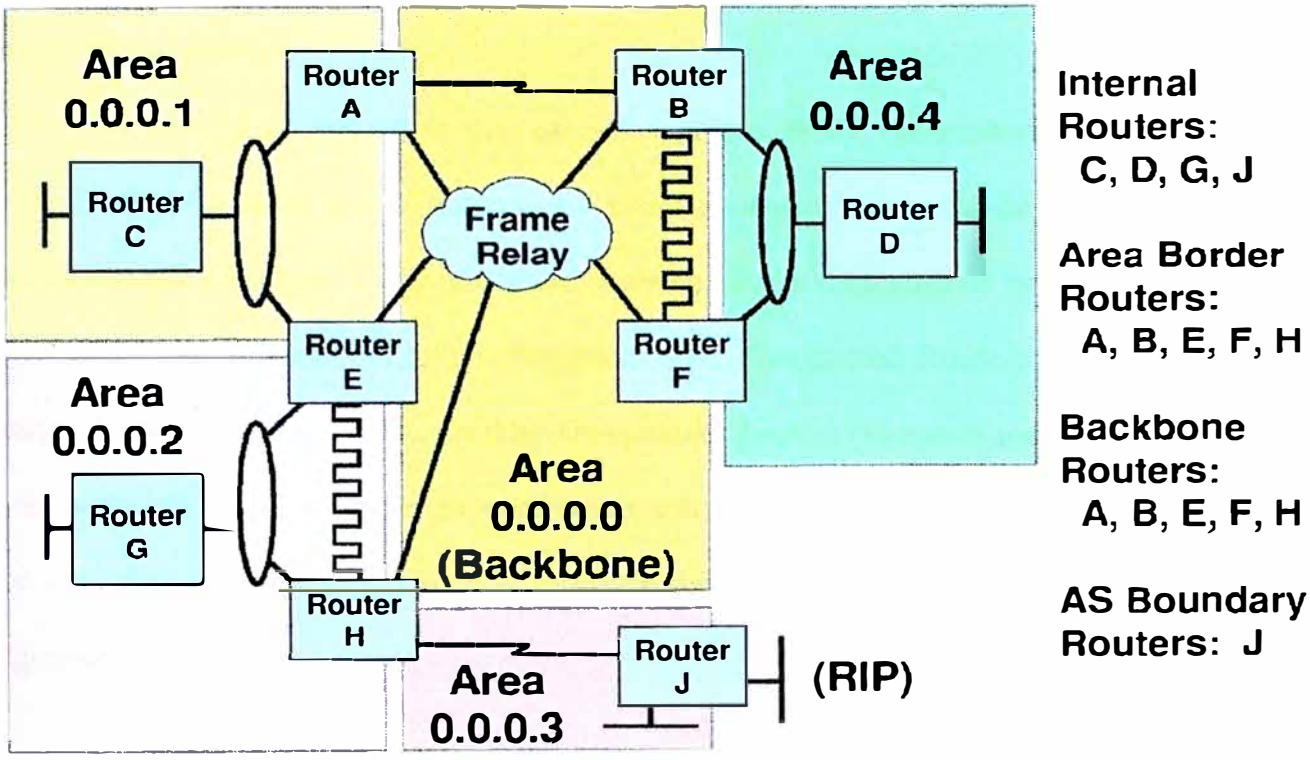


Figura 4.4.10.3 Tipos de Routers OSPF.

- **TIPOS DE REDES OSPF**

Los routers OSPF forman adyacencias diferentemente basados en los tipos de redes. Sin embargo, un protocolo no puede determinar el tipo de red al cual es conectado.

Debemos declarar el tipo de red en la configuración inicial. Fallas en esto pueden producir operaciones incorrectas de una interfase.

- **Red punto a punto**

Esta red conecta un único par de routers. Este es un enlace con solo un router en cada extremo. Enlaces tales como HSSI "High-Speed Serial Interface", T1 y sincronos, corriendo el protocolo PPP "Point –to-point Protocol" estándar son

ejemplos de redes punto a punto. Una red punto a punto puede ser tanto numerada como no numerada.

Es un tipo de red en la que un único enlace WAN (generalmente un PVC Frame Relay) conecta a dos routers. Es posible interconectar más de dos routers mediante varios enlaces. Cada uno debe tener su propia dirección de red lógica. En este entorno no se elige un router designado (DR, Designated Router) ni un router designado de seguridad (BDR, Backup Designated Router) (tampoco son necesarios) y las adyacencias de vecindad se configuran automáticamente. El tiempo de saludo por omisión es de 10 segundos y el intervalo de desconexión por omisión es de 40 segundos.

- **Red de broadcast (Difusión o multiacceso)**

Esta red soporta más de dos routers conectados. Este puede soportar el envío de un único mensaje a todos los routers (mensajes multicast). Ethernet, Token Ring, FDDI, y SMDS son ejemplos de medios soportando redes de broadcast. El switch Passport 8600 soporta redes de broadcast.

Se trata de una red que sigue las convenciones básicas Ethernet, donde cada anfitrión que forma parte de la misma red lógica puede comunicarse con cualquier otro anfitrión. En esta configuración se eligen los routers designado (DR, Designated Router) y los routers designado de seguridad (BDR, Backup Designated Router), mientras que el establecimiento de vecindad y adyacencia es automático. El tiempo de saludo por omisión en esta red es de 10 segundos y el intervalo de desconexión por omisión es de 40 segundos.

- **Red multiacceso no broadcast (NBMA, "Non-broadcast Multi-access")**

Esta red soporta más de dos routers conectados, pero no tiene capacidad de broadcast. Los paquetes OSPF que son normalmente multicast son enviados a la dirección IP de cada router vecino. Redes como X25, Frame Relay y ATM "Asynchronous Transfer Mode" son ejemplos de redes NMBA. El switch Passport 8600 soporta redes NMBA.

- **Red punto a Multipunto (std)**

Esta red soporta capacidades OSPF en un ambiente de modos de grupos Frame Relay. (malla parcial y malla total).

Una ***red punto a multipunto, NBMA con emulación de difusión y en malla total*** es un tipo de red en la que cada router tiene una conexión punto a multipunto para cada router. Hay que observar que no se trata de una conexión multipunto individual que va de un router central a los demás routers (lo que equivaldría a una topología estrella), sino de una conexión multipunto desde cada router a los demás (convirtiendo la topología en una malla total). En este entorno resulta posible configurar todos los routers para que utilicen la misma red lógica con respecto a la malla y activar las difusiones a las conexiones multipunto. Por otro lado, en este entorno se eligen los DR y los BDR y se configuran automáticamente las adyacencias de vecino. En lo que respecta a esta red, el tiempo de saludo por omisión es de 10 segundos y el intervalo de desconexión por omisión es de 40 segundos.

Una ***red punto a multipunto, (NBMA con malla total)*** es un tipo de red en la que cada router tiene una conexión punto a multipunto con los demás routers. Hay

que observar que no se trata de una conexión multipunto individual desde un router central con los demás routers (lo que equivaldría a una topología en estrella), sino que, en su lugar, se usa una conexión multipunto para comunicar a cada router con los demás (lo que configura una topología de malla total). Todos los routers utilizan la misma dirección de red lógica, pero, en este caso, se desactiva la emulación de difusión. En este entorno se eligen los DR y los BDR y las adyacencias de vecino se configuran manualmente. El tiempo de saludo por omisión en esta red es de 30 segundos y el intervalo de desconexión por omisión es de 120 segundos.

Una ***red punto a multipunto, (NBMA estrella o malla*** parcial***)*** es un tipo de red con uno o más routers en una malla parcial o topología radial que comporta la existencia de enlaces punto a multipunto. En estas topologías, todos los routers utilizan la misma dirección de red lógica. En este entorno no se eligen los DR y los BDR (tampoco son necesarios), y las adyacencias de vecino deben configurarse manualmente. El tiempo de saludo en esta red es de 30 segundos y el intervalo de desconexión por omisión es de 120 segundos.

- **Interfase pasiva**

El switch Passport 8600 soporta una interfase pasiva permitiendo los anuncios de rutas internas sin formar adyacencias.

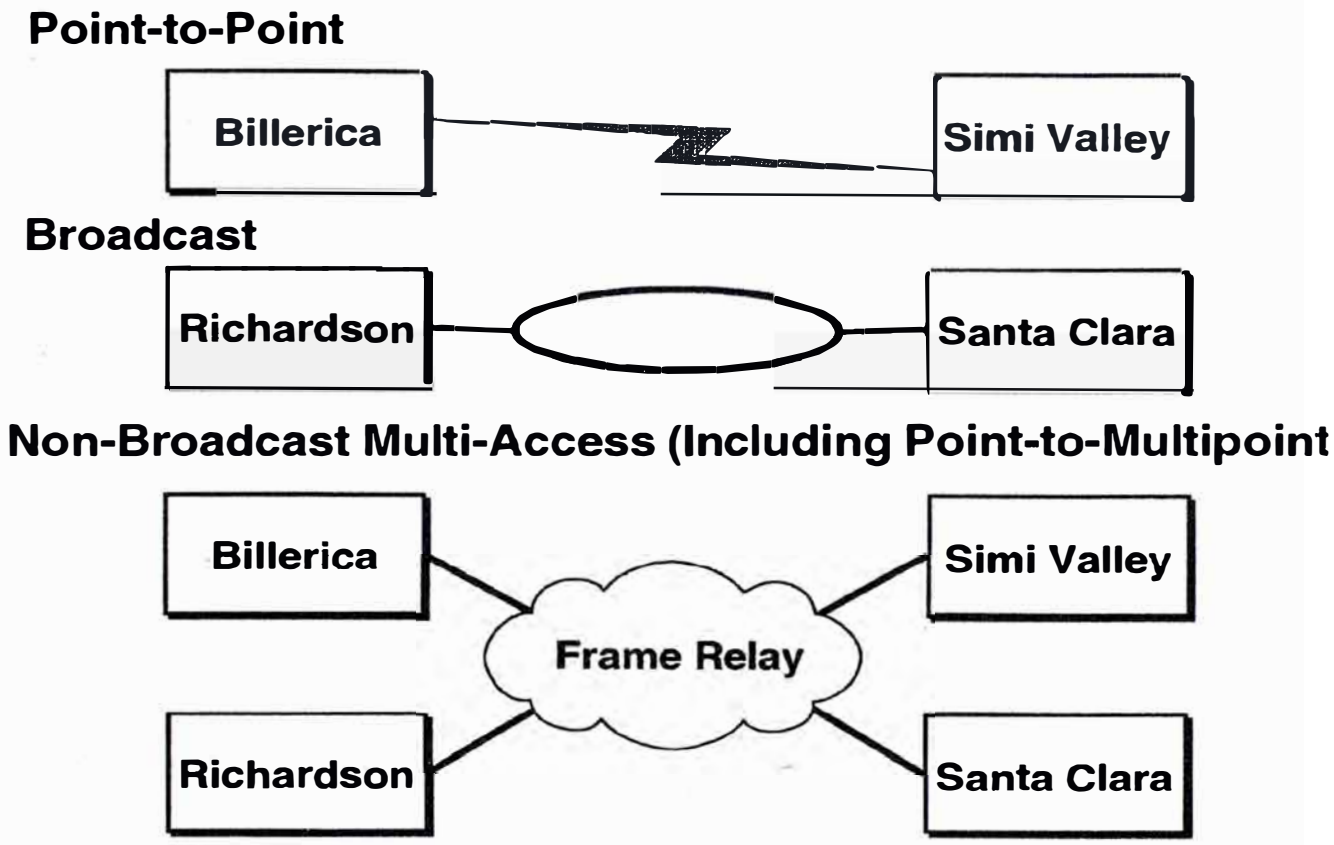


Figura 4.4.10.4 Tipos de Redes soportado por OSPF.

- **TIPOS DE PAQUETES OSPF**

Paquetes OSPF son encapsulados directamente en un paquete IP sin necesidad de ningún transporte:

DL Header	IP Header	OSPF packet

El ID del área, el checksum y la autentificación son validado para cada paquete OSPF. Si cualquiera de esto falla, el paquete OSPF es desechado y un error apropiado es anotado.

El campo tipo dentro de la cabecera del paquete OSPF indica cual tipo de paquete esta en el campo data del paquete OSPF. La siguiente tabla explica los tipos de código para cada tipo de paquete:

Tipo de código	Tipo de paquete OSPF
1	Saludo "Hello"
2	Descripción de la base de datos "Database description"
3	Petición de estado del enlace, "Link state request"
4	Actualización de estado del enlace, "Link state update"
5	Acuse de recibo de estado del enlace, "Link state acknowledment"

Tabla 4.4.10.3 : Tipos de código para paquetes OSPF

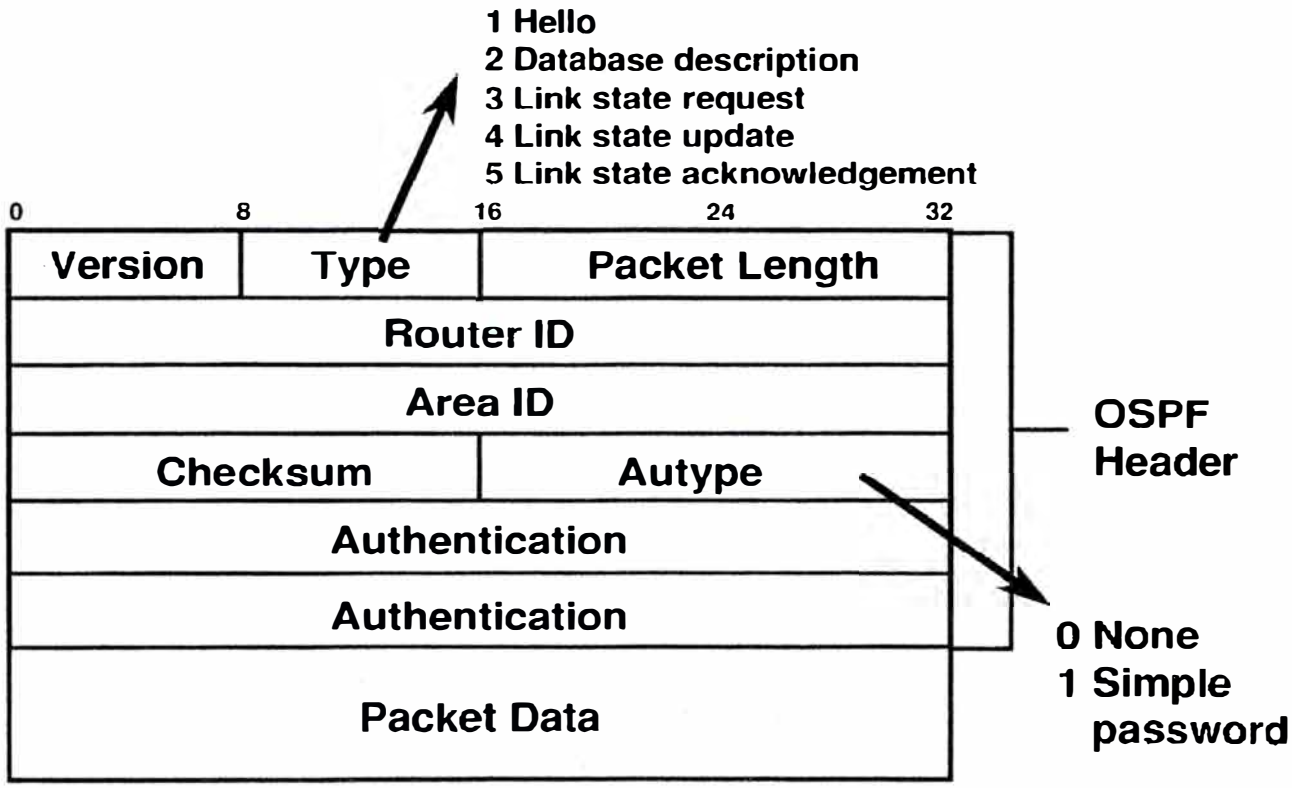


Figura 4.4.10.5 Tipos de paquetes OSPF

Explicando brevemente los tipos de paquetes OSPF y sus respectivos componentes mencionaremos:

- **Encabezamiento de paquete OSPF (incluido en todos los tipos)**

Incluyen información básica relacionada con el router, como es el caso de la versión de OSPF, el tipo de paquete, el identificador de router y el identificador de área.

- **Paquetes tipo 1 (saludo, "Hello")**

Permiten establecer y mantener adyacencias. Los paquetes de saludo incluyen toda la información necesaria para establecer una relación de vecindad, incluyendo los intervalos de saludo y de no operatividad, la contraseña, la máscara de red correspondiente al enlace al que se envió el saludo, el indicador de área de módulo, los DR y los BDR elegidos y cualquier vecino conocido.

La figura 4.4.10.6 ilustra el paquete "Hello".

Los mensajes "Hello" de OSPF es importante debido a que estos habilitan a los router a:

- Descubrir otros routers.
- Decidir si o no forma adyacencia.
- Mantener adyacencias.

Los mensajes "Hello" tiene los siguientes como destinos IP:

- 224.0.0.5 ("AllSPFRouters") en redes punto a punto y redes broadcast.
- Una dirección IP vecina definida estáticamente sobre una red NBMA y por enlaces virtuales.

Los mensajes "Hello" llevan la siguiente información:

- La máscara de red asociada con esta interfase.
- El intervalo de "Hello" especificando que tan frecuente espera el "Hello"
- Prioridad del router enviador.

- El temporizador del intervalo muerto "Dead interval timer" especificando cuanto tiempo el enviador espera recibir ningún "Hellos" antes de romper la adyacencia.
- DR por su dirección IP
- BDR por su dirección IP
- Lista de los routers vecinos sobre la red dada por el ID de los routers.

- **Paquetes tipo 2 (descripción de base de datos, "Database Description")**

Construye la base de datos de estado del enlace que hay en el router cuando se inicializa una adyacencia. Los paquetes de descripción de base de datos incluyen encabezamientos LSA (no todo el LSA) para que el router receptor confirme que tiene todos los LSA requeridos.

- **Paquetes tipo 3 (petición de estado del enlace, "Link state request")**

Solicita los LSA específicos desde los vecinos. Los paquetes de petición de estado del enlace se envían basándose en las entradas situadas en el listado de petición de estado del enlace.

- **Paquetes tipo 4 (actualización de estado del enlace, "Link state update")**

Suministra los LSA a los routers remotos. Se considera que están *inundados* cuando un LSA cambia, o bien cuando se recibe una petición de estado del enlace. Los paquetes tipo 4 deben reconocerse.

- **Paquetes tipo 5 (acuse de recibo de estado del enlace, "Link state acknowledment")**

Envío de un acuse de recibo explícito a uno o más LSA.

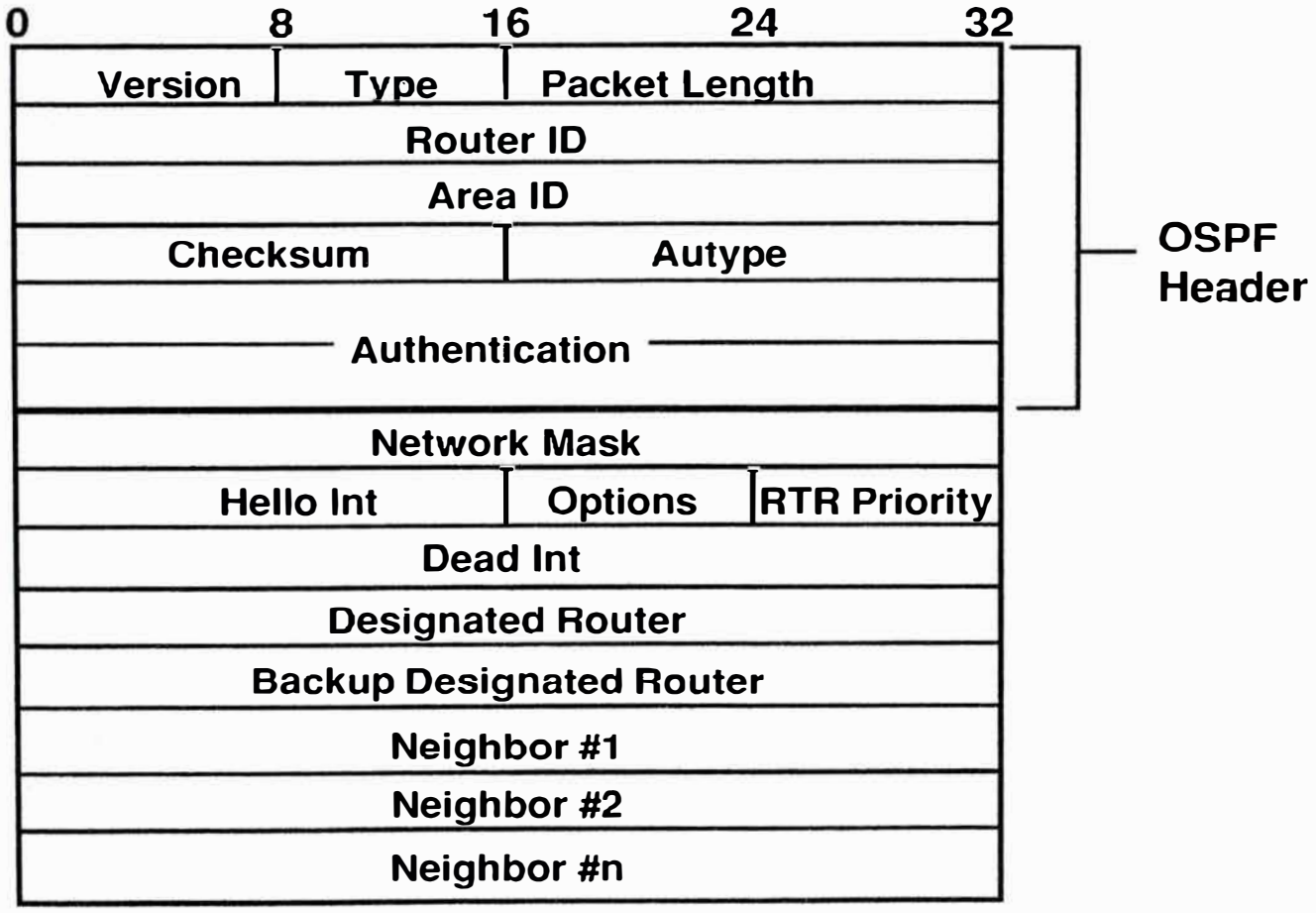


Figura 4.4.10.6 paquete Hello

- **TIPOS DE ANUNCIO DE ESTADO DEL ENLACE (LSA, LINK STATE ADVERTISEMENTS)**

Los seis tipos de LSAs representan una pieza de la red OSPF .

- **LSA tipo 1 (entrada de enlace de router, "Router link advertisement")**

Lo genera el router correspondiente a cada área de la que forma parte dicho router. Estos LSA contienen el estado de todos los enlaces de router de un área dada e inundan a todos los enlaces de la misma área.

En otras palabras, el LSA tipo 1 describe un enlace de un router en la red. Este es pasado solo dentro de un área.

El ID del estado del enlace = ID del router originante.

- **LSA tipo 2 (entrada de red, "Network link advertisement")**

Los genera los DR que están en todas las redes que no sean punto a punto (es decir, multiacceso). Los LSA tipo 2 incluyen a todos los routers vinculados a la red en la que el router actúa como DR.

En otras palabras, el LSA tipo 2 describe a las redes multiacceso. Este es pasado solo dentro de un área.

El ID del estado del enlace = La dirección de la interfase IP de los router designado (DR) de las redes.

- **LSA tipo 3 (entrada de estado del enlace de red resumen, "Summary link advertisement")**

Los generan los ABR y anuncian redes internas procedentes de un área específica a otros ABR. Luego , los ABR restantes eligen el mejor camino que conduce a la red o redes basándose en los LSA tipo 3 recibidos, inundando el mejor camino en áreas no troncales mediante el uso de este tipo de LSA.Hay que observar que estos LSA pueden constituir o no entrada de red resumida. Para resumir redes en los LSA tipo 3 hay que configurar los ABR con el objeto de resumir las entradas. Los LSA tipo 3 no se distribuyen a las áreas totalmente modulares (salvo un único tipo 3 para la ruta por omisión).

En otras palabras, el LSA tipo 3 describe a las redes dentro de un área. Este es pasado entre áreas.

El ID del estado del enlace = La dirección IP de la red destino.

- **LSA tipo 4 (entrada de estado del enlace de ASBR de resumen, "AS summary link advertisement")**

Los utilizan los ABR para anunciar los mejores caminos que conducen a los ASBR. Los LSA tipo 4 no inundan las áreas modulares, las áreas totalmente modulares ni las áreas no tan modulares(NSSA, Not-So-Stubby-Areas).

En otras palabras, el LSA tipo 4 describe una ruta al router de borde de sistema autónomo (ASBR "AS boundary router"). Este es pasado entre áreas.

El ID del estado del enlace = El ID del router del ASBR descrito.

- **LSA tipo 5 (entrada externa de AS,también denominada *entrada externa* "AS external link advertisement")**

Los envían los ASBR y anuncian los destinos externos a los AS (destinos redistribuidos desde otros AS OSPF u otro protocolo de enrutamiento). Las entradas de tipo 5 inundan todo el AS, salvo las áreas modulares, totalmente modulares y no tan modulares. Dichas entradas se dividen en dos subclases distintas,dependiendo del cálculo métrico utilizado:

- **Entrada externa tipo 1 (E1)** – Las entradas E1 tienen una métrica que se calcula como la suma del coste de la ruta redistribuida y el coste de los enlaces al router emisor. Habitualmente, las entradas E1 se emplean cuando más de un ASBR anuncia un destino externo determinado.
- **Entrada externa tipo 2 (E2)** – Las entradas E2 tienen una métrica que se calcula como el coste de la ruta distribuida (no se tiene en cuenta los costes de los enlaces internos que conducen al ASBR anunciado). Por esta razón, las entradas E2 resultan más <<económicas>> y los routers suelen preferirlas en lugar de las entradas E1.

En otras palabras, el LSA tipo 5 describe destinos externos originados sobre un router de borde de sistema autónomo (ASBR "AS boundary router"). Este es pasado entre áreas.

El ID del estado del enlace = La dirección IP de la red destino.

- **LSA tipo 7 (entrada de enlace externo NSSA, "AS external link advertisement in NSSA")**

Sólo los generan los ASBR en las NSSA. Los LSA tipo 7 sólo inundan las NSSA. Los ABR convierten los LSA tipo 7 en LSA tipo 5 para distribuirlos por el resto del AS. Estos LSA también se dividen en dos subclases:

- **Tipo 1 externo NSSA (N1)** – Las entradas N1 calculan su métrica como la suna del coste de la ruta redistribuida y el coste de los enlaces al router emisor. Habitualmente, las entradas N1 se utilizan cuando más de un ASBR anuncia un destino externo determinado.
- **Tipo 2 externo NSSA (N2)** – Las entradas N2 calculan su métrica simplemente como el coste de la ruta redistribuida (no se tiene en cuenta el coste de los enlaces internos al ASBR que realiza los anuncios). Por esta razón, las entradas N2 son más <<económicas>> y los routers suelen preferirlas en lugar de las entradas N1.

En otras palabras, el LSA tipo 7 describe destinos externos originados sobre un router de borde de sistema autónomo (ASBR "AS boundary router") en un NSSA. Los enlaces tipo 7 son trasladados en los ABRs a LSA tipo 5.

El ID del estado del enlace = La dirección IP de la red destino.

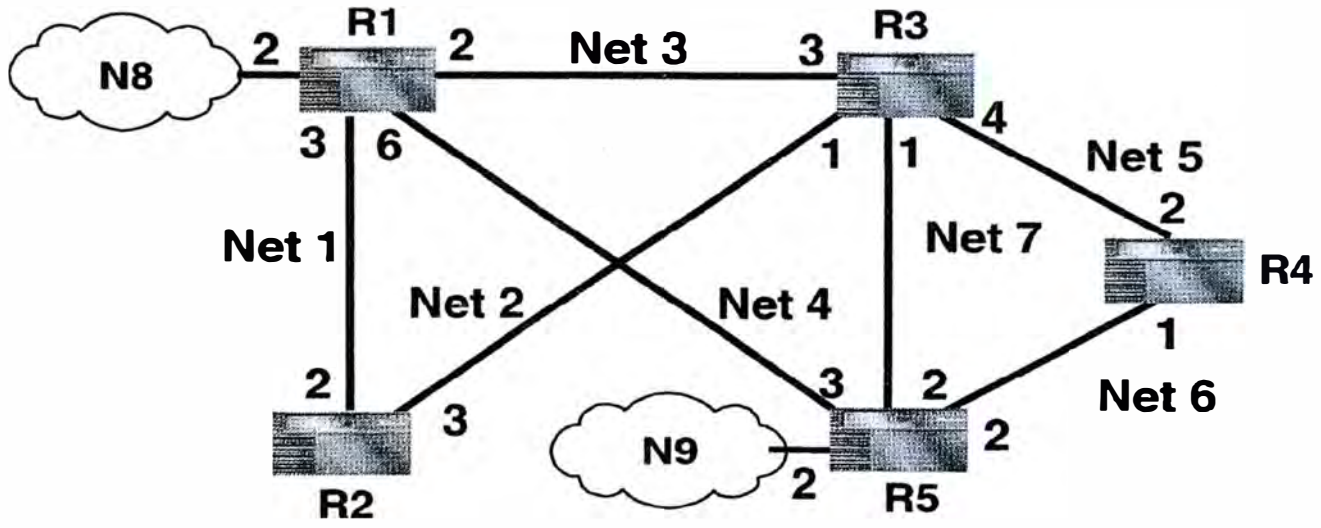
▫ CONSTRUYENDO LOS LSDB

Cada router construye un anuncio describiendo su entorno inmediato. Estos anuncios contendrán routers y redes vecinas.

En el anuncio, solo redes conectadas directamente son incluidas.

LSA puede propagarse a lo largo del dominio OSPF.

En la figura 4.4.10.7, los LSDB de todos los routers contienen información acerca de la red completa.Esta información es compuesta junto con los otros anuncios recibidos de los otros routers participante dentro del dominio OSPF.



Link State Database (all routers)
R1 Net 1/3, Net 3/2, Net 4/6, Net 8/2, R2/3, R3/2, R5/6
R2 Net 1/2, Net 2/3, R1/2, R3/3
R3 Net 3/3, Net 2/1, Net 7/1, Net 5/4, R1/3, R5/1, R2/1, R4/4
R4 Net 5/2, Net 6/1, R3/2, R5/1
R5 Net 4/3, Net 7/2, Net 6/2, Net 9/2, R1/3, R3/2, R4/2

Figura 4.4.10.7 Construyendo el LSDB.

ADYACENCIAS OSPF

¿Porque formar adyacencias entre los Routers?

OSPF crea adyacencias entre los routers vecinos con el propósito de intercambiar información de la LSDB. El switch Passport 8600 capa 3 soporta hasta 480 adyacencias.

El protocolo "Hello" es usado para determinar si dos routers serán puesto como adyacentes. El protocolo "Hello" verifica que ambos routers están en la misma área, tiene la misma temporizaciones de interfase y máscara de red y concuerdan sus capacidades de router. Si todas estas pruebas son pasadas, los routers pueden entonces intercambiar información de estado del enlace.

Formación de una adyacencia

El proceso general que los routers OSPF usan para formar una adyacencia es listado a continuación. Para información más detallada acerca de este proceso referirse al RFC 2328.

1. Los routers A y B intercambian paquetes "Hello". Basados en el contenido A y B deciden si se convertirán en completamente adyacentes.
2. Router A y B comparan LSDBs intercambiando paquetes con la descripción de la base de datos. Estos paquetes no proveen el suficiente detalle para realmente actualizar la base de datos, solo proveen el suficiente detalle para averiguar cuales LSAs no están

todavía en la base de datos local y cuales LSAs presentemente en la base de datos están fuera de fecha.

3. Cada router actualiza su base de datos trasmitiendo una petición de estado del enlace al otro router. La petición es considerada cumplida cuando un estado del enlace actualizado es recibido conteniendo los LSAs solicitados.

   Cada router actualiza su base de datos con información que este considera mejor que el que ya tiene. Un número de secuencia contenida en cada LSA determina que información constituye mejor. La recepción de cada LSA es reconocido usando el paquete de estado del enlace ACK.

4. Cuando el proceso es completado, la adyacencia es formada, las bases de datos de estado del enlace son sincronizadas y el estado de vecindad es completado.

5. Los dos routers continuarán intercambiando mensajes “Hello” manteniendo su adyacencia. Cualquier LSA aprendido por un router es propagado a sus vecinos,de otra manera el enlace esta en reposo.

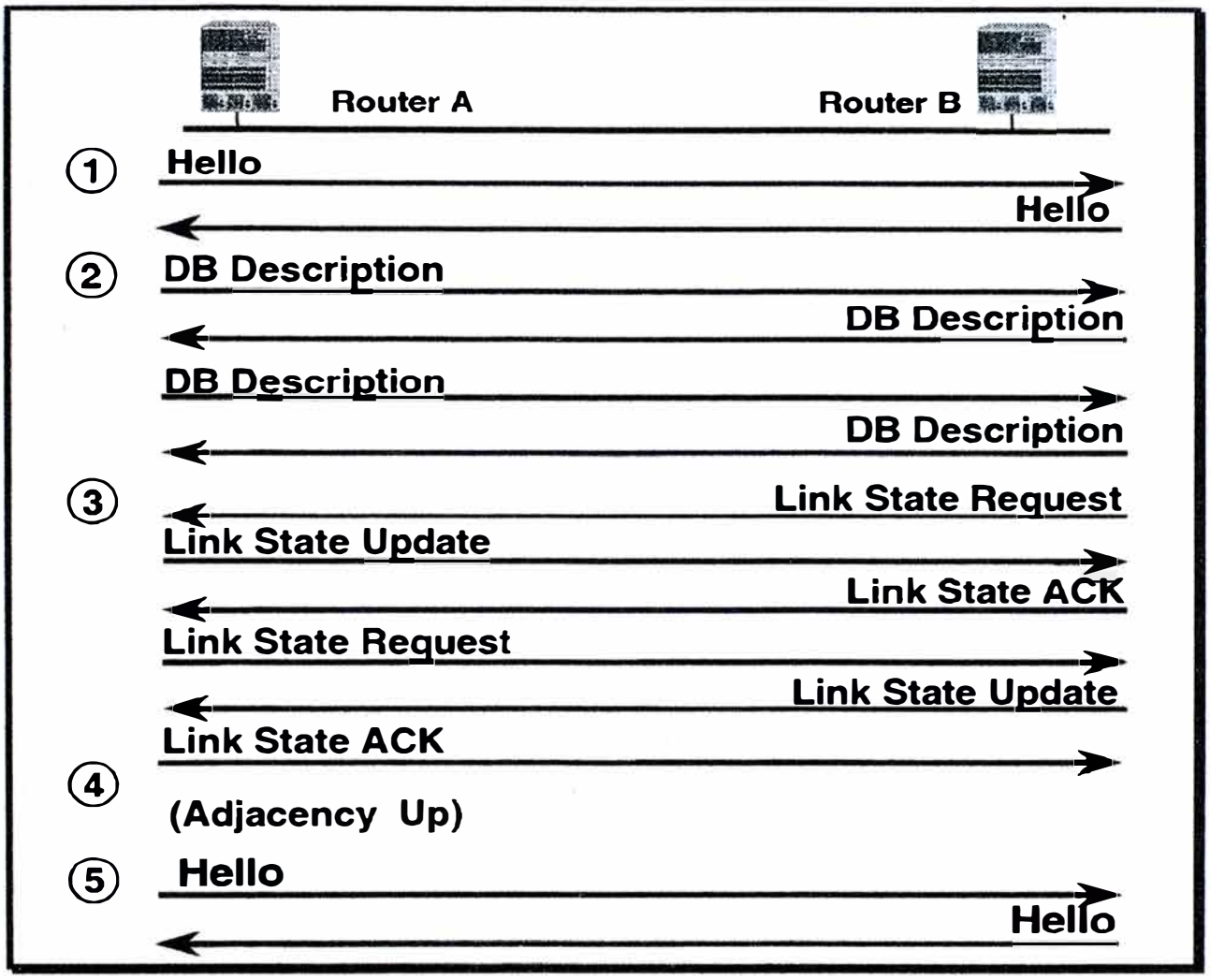


Figura 4.4.10.8 Formación de una adyacencia.

- **ESTADOS DE VECINDAD**

La figura 4.4.10.9 ilustra los estados de vecindad.

La conversación entre routers vecinos tiene definidos estados. Sobre los routers , veremos algunos de estos estados cuando veamos el archivo log o trace.. Los estados que pueden existir entre los routers vecinos son:

- **Desactivado "Down"** – Este es el estado inicial de una conversación de vecindad. No ha habido reciente información recibida desde el vecino. Aparece solo para vecinos configurados estáticamente.
  Es el estado inicial de un vecino. Los vecinos que están en estado desactivado no aparecen reflejados en la tabla de vecindad.

- **Intento "Attempt"** - Este estado solo ocurre en redes no broadcast. Este indica que ninguna información reciente ha sido recibida desde un vecino.
  En las redes NBMA se trata del estado en el que se intenta establecer la vecindad. En dichas redes, el estado de vecindad debe configurarse de forma manual. De esta manera, se enviarán saludos a todos los vecinos configurados con la opción de unidifusión para intentar establecer una relación de vecindad.
- **Init** – Un paquete "Hello" es visto desde el vecino pero la comunicación bidireccional no es establecida con el vecino.
  Este estado indica que el router ha oído recientemente un saludo procedente de su vecino (el intervalo de desactivación no ha caducado desde que se oyó el último saludo), pero aún tiene que esperar la aparición de su propio identificador de router en el paquete de saludo de su vecino (lo que implica que el vecino aún tiene que oír un saludo por parte de este router). Una vez que un router alcanza este estado con un vecino comenzará a incluir el identificador de router del vecino en sus paquetes de saludo.

- **Bidireccional "Two-Way"** – Comunicación entre los dos routers es bidireccional. Esto ocurre cuando el routerA recibe "Hello" del router B y se ve así mismo listado como un vecino.

  Es el estado en el que el router ha visto su propio identificador de router en el paquete de saludo del vecino, lo que implica que este último está recibiendo el saludo y que se ha establecido una comunicación bidireccional.

- **ExStart** – Este es el primer paso en la creación de una adyacencia. Una relación maestro o esclavo es negociada, gobernando los subsecuentes intercambio de mensajes.

  Es el estado en el que ya se han elegido dos vecinos para formar una adyacencia y están en proceso de determinar cómo transferirse los paquetes de descripción de bases de datos (es decir, los paquetes OSPF tipo 2).

- **Intercambio "Exchange"** – El router esta describiendo su LSDB completa enviando paquetes con la descripción de la base de datos al vecino. El router con el ID de router más alto será el maestro.

  Es el estado en el que los routers intercambian los paquetes de descripción de base de datos (paquetes OSPF tipo 2).

- **Carga "Loading"** – Paquetes de petición de estado del enlace son enviados al vecino preguntando por los anuncios más recientes que fueron aprendidos pero no recibidos, y actualizaciones de estado del enlace son enviadas en respuesta.

  Es el estado en que los router envían paquetes de petición de estado

del enlace (paquete OSPF tipo 3) para todos los LSA incluidos en la lista de petición de estado del enlace y reciben a cambio paquetes de actualización de estado del enlace (paquete OSPF tipo 4)

- **Completo "Full"** – Los routers vecinos son completamente adyacentes, y los LSDB son idénticos.

  Es el estado en el que los vecinos son totalmente adyacentes y deben tener copias idénticas de la base de datos del estado del enlace correspondiente al área.

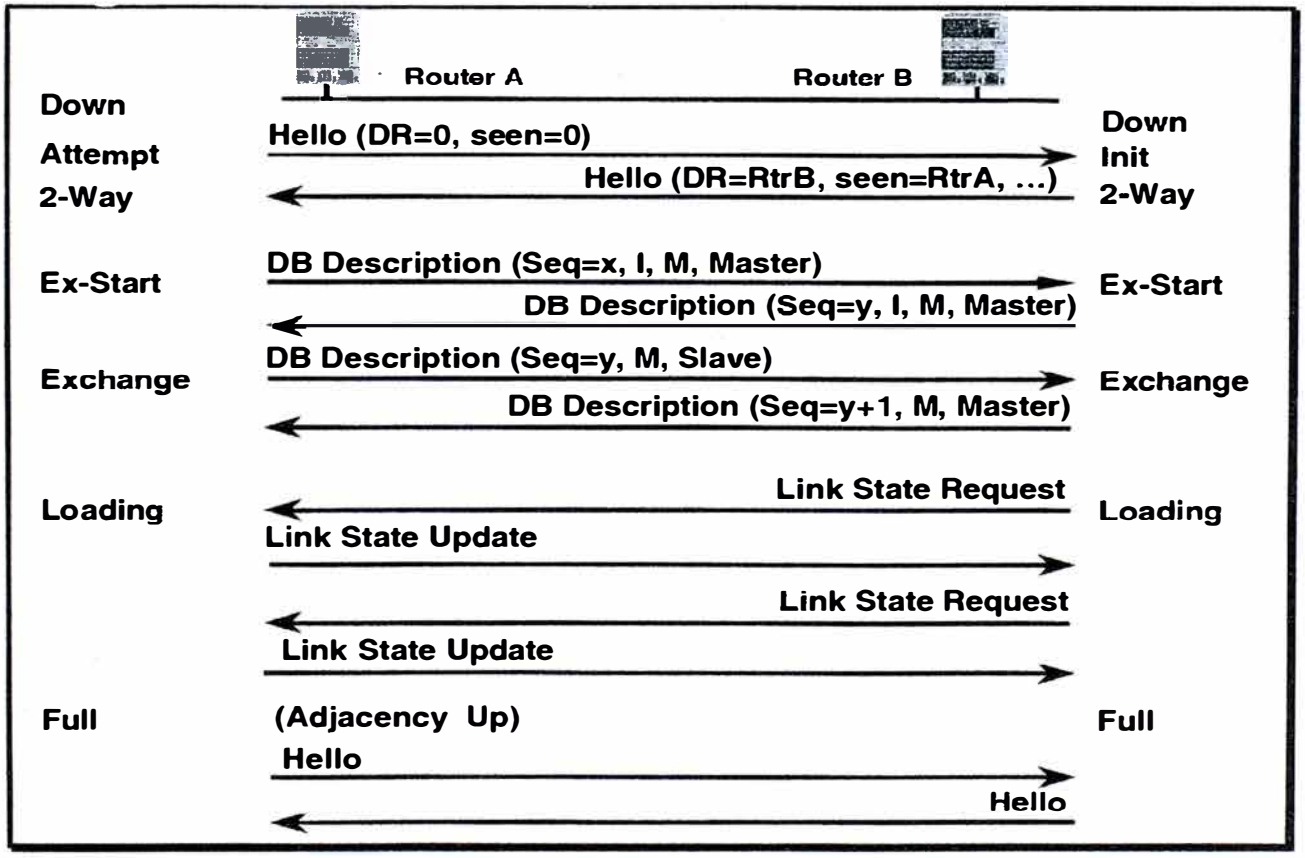


Figura 4.4.10.9 Estado de vecindad.

- **ADYACENCIAS EN UNA RED BROADCAST**

Una adyacencia es un acuerdo para intercambiar información de base de datos. Formando una adyacencia puede usar intensivo ancho de banda y intensivo recursos.

En un ambiente multiacceso tal como una red Ethernet, teniendo a todos los routers manteniendo adyacencias con todos los otros routers dentro de un dominio de broadcast requiere innecesario overhead.

En la figura 4.4.10.10, si el Router A es adyacente a los Routers B, C y D, sus LSDB son idénticos. Por consiguiente, no hay necesidad de formar adyacencia entre los routers C y D, B y D, o B y C.

Para reducir el overhead en ambientes multiacceso, un router designado (DR, "Designated router") es elegido usando información contenida en los mismos mensajes "Hello" usado para formar una adyacencia.

En el mensaje "Hello", el router con el valor más alto en el parámetro prioridad dicta que router será el DR. En el caso de igual prioridades de router, el router con el ID de router más alto alto (un parámetro global de OSPF) será el DR.

Cuando una interfase de un router es inicializada, este chequea por un DR. Si uno ya existe, el router lo difiere a él, independiente de su prioridad configurada.

El DR mantiene adyacencias con todos los routers sobre la misma red física. Este router envía actualizaciones de estado del enlace a la dirección multicast ALLSPFRouters (224.0.0.5). Esto elimina la necesidad de enviar una actualización separada a la dirección de cada router adyacente.

Los routers que no son el DR envían actualizaciones a la dirección ALLDRouters (224.0.0.6).

Un router puede ser prevenido de volverse el DR configurando el valor de su prioridad de router en 0.

Un router designado de seguridad (BDR, "Backup Designated Router") es tambien elegido en el caso que el DR falle. Todos los routers incluyendo al DR, serán adyacente con un BDR.

- **ROUTERS FORMANDO ADYACENCIAS**

  Un router intenta formar una adyacencia en las siguientes maneras:

  - En una red punto a punto, este forma una adyacencia con el router que esta en el otro extremo de la red.
  - En una red multiacceso, este forma una adyacencia con el router designado (DR "Designated Router") y con el router designado de seguridad (BDR "Backup Designated Router").

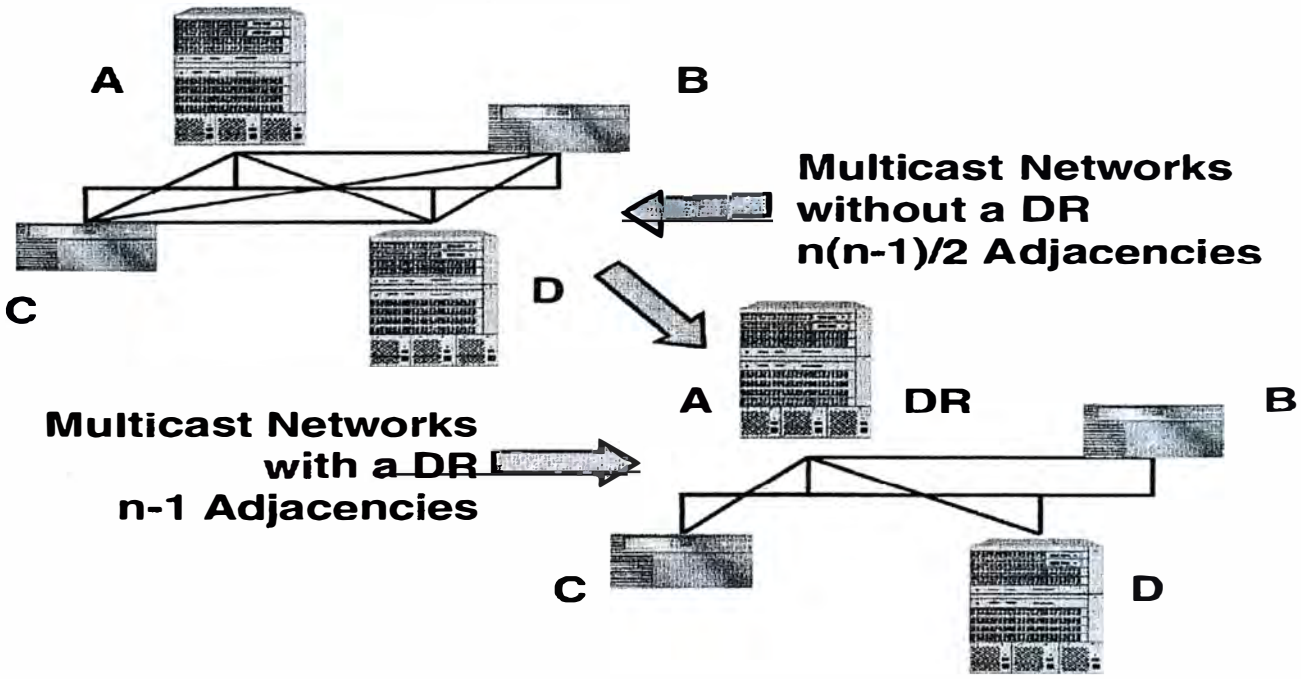


Figura 4.4.10.10 Adyacencia en una red broadcast (multiacceso).

- **PROPAGANDO EL ARRIBO DE UNA NUEVA ADYACENCIA**

Si un nuevo router OSPF viene dentro de la red, este debe formar al menos una adyacencia. La presencia de un nuevo router significa que hay nuevas redes disponibles y este debe ser propagada a través de la red. La LSDB de todos los routers OSPF deben ser actualizadas y el árbol SPF recalculada.

En la Figura 4.4.10.11,esta transición ocurre como sigue:

1. El router A inicializa y empieza a trasmitir mensajes "Hello" OSPF a través del enlace punto a punto.

   La dirección IP destino : 224.0.0.5 (AllSPFRouters)
2. Los routers B y A forman una adyacencia resultando en la sincronización de su base de datos.
3. El router B envía un paquete de actualización del estado del enlace al DR de la red multiacceso.

   La dirección IP destino : 224.0.0.6 (AllDRRouters)
4. El DR anuncia la nueva entrada a todos los routers adyacentes sobre la red broadcast.

   La dirección IP destino : 224.0.0.5 (AllSPFRouters).
5. Los routers receptores reconocen la nueva información en la actualización; cambian sus LSDBs; y fluyen la nueva información a todas sus adyacencias.

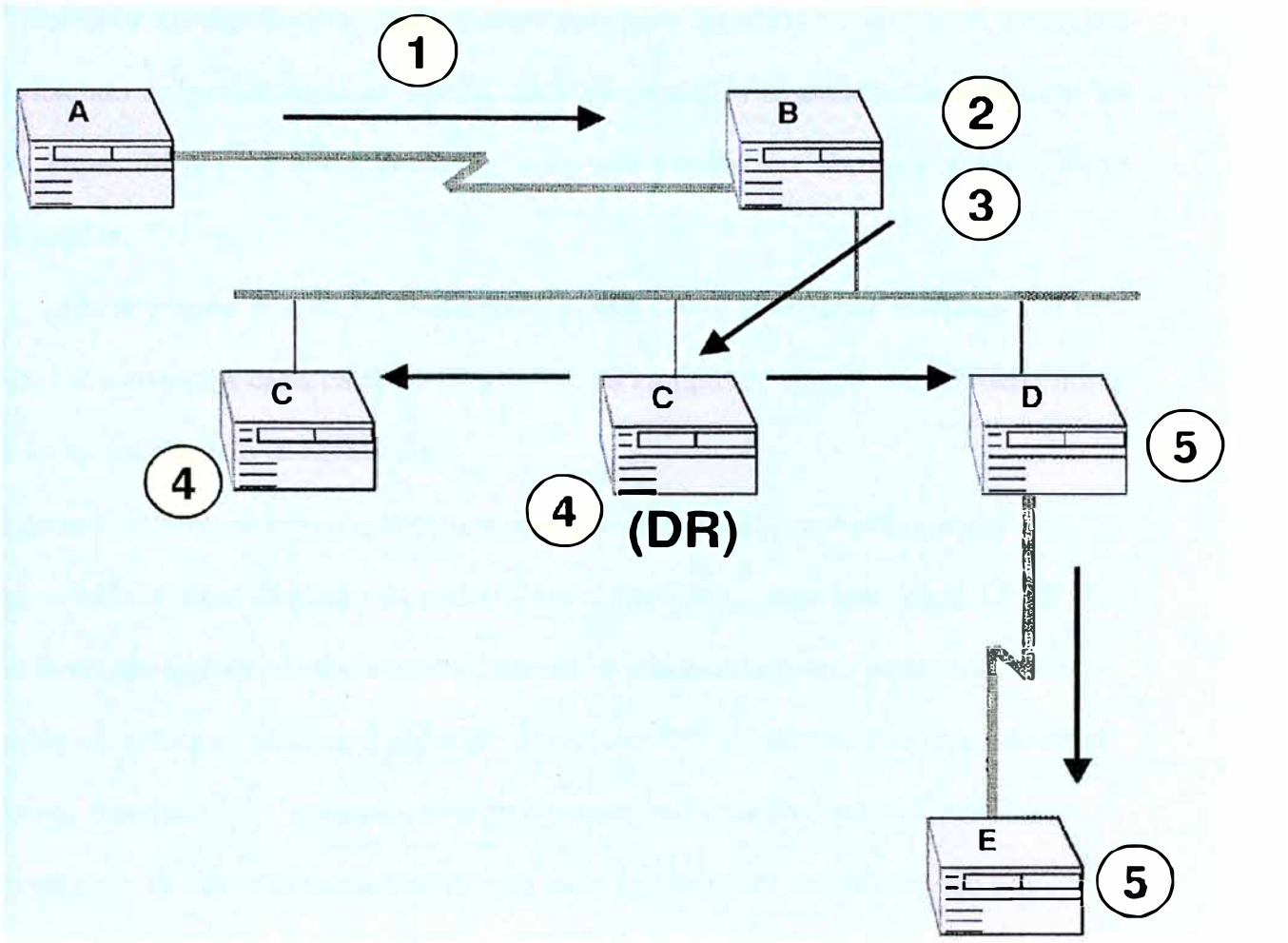


Figura 4.4.10.11 Propagando el arribo de una Nueva Adyacencia.

- **EJEMPLOS DE REDES OSPF**

En la Figura 4.4.10.12 ilustra una red OSPF simple de un área única. Todos los routers están en el área 0.0.0.0. Cada router tiene cinco redes configuradas en la subnetwork clase B, y los enlaces interswitch están usando IRPs.

El modelo de área única produce una sola LSDB describiendo el sistema autónomo completo. En redes extremadamente grandes y complejas, donde el

modelo de área única no es practico, la red puede ser subdividida en áreas. En una red diseñada correctamente, cada router entonces mantiene una LSDB completa describiendo su propia área en detalle, más los anuncios resumidos describiendo las otras áreas. Múltiples áreas permiten a la red escalar sin abrumar a los routers individuales.

En la Figura 4.4.10.13 se ilustra una red OSPF con áreas múltiples. El área 0.0.0.0 se conecta a cada campus remoto. Cada campus remoto a su vez tiene uno o más áreas conectando al backbone.

Las áreas OSPF constituyen una mejora que permite que el protocolo admita un número virtualmente ilimitado de routers. En el caso de un área individual, OSPF debe llevar un registro de cada enlace individual sobre cada router para toda la red. Cuando un enlace se modifica, provoca un cálculo SPF en cada router presente en el entorno. Aunque OSPF consume muy pocos recursos cuando una red es estable y convergente, debido a la necesidad de que cada router OSPF sea alcanzado por completo y que contenga información topológica para cada enlace presente en el área en un entorno de grandes proporciones, los cambios OSPF pueden provocar que todos los routers consuman grandes cantidades de recursos de CPU y de memoria. Por esta razón es posible dividir OSPF en áreas múltiples reduciendo el número de enlaces que cada router OSPF requiere (exceptuando los ABR) sólo a los enlaces situados dentro de su área específica.

La tabla 4.4.10.4 proporciona las mejores prácticas para establecer los tamaños de red OSPF:

	Mínimo recomendado	Máximo recomendado
Routers por AS	20	1000
Areas por AS	1	60
Routers por área	20	350

Tabla 4.4.10.4 : Las mejores prácticas para las áreas OSPF y los tamaños de AS

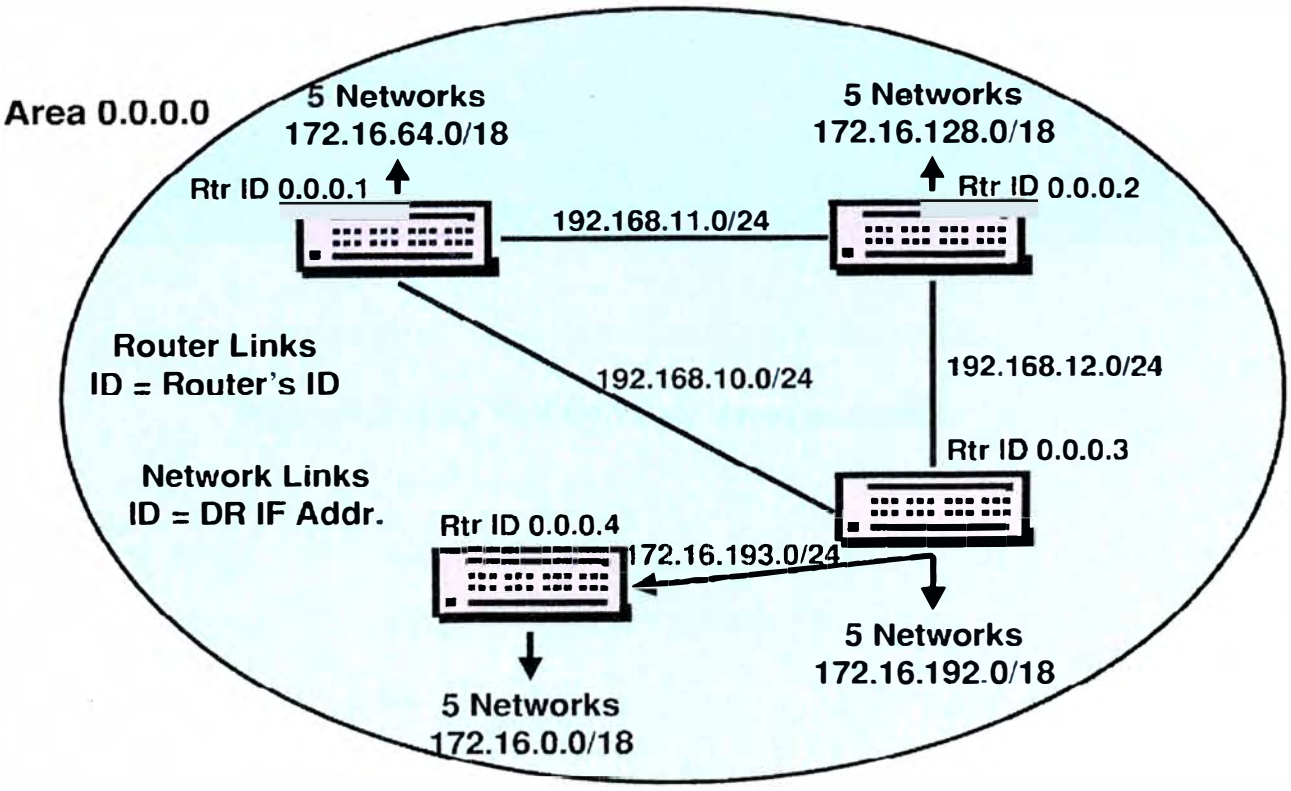


Figura 4.4.10.12 Red OSPF de una única área.

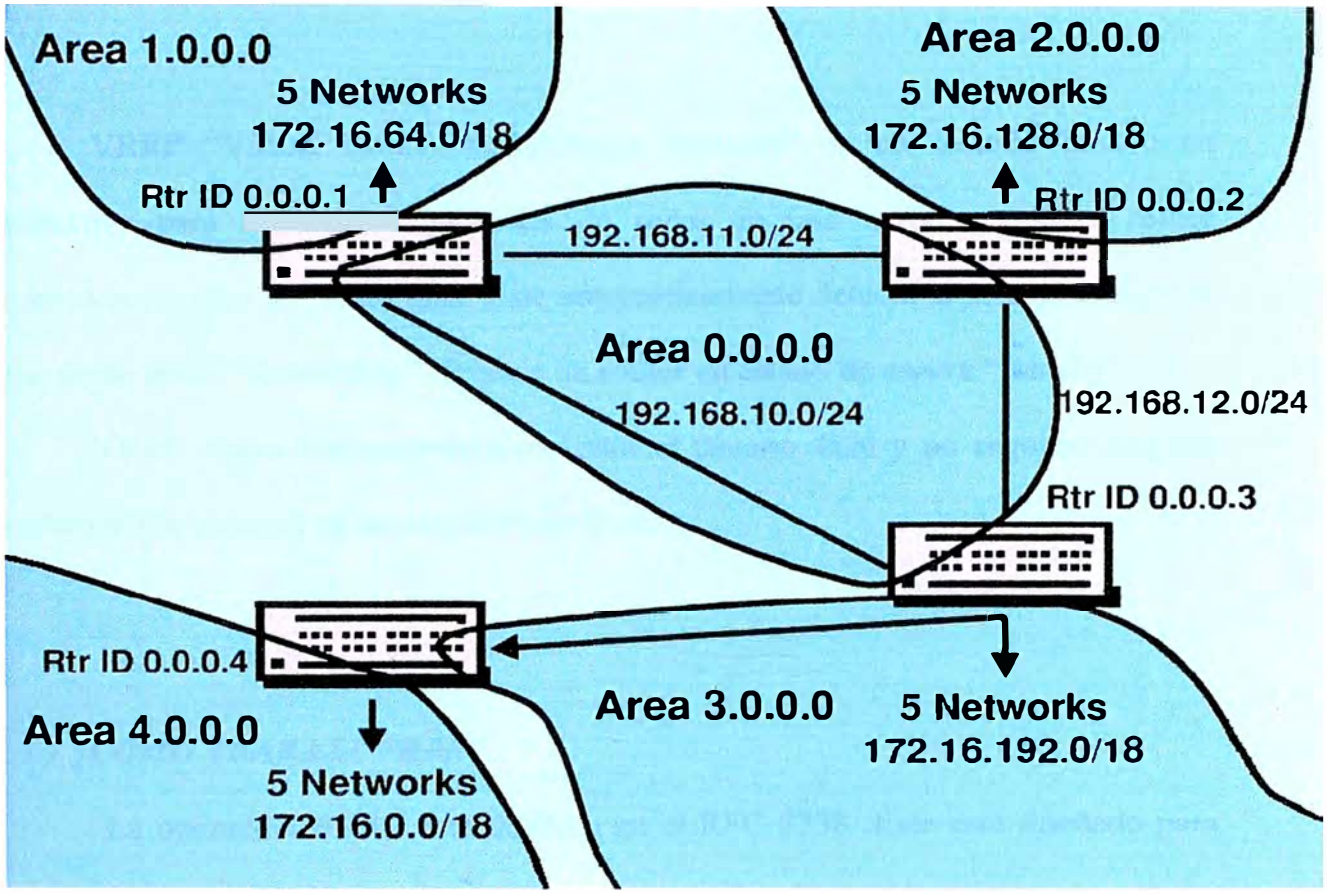


Figura 4.4.10.13 Red OSPF de áreas múltiples.

4.5 EL PROTOCOLO VRRP "VIRTUAL ROUTER REDUNDANCY PROTOCOL"

VRRP "Virtual Router Redundancy Protocol" es un método basado en estándares para mantener conexiones de redes en una LAN cuando el router conectado al resto de la red falla. Este automáticamente detecta la falla y reasigna la función de envío "forwarding" IP hacia un router en estado de espera "standby".

VRRP opera transparentemente para el usuario final y no requiere ninguna configuración especial en los dispositivos host.

4.5.1 ***¿CÓMO TRABAJA VRRP?***

La operación VRRP esta definida en el RFC 2338 .Este esta diseñado para eliminar el único punto de falla que puede ocurrir cuando el router gateway por default configurado estáticamente para una estación final es perdida. Este usa el concepto de una dirección IP virtual compartida entre dos o más routers conectando una subred a la red corporativa. Con la dirección IP virtual , como el gateway por default en los hosts finales, VRRP provee redundancia de gateway por default dinámica en el caso de una falla (ver figura 4.5.1.1).

El router VRRP controlando las direcciones IP asociado con un router virtual es llamado el Master y envía "fowards" paquetes a estas direcciones IP. El proceso de elección provee un "fail-over" dinámico de envío responsable si el master se pone no disponible.

En la Figura 4.5.1.2, los primeros tres hosts tienen instalado una ruta por default hacia la dirección IP1 del router virtual y los otros tres host tienen instalados una ruta por default hacia la dirección IP2 del router virtual. Esto no solo tiene el efecto de compartir la carga del tráfico saliente, sino también provee redundancia completa.. Si cualquiera de las interfase de los routers falla, el otro router asume la responsabilidad de ambas direcciones. En efecto los dos routers actúan como backups uno del otro.

- **¿QUÉ PROBLEMAS RESUELVE VRRP?**

En la mayoría de las redes IP, las estaciones finales están estáticamente configurados con una única dirección de router conocido como un gateway por default. Esto es donde los hosts envían todo el tráfico destinados a subredes diferentes de la suya. Si el gatway se cae, todo el tráfico es desechado. Corriendo un protocolo de enrutamiento dinámico tal como RIP o OSPF es una solución potencial, pero esto requiere esfuerzo administrativo extra para configurar y mantener sobre cada estación final.

Con VRRP, los usuarios pueden tener redundancia, aun así tengan una única dirección de gateway estática sobre cada host.

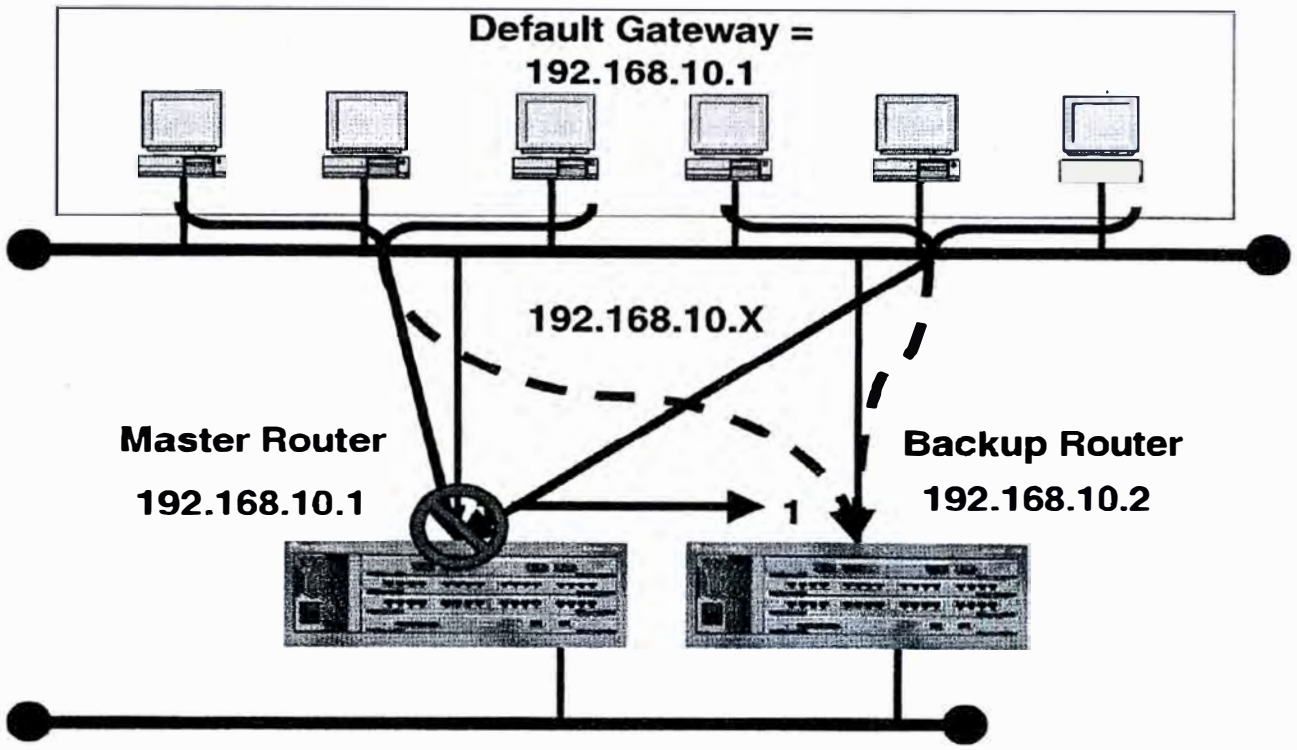


Figura 4.5.1.1 VRRP provee redundancia dinámica de gateway por default

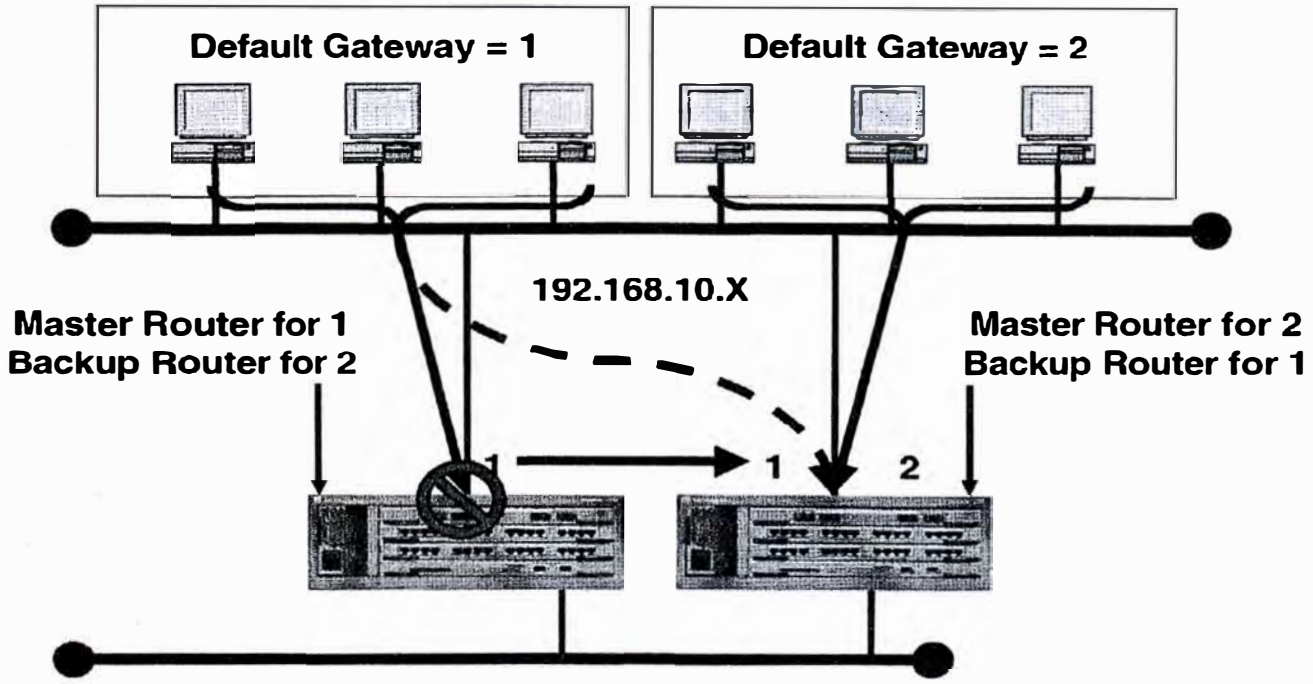


Figura 4.5.1.2 Configuración de VRRP donde provee compartición de la carga del tráfico saliente y redundancia completa

4.5.2 TÉRMINOS FUNDAMENTALES DE VRRP

Para discutir VRRP, un número de términos deben ser definidos.

- **Router VRRP**

El router VRRP es un router en el que esta corriendo el protocolo VRRP ("Virtual Router Redundancy Protocol"). VRRP puede participar en uno o más routers virtuales.

- **Router Virtual**

Un router virtual es un objeto abstracto manejado por VRRP que actúa como el siguiente salto ("next hop") o router por default para los host sobre una LAN compartida. los usuarios pueden tener redundancia, aun así tengan una única dirección de gateway estática sobre cada host. Piense que este actúa como un router fantasma "ghost router" consistente de un identificador de router virtual y un conjunto de direcciones IP asociadas a través de una LAN común. Un router VRRP puede respaldar a uno o más routers virtuales.

- **El dueño de la dirección IP ("IP Address Owner")**

El dueño de la dirección IP es el router virtual que tiene la dirección IP o las direcciones IP del router virtual como dirección o direcciones de interfase reales. Este es el router que, responde a los paquetes direccionados a una de estas direcciones IP para paquetes SNMP ("Simple Network Management Protocol") y conexiones TCP ("Transmisión Control Protocol"), etc.

- **Dirección IP principal ("Primary IP address")**

La dirección IP principal es una dirección IP seleccionada del conjunto de direcciones de interfase reales. Un posible algoritmo de selección esta siempre seleccionando la primera dirección. Los anuncios VRRP son siempre enviados usando la dirección IP principal como la fuente del paquete IP.

- **Router virtual maestro ("Virtual Router Master")**

El router virtual maestro es el router VRRP que esta asumiendo la responsabilidad de envío (forwarding) de paquetes enviados a la dirección o direcciones asociadas con el router virtual y respondiendo peticiones ARP (Address Resolution Protocol) por estas direcciones IP.

- **Router virtual de respaldo ("Virtual Router Backup")**

Un router virtual de respaldo es un conjunto de routers VRRP disponible para asumir la responsabilidad de envío de un router virtual, cuando el actual router virtual maestro falle.

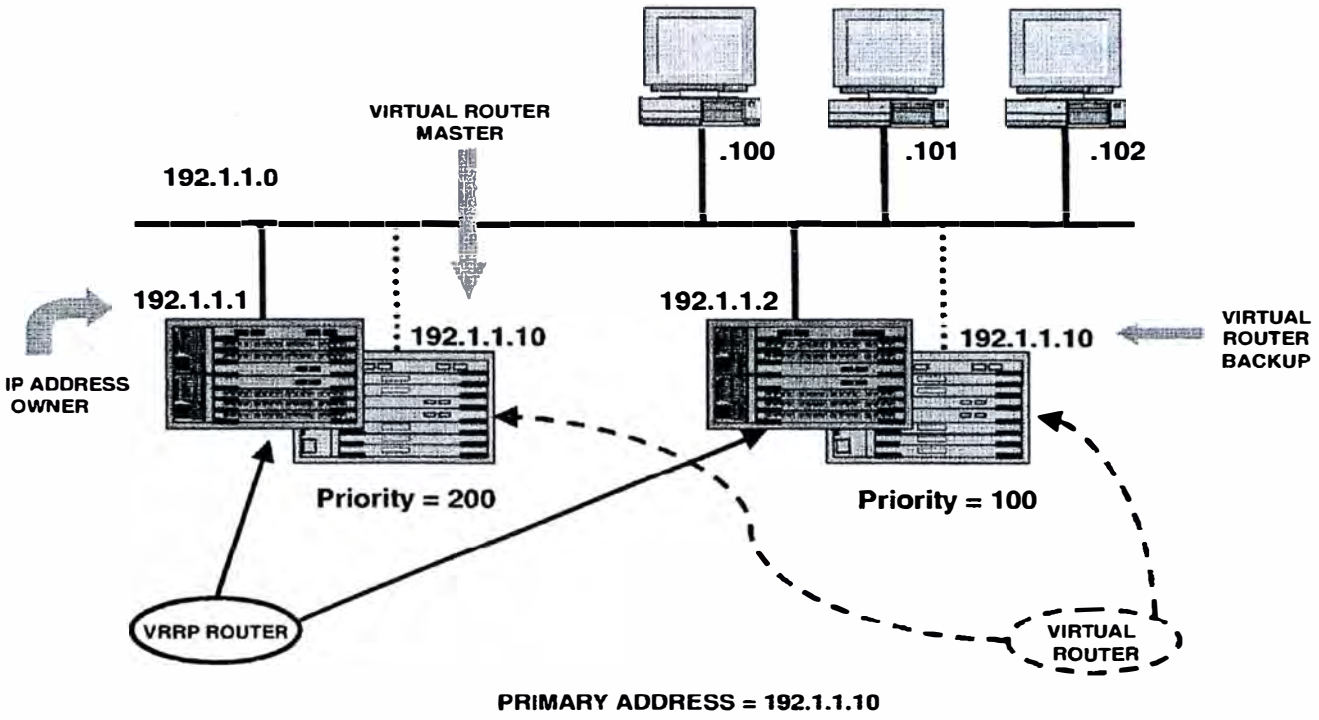


Figura 4.5.2 Definiciones de VRRP

4.5.3 PARAMETROS DE VRRP

- **Identificador de router virtual (VRID, "Virtual Router Identifier")**

El VRID es un ítem configurado en el rango de 1-255 (decimal). No hay default.

- **Prioridad ("Priority")**

El valor de la prioridad es usado por el router VRRP para la elección del maestro entre los routers virtuales.El valor de 255(decimal) es reservado para el router que es dueño de las direcciones IP asociadas con el router virtual. El valor de 0

(cero) es reservado para el router maestro para indicar que se esta liberando de la responsabilidad de router virtual. El rango de 1-254 (decimal) esta disponible para routers VRRP respaldando al router virtual. El valor por default es 100.

- **Intervalo de anuncios ("Advertisement_Interval")**

Es el intervalo de tiempo entre ANUNCIOS (en segundos). El default es 1 segundo.

- **Skew time**

Intervalo de tiempo en segundos para saber que el maestro esta caído "Master Down Interval" Este es calculado como:

((256 – Prioridad))/256)

- **Intervalo de caída del maestro ("Master_Down_Interval")**

Intervalo de tiempo de respaldo para declarar que el Maestro esta caído (en segundos) Este es calculado como

(3 * Advertisement_Interval) + Skew_time

- **Preempt_Mode**

Controla si un router de respaldo con prioridad más alta desplaza a un maestro con prioridad más baja. Los valores son True (para permitir) y False (para no permitir) el control de la apropiación al menos que el router sea dueño de las direcciones IP. El default es True.

- **Master_Down_Timer**

Un reloj o temporizador que se activa cuando un ANUNCIO ha sido escuchado por el Intervalo de caída del maestro ("Master_Down_Interval").

- **Adver_Timer**

Un reloj que se activa para disparar el envío de un ANUNCIO basado en el Intervalo de anuncio ("Advertisement_Interval").

- **Virtual Router Identifier, Advertisement Level, Master_Down_Interval, Adver_Timer**

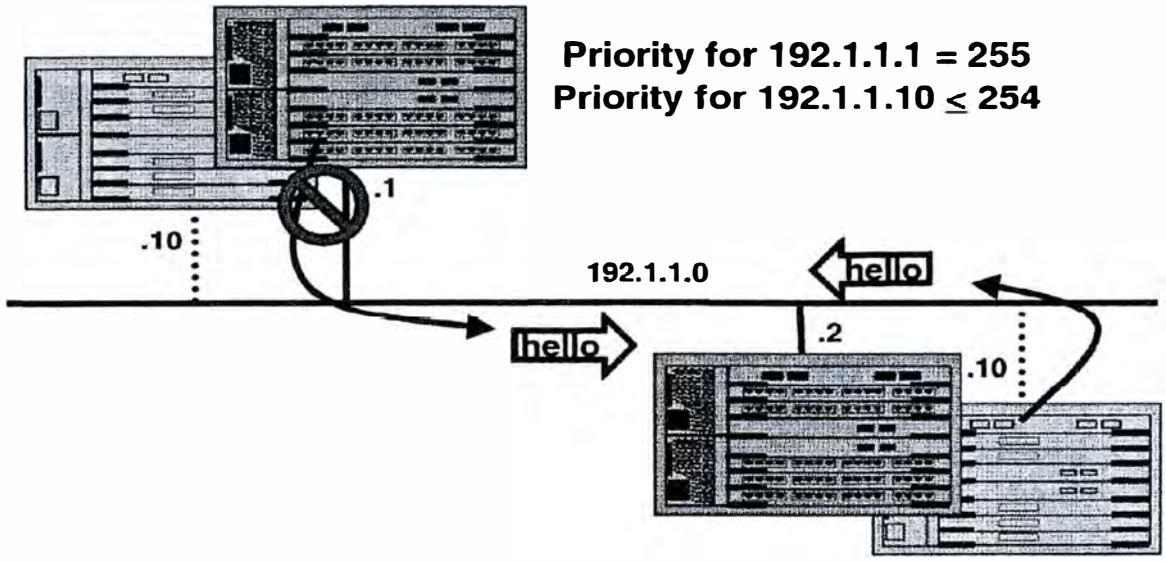


Figura 4.5.3 Parámetros de VRRP

4.5.4 LA MAQUINA DE ESTADOS DE VRRP

- **COMO TRABAJA VRRP**

VRRP especifica un protocolo de elección que dinámicamente asigna responsabilidad a un router virtual de unos de los routers VRRP en una red de área local (LAN). El router VRRP controlando la dirección o las direcciones IP asociada con el router virtual es llamado el Maestro, y envía (fowards) paquetes enviados a estas direcciones IP. El proceso de elección provee fail-over dinámico en la responsabilidad de envío si el master se pone no disponible. Cualquiera de las direcciones IP del router virtual en una LAN puede ser entonces usadas como el router del primer salto "first-hop" por default por las estaciones finales.

Cuando un router VRRP es inicializado, si este es el dueño de la dirección IP, su prioridad es 255 y envía un anuncio VRRP. El router VRRP también difunde una solicitud ARP conteniendo la dirección MAC del router virtual por cada dirección IP asociada con el router virtual. El router virtual VRRP luego transita o pasa al estado de controlación.

En el estado de controlación , el router VRRP funciona como el router de envío (forwarding) de las direcciones IP asociadas con el router virtual. Este responde a solicitudes ARP por estas direcciones IP, envía paquetes con una dirección MAC destino igual a la dirección MAC del router virtual y acepta solo paquetes direccionados a las direcciones IP asociadas con el router virtual si este es el dueño de la dirección IP. Si la prioridad no es 255, el router transita o pasa al estado de respaldo para asegurar que todos los switches capa 2en el camino de caída reaprendan el nuevo origen de las direcciones MAC VRRP.

En el estado de respaldo (backup), un router VRRP monitorea la disponibilidad y estado del router principal o primario. Este no responde a solicitudes ARP y debe desechar paquetes con una dirección MAC igual al a dirección MAC del router virtual. Este no acepta paquetes direccionados a direcciones IP asociada con el router virtual. Si una caída (shutdown) ocurre, este transita del estado de respaldo al estado de inicialización. Si el router principal cae,el router de respaldo envía el anuncio VRRP y solicitud ARP y pasa al estado de controlación.

Si un reloj de anuncios se dispara, el router envía un anuncio. Si un anuncio es recibido con una prioridad 0, el router envía un anuncio. Si la prioridad es mayor que la prioridad local o si es igual a la prioridad local y la dirección IP principal del emisor es mayor que la dirección IP principal local, el router transita al estado de respaldo (backup). De otra manera, este desecha el anuncio. Si una caída (shutdown) ocurre, el router principal envía un anuncio VRRP con prioridad de 0 y transita al estado de inicialización.

- **Estado INIT**

  El propósito de este estado es esperar por evento de arranque "startup".

  Si un evento de "startup" es recibido, entonces:

  Sí la prioridad =255 (por ejemplo el router dueño de las direcciones asociadas con el router virtual)

  - Envía un ANUNCIO "ADVERTISEMENT"
  - Difunde "broadcast" una petición ARP gratuita conteniendo la dirección MAC del router virtual por cada dirección IP asociada con el router virtual.

- Set el parámetro Adver-Timer a Advertisement_Interval (default = 1 segundo)
- Transición al estado MAESTRO "MASTER"

Si no "Else"

- Set el Master_Down_Timer a Master_Down_Interval.
- Transición al estado de RESPALDO "BACKUP"
-

Un reloj que se activa para disparar el envío de un ANUNCIO basado en el Intervalo de anuncio ("Advertisement_Interval").

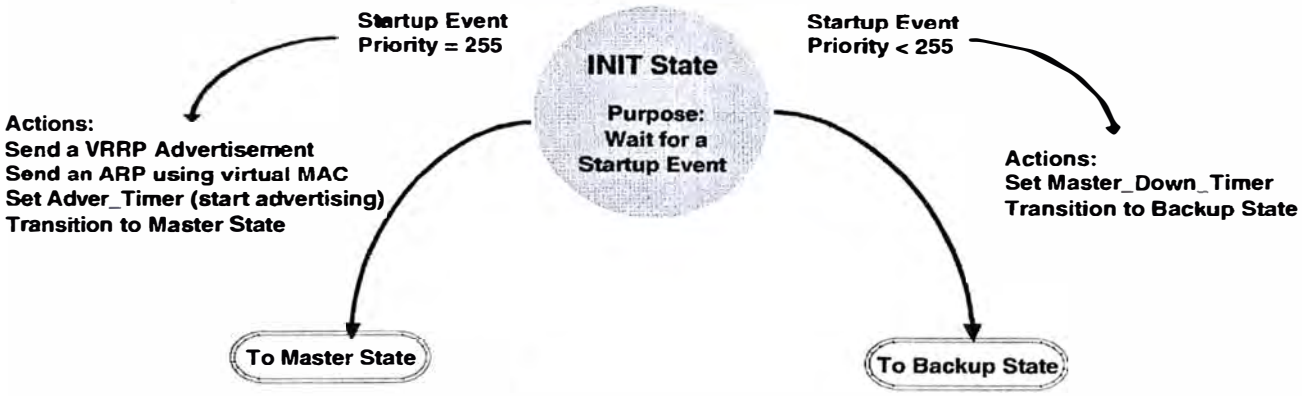


Figura 4.5.4.1 Estado Init

- **Estado de Respaldo ("Backup State") de VRRP**

El propósito del estado de respaldo es monitorear la disponibilidad y estado del router maestro.

Mientras en este estado, un router VRRP:

- NO DEBE responder a solicitudes ARP por la dirección o direcciones IP asociada con el router virtual.
- DEBE desechar paquetes con una dirección MAC destino de la capa de enlace igual a la dirección MAC del router virtual.
- NO DEBE aceptar paquetes direccionados a la dirección o direcciones IP asociada con el router virtual.

Si un evento de caída ("shutdown") es recibido, entonces:

- Cancela el "Master Down Timer".
- Transita al estado de Inicialización.

Si el "Master_Down_Timer" se activa, entonces:

- Envía un ANUNCIO "ADVERTISEMENT".
- Difunde (Broadcast) una solicitud ARP gratuita conteniendo la dirección MAC del router virtual por cada dirección IP asociada con el router virtual.
- Set el Adver_Timer a Advertisement_Interval.
- Transita al estado de MAESTRO "MASTER".

Si un ANUNCIO "ADVERTISEMENT" es recibido, entonces:

- Si la prioridad en el ANUNCIO es cero, entonces:

  - Set el "Master_Down_Timer" a "Skew Time"

Sino :

- Sí el "Preempt :Mode" es falso, o si la prioridad en el ANUNCIO es mayor o igual a la prioridad local , entonces:

  -Reset el Master Down Timer a Master Down Interval.

Sino :

- Desecha el ANUNCIO.

Mientras que en el estado de respaldo el router básicamente esta en un estado de espera. Este espera y escucha por anuncios desde el router maestro. Si, sin embargo, Este detiene la recepción de estos anuncios, entonces el router transitará al estado de Anuncio. En este momento el router podría ser el maestro o ser reemplazado por un router con mayor prioridad.

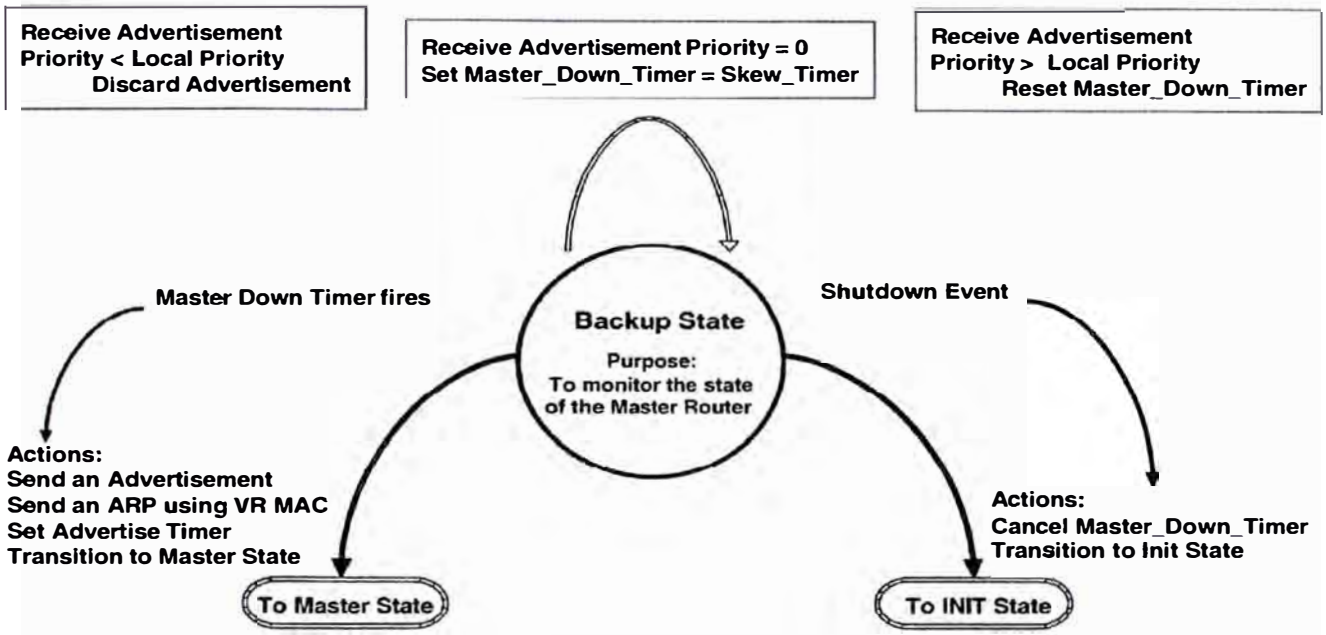


Figura 4.5.4.2 Estado de respaldo de VRRP

- **Estado Maestro ("Master") de VRRP**

Mientras en el estado Maestro el router funciona como el router de envío para las direcciones IP asociadas con el router virtual.

Mientras en este estado, un router VRRP:

- DEBE responder a solicitudes ARP por la dirección o direcciones IP asociada con el router virtual.
- DEBE enviar paquetes con una dirección MAC destino de la capa de enlace igual a la dirección MAC del router virtual.
- NO DEBE aceptar paquetes direccionados a la dirección o direcciones IP asociada con el router virtual si este no es el dueño de la dirección IP.

- DEBE aceptar paquetes direccionados a la dirección o direcciones IP asociada con el router virtual si este es el dueño de la dirección IP.

Si un evento de caída ("shutdown") es recibido, entonces:

- Cancela el "Adver Timer".
- Envía un ANUNCIO con prioridad = 0.
- Transita al estado de Inicialización.

Si el "Adver_Timer" se activa, entonces:

- Envía un ANUNCIO "ADVERTISEMENT".
- Reset el "Adver Timer" a "Advertisement Interval".

Si un ANUNCIO "ADVERTISEMENT" es recibido, entonces:

Si la prioridad en el ANUNCIO es cero, entonces:

- Envía un ANUNCIO "ADVERTISEMENT".
- Reset el Adver Timer a Advertisement Interval.

Sino :

Si la prioridad en el ANUNCIO es mayor que la prioridad local, o si la prioridad en el ANUNCIO es igual a la prioridad local y la dirección IP principal del emisor es mayor que la dirección IP principal local, entonces:

- Cancela el Adver_Timer.
- Set el Master_Down_Timer a Master _Down_Interval.
- Transita al estado de respaldo.

Sino :

- Desecha el ANUNCIO.

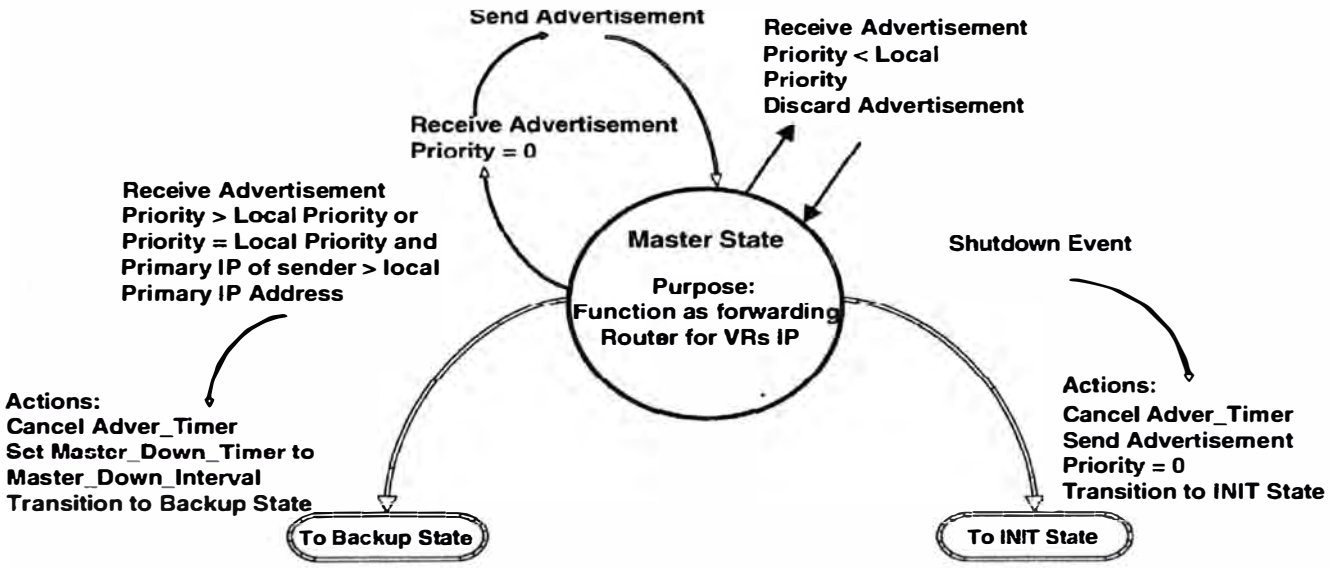


Figura 4.5.4.3 Estado Maestro de VRRP

4.5.5 ANUNCIO VRRP ("VRRP ADVERTISEMENT")

- **CONSTRUCCIÓN DEL PAQUETE DE ANUNCIO ("ADVERTISEMENT PACKET CONSTRUCTION")**

Los anuncios VRRP son construidos en un data-frame IP. La figura 4.5.5.1 ilustra la construcción de un anuncio VRRP. Lo siguiente detalla los valores requeridos para los campos en la cabecera IP y los anuncios VRRP.

- **Cabecera de Enlace de Datos ("Datalink Header")**
  - **Dirección MAC del Router Virtual**

    La dirección MAC de la interfase del router virtual es

    00-00-5E-00-01-<vrid>

- **Cabecera IP ("IP Header")**
  - **Dirección Fuente**

    La dirección IP principal desde donde los paquetes están siendo enviados.
  - **Dirección Destino**

    La dirección IP multicast asignada por IANA ("Internet Assigned Numbers Authority) para VRRP es: 224.0.0.18.
  - **TTL**

    El tiempo de vida (TTL "Time to Live") Debe ser colocado en 255.

- **Protocolo**

  El número de protocolo IP asignado por IANA para VRRP es 112 (en decimal).

- **Descripción de los campos de VRRP**

  - **Versión**

    La versión del protocolo VRRP de este paquete; la actual versión es dos.

  - **Tipo**

    El campo tipo especifica el tipo de este paquete VRRP. El único tipo de paquete definido en esta versión del protocolo es 1, ANUNCIO "ADVERTISEMENT".

  - **ID del Router Virtual (VRID "Virtual Router ID")**

    El campo VRID identifica al router virtual en este paquete reportando el estado.

  - **Prioridad**

    El campo prioridad especifica la prioridad del router VRRP de envío para el router virtual. A valores más alto mayor prioridad. El valor de la prioridad para el router VRRP que es dueño de las direcciones IP asociada con el router virtual DEBE ser 255 (en decimal). Routers VRRP respaldando a un router virtual DEBEN usar valores de prioridad entre 1-254 (en decimal). El valor de la prioridad por default

para routers VRRP respaldando a un router virtual es 100 (en decimal).

El valor cero (0) de la prioridad tiene especial significado, indicando que el Maestro actual ha detenido su participación en VRRP. Esto es usado para disparar los routers de respaldo para que transiten rápidamente al estado Master sin tener que esperar por tiempo de caducidad "timeout" del Maestro actual.

- **Count IP Addrs**

  El número de direcciones IP contenidas en este anuncio VRRP.

- **Tipo de autentificación**

  El campo tipo de autentificación identifica el método de autentificación que esta siendo utilizado. El tipo de autentificación es único sobre una interfase básica. Los métodos de autentificación actualmente definidos son:

  - 0 – No autentificación
  - 1 – Password en texto simple
  - 2 – Cabecera de autentificación IP

- **Intervalo de anuncios (Adver_Int, "Advertisement Interval")**

  Este campo displaya el intervalo de tiempo entre anuncios VRRP.

- **Checksum**

  El campo checksum es usado para detectar la corrupción de la data en los mensajes VRRP.

- **Dirección(es) IP**

  Este campo displaya una o más direcciones IP que son asociadas con el router IP. El número de direcciones incluidas es especificada en el campo "Count IP Addrs". Estos campos son usados para resolver problemas de routers mal configurados.

- **Autentificación de la Data**

  La cadena "string" de autentificación es actualmente solo usada para autentificación de texto simple, hasta 8 caracteres de texto llano.

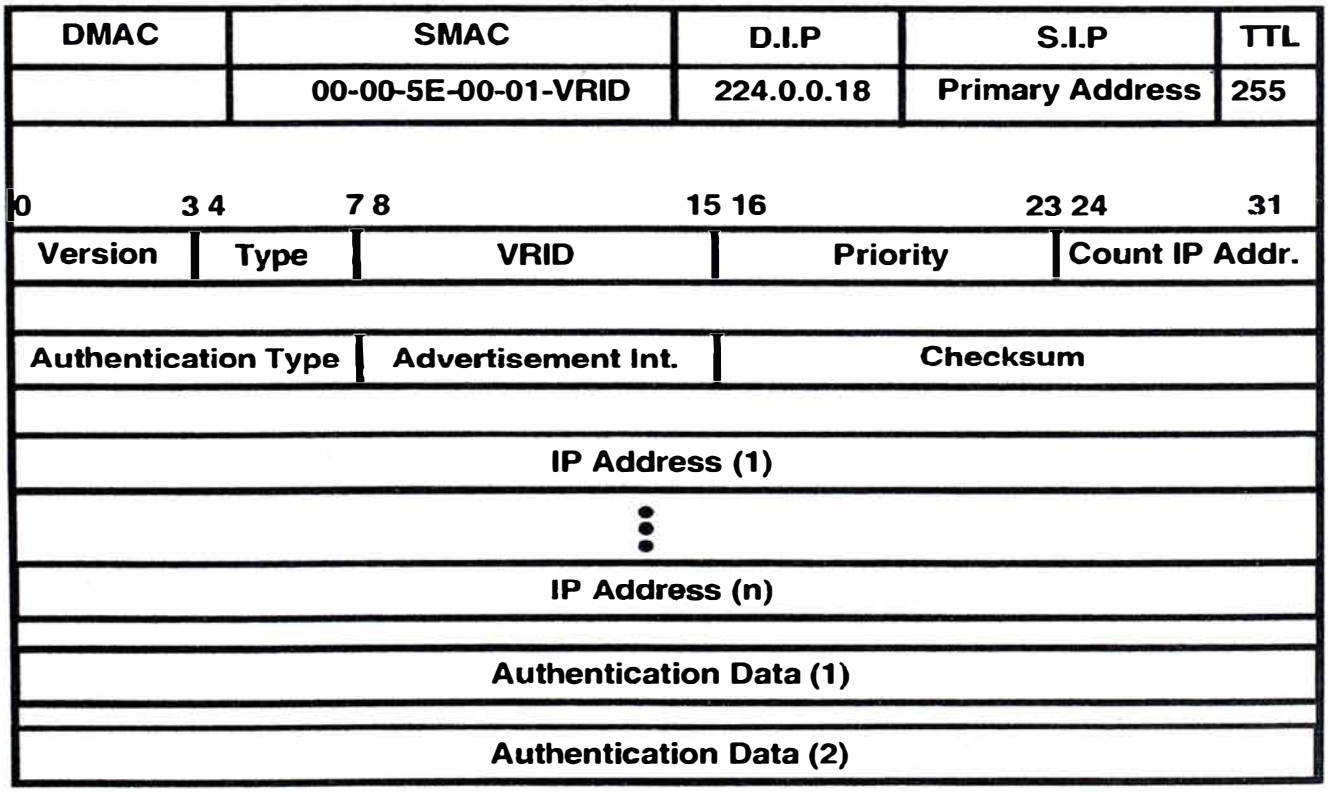


Figura 4.5.5.1 Anuncio VRRP

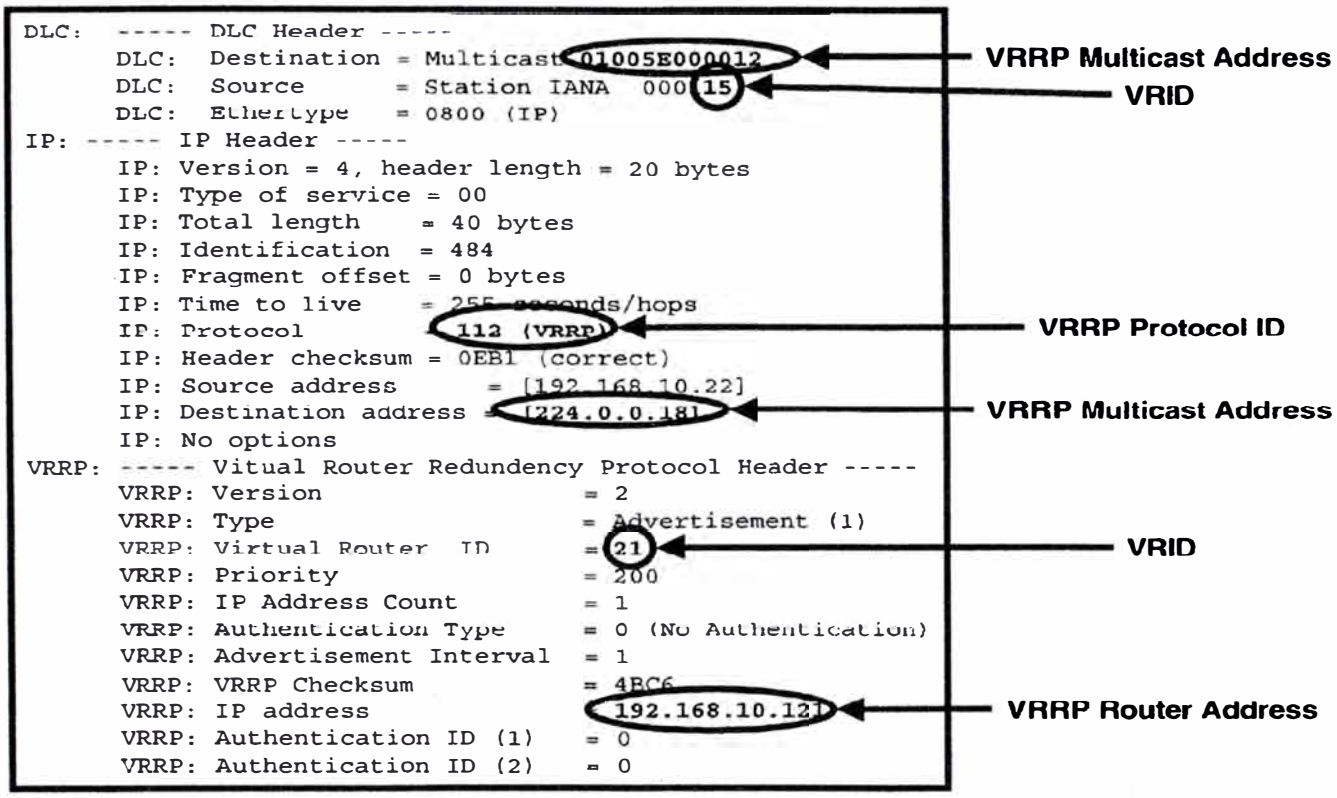


Figura 4.5.5.2 Ejemplo de Anuncio VRRP

CAPÍTULO V

SOLUCIÓN PROPUESTA E IMPLEMENTADA PARA LA RED LAN DE LA SEDE TECNOLÓGICA

En la figura 5 se muestra una visión general de la red corporativa de la empresa y las dos redes LANs que se implementaron para sus sedes principales (Tecnológica y Administrativa). Nosotros nos enfocamos en el presente informe solo en el diseño e implementación de dichas redes LANs y su integración a la red corporativa existente.

Las LANs planteadas bajo un esquema de redes de alto desempeño disponibilidad y escalabilidad, están basadas en tecnología Gigabit Ethernet y en conceptos como VLANs para dar flexibilidad y optimizar el tráfico de las redes, el enrutamiento de las VLANs mediante el protocolo OSPF (que es el protocolo corriendo en toda la red corporativa), la implementación del estándar 802.1q para extender las VLANs entre los switches, la aplicación del protocolo de redundancia de nivel 3 como VRRP, la implementación de enlaces redundantes entre los switches (MLT). Para la integración de estas redes LANs con la red corporativa existente se trato en lo posible usar protocolos estándares para así lograr la conectividad y la compatibilidad entre las diferentes marcas (Cisco/Nortel Networks) de dispositivos que conforman la red corporativa y obtener una red con la máxima efectividad y facilidad de uso.

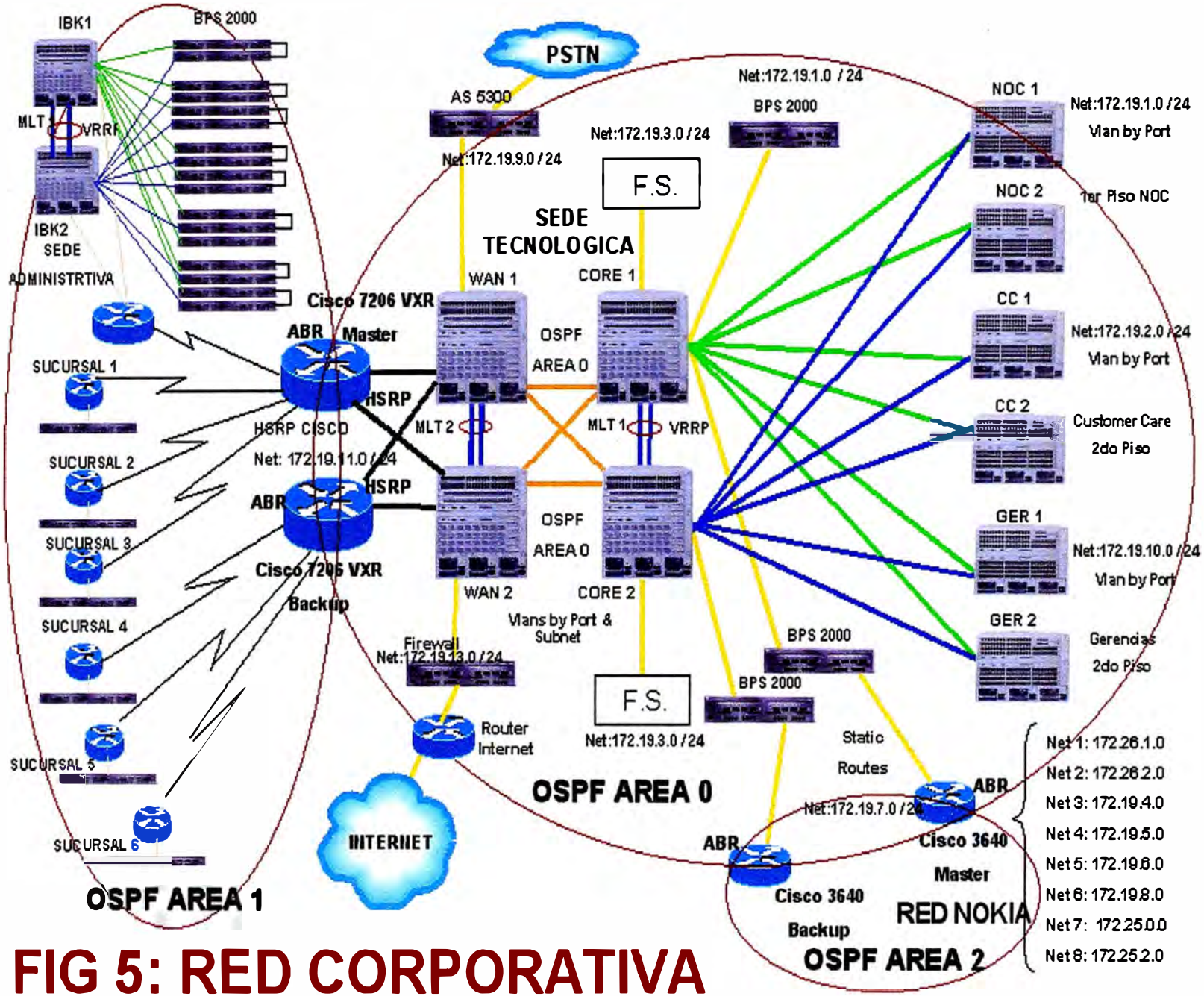


FIG 5: RED CORPORATIVA

5.1. SELECCIÓN DE EQUIPOS DE COMUNICACIONES

La solución implementada para la red LAN de la Sede Tecnológica fue una red Gigabit Ethernet con Equipos Nortel Networks, la misma que reemplazó a los Equipos Alcatel.

La solución LAN propuesta e implementada basada en los switches passport 8600 y passport 8100 se compone de equipos CORE L3 Gigabit routing switches y equipos de BORDE L2 Gigabit switch y que dan servicios de enrutamiento (solo los switches Passport 8600 L3) y conmutación "switching" con administración de políticas.

❑ EL SWITCH PASSPORT 8600

El Switch Routing Passport 8600 –ver fig. 5.1.1- es un switch multicapa, cuya funcionalidad está orientada a aplicaciones de misión crítica y fundamentalmente para grandes capacidades de conmutación y enrutamiento, alta disponibilidad, crecimiento y calidad de servicio (QoS) que permiten la integración de los servicios de la institución

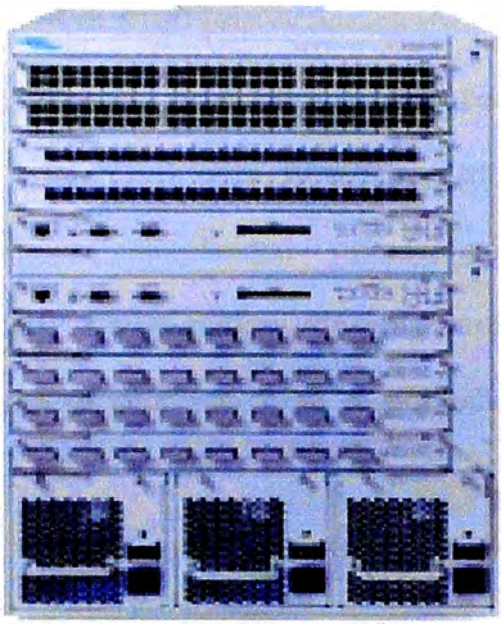


Figura 5.1.1. El Passport 8600 Routing Switch. Nortel Networks entrega integración de la tecnología para el borde de la LAN, el Backbone de la LAN Backbone y el borde de la MAN, proporcionando una verdadera solución para la unificación del campus

Los módulos del Passport 8600 soportan una gran performance en capa 2 y capa 3 a través de una arquitectura de switching que entrega una velocidad de 128 Gbps de capacidad para una gran performance de las aplicaciones de hoy, escalable hasta 256 Gbps. El switching y routing entre dos puertos cualquiera del switch son realizadas con una latencia menor a 10µS, haciendo que el Passport 8600 sea una plataforma de Backbone ideal para soportar aplicaciones de misión crítica y las soluciones de Redes Unificadas de mañana utilizando Internet Telephony. La perfomance de los módulos del Switch Routing Passport 8600 es NO BLOCKING en su máxima densidad.

El Chasis del Passport 8600 y Passport 8100 provee características dirigidas a asegurar una gran disponibilidad para su red, gran performance para cualquier situación, a través de Non-blocking, wire-speed para Ethernet, Fast Ethernet y Gigabit Ethernet, mientras mantiene la simplicidad operacional para los administradores de red. El chasis tiene características de una arquitectura de switching pasiva que está diseñada para ofrecer una gran disponibilidad para un amplio rango de tecnologías soportadas.

El Passport 8600 soporta una completa configuración de seguridad para el campus LAN, restringiendo el acceso a la red para usuarios autorizados y controlando el acceso a departamentos, servidores y aplicaciones críticas.

El Passport 8600 soporta switcheo distribuido y administración con lo que se elimina simples punto de falla y provee total resilencia al sistema futuro

Las facilidades de redundancia y alta disponibilidad de puertos están dadas por técnicas tales como VRRP (Virtual Routing Redundant Protocol), MLT (Multilink Trunking) y DMLT (Distributed Multilink Trunking); a continuación un breve repaso con la explicación de las mismas:

- **VRRP**

Virtual Router Redundancy Protocol (VRRP) utiliza las direcciones MAC basadas en el Virtual Router ID. Por default el intervalo de advertencia es de un segundo, después de 3 avisos perdidos, el VRRP de Backup se convierte en el VRRP Master. Nortel Networks provee una mejora: soporte para direcciones críticas IP.

Debido a que las estaciones finales no soportan los protocolos de enrutamiento como el RIP y el OSPF, los Default Gateways debes ser configurados estáticamente. Estos Default Gateways son punteros de sus subredes IP. La pérdida de los default gateways ocasiona una imposibilidad de comunicación de las subredes, las cuales en la mayoría de los casos están conformadas por recursos y servicios. El VRRP está diseñado para eliminar el único punto de falla que puede ocurrir cuando una sola dirección estática del default gateway router para una estación final, se pierde. Esto nos introduce al concepto de una dirección IP virtual (transparente a los usuarios) compartida entre dos o más routers conectados a una subred común en la red empresarial.

VRRP utiliza los Multicast Hellos entre las interfaces de los routers participantes para detectar cuál de las interfaces se convertirá en el Master. La interfase con la mayor prioridad es seleccionada como Master y entonces constantemente envía paquetes hello sobre la interfase protegida VRRP. Las otras interfaces VRRP potenciales escuchan estos hellos y toman el rol de VRRP Master en el caso de que falle el VRRP Master original. Las interfaces VRRP comparten una dirección MAC común, la cual es construida fuera del espacio MAC reservado para el VRRP y el VRRP ID:

Dirección Virtual Router MAC:

00-00-5E-00-01-XX donde XX es el VRID en Hex

En el caso de una falla esta dirección MAC es movida al nuevo VRRP Master. El nuevo Master enviará broadcast target-less como el origen, para estar seguro de que todos los switches de capa 2 en la interfase protegida VRRP, puedan volver a aprender la dirección VRRP Master original.

❑ MULTILINK TRUNKING

El Multilink Trunking de Nortel Networks, o MLT, ha sido diseñado para agregar múltiples puertos del switch dentro del Grupo de Multilink Trunk para una conexión de "Tubería ancha" entre los switches que lo soportan y los servidores de red.

Implementando el MLT se incrementará el "throughput" agregado en la interconexión entre dos dispositivos. MLT puede incluso ser usado sobre enlaces de misión crítica para redundancia, y el MLT puede ser configurado de manera distribuida sobre múltiples slots en el chasis del Passport 8600.

Debemos aclarar que para implementar el MLT en el Passport, todos los puertos que lo conforman deberán ser configurados idénticamente (full / half duplex, velocidad, etc.). El MLT es una conexión punto a punto, así el nodo conectado directamente a cualquier Passport con el MLT debe incluso soportar esta característica, es decir el MLT. Esto incluye a los switches Ethernet, Multi ports Network Interface Cards en servidores, y cualquier dispositivo de terceros.

El Multilink Trunking Distribuido (DMLT) agrega un nivel extra de redundancia a los enlaces MLT. Con la configuración del DMLT a través de diferentes slots dentro del mismo chasis, si una falla ocurre ya sea en un puerto o en un módulo, el enlace se mantiene porque los otros módulos en el DMLT continuarán funcionando apropiadamente.

MLT puede ser usado en conjunto con el protocolo "spanning tree" para una redundancia de la topología. El Spanning Tree detectará un loop en la topología y bloqueará la última ruta no deseada.

Es importante entender que el MLT en el Passport Routing Switch debe ser configurado en una VLAN activa. Si el enrutamiento es aplicado a esta VLAN, y el spanning tree es configurado, todos los protocolos de enrutamiento serán bloqueados hasta que la convergencia en la Capa 2 sea lograda.

❑ CUALES SON LAS CARACTERÍSTICAS Y BENEFICIOS DEL SWITCH CAPA 3?

La Tabla 5.1.1 define las características claves del Passport 8600 y sus beneficios asociados.

Característica Passport 8600	Beneficio Passport 8600
Gran Disponibilidad	
Chasis completamente redundante – N+1 power, dual bandeja de ventiladores	Hace a la red completamente resiliente en el improbable evento de una falla de la fuente de alimentación o ventilador – los usuarios no se verán afectados
Elección de alimentación AC o DC	Soporta flexibilidad para un amplio variedad de ambientes de redes
Componentes del chasis (fuentes de alimentación y bandeja de ventiladores) y módulos de interfaces son intercambiable en caliente	Asegura la disponibilidad de la red
Resilencia del riser, de las conexiones del backbone y del servidor vía multilink distribuido	Elimina un único punto de falla (los puertos que forman el trunk pueden ser distribuidos a través de módulos separados)
Seguridad de la red basada en departamento, usuarios, o aplicaciones	Restringe el acceso a la red a usuarios no autorizados y controla el acceso a departamentos, servidores y aplicaciones criticas

Característica Passport 8600	Beneficio Passport 8600
Simplicidad Operacional	
Todos los componentes del chasis, los módulos del sistema e interfaces con accesibles desde la parte frontal del chasis	Elimina la necesidad de tiempos de bajada de la red para componentes intercambiables en caliente
Enlaces escalables de riser, server, y backbone hasta 32 Gbps usando MLT	Añade gran perfomance y provee escalabilidad y resiliencia vía agregación de ancho de banda
Eficiente, control automático de aplicaciones Multicast usando protocolos estándar IETF	Ayuda a distribuir ancho de banda rápidamente al trafico intensivo de multicast de una manera estándar
Soporte para Optivity, incluyendo comandos comunes de interfase de línea	Provee capacidad de administración acorde a los estándares de la industria así como el acceso a las características de valor añadido provistas por Nortel que conduce la plataforma Optivity
Soporte para Optivity policy management de extremo a extremo	Clave para habilitar prioritización del trafico a través de la red
Bajo costo de propiedad	
Plataforma futura que integra soporte para switcheo en capa 2 y capa 3, multi-servicio MAN/WAN y futura tecnología de telefonía IP	Provee protección de la inversión través de la capacidad de integrar tecnologías multiservicio en el futuro
Partes comunes para chasis, fuentes de poder, bandejas de ventiladores y módulos de interfaces	Reduce el mantenimiento y costos de soporte

Tabla 5.1.1. Passport 8600: Características Claves y beneficios

❑ CARACTERÍSTICAS TÉCNICAS DEL PASSPORT 8600

Entre las características del Passport 8600 L3 podemos mencionar:.

- Switch con capacidad de operación en las capas 2 y capa 3 (filtering en capa 4) del modelo OSI
- Fuente de alimentación redundantes (hot swap) para 220 VAC 60Hz.
- Backplane único y pasivo

- La velocidad de conmutación del backplane ofrecido es de 128 Gbps, con un crecimiento futuro a 256 Gbps.
- Chassis montable en bastidor de 19" de ancho (rack mountable).
- Backplane único y pasivo.
- La capacidad de "Forwarding Rate" del procesador en Layer 2 es de 96 Mpps.
- La capacidad de "Forwarding Rate" del procesador en Layer 3 es de 96 Mpps.
- Capacidad de manejo de políticas en Layer 4 para filtros y priorización.
- Capacidad operativa de filtrado de broadcast para los protocolos IP.
- Capacidad de ruteo IP,IPX y Bridging
- El equipo es escalable y modular.
- Arquitectura No-Blocking Full Duplex, en todos los puertos Ethernet, FastEthernet y GigabitEthernet.
- Módulos Gigabit Ethernet de 8 puertos en fibra óptica o módulos MDA de bajo costo.
- Soporta los estándares 802.1Q (QoS Quality of Service y CoS Class of Service)
- Soporta el protocolo "Spanning Tree"
- Capacidad de balancear de tráfico en los puertos Fast Ethernet y Gigabit ethernet
- Soporta los estándares: 802.1d, 802.1Q, 802.3z (flow Control y full duplex) 802.1P, IEEE 802.3X, 10Base-T,100Base TX e IEEE 802.3U, 802.3Z.

- Capacidad de soportar al menos 2000 VLANs
- Incluye soporte de protocolos de enrutamiento RIP, RIP2, OSPF, SNMP, RMON (4 Grupos RMON: estadísticas, historial, eventos y alarmas), IGMP, RSVP, VRRP y con capacidad de redistribución de tablas de enrutamiento entre ellos cuando utiliza capa 3.
- Capacidad de ser administrado vía telnet, web browser y/o vía módem.
- Incluye acceso a consola de administración vía CLI, Telnet.
- En adición de uno o dos módulos 8690SF, hasta 8 módulos Passport 8600 pueden ser instalados en un chassis de 10 slot.

❑ MÓDULOS DEL PASSPORT 8600

Los módulos del Passport 8600 routing switch usan una altamente eficiente salida buferizada, arquitectura de memoria compartida en un avanzado chasis modular para entregar gran densidad de puertos y gran disponibilidad. La próxima generación de ASICs han sido diseñados para proveer gran perfomance en arquitectura de envío de paquetes totalmente basado en hardware

Los módulos del Passport 8600 son no Blocking en su máxima densidad.

La característica Express Classification (XC) de los módulos del Passport 8600 integra filtrado basado en hardware para seguridad y clasificación de trafico, para wire-speed en capa 2, capa 3 y capa 4. La tecnología distribuida XC nos habilita a satisfacer los exactos requerimientos de nuestras aplicaciones de negocios

críticas sin sacrificar la perfomance de la red, tales como requerimientos para el flujo sensitivo a la latencia, incluido video y voz en tiempo real

A continuación tenemos una breve explicación de los módulos del Passport 8600 routing switch

- **MÓDULO PASSPORT 8690 SWITCH FABRIC/CPU**

Requerido en todas las configuraciones de los routing switches Passport 8600, el modulo Passport 8690SF está optimizado para entregar una alta perfomance en el switching de tráfico en capa 2 y capa 3. Todo la conmutación "switching" ocurre en el Switch Fabric dentro del Passport 8690SF, mientras los módulos de I/O realizan el buffering, la resolución de las direcciones, la clasificación del trafico y proveen la interfase de la capa física a la red.

Una característica clave del Routing Switch Passport 8600 es el soporte de switch fabric duales. La adición de un segundo módulo Passport 8690SF no solo provee redundancia sino que optimiza la perfomance automáticamente doblando la capacidad del switch fabric, debido a que ambos están activamente reenviando tráfico. En el caso de una falla del switch fabric, el sistema revierte la operación con un único fabric. El CPU del módulo Passport 8690SF principal actúa como la máquina de control de software Master.

El CPU utilizado de la placa es un powerPC que provee todo el control del sistema. El CPU ejecuta todos los protocolos de bridging y routing, computa la base

de datos de envío y distribuye esa base de datos a caches de direcciones sobre los módulos I/O.

El CPU también realiza aprendizaje independiente de dispositivos desconocidos y actualizaciones de la topología para que así el switch fabric sea dedicado al switcheo de trafico de aplicaciones de negocio critico. En el caso de una falla de un switch Fabric el trafico es automáticamente switcheado al modulo Passport 8690SF restante, en menos de un segundo.

En el chasis de 10 Slots, el Passport 8690SF debe ser instalado en los slots 5 o 6 (o en ambos). Un almacenamiento No Volátil para el run.time code es proveída por la memoria flash run-time de 16 Mb. Un slot frontal para una PCMCIA acepta un ATA Flash Card como otra opción para el almacenamiento del run-time code.

El módulo Passport 8690SF está equipado con un puerto de consola en el panel frontal. Este puerto tiene un conector DB-9 es seleccionable desde el panel frontal para operar como DCE o DTE para operar como puerto remoto con un módem o como puerto de consola local. Incluso tiene un puerto 10/100 Ethernet para administración.

- **MÓDULO PASSPORT 8648TX FAST ETHERNET ROUTING SWITCH**

El módulo Passport 8648TX es optimizado para alta densidad de granja de servidores empresariales y gabinetes de cableados, entregando un efectivo costo-beneficio en conmutación y enrutamiento a 10/100.

El Passport 8648TX provee 48 puertos 10/100 BASE-TX con conector RJ45 autosensing. El módulo soporta operaciones tanto en half duplex como en full duplex y cumple con el standard IEEE 802.3u para autonegociación. Incrustados dentro de cada conector del puerto existen dos LEDs unicolor que muestra la velocidad (en el lado izquierdo de un puerto) y el status de enlace/actividad (a la derecha de un puerto).

Cuando el puerto está operando a 100 Mbps, el LED de velocidad está iluminado. Cuando el LED de enlace/actividad está en off, el puerto es deshabilitado, particionado o sin enlace. Una luz estable en verde indica un buen enlace sin tráfico, y una luz verde parpadeante indica que ya sea la transmisión o recepción de tráfico. Si el LED no está iluminado, esto indica que el módulo no está en funcionamiento todavía. Una luz en ámbar parpadeante indica inicialización, mientras que una luz ámbar estable indica que existe un fallado power-on self-test. Si el LED está en verde el módulo ha inicializado con éxito.

- **MÓDULO PASSPORT 8608GBIC GIGABIT ETHERNET ROUTING SWITCH**

El módulo 8608GBIC provee 8 puertos GBIC usando módulos GBIC plug-in, con conectores SC, también soporta conexiones de Servidores y riser. Optimizado para backbones de campus, el módulo Passport 8608 GBIC habilita interconexiones de larga distancia sobre fibra monomodo o multimodo, entregando hasta 16 Gbps de ancho de banda en un solo trunk usando Distributed Multilink (DMLT).

El Módulo 8608GBIC cumple con el estándar 802.3z.

El módulo Passport 8608GBIC tiene 8 puertos GBIC que pueden soportar simultáneamente 1000 Base SX, 1000 Base LX, todos operando a full duplex. Cada Passport 8606 GBIC tiene un LED que indica la velocidad del puerto y la actividad por cada uno y adicionalmente LEDs para indicar el encendido y el status del diagnóstico.

El mayor beneficio de este módulo es la posibilidad de tener diferentes opciones Gigabit Ethernet en un solo módulo.

Los GBICs (Gigabit Interface Converters) estan disponibles en SX, LX, XD y ZD para usarlo con el modulo 8608GBIC

❑ MÓDULOS DEL PASSPORT 8100

Los módulos del Passport 8100 Edge Switch entregan alta perfomance de switcheo en Capa 2 para la plataforma de switch empresariales Passport 8000. Los módulos 8100 Edge Switch entregan gran disponibilidad, simplicidad operacional y bajo costo de posesión requeridos actualmente para los gabinetes de cableado de alta densidad, entregando un para las conexiones desktop 10/100 0 100 BASE-FX e integrando risers Fast Ethernet, Gigabit Ethernet o ATM para conectividad con el core de la red.

Los módulos del Passport 8100 Edge Switch soportan alta perfomance de switcheo en arquitectura de capa 2 entregando hasta 50 Gbps de capacidad de switcheo hoy, (escalando hasta 256 Gbps en el futuro) y 24 Mpps con menos de 10 microsegundos de latencia para soportar las aplicaciones del negocio.

Hay que resaltar que, todos los módulos de la serie Passport 8000 son "hot swap".

- **MÓDULO PASSPORT 8190 SWITCH FABRIC/CPU**

Los chasis de 6 y 10 slots requieren un 8190 SM para el sistema de switcheo 8100

El modulo de administración 8190SM trae una tarjeta CPU para la gerencia y administración de los módulos 8100 Edge switch. Una completo administración de file system provee capacidades importantes tales como imagen de software y almacenamiento del archivo de configuración, cargar y descargar archivos, edición de archivos ASCII y lista de acceso administrativa para SNMP y telnet

Dos módulos 8190SM pueden ser instalados para una total resilencia. En el caso de la falla de un CPU, el control es automáticamente pasado al módulo 8190SM secundario en menos de un segundo

El 8190SM un puerto de consola y modem estándar DB9, un slot PCMIA para tarjetas de tipo ATA y un puerto 10/100 ethernet para administración out-of-band facilitando la administración del switch

El módulo 8190SM también trae indicadores luminosos para indicar temperatura, fuente de alimentación y estado de bandeja de ventiladores, estado master/secundario, utilización del CPU gerencia del enlace del puerto y velocidad

- **MÓDULO PASSPORT 8148TX EDGE SWITCH**

Proveyendo soluciones en cobre, el módulo Fast Ethernet Edge Swith ofrece alta disponibilidad, densidad de puertos máxima y simplicidad operacional requerido por los gabinetes de cableados empresariales.

El módulo 8148TX es óptimo para gabinetes de cableado de alta densidad, trayendo 48 puertos autosensing 10/100 para la conectividad del usuario desktop a través de la interfase estándar RJ45.

El módulo contiene indicadores luminosos de velocidad y actividad de cada cuerpo, así como diagnostico de estado y energía

Hasta un máximo de 8 módulos edge switch pueden ser instalados en un chasis de 10 slots, soportando hasta 384 puertos 10/100.

- **MÓDULO PASSPORT 8108GBIC EDGE SWITCH**

EL Módulo 8108GBIC provee 8 puertos para conectores de interfaces Gigabit (GBIC) para conectividad del riser y servidores usando módulos GBIC plug-in con conectores SC. Los módulos plug-in GBIC están disponibles en SX, LX, XD y DX.

El módulo 8108GBIC esta optimizado para granjas de servidores de alta densidad y puntos de agregación en redes de campos empresariales y para aplicaciones backbone/core en redes de campo de mediano tamaño.

El módulo tiene indicadores luminosos de enlace y actividad por cada puerto y adicionalmente para indicar energía, fallas y estado del reloj principal

❑ DISTRIBUCIÓN DE LOS EQUIPOS EN EL BACKBONE

Se han definido 4 áreas físicas de acuerdo a la disposición en el local de la sede tecnológica .

▪ Nodo Principal : Centro de Cómputo (Data Center)

En este ambiente se diferencian 2 sectores:

Switches CORE : Que atenderán directamente a los servidores de la red de Datos donde se encuentran, por ejemplo los Servidores Pre-Pago, Billing, Medición, Fraude, CMR, etc, además de atender a usuarios. La capacidad de estos switches CORE son de 16 puertos Gigabit Ethernet GBIC Capa 3 y 144 puertos 10/100 Mbps Fast Ethernet Capa 3 cada uno.Estos switches están conectados mediante un enlaces MLT de 2 Gbps

Switches WAN : Cuya función es soportar todo el tráfico originado en los locales remotos (Sucursales) y Sede Administrativa. La capacidad de estos switches WAN son de 8 puertos Gigabit Ethernet GBIC Capa 3 y 48 puertos 10/100 Mbps Fast Ethernet Capa 3 cada uno. Estos switches están conectados mediante un enlaces MLT de 2 Gbps

Los Switches CORE y los Switches WAN están conectados en forma de malla permitiendo formar enlaces activos y simultáneos, redundante de red que permite disponibilidad por múltiples caminos.

- **Nodo Secundario: NOC (1er Piso)**

En este ambiente se encuentran las áreas de Oficinas de Red, Técnicos de Operaciones y áreas de NOC. La capacidad necesaria de los Switches NOC son de 8 puertos Gigabit Ethernet GBIC capa 2 y 144 puertos Fast Ethernet capa 2 cada uno.

- **Nodo Secundario: GERENCIAS (2do Piso)**

En este ambiente se encuentran las Oficinas de direcciones y gerencias . La capacidad necesaria de los Switches GER son de 8 puertos Gigabit Ethernet GBIC capa 2 y 144 puertos Fast Ethernet capa 2 cada uno.

- **Nodo Secundario: CUSTOMER CARE (Call Center 2do Piso)**

En este ambiente se encuentran las Oficinas de atención al cliente. La capacidad necesaria de los Switches CC son de 8 puertos Gigabit Ethernet GBIC capa 2 y 144 puertos Fast Ethernet capa 2 cada uno.

En la Figura 5.1.2 se muestra la red LAN implementada para la sede Tecnológica bajo un esquema de alta disponibilidad, desempeño y escalabilidad.

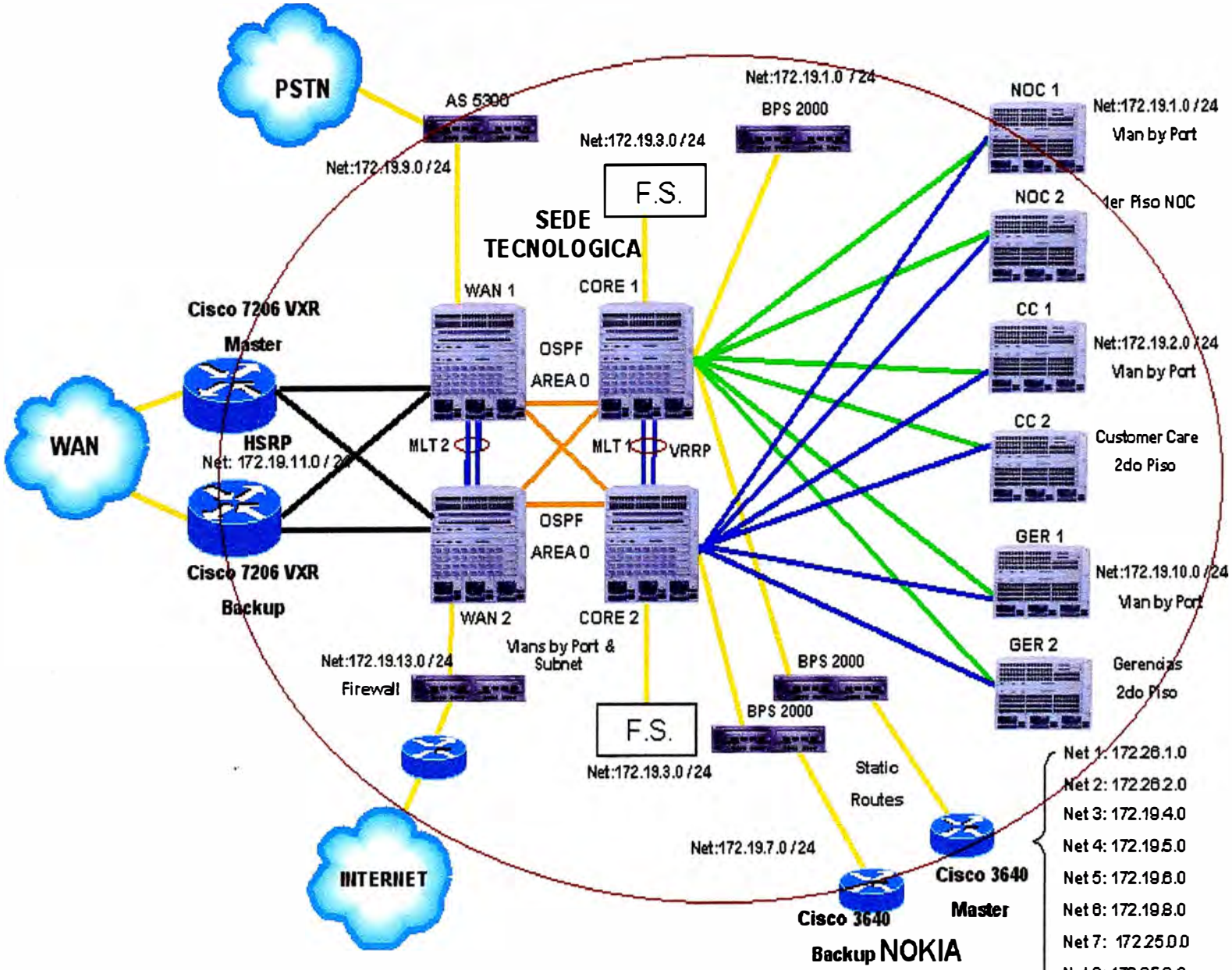


FIG 5.1.2 RED LAN SEDE TECNOLOGICA

- **CONFIGURACIÓN DE LOS SWITCHES CORE L3 PARA EL DATA CENTER 1er PISO**

Para este nodo se propuso dos Switches Passport 8600 capa 3 con la siguiente configuración para cada switch: Chassis de 10 Slots, 144 puertos 10/100 Mbps Fast Ethernet Capa 3, 16 puertos Gigabit Ethernet GBIC Capa 3 (12 puertos con Convertidores GBIC y 4 puertos vacíos), 12 módulos Convertidores GBIC para enlaces Gigabit Ethernet. Se incluyó Redundancia de Procesador y Fuentes de Poder Redundantes.

Con esta configuración se tiene 7 Slots ocupado (con 2 módulos 8690SF/CPU, 3 módulos 8648TX y 2 módulos 8608 GBIC) quedando 3 slots libres.

Cada Switch propuesto tiene la siguiente configuración que se muestra en la tabla 5.1.2:

	PASSPORT 8600 SERIES: Switch CORE LAYER 3 Primer Piso: Data Center	
	144 puertos Fast Ethernet 16 puertos GigabitEthernet con 12 Converter GBIC incluido	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
DS1410003-3.1	Licencia de Software y Kit de Software del Passport 8000 Enterprise Routing Switch (Incluye licencia, software Device Manager, y toda la documentación). Una licencia requerida por cada chasis del switch routing. Versión 3.1.	1
DS1402001	Passport 8010 chassis de 10 slot. Incluye chassis, dual backplane, dos bandejas de ventiladores, cable RS232 para administración de consola, kit para montar en Rack y Kit guía cable. Requiere una o dos Fuentes de alimentación dependiendo de la configuración; Hasta tres fuentes de alimentación es soportada.	1
DS1405E01	Passport 8001PS fuente de alimentación de 100-240 VAC. Al menos una fuente de alimentación es requerida por cada chasis del Passport 8000. (Incluye cable de poder tipo Norte Americano)	3
DS1404001	Módulo Passport 8690SF Enterprise Routing Switch ; Módulo CPU/Switch Fabric - Uno requerido por cada chassis Passport 8000 Routing Switch . Incluye tarjeta de memoria flash PCMCIA.	2
DS1404002	Módulo Passport 8648TX Enterprise Routing Switch. Interfase de conmutación Ethernet Capa 3 de 48 puertos autosensing 10BASE-T/100BASE-TX.	3
DS1404015	Módulo Passport 8608GB Enterprise Routing Switch de 8-puertos 1000 Base GBIC (GBICs son vendidos separadamente)	2
AA1419001	1-puerto 1000Base-SX Gigabit Interface Converter (GBIC)	12

Tabla 5.1.2 Configuración de cada Switch CORE

El siguiente gráfico muestra la configuración de los 2 Equipos propuesto para este nodo.

CORE 1

1	8 port 1000BASE-GBIC 8608GBIC (06 GBIC-SX)
2	8 port 1000BASE-GBIC 8608GBIC (06 GBIC-SX)
3	48 port 10/100BASE-TX 8648TX
4	48 port 10/100BASE-TX 8648TX
5	8690 SF SWITCH FABRIC
6	8690 SF SWITCH FABRIC
7	48 port 10/100BASE-TX 8648TX
8	
9	
10	
PS1	PS2 PS3

CORE 2

1	8 port 1000BASE-GBIC 8608 GBIC (06 GBIC-SX)
2	8 port 1000BASE-GBIC 8608GBIC (06 GBIC-SX)
3	48 port 10/100BASE-TX 8648TX
4	48 port 10/100BASE-TX 8648TX
5	8690 SF SWITCH FABRIC
6	8690 SF SWITCH FABRIC
7	48 port 10/100BASE-TX 8648TX
8	
9	
10	
PS1	PS2 PS3

Figura 5.1.3. Configuración de los dos Switches CORE Passport 8600 Capa 3 propuesto para el Data Center. Capacidad total instalada de 288 puertos 10/100BASE-TX y 32 puertos 1000BASE-GBIC

- **CONFIGURACIÓN DE LOS SWITCHES WAN L3 PARA EL DATA CENTER 1er PISO**

Para este nodo se propuso dos Switches Passport 8600 con la siguiente configuración para cada switch: Chasis de 10 Slots, 48 puertos 10/100 Mbps Fast Ethernet Layer 3, 8 puertos Gigabit Ethernet GBIC Layer 3 (4 puertos con Converter GBIC y 4 puertos vacíos), 4 módulos Converter GBIC para enlaces Gigabit Ethernet. Se incluyó Redundancia de Procesador y Fuentes de Poder Redundantes.

Con esta configuración se tiene 4 Slots ocupado (con 2 módulos 8690SF/CPU, 1 módulos 8648TX y 1 módulo 8608 GBIC) quedando 6 slots libres.

Cada Switch propuesto tiene la siguiente configuración que se muestra en la tabla 5.1.3:

PASSPORT 8600 SERIES: Switch WAN LAYER 3 Primer Piso: Data Center		
	48 puertos Fast Ethernet 8 puertos GigabitEthernet con 4 Converter GBIC incluido	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
DS1410003-3.1	Licencia de Software y Kit de Software del Passport 8000 Enterprise Routing Switch (Incluye licencia, software Device Manager, y toda la documentación). Una licencia requerida por cada chasis del switch routing. Versión 3.1.	1
DS1402001	Passport 8010 chassis de 10 slot. Incluye chassis, dual backplane, dos bandejas de ventiladores, cable RS232 para administración de consola, kit para montar en Rack y Kit guía cable. Requiere una o dos Fuentes de alimentación dependiendo de la configuración; Hasta tres fuentes de alimentación es soportada.	1
DS1405E01	Passport 8001PS fuente de alimentación de 100-240 VAC. Al menos una fuente de alimentación es requerida por cada chasis del Passport 8000. (Incluye cable de poder tipo Norte Americano)	3
DS1404001	Módulo Passport 8690SF Enterprise Routing Switch ; Módulo CPU/Switch Fabric - Uno requerido por cada chassis Passport 8000 Routing Switch . Incluye tarjeta de memoria flash PCMCIA.	2
DS1404002	Módulo Passport 8648TX Enterprise Routing Switch. Interfase de conmutación Ethernet Capa 3 de 48 puertos autosensing 10BASE-T/100BASE-TX.	1
DS1404015	Módulo Passport 8608GB Enterprise Routing Switch de 8-puertos 1000 Base GBIC (GBICs son vendidos separadamente)	1
AA1419001	1-puerto 1000Base-SX Gigabit Interfase Converter (GBIC)	4

Tabla 5.1.3 Configuración de cada Switch WAN

El siguiente gráfico muestra la configuración de los 2 Equipos propuesto para este nodo.

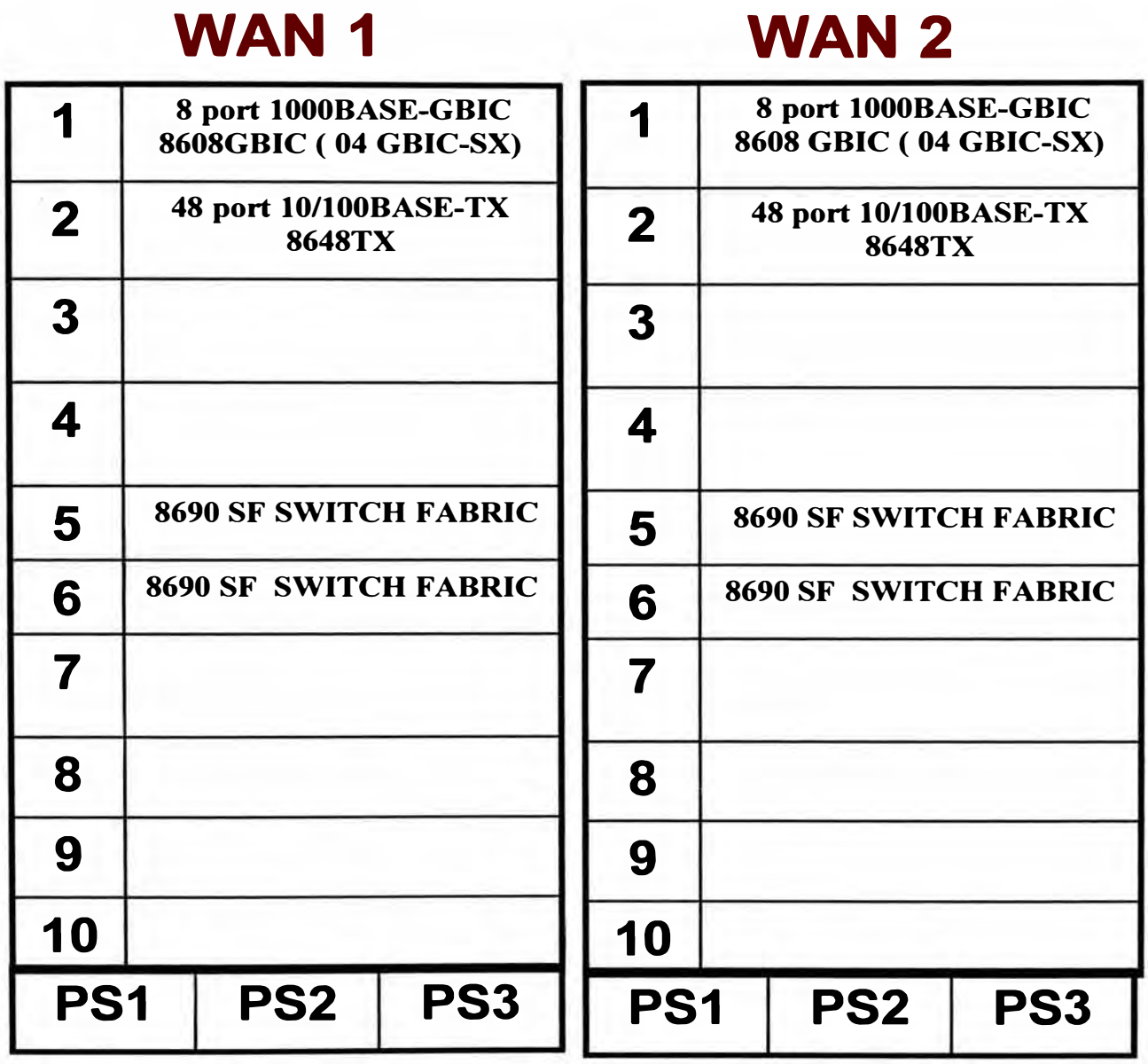


Figura 5.1.4. Configuración de los dos Switches WAN Passport 8600 Capa 3 propuesto para el Data Center. Capacidad total instalada de 96 puertos 10/100BASE-TX y 16 puertos 1000BASE-GBIC

- **CONFIGURACIÓN DE LOS SWITCHES NOC L2 PARA EL NODO SECUNDARIO CENTRO DE OPERACIONES DE RED 1er PISO**

Para este nodo se propuso dos Switches Passport 8100 con la siguiente configuración para cada switch: Chassis de 10 Slots, 144 puertos 10/100 Mbps Fast Ethernet capa 2, 8 puertos Gigabit Ethernet GBIC capa 2 (4 puertos con Converter GBIC y 4 puertos vacíos), 4 módulos Converter GBIC para enlaces Gigabit Ethernet. Se incluyó Redundancia de Procesador y Fuentes de Poder Redundantes.

Con esta configuración se tiene 6 Slots ocupado (con 2 módulos 8190SM/CPU, 3 módulos 8148TX y 1 módulos 8108 GBIC) quedando 4 slots libres.

Cada Switch propuesto tiene la siguiente configuración que se muestra en la tabla 5.1.4:

	PASSPORT 8100 SERIES: Switch NOC LAYER 2 Primer Piso: Network Operation Center	
	144 puertos Fast Ethernet 8 puertos GigabitEthernet con 4 Converter GBIC incluido	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
DS1410001-3.1	Licencia de Software y Kit de Software del Switch de borde Passport 8100 (Incluye licencia, software Device Manager, y toda la documentación). Una licencia requerida por cada chasis del switch de borde . Versión 3.1.	1
DS1402001	Passport 8010 chassis de 10 slot. Incluye chassis, dual backplane, dos bandejas de ventiladores, cable RS232 para administración de consola, kit para montar en Rack y Kit guía cable. Requiere una o dos Fuentes de alimentación dependiendo de la configuración; Hasta tres fuentes de alimentación es soportada.	1
DS1405E01	Passport 8001PS fuente de alimentación de 100-240 VAC. Al menos una fuente de alimentación es requerida por cada chasis del Passport 8000. (Incluye cable de poder tipo Norte Americano)	3
DS1404014	Módulo de Administración Passport 8190SM Uno requerido por cada chasis del switch de borde Passport 8100 . Incluye kit de licencia de software del Switch de borde y tarjeta de memoria flash PCMCIA.	2
DS1404007	Módulo para el switch de borde Passport 8148TX. Interfase de conmutación Ethernet Capa 2 de 48 puertos autosensing 10BASE-T/100BASE-TX.	3
DS1404009	Módulo para el switch de borde Passport 8108GB de 8-puertos 1000 Base GBIC (GBICs son vendidos separadamente)	1
AA1419001	1-puerto 1000Base-SX Gigabit Interfase Converter (GBIC)	4

Tabla 5.1.4 Configuración de cada switch NOC

El siguiente gráfico muestra la configuración de los 2 Equipos propuesto para este nodo.

NOC 1

1	8 port 1000BASE-GBIC 8108GBIC (04 GBIC-SX)
2	48 port 10/100BASE-TX 8148TX
3	48 port 10/100BASE-TX 8148TX
4	48 port 10/100BASE-TX 8148TX
5	8190 SM SWITCH FABRIC
6	8190 SM SWITCH FABRIC
7	
8	
9	
10	

PS1	PS2	PS3

NOC 2

1	8 port 1000BASE-GBIC 8108 GBIC (04 GBIC-SX)
2	48 port 10/100BASE-TX 8148TX
3	48 port 10/100BASE-TX 8148TX
4	48 port 10/100BASE-TX 8148TX
5	8190 SM SWITCH FABRIC
6	8190 SM SWITCH FABRIC
7	
8	
9	
10	

PS1	PS2	PS3

Figura 5.1.5. Configuración de los dos Switches NOC Passport 8100 Capa 2 propuesto para el Centro de Operaciones de Red. Capacidad total instalada de 288 puertos 10/100BASE-TX y 16 puertos 1000BASE-GBIC

- **CONFIGURACIÓN DE LOS SWITCHES GER L2 PARA EL NODO SECUNDARIO GERENCIAS 2do PISO**

Para este nodo se propuso dos Switches Passport 8100 con la siguiente configuración para cada switch: Chassis de 10 Slots, 144 puertos 10/100 Mbps Fast Ethernet capa 2, 8 puertos Gigabit Ethernet GBIC capa 2 (4 puertos con Converter GBIC y 4 puertos vacíos), 4 módulos Converter GBIC para enlaces Gigabit Ethernet. Se incluyó Redundancia de Procesador y Fuentes de Poder Redundantes.

Con esta configuración se tiene 6 Slots ocupado (con 2 módulos 8190SM/CPU, 3 módulos 8148TX y 1 módulos 8108 GBIC) quedando 4 slots libres.

Cada Switch propuesto tiene la siguiente configuración que se muestra en la tabla 5.1.5:

	PASSPORT 8100 SERIES: Switch GER LAYER 2 Segundo Piso: Gerencias	
	144 puertos Fast Ethernet 8 puertos GigabitEthernet con 4 Converter GBIC incluido	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
DS1410001-3.1	Licencia de Software y Kit de Software del Switch de borde Passport 8100 (Incluye licencia, software Device Manager, y toda la documentación). Una licencia requerida por cada chasis del switch de borde . Versión 3.1.	1
DS1402001	Passport 8010 chassis de 10 slot. Incluye chassis, dual backplane, dos bandejas de ventiladores, cable RS232 para administración de consola, kit para montar en Rack y Kit guía cable. Requiere una o dos Fuentes de alimentación dependiendo de la configuración; Hasta tres fuentes de alimentación es soportada.	1
DS1405E01	Passport 8001PS fuente de alimentación de 100-240 VAC. Al menos una fuente de alimentación es requerida por cada chasis del Passport 8000. (Incluye cable de poder tipo Norte Americano)	3
DS1404014	Módulo de Administración Passport 8190SM Uno requerido por cada chasis del switch de borde Passport 8100 . Incluye kit de licencia de software del Switch de borde y tarjeta de memoria flash PCMCIA.	2
DS1404007	Módulo para el switch de borde Passport 8148TX. Interfase de conmutación Ethernet Capa 2 de 48 puertos autosensing 10BASE-T/100BASE-TX.	3
DS1404009	Módulo para el switch de borde Passport 8108GB de 8-puertos 1000 Base GBIC (GBICs son vendidos separadamente)	1
AA1419001	1-puerto 1000Base-SX Gigabit Interfase Converter (GBIC)	4

Tabla 5.1.5 Configuración de cada switch GER

El siguiente gráfico muestra la configuración de los 2 Equipos propuesto para este nodo.

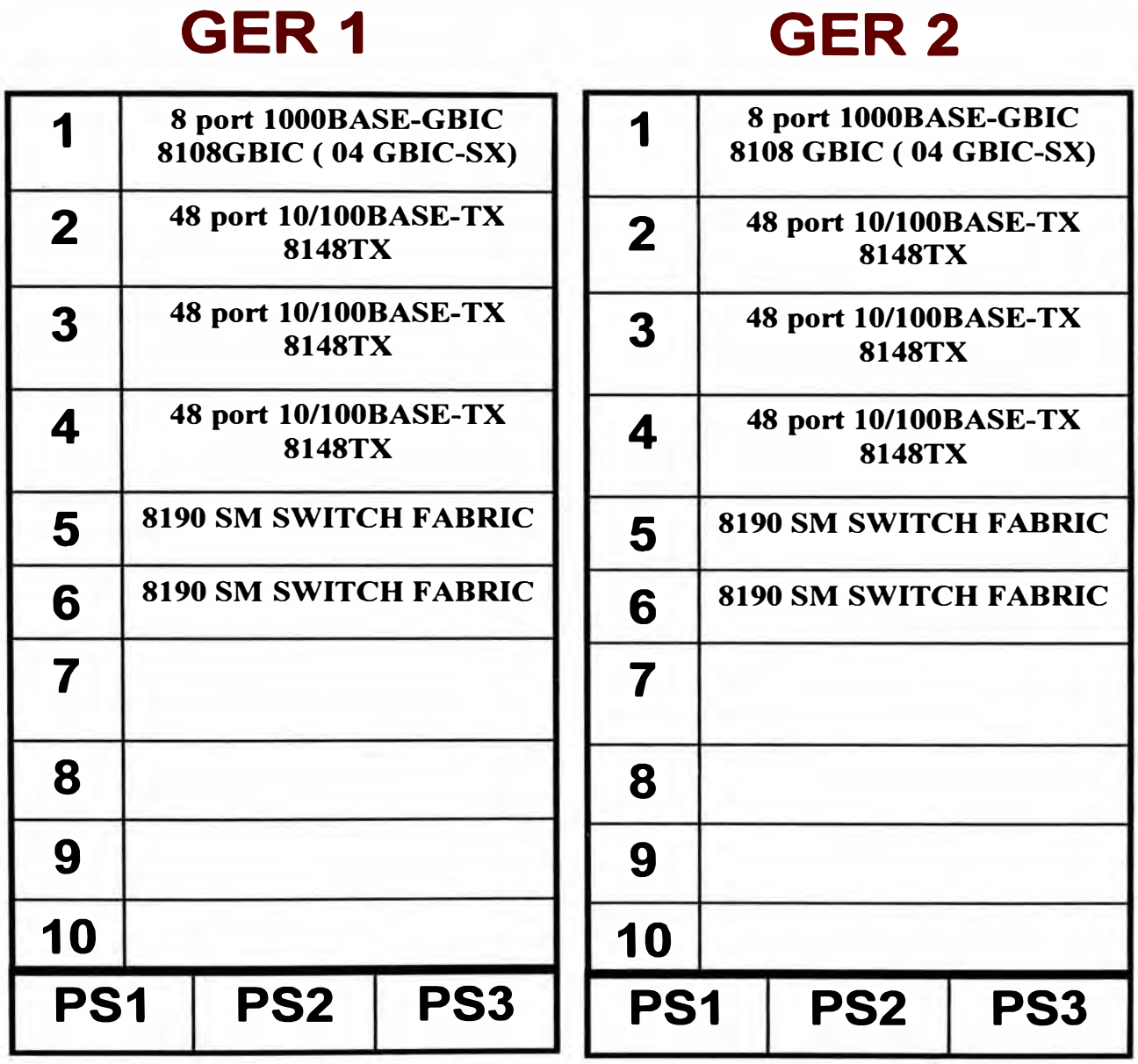


Figura 5.1.6. Configuración de los dos Switches GER Passport 8100 Capa 2 propuesto para el Centro de Operaciones de Red. Capacidad total instalada de 288 puertos 10/100BASE-TX y 16 puertos 1000BASE-GBIC

- **CONFIGURACIÓN DE LOS SWITCHES CC L2 PARA EL NODO SECUNDARIO CUSTOMER CARE (CALL CENTER 2do PISO)**

Para este nodo se propuso dos Switches Passport 8100 con la siguiente configuración para cada switch: Chassis de 10 Slots, 144 puertos 10/100 Mbps Fast Ethernet capa 2, 8 puertos Gigabit Ethernet GBIC capa 2 (4 puertos con Converter GBIC y 4 puertos vacíos), 4 módulos Converter GBIC para enlaces Gigabit Ethernet. Se incluyó Redundancia de Procesador y Fuentes de Poder Redundantes.

Con esta configuración se tiene 6 Slots ocupado (con 2 módulos 8190SM/CPU, 3 módulos 8148TX y 1 módulos 8108 GBIC) quedando 4 slots libres.

Cada Switch propuesto tiene la siguiente configuración que se muestra en la tabla 5.1.6:

	PASSPORT 8100 SERIES: Switch CC LAYER 2 Segundo Piso: Call Center	
	144 puertos Fast Ethernet 8 puertos GigabitEthernet con 4 Converter GBIC incluido	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
DS1410001-3.1	Licencia de Software y Kit de Software del Switch de borde Passport 8100 (Incluye licencia, software Device Manager, y toda la documentación). Una licencia requerida por cada chasis del switch de borde . Versión 3.1.	1
DS1402001	Passport 8010 chassis de 10 slot. Incluye chassis, dual backplane, dos bandejas de ventiladores, cable RS232 para administración de consola, kit para montar en Rack y Kit guía cable. Requiere una o dos Fuentes de alimentación dependiendo de la configuración; Hasta tres fuentes de alimentación es soportada.	1
DS1405E01	Passport 8001PS fuente de alimentación de 100-240 VAC. Al menos una fuente de alimentación es requerida por cada chasis del Passport 8000. (Incluye cable de poder tipo Norte Americano)	3
DS1404014	Módulo de Administración Passport 8190SM Uno requerido por cada chasis del switch de borde Passport 8100 . Incluye kit de licencia de software del Switch de borde y tarjeta de memoria flash PCMCIA.	2
DS1404007	Módulo para el switch de borde Passport 8148TX. Interfase de conmutación Ethernet Capa 2 de 48 puertos autosensing 10BASE-T/100BASE-TX.	3
DS1404009	Módulo para el switch de borde Passport 8108GB de 8-puertos 1000 Base GBIC (GBICs son vendidos separadamente)	1
AA1419001	1-puerto 1000Base-SX Gigabit Interfase Converter (GBIC)	4

Tabla 5.1.6 Configuración de cada switch C.C.

El siguiente gráfico muestra la configuración de los 2 Equipos propuesto para este nodo.

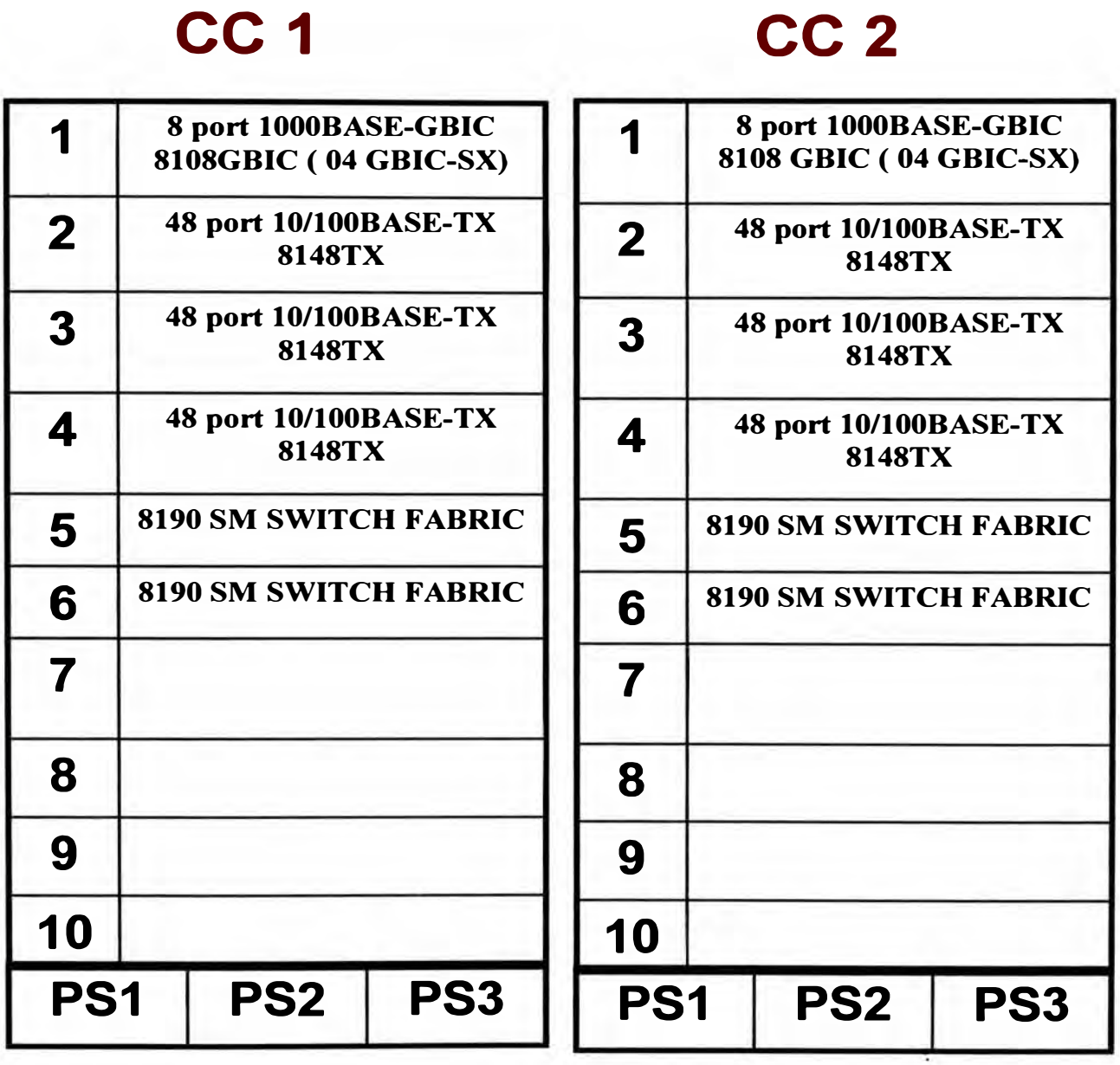


Figura 5.1.7. Configuración de los dos Switches CC Passport 8100 Capa 2 propuesto para el Call Center. Capacidad total instalada de 288 puertos 10/100BASE-TX y 16 puertos 1000BASE-GBIC

5.2. PLANIFICACIÓN DE VLANS

Las siguientes Tablas muestran la distribución de los puertos y las VLANs creadas sobre los switches. Donde

Id : significa la identificación de la VLAN.

Nombre: significa el Nombre de la VLAN

Tipo: El tipo de VLAN creada

Puertos Miembros : Los puertos del Switch que pertenecen a dicha VLAN. Donde **x/y** se lee como el puerto y del Modulo que esta en el slot x , **x/y-x/z** se lee como los puertos **y** hasta la **z** del Módulo que esta en el slot x .

Dirección IP : significa Dirección IP asignada a la VLAN que actúa semejante a una dirección de una interfase de Router virtual para la VLAN. Esta interfase de Router Virtual no tiene ninguna asociación con ningún puerto en particular, pero puede ser alcanzada a través de cualquiera de los puertos que pertenecen a dicha VLAN y es la dirección IP que sirve como gateway a través del cual un frame es ruteado fuera de la VLAN.

Máscara : Es la máscara que identifica a que subred pertenece la VLAN cuando el enrutamiento es configurado.

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
9	VLAN9	Por Puerto	1/1-1/2 2/1-2/5	172.19.9.8	255.255.255.0 (24 bits)	Conectado al RAS AS 5300
11	VLAN11	Por Puerto	1/1-1/2 2/6-2/10	172.19.11.8	255.255.255.0 (24 bits)	Conectado al Router WAN 7206
13	VLAN13	Por Puerto	1/1-1/2 2/11-2/15	172.19.13.8	255.255.255.0 (24 bits)	Conectado al Firewall.
50	VLAN50	Por Puerto	1/1-1/2	172.19.12.33	255.255.255.224 (27 bits)	Para Administración

Tabla 5.2.1 : Vlans creadas sobre el switch WAN 1

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
9	VLAN9	Por Puerto	1/1-1/2 2/1-2/5	172.19.9.9	255.255.255.0 (24 bits)	Conectado al RAS AS 5300
11	VLAN11	Por Puerto	1/1-1/2 2/6-2/10	172.19.11.9	255.255.255.0 (24 bits)	Conectado al Router WAN 7206
13	VLAN13	Por Puerto	1/1-1/2 2/11-2/15	172.19.13.9	255.255.255.0 (24 bits)	Conectado al Firewall.
50	VLAN50	Por Puerto	1/1-1/2	172.19.12.34	255.255.255.224 (27 bits)	Para Administración

Tabla 5.2.2 : Vlans creadas sobre el switch WAN 2

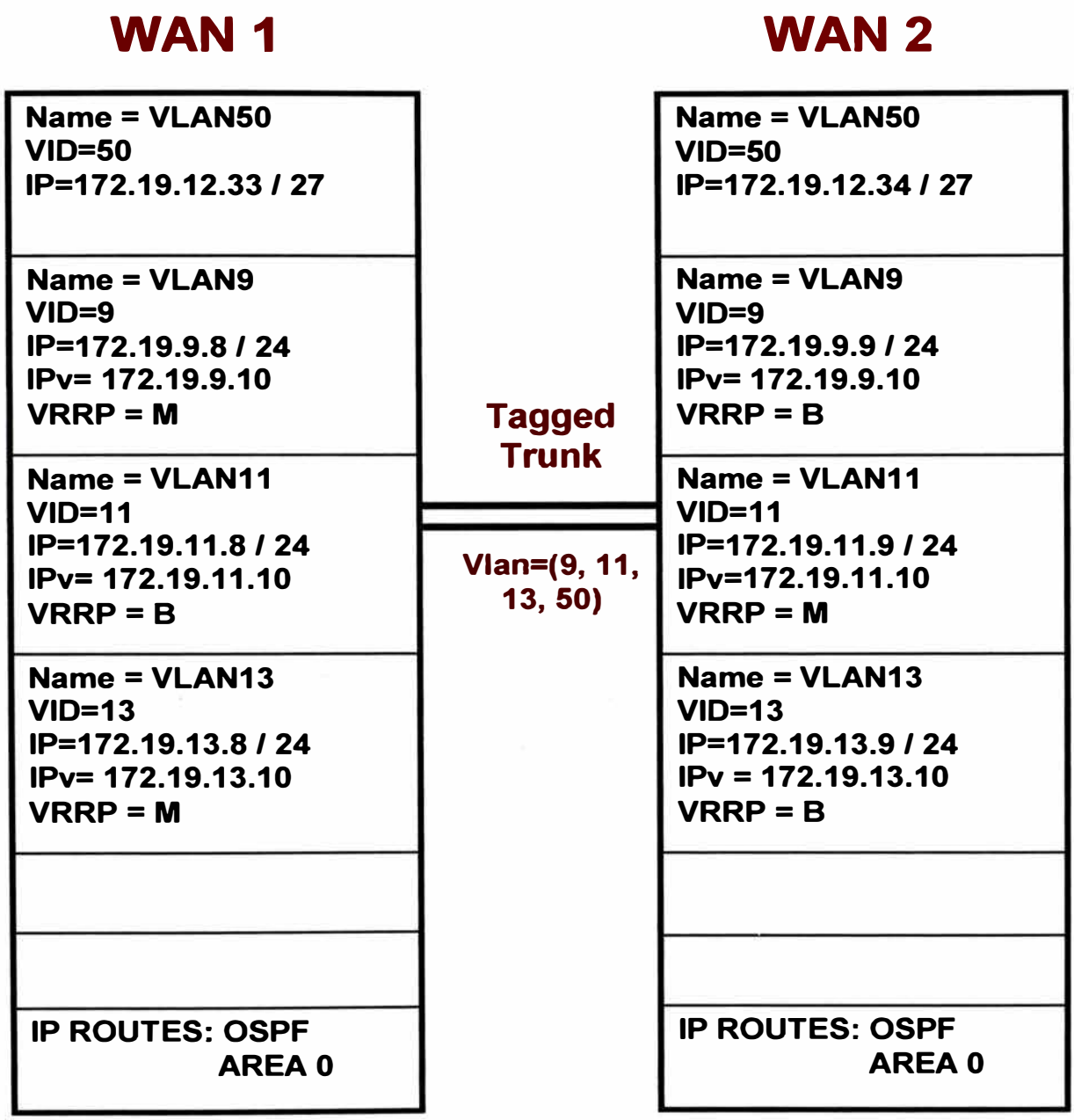


Figura 5.2.1 VLANs sobre los Switches WAN Passport 8600

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
101	VLAN101	Por Subred	1/1,1/4,1/6, 2/1,2/6, 3/1-3/48 4/1-4/48 7/1-7/48	172.19.1.8	255.255.255.0 (24 bits)	Para enlaces y usuarios del NOC
2	VLAN2	Por Subred	1/2,1/6, 2/2,2/6 3/1-3/48 4/1-4/48 7/1-7/48	172.19.2.8	255.255.255.0 (24 bits)	Para enlaces y usuarios de Customer Care (C:C)
3	VLAN3	Por Subred	1/6,2/6, 3/1-3/48 4/1-4/48 7/1-7/48	172.19.3.8	255.255.255.0 (24 bits)	Para Servidores
7	VLAN7	Por Puerto	2/6 1/5-1/6	172.19.7.8	255.255.255.0 (24 bits)	Conectado a la Red Nokia
10	VLAN10	Por Puerto	1/2,1/6, 2/2,2/6	172.19.10.8	255.255.255.0 (24 bits)	Para Enlaces y usuarios de GER
15	VLAN15	Por Puerto	1/1-1/2 2/11-2/15	172.19.15.8	255.255.255.0 (24 bits)	Para Servidores SAP.
51	VLAN51	Por Puerto	1/1-1/2	172.19.12.1	255.255.255.224 (27 bits)	Para Administra-ción

Tabla 5.2.3 : Vlans creadas sobre el switch CORE 1

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
101	VLAN101	Por Subred	1/1,1/4,1/6, 2/1,2/6, 3/1-3/48 4/1-4/48 7/1-7/48	172.19.1.9	255.255.255.0 (24 bits)	Para enlaces y usuarios del NOC
2	VLAN2	Por Subred	1/2,1/6, 2/2,2/6 3/1-3/48 4/1-4/48 7/1-7/48	172.19.2.9	255.255.255.0 (24 bits)	Para enlaces y usuarios de Customer Care (C:C)
3	VLAN3	Por Subred	1/6,2/6, 3/1-3/48 4/1-4/48 7/1-7/48	172.19.3.9	255.255.255.0 (24 bits)	Para Servidores
7	VLAN7	Por Puerto	2/6 1/5-1/6	172.19.7.9	255.255.255.0 (24 bits)	Conectado a la Red Nokia
10	VLAN10	Por Puerto	1/2,1/6, 2/2,2/6	172.19.10.9	255.255.255.0 (24 bits)	Para Enlaces y usuarios de GER,
15	VLAN15	Por Puerto	1/1-1/2 2/11-2/15	172.19.15.9	255.255.255.0 (24 bits)	Para Servidores SAP.
51	VLAN51	Por Puerto	1/1-1/2	172.19.12.2	255.255.255.224 (27 bits)	Para Administración

Tabla 5.2.4 : Vlans creadas sobre el switch CORE 2

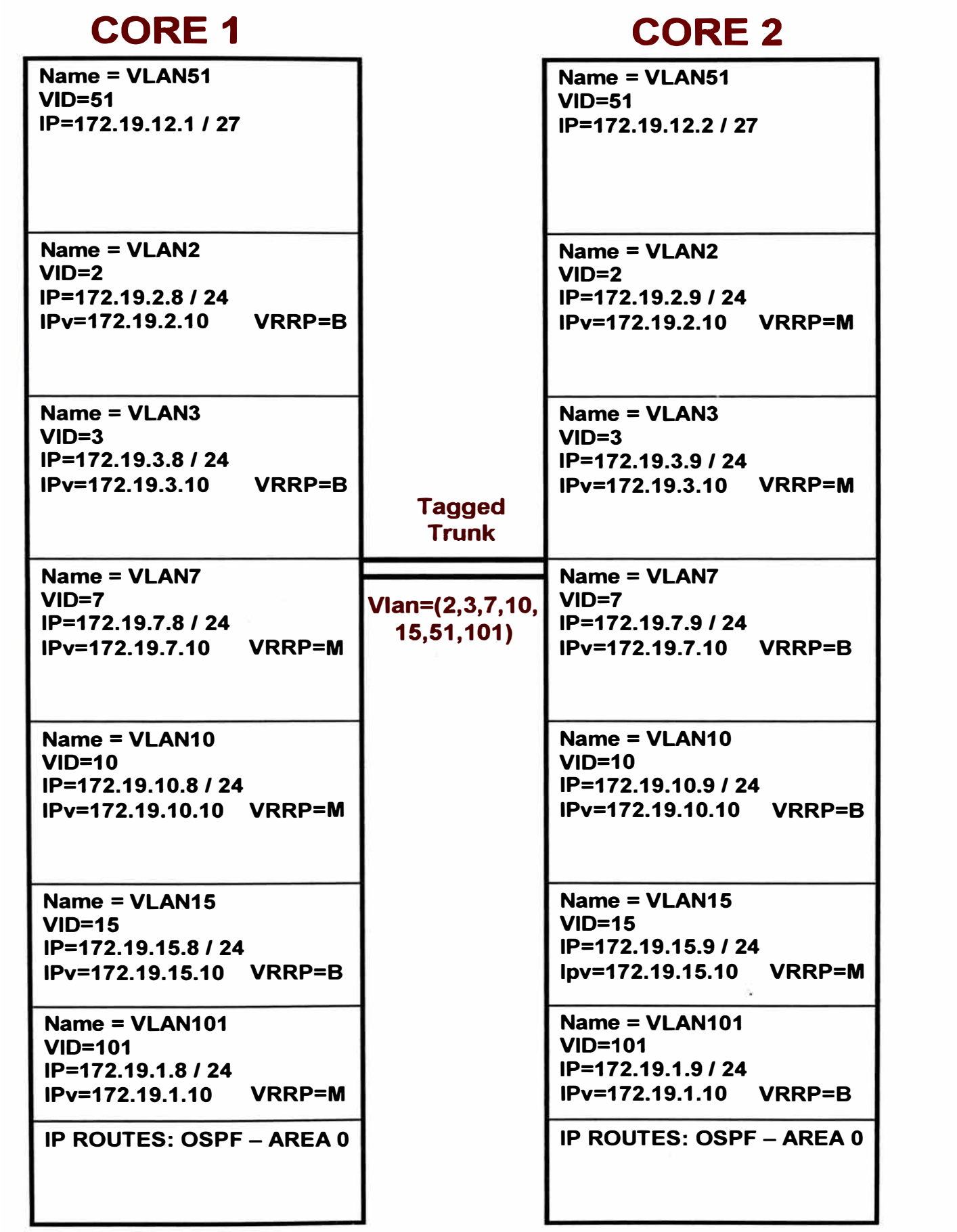


Figura 5.2.2 VLANs sobre los Switches CORE Passport 8600

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	1/1-1/8			
101	VLAN101	Por Puerto	1/1-1/2 2/1-2/48 3/1-3/48 4/1-4/48			Para enlaces y usuarios del NOC

Tabla 5.2.5 : Vlans creadas sobre el switch NOC 1

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	1/1-1/8			
101	VLAN101	Por Puerto	1/1-1/2 2/1-2/48 3/1-3/48 4/1-4/48			Para enlaces y usuarios del NOC

Tabla 5.2.6 : Vlans creadas sobre el switch NOC 2

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	1/1-1/8			
2	VLAN2	Por Puerto	1/1-1/2 2/1-2/48 3/1-3/48 4/1-4/48			Para enlaces y usuarios de Customer Care (C:C)

Tabla 5.2.7 : Vlans creadas sobre el switch CC 1

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	1/1-1/8			
2	VLAN2	Por Puerto	1/1-1/2 2/1-2/48 3/1-3/48 4/1-4/48			Para enlaces y usuarios de Customer Care (C:C)

Tabla 5.2.8 : Vlans creadas sobre el switch CC 2

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	1/1-1/8			
10	VLAN10	Por Puerto	1/1-1/2 2/1-2/48 3/1-3/48 4/1-4/48			Para Enlaces y usuarios de GER.

Tabla 5.2.9 : Vlans creadas sobre el switch GER 1

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Mascara	Comentario
1	VLAN1	Por Puerto	1/1-1/8			
10	VLAN10	Por Puerto	1/1-1/2 2/1-2/48 3/1-3/48 4/1-4/48			Para Enlaces y usuarios de GER.

Tabla 5.2.10 : Vlans creadas sobre el switch GER 2

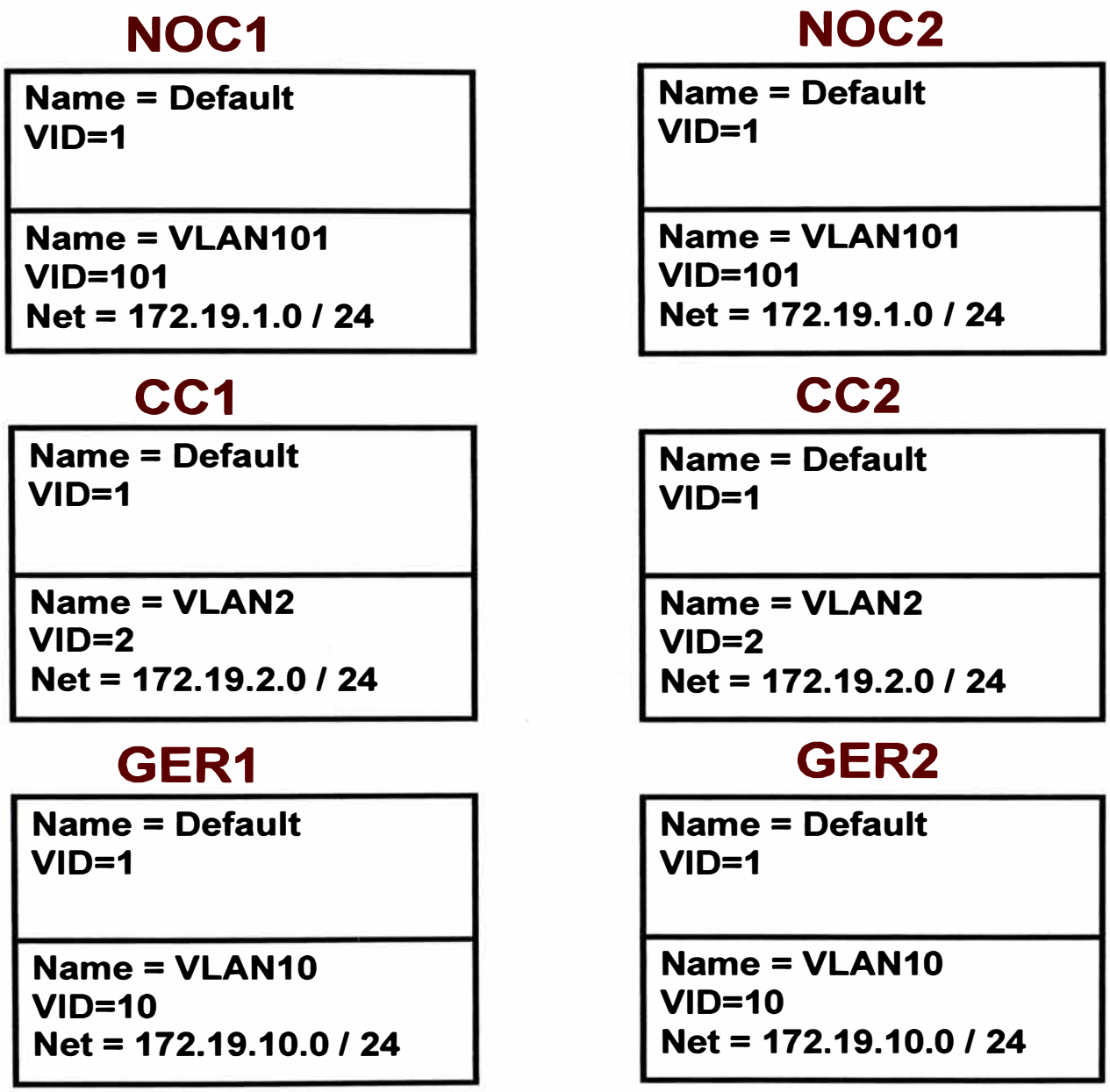


Figura 5.2.3 VLANs sobre los Switches de borde NOC,CC, GER Passport 8100

❑ CONFIGURACIÓN DEL MLT ENTRE LOS SWITCHES WAN

Las siguientes Tablas muestran los puertos troncales Multi-enlaces (Multi-Link Trunking o **MLT**) creados sobre los switches WAN. En este caso el MLT esta formado por 2 conexiones físicas Gigabit Ethernet entre los 2 switches WAN, el cual es visto como un solo enlace lógico de 2 gigabit Ethernet . Donde

Id : significa la identificación del MLT.

Nombre: significa el Nombre del MLT.

Tipo: El tipo de puerto creado (en este caso es Troncal). Además de ser Etiquetado (tagged) para extender las VLANs entre los switches WAN.

Puertos Miembros : Los puertos del Switch que pertenecen a dicho MLT. Donde x/y se lee como el puerto y del Modulo que esta en el slot x , x/y-x/z se lee como los puertos y hasta la z del Módulo que esta en el slot x .

Id del MLT	Nombre del MLT	Tipo de Puerto	Puertos Miembros	VLAN ID
1	WAN1-WAN2	TRUNK (tagged)	1/1-1/2	VLAN 9 VLAN 11 VLAN 13 VLAN 50

Tabla 5.2.11 : MLT creadas sobre el switch WAN 1

Id del MLT	Nombre del MLT	Tipo de Puerto	Puertos Miembros	VLAN ID
1	WAN2-WAN1	TRUNK (tagged)	1/1-1/2	VLAN 9 VLAN 11 VLAN 13 VLAN 50

Tabla 5.2.12 : MLT creadas sobre el switch WAN 2

Para mayor ilustración ver la figura 5.2.1 donde se muestra el Multilink Trunking creado entre los 2 Switches WAN donde los puertos MLT en ambos switches son etiquetados para esparcir las VLANs entre ambos switches.

- **CONFIGURACIÓN DEL MLT ENTRE LOS SWITCHES CORE**

Las siguientes Tablas muestran los puertos troncales Multi-enlaces (Multi-Link Trunking o **MLT**) creados sobre los switches CORE. En este caso el MLT esta formado por 2 conexiones físicas Gigabit Ethernet entre los 2 switches CORE, el cual es visto como un solo enlace lógico de 2 gigabit Ethernet . Aprovechamos que hay 2 módulos Gigabit Ethernet por cada Switch Core para tomar un puerto de cada módulo Gigabit Ethernet para que sean miembros de la troncal y así obtener un Distributed Multilink Trunking o DMLT. Donde

Id : significa la identificación del MLT.

Nombre: significa el Nombre del MLT.

Tipo: El tipo de puerto creado (en este caso es Troncal). Además de ser Etiquetado (tagged) para extender las VLANs entre los switches WAN.

Puertos Miembros : Los puertos del Switch que pertenecen a dicho MLT. Donde x/y se lee como el puerto y del Modulo que esta en el slot x , x/y-x/z se lee como los puertos y hasta la z del Módulo que esta en el slot x .

Id del MLT	Nombre del MLT	Tipo de Puerto	Puertos Miembros	VLAN ID
1	CORE1-CORE2	TRUNK (tagged)	1/6 2/6	VLAN 2 VLAN 3 VLAN 7 VLAN 10 VLAN 15 VLAN 51 VLAN 101

Tabla 5.2.13 : MLT creadas sobre el switch CORE 1

Id del MLT	Nombre del MLT	Tipo de Puerto	Puertos Miembros	VLAN ID
1	CORE2-CORE1	TRUNK (tagged)	1/6 2/6	VLAN 2 VLAN 3 VLAN 7 VLAN 10 VLAN 15 VLAN 51 VLAN 101

Tabla 5.2.14 : MLT creadas sobre el switch CORE 2

Para mayor ilustración ver la figura 5.2.2 donde se muestra el Multilink Trunking creado entre los 2 Switches CORE donde los puertos MLT en ambos switches son etiquetados para esparcir las VLANs entre ambos switches.

5.3. PLANIFICACIÓN DEL ESQUEMA DE DIRECCIONAMIENTO

La Tabla 5.3.1 muestra la dirección de red IP de cada subnet asociada a cada Vlan creada dentro de los switches y de otras Subredes que conforman la Red Corporativa .

Ambiente	Dirección IP	Máscara	Comentario
Estaciones de Trabajo del 1er Piso (NOC)- Tienda Externa	172.19.1.0	255.255.255.0 (24 bits)	VLAN101
Estaciones de Trabajo del 2do Piso Customer Care (C. C)	172.19.2.0	255.255.255.0 (24 bits)	VLAN2
Servidores	172.19.3.0	255.255.255.0 (24 bits)	VLAN3
Red Nokia	172.19.7.0	255.255.255.0 (24 bits)	VLAN7
RAS AS 5300	172.19.9.0	255.255.255.0 (24 bits)	VLAN9
Estaciones de Trabajo del 2do Piso Gerencias (GER)	172.19.10.0	255.255.255.0 (24 bits)	VLAN10
Router WAN 7206VXR	172.19.11.0	255.255.255.0 (24 bits)	VLAN11

Ambiente	Dirección IP	Máscara	Comentario
Administración de Switches	172.19.12.0	255.255.255.224 (27 bits)	VLAN50 VLAN51
Enrutamiento entre Switches	172.19.12.0	255.255.255.248 (29 bits)	Puertos BROUTERS en los Switches L3 CORE1, CORE2, WAN1, WAN2
Firewall	172.19.13.0	255.255.255.0 (24 bits)	VLAN13
Servidores SAP	172.19.15.0	255.255.255.0 (24 bits)	VLAN15
Red Nokia a SMS, IN, VMS, NMS1, NMS2	172.19.4.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA
Red Nokia a Estaciones de Trabajo	172.19.5.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA
Red Nokia a HLR, MSC, BSC	172.19.6.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA
Red Nokia a NMS1, NMS2	172.19.8.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA
Red Nokia a SMPR1	172.26.1.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA
Red Nokia a SMPR1	172.26.2.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA
Red Nokia a MS	172.25.2.0	255.255.255.0 (24 bits)	Subredes internas del a Red Lan de NOKIA

Tabla 5.3.1 : Plan Global de Direccionamiento IP

Para la comunicación entre las VLANs Subnet se habilitó el protocolo de enrutamiento OSPF en los Switches Capa 3 siendo la Red LAN de la Sede Tecnológica considerada como el AREA 0 de toda la Red WAN Corporativa.

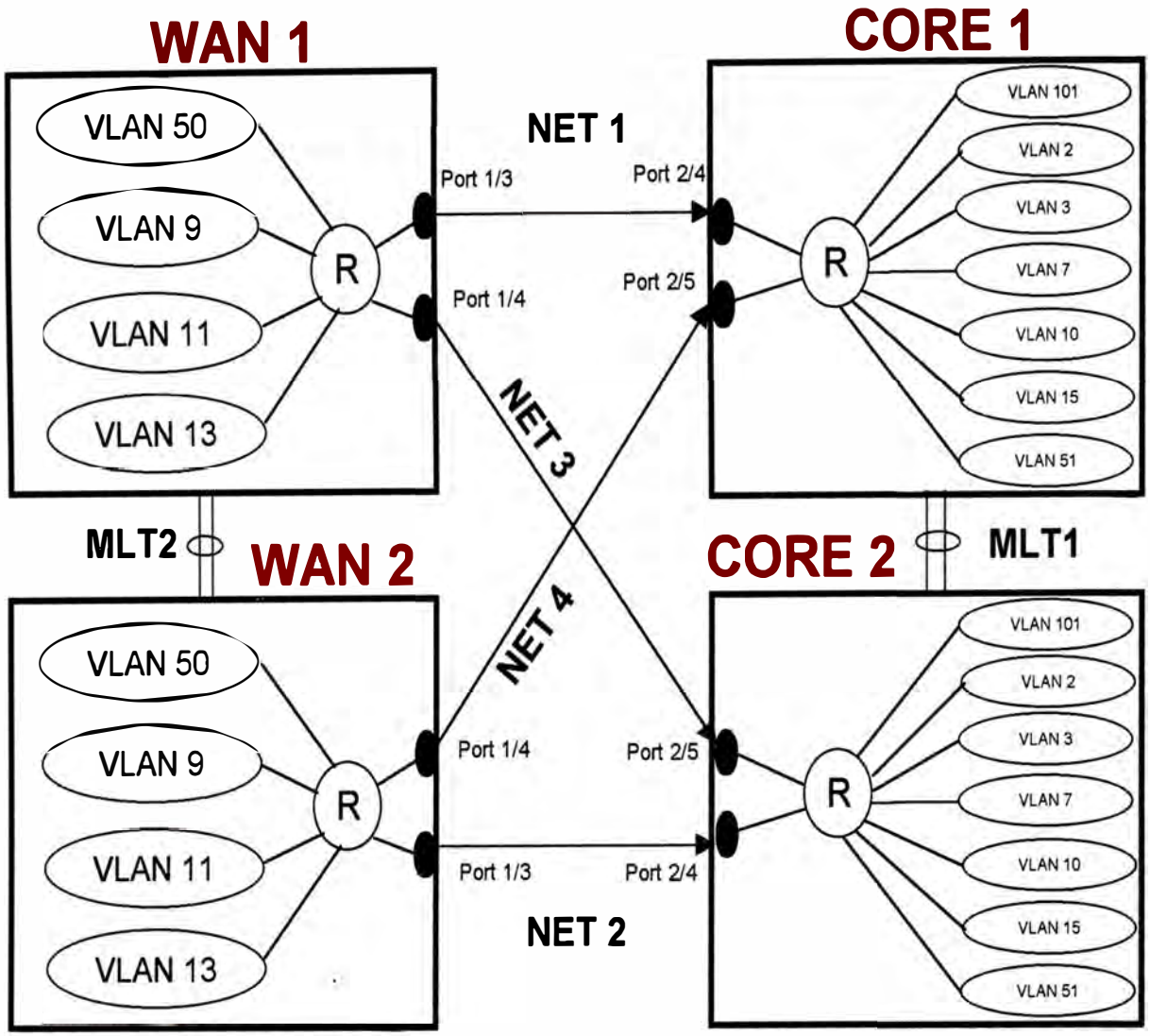
Para el enrutamiento entre los switches capa 3 WAN1 y WAN2 con los Switches CORE1 y CORE2 se empleó el concepto de puertos Brouter que son soportado por los switches Passport. Un puerto brouter es una VLAN de un único puerto que puede enrutar paquetes IP así como también conmutar (bridge) todo el trafico no enrutable .

La tabla 5.3.2 muestra las Subredes formada para los enlaces entre los Switches WAN1, WAN2 y los Switches CORE1 y CORE2, la dirección IP de la Subred y los puertos miembros de esas subredes con sus respectivas direcciones IP.

Nombre de la Subred	Dirección IP / Máscara	Puertos Miembros	Puertos Miembros	Coment.
NET 1	172.19.12.128 / 255.255.255.248 (29 bits)	1/3 (WAN1) 172.19.12.129 / 29	2/4 (CORE1) 172.19.12.130 / 29	Enlace entre Switches WAN1 y CORE1
NET 2	172.19.12.136 / 255.255.255.248 (29 bits)	1/3 (WAN2) 172.19.12.137 / 29	2/4 (CORE2) 172.19.12.138 / 29	Enlace entre Switches WAN2 y CORE2
NET 3	172.19.12.144 / 255.255.255.248 (29 bits)	1/4 (WAN1) 172.19.12.145 / 29	2/5 (CORE2) 172.19.12.146 / 29	Enlace entre Switches WAN1 y CORE2
NET 4	172.19.12.152 / 255.255.255.248 (29 bits)	1/4 (WAN2) 172.19.12.153 / 29	2/5 (CORE1) 172.19.12.154 / 29	Enlace entre Switches WAN2 y CORE1

Tabla 5.3.2 : Enrutamiento entre los Switches Capa 3 Passport 8600

La Figura 5.3.1 muestra el enrutamiento entre los switches capa 3 Passport 8600 .



Protocolo de enrutamiento : **OSPF**

IP de los Puertos Brouter :

NET 1 : 172.19.12.128 / 29

Port 1/3 (WAN1) : 172.19.12.129 / 29

Port 2/4 (CORE1) : 172.19.12.130 / 29

NET 2 : 172.19.12.136 / 29

Port 1/3 (WAN2) : 172.19.12.137 / 29

Port 2/4 (CORE2) : 172.19.12.138 / 29

NET 3 : 172.19.12.144 / 29

Port 1/4 (WAN1) : 172.19.12.145 / 29

Port 2/5 (CORE2) : 172.19.12.146 / 29

NET 4 : 172.19.12.152 / 29

Port 1/4 (WAN2) : 172.19.12.153 / 29

Port 2/5 (CORE1) :172.19.12.154 / 29

Fig. 5.3.1 Enrutamiento entre Switches PP8600

❑ CONFIGURACIÓN DEL VRRP ENTRE LOS SWITCHES CORE

Para la implementación del protocolo VRRP (Virtual Router Redundancy Protocol) el cual esta diseñado para eliminar el único punto de falla que puede ocurrir cuando el router gateway por default configurado estáticamente en las estaciones finales sea perdida. Estamos empleando el concepto de una IP virtual compartida que usa VRRP, entre los dos switches CORE de capa 3 que están conectando a las subredes en la red corporativa. Con esta dirección IP virtual como el default gateway de las estaciones finales, VRRP nos provee redundancia de gateway por default (defecto) en forma dinámica en el caso de una falla de uno de los switches de CORE.

La Tabla 5.3.3 muestra las IP virtuales creadas para las interfaces IP de las Vlans extendidas entre los Switches CORE para la implementación del VRRP para proveer redundancia de gateway por default a las estaciones conectadas a los Swiches de borde GER, NOC, C.C. Donde

VRID : significa la identificación del Router Virtual.

Dirección IP de la Interfase: significa la dirección IP de la interface real para las VLAN

Dirección IP Virtual: significa la dirección virtual creada para que sea el Default Gateway de las estaciones finales.

En la Tabla 5.3.3 se observa que la mayor prioridad usada para la elección del "master" entre los routers virtuales configurado en cada switch de CORE lo hemos seleccionado en forma alternada para proveer compartición de la carga del tráfico saliente entre los switches CORE1 y CORE2.

Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 2**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
CORE1	2	172.19.2.8 /24	172.19.2.10 /24	100	BACKUP
CORE2	2	172.19.2.9/24	172.19.2.10/24	200	MASTER
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 3**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
CORE1	3	172.19.3.8 /24	172.19.3.10 /24	100	BACKUP
CORE2	3	172.19.3.9/24	172.19.3.10/24	200	MASTER
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 7**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
CORE1	7	172.19.7.8 /24	172.19.7.10 /24	200	MASTER
CORE2	7	172.19.7.9/24	172.19.7.10/24	100	BACKUP
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 10**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
CORE1	10	172.19.10.8 /24	172.19.10.10 /24	200	MASTER
CORE2	10	172.19.10.9/24	172.19.10.10 /24	100	BACKUP

Nombre del Switch	Vrid	Dirección IP reales de las interfaces para la VLAN 15	Dirección IP virtual (Default Gateway para las Estaciones)	Prioridad	Estado
CORE1	15	172.19.15.8 /24	172.19.15.10 /24	100	BACKUP
CORE2	15	172.19.15.9/24	172.19.15.10 /24	200	MASTER
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 101**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
CORE1	101	172.19.1.8 /24	172.19.1.10 /24	200	MASTER
CORE2	101	172.19.1.9/24	172.19.1.10 /24	100	BACKUP

Tabla 5.3.3 :Implementación del VRRP entre los switches CORE 1 y CORE 2

La Figura 5.1.2 muestra la implementación del protocolo VRRP entre los switches CORE, capa 3 Passport 8600 con respecto a los Switches de borde Passport8000 capa 2 .

5.4. CONFIGURACIÓN DE LOS SWITCHES (PROGRAMACION)

A continuación se muestra la configuración del switch Passport 8600 WAN1, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH WAN 1**

```
WAN1:5# sh config
#
# WED SEP 19 18:38:33 2001 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot   1  8608GB  20325108  00000000    IO: GMAC= 4 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot   2  8648TX  20210130  00000000    IO: PLRO= 3 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot  3        00000001 00000000
# Slot  4        00000001 00000000
```

```
# Slot   5  8690SF  200e0100  00000000   CPU: CPLD=15 OP=2 TMUX=2
  SWIP=2 FAD=1 CF=11
# Slot   6  8690SF  200e0100  00000000   CPU: CPLD=15 OP=2 TMUX=2
   SWIP=2 FAD=1 CF=11
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10        00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "WAN1"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rwa XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
sys set snmp trap-recv 172.19.12.90 v1 public
sys set snmp trap-recv 172.19.14.249 v1 public
#
# LINK-FLAP-DETECT CONFIGURATION
#
```

```
sys link-flap-detect interval  60
# MLT CONFIGURATION
#
mlt 1 create
mlt 1 name "WAN1-WAN2"
mlt 1 perform-tagging enable
mlt 1 add ports 1/1-1/2
mlt 2 create
mlt 2 name "WAN1.1-WAN2.1"
mlt 2 perform-tagging enable
mlt 2 add ports 2/47-2/48
#
# STG CONFIGURATION
#
stg 1  add ports 1/1-1/2,2/47-2/48
stg 1  priority 10
#
# VLAN CONFIGURATION
#
vlan 1 add-mlt 1
vlan 1 add-mlt 2
vlan 1 ports remove 1/3-1/8,2/1-2/46 member portmember
vlan 9 create byport 1 name "VLAN9"
vlan 9 add-mlt 1
```

vlan 9 add-mlt 2

vlan 9 ports remove 1/3-1/8,2/6-2/46 member portmember

vlan 9 ports add 1/1-1/2,2/1-2/5,2/47-2/48 member portmember

vlan 9 ip create 172.19.9.8/255.255.255.0 mac_offset 3

vlan 9 ip ospf enable

vlan 9 ip ospf metric 10

vlan 9 ip vrrp 9 action none

vlan 9 ip vrrp 9 address 172.19.9.10

vlan 9 ip vrrp 9 priority 200

vlan 9 ip vrrp 9 enable

vlan 11 create byport 1 name "VLAN11"

vlan 11 add-mlt 1

vlan 11 add-mlt 2

vlan 11 ports remove 1/3-1/8,2/1-2/5,2/11-2/46 member portmember

vlan 11 ports add 1/1-1/2,2/6-2/10,2/47-2/48 member portmember

vlan 11 ip create 172.19.11.8/255.255.255.0 mac_offset 4

vlan 11 ip ospf enable

vlan 11 ip ospf metric 10

vlan 11 ip vrrp 11 action none

vlan 11 ip vrrp 11 address 172.19.11.10

vlan 11 ip vrrp 11 enable

vlan 13 create byport 1 name "VLAN13"

vlan 13 add-mlt 1

vlan 13 add-mlt 2

```
vlan 13 ports remove 1/3-1/8,2/1-2/10,2/16-2/46 member portmember
vlan 13 ports add 1/1-1/2,2/11-2/15,2/47-2/48 member portmember
vlan 13 ip create 172.19.13.8/255.255.255.0 mac_offset 5
vlan 13 ip ospf enable
vlan 13 ip ospf metric 10
vlan 13 ip vrrp 13 action none
vlan 13 ip vrrp 13 address 172.19.13.10
vlan 13 ip vrrp 13 enable
vlan 50 create byport 1 name "VLAN50"
vlan 50 add-mlt 1
vlan 50 add-mlt 2
vlan 50 ports remove 1/3-1/8,2/1-2/46 member portmember
vlan 50 ports add 1/1-1/2,2/47-2/48 member portmember
vlan 50 ip create 172.19.12.33/255.255.255.224 mac_offset 2
vlan 50 ip ospf metric 10
vlan 50 ip vrrp 50 action none
vlan 50 ip vrrp 50 address 172.19.12.40
vlan 50 ip vrrp 50 priority 200
vlan 50 ip vrrp 50 enable
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/3 ip create 172.19.12.129/255.255.255.252 1001 mac_offset 0
ethernet 1/3 ip ospf enable
```

```
ethernet 1/3 ip ospf metric 1
ethernet 1/3 stg 1 stp disable
ethernet 1/4 ip create 172.19.12.145/255.255.255.252 1002 mac_offset 1
ethernet 1/4 ip ospf enable
ethernet 1/4 ip ospf metric 1
ethernet 1/4 stg 1 stp disable
ethernet 2/47 stg 1 pathcost 65535
ethernet 2/48 stg 1 pathcost 65535

#
# IP & RIP CONFIGURATION
#

ip ip-supernet enable
ip static-route create 0.0.0.0/0.0.0.0 next-hop 172.19.13.20 cost 1
ip static-route create 172.19.4.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.19.5.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.19.6.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.19.7.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.19.8.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.25.0.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.26.1.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.26.2.0/255.255.255.0 next-hop 172.19.12.130 cost 1
ip static-route create 172.45.1.0/255.255.255.0 next-hop 172.19.11.252 cost 1
```

```
#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf router-id 3.0.0.0
ip ospf enable
#
back
```

A continuación se muestra la configuración del switch Passport 8600 WAN2, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH WAN 2**

```
WAN2:5# sh config
#
# WED SEP 19 18:46:02 2001 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
```

```
#
# Slot   1 8608GB 20325108 00000000    IO: GMAC= 4 OP=2 TMUX=2
         RARU=2 CPLD=4
# Slot   2 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot  3        00000001 00000000
# Slot  4        00000001 00000000
# Slot   5 8690SF 200e0100 00000000   CPU: CPLD=15 OP=2 TMUX=2
  SWIP=2 FAD=1 CF=11
# Slot   6 8690SF 200e0100 00000000   CPU: CPLD=15 OP=2 TMUX=2
  SWIP=2 FAD=1 CF=11
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10   --   00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "WAN2"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
```

```
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.1.100 v1 public
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
sys set snmp trap-recv 172.19.3.100 v1 public
sys set snmp trap-recv 172.19.12.90 v1 public
sys syslog host 1 create
sys syslog host 1 address 172.19.14.91
sys syslog host 1 host enable
sys syslog host 1 severity info warning error fatal
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# MLT CONFIGURATION
#
mlt 1 create
mlt 1 name "WAN2-WAN1"
mlt 1 perform-tagging enable
mlt 1 add ports 1/1-1/2
mlt 2 create
mlt 2 name "WAN2.1-WAN1.1"
mlt 2 perform-tagging enable
mlt 2 add ports 2/47-2/48
```

```
#
# STG CONFIGURATION
#
stg 1  add ports 1/1-1/2,2/47-2/48
stg 1  priority 20
#
# VLAN CONFIGURATION
#
vlan 1 add-mlt 1
vlan 1 add-mlt 2
vlan 1 ports remove 1/3-1/8,2/1-2/46 member portmember
vlan 9 create byport 1 name "VLAN9"
vlan 9 add-mlt 1
vlan 9 add-mlt 2
vlan 9 ports remove 1/3-1/8,2/6-2/46 member portmember
vlan 9 ports add 1/1-1/2,2/1-2/5,2/47-2/48 member portmember
vlan 9 ip create 172.19.9.9/255.255.255.0 mac_offset 2
vlan 9 ip ospf enable
vlan 9 ip ospf metric 10
vlan 9 ip vrrp 9 action none
vlan 9 ip vrrp 9 address 172.19.9.10
vlan 9 ip vrrp 9 enable
vlan 11 create byport 1 name "VLAN11"
vlan 11 add-mlt 1
```

```
vlan 11 add-mlt 2
vlan 11 ports remove 1/3-1/8,2/1-2/5,2/11-2/46 member portmember
vlan 11 ports add 1/1-1/2,2/6-2/10,2/47-2/48 member portmember
vlan 11 ip create 172.19.11.9/255.255.255.0 mac_offset 3
vlan 11 ip ospf enable
vlan 11 ip ospf metric 10
vlan 11 ip vrrp 11 action none
vlan 11 ip vrrp 11 address 172.19.11.10
vlan 11 ip vrrp 11 priority 200
vlan 11 ip vrrp 11 enable
vlan 13 create byport 1 name "VLAN13"
vlan 13 add-mlt 1
vlan 13 add-mlt 2
vlan 13 ports remove 1/3-1/8,2/1-2/10,2/16-2/46 member portmember
vlan 13 ports add 1/1-1/2,2/11-2/15,2/47-2/48 member portmember
vlan 13 ip create 172.19.13.9/255.255.255.0 mac_offset 4
vlan 13 ip ospf enable
vlan 13 ip ospf metric 10
vlan 13 ip vrrp 13 action none
vlan 13 ip vrrp 13 address 172.19.13.10
vlan 13 ip vrrp 13 priority 200
vlan 13 ip vrrp 13 enable
vlan 50 create byport 1 name "VLAN50"
vlan 50 add-mlt 1
```

```
vlan 50 add-mlt 2
vlan 50 ports remove 1/3-1/8,2/1-2/46 member portmember
vlan 50 ports add 1/1-1/2,2/47-2/48 member portmember
vlan 50 ip create 172.19.12.34/255.255.255.224 mac_offset 5
vlan 50 ip ospf metric 10
vlan 50 ip vrrp 50 action none
vlan 50 ip vrrp 50 address 172.19.12.40
vlan 50 ip vrrp 50 enable
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/3 ip create 172.19.12.137/255.255.255.252 1001 mac_offset 0
ethernet 1/3 ip ospf enable
ethernet 1/3 ip ospf metric 1
ethernet 1/3 stg 1 stp disable
ethernet 1/4 ip create 172.19.12.153/255.255.255.252 1002 mac_offset 1
ethernet 1/4 ip ospf enable
ethernet 1/4 ip ospf metric 1
ethernet 1/4 stg 1 stp disable
ethernet 2/47 stg 1 pathcost 1
ethernet 2/48 stg 1 pathcost 1
#
ip static-route create 0.0.0.0/0.0.0.0 next-hop 172.19.13.20 cost 1
ip static-route create 172.19.4.0/255.255.255.0 next-hop 172.19.12.154 cost 5
```

```
ip static-route create 172.19.5.0/255.255.255.0 next-hop 172.19.12.154 cost 5
ip static-route create 172.19.6.0/255.255.255.0 next-hop 172.19.12.154 cost 5
ip static-route create 172.19.7.0/255.255.255.0 next-hop 172.19.12.154 cost 5
ip static-route create 172.19.8.0/255.255.255.0 next-hop 172.19.12.154 cost 5
ip static-route create 172.25.0.0/255.255.255.0 next-hop 172.19.12.154 cost 5
ip static-route create 172.25.1.0/255.255.255.0 next-hop 172.19.12.154 cost 5
ip static-route create 172.26.1.0/255.255.255.0 next-hop 172.19.12.154 cost 1
ip static-route create 172.26.2.0/255.255.255.0 next-hop 172.19.12.154 cost 1
ip static-route create 172.45.1.0/255.255.255.0 next-hop 172.19.11.252 cost 1
#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf router-id 4.0.0.0
ip ospf enable
#
back
```

A continuación se muestra la configuración del switch Passport 8600 CORE1 mediante la salida del comando de línea “show config”:.

- **CONFIGURACIÓN DEL SWITCH CORE 1**

```
CORE1:5# sh config
#
# WED SEP 19 18:53:03 2001 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot   1 8608GB 20325108 00000000    IO: GMAC= 5 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot   2 8608GB 20325108 00000000    IO: GMAC= 5 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot   3 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot   4 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
  RARU=2 CPLD=4
# Slot   5 8690SF 200e0100 00000000  CPU: CPLD=15 OP=2 TMUX=2
  SWIP=2 FAD=1 CF=11
```

```
# Slot   6  8690SF  200e0100  00000000   CPU: CPLD=15 OP=2 TMUX=2
  SWIP=2 FAD=1 CF=11
# Slot   7  8648TX  20210130  00000000    IO: PLRO= 3 OP=2 TMUX=2
   RARU=2 CPLD=4
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10        00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "CORE1"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp community rwa XXX-NET
sys set snmp trap-recv 172.19.1.249 v1 public
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
sys set snmp trap-recv 172.19.12.90 v1 public
sys syslog host 1 create
sys syslog host 1 address 172.19.14.91
sys syslog host 1 host enable
```

```
sys syslog host 1 severity info warning error fatal
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
ethernet 1/3 perform-tagging enable
ethernet 2/1 perform-tagging enable
ethernet 2/2 perform-tagging enable
ethernet 2/3 perform-tagging enable
#
# MLT CONFIGURATION
#
 mlt 1 create
 mlt 1 name "CORE1-CORE2"
 mlt 1 perform-tagging enable
 mlt 1 add ports 1/6,2/6
 mlt 2 create
 mlt 2 name "CORE1.1-CORE2.1"
 mlt 2 perform-tagging enable
```

```
mlt 2 add ports 7/47-7/48
#
# STG CONFIGURATION
#
stg 1  add ports 1/6,2/6,7/47-7/48
stg 1  priority 10
#
# VLAN CONFIGURATION
#
vlan 1 add-mlt 1
vlan 1 add-mlt 2
vlan 1 ports remove 1/4-1/5,1/7-1/8,2/4-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-
7/46 member portmember
vlan 2 create byipsubnet 1 172.19.2.0/255.255.255.0 name "VLAN2"
vlan 2 add-mlt 1
vlan 2 add-mlt 2
vlan 2 ports remove 1/1,1/3-1/5,1/7-1/8,2/1,2/3-2/5,2/7-2/8 member
portmember
vlan 2 ports add 1/2,1/6,2/2,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member
 portmember
vlan 2 ports add 1/2,1/6,2/2,2/6,7/47-7/48 member static
vlan 2 ip create 172.19.2.8/255.255.255.0 mac_offset 4
vlan 2 ip ospf enable
vlan 2 ip ospf metric 10
```

vlan 2 ip vrrp 2 action none

vlan 2 ip vrrp 2 address 172.19.2.10

vlan 2 ip vrrp 2 enable

vlan 3 create byipsubnet 1 172.19.3.0/255.255.255.0 name "VLAN3"

vlan 3 add-mlt 1

vlan 3 add-mlt 2

vlan 3 ports remove 1/1-1/5,1/7-1/8,2/1-2/5,2/7-2/8 member portmember

vlan 3 ports add 1/6,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember

vlan 3 ports add 1/6,2/6,7/47-7/48 member static

vlan 3 ip create 172.19.3.8/255.255.255.0 mac_offset 6

vlan 3 ip ospf enable

vlan 3 ip ospf metric 10

vlan 3 ip vrrp 3 action none

vlan 3 ip vrrp 3 address 172.19.3.10

vlan 3 ip vrrp 3 enable

vlan 7 create byport 1 name "VLAN7"

vlan 7 add-mlt 1

vlan 7 add-mlt 2

vlan 7 ports remove 1/1-1/4,1/7-1/8,2/1-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember

vlan 7 ports add 1/5-1/6,2/6,7/47-7/48 member portmember

vlan 7 ip create 172.19.7.8/255.255.255.0 mac_offset 7

vlan 7 ip ospf metric 10

vlan 7 ip vrrp 7 action none

vlan 7 ip vrrp 7 address 172.19.7.10

vlan 7 ip vrrp 7 priority 200

vlan 7 ip vrrp 7 enable

vlan 10 create byport 1 name "VLAN10"

vlan 10 add-mlt 1

vlan 10 add-mlt 2

vlan 10 ports remove 1/1-1/2,1/4-1/5,1/7-1/8,2/1-2/2,2/4-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember

vlan 10 ports add 1/3,1/6,2/3,2/6,7/47-7/48 member portmember

vlan 10 ip create 172.19.10.8/255.255.255.0 mac_offset 5

vlan 10 ip ospf enable

vlan 10 ip ospf metric 10

vlan 10 ip vrrp 10 action none

vlan 10 ip vrrp 10 address 172.19.10.10

vlan 10 ip vrrp 10 priority 200

vlan 10 ip vrrp 10 enable

vlan 15 create byipsubnet 1 172.19.15.0/255.255.255.0 name "VLAN15"

vlan 15 add-mlt 1

vlan 15 add-mlt 2

vlan 15 ports remove 1/1-1/5,1/7-1/8,2/1-2/5,2/7-2/8 member portmember

vlan 15 ports add 1/6,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember

vlan 15 ports add 1/6,2/6,7/47-7/48 member static

vlan 15 ip create 172.19.15.8/255.255.255.0 mac_offset 8

vlan 15 ip ospf enable

vlan 15 ip ospf metric 10

vlan 15 ip vrrp 15 action none

vlan 15 ip vrrp 15 address 172.19.15.10

vlan 15 ip vrrp 15 enable

vlan 51 create byport 1 name "VLAN51"

vlan 51 add-mlt 1

vlan 51 add-mlt 2

vlan 51 ports remove 1/4-1/5,1/7-1/8,2/4-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember

vlan 51 ports add 1/1-1/3,1/6,2/1-2/3,2/6,7/47-7/48 member portmember

vlan 51 ip create 172.19.12.1/255.255.255.224 mac_offset 2

vlan 51 ip ospf metric 10

vlan 101 create byipsubnet 1 172.19.1.0/255.255.255.0 name "VLAN101"

vlan 101 add-mlt 1

vlan 101 add-mlt 2

vlan 101 ports remove 1/2-1/3,1/5,1/7-1/8,2/2-2/5,2/7-2/8 member portmember

vlan 101 ports add 1/1,1/4,1/6,2/1,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember

vlan 101 ports add 1/1,1/4,1/6,2/1,2/6,7/47-7/48 member static

vlan 101 ip create 172.19.1.8/255.255.255.0 mac_offset 3

vlan 101 ip ospf enable

vlan 101 ip ospf metric 10

```
vlan 101 ip vrrp 101 action none
vlan 101 ip vrrp 101 address 172.19.1.10
vlan 101 ip vrrp 101 priority 200
vlan 101 ip vrrp 101 enable

#
# PORT CONFIGURATION - PHASE II
#
ethernet 2/4 ip create 172.19.12.130/255.255.255.252 1001 mac_offset 0
ethernet 2/4 ip ospf enable
ethernet 2/4 ip ospf metric 1
ethernet 2/4 stg 1 stp disable
ethernet 2/5 ip create 172.19.12.154/255.255.255.252 1002 mac_offset 1
ethernet 2/5 ip ospf enable
ethernet 2/5 ip ospf metric 1
ethernet 2/5 stg 1 stp disable
ethernet 7/47 auto-negotiate disable
ethernet 7/47 speed 100
ethernet 7/47 duplex full
ethernet 7/48 auto-negotiate disable
ethernet 7/48 speed 100
ethernet 7/48 duplex full

#
```

```
ip static-route create 0.0.0.0/0.0.0.0 next-hop 172.19.12.153 cost 1
ip static-route create 172.19.4.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.5.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.6.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.8.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.9.0/255.255.255.0 next-hop 172.19.12.129 cost 1
ip static-route create 172.25.0.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.25.2.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.26.1.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.26.2.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.45.1.0/255.255.255.0 next-hop 172.19.12.129 cost 1
#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf router-id 1.0.0.0
ip ospf enable
#
back
```

A continuación se muestra la configuración del switch Passport 8600 CORE2, mediante la salida del comando de línea “show config”:.

- **CONFIGURACIÓN DEL SWITCH CORE 2**

```
CORE2:5# sh config
#
# WED SEP 19 19:02:18 2001 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot   1 8608GB 20325108 00000000    IO: GMAC= 4 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   2 8608GB 20325108 00000000    IO: GMAC= 4 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   3 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   4 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   5 8690SF 200e0100 00000000   CPU: CPLD=15 OP=2 TMUX=2
SWIP=2 FAD=1 CF=11
```

```
# Slot   6  8690SF  200e0100  00000000   CPU:  CPLD=15  OP=2  TMUX=2
SWIP=2 FAD=1 CF=11
# Slot   7  8648TX  20210130  00000000    IO:  PLRO= 3  OP=2  TMUX=2
RARU=2 CPLD=4
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10        00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "CORE2"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rwa XXX-NET
sys set snmp trap-recv 172.19.1.230 v1 public
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
sys set snmp trap-recv 172.19.12.90 v1 public
sys syslog host 1 create
sys syslog host 1 address 172.19.14.91
sys syslog host 1 host enable
sys syslog host 1 severity info warning error fatal
```

```
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
ethernet 1/3 perform-tagging enable
ethernet 2/1 perform-tagging enable
ethernet 2/2 perform-tagging enable
ethernet 2/3 perform-tagging enable
#
# MLT CONFIGURATION
#
mlt 1 create
mlt 1 name "CORE2-CORE1"
mlt 1 perform-tagging enable
mlt 1 add ports 1/6,2/6
mlt 2 create
mlt 2 name "CORE2.1-CORE1.1"
mlt 2 perform-tagging enable
mlt 2 add ports 7/47-7/48
```

```
#
# STG CONFIGURATION
#
stg 1  add ports 1/6,2/6,7/47-7/48
stg 1  priority 20
#
# VLAN CONFIGURATION
#
vlan 1 add-mlt 1
vlan 1 add-mlt 2
vlan 1 ports remove 1/4-1/5,1/7-1/8,2/4-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember
vlan 2 create byipsubnet 1 172.19.2.0/255.255.255.0 name "VLAN2"
vlan 2 add-mlt 1
vlan 2 add-mlt 2
vlan 2 ports remove 1/1,1/3-1/5,1/7-1/8,2/1,2/3-2/5,2/7-2/8 member portmember
vlan 2 ports add 1/2,1/6,2/2,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember
vlan 2 ports add 1/2,1/6,2/2,2/6,7/47-7/48 member static
vlan 2 ip create 172.19.2.9/255.255.255.0 mac_offset 4
vlan 2 ip ospf enable
vlan 2 ip ospf metric 10
vlan 2 ip vrrp 2 action none
```

vlan 2 ip vrrp 2 address 172.19.2.10

vlan 2 ip vrrp 2 priority 200

vlan 2 ip vrrp 2 enable

vlan 3 create byipsubnet 1 172.19.3.0/255.255.255.0 name "VLAN3"

vlan 3 add-mlt 1

vlan 3 add-mlt 2

vlan 3 ports remove 1/1-1/5,1/7-1/8,2/1-2/5,2/7-2/8 member portmember

vlan 3 ports add 1/6,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember

vlan 3 ports add 1/6,2/6,7/47-7/48 member static

vlan 3 ip create 172.19.3.9/255.255.255.0 mac_offset 6

vlan 3 ip ospf enable

vlan 3 ip ospf metric 10

vlan 3 ip vrrp 3 action none

vlan 3 ip vrrp 3 address 172.19.3.10

vlan 3 ip vrrp 3 priority 200

vlan 3 ip vrrp 3 enable

vlan 7 create byport 1 name "VLAN7"

vlan 7 add-mlt 1

vlan 7 add-mlt 2

vlan 7 ports remove 1/1-1/4,1/7-1/8,2/1-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember

vlan 7 ports add 1/5-1/6,2/6,7/47-7/48 member portmember

vlan 7 ip create 172.19.7.9/255.255.255.0 mac_offset 7

vlan 7 ip ospf metric 10

vlan 7 ip vrrp 7 action none

vlan 7 ip vrrp 7 address 172.19.7.10

vlan 7 ip vrrp 7 enable

vlan 10 create byport 1 name "VLAN10"

vlan 10 add-mlt 1

vlan 10 add-mlt 2

vlan 10 ports remove 1/1-1/2,1/4-1/5,1/7-1/8,2/1-2/2,2/4-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember

vlan 10 ports add 1/3,1/6,2/3,2/6,7/47-7/48 member portmember

vlan 10 ip create 172.19.10.9/255.255.255.0 mac_offset 5

vlan 10 ip ospf enable

vlan 10 ip ospf metric 10

vlan 10 ip vrrp 10 action none

vlan 10 ip vrrp 10 address 172.19.10.10

vlan 10 ip vrrp 10 enable

vlan 15 create byipsubnet 1 172.19.15.0/255.255.255.0 name "VLAN15"

vlan 15 add-mlt 1

vlan 15 add-mlt 2

vlan 15 ports remove 1/1-1/5,1/7-1/8,2/1-2/5,2/7-2/8 member portmember

vlan 15 ports add 1/6,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember

vlan 15 ports add 1/6,2/6,7/47-7/48 member static

vlan 15 ip create 172.19.15.9/255.255.255.0 mac_offset 8

vlan 15 ip ospf enable

vlan 15 ip ospf metric 10

vlan 15 ip vrrp 15 action none

vlan 15 ip vrrp 15 address 172.19.15.10

vlan 15 ip vrrp 15 priority 200

vlan 15 ip vrrp 15 enable

vlan 51 create byport 1 name "VLAN51"

vlan 51 add-mlt 1

vlan 51 add-mlt 2

vlan 51 ports remove 1/4-1/5,1/7-1/8,2/4-2/5,2/7-2/8,3/1-3/48,4/1-4/48,7/1-7/46 member portmember

vlan 51 ports add 1/1-1/3,1/6,2/1-2/3,2/6,7/47-7/48 member portmember

vlan 51 ip create 172.19.12.2/255.255.255.224 mac_offset 2

vlan 51 ip ospf metric 10

vlan 101 create byipsubnet 1 172.19.1.0/255.255.255.0 name "VLAN101"

vlan 101 add-mlt 1

vlan 101 add-mlt 2

vlan 101 ports remove 1/2-1/3,1/5,1/7-1/8,2/2-2/5,2/7-2/8 member portmember

vlan 101 ports add 1/1,1/4,1/6,2/1,2/6,3/1-3/48,4/1-4/48,7/1-7/48 member portmember

vlan 101 ports add 1/1,1/4,1/6,2/1,2/6,7/47-7/48 member static

vlan 101 ip create 172.19.1.9/255.255.255.0 mac_offset 3

vlan 101 ip ospf enable

vlan 101 ip ospf metric 10

vlan 101 ip vrrp 101 action none

```
vlan 101 ip vrrp 101 address 172.19.1.10
vlan 101 ip vrrp 101 enable
#
# PORT CONFIGURATION - PHASE II
#
ethernet 2/4 ip create 172.19.12.138/255.255.255.252 1001 mac_offset 0
ethernet 2/4 ip ospf enable
ethernet 2/4 ip ospf metric 1
ethernet 2/4 stg 1 stp disable
ethernet 2/5 ip create 172.19.12.146/255.255.255.252 1002 mac_offset 1
ethernet 2/5 ip ospf enable
ethernet 2/5 ip ospf metric 1
ethernet 2/5 stg 1 stp disable
ethernet 7/47 auto-negotiate disable
ethernet 7/47 speed 100
ethernet 7/47 duplex full
ethernet 7/47 stg 1 pathcost 1
ethernet 7/48 auto-negotiate disable
ethernet 7/48 speed 100
ethernet 7/48 duplex full
ethernet 7/48 stg 1 pathcost 1
#
ip static-route create 0.0.0.0/0.0.0.0 next-hop 172.19.12.137 cost 1
ip static-route create 172.19.4.0/255.255.255.0 next-hop 172.19.7.1 cost 1
```

```
ip static-route create 172.19.5.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.6.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.8.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.19.9.0/255.255.255.0 next-hop 172.19.12.145 cost 1
ip static-route create 172.25.0.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.25.2.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.26.1.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.26.2.0/255.255.255.0 next-hop 172.19.7.1 cost 1
ip static-route create 172.45.1.0/255.255.255.0 next-hop 172.19.12.145 cost 1
#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf router-id 2.0.0.0
ip ospf enable

#

back
```

A continuación se muestra la configuración del switch Passport 8100 NOC 1, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH NOC 1**

```
NOC1:5# sho config
#
# WED APR 22 17:20:39 1998 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot  1 8108GB 30325108 00000000
# Slot  2 8148TX 30210130 00000000
# Slot  3 8148TX 30210130 00000000
# Slot  4 8148TX 30210130 00000000
# Slot  5 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  6 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10   --   00000001 00000000
config
#
```

```
# CLI CONFIGURATION
#
cli prompt "NOC1"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
sys set snmp trap-recv 172.19.3.100 v1 public
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
#
# VLAN CONFIGURATION
#
vlan 1 ports remove 2/1-2/48,3/1-3/48,4/1-4/48 member portmember
vlan 101 create byport 1 name "VLAN101"
```

vlan 101 ports remove 1/3-1/8 member portmember

vlan 101 ports add 1/1-1/2,2/1-2/48,3/1-3/48,4/1-4/48 member portmember

#

PORT CONFIGURATION - PHASE II

#

ethernet 1/2 stg 1 pathcost 200

#

back

A continuación se muestra la configuración del switch Passport 8100 NOC 2, mediante la salida del comando de linea "show config":.

- **CONFIGURACIÓN DEL SWITCH NOC 2**

NOC2:5# show config

#

THU APR 30 23:16:59 1998 UTC

box type : Passport-8010

software version : 3.1.2.0

monitor version : 3.1.2.0/011

#

Asic Info :

SlotNum|Name |CardType|MdaType |Parts Description

#

```
# Slot  1 8108GB 30325108 00000000
# Slot  2 8148TX 30210130 00000000
# Slot  3 8148TX 30210130 00000000
# Slot  4 8148TX 30210130 00000000
# Slot  5 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  6 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10   --   00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "NOC2"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
#
# LINK-FLAP-DETECT CONFIGURATION
#
```

```
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
#
#
# VLAN CONFIGURATION
#
vlan 1 ports remove 2/1-2/48,3/1-3/48,4/1-4/48 member portmember
vlan 101 create byport 1 name "VLAN101"
vlan 101 ports remove 1/3-1/8 member portmember
vlan 101 ports add 1/1-1/2,2/1-2/48,3/1-3/48,4/1-4/48 member portmember
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/2 stg 1 pathcost 200
#
back
```

A continuación se muestra la configuración del switch Passport 8100 C.C. 1, mediante la salida del comando de línea “show config”:.

- **CONFIGURACIÓN DEL SWITCH C.C. 1**

```
CC1:5# show config
#
# FRI JUL 03 07:46:27 1998 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot  1 8108GB 30325108 00000000
# Slot  2 8148TX 30210130 00000000
# Slot  3 8148TX 30210130 00000000
# Slot  4 8148TX 30210130 00000000
# Slot  5 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  6 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10        00000001 00000000
```

```
config
#
# CLI CONFIGURATION
#
cli prompt "CC1"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
sys set snmp trap-recv 172.19.3.100 v1 public
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
#
# VLAN CONFIGURATION
#
```

```
vlan 1 ports remove 2/1-2/48,3/1-3/48,4/1-4/48 member portmember
vlan 2 create byport 1 name "VLAN2"
vlan 2 ports remove 1/3-1/8 member portmember
vlan 2 ports add 1/1-1/2,2/1-2/48,3/1-3/48,4/1-4/48 member portmember
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/2 stg 1 pathcost 200
#
back
```

A continuación se muestra la configuración del switch Passport 8100 C.C. 2, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH C.C. 2**

```
CC2:5# show config
#
# FRI MAY 15 19:35:44 1998 UTC
# box type          : Passport-8010
# software version  : 3.1.2.0
# monitor version   : 3.1.2.0/011
#
# Asic Info :
```

```
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot  1 8108GB 30325108 00000000
# Slot  2 8148TX 30210130 00000000
# Slot  3 8148TX 30210130 00000000
# Slot  4 8148TX 30210130 00000000
# Slot  5 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  6 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  7         00000001 00000000
# Slot  8         00000001 00000000
# Slot  9         00000001 00000000
# Slot 10         00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "CC2"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
#
```

```
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
#
# VLAN CONFIGURATION
#
vlan 1 ports remove 2/1-2/48,3/1-3/48,4/1-4/48 member portmember
vlan 2 create byport 1 name "VLAN2"
vlan 2 ports remove 1/3-1/8 member portmember
vlan 2 ports add 1/1-1/2,2/1-2/48,3/1-3/48,4/1-4/48 member portmember
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/2 stg 1 pathcost 200
#
back
```

A continuación se muestra la configuración del switch Passport 8100 GER 1, mediante la salida del comando de linea “show config”:.

- **CONFIGURACIÓN DEL SWITCH GER 1**

```
GER1:5# show config
#
# THU MAY 14 21:08:18 1998 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot  1 8108GB 30325108 00000000
# Slot  2 8148TX 30210130 00000000
# Slot  3 8148TX 30210130 00000000
# Slot  4 8148TX 30210130 00000000
# Slot  5 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  6 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10        00000001 00000000
config
```

```
#
# CLI CONFIGURATION
#
cli prompt "GER1"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
#
#
# VLAN CONFIGURATION
#
vlan 1 ports remove 2/1-2/48,3/1-3/48,4/1-4/48 member portmember
```

```
vlan 10 create byport 1 name "VLAN10"
vlan 10 ports remove 1/3-1/8 member portmember
vlan 10 ports add 1/1-1/2,2/1-2/48,3/1-3/48,4/1-4/48 member portmember
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/2 stg 1 pathcost 200
#
back
```

A continuación se muestra la configuración del switch Passport 8100 GER 2, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH GER 2**

```
GER2:5# sho config
#
# THU JAN 01 00:06:25 1998 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
```

```
#
# Slot  1 8108GB 30325108 00000000
# Slot  2 8148TX 30210130 00000000
# Slot  3 8148TX 30210130 00000000
# Slot  4 8148TX 30210130 00000000
# Slot  5 8190SM 200e0100 00000000  CPU: CPLD=15
# Slot  6 8190SM 200e0100 00000000  CPU: CPLD= 0
# Slot  7         00000001 00000000
# Slot  8         00000001 00000000
# Slot  9         00000001 00000000
# Slot 10         00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "GER2"
#
# SYSTEM CONFIGURATION
#
sys set snmp community ro XXX-RO
sys set snmp community rw XXX-NET
sys set snmp trap-recv 172.19.3.81 v2c XXX-NET
#
# LINK-FLAP-DETECT CONFIGURATION
```

```
#
sys link-flap-detect interval  60
#
# PORT CONFIGURATION - PHASE I
#
ethernet 1/1 perform-tagging enable
ethernet 1/2 perform-tagging enable
#
# VLAN CONFIGURATION
#
vlan 1 ports remove 2/1-2/48,3/1-3/48,4/1-4/48 member portmember
vlan 10 create byport 1 name "VLAN10"
vlan 10 ports remove 1/3-1/8 member portmember
vlan 10 ports add 1/1-1/2,2/1-2/48,3/1-3/48,4/1-4/48 member portmember
#
# PORT CONFIGURATION - PHASE II
#
ethernet 1/2 stg 1 pathcost 200
#
back
```

5.5 EVALUACIÓN ECONÓMICA

La Tabla 5.5 muestra un resumen económico de los switches propuestos.

Orden No.	Descripción del Producto	P.U.US$	Cantidad	P.T. U.S$
NORTEL NETWORKS				
Core SW Data Center 1er Piso	01 PP8600 con la siguiente configuración cada uno: Chasis de 10 Slots, 144 Puertos 10/100Mbps Fast Ethernet Layer 3, 16 Puertos Gigabit Ethernet GBIC Layer 3, 12 Modulos para enlaces Gigabit Ethernet GBIC. Se incluye Redundancia de Procesador, Fuentes de Poder Redundantes.	73,378	2	146,756
SW WAN Data Center 1er Piso	01 PP8600 con la siguiente configuración cada uno: Chasis de 10 Slots, 96 Puertos 10/100Mbps Fast Ethernet Layer 3, 08 Puertos Gigabit Ethernet GBIC Layer 3, 04 Modulos para enlaces Gigabit Ethernet GBIC. Se incluye Redundancia de Procesador, Fuentes de Poder Redundantes.	53,913	2	107,826
SW NOC Primer Piso	01 PP8100 con la siguiente configuración cada uno: Chasis de 10 Slots, 144 Puertos 10/100Mbps Fast Ethernet Layer 2, 08 Puertos Gigabit Ethernet GBIC Layer 2, 04 Modulos para enlaces Gigabit Ethernet GBIC. Se incluye Redundancia de Procesador, Fuentes de Poder Redundantes.	38,558	2	77,116
SW Gerencias Segundo Piso	01 PP8100 con la siguiente configuración cada uno: Chasis de 10 Slots, 144 Puertos 10/100Mbps Fast Ethernet Layer 2, 08 Puertos Gigabit Ethernet GBIC Layer 2, 04 Modulos para enlaces Gigabit Ethernet GBIC. Se incluye Redundancia de Procesador, Fuentes de Poder Redundantes.	38,558	2	77,116
SW Customer Care Segundo Piso	01 PP8100 con la siguiente configuración cada uno: Chasis de 10 Slots, 144 Puertos 10/100Mbps Fast Ethernet Layer 2, 08 Puertos Gigabit Ethernet GBIC Layer 2, 04 Modulos para enlaces Gigabit Ethernet GBIC. Se incluye Redundancia de Procesador, Fuentes de Poder Redundantes.	38,558	2	77,116
			TOTAL VALOR VENTA U.S.$	**485,930**

Tabla 5.5 Resumen Económico de los switches propuesto para la Red LAN de la Sede Tecnológica.

CAPÍTULO VI

SOLUCIÓN PROPUESTA E IMPLEMENTADA PARA RED LAN DE LA SEDE ADMINISTRATIVA

6.1 SELECCIÓN DE EQUIPOS DE COMUNICACIONES

La solución implementada para la red LAN de la Sede Administrativa fue una red Gigabit Ethernet con Equipos Nortel Networks.

La solución LAN se baso en los switches passport 8600 L3 como equipos de CORE y los switches de borde BPS2000 L2 con QoS. para los pisos.

Con los Passport 8600 Routing Switches como switches de CORE se ofreció los niveles de prioridad, respaldo, seguridad y escalabilidad que la empresa necesitaba para su red LAN.

Con los switches de borde BPS2000 (Business Policy Switch)nos permitió entregar QoS al escritorio y priorizar el trafico de red, asegurando confiabilidad a la red para aplicaciones tales como telefonía IP, SAP, e-commerce, y videoconferencia.

▫ REPASO DEL SWITCH DE CORE PASSPORT 8600

El Switch Routing Passport 8600 es un switch multicapa, cuya funcionalidad está orientada a aplicaciones de misión crítica y fundamentalmente para grandes capacidades de conmutación y enrutamiento, alta disponibilidad, crecimiento y

calidad de servicio (QoS) que permiten la integración de los servicios de la institución.En el capitulo 5 se trato con detalles las características del Switch Passport 8600.

❑ SWITCHES DE BORDE BPS2000

Los switches de borde Business Policy Switch 2000 (BPS2000) ver fig. 6.1.1 con QoS que se utilizo en los pisos, entregan una solución sin paralelo para mejorar la perfomance y productividad de la red esenciales para el negocio. La QoS. Es la clave para proveer una perfomance consistente, confiable y predecible para aplicaciones de e-business y de misión critica.

El Switch BPS2000 es una solución Ethernet stackeable (hasta 8 switches) de alta densidad de 24 puertos 10/100 Mbps capa 2 que entrega clasificación de paquetes en capa3/capa 4 y priorización al escritorio, ofreciendo altos niveles de disponibilidad, densidad, administrabilidad y confiabilidad de la red .

El BPS2000 es un sistema Ehternet stackable 10/100 Mbps, con caracteristicas avanzada de QoS . Esta característica permite a las compañías optimizar los recursos y la inversión de sus redes a su máximo potencial..

El BPS2000 puede clasificar y priorizar tráfico en múltiple caminos: por 802.1p, por DiffServ Code Point (DSCP), por la dirección IP fuente/destino, por el puerto TCP/UDP fuente/destino, por el puerto fuente de ingreso, por la VLAN ID, y por el protocolo IP . Por consiguiente cada tipo de tráfico puede ser tratado distinto y apropiadamente.

Debido a la clasificación, priorización, políticas y etiquetado del trafico LAN IP (con DiffServ Code Point / TOS Byte), las redes LAN pueden ofrecer conectividad confiable y el ancho de Banda requerido para aplicaciones de misión critica tales como la telefonía IP a grupos y usuarios específicos y para dispositivos individuales tales como Servidores de e-commerce.

Caracterizado por su avanzada QoS, por sus capacidades de administración basadas en Web y por su razonable precio por puerto, los BPS 2000 fue uno de los primeros switches de su clase especialmente diseñado para la administración y etiquetado del trafico LAN IP dando al administrador la habilidad de priorizar y formar el flujo del trafico de todos los caminos hacia los extremos de la red.

Figura 6.1.1. Entregando Calidad de Servicio a la red corporativa con sus cuatro colas basadas en hardware sobre cada puerto, el switch de borde Business Police Switch (BPS2000) soporta avanzada QoS, maximizando la disponibilidad, confiabilidad y predictibilidad de la red

Las características principales del switch BPS2000 (Business Policy Switch) incluyen:

- Clasificación de paquetes L2/L3/L4, etiquetado, priorización y capacidades de políticas.
- Cuatro colas de clase de servicios por puerto para 10/100 y 8 colas de clase de servicio para los nuevos Módulos liberados.
- 24 puertos 10/100 Mbps autosensing en UTP.
- Un slot para Módulos con puertos para enlaces de subida con seguridad de enlaces (LinkSafe uplink).
- Apilabilidad (stackabilidad) contra fallas de hasta 8 unidades y 224 puertos administrados por stack. (Ver figura 6.1.2)
- Opciones mediante Módulos de expansión de puerto: Gigabit Ethernet (incluyendo convertidores GBIC para 1000BASE-SX, -LX, -XD, y ZX, GBICs CWDM), 100BASE-FX, 10/100BASE-TX, más dos nuevos modulos con puertos GBIC "Small Form Factor"- asi com tambien modulos con un unico puerto y con puertos duales 1000BASE-TX.
- Soporta el protocolo EAP (Extensible Authentication Protocol).
- Las políticas de tráfico permiten provisionar diferentes niveles de servicios limitando la velocidad de trasmisión (throughput) del tráfico en cualquier puerto de ingreso

The Business Policy Switch puede priorizar el tráfico IP basado en:

- En la prioridad 802.1p (Capa 2)
- En la IP fuente/destino o subred (Capa 3)

- En los puertos TCP/UDP fuente/destino (Capa 4)
- En la ID de la VLAN (Capa 3 y Capa 4).
- En el número de puerto de ingreso, en la ID del protocolo IP (Ejemplo TCP,UDP,IGMP), en los protocolos L3 (IP e IPX)

Table 6.1 define las características y beneficios del switch BPS2000 de Nortel Networks.

❑ CARACTERÍSTICAS Y BENEFICIOS DEL SWITCH BPS2000

En la Tabla 6.1.1 muestra las características y beneficio del switch BPS2000 propuesto para la red LAN de la Sede Administrativa

Característica del Business Policy Switch	**Beneficio del Business Policy Switch**
Cuatro colas basadas en hardware en cada puerto, lee, altera y vigila(polices) el tráfico L2/L3/L4 en el ingreso. Los nuevos módulos Gigabit proveen formación (shaping) en el tráfico de egreso así como también ocho colas basadas en hardware	Capacidades avanzadas de QoS , maximizando la disponibilidad , confiabilidad y predictibilidad de la red.
Slot para módulos de subida (uplink) de alta velocidad.	Flexibilidad para llenar cualquier tipo de backbone de alta velocidad

Característica del Business Policy Switch	Beneficio del Business Policy Switch
Administración basada enWeb.	Fácil administración; Políticas de QoS pueden ser configuradas vía el asistente de Qos basado en Web del BPS2000
Envio (forwarding) del Frame en 3 Millones de paquetes por segundo por switch (24 millones de paquetes por segundo por stack	Red de alta velocidad.
Opciones flexibles de enlaces de subida (uplink) de alta velocidad con seguridad de enlace (LinkSafe uplink) en Gigabit.	Permite conexiones a los switches de core Passport 8600 capa 3 o a otros switches de alta velocidad en el centro de la la red
Troncales multienlaces (MLT, "MultiLink Trunking") y troncales multienlaces distribuidos (DMLT, "Distributed MultiLink Trunking) a traves del stack	Redundancia y ancho de banda incrementado para conectividad confiable para servidores de misión critica y centros de red.
Apilabilidad (stackability) contra fallas (Fail-safe)	Alta densidad y continuo uptimes de la red
Características avanzada de software	Red a prueba del futuro

Tabla 6.1.1. Característica y beneficio del Business Policy Switch

Figura 6.1.2. Stack de Business Policy Switch configurado para redundancia .Con su arquitectura robusta contra fallas (fail-safe) y componentes resilentes, el Business Policy Switch entrega una verdadera apilabilidad (stackability) con 2.5 Gbps de ancho de banda de stacking.

❑ DISTRIBUCIÓN DE LOS EQUIPOS EN EL BACKBONE

La Sede Administrativa ubicada en un edificio, comprendía los Pisos 6 al Piso 11, donde se realizo un cableado estructurado el cual abarcaba el cableado Horizontal CAT 6 para los pisos y el cableado vertical con fibra Optica para red troncal. Basado en esta infraestructura física se instalarón los Equipos de comunicaciones Gigabit Ethernet de Nortel.

- **Nodo Principal : Centro de Cómputo (Piso 9)**

En este ambiente se instalaron 2 switches de Core Passport 8600 capa 3

Estos Switches CORE, atienden directamente a los servidores de la red de Datos donde se encuentran, por ejemplo los Servidores DHCP, etc, además de

atender a usuarios del Piso (Departamento de Logística). La capacidad de estos dos switches CORE son de 16 puertos Gigabit Ethernet GBIC Capa 3 y 96 puertos 10/100 Mbps Fast Ethernet Capa 3 cada uno. Estos switches están conectados mediante un enlaces MLT de 2 Gbps

A estos Switches llegan las conexiones de los switches de los nodos secundarios (Piso 6, Piso 7, Piso 8, Piso 10, Piso 11) mediante enlaces redundantes de Fibra Optica.

- **Nodos Secundarios: (PISO 6, PISO 7, PISO 8, PISO 10 y PISO 11)**

En estos ambiente se encuentran las áreas de Oficinas de Ventas.(Piso 6 y 7), del Departamento de IT (Piso 8), de Recursos Humanos (Piso 10) y Gerencias (Piso 11). Dependiendo de la cantidad de usuarios por piso se propuso una solución apilable de switches BPS2000 de 24 puertos 10/100 cada uno, para cubrir los requerimientos de cada piso. La cantidad total detallada de switches BPS2000 propuesto para los pisos se muestra en la tabla 6.1.2

Switches de borde BPS2000		
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
AL2001E15	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX más 1 MDA y 1 slot deCascada) (Incluye cable de poder tipo Norte-Americano)	17
AL2033005	450-1SX 1-port 1000BASE-SX Single PHY MDA (Para los BPS2000)..	17
AL2033010	BayStack 400-ST1 Cascade Module (Para BPS2000, incluye cable de stack).	17

Tabla 6.1.2 Cantidad total de switches de borde BPS2000 propuesto

En la Figura 6.1.3 se muestra la red LAN implementada para la sede Administrativa bajo un esquema de alta disponibilidad,desempeño y escalabilidad.

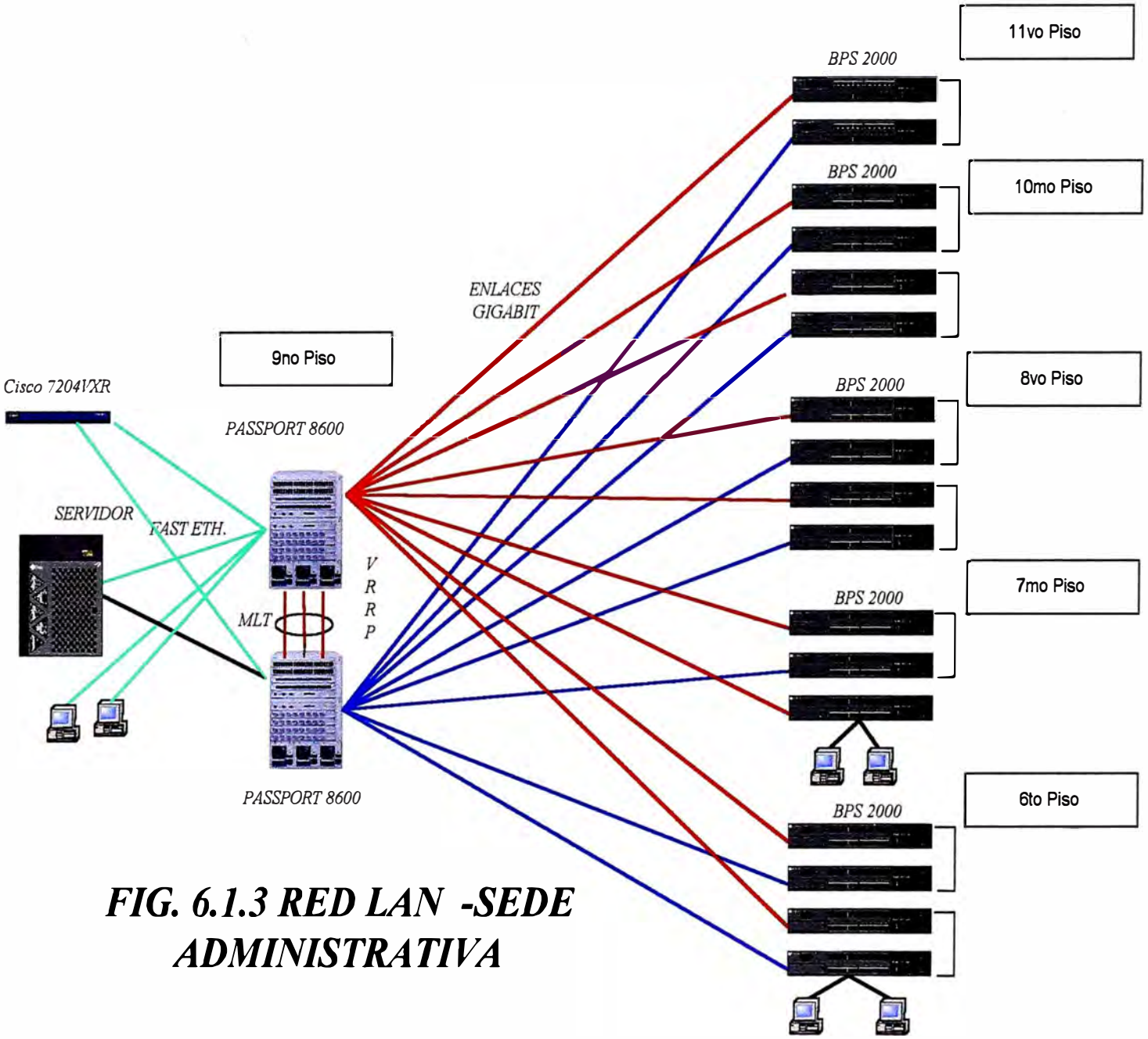


FIG. 6.1.3 RED LAN -SEDE ADMINISTRATIVA

- **CONFIGURACIÓN DE LOS SWITCHES DE CORE L3 (IBK01, IBK02) PARA EL DATA CENTER (PISO 9)**

Para este nodo principal se propuso dos Switches Passport 8600 capa 3 con la siguiente configuración para cada switch: Chassis de 10 Slots, 96 puertos 10/100 Mbps Fast Ethernet Capa 3, 16 puertos Gigabit Ethernet GBIC Capa 3 (13 puertos con Convertidores GBIC y 3 puertos vacíos), 13 módulos Convertidores GBIC para enlaces Gigabit Ethernet. Se incluyó Redundancia de Procesador y Fuentes de Poder Redundantes.

Con esta configuración se tiene 6 Slots ocupado (con 2 módulos 8690SF/CPU, 2 módulos 8648TX y 2 módulos 8608 GBIC) quedando 4 slots libres.

Estos dos switches están unidos mediante una troncal multi-enlace (MLT) conformado por 3 conexiones físicas Gigabit Ethernet entre los 2 switches de core, el cual es visto como un solo enlace lógico de 3 gigabit Ethernet

Cada Switch propuesto tiene la siguiente configuración que se muestra en la tabla 6.1.3:

PASSPORT 8600 SERIES: Switch de core L3 IBK01,IBK02 Piso 9: Data Center		
	96 puertos Fast Ethernet 16 puertos GigabitEthernet con 13 Converter GBIC incluido	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
DS1410003-3.1	Licencia de Software y Kit de Software del Passport 8000 Enterprise Routing Switch (Incluye licencia, software Device Manager, y toda la documentación). Una licencia requerida por cada chasis del switch routing. Versión 3.1.	1
DS1402001	Passport 8010 chassis de 10 slot. Incluye chassis, dual backplane, dos bandejas de ventiladores, cable RS232 para administración de consola, kit para montar en Rack y Kit guía cable. Requiere una o dos Fuentes de alimentación dependiendo de la configuración; Hasta tres fuentes de alimentación es soportada.	1
DS1405E01	Passport 8001PS fuente de alimentación de 100-240 VAC. Al menos una fuente de alimentación es requerida por cada chasis del Passport 8000. (Incluye cable de poder tipo Norte Americano)	3
DS1404001	Módulo Passport 8690SF Enterprise Routing Switch ; Módulo CPU/Switch Fabric - Uno requerido por cada chassis Passport 8000 Routing Switch . Incluye tarjeta de memoria flash PCMCIA.	2
DS1404002	Módulo Passport 8648TX Enterprise Routing Switch. Interfase de conmutación Ethernet Capa 3 de 48 puertos autosensing 10BASE-T/100BASE-TX.	2
DS1404015	Módulo Passport 8608GB Enterprise Routing Switch de 8-puertos 1000 Base GBIC (GBICs son vendidos separadamente)	2
AA1419001	1-puerto 1000Base-SX Gigabit Interfase Converter (GBIC)	13

Tabla 6.1.2 Cantidad total de switches de borde BPS2000 propuesto

El siguiente gráfico muestra la configuración de los 2 Equipos propuesto para este nodo.

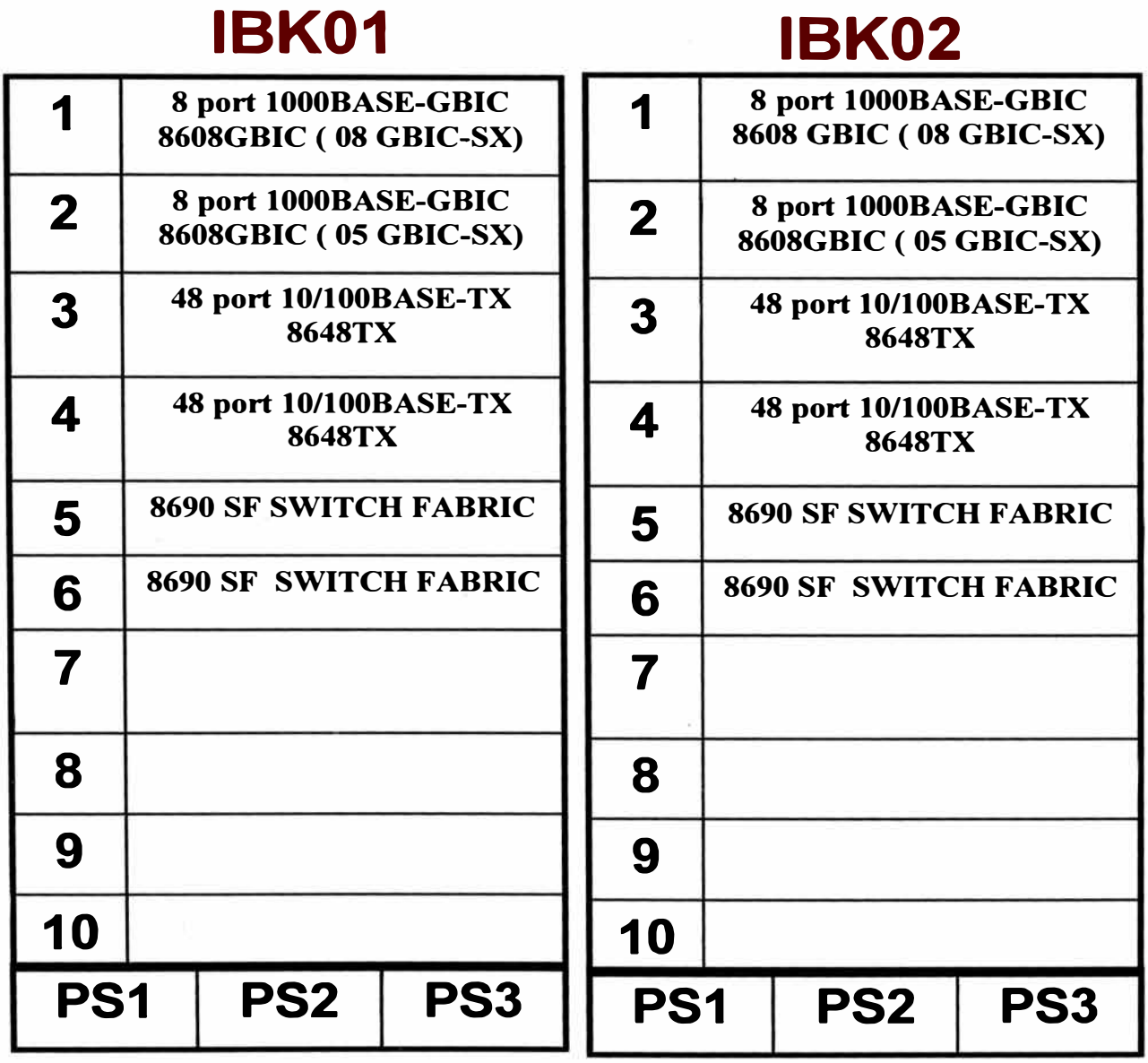


Figura 6.1.4. Configuración de los dos Switches de core (IBK01,IBK02) Passport 8600 Capa 3 propuesto para el Data Center. Capacidad total instalada de 192 puertos 10/100BASE-TX y 32 puertos 1000BASE-GBIC

- **CONFIGURACIÓN DE LOS SWITCHES DE BORDE BPS2000 PARA EL NODO SECUNDARIO PISO 11**

Para este nodo se propuso dos Switches BPS2000 con la siguiente configuración para cada switch: 24 puertos 10/100 Mbps Fast Ethernet Capa 2, un puerto Gigabit Ethernet 1000BASE-SX, un modulo de cascada (stack)

Con esta configuración se tiene 2 switches BPS2000 en una configuración en stack (obteniendo 48 puertos 10/100 más 2 puertos Gigabit en total por stack) que cubren los puntos de red necesarios para el piso. Esta pila de switches se conectan a los switches de core mediante 2 enlaces Gigabit 1000BASE-SX (Un enlace se conecta al switch de core IBK01 y el otro enlace al switch de Core IBK02) obteniendo así la redundancia de enlaces.

La cantidad de Switches BPS200 propuesto para este nodo se muestra en la tabla 6.1.4:

Switches de borde BPS2000		
	48 puertos Fast Ethernet 2 puertos GigabitEthernet	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
AL2001E15	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX más 1 MDA y 1 slot de Cascada) (Incluye cable de poder tipo Norte-Americano)	2
AL2033005	450-1SX 1-port 1000BASE-SX Single PHY MDA (Para los BPS2000)..	2
AL2033010	BayStack 400-ST1 Cascade Module (Para BPS2000, incluye cable de stack).	2

Tabla 6.1.4 Cantidad de switches de borde BPS2000 propuesto para el nodo secundario del PISO 11

❑ CONFIGURACIÓN DE LOS SWITCHES DE BORDE BPS2000 PARA EL NODO SECUNDARIO PISO 10

Para este nodo se propuso cuatro Switches BPS2000 con la siguiente configuración para cada switch: 24 puertos 10/100 Mbps Fast Ethernet Capa 2, un puerto Gigabit Ethernet 1000BASE-SX, un modulo de cascada (stack)

Con esta configuración se tiene 2 stack de dos switches BPS2000 por cada stack (obteniendo 48 puertos 10/100 más 2 puertos Gigabit en total por stack) . Cada una de estas dos pilas de switches se conectan a los switches de core mediante 2 enlaces Gigabit 1000BASE-SX (Un enlace se conecta al switch de core IBK01 y el otro enlace al switch de Core IBK02) obteniendo así la redundancia de enlaces.

Mediante los dos stack de switches,en total estamos entregando 96 puertos 10/100 más 4 puertos Gigabit para cubrir los puntos de red necesarios del piso

La cantidad de Switches BPS200 propuesto para este nodo se muestra en la tabla 6.1.5:

Switches de borde BPS2000		
	96 puertos Fast Ethernet 4 puertos GigabitEthernet	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
AL2001E15	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX más 1 MDA y 1 slot de Cascada) (Incluye cable de poder tipo Norte-Americano)	4
AL2033005	450-1SX 1-port 1000BASE-SX Single PHY MDA (Para los BPS2000)..	4
AL2033010	BayStack 400-ST1 Cascade Module (Para BPS2000, incluye cable de stack).	4

Tabla 6.1.5 Cantidad de switches de borde BPS2000 propuesto para el nodo secundario del PISO 10

❑ CONFIGURACIÓN DE LOS SWITCHES DE BORDE BPS2000 PARA EL NODO SECUNDARIO PISO 8

Para este nodo se propuso cuatro Switches BPS2000 con la siguiente configuración para cada switch: 24 puertos 10/100 Mbps Fast Ethernet Capa 2, un puerto Gigabit Ethernet 1000BASE-SX, un modulo de cascada (stack)

Con esta configuración se tiene 2 stack de dos switches BPS2000 por cada stack (obteniendo 48 puertos 10/100 más 2 puertos Gigabit en total por stack) . Cada una de estas dos pilas de switches se conectan a los switches de core mediante 2 enlaces Gigabit 1000BASE-SX (Un enlace se conecta al switch de core IBK01 y el otro enlace al switch de Core IBK02) obteniendo así la redundancia de enlaces.

Mediante los dos stack de switches,en total estamos entregando 96 puertos 10/100 más 4 puertos Gigabit para cubrir los puntos de red necesarios del piso

La cantidad de Switches BPS200 propuesto para este nodo se muestra en la tabla 6.1.6:

Switches de borde BPS2000		
	96 puertos Fast Ethernet 4 puertos GigabitEthernet	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
AL2001E15	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX más 1 MDA y 1 slot de Cascada) (Incluye cable de poder tipo Norte-Americano)	4
AL2033005	450-1SX 1-port 1000BASE-SX Single PHY MDA (Para los BPS2000)..	4
AL2033010	BayStack 400-ST1 Cascade Module (Para BPS2000, incluye cable de stack).	4

Tabla 6.1.6 Cantidad de switches de borde BPS2000 propuesto para el nodo secundario del PISO 8

❑ CONFIGURACIÓN DE LOS SWITCHES DE BORDE BPS2000 PARA EL NODO SECUNDARIO PISO 7

Para este nodo se propuso tres Switches BPS2000 con la siguiente configuración para cada switch: 24 puertos 10/100 Mbps Fast Ethernet Capa 2, un puerto Gigabit Ethernet 1000BASE-SX, un modulo de cascada (stack)

Con esta configuración se tiene un stack de dos switches BPS2000 (obteniendo 48 puertos 10/100 más 2 puertos Gigabit en total por stack) y un switch BPS2000 independiente de 24 puertos 10/100 y 1 puerto Gigabit.. La pila de switches se conectan a los switches de core mediante 2 enlaces Gigabit 1000BASE-SX (Un enlace se conecta al switch de core IBK01 y el otro enlace al switch de Core IBK02) obteniendo así la redundancia de enlaces. El switch BPS2000 independiente se conecta al switch de core IBK01.

Mediante el stack de switches y el switch independiente ,en total estamos entregando 72 puertos 10/100 más 3 puertos Gigabit para cubrir los puntos de red necesarios del piso. La cantidad de Switches BPS200 propuesto para este nodo se muestra en la tabla 6.1.7:

Switches de borde BPS2000		
	72 puertos Fast Ethernet 3 puertos GigabitEthernet	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
AL2001E15	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX más 1 MDA y 1 slot de Cascada	3
AL2033005	450-1SX 1-port 1000BASE-SX Single PHY MDA (Para los BPS2000)..	3
AL2033010	BayStack 400-ST1 Cascade Module (Para BPS2000, incluye cable de stack).	3

Tabla 6.1.7 Cantidad de switches BPS2000 propuesto para PISO 7

❑ CONFIGURACIÓN DE LOS SWITCHES DE BORDE BPS2000 PARA EL NODO SECUNDARIO PISO 6

Para este nodo se propuso cuatro Switches BPS2000 con la siguiente configuración para cada switch: 24 puertos 10/100 Mbps Fast Ethernet Capa 2, un puerto Gigabit Ethernet 1000BASE-SX, un modulo de cascada (stack)

Con esta configuración se tiene 2 stack de dos switches BPS2000 por cada stack (obteniendo 48 puertos 10/100 más 2 puertos Gigabit en total por stack) . Cada una de estas dos pilas de switches se conectan a los switches de core mediante 2 enlaces Gigabit 1000BASE-SX (Un enlace se conecta al switch de core IBK01 y el otro enlace al switch de Core IBK02) obteniendo así la redundancia de enlaces.

Mediante los dos stack de switches,en total estamos entregando 96 puertos 10/100 más 4 puertos Gigabit para cubrir los puntos de red necesarios del piso

La cantidad de Switches BPS200 propuesto para este nodo se muestra en la tabla 6.1.8:

Switches de borde BPS2000		
	96 puertos Fast Ethernet 4 puertos GigabitEthernet	
CODIGO	DESCRIPCIÓN DE LOS PRODUCTOS	CANTIDAD
AL2001E15	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX más 1 MDA y 1 slot de Cascada) (Incluye cable de poder tipo Norte-Americano)	4
AL2033005	450-1SX 1-port 1000BASE-SX Single PHY MDA (Para los BPS2000)..	4
AL2033010	BayStack 400-ST1 Cascade Module (Para BPS2000, incluye cable de stack).	4

Tabla 6.1.8 Cantidad de switches de borde BPS2000 propuesto para el nodo secundario del PISO 6

6.2 PLANIFICACIÓN DE LAS VLANS

Las siguientes Tablas muestran la distribución de los puertos y las VLANs creadas sobre los switches. Donde

Id : significa la identificación de la VLAN.

Nombre: significa el Nombre de la VLAN

Tipo: El tipo de VLAN creada

Puertos Miembros : Los puertos del Switch que pertenecen a dicha VLAN. Donde **x/y** se lee como el puerto y del Modulo que esta en el slot x , **x/y-x/z** se lee como los puertos **y** hasta la **z** del Módulo que esta en el slot x .

Dirección IP : Significa Dirección IP asignada a la VLAN que actúa semejante a una dirección de una interfase de Router virtual para la VLAN. Esta interfase de Router Virtual no tiene ninguna asociación con ningún puerto en particular, pero puede ser alcanzada a través de cualquiera de los puertos que pertenecen a dicha VLAN y es la dirección IP que sirve como gateway a través del cual un frame es ruteado fuera de la VLAN.

Máscara : Es la máscara que identifica a que subred pertenece la VLAN cuando el enrutamiento es configurado.

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	3/1-3/10	172.35.1.3	255.255.255.0 (24 bits)	Para Servidores y el router (incluye al Servidor DHCP (172.35.1.11) perte-neciente a la VLAN1
6	VLAN6	Por Puerto	1/1,2/1, 3/11	172.35.6.3	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 6 , incluye al Servidor DHCP (172.35.6.11) perte-neciente a la VLAN6
7	VLAN7	Por Puerto	1/2,2/2, 3/12	172.35.7.3	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 7 , incluye al Servidor DHCP (172.35.7.11) perte-neciente a la VLAN7
8	VLAN8	Por Puerto	1/3,2/3 3/13	172.35.8.3	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 8 , incluye al Servidor DHCP (172.35.8.11) perte-neciente a la VLAN8
9	VLAN9	Por Puerto	3/14,3/17, 4/1	172.35.9.3	255.255.255.0 (24 bits)	Para usuarios del Piso 9 , incluye al Servidor DHCP (172.35.9.11) perte-neciente a la VLAN9
10	VLAN10	Por Puerto	1/4,2/4 3/15	172.35.10.3	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 10 , incluye al Servidor DHCP (172.35.10.11) perte-neciente a la VLAN10
11	VLAN11	Por Puerto	1/5,2/5 3/16	172.35.11.3	255.255.255.0 (27 bits)	Para enlaces a los BPS2000 y usuarios del Piso 11, incluye al Servidor DHCP(172.35.11.11) perteneciente a la VLAN11

Tabla 6.2.1 : Vlans creadas sobre el switch de core IBK01

Id	Nombre	Tipo	Puertos Miembros	Dirección IP	Máscara	Comentario
1	VLAN1	Por Puerto	3/1-3/10	172.35.1.2	255.255.255.0 (24 bits)	Para Servidores y el router (incluye al Servidor DHCP (172.35.1.11) perte-neciente a la VLAN1
6	VLAN6	Por Puerto	1/1,2/1, 3/11	172.35.6.2	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 6 , incluye al Servidor DHCP (172.35.6.11) perte-neciente a la VLAN6
7	VLAN7	Por Puerto	1/2,2/2, 3/12	172.35.7.2	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 7 , incluye al Servidor DHCP (172.35.7.11) perte-neciente a la VLAN7
8	VLAN8	Por Puerto	1/3,2/3 3/13	172.35.8.2	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 8 , incluye al Servidor DHCP (172.35.8.11) perte-neciente a la VLAN8
9	VLAN9	Por Puerto	3/14,3/17, 4/1	172.35.9.2	255.255.255.0 (24 bits)	Para usuarios del Piso 9 , incluye al Servidor DHCP (172.35.9.11) perte-neciente a la VLAN9
10	VLAN10	Por Puerto	1/4,2/4 3/15	172.35.10.2	255.255.255.0 (24 bits)	Para enlaces a los BPS2000 y usuarios del Piso 10 , incluye al Servidor DHCP (172.35.10.11) perte-neciente a la VLAN10
11	VLAN11	Por Puerto	1/5,2/5 3/16	172.35.11.2	255.255.255.0 (27 bits)	Para enlaces a los BPS2000 y usuarios del Piso 11, incluye al Servidor DHCP(172.35.11.11) perteneciente a la VLAN11

Tabla 6.2.2 : Vlans creadas sobre el switch de core IBK02

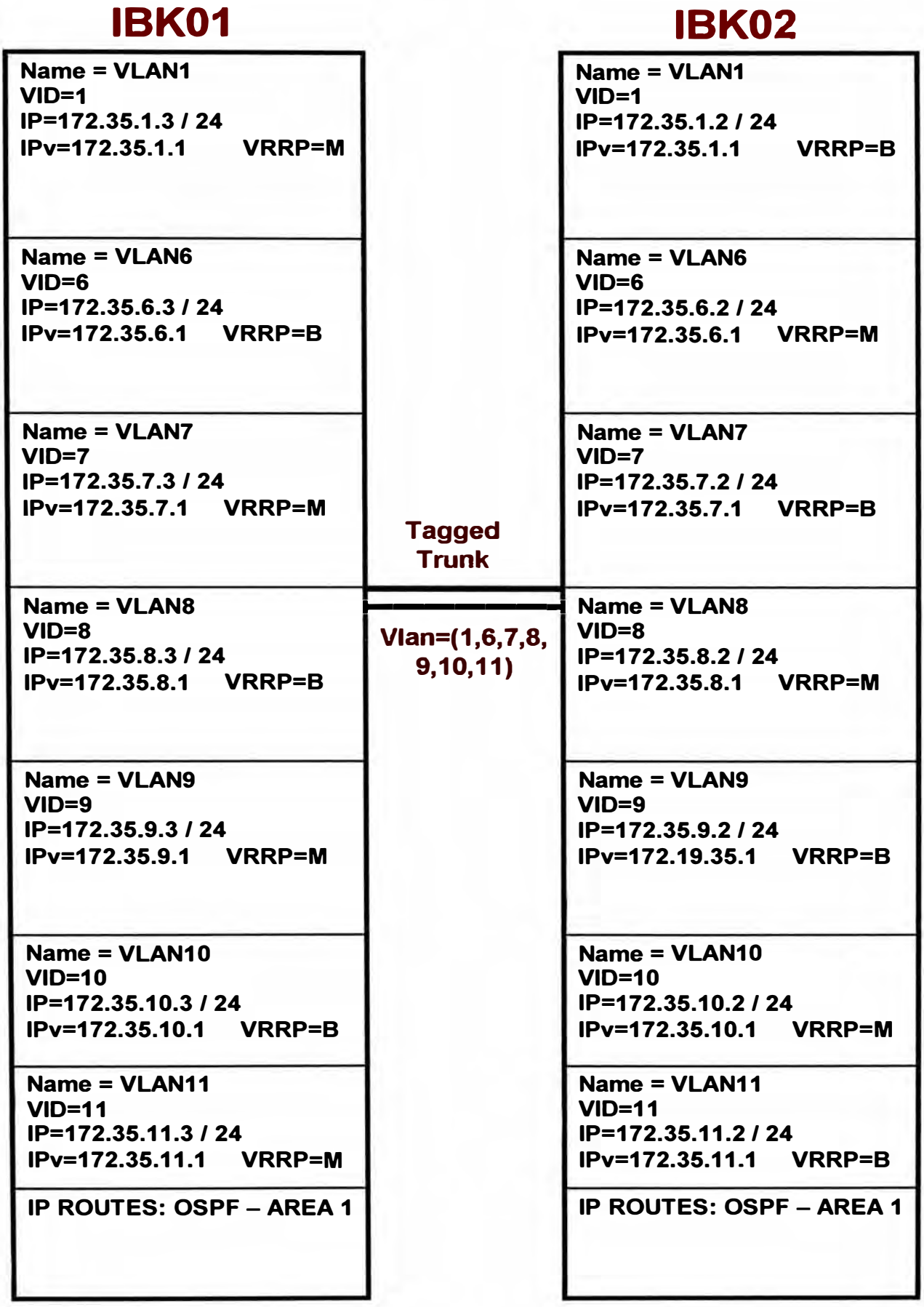


Figura 6.2.1 VLANs sobre los Switches de core Passport 8600, IBK01 y IBK02

❑ CONFIGURACIÓN DEL MLT ENTRE LOS SWITCHES DE CORE IBK01,IBK02.

Las siguientes Tablas muestran los puertos troncales Multi-enlaces (Multi-Link Trunking o **MLT**) creados sobre los switches de core IBK01 , IBK02. En este caso el MLT esta formado por 3 conexiones físicas Gigabit Ethernet entre los 2 switches de core, el cual es visto como un solo enlace lógico de 3 gigabit Ethernet . Aprovechamos que hay 2 módulos Gigabit Ethernet por cada Switch Core para tomar puertos de cada módulo Gigabit Ethernet para que sean miembros de la troncal y así obtener un Distributed Multilink Trunking o DMLT. Donde

Id : Significa la identificación del MLT.

Nombre: Significa el Nombre del MLT.

Tipo: El tipo de puerto creado (en este caso es Troncal). Además de ser Etiquetado (tagged) para extender las VLANs entre los switches WAN.

Puertos Miembros : Los puertos del Switch que pertenecen a dicho MLT. Donde x/y se lee como el puerto **y** del Modulo que esta en el slot **x** , x/y-x/z se lee como los puertos **y** hasta la **z** del Módulo que esta en el slot **x** .

Id del MLT	Nombre del MLT	Tipo de Puerto	Puertos Miembros	VLAN ID
1	IBK01-IBK02	TRUNK (tagged)	1/6,1/7 2/6	VLAN 1 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10 VLAN 11

Tabla 6.2.3 : MLT creadas sobre el switch de core IBK01

Id del MLT	Nombre del MLT	Tipo de Puerto	Puertos Miembros	VLAN ID
1	IBK02-IBK01	TRUNK (tagged)	1/6 2/6	VLAN 1 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10 VLAN 11

Tabla 6.2.4 : MLT creadas sobre el switch de core IBK02

Para mayor ilustración ver la figura 6.2.1 donde se muestra el Multilink Trunking creado entre los 2 Switches de core IBK01 , IBK02 donde los puertos MLT en ambos switches son etiquetado para esparcir las VLANs entre ambos switches.

6.3 PLANIFICACIÓN DEL ESQUEMA DE DIRECCIONAMIENTO

La Tabla 6.3.1 muestra la dirección de red IP de cada subnet asociada a cada VLAN creada dentro de los switches que conforman la Red LAN de la Sede Administrativa

Para la comunicación entre las VLANs Subnet se habilitó el protocolo de enrutamiento OSPF en los Switches Capa 3 siendo la Red LAN de la Sede Administrativa considerada como el AREA 1 dentro de la Red WAN Corporativa

Ambiente	Dirección IP	Máscara	Comentario
Servidores,Router	172.35.1.0	255.255.255.0 (24 bits)	VLAN1
Estaciones de Trabajo del 6to Piso (Ventas)	172.35.6.0	255.255.255.0 (24 bits)	VLAN6
Estaciones de Trabajo del 7mo Piso (Ventas)	172.35.7.0	255.255.255.0 (24 bits)	VLAN7
Estaciones de Trabajo del 8vo Piso (IT)	172.35.8.0	255.255.255.0 (24 bits)	VLAN8
Estaciones de Trabajo del 9no Piso (Logística)	172.35.9.0	255.255.255.0 (24 bits)	VLAN9
Estaciones de Trabajo del 10mo Piso (Recursos Humanos)	172.35.10.0	255.255.255.0 (24 bits)	VLAN10
Estaciones de Trabajo del 11vo Piso (Gerencia)	172.19.11.0	255.255.255.0 (24 bits)	VLAN11

Tabla 6.3.1 : Plan Global de Direccionamiento IP

❑ CONFIGURACIÓN DEL VRRP ENTRE LOS SWITCHES DE CORE IBK01, IBK02

Para la implementación del protocolo VRRP (Virtual Router Redundancy Protocol) el cual esta diseñado para eliminar el único punto de falla que puede ocurrir cuando el router gateway por default configurado estáticamente en las estaciones finales sea perdida. Estamos empleando el concepto de una IP virtual compartida que usa VRRP, entre los dos switches de core IBK01, IBK02 de capa 3 que estan conectando a las subredes en la red LAN. Con esta dirección IP virtual como el default gateway de las estaciones finales, VRRP nos provee redundancia de gateway por default (defecto) en forma dinámica en el caso de una falla de uno de los switches de core.

La Tabla 6.3.2 muestra las IP virtuales creadas para las interfaces IP de las Vlans extendidas entre los Switches de core IBK01 e IBK02 para la implementación del VRRP para dar redundancia de gateway por default a las estaciones conectadas a los stack de Swiches de borde de los Pisos. Donde

VRID : Significa la identificación del Router Virtual.

Dirección IP de la Interfase: Significa la dirección IP de la interface real para las VLAN

Dirección IP Virtual: Significa la dirección virtual creada que sea el Default Gateway de las estaciones finales.

En la Tabla 6.3.2 se observa que la mayor prioridad usada para la elección del "master" entre los routers virtuales configurado en cada switch de Core lo hemos seleccionado en forma alternada para proveer compartición de la carga del tráfico saliente entre los switches de core IBK01 e IBK02.

Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 1**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
IBK01	1	172.35.1.3 /24	172.35.1.1 /24	200	MASTER
IBK02	1	172.35.1.2/24	172.35.1.1/24	100	BACKUP
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 6**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
IBK01	6	172.35.6.3 /24	172.35.6.1 /24	100	BACKUP
IBK02	6	172.35.6.2/24	172.35.6.1/24	200	MASTER
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 7**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
IBK01	7	172.35.7.3 /24	172.35.7.1 /24	200	MASTER
IBK02	7	172.35.7.2/24	172.35.7.1/24	100	BACKUP
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 8**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
IBK01	8	172.35.8.3 /24	172.35.8.1 /24	100	BACKUP
IBK02	8	172.35.8.2/24	172.35.8.1/24	200	MASTER

Nombre del Switch	Vrid	Dirección IP reales de las interfaces para la VLAN 9	Dirección IP virtual (Default Gateway para las Estaciones)	Prioridad	Estado
IBK01	9	172.35.9.3 /24	172.35.9.1 /24	200	MASTER
IBK02	9	172.35.9.2/24	172.35.9.1/24	100	BACKUP
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 10**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
IBK01	10	172.35.10.3 /24	172.35.10.1 /24	100	BACKUP
IBK02	10	172.35.10.2/24	172.35.10.1/24	200	MASTER
Nombre del Switch	**Vrid**	**Dirección IP reales de las interfaces para la VLAN 11**	**Dirección IP virtual (Default Gateway para las Estaciones)**	**Prioridad**	**Estado**
IBK01	11	172.35.11.3 /24	172.35.11.1 /24	200	MASTER
IBK02	11	172.35.11.2/24	172.35.11.1/24	100	BACKUP

Tabla 6.3.2 :Implementación del VRRP entre los switches IBK01 y IBK02

La Figura 6.1.3 muestra la implementación del protocolo VRRP entre los switches de core IBK01 e IBK02, capa 3 Passport 8600 con respecto a los Switches de borde BPS2000 capa 2 .

6.4 CONFIGURACIÓN DE LOS SWITCHES (PROGRAMACIÓN)

A continuación se muestra la configuración del switch Passport 8600 IBK01, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH DE CORE IBK01**

```
IBK01:5# sh config
#
# SUN SEP 09 13:36:30 2001 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
# Slot   1 8608GB 20325108 00000000    IO: GMAC= 5 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   2 8608GB 20325108 00000000    IO: GMAC= 5 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   3 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   4 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
RARU=2 CPLD=4
```

```
# Slot  5 8690SF 200e0100 00000000  CPU: CPLD=15 OP=2 TMUX=2
SWIP=2 FAD=1 CF=11
# Slot  6 8690SF 200e0100 00000000  CPU: CPLD=15 OP=2 TMUX=2
SWIP=2 FAD=1 CF=11
# Slot  7       00000001 00000000
# Slot  8       00000001 00000000
# Slot  9       00000001 00000000
# Slot 10       00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "IBK01"
#
# SYSTEM CONFIGURATION
#
sys set snmp trap-recv 172.35.1.90 v1 public
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
#
#
```

```
#
# MLT CONFIGURATION
#
mlt 1 create
mlt 1 name "IBK01-IBK02"
mlt 1 perform-tagging enable
mlt 1 add ports 1/6,1/7,2/6
#
# STG CONFIGURATION
#
stg 1  add ports 1/6,1/7,2/6
stg 1  priority 10
#
# VLAN CONFIGURATION
#
vlan 1 add-mlt 1
vlan 1 ports remove 1/1-1/5,2/1-2/5,3/11-3/48,4/1-4/48 member portmember
vlan 1 ip create 172.35.1.3/255.255.255.0 mac_offset 0
vlan 1 ip ospf enable
vlan 1 ip ospf metric 10
vlan 1 ip vrrp 1 action none
vlan 1 ip vrrp 1 address 172.35.1.1
vlan 1 ip vrrp 1 priority 200
vlan 1 ip vrrp 1 enable
```

vlan 6 create byport 1 color 2

vlan 6 add-mlt 1

vlan 6 ports remove 1/2-1/5,2/2-2/8,3/1-3/10,3/12-3/48,4/1-4/48 member portmember

vlan 6 ports add 1/1,2/1,1/6,1/7,2/6,2/1,3/11 member portmember

vlan 6 ip create 172.35.6.3/255.255.255.0 mac_offset 1

vlan 6 ip ospf enable

vlan 6 ip ospf metric 10

vlan 6 ip vrrp 6 action none

vlan 6 ip vrrp 6 address 172.35.6.1

vlan 6 ip vrrp 6 enable

vlan 7 create byport 1 color 3

vlan 7 add-mlt 1

vlan 7 ports remove 1/1,1/3-1/5,2/1,2/3-2/8,3/1-3/11,3/13-3/48,4/1-4/48 member portmember

vlan 7 ports add 1/2,2/2,1/6,1/7,2/6, 3/12 member portmember

vlan 7 ip create 172.35.7.3/255.255.255.0 mac_offset 2

vlan 7 ip ospf enable

vlan 7 ip ospf metric 10

vlan 7 ip vrrp 7 action none

vlan 7 ip vrrp 7 address 172.35.7.1

vlan 7 ip vrrp 7 priority 200

vlan 7 ip vrrp 7 enable

vlan 8 create byport 1 color 4

vlan 8 add-mlt 1

vlan 8 ports remove 1/1-1/2,1/4-1/5,2/1-2/2,2/4-2/8,3/1-3/12,3/14-3/48,4/1-4/48 member portmember

vlan 8 ports add 1/3, 2/3,1/6,1/7,2/6,3/13 member portmember

vlan 8 ip create 172.35.8.3/255.255.255.0 mac_offset 3

vlan 8 ip ospf enable

vlan 8 ip ospf metric 10

vlan 8 ip vrrp 8 action none

vlan 8 ip vrrp 8 address 172.35.8.1

vlan 8 ip vrrp 8 enable

vlan 9 create byport 1 color 5

vlan 9 add-mlt 1

vlan 9 ports remove 1/1-1/5,2/1-2/8,3/1-3/13,3/15-3/16 member portmember

vlan 9 ports add 1/6,1/7,2/6,3/14,3/17-3/48,4/1-4/48 member portmember

vlan 9 ip create 172.35.9.3/255.255.255.0 mac_offset 4

vlan 9 ip ospf enable

vlan 9 ip ospf metric 10

vlan 9 ip vrrp 9 action none

vlan 9 ip vrrp 9 address 172.35.9.1

vlan 9 ip vrrp 9 priority 200

vlan 9 ip vrrp 9 enable

vlan 10 create byport 1 color 6

vlan 10 add-mlt 1

```
vlan 10 ports remove 1/1-1/3,1/5,2/1-2/3,2/5-2/8,3/1-3/14,3/16-3/48,4/1-4/48
member portmember
vlan 10 ports add 1/4, 2/4, 1/6,1/7,2/6,3/15 member portmember
vlan 10 ip create 172.35.10.3/255.255.255.0 mac_offset 5
vlan 10 ip ospf enable
vlan 10 ip ospf metric 10
vlan 10 ip vrrp 10 action none
vlan 10 ip vrrp 10 address 172.35.10.1
vlan 10 ip vrrp 10 enable
vlan 11 create byport 1 color 7
vlan 11 add-mlt 1
vlan 11 ports remove 1/1-1/4,2/1-2/4,2/6-2/8,3/1-3/15,3/17-3/48,4/1-4/48
member portmember
vlan 11 ports add 1/5, 2/5,1/6,1/7,2/6,3/16 member portmember
vlan 11 ip create 172.35.11.3/255.255.255.0 mac_offset 6
vlan 11 ip ospf enable
vlan 11 ip ospf metric 10
vlan 11 ip vrrp 11 action none
vlan 11 ip vrrp 11 address 172.35.11.1
vlan 11 ip vrrp 11 priority 200
vlan 11 ip vrrp 11 enable

#
#
```

```
#
# IP & RIP CONFIGURATION
#
ip static-route create 0.0.0.0/0.0.0.0 next-hop 172.35.1.254 cost 1
#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf router-id 7.0.0.0
ip ospf enable
ip ospf area 0.0.0.1 create
ip ospf interface 172.35.1.3 area 0.0.0.1
ip ospf interface 172.35.6.3 area 0.0.0.1
ip ospf interface 172.35.7.3 area 0.0.0.1
ip ospf interface 172.35.8.3 area 0.0.0.1
ip ospf interface 172.35.9.3 area 0.0.0.1
ip ospf interface 172.35.10.3 area 0.0.0.1
ip ospf interface 172.35.11.3 area 0.0.0.1
#
back
```

A continuación se muestra la configuración del switch Passport 8600 IBK02, mediante la salida del comando de línea "show config":.

- **CONFIGURACIÓN DEL SWITCH DE CORE IBK02**

```
IBK02:5# sh config
#
# SUN SEP 09 13:08:00 2001 UTC
# box type            : Passport-8010
# software version    : 3.1.2.0
# monitor version     : 3.1.2.0/011
#

#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot   1 8608GB 20325108 00000000    IO: GMAC= 5 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   2 8608GB 20325108 00000000    IO: GMAC= 5 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   3 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   4 8648TX 20210130 00000000    IO: PLRO= 3 OP=2 TMUX=2
RARU=2 CPLD=4
# Slot   5 8690SF 200e0100 00000000  CPU: CPLD=15 OP=2 TMUX=2
SWIP=2 FAD=1 CF=11
```

```
# Slot   6 8690SF 200e0100 00000000   CPU: CPLD=14 OP=2 TMUX=2
SWIP=2 FAD=1 CF=11
# Slot  7        00000001 00000000
# Slot  8        00000001 00000000
# Slot  9        00000001 00000000
# Slot 10        00000001 00000000
config
#
# CLI CONFIGURATION
#
cli prompt "IBK02"
#
# SYSTEM CONFIGURATION
#
sys set snmp trap-recv 172.35.1.90 v1 public
#
# LINK-FLAP-DETECT CONFIGURATION
#
sys link-flap-detect interval  60
#
# MLT CONFIGURATION
#
mlt 1 create
mlt 1 name "IBK02-IBK01"
```

```
mlt 1 perform-tagging enable
mlt 1 add ports 1/6,1/7, 2/6
#
# STG CONFIGURATION
#
stg 1  add ports 1/6,1/7,2/6
stg 1  priority 20
#
# VLAN CONFIGURATION
#
vlan 1 add-mlt 1
vlan 1 ports remove 1/1-1/5,2/1-2/5,3/11-3/48,4/1-4/48 member portmember
vlan 1 ip create 172.35.1.2/255.255.255.0 mac_offset 0
vlan 1 ip ospf enable
vlan 1 ip ospf metric 10
vlan 1 ip vrrp 1 action none
vlan 1 ip vrrp 1 address 172.35.1.1
vlan 1 ip vrrp 1 enable
vlan 6 create byport 1 color 2
vlan 6 add-mlt 1
vlan 6 ports remove 1/2-1/5,2/2-2/8,3/1-3/10,3/12-3/48,4/1-4/48 member
 portmember
vlan 6 ports add 1/1,2/1, 1/6,1/7,2/6,2/1,3/11 member portmember
vlan 6 ip create 172.35.6.2/255.255.255.0 mac_offset 1
```

vlan 6 ip ospf enable

vlan 6 ip ospf metric 10

vlan 6 ip vrrp 6 action none

vlan 6 ip vrrp 6 address 172.35.6.1

vlan 6 ip vrrp 6 priority 200

vlan 6 ip vrrp 6 enable

vlan 7 create byport 1 color 3

vlan 7 add-mlt 1

vlan 7 ports remove 1/1,1/3-1/5,2/1,2/3-2/8,3/1-3/11,3/13-3/48,4/1-4/48 member portmember

vlan 7 ports add 1/2, 2/2,1/6,1/7,2/6, 3/12 member portmember

vlan 7 ip create 172.35.7.2/255.255.255.0 mac_offset 2

vlan 7 ip ospf enable

vlan 7 ip ospf metric 10

vlan 7 ip vrrp 7 action none

vlan 7 ip vrrp 7 address 172.35.7.1

vlan 7 ip vrrp 7 enable

vlan 8 create byport 1 color 4

vlan 8 add-mlt 1

vlan 8 ports remove 1/1-1/2,1/4-1/5,2/1-2/2,2/4-2/8,3/1-3/12,3/14-3/48,4/1-4/48 member portmember

vlan 8 ports add 1/3, 2/3, 1/6,1/7,2/6,3/13 member portmember

vlan 8 ip create 172.35.8.2/255.255.255.0 mac_offset 3

vlan 8 ip ospf enable

vlan 8 ip ospf metric 10

vlan 8 ip vrrp 8 action none

vlan 8 ip vrrp 8 address 172.35.8.1

vlan 8 ip vrrp 8 priority 200

vlan 8 ip vrrp 8 enable

vlan 9 create byport 1 color 5

vlan 9 add-mlt 1

vlan 9 ports remove 1/1-1/5,2/1-2/8,3/1-3/13,3/15-3/16 member portmember

vlan 9 ports add 1/6,1/7,2/6,3/14,3/17-3/48,4/1-4/48 member portmember

vlan 9 ip create 172.35.9.2/255.255.255.0 mac_offset 4

vlan 9 ip ospf enable

vlan 9 ip ospf metric 10

vlan 9 ip vrrp 9 action none

vlan 9 ip vrrp 9 address 172.35.9.1

vlan 9 ip vrrp 9 enable

vlan 10 create byport 1 color 6

vlan 10 add-mlt 1

vlan 10 ports remove 1/1-1/3,1/5,2/1-2/3,2/5-2/8,3/1-3/14,3/16-3/48,4/1-4/48 member portmember

vlan 10 ports add 1/4, 2/4,1/6,1/7,2/6,3/15 member portmember

vlan 10 ip create 172.35.10.2/255.255.255.0 mac_offset 5

vlan 10 ip ospf enable

vlan 10 ip ospf metric 10

vlan 10 ip vrrp 10 action none

```
vlan 10 ip vrrp 10 address 172.35.10.1
vlan 10 ip vrrp 10 priority 200
vlan 10 ip vrrp 10 enable
vlan 11 create byport 1 color 1
vlan 11 add-mlt 1
vlan 11 ports remove 1/1-1/4,2/1-2/4,2/6-2/8,3/1-3/15,3/17-3/48,4/1-4/48
member portmember
vlan 11 ports add 1/5, 2/5,1/6,1/7,2/6,3/16 member portmember
vlan 11 ip create 172.35.11.2/255.255.255.0 mac_offset 6
vlan 11 ip ospf enable
vlan 11 ip ospf metric 10
vlan 11 ip vrrp 11 action none
vlan 11 ip vrrp 11 address 172.35.11.1
vlan 11 ip vrrp 11 enable
#
# IP & RIP CONFIGURATION
#
ip static-route create 0.0.0.0/0.0.0.0 next-hop 172.35.1.254 cost 1
#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf router-id 8.0.0.0
ip ospf enable
```

```
ip ospf area 0.0.0.1 create
ip ospf interface 172.35.1.2 area 0.0.0.1
ip ospf interface 172.35.6.2 area 0.0.0.1
ip ospf interface 172.35.7.2 area 0.0.0.1
ip ospf interface 172.35.8.2 area 0.0.0.1
ip ospf interface 172.35.9.2 area 0.0.0.1
ip ospf interface 172.35.10.2 area 0.0.0.1
ip ospf interface 172.35.11.2 area 0.0.0.1
#
back
```

6.5 EVALUACIÓN ECONÓMICA

La Tabla 6.5. muestra un resumen económico con los precios referenciales de los switches propuestos.

Orden No.	Descripción del Producto	P.U.US$	Cantidad	P.T. U.S$
NORTEL NETWORKS				
	Switch de Core 9no Piso			
Switch de Core	02 PP8600 con la siguiente configuracion cada uno: Chasis de 10 Slots, 96 Puertos 10/100Mbps Fast Ethernet Layer 3, 16 Puertos Gigabit Ethernet 1000Base-SX. Se inckuye Redundancia de Procesador y Fuentes de Poder.	62,092	2	124,184
	Switch de borde			
11vo Piso	La propuesta incluyo: 02 Business Policy Switch 2000, 02 Módulos de Stack y Cables, 02 Módulos para enlaces Gigabit Ethernet 1000BASE-SX.	3,450	2	6,900
10mo Piso	La propuesta incluyo: 04 Business Policy Switch 2000, 04 Módulos de Stack y Cables, 04 Módulos para enlaces Gigabit Ethernet 1000BASE-SX.	3,450	4	13,800
8vo Piso	La propuesta incluyo: 04 Business Policy Switch 2000, 04 Módulos de Stack y Cables, 04 Módulos para enlaces Gigabit Ethernet 1000BASE-SX.	3,450	4	13,800
7mo Piso	La propuesta incluyo: 03 Business Policy Switch 2000, 03 Módulos de Stack y Cables, 03 Módulos para enlaces Gigabit Ethernet 1000BASE-SX.	3,450	3	10,350
6to Piso	La propuesta incluyo: 04 Business Policy Switch 2000, 04 Módulos de Stack y Cables, 04 Módulos para enlaces Gigabit Ethernet 1000BASE-SX.	3,450	4	13,800
			TOTAL VALOR VENTA U.S.$	**182,834**

Tabla 6.5 Resumen Económico de los switches propuesto para la Red LAN de la Sede Administrativa.

CONCLUSIONES Y RECOMENDACIONES

1. La red implementada para la empresa en mención es una red construida solidamente y confiable. Algunas mejoras y optimizaciones pueden aún ser realizadas para hacerla aún mejor. Es más, manteniendo las actualizaciones del release de software a la última versión estable, podría proveer nuevas características y reparación de fallas de software "bug fixes".que aunque no estén presente en la red, podrían afectar la correcta operación de la red.
2. Al actualizar los switches de core con la última versión de software liberado, podríamos implementar nuevas características disponibles en los switches de core Passport 8600 para optimizar la red tales como : La implementación de SMLT "Split Multilink Trunking" sobre los switches de core para obtener mayor redundancia en capa 2 incrementando la disponibilidad de la red , la implementación de mecanismo de seguridad, tales como SNMPv3, SSHv2 y autentificación mediante RADIUS.
3. Igualmente podríamos habilitar la QoS en capa 3 (DiffServ) sobre todos los switches vía filtros estáticos o vía filtros dinámicos usando herramientas de software como el "Optivity Policy Service" proveído por el fabricante Nortel Networks. También podríamos realizar una efectiva administración de la red vía el software Optivity NMS.

4. Otra mejora que se puede realizar es ir eliminando las rutas estáticas y dejar que el protocolo OSPF implementado en la red se encargue del enrutamiento, teniendo en cuenta que a más rutas estáticas el control se hace más complejo.En el caso que sea necesario una ruta estática, también se puede publicar esa ruta dentro del protocolo OSPF, pero esta funcionalidad propia de los switches Passport 8600 hay que configurarla.

BIBLIOGRAFÍA

[1] Alfredo Rodríguez, "Redes de Telecomunicaciones", Universidad Nacional de Ingeniería – Perú, Notas de Curso, 2002

[2] Nortel Networks, "Passport 1000/8000 Configuration and Management Student Guide (7515)" , April 2001.

[3] Nortel Networks, "Passport 8600 Advanced Layer 2-7 Configuration Student Guide (7516)" June 2002.

[4] Nortel Networks, "Networking Concepts for the Passport 8000 Series Switch", Part Number 207307-D, July 2001.

[5] Nortel Networks, "Passport 8000 Series Network Design Guidelines Release 3.2 Implementation Notes", Part Number 313197-A, April 2002

[6] Steve MCQuerry, "Interconexión de Dispositivos de Red Cisco", Editorial Cisco Press, 2000

[7] Brian Hill, "Manual de referencia CISCO", Editorial McGraw-Hill, 2002.

[8] James Edwards, "Manual de Nortel Networks", Editorial MCGraw-Hill, Noviembre 2001

[9] Merilee Ford, "Tecnologías de Interconectividad de Redes", Editorial Cisco Press, 1998.

[10] Willian Stallings, "Comunicaciones y Redes de Computadores", Editorial Prentice Hall, 2000

[11] Kitty Haller, "Designing Campus Networks", Editorial Cisco Press, 1998

[12] Karen Webb, "Building Cisco Multilayer Switched Networks", Editorial Cisco Press, 2000

[13] Catherine Paquet, "Creación de Redes Cisco Escalables", Editorial Cisco Press, 2001

[14] Kennedy Clark, "CCIE Professional Development Cisco LAN Switching" Editorial Cisco Press 1999.