UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

"DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO E INTERCONEXIÓN DE REDES LAN"

INFORME DE INGENIERIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALDO ALAN CHAGUA SALINAS

PROMOCIÓN
1995-I

LIMA – PERU
2004

Dedicatoria:

A mis padres Marcial y Elvira, mis hermanos, y familiares por su apoyo de siempre.

A mi hermano Marlon por toda la ayuda y el apoyo.

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CABLEADO ESTRUCTURADO E INTERCONEXIÓN DE REDES LAN

SUMARIO

Internetworking – la comunicación entre dos o mas redes – que une cada aspecto de la conectividad entre computadoras. Las Internetworks han crecido bastamente y soportan requerimientos de comunicación de sistemas finales ampliamente dispersas. Una Internetwork requiere muchos protocolos y características para permitir una escalabilidad y una administrabilidad sin la intervención manual constante.

A pesar de los mejoramientos en la performancia de los equipos y las capacidades del medio, el diseño de "Internetwork" viene a ser muy difícil. La tendencia es mas y mas hacia ambientes complejos envolviendo múltiples medios, múltiples protocolos y la interconexión a redes externas al control y dominio de cualquier organización. El presente informe de ingeniería nos muestra muchas de las tecnologías de redes disponibles hoy en día, y que el uso adecuado, cuidados y complementado de cada uno de ellas nos permite desarrollar e implementar Internetworks con alta funcionalidad, adaptabilidad, escalabilidad y administrabilidad.

ÍNDICE

CAPÍTULO II

CAPÍTULO III

CAPÍTULO VII

CAPÍTULO VIII

INTRODUCCIÓN

Hoy en día, las redes de datos se han convertido en una parte fundamental e indispensable para la operación y gestión de las empresas, a través del cual es posible el acceso a los Sistemas de Información, Bases de Datos, Programas de Aplicación, acceso a Internet, etc. Así por ejemplo, las redes globales reúnen datos sobre temas diversos, como condiciones atmosféricas, la producción de cosechas, el tráfico aéreo, y muchos otros mas. Otros grupos establecen listas de correo electrónico para poder compartir información de interés común.

Hace 15 años evolucionó la tecnología que hizo posible la interconexión de muchas redes físicas diferentes y las hizo funcionar como una unidad coordinada. Esta tecnología, llamada Internetworking, unifica diferentes tecnologías de hardware al proporcionarnos un conjunto de normas de comunicación y una forma de interconectar redes heterogéneas.

El presente informe diseña e implementa una Red de datos, mediante la selección y el complemento de las diversas tecnologías existentes en la actualidad, para finalmente obtener una Red de datos de excelente performance. El diseño de la Red responde a las características y requerimientos particulares de la empresa AmericaCom. Debemos señalar

que el diseño desarrollado no es la única, y que su variación va a depender de la tecnología, el tipo de topología y modelo de red que se ajuste a las necesidades particulares de cada empresa.

El informe se divide en ocho capítulos, cada unos de las cuales fueron necesarias para el entendimiento de las nuevas tecnologías que se han desarrollado en el mundo de la red de datos. En el primer capítulo hacemos un recuerdo breve de las tecnologías antiguas para la red de datos, identificamos los tipos de redes existentes y finalmente explicamos los motivos de una estandarización de los productos a través del modelo de referencia OSI. El segundo capítulo nos centralizamos en las tecnologías desarrolladas sobre las redes Ethernet. El tercer capítulo abarca un concepto muy importante, que a veces no es tomado en cuenta y que finalmente nos lleva a una red con baja performance, nos referimos a las tecnologías empleadas en el cableado físico para redes de datos. El cuarto y quinto capítulo mostramos las diversas tecnologías desarrolladas a través de los años, tanto para el proceso de switching como para la del routing respectivamente. En el sexto capítulo desarrollamos las técnicas de diseño y determinamos los requerimientos y consideraciones de diseño para una red de datos. En el séptimo capítulo explicamos los diferentes modos de utilización de las diferentes tecnologías aplicadas a las redes de datos, la cual nos permitió seleccionar las tecnologías que mejor serán aplicadas a los requerimientos de la empresa. Y en el último capítulo implementamos el tipo específico de modelo de red seleccionado, así como también mostramos las

configuraciones realizadas para cada equipo de comunicación y el presupuesto para la implementación del diseño seleccionado.

Para la elaboración del informe, nos basamos por los conceptos vertidos en la documentación a través de los manuales, libros y página web desarrollados por la compañía Cisco System SA. Así como también la documentación de seminarios y cursos de certificación en cableado estructurado. Y lo mas importante, se basó en la experiencia de trabajos de campo y pruebas de laboratorio desarrollados por el personal, debido a las actualizaciones de hardware y software para las nuevas tecnologías emergentes, constituyendo de esta manera el "Know How" que toda empresa debería enfocar.

CAPÍTULO I

CONCEPTOS GENERALES

1.1.- EVOLUCION DE LA INTERNETWORK

La evolución de las Redes es en gran medida una evolución de funciones y capacidades. Cada fase nueva en la evolución de networking incorpora y expande la funcionalidad (como métodos de comunicación y velocidades de acceso) de la fase previa, comenzando en 1960 y continuando hasta los días presentes.

En 1960 y comienzos de 1970, la comunicación de las computadoras fue organizada típicamente en forma de terminales tontos conectados a un Host principal (mainframe). Todo el procesamiento y las memorias residían en el Host. Este ambiente de computación centralizado requería líneas de acceso de baja velocidad que el terminal usaba para comunicarse con el Host centralizado. Esta tecnología de networking habilitó a los usuarios a acceder a los recursos centralizados compartidos.

Las redes computadoras IBM con System Network Architecture (SNA) y redes de datos X.25 son típicamente ejemplos de este tipo de ambientes.

Una única computadora, accesando a los recursos, corriendo programas y copiando archivos son relativamente trabajos muy duros y tediosos, ya que tienen que identificar la solicitud del usuario y el dispositivo destino o el programa, y luego coordinar el acceso entre ellos. Una computadora es el master de todos los recursos y así fácilmente puede administrar y coordinar. En una Red estas actividades son mas complejas.

En los años 70´s y 80´s las PC´s revolucionaron la comunicación tradicional y las redes de computadoras, las PC fueron dispositivos Stand Alone que ponen en la carpeta del usuario capacidades de procesamiento y amplia memoria. Sin embargo, algunos de los recursos, tales como impresoras y discos duros para aplicaciones intensivas de memoria fueron costosos y no eficientes para cada carpeta. Las LAN´s (Local Area Network) fueron en un primer lugar habilitadas para compartir los recursos caros.

La importancia estratégica de las redes interconectadas fue rápidamente desarrollada. Las Organizaciones empezaron a moverse hacia las LAN aisladas. Las redes interconectadas han provisto las bases para las aplicaciones wide-enterprice, tales como e-mail y transferencia de archivos. Estas aplicaciones incrementaron su productividad y competitividad.

Adicional a las PC´s, las minicomputadoras y WANs compartidos (Wide Area Network) se desarrolló en los 70´s y 80´s. Las minicomputadoras, algunas veces ubicados fuera del centro de datos, facilitó

la emergencia de distribuir el procesamiento de datos, mediante el cual el procesamiento de la información ocurría fuera de la minicomputadora en un terminal que soportaba un procesador y una memoria. Ejemplos de este sistema son el Digital Equipment Corporation VAX system y redes DECnet.

En general, las aplicaciones de diferentes ambientes de computación permanecen separados uno del otro. Diferentes protocolos de comunicación fueron desarrollados para soportar comunicaciones entre varios ambientes, como por ejemplo LAN y SNA.

En 1980 y 1990 las Internetworks juntan a la LAN y la WAN, los sistemas de computadoras, los softwares y una variedad de dispositivos diferentes se juntan para formar una infraestructura de comunicación corporativa. Por ejemplo la figura 1-1 denota una red que consiste de un mainframe, minicomputadoras y dispositivos basados en PC juntados a través de una variedad de medios e interconectados a través de enlace Wan públicas y privadas. Esta Internetwork mueve información desde cualquier lugar dentro de una corporación hacia sus clientes o partners externos. Sirviendo como highway de información de la organización, las internetworks viene a ser la estrategia clave y la ventaja competitiva.

Los routers son un elemento clave en este internetwork por que permiten o niegan la comunición entre LANs y WANs.

Las internetwork de hoy día combina una variedad de dispositivos, tipos de medios y métodos de transmisión. Para muchos negocios las redes de hoy son una mezcla ad-hoc de tecnologías antiguas y nuevas. Las redes locales, redes públicas y privadas, líneas dedicadas y canales mainframe de alta velocidad, se han adicionado a la Internetwork justo a tiempo,

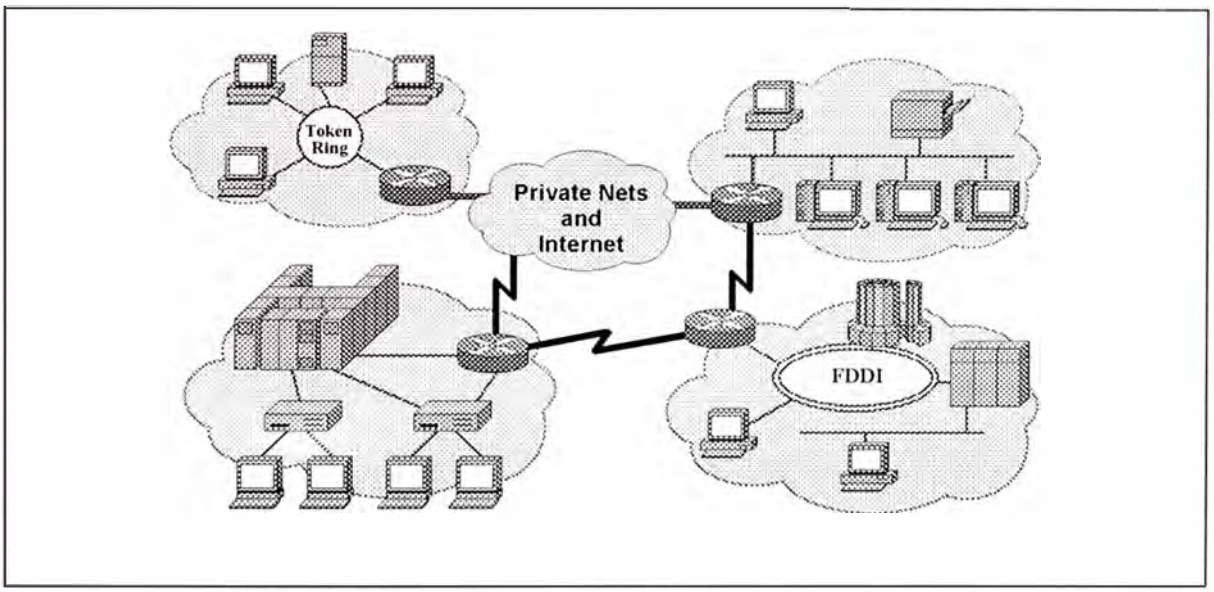


Fig: 1-1 Las internetworks de hoy combinan una variedad de equipos, tipos de medios y métodos de transmisión.

La ventaja en la mayoría de las organizaciones de comunicación, es cambiar rápidamente en respuesta a las nuevas tecnologías , envolviendo requerimientos de negocios y la necesidad para la transferencia de conocimiento instantáneo. Para encontrar estos requerimientos, las internetworks sea cual fuere la forma que tome, tiene que ser flexible, escalable y adaptable para cualquier nivel organizacional. Tiene que ser cuidadosamente diseñado para reflejar los patrones de tráfico de red esperados. Los ingenieros de red y los administradores tiene que conocer y

entender como los packetes de datos son ruteados a través de la red, para asegurar que un sistema de interconexión eficiente se ha ubicado en el lugar para manipular la demanda de las redes de hoy crecientes rápidamente.

En los 90´s la presión mas grande en la red en un futuro inmediato es la globalización de negocios, y el soporte de aplicaciones requeridos para conducir el negocio internamente y con clientes alrededor del mundo. No es inusual ahora que una compañía requiera de 100 aplicaciones para funcionar en una internetwork global.

Los estudios manifiestan que las redes requieren mas ancho de banda para soportar estas aplicaciones y conexiones de internetwork. Las redes necesitarían de encontrar tales requerimientos para proveer bajo retardo, ancho de banda en demanda, y otros nuevos servicios. Las redes actuales y futuras tendrían mas funciones distribuidas y tienen que proveer la integración de voz, data y video.

Como ejemplo tomemos la figura 1-2. Esta internetwork global soporta una variedad de equipos y aplicaciones que tiene necesidades de velocidad y ancho de banda variada. En el caso de video streaming, transferencia de audio y transferencia de archivos gráficos por ejemplo, la ruta de la data tiene que proveer bajo retardo de comunicación end-to-end confiables ofrecidas a través de la tecnología de switching ATM. Las minicomputadoras y computadoras portátiles, las cuales requieren soporte

para tráfico bursty, pueden ser globalmente ruteados a través de conexiones seriales.

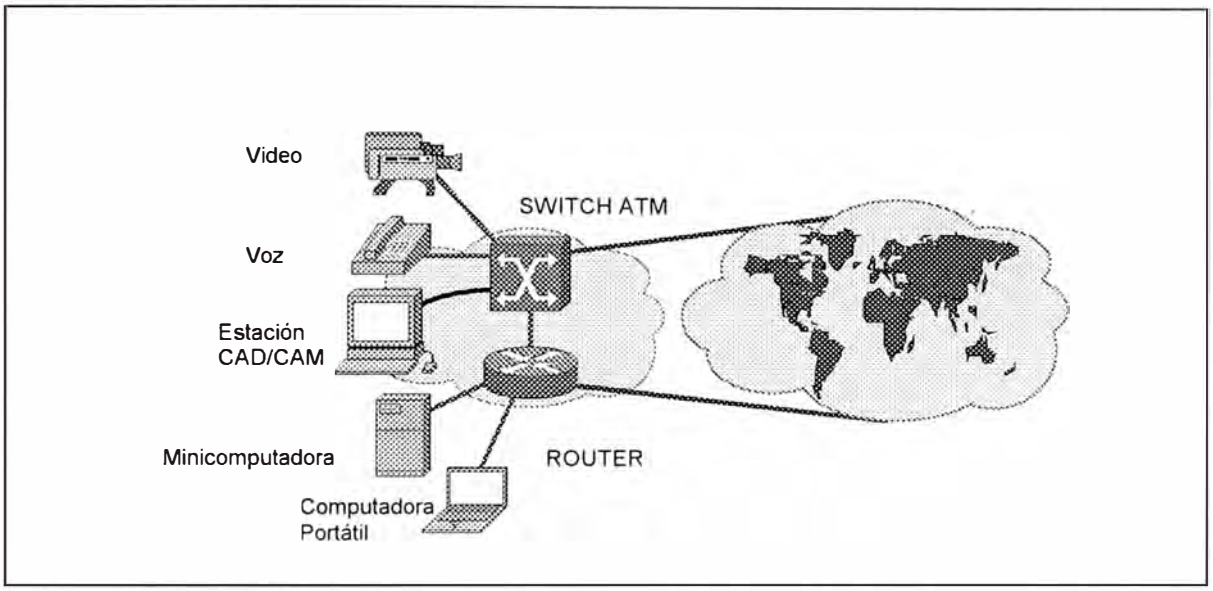


Fig. 1-2 Las internetwork globales soportan una variedad de tipos de tráfico.

Los siguientes son características de las redes globales:

- Uso incrementado de gráficas e imagen
- Archivos extensos
- Programas extensos
- Computing Cliente/servidor
- Tráfico de red bursty

El internetworking global proveería ambientes para aplicaciones emergentes que requerirían grandes cantidades de ancho de banda. Muchas de estas aplicaciones son guiados por la evolución de los requerimientos de la multimedia que tiene una imagen de alta definición, video full movimiento o componentes de audio digitalizado.

1.2.- TIPOS DE REDES Y DISPOSITIVOS

Las Internetworks globales de hoy puedes ser divididos en tres tipos distintos:

- Local Area networks (LANs)
- Wide Area Networks (WANs)
- Enterprice Networks

Cada tipo de red usa un tipo diferente de dispositivos. Es necesario familiarizarnos con cada uno de ellos para poder entender como estos dispositivos se relacionan con los otros y como el tráfico ocasionado por ellos puede o no ser ruteado a través de la internetworking.

1.2.1.- Local Area Networks (LANs)

Las LANs son diseñados para operar dentro de un área geográfica limitada y permite a múltiples usuarios acceder simultáneamente al medio de alto ancho de banda. Típicamente las LANs conectan dispositivos físicamente adyacentes y son controlados por la administración local.

Las características de las LAN son las siguientes:

- La RED opera dentro de un edificio o piso de un edificio. Debido al incremento dee la potencia de los dispositivos desktop, la clave es reducir el tamaño de las LANs y conectar pequeñas LANs juntas usando routers.

- Las LANs proveen múltiples dispositivos conectados (usualmente PCs) con acceso a un medio con alto ancho de banda.
- Un enterprice adquiere el medio y las conexiones usadas en la LAN, este puede privadamente controlar la LAN como este elija.
- Los servicios locales están usualmente disponibles; Las LANs raramente desconectan o restringen el acceso a las estaciones conectadas.

Típicamente los dispositivos LAN incluyen repetidores , bridges, hubs, switches, routers y gateways.

Repetidores.- Estos dispositivos generan y propagan señales desde un segmento de red a otro. Ellos no cambian la direcciones o la data en si, únicamente pasan la data . Los repetidores no pueden filtrar paquetes, aunque un repetidor ayuda a extender la distancia de la red mediante la regeneración de la señal. Además debemos de tener en cuenta que usar un repetidor resulta de combinar varios segmentos de red y unirlos en una sola. La figura 1-3, nos muestra como aparece un repetidor en una red LAN.

Algunos repetidores son usados entre el host fuente y el host destino para ayudar a compensar la degradación de la señal debido a la atenuación, lo cual trae como resultado una fuente de latencia, siendo esta el tiempo que le toma a una señal viajar entre el host fuente y el destino.

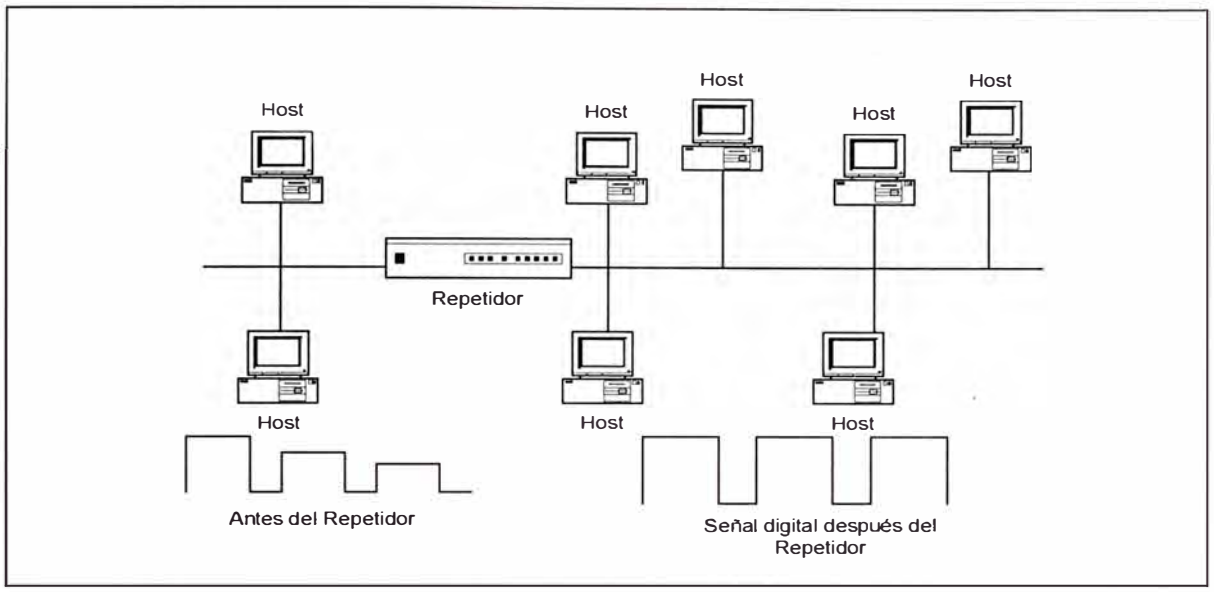


Fig. 1-3 Repetidores en una Red de Área Local (LAN).

Bridges.- Estos dispositivos también regeneran la señal, pero son más inteligentes que los repetidores. Un bridge puede leer la dirección Mac (Media Access Control) del host destino o dirección de hardware desde la trama de data, y determina si el host destino esta en el segmento local (el segmento desde el cual es recibido la trama) ó a otro segmento. Si el host destino está en el segmento local, no forwardea la trama, caso contrario el brigde forwardea la trama a todos los otros segmentos de red. La figura 1-4 muestra como un bridge trabaja en una LAN.

Cuando se usa un bridge en vez que un repetidor, nos da mayor ancho de banda por usuario, ya que se traduce en pocos usuarios por segmentos de red. Pero todo esto se puede traducir en problemas de latencia de hasta un 20 a 30 % debido al procesamiento y filtrado de tramas. Hay que adicionar

también que los bridges generan broadcasts y lo propagan a todos los demás segmentos.

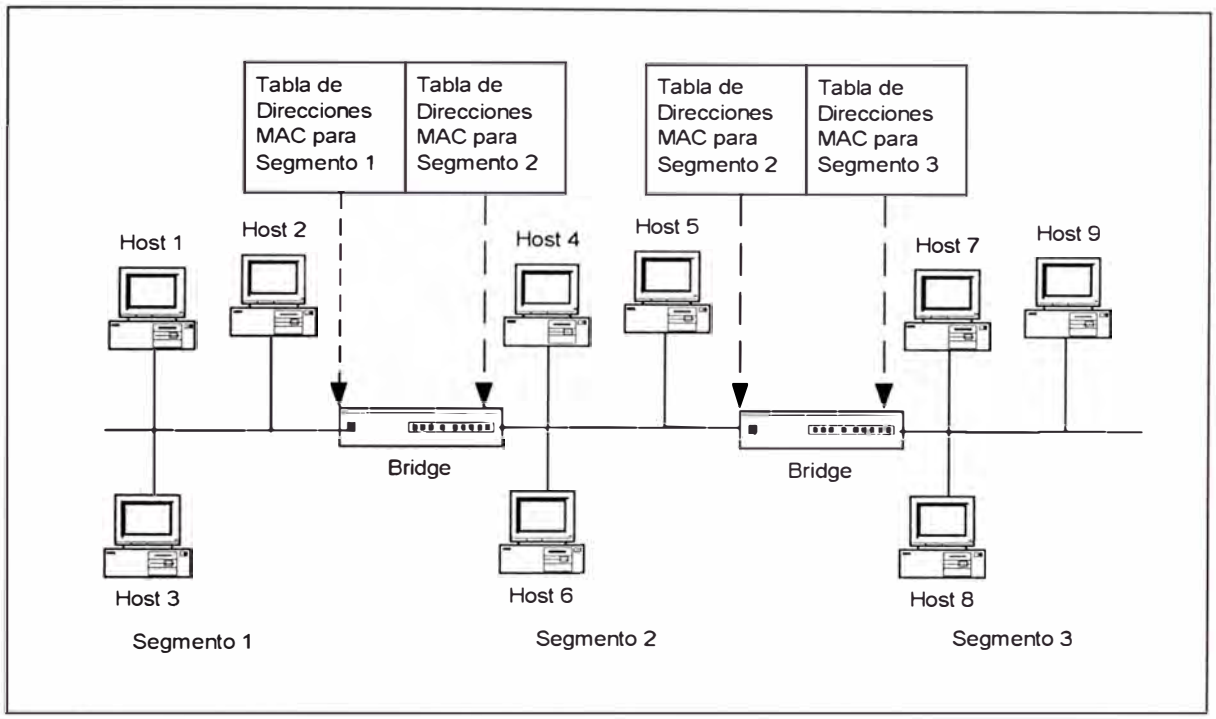


Fig. 1-4 Bridging en una Red de Área Local (LAN).

Hubs.- El hub conecta todas las conexiones de una LAN dentro de un concentrador, estos dispositivos pueden considerarse como un repetidor multipuerto. Las PCs puede conectarse usando cable coaxial o par trensado, o también en radio frecuencia (RF). Cuando una PC transmita una señal dentro de la Red, esta señal es transmitido a todos los otros segmentos que están conectados al hub.

Switches.- A diferencia de los Hubs, los switches pueden operar en modo full dúplex, esto significa que las computadoras y el switch puede transmitir y recibir información simultáneamente. La mas grande diferencia entre el switch y el hub es que cuando una computadora transmite una señal digital

al hub, este es enviado a todos los puertos de hub, sin embargo un switch enviará la señal digital únicamente al puerto específico donde la dirección MAC del destino es localizado. Así podemos imaginar que cada puerto de un switch es un extremadamente rápido bridge multipuerto.

Routers.- Estos dispositivos están un paso mas arriba que los bridges. Los bridges filtran las direcciones MAC, pero los routers pueden filtrar las direcciones MAC y las direcciones de red (IP address). Cuando un bridge forwardea paquetes, este lo envía todos les segmentos conectados, mientras que un router sólo lo hace al segmento de red al cual el paquetes es destinado. Los routers económicamente previenen tráfico de Red innecesario debido a que primero leen la dirección de Red de los paquetes que llegan antes de forwardearlos. La fig 1-5 muestra una red típica segmentada por un router

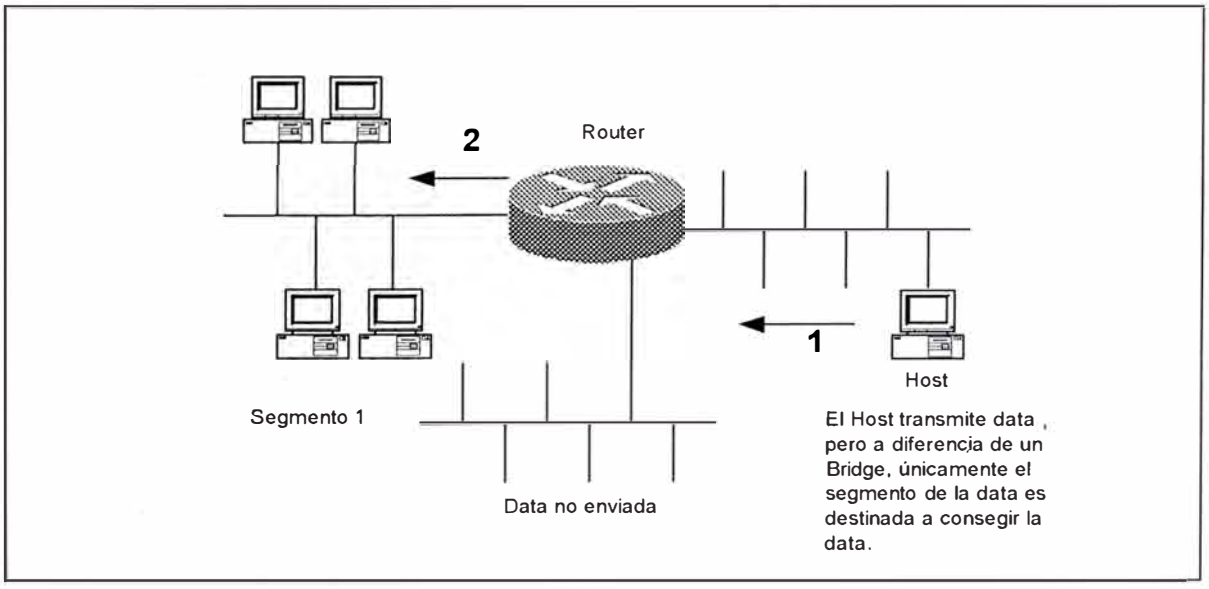


Fig. 1-5 Un Router segmentando una Red de Área Local (LAN).

Gateways.- Estos dispositivos fueron creados con software, la cual pueden operar en PCs y routers. Ellos enlazan diferentes programas y protocolos y examinan el paquete entero, incluyendo la porción de la data, con la finalidad traducir protocolos incompatibles. Por ejemplo, para intercambiar e-mail entre un CCMail server y un Exchange server, se deberías tener instalado un mail gateway. Otro ejemplo son los servicios gateway que operan en un router, que podrían enlazar un red IP a una red IPX para que los usuarios en ambas redes puedan comunicarse transparentemente.

Switches ATM (Asynchronous Transfer Model).- Estos dispositivos proveen switching de celdas a altas velocidades. ATM usa la tecnología cell relay que combina las ventajas de un circuito convencional y el sistema de conmutación de paquetes.

1.2.2.- Wide Area Networks (WANs)

Las redes WANs son diseñados para operar entre una mezcla grande de Carrier de telecomunicaciones,y típicamente permite los accesos sobre interfaces operando a bajas velocidades. Las WANs pueden ser diseñados para proveer conectividad full–time o part-time (Dial on Demand) sobre área amplias y globales.

Las características mayores de una red WAN son las siguientes.

- La redes operan mas allá de la ubicación geográfica de las redes LAN. Usa servicos de Carriers como AT&T LA , Bellsouth, Telefónica y Global Crosing en el Perú
- Las Wans usan conexiones seriales de varios tipos para acceder al ancho de banda sobre áreas geográficas amplias.
- Una enterprice paga a los carrier proveedor de servicios para conexiones usadas en las WAN . Los enterprice pueden elegir que servicio usar. Los Carrier son usualmente reguladas por tarifas.
- Las WANs raramente se cortan, pero debido a que el enterprice tiene que pagar por el servicio usado, este pueden restringir el acceso a las estaciones de trabajo conectadas. No todos los servicios WAN son disponibles en todas partes.

Los dispositivos WAN típicos son los siguientes.

Routers.- Estos dispositivos ofrecen muchos servicios, tales como internetworking y control de interface WAN.

Switches.- Son dispositivos que conectan comunicaciones de voz, data, video, Frame relay, X.25 al ancho de banda de la WAN. Estos switches WAN pueden compartir ancho de banda de acuerdo a las prioridades del servicios, proveer sistemas de administración y diseños de red.

Modems.- Son equipos que interactúan con servicios de grado de voz, como por ejemplo, las CSU/DSU channel service units/digital service units interactúan con los servicios E1/T1. TA/NT1 termninal adapters/network Termination 1 interactúan con los servicios ISDN Integrated Service Digital Network

Access Server.- Son equipos que concentran comunicaciones análogas dial-in y dial-out y proveen otros servicios, tales como traducción de protocolos entre Telnet y el protocolo PAD assembler de X.25.

Multiplexores.- Son equipos que permiten que mas de una señal sea transmitido fuera simultáneamente sobre una circuito físico.

Switches ATM.- Son los que nos proporcionan switching de celdas a altas velocidades.

1.2.3.- Redes Enterprice

Enterprice, es una corporación, agencia, proveedor de servicios u otra organización que une su data, sistema de computo, comunicaciones, y sus recursos. Una red Enterprice usualmente contienen elementos de red pública y privada. Cualquier o todos los dispositivos LAN y WAN descritos pueden ser encontrados en una red Enterprice. El desarrollo de redes Enterprice incluyen:

- LANs interconectados para proveer aplicaciones cliente/servidor integradas con la aplicaciones tradicionales desde los cetros de data (mainframes).
- Las necesidades de los usuarios finales para mayor ancho de banda en las LANs, los cuales pueden ser consolidados como un switch y llevados a través de un medio dedicado.
- Integración de redes separadas, para que el tráfico nonbursty provenientes de aplicaciones ded voz y video coexistan en una única red.
- Relaying tecnologías para servicios WAN, con un rápido crecimiento en Frame Realy y otro crecimiento gradual en cell relay (por ejemplo TAM).

1.3.- EL MODELO DE REFERENCIA OSI

Cuando las redes llegaron, las nubes de computadoras, típicamente se comunicaban únicamente con las computadoras de los mismos fabricantes, así por ejemplo muchas Compañías tenían implementado una solución DEC-Net o una solución IBM, pero no ambos juntos. A comienzos de 1980 el modelo OSI (Open System Interconection) fue creado por el International Standars Organitation (ISO) para quebrar esta barrera. Esto significó ayudar a los vendedores a crear dispositivos de Red Inter-operables.

El modelo OSI es el primer modelo de arquitectura para redes. Describe como la data y la información de red es comunicada desde la aplicación en una computadora, a través del medio de red, a otra aplicación en otra computadora.

1.3.1.- El Modelo de Capas

El modelo de referencia es conceptual y nos indica como las comunicaciones deben de realizarse. Direcciona todos los procesos requeridos para una comunicación efectiva y divide estos procesos en grupos lógicos llamados Capas (Layers en Inglés) . Cuando un sistema de comunicación es diseñado de esta manera es conocido como un layered architecture (arquitectura de capas).

Hay muchas ventajas de usar el modelo de referencia OSI, las causas mas importantes del por qué la industria usa un modelo de capas son:

- Nos manifiesta de forma clara las funciones generales, en vez de especificar como hacerlo.
- Divide la complejidad de las redes en sub-capas mas administrables.
- Define las interfaces estándares para una compatibilidad (plug and play) e integración multivendedor.
- Permite a los ingenieros realizar un diseño especializado y desarrollar esfuerzos en funciones modulares, para crear nuevas aplicaciones y servicios sin cambiar todo el código.

- Promueve la especialización, el cual ayuda al progreso de la industria.
- Permite un fácil diagnostico de averías.

El modelo de referencia OSI tiene siete capas:

1. Aplications (Aplicación).
2. Presentation (Presentación)
3. Session (Sessión)
4. Trasnport (Transporte)
5. Network (Red)
6. Data Link (Enlace de Datos)
7. Physical (Físico)

La figura 1-6 muestra como las capas se juntan.

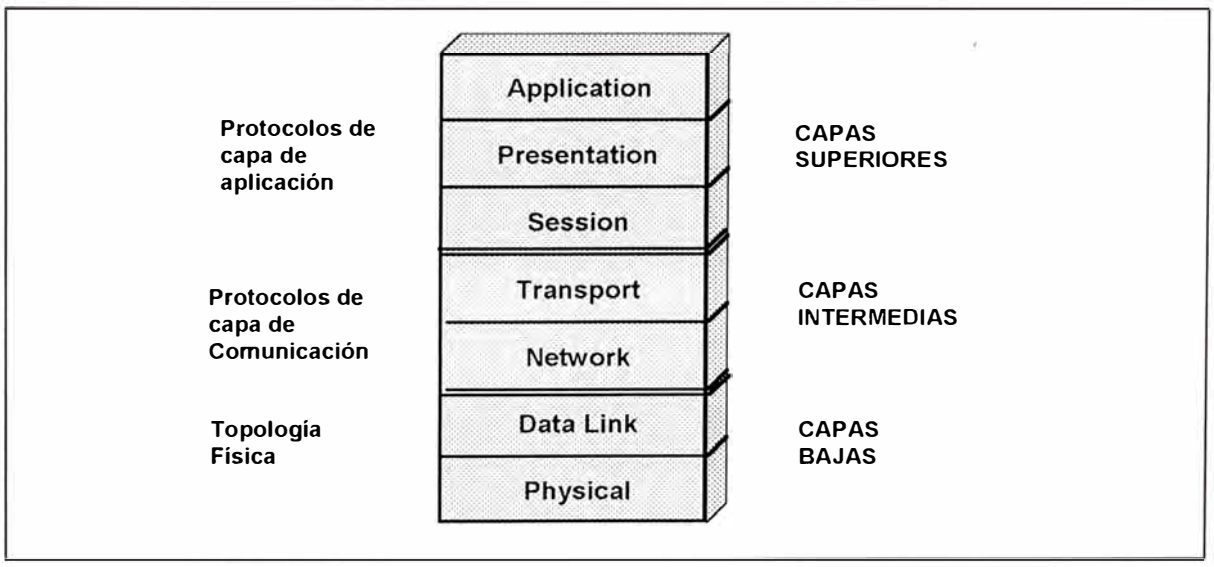


Fig. 1-6 Las capas del modelos de referencia OSI

La tres capas superiores del modelo de referencia OSI – Aplication, Presentation y Session – tratan con funciones que las

aplicaciones hacen posible la comunicación con otras aplicaciones. Ellos especialmente tratan con tareas como formatos de archivos, conjunto de códigos, interfaces de usuario, compresión, encriptación y otras funciones relacionadas al intercambio que ocurre entre aplicaciones. La figura 1-7 muestra las funciones definidas para cada capa en el modelo OSI.

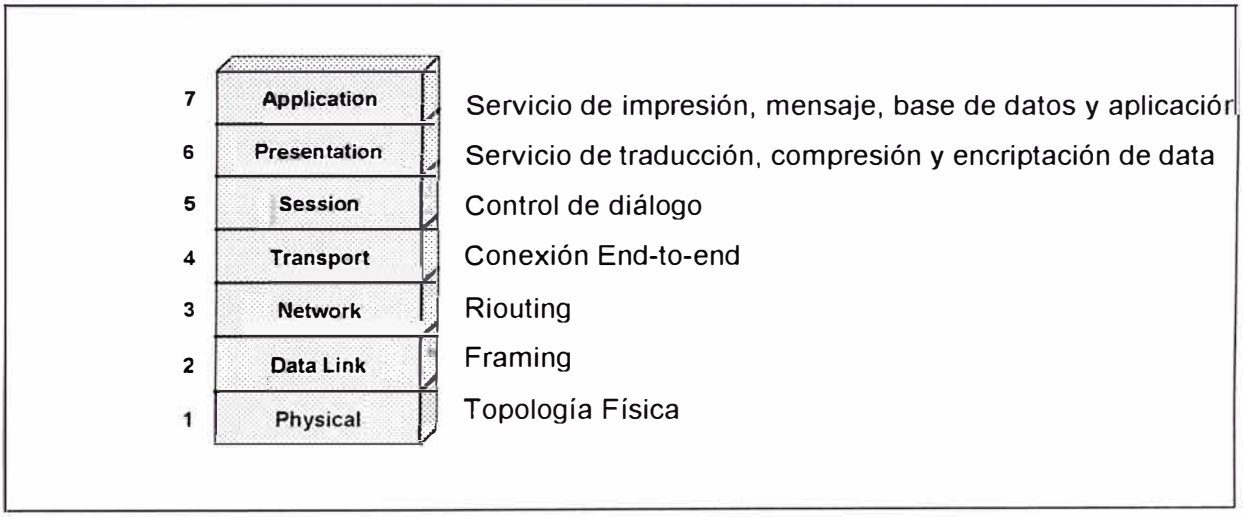


Fig. 1-7 Funciones de las capas del modelo de referencia OSI

La Capa de Aplicación.- La capa de aplicación del modelo OSI, soporta los componentes que tratan con los aspectos de comunicación de una aplicación. La capa de aplicación es responsable de identificar y establecer la disponibilidad del "partner" de comunicación . También es responsable de determinar si hay suficientes recursos para la comunicación a realizar.

Aunque algunas veces las aplicaciones de las computadoras requieren únicamente los recursos del desktop, los componentes de comunicación de una aplicación pueden unir mas de una aplicación de red.

La Capa de Transporte.- La capa de trasporte se encarga de segmentar y reensamblar la data de las aplicaciones superiores, y unirlo en el mismo data stream. Ellos proveen servicio de transporte de datos end-to-end y establece la conexión lógica entre el host transmisor y el host receptor en una internetwork. La capa de transporte es responsable de proveer los mecanismos para la multiplexación de las aplicaciones de la capa superior, establece la sesión y tear-down los circuitos virtuales.

La integridad de la data es asegurada en esta capa por medio del control de flujo y por permitir al usuario la selección de transporte de datos confiable entre sistemas. El control de flujo previene que el host transmisor sobrecarge el buffer del host receptor. Para un transporte de datos confiable se emplea una sesión de comunicación orientada a conexión entre sistemas, y los protocolos aseguran que se realice lo siguiente:

- Los segmentos enviados son "acknowledged back" al transmisor después de su recepción.
- Cualquier segmento no acknowledged son retransmitidos
- Los segmentos son enviados de regreso en forma secuencial en el orden que han llegado a su destino.
- Un flujo de datos administrable es mantenido con la finalidad de evitar congestión, sobrecarga y pérdida de cualquier data.

Una importante razón para que las capas existan en el modelo OSI, es que permite compartir las conexiones de transporte para mas de una aplicación. Esto es posible debido a que las funciones de la capa de transporte ocurre segmento por segmento, y cada segmento es independiente de los otros. Esto nos permite que diferentes aplicaciones envíen segmentos consecutivos, procesados en un primer instante, por un host de destino o por múltiples host

La figura 1-8 muestra como la capa de transporte envía data desde un "host" fuente, originados por varias aplicaciones para comunicarse con la aplicación paralela en uno o muchos "hosts". El número de puerto específico para cada software de aplicación es configurado por el software dentro de la máquina fuente antes de su transmisión. Cuando transmite un mensaje, la computadora fuente agrega bits extras que codifican el tipo de mensaje, el programa con el que fue creado y el protocolo que fue usado. Cada software de aplicación que transmite segmentos en "data stream", usa el mismo puerto preordenado. Cuando la computadora destino recibe el "data stream", es facultado para seleccionar y reunir los segmentos de la aplicación, de esta manera se provee a la capa de transporte con todas las necesidades para pasar la data a su aplicación "peer" de la capa superior.

En operaciones de transporte confiable, un usuario primero establece una sesión orientada a conexión con su sistema "peer". Así, en la

figura 1-9 nos muestra los mensajes enviados en una típica sesión orientada a conexión, efectuado entre el sistema transmisor y receptor.

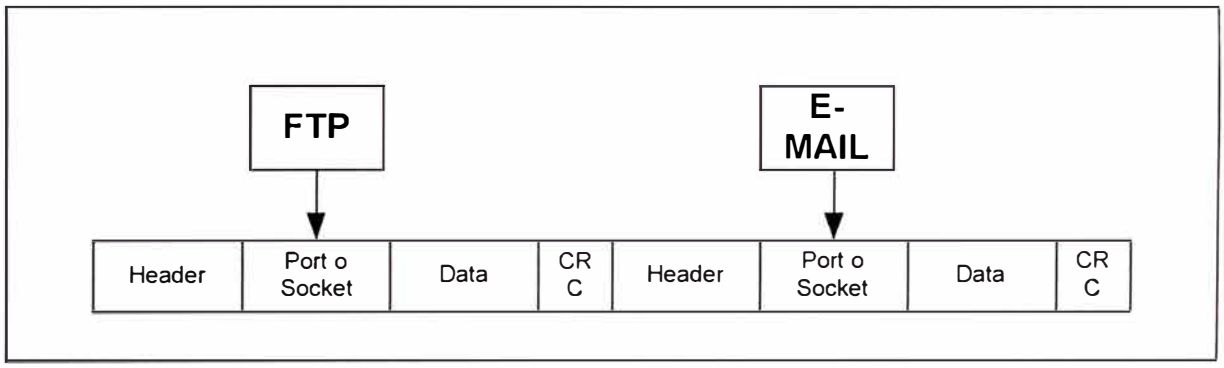


Fig. 1-8 La capa de Transporte segmenta la Data compartiendo un stream de tráfico

Es así que ambos programas de aplicación de los dos host comienzan notificando a sus sistemas de operación individual que una conexión se va a iniciar. Los dos sistemas de operación se comunican enviando mensajes sobre la red confirmando que la transferencia es aprobada y que ambos lados están listos. Una vez que la sincronización requerida es completada, una conexión es establecida completamente y la transferencia de datos comienza.

Mientras que la información está siendo transferida entre los "hosts", las dos máquinas periódicamente se comunican a través del software de protocolo, para asegurar que todo está bien y que los datos estan siendo recibidas apropiadamente. El proceso de conexión mostrado en la figura 1-9 se detalla a continuación.

- El primer segmento "acuerdo de conexión " es una solicitud para sincronización.
- El segundo y tercer segmento confirma (acknoledge) la solicitud y establece los parámetros de conexión entre host.
- El segmento final es también una confirmación (acknoledge), que notifica al host destino que el acuerdo de conexión a sido aceptada y que la conexión actual se ha establecido. La transferencia de datos puede ahora comenzar.

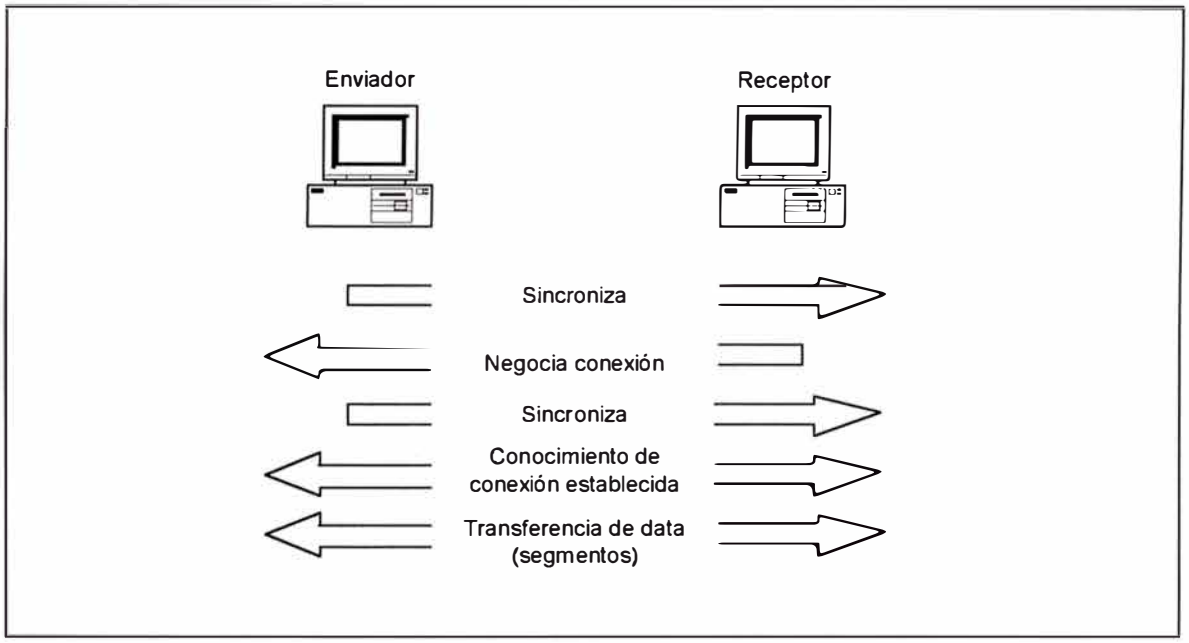


Fig. 1-9 Estableciendo una sesión orientada a conexión.

Durante una transferencia, puede ocurrir una congestión debido a que una computadora de alta velocidad genera tráfico mas rápidamente que la red pueda transferir, o por que muchas computadoras están simultáneamente enviando datagramas a través de un gateway o destino. En ambos casos, el problema es básicamente como un cuello de botella (mucho tráfico para tan pequeña capacidad).

Cuando una máquina recibe un flood de datagramas tan rápidamente que no es posible procesarla, este lo almacena en su memoria. Esta acción de almacenamiento resuelve el problema si los datagramas es parte de un pequeño burst, sin embargo si los datagramas continúan, la memoria del equipo se saturará por lo que su capacidad de flood sería excedido, y descartaría cualquier datagrama adicional. Como el sistema de control de flood trabaja muy bien, en vez de descartar los datagramas y permitir que la data se pierda, el red de transporte puede mandar un indicador de "not ready ", como mostrado en la figura 1-10, a la fuente del flood. Este mecanismo trabaja como un semáforo, indicando al transmisor parar la transmisión de segmentos a su correspondiente peer. Cuando el peer receptor ha procesado los segmentos que se encuentran en su memoria, envía un indicador "ready". La máquina que está esperando transmitir el resto de datagramas recibe el indicador "go", continúa con su trasmisión.

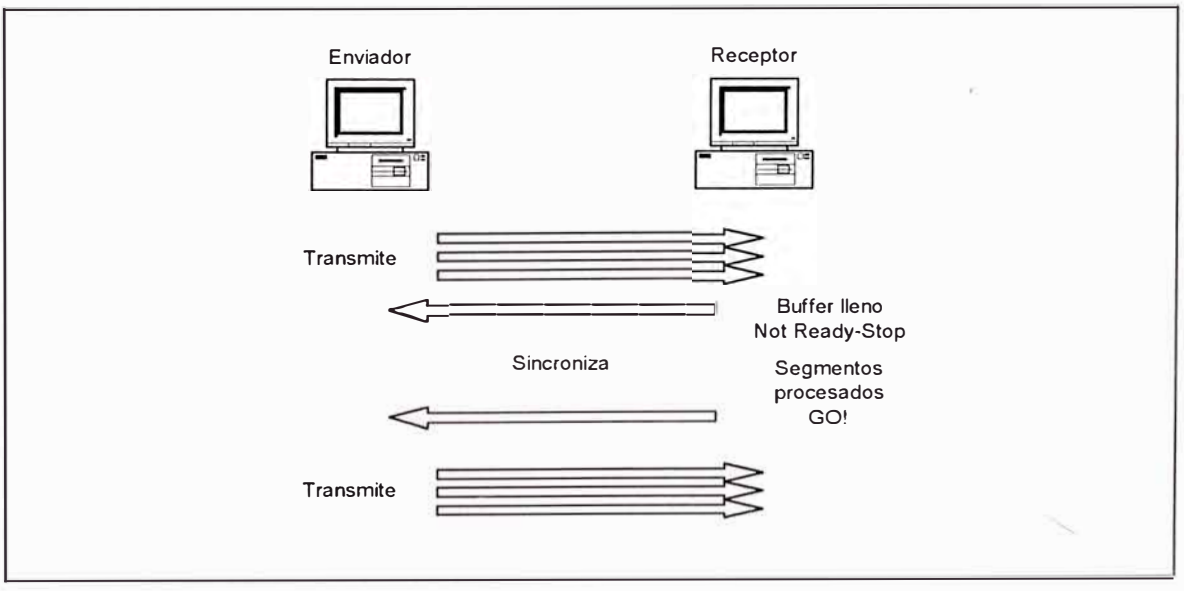


Fig. 1-10 Transmitiendo segmentos con control de flujo.

En una trasferencia de datos orientado a conexión confiable, los datagramas son recibidos en el host receptor en la misma secuencia que fueron enviados, la trasmisión falla si el orden es quebrado. Si cualquier segmento de datos es perdido, duplicado, o dañado a lo largo del camino, es considerado como una falla de transmisión. La respuesta al problema es tener un "host" recibiendo una confirmación (acknoledge) por cada segmento de data enviada.

El "throghput" de datos sería muy bajo si la máquina transmisora tiene que esperar por una confirmación después de enviar cada segmento, esto hace que la comunicación sea lenta y tediosa. Como muchos segmentos pueden ser transmitidos antes que la máquina transmisora reciba una confirmación, esto proceso es llamado " WINDOW".

El windowing controla cuanta información es transferida de un lado a otro. En la figura 1-11 nos muestra un tamaño de window de 1 y un tamaño de window de 3. Cuando es configurado un tamaño de 1, la máquina transmisora espera por una confirmación por cada segmento que transmite antes de enviar otra. Configurando un tamaño de 3, es permitido enviar 3 segmentos de datos antes que una confirmación sea recibida.

El transporte de los datos confiable asegura la integridad del stream de data enviado desde una máquina a otra a través de una red completamente funcional. Esto garantiza que toda la data no se pierdan o

se dupliquen. El método que realiza esta transmisión es conocida como "positive acknoledgment with retransmission". Es técnica necesita que una máquina receptora se comunique con la transmisora mediante el envío de un mensaje de confirmación al transmisor cuando recibe data. El transmisor documenta cada segmento y espera por una confirmación antes de enviar el próximo segmento. Cuando este envía un segmento, la máquina transmisora inicia un timer y retransmite si expira el tiempo antes de que una confirmación para el segmento es retornado desde el receptor.

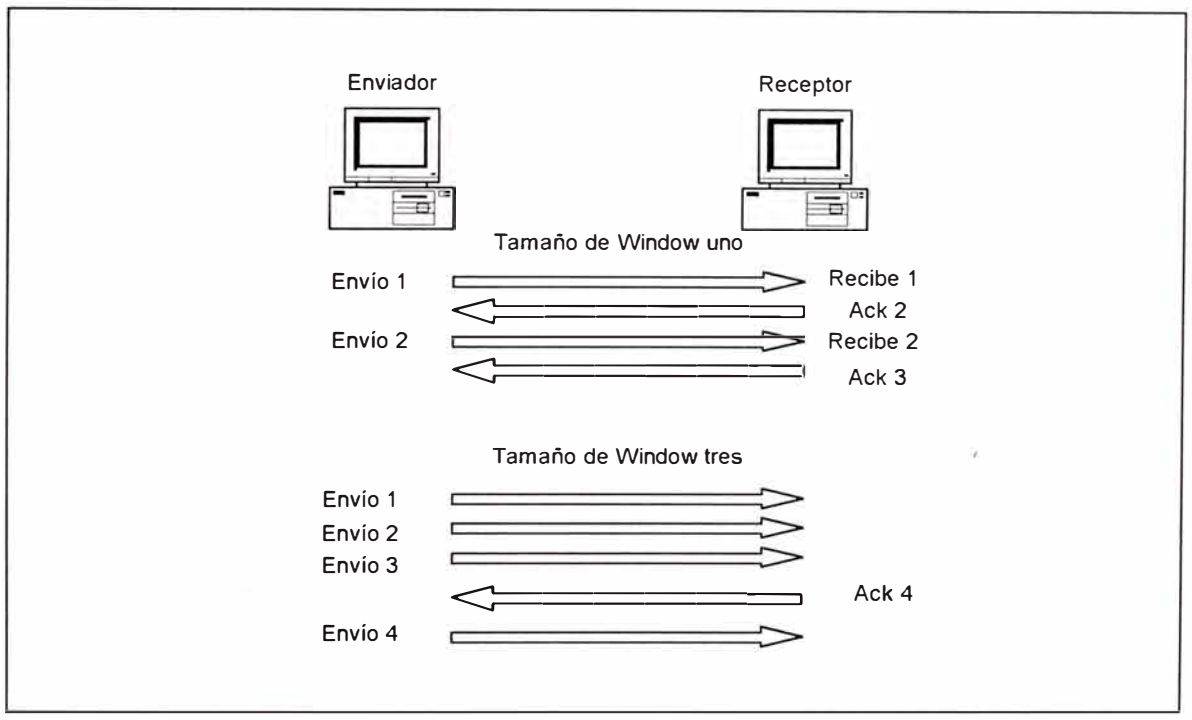


Fig. 1-11 Transmitiendo segmentos a través del windowing

En la figura 1-12, la máquina transmisora envía segmentos 1,2 y 3, la máquina receptora confirma que los ha recibido mediante la solicitud de segmento 4. Cuando recibe la confirmación, el transmisor envía el segmento 4, 5 y 6. Si el segmento 5 no llegó a su destino, el receptor confirma con una solicitud para el que el segmento perdido sea reenviado. La máquina

transmisora reenviaría el segmento perdido y esperaría por una confirmación, quine tiene que recibir en orden para continuar con la transmisión del segmento 7.

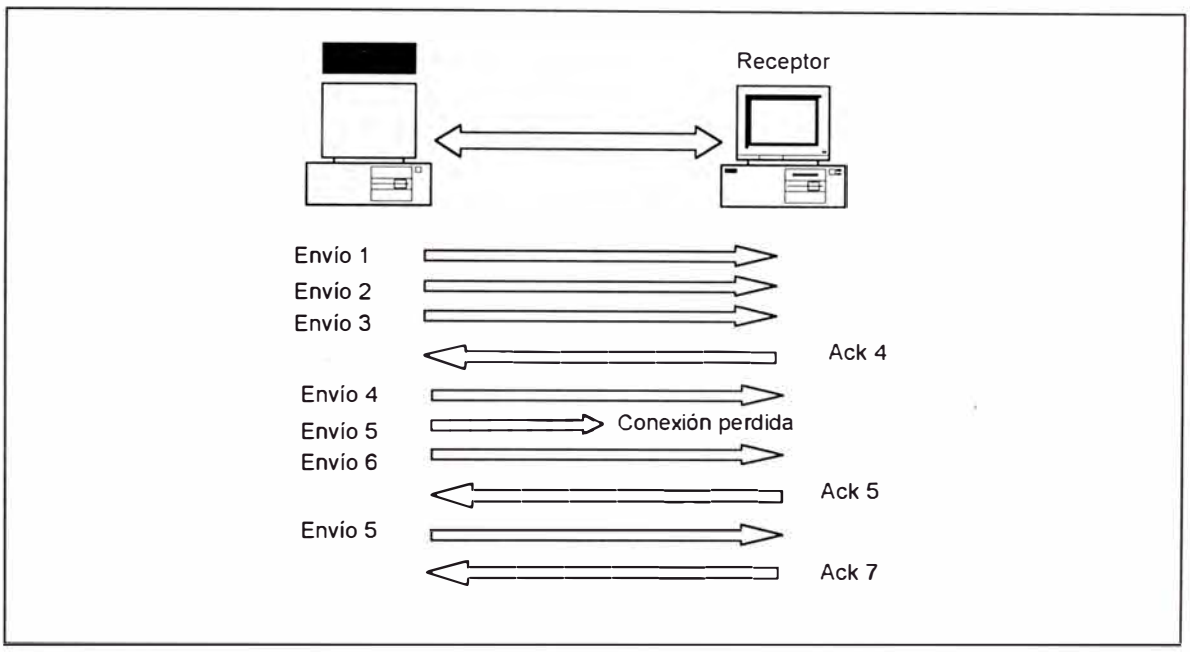


Fig. 1-12 Envío confiable de la capa de Transporte

La Capa de Red.- La capa de red interactúa con las redes, y provee el mejor esfuerzo para llevar los paquetes end-to-end de sus usuarios. La capa de transporte envía paquetes desde la red fuente a la red destino, por lo que una apropiada ruta través de ellos es determinado por protocolos residentes en la capa 3 del modelo OSI. La determinación de ruta hace posible que un router verifique todas las rutas disponibles a un destino dado y decide por la mejor. Los routers usan información de topología de red para orientarse a si mismo en la red y evaluar las rutas diferentes a través de esta. Esa Red " topo maps" puede ser configurada manualmente por los administradores de red o ser obtenida a través de procesos dinámicos operando en la red. La

interface de la capa de red es conectada a la red, y es empleado por la capa de transporte para proveer el mejor servicio de envío de paquetes end-to-end. El trabajo de enviar paquetes desde la red fuente a la red destino es la función primaria de la capa de red. Después que el router decide la mejor ruta desde un punto A a un punto B, procede con el switcheo de los paquetes a través de esta, esto es conocido como "packet switching", que es esencialmente el envío de paquetes recibidos por el router en una interface de red o puerto, hacia el puerto que conecta a la mejor ruta a través de la nube de red.

Una internetwork tiene que continuamente designar todas las rutas de sus medios de conexión. En la figura 1-13, cada router conectado a una línea es numerada, y estos números son usados por el router como direcciones de red, estas direcciones poseen información importante acerca de la ruta del medio de conexión, y son usados por los protocolos de enrutamientos para pasar paquetes de una fuente a su destino. La capa de red crea un compuesto "network map" (un sistema de comunicación estratégica) mediante la combinación de información como el conjunto de enlaces en una internetwork con determinación de ruta, path-swithing, y funciones de procesamiento de ruta. Puede también usar estas direcciones para proveer capacidad confiable e interconectar redes independientes. Las direcciones capa 3 también perfeccionan la performance de la internetwork, no permitiendo broadcast innecesario que consuma ancho de banda. Innecesario broadcast incrementa el overhead de la red y desperdicia la

capacidad en cualquier enlace y las máquinas que no necesitan recibirlo. Usando consistente direccionamiento end-to.-end que describa precisamente la ruta de los medios de conexión permite que la capa de red determine la mejor ruta a un detino sin encumbering el dispositivo o enlaces en la internetwork con broadcast innecesario.

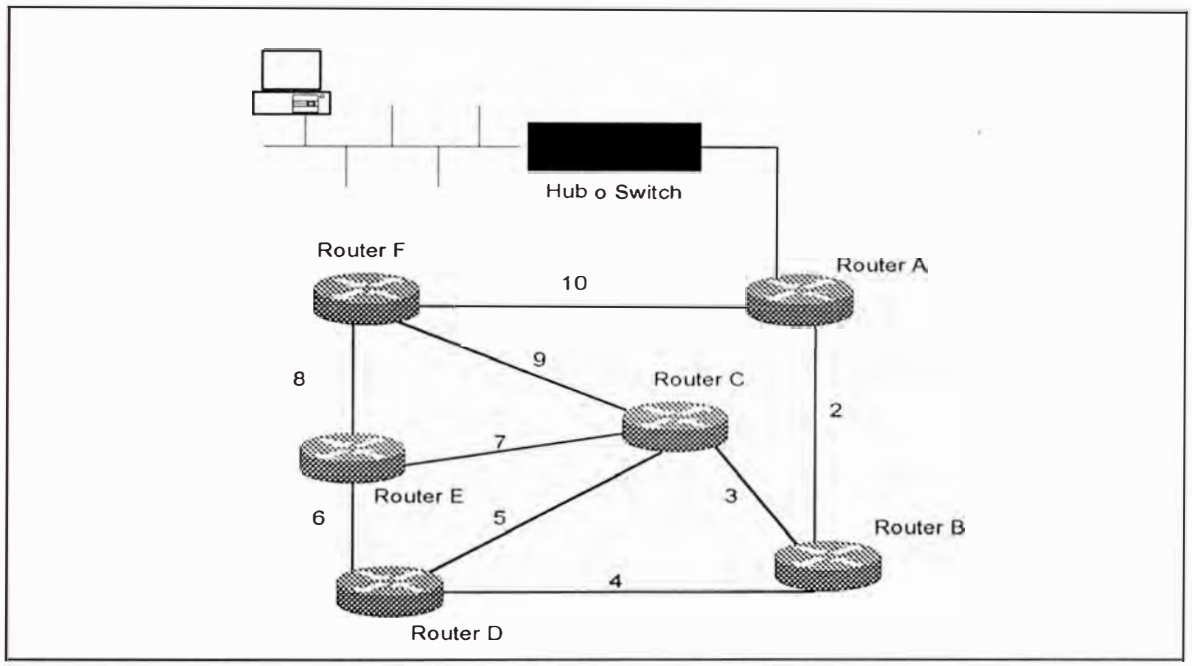


Fig. 1-13 Comunicación a través de una Internetwork.

Cuando una aplicación en un host quiere enviar un paquete a un destino ubicado en una red diferente, una trama de enlace de datos es recibida en un de las interfaces de router, el router procede a de-encapsular la trama, luego lo examina para establecer que clase de data de capa de red es in tow. Después que se ha determinado, la data es enviado al proceso de capa de red apropiado. La misión de la trama es completado y es simplemente descartado.

El proceso de la capa de red es detallada en la figura 1-14, donde examina la cabecera de los paquetes para descubrir la red a la cual está destinado, luego se refiere a su tabla de enrutamiento para encontrar las conexiones que la red actual tiene con la interfaces de red externas. Después que uno es seleccionado, el paquete es re-encapsulado en su trama de enlace de datos con la información de la interface de red seleccionado y espere para llevarlo al próximo salto en la ruta hacia el destino, este proceso es repetido cada vez que el paquete comnuta a otro router. Cuando este alcanza finalmente el router conectado ala red en el cual el host destino es ubicado, el paquete es encapsulado en un tipo de trama de enlace de datos de la red destino. En estos momentos es empaquetado apropiadamente y listo para levarlo al protocolo stack en el host destino.

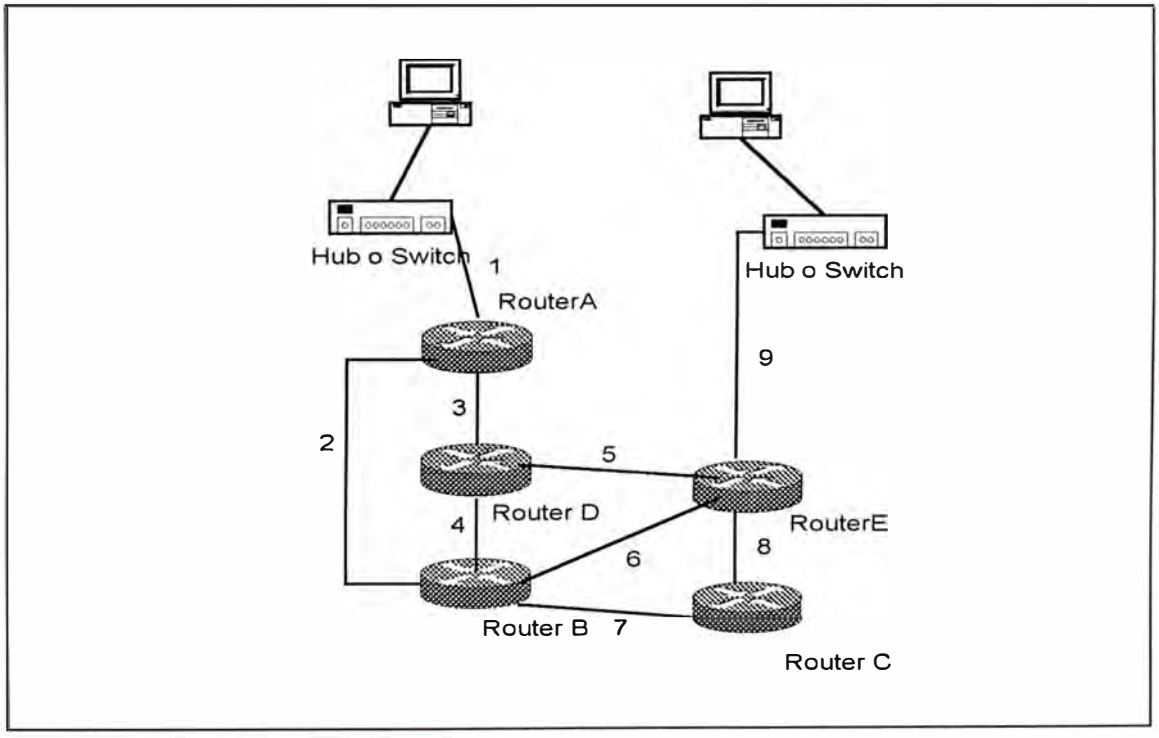


Fig. 1-14 Proceso de la capa de Red.

Los procesos de la capa de red son descritos a continuación:

- La PC transmisora envía un datagrama a una PC ubicada en la red 9
- El router A recibe el datagrama y chequea la red de destino. El router A envía el paquete basado en su conocimiento de donde está ubicada la red.
- El router B recibe el paquete y también chequea la red estino. El router B envía el paquete al router E, después de chequear la mejor ruta para llegar a la red 9.
- El router E, recibe el paquete, lo pone en una trama con el hardware destino de la PC receptora y suelta la trama.

Existe alguna confusión entre los términos similares: routing protocol y routed protocol. Estos se explican a continuación.

Un routed protocol es un protocolo que contiene suficiente información de direcciones de capa de red para que el tráfico de los usuarios sean direccionados desde una red a otra. Los routed protocols definen el formato y uso de los campos dentro de un paquete, los paquetes que usan routed protocols son conveyed de un sistema a otro sistema final a través de la internetwork. El protocolo Internet IP y Novell´s IPX son ejemplos de routed protocols.

Un routing protocol soporta un routed protocol mediante la provisión de mecanismos para compartir información de enrutamiento. Los

mensajes del routing protocol se mueven entre los router y permiten que se comuniquen con otros routers para actualizar y mantener su tabla de enrutamiento. Los mensajes del routing protocol no llevan tráfico de usuario final de red. Un routing protocol usa los routed protocol para pasar información entre routers. Ejemplos de routing protocols TCP/IP son Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP) y Open Shorest Path First (OSPF).

La Capa de Enlace de datos.- La capa de enlace de datos asegura que los mensajes sean llevados al equipo apropiado y convierte los mensajes provenientes de la capa superior en bits, para que la capa física lo transmite. La capa de enlace de datos formatea los mensajes en tramas y le adiciona una cabecera conteniendo la dirección hardware fuente y destino, esta información adicionada forma un sort de cápsula que surrounds el mensaje original. La trama de datos que está empaquetada y listo para ser llevado en la red sigue el formato de la figura 1-15.

Los elementos de la trama de data son descritos a continuación.

- El Preámbulo o indicador de inicio es hecho de un patrón de bits especial que alerta a los equipos de hay un inicio de trama dee datos.
- La dirección de destino (AD), la capa de enlace de datos de cada dispositivo en la red examina esto para ver si macha con su propia dirección.

- La dirección fuente (SA) es la dirección del dispositivo transmisor, esto facilita los replies de los mensajes.
- En tramas Ethernet II, el campo de dos bytes seguido de la dirección fuente es una campo tipo, este campo especifica que protocolo de la capa superior reciviría la data después que el procesamiento de enlace de datos es completado.
- En tramas 802.3, el campo de dos bytes seguido de la dirección fuente es un campo de longitud, que indica el número de bytes de la data que hay entre este campo y el campo Frame Check Sequence (FSC). Seguido del campo longitud podría estar la cabecera 802.2 con información Logical Link Control (LLC), esta información es necesitado para especificar el proceso de la capa superior.
- La data es el mensaje actual mas toda la información enviada a la capa de enlace de datos del dispositivo transmisor desde las capas superiores.

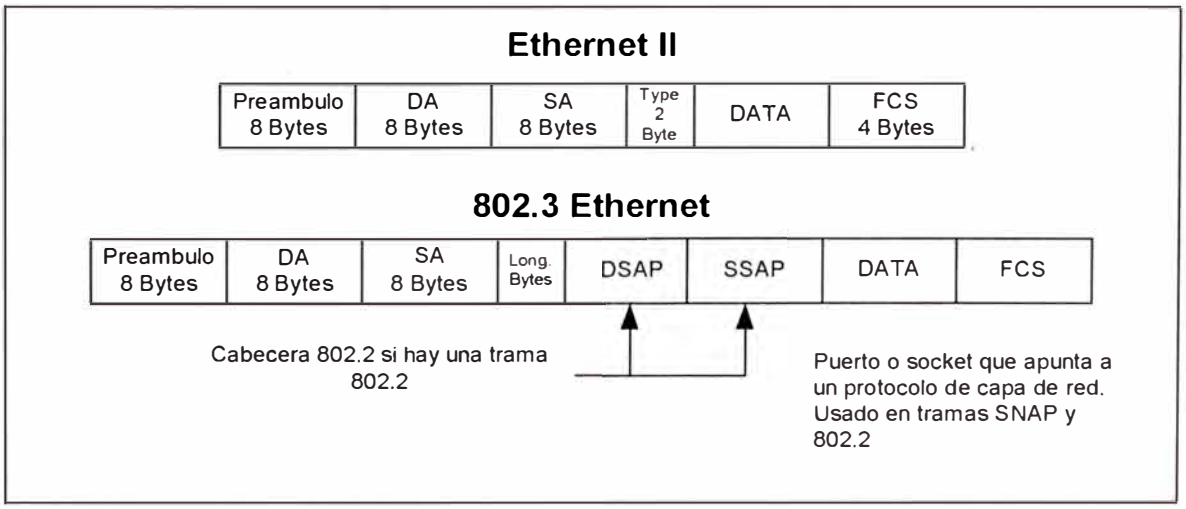


Fig. 1-15 Tramas Ethernet II y 802.3.

- Finalmente hay un campo FCS, que contiene al Cyclical Redundancy Checksum (CRC). El FCS permite al receptor determinar si una trama recibida fue dañada o corrupta mientras se transmitía.

La Sub-capa de Control de Enlace Lógico (LLC) de la capa de enlace de datos provee flexibilidad a los protocolos operando en la capas superiores e inferiores. El LLC opera entre la capa de red y la sub-capa MAC de la capa de enlace de datos, permitiendo que protocolos de la capa de red como IP operen sin la responsabilidad de tener que estar preocupados de saber que está pasando en la capa física, ya que los protocolos de la capa de red saben que el LLC es responsable de asegurar que la sub-capa MAC y la capa física están haciendo su trabajo. Por otro lado los protocolos de la capa inferior no necesitan estar preocupados por lo que ocurra arriba.

La sub-capa LLC usa "Source Service Acces Point" (SSAP) y "Destination Service Access Point" (DSAP) para ayudar a las capas mas bajas a comunicarse con los protocolos de la capa de red. Es importante que la sub-capa MAC entienda que hacer con los datos después que sea retirada la cabecera de la trama, es allí donde interviene el DSAP y el SSAP.

La sub-capa LLC es responsable de la sincronización y el control de flujo, como lo hacen algunos protocolos "stack", similar a los protocolos sin conexión y orientado a conexión.

La Sub-capa de Control de Acceso al Medio (MAC), es responsable del trameo (framing), es decir construye tramas desde unos y ceros recibido de la capa física desde el medio como una señal digital. Primero chequea el CRC para asegurar que nada fue dañado en la transmisión, luego determina si la dirección de hardware macha o no, si macha el LLC envía la data a un protocolo de la capa superior, esta capa también acepta la trama si la dirección de destino es un broadcast o multicast.

La subcapa MAC es responsable del acceso al medio, a través de esto la estación de trabajo puede comunicarse sobre la red. Esto es una operación de hardware y software parcial definido por el la tarjeta de interface de red (NIC) y por los drivers de la tarjeta.

Los protocolos de enlace de datos WAN, describen como las tramas son llevado entre sistemas en un enlace de datos único. Incluyen protocolos diseñados para operar sobre facilidades dedicados punto a punto, facilidades multipunto y servicios multi-acceso conmutado como Frame relay.

Las encapsulaciones típicas para líneas seriales síncronos en una capa de enlace de datos son:

- Hig-Level Data Link Control (HDLC): El ISO creó el estándar HDLC para soportar configuraciones punto a punto y punto a multipunto.

- Synchronous Data Link Control (SDLC): Protocolo creado por IBM para hacer que las conexiones de las oficinas con los mainframes sean mas fáciles, usa el método pooling para acceder al medio.
- Link Acces Procedure, Balanced (LAPB): Creado para usar con X.25, define tramas y la capacidad de detectar tramas perdidas o fuera de secuencia.
- X.25: La primera red conmutada ded paquetes, define una comunicación punto a punto entre un DTE y un DCE y soporta SVC´s y PVC´s.
- Serial Line IP (SLIP): Una industria estándar desarrollo en 1984 para soportar TCP/IP sobre interfaces seriales de baja velocidad.
- Point to Point Protocol (PPP): Toma las especificaciones de SLIP y construye PPP adicionando login, password, y capacidades ded detección de error. PPP es un protocolo de enlace de datos que puede ser usadp por muchois protocolos de la capa ded red, tales como IP, IPX y Apple Talk.
- Integrated Services Digital Network (ISDN): Este opera a través de líneas analógicas convertidas para usar señal digital, con ISDN se puede transmitir voz y datos.
- Frame Relay: >Es una actualización de X.25 para ser usado donde LAPB no es muy utilizado. Es el protocolo Wan mas rápido listado por que simplifica el trameado, el cual no tiene corrección de error. Frame Relay usa SVC´s y PVS´s y DLCI´s (Data Link Connection Identifier) para direccionamiento.

La Capa Física.- La capa física tiene dos responsabilidades: enviar bits y recibir bits. Los bits vienen únicamente en valores de unos y ceros, un código morse con valores numéricos. La capa física se comunica directamente con la diferentes tipos de medios de comunicación actual, los diferentes medios representan estos bits de diversas maneras, algunos usan tonos de audio, mientras que otros usan estados de transición (cambios de voltaje de alto a bajo y de bajo a alto); por esta razón se usan protocolos específicos para cada tipo de medio.

En la capa física, es identificado la interface entre el equipo terminal de datos o DTE y el equipo de terminación de circuito de datos DCE. El DCE usualmente ubicado en el service provider, mientras que el DTE es el dispositivo adjunto. Los servicio disponibles al DTE son mayormente accedidos vía un módem o channel service unit/data service unit (CSU/DSU). Los siguientes estándares de capa física definen esta interface.

- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35
- X.21
- G.703
- EIA-530
- High-Speed Serial Interface (HSSI)

1.3.2 Movimiento Fisco y Movimiento Lógico (Peer-to–Peer)

Son los dos principales conceptos que necesitan ser explicados en un modelos de referencia OSI. En la figura 1-16, el movimiento físico de los datos comienza en la capa mas alta y continua hacia abajo en el modelo capa por capa. El trabajo es como sigue: Alguien crea una información en una aplicación en la capa mas alta, los protocolos lo pasan abajo hacia un protocolo que lo empaqueta, luego lo lleva abajo hacia un protocolo de transmisión para el transporte físico de la data la data. La data se mueve a través del modelo y a través de un tipo de canal físico como cable, fibra, frecuencias de radio o micro ondas.

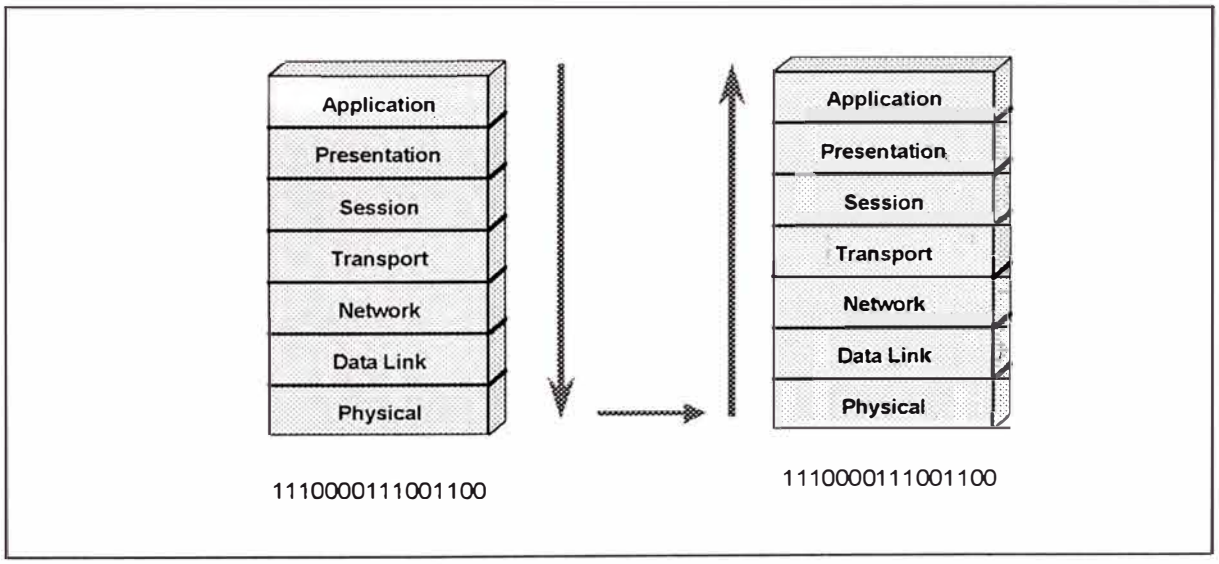


Figura 1-16 Flujo de la data a través de un modelo.

Cuando la data alcanza la computadora de destino, se mueve hacia arriba del modelo. Cada capa en el destino, ve y analiza únicamente los datos que fue empaquetado por su contraparte en el lado de envío. Refiriéndonos a nuestro ejemplo del ejecutivo y la carta, el departamento de empaques en el destino , quien ve la información del paquete de embarque y

la provista por el departamento de empaque del lado transmisor. El departamento de empaque del destino no ve la carta por que sería una ofensa y sería contra el propio protocolo. Hay un ejecutivo en la compañía de destino en la capa mas alta quien actualmente abriría y procesaría la carta.

El movimiento lógico es otro concepto. Cada capa se comunica únicamente con la capa contraparte en el otro lado (ver figura 1-17). Así como la comunicación en los humanos fluye mejor cuando ocurre entre personas con funciones iguales, del mismo nivel, o capa, es lo mismo con las computadoras. Este tipo de comunicación lógica es llamado comunicación peer-to-peer .

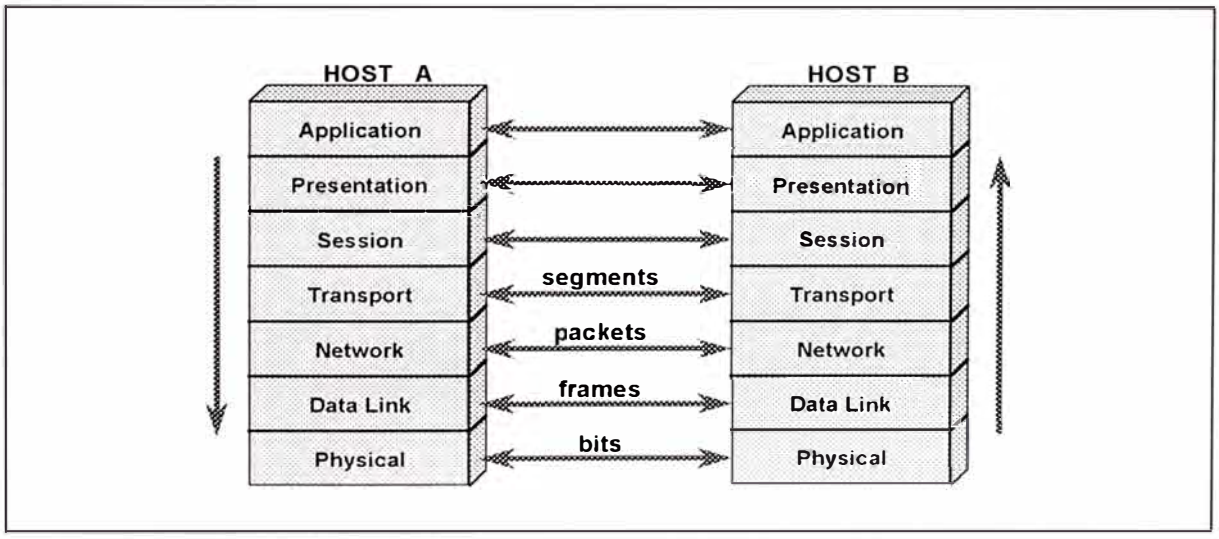


Figura 1-17 Flujo lógico de la data entre capas peer.

Cuando mas de un protocolo es necesitado para satisfactoriamente completar un procesos de comunicación , ellos son agrupados en un equipo llamado protocolo stack . Las capas en un protocolo

stack de un sistema se comunican únicamente con el protocolo stack del otro sistema correspondiente.

1.3.3.- Encapsulación de la Data y Cabeceras

cada capa en el modelo OSI depende de la función de servicio de las capas inferiores. Para proveer un servicio, la capa inferior usa el encapsulamiento para poner el PDU (Protocol Data Unite) del protocolo superior dentro de sus campo de datos, luego la capa mas baja adiciona una cabecera y un trailer, la cual le sirve para llevar a cabo su función. La figura 1-18 muestra las cabeceras adicionadas.

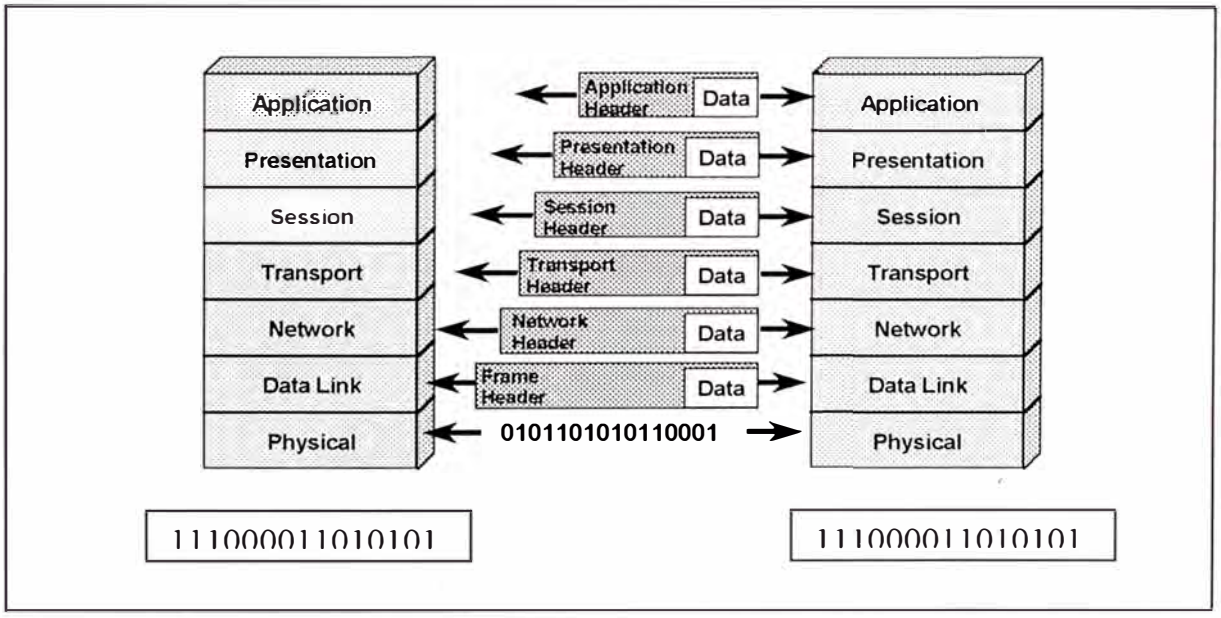


Figura 1-18 Las cabeceras son adicionadas al frente de la data en cuanto este pasa abajo a través de las capas funcionales.

La capa de Enlace de datos (Data Link) provee un servicio para la capa de Red (Network), quien encapsula la información de la capa de red en una trama. La cabecera de la trama contiene información requerida para completar las funciones de Data-Link. Por ejemplo, la cabecera de la trama

contiene direcciones físicas. La capa física también provee un servicio a la capa de enlace de datos. Este servicio la codificación de la trama Data Link en patrones de unos y ceros para la transmisión en un medio.

Como las internetworks llevan a cabo servicios para usuarios, el flujo y empaquetado de la información cambia, la figura 1-19 muestra un ejemplo. En un dispositivo de transmisión , el método de encapsulación es como sigue:

- La información del usuario es convertida en Data
- La Data es convertida en segmentos.
- Los segmentos son convertidos en paquetes o datagramas.
- Los paquetes o datagramas son convertidos en frames.
- Los frames son convertidos en bits.

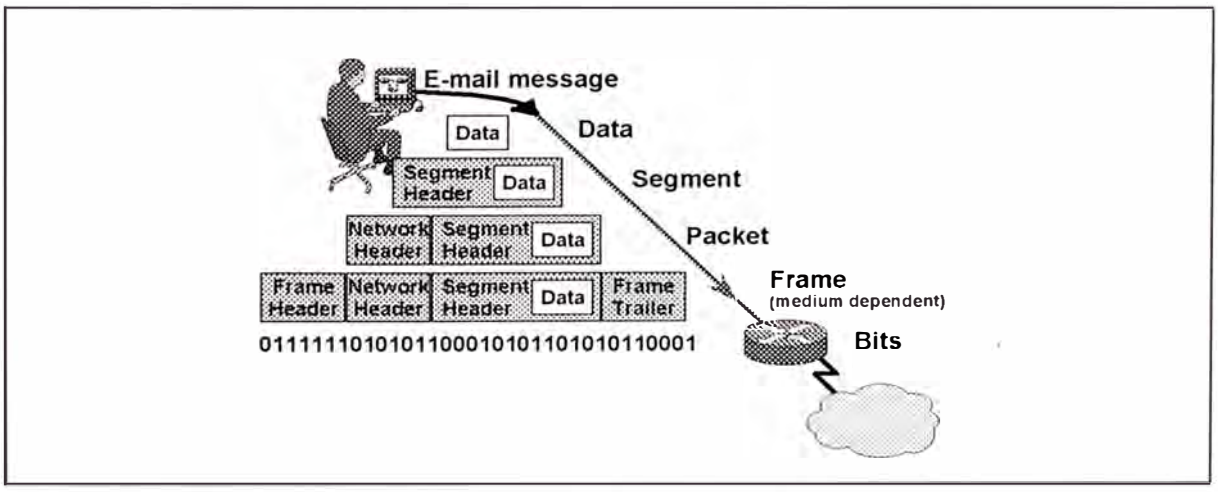


Figura 1-19 Un ejemplo de encapsulación durante el browsing de un web server .

1.4.- TECNOLOGIAS LAN (LOCAL AREA NETWORK)

Aquí describiremos las características básicas de las cuatro tecnologías Ethernet, Token Ring, FDDI y ATM, cuatro tecnologías con que cuentan prácticamente todas las LANs desarrolladas, tomaremos también un mirada a sus capas de enlace de datos y físicas de cada uno de ellos.

- Ethernet: Es un de los primeras tecnologías empleadas, siendo empleada por la LAN mas grande instalada.
- Token Ring: Fue una creación de IBM ampliamente usado en un número grande de corporaciones que migraron de mainframes a LANS
- FDI: Fue típicamente usado como backbone LAN entre los closets de datos. Es un Campus LAN muy popular por que es mas rápido que el Ethernet y el Token Ring.
- ATM: Toma el lugar del FDI en el backbone. Esta ganando popularidad ya que puede operar en ambientes WAN y LAN a velocidades increíbles.

1.4.1.- Ethernet e IEEE 802.3

En 1980, Digital, Intel y Xerox (DIX) crearon el Ethernet I original, posteriormente siguió el Ethernet II, y fue dejado en 1984. El Ethernet II es también descrito como Carrier Sens Múltiple Access with Collision Detect (CSMA/CD). En respuesta el IEEE formó el subcomité 802.3 para crear un estándar Ethernet que pasó a ser idéntico a la versión Ethernet II o Ethernet. Ambos difieren únicamente en la descripción de su capa enlace de

datos. El Ethernet II tiene un campo type, mientras que el 802.3 tiene un campo longitud; aunque ambos son comunes en la especificación de la capa física, direcciones MAC, y las responsabilidades de la capa LLC.

El Ethernet II y el 802.3 definen una topología de bus LAN a 10 Mbps y el cableado estándar definido son idénticos:

- 10Base2/Thinnet: Segmentos de hasta 185 metros usando cable coaxial RG58 de 50 ohms.
- 10Base5/Thicknet: Segmentos de hasta 500 metros usando cable RG58 o RG11 de 50 ohms.
- 10BaseT/UTP: Todos los host se conectan usando cable par trensado sin pantalla a un dispositivo central (hub o switch). Para 10 Mbps es especificado el cable UTP CAT 3, para 100 Mbps le corresponde la CAT 5 y para 155 Mbps se utiliza un cable CAT 6 y finalmente para 1Gbps utiliza cable CAT 7.

CSMA/CD.- El Carrier Sense Múltiple Access with Collision Detect fue creado para corregir en gran medida el problema de colisiones que ocurre cuando los paquetes son transmitidos simultáneamente de diferente host. Un buen administrador es importante, ya que cuando un host transmite en una red CSMA/CD, todos los otros host en la red reciben y examinan la transmisión. Únicamente los bridge y los routers previenen la propagación de una transmisión a través de la red entera.

El protocolo CSMA/CD trabaja de la manera siguiente: Cuando un "host" quiere transmitir sobre una red, primero verifica la presencia de una señal digital en el cable. Si todo está claro (no hay otro host transmitiendo), el "host" procedería con el inicio de la transmisión. El "host" transmitiendo constantemente está monitoreando el cable para asegurarse que ningún otro "host" inicie una transmisión. Si el "host" detecta otra señal en el cable, entonces envía una señal "jamp" que causa que todos los nodos paren de enviar datos. Los nodos responden a la señal "jam" mediante la espera de unos segundos antes de empezar a trasmitir de nuevo. Si después de 15 intentos las colisiones se mantienen, los nodos intentando transmitir se irían a un "time-out" por un determinado tiempo.

1.4.2 Fiber Distributed Data Interface (FDDI)

Como el "Token Ring", el "Fiber Distributed Data Interface", es una topología de acceso al medio mediante el "token pasing". El American National Standard Intitute define el estándar (ANSI X3T9.5) para una LAN dual "token ring" operando a 100 Mbps sobre fibra óptica. "Copper Distributed Data Interface" puede ser usado con cable UTP para conectar servidores u otras estaciones directamente en el anillo

Las ventajas del FDDI incluyen lo siguiente:

- FDDI puede operar sobre distancias muy largas y ambientes eléctricamente hostiles donde estan presentes el electromagnetismo, señales de radio, e interferencia de frecuencias.

- Opera a altas velocidades comparado con Redes LAN Ethernet a 10 Mbps y Token Ring a 4/16 Mbps.
- El FDDI emplea un acceso al medio por token passing con un anillo dual operando en sentidos opuestos. Típicamente un anillo está activo en un tiempo dao, de esa manera si uno se quiebra por causa de una rotura, el anillo FDI se wrape back a la otra dirección, manteniendo el anillo intacto. Algunas estaciones pueden ser adjuntados a ambos anillos por razones de redundancia, estos son conocidos como Dual Attachment Station (DAS), las cuales serían utilizados por equipos de alta disponibilidad como servidores.
- El FDDI es un anillo lógico y físico y es la única LAN que es un actualmente un anillo. Como un Token Ring, el FDI provee retardo determinístico predicible y prioridades.
- FDDI usa direcciones MAC como otras LAN, pero usa un esquema numérico diferente, aplica símbolos de cuatro bits. El FDDI tiene doce símbolos de cuatro bits con la que contruye sus direcciones MAC.
- La red Token Ring solamente permite un token en el anillo en cualquier tiempo dado, mientras que FDDI permite la presencia de muchos token en el anillo.

Algunos drawbacks de migrar a FDI incluyen lo siguiente:

- Relativamente alta latencia ocurre cuando se produce una traducción de FDDI a Ethernet y Ethernet a FDDI es llevado a cabo entre LANs.

- La capacidad es aun compartida, por que el anillo dual FDDI es una LAN compartida.
- No hay capacidad Full Dúplex en redes compartidas.
- Los componentes FDDI son muy caros, tales como hub y NICs, nos on exactamente equipos bargain

Cuando una estación informa que ningún token ha sido recibido de su vecino superior activo mas cercano (NAUN) por un periodo de tiempo predeterminado, envían un beacon como una alerta y como un intento de ubicar la falla. Una vez que empiece a recibir sus propios beacons, asume que ahora el anillo está activo y operando. Si no recibe su beacon por un tiempo predeterminado, el anillo primario will wrap al anillo secundario como se muestra.

1.4.3 Token Ring

IBM creó el Token Ring en 1970, fue muy popular con clients que necesitaron migrar de ambientes mainframes. Token Ring perdió popularidad con con Ethernet por comparación de precios, sin embargo depende de lo que se está buscando, Token Ring es una red mas resilient, especialmente bajo cargas pesadas.

Al igual que Ethernet, Token Ring opera bajo una topología estrella usando cable par trensado apantallado (STP), cada estación se conecta a una central hub llamado un Multistatio Access Unit (MSAU).

Lógicamente opera en un anillo donde cada estación espera recibir una señal desde su NSAU y repite esta señal a su vecino de abajo.

El anillo Token Ring usa direcciones MAC como Ethernet, pero es aquí donde la similitud termina. El acceso al medio en Token Ring es descrito punto por punto a continuación:

- Las estaciones no pueden transmitir cuando ellos quieran, como si lo hace las estaciones ethernet. En vez de eso, ellos tienen que esperar a tener una trama especial llamado token. Cuando una estación recibe un token, este hace uno de dos cosas:
    a. Este appends la data que quiere enviar dentro del final de la trama, luego cambia el bit T en la trama. Esto permite alertar a la estación receptora que la data está adjunta.
    b. Si la estación que consigue el token no necesita enviar data, simplemente lo pasa a la próxima estación en el anillo.
- La trama de información circula en el anillo hasta que consiga la estación destino. La estación destino copia la trama y luego etiqueta la trama como es copiado. La trama continua hasta que llegue a la estación origen, el cual lo remueve de la red.
- Típicamente, solo una trama puede estar en el anillo en cualquier tiempo dado. Sin embargo, usando early token release, una estación puede transmitir un nuevo token dentro del anillo después de transmitir su primera trama.

- Las colisiones no ocurren por que ellos no pueden transmitir a menos que tengan el token.

La trama en una red "Token Ring" es diferente de las tramas Ethernet. La trama token usa un sistema de prioridad que permite que ciertos usuarios designados como estaciones de alta prioridad usen la red frecuentemente. El campo de control de acceso al medio de la trama es mostrado abajo:

Los dos campos que controlan la prioridad son el campo prioridad y el campo de reservación. Si una prioridad de token es transmitida, únicamente las estaciones con prioridad igual o mas alta que la prioridad de ese token pueden retenerlo. Los niveles de prioridad son configurados por el administrador. Después que el token es retenido y cambiado a una trama de información, únicamente las estaciones con una prioridad mas alta que la estación transmitiendo puede reservar el token para la próximo paso alrededor de la red. Cuando el próximo token es generado, este incluye la mas alta prioridad para la estación reserving. Las estaciones que alcanzan la prioridad del token tienen que reinsertar el nivel de prioridad mas baja después que su transmisión este completa.

El campo de estado de trama es mostrado en la figura 1-20. Las direcciones, ó el bit A, y el copiado ó bit C son usados para indicar el estado de una trama excepcional.

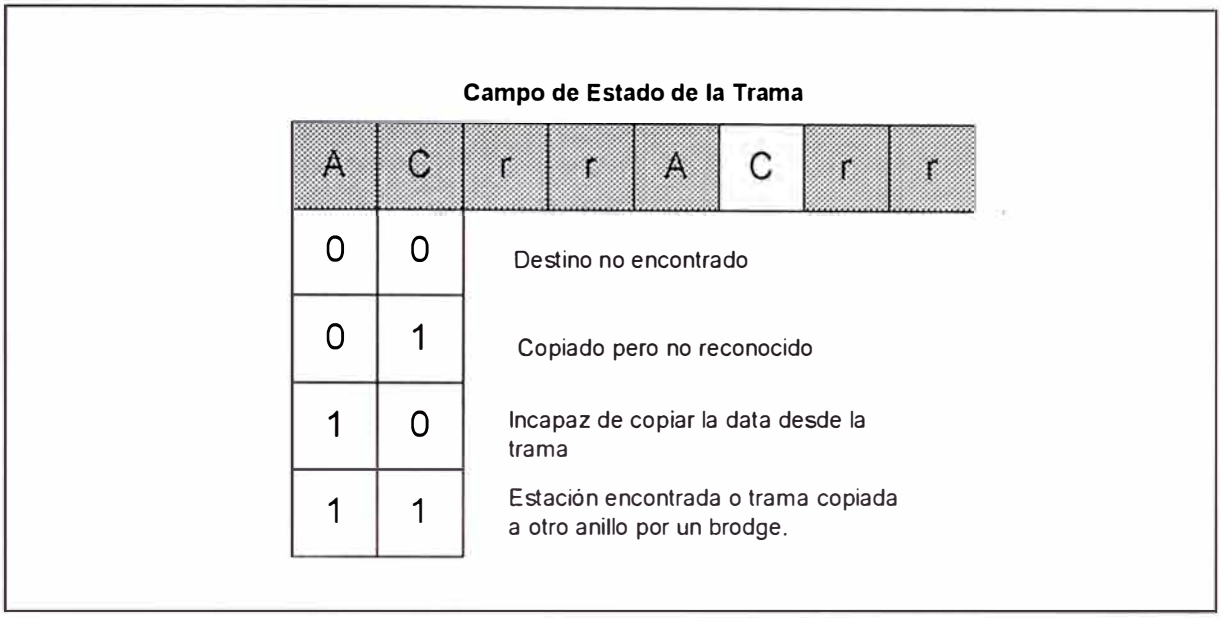


Figura 1-20 Estado de las tramas Token Ring.

Ambos bits son apagados cuando la estación trasmite la trama. Cuando la estación transmisora recibe la trama otra vez, la estación leería la información para asegurarse que la data fue recibida correctamente por la computador destino o que necesita ser retransmitido.

1.4.4 Tecnología ATM

Iniciales de Asysnchronous Transfer Mode (ATM), es una tecnología de bajo retardo y muy alto ancho de banda, que usa el switching y multiplexing. ATM usa celdas de tamaño fijo de 53 bytes en vez de tramas Ethernet. ATM es una tecnología muy adaptable que trabaja con ambientes LAN y WAN. Puede permitir utilización de ancho de banda en demanda haciendo la mas grande solución para aplicaciones bursty.

Mientras ATM no es dependiente en una implementación de la capa física, requiere medios de alta velocidad y ancho de banda como fibras ópticas.

ATM puede ser usado para soportar las siguientes aplicaciones:

- Multimedia interactivo.
- Video en tiempo real.
- Base de Datos cliente/servidor
- Interconexión de redes existentes.

La ITU-T y el ATM forun han trabajado juntos para crear los estándares para ATM.

CAPÍTULO II

LA RED DE AREA LOCAL: ETHERNET

2.1.- TECNOLOGIAS DESKTOP

La red Ethernet fue creado en 1970 como un resultado de trabajos experimentales llevadas a cabo por la Corporación Xerox en Palo Alto Research Center (PARC). La primera LAN ethernet se extendió a una distancia de un kilómetro (Km), soportando 100 estaciones, y alcanzando velocidades de datos de 2.94 Mbps. El término Ethernet fue elegido en honor de una sustancia no definida llamada ether.

Basado en su popularidad, Ethernet llegó a ser un estándar de facto .Corporaciones como DEC (Digital Equipment Corporation) y Xerox propusieron la adopción de Ethernet como un estándar 802. La propuesta Ethernet fue renombrada como IEEE 802.3. Desafortunadamente hay importantes diferencias entre el estándar original Ethernet y el IEE802.3 que limita la comunicación entre los dos sistemas.

2.1.1.- Legacy Ethernet

Cuando las computadoras mainframes dominaron la industria, los terminales (usuarios) adjuntos directamente al puerto en la computadora

o a un controlador que da la apariencia de una conexión directa . Cada alambre de conexión fue dedicado a un terminal individual. Los usuarios ingresaban la data y el terminal inmediatamente transmitía la señal al host. La performancce fue dirigida a la potencia del host. Si el host se sobrecargaba, los usuarios experimentaban retardos en respuesta. Los usuarios tienen el ancho de banda del medio completamente lleno como consecuencia de la carga de trabajo del dispositivo.

Uno de los beneficios inmediatos de las LANs fue reducir los costos de instalación y mantenimiento, eliminando la necesidad de instalar líneas dedicadas a cada usuario. En vez de eso un único cable pulled desde usuario a usuario, permitiendo a los usuarios compartir un infraestructura común en vez de tener un infraestructura dedicada para cada estación.

Un problema de la tecnología alcanzó cuando los usuarios comparten un cable. Se pensó como el controlar en la red quien usa el cable y cuando?. La tecnología Broadband como Cable Televisión (CATV) soportan múltiples usuarios, debido a que multiplexa la data en diferentes canales (frecuencias). Este es un ejemplo de multiplexación por división de frecuencia (FDM). Las LANs iniciales fueron concebidas como tecnologías banda base, la cual no tiene múltiples canales. La tecnología Bandabase no transmite usando FDM, ellos usan bandwith-sharing , lo cual significa que los usuarios se turnan para transmitir.

Ethernet define un conjunto de reglas conocida como método de acceso para compartir el cable.

Carrier Sense Múltiple Access UIT Colition Detect (CSMA/CD).- Describe el método de acceso Ethernet, el cual sigue la regla general en una conversación entre persona. En una conversación todos los individuos tienen derecho a hablar, la regla no hablada que todos siguen es la siguiente: "únicamente una persona puede hablar a la vez". Si tu tienes algo que decir, primero necesitas escuchar si alguien está hablando. Si alguien ya esta hablando, tienes que esperar hasta que ellos finalicen. Cuando inicias la conversación, necesitas continuar escuchando en caso alguien mas decida hablar a la vez. Si esto ocurre, ambas partes paran de hablar y esperan un tiempo aleatorio. Únicamente continua aquellos que tienen el derecho de empezar otra vez. Si hay una falla de un individuo cumplir con el protocolo de un hablante a la vez, la comunicación no es efectiva.

En Ethernet, el Múltiple Access es la terminología debido a que existen muchas estaciones adjuntos a un medio y tiene la oportunidad de transmitir. Ninguna estación tienen prioridad sobre otra. Sin embargo ellos necesitan tener turnos para el algoritmo de acceso.

Carrier Sense, se refiere al proceso de escuchar antes de hablar. El dispositivo Ethernet que desea comunicarse busca energía en el medio (una portadora eléctrica). Si existe una portadora, significa que el

cable está en uso y el dispositivo tiene que esperar su turno. Muchos dispositivos Ethernet mantienen un contador que te indican con que frecuencia ellos necesitan esperar antes de poder transmitir. Algunos dispositivos lo llaman contador deferral o back-off, si el contador deferral excede un valor umbral de 15 intentos, el dispositivo intentando transmitir asume que nunca conseguiría acceder al cable para transmitir un paquete. En esta situación, el dispositivo fuente descarta la trama. Esto podría ocurrir si hay muchos dispositivos en la red, lo que implicaría que no hay suficiente ancho de banda de banda disponible.

SI el nivel de potencia excede el umbral, significa que una colisión ha ocurrido en el sistema. Cuando una estación detecta una colisión, los participantes generan una señal collision enforcement, esta señal enforcement es tan grande como el tamaño de trama mas pequeño, que en el caso de Ethernet es de 64 Bytes, esto asegura que todas las estaciones conozcan de la existencia de la colisión y permite que ninguna otra estación intente transmitir durante el evento de la colisión. SI una estación experimenta muchísimas colisiones consecutivas, la estación para la transmisión de la trama. Algunos Workstation muestran un mensaje de error Media not available , el mesaje difiere de cada estación pero nos indican la incapacidad de acceder al medio y por lo tanto incapaz de enviar data.

Direccionamiento en Ethernet..- Cómo identifican las estaciones una de otras?. De la misma manera que en una conversación la identificación se realiza por nombres. Podemos elegir uno para un grupo entero, un conjunto de individuos, o personas específicas. Si hablamos de un grupo equivale a un Broadcast, un conjunto de individuos a un Multicast, y a una persona equivale a un unicast. El mayor tráfico en una red es unicast por naturaleza, caracterizado como tráfico de una estación a otra estación específica. Algunas aplicaciones generan tráfico multicast y broadcast, como por ejemplo IP genera paquetes broadcast para el proceso ARP, los roouters algunas veces transmiten routing updates como tramas broadcast.

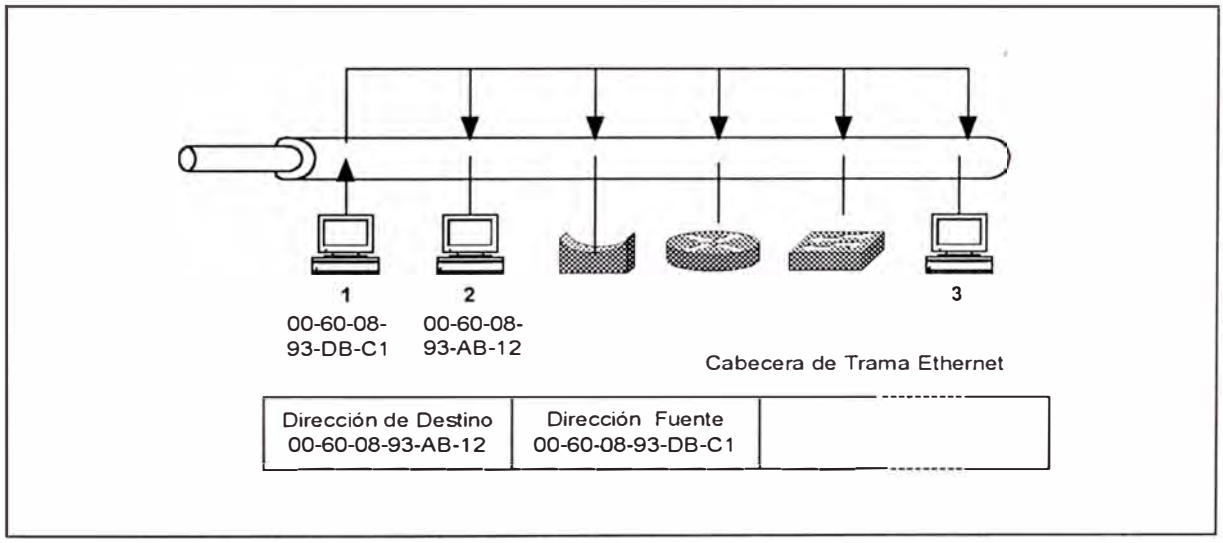


Figura 2-1 Una simple Red Ethernet.

La figura 2-1 muestra un sistema ethernet con muchos dispositivos adjuntos, cada dispositivos tiene una tarjeta adaptadora de red que contiene una dirección de 48 bits (6 octetos) construido en el módulo identifica únicamente a la estación. Esta dirección es llamado Media Access Control (MAC), o dirección de hardware . Todos los dispositivos en una LAN

tiene que tener una única dirección MAC. Esta direcciones MAC son expresadas por valores hexadecimales , o algunas veces separados por hyphens (-), o por colons (:), o por periodos (.). Hay tres formatos : 00-60-97-8F-4F-86, 00:60:97:8F:4F:86 y 0060.978F.4F86 , todos especifican el mismo host.

Los primeros tres octetos en una dirección MAC indican el fabricante de la tarjeta de interface. Es conocido como Organizational Unique identifier (OUI). Cada fabricante tiene un único valor OUI que es adquirido de la IEEE, quien es el administrador global de valores OUI.

Los últimos tres octetos de la dirección MAC equivale al identificador para el dispositivo , los cuales son localmente asignados por el vendedor. La combinación de OUI y el número de host crean una única dirección para un dispositivo.

Existen tres tipos de tramas, las cuales se explican a continuación:

- Tramas Unicast: En una LAN, las estaciones tiene que usar la dirección MAC como direcciones capa 2 (modelo OSI) en la trama, para identificar la fuente y el destino. Cuando la estación 1 transmite hacia la estación 2 en la figura (pag 8 lan s), la estación 1 genera una trama que incluye la dirección MAC de la estación 2 (00-60-08-93-AB-12) como destino, y la dirección ded la estación 1 (00-60-08-93-DB-C1) como dirección fuente. Este es una trama unicast, debido a la

LAN es un medio compartido, todas las estaciones reciben una copia de la trama y únicamente la estación 2 lleva a cabo el procesamiento de la trama, aunque todas las estaciones comparan la dirección MAC con su propia dirección MAC. Si la dirección no macha entonces la tarjeta de interface descarta (ignora) la trama, previniendo así que se consuma recursos de CPU en el dispositivo. La estación 2 al compara la dirección MAC se da cuenta que macha y envía el paquete a su CPU para el procesamiento. El CPU examina el protocolo de red y la aplicación dirigida y decide si dropear o usar el paquete.

- Tramas Boradcast: Algunas tramas enviadas por las estaciones tienen direcciones broadcast y multicast, y los tratan de una manera diferente que las tramas unicast. Las estaciones ven a las tramas broadcast como anuncios de servicios público. Una trama broadcast tiene una dirección MAC de destino FF-FF-FF-FF-FF-FF (todos los binarios 1s). Al igual que las tramas unicast, todas las estaciones reciben la trama y comparan la dirección MAC con el propio, como la dirección MAC de un multicast no machará, el módulo de interface es diseñado para que la trama broadcast pase aún al procesador, debido a que podría tener una información o solicitud importante . Desafortunadamente unas pocas estaciones realmente necesitan recibir el mensaje broadcast. Así por ejemplo una solicitud IP ARP crea una trama broadcast , aunque es solo dirigido a una estación para que responda, los protocolos de enrutamiento envían broadcast

para anunciar su tabla de enrutamiento. Todo esto consume ciclos de CPU en cada dispositivos, si el número de broadcast en la red es muy excesivo, las estaciones no pueden hacer las cosas, que ellos necesitan hacer, tales como correr un procesador Word o simuladores de vuelo, debido a que las estaciones están muy ocupados procesando tramas no sin uso.

- Tramas Multicast: Una trama Multicast son direccionados a un grupo de dispositivos con un interés común y permiten que la fuente envíe únicamente un copia de la trama en la red, aunque tiene la finalidad de que muchas estaciones lo reciban . Cuando una estación recibe un trama multicast, compara la dirección multicast con su propia dirección, a menos que la tarjeta sea configurada para aceptar tramas multicast, es descartada en la interface y no consume ciclos de CPU.

Tramas de la Red de Área Local (LAN).- Cuando las estaciones quieren comunicarse con las otras, formatean la data de una manera estructurada para que los dispositivos conozcan que significado o información tiene cada uno de los octetos. Hay varios formatos de tramas, por lo tanto uno de ellos tiene que ser definido en tu estación.

En la figura 2-2, muestra cuatro formatos comunes de trama para Ethernet.

	◄---------- Trama ----------►										
				◄---------- Paquete ----------►							
Formato Trama	**Campo de la Cabecera capa 2 14 - Octetos**			◄---------- Campo de Data 1500 Octetos ----------►							
Ethernet v2 (ARPA)	MAC DA 6-Octet.	MAC SA 6-Octet.	Tipo 2-Octet.	Data							F O S
802.3	MAC DA 6-Octet.	MAC SA 6-Octet.	Length 2-Octet.	Data							
802.3/802.2	MAC DA 6-Octet.	MAC SA 6-Octet.	Length 2-Octet.	DSAP 1-Octet.	SSAP 1-Octet.	Control	Data				
802.3/802.2 SNAP	MAC DA 6-Octet.	MAC SA 6-Octet.	Length 2-Octet.	0xAA 1-Octet.	0xAA 1-Octet.	0x03 1-Octet.	Org Code 1-Octet.	Tipo 2-Octet.	Data	Octet	

Figura 2-2 Cuatro formatos de Trama Ethernet

En la figura anterior, para el formato Ethernet nos muestra que después del preámbulo, los 6 octetos corresponden a la dirección MAC de destino, mientras que los próximos 6 octetos contiene la dirección MAC fuente. Los dos bytes seguidos indican el protocolo de capa 3 para la cual está dirigido. Por ejemplo si el paquete va dirigido a IP, el valor del campo type es 0x0800, la tabla mostrada a continuación muestra muchos protocolos comunes y sus correspondientes valores type.

PROTOCOLO	VALOR TIPO HEXADECIMAL
IP	0800
ARP	0806
Novell IPX	8137
Apple Talk	809B
Banyan Vines	0BAD
802.3	0000-05DC

Tabla 2-1 Protocolos Ruteados comunes y sus valores de tipo hexadecimal.

Siguiendo el valor type, el receptor espera ver la cabecera del protocolo adicional, si el valor type es para IP, el receptor espera encontrar cabecera IP para su decodificación. Si el valor es 8137 el receptor espera decodificar cabecera de un paquete Novell.

La IEEE definió un formato de trama alternativo, En los formatos IEE 802.3 las direcciones MAC fuente y destino se mantienen, pero en vez del campo type, existe un campo length que indican la longitud del campo de datos. Adicionalmente existe derivados del 802.3: El 802.3 con 802.3 LLC y el 802.3 con 802.2 y SNAP. Un receptor reconoce que un paquete sigue la formato 802.3 por el valor del campo de dos bytes seguido de la dirección fuente. Si el valor cae dentro del rango del 0x0000 y 0x05DC, el valor indica longitud. Los valores del campo type empiezan a después del 0x05DC.

Ethernet SlotTimes.- Como la regla para CSMA/CD es detectar colisión en el medio y reportar lo ocurrido a los participantes, Ethernet define un SlotTimes para un trama que viaja de un extremo de la red a otra. En la figura 2-3, muestra la ocurrencia de una colisión debido a que la trama enviada por la estación 1 se demoró en llegar a la estación 2 y esta al asumir que el medio estaba desocupada también envió otra trama, resultando en una colisión. El timing envuelve el valor del peor en la detección y reporte de colisión.

La regla ethernet indica que una estación tiene que detectar y reportar una colisión entre los puntos mas lejano en la red antes de que la

fuente complete la transmisión de la trama. Especialmente para Ethernet legacy de 10 Mbps, todo tiene que ocurrir dentro de 51.2 us. Este tiempo es basado en el tamaño de trama mas pequeño para Ethernet, el cual corresponde a la ventana de tiempo mas pequeño para detectar y reportar una colisión. El tamaño de trama mínima para Ethernet es de 64 bytes, que tiene 512 bits, cada tiempo de bit tiene 0.1 us de longitud, calculado sobre una velocidad en Ethenert dee 1/106 . Así el slotTime para Ethernet es:

(0.1 microsegundos / bit)*(512 bits) = 51.2 microsegundos

Luego, las especificaciones se traducen en distancias, como la señal se propaga por diferentes componentes en el domino de colisión, entonces los retardos son introducidos. Los valores de retardo de tiempo son calculados para cables de cobre, fibra óptica y repetidores, además la cantidad de retardo introducida por cada componente varía por las características del medio. Un buen diseño de red asegura que la totalidad de retardos introducida por los diferentes componentes en la red no superen los 51.2 microsegundos. Muchos problemas se pueden originar si se viola la regla del SlotTime, mediante la extensión de las distancias de la red, el cual produciría un malfuncionamiento de la red.

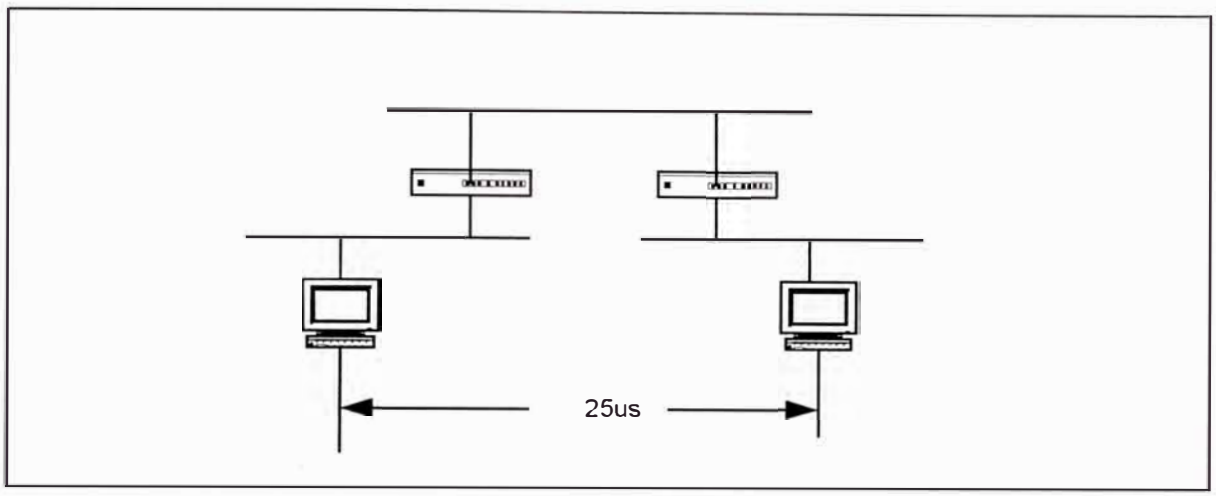


Figura 2-3 Ejemplo del peor caso de una Colisión..

2.1.2.- Fast Ethernet

Debido a la creciente demanda de ancho de banda y redes de alta velocidad, la IEEE formó el comité 802.3u para trabar en una tecnología de 100 Mbps y que opere sobre cables de par trensado. En Junio de 1995, la IEEE aprobó las especificaciones 802.3u definiendo un sistema que ofreció Inter-operatibilidad a 100 Mbps.

Al igual que la tecnología de 10 Mbps, el sistema 100 Mbps usa CSMA/CD pero posee un mejoramiento, debido a que opera 10 veces mas rápido que la red Ethernet 10Mbps. Todos los factores se reducen por un factor de 10, por ejemplo el SlotTime es de 5.12 microsegundos mejor que 51.2 microsegundos.

Un objetivo del estándar 100BaseX fue mantener una trama común con la trama Ethernet legacy. Así el estándar 100BaseX usa los mismos formatos de trama y tamaños que el 10BaseX. Todo lo demás se

escala por una Tenth la razón de data mas alta. Cuando pasas tramas de un sistema de 10BaseX a 100BaseX, el dispositivo de interconexión no necesita mas que recrear la cabecera de la trama por que ellos son idénticos en ambos sistemas.

Tres variedades de 100BaseT son estandarizados , basado en las especificaciones de la capa física:

- 100BASE-TX
- 100BASE-T4
- 100BASE-T2
- 100BASE-FX

Full - Duplex y Half – Duplex.- En sistemas de 10 Mbps, la totalidad del ancho de banda disponible es dedicado a transmitir y recibir dependiendo si la estación es transmisora o receptora. Esta función se describe como half dúplex.

El estándar LAN original operaba en modo half dúplex, permitiendo únicamente a una estación transmitir o recibir a la vez, este fue implementado con estándares 10Base5 y 10Base2 donde todas las estaciones estaban adjuntas al mismo cable. En 10BaseT se desarrollaron Hubs en la que las estaciones de trabajo estaban adjuntas por medio de enlaces punto a punto, en esta topología no se comparte el medio. 100BaseX usa hubs con enlaces dedicados punto a punto, mediante el cual

cada enlace no es compartido y es independiente, permitiendo la factibilidad de un nuevo modo de operación llamado Full dúplex . Este modo de operación permite a las estaciones transmitir y recibir a la vez, eliminando la necesidad de detectar colisiones. Cuando las estaciones operan en modo Full dúplex, las estaciones transmiten y reciben en el ancho de banda completo para cada dirección. El ancho de banda máximo a esperar en un legacy Ethernet es de 10 Mbps, tanto para escuchar o transmitir. En sistemas de 100BaseX, los dispositivos operando en modo Full dúplex ven 200 Mbps de ancho de banda, 100 Mbps para transmitir y 100 Mbps para recibir.

El comité IEEE802.3x diseñó un estándar para el modo de operación Full dúplex que cubre 10BaseT, 100BaseX y 1000BaseX, así como también diseñó los mecanismos de control de flujo, permitiendo que el receptor envíe una trama especial de regreso a la fuente para ver si los buffers del receptor estaban overflow. El receptor envía un paquete especial llamado pause frame, en esta trama, el receptor puede solicitar a la fuente que se detenga de enviar tramas por un periodo de tiempo. Si el receptor puede manipular el tráfico antes de que el valor del timer en un pause frame expire , el receptor puede enviar otro pause frame con el timer configurado a cero. Este le dice al receptor que puede empezar a transmitir otra vez.

Aunque 100BaseX soporta los modos de operación full dúplex y Half dúplex, se puede desarrollar hubs de 100 Mbps que operen en modo Half dúplex, en este caso las estaciones tiene que operar en modo Half dúplex. Para operar en modo Full dúplex, los dispositivos y el hub (switch) tienen que soportar y ser configurados en modo Full dúplex.

Por lo mencionado anteriormente, la configuración de los dispositivos resultaría en una confusión, para evitar esto se desarrolló la autonegociación , mediante el cual lso dispositivos y el hub automáticamente acuerdan a un nivel de operación común. El comité 802.3u definió el Fast Link Pulse (FLP) que soporta el proceso de autonegociación. El FLP que es una versión mejorada de Integridad de enlace de 10BaseT, envía una serie de pulsos en el enlace anunciando su capacidad. El otro terminal también transmite anuncios FLP y los dos terminales se configuran en cualquier método que tenga la prioridad mas alta común entre ellos. A continuación se detalla el esquema de prioridades en la Tabla 2-1.

ESTANDAR	TIPO DE CABLE	MODOS	PARES REQUERIDOS	DISTANCIA (mts)
10BaseT	Categoría 3,4,5	Half Duplex	2	100
100BaseTX	Categoría 5	Half Duplex Full Duplex	2	100
100BaseT4	Categoría 3	Half Duplex	4	100
100BaseT2	Categoría 3,4,5	Half Duplex Full Duplex	2	100
100BaseFX	Multimodo	Half Duplex Full Duplex	1	412 (Half Duplex) 2000 (Full Duplex
100BaseFX	Monomodo	Half Duplex Full Duplex	1	10 Kms

Tabla 2-2 Comparación entre medios 100BaseX.

La prioridad es determinada por la velocidad, los tipos de cables soportados y el modo de operación dúplex. Así por ejemplo un sistema siempre prefiere 100 Mbps sobre 10 Mbps, Full dúplex sobre Half dúplex.

- 100BaseTX: Muchos sistemas 10Mbps para trensado usan una infraestructura de cable basado en categoría 5 (unshielded twisted pair) UTP y (shielded twisted pair) STP. Los dispositivos usan dos pares del cable: un para usa el pin 1 y 2 para transmitir y el otro para en el pin 3 y 6 para recibir y detectar colisión. El estándar 100BaseTX también usa esta infraestructura, y usa el cable Categoría 5 para 10BaseT, lo cual implica que 100BaseTX trabaja hasta 100 metros al igual que 10BaseT. 100BaseTX usa un esquema de codificación como FDDI consistente en 4B/5B, este esquema adiciona un quinto bit por cuatro bits de data de usuario, lo que significa que hay un 25 por ciento de overhead en la transmisión que soporta la codificación. Aunque 100BaseTX lleva 100Mbps dee data de usuario, este opera a 125 Megabaudio.
- 100BaseT4: Como los cables categoría 3 fueron instalados en muchos edificios para soportar transmisiones de voz y frecuentemente es referido como cable de grado de voz. Este cable es probado para voz y aplicaciones de data de baja velocidad hasta 16 MHz- El cable Categoría 5, por otro lado fue intentado para aplicaciones de data y es probado a 100MHz. Debido a que el cale categoría 3 coexiste en muchas instalaciones, y por que muchas instalaciones 10BaseT están en cable Categoría 3, el comité

IEE802.3u incluyó esto como una opción. Los enlaces 100BaseT4 trabaja a 100 metros, así mismo para soportar altas velocidades 100BaseT4 usa mas pares de cables, tres pares son destinados para transmisión y un par para detección de colisión . Otra tecnología para alcanzar altas velocidades viene de las técnicas de codificación, 100baseT4 usa método de codificación 8B/6B (8 bits / 6señales ternarias), el cual baja significativamente la frecuencia de la señal, haciéndola mas útil para alambres de grado de voz.

- 100BaseT2: Aunque 100BaseT4 provee una solución para cables Categoría 3, necesita cuatro pares para su operación. Como los cables categoría 3 fueron creados para soportar comunicaciones de voz, 100BaseT4 usa cuatro pares, por lo que no existe pares para soportar comunicaciones de voz. 100BaseT2 fue completado por IEEE en 1997 y lo llamó 802.3y, el cual opera en cables categoría 3,4 y 5 y únicamente requiere dos pares de cables. Adicionalmente se desarrolló chips de procesamiento de señal digital y métodos de codificación llamado PAM 5x5 para funcionar sobre tipos de cables de ancho de banda muy bajos. 100BaseT2 trabaja con longitudes de cables de 100 metros.
- 100BaseFX: El estándar 802.3u especifica una variante para cables de fibra óptica multimodo y monomodo. 100BaseFX usa dos strands de cable de fibra óptica, uno para transmitir y otro para recibir. Al igual que 100BaseTx, 100BaseFX usa codificación 4B/5B a 125 MHz en la fibra óptica. La fibra óptica multimodo soporta hasta 2000

metros en modo de operación Full dúplex, 412 metros en modo Half dúplex. La fibra monomodo trabaja hasta 10 Km, la cual es una distancia significativa. Otra venta de la fibra incluye sus propiedades de aislante eléctrico, el cable de fibra es inmune a los ruidos eléctricos los cual lo hace ideal para estos ambientes.

2.2.3.- Gigabit Ethernet

En Junio de 1998 fue desarrollado otra tecnología con ancho de banda mas alta. El estándar IEE802.3z Gigabit Ethernet nos especifica la operación a 1000 Mbps, otro mejoramiento del ancho de banda. Gigabit Ethernet propone las expectativas para encontrar una tecnología backbone o un pipe dentro de muchos servidores de archivos de alta velocidad. Esta tecnología contrasta con Fast Ethernet ya que 100 Mbps pueden desarrollarse sobre clientes, servidores, o usar esto como una tecnología backbone. Gigabit Ethernet no sería usado para conectar directamente a clientes, debido a que algunos estudios indican que la señalización de interface de 1000 Mbps en un workstation de clase pentium dismiuiría su performance producido por interrupciones de software.

En una Red de Catalyst (switxhes cisco), La tecnología Gigabiut Ethernet interconectan catalyst para formar un backbone de alta velocidad. En la figura 2-4, el catalyst tiene estaciones conectadas a él a bajas velocidades (10 y 100Mbps) pero tiene 1000 Mbps para pasar tráfico entre workstations. Un servidor de archivos en la red también se beneficia gracias

a la conexión de 1000 Mbps que soporta mayor cantidad de accesos de clientes actuales.

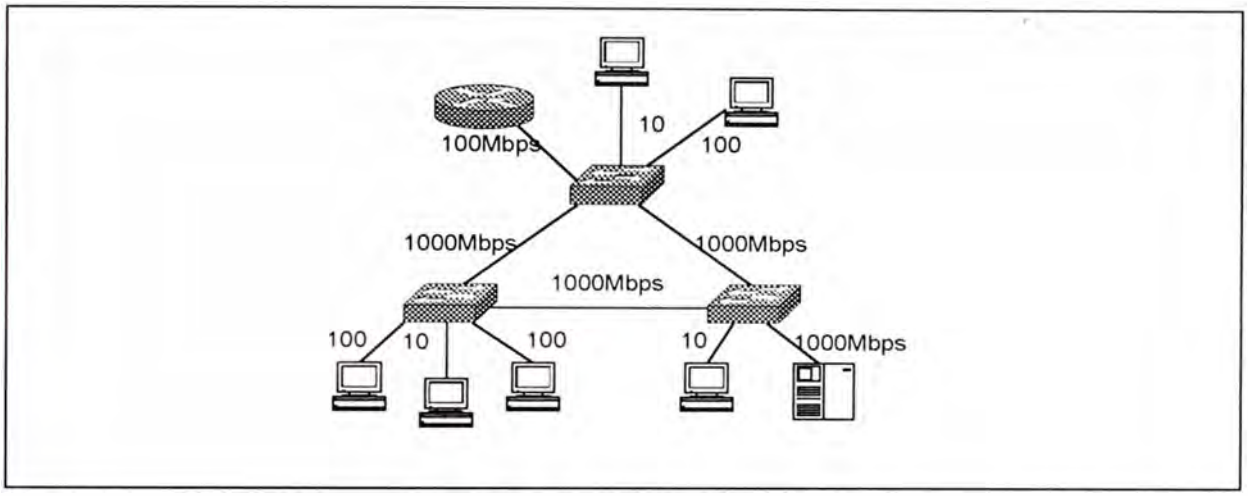


Figura 2-4 Conexiones Gigabit Ethernet entre Swtchies.

Arquitectura de Gigabit Ethernet.- Gigabit Ethernet emerge aspectos de Ethernet 802.3 y Fiber Channel, una tecnología creada para interconexiones de altas velocidades entre servidores de archivos como un LAN replacement. El estándar Fiber Channel detalla un modelo de red de capas capaza de escalar hasta 4 GBps y extenderse a distancias de 10 Km. Gigabit Ethernet toma prestado las dos capas mas bajas del estándar: FC-1 para codificación y decodificación y FC-0 la capa de interface y medio, FC-1 y FC-0 reemplazan la capa física del modelo legacy 802.3. La MAC 802.3 y la subcapa LLC contribuyen a los niveles mas altos de Gigabit Ethernet . la figura 2-5 ilustra el merger de los estándares para formar Gigabit Ethernet.

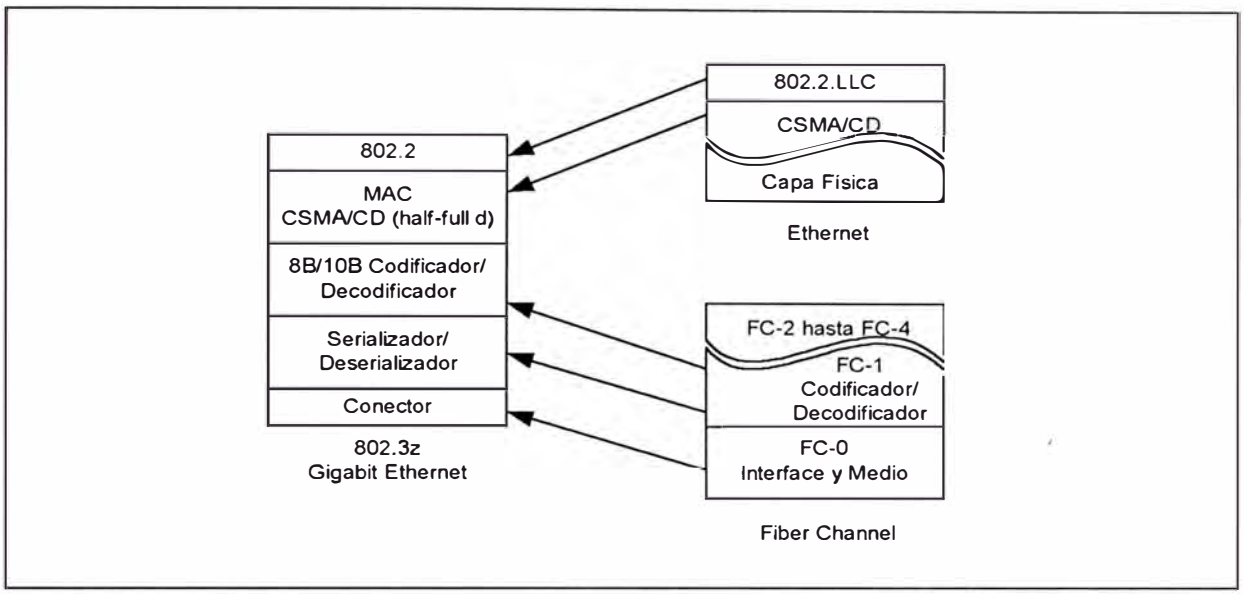


Figura 2-5 La formación del estándar Gigabit Ethernet.

El estándar Fiber Channel incorporado por Gigabit Ethernet transmite a 1.062 MHz sobre fibra óptica y soporta 800 Mbps de throughput de data. Gigabit Ethernet incrementa la razón de señalización a 1.25 GHz, además usa codificación 8B / 10B, el cual significa que 1 Gbps es disponible para data, esta técnica de codificación hace mas simple el diseño de fibras ópticas a esta velocidad alta de datos. El conector óptico usado por Fiber Channel y además por Gigabit Ethernet es el tipo SC. La cual es push-in / pull-out , usado por los fabricantes para sobrellevar deficiencias del conector ST

Full-Duplex y Half-Duplex.- Gigabit Ethernet soporta modos de operación full duplex y half duplex con control de flujo. En modo half duplex el sistema opera usando CSMA/CD y se tiene que considerar la reducción de evento SoltTime mas que en Fast Ethernet. Sabemos que el slottime para

100BaseX es de 5.12 us, derivados del tamaño de trama de 64 octetos, y traducido en una distancia de 200 metros. Si se usa el mismo tamaño ded trama en Gigabit Ethernet, el SoltTime se reduce a .512 us y hacerca de 20 metrtos en diámetro, lo cual lo hace no razonable. El estándar 802.3z desarrolló una extensión de la potadora que nos habilita extender las distancias de red further in full duplex y aun soportar los paquetes 802.3 mas pequeños.

El proceso de extensión de portadora incrementa el SoltTime a un valor de 4096 bits o 4.096 us. La estación transmitiendo expande el tamaño de la trama transmitida para asegurar que encuentre los requerimientos de slottime mínimos, adicionándole símbolos no-data después del campo FCS de la trama. No todas las tramas requieren extensión de portadora. El esquema de codificación 8B /10B usado en Gigabit Ethernet define varias combinaciones de bits llamados símbolos, algunos símbolos señalan la data real mientras que el resto señalan no-data. La estación receptora identifica el símbolo no-data, retira los bytes de extensión de portadora y recobra el mensaje original. La figura 2-6 muestra una trama extendida.

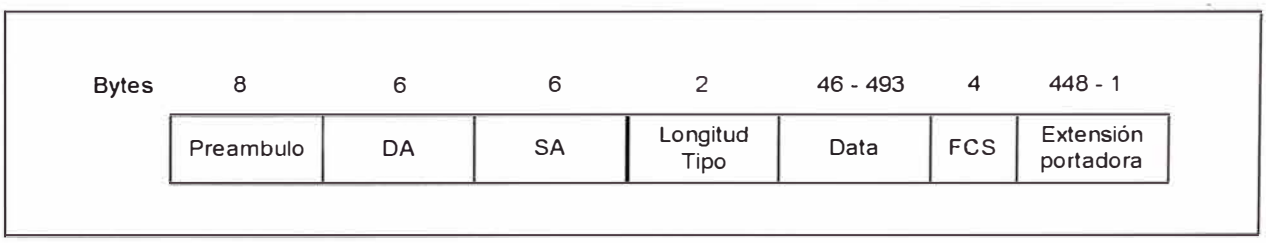


Figura 2-6 Una trama Gigabit Ethernet extendida.

Opciones de Medio Gigabit.- El IEEE 802.3z especifica muchos opciones de medio para soportar diferentes grados dee cable de fibra óptica y una versión para soportar un nuevo tipo de cable de cobre. Las opcines de fibra óptica varían por el tamaño de la fibra y por el ancho de banda modal. La tabla 2-3 mostrada a continuación muestra las opciones y las distancias soportadas por cada una.

ESTANDAR	TAMAÑO DEL CABLE (um)	Bw DEL CABLE (Mhz-Km)	DISTANCIA (mts)
1000BaseSX	62.5	160	220
1000BaseSX	62.5	200	275
1000BaseSX	50	400	500
1000BaseSX	50	500	550
1000BaseLX	62.5	500	550
1000BaseLX	50	400	550
1000BaseLX	50	500	550
1000BaseLX	9/10	N/A	5000
1000BaseLH	9/10	N/A	10000
1000BaseZX	9/10	N/A	90000

Tabla 2-3 Opciones de Medio para Gigabit Ethernet.

- 1000BaseSX: Usa la longitud de onda de 850 nm. Aunque esto es un sistema basado en laser, las distancias soportadas son generalmente mas cortas que para 1000BaseLX. Este resulta de la interacción de la luz con el cable de fibra en esa longitud de onda. Usamos 1000BaseFx por que los componentes son menos caros que 1000BaseLx. Se usa este método menos caro para distancia de enlace cortos.

- 1000BaseLX: En sistemas de fibra óptica, las fuentes de luz difiere en el tipo de dispositivo (LED o LASER) que genera la señal óptica y la longitud de onda que ellos generan. La longitud de onda se relaciona con la frecuencia en los sistemas RF. En el caso óptico, especificamos logitud de onda mejor que frecuencia. En términos prácticos se refiere al color dee la luz, la cual típicamente para 850 nm es de color rojo y visible para los humanos, mientras que para 1300 nm es invisible. 1000BaseLX usa fuentes ópticas de 1300 nm . En realidad la L de LX significa long wavelength. 1000BaseLX usa fuentes LASER, razón por la cual no se debe mirar directamente al puerto de la fibra, puede ser dañino para la salud de los ojos.
- 1000BaseCX: No incluido en la tabla, es una opción con medio de cobre. Usa cable de cobre balanceado apantallado de 150 ohms. Soporta transmisiones de cable hasta 25 metros. Estos es creado para ser usado en la interconexión de dispositivos colocados dentro de un rack el cual tienen distancias muy cortas.
- 1000BaseT: Una versión de cable final es el estándar 1000BaseT el cual usa cable categoría 5 par trensado. Este soporta hasta 100 metros, pero usa cuatro pares en el cable. Este ofrece otra alternativa a bajo costo que 1000BaseSX y 1000BaseLX y no depende del uso de un cable especial como sucede para el estándar 1000BaseCX. Este est{andar esta bajo el purwiew del comité 802.3ab.

2.2.- SEGMENTACION DE REDES DE ÁREA LOCAL

Con la combinación de workstation poderosos, audio y video en el desktop, y aplicaciones intensivas de red, las redes Ethernet 10Mbps no ofrecen suficiente ancho de banda para cumplir con los requerimientos de los negocios grandes típicos.

Como mas y mas usuarios son conectados a la red, la performancia de una red Ethernet comienza con la pelea de los usuarios por mas ancho de banda. Al igual que muchos carros tratan de ingresar a una súper carretera en hora punta, esto incrementa la utilización y la congestión, debido a que muchos usuarios tratan de acceder los mismos recursos. La congestión causa que los usuarios scream por mas ancho de banda, sin embargo con el simple hecho de aumentar el ancho de banda no siempre se puede resolver el problema. Algunos inconvenientes como tener un CPU de baja velocidad o insuficiente memoria RAM en los workstations y servidores deberían ser tomados en cuenta.

Una forma de resolver los problemas de congestión e incrementar la performance de red en una LAN es dividir un segmento Ethernet en muchos segmentos de red, esto maximiza la disponibilidad de ancho de banda. Algunas de las tecnologías que se pueden usar para desarrollar la segmentación son las siguientes:

- Segmentación Física :Se puede segmentar la red con bridges y routers, de esa manera quebramos los dominios de colisión. Esto

minimiza la colisión de los paquetes debido al decremento del número de estaciones en un mismo medio físico.

- Tecnología Network Switching (micro-segmentación) : A igual que un bridge y un router, los switches puede también brindarnos la capacidad de segmentación de LAN. Los switches LAN proveen conexiones de conmutación de paquetes dedicado y punto a punto, entre sus puertos. Los switches incrementan la cantidad de ancho de banda para cada estación debido a que prosee conmutación de paquetes en forma simultánea entre sus puertos.
- Dispositivos Ethernet Full-Duplex : La tecnología Ethernet full-duplex puede proveer casi el doble de ancho de banda que una red legacy, sin embargo, para que esto funciones todas las tarjetas de interface de red (NIC) tienen que operar en modo full-duplex.
- Fast Ethernet : Usando switches Fast Ethernet se puede proveer 10 veces la cantidad de ancho de banda disponible que 10BaaseT
- FDDI : Una tecnología antigua y sólida que puede proveer 100Mbps de ancho de banda, y que tiene la capacidad de operar hasta 299Mbps debido a que puede operar con anillos duales, es típicamente usado entre closet , pisos o en un ambiente campus.

Por todo esto, no debería sorprender que el reducir el número de usuarios por dominio de colisión aumenta el ancho de banda en un segmento de red. Esto debido a que si mantenemos el tráfico en un segmento de red, los usuarios tienen mas ancho de banda disponible y notar

mejoras en los tiempos de respuesta que si simplemente se tuviera un gran backbone en el lugar.

2.2.1.- Segmentando LANs con Bridges

Los Bridges nos dan una solución cuando necesitamos adicionar mas usuarios o extender la distancia del segmento al tener una red que está trabando en los límites de la regla Ethernet de distancia y números de estaciones. Cuando conectamos la red como la figura 2-7 (pag 42 lans), mediante un bridge, este dispositivo impide que la trama generada por un estación ubicada en un segmento llegue a las demás estaciones ubicadas en el otro segmento. Esto se debe a que los bridges usan procesos de filtrado para determinar si o no enviar una trama a otras interfaces.

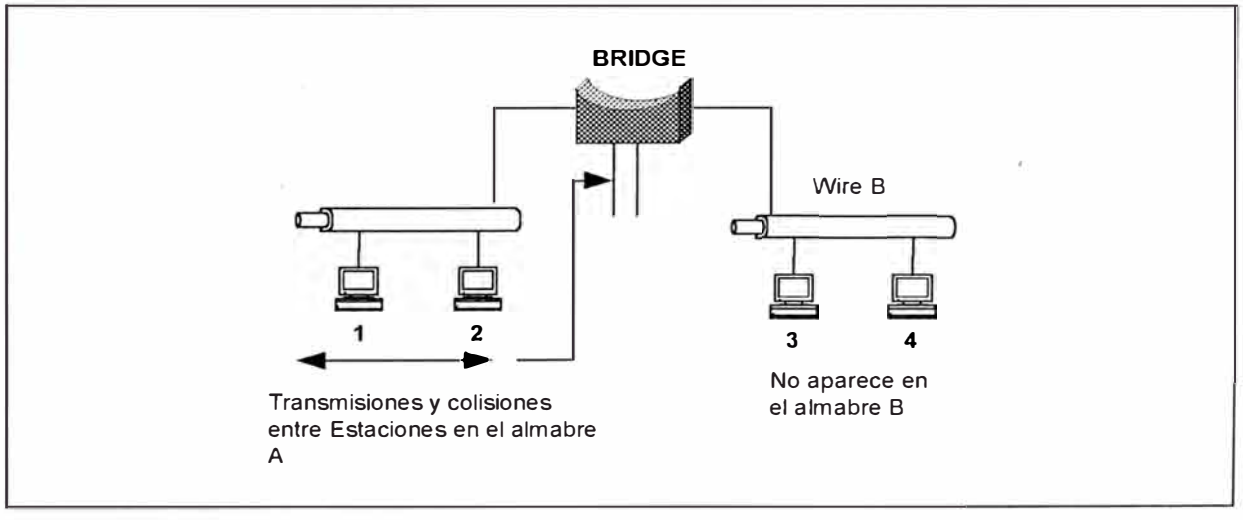


Figura 2-7 Interconectando segmentos con un Bridge.

Los bridges operan en la capa 2 del modelo OSI, la capa de enlace de datos, razón por la cual los bridges tienen la capacidad de

examinar la cabecera MAC de las tramas y hacer decisiones de envío basado en esta información.

Mas importante que saber que los "bridges" interconectan dominios de colisión, es saber que los dominios de colisión independientes aparecen como si estos estuviesen conectados, sin propagar las colisiones entre los segmentos.

La figura 2-8, nos muestra que el ancho de banda de la red fue dividido en cuatro segmentos, donde cada segmento viene a ser un dominio de colisión diferente. Si esto fuese una red "legacy Ethernet" de 10Mbps, cada segmento debería tener su propio 10Mbps de ancho de banda, por consiguiente tenemos un ancho de banda colectivo de 40Mbps.

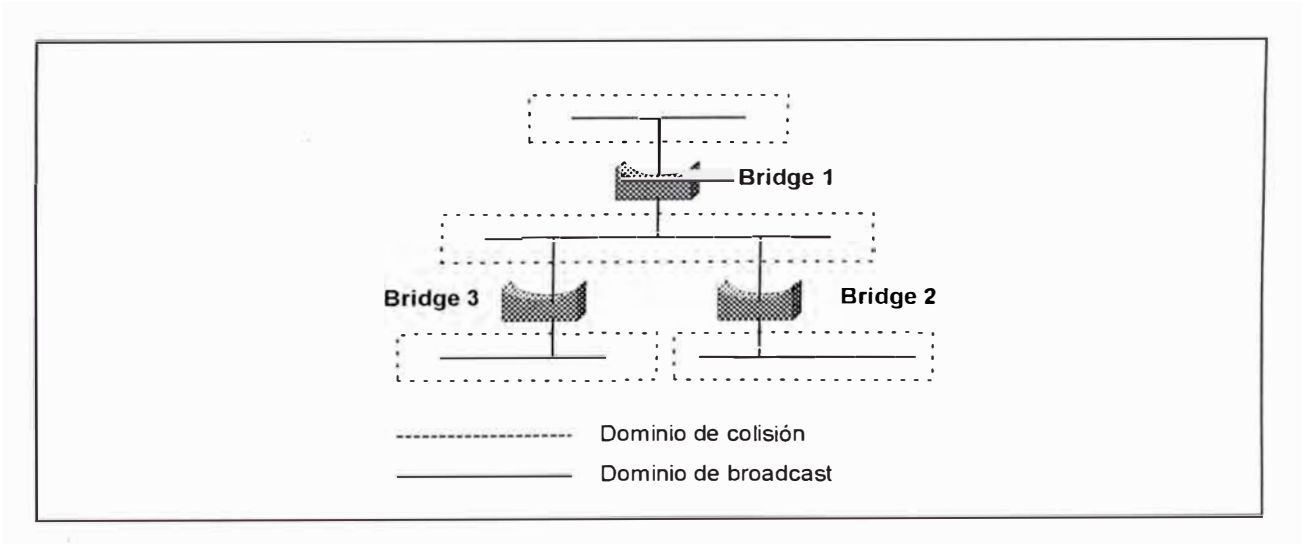


Figura 2-8 Los Bridge crean mútiples dominios de Colisión y uno de Broadcast.

Este mejoramiento en el ancho de banda demuestra por que al segmentar la red trae consigo beneficios para el usuario. El mismo número

de usuarios en esta red tienen ahora mas ancho de banda que si todos estuviesen conectados juntos.

Otra ventaja de los “bridges” está en su capacidad de operación en la capa 2 del modelo OSI. Cada segmento conectado a un “bridge” puede extenderse hasta su distancia máxima, tener su propio valor de “SlotTime”, no enviar colisiones a otros segmentos y en teoría extender la red indefinidamente.

Si bien es cierto que los bridge filtran el trafico generado en un segmento, los “broadcast” y “multicast” son la excepción a esto. Si un “bridge” recibe un “broadcast” o “multicast”, este envía el mensaje a todas las interfaces (flooding). Una red “bridged” puede ser abrumado con tráfico “broadcast” y “multicast” si existe aplicaciones que generan este tipo de tráfico. Así por ejemplo aplicaciones como video conferencia sobre IP crean tráfico multicast, tramas de todos los participantes se propagan por cada segmento, reduciendo el ancho de banda de la red y haciéndola parecer como una red gigante. En al mayoría de redes, las tramas generalmente no son “broadcast”, algunos protocolos generan más tráfico que otros, pero el ancho de banda consumida por estos protocolos que generan “broadcast” son porcentajes relativamente pequeños al ancho de banda en la LAN.

A continuación explicaremos el funcionamiento de los “bridges”. Cuando un dispositivo fuente y destino se encuentran en un mismo

segmento (o interface), el bridge filtra la trama y no envía el tráfico a cualquier otra interface (siempre y cuando no sea un broadcast o multicast). Si la fuente y destino residen en puertos diferente relativos a un bridge, el bridge envía la trama a la interface apropiada para llegar a su destino. El proceso de filtrado y envío selectivo preserva el ancho de banda de otros segmentos.

Cuando un bridge envía el tráfico, no cambia la trama. Al igual que los repetidores, un bridge no hace da mas que limpiar la señal antes de enviarla a otro puerto. Las direcciones dee capa 2 y 3 se mantienen cuanto pasan a través de un bridge. Un router difiere en que si puede cambiar las direcciones de capa 2.

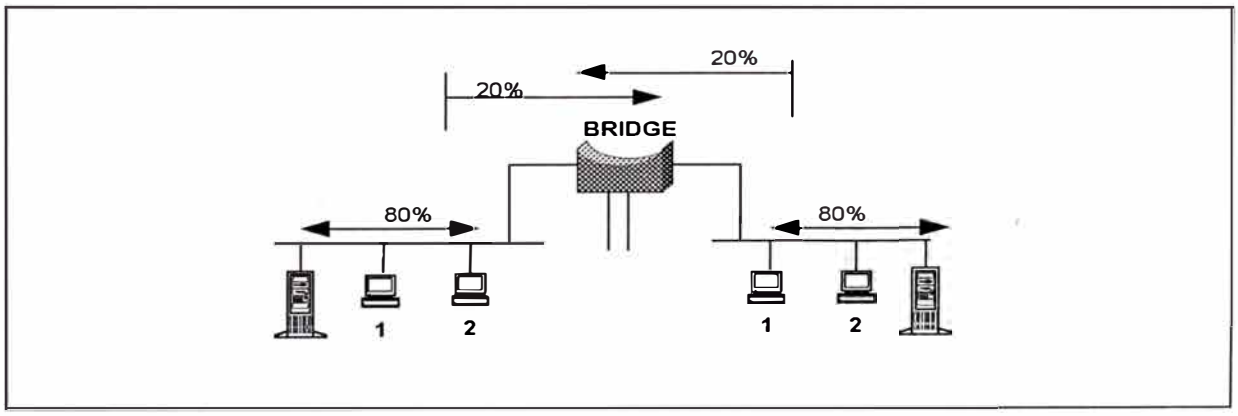


Figura 2-9 La regla de 80/20 demostrado en una red tradicional.

Una regla en el diseño de redes con Bridge es la regla del 80/20. Los cual significa que el 80 % de trafico en el segmento es local y el 20% de tráfico en el segmento necesita pasar a través del bridge a otro segmento. Esta regla originada de diseños de redes tradicionales donde los recursos de

servidores residían en el mismo segmento con los clientes, como mostrado en la figura 2-9.

Otra ventaja de los bridges es que ellos previenen la transmisión de tramas erróneas a otro segmento. Si el bridge observa que la trama tiene errores o que viola el método de acceso al medio, el bridge dropea la trama. Esto protege a los demás segmentos de tramas erradas que no hacen mas que consumir ancho de banda, para que la final sean descartadas por el dispositivo final. Las colisiones en las redes legacy algunas veces producen fragmentos de trama que son llamados tramas runt, estas tramas, violan la regla del tamaño mínimo de una trama que es 64 Bytes, las cuales son bloqueadas por los bridges, a diferencia de los repetidores que envían estas tramas runt a otros segmentos

2.2.2.- Segmentando LANSs con Routers

Los routers operan en la capa 3 del modelo de referencia OSI, adiciona funcionalidad a la red mejor que los bridges, extienden la red como los bridges pero no solamente crean dominios de colisión como estos, sino que también crean dominios de broadcast. Los routers previenen que los broadcast se propaguen por la red, este aislamiento crea el domino de broadcast no encontrado con los bridges. La figura 2-10 muestra una red construida con routers e identifica dominios de broadcast y colisión.

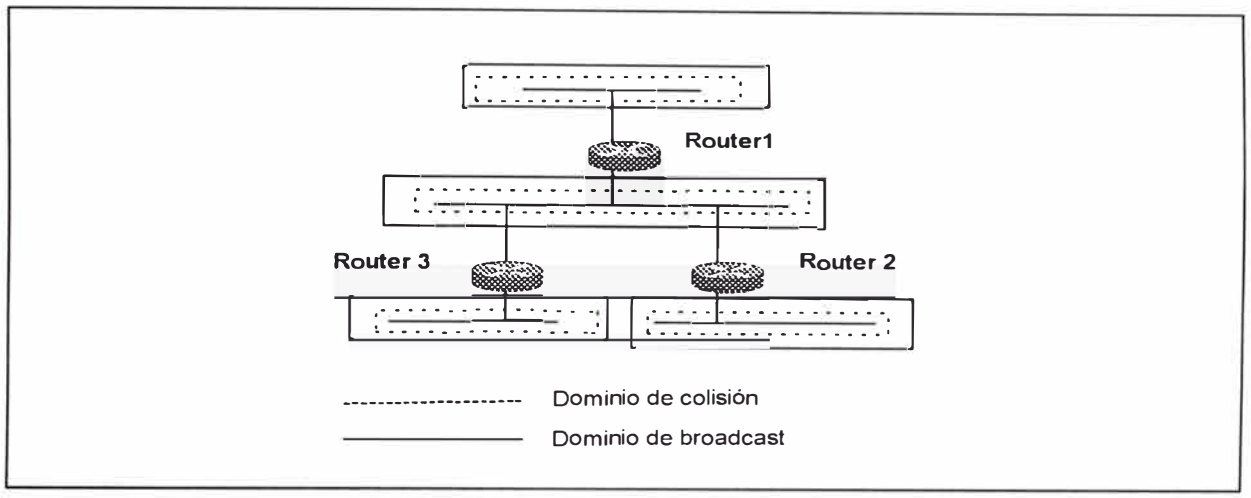


Figura 2-10 Dominios de Colisión y Broadcast en una red ruteada

El efecto de separar dominios de "broadcast" demuestra por si mismo el comportamiento de los routers. En una red basada en repetidores y "bridges", todas las estaciones pertenecen a la misma subred por que todos pertenecen al mismo dominio de "broadcast". En una red basada en routers, se crea múltiples dominios de "broadcast", donde cada segmento pertenece a una diferente subred. Para ilustrar como las tramas fluyen a través de un router y como las estaciones se comportan de manera diferente con la presencia de un router, mostramos la figura 2-11. En una red con repetidores y "bridges", las estaciones transmiten como si la fuente y destino estuviesen en un mismo dominio de colisión, el aspecto que permite comportarse así es que verdaderamente en una red con "bridges", ellos están en un mismo dominio de "broadcast". Sin embargo cuando ellos están en diferentes dominios de "broadcast", como cuando se introduce un router en vez que un "bridge", la fuente y el destino tienen que estar conscientes del router y deberán direccionar su tráfico hacia él.

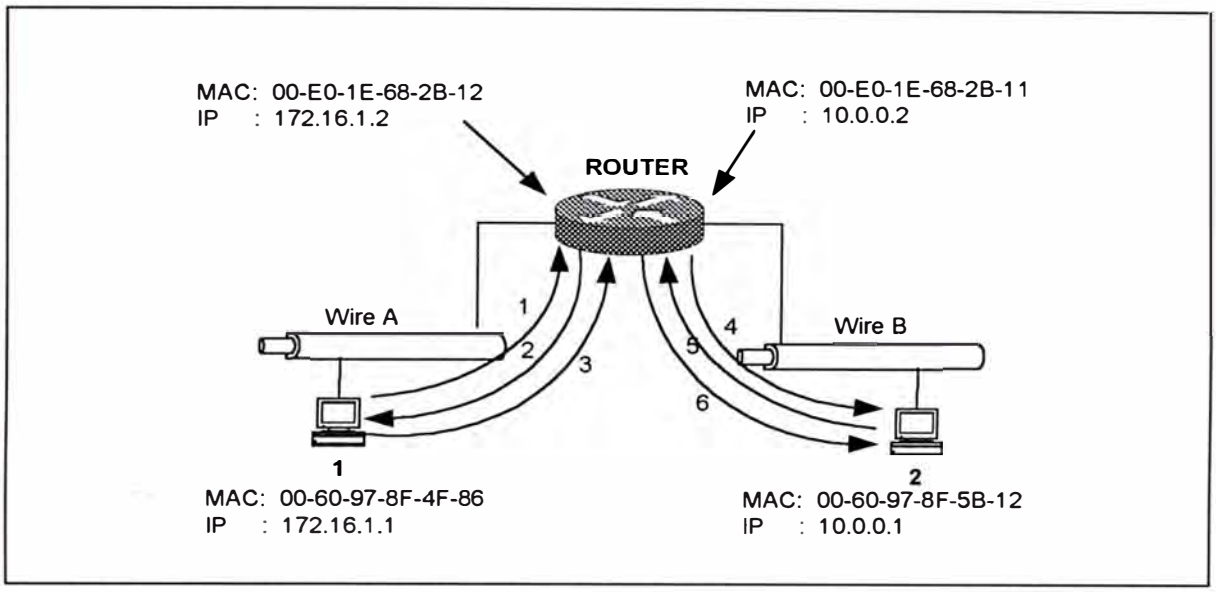


Figura 2-11 Cambios en la cabecera de trama a través de un router.

CABECERA CAPA 2 MODIFICADO			CABECERA CAPA 3 NO MODIFICADO	
TRAMA	**MAC DE DESTINO**	**MAC FUENTE**	**FUENTE IP**	**DESTINO IP**
1*	FF-FF-FF-FF-FF-FF	00-60-97-8F-4F-86	172.16.1.1	172.16.1.2
2**	00-60-97-8F-4F-86	00-E0-1E-68-2B-12	172.16.1.2	172.16.1.1
3***	00-E0-1E-68-2B-12	00-60-97-8F-4F-86	172.16.1.1	10.0.0.1
4*	FF-FF-FF-FF-FF-FF	00-E0-1E-68-2B-11	10.0.0.2	10.0.0.1
5**	00-E0-1E-68-2B-11	00-60-97-8F-5B-12	10.0.0.1	10.0.0.2
6***	00-60-97-8F-5B-12	00-E0-1E-68-2B-11	172.16.1.1	10.0.0.1

* ARP request
** ARP reply
*** Trama de datos de usuario

Tabla 243 Intercambio de tramas en una Red ruteada.

Cuando la estación 1 quiere conversar con la estación 2, la estación 1 se da cuenta que el destino está en una red diferente, por la comparación de la otra dirección lógica con la suya. Sabiendo que ellos están en diferentes redes, fuerza al host fuente a comunicarse a través del router. El router es identificado a través del default gateway, que es configurado en las estaciones. Para comunicarse con el router, la fuente

tiene que direccionar al router en la capa 2 usando la dirección MAC del router. Para obtener la dirección MAC del router, la fuente primero manda una trama ARP al router (ver tramas 1 y 2). La fuente luego crea una trama con la dirección MAC del router como dirección MAC de destino y con la dirección lógica de la estación 2 para la dirección de capa 3 de destino (ver trama 3). Cuando la trama entra la router, este determina como conseguir la red de destino. En este ejemplo la red de destino está directamente adjunto al router. El router ARPs a la estación 2 (trama 4 y 5 en la figura) y crea una trama con la dirección MAC de la estación 2 como dirección de capa 2 de destino y la dirección Mac del router como fuente (ver trama 6). El router en todo momento usa direcciones de capa 3 para la estación 1 y 2. La cabecera de la capa enlace de datos cambia a medida que la trama se mueve a través del router, mientras que la cabecera de la capa 3 permanece intacto.

2.2.3.- Segmentando LANs con Switches

Los switches LAN son una gran estrategia para segmentación de LANs. Los switches LAN mejoran la performance por el empleo de la tecnología packet-switching que permite intercambio de datos a altas velocidades. Al igual que los bridge, los switches usan direcciones de capa 2 del modelo OSI con la finalidad de asegurar que los paquetes sean enviados por el puerto correcto.

Existe tres diferentes términos switching: puerto, trama y cell switching (ATM).

- El switching por configuración de puerto, permite a un puerto ser asignado a una segmento de red física bajo el control dedl software. Esto es la forma mas simple de switching.
- Frame Switching es usado para incrementar la disponibilidad del ancho de banda en la red. Esto permite que múltiples transmisiones ocurran en paralelo.
- Cell Switching (ATM) es similar a frame switching. ATM usa pequeñas celdas de longitud fija que son switched en una red.

Un switch LAN nos abastece con considerablemente alta densidad de puertos a bajo costo, desde que las LAN switches permites pocos usuarios por segmentos, el promedio disponible de ancho de banda por usuario incrementa. Este trend de pocos usuarios por segmento se conoce como micro-segmentación, y te permite crear segmentos dedicados. Cuando se tiene un usuario por segmento, cada uno puede acceder al ancho de banda completo del medio, en vez de competir por esto con otro usuarios.

Los LAN switches soportan las siguientes características:

- Numerosas y simultáneas conversaciones
- Intercambio de datos a altas velocidades
- Baja latencia y alta razón de frame –forwarding
- Comunicación dedicada entre dispositivos
- Comunicación full-duplex

- Velocidad de adaptación al medio (10 y 100Mbps pueden trabajar en la misma red)
- Una habilidad para trabajar con los tarjetas de interface de red 802.3 legacy y cableados estándares.

Debido a la comunicación dedicada, libre de colisión entre los dispositivos en la red, el throughput de la transferencia de archivos es incrementado. Muchas conversaciones pueden ocurrir simultáneamente por el envío o conmutación de muchos paquetes a la vez, el cual expande la capacidad de la red por la cantidad de conversaciones soportadas.

Otra ventaja de la utilización de LAN switches en las redes, significa que algunas veces no es necesario cambiar los hubs, las interfaces de red (NIC) o el cableado existente.

CAPÍTULO III

SISTEMAS DE CABLEADO ESTRUCTURADO PARA LAN´s

El número uno de causas de problemas en LANs es el cableado, los alambres, cables y algunas veces otros medios de transmisión que enlazan cada uno de los dispositivos de red. Comparado a las computadoras existentes, periféricos y software usados en LANs, el sistema de cableado o cabling plant puede parecer simple y básico. Sin embargo, el cableado cuidadosamente planeado e instalado es absolutamente crítico para la funcionalidad de la LAN.

En muchas de los ambientes de oficina de hoy en día, el cableado de la red de datos ha sido instalado incrementalmente, respondiendo a los cambios de tecnología, necesidades de red y planes de la compañía. Tipicamente, este deja un legacy de sistemas incompatibles el cual puede incluir sistemas de conmutación telefónica, mainframes o sistemas de minicomputadoras, LANs basados en PC, y otros equipos de comunicación . Por que cada sistema es instalado dee acuerdo a su propio conjunto de criterios de alambrado, usando diferentes tipos de cables, ellos son difíciles de interconectar, y especialmente difíciles de mantener y expandir. Esta situación es típica de un sistema de alambrado no

estructurado, donde no hay conjuntos simples de estándares para la interconexión.

Aunque los costos iniciales son comparativamente bajos para un alambrado no estructurado, en grandes términos la dificultad y encarecimiento de la integración o reemplazo de sistemas alambrados incompatibles son considerables.

En años recientes, una clara tendencia de los diseñadores de red, ha sido implementar un cableado de redes acorde con un estándar uniforme y planificado como un sistema de cableado estructurado.

Esto envolucra un salto en la perspectiva. Mejor que ver un simple cableado como una forma de conectar dispositivos, el cableado es visto como una entidad arquitectural importante: El "cabling plant", "cabling system", ó "premises wiring". La intensión es proveer una capacidad de cableado instalado que no únicamente provea Inter-operatibilidad para tecnologías de red existentes, sino también que permita la eficiente reconfiguración, anticipando el futuro crecimiento.

Al implementar un sistema de cableado estructurado, es mas eficiente instalar cuando un edificio está en construcción ó remodelado, que regresar mas tarde e instalar los alambres a través de las paredes existentes, bandejas y pisos. Como un tema práctico, los Arquitectos y

dueños de edificios algunas veces necesitan instalar cables antes que saber que tipo de red se tendrá. En este aspecto, el cableado estructurado puede proveer una orientación para un sistema de cableado universal que podría ser adaptado en la mayoría de los requerimientos de red.

El interés en el cableado universal es soportado por tres tendencias:

- Convergencia en tres tipos de cables
- Uso de una topología distribuida en estrella física basada en hub
- Surgimiento de los estándares de la industria.

La habilidad para preinstalar el cableado de planta esta basado en que, todas las tecnologías LAN mayores pueden ser soportados por tres tipos de cables

- Shielded twister-pair (STP)
- Unshielded twister-pair (UTP)
- Fiber óptic

Cada tecnología LAN significativa puede ser soportado por STP o UTP para la mayoría de segmentos de longitud corta y media. El cable de Fibra Óptica puede ser reservado para grandes conexiones backbones, o donde hay una necesidad grande por la inmunidad a las intermitencias.

Esto nos provee puntos centralizados para la interconexión, mantenimiento, y aislamiento de fallas. Los hubs son la clave de los

dispositivos integrados, debido a su habilidad para proveer expansión flexible. Los Hubs pueden ser conectados juntos por segmento "backbone", para formar una topología física estrella multiple, algunas veces conocido como una estrella distribuida. Un sistema de cableado universal puede ser instalado con confianza de que cualquier hub esta eventualmente instalado, debido a que cada fabricante de hub proveerá interfaces para los tres tipos de cables.

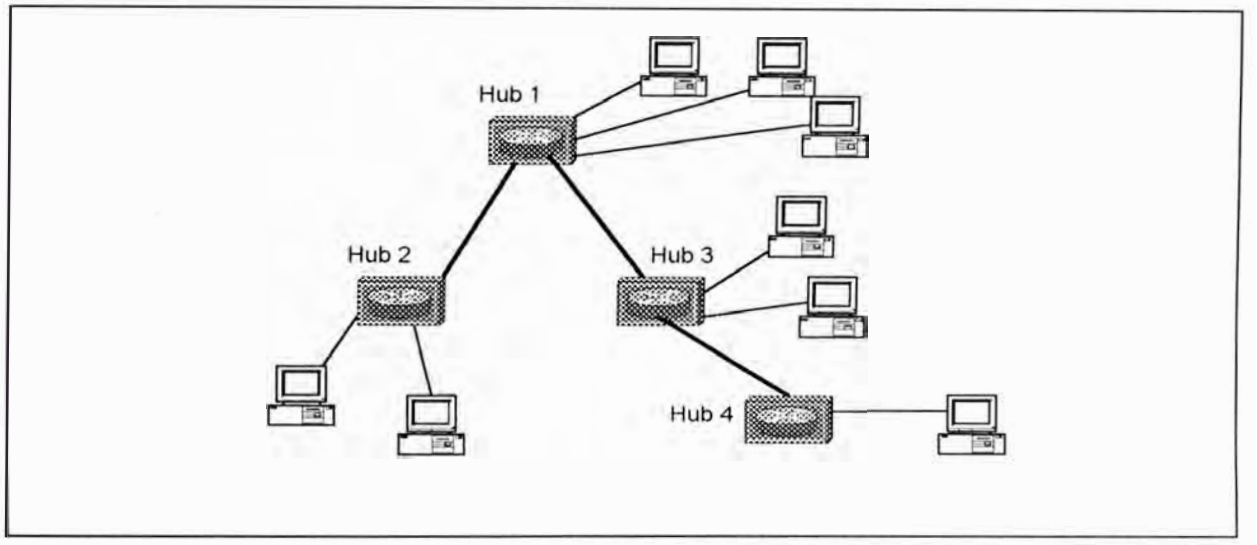


Figura 3-1 Topología estrella distribuido.

Los mas importantes vendedores están entre los primeros en darse cuenta de la importancia de los sistemas de cableado estrcuturado, respondiendo con planes de cableado "pre-engineering", el cual aseguró la apropiada funcionalidad de sus dispositivos en una red "enterprice". Las compañías telefónicas estuvieron entre los primeros, basados en sus experiencias con instalaciones de cable telefónico. Algunos de los mayores sistemas de cableado estructurado son listados en la Tabla 3-1.

VENDOR	PLAN DE CABLEADO ESTRUCTURADO
AT&T	Systrimax premises Distribution System
DEC	DEConnect
IBM	IBM Cabling System
Northern Telecom	Integrated Building Distribution Network (IBDN)

Tabla 3-1 Planes de Cableado Estructurado.

El Electronic Industry Associates (EIA) y el Telecomunications Industry Association (TIA) han tomado el liderasgo en proveer un estándar abierto para la industria del cableado que no está unido a un vendeor específico. Una relevancia particular es su estándar de cableado de telecominication en edificios comercial (EIA/TIA-568) el cual da a los usuarios y vendedores guias para las premisas del cableado. Esto incluye:

- Sample topologies
- Limitaciones de distancia
- Tipos de cable para una velocidad de red dada
- Tipo de conector a ser usado con el tipo de cable dado
- Especificaciones ded performancia mínima para conectores y cables.

El EIA/TIA-568 esta siendo renombrado a EIA/TIA SP-2840 . Otros estándares EIA/TIA importantes incluyen:

- Estándar para edificios comerciales para espacios y pathway de telecomunicaciones (EIA/TIA-569).
- Estándar dee cableado de telecomunicaciones para Light Comercial y Residencial /EIA/TIA-570)

En resumen, los bene0ficios de un sistema de cableado estructurado basado en estándar son:

- Interoperatibilidad ded dispositivos regardless de vendedor.
- Efectividad de costos en término largo basado en la instalación de sufiiciente cable para las necesidades del futuro, proveyendo un ruta de actualización para nuevas tecnologías, y mantenimiento reducido debido a una arquitectura y materiales existentes.

3.1.- OVERVIEW DEL CABLE DE PLANTA

El concepto de cableado estructurado se parece al cableado de planta en términos de edificios de oficinas. En la industria telefónica, la oficina de un cliente es conocido como la customer´s premises, y el cable instalado allí es conocido como premises wiring

3.1.1.- Subsistemas de Cableado Estructurado

Los sistemas de cableado estructurad como EIA/TIA – 568 refiere a premisas del cableado en términos de seis subsistemas modulares:

- Entrada a la construcción.
- Cuarto de equipos
- Backbone vertical
- Closet de cableado
- Cableado Horizontal
- Area de trabajo

Cada subsistema es caracterizado por típicos tipos de dispositivos e interconexiones. La figura 3-2 muestra un ejemplo simplificado de un edificio con sus subsistemas de cableado.

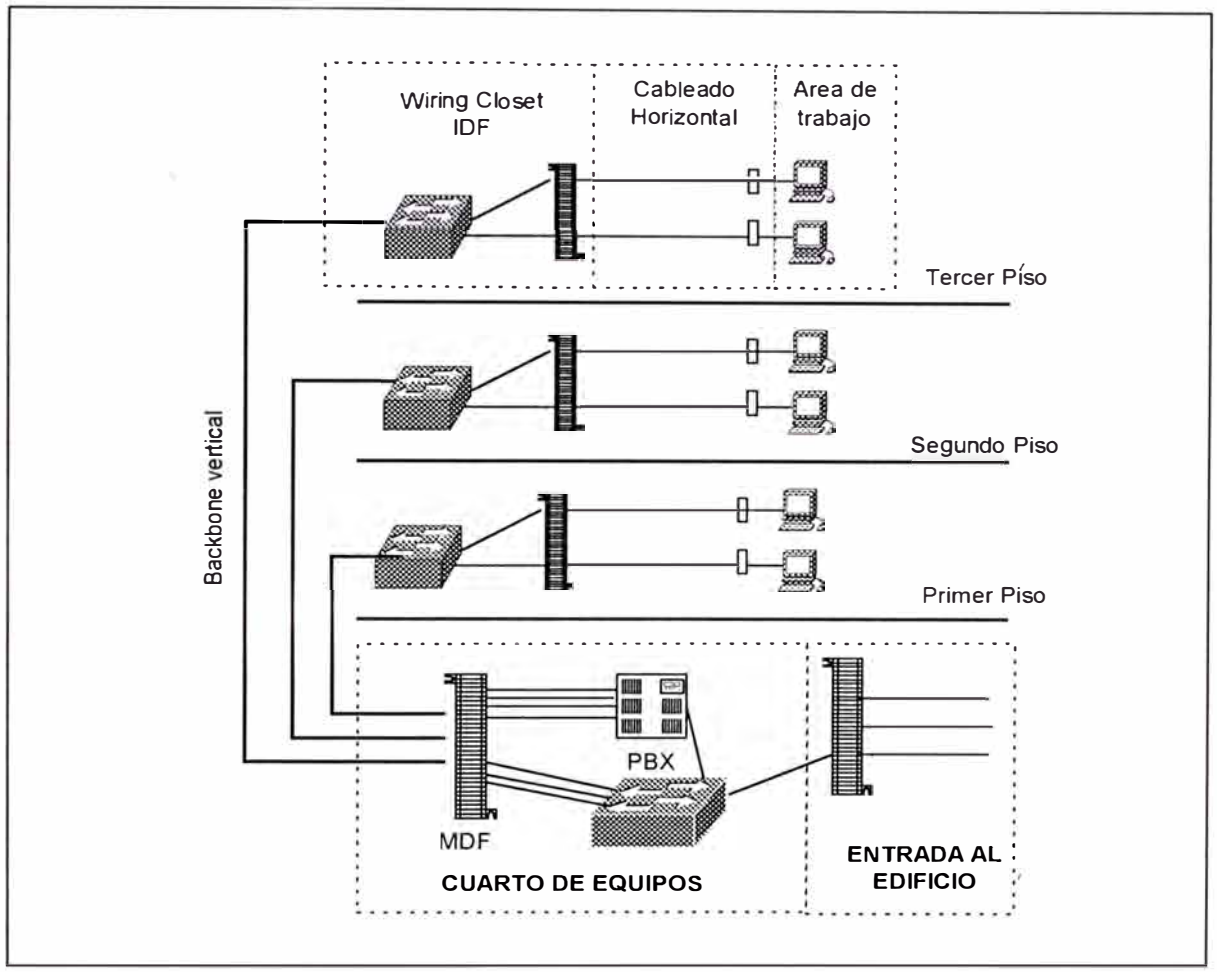


Figura 3-2 Subsistema de Cableado Estructurado

Entrada a la Construcción.- En una típica construcción de oficina, hay un punto de entrada y salida para todos las líneas de telecomunicaciones, incluyendo teléfonos, backbone de data }, y otras facilidades de transmisión WAN. Este puede ser un closet separado o un ambiente, o puede ser compartido con un cuarto de comunicaciones. Dentro de la entrada del edificio, un dispositivo cross-connect típicamente provee un punto ndee

terminación para cables y permite la interconexión de dispositivos de una manera limpia y sistemática. Hay dos tipos de dispositivos de "cross-connect":

- Punch-down block
- Patch Panel

Los "Punch-down" block fueron desarrollados para proveer un punto de conexión para los cables telefónicos. Ellos simplifican la instalación del cable, debido a que provee un único punto de terminación para el ingreso de cables al edificio o al closet de cableado. Cada filamento del cable par trensado es presionado semi-permanentemente dentro de un canal en el bloque "punch-down". El canal fija el filamento y penetra el aislante para proveer la conexión eléctrica.

Desde el bloque punch-down, los cables patch pueden ser corridos mas tarde al puerto apropiado del equipo tal como un hub (para cables LAN) o hacia un "Private Branch Exchange" (PBX) para los cables de voz.

Los bloques punch-down son típicamente montados en paneles adjuntos a la pared del closet de cableado. Algunos bloques punch-down vienen con una serie de salidas RJ45 para que cada cable individual pueda ser punchado en un lado, y los cables patch conectorizados puedan estar adjuntados en el otro lado.

Los patch-panel son diseñados para máxima facilidad de reconfiguración, ya que provee puertos conectorizados para la interconexión de equipos. Por ejemplo, un típico patch-panel para UTP debería tener una serie de salidas RJ45 para aceptar terminaciones de cables RJ45 o patch-cords. Los patch-panel son algunas veces montados en racks de equipos. La figura 3-3 nos muestra un punch-down block y configuraciones de patch panel en un closet de cableado.

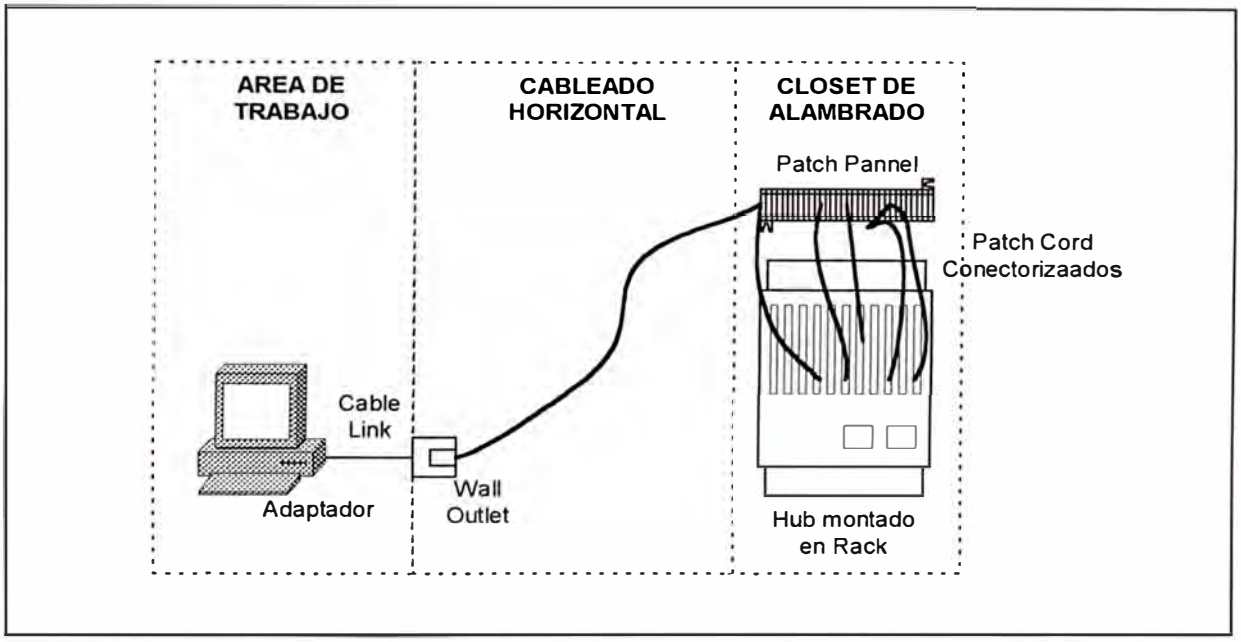


Figura 3-3 Diagrama del Closet de alambrado y Cross-Connexión.

Muchos dispositivos cross-conect son pre-alambrados con un jack de 50 conectores en un terminal conocido como conector telco, y el cual es diseñado para un cable de 25 pares. Estos son típicamente usados para interconectar el cross-conect y el dispositivo de red tal como hubs, switches y routers. El cable de 25 pares viene en una variedad de configuraciones que incluyen:

- Interface de 50-conectores en cada terminal
- Interface de 50 conectores en un terminal y ocho plugs machos RJ45 separados en el otro. (un octopus).
- Interface de 50 conectores en un terminal y un grupo de ocho salidas RJ45 (una harmonica)

Cuarto de Equipos.- En grandes oficinas, puede haber un cuarto de equipo centralizado para almacenar dispositivos como sistemas telefónicos PBX, banco de modems, y Hubs LAN. En términos de cableado LAN estructurado, este incluiría un principal cross-conect, algunas veces conocido como un main distribution frame (MDF). El MDF provee un punto de interconexión central para el cableado de red.

Los dispositivos IDF colapsan a uno o mas dispositivos Main Distribution Frame (MDF) en una estrella. Cada IDF usualmente conecta a dos dispositivos MDFs diferentes para proveer adecuada redundancia. Algunas organizaciones ubican ambos dispositivos MDF en el mismo closet físico y confían en un enrutamiento desigual del cableado vertical para redundancia. Otras Organizaciones prefieren ubicar el dispositivo MDF en closets separados pero próximos. Las relaciones entre edificios y MDF no es una regla dura, cuanto mas grande el edifico, podría tener mas que dos switches MDF, mientras un par de dispositivos redundantes MDFs podrían ser capaz de soportar múltiples edificios que son mas pequeños en tamaño.

La figura 3-4 muestra tres edificios con closets MDF. Para encontrar los requerimeintos de redundancia de cada edifico, generalmente aloja dos dispositivos MDFs. Los dispositivos MDFs pueden también ser usado para interconectar los tres edificios.

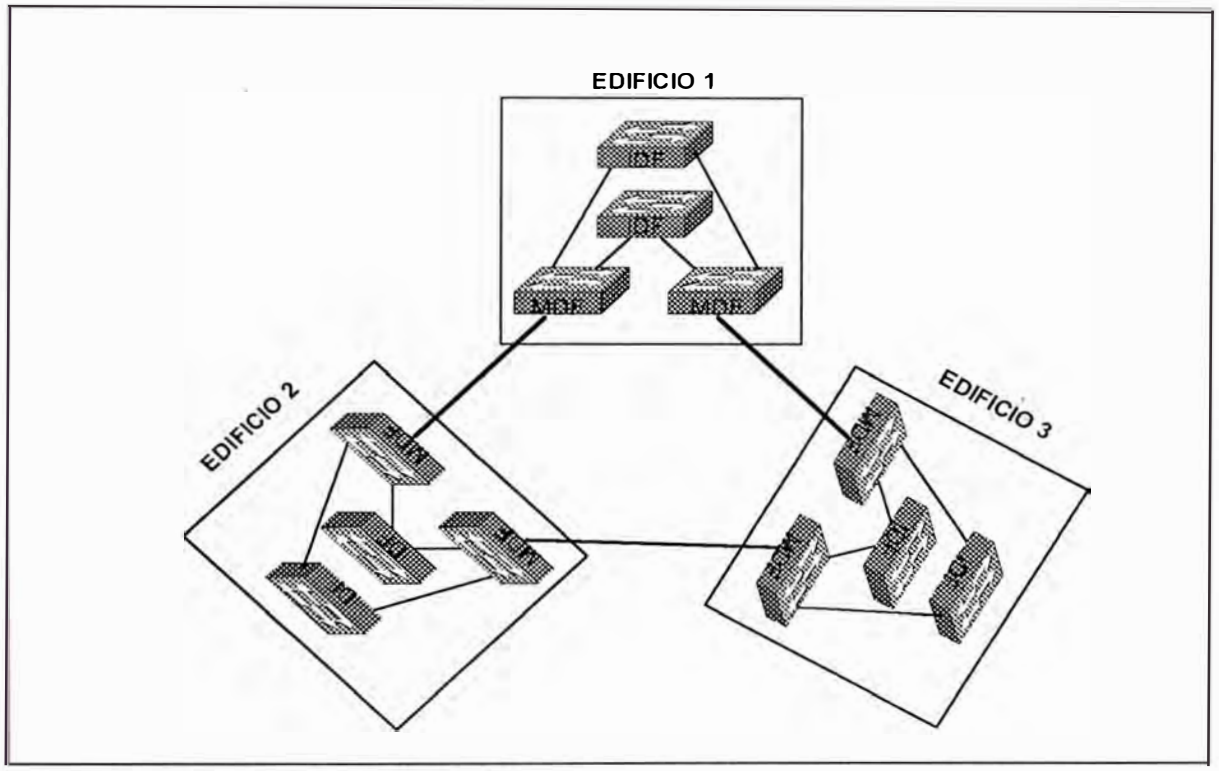


Figura 3-4 Tres edificios con sus respectivos closet de alambrado IDF y MDF

Los closets MDF tienen un conjunto diferente de requerimientos y concerns que los closets MDF:

- Troughput
- Alta disponibilidad
- Capacidades de enrutamiento

Dado que ellos actúan como puntos de concentración para el tráfico IDF, los dispositivos MDFs tiene que ser capaz de llevar niveles de tráfico extremadamente altos. Sin embargo muchas de las estrategias de alcanzar diseños robustos y escalables requieren enrutamiento en los MD´s.

Alta disponibilidad es un requerimiento importante para dispositivos MDFs. Aunque la falla de un switch MDF o IDF potencialmente afecta muchos usuarios, hay una distinción entre estas dos situaciones. La falla de un dispsoitivo IDF completamente deshabilita cientos de usuarios adjuntos a las estaciones finales. Por otro lado, debido a que los MDFs son casi siempre desarrollados en pares, la falla raramente resulta en una completa pérdida de conectividad. Sin embargo, este no es dicho que fallas de MDF son inconsecuentes. Por lo contrario, las fallas MDF algunas veces afectan a cientos de usuarios, mucho mas que con una falla de IDF. Esto requiere que tantas características como sea posible transparentemente reenruten el tráfico alrededor ded un problema de MDF.

Tres tipos de dispositivos pueden ser utilizados en closet MDFs:

- Switches capa 2
- Hybrido, switches dee enrutamientos como MLS
- "Switching routers " como el catalyst 8540

El priemro es el mas simple, un switch de capa 2. El costo modedrado y alto troughput de estos dispositivos pueden hacer de ellos una

opción muy atractiva. Ejemplo de estos dispositivos incluyen el catalyst 4000 y el tradicional catalyst 5000 sin un Route Switch Module (RMS) o NFFC.

Sin embargo hay razones convincentes para usar procesamiento de capa 3 en el MDF. Esto guía a muchos diseños de red a utilizar la tercera opción, un switch de capa 3 que es funcionalmente como un router basado en hardware. El swtiche catalyst 8540 es un excelente ejemplo de este dispositivo.

Cableado Backbone vertical.- El cableado backbone es usualmente conocido como cableado vertical. Un ejemplo es el cable que corre desde un cuarto de equipos en la base hacia un closet de cableado en un piso superior. Los cables backbone, separados algunas veces correrían desde el MDF cross-conect a cada uno de los closet de cableado. En otros casos, los closets de cableado pueden ser directamente conectados a cada uno con cables backbone. Este es conocido como un enlace Inter-closet. El cableado backbone puede ser cable UTP, STP, o Fibra óptica.

Closet de Cableado.- Los closet de cableado, típicamente al menos uno en cada piso, almacena uno o mas hubs. Los hubs son interconectados a las estaciones ubicadas en cada piso. Aunque un esquema específico variaría de lugar en lugar, típicamente habría uno o mas equipos de cross-conect el cual interconecta el hub montado en rack a los cables backbone y a los cables individuales que van hacia las placas de las paredes en cada área de

trabajo del usuario. Los cables cortos usados para interconectar el hub y el cross-conect son llamados patch cables. El equipo en el closet de cableado es conocido como equipo Intermediate distribution frame (IDF).

Los closet de cableado IDF son usados para conectar dispositivos de estaciones finales tales como PC´s y terminales de red. Este "cableado horixontal" conecta al wall plate jack en un terminal y típicamente consiste de cable de par trensado sin apantallar (UTP) que forma una estrella hacia el closet de cableado IDF. Como mostrado en la figura 3-5, cada piso de un edificio generalmente contiene uno o mas switches IDF. Cada estación final conecta ala closet de cableado IDF mas cercano. Todos los IDF´s en un edificio generalmente conectan a un par de dispositivos MDF algunas veces localizados en la base dedl edificio o piso bajo tierra.

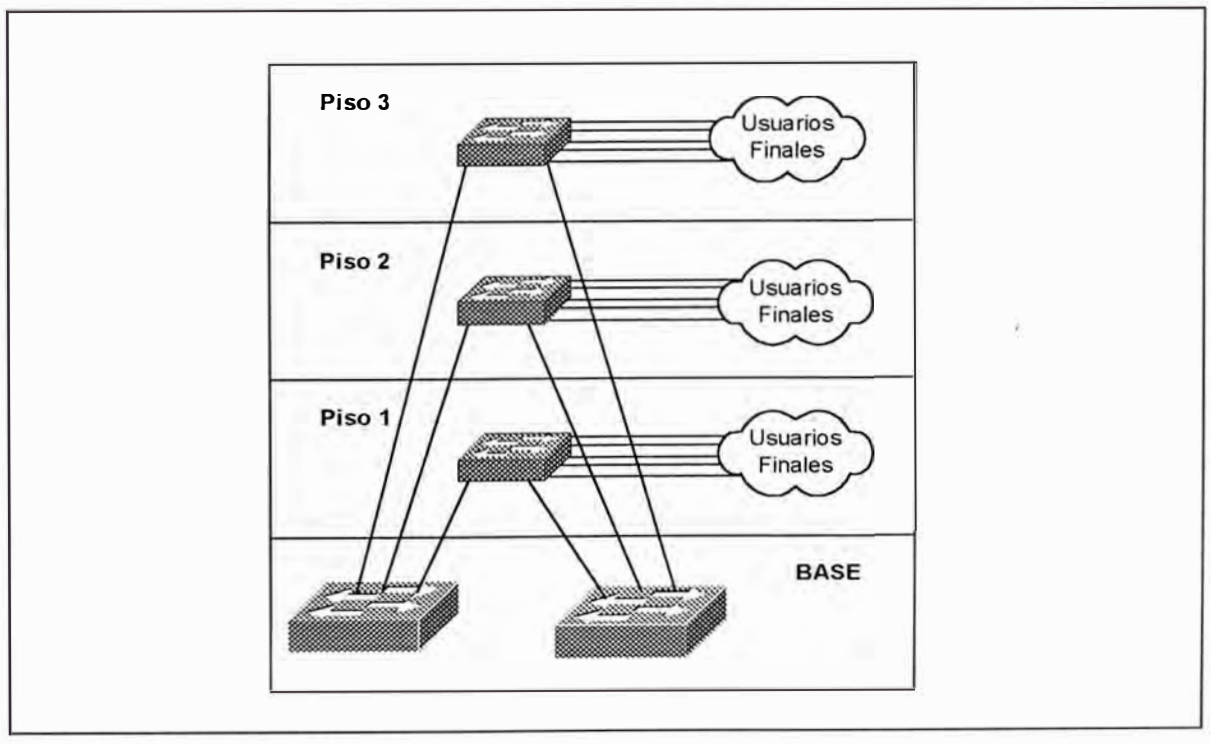


Figura 3-5 Multiples Closet de Alambrado IDF´s

Dado la regla que ellos llevan a cabo, los "closet" de cableado IDF tienen muchos requermientos específicos:

- Densidad de puerto: Debido a que un gran número de estaciones necesitan conectarse a cada IDF, hay que tener una alta densidad de puertos.
- Costo por puerto: Dado una densidad de puertos alto encontrado en un típico IDF, los costos por puerto tienen que ser razonables.
- Redundancia: Debido a que cientos de estaciones se conectan hacia cada dispositivo IDF, una falla simple de un IDF puede crear un problema significante.
- Confiabilidad: Este punto está obviamente relacionado al punto previo, sin embargo, esto resalta el hecho de que un dispositivo IDF que es usualmente una estación final, únicamente se conecta al resto del mundo.
- Fácil administración: El alto número de conexiones requiere que la administración por puerto sea mantenida a un mínimo.

Debido a los numerosos usuarios finales directamente conectados, la redundancia y la confiabilidad son críticos para la función del dispositivo IDF. Como resultado, los IDF´s no únicamente deberían utilizar hardware redundante tales como supervisor dual y power supply, deberían también tener múltiples enlaces a los dispositivos MDF´s. Una rápida respuesta a falla de estos componentes redundantes es también crítico.

La confiabilidad de los IDF´s nos llevan a un punto interesante acerca de las conexiones de las estaciones finales. Fuera de los ambientes limitados, tales como el piso de "finanzas traiding", la relación costo y efecto no es muy bueno al tener estaciones finales conectados a mas de un dispositivo IDF. Además, el cableado horizontal sirve como un único punto de falla para la mayoría de las redes. Sin embargo, notar que estas fallas generalmente afectan únicamente a las estaciones finales. Para estaciones finales de importancia, tales como servidores, tarjetas de interface de red de puerto-dual, pueden ser utilizados conexiones con múltiples enlaces a los switches de "servidores farm" redundantes.

El equipo tradicional para uso en un IDF es el Hub. Debido a que la mayoría de hubs son dispositivos muy simples, el precio por puerto puede ser muy atractivo. Sin embargo, la naturaleza compartida de los hubs obviamente puede proveer menos disponibilidad de ancho de banda. Por otro lado, los routers y swtiches capa 3 pueden proveer decisiones de ancho de banda compartido extremadamente inteligente. En el lado débil, estos equipos pueden ser muy caros y generalmente tienen densidad de puertos limitados.

Para emitir un balance entre costo, ancho de banda disponible, y densidad de puertos, casi todas las recientes "redes campus" desarrolladas usan switches capa 2 en el IDF. Esto puede ser una buena manera de

reducir la razón costo efecto, para proveer 500 o mas estaciones finales con acceso a altas velocidades dentro del "backbone campus"

Cableado Horizontal.- El cableado horizontal es el cableado desde el "closet" de cableado a la placa de pared cerca de la estación del usuario. El cableado horizontal es típicamente cable UTP o STP.

Área de Trabajo.- El subsistema de área de trabajo consiste del cable y otros dispositivos (tales como un transeiver ethernet) conectando la estación del usuario a la placa de la pared. El cableado del área de trabajo es típicamente UTP o STP. Los cables del área de trabajo son usualmente conectorizados en ambos extremos para unir el adaptador de puerto de la tarjeta y la placa de pared de salida.

3.1.2.- Subsistemas de Cableado Universal

No todas las premisas del cableado pueden ser consideradas como universal. El sistema de cableado universal principalmente consiste de un subsistema de cableado horizontal y un subsistema de cableado "backbone", incluyendo paneles "cross-conect" en el "closet" de cableado y sala de equipos. Estos son partes de una planta de cableado estructurado, el cual es independiente del vendedor y puede ser pre-instalado a priori a todo el diseño de red. Las otras partes del equipo y cableado, variarán según las especificaciones por fabricante y por el tipo de tecnología LAN elegido.

3.1.3.- Distancias de Cableado Estructurado

El estándar EIA/TIA-568 recomienda las distancias de cableado máximo por subsistema de equipamiento y tipo de cable. Algunos de estos son listados en la Tabla 3-2

SUBSISTEMA	FUBRA OPTICA	U.T.P.	S.T.P
Backbone	2000 m	800 m	700 m
Enlace Inter closet	2000 m	800 m	700 m
Cableado Horizontal * Closet - wall Plate * Wall Plate - adaptador	 N/A N/A	 90 m 10 m	 90 m 10 m

Tabla 3-2 Máximas distancias de cableado

Sin embargo, estos son guías flexibles y tienen que ser comparados para limitaciones mas específicas y parámetros provistos por fabricante y por los estándares IEEE y ANSI FDDI

3.2.- SEÑALES DE TRANSMISIÓN BASICA PARA MEDIOS DE COBRE

La variedad mas común de cableado para LAN son hechos de cable de cobre, siendo el mas prevaleciente de estos el "Unshielded twister pair" (UTP), "shielded twister pair" (STP) y cable coaxial.

La transmisión de patrones de bits sobre cables de cobre es llevada a cabo al variar los niveles de voltaje en la línea, en un patrón preciso, ó código, para representar un binario uno ó cero. Estas señales tienen que ser sincronizados precísamente, y el circuito de sincronización en

las estaciones de envío y recepción tienen que estar coordinados. Cuando una señal es transmitida, cada bit tiene una ventana específica de tiempo, cuya longitud depende de la razón de transmisión total. Este es llamado un bit time y la secuencia de bits es llamado bit stream.

Como un bit stream es transmitido en la linea, muchos parámetros tiene que ser mantenidos para preservar la comunicación de data precisa:

- Timing circuits tiene que ser mantenidos sincronizados con el bit stream.
- El voltaje builtup tiene que ser evitado.
- La señal tiene que ser fuerte y suficientemente clara para que los equipos receptores interpreten esto precisamente.

Voltaje Built up.- Para evitar daños a los dispositivos de red, excesivo voltaje DC no tiene que ser permitido para construir la linea. Como ejemplo teórico, si el código de línea representa un binario uno con voltaje positivo, y un binario cero sin voltaje, resultaría en una señal como en la figura 3-6.

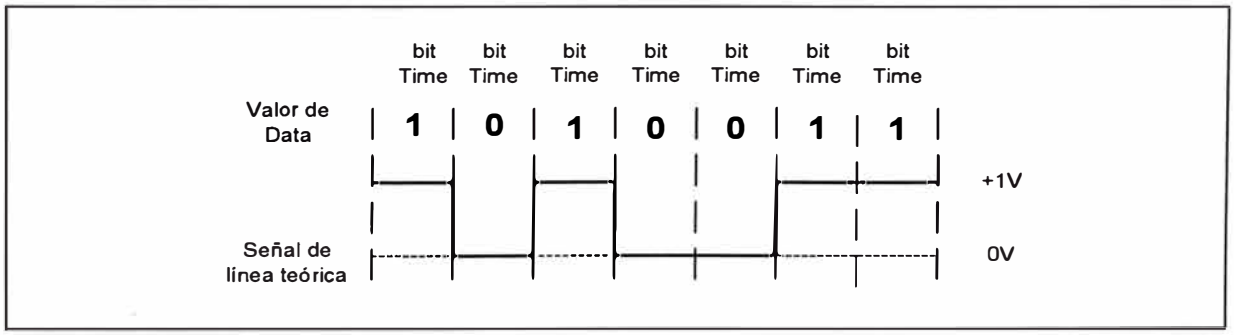


Figura 3-6 Señal de línea teórica que resulta en un voltaje Buildup

Continuando la transmisión de un voltaje positivo para binarios unos, un voltaje positivo DC sería construido en la línea y potencialmente dañar el equipo adjunto. Esta situación es evitada por un número de técnicas de codificación de líneas el cual alterna los voltajes positivos y negativos. Usando estos códigos, el normal bit stream causa voltajes positivos y negativos para cancelarse mutuamente . Por ejemplo , la codificación Manchester usado para ethernet LAN provee un cambio de voltaje dentro de cada bit time. Como mostrado en la figura 3-7, un binario uno es representado por una transición de un voltaje positivo a uno negativo, y un binario cero es represemntado por una transición de un voltaje negativo a uno positivo.

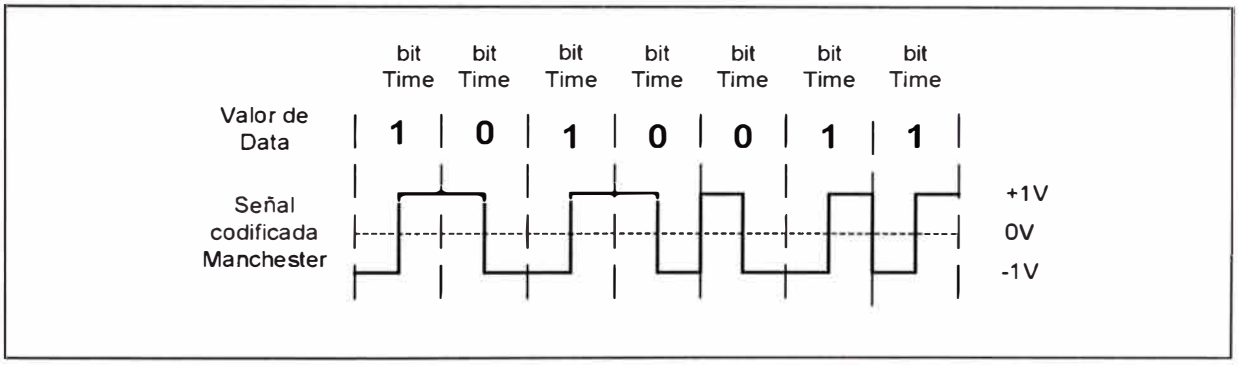


Figura 3-7 Codificación de Línea Manchester

Sincronización de Tiempo.- Para precisamente interpretar el bit stream, el circuito de sincronización del equipo receptor tiene que estar sincrinizado con los pulsos de señal. Los esquemas de codificación de línea provee una manera para que esto ocurra. Una técnica para el circuito de sincronización es coordinar con la transmisión del voltaje ocurra en el bit stream. La codificación Manchester, por ejemplo provee una transición de voltaje cada

bit time, haciendo esto facil para los dispositivos receptores para sincronizar las transmisiones de voltaje numerosos. Técnicas similares usados con otros sistemas de codificación de linea, incluyendo "Manchester" diferencial usado con FDDI.

Fuerza de la Señal.- Para que un bit stream sea reconocible, los pulsos de voltaje tiene que ser fuertes para ser registrados por el circuito receptor. Una característica de la señal debido a que viaja a lo largo de un conductor es la pérdida de fuerza, o amplitud. Este problema de pérdida de amplitud es conocido como atenuación.

3.3.- PROBLEMAS DE TRANSMISIÓN

La performancia actual de los medios de cable de cobre pueden ser dramáticamente influenciados por muchos problemas típicos y características del cable. Estos incluyen:

- Wired MAP
- Ruidos eléctricos
- Crosstalk NEXT
- Power Sum NEXT
- FELXT y ELFEXT
- Atenuación
- Razón de Atenuación a Crosstalk (ACR)
- Capacitancia
- Impedancia

- Resistencia DC
- Continuidad y polaridad
- Longitud del cable
- Retardo
- Retardo "Skew"

Cada uno de estas características pueden ser cuantificados y verificados, los estándares para cada tipo de cable han sido establecidos por la EIA/TIA y el "Underwriter´s Laboratory" (UL). Como regla general, todas las instalaciones de cable deberían ser sometidos a procesos de "Test".

"Wired MAP".- El wiremap es usado para identificar los errores de instalación. Para cada uno de los 8 pares de conductores en el cable, el "wiremap" indica:

- Apropiada terminación de pin en cada terminal
- Continuidad al terminal remoto
- Cortocircuito entre cualquiera de dos o mas conductores
- Pares cruzados
- Pares revertidos
- Pares superpuestos
- Cualquier otro error de alambrado

La correcta conectividad es ilustrado en la figura 3-8:

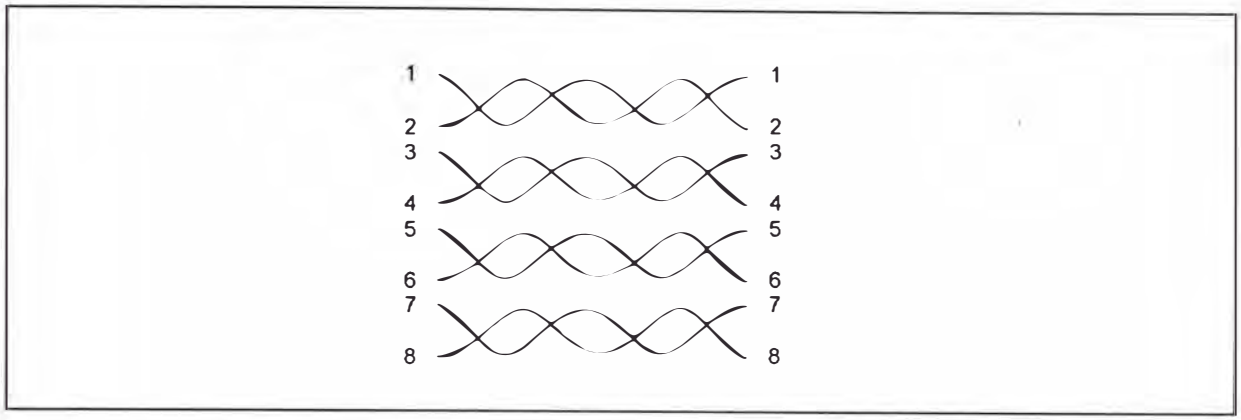


Figura 3-8 Conectividad correcta de los pares de un cable

Un par reservado ocurre cuando la polaridad de un par de alambre es reservado en un terminal del enlace (también llamado un tip/ring reversal). Un par cruzado ocurre cuando los dos conductores en un par de alambre son conectados a la posición para un para diferente en el conector remoto. El par split son ocurre cuando la continuidad pin a pin es mantenida pero los pares físicos son separados. Refiérete a la figura 3-9 para una ilustración ded un par reservado, para cruzado y par split

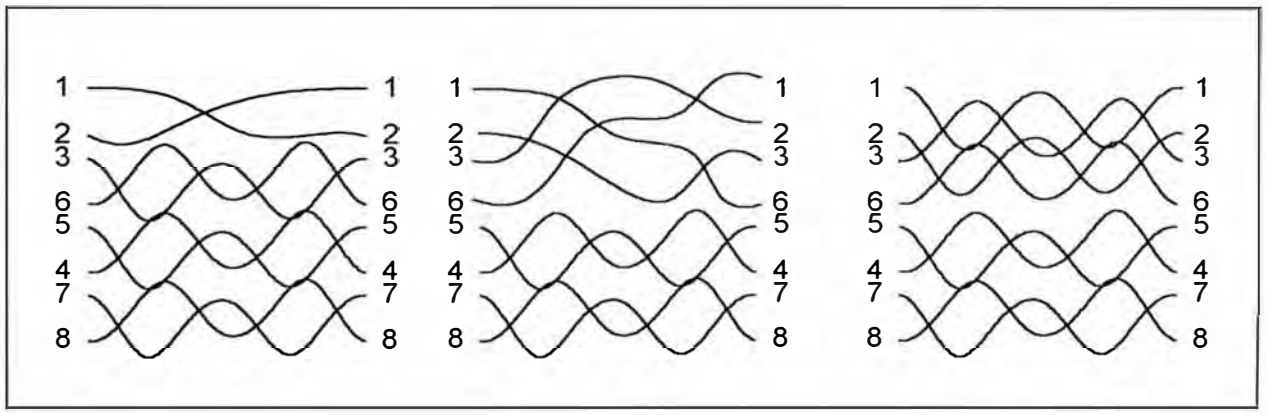


Figura 3-9 Pares revertidos, pares cruzados y pares superpuestos

Ruido Eléctrico.- La actividad eléctrica en la vecindad de un cable de cobre LAN puede distorsionar la señal LAN, causando ruidos y errores. Esto es debido al principio físico que un voltaje fluctuante en un conductor o

dispositivo produce un campo magnético cambiante alrededor de esta. Cuando ese campo magnético cambiante cruza otro conductor, induce un cambio de voltaje en ese conductor, causando distorsión de la señal y ruido. Esta propiedad de un dispositivo o señal de interferir a otro es también conocido como Interferencia Electromagnética (EMI), Interferencia de Radio Frecuencia (RFI) ó como EMI/RFI.

El ruido es medido en unidades de milivoltios(mV) ó decibelios milivoltios (dBmV) sobre un periodo de tiempo, y es usualmente categorizado como bajo, medio o frecuencia alta. Fuentes de ruido incluyen luces fluorescentes, luces "dimmers", líneas AC, intercomunicadores, computadoras, copiadoras, equipos médicos (algunas veces una fuente extremadamente alta), radios, televisores, motores, y switches de alta capacidad.

"Crosstalk" (NEXT).- El "crosstalk" es un ruido causado por una señal eléctrica en un cable, induciendo un voltaje de fluctuación en un cable adyacente. En líneas telefónicas, el "crosstalk" puede algunas veces ser escuchado como la conversación de alguien mas en la línea. En líneas de datos, esto puede guiar a errores. El "crosstalk" es típicamente descrito como "Near end crosstalk" (NEXT) y calibrados en decibelios. El NEXT es medido al inyectar una señal conocida en una línea y midiendo la fuerza de la señal inducida en la línea adyacente. Estos resultados son descritos como la razón de la señal primaria a la señal inducida, además un número alto es

bueno. Este es algunas veces conocido como signal to noise ratio (SNR). Los estándares publicados describen el NEXT aceptable para cables bajo situaciones ideales, unspooled y lejos de cualquier fuente de EMI/RFI. Sin embargo, el NEXT para las instalaciones actuales pueden variar dramáticamente, y deberían también ser probados upon la instalación.

El corsstalk se incrementa con altas frecuencia de la señal y pueden exibir picos y valles, a lo alrgo del espectro de frecuencias y en relación a la posición del cable corrido. Cuando mas largo sea el cable, es menos inmune al crosstalk.

Cuando la corriente fluye en un alambre, un campo electromagnético es creado el cual puede interferir con la señal en al almabre adyacente. Como la frecuencia se incrementa, este efecto viene a ser mas fuerte. Cada par es tresado por que esto permite campos opuestos en el par de alambre para cancelar cada unoi. A medida que sea mas trensado el para de alambres, es mas efectivo la cancelación , y mas alta la razón de data soportado por el cable. Manteniendo esta razón de trensado es simplemente el factor mas importante en cuanquier instalación UTP satisfactoria.

Si los alambres no son trensados, el resultado es un near end crosstalk (NEXT). Si tu has tenido una llamada telefónica donde tu podrías escuchar otra conversación en el fondo, tu tienes una experiencia de

"crosstalk". En realidad, el nombre crosstalk deriva de las aplicaciones de telefonía donde "talk" viene "across". En LANs, el NEXT ocurre cuando una señal fuerte en un par de alambres es recogido por un par adyacente de alambres. El NEXT es la porción de la señal transmitida que es electromagnéticamente acoplado en la señal recibida. El receptor puede no ser capaz de distinguir entre la señal real recibida y el ruido "crosstalk".

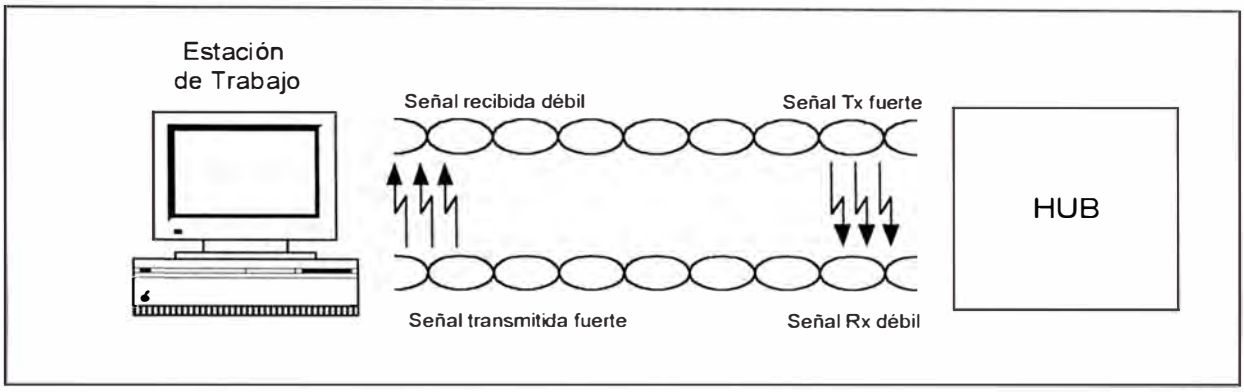


Figura 3-10 Ejemplo de un Near End crosstalk.

Si nosotros permitimos que la radiación electromagnética creada por el "crosstalk" sea tan alta, nosotros creamos dos problemas: no únicamente hacemos la performace impar en el cable, también creamos emisiones inaceptables al FCC. Esto crea un dilema frustante. Si hacemos los niveles de transmisión tan fuertes no seríamos capaz de encontrar los requerimientos FCC, pero si hacemos la señal tan débil sería difícil diseñar receptores que eviten errores debido al ruido "crosstalk".

Notar que un bajo NEXT es un número alto (ejemplo 45 dB). Esto significa que hay una gran diferencia entre la magnitud de una señal transmitida y su "crosstalk" asociado. Alto NEXT, el cual es indeseable, es

bajo número (ejemplo 20 dB) significa que el corsstalk es mas significante relativo a la fuerza de la señal transmitido.

Para encontrar los estándares de la categoría 5, todos las conexiones de cables son permitidas a maximo de 13 mm de conductores no trensados en el punto de terminación.

Las causas comunes de excesos de NEXT incluyen:

- Uso de cables patch no trensados
- Pobres prácticas de terminación
- Uso de bloques punch down antiguos
- Uso de conectores no degradables
- Uso de cables de grado de voz
- Uso de acopladores modulares de 8 hembra a hembra.

Es extremadamente importante medir el NEXT desde ambos extremos del cable o enlace bajo prueba. El NEXT es específico a cada terminal del enlace, y es normal obtener resultados diferentes significantes a cada terminal. Todos los estándartes el cual incluye mediciones de NEXT requiere esto.

La figura 3-11 ilustra la forma típica de una curva NEXT para un enlace de categoría 5.

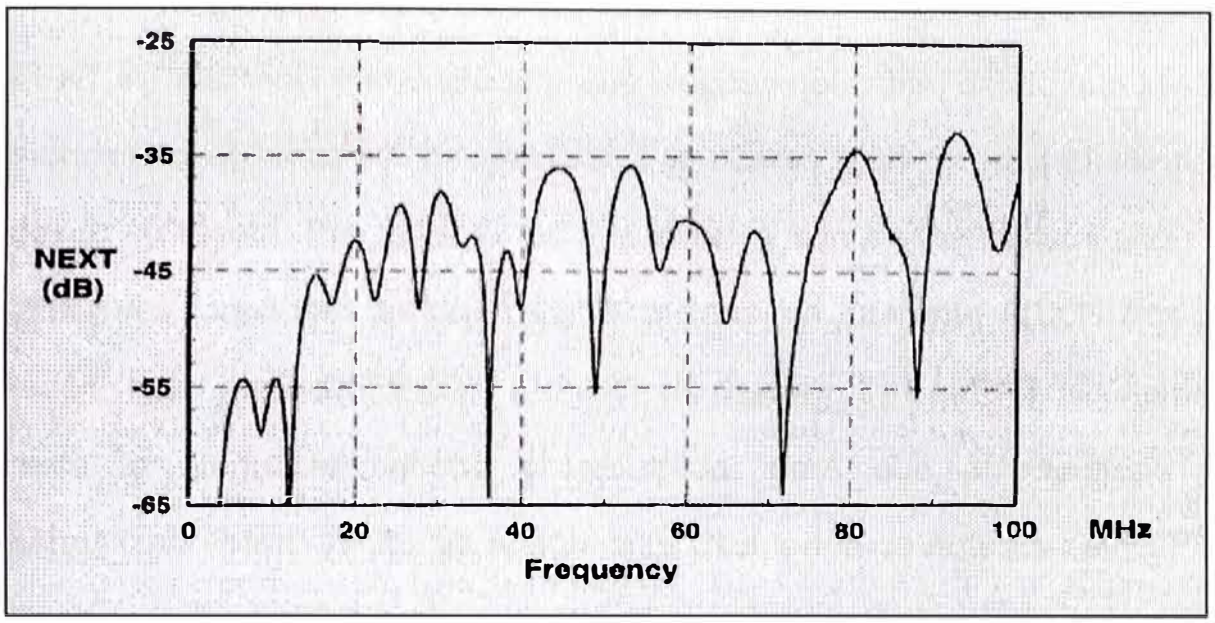


Figura 3-11 Near End crosstalk de una enlace Cat 5

Power Sum NEXT.- El Power Sum NEXT (PSNEXT) es actualmente un cálculo, no una medición. El PSNEXT es derivado desde un resumen algebraico de los efectos NEXT individuales en cada par por los otros tres pares. El PSNEXT y el ELFEXT son importantes mediciones para calificar cableados diseñados para soportar esquemas de transmisiones en los cuatro pares, tales como Ethernet Gigabit. Hay cuatro pares de resultados PSNEXT en cada terminal del enlace por enlace probados.

FEXT y ELFEXT.- El Far End Crosstalk (FEXT) es similar al NEXT, excepto que la señal es enviada desde el terminal local y el crosstalk es medido en el terminal lejano. El FEXT tiene que ser medido desde ambos terminales.

El FEXT por si solo no es una medición muy usual. Por que?. El FEXT es altamente influenciado por la longitud del cable, desde que la señal induciendo el crosstalk es afectado por cuanto esto ha estado atenuado desde su fuente. Por lo tanto los dos enlaces con similar construcción con diferentes longitudes tendrían significativamente diferente FEXT. Por esta razón, Igual nivel de FEXT o ELFEXT es medido. El ELFEXT simplemente resta la atenuación desde el resultado, para que el resultado sea normalizado para efectos de atenuación. Otra forma de entender el ELFEXT es pensar de un ACR del terminal lejano.

Para hacer las mediciones ELFEXT precisos requiere un probador de campo con rango dinámico al menos 20 dB mas bajo que el nivel de señal esperado.

Atenuación.- La atenuación es la pérdida de la amplitud de la señal o fuerza, cuando una señal pasa a través del medio de transmisión. Esto es medido en decibelios. Hay dos fuentes primarias de atenuación:

- Características eléctricas del cable, especialmente la resistencia.
- Pérdida de inserción donde el cable es interconectado, terminado, o quebrado.

La atenuación incrementa con la longitud del cable y tiene que ser medido después de que este esté instalado. Este puede ser minimizado por las conexiones cuidadosas y conectores de calidad.

Toda señal electromagnética pierde fuerzaa como ellos se propagan a lo largo de su fuente, y las señales LAN sobre los cables no son la excepción. Esta pérdida del nivel de señal con la distancia es llamado pédrida de atenuación. La atenuación es medida en desibelios (dB). Desde que esto es una pérdida, es usualmente expresado como un valor negativo. Así , -10 dB es una señal mas weaker que –8 dB. Los dedcibelios son logaritmicos, tal que si cualquiera de dos señales son 6 dB diferentes en fuerza, uno es dos veces el voltaje del otro. Así, una señal de –10dB tiene mas que dos veces el voltaje que una señal de –16 dB, y cuatro veces el voltaje de una señal de –22 dB.

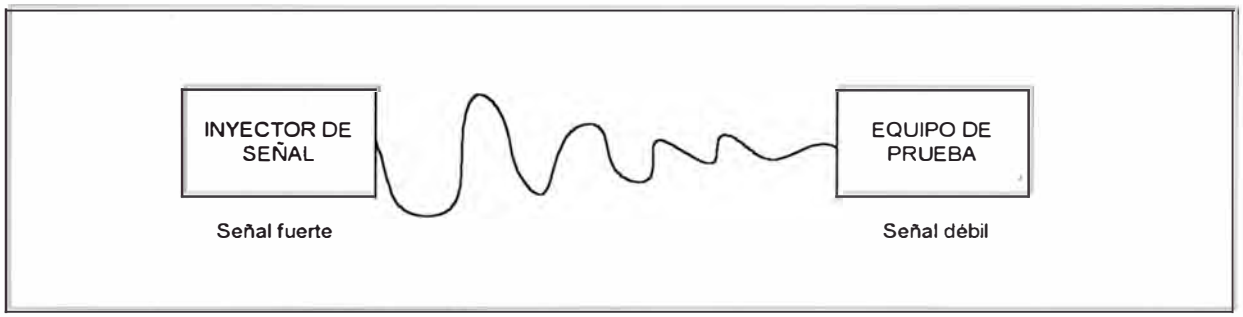


Figura 3-12 Atenuación del cable

Las dos principales contribuciones para la atenuación son el efecto skin y la pérdida dieléctrica. Cuando la corriente fluye en un alambre a altas frecuencias, su densidad no es uniforme a través del conductor pero es concentrado en la superficie o skin del conductor. Este efectivamente reduce el área de conductor llevando la corriente, y resulta en pérdida el cula son aproximadamente proporcional a la square root de la frecuencia. Esto explica por que la atenuación incremente con la frecuencia, y por que los cores solidos de los cables generalmente outperforms stranded cable.

La temperatura también afecta la atenuación en algunos cables. El material dieléctrico que forma el aislamiento del conductor y la chaqueta del cable, absorve algo de las señales transmitidas a medida que estos se propagan a lo largo del cable. Esto es verdaderamente cierto en cables conteniendo PVC en el aislamiento, tales como muchos cables de categoría 3. El PVC contiene un átomo clorado que es eléctricamente activo y forma dipolos en el material aislante. Estos dipolos oscilan en respuesta al campo electromagnético circundando los alambres, y a medida que ellos más vibran, más energía es perdida en la señal. La temperatura incrementa el problema, debido a que ellos hacen mas fácil que los dipolos vibren en el aislamiento, esto trae como resultado incrementos de pérdida por temperatura. Finalmente, debido a que los estándares tienden a especificar los requerimientos de atenuación ajustado a 20 ºC, y si los cables van a ser operados a temperaturas muchos mas altas, es necesario elegir los cables adecuados con el proveedor.

La figura 3-13 indica la forma típica de una curva de atenuación para un enlace de categoría 6. Notar que en contraste al NEXT, las características de atenuación de un cable son típicamente bastante llano y a loargo de la curva.

Para medir una atenuación precisa, es escencial que hagamos una medición en una dirección, mejor que una medión en loopback y dividir la pérdida total en dos.

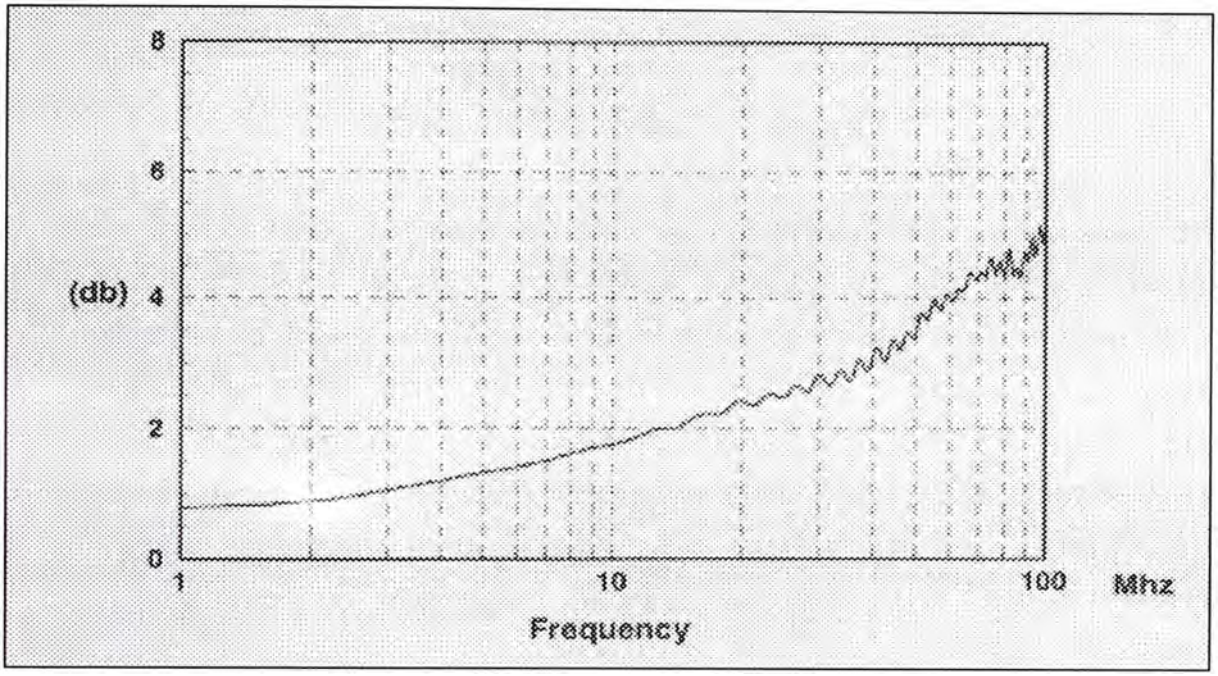


Figura 3-13 Atenuación de un enlace de Categoría 6

Razón de Atenuación a Crosstalk (ACR).- Debido a los efectos de atenuación, las señales estan en su weakest en el receptor final del enlace. Pero estos es también donde el NEXT es mas fuerte. La señal que sobrevive a la atenuación no tiene que tener pérdidas debido a los efectos del NEXT. En redes de pares trensados sin apantallar (UTP), la atenuación determina la fuerza de la señal recibida, mientras el ruido es primeramente el NEXT desde la estación del propio transmisor. La razón de atenuación a corsstalk (ACR) es la diferencia entre la pérdia crosstalk y la atenuación para el pat en enlace siendo probado. El ACR es una figura de mérito para el cable. En escencia, es una medición de cuanto "overhead" tu tienes entre el tamaño de la señal en el recptor, y el tamaño del ruido crosstalk. Así, cuando mas grande sea el ACR, es mejor. El ACR es especificado en los estándares ISO y el IEEE.

Notar por que el NEXT es diferente en cada terminal final, el ACR resultante sería también diferente en cada terminal. El peor caso de resultado ACR tiene que ser usado. Usando PSNEXT y atenuación, el "power sum ACR" (PSACR) puede ser calculado.

Capacitancia.- La capacitancia es la tendencia indeseable de un cable de almacenar energía eléctrica. Típicamente la capacitancia del cable es probado mientras aún esta en la bobina, pero la prueba de campo también puede darnos indicios de arrugas y estiramientos en el cable instalado.

Impedancia.- La impedancia es la oposición al cambio de corriente en un circuito eléctrico. Esto es frecuentemente dependiente, y puede ser alterado ó modificado siempre que una transición física ocurra, tales como en un "punch-down block", "patch pannel", ó dispositivos de conexión. El cable es medido por su impedancia característica (medido en ohms) y es garantizado por los fabricantes. No es típicamente medido en cables instalados.

Los cables deberían tener una impedancia igual al de los componentes eléctricos en la tarjeta de interface y otros circuitos para un tipo dado de LAN. Los cables con valores de impedancia diferentes no deberían ser interconectados por que la reflexión de la señal resultante puede causar una excesiva distorsión de la señal de datos.

Resistencia DC.- La resistencia a la corriente DC es la resistencia al flujo de corriente a través de un conductor. Este es medido en ohms, e incrementa con la longitud del cable, a diferencia de la impedancia el cual es consistente para un cable dado. El cable es probado y certificado para resistencias DC aceptable por el fabricante.

Continuidad y Polaridad.- El término continuidad y polaridad simplemente se refiere a correctamente conectar cada alambre individual en cada "punch-down block" y el conector, para proveer una conexión eléctrica continua. Por ejemplo, cada par de alambre en un cable UTP de cuatro pares tiene un par transmisor mas/menos y un par receptor mas/menos.

La desunión de los alambres individuales para que puedan ser invertidos ó no iguales a la correcta configuración de "pinout" en el conector, resultaría en una falla del "host". Las pruebas de continuidad y polaridad es un pre-requisito para las otras pruebas del cable de par trensado instalado.

Longitud del Cable.- Por que medimos la longitud?. Para la mayoría de conexiones UTP, la medición es realizada para que el retardo de la señal de propagación provista no exceda los requerimientos del sistema, la longitud actual es mucho menos importante que la atenuación y el NEXT del enlace. La longitud es la mejor medición para encontrar abiertos, cortocircuitos y roturas en el cable. Excesiva longitud del cable es mucho mas común en LAN coaxiales que en UTP, pero los principios de longitud son los mismos.

La longitud es mas comúnmente medido usando la técnica llamada Time Domain Reflectometer (TDR). El TDR puede ser pensado como un "cable radar". Típicamente, el cable tester genera un pulso hacia el alambre. Cuando el pulso encuentra un cambio en la impedancia, tales como un abierto, corto o conexión pobre, todas o parte de la energía del pulso es reflejado hacia atrás al tester. El tester mide el retardo entre cuando el pulso fue enviado y cuando la reflexión fue recibida. Conociendo la velocidad que el electrón viaja en el cable (Nominal Velocity of Propagation o NVP), el tester puede entonces calcular la distancia a la falla. El NVP es normalmente expresado como un porcentaje de la velocidad de la luz (C), tal como 0.82c.

El tamaño del pulso reflectado sería proporcional a la magnitud del cambio de la impedancia. Así, un gran cambio en la impedancia tal como un abierto o corto causaría una gran reflexión, y un menor cambio en la impedancia, tal como una conexión pobre, crearía una pequeña reflexión.

Las mediciones de longitud serían únicamente tan precisos de acuerdo a la configuración de NVP que se usa, el cual varía de 0.6c a 0.9 c para la mayoría de tipos de cable. Así, si el NVP de tu tester es configurado para 0.6c y el NVP de tu cable es de 0.9c, tus resultado podrían ser mas que 30% imprecisos. Para evitar estos errores en el campo, es buena idea buscar un tester con una amplia variedad de tipos de cables de propagación.

Es muy dificil alcanzaar una precisión mejor que el 2% usando un TDR, debido a que NVP tambien varía por hasta 4 – 6 % entre diferentes pares en el mismo cable. Mas, la longitud del cable trensado es siempre mas grande que la longitud de la cubierta lineal. Finalmente, por la longitud del cable, el pulso rectangular es algunas veces distorcionado dentro de un tramo de forma rugoso creada por el cable mismo. Va a depender de tu muestra de voltaje en el tope o en la parte inferior de este pulso retornado de forma irregular, que tu tiempo de retardo pueda variar por muchos nanosegundos, el cual luego correspondería a una diferencia de longitud de muchos metros en tu resultado.

Muchos tester de cables tiene una "zona muerta" de acerca de 6 metros donde ellos no pueden ver ninguna falla. Esto se debe a que el pulso incidente que ellos usan es cerca de 20 nanosegundoa (ns) de longitud, y dado que la señal viaja cerca de 3 ns/metros, esto significa que el pulso no ha dejado completamente el tester hasta cerca de 6 metros de longitud. Tales tester son incapaces de buscar una reflexión hasta que el pulso transmitido ha salido completamente. Dado que muchas fallas de cables son encontrados en los "patch", y otras cosas menos que en los 6 metros desde el punto de prueba, es necesario encontrar un TDR sin esta limitación.

Si estamos buscando fallas en cables trensados con un TDR, debemos estar bien seguros de conseguir uno que muestre la longitud de

todos los pares. Por que un par tiene 50 metros de longitud no significa que el otro par no esté abierto a 3 metros en el bloque de "puncheo".

Un TDR (Time Domain Reflectometer) es una herramienta poderosa para encontrar fallas en coaxiales o par trensado, y debería ser la primera línea de defensa para instaladores de cables o administradores de redes LANs contra problemas de cables.

Retardo.- El retardo ó retardo de propagación, es una medición del tiempo requerido por una señal para propagarse desde un terminal de un circuito a otro. El retardo de un par es directamente proporcional a su NVP. El retardo es usualmente medido en nanosegundos (ns). Típicamente los retardos para cable UTP Cat 5 es alrededor de 5.7 ns por metro. Los estándares internacionales dictan que el peor caso de retardo no excede 1 microsegundo para un enlace de 100 metros.

El retardo es la principal razón por que hay una limitación de impedancia en cables LAN. En algunas aplicaciones de networking, tales como un Ethernet Gigabit, la variación en el retardo entre diferentes pares del mismo cable puede ser un parámetro importante.

Retardo "Skew".- El retardo "Skew" de propagación es la diferencia entre el retardo de propagación del par mas rápido y el mas lento en un cable UTP. Debido a la insuficiencia de Teflon, el cual es algunas veces usado como un

material de aislamientoen cables de cat 5, algunos fabricantes de cable han substituido otro material en un dos de los cuatro pares. Tales cables híbridos, aunque ccompletamente cumplen con todos los parámetros de la cat 5, pueden exhibir alto skew.

El skew es importante por que muchas tecnologías de redes de velocidades altas, notablemente Gigabit Ethernet usa todos los cuatyro pares en el cable UTP. Si el retardo en uno o dos pares es significativamente diferente, entonces la señal el cual son todos enviados al mismo tiempo desde un terminal puede llegar en tiempos significantemente diferentes en el receptor. Mientras todos los receptores son diseñados para permitir alguna variación de luz en retardo, un gran skew haría esto imposible a recombinar la señal original.

El skew de peor caso para un enlace de 100 metros debería ser mentenida bajo 50 nanosegundos, pensando que 35 ns o menos es preferible.

Limitando Ruido y Crosstalk.- Hay dos formas mayores que el diseño de cable delas con limitando ruido y corsstalk:

- Shielding
- Cancellation

La protección es provisto por la envoltura del conductor principal con otra malla conductiva. Esto proteje al conductor de acero del EMI/RFI, y también ayuda a evitar de que el cable sea una antena y de ese modo producir EMI/RFI en otros cables ó equipos.

La cancelación del EMI/RFI es producida por el trensado de dos conductores alrededor de cada uno, en un patrón que causa que el campo magnético radiado en cada alambre cancele el campo en el otro. Los alambres paralelos no trensado pueden actuar como antena, radiando señales RF que pueden inducir ruido en otras líneas. El trensado también asegura que ambos alambres en el par sean igualmente influenciados por el EMI/RFI de otras fuentes. Esto ayuda al circuito receptor filtrar el ruido.

3.4.- CARACTERISTICAS DEL MEDIO DE COBRE

3.4.1.- Características del Cable Coaxial

El cable coaxial fue uno de los primeros tipos de cable usado en redes de datos y LANs. Este es usado con estándares de cableado 10Base-5 y 10 Base-2 por la IEEE 802.3

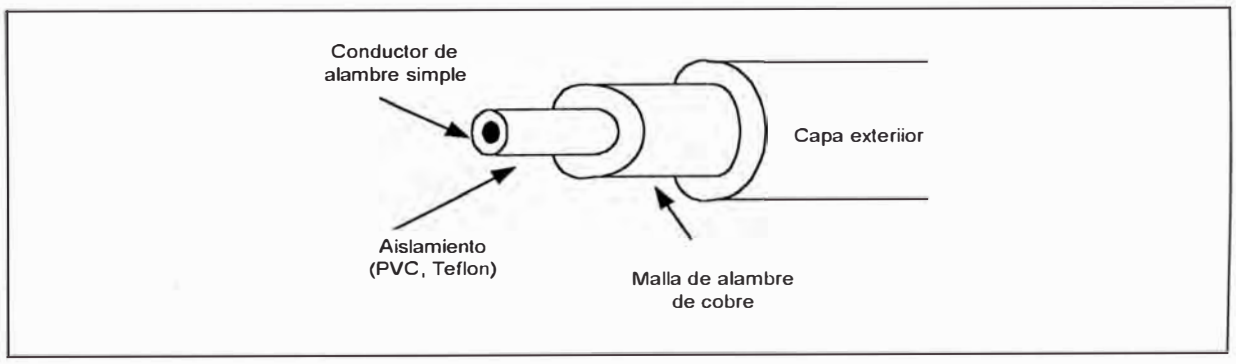


Figura 3-14 Extructura de un cable coaxial

El cable coaxial típicamente consiste de un cobre central o conductor de cobre envuelto por un aislante flexible, una cubierta de malla, y una chaqueta plástica exterior. La malla de alambre de cobre es el segundo conductor, y actua como una malla para disipar el EMI/RFI. En cables ethernet thick (10base-5), hay tambien dos capas de cubierta de aluminio y una malla apantallada de cobre adicional . El cable coaxial es algunas veces referenciado por el "radio government" (RG) standar. Ejemplos de cables coaxiales, sus estándares RG y características de impedancia son listado en la Tabla 3-3.

TIPO DE LAN	TIPO DE CABLE	IMPEDANCIA (Ohm)
10BASE-2 (thin Ethernet)	RG - 58	50
10BASE-5 (thick Ethernet)	RG - 8	50
10BROAD-36	RG - 6	75
ARCnet	RG - 62	93
IBM 3270 networks	RG - 62	93

Tabla 3-3 Tipos de cable Coaxial.

En general, el cable coaxial esta siendo tomado por instalaciones de cable de fibra óptica y par trensado. Aunque este tiene buena resistencia al EMI/RFI, es voluminoso y dificultoso de instalar a través de ductos y otros espacios dentro de un edificio

3.4.2.- Caracateristicas del Cable de Par Trensado

Los cables de par trensado consiste de dos o mas pares de alambres trensados de cobre aislado y delgados alrrededor de cada uno con

la finalidad de cancelar el EMI/RFI. El cable de par trensado viene en dos estándares: "Unshielded Twisted Pair" (UTP), y "Shielded Twisted Pair" (STP). Recientemente un nuevo tipo de par trensado ha sido ofrecido por algunos fabricantes: "Screened twisted pair" (ScTP)

Cables "Unshielded Twisted Pair" (UTP).- El UTP es el mas popular cable LAN. Es varato, ligero y fácil de instalar. Este viene en pares de alambres trensados en forma precisa, para minimizar el EMI/RFI, y no es cubierto por un conductor externo. El número de trensados va desde 2 a 12 por pie. Aunque el UTP es similar en apariencia a los cables telefónicos estándares, este tiene que encontrar el mas alto criterio con la finalidad de performar como cable de grado de datos. En particular, es importante evitar el uso de longitudes sin trensar de cable tipo telefónico.

En los años recientes, dos estándares de cinco niveles compatibles han sido establecidos para cables UTP por el EIA/TIA y el "Underwriter´s Laboratory" (UL). El sistema UL usa el término nivel y el EIA/TIA usa el término categoría. Otra difrencia es que el estándar UL incluye criterios de performance para cuidado contra fuego similar a los especificados por el "National Electric Code" (NEC). Las categorías EIA/TIA y los niveles UL son usados intercambiablemente.

- Categoría 1: Es usado para voz digital y análogo (teléfonos) y aplicaciones de datos de baja velocidad.

- Categoría 2: Es para voz, ISDN y datos de media velocidad hasta 4 Mbps. Este cable es equivalente al cable tipo 3 dee IBM.
- Categoría 3: Es para datos de alta velocidad y tráfico de LAN hasta 16 Mbps
- Categoría 4: Es para tráfico de LAN de gran distancia hasta 20 Mbps
- Categoría 5: Es para tecnologías LAN de 100 Mbps tales como Ethernet de 100 Mbps.
- Vategoría 6: Es para tecnologías Ethernet, Fast Ethernet , Gigabit Ethernet , ATM, señales de video y demás.

Ünicamente las categorías 3 y superiores son reomendados para instalaciones de red de datos. Muchos análisis recomendo la instalacion únicamente de cable categoría 5 para proveer eficiente capacidad de ancho de banda para futuras necesidades. El UTP categoría 3 tiene una impedancia caratcerística de 100 ohms.

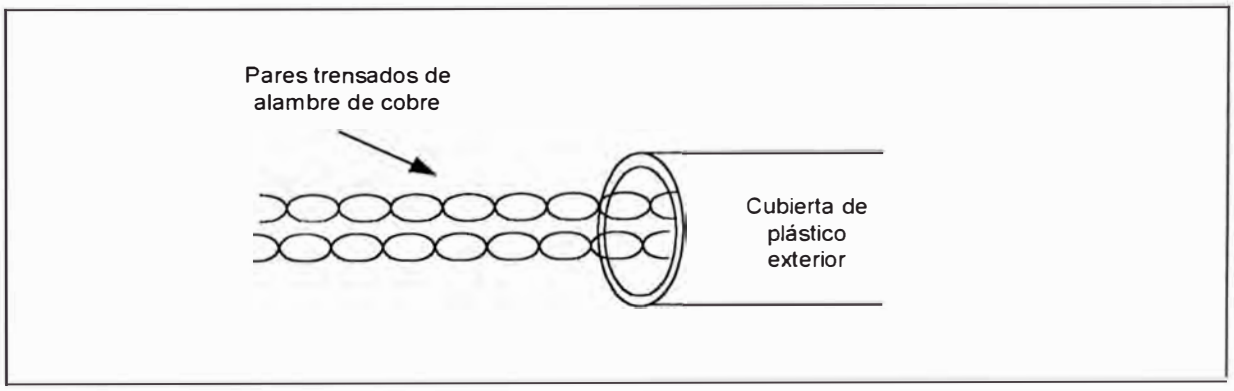


Figura 3-15 Cable de par trensado sin apantallar.

Hay que tener especial cuidado cuando se instala sistemas de cableado categoría 5. El cable no solamente tiene que encontrar sus especificaciones, sino también los conectores tienen que ser de alta calidad. Cuando un cable categoría 5 es conectado a un "block punch-down", no mas que la mitad de una pulgada del trensado tiene que ser deshilado. Hay que tener cuidado de no exceder el radio de curvatura de los cables, por el contrario ondularlo. Esto puede causar que no se alinien los pares trensados y nos guíe a transmitir errores.

"Cables Shielded Twisted Pair" (STP).- El alambrado "shielded twister pair" fue originalmente un cable especificado para redes "token ring". Dos o mas pares trensados de alambre de cobre son cubiertos por un aislante flexible, una cubierta de papel de aluminio, y una vaina de cubierta plástica. En algunos tipos de cables STP multialambrado, los pares trensados individualmente pueden ser envueltos por su propio papel de aluminio. La cubierta de aluminio ayuda a disipar la interferencia electromagnética, particularmente en velocidades mas altas de token ring de 16 Mbps.

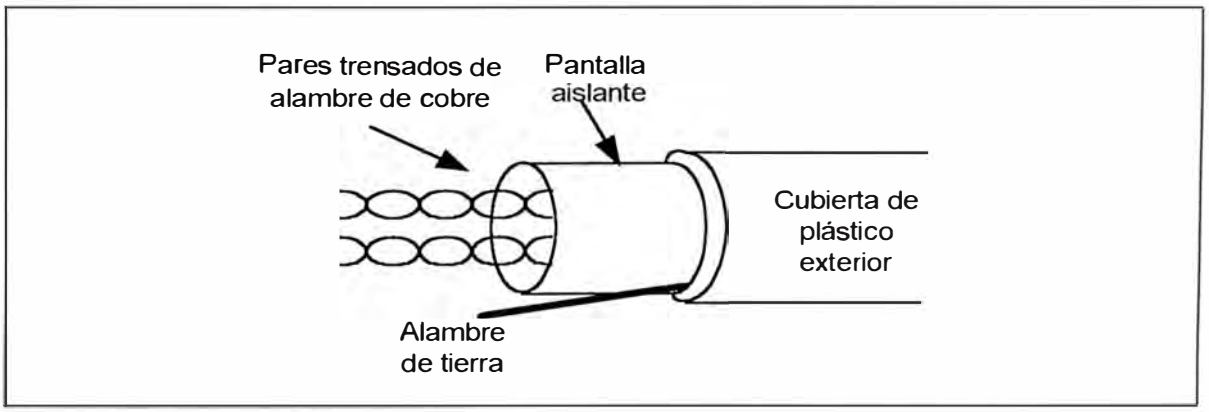


Figura 3-16 Cable par trensado apantallado.

El cable STP es también usado para instalaciones FDDI bajo la especificación de cableado TP_PMD. STP tiene una impedancia característica de 150 ohm. STP provee considerablemente mas resistencia a EMI/RFI que UTP, pero es también mas bulky, menos flexible, y mas caro ded instalar.

El sistema de cableado IBM especifica varios tipos de STP, fibra óptica, y cables UTP para uso en su plan e cableado estructurado. Los tipos de cable IBM son descritos líneas abajo. Notar que tipo 1 y 3 son los mas comunmente referenciados cuando hablamos de planes de cableado universal.

- Tipo 1 : Consiste de dos pares STP para transmision de data y es el estándar hitórico para cables token ring. Cada par es apantallado con un foil sheath y un pantalla exterior de plástico o metal corrugado. El cable tipo 1a es mas nuevo, dedel mismo tipo general y de mas alta performancia.
- Tipo 2 : Incluye seis pares de alambre, dos pares STP para data y cuatro pares UTP para voz. Este cable es usado donde las líneas de data y teléfonos terminan en un mismo wall outlet , o por facilita la instalación de cableado de líneas telefónicas y ded datos entre closet ded cableado.
- Tipo 3 : Consiste de cables UTP de grado telefónico. La especificación de cable tipo 3 original

- Fue intentado a ser compatible con cables de grado telefónico existente., el cual debería ser equivalente al cable UTP categoría 2 de la EIA/TIA, el cual fue recomendado únicamente para anillos de 4 Mbps. Actualmente IBM recomienda el uso de UTP de grado de data (equivalente a los categoría 3, 4 y 5 de EIA/TIA) para instalaciones de 4 y 16 Mbps, y únicamente categorías 4 y 5 son recomendados para nuevas instalaciones.
- Tipo 5 : Consiste ded dos cables ded fibra óptica de 100/140 µm. IBM actualmente recomienda fibras ópticas de 62.5/125 µm para instalaciones ded fibra óptica. El cable de fibra óptica es típicamente usado con un par de repetidores óptios para conectar MAUs en LANs token ring.
- Tipo 6 : Usa dos pares trensados para transmisión y es equivalente al tipo 1, pero mas flexible, El tipo 6 usado para conectar workstation a wall oulet y por patch cord entre el MAU token ring.
- Tipo 8 : Consiste de dos pares apantallados con un plástico plano alojado y es diseñado para usos under-carpet.
- Tipo 9 : Un cable tipo 1 mas delgado y de mas bajo costo. Este cable de tipo 9 soporta distancias dee transmisión mas corta que los cables de tipo 1.

Cables de Par Trensado Screened (ScTP).- Los pares trensados screened consiste de cuatro pares de cobre apantallado en una malla foil ded aluminio, con un chaqueta de PVC. La malla foil provee significante EMI/RFI

shielding y resulta en uncable que cae entre UTP y STP en términos de costo y performance, y difícilmente de instalar. ScTP también es conocido como Foil Twisted Pair (FTP) por algunos fabricantes. Los beneficios de ScTP sobre cables UTP categoría 5 son aún debatidos.

3.5.- CARACTERISTICAS DEL MEDIO DE FIBRA OPTICA

Los cables de Fibra Óptica tiene un número de beneficios como un medio LAN. Es capaz de soportar velocidades de datos de alta velocidad, teóricamente tan altas como 50 Gbps. Permite transmisión a gran distancia (típicamente de hasta 2 Km). Por que usa ondas de luz mejor quie cambios de voltaje a lo largo deel conductor, es inmune al EMI/RFI. Es un medio altamente seguro, por que es difícil emplamar dedntro de un cable dee fibra óptica sin ser detectados.

La primera desventaja dee los cables de fibnra óptica es su costo. Los cables de fibra óptica y equipos es relativamentee caro en terminos de materiales y la instalación.

La transmisión de fibra óptica puede ser usado virutalmente en todos los sistemas LAN, incluyendo Ethernet, token ring, y FDDI. Los detalles varían de protocolo estándar a protocolo estándar, pero la base es similar. Esta sección describe algunos de los componentes típicos de los sistemas de fibra óptica y las características de la transmisión de fibra óptica.

3.5.1.- Sistema de Comunicación por Fibra Optica

El modelo básico para un sistema de comunicación inluye un transmisor, un receptor, y un cableado que los conecta. La figura 3-17 nos muestra un sistema de comunicación genérica de fibra óptica.

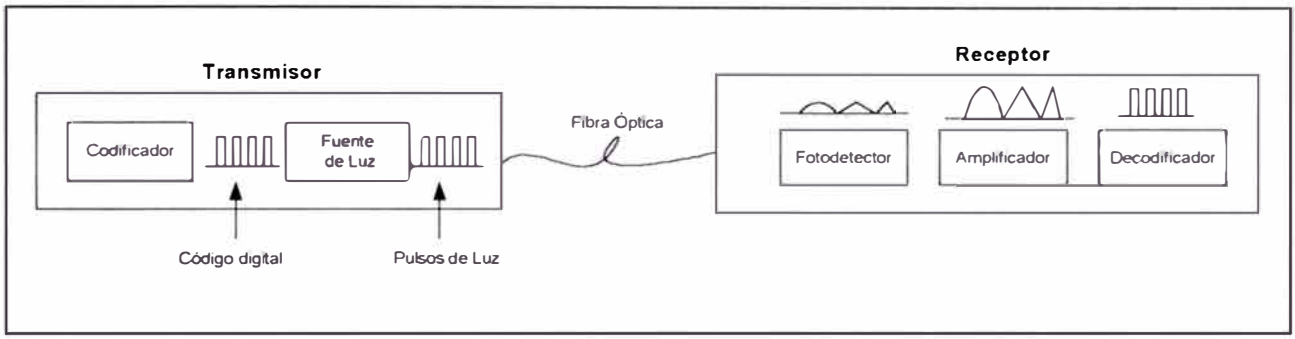


Figura 3-17 Sistema de comunicación por Fibra Óptica.

En un sistema de fibra óptica, cada dispositivo tendría un transmisor y un receptor, o transeivers.

Los componentes del transmisor incluyen lo siguientes:

- Un codificador que convierte la intrada dentro de pulsos eléctricos digitales (señal)
- Una fuente de luz que modula la señal.
- Un conector que acopla la fuente de luz a la fibra a través del cual viajan los rayos de luz.

El transmisor acepta señales léctricas que luego lo codifica. En un sistema de red de computadoras, el código es digital. La fuente de luz

modula el código digital dentro de pulsos de luz que son enviados al receptor a través de la fibra óptica.

Hay dos tipos básicos de fuentes de luz para sistemas de fibra óptica:

- Light emitting diode (LED)
- Laser diode

La fuente de luz LED son de mas baja potencia y considerablemente menos caro que el laser. El LED puede ser usado con cables multimodo, y son la fuente de luz mas común. Ellos proveen un ancho de banda de aproximadamente 250 MHz.

La luz láser es usado con fibra monomodo para transmisión a gran distancia. La luz láser es mas poderosa y coherente, con los rayos de luz radiados en paralelo, causa menos atenuación y dispersión. Los diodos láser pueden proveer ancho de banda mucho mas alto (hasta un maximo teórico de 10 Gigahertz)

La fibra óptica es usualmente elegido por la habilidad de transmitir mensajes a grandes distancias sin un repetidor. Los conectores acoplan la fibra al transmisor y al receptor.

Un receptor convierte los pulsos de luz modulados en señales eléctricas y los codifica. El receptor, contenido dentro de la computadora de destino, incluye:

- Un fotodetector, que convierte los pulsos de luz en señales eléctricas.
- Un amplificador si necesitado
- Un decodificador de mensaje

3.5.2.- El Cable de Fibra Óptica

El cable de fibra óptica consiste de tres partes:

- Core : El conductor central para la luz. El diámetro y consistencia del core varía dependiendo de las especificaciones de la fibra óptica. Un core con consistencia uniforme es conocido como fibra de step-index. Un core con una variación consistente es conocido como fibra de graded-index.
- Cladding : Diseñado para reflejar la luz hacia el core, therby minimizando la pérdida de la señal.
- Cubierta Protectora : Provee de una chaqueta para shield la fibra ded daños posibles

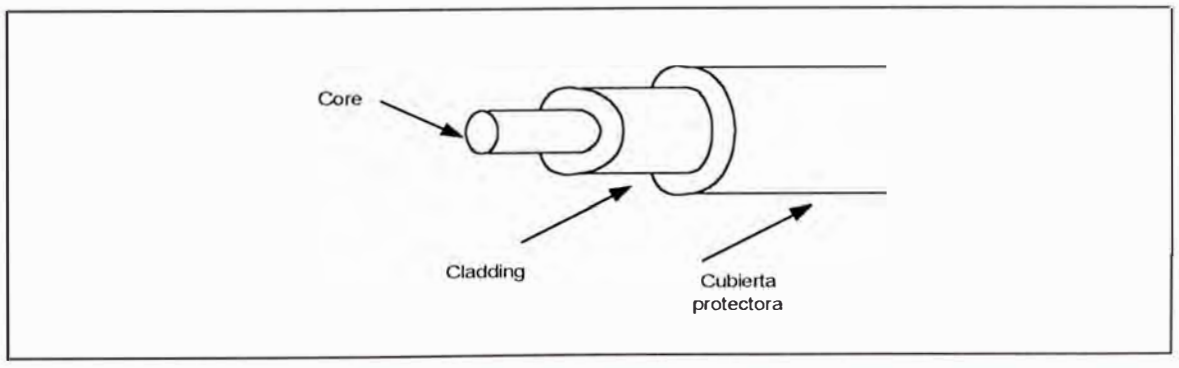


Figura 3-18 El cable de Fibra Óptica.

Cada core de la fibra óptica conduce luz en una dirección únicamente, por lo que envía o recibe pulsos de luz. Los dispositivos son usualmente conectados por dos hilos de fibra óptica. Los cables dúplex son mas comúnmente usados que los cables simplex.

Los hilos de fibra óptica pueden consistir de varios paquetes, usados en "backbones" de alta capacidad para conexiones exteriores entre edificios campus.

Los cables de fibra óptica son muy delgadas. El diámetro del core de fibra y cladding son específicamente micrones (la milésima parte de un metro). El cable de fibra óptica mas delagado (monomodo) tiene un diámetro de core de 5 – 10 µm. El cable de fibra óptica es un poco mas grueso (multimodo) va de 50 – 100 µm de diámetro de core. El diámetro de core es también conocido como la apertura, por que este determina el máximo ángulo desde el cual el cable puede aceptar luz. El cable de fibra óptica es algunas veces listado en términos del diámetro de su core y cladding. Por ejemplo, el tipo de cable mas común de fibra óptica es el cable 62.5/125 µm, donde 62.5 se refiere al diámetro del core y 125 al diámetro del cladding.

Tipos de cable de Fibra Optica.- Los cables de fibra óptica vienen en dos tipos generales:

- Fibra óptica multimodo : Cada rayo de luz pasa a través de un cable llamdo un modo. El cable dee fibra óptica multimodo es mas amplio que el monomodo, y debido a este medio un poco amplio, permite suficicente espacio para mas que un rayo de luz pase a través del cable. Estos rayos tendrían diferentes angulos de incidencia y reflexión como ellos son reflejados dedl cadding. La figura 3-22,uestra una fibra óptica multimodo cono varios rayos de luz incidiendo en el core.

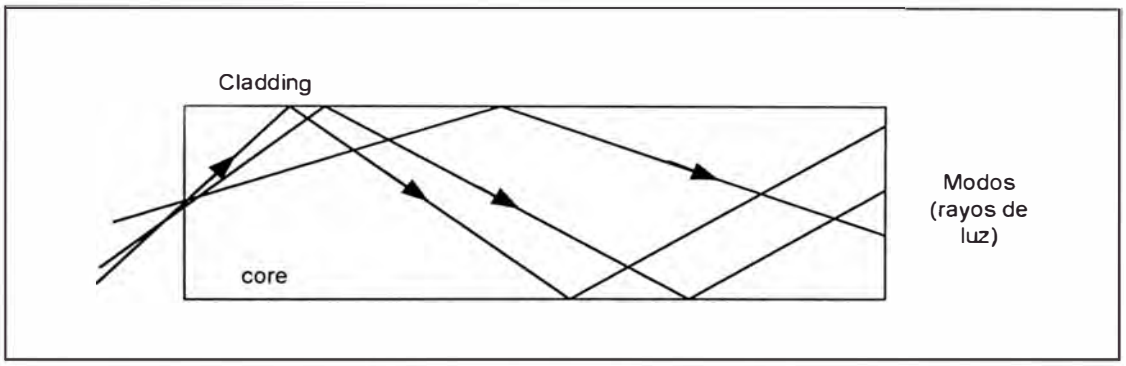


Figura 3-19 El cable de Fibra Óptica Multimodo.

Cuando usamos señalización multimodo, no todos los rayos de luz viajan a la misma distancia. Algunos rayos de luz viajarían straight a través del core mientras otros continuamente bounce off el cladding antes de alcanzaar el final de la fibra. Con modos viajando a diferentes distancias, pero a la misma velocidad, el spread de la señal incrementa el tiempo, y pueded causar errores de data debido a sobreposición de los pulsos de luz. Este problema es conocido como dispersión. La construcción de la fibra multimodo tiene un efecto significativos en este problema. Hay dos tipos de fibra multimodo:

1. Step-index: Es el cable ded fibra que consiste de únicamente dos materiales transparentes, el core y el cladding. La fibra ded step-index no compensa la dispersión de la señal.
2. Grades-index: Especifica un cladding de fibnra que tiene muchas capas transparentes. Esta inconsistencia planeada causa que los múltiples rayos de luz alcancen el final ded la fibra de un modo uniforme.

La fibra de graded-index permite que la luz viaje a diferentes velocidades a través del "core." La velocidad al cual el modo viaja depende sobre que parte del core esté viajando. Los modos viajando mas abajo del centro del core tiene mas baja velocidad que los que viajan refractados del caldding. Así todos los modos alcanzan el final de la fibra uniformemente. La fibra mas comunmente usado es el 62.57125 µm multimodo de graded-index.

- Fibra óptica monomodo.- La fibra monomodo tiene un diámetro entallado a la longitud de onda que ellos son diseñados para llevar, el diámetro de core que una fibra monomodo típica tiene es de 8 µm. Unicamente un modo se propagaría a través de la fibra con este diámetro de core, si la longitud de onda especificado (por ejemplo 1.3 µm) es enviado a través de la fibra óptica. Debido a que la fuente de luz monomodo es más coherente que la multimodo, el cable de fibra óptica monomodo puede soportar transmisiones a grandes distancias

mas que la fibra multimodo. La fibra monomodo es también mas estrecho, el cual hace que se ignore la dificultad y lo caro que es instalarlo correctamente.

Las fibras monomodo son generalmente fibras de step-index, ya que únicamente un modo viaja a lo largo de la fibra. El problema de difusión "spreading" dentro de otro no ocurre en fibras monomodo. La fibra monomodo mostrado en la figura 3-20, nos muestra una fibra de step-index consistiendo de un core y un cladding.

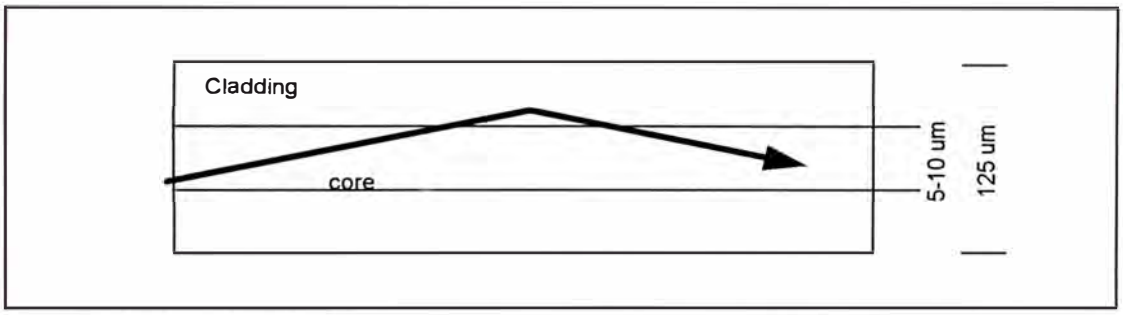


Figura 3-20 El cable de Fibra Óptica Monomodo.

Power Budget.- La luz emitida desde un transmisor se atenua a medida que viaja por el sistema de comunicación. Cuando eligimos los componentes del sistema, el diseñador tiene que ser capaz de determinar el nivel de potencia en diferentes puntos del enlace, para asegurar que una potencia optica suficiente llegue al recepetor desde el transmisor.

Los factores que causan la pérdida de potencia son predicibles. La herramienta para rastrear los niveles de potencia en un punto de un enlace de comunicación es un power budget. Un power budget nos muestra pérdidas conocidas o típicas en puntos del enlace de comunicación. Estas

fuentes de pérdida incluyen todas las conexiones a lo largo del enlace y la atenuación en la fibra por sí misma. En un lugar ded instalación dada, los diseñadores pueden determinar si la fibra puede ser empalmada o si tiene que ser una longitud continua.

Las fuentes de pérdida de potencia incluyen:

- Pérdida de la fibra
- Conexión del transmisor a la fibra
- Conexión de la fibra la receptor
- Conectores en hubs o bloques de distribución.
- Empalmes

Como un pulso deluz viaja a lo largo de un cable de fibra óptica normal, su amplitud es disminuida, resultando en una atenuación, o pérdida dee potencia. Las fuentes dee pérdida de potencia incluyen el scattering de los rayos de luz ya que ellos “bump” dentro de la estructura molecular del vidrio del cable. Este proceso es conocido como Rayleigh scattering, y es nombrado así por los científicos como el primero que demostró el fenómeno. Otras pérdidas en la fibra son debidas a la absorción de los rayos ed luz dentro de otras en ciertas frecuencias. Esta pérdida es conocida como infrared-absortion.

Una manera de usar un power budget es plot out la pérdidas para determinar si la potencia óptica del transmisor estaría arriba del nivel de

potencia mínima requerido en el receptor una vez que todas las pérdidas son plotted.

La potencia óptica es medida en decibelios metros (dBm). Este es algunas veces diferente ded un decibelio, el cual es una medición relativa ed potencia en un punto relativo a otro. La pérdida de potencia normal para tipos dee conexiones debería ser listado en decibelios, indicando la pérdida de potencia en ese punto. La potencia absoluta ded la señal debería ser listado en dBm o –dBm en cualquier punto dado. La figura 3-21 muestra el power budget para una instalación FDDI.

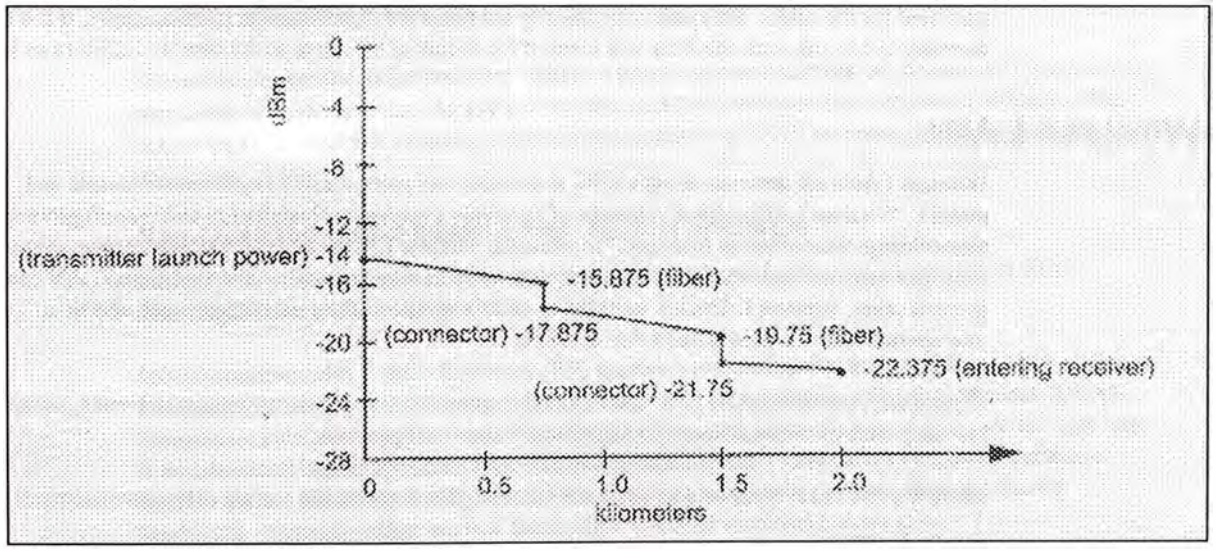


Figura 3-21 Grafica de una medición de un cable de Fibra Óptica.

El receptor está a dos kilómetros del transmisor. El receptor requiere que el nivel de potencia que es no menor de –25 dBm y el requerimeinto de FDDI especifica la pérdida en dB entre estaciones que no puede exceder –11 dBm. El plan llama por dos conectores, uno a 0.75 Km y

otro a 1.5 km. Los siguientes son conocidos como niveles de potencia y pérdida:

- Potencia en el transmisor : -14 dBm
- Fibra : 2.5 dB por Km
- Conectores : 2 dB en cada conector.

Los niveles de potencia en el receptor tienen que ser no menor que –31 dBm. El "power budget" muestra que habría un adecuado nivel de potencia en el receptor. (-22.375 dBm)

El "power budget" es muy usual y necesario para calcular la performance de los sistemas de fibra. Sin embargo, una instalación descuidada puede causar pérdidas de potencia que exceden el normal "power budget". Particularmente vulnerables son los empalmes y conexiones de cable de fibra óptica.

Instalación del cable de Fibra Optica.- Los cables de fibra óptica son difíciles de instalar correctamente, y además requiere de técnicos de instalación cuidadosos y bien entrenados. Así, combinado con el natural consumo de tiempo de cada conexión, hace que los cables de fibra óptica sean los mas caros de instalar. Las conexiones y empalmes de los cables de fibra óptica son particularmente difíciles de hacer. Cada terminal del cable tiene que ser cortado en un ángulo perfecto, pulido de manera manual o por máquina, y el

cable precísamente alineado al conector. En algunos sistemas , el cable es expuesto al conector, en otros la conexión es "crimpeada".

Los instaladores tienen que tener cuidado para no doblar el cable de fibra óptica mas que el radio de curvatura mínimo especificado por el fabricante. Este radio es típicamente 10 veces el diámetro de la fibra. Por ejemplo, si el diámetro de la fibra es 125 µm, la fibra se quebraría si el radio de la curva es 1.25 µm o menos.

Mediciones de Fibra Optica.- En pruebas de LAN con fibra óptica, hay dos principales clases de instrumentos de prueba: "Optical Loss Test Sets" y los OTDRs. El "Optical Loss Test Set" incluye fuente óptica y medidores de potencia. Ellos son usados para medir la pérdida "end-to-end" a través de un enlace de fibra. Ellos son también usados para medir la fuerza de la potencia transmitida, la potencia de la señal recibida, o la pérdida del enlace. El "Optical Loss Test Set" es relativamente no muy costoso y es el más usado por los instaladores de fibra óptica.

El "Optical Time Domain Reflectometer" u OTDR, es un instrumento mucho mas sofisticado, el cual es capaz de ubicar cortes en la fibra, identifica conexiones pobres, y mide la longitud total de la fibra. Es comunmente usado en el mundo de las fibras monomodo, donde estas son típicamente mucho mas largas e incluyen muchas mas conexiones en el enlace. Los OTDRs pueden tambien ser usados para medir pérdidas end-to-

end. Ellos son raramente usados en fibras multimodo excepto para medir la longitud, por que las fibras cortas tienen menos conexiones y son fácil de diagnosticar.

Una alternativa para los OTDR es el Fault Finder. Estos son escencialmente pequeñas versiones de OTDR con funcionalidad reducida, velocidad, precisión y precio. El principal propósito de un Fault Finder es encontrar la ubicación exacta de una falla.

Una nueva clasificación de herramientas de fibra óptica es la Herramienta de Certificación. Un certificador de fibra es una herramienta que automátiza el proceso de prueba y compara resultados a un estándar predefinido. Por ejemplo los certificadores tienen una función autotest que lleva a cabo los test siguientes: Medición bidireccional de pérdida de potencia en ambas ventanas 850 y 1300 nm en dos fibras, mide la lobgitud y el retardo de propagación del enlace, luego compara todos estos resultados con los estándares de la industria tales como TIA 568ª, IS1 1801, FDDI, 10 BaseF, Fiber Channel, y otros. El operador luego consigue un PASS/FAIL apara el enlace.

Las mediciones de fibra típicas incluyen atenuación y longitud. Un importante requerimiento cuando prueban cables de fibra es saber el budget deel enlace optico, o OLB. El OLB es la pérdida máximo permitible

para el circuito o aplicación. Esto te permite saber si o no tus aplicaciones correrían o si la instalación ha sido apropiadamente instalado.

Como un ejemplo considere 88 metros de fibra multimodo a ser probado a 850 nm. Que es el OLB, o en otras palabras, como sabemos que es bueno.

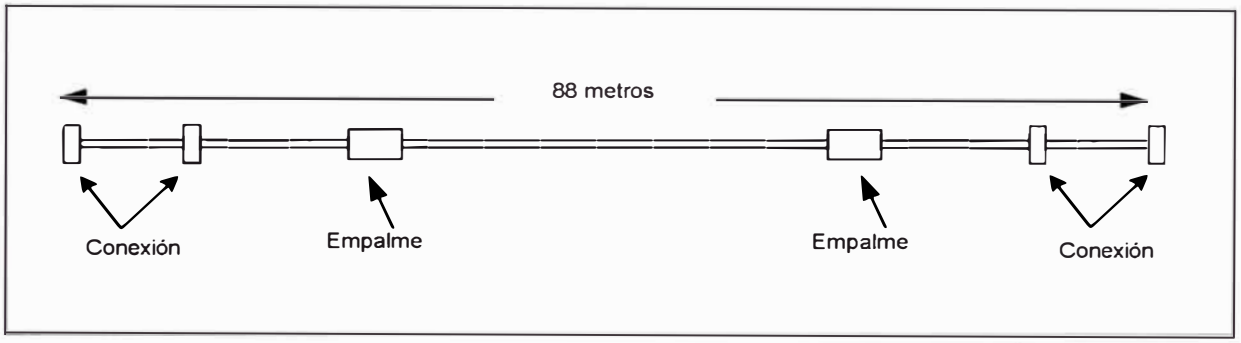


Figura 3-22 Enlace de una Fibra Óptica típica.

El TIA 568A permite: 0.75 dB por conexión, +0.3 dB por empalme, +3.75 dB por Km a 850 nm. En este ejemplo nosotros tenemos:

1. 04 conexiones a 0.75 = 3 dB
2. 01 empalme a 0.3 dB = 0.3 dB
3. 0.088 km x 3.75 dB / km = 0.33 dB

El Optical Link Budget = 3 + 0.3 + 0.33 = 3.63 dB a 850 nm

La mayoría de instaladiores no hacen esto para cada enlace y cada longitud de onda. El probelma es que no saben cuando PASS esto. Esto es un problema real. Un instaladoir en el campo quien prueba dos

fibras, y encuentra que ambos fueron 6.2 dB, deebería probablemente asumir que ambos fueron OK. Si uno tiene únicamente dos conexiones mated, sin empalmes, y es corto, mientras que el otro tiene 4 mated conexiones y es largo, "6.2 dB" representa un PASS para el primero y FAIL para el segundo. Estos es la razón importante para que tu probador de campo automáticamente calcule el OLB para ti cuando pruebas cables ded fibra .

3.6.- ESTANDARES DE CABLEADO ESTRUCTURADO

Diferentes estándares de organizaciones influyen en el cableado de data, Los mas importantes se muestran en la tabla 3.3

ORGANIZACIÓN	SUBCOMITE ESPECÍFICO	AREA DE INFLUENCIA
EIA/TIA	TR41.8.1	Norte América
CENELEC	TC 215 WG1	Europa
ISO/IEC	ISO/IEC JTC1 SC25 WG3	Mundo entero
IEEE	802.3x	Mundo entero
ATM Forum	PHY	Mundo entero

Tabla 3-4 Estándares de cableado estructurado.

Adicionalmente hay asociaciones de industrias de profesionales de cableado que tiene creciente influencia en la insdustria. El mas grande de estos es BICSI (Building Industry Consulting Service International) con base en Tampa Florida. A continuación examinaremos los estándares de cableado publicados.

ESTÁNDAR	DESCRIPCIÓN	AREA DE INFLUENCIA
TIA TSB - 67	Especifica los requerimientos de pruebas de campoi para los cables UTP instalados.	Norte América
TIA 568 A	Estándar de Telecomunicaciones para edificios comerciales.	Norte América
ISO/IEC IS11801	Cableado Genérico para premisas del cliente.	Mundo entero
CENELEC EN 50173	Cableado de premisas del cliente para tecnología de la Información.	Europa

Tabla 3-5 Estándares de cableado estructurado publicados.

Estos estándares definen y especifican la performence de los enlaces cableados hasta 100 MHz. Los estándares de performancia de TIA son especificados como Categorías. Las especificaciones internacionales usan la designación de Categoría para componentes y cables, pero usa el término Clase para performancia del enlace. El protocolo de nombramiento de enlace y al ancho de banda del cableado actual y propuesto es mostrado en la tabla 3-6. y 3-7

ESTANDAR	TIA	ISO/IEC	CENELEC
Conectores	Categoría	Categoría	Categoría
Cables	Categoría	Categoría	Categoría
Enlace	Categoría	Clase	Clase

Tabla 3-6 Protocolo de nombramiento al enlace.

ESTANDAR	TIA	ISO/IEC	CENELEC
Enlace 16 MHz	Categoría 3	Clase C	Clase C
Enlace 100 MHz	Categoría 5	Clase D	Clase D
Enlace 200 MHz	Categoría 6	Clase E	Clase E
Enlace 600 MHz	Categoría 7	Clase F	Clase F

Tabla 3-7 Ancho de Banda del cableado, Categorías y Clses.

CAPÍTULO IV

LAN SWITCHING

4.1.- TECNOLOGIA SWITCHING (BRIDGING)

4.1.1.- Switching Transparente

Los switches proveen mas ancho de banda reduciendo el número de dispositivos contenidos en cada segmento y controlando el flujo de data en la red. Los switches envían tráfico únicamente a la interface que necesita recibir el tráfico, es decir a un único puerto mejor que enviarlo a todos los demás puertos. Switching transparente fue definido en los documentos IEEE 802.1d, que describe cinco procesos para dedterminar que hacer con una trama. Estos procesos son como sigue:

- Learning o Aprendizaje
- Flooding o envío múltiple
- Filtering ó no envío de tramas
- Forwarding ó envío de tramas
- Aging ó

La figura 4-1 mostrada a continuación muestra los cinco procesos que se dan en un switching transparente:

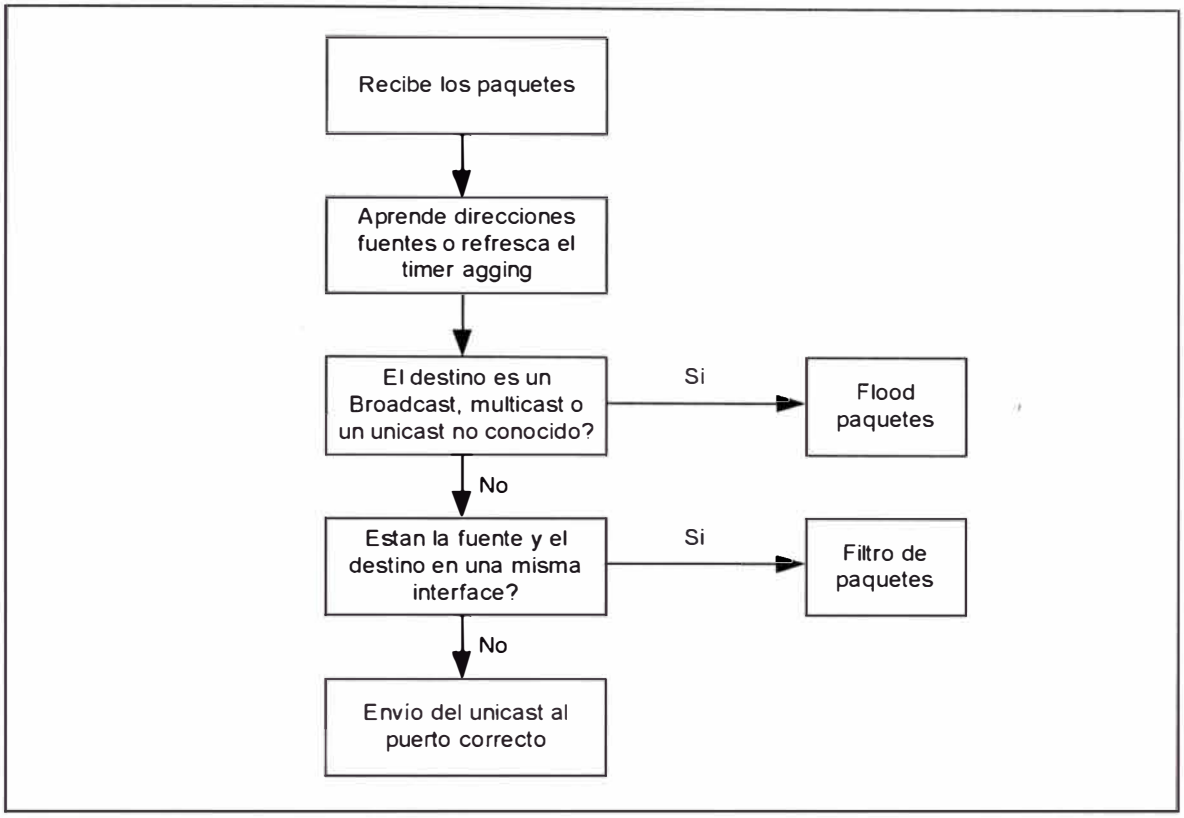


Figura 4-1 Diagrama de flujo de un Bridge transparente.

Cuando una trama ingresa a un switch transparente, el switch agrega la dirección MAC fuente (SA) y el puerto fuente a su tabla de switching. Si la dirección fuente ya existe en la tabla, el switch actualiza el timer agging. El switch examina la dirección MAC de destino (DA). Si el DA es un broadcast, multicast o un unicast conocido, el swtich floods la trama a todos puertos del switch en el estado de Sanning Tree Forwarding , a excepción del puerto fuente. Si la dirección de destino y fuente están en la misma interface, el switch descarta (filtra) la trama. De otra manera el switch envía la trama a la interface donde el destino es conocido en su tabla de switching.

A continuación explicaremos en detalle cada uno de los cinco procesos, para lo cual mostramos la figura 4-2.

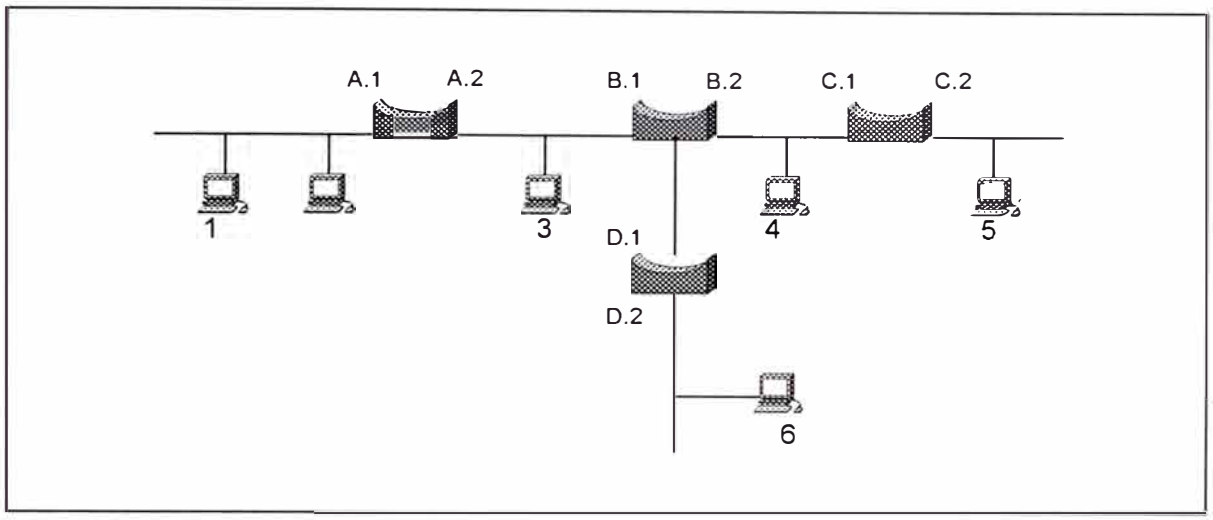


Figura 4-2 Ejemplo de una Red Bridged.

Learning.- Cada switch tiene una tabla que graba todas las estaciones que son conocidas por cada una de sus interfaces. Especialmente el switch graba la dirección MAC fuente y el puerto fuenteen la tabla cuando un switch ve una trama proveniente de un dispositivo. Este es el proceso de Learning del switch, donde únicamente aprenden de la dirección fuente unicast. Una estación nunca genera una trama con una dirección fuente multicast o broadcast. Los switch aprenden la dirección MAC con la finalidad de enviar data inteligentemente al segmento destino apropiado. Cuando el switch recibe una trama, este se soporta de su switching table para dedterminar en que puerto existe la dirección MAC de destino. El switch usa la información en la tabla para filtrar el tráfico (si la fuente y el destino están en una misma interface) o enviar la trama a la interface o las interfaces apropiadas.

Cuando el switch es prendido, su tabla no contiene ni una data, por lo que asume que todos los switches de la figura 4-2 fueron prendidos recientemente y ninguna estación a transmitido aún. Además las tablas en los cuatro switches de la figura están vacías.. Ahora asume que la estación 1 transmite una trama unicast a la estación 2. Todas las estaciones en ese segmento, incluyendo el swtich recibe la trama por la naturaleza del medio compartido. El switch A aprende que la estación 1 existe a través del puerto A1 observando la dirección fuente en la cabecera de la trama de enlace de datos. El switch A ingresa en su tabla la dirección MAC fuente y el puerto del switch.

Flooding.- Continuando con la figura del ejemplo, cuando la estación 1 transmite, el switch A también observa la dirección de destino de la cabecera de enlace de datos, para ver si tiene una entrada en la tabla. En este punto, el switch A únicamente conoce la estación 1. Cuando el switch recibe una trama unicast no existe entradas en la tabla para este DA. El switch recibe una trama unicast no conocida. La regla del switch manifiesta que tiene que enviar un trama unicast no conocida a todos los puertos o interfaces a excepción de la interface fuente. Esto es conocido como Flooding. Adedmás el switch A flood la trama a todas las interfaces a pesar de que la estación 1 y 2 estén en un mismo segmento. El switch B recibe la trama y ejecuta los mismos procesos de learning y flooding que el switch A . El switch B flood la trama al switch C y D y ellos también ejecutan el proceso de learning y flooding. Ahora la tabla de switching se observa como la tabla

4-1. Los demás switches no conocen de la estación 2 por que este no ha transmitido aún.

PUERTO DEL BRIDGE	A.1	A.2	B.1	B.2	B.3	C.1	C.2	D.1
Dirección MAC	1		1			1		1

Tabla 4-1 Tabla de un bridge después del flooding.

Aún considerando la figura de ejemplo, todos los switches en la red tienen una entrada para la estación 1 asociado con una interface, apuntando hacia la estación 1. La tabla del switch indica la ubicación relativa de una estación con respecto a un puerto. Examinando la tabla del switch C, una entrada para la estación 1 es asociada con el puerto C1. Esto no significa que la estación 1 esté conectada directamente al puerto C1, sino que refleja que el switch C escucha a la estación 1 a través de este puerto. Adicionalmente a flod tramas unicast no conocidas, los switch también flood dos tipos de tramas: Unicast y Broadcast. .

Filtering.- Que pasa cuando la estación 2 responde a la estación 1?. Todas las estaciones en el segmento de puerto A1 incluyendo el switch A recibe la trama.El switch A aprende acerca de la presencia de la estación 2 y lo adiciona su dirección MAC a la tabla del switch conjuntamente con el puerto identificador (A1). El switch A también observa la dirección MAC de destino, para determinar donded enviar la trama. El switch A conoce que la estación 1 y 2 existen en el mismo puerto. Esto concluye que no es necesario enviar

la trama a otro lugar. Además el switch A filtra la trama, lo cual ocurre cuando la fuente y destino residen en la misma interface. El switch A podría enviar la trama a todas las otras interfaces, pero esto gastaría el ancho de banda en los otros segmentos, el algoritmo bridging especifica que se debe descartar la trama. Hay que notar que únicamente el switch A sabe de la existencia de la estación 2 por que ninguna trama de esa sección ha cruzado el switch.

Forwarding.- En la figura del jemplo, la estación 2 envía una trama a la estación 6, los switches floods la trama por que no existe entrada para la estación 6. Todos los switch aprenden la dirección MAC fuente de la estación 2 y la ubicación relativa. Cuando la estación 6 responde a la estación 2, el switch D examina su tabla de switching y ve que para alcanzar a la estación 2 tiene que enviarla por el puerto D1. Un switch envía la trama cuando la dirección de destino es un unicast conocido (es decir si tiene una entrada en su tabla) y la dirección fuente y destino están en diferentes interfaces. La trama alcanza el switch B, el cual lo envía a la interface B1. El switch B recibe la trama y lo envía hacia A1. únicamente los switches A, B y D aprende acerca de la estación 6. La tabla 4-2, nos muestra la tabla de "switching" actual.

PUERTO DEL BRIDGE	A.1	A.2	B.1	B.2	B.3	C.1	C.2	D.1	D.2
Dirección MAC	1		1			1		1	
	2		2*			2*		2*	
		6			6				6

* B.1, C.1 y D.1 no aprendió acerca de la estación 2 hasta que la estación 2 transmitió a la estación 6

Tabla 4-2 Tabla de un bridge después del fordwarding.

"Aging".- Cuando un switch "aprende" una dirección fuente, este identifica la entrada. Cada vez que el switch ve una trama de esa fuente, el switch mantiene la entrada activa. Si el switch no escucha nada acerca de la fuente antes de que el "timer aging" expire, el switch retira la entrada de su tabla.

Los switches tienen una cantidad finita de memoria, limitando el número de direcciones que puedan grabar en su tabla de "switching". Por ejemplo, el switch con mas capacidad puede recordar hasta 16000 direcciones, mientras algunas unidades de mas baja capacidad puede recordar hasta 4096. Si un switch se encuentra lleno con sus 16000 entradas y una estación 16001 quiere transmitir, el switch envía a sus demás puertos (flooding) todas las tramas provenientes de esa estación hasta que exista un espacio en la tabla que permita al switch "aprender" acerca de la estación. Las entradas van a estar disponibles mientras el "timer aging" no expire para esa dirección. El "aging" ayuda a limitar el "flooding" debido a almacenamiento de las direcciones de las estaciones activas en la red.

Los switches también usan el aging para permitir el movimiento de las estaciones., En la tabla 4-3 los switches saben la ubicación de la estación 1, 2 y 6. Si la estación 6 se mueve a otra ubicación , los dispositivos no serían capaz de alcanzazr a la estación 6. Por ejemplo si la estación 6 se reubica en C2 y la estación 1 transmite una trama a la estación 6, la trama nunca alcanzaría a la estación 6. El switch A enviaría la trama al switch B, pero el switch B aún piensa que la estación 6 esta ubicado en le puerto B3. El aging permite que los switches "olviden" la entrada de la estación 6. Después que el switch B olvida la entrada estación 6, este flood las tramas destinadas a la estación 6 hasta que el switch B aprensa su nueva ubicación. Por otro lado si la estación 6 inicia la transmisión a la estación 1, los switches inmediatamente aprenden la nueva ubicación de la estación 6.

4.1.2.- Modos de Switching

Los switches hacen decisiones de forwarding de la misma manera que los bridges, debido a que un switch es considerado como un múltiple bridge. Actualmente existe tres modos particulares de forwarding en la industria y son: store-and-forward, cut-through y fragment-free. La figura 4-3 nos indica los puntos característicos para los tres métodos.

Cada uno tiene sus ventajas y desventajas que serán detalladas a continuación. Como resultado de los puntos característicos dstintos, la diferencia efectiva entre estos modos son el manipuleo del error y la latencia.

La tabla 4-3 resume como cada modelo manipula la trama conteniendo errores y la latencia característica asociada.

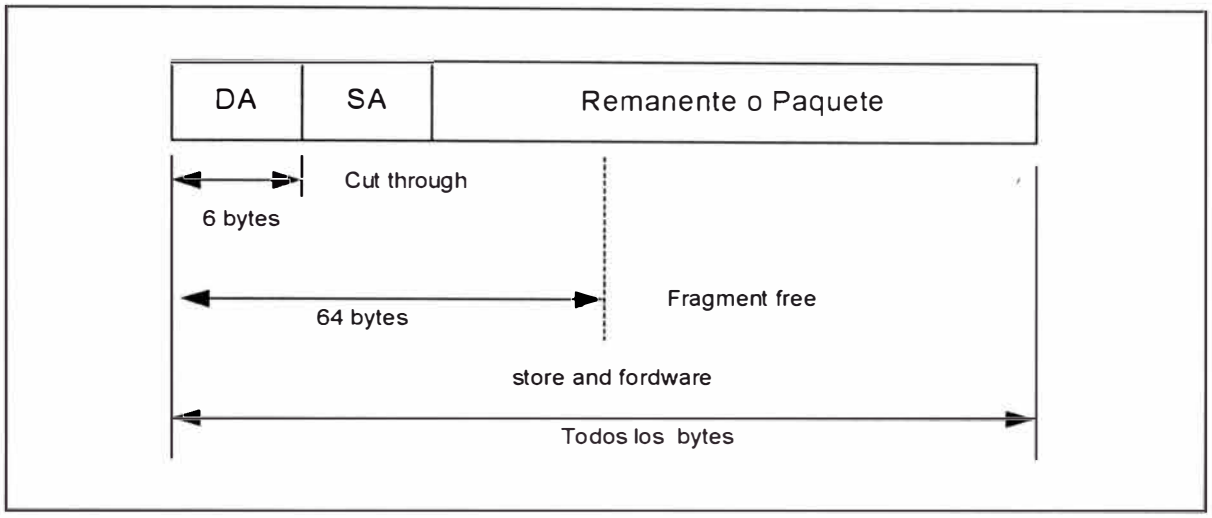


Figura 4-3 Ejemplo de una Red Bridged.

MODO DE SWITCHING	MANIPULANDO TRAMAS ERRADAS	LATENCIA
Store and Forward	Drop	Variable
Cut - Through	Forwards	Bajo-fijado
Fragment Free	Drops si hay errores detectados en los primeros 64 octetos	Moderado-fijado

Tabla 4-3 Modo de comparación de los switches.

Uno de los objetivos del switching es proveer mas ancho de banda a los usuarios. Cada puerto en el switch define un nuevo dominio de colisión y ofrece un ancho de banda completo. Si una estación está adjunto al puerto del switch, esa estación tienen el ancho de banda dedicado y no necesita compartirlo con otro dispositivo. Todos los modos de switching soportan la característica de ancho de banda dedicado.

Store-and-Forward Switching.- El modo de switching store-and-forward recibe la trama entera antes de comenzar el proceso de switching. Cuando recibe la trama completa, el switch examina la trama buscando la dirección fuente y destino y cualquier error que pueda contener, y luego se aplique cualquier filtro especial que se haya creado por el administrador de la red para modificar el comportamiento de forwarding por defecto. Si el switch observa cualquier en la trama, este es descartada, previniendo así que las tramas erradas consuman el ancho de banda del segmento destino. Si tu red experimenta altas razones de frame alignment o errores FCS, el modo ded switching estore-and-forward es el mejor. La solución absoluta es fijar la causa del error, el usar store-and-forward en este caso es simplemente un bandage.

Si tu segmento fuente y destino usan medios diferentes, entonces se debe usar este modo de switching. Los medios diferente algunas veces tienen issues cuando transfieren la data.

Como el switch tiene que recibir la trama entera antes de iniciar el envío, la latencia de transferencia varía de acuerdo al tamaño de la trama. En 10BaseT, la trma mínimo es 64 octetos, el cual toma 51.2 microsegundos en recibirlo. Por otro lado un trama de 1518 octetos requiere al menos 1.2 milisegundos. La latencia para 100BaseX es un décimo que para 10BaseT.

Cut-Through Switching.- El modo cut-through permite a un switch iniciar el proceso de envío tan pronto como este recibe la dirección de destino. Este reduce la latencia al tiempo necesario para recibir los 6 octetos de la dirección de destino correspondiente a 4.8 microsegundos. Pero como cut-through no puede chequear tramas erradas antes de enviarlos, este los pasa a través del switch, gastando consecuentemente el ancho de banda para que le final el dispositivo final descarte la trama.

Como la velocidad del procesador incrementa, la latencia viene a ser menos relevante. En ambientes de alta velocidad, el tiempo que recibe y procesa una trama se reduce significativamente, minimizazndo las ventajas del modo cut-through. Store-and-Forward viene a ser una atractiva elección para la mayoría de redes.

Algunos switches soportan modo cut-through y store-and-forward, tales swityches usualmente contiene un tercer modo llamado cut-through adaptivo . Este switches multimodal usan cut-through por defecto y selectivamente activan store-and-forward. Los switches monitorean la trama cuando pasan en busca de errores. Aunque un switch no puede para una trama errada, este cuenta cuantos ve. Si el switch observa que muchas tramas contienen errores, el switch automáticamente activa el modo store-and-forward. Este modo de operación es conocido como cut-through adaptivo, el cual tiene la ventaja de proveer baja latencia mientras que la red

opera bien, y provee protección automática para segmentos fuera de banda si el segmento en banda experimenta problemas.

Fragment-Free Switching.- Esta alternativa ofrece algunas ventajas del switching cut-through y store-and-forward. El switching Fragment-Free se comporta como cut-through en la medida que no espera recibir la trama entera para enviarla. Fragment-Free envía la trama después que este recibe los primeros 64 octetos de la trama, protegiendo así al segmento destino de tramas pequeñas lladas fragmentos o runts producto de colisiones en la red Ethernet. Debido a que las colisiones ocurren durante los primeros 64 octetos y por que la mayoría de tramas erradas se mostrarían en estos octetos, el modo de switching Fragment-Free puede detectar la mayoria dee tramas malas y descartarlos en vez que enviarlos. Fragment-Free tiene la latencia mas alta que cut-trhough, debido a que tiene que espera por 58 octetos mas antes de enviar la trama. Las ventajas de Fragment-Free son mínimas debido a las redes de alta velocidad y procesadores de switches mas rápidos.

4.2.- VIRTUAL LANS : VLAN

Para ser capaz de tener diferentes puertos en el switch que puedan ser parte de diferentes sub-redes, necesitamos crear LANs virtuales dentro del switch. Las Redes de Area Local Virtuales (VLAN) son una agrupación lógica de usuarios de red y recursos conectados para definir

puertos en el switch. Una VLAN se parece y es tratado como tal a una sub-red.

Una VLAN permite que un grupo de usuarios compartan un dominio de broadcast común sin importar su ubicación física en la red. Creando VLAN mejora la performance y seguridad de la red mediante el control de la propagación del broadcast. Una VLAN es un dominio de broadcast lógico que puede span múltiples segmentos de LAN físicos. Puede ser diseñado para establecer estaciones segmentadas lógicamente por funciones, equipos de proyectos, o aplicaciones sin importar la ubicación física de los usuarios. Cada switch puede se asignado a únicamente una VLAN. Los puertos en una misma VLAN comparten los broadcast, los puertos en un switch asignados a diferentes VLAN no comparten broadcast. Esto mejora la performancec de la red en su totalidad.

Dentro de una iter-red switched. Las VLAN proveen segmentación y flexibilidad organizacional. Usando al tecnología VLAN, se puede agrupar los puertos de l switch y sus usuarios conectados en una comunidad lógicamente definida, tal como co-trabajadores dentro de un mismo departamento, un equipo de producto cros-funcional, o diversos grupos de usuarios compartiendo la misma aplicación de red.

Una VLAN puede existir en un switch o múltiples switches. Esto puede incluir estaciones en un edificio o múltiples edificios, o esto puedee conectar a través de una WAN.

Los beneficios de las VLANs son los mencionan a continuación:

- Simplifica los movimientos, adiciones y cambios.
- Reduce los costos administrativos.
- Tienen un mejor control de los boradcast.
- Tighten la seguridad de la red.
- Proporciona Micro-segmentación con escalabilidad.
- Distribuye la carga de tráfico.
- Reubica servidores dentro de zonas seguras.

Debido a la introducción de soluciones VLAN de vendedores múltiples, la IEEE formó la comisión 802.3Q para desarrollar interoperatibilidad virtual en redes de área local switched. Este comité describió los conceptos llamados shared VLAN (SVL) e independient VLAN (IVL). Estos conceptos definen como los switches almacenan las direcciones MAC en su switching Table.

4.2.1.- Operación de las VLAN

Un switch opera en la red como un bridge tradicional. Cada VLAN configurado en el switch implementa los procesos de learning,

forwarding, filtering y flooding, como si fueran un bridge físicamente separados.

Internamente, el switch implementado con VLAN restringe el envío de data hacia el puerto destino ubicado en la misma VLAN que el puerto originador, es decir cuando una trama llega a un puerto del switch, este tiene que trasmitir la trama únicamente a los puertos que están en la misma VLAN.

Normalmente, un puerto lleva tráfico únicamente para la VLAN a la cual el pertenece. Para que una VLAN se expanda por múltiples switches, un Trunk es requerido para conectar dos switches. Un trunk puede llevar tráfico para múltiples VLAN. Los puertos en una VLAN son configurados con una identificación para determinar a que VLAN pertenece.

Las VLAN pueden ser asignados de dos diferentes maneras como se menciona a continuación:

- Estático: El asignamiento de los puertos a una VLAN puede ser configurado estáticamente por el administrador.
- Dinámico: Los switches soportan asignamiento dinámico de VLAN, a través del uso de un VLAN membership Policy Server (VMPS). El VMPS puede ser un switch o un servidor. El VMPS contiene una base de datos que mapea las direcciones MACs asignadas a una VLAN.

Un ejemplo del funcionamiento de las VLAN se muestra en la figura 4-4.

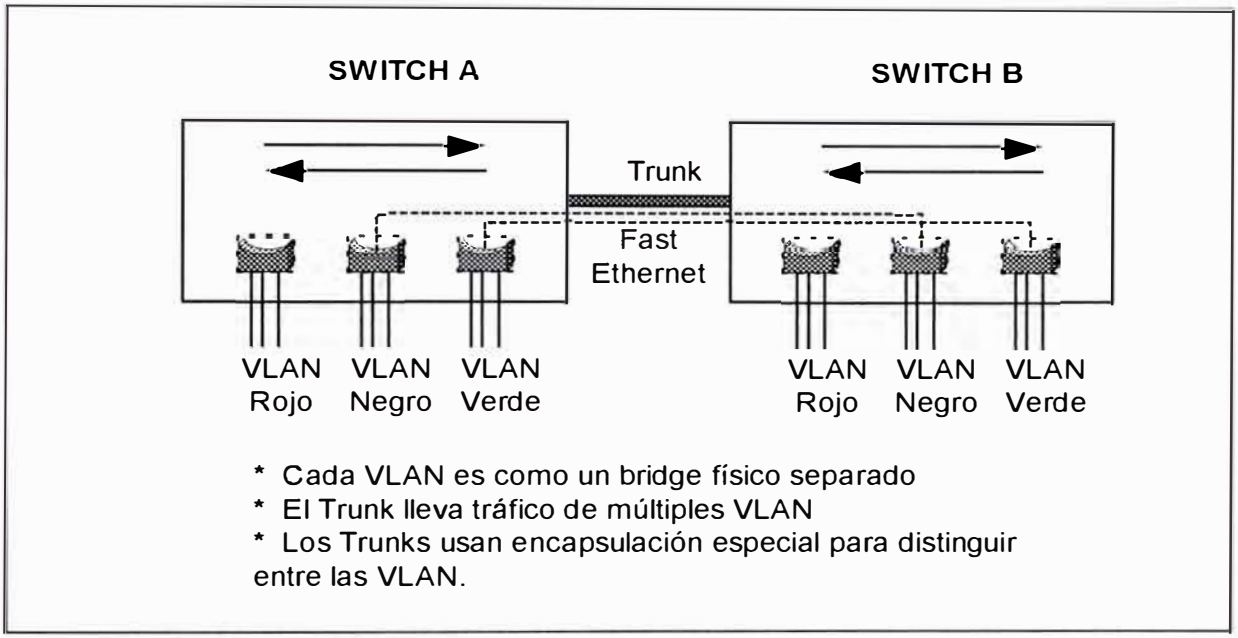


Figura 4-4 Operación de las VLAN en un Switch.

4.2.2.- Justificando la Necesidad de VLAN

En redes legacy, los administradores de red asignan usuario basados en la localización geográfica, es así que un usuarió de Ingeniería que se sentaba cerca de uno de Administración deberían pertenecer a la misma red. El uso de VLAn ayuda a resolver muchos problemas asociados con el diseño de redes legacy. A continuación presentamos cinco items que garantizan la implementación de una VLAN.

Problema 1 - Seguridad de RED .- El primer problema es el medio compartido de redes legacy. Cuando una estación transmite en una red compartida como el sistema 10BaseT, todas las estaciones adjuntas al

segmento reciben una copia de la trama, aunque ellos no sean los destinatarios de la trama. Esto no previene la red desde su funcionamiento, pero los software package que monitorean el tráfico de red tienen disponibilidad de lectura y pueden operar en un número de plataformas. Cualquiera con ese paquete puede capturar password, e-mail sensibles y cualquier otro tráfico en la red.

Cuando los usuarios de departamentos mezclados comparten un segmento, puede ocurrir la captura de información no deseada. Si alguien ded recursos humanos o accounting envía data sensitive como salarios, opcines ded stock, record ded salud en una red compartida, cualquiera que tenga un software de monitoreo de red puede decodificar la información.

El uso de VLAN te permite ubicar todos los usuarios relacionados a procesos en un mismo dominio de broadcast y aislarlos de otros usuarios de otros dominios de broadcast, es así que se puede asignar a todos los usuarios de accounting en un mismo VLAN indpendiente de su ubicación geográfica; todos los usuarios de Ingenieria a otra VLAN y los de Marqueting a un tercero.

Creando VLAN en redes switched, se crea otro nivel de protección. El tráfico de switches bridge dentro de una VLAN, es decir dentro de una VLAN se produce todas técnicas de conmutación de paquetes. Cuando una estación transmite, la trama siolo va al destino buscado. El

Switch no distribuye la trama a todos los usuarios en la VLAN. Un ejemplo se muestra en la figura 4-5.

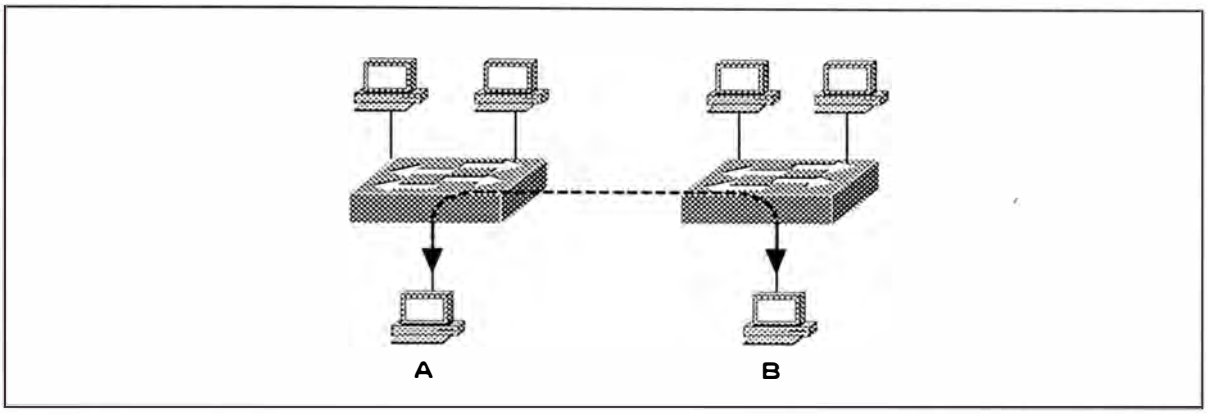


Figura 4-5 Una trama Unicast conocida en una Red Switched.

En esta figura la estación A trasmite una trama a la estación B adjunta a otro switch. Aunque la trama cruza a través del switch, únicamente el destino recibe una copia de la trama. Los swjtches filtran la trama a las otras estaciones, si ellos pertenecen a otra VLAN. En este punto es necesario mencionar que únicamente los tramas flooded puede ser capturado.

Problema 2 - Distribución de Broadcast.- Desafortunadamente muchos protocolos crean tráfico broadcast, así por ejemplo Apple Talk envía routing updates cada diez segundos, NetBEUI crea muchas tramas broadcast, TCP IP al igual que Aplle Talk genera broadcast debido a los routing updates, ARP y otros procesos. Las aplicaciones multimedia también creantráfico broadcast y multicast dentro de un dominio de broadcast.

El tráfico broadcast afectan la performance de las estaciones. Cualquier broadcast recibido interrumpe el CPU evitando que continúe trabajando en la aplicación de usuario. Si el número de broadcast por segundo incrementa en la interface, la utilización efectiva del CPU disminuye.

Si existe problemas de broadcast en la red, se debe crear VLAN adiconales y adjuntar algunos dispositivos a cada uno, la efectividad de esta acción depende de encontrar la fuente del broadcast. Creando múltiples dominios podría ayudar a reducir el número de broadcast en cada dominio.

Problema 3 - Utilización del Ancho de Banda.- Cuando los usuarios se adjuntan a un mismo medio compartido, los usuarios comparten ancho de banda, esto se traduce en menos promedio de ancho de banda por cada usuario, trayendo como consecuencia el inicio de solicitudes por mas ancho de banda. Las VLAN, creados en switches LAN, pueden ofrecer mas ancho de banda a los usuarios que son inherente en el medio compartido.

Cada puerto en el Switch se comporta como un legacy bridge. Los bridge filtran tráfico que no necesita ir a otros segemntos, si es necesario atravesar el bridge, este envía la trama a la correcta interface y no a las otras. Si el bridge no sabe donde reside el destino, este floods la trama a todos los puertos en el dominio de broadcast (VLAN).

Problema 4 - Latencia de Red desde Routers.- En la figura 4-6, los usuarios del departamento Accounting en los dos segmentos tienen que atravesar el segmento de Ingeniería para transferir cualquier data. Las tramas tienen que pasar a través de dos routers. Al atravesar a través de los routers, estos introducen latencia (el tiempo necesario en transportar una trama desde el puerto de ingreso al puerto ded salida) end-to-end, adicionalmente cada segmento congestionado que la trama tiene que atravesar incrementa también la latencia. Moviendo a todos los usuarios ded accounting dentro de una **VLAN**, la necesidad de atravesar a través de dos routers y segmentos es eliminado. Si tu puedes eliminar la necesidad de pasar tráfico de usuario a través ded un router, mediante la ubicación de usuarios en una misma **VLAN**, tu puedes eliminar la latencia acumulativa introducida por el router.

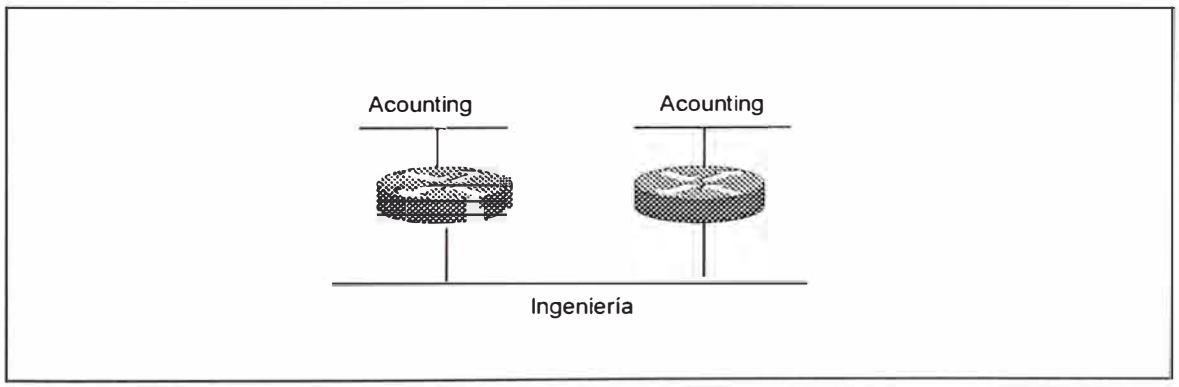


Figura 4-6 Problemas de seguridad en una Red leagcy.

Las **VLAN** nos ayudan a reducir la latencia debido a la reducción de la congestión de los segmentos. Este puede ser dramáticamente mejorado si las conexiones originales de las estaciones a un medio compartido congestionado, ahora dichas conexiones de cada estación tiene un puerto del switch dedicados.

Problema 5 - Lista de Acceso Compleja.- Las listas de acceso son políticas que permiten controlar el tráfico entre estaciones o redes, estos se encuentran exclusivamente en los routers. En el ejemplo d la figura (pag 124 lans), los filtros en lso routers adjuntos al segmento de Ingeniería puede incluir lista de accesos permitiendo que una cantidad de tráfico pase a través de dicho segmento, pero nunca conversar con cualquier estación de Ingeniería. Aunque esto no previene a los usuarios de Ingeniería monitorear la red, previene la comunicación entre el departamentod e Ingenieria y el de Accounting.

Las VLAN pueden ayudarnos permitiéndote tener todas los usuarios de Accounting en una VLAN. Luego su tráfico no necesita pasar a través del router para conseguir a su peer en la VLAN. Esto puede simplificar el diseño de nuestra lista de acceso por que puedes tratar las redes como grupos con iguales o similares requerimientos de acceso.

4.3.- SAPANNING TREE PROTOCOL

La mayoría de administradores y diseñadores de red subestimaron la importancia de Sapnning –Tree Protocol (STP). Como los router llegaron a ser muy populares en los comienzos de los 90, STP faded en el olvido como el protocolo menos importante que trabajó. Sin embargo, con el reciente avance de la tecnología swtiching, el STP una vez mas ha llegado a ser un factor importante que puede tener tremendo impacto en la performance de la red.

El spanning-tree protocol, es un protocolo bridge to bridge desarrollado por el Digital Equipment Corporation (DEC). El algoritmo spanning-tree DEC fue subsecuentemente revisado por el comité IEEE 802 y publicó la especificación 802.1d. El algoritmo DEC y el IEEE 802.1d no son los mismos y por consiguiente no son compatibles.

El propósito de sapnning-tree protocol es mantener una red libre de loops. Una ruta libre de loop es acomplished cuando un dispositivo reconoce un loop en la topología y bloquea uno o mas puertos.

El Sapnning-Tree continuamente explora la red para que una falla o la adición de un switch link o una bridge sea descubierto rápidamente. Cuando la topología de la red cambia, el Spanning–tree reconfigura los puertos del switch o el bridge para evitar perdida de conectividad o creación de nuevos lopps.

4.3.1.- Por Que Usar Spanning-Tree Protocol

Los loops ocurren en la red por una variedad de razones. La razón mas común ded encontrar loops en la red es el intento deliberado de proveer redundancia a la red, por el caso de que si un sitch falla, otro switch tome su lugar. Son embargo los loops también pueden ocurrir por error.

Broadcast Loop.- Los switches flood las tramas broadcast a todos los puertos excepto al puerto del cual la trama es recibido. Debido a esto,

pueden ocurrir problemas de "broadcast storm" como el ilustrado en la figura 4-7.

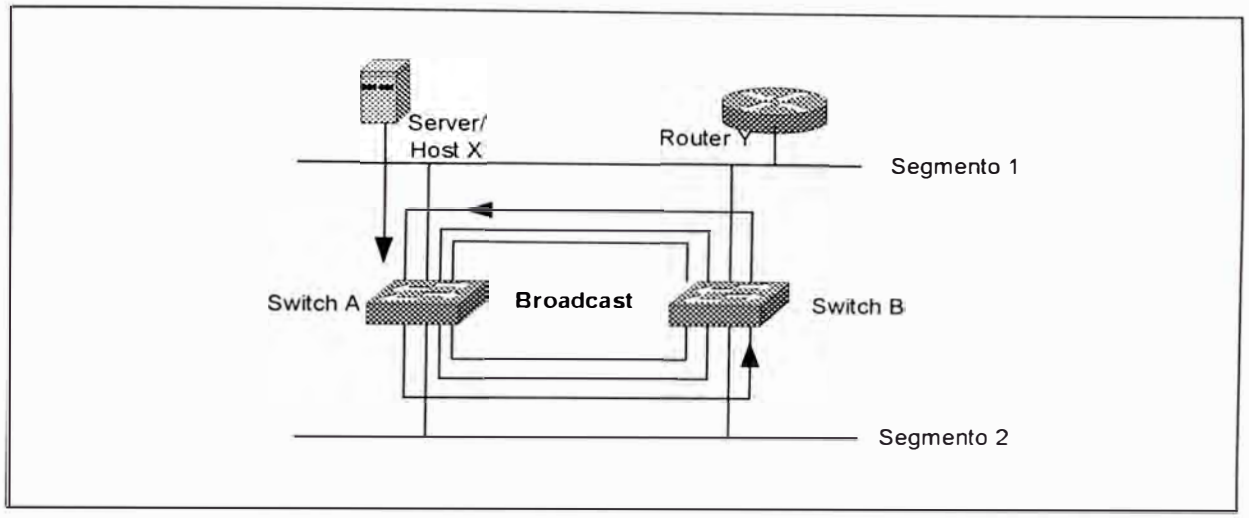


Figura 4-7 Los switches continuan propagando el tráfico broadcast por siempre.

Cuando el "host X" envía una trama "broadcast", tal como un "Address Resolution Protocol" (ARP) para su "default gateway" en el router Y, la trama sería recibida por el switch A. El switch A examina la dirección de destino en la trama y determina que la trama tiene que ser enviada (a todos los puertos) al enlace ethernet de abajo, que es el segmento 2.

Cuando esta copia de la trama llega al switch B, el proceso se repite y una copia de la trama es transmitida en el segmento ethernet de arriva, segmento 1. Desde que una copia de la trama original llega al switch B via el ethernet 1, estas tramas viajan alrededor del lazo en ambas direcciones aún después que la estación destino ha recibido una copia de la trama.

Los protocolos de capa 2 como ethernet, carecen de un mecanismo para reconocer y eliminar las tramas de lazos no deseados. Algunos protocolos de capa 3 implementan el mecanismo Time-to-Live (TTL) que limita el número de veces que un paquete pueda ser retransmitido por un dispositivo de red de capa 3. Careciendo de dicho mecanismo, los dispositivos de capa 2 continúan retransmitiendo el tráfico indefinidamente.

Inestabilidad De Switching Table.- Una inestabilidad de la base de datos de los switches ocurre cuando múltiples copias de tramas llegan por diferentes puertos de un switch. En la figura 4-8, el switch B instala un mapeo entre la estación X y el puerto conectado al segmento 1, cuando la primera trama llega. Mas tarde, cuando la copia de la trama transmitida a través del switch A llega, el switch B tiene que retirar la primera entrada, e instalar uno que mapea la dirección MAC de la estación X al puerto conectado al segmento 2.

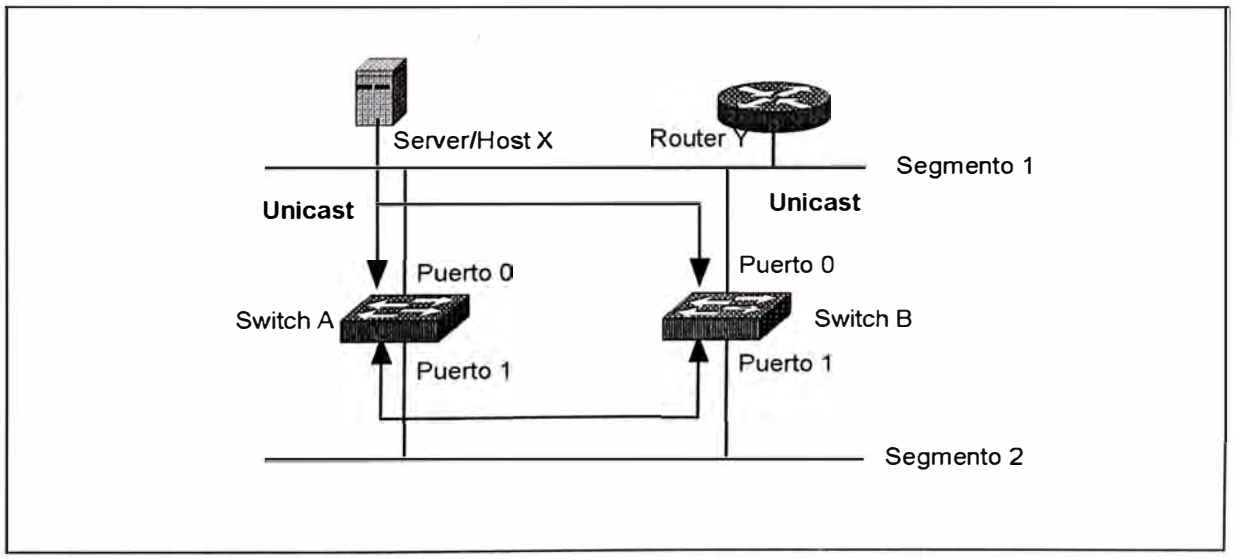


Figura 4-8 Inestabilidad de la Base de Datos MAC.

Dependiendo de la arquitectura interna del swirtch en cuestión , este puede o no solucionar los rápidos cambios en la base de datos MAC. En esta instancia la solución para evitar lazos debería eliminar este problema previniendo que uno de los cuatro interfaces transmita o reciba tramas durante la operación normal.

4.3.2.- Dos Conceptos de Spanning-Tree Protocol

Los cálculos de Spanning-Tree hacen uso extensivo de dos conceptos cuando crean una topología lógica libre de lazo.

- Bridge ID (BID)
- Path Cost

Bridge IDs.- Un bridge ID (BID) es un simple campo de 8 bytes que esta compuesto de dos subcampos, tal como se ilustra en la figura 4-9.

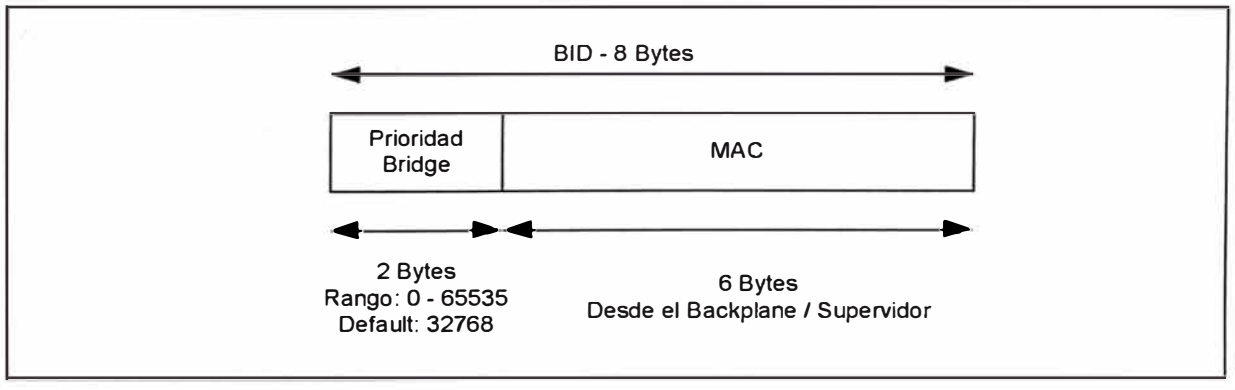


Figura 4-9 El Bridge ID esta compuesto por una Prioridad de Bridge y una dirección MAC

El subcampo mas bajo consiste de una dirección de 6 bytes asignado al swith. Este es un número que no está diseñado para ser cambiado por el usuario. La dirección MAC es expresado en formato hexadecimal usual de base 16.

El subcampo mas alto está referido como la prioridad del bridge. No hay que confundir prioridad de bridge con varias versiones de prioridad de puerto. El campo prioridad de bridge es un valor de 2 bytes, siendo el valor de prioridad el punto medio de todos los valores de 0 a 65535 que se producen al combinar 16 bits y tener 216 valores. Siendo este número igual a 32768 la cual es típicamente expresado en formato decimal.

Path Cost.- Los switch usan el valor de costo para evaluar cuancerca están de otros switches. El original 802.1d difinió costos como 1000 Mbps dividido por el ancho dee banda del enlace en Mbps. Por ejemplo un enlace de 10Mbps tiene un costo de 100 (1000/10). Fast Ethernet tiene un costo de 10 (1000/100). Este esquema ha servido por años, pero que pasa con Gigabit Ethernet y ATM OC-48, los costos que resultarían serían inválidos. Una opción es usar un valor ded 1 a todos los enlaces igual o mas grandes que 1 Gbps, la cual previene al STP de precisamente elegir la mejor ruta en redes Gigabit.

Como solución a este dilema, el IEEE ha decidido modificar los costos y usar una escala no lineal. La Tabla 4-4 lista los nuevos valores de costos.

ANCHO DE BANDA	COSTO STP
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
2 Gbps	2

Tabla 4-4 Valores del costo STP para Redes Bridged.

Los valores en la tabla han sido cuidadosamente elegidos para que antiguos y nuevos esquemas interoperen para las velocidades de uso común de hoy en día.

El punto parta recordar lo concerniente a los valores de los costos de STP es que los costos mas bajos son los mejores.

4.3.3.- Secuencia de Decisión de STP

Cuando se crea un topología lógica libre de lazo, el Spanning-Tree usa la misma secuencia de decisión de cuatro pasos:

- Paso 1 : El mas bajo Root BID
- Paso 2 : El mas bajo Costo de Ruta para el Root Bridge

- Paso 3 : El mas bajo sendeer BID.
- Paso 4 : El mas bajo Port ID

Los bridges pasan información de STP entre ellos mismos usando una trama especial conocido como Bridge protocol Data Unit (BPDU). Un bridge usa la secuencia de cuatro pasos para guardar una copia del mejor BPDU visto en cada puerto. Cuando hace esta evaluación, considera a todos los BPDUs recibidos en el puerto como el BPDU que debería ser enviado en ese puerto. Cuando cada BPDU llega, este es chequeado con la secuencia de cuatro pasos para ver si este es mas atractivo (es decir es mas bajo en valor) que el BPDU existente para ese puerto. Si el nuevo BPDU (o el localmente generado) es mas atractivo, el antiguo es reemplazado.

Adicionalmente el proceso de guardar el mejor BPDU, también controla el envio dee BPDUs. Cuando un bridge llega a activarse por primera vez, todos los puertos están enviando BPDUs cada 2 segundos por default. Sin embargo, si un puerto escucha un BPDU de otro bridge que es mas atractivo que el BPDU que ha sido enviado, el puerto local para de enviar BPDUs. Si el BPDU mas atractivo para de legar del bridge vecino por un periodo de tiempo (20 segundos por deefault), el puerto local puede una vez mas resume el envío de BPDUs.

4.3.4.- Tres Pasos de Convergencia Inicial STP

En esta sección consideramos el algoritmo que el Spanning-Tree usa para converger en una topología lógica libre ded loop. Acunque hay muchas facetas para el STP, la convergencia inicial puede se dividida en tres simples pasos:

- Paso 1 : Elegir un Root Bridge
- Paso 2 : Elegir un Root Port
- Paso 3 : Elegir un Designated Port.

Cuando la red se inicia, todos los bridges están anunciando una caótica mezcla de información de BPDUs. Sin embargo los bridges inmediatamente comienzan aplicar la secuencia de dedcisión de cuatro pasos explicada anteriormente. Un único Root bridge es elegido para ser el centro del universo para esa red (Paso 1). Todos los Bridge que quedan calculan un conjunto de Root Ports (Paso 2) y un Designated Port (Paso 3) para construir una topología libre de loop. Se puede pensar que la topología resultante viene a ser como un ciclo, donde el Root Bridge es el Hub con las rutas activas libre de lazos radiando hacia afuera. En una red de estado estable, los BPDUs fluyen de un Root Bridge a través de un radio libre de lazos a cada segmento en la red.

Después que la red ha convergido en una topología activa libre de lazo utilizando este proceso, los cambios adicionales son manejados utilizando el proceso de Topology Change.

Nos referiremos a la figura 4-10 como modelo para las explicaciones que continúan.

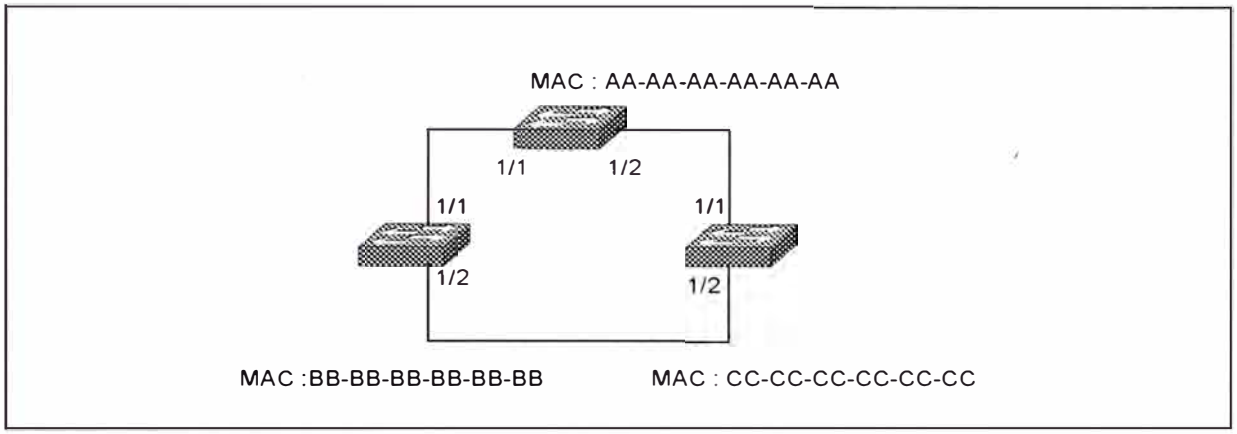


Figura 4-10 Modelo de RED para discusiones de Operaciones STP básicos.

Esta red consiste de tres bridges conectados en un configuración de loop., donde a cad uno se le ha asignado una MAC ficticia.

Paso 1 - Elección de un Root Bridge..- Los switches primero necesitan elegir un Root Bridge observando el Bridge con el mas bajo Bridge ID (BID). De la figura ejemplo, podemos ver que el Cat A tiene un BID por default de 32768. AA-AA-AA-AA-AA-AA (mezcla de Prioridad de Bridge con dirección MAC). El Cat B asume un default BID de 32768.BB-BB-BB-BB-BB-BB y el Cat C usa el 32768.CC-CC-CC-CC-CC-CC. Debido a que los tres bridge están usando el default BID, la mas baja dirección MAC (AA-AA-AA-AA-AA-AA) es tomado, por lo que el CAT A viene a ser el Root bridge.

Los bridges aprendieros que el CAT A tiene el mas bajo BID a través del intercambio de BPDUs explicado anteriormente. La figura 4-11 muestra un esquema de un BPDU.

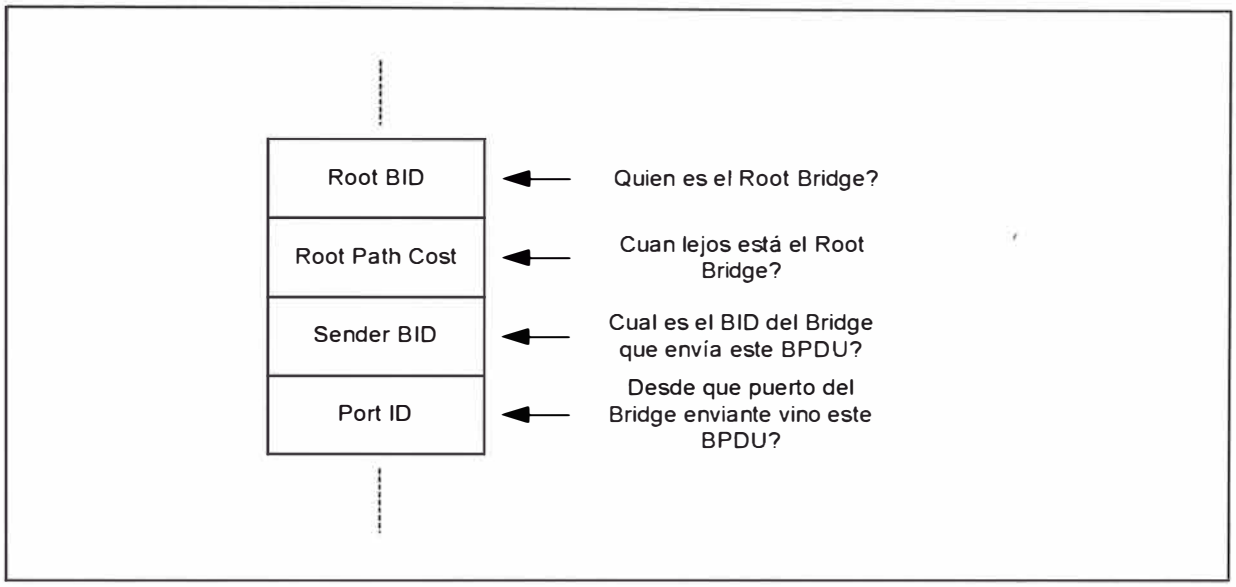


Figura 4-11 Diagrama básico de un BPDU.

Para propósitos de la selección del root bridge, la discusión es concerniente únicamente a los campos Root BID y Sender BID. Cuando un Bridge genera BPDUs cada 2 segundos, este ubica como el bridge que cree que es el Root Bridge en el instante de tiempo en el campo Root BID. El bridge simpre ubica su propio BID en el sender BID.

Supongamos que le Cat B bootea primero y empieza a enviar BPDU anunciándose como el Root Bridge cada 2 segundos. Pocos minutos después el Cat C botea y se anuncia como el Root Bridge; cuando el BPDU del Cat C llega al Cat B, este descarta el BPDU por que el Cat B tiene el BID mas bajo grabado en su puerto (su propio BID). Tan pronto como el Cat B

transmite un BPDU, el Cat C aprende que no es tan importante como asumió inicialmente, en este punto el Cat C envía BPDUs que lista al Cat B como el Root BID y el cat C como el Sender BID. La red esta en acuerdo que el Cat B es el Root bridge.

Cinco minutos mas tarde el Cat A bootea, y envia anuncios indicando que él es el Root Bridge, cuando estos BPDUs llegan al Cat B y Cat C, estos switches abdican la posición de Root Bridge al Cat A, todos los tres switches están enviando BPDUs que anuncian que el Cat A es el Root Bridge y los restantes como el Sendedr BID.

Paso 2 - Elección de un Root Port..- Después de seleccionar el root Bridge, los switches se mueven para seleccionar los Root Ports. Un Root Port de un Bridge es el puerto que está mas próximo al Root bridge. Cada Bridge que no es un Root Bridge tiene que seleccionar un Root Port.

Como los switches usan el concepto de costo para determinar su proximidad, usan este concepto para seguir algo llamado Root Path Cost, que es el costo acumulativo de todos los enlaces para llegar al Root Bridge. La figura 4-12 nos muestra como este valor es calculado a través de múltiples bridges y el proceeso de selección del Root Port.

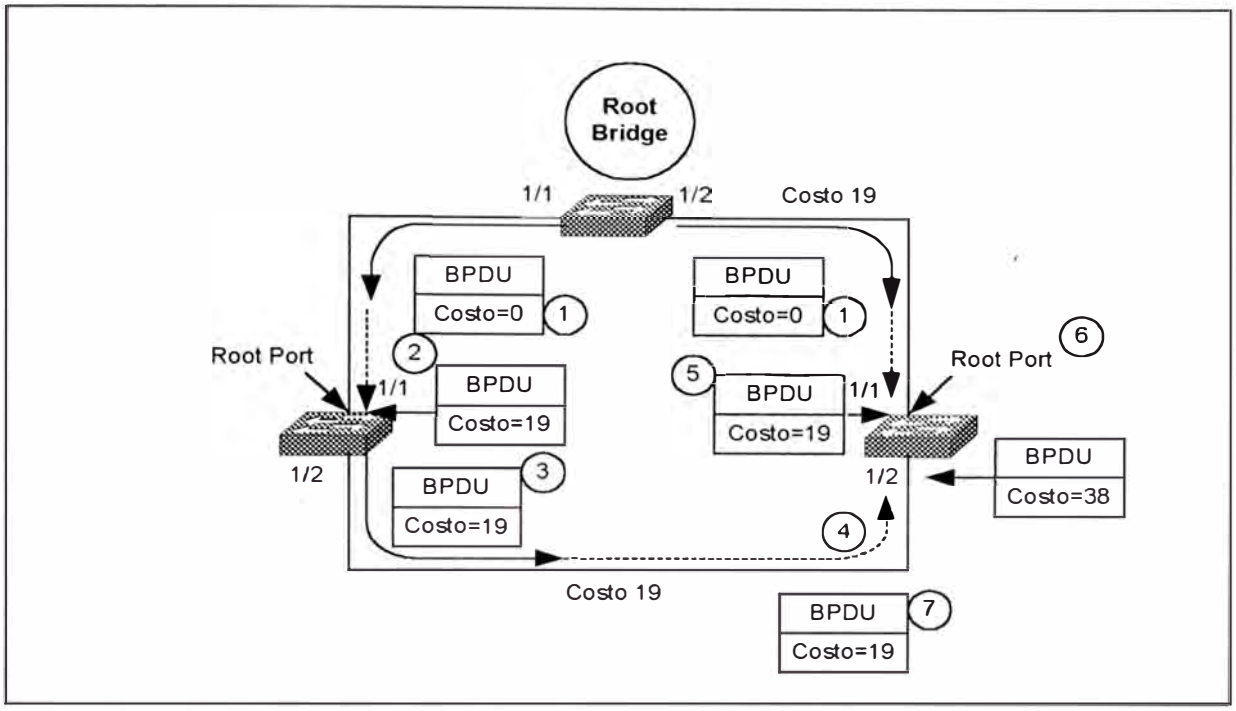


Figura 4-12 Cada Non-Root Bridge tienen que seleccionar un Root Bridge.

Cuando el Cat A (el Root Bridge) envía sus BPDUs, ellos continen un Root Path Cost igual a 0 (paso 1). Cuando el Cat B recibe estos BPDUs, le adiciona el Path Cost del puerto 1/1 al Root Path Cost contenido en el BPDU recibido. Asumeiendo que todos los enlaces son Fast Ethernet, el Cat B recibe un Root Path Cost de 0 y adiciona el costo de 19 al Puerto 1/1 (Paso 2). El Cat B luego usa el valor de 19 internamente y envía BPDUs con un Root Path Cost de 19 al puerto ½ (paso 3).

Cuando el Cat C recibe estos BPDUs desde el Cat B (Paso 4), este incrementa el Root Path Cost a 38 (19+19) . Sin embargo el Cat C está también recibiendo BPDUs del Root Bridge en el puerto 1/1. Estos ingresan al Cat C en el puerto 1/1 con un costo de 0, y el Cat C incrementa el costo a

19 internamente (paso 5). Entonces el Cat C tiene que hacer una descisión : tiene que seleccionar un único Port Root, el puerto que está mas próximo Root Bridge. El Cat C ve un Root Path Cost de 19 en el puerto 1/1 y 38 en el puerto ½, por lo tanto el puerto 1/1 viene a ser el Root Port (Paso 6). El Cat C comienza a advertir este Root Path Cost de 19 a los swtiches dee abajo (Paso 7). También debemos mencionar que el Cat B también realiza un proceso similar que el Cat C. Debemos notar que los costos son incrementados en la medida que los BPDUs son recividos en un puerto.

Paso 3 - Elección de un Designated Port..- La parte de prevención de loop en STP viene a ser obvio durante el tercer paso de convergencia inicial. Cada segmento en una red bridged tiene un Designated Port. Este puerto funciona como un simple puerto bridge que envía y recibe tráfico entre el segmento y el Root Bridge. La idea es que si únicamente un puerto manipula tráfico por cada enlace, todos los loop han sido quebrados. El bridge conteniendo el puerto designado para un segmento dado es referido como el Designated Bridge para ese segmento.

Al igual que la selección deel Root Port, los Designated Port son elegidos basado en acumulativos Root Path Cost hacia el Root Bridge.

Para ubicar el Designated Port, miremos a cada segmento. Primero miremos el segmento 1, el enlace entre el Cat A y el Cat B. Hay dos puertos bridge en el segmento: Cat A port 1/1 y el Cat B port 1/1, el Cat A

port 1/1 tiene un Root Path Cost de 0, mientras que el Cat B port 1/1 tiene un Root Path Cost de 19, como el Cat A port 1/1 tiene tiene el mas bajo Root Path Cost, este viene a ser el Designated Port para este enlace. De igual manera se lleva a cabo la elleción deel Cat A port ½ como Designated Port.

Ahora miremos al segmento 3, ambos Cat B port ½ y Cat C port ½ tiene el mismo Root Path Cost de 19. existe una tie, en este punto hacemos uso de la secuencia de decisión de cuatro pasos discutido anteriormente.

En el ejemplo de la figura 4-12 los tres brdiges estan de acuerdo que el Cat A es el Root Bridge, por lo que evaluaríamos el Root Path Cost. Pero ambos switches Cat B y Cat C tienen el mismo costo de 19. por lo que continuamos con el criterio del BID. Notamos que el BID del Cat B (32768.BB-BB-BB-BB-BB-BB) es mas bajo que el BID del Cat C (32768.CC-CC-CC-CC-CC-CC); El port ½ del Cat B viene a ser el Designated Port para el segmento 3. El Cat C port ½ viene a ser un non-Designated Port.

4.3.5.- Estado de los Puertos Spanning – Tree

Después que los bridges han clasificado sus puertos como Root, Designated o non-Designated, la creación de una topología libre de loop es straighforward. Los puertos Root y Designated pueden enviar tráfico, mientras que un puerto non-Designated bloquea el tráfico. Aunque los

estados Forwarding y Blocking son los dos únicos estados presentes en una red estable, la tabla a continuación muestra cindo estados del STP.

ESTADOS	PROPOSITO
Forwarding	Sending/Receiving user data
Learning	Building bridging table
Listening	Building "active" topology
Blocking	Receives BPDU only
Disabled	Administratively down

Tabla 4-5 Valores del costo STP para Redes Bridged.

El estado Disable permite que los administradores de red manualmente shut down un puerto. Después de la inicialización, los puertos inician en el Estado Blocking, donde ellos solo escuchan los BPDUs. Una variedad de eventos causan que le bridge pase al estado Listening. En este punto ningún dato de usuario esta siendo pasado, este puerto está enviando y recibiendo BPDus en un esfuerzo por determinar la topología activa. Es durante el estado Listening que los tres pasos de convergencia se lleva a cabo. Los puertos que han llegado a ser non-Designated Port regresan al estado Blocking.

Los puertos que permanecen como Designated o Root Ports después de 15 segundos (tiempo por default) pasan a estado Learning. Este es otro periodo de 15 segundos donde el bridge no esta aún pasando tramas de data de usuarios. En vez de eso, los bridges están construyento su bridging table a través de la tramas recibidas y mapeando direcciones MAC

fuente con los puertos deel cual son recibidos. El estado Learning reduce la cantidad de flooding cuando el envío dee data comienza.

Si un puerto queda aún como Designated o Root Port al final del periodo Learning, el puerto pasa al estado Forwarding. En este estado, los bridge comienzan a enviar y recibir tramas de data de usuario.

4.3.6.- STP Timers

El Spanning-Tree Protocol es controlado por tres timers documentados en la Tabla 4-6

TIMER	PROPOSITO PRIMARIO	DEFAULT
Hello Time	Tiempo entre el envio de la configuración BPDU	2 segundos
Forward Delay	Duración de los estadoss listening y learning	15 segundos
Max Age	Tiempo BPDU almacenado	20 segundos

Tabla 4-6 Tiempos para el Spanning Tree Protocol,

El Hello Time controla el intervalo de tiempo entre el envío de Configuración BPDUs. El 802.1d especifica el valor por default de 2 segundos, este valor únicamente controla la configuración BPDu que son generados en el Root Bridge (otros dispositivos propagan los BPDUs del Root Bridge ni bien son recibidos). En otras palabras si los BPDUs paran de llegar desde el Root Bridge por un disturbio en la red, los non-root bridge paran también de enviar periódicos BPDUs durante ese tiempo.

El Forward Delay es el tiempo que el bridge gasta en los estados Listening y Learning. Este es un único valor que controla ambos estados. El valor de 15 segundos fue derivado asumiendo un tamaño de red máximo de siete saltos bridge, un máximo de tres BPDus perdidos y un intervalo Hello de 2 segundos.

El Max Age es el tiempo que un Bridge almacena un BPDU antes de descartarlo. Como mencionamos anteriormente los bridge reciben continuos BPDUs cada 2 segundos, el bridge receptor matiene copias continuas de valores BPDUs. Sin emabargo si el dispositivo transmitiendo el mejor BPDUs falla, algún mecanismo tiene que existir para permitir que otros Brdige tomen su lugar.

En Algunas situaciones, los bridge puededn detectar cambios de topología en los enlaces directamente conectados a sus puertos e inmediatamente pasar al estado Listening sin esperar los segundos del Max Age.

Hay dos puntos clave para recordar referente al usu de Timers en STP: Primero, No cambies el valor del Default timer sin hacer algunas consideraciones con cuidad. Segundo, Se debería únicamente modificar los timer STP desde el Root Bridge.

Existe dos tipos de BPDUs intercambiándose en una red estable: Cofiguration BPDUs, las cuales son originados por el Root Bridge y fluyen a los largo de las rutas que radian desde el root bridge. Topology Change Notification BPDU fluyen hacia el Root Bridge para alertar al Root Bridge que la topología activa ha cambiado.

4.3.7.- Balanceo de Carga en Spaning-Tree

El balanceo de carga en STP requiere de dos características a ser construidas en la red:

- Múltiples rutas que forman loops
- Múltiples VLAN

Como no se puede construir loops en una red que este operando Spanning-Tree Protocol, debido a que los loops en la red pertenecen a un mismo dominio de STP, estos dominios múltiples son posibles gracias a la tecnología VLAN. Mediante el diseño intencional de diferentes topologías activas dentro de cada VLAN, podemos utilizar múltiples rutas redundantes. Dentro de una VLAN el tráfico es libre de loops y únicamente utiliza una ruta para alcanzazr su deestino. Pero dos VLANs pueden usar enlaces redundantes que se ha instalado en el switch.

Hay cuatro técnicas disponibles para el balanceo de carga en Spanning-Tree.

Root Bridge Placement.- El flujo de tráfico puede ser influenciada por la ubicación cuidadosa del Root Bridge a través de la Red. Esta opción es extremadamente viable y muy usual para organizaciones usando un diseño de modelo multicapas. Sin embargo en redes que no usuan diseños jerárquicos, esto puede ser imposible.

Port/VLAN Priority – set spantree portvlanpri.- Esto puede ser usado para hacer balanceo de cargas entre switches conectados back-to-back. Esta técnica permite a los administradores de red modificar los valores de Port ID en los switches upstream para influenciar en las decisiones de Forwarding y Blocking en los switches downstream. Esta opción es raramente usada.

Bridge Priority.- Esta técnica puede ser usada en softwares antiguos, donde set spantre portvlancost no es disponible. Al igual que Port/VLAN Priority, esta técnica requiere que los parámetros del balanceo de carga sean ingresados en el switch que está upstream al switch que está actualmente llevando a cabo el balanceo de carga.

Port/VLAN Cost – set spantree portvlancost.- Esta técnica es la opción mas flexible disponible para el balanceo de carga en STP. En redes planas, es también mas simple de implementar. Esto permite que los comandos sean ingresados y observados en el switch actual donde el balanceo de carga se está llevando a cabo.

4.4.- TRUNKING

Cuando los switches en una red soportan VLANs y necesitan conectividad entre ellos, se puede establecer enlaces entre los switches para transportar tráfico inter-VLANs. Un aproach para interconectar switches Catalyst usa enlaces dedicados para cada VLAN individual. Si tenemos una red constituida de únicamente un VLAN, se puede crear rutas de conexión entre dos catalyst llamados enlaces de acceso, las cuales utilizarán enlaces físicos y puertos de ambos switches. Pero si existen mas de una VLAN en la red, se tendrán que crear tantos enlaces de acceso entre los switches como VLANs ubiesen. Esto causa que se desperdicie puertos en ambos catalyst, cables para el enlace físico y además no resulta escalable debido a los costos del sistema. Un ejemplo de esto se muestra en la figura 4-13.

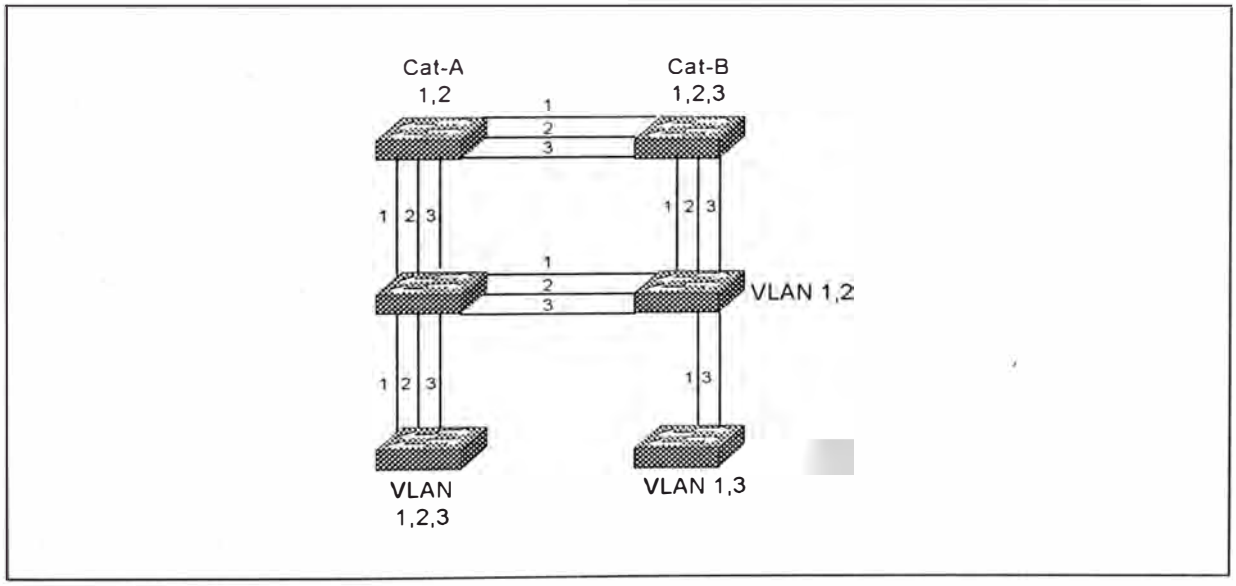


Figura 4-13 Una Red Multi VLAN sin enlaces Troncales.

Alternativamente, podemos habilitar trunk link entre catalyst. Estas trunks permiten distribuir la conectividad de VLANs sin la necesidad de

usar muchas interfaces y cables. Un Trunk multiplexa el tráfico de múltiples VLANs sobre un único enlace. La figura 4-14 muestra la red de la figura 4-13 desarrolado con Truunks.

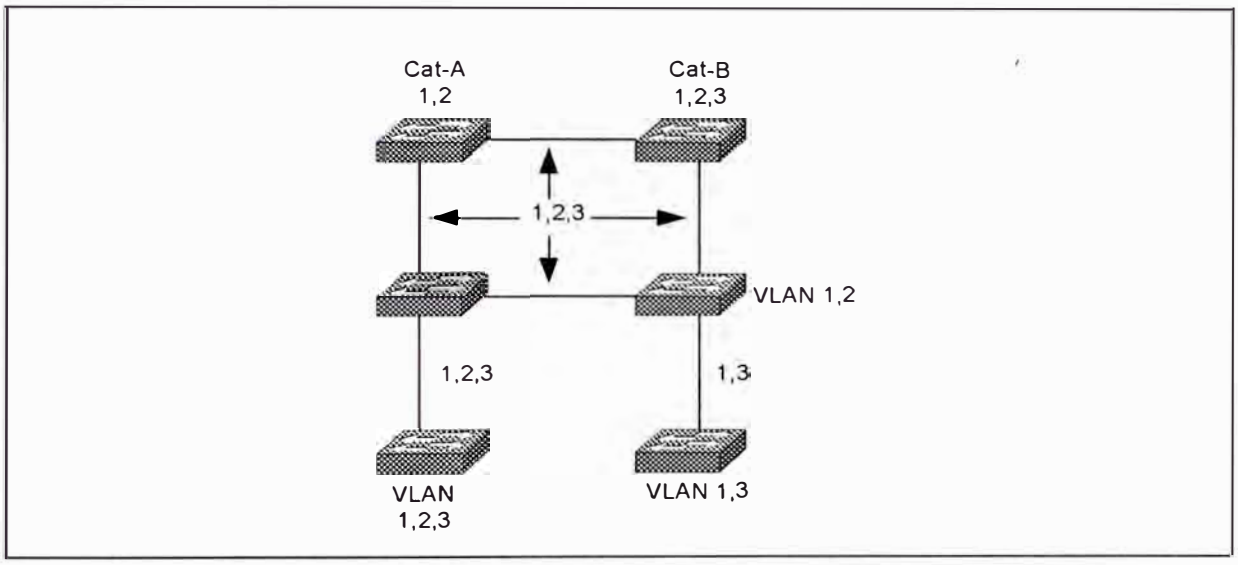


Figura 4-14 La red de la figura 4.13 con enlaces Troncales.

En esta red únicamente 12 puertos y 6 enlaces son usados. Aunque las VLANs comparten el ancho de banda del enlace, se conserva los recursos de la red .

El uso de Trunks no está limitado a interconectar switches Catalyst, también son utilizados para conectar routers y servidores de archivos a switches. Es posible soportar múltiples VLANs sin usar puertos adicionales.

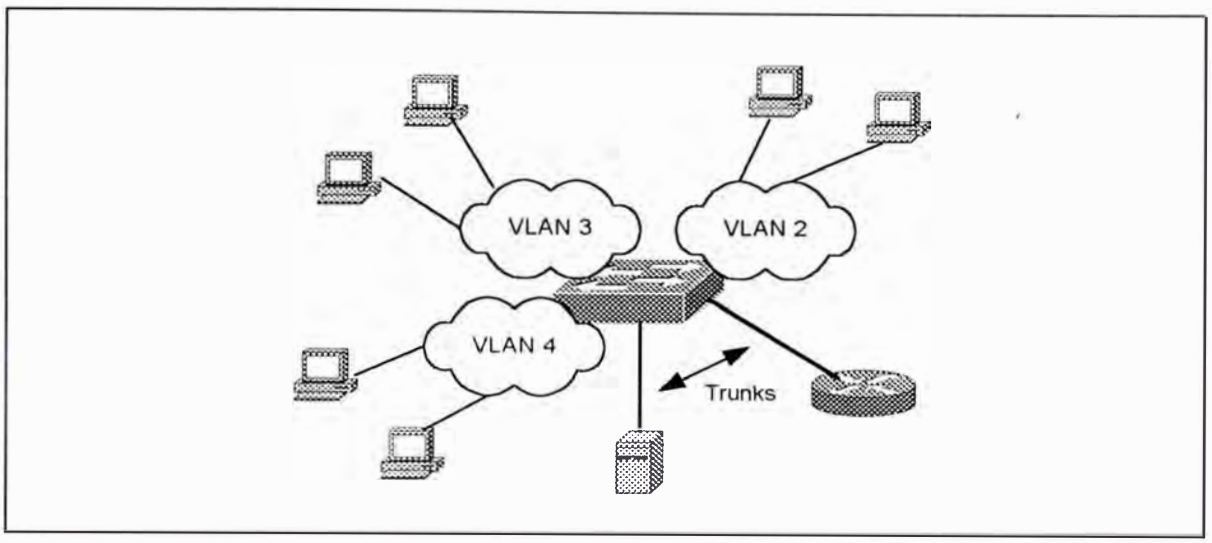


Figura 4-15 Conectando Servidores de archivos y Routers en una Red Multi-VLAN.

En la figura 4-15, los workstation ubicados en las VLAN 2, 3 y 4 no pueden comunicarse entre ellos debido a que estan en diferentes dominios de broadcast, pero si a través del router. Los Trunks conectan un servidor de archivos y el router a la red switched. La conexión trunk al router habilita la conectividad entre las VLANs. Sin los Trunks podemos hacer múltiples interfaces en el router y adjuntar cada una a diferentes puertos en el switch.

Asi mismo podemos introducir un servidor de archivos para mas de una VLAN a través de múltiples tarjetas de interfaces, los cual hacee la red no escalable y aumentar los costos como mencioanmos anteriormente.

Cuando un router o un seridor de archivo se adjuntan como un trunk al switch, hay que enterder como identificar la data que curza desde las diferentes VLANs. El router tiene que además entender la tecnica de multiplexación usada en el enlace. En ambientes Cisco esto se puede realizaar por ISL o 802.1Q sobre Ethernet, 802.10 sobre FDDI, o LANE /MPOA sobre ATM. En un ambiente multivendedor, podemos usar Trunk 802.1Q o LANE/MPOA.

4.4.1.- Ethernet Trunks

La mayoría de implementaciones usan Trunks ethernet. Podemos construir Trunks Ethernet usando Fast Ethernet o Gigabit Ethernet, dependiendo de las necesidades de ancho de banda. EtherChannel crea opciones de ancho de banda adiconal mediante la combinación múltiples enlaces Fast Ethernet o Gigabit Ethernet. Los enlaces combinados se comportan como una sola interface, distribuye la carga de tramas por cada segmento en el EtherChannel, y nos provee enlaces resilency.

Para crear una Trunk no únicamente se necesita conectar los switches por puertos ethernet, esto simplemente crearia por default enlaces de acceso. Para hacer un Trunk, se tiene que habilitar el proceso de Trunk. Cisco desarrolló protocolos para crear Trunks sobre ehternet, permitiendo multiplexar tráfico de VLANs . El esquema de multiplexación encapsula la data del usuario e identifica la fuente VLAN para cada trama. El protocolo llamado Inter-Switch Link (ISL) habilita a múltiples VLAN compartir un

enlace virtual de tal manera que el catalyst sepa a que VLAN pertenece el paquete.

EtherChannel.- Nos provee incrementos de la velocidad de los trunks entre Fast Ethernet y Gigabit Ethernet, o aunque velocidades mas grandes que Gigabit Ethernet. Sin Etherchannel, los enlaces están limitados a las velocidades provista por la interface. Si se necesita velocidades mayores que fast Ethernet, tenemos que introducir un módulo Gigabit Ethernet e inmediatamente cambiar a esa nueva tecnología. Adiconalmente podemos crear múltiples enlaces trunk pero el protocolo STP eliminaría tods y dejaría solo uno debido su algoritmo de evitar loops en la red.

Etherchannel nos permite construir enlaces con incrementos de velocidades sin la necesidad de incorporar nuevas tecnologías. Esto nos provee opciones de escalabilidad en la velocidad de algunos enlaces, a través de la mezcla o empaquetado de los enlaces Fast Ethernet o Gigabit Ethernet, y hacer que el catalyst use los puertos mezclados como un único puerto. Además si se quiere conseguir velocidades mayores a 1 Giagbit, podemos crear Gigabit Etherchannel mezclando puertos Gigabit Ethernet en un EtherChannel. EtherChannel trata el paquete de enlaces como un simple puerto Spanning-Tree y no crea lazos.

EtherChannel trabaja como un enlace de acceso o Trunk, en ambos casos EtherChannel ofrece mas ancho de banda que cualquier

simple segmento en el EtherChannel, es decir podemos combinar segmentos fast Ethernet y Giagbit ethernet para ofrecer mas ancho de banda aparente. Desded el punto de vista Spanning-Tree, un EtherChannel es tratado como un único puerto enb vez de múltiples, además cuando STP ubica un etherChannel en estado Foward o Blocking también pone todos los segmentos en el mismo estado que el EtherChannel.

Inter-Switch Link – ISL.- Cuando multiplexamos tramas provenientes de diferentes VLAN sobre un Fast Ethernet o Fast EtherChannel, el catalyst transmitiendo tiene que identificar la VLAN de la trama del cual es miembro., permitiendo que el catalyst receptor envíe la trama a la misma VLAN. La encapsulación Inter-Link Switch (ISL) propietario de Cisco, nos permite compartir un enlace común entre catalysts mientras permite al receptor separar las tramas a la correcta VLAN.

Cuando un catalyst envía o floods una trama a una interface trunk habilitada como ISL, este encapsula la trama original identificando la VLAN fuente. Generalmente, la encapsulación se vee como en la figura 4-16. Cuando la trama deja la interface trunk en el catalyst fuente, este prepend auna cabecera dee 26 octetos y append un CRC de 4 octetos a la trama. Estos es llamado double-tagging o two.level tagging encapsulation.

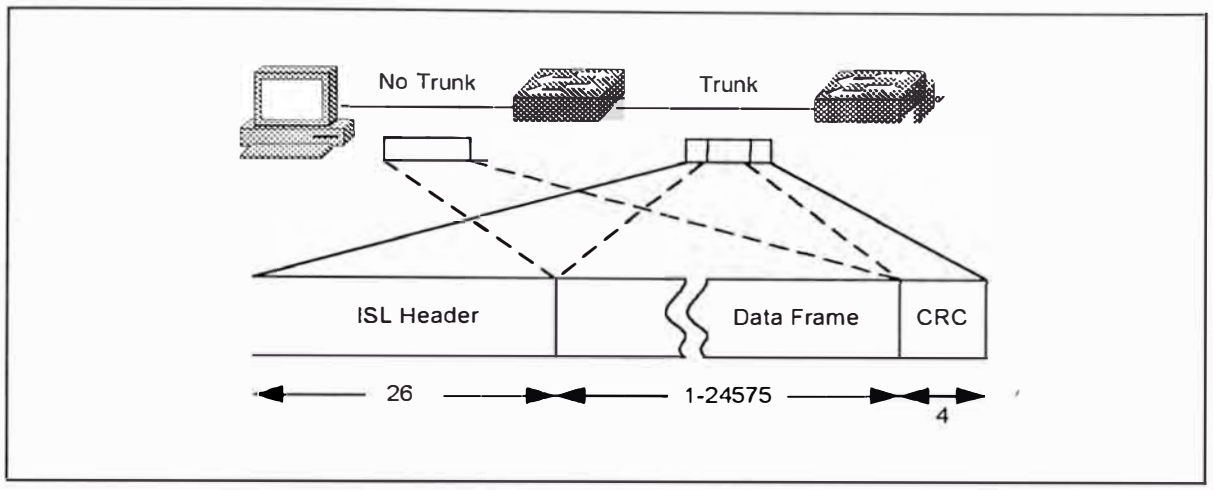


Figura 4-16 Encapsulación doble tagging ISL.

Los enlaces trunk ISL puede llevar tráfico de fuentes LAN a otros que no sean Ethernet. Por ejemplo los segmentos Token Ring y FDDI puedeen comunicarse através de un trunk ISL. Desafortunadamente los atributos de Token Ring difiere significativamente de ethernet, las diferencias incluyen: Tamaño de trama, las cuales osn mas pequeñas y mucho mas grandes que ethernet. Routing Information Field, las tramas Token ring pueden incluir un RIF el cual es meaningles en un sistema ethernet. Explorer Frames, las estaciones Token Ring pueden transmitir una trama explorer para descubrir la ubicación relativa des dispositivo destino.

Cuando Cisco desarrolló ISL incluyó una provisión para Token Ring y FDDI sobre ethernet. La cabecera ISL incluye un espacio para llevar información específica de cabecera Token Ting y FDDI. Estos son llevados en el campo Reserved de la cabecera ISL.

Cuando específicamente tratamos con Token Ring sobre ISL, la encapsulación es llamado Token Ring ISL (TRISL). TRISL adiciona 7 octetos a la encapsulación estándar ISL para llevar información Token Ring. Los trunks pasan las tramas encapsuladas en ISL y TRISL.

En versiones tempranas del Catalyst, se tenía que habilitar manualmente el ISL en ambos puertos terminales del enlace. Con el release 2.1 un método automático de habilitar ISL fue introducido el cual requería que únicamente se configure ISL en un solo terminal del enlace. El protocolo propietario de Cisco Dynamic Inter-Switch Link (DISL) habilita a un catalyst a negociar con el lado remoto de un enlace punto a punto Fast Ethernet, Giagbit Ethernet o EtherChannel a habilitar o desabilitar ISL. El protocolo de enlace de datos DISL, transmite información de configuración ISL con una dirección MAC multicast ded destino de 01-00-0C-CC-CC-CC. Cisco usa este multicast para varios protocolos propietarios.

Una interface del Catalyst puede soportar uno de cinco modos trunk: off, on, desirable, auto, o nonegotiate. Cuando se configura a off, on, auto o desirable, el catalyst envía tramas de configuraciones ISL cada 30 segundos para asegurarse que el otro terminal sincroniza a la configuración actual. La tabla muestra las diferentes combinaciones de modos de trunk y el correspondiente efecto.

MODO LOCAL → / MODO REMOTO ↓	OFF	ON	AUTO	DESIRABLE	NONEGOTIATE
Off	Local : Off Remoto:Off	Local : On Remoto:Off	Local : Off Remoto:Off	Local : Off Remoto:Off	Local : On Remoto:Off
On	Local : Off Remoto:On	Local : On Remoto:On	Local : On Remoto:On	Local : On Remoto:On	Local : On Remoto:On
Auto	Local : Off Remoto:Off	Local : On Remoto:On	Local : Off Remoto:Off	Local : On Remoto:On	Local : On Remoto:Off
Desirable	Local : Off Remoto:Off	Local : On Remoto:On	Local : On Remoto:On	Local : On Remoto:On	Local : On Remoto:On
Negotiate	Local : Off Remoto:On	Local : On Remoto:On	Local : Off Remoto:On	Local : On Remoto:On	Local : On Remoto:On

Tabla 4-7 Resultados de Modos DISL mezclados.

802.1Q / 802.1p.- En un esfuerzo de proveer soporte multivendedor, la IEE 802.1Q comité definió un método para multiplexar VLAN en redes de area local y metropolitana. El método de multiplexación, similar a ISL, ofrece un protocolo trunk alternativo en una red switched. Al igual que ISL, 802.1Q explícitamente tags la trama para identificar la VLAN a la cual pertenece. El esquema de tagging difiere de ISL, debido a que ISL usa un tag externo y 802.1Q usa un tag interno.

La IEEE también trabajó en el estándar llamado 802.1p, el cual permite a los usuarios especificar prioridades para sus tráficos. El valor de prioridad es insertado dentro del campo de prioridad de la cabecera 802.1Q. Si un switch LAN soporta 802.1p, el switch podría enviar tráfico flagged como prioridad alta antes de que este envie otro tráfico.

El esquema de tag extermo de ISL adiciona octetos al comienzo y al final de la trama de data original. Debido a esto es llamado algunas veces double tagging. El 802.1Q es llamado internal tag scheme, por que adiciona octetos dentro de la trama de data original. En contraste con el esquema ISL de cisco, el 802.1Q es llamdo single-tag scheme. La figura 4-17 muestra un trama 802.1Q tagged.

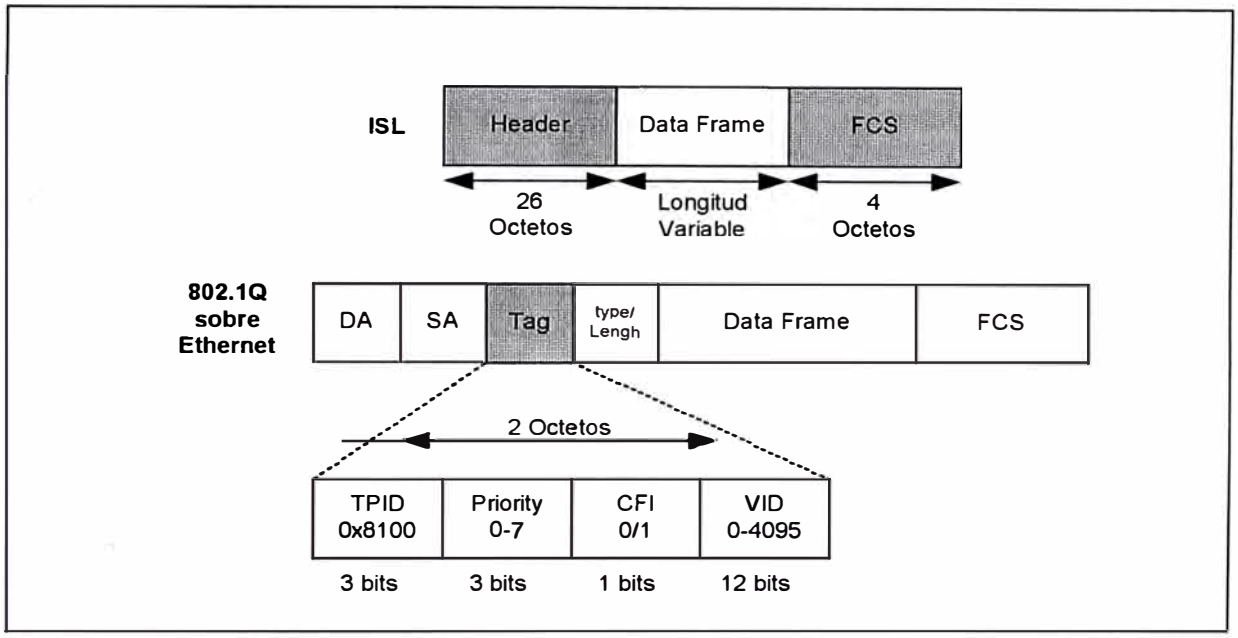


Figura 4-17 Trama Tagging 802.1Q/802.1p comparadio con ISL.

En este punto sucede una situación en el esquema 802.1Q tag. Si el tag es adiconado en una trama que con un tamaño ethernet máximo, esta trama excede el tamaño especificado por la IEEE802.3. Para llevar tag en un trama de maximo tamaño requiere 1522 octetos, cuatro mas que el permitido. El comité 802.3 creó un grupo de trabajo, el 802.3ac para extender las tramas ethernet a un tamaño de 1522 octetos.

Dynamic Trunk Protocol – DTP.- 802.1Q ofrece una alternativa para el protocolo de encapsulación ISL propietario de Cisco. Esto significa que los enlaces Fast Ethernet/EtherChannel tiene mas combinaciones para hacer que un trunk use encapsulacion ISL o 802.1Q tags. Al igual que ISL , el 802.1Q puede puede ser configurado a off, on, desirable o auto. Sin embargo ambos enlaces tiene que estar en modo ISL o 802.1Q . En el release 4.2, cisco introdujo un nuevo protocolo de negociación llamado Dyanmic Trunk Protocol (DTP) el cual mejora la funcionalidad de DISL. DTP negocia en los dos terminales del enlace el modo compatible, reduciendo la posibilidad de incompatibilidad cuando configuramos un enlace.

4.4.2.- FDDI Trunks y Encapsulación 802.1Q

Encapsulación ISL trunk es diseñado para trunk sobre conecciones punto-a-punto entre dos Catalyst usando ethernet. Esto contrasta con la conectividad sobre sistemas FDI. Este sistema opera como un medio de red compartido (half duplex) y puede tener mas que dos paraticipantes en la red. Un diferente esquema de encapsulamiento es usado cuando trunking sobre redes FDDI. Cisco adpasto un estándar IEEE para asegurar el gridging sobre una red basada en 802 y lo aplicó al Trunking FDDI entre catalyst. IEEE 802.10 divisó el estándar para facilitar el transporte dee fuentes de tráfico múltiples sobre redes metropolitanas y locales compartidos y aún retiene aislamiento lógico entre las redes fuente en el receptor.

Podemos crear interconexiones entre Catalyst dondee todos las interfaces del catalyst FDDI mas alla de la misma VLAN. Únicamente una VLAN transporta sobre el FDI, sin embargo, podemos hacecr esto si tenemos una simple VLAN diseñada y tenemos un segmento FDDI existente que necesitas coninuar usar. Los componentes de la red legacy no podrían soportar 802.10, forzándote a configurar el catalyst para que ellos puedan compartir la red FDI. Un uso típico, sin embargo, podría permitir compartir el backbone a múiltiples VLANs, como en la figura 4-18.

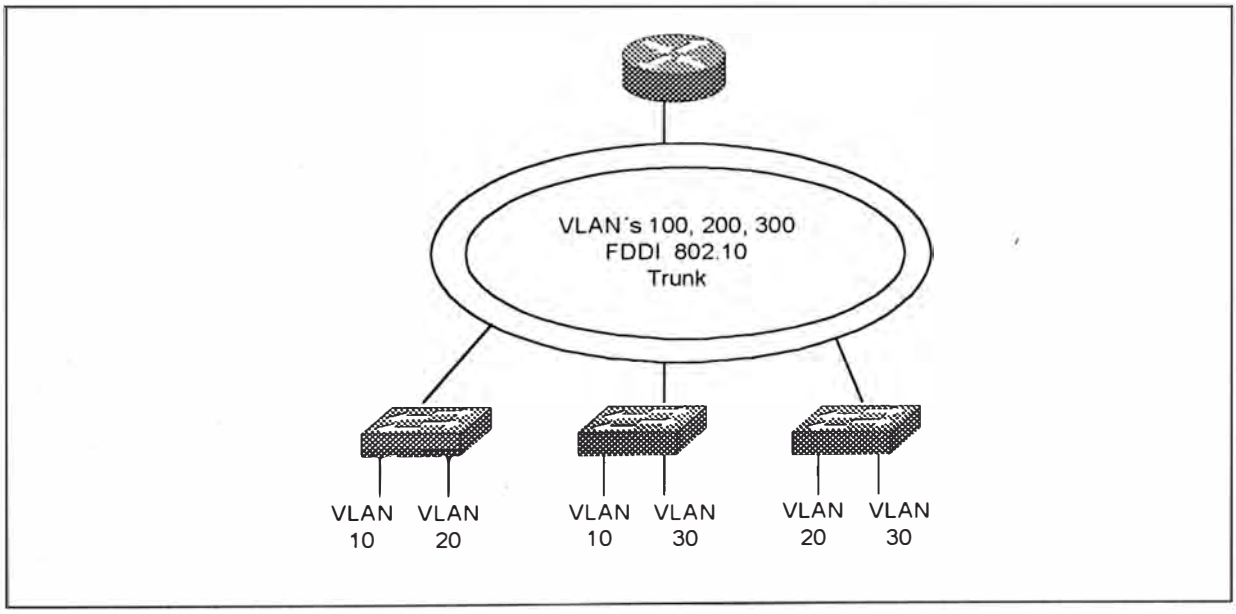


Figura 4-18 Un ejemplo de Trunk FDDI con encapsulación 802.10.

Habilitando encapsulación 802.10 en las interfaces en la red, el backbone FDI viene a ser un trunk del catalyst. La red en la figura mostrada anteriormente adjunta muchos catalyst permitiéndoles transportar data dedsde VLAN distribuidos sobre el trunk FDI. Las estaciones miembros de la VLAN 10 en le Cat A pueden comunicarse con las estaciones ubicadas mas

alla en la VLAN 10 del cat-B. Por consiguiente, los miembros de la VLAN 20 pueden comunicarse con cada uno sin importar la ubicación en la red.

Al igual que múltiples redes VLAN, los routers interconectan VLANs. El router de la figura, adjunta a la red FDDI entiende encapsulación 802.10 y puede además rutear tráfico entre LANs.

La figura 4-19 ilustra encapsulación 802.10. La cabecera 802.10 contiene la cabecera MAC, una cabecera Clear y cabecera Protected. La cabecera MAC continene la dirección MAC fuente y destino usual encontrado en redes FDDI, Ethernet y Token Ring. Las cabeceras Clear y Protected, sin embargo, son adicionados del estándar 802.10. La cabecera Protected duplica la dirección MAC fuente para asegurar que la estación no haga una copia falsa de la fuente real. Si la dirección fuente en la cabecera MAC y Protected difiere, otra estación se apoderó de la sesión.

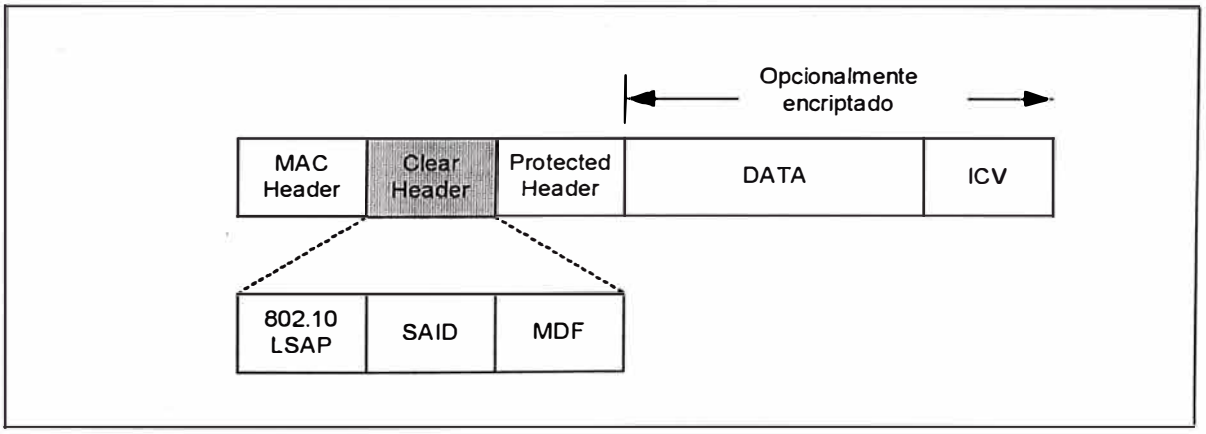


Figura 4-19 Encapsulación 802.10.

La figura 4-19 muestra tres campos en la porción de cabecera Clear. Unicamente el campo Security Association Identifaer (SAID) es relevante para las VLANs. Adedmás, los otros dos campos (802.10 LSAP y MDF) son ignorados en esta discusión. El campo SAID usado por Cisco identifica la fuente VLAN. Los cuatro bytes SAID permite a muchos VLANs identificarse ne la red FDI.

4.4.3.- ATM Trunks

La tecnología Asynchronous Transfer Mode (ATM) tiene una capacidad inherente para transportar, voz, video y data sobre una misma infraestructura. Y por que ATM no tiene un distancia dee dominio de colisión como la tecnología LAN. ATM ofrece a los usuarios la oportunidad de desarrollar una infraestructura suitable consolidando que son redes independientes tradicionales. Por ejemplo, algunas compañías tienen una infraestructura ded voz privada entre la corporación y las oficinas remotas. Los negocios dedjan que los servicios T1 y E1 interconecten PBX entre oficinas. La compañía pude desarrollar una red separada para transportar data entre oficians. Y finalmente, para soportar video conferencia, es instalado un servicio ISDN. Cada uno de estas redes es un propio requerimiento de equipos y costos. Consolidando todos los servicios dentro de una red ATM, la infraestructura compleja se reduce. Y mejor aún los costos se reducen.

Para las instalaciones donde ATM provee un servicio Backbone, los usuarios puden tomar ventaja de la infraestructura ATM para trunk entre catalyst. Insertando un módulo LANE en el cátalyst, este pude enviar y recibir tramas de data sobre la red ATM. El catalyst bridge el tráfico LAN dentro de la red ATM para transportar las tramas (segmentado en celdas por el módulo LANE) a través del sistema ATM y recibir por otro catalsyt o router ATM.

Los catalyst soportan dos modos de transporte de data sobre redes ATM: LANE y MPOA. Cada uno .

Lane.- LANE emula redes ethernet y token ring sobre ATM. Emulando ethernet o token ring sobre ATM define un Emulated LAN (ELAN). Un miembro del ELAN is referido como un LANE Client (LEC). Cada ELAN es un dominio dee broadcast independiente. Un LEC puede belong a únicamente un ELAN. Ambas redes ethernet y token ring son descritos como redes broadcast; si una estación genera un mensaje broadcast, todos los componentes en la red recibe una copia de la trama. La redes ATM , por otro lado, crea una conexión punto-a-punto entre usuarios. Esto crea un problema cuando un cliente transmite una trama broadcast. Crear ELAN a todos los miembros sería una solución impractica debido a la cantidad de conexiones virtuales que necesita establecer aún en una red moderadamente mediano. Besides, un cliente no necesariamente conoce acerca de los demás clientes en la Red. LANE provee una solución,

definiendo un servidor especial responsable de distribuir el broadcast dentro de una ELAN.

En la figura 4-20, tres catalyst y un router interconectan sobre una red ATM. En el lado LAN, cada catalyst soporta tres VLANs. En el lado ATM, cada catalyst tiene tres liente para ser miembros de tres ELAN.

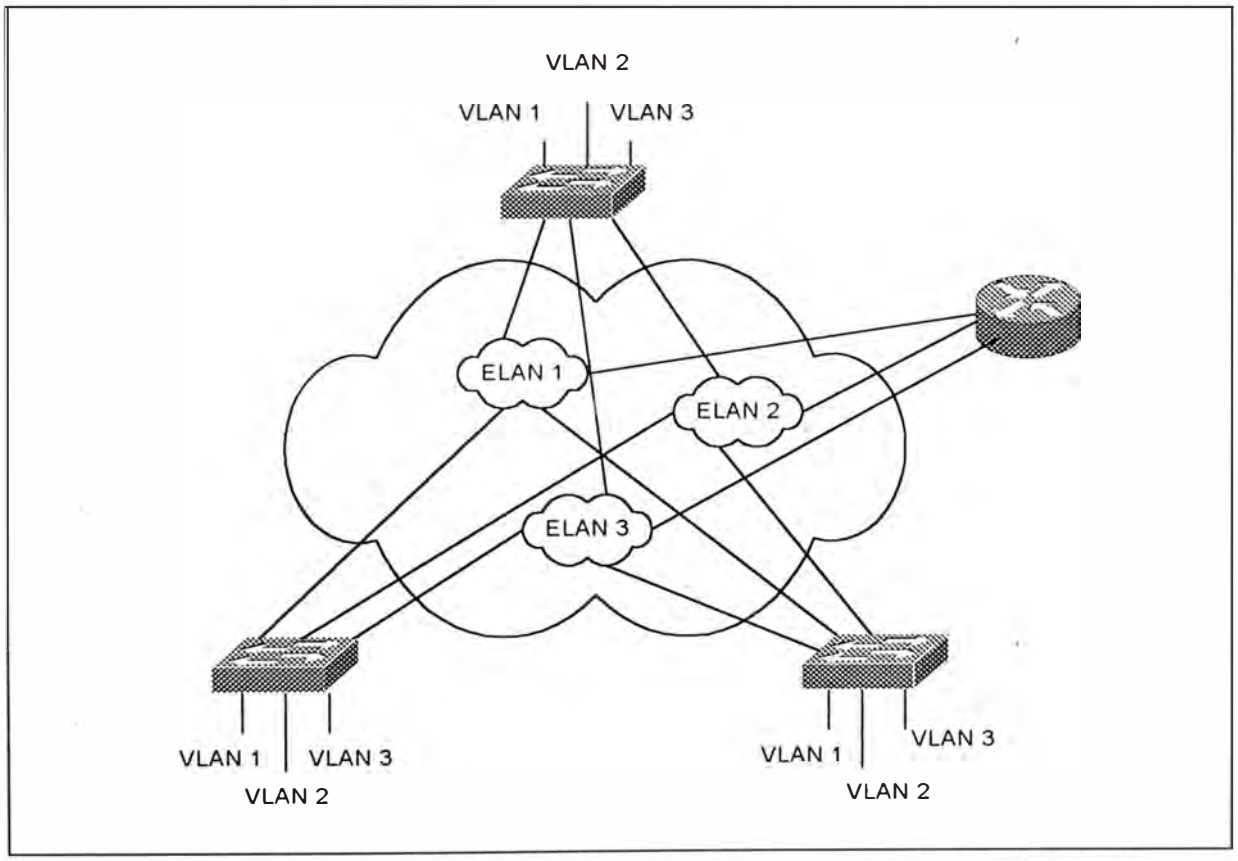


Figura 4-20 El Catalyst en un ambiente LANE adjunto a tres ELAN.

Dentro de cada configuración de catalyst, cada VLAN mapea a un ELAN. Este merge el dominio de broadcast para que las VALN distribuidas puedan intercomunicar sobre la red ATM. La figura 4-21 muestra

una dedpiction lógica del mapeo VLAN a ELAN que ocurre dentro del catalyst.

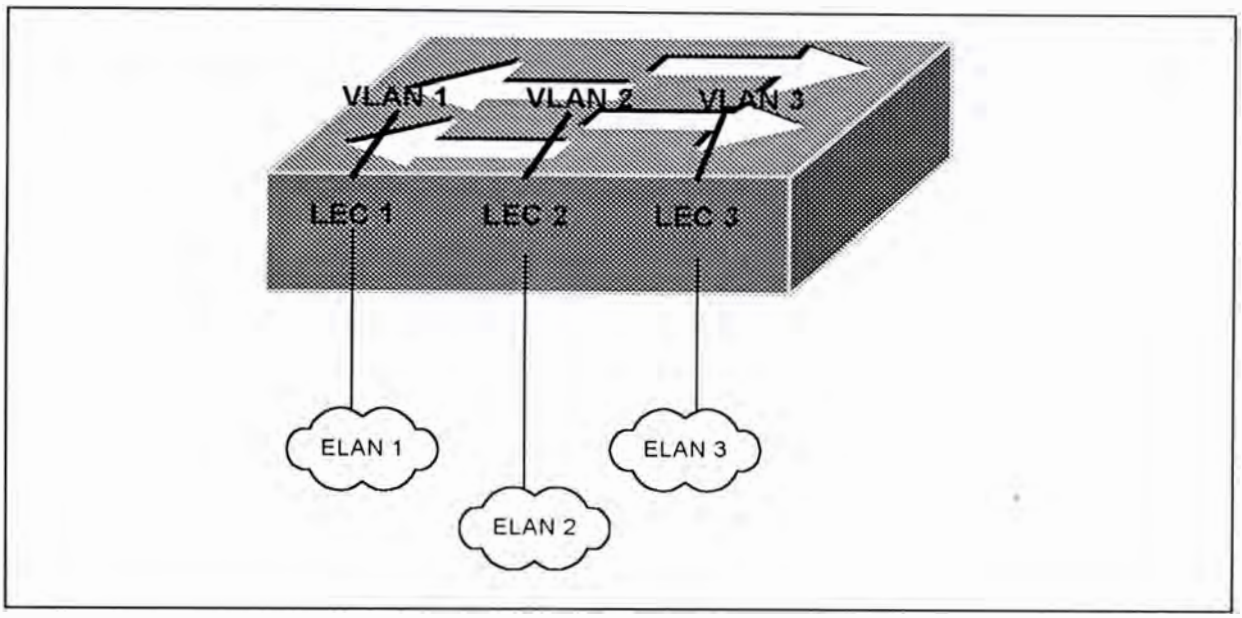


Figura 4-21 Un Catalyst con tres LEC´s configurados para adjuntar tres ELAN´s.

Necesitamos el router mostrado en la figura 4-20 si es que una estación en una VLAN desea comunicar con otra estación en otra VLAN. El router puede reside en el lado LAN del catalyst, pero este ejemplo ilustra al router en el lado ATM. Cuando una estación en la VLAN 1 intenta comunicarse con una estación en la VLAN2, el catalyst bridge la trama fuera del LEC 1 hacia el router. El router, el cual también tiene tres cliente, rutea la trama al LEC el cual es miembro de la ELAN 2 hacia el catalyst destino. El catalyst dedstino recibe la trama en el LEC 2 y bridge la trama al puerto VLAN correcto.

MPOA.- En la mayoria de redes, muchos routers interconectan subrededs. Únicamente en al rede mas pequeña el router es miembro de todas las

subredes. En grandes redes, además , la trama puede atravesar múltiples routers para conseguir el destino intentado. Cuando esto ocurre en una red ATM, la misma información viaja a través de la nube ATM tantas veces como saltos Inter.-router hay. En la figura 4-22 una estación en la VLAN 1 adjunto al Cat A desea comunicarse con la estación en la VLAN 4 en el cat-B. Normalmente, la trama existye del cat-A hacia el router 1, el default gateway. El router 1 envía la trama al router 2, el cual envía la trama al router 3. El router 3 transfiere la trama al destino cat-B. Este es el default path y requiere cuatro transferencias a través de la red ATM, un muy ineficiente uso del ancho de banda. Este es frustante por que la red ATM puede crear un circuito virtual directamente entre el cat-A y Cat-B. .

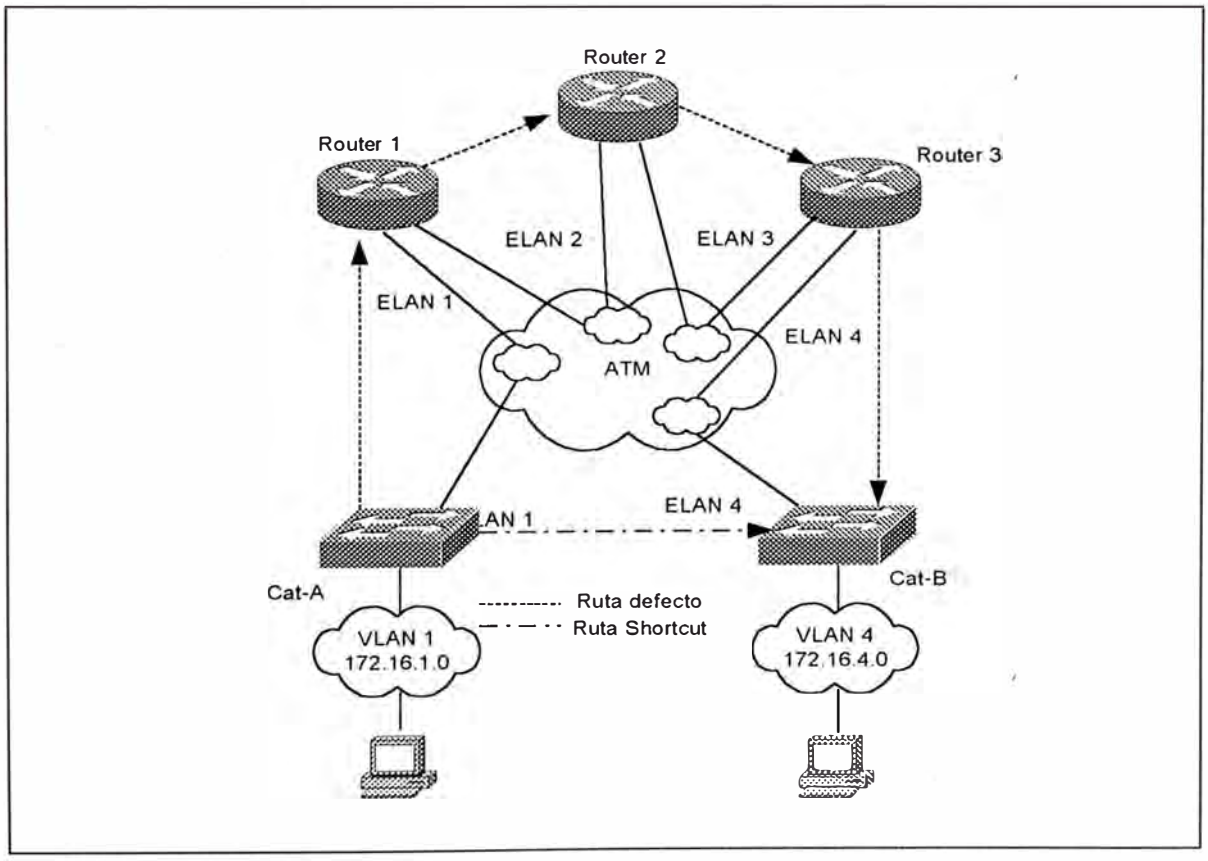


Figura 4-22 Un Ctalayst en un ambiuente MPOA.

MPOA habilita a los dispositivos circunvent el default path y establecer una conexión directa entre los dispositivos, even though tie belong to different subnets. Esta ruta corta ilustrada en la figura (pag 335 lans), elimina los múltiples tránsitos del default path conservando el ancho de banda ATM y reduciendo el retardo dee transito overall.

MPOA no reemplaza al LANE, pero si lo suple. En realidad, MPOA requiere LANE como uno de sus componentes. Las comunicaciones de dominio intra-broadcast (transferencia dentro de una ELAN) usa LANE, MPOA kicks in únicamente cuando estaciones de diferente ELAN intentan comunicarse con cada uno. MPOA, podría no siempre get involved. Una razón es que MPOA es dedependiente de protocolo. Actualmente IP es le protocolo dominante soportado. Para que MPOA solicite un shorcut, el MPOA cliente tiene que detectar suficiente tráfico entre los dos host para merit cualquier esfuerzo por shorcut. Esto es determinado por un therhold configurable administrativamente o paquetes por secundo entre las dos estaciones. Si el cliente detecta una razon de un paquete por segundo entre la fuente IP y un IP de destino mas grande que el threshold configurado, el cliente intenta crear un shorcut para el IP de destino. Pero si los paquetes por segundo nunca exceden el threshold, las tramas continúan el viaje a través de la ruta por default.

4.5.- SWITCHING CAPA 3

Muchos factores han creado confusión con la terminología switching capa 3. Algunos de estos bewildement llegan de muchas tecnologías recientemente emergientes. En el pasado, los switches y routers han sido dispositivos separados y distintos. El término switch fue reservado para plataformas basados en hardware, que generalmente funcionabanen capa 2 del modelo OSI. El término router ha sido usado para referirse a dispositivos que corren protocolos de enrutamiento para decubrir toplogías capa 3 y hacer descisiones de envío basados en direcciones de capa 3. Debido a lo complicado de esto, los routers han sido dispositivos basados en software.

El término switching capa 3 cubreuna amplia variedad de técnicas que seek para mostrar los beneficios de estas tecnologías previamente separadas. La clave es capturar la velocidad del switching y la escalabilidad del routing. En general, las técnicas del switching capa3 pueden ser agrupados en dos categorias.

- Routing switches
- Switching routers

Como una categoria broad, los routing swtiches usan hardware para crear rutas cortas a través del middle de la red, baypasing el tradicional router basado en software. Algunos routing switches han sido referidos como un router acelerador. Los routing switches no corren protocolos de enrutamiento

tales como OSPF ó EIGRP- En vez de eso, ellos utilizan varias técnicas para descubrir, crear, o capturar informacion de shorcut.

A diferecia de los routing switches, los switching routers si coren protocolos de enrutamiento tales como OSPF. Estas operaciones son típicamente ejecutadas en el CPU de propósito general como con una plataforma de router tradicional. Sin embargo, a diferencia de los routers tradicionales que utilizan CPU de propósito general para funciones de control-plane y data-plane, Los switches capa 3 usan circuitos integrados específicos para aplicaciones de alta velocidad (ASIC´s) en el dta plane. Removiendo el uso del CPU desde la ruta de data-fordwarding, se puede obtener una performacia igual a la velocidad física. Esto resulta en una versión mucho 2as rápida de un router tradicional. Aunque el término routing switch y switching router parecen ser próximos, los términos son actualmente muy descriptivos de algunos sutiles diferencias entre estos tipos de dispositivos.

4.5.1.- Router-on-a-Stick

Los diseños tempranos de VLAN relied en routers conectados a VLA-capable switches, tal como se muestra en la figura 4-23. En este aproach, los routers tradicionales son conectados via un o mas enlaces a la red switched. La figura anterior muiestra un único enlace, el stick, conectando el router al resto de la red acmpus. El tráfico inter VLAN tiene que cruzar el backbone de capa 2 para alcanzar el router donde este puede moversse entre VLAN´s. Este luego viaja de regreso a la estacion final deseada,

usando forwarding de capa 2 normal. Este flujo "out to the router and back" es característico de todo diseño router-on-a-stick.

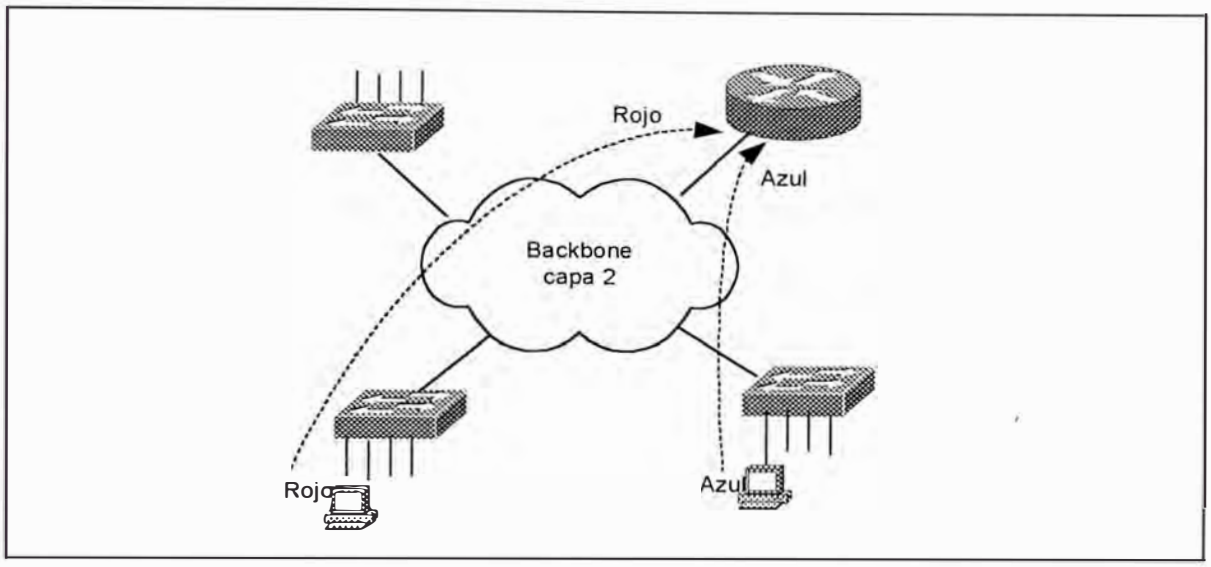


Figura 4-23 Diseño de un Router-on-Stick.

La figura 4-23 muestra la conexión del router en un sentido general. Cuando se discute opciones específicas para enlazazr a una red switcheada, dos alternativas son disponibles:

- One-link-per-VLAN
- Trunk-connected router

One-link-per-VLAN.- Una de las técnicas tempranas para conectar una red switcheada a un router, fue el uso ded one-link-per-VLAN como mostrado en la figura 4-24.

En este caso, las redes switcheadas llevan tres VLANs: Rojo, Azul y Verde. Troncales ISL (inter Switch Link) son usados para conectar los

tres switches juntos, permitiendo un único enlace para llevar las tres VLANs. Sin embargo, las conexiones al router usa un enlace separado para cada VLAN. La figura 4.24 ilustra el uso de puertos deel router de 10 Mbps, sin embargo, pueden ser usados otros medios como Fast Ethernet, Gigabit Ethernet, ATM o FDDI.

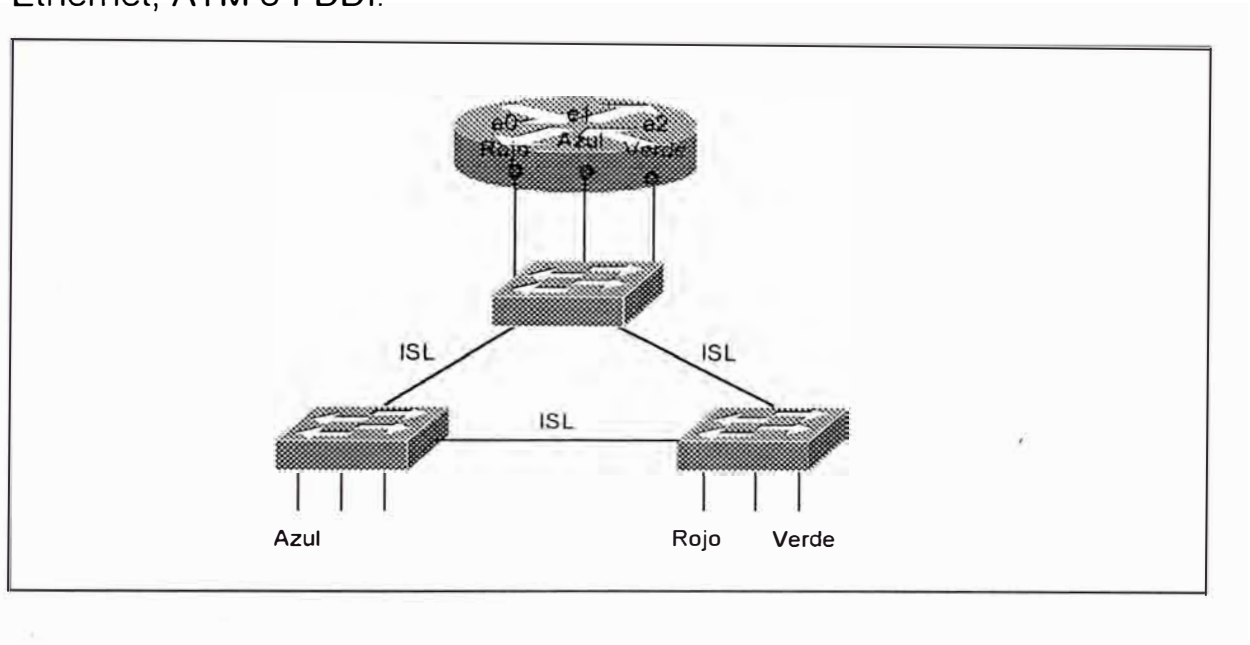


Figura 4-24 Diseño de un One-per-VLAN.

Hay muchas ventajas para usar un one-link-peer-VLAN:

- Permite que los equipos existentes sean redepolyed en una infraestructura switcheada, con el consecuente ahorro de dinero.
- Es simple de entender e implementar. Los administradores de red no tienen que aprender cualquier concepto nuevo o comandos de configuración para aplicar el one-link-peer-VLAN.
- Por que esto relies múltiples interfaces, este puede proveer alta performance.

Notar además que cada interface del router es ajeno a la infraestructura VLAN (ellos son puertos de acceso). Esto permite al router utilizar su procesamiento normal para mover paquetes entre VLAN´s. En otras palabras, no hay procesamiento adicional u "overhead".

Aunque hay ventajas en el diseño, también sufre de muchos aspectos críticos:

- Este puede requerir mas interfaces. En efecto, esto limita al "one-link-per-VLAN" a llevar menos que 1 VLAN. Intentar este modelo en redes que llevan 15 o mas VLANs es generalmente no factible debido a limitaciones de costo y densidad de puertos.
- Aunque esto puede inicialmente ahorrar dinero, debido al reuso de equipos existentes. Esto puede llegar a ser muy costoso a medida que el número de VLANs crece en el tiempo. Hay que tener presente que cada VLAN requiere un puerto adicional tanto en el router como en el switch.
- Puede ser dificil mantener la red a través del tiempo. Aunque el diseño "one-link-per-VLAN" puede ser simple para la configuración inicial, puede llegar a ser muy embarazoso a medida que el número de VLANs crece.

"Trunk-connected Router".- Como las tecnologías tales como ISL llegan a ser comunes, los diseñadores de red inician el uso de enlaces troncales para

conectar los routers al backbone campus. La figura 4-25 ilustra un ejemplo de esto.

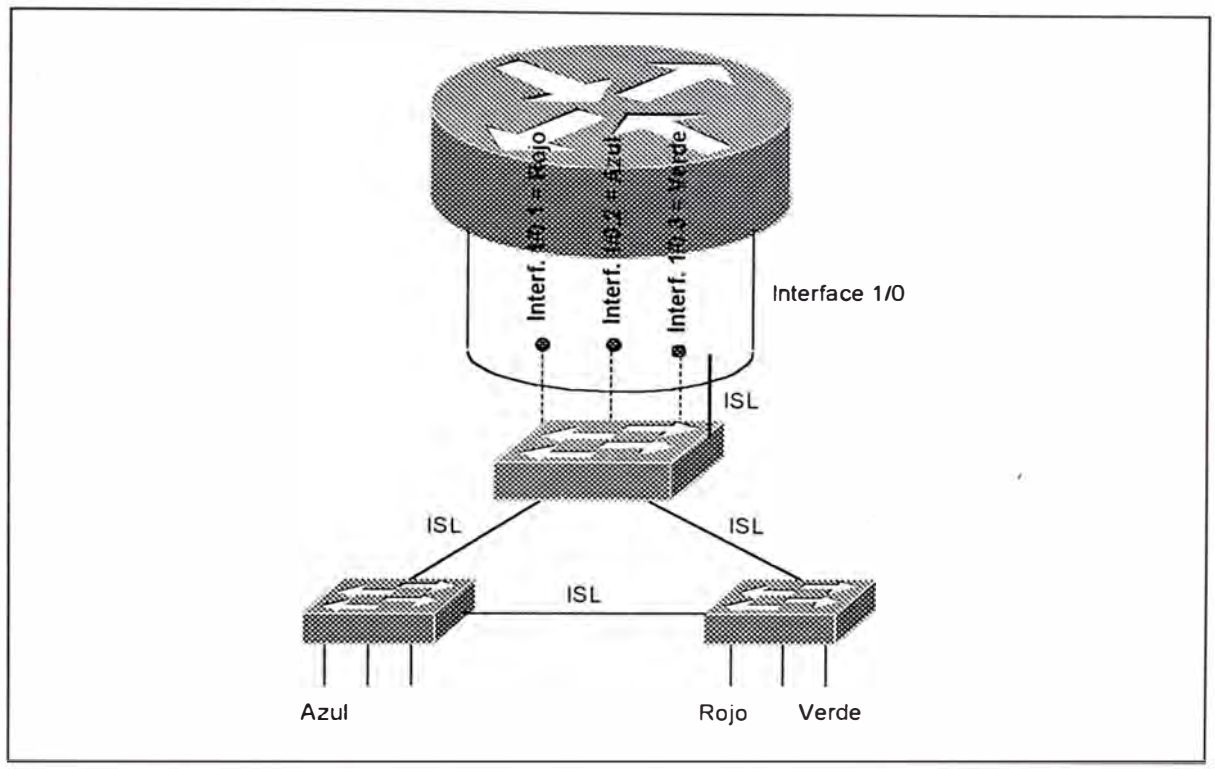


Figura 4-25 Router conectado con Trunk´s.

Aunque cualquier tecnología truncal tales ISL, 802.1Q, 802.10, LAN Emulation (LANE) o MPOA puede ser usado. El aproach basado en ethernet son mas usados (ISL y 802.1Q).. La figura pag 457 lans usa ISL corriendosobre Fast Ethernet. Las líneas sólidas se refieren a un único enlace físico cooriendo entre el Catalyst y el router. Las líneas punteadas se refiere a los multiples enlaces lógicos corriendo sobre este enlace físico.

La primera ventaja de usar enlaces troncales es la reducción de puertos en el router y el switch, permitiendo un ahorro de dinero y

disminuyendo la complejidad de la configuración. Consecuentemente los routers conectados a troncales, pueden escalar a redes con mas VLANs que el diseño one-link-peer-VLAN.

Sin embargo hay desventajas para la configuración del router conectado a troncal, incluyendo lo siguiente:

- Inadecuado ancho de banda para cada VLAN
- Adiconal overhead en el router
- Versiones antiguas de IOS únicamente soportan un conjunto limitado de características en las interfaces ISL.

Con el inadecuado ancho de banda para cada VLAN, considere por ejemplo el uso de enlaces Fast Ethernetdonde todas las VLANs tiene que compartir 100 Mbps de ancho de banda. Un único VLAN podria fácilmente consumir la capacidad entera del router o los enlaces.

Con el adicional overhead en el router causado por usar rouiter conectado a troncal, no únicamente el router tiene que llevar a cabo enrutamiento normal y forwardeo de data, este tiene manipular encapsulación adicional usado por el protocolo troncal.

La tercera desventaja de usar verisones antiguas de IOS únicamente soporta un limitado conjuntoi de características en las interfaces ISL. Aunque la mayoria de limitaciones fueron removidas de versiones 11.3 y

algunos anteriores como la imagen 11.2, las redes usando images antiguas necesitan cuidadosamente planear el enrutamiento inter VLAN en su red. Algunas de las limitaciones mas siginificantes prior a la imagen 11.3 son:

- Soporta únuicamente IP e IPX. Todos los otros protocolos (Apple Talk y DECNet) tiene que ser bridged. Inter-VLAN bridging es casi siempre una mala idea.
- IPX únicamente soporta la encapsulación novell-ether (Novell se refiere a esto como Ethernet 802.3)
- HSRP no es soportado. Este puede hacer muıy difícil o imposible proveer defaul gateway redundante.
- Direcciones IP secundarias no son soportados.

4.5.2.- Routing Switches

Multilayer Switches (MLS) es una tecnología routing Switch basado en Ethernet dee Cisco. >El MLS es actualmente soportado en dos plataformas: El catalyst 5000 y el catalyst 6000.. El Catalyst 5000 hace uso del NetFlow Feature Card (NFFC) I o II para proveer enrutamiento asistido en hardware. El Ctalyst 6000 lleva a cabo la misma operación usando el Multilayer Switch Feasture Card (MSFC) en conjunto con el Policy Feature Card (PFC).

En el sentido mas básico, el NFFC es un pattern-matching engine. Este permite al Catalyst reconocer a una amplia variedad de

diferentes paquetes. Machando varias combinaciones de direcciones y números de puertos, la forma de routing switch de switching capa 3 puede ser llevada a cabo. Sin embargo, un host de otras características son también posible. Machando el tipo dee protocolo capa 3, una característica llamada Protocolo Filtering es implemantado. Machando paquetes Internet Group Management Protocolo (IGMP) , se puede llevar a cabo el IGMP Snooping para dinámicamente construir tablas de forwardeo multiccast eficiente. Finalmente, machando información QoS y COS de capa 2 y capa 3, se puede llevar cabo clasificación ded tráfico y diferenciación.

Una de las mas importantes cosas de mantner en mente cuando se discute MLS es que, como todo mecanismo de switching shorcut, esta es una técnica caching. El NFFC no corre ningun protocolo tales como OSPF, EIGRP o BGP.

Es importante realice que MLS, conocido como NetFlow LAN Switching, es un mecanismo completamente diferente que el NetFlow Switching en los routers basadfos en software de Cisco. En su implementación reciente, NetFlow en los routers es apuntado como una poderosa herramienta de colección de data vía NetFlow Data Export (aunque esto también puede ser usado para reducir el overhead asociado con cosas como listas de acceso complejas) .

Debido a que el NFFC no corre ningun protocolo de enrutamiento, este tiene que rely en su capacidad de macheo de patrones para descubrir paquetes qye han sido enviados a un router y luego enviado de regreso al mismo Catalyst. Esto permite al NFFC shorcut futuros paquetes en una manera que bypass el router. En efecto, el NFFC nota que este envía un paquete particular al router, únicamente para que el router lo envíe de regreso. Este luego empieza a shorcuting todos los paquetes siguiendo la misma ruta.

Teoría de Operación del MLS.- El MLS hace uso de tres componentes: MLS Route Processor (MLS-RP), el MLS Switching Engine (MLS-SE) y el Multilayer Switching Protocolo (MLSP). El MLS-RP actua como el router en la red (notar que mas que uno puede ser usado). Este dispositivo manipula el primer paquete en cada flujo, permitiendo que el MLS-SE construya entradas shorcut en una tabla CAM capa 3. El MLSP es un protocolo ligero usado por el MLS-RP para inicializar el MLS-SE y notificar cambios en la topología capa 3 o requerimientos de seguridad. Por simplicidad, nos referiremos al MLS-RP como le router y el MLS-SE como el NFFC.

MLS usa un proceso de cuatro pasos:

- Paso 1 Paquetes Hello MLSP son enviados por el router
- Paso 2 El NFFC idientifica los paquetes candidatos
- Paso 3 El NFFC identifica paquetes habilitados
- Paso 4 El NFFC shorcut paquetes futuros.

A continuación describiremos cada uno de estos pasos usando el la red mostrado en la figura 4-26

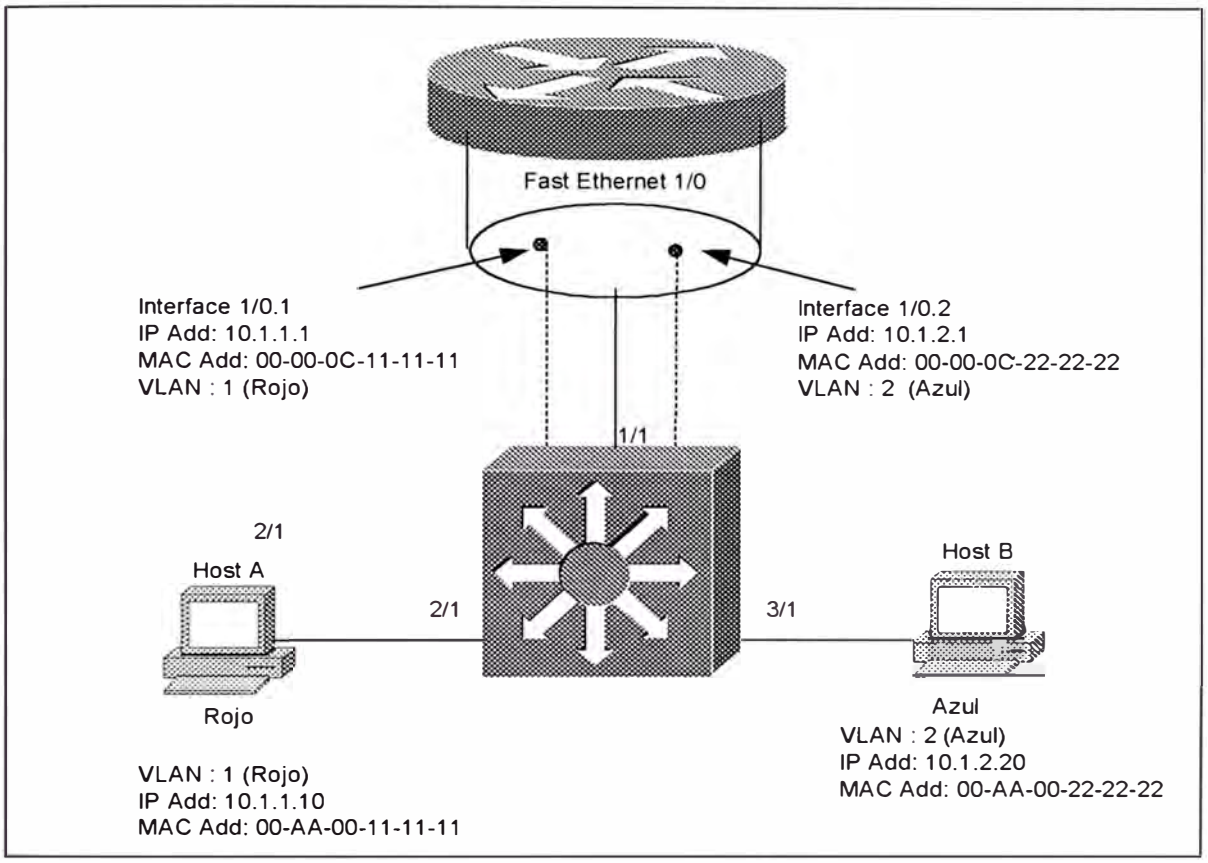


Figura 4-26 Ejemplo de una Red MLS.

Esta red consiste en dos VLANs, la VLAN 1 (Rojo) y la VLAN 2 (Azul). Las dos estaciones finalesson mostrados. El Host-1 ha sido asigando a la VLAN Rojo y el Host-2 a la VLAN Azul. Un router adjunto con un ISL también ha sido incluido. Su único interface Fast Ethernet (Fast Ethernet 1/0) ha sido lógicamente particionado en dos subinterfaces, uno por VLAN. Las direcciones IP y MAC para cada subinterface son mostrados.

- Paso 1: Paquetes hello MLSP son enviados por el router.- Cuando el router bootea, este comienza enviando paquetes hello MLSP cada 15

segundos. Estos paquetes contiene información en la VLAN y direcciones MAC en uso en el router. Escuchando estos pquetes hello, el NFFC puede aprender los atributos de cualquier router MLS_capable en la rede capa 2. El NFFC asocia un único valor XTAG con cada router MLS que este identifica. Debido a que los hello MLSP son periódicos , ello permite a los routers y catalyst bootear a tiempos aleatorios, mientras también sirven como un mecanismo de router keepalive para el NFFC. La figura 4-27 ilustra el proceso MLSP.

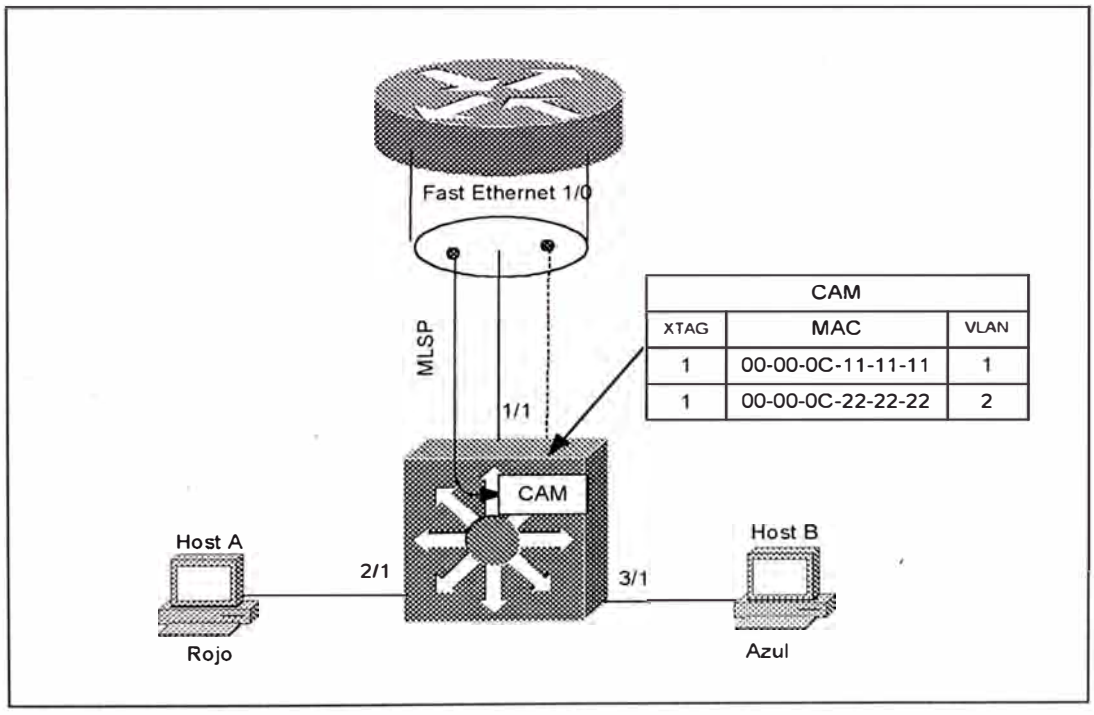


Figura 4-27 Proceso Hello MLSP.

Como mostrado en la figura anterior, los paquetes MLSP son sourced desde la subinterfaces Fast Ethernet 0.1 en el router. Estos paquetes son luego usados para populate la tabla CAM capa 2 con

entradas especiales que son usados para identificar paquetes que van o vienen de una interface de un router. Cada router es asigando un único valor XTAG. Si un segundo router fuera presentado en la figura pag 471 lans , este debería recibir un valor diferente XTAG al 1 asigando al primer router. Sin embargo notar que todas las MAC address y VLANs para un único router son asociados con un simple valor XTAG.

- Paso 2: El NFFC identifica Paquetes Candidatos.- Después que el paso 1 ha permitido que el NFFC adquiera las direcciones dee los routers MLS_capable, el NFFC inicia el uso de su capacidad de machar patrones para buscar paquetes que son destinados a estas direcciones. Si un paquete es encabezado al router y no tiene una entrada shorcut existente, este es clasificado como un paquete candidato. El paquete usa el normal proceso de forwardeo capa 2 del Catalyst y consigue salir al puerto conectado al router.

  Por ejemplo, si nos referimos a la figura 4-27 y asume que el Host-A Telnets al Host-B. Reconociendo que el Host-B esta en uan subnet diferente, el Host-A envía los paquetes a su defaul gateway, la suginterface 1/0.1 en el router.

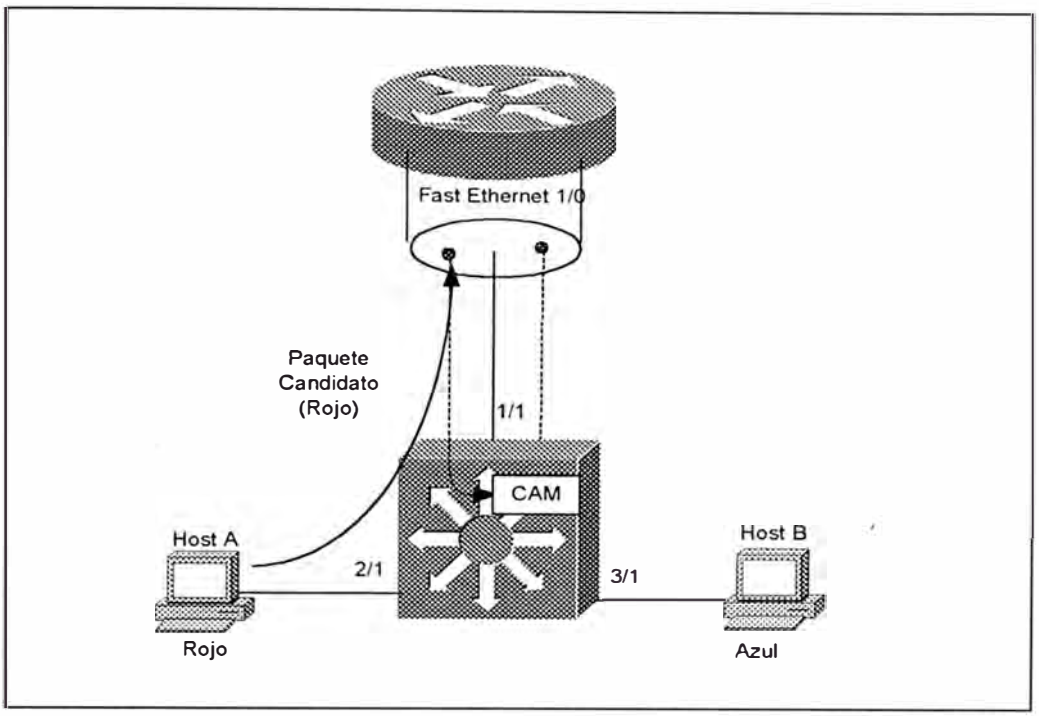


Figura 4-28 Un paquete cadidato.

La figura 4-29 ilustra los campos relevantes en este paquete cuando este atraviesa el enlace ISL al router.

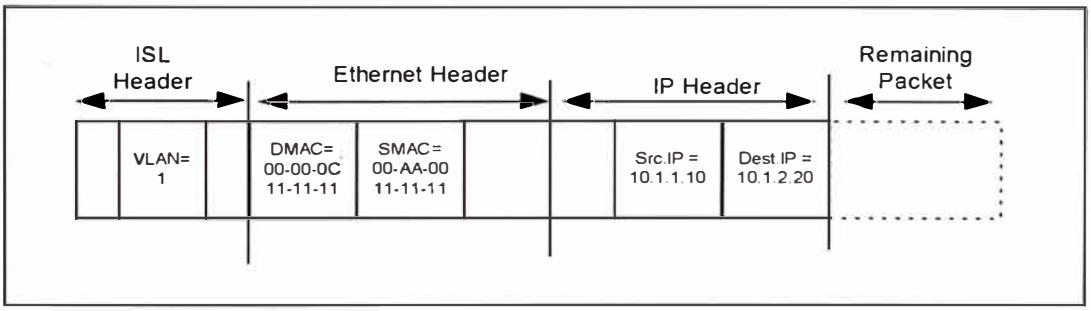


Figura 4-29 Campos de un paquete candidato.

La cabecera ISL contiene una VLAN IP de 1. La cabecera Ethernet contiene una dirección fuente MAC igual al Host-A y una direccion destino igual a 00-00-0C-11-11-11, que es la MAC address dee la subinterface del router. La dirección fuente y destino del Host-

A y Host-B respectivamente. El switch usa la dirección MAC de destino para llevar a cabo dos acciones:

1. Envía el paquete fuera del Puerto 1/1 hacia el router usando el "switching capa 2"
2. Reconoce la dirección MAC destino como una de las direcciones del router aprendidas en el Paso 1. Este busca una entrada rápida de capa 3 basado en la dirección IP de destino.

- Paso 3: El NFFC Identifica Paquetes Habilitados.- El router recibe y rutea los paquetes normalmente. Reconociendo la dirección de destino como estando directamente conectado a la subinterface Fast Ethernet 1/0.2, el router envía el paquete de regreso a través del enlace ISL encapsulado en la VLAN 2 como ilustrado en la figura 4-30.

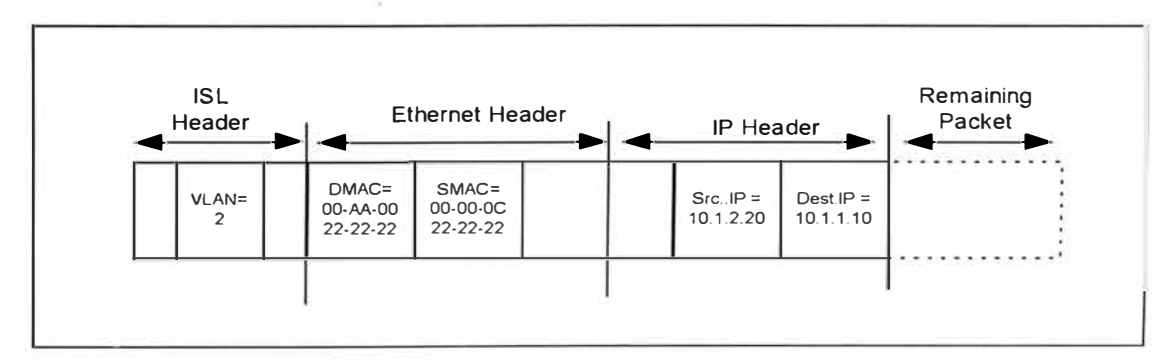


Figura 4-30 Campos de un paquete Enable.

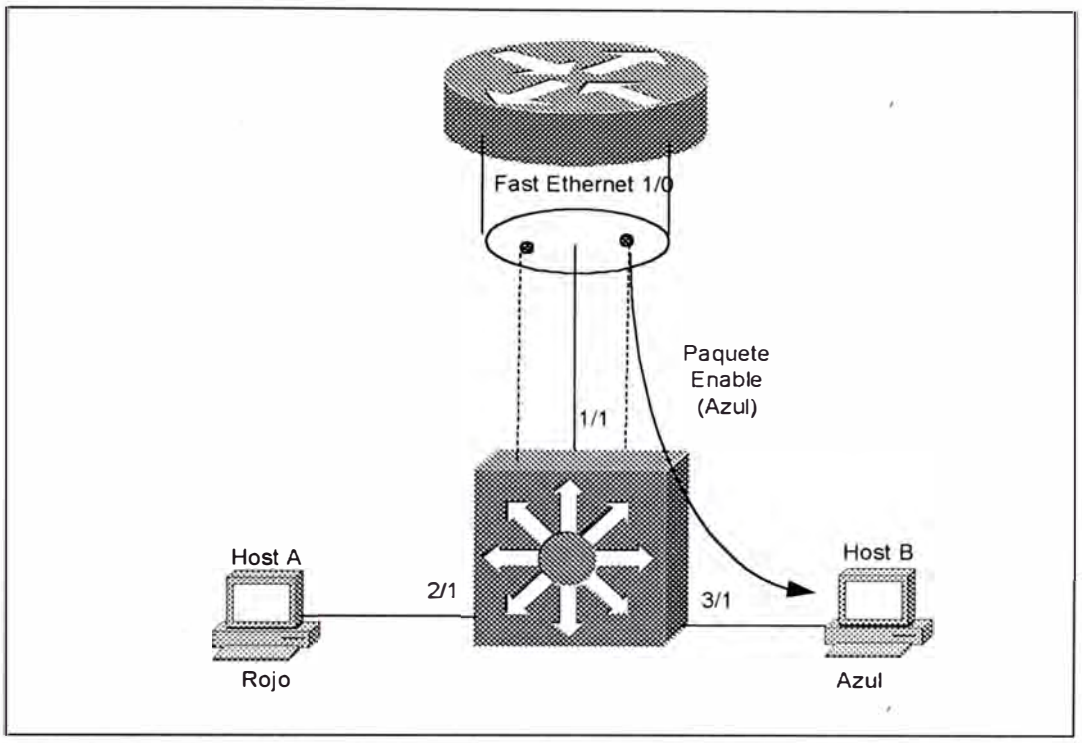


Figura 4-31 UN paquete Enable.

El router ha reescrito la cabecera de capa 2. No únicamente ha cambiado el número dee VLAN en la cabecera ISL, este ha modificado ambas direcciones MAC. La dirección MAC fuente ahora es igual a 00-00-0C-22-22-22, la dirección MAC usada en la subinterface Fast Ethernet 1/0.2 del router, y la dirección de destino es configurado al Host-B. Aunque las direcciones IP no han sido cambiados, el router tiene que mofdificar la cabecera IP por dedcrementar el campo Time to Live (TTL) y actualizaz el checksum.

Como el paquete atraviesa el catalyst en su forma desde el router al Host-B, cinco funciones son llevadas a cabo:

1. La dirección MAC destino es usado para switchear en capa 2 los paquetes fuera del puerto 3/1.
2. El NFFC reconoce la dirección MAC fuente como uno de las entradas creadas en el paso 1 via el proceso hello.
3. El NFFC usa la dirección IP de destino para observar la entrada shorcut parcial existente creada en el Paso 2
4. El NFFC compara el valor XTAG asociado con la dirección MAC fuente de este paquete y la entrada shorcut parcial. Debido a que ellos machan, el NFFC sabe que este es un paquete habilitado viniendo dedsde el mismo router apuntado por el paquete candidato.
5. El NFFC completa la entrada shorcut. Esta entrada contendría toda la información necesaria para rescribir la cabecera de futuros paquetes.

- Paso 4: El NFFC shorcut futuros paquetes.- Como futuros paquetes son enviados por el Host-A, el NFFC usa la dirección de destino IP para observar la entrada shorcut completa creada en el paso 3. Encontrando un mach, este usa un rewrite engine para modificar la informaciónd ecabecera necesaria y luego enviá el paquete directamente al Hos-B. La operación de rewrite modifica todos los mismos campos que inicialmente modificó el router para el primer paquete. Desde las perspectiva del Host-B, este no tiene idea que el

NFFC ha interceptado el paquete. La figura 4-32 lans ilustra la operación.

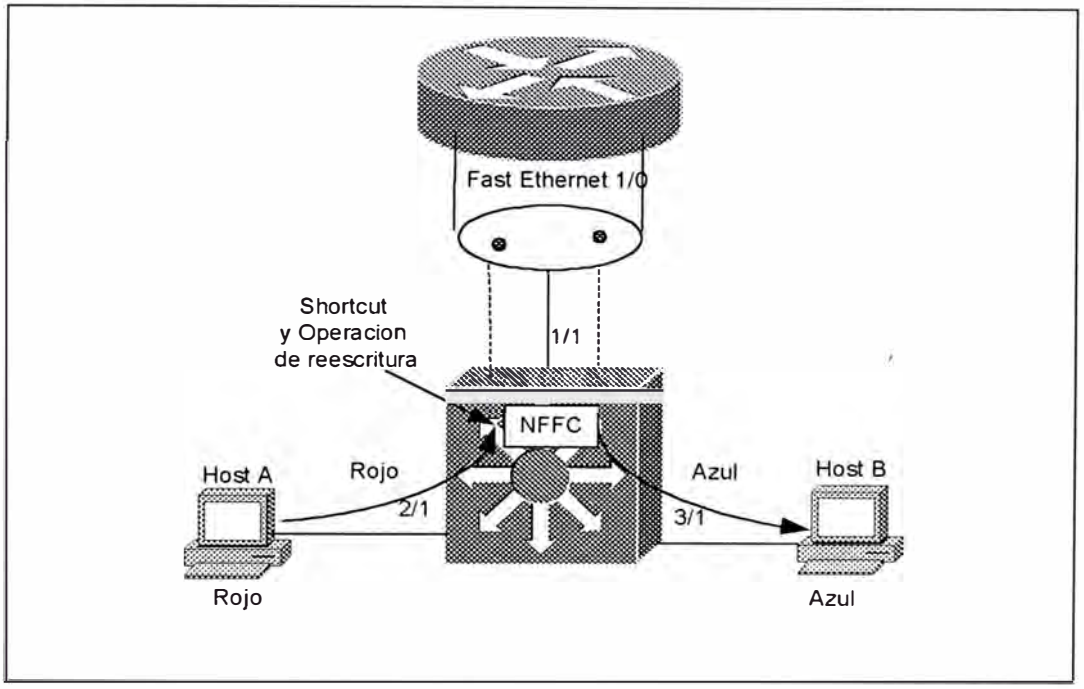


Figura 4-32 Un paquete Shorcut.

El mecanismo de rewrite puede modificar los siguientes campos:

1. Direcciones MAC fuente y destino
2. VLAN ID
3. TTL
4. Encapsulación (Por ejemplo , ARPA, SNAP)
5. Checksum
6. ToS COS

Cuando Usar MLS.- MLS´s asistido por hardware para enrutamiento, puede ser muy usual cuando tecnicas como router on-a-stick no tiene suficiente capacidad. En realidad, uno de los beneficios de MLS es que este puede ser

fácilmente adicionado a una red existente para turbocargar la performance de enrutamiento. Además, el argumento mas común para usar MLS es el throughput. Las capacidades adicionales del NFFC para manipular task tales como Protocol Filtering, IGMP Snooping, NetFlow data collection, y QoS pueden hacer del MLS un opción mas atractiva que simplemente usar esto para obyener un enrutamiento rápido.

4.5.3.- Switching Router

Mientras MLS relise en caching basado en hardware para lleva r a cabo switching shorcut, el Catalyst 8500 relies en hardware para llevar a cabo el mismo task como un router tradicional, únicamente mas rápido. Para acomplish el extremadamente alto throughput requerido en modernos backbone campus , el 8500 split enrutamiento dentro de dos grupos funcionales. El trabajo ded correr protocolos de enrutameinto tales como OSPF e IGRP para propósitos de descubrir topologías y determinación de rutas son manipuladas por un propósito general, CPUs basados en RISC. El trabajo dee hacer tabla de enrutameinto forwardeo ded data es manipulado por ASIC´s de alta velocidad. Combinado, esto crea una plataforma muy rápida pero de caracteristica rica y flexibilidad.

En el caso del Catalyst 8510, el primer switching router ded Cisco apuntó al mercado campus, la función de enrutamiento son llevadas a cabo por el Switch Route Processor (SRP). Desde una perspectiva de hardware, el SRP es esencialmente lo mismo como el ATM Switch

Processor (ASP) desde un Lighstream 1010ATM. Sin embargo mejor que correr protoclos de enrutameinto ATM tales como PNNI, el SRP es usado para correr protocolos de enrutameinto de datagramas tales como RIP y OSPF.

Después que el protocolo de enrutameinto ha sido usado para construir una tabla de enrutameinto, el CPU usa esta información para crear lo que es llamado una tabla Cisco Express Forwarding (CEF) . Como la tabla de enrutameinto lista todas las ubicaciones posibles, este router puede llevar paquetes. La tabla CEF contiene una entrada indicando como alcanzar cada ubicación conocida en la red. Sin embargo, a diferencia de una tabla de enrutameinto, el cual es limitado a información muy básica tal como ruta de destino, next hope, y métricas de enrutamiento, la tabla CEF puede ser usado para almacenar una variedad de información que corresponde a características tales como Queuing y QoS/COS. Además, debido a que esto es almacenado en un formato que provee longest-match extremadamente eficiente, este es muy rápido. El CEF llena la competente finalidad de velocidad y funcionalidad, y representa un importante paso de avanzada a tecnologías de enrutamiento. Cisco ha estado usando CEF con gran satisfacción en sus plataformas de enrutamiento orientados a internet.

Aunque el concepto básico de CEF es disponible a través de la línea de productos de Cisco, el 8510 introdujo un nuevo uso de esta tecnología. El CPU ubicado en el SRP es usado para crear la tabla CEF,

tecnología. El CPU ubicado en el SRP es usado para crear la tabla CEF, pero este no es usado para hacer descisiones de forwardeo. En vez de eso, el CPU descarga una copia de la tabla CEF a cada tarjeta de línea. Las tarjetas de línea luego contiene ASICs que llevan a cabo el actual CEF lookup a velocidades físicos. Desde el punto de vista de los puertos de ingreso en el 8510, este tiene un bunch de circuitos virtuales que conectan a cada puerto en la caja. Podeemos pensar que estos circuitos Virtuales VCs son como tubos que el puerto de entrada puede usar para enviar data a cada puerto de salida. El resultado es un mecanismo que usa un conjunto distribuido de ASICs de alta velocidad para manipular los resources, intensive el proceso de deeterminar como mover las tramas a través de la caja.

El 8540, que es el siguiente switching router de Cisco, usa la misma técnica ppero con diferente hardware. La diferencia principal es un conjunto nuevo de tarjetas de línes y un chasis mas grande qúe soporta mas interfaces y un backplane/fabric de alta velocidad. En el 8540 , un único SRP del 8510 ha sido aplit dentro del Route Processor (RP) y el Switch Processor (SP). El RP manipula funciones tales como correr protocolos de enrutameinto y construir tablas CEF. La tarjeta de línea aún contine ASICs que usa una copia local de la tabla CEF para hacer descisiones dee forwardeo.. Sin embargo, para mover data a través del backplane/fabric, las tarjetas de línea tiene que usar el servicio del SP.

4.5.4.- El Hot Standby Router Protocol (HSRP)

El Hot Standby Router Protocol de Cisco (HSRP) juega un papel importante en la mayoría de redes campus. La primera misión dee HSRP es provisionar un gateway redundante para las estaciones finales. Sin embargo este puede sser usado también para prove4er balanceo de carga.

Muchas estaciones finales permiten únicamente un defaul gateway. Normalmente esto hace que los host dependan en un único router cuando se comunican con todos los nodos de la subnet local. Para evitrar esta limitación, HSRP provee un mecanismo que permite que una única dirección IP sea compartida por dos o mas routers como ilustardo en la figura 4-33.

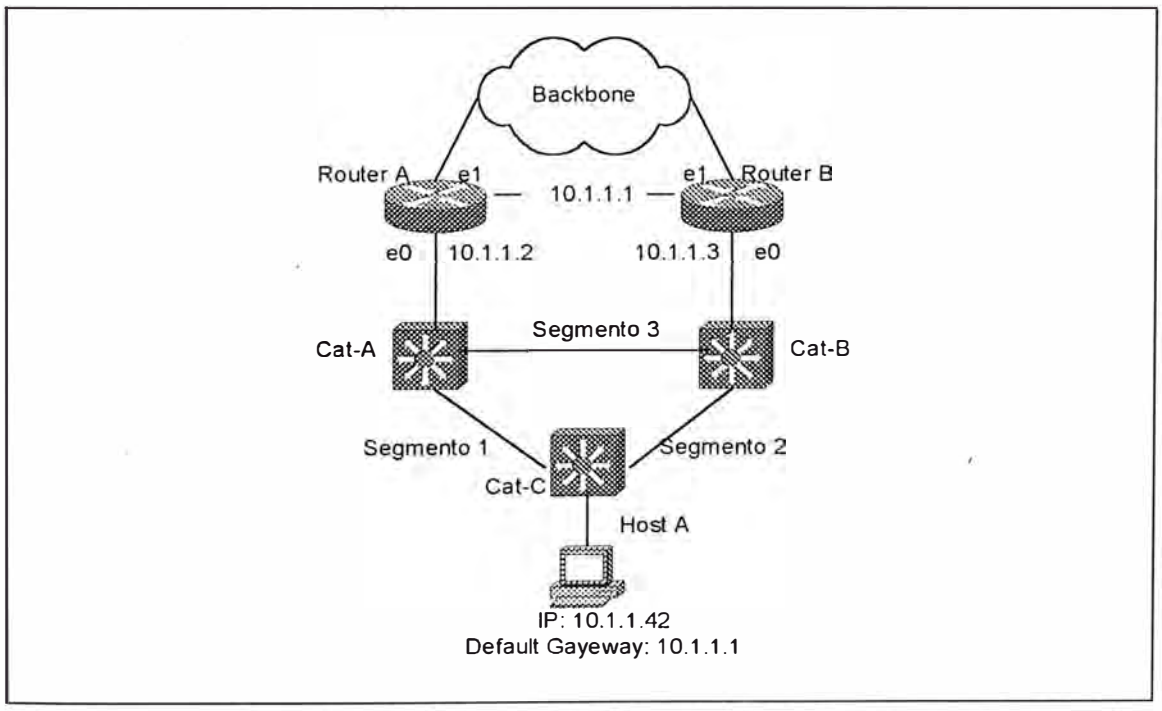


Figura 4-33 HSRP permite que múltiples Routers compartan direcciones IP y MAC

Aunque ambos routers son asignados una única dirección IP como normal (10.1.1.2 y 10.1.1.3), HSRP provee una tercera dirección IP que ambos routers comparten. Los dos routers intercambian mensajes hello periódicos (cada tres segundos por defecto) para monitorear el estado de cada router. Un router es elegido como el HSRP peer activo y manipula todos responsabilidades para la direección compartida. El otro nodo luego actua como un HSRP peer en standby. Si el peer standby pierde tres hello HSRP , este luego asume que el peer HSRP activo ha fallado y toma el rol de peer HSRP activo.

Uno de las sutileza de HSRP es que los routers solo comparten una dirección IP. Para crear un mecanismo de falla transparente, ellos también tienen que compartir la MAC address. Los routers además usan un algoritmo para crear una dirección MAC virtual compartida. Aĺ igual que una dirección IP compartida, el peer activo es el único nodo que usa la dirección MAC derivada.. Sin embargo, si el activo peer falla, el otro dispositivo no únicamente adopta la dirección IP compartida, también comparte la dirección MAC. Haciendo eso, el cache ARP de ubicado en cada estación final en la red no requiere actualización después de una situación de falla.

Notar que HSRP puede ser muy usual aun en casos donde el stack TCP/IP operando en los cleintes soportan múltiples dedfault gateways. En algunos casos, el mecanismo usado por estos stacks para fallar hacia un defaul gateway alternativo no trabaja confiablemente. En otros casos, tales

como el actual Microsoft stack, la redundancia únicamente trabaja para ciertos protocolos (tales como TCP, pero no UDP). En los dos casos, la mayoría de organizaciones no quieren dejar la confiabilidad del default gateway y en vez de eso implementan el HSRP..

En la mayoría de diseño campus, algunos pensaban que debería ser dado como la ubicacióon apropiada del peer activo. En general, las siguientes dos líneas-guía deberían ser usados:

- El peer HSRP activo debría ser ubicado cerca de un Root Bridge Spanning Tree.
- El router debería abandonar su role como el HSRP peer activo si este pierde su conexión al backbone.

En redes que continen loop capa 2, el Spanning Tree Route Bridge actúa como el centro del universo. Otros bridge luego busacan la ruta mas eficientea este dispositivo. Ubicando el HSRP peer activo cerca al Route Bridge, el Sapnning Tree Protocol automáticamente ayuda que el tráfico de los usuarios finales siga la mejor ruta al default gateway. Por ejemplo, si el Router-A es el HSRP peer activo en la figura pag 514 lans pero el Cat-B es el Spanning-Tree Root Bridge, El Segmento-1 tiene un puerto en el estado blocking. Esto fuerza que todo el tráfico del defaul gayeway tomen una ruta ineficiente a través del Cat-B. Por colocando el peer HSRP activo y el Root Bridge en el Cat-A y el Router-A, este hop de bridge innecesario puede ser eliminado.

Para forzar al Cat-A a ser el Root Bridge, y el Router-A el activo HSRP, se utilizan comados comunes de cisco. El peer con el mas alto valor de prioridad viene a ser el peer activo (el default es 100). En este caso, el Router-A tiene una prioridad configurada de 110, haciendo que este gane la elección de peer activo. Sin embargo, si el Router-A boots después del Router-B, este no cede al Router-B por default (este espera a que el Router-B falle primero), creando el mismo patrón ineficiente mencionado anteriormente, este puede ser evitado si configuramos con el comando standby group-number preempt . Este causa que un Router tome instantáneamente tan pronto como sea posible la prioridad mas alta.

La segunda línea-guía habla de una situación donde un router tiene la mas alta prioridad, pero este ha pérdido su conexión al resto de la red. Por ejemplo, el Router-A es el activo HSRP peer pero su enlace Ethernet1 cae. Aunque esto no evita que el tráfico alcance el backbone (el Router-A puede usar su interface Eth 0 para enviar tráfico hacia el backbone a través del Router-B), esto nos guía a un flujo ineficiente. Para prevenir esta situación, la opción standby track puede ser usado.

Aunque la configuración utilizada en esta sección provee un default gateway redundante para las estaciones finales conectados al Cat-C, esto sufre una limitación: El Router-A está manipulando todo el tráfico. Para eliminar este problema, múltiples VLANs deberían ser creados en el Cat-C. Cada VLAN usa un group-number separado en el camando standby. Luego,

las VLANs deberían alternar peers activos entre los dos routers. Por ejemplo en Router-A podría ser el peer activo para todas las VLANs numeradas impares, y el Router-B podría ser el peer activo para todas las VLAN numeradas pares.

Balanceo de Carga con MHSRP.- Usando Spanning Tree y múltiples VLAN pueden ser efectivos si los lazos de capa 2 y múltiples VLAN existen en el Cat-C, el switch MDF. Sin embargo, este no es siempre el caso. Muchos diseñadores desean desarrollar redes similares a lo ilustrado en la figura 4-34.

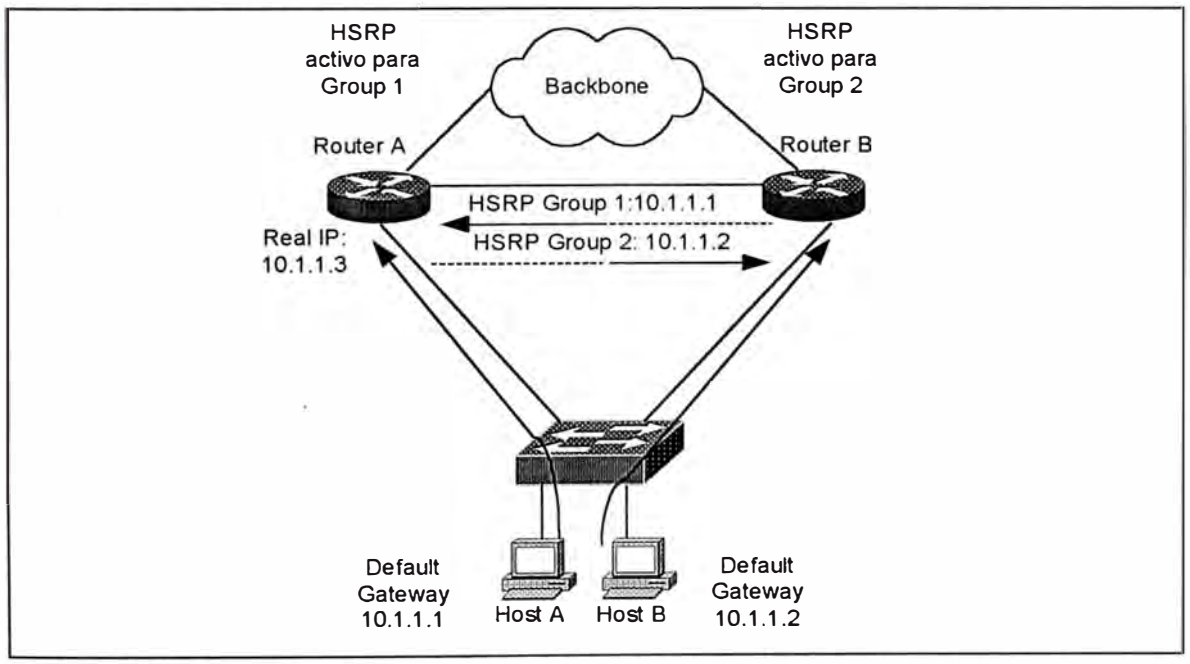


Figura 4-34 Una red usando una única VLAN en un Closet de alambrado

El diseño en la figura 4-34 tiene un switch MDF directamente conectado a un par de Switching Routers tales como el Catalyst 8500. Este elimita todos los lazos de capa 2 y retira el Spanning Tree desde la

ecuación. Además, debido a que solo una VLAN esta en uso en el Cat-C, el switch MDF, la VLAN alternativa no puede ser usado.

En este caso, la solución mas efectiva es el uso de Multigroup HSRP (MHSRP). Esta característica permite que múltiples HSRP group-number sean usados en una simple interface. La tabla 4-8 muestra un ejemplo con la posible configuración del Router-A.

```
Interface FastEthernet 0/0/0
description link to wiring closet Catalyst
ip address 10.1.1.3 255.255.255.0
standby 1 ip  10.1.1.1
standby 1 priority 110
standby 1 track FastEthernet 0/0/1 15
standby 1 preempt
standby 2 ip 10.1.1.2
standby 2 priority 100
standby 2 preempt
```

Tabla 4-8 Configuración MHSRP en unCatalyst 8540

El código en la tabla crea dos direcciones compartidas entre los Router-A y el Router-B para una única subnet. El balanceo de carga puede luego ser implementado teniendo que la mitad de los host en el Cat-C usen el 10.1.1.1 como default gateway y la otra mitad usen el 10.1.1.2. La caida potencial es que se tiene que configurar diferente host para usar diferentes default gateway. Afortunandamente, DHCP provee una simple y efectiva técnica para lograr esto.

4.5.5.- Integración Entre Routing y Bridging

Anteriormente se trató de las ventajas de tener una barrera o partición en capa 3 en la red. Sin embargo, por una variedad de razones, muchas personas quieren evitar la "barrera dura" fromada por esta propuesta. En vez de eso ellos buscan " barreras suaves" donde algunos protocolos o VLAN son terminados mientras otros pasan a través de ellos. Esto requiere de una mixtura de enrutamiento (es decir, switching capa3) y bridging (es decir, switching capa2). A continuación veremos las dos formas mas comunes de mezclar enrutamiento y bridging.

Brdging entre VLANs.- Una de las maneras mas simples de evitar la dureza de la barrera capa 3 es haciendo bridging entre múltiples VLANs. Muchos diseñadores de red quieren hacer esto cuando tienen dos VLAN separadas que necesitan compartir protocolos no ruteables tales como Local-area transport (LAT) o NetBIOS/NetBEUI.

Esta clase de bridging puede ser fácilmente configurado usando la misma tecnología bridge-group que los routers Cisco han soportado por años. En la tabla 4-9 muestra una configuración donde habilita bridging entre las VLAN 2 y 3 en un 8500.

```
Interface FastEthernet 0/0/0
no ip address
!
Interface FatsEthernet 0/0/0.1
encapsulation isl 1
ip addresss 10.1.1.1 255.255.255.0
!
Interface FatsEthernet 0/0/0.2
encapsulation isl 2
ip addresss 10.1.2.1 255.255.255.0
ipx network 2
bridge-group 1
!
Interface FatsEthernet 0/0/0.3
encapsulation isl 3
ip addresss 10.1.3.1 255.255.255.0
ipx network 3
bridge-group 1
!
Interface FatsEthernet 0/0/0.4
encapsulation isl 4
ip addresss 10.1.4.1 255.255.255.0
ipx network 3
!
bridge 1 protocol ieeet
```

Tabla 4-9 Usando un Bridge group paraconmutar entre VLANs

La configuración en el ejemplo anterior resulta de que el tráfico IP e IPX son ruteados entre las sibinterfaces Fast Ethernet1/0.2 y 1/0.3, mientras que otros protoclos son brdged. Ningun bridging es llevado a cabo las subinterfaces Fast Ethernet1/0.1 y 1/0.4. Notar que esto requiere que los usuarios IP en las VLAN 2 y 3 usen diferentes subnets IP (y redes IPX) pero el mismo rango de cable Apple Talk.

Esta técnica es aplicable solo cuando un protocolo es bridged o routed en un dispositivos particular o específico. El procesamiento bridge-group no te permite brdige IP entre dos interfaces y rutear estos entre otros

dos interfaces . Para hacer eso necesitamos de una característica llamado Integrated Routing and Bridging (IRB).

Integrated Routing and Bridging (IRB).- El IRB es una técnica que permite a un simple protocolo ser bridged o Routed en la misma caja. El IOS 11.1 introdujo un precursosr a IRB llamado Concurrent Routing and Bridging (CRB). Esto permitió que un protocolo particular tal como IP, sea Bridged y Routed en un mismo dispositivo. Esto pérmitió que todas las interfaces routed se comuniquen y así mismo se comuniquen también todas las interfaces bridged. Sin embargo CRB no permitió que las interfaces routed se comuniquen con las interfaces bridged. En otrtas palabras, el mundo routed y bridged para el protocolo configurado fuera tratadop como dos islas separadas.

IRB llenó este espacio permitiendo la comunicación entre estas dos islass. Esto habilitó configuraciones tal como mostrado en la figura 4-35.

Las interfaces en el lado derecho del router (fa0/0/0, fa0/0/1 y fa 0/0/2) todos usan direcciones Ipen subredes IP separados. Consecuentemente, las interfaces en el lado izquierdo (fa0/0/3 y fa0/0/4) ambos caen en la misma subred. Y porque IRB está en uso, el 10.1.4.62 puede hacer ping al 10.1.1.20 (esto no es posible en CRB).

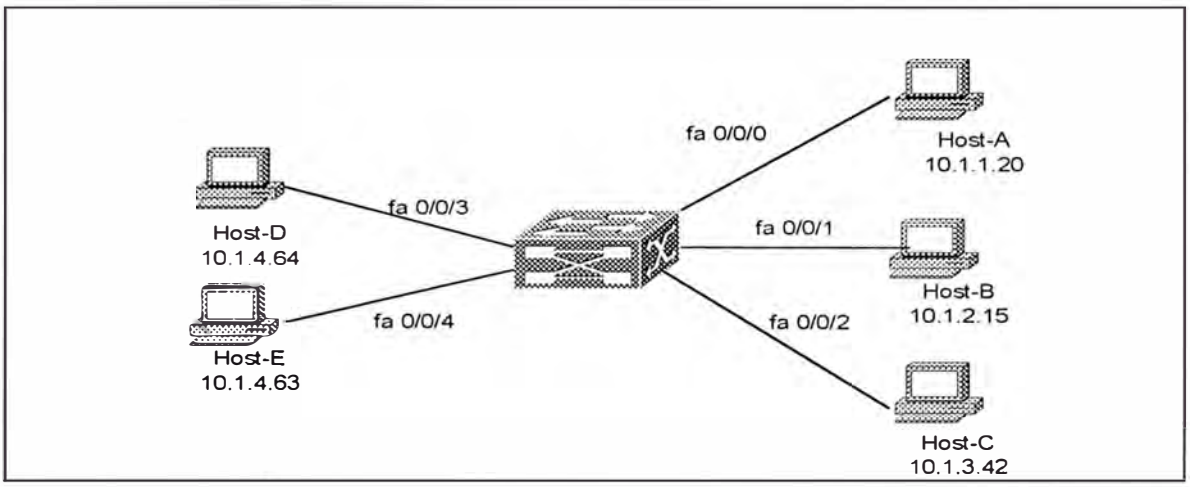


Figura 4-35 Un ejemplo de onfiguración IRB.

Para crear enlaces entre los dominios routed y bridged, Cisco creó una interface virtual especial conocido como una Bridged Virtual Interface (BVI). El BVI puede ser configurado con direcciones capa 3 (este bno puede sser configurado como sentencias bridging) y actua como ua interface routed dentro del resto de la caja. Por ejemplo el BVI en la figura 4-35 usa una dirección IP de 10.1.4.1, como ilustrado en la figura 4-36.

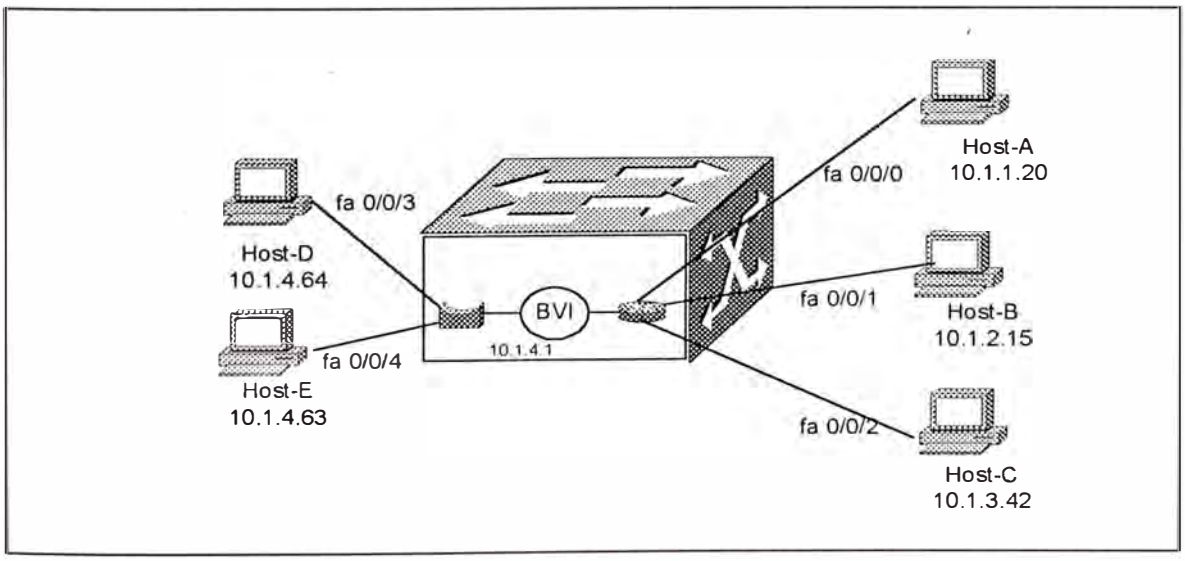


Figura 4-36 Una representación lógica de una BVI.

Si la interface fa0/0/4 recibe una trama con la dirección MAC del Host D, este lo bridges fuera de la interface fa0/0/3. Sin embargo si el Host-D hace oping al Host-A, el Host-D envía un paquete IP a su default gateway, la dirección 10.1.4.1 (la dirección BVI). Si es necesario , el Host-D ARPs por 10.1.4.1 para aprender la dirección MAC de la BVI. Cuando la interface fa0/0/4 recibe tráfico con direcciones MAC que van mas alla de la BVI, este sabe rutear el tráfico. El normal proceso de enrutamiento luego envía el tráfico fuera de la interface fa0/0/0.

La BVI escencialmente actúa como una simple interface ruteada en la mitad de tdodo las interfaces bridged en una VLAN particular. En la figura pág 525 lans, la BVI se comunica con el lado derecho de la caja a través del enrutamiento, mientras para el lado izquierdo usa bridging.

El IRB es una caracteristica importante en plataformas tales como el Catalyst 8500. Por instacia, considera el caso donde se quiera conectar directamente 10 servidores a un 8540 a lo largo con 20 trunks que guian separado switches MDF. Asume que los servidores vana ser ubicados en el mismo subnet (ademas bridging tráfico IP), mientras cada switch MDF un separado subred (ademas de enrutameinto IP). Sin IRB, esto sería poc}sible rutear y bbridges el tráfico IP en un dispositivo. En otras palabras, IRB permite rutear subredes IP mientras también extiende el server farm VLAN a través del router. Otra ventaja del IRB es que este es llevado a cabo cerca de la velocidad fisicaen el 8500.

Sin embargo, IRB tienen sus desventajas. El mas importante, el uso extensivo de IRB puede crear configuraciones terribles. Por ejemplo, considere un 8540 con 100 interfaces y 30 o 40 BVI (una para cada VLAN que necesita mezclar enrutamiento y brdiging). También, puede rápidamente reducir el número de interfaces lógicas disponibles soportados por el IOS (Internetwork Operating System). Para evitar esto, el IRB debería ser usado para resolver problemas específicos definidos. No intentar construir tu red entera con IRB.

Recomendaciones de Mezclar Bridging y Routing .- En general, el mejor consejo es evitar el bridging entre VLAN donde sea posible. Ya que no únicamente crea un problema de demasiado broadcast, sino también introduce un amplio problema de escalabilidad.

La mas simple manera de evitar el bridging entre VLAN es poner a todos los hosts que necesitan comunicarse via protocolos no ruteables en una única VLAN. Si esta VLAN necesita comnucarse con múltiples switching routers en la red core, una única interface BVI puede ser creado sin problemas significativos. Si mas que una VLAN necesita ser usado para tráfico no ruteable, hay que hacer lo posible para limitarlos.

Finalmente recuerda el único beneficio provisto por la conbinación de MLS y RSM. La arquitectura de capa 2 del Catalyst hace muy fácil agrupar varias combinaciones de puertos dentro de múltiples

VLANs,. El único diseño RSM que trata todos los puertos en una VLAN como un simple interface de router también hace que esto sea fácil rutear entre estas VLAN. Este aproach es considerablemente mas simple y mas escalable que el IRB.

4.6.- VLAN TRUNKING PROTOCOL

Algunas características de los catalyst soin específicas para los productos LAN Switching de Cisco, un ejemplo de ello es que incluyen el VLAN Trunking Protocol (VTP) la cual es descrito a continuación. Esta caraterística mejora la manera como el Catalyst lleva a cabo la performancia de red y la fácil administración inherente a cuan grande sea la LAN implementada. Algunas características avanzadas en el catalyst provee mejoramiento en la performancia de red, mediante la reducción del tráfico flloded en tu red.

4.6.1.- Conceptos de VTP

VTP es un protocolo usado para distribuir y sincronizar información identificada de VLANs configurados a través de una red switcheada. Las configuraciones hechas en un simple VTP server, son propagadas a través de los enlaces a todos los swtiches conectados en la red. VTP permite escalar soluciones de red sitcheada a redes de gran tamaño mediante la reducción de la necesidad de configuración manual en la red.

VTP es un protocolo de mensajes de capa 2 que mantiene las configuaraciones de VLANs consistente mediante la adición, borrado y cambios de nombres de VLANs a través de la red. VTP minimiza las cofiguraciones erradas e inconsistentes que puedan causar problemas, tales como duplicidad de nombre de VLAN o especificaciones de tipo de VLAN incorrectas.

Un dominio VTP es un switch o muchos switches interconectados compartiendo en mismo ambiente VTP. Un switch es configurado para pertenecer a únicamente un dominio de VTP.

Por defecto, un switch catalyst Cisco está en un estado de dominio no administrado hasta que reciba una advertencia por un dominio sobre un enlacec troncal, o hasta que se configure un dominio administrado.

4.6.2.- Modos de VTP

Los switches catalyst pueden ser configurados en uno de los tres modos siguientes: server, client , o transparente. La diferencia consiste en como ellos son fuentes ded VTP y en como responden cuando reciben un mensaje VTP. La tabla 4-8 (pag 545 lans) resume las diferencia entre los tres modos.

CARACTERISTICAS	SERVER	CLIENT	TRANSPARENT
Source VTP Messages	SI	SI	NO
Listening to VTP Messages	SI	SI	NO
Create VLANs	SI	NO	SI*
Remember VLANs	SI	NO	SI*

* Signifaco local únicamente.

Tabla 4-10 Comparación de Modos VTP

"Source VTP Messages".- Siempre que se crea una VLAN requerida, VTP automáticamente distribuye dicha VLAN en cada "catalyst" dentro del dominio administrado; debemos crear las VLAN´s siempre en un "catalyst" configurado como "VTP Server". Después que se crea la VLAN, el "VTP Server" automáticamente distribuye la información de VLAN a través de un mensaje VTP llamado "VTP subset advertisement". Este mensaje informa a todos los otros "catalyst" que se encuentran dentro del dominio administrado, acerca del nuevo VLAN creado. El "catalyst" donde se configura el nuevo VLAN genera el "subset advertisement" inicial, el cual lo envia a su interface "trunk". Los otros servidores y clientes continúan la propagación hacia los otros "catalyst" en la red.

Los "catalyst" configurados en modo transporte, nunca generan mensajes VTP. Cuando se crea una VLAN en un dispositivo transparente, la información de VLAN permanece local y no es comunicada a otros dispositivos, aún si este tiene conexiones "trunk" a otros "catalyst" en la red.

Listen to VTP Messages.- Ünicamente los catalyst configurados como server y cliente ponen atención a los mensajes VTP. En cualquier lugar que ellos reciban el mensaje con la dirección multicast VTP 01-00-0C-CC-CC-CC y un valor tipo SNAP de 0x2003, el catalyst receptor envía la trama al módulo supervior donde este es procesado. Si el supervisor determina que la información incluida en el update supercedes la información que tiene, este actualiza la información de VLAN y crea mensajes update a otros catalyst vecinos. El catalyst usa el número de revisión de la configuración VTP para reconocer si tiene data antiguas o actuales.

Cuando un catalyst configurado en modo transparente recibe un update VTP, el catalyst no envía trama al supervisor. , este localmente ignora la trama. Si ademas ewl catalyst tiene otros enlaces trunk conectados, este floods la trama a otros puertos trunk. Pero el mensaje VTP no cambia la configuración del catalyst de modo transparente, como si lo hace para un dispositivo server o cliente.

Create VLANs.- Si tu deseas crear VLAN, tienes que crearlo en un catalyst configurado en modo server o transparente. Estos son los modos únicos autorizados para aceptar los comandos de creación y borrado de VLANs. En el caso del modo server, el catalyst envía VTP advertisement a todos los puertos trunk al catalyst vecino. El catalyst en modo transparente no issue cualquier tipo de anuncios VTP cuando una VLAN es creada, el nuevo VLAN tiene significado úniucamente local.

Los "catalyst" configurados en modo cliente no pueden crear VLAN´s. Si asociamos un puerto del switch en modo cliente a una VLAN que este no conoce, el "catalyst" genera un mensaje informando si se tiene que crear una VLAN en el switch modo "server", antes que se pueda asignar el puerto a la VLAN. Cuando se crea VLAN´s en un "server" en el mismo dominio administrado que se encuentra el cliente, el cliente eventualmente escucha sobre la nueva VLAN creada e interpreta esto como una autorización para activar puertos en la nueva VLAN.

En forma similar, no podemos borrar VLANs en un switch en modo cliente, únicamente los podemos hacer en un switch en modo servidor ó en dispositivos configurados en modo transparente. Si borramos VLANs en un dispositivo transparente únicamente afecta al dispositivo local, no así si se borra en un dispositivo configurado en modo servidor. Cuando borramos VLANs en un server, se obtiene un mensaje de cuidado en el "catalyst", informándonos que esa acción pondría a cualquier puerto asignado a esa VLAN en un modo suspendido.

Recordar VLANs.- Cuando creamos, borramos o suspendemos una VLAN en un "catalyst" server ó transparente, el "catalyst" almacena la información de configuración en la NVRAM para que en el "power up" recobre la última configuración de VLAN conocida. Si la unidad es un "server", éste también transmite la información de configuración a los "catalyst" vecinos.

Los clientes por otro lado no almacenan información de VLAN. Cuando un catalyst configurado en modo cliente pierde energia, este olvida todas las VLAN´s que aprendió excepto la VLAN 1, que es la VLAN por defecto. En un power up, el cliente no puede localmente activar cualquier VLAN, excepto la VLAN 1, hasta escuchar de un VTP server la autorización para un conjunto de VLAN´s. Cualquier puerto asignado a una VLAN diferente que el 1, permanece en estado suspendido hasta que reciban un anuncio VTP desde el servidor. Cuando el cliente recibe un VTP update desde el server, este puede activar cualquier puerto asignado a la VLAN incluida en el "VTP announcement".

4.6.3.- El Mecanismco de Trabajo de VTP

El VLAN Trunking Protocol desarrollado por Cisco opera como un protocolo de capa 2 para los productos catalyst. Cuando transmitimos un mensaje a otros catalyst en una red, un catalyst encapsula el mensaje VTP en una trama de protocolo trunking, tal como una trama ISL o 802.1Q. La figura 4-37 nos muestra la encapsulación genérica para VTP dentro de una trama ISL. La encapsulación ISL inicia con la información de cabecera. La cabecera VTP varía dependiendo el tipo mensaje VTP, pero generalmente, cuatro items son encontrados en todos los mensajes VTP:

- VTP protocol versión – Versión 1 o 2
- VTP message type - Indica uno de cuatro tipos

- Management domain name lengh – Indica el tamaño del nombre que sigue
- Management domain name – Indica el nombre configurado para el dominio administrado.

Los mensajes VTP siempre viajan sobre la VLAN por defecto para el medio. Por ejemplo en un trunk Ethernet, VTP se transporta sobre la VLAN 1; en FDDI, es transportado sobre la VLAN 1002 ; y sopbre ATM, el VTP se transporta sobre la ELAN por defecto. Como no podemos borrar la VLAN por defecto, los mensajes VTP siempre se propagan sobre los puertos trunk LAN. Sin embargo VTP no siempre se transporta sobre trunks ATM. La ELAN por defecto debe habilitarse para que VTP cruce la red ATM.

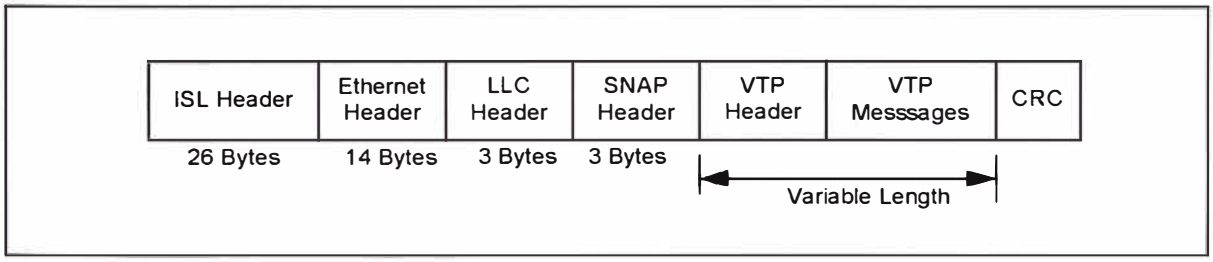


Figura 4-37 Encapsulación VTP sobre Troncales ISL.

Aunque los routers cisco entienden los protocolos trunking como ISL, LANE, y 802.1Q, ellos actualmente no participan en VTP: los roputers ignoran los mensajes VTP y lo descartan en la interface del router. Además, los mensajes VTP se propagan no mas allá de la interface del router, o a otro catalyst que pertenece a un dominio de administración VTP diferente. La figura 4-38 nos muestra muy a detalle un sistema que presenta los tres

dominios de administración aislados a través de asignamiento de dominio variado y a través de un router. El dominio 1 tiene tres puntos de borde de dominio administrado, uno hacia el router y dos hacia el dominio 2.

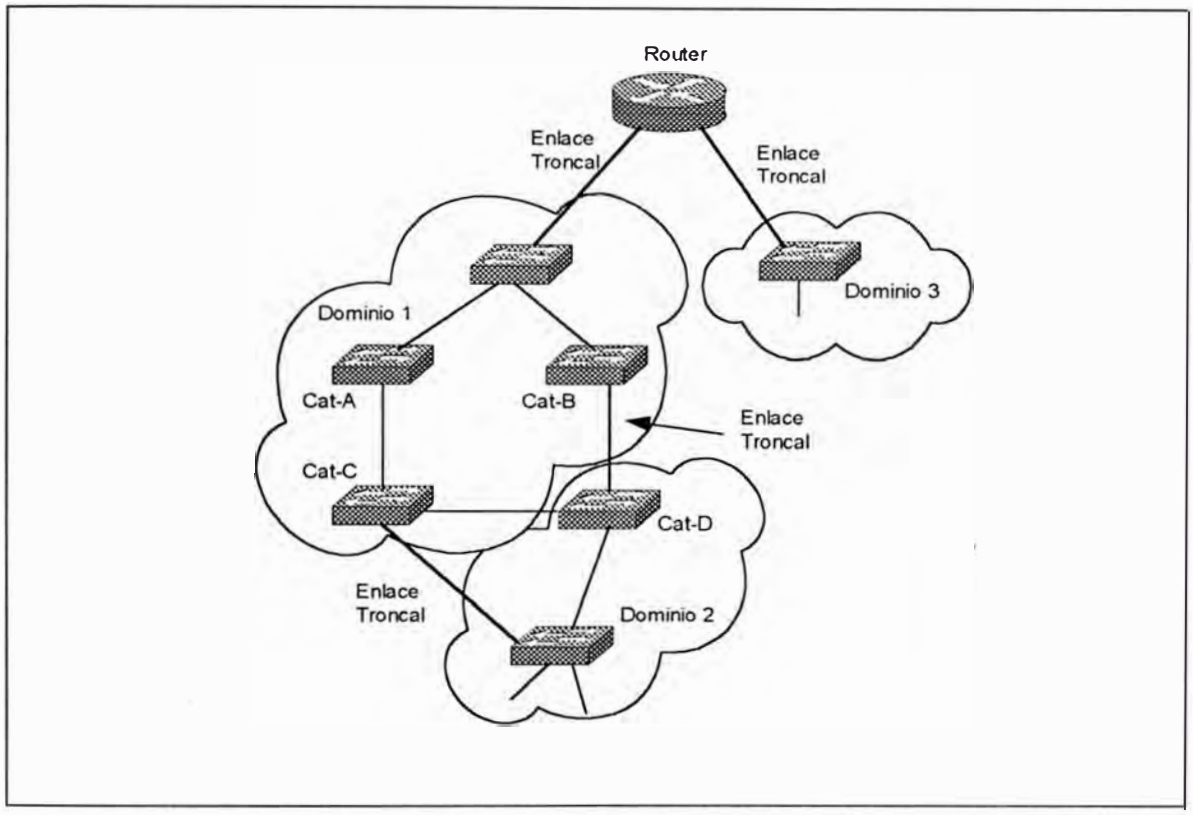


Figura 4-38 Una vecindad VTP.

Cuando el Cat-A en el dominio 1 issues un mensaje VTP, el mensaje es distribuidoi a todos los otros catalyst en el dominio. El Cat-B y el Cat-C reciben el mensaje y lo envían a los dos catalyst en el dominio 2. Sin embargo, estos catalyst observan que el dominio fuente fuente difiere de su propio dominio y descarta el mensaje VTP.

El mensaje VTP generado en el dominio 1 también se propaga al router. Pero el router no participa con VTP y descarta el mensaje. De igual

manera, Los mensajes VTP generados en el Dominio 2 o Dominio 3 nunca afecta a los dispositivos fuera de sus dominios.

VTP define cuatro tipos de mensajes:

- Summary Advertisements
- Subset Advertisements
- Advetisement requests
- VTP join messages

Los primeros tres tipos de mensajes describen la interacción entre servers VTP y clientes, para la distribución de información de VLAN. Estos mensajes ocurren por defecto en cualquier lugar que se habilite un trunk entre catalyst configurados como server y /o clientes. El cuarto tipo de mensaje es deshabilitado por defecto y es únicamente habilitado en cualquier lugar que se active el VTP pruning.

Summary Advertisement.- Por defecto los catalyst server y cliente proveen "summary advetisement" cada cinco minutos. Este informa a los catalysts vecinos que ellos creen ser el actual número de revisión de configuración VTP (valor que se incrementa si se adiciona, borra o suspende una VLAN) y miembro del dominio administrado. El catalyst receptor compara los nombres de dominio y, si ellos difieren ignoran el mensaje; si este concuerda, se compara el número de revisión de configuración. Si el advertisement contiene un número de revisión mas alta que el que tiene actualmente el

catalyst receptor, este provee una solicitud de advertisement para una nueva información de VLAN. La figura 4-39 muestra un formato de protocolo para el summary advertisement.

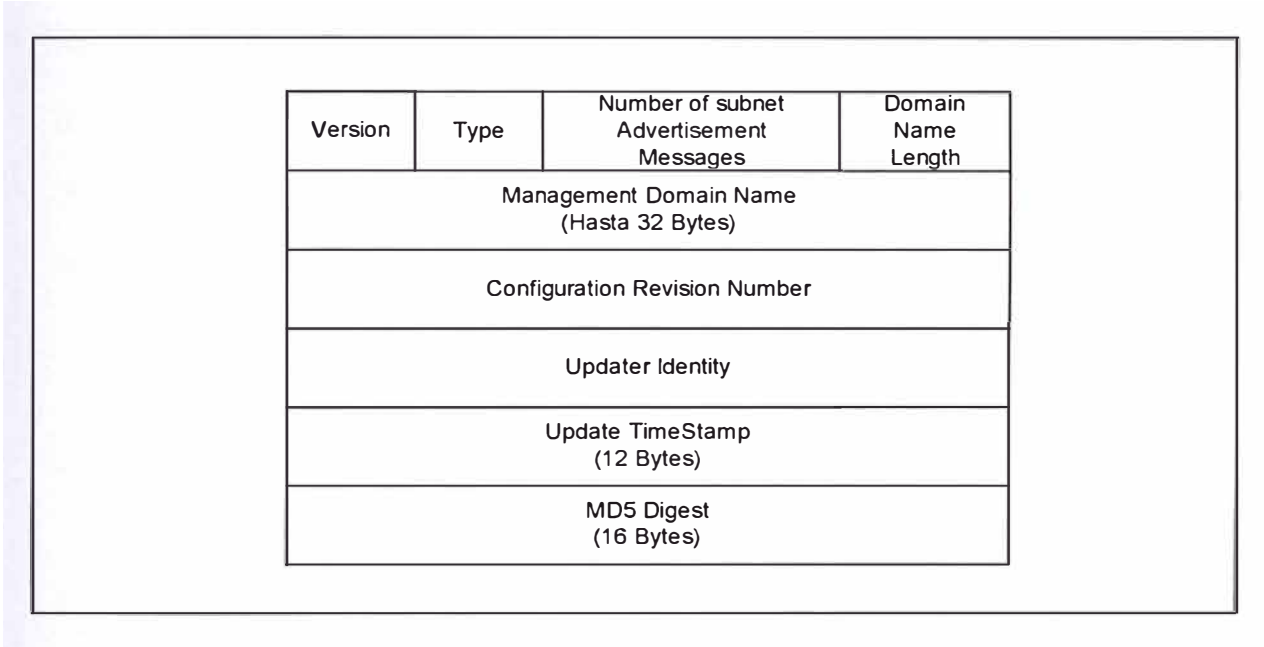


Figura 4-39 Un formato de VTP Summary Advertisement.

Cada fila en la figura anterior son cuatro octetos de longitud. La versión, tipo, número de subnet advertisement mesage, y los campos de longitud de nombre de dominio son todos de longitud igual a un octeto. Algunos de los campos pueden extenderse mas allá de cuatro octetos y son indicados en la figura.

La cabecera VTP contine una versión de VTP en uso, todos los catalyst tiene que operar a la misma versión. El valor de tipo de mensaje indica cual de los cuatro tipos de mensajes VTP fue transmitido por el catalyst fuente.

El siguiente campo, Number of Subnet Advertisement Message, indica como muchos mensajes VTPs de tipo 2 siguen a la trama summary advertisement. Este valor puede estar entre cero y 255. Cero indica que ningun subnet advertisement sigue. Un catalyst únicamente transmite el subnet advertisement si hay un cambio en el sistema, o en respuesta a un mensaje de solicitud dee advertisement.

El Domain lengh and name sigue a este campo con cualquier padding bytes necesarios para completar el campo Domain Name.

La fuente también transmite número de revisión de configuración VTP e identifica por si misma a través de su direccióin IP.

El mensaje incluye un tiemstamp el cual indica el tiempo en el que el valor de número de revisión de configuración aumetó al actual. El tiemstamp tiene un formato de yymmddhhmmsss.

Finalmente, la fuente leva a cabo un MD5 one-way hash en la información de cabecera. Un MD5 (mensaje digest tipo 5) hash algoritmo is frecuentemente usado en sistemas de seguridad como un proceso de encryption no reversible. El ctalyst receptor también lleva a cabo un hash y compara el resultado de detectar cualquier corrupción en la trama. Si el hashes no macha, el catalyst receptor descarta el mensaje VTP.

Subset Advertisement.- En cualquier lugar que cambies una VLAN en un dominio administrado, el catalyst server donde configuraste el cambio issue un sumamry advertisement seguido por uno o mas mensajes sbset advertisement. Los cambios que trigger el subset advertisement incluyen:

- Creando o Borrando una VLAN
- Suspendiendo o Activando una VLAN
- Cambiando el nombre ded una VLAN
- Cambiando el MTU de una VLAN

La figura 4-40 muestra el formato de paquete VTP subset advertisement

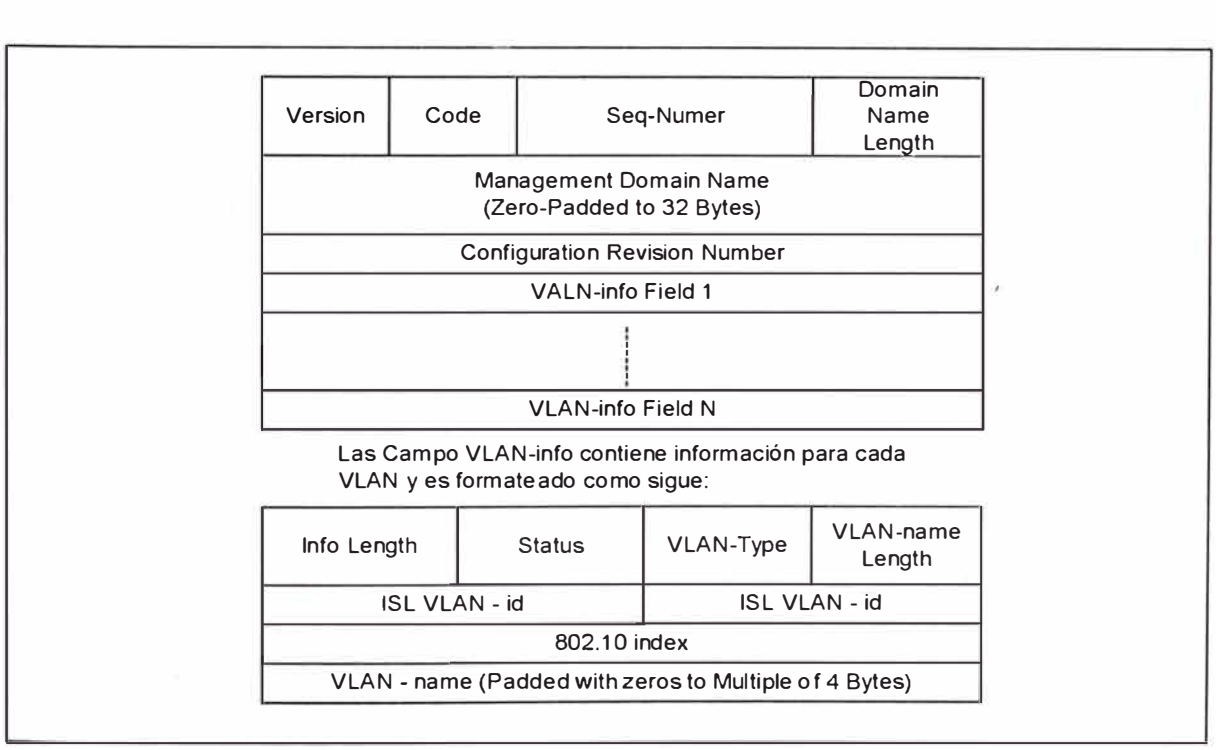


Figura 4-40 Un formato de VTP Summary Advertisement.

El summary advertisement tiene un campo Seq-Number en la cabecera indicando el número de subset advertisement que sigue. Si tu tienes una lista de VLAns larga, VTP podría necesitar enviar la lista entera sobre múltiples subset advertisement.

Advertisement Requests.- Un catalyst issuing un tercet tipo de mensaje, un advertisement request solicita summary y subset advertisement desde un server en el dominio amdnimistrado. Los Catalyst transmiten una solicitan un advertisement request en cualquier lugar que tu resetes el catalyst, en cualquier lugar que cambies su VTP domain membership, o en cualquier lugar que escuhe un VTP summary advertisement con un número ded revisión ded configuración alto que el que actualmente tiene. Esto puede oicurrir si el catalayst es particionado temporalmente desde la red y un cambio ocurre en el dominio.

La figura 4-41 muestra un formato de trama VTP advertisement request.

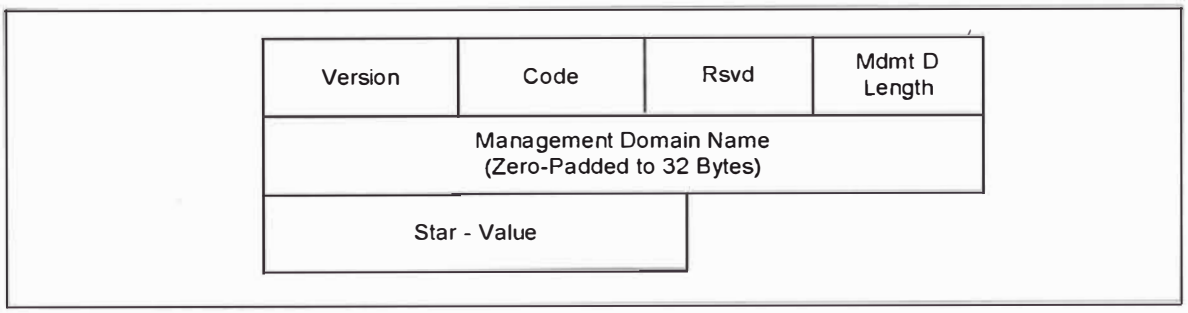


Figura 4-41 Formato de VTP Advertisement Request.

Un advertisement request incluye seis campos. La versión, que identifica la versión VTP usado por el dispositivo. El Code, identifica como un advertisement request. La porción resevada (Rsvd) es configurada a cero. El Management Domain Length indica la longitud del nombre del dominio en el campo siguiente. Estos cuatro campos son seguidos por el Management Domain Name. Finalmente, si el catalyst espera recibir un subset advertisement pero falló en recebir uno o mas, este puede solicitar un reenvío iniciando en el valor subset particular. Este es señalado en el campo Star-Value . Por ejemplo si un catalyst espera ver tres subset advertisement pero únicamente recibió las instanacias 1 y 3, este puede solicitar un reenvio iniciando en la instancia 2.

4.6.4.- VTP Prunning

VTP prunning usa VLAN adsvertisement para determinar cuando una conexión trunk esta flooding tráfico innecesariamente. Por defecto, una conexión trunk lleva tráfico para todoas las VLANs en elñ VTP management domain. Comúnmente, algunos switches en la red no tiene puertos locales configurados en cada VLAN. En la figura 4-42 los switches 1 y 4 soportan pueretos estadísticamente configurados en la red VLAN.

VTP prunning incrementa el ancho de banda disponible mediante la restricción ded tráfico flooded a los enlaces trunk que el trafico tiene que usar para acceder al equipo de red apropiado.

La figura 4-42 muestra una red switched con VTP prunning habilitado. El tráfico broadcast desde la estación A no es enviada a los switches 3,5 y 6, por que el tráfico para la red VLAN ha sido pruned en los enlaces indicados en los switches 2 y 4.

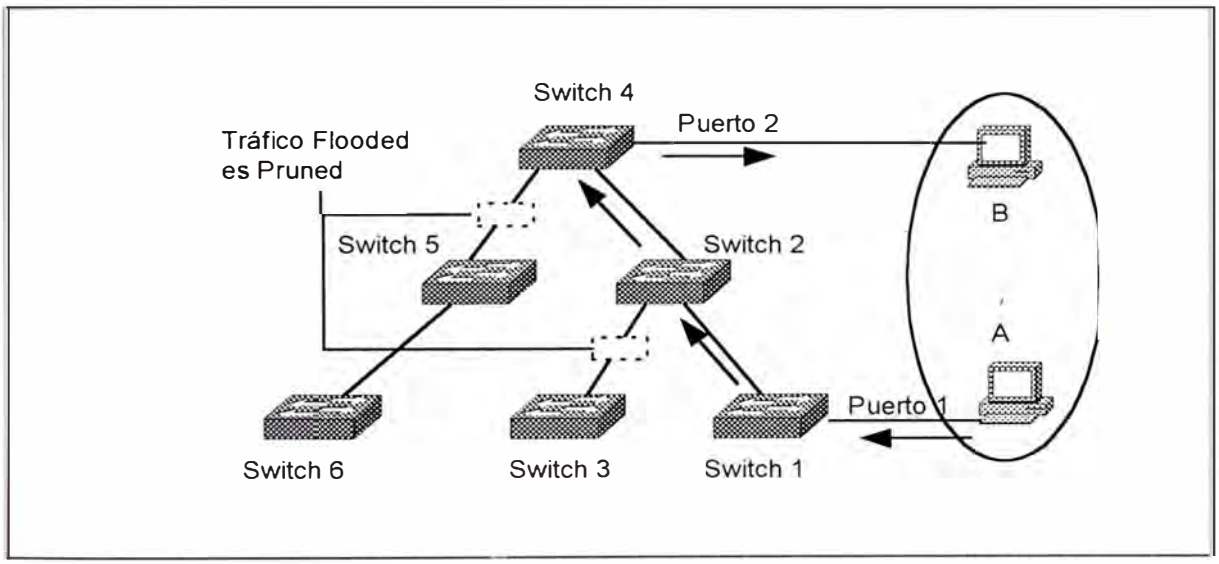


Figura 4-42 Operación del VTP Pruning.

CAPÍTULO V

ROUTING

5.1.- TCP/IP ADDRESS OVERVIEW

En un ambiente TCP/IP, las estaciones finales se comunican similarmente con servidores u otras estaciones finales. Esta comunicación ocurre por que cada estación usando el protocolo TCP/IP suite tiene una única dirección lógica de 32 bits.

Algunas veces el tráfico es enviado a través de la internetwork basado en el nombre de una organización mejor que por una persona individual o host. Si los nombres son usados en vez de direcciones, los nombres tienen que ser traducidos a la dirección numérica antes de que el tráfico pueda ser enviado. La ubicación de la organización indicaría la ruta que la data debe seguir a travé de la internetwork.

Cada compañía en la internetwork es tratada como una simple red que tiene que ser alcanzado antes de que cualquier host dentro de una compañía pueda ser contactada. Cada red de la compañía tiene una dirección, los host que pueblan la red comparten los mismos bits, pero cada host es identificado por solo un único bits remanente.

5.1.1.- Direccionamiento IP Overview

Una dirección IP es un grupo ded 32 bits de longitud y tiene dos partes:

- El número de Red
- El número de Host

Los 32 bits son divididos dentro de cuatro octetos (un octeto es un grupo de ocho bits, es decir un byte). Aunque las computadoras no tienen dificultad en tratar con números de 32 bits, los humanos si; además tenemos que traducir el valor binario de cada octeto en su equivalente decimal para crear un formato de dirección concido como dotted-decimal notation, como muestra la figura 5-1. Un ejemplo de dirección dotted-decimal es 172.16.122.204

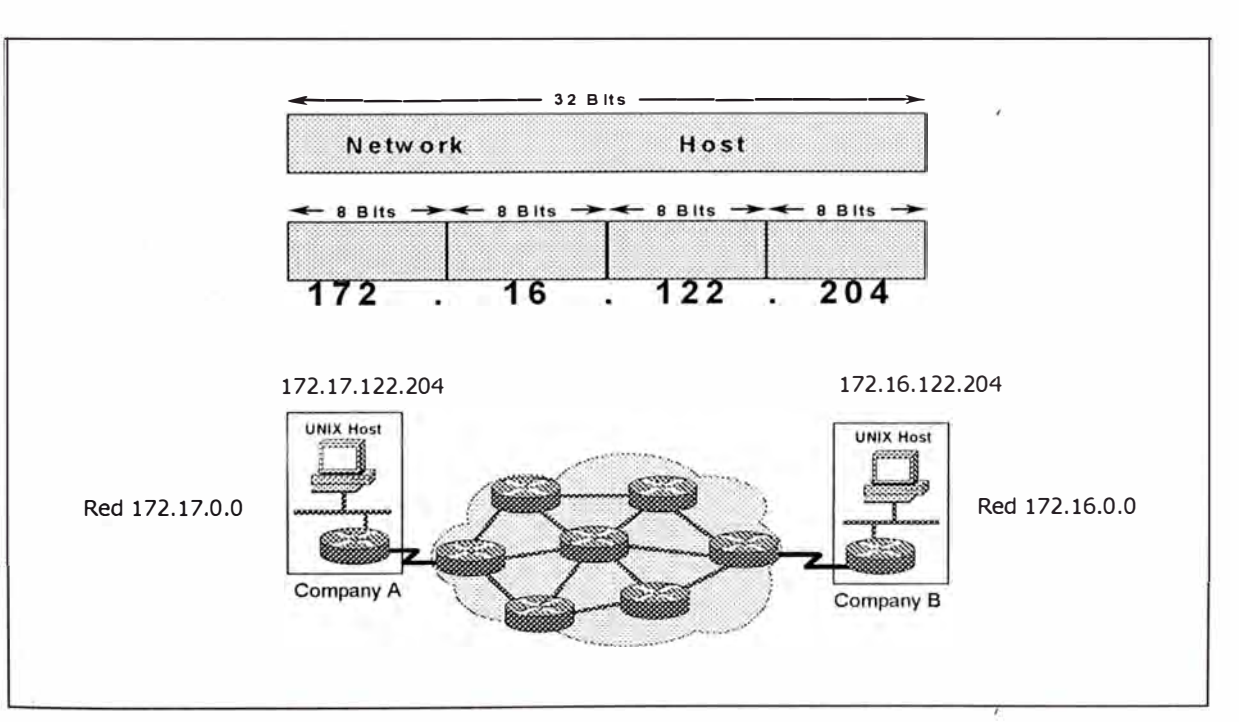


Figura 5-1Las direcciones IP son cuatro octetos y contienen porción de Red y Host

El valor mínimo para un octeto es 0; este contiene todos ceros. El máximo valor para un octeto es 255; el cual todos son unos.

La ubicación de las direcciones es administrado por una autoridad central: El Internet Assigned Numbers Authority (IANA). Esta forma muy común de direccionamiento refleja el IP version 4 ampliamente usado. Encarado con el problema de reducción de direcciones disponibles, el Internet Engineering Task Force (IETF) trabaja para desarrollar una nueva generación compatible de IP (Ipng, referido ahora como IP v6).

Ipv6 ofrecería enrutamiento expandido y capacidades de direccionamiento con direcciones de 128 bits mejor que las direcciones de 32 bits. Las direcciones de ambas versiones coexistirían. Las ocurrencias iniciales de la dirección Ipv6 probablemente estarían en ubicación con softwares traductores de dirección y firewalls.

5.1.2.- Clases de Direcciones IP

Cuando IP fue desarrollado, no habían clases de direcciones. Ahora, para fácil administración, las direcciones IP son divididas en clases, como mostrado en la figura 5-2.

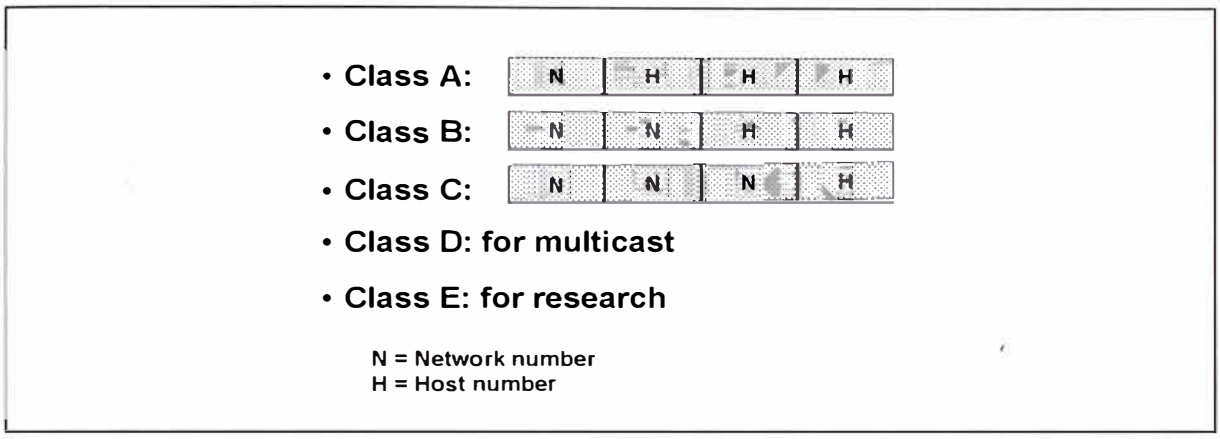


Figura 5-2 Las direcciones de Clase A, B y C son usados para redes IP.

Hay únicamente 126 direcciones de clase A, pero cada dirección puede soportar hasta 16 millones de host. Hay 64000 direcciones de clase B, el cual puede soportar hasta 64000 host. Hay mas de 16 millones de direcciones de clase C posibles, cada uno soportando hasta 254 host. Las direcciones de clase D inician en 224.0.0.0 y son usados para propósitos multicast. Las direcciones dee clase E inician en 240.0.0.0 y son usados para propósitos experimentales a cargo de diseñadores de red e Ingenieros.

Para definir el número de direcciones de host posibles, hay que efectuar la siguiente ecuación, donde n es el número de bits en la porción de host,

(2n – 2) = direcciones de host disponibles.

Por ejemplo considere la dirección de red 200.99.44.0. (una dirección de clase C). Hay ocho bits disponibles en la porción ded host. La fórmula es (28 – 2) = 254.

La razón por la que se tiene que substraer dos de los números es para reservar dos números ID de host especiales: todos ceros y todos unos. Todos ceros es usado para indicar la red (por ejemplo 200.99.44.0), y todos unos es la porción ID de host que es reservado para broadcast de red (por ejemplo: 200.99.44.255).

Este esquema de direccionamiento permite que las direcciones sean asignadas basados en el tamaño ded la red. Este diseño de dirección fue basado en la suposición de que habría mas redes pequeñas que grandes en el mundo. Como el número de redes crece, las clases puedeen eventualmente ser reemplazados por otros mecanismos de direccionamiento, tales como Classless Interdomain Routing (CIDR). Los RFC 1467 y RFC 1817 presentan información refernete a CIDR.

5.1.3.- Patrones de Bits de Direcciones IP

La figura 5-3 muestra una estructura de direcciones de Clase A, B y C

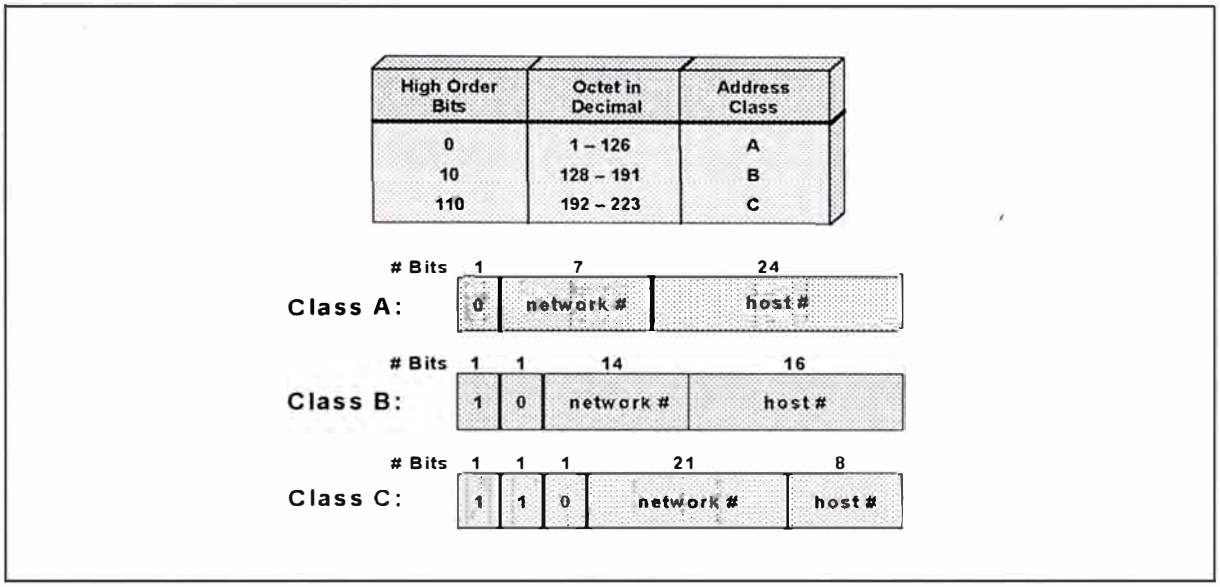


Figura 5-3 Los primeros valores del Byte puede ser usado para indicar la Clase de la dirección.

El valor del primer byte de una dirección determina la clase de la dirección, al igual que la cantidad de bits ubicadas en la porción de red. El scope de cada Clase es como sigue:

- Clase A: Rango de número de direcciones: 1.0.0.0 a 126.0.0.0 Número de direcciones host : 16,777,214 (16,777,2160 - 2)
- Clase B: Rango de número de direcciones: 128.0.0.0 a 191.255.0.0 Número de direcciones host : 65,534 (65,536 - 2)
- Clase C: Rango de número de direcciones: 192.0.0.0 a 223.255.255.0. Número de direcciones host : 254 (256 - 2)
- Clase D: Rango de número de direcciones: 224.0.0.0 a 239.255.255.0

5.1.4.- La Regla del Primer Octeto

La regla del primer octeto states que la clase de dirección n puede ser determinado por valor numérico del primer octeto.

Una vez que la regla del primer octeto es aplicado, el router identifica como cuantos bits tiene que machar para interpretar la porción de red de la dirección, como mostrado en la figura 5-3. Si no hay mas identificación de bits adicionales a usar como parte de la dirección de red , el router puede hacer una descición ded enrutamiento usando esta dirección.

El rango de direcciones para cad clase es como sigue, con el primer octeto representado en decimal:

- 001 a 126 Direcciones de Clase A
- 128 a 191 Direcciones de Clase B
- 192 a 223 Direcciones de Clase C
- 224 a 239 Direcciones de Clase D
- 240 a 225 Direcciones de Clase E

Notar que el número 127.0.0.0 es reservado para el loopback address. El loopback addres es usado por un dispositivo para direccionarse a si mismo internamente. Esta técnica es usada para probar los dispositivos locales TCP/IP stack e identificar posibles coruptos stacks.

5.2.- CONCEPTOS DE CONFIGURACIÓN DE DIRECCIONES IP

En esta parte nos enfocaremos en conceptos básicos que necesitas entender antes de configurar una dirección IP. Examinando varios requerimientos de red, podemos seleccionar la clase correcta de dirección y definir como establecer una subnet IP.

5.2.1.- Direcciones de Host

Cada dispositivo o interface tiene que tener un número de host no-cero. Una dirección de host de todos unos es reservado para un IP broadcast dentro de una red, como mostrado en la figura 5-4.

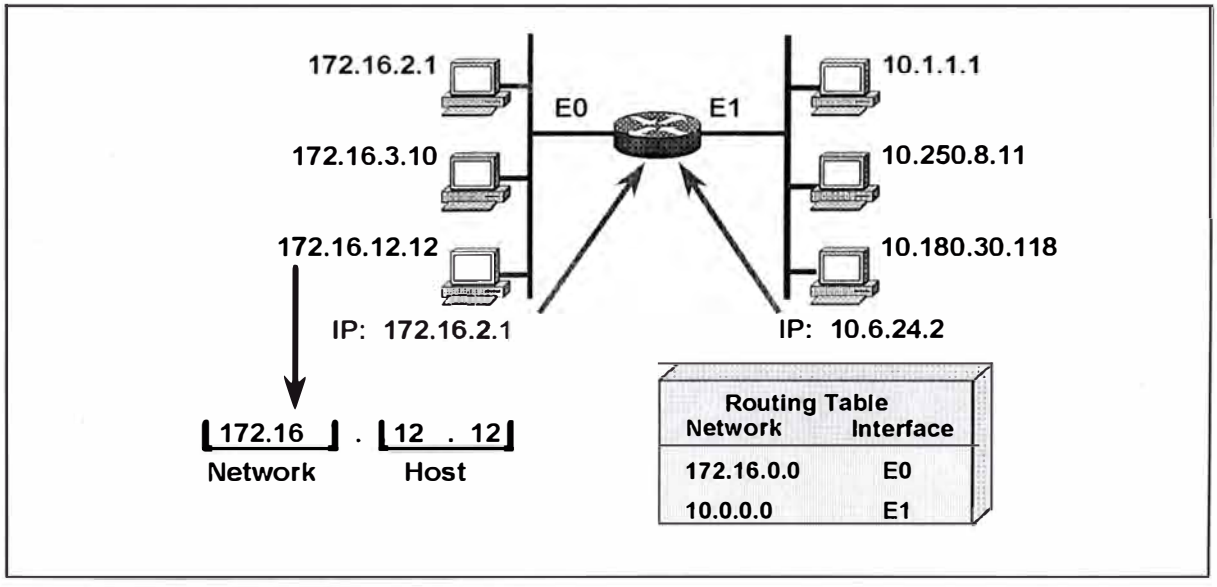


Figura 5-4 Todos los Host deben tener direcciones IP sin cero..

Un valor de cero se refiere a "esta red" o "el alambre por si mismo". El uso de ceros es llamado subnet cero. Por convención, el subnet cero es ahora reservado y no puede ser usado para representar interfaces.

La tabla de enrutamiento contiene entradas para redes o direcciones fisicas; Este no contine ninguna información de host.

Una dirección IP y direcciones de subnet en una interface achive tres propósitos:

- Habilita al sistema para procesar la recepción y transmisión de paquetes.
- Especifica la dirección local del dispositivo
- Especifica el rango ded direcciones que comparte el cable con el dispsoitivo.

El router es capaz de distinguir la porción de red desde la porción de host de la dirección por el uso de una mascara que se configura en la interface del router. Las Mascaras también usan formato dotted-decimal. La mascara por defecto o estándar para una dirección de Clase B es similar a los siguiente: 255.255.0.0

El estándar o defecto de las máscaras dee Clase A, B y C son:

- A – 255.0.0.0
- B – 255.25.0.0
- C – 255.255.255.0

Estas máscaras por defecto tienen todos los bits dee la posrción de red configurado a uno.

Direccionando sin subnets.- El mundo exterior observa a una organización como una única red, y no es requerido un conocimiento detallado de su estructura interna. Por ejemplo, en la figura 5-5, todos los datagramas direccionados al 172.16 son tratados de la misma manera, sin tener en cuenta el tercer y cuarto octeto de la dirección. Un beneficio de esta configuración es la corta tabla de enrutamiento que los routers puedan usar.

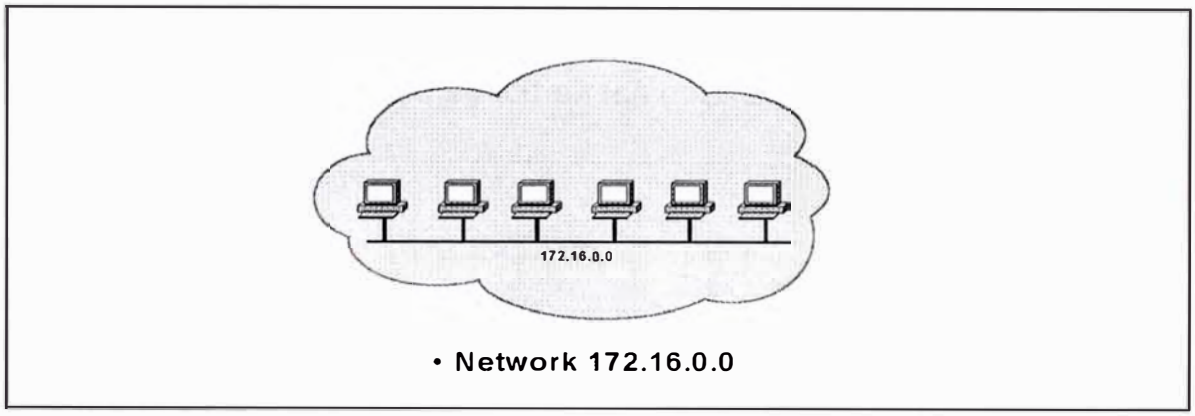


Figura 5-5 Dreccionamiento Straighforward no usa subnets.

Las redes se direccionan con el esquema configurado de tal manera que no tenga forma de distinguir segmentos individuales dentro de la red. Si dentro de la nube no tenemos subnets, tendremos un único y gran dominio de broadcast; todos los sistemas en la red se encontrarian con todos los broadcast de la red. Este tipo de configuración nos guiaría a un relativamente pobre performancia de red.

Por defecto, un espacio de dirección de clase B define un segmento con 65,000 estaciones. Los subnets te permiten dividir este gran segmento en muchos segmentos pequeños.

Direccionando con Subnets.- Con subnets, el uso de dirección de red es mas eficiente. No hay cambios en como el mundo exterior ve la red, pero dentro de la organización, hay estructuras adicionales.

En el ejemplo de la figura 5-6, la red 172.16.0.0 es subdividida o quebrada en cuatro subnets:172.16.1.0, 172.16.2.0, 172.16.3.0 y 172.16.4.0. Los routers determinan la red de destino usando las direcciones de subnet, así limitando la cantidad de tráfico en los otros segmentos de red.

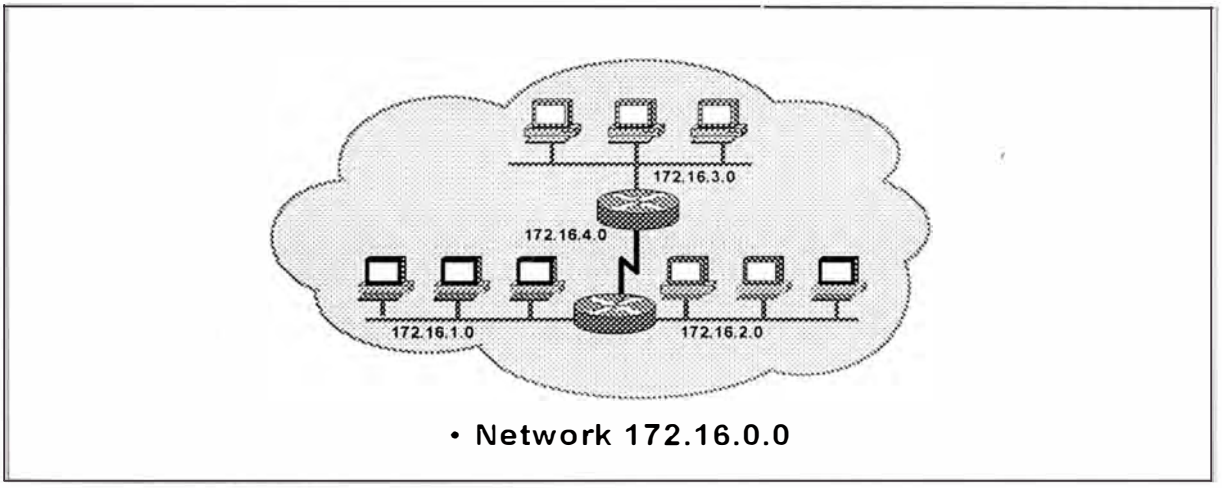


Figura 5-6 Desde el mundo externo no es factible observar la Red subnet.

Un dispositivo de red usa una mascara de subnet para determinar que parte de la dirección IP es usada para la red, suibnet y la dirección de host o IP. Un subnet mask es un valor de 32 bits conteniendo un número de bits unos que corresponde a la porcióndee red y subnet de la dirección, y un número de bits cero que corresponde a la porción de host.

Dado su propia dirección IP y subnet mask, un dispositivo puede determinar si un paquete IP es determinado para lo siguiente:

- Un dispositivo en sus propio subnet
- Un dispositivo en un diferente subnet en su propia red
- Un dispositivo en una red diferente.

Un dispositivo puede determinar que clase de dirección ha sido asignado al dispositivo desde su propia dirección IP. La mascar de subnet luego le dice dondee el boundary esta entre el subnet ID y el host ID.

5.2.2.- Subnetting Addressing

Los subnets son una extensión del n´pumero de red. Los administradores de reddeciden el tamaño de los subnets basado en las necesidades organizacionales y de crecimiento. Los dispósitivos de red usan subnet mask para identificar que parte de la dirección es considerada red y que parte es dirección de host, como mostrado en la figura 5-7.

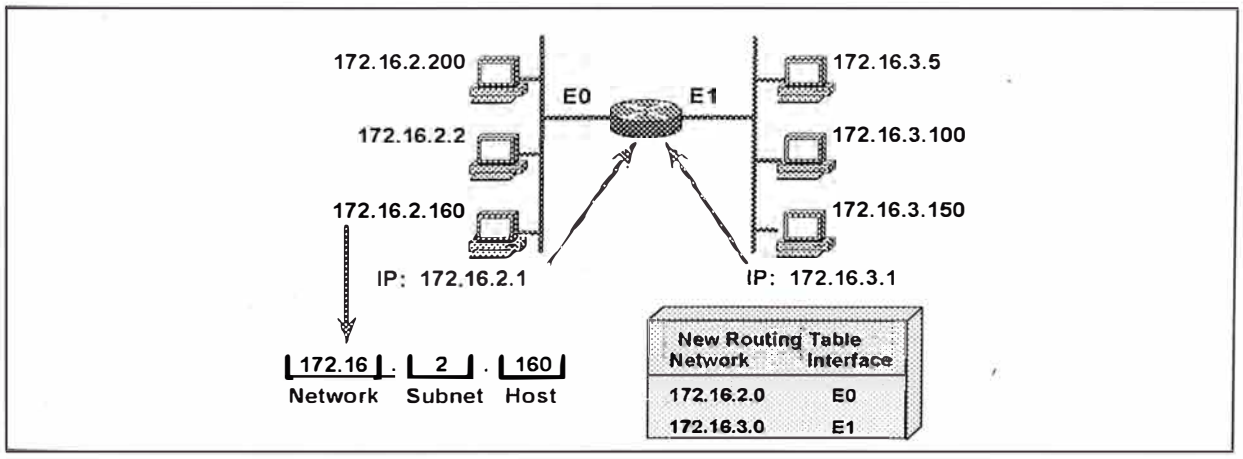


Figura 5-7 Las mascaras de subred usan parte de la dirección Host como subnet.

Máscara de Subnet.- Como notado tempranamente, una dirección IP es una dirección de 32 bits ded tamaño, escrito con cuatro octetos. Una mascara de subnet es también 32 bits de tamaño, escrito como cuatro octetos y consiste de una serie dee unos contiguos seguido por ceros contiguos. Como direcciones IP, los subnet mask pueden ser expresados en dotted-decimal como tambien en decimal binario.

Los subnet mask indican cual de los bits en el campo host de la dirección IP son usados para especificar diferentes partes (subnets) de una red particular. La figura 5-8 muestra una dirección IP y dos mascaras de subnets relevantes. La primera mascara es la mascara por defecto. Este resreva los primeros dos bytes para la porción de red y los últimos dos bytes para la porción de host. La segunda mascara mostrado es un subnet mask que se presta bits de la porción de host para incrmentar el número de posibles redes.

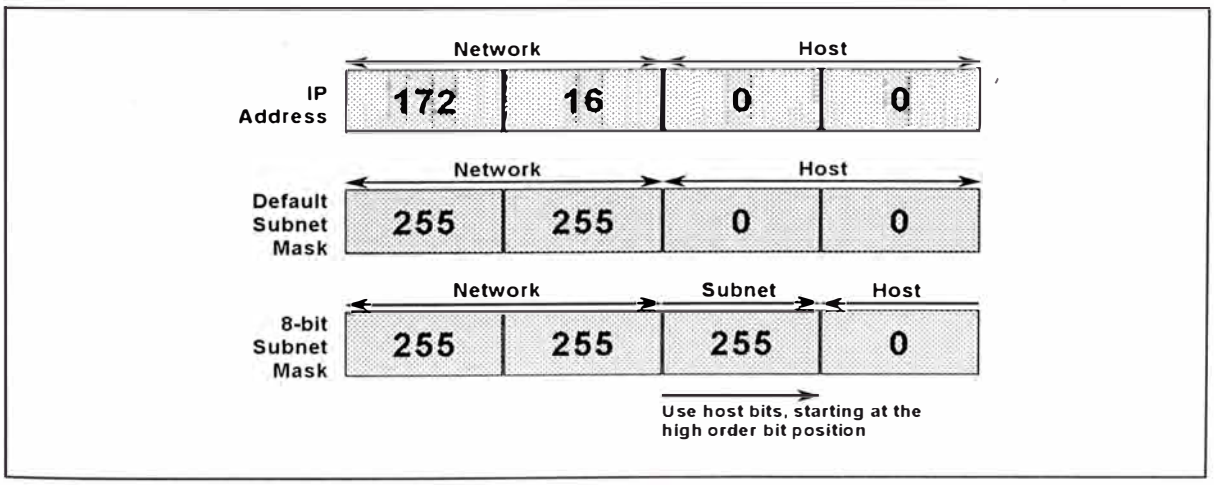


Figura 5-8 La máscara de subnet identifica secciones (subredes) de una gran Red

El layout del campo del subnet mask es como sigue:

- Binary 1 para los bits de red
- Binary 1 para los bits de subnet
- Binary cero para los bits de host

Equivalente Decimal de Patrones de Bits.- Los bits de subnets viene desde los bits de orden mas alto del campo de host. Para dedterminar una mascara de subnet para una dirección, adiciona el valor decimal de cada porción que tiene un 1. Por ejemplo, en la figura 5-9, los valores de cada posición de bit son mostrados. Como notamos, llevamos a cabo una conversión ded binario a decimal, simplemente adicionando el bit equivalente representado por un 1 en su posisición de bit. Por ejemplo

224 = 128 + 64 + 32

Por que la mascara de subnet no está definida por octetos, pero si por bits, necesitamnos convertir direcciones dotted-decimal a binario y viceversa.

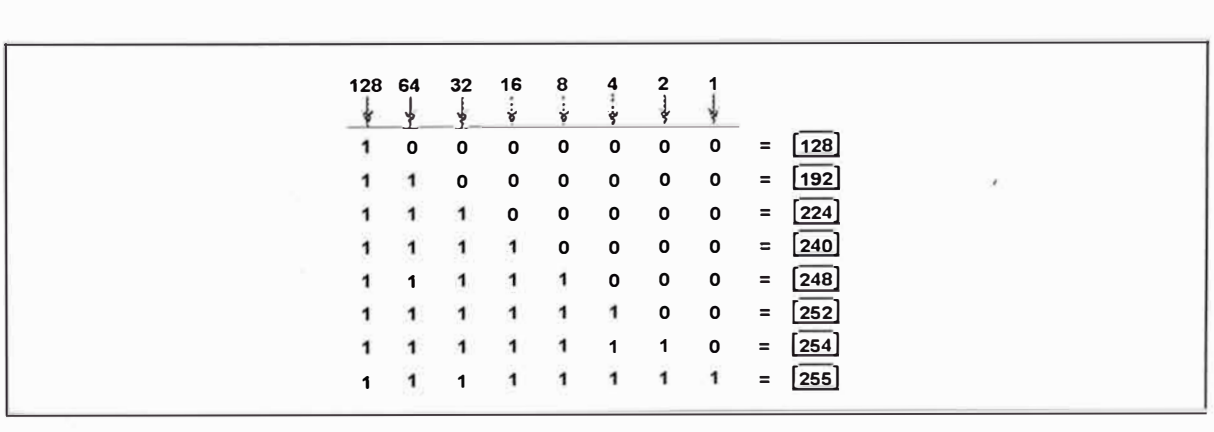


Figura 5-9 Cada posición de Bit tiene una notación decimal.

Máscara de Subnet sin Subnet.- Una mascara de subnet por defecto, también conocido como mascara de subnet estándar o internal, es asociado con una dirección IP cuando ninguna subnet es requerido. La primera mascara de subnet de la figura 5-8 es una mascara por defecto. En binario, una mascara por dedfecto tiene todos unos para la porción de red de la dirección IP y todos ceros para la porción de host.

El router extrae la dirección de destino IP desde el paquete y recupera la máscara de subnet interna. El router examina los bits que han sido iguales a la porción de red para obtener el número de red. Durante el proceso de determinar la dirección de red, la porción de host de la dirección de destino es retirado. Las decisiones de enrutamiento son luego basados en el número de red únicamente. Usando el ejemplo de la figura 5-7:

Dirección IP de paquete : 172.16.12.160
Mascara de subnet por defecto : 255.255.0.0
Red : 172.16.0.0
Con no subneting, el número de red que es extraido es :172.16.0.0

Máscara de Subnet con Subnets.- Cuando es requerido el subneting de una dirección IP , la mascara de subnet binario consiste de todos unos para la porción de red y subnet de la dirección, y todos ceros para la porción de host. La segunda mascara en la figura 5-8 es una mascara de subnet de 8

bits. Es decir comparado a la mascara por defecto, ocho bits adicionales han sido activados. (hecho binarios unos)

Continuando el ejemplo de la figura 5-7, con ocho bits de subnetting (255.255.255.0), la n{umero de red extraida (subnet)de la dirección 172.16.2.160 es 172.16.2.0.

Tu llegas a este número mediante el masking de los tres primeros bytesde la dirección total como definido por la mascara 255.255.255.0

Paquete IP address : 172.16.2.160

8-bit subnet mask : 255.255.255.0

Red : 172.16.2.0

5.2.3.- Planeando el Subnet

En la figura 5-10 ha sido asignada a la red una sirección de clase C dee 201.222.5.0. Asumimos que 20 subnets son necesitados, con cinco host por subnet. Necesitamos subdividir los últimosa octetos dedntro de una subnet y una porción de host, y deeterminar que mascara de subnet sería.

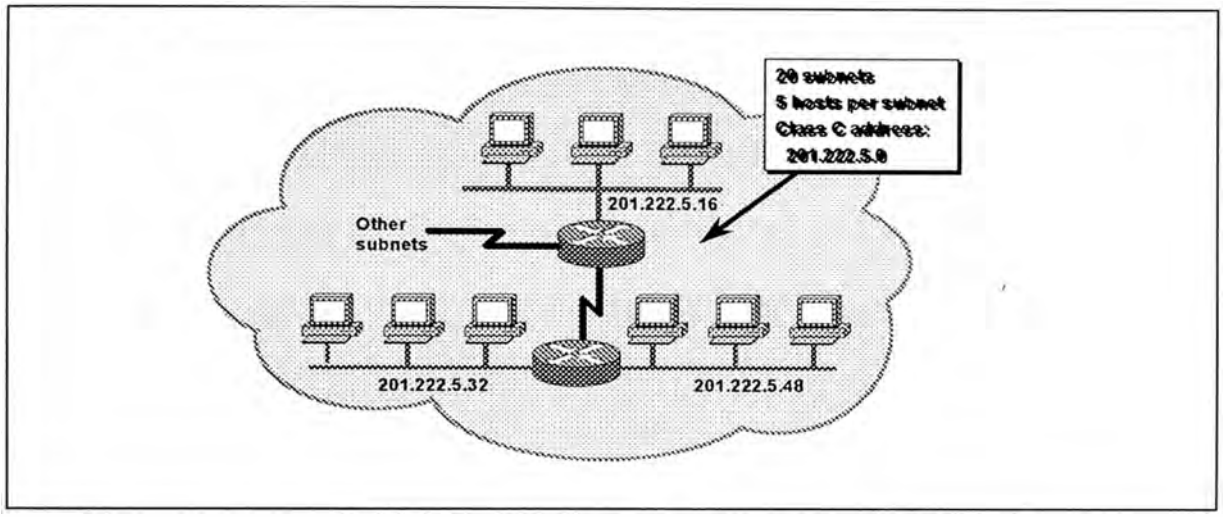


Figura 5-10 Considerar el número de Redes y Host por Network cuando se selecciona una máscara de subnet.

Seleccione un tamaño de campo de subnet que yield suficiente subredes. En este ejemplo, elegiendo una mascara de 5 bits permite tener 30 subnets (32-2=30 posibles subnets totalkes). En el ejemplo, las direcciones ded subnets son múltiples de 8, tales como 201.222.5.8, 201.222.5.16 y 201.222.5.24.

Los bits remanentes en el último octeto son usados en el campo de host. Los tres bits en el ejemplo permiten suficiente host para cubrir los cinco host requeridos por segemnto. Los números de host serían 1, 2, 3 y así sucesivamente.

La dirección de host final son una combinación de la red/subnet empezando con la dirección mas cada valor de host. Los host en el subnet 201.222.5.16 deberían ser direccionados como 201.222.5.17, 201.222.5.18, 201.222.5.19 y así sucesivamente.

La tabla 5-1 muestra un ejemplo planeamiento de subnet para una direcciónd e clase B; un ejemplo de enrutamiento combina una dirección IP llegando con la mascara de subnet para derivar al número de subnet. El número de subnet extraido debería ser típico do los subnets generados durante este ejercicio de planeamiento. Para una tabla extendida de subnetting, refierte al RFC 1878.

Nº BITs	MASCARA DE SUBRED	Nº DE SUBRED	Nº DE HOST
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

Tabla 5-1 Ejemplo de planeamiento de subnet para una dirección de clase B.

Clase B Subnet Planing Example.- Considere una subnet Clase B basada en la siguiente información.

Dirección de Subnet 172.16.2.0

Mascara de Subnet 255.255.255.0

El tercer byte entero de la dirección es disponible para subnetting; el cuarto byte entero es disponible para direcciones de host (172.16.2.1 a 172.16.2.254). La dirección de red para esta subnet es 176.16.2.0. La dirección broadcast para esta subnet es 172.16.2.255. La red tiene 8 bits de subnetting que provee hasta 254 subnets y 254 direcciones ded host.

Clase C Subnet Planning Example.- Las direcciones de clase C son mucho mas difícilespara subnet, por que se tiene que split up los últimos bytes dedntro de dos porciones: la porción de subred y la porción dee host. En la figura 5-11, una red de clase C es subnetting para proveer seis direcciones dee host y 30 subnets.

Nº BITs	MASCARA DE SUBRED	Nº DE SUBRED	Nº DE HOST
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Tabla 5-2 Ejemplo de planeamiento de subnet para una dirección de clase C.

La tabla 5-2 nos ayudaría en este proceso. La primera columna (Nº de bits) indica cuantos bits tiene que ser prestado desde la porción de host para crear una dirección de subred. La segunda columna (subnet mask) provee el valor decimal de la mascara de subnet usada. La tabla 5-2 también

indica el número de subredes y host por subred que son posibles con cada una de esas mascaras.

Tomemos una mirada a la subnet Clase C mostrada en la figura 5-10. Hemos masked off cinco bits de la porción ID de host para usar como el área de subnet (11111000). Ahora la mascara de subnet es como sigue:

255.255.255.248

11111111.11111111.11111111.11111000

El número de subnet es definido basado en la mascara, como mostrado en la figura 5-11.

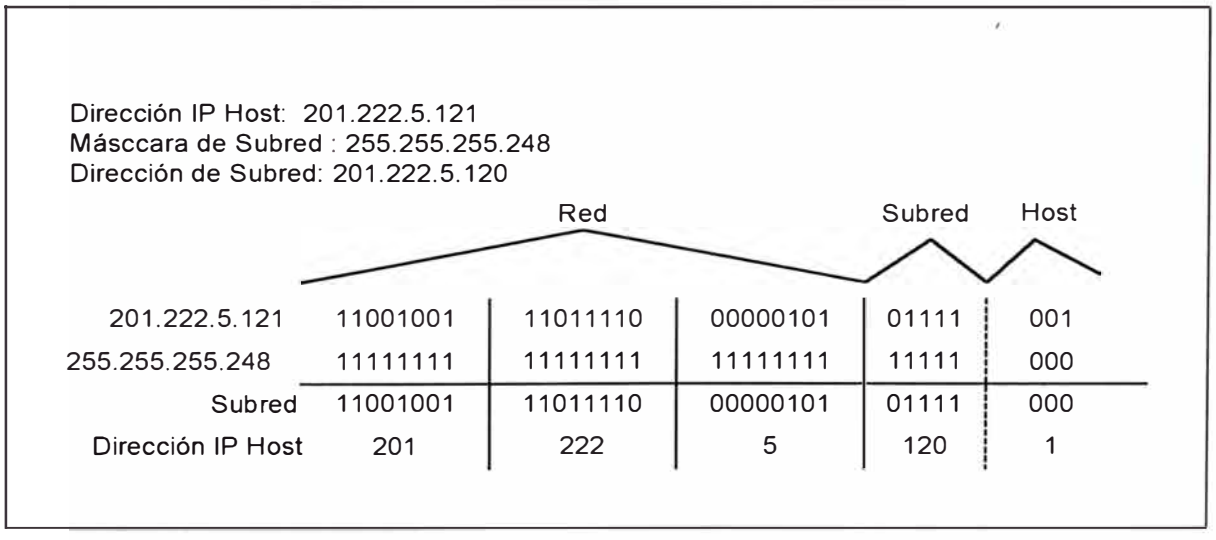


Figura 5-11 Préstarno de bits de la parte de Host para una crear subredes.

5.2.4.- Direcciones Broadcast

Broadcasting es soportado en el internet. Broadcast messages son aquellos que usamos para ver a cada host en la red. La dirección broadcast es formado usando todos unos dentro de una dirección de red IP.

Hay dos tipos de broadcast

- Broadcast dirigidos (subnet broadcast)
- Broadcast Flooded (Broadcast local)

El broadcast flooded (255.255.255.255) no son propagados pero son considerados broadcast local, como mostrado en la figura 5-12. Los broadcast dirigidos dentro de una red específica son permitidos y son enviados por el router. Estos broadcast dirigidos contienen toda la porción de host de la dirección configurados a uno unos.

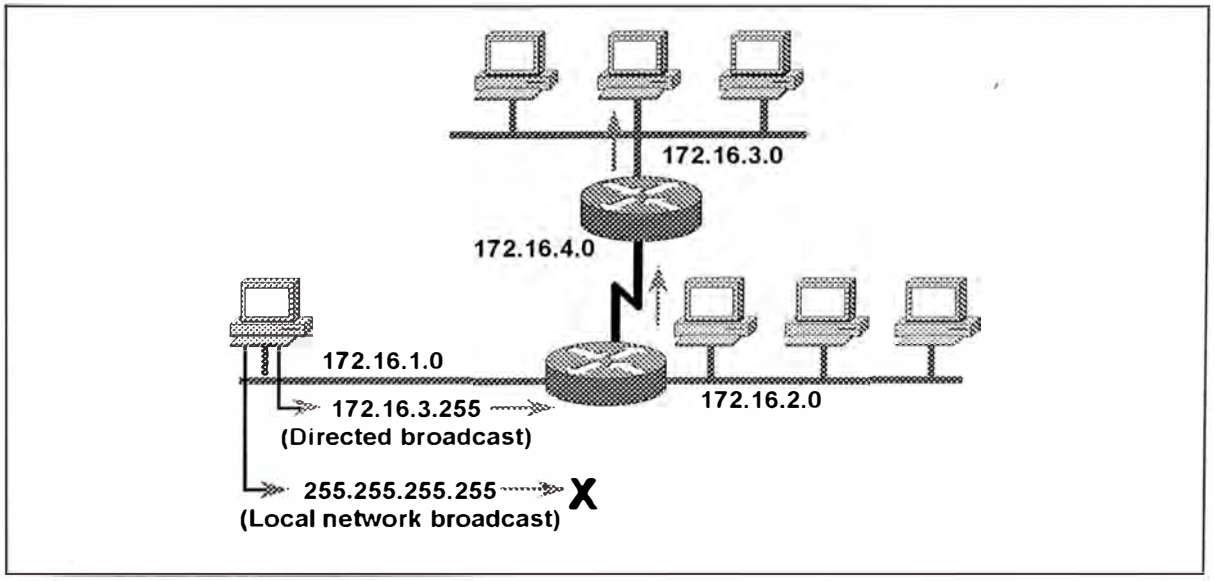


Figura 5-12 El Broadcast es alcansable a cualquier subnet.

Podemos también broadcast mensajes a todos los host dentro de una subnet y para todos los subnets en un red. Para broadcast un mensaje a todos los host dentro dee una subnet, la porción dee host de la dirección debe contener todos unos. El siguiente ejemplo broadcast mensajes para todos los host en al red 172.16, subnet 3 (asumiendo unamascara de 255.255.255.0)

Todos los host en una subnet específica : 172.16.3.255

Podemos también broadcasr mensajes a todos los host en todos los subnets dentro de una red. Para broadcast un mensaje a todos los host en todos los subnets dentro de una única red, la porción de host y la subnet de la dirección contendrían todos unos. El siguiente ejemplo broadcast mensajes a todos los host en todos los subnets en la red 172.16:

Todos los host en todos los subnets en una red específica : 172.16.255.255

5.3.- ENRUTAMIENTO IP

El enrutamiento IP es el proceso de enviar data desde un host en ua red hacia un host remoto en otra red a través de un o varios router. La ruta que un router usa para llevar un paquete esta definido en su tabla de enrutamiento. Una tabla de enrutamiento contiene las direcciones IP de las interfaces del router que conecta a las otras redes con el el router puede comunicarse. La tabla de enrutamiento es consultado para una ruta que en

la dirección de destino del paquete es indicado. Si no es encontrado una ruta, el paquete es enviado a la dirección por defecto del router (si y solo si uno es configurado). Por defecto, un router puede enviar paquetes a cualquier red para el cual tiene una interface configurada. Cuando un host intenta comunicarse con otro en una red diferente, IP usa la dirección gateway por defecto del host para llevar el paquete al router correspondiente. Cuando un router es ubicado, el paquete es enviado a la red apropiada, luego avanza hacia el host de destino específico. Si una ruta no es encontrada, un mensaje de error es enviando hacia el host fuente.

Cuando el destino de un datagrama es ubicado en una red vecina, el proceso de IP routing es muy directa. Con esta clase de situación, un router sigue un simple procedimiento como mostrado en la figura 5-13.

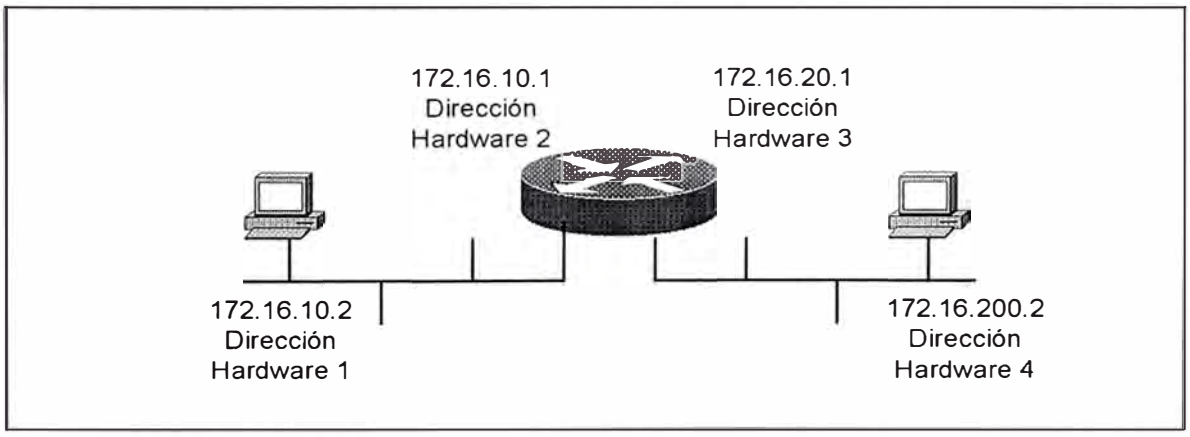


Figura 5-13 La figura un simple enrutamiento entre dios redes.

Primero, cuando una estación quiere enviar un paquete a un host destino (en esta instancia 172.16.10.2 transmite a 172.16.20.2), el host 172.16.10.2 verifica la dirección de destino IP. Si este determina que la

dirección no esta en la red local, entonces este tiene que ser ruteado. Luego, 172.16.10.2 llama con ARP (Address Resolution Protocol) para obtener la dirección hardware de su gateway por defecto. La dirección IP del gateway por defecto es configurado en la máquina 172.16.10.2, pero 172.16.10.2 aún necesita encontrar la dirección hardware del gateway por defecto. Para hacer esto, este verifica el cache ARP, y luego procede a direccionar el paquete con la nueva dirección de hardware obtenida de su router por defecto. La información utilizada para direccionar el paquete incluye:

- Dirección de hardware fuente 1
- Dirección IP fuente 172.16.10.2
- Dirección de hardware destino 2
- Dirección IP de destino 172.16.20.2

IP, en el router receptor con la dirección de hardware 2, establece que nos es el final, por la inspección de la dirección IP de destino del paquete. Esa dirección indica que tiene que ser enviada a la red 172.16.20.0. IP usa entonces ARP para determinar la dirección hardware para 172.16.20.2. Y el router pone la dirección de hardware nuevo identificado dentro del cache ARP para fácil referencia la próxima vez que es llamado para rutear un paquete a ese destino.

Finalmente, el router envía el paquete a la red 172.16.20.0 con una cabecera que incluye:

- Dirección ded hardware fuente 3
- Dirección IP fuente 172.16.10.2
- Dirección dee hardware destino 4
- Dirección IP destino 172.16.20.2

Como el paquete viaja a lo largo de la red 172.16.20.0, este mira la dirección hardware 4, con la dirección IP 172.16.20.2. Cuando un NIC (Network Interface Card) reconoce su dirección hardware, este grabs el paquete.

Es importante mencionar que en todos estos procesos, la direccción IP de la fuente y el destino no cambia, no así la dirección de hardware que cambia con cada salto que el paquete hace.

Pero como el router hizo para saber como enviar el paquete a la red 172.16.20.0?. Esto es posible gracias a la tabla de enrutamiento mantenidad en los router IP. IP consulta estas tablas para deeterminar dondee la red esta, para que esto pueda enviar su paquete allí. Las tablas de enrutamiento de cada internetwork comnpleja debería deesignar todas las rutas disponibles para una red destino, además provee un advising estimado de la eficiencia de cada ruta potencial. Las tablas de enrutamiento mantienen entradas de Where networks – not host – are located.

Las tablas de enrutamiento almacenan información de enrutamiento. El algoritmo de enrutamiento inicializa y mantiene estas tablas de enrutamiento. Inicialmente, un router conoce únicamente como alcanzazr las redes o subnets que estan directamente conectados a este.

Los routers aprenden las rutas hacia otras redes de tres maneras diferentes:

- Enrutamiento Estático
- Enrutamiento por Default
- Enrutamiento Dinámico

Enrutamiento Estático.- Las rutas estáticas requieren que la tabla de enrutamiento sea construido y actualizado manualmente. Si una ruta cambia, las rutas estáticas no comparten automáticamente esta información para comunicar a los otros hacerca de los eventos. Un administrador tiene que manualmente actualizar las entradas de las rutas estáticas en cualquier lugar donde los cambios de topología de red es requerido.

Un beneficio para crear rutas estáticas es que el ancho de banda es conservado, debido a que el broadcast que envía los router para actualizar las rutas no son enviadas continuamente sobre la red. Otra ventaja es la seguridad. Con enrutamiento estático, los routers conocen únicamnete lo que tu quieres que conozcan.

Es buena idea limitar rutas estáticas para los destinos remotos alcanbles a través ded un único router. El enrutamiento estático debería también ser usado cuando una red es alcanzable por únicamente una ruta (llamado un stub network). Configurando rutas estáticas para stub networks, el overhead adicionado de actualizaciones dinámicas es evitado.

Las rutas estáticas pueden ser configurados en los equipos Cisco por el comando ip route. Por ejemplo, configure una ruta estática para una red remota de 172.16.50.0, nosotros usaremos el siguiente comando:

IP Command	Remote network	Subnet Mask	Default gateway
IP route	172.16.50.0	255.255.255.0	172.16.20.2

Entonces el router ya sabe que cualquier paquete proveniente de la dirección de red fuente 172.16.50.0 será direccionado a la dirección IP 172.16.20.2. El router tendría luego que enviar el paquete a su destino final o dropear o descartar el paquete por que no tiene una ruta para la red de destino.

Unos ejemplos de configuración de rutas estaticas son mostradas a continuación a través de la red siguiente:

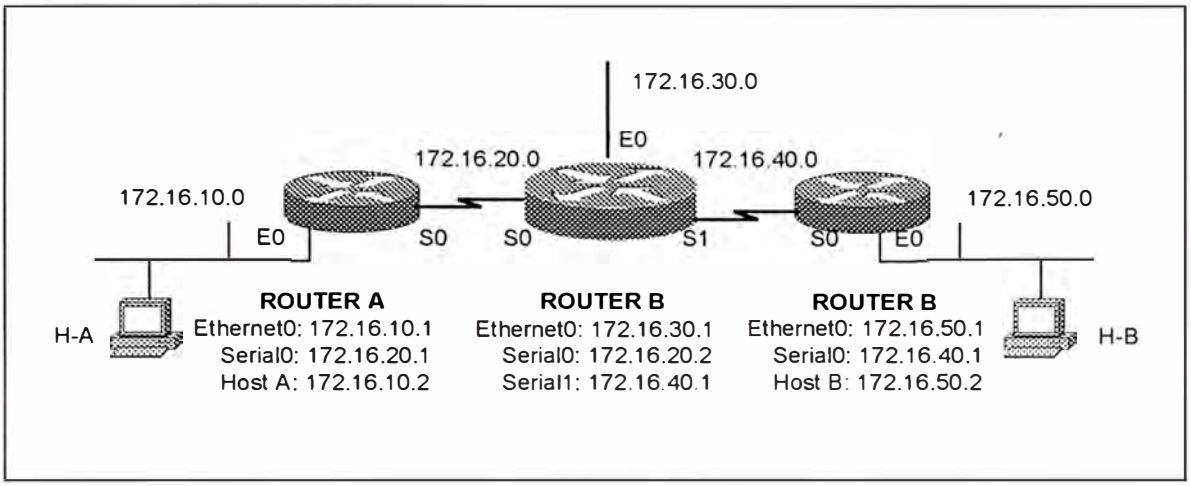


Figura 5-14 Ejemplo de una interconexión de routers en una internetwork

Configurando el router A

```
RouterA#Config t
Enter configuration commands, ine per line. End with CNTL/Z.
RouterA(config)#ip route 172.16.30.0 255.255.255.0 172.16.20.2
RouterA(config)#ip route 172.16.40.0 255.255.255.0 172.16.20.2
RouterA(config)#ip route 172.16.40.0 255.255.255.0 172.16.20.2
RouterA(Config)# Z
RouterA#copy run star
```

Configurando el router B

```
RouterB#Config t
Enter configuration commands, ine per line. End with CNTL/Z.
RouterB(config)#ip route 172.16.10.0 255.255.255.0 172.16.20.1
RouterB(config)#ip route 172.16.50.0 255.255.255.0 172.16.40.2
RouterB(Config)# Z
RouterB#copy run star
```

Configurando el router C

```
RouterC#Config t
Enter configuration commands, ine per line. End with CNTL/Z.
RouterC(config)#ip route 172.16.10.0 255.255.255.0 172.16.40.1
RouterC(config)#ip route 172.16.20.0 255.255.255.0 172.16.40.1
RouterC(config)#ip route 172.16.30.0 255.255.255.0 172.16.40.1
RouterC(Config)# Z
RouterC#copy run star
```

Enrutamiento por Defecto.- En primer lugar una ruta por default deberia debería ser configurado en cada router para que si un router no conoce la ruta para cierta red, este pueda usar esta ruta por default como un host usa un default gateway. Configurandio rutas por default en los router Cisco es realizado de la misma manera que las rutas estáticas; sin embargo, tu creas una entrada dee ruta por default usando la red y la mascara de subnet de todos ceros. Por ejemplo , para configurar la ruta por default para el router A de la figura (pag 194 ccna)+

Router A (config)// ip route 0.0.0.0 0.0.0.0 172.16.20.2

Esto le dice al router A que si no conoce que hacer con un datagrama, este lo debería de enviar a 172.16.20.2 (la interface del router B). Para el router B y C, se configura las rutas por defecto de modo similar.

Enrutamiento Dinámico.- El desarrollo de este tema se verá con mas detalle en la siguiente sección.

5.4.- ENRUTAMIENTO IP DINÁMICO

En grandes interredes, el enrutamientos dinámico es generalemnte el método de elección, por que el mantenimiento manual de las tablas de enrutamiento estático sería completamente tediosos (por no decir imposible) para los administradores de red. Diferentemente, solo unas configuraciones mínimas son necesarias con enrutamiento dinámico.

En esta parte analizaremos el enrutamiento dinámico y exploraremos como los routers se comunican y que protocolos son usados. Examinaremos los diferentes clase de protocolos de enrutamiento dinámico que son aplicados. Los protocolos de enrutamientos dinámico se agrupan en dos grandes grupos: Protocolos de Enrutamiento Interior y Protocolos de Enrutamiento Exterior.

5.4.1.- Sistemas Autónomos

Un sistema autónomo es un conjunto ded routers y redes bajo una mismoa administración. Un sistema autónomo puede consistir de un router directamente conectado a una LAN a Internet; o un sistema autónomo puede ser una red corporate enlazando muchos redees locales a través de un backbone corporate. El sistema autónomo presenta una consistente vista ded enrutamiento hacia el mundo exterior. Para que un router belong to un sistema autónomo, todos los routers en ese sistema deben estar:

- Interconectados
- Corriendo el mismo protocolo de enrutamiento
- Asignado al mismo sistema autónomo

El Network Information Center (Inter NIC) asigna un único sistema autónomo a enterprices. Este sistema autónomo es un número dee 16 bits. Un protocolo de enrutamiento tal como Interior Gatway Routing Protocol (IGRP) requier e que se especifique ese único número de sistema

autónomo asignado en la configuración. Un número de sistema autónomo es necesario si la organización planea usar un exterior router protocol, tal como un Border Gateway Protocol (BGP). Si la compañía lleva a cabo únicamente Interior routing, se necesita únicamente se necesita consistencia y uniqueness dee número de sistemas autónomos dentro de la organización.

5.4.2.- Protocolos de Enrutamiento Interior

El enrutamiento interior es implementado en la capa internet del protocolo TCP/IP. Un router interior puede usar un protocolo ded enrutamiento y un algoritmo de enrutamiento para aconplish routing.
Ejemplos de protocolos de enrutamiento IP interior incluyen:

- RIP : Un protocolo de enrutamiento distance-vector
- IGRP: Un protocolo de enrutamiento distance-vector propietario de Cisco
- OSPF: Protocolo de enrutamiento Link-State
- Enhanced IGRP: Un protocolo de enrutamiento distance-vector balanceado propietario de Cisco

Los protocolos de enrutamiento mencionados, anteriormente pueden ser clasificados en dos categorias básicas: Distance-vector y Link-state

- Distance-vector entiende la dirección y distancia para cualquier conexión de red a una interred. Distance-vector escucha información de segunda mano para obtener sus actualizaciones.

- "Link-state", ó "shortest path first", entiende la red entera mejor que "distance-vector" y nunca escucha información de segunda mano. Por tanto este puede hacer decisiones de enrutamiento en forma mas precisa e informado.

"Distance-Vector".- Que sucede cuando un enlace se cae o se quiebra?. Todos los routers tienen que informar a los otros routers para actualizar su tabla de enrutamiento. Pero algunas veces se escucha a algunas personas lamentarse que el protocolo de enrutamiento baja la performance de su red. Eso puede ser causado por el tiempo de convergencia.

Pero que es el tiempo de convergencia?. Es el tiempo que toma a todos los routers actualizar sus tablas de enrutamiento cuando una reconfiguración, ó un enlace cae, básicamente cuando ocurre un cambio. Ningún dato es transferido durante ese tiempo, y un "slow-down" es inminente. Una vez que la convergencia es completada, todos los routers dentro de la "internetwork" están operando con el mismo conocimiento de la red, y se dice que la "internework" ha convergido. Si la convergencia no ocurre, los routers tendrán sus tablas desactualizadas y harán decisiones de enrutamiento basados en una información potencialmente inválida.

Los protocolos de enrutamiento "distance-vector" actualizan cada 30 y 90 segundos. Cuando ellos hacen eso, permiten que los routers transfieran su tabla de enrutamiento completa a los otros routers conocidos.

Como ejemplo, supongamos que tenemos tres routers A, B y C, como mostrado en la figura 5-15. El router A tiene conexiones directas a la red 1 y 2. El router B tiene conexiones directas a la red 2 y 3. El router C tiene conexiones directas a la red 3 y 4

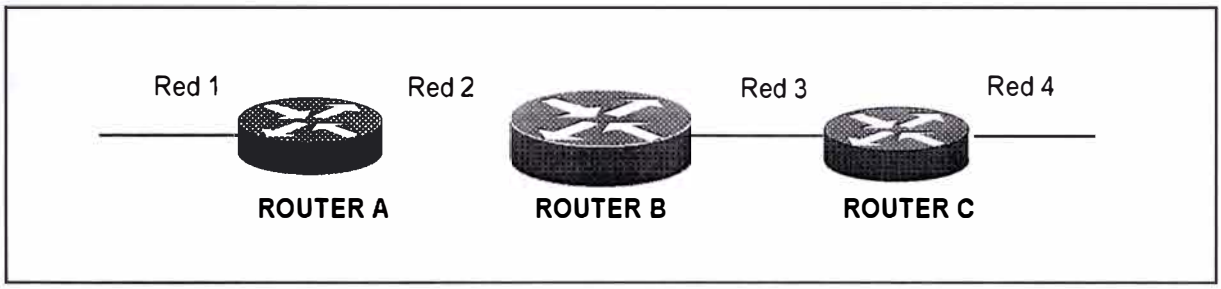


Figura 5-15 Tablas de enrutamiento Distance – vector.

Cuando los routers distance-vector inician su power on, Ellos logran conocer a sus vecinos; es decir aprenden métricas (hops) hacia los otros routers en cada una de las interfaces de red. Como los updates para network-discovery de distance-vector continúan (cada 30 segundos para RIP), los routers descubren la mejor ruta a la red de destino. Las rutas son calculadas por y basadas en el número de saltos (hops) que hacen en cada router. En la figura 5-15, el router C conoce que el router B está conectado a la red 1 por una métrica igual a 1. Esto quiere decir que se tiene que estar en una métrica de dos para que el router C llegue a la red 1. El router C nunca estaría al tanto de la red entera, este únicamente conoce de segunda mano lo que es llamado como "chismorreo".

En cualquier lugar que la toplogía ded red cambia por cualquier razón, las actualizaciones de la tabla de enrutamiento ocurren debido a que cada router envía su tabla de enrutamiento entera en forma de broadcast a todos los otros routers. Cuando un router recibe la tabla, compara con su propia tabla. Si este descubre una nueva red, o que este considere un camnio mas rápido para llegar, este actualiza su tabla acorde con es ainformación.

- Hop Count: Cual es el mejor camino a una red?. Distance-vector menciona que " cuanto mas pocos saltos es mejor", y usa únicamente hop count cuando hace sus desciciones de enrutamiento. Observemos la figura 5-16.

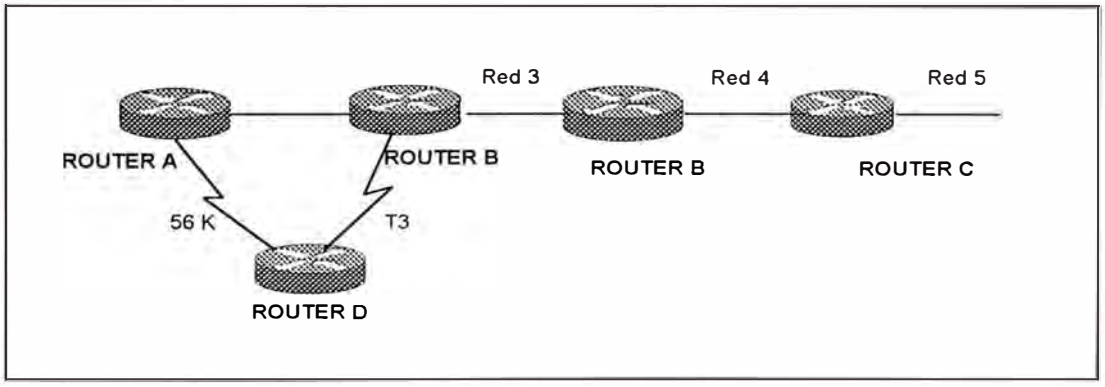


Figura 5-16 Descisiones de red Distance – vector.

El router A esta consiguiendo al router D a través de un enlace Wan de 56 KB. El router A puede también alcanzar al router D via el router B, el cual puede conseguir al router D a través de una enlace T3. Cual es mas rápido?. De acuerdo a distance-vector, la ruta mas rápida debería ser a través de 56 KB. Imagina enviar un archivo ded

500 MB a un server plugged dentro ded un hub yendo al router D. Este debería tomar todo el día (y noche). Pero por que se deberia elegir esta ruta?. Por que distnace-vector usa únicamente métricas (hops) para sus descciones de enrutamiento, y en su opinion, un hop es mejor que dos. La solución por supuesto, es to lie al router A que la métrica al router D via 56 KB es realmente tres. Este puede ser hecho manualmente y causaría que el router A determine uqe dos hops son mejor que tres.

- Routing Loops: Un problema con distance-vector es el routing loops. Este puede ocurrir por que cada router no se actualiza a la misma vez. Permítanos decir que la interface a la red 5 en la figura (pag 216 ccna) falla. Todos los router saben hacerca de la red 5 desde la red E. El router A, en su tabla, tiene una ruta a la red 5 a través de los routers B, C y E. Cuando la red 5 falla, El router E le dice al router C. Esto provoca que el router C pare de enrutar a la red 5 a través del router E. Pero los routers A, B y D no conocen ded la red 5 aún, y por lo tanto continúan enviando información de updates. El router C eventualmente enviaría su update y causa que el router B pare de enrutar a la red 5, pero el router A y el D no están actualizados todavía. Para el router A y D, este aparece que la red 5 está aun disponible a través del router B con una metrica de tres.

Entonces el router A enviaría su mesage regular de 30 segundos " hello, I´m still here-estos son lso emnsajes que yo conosco", el cual incluye reachability para la red 5. Los routers B y D reciben luegola noticia que la red 5 puede ser alcanzada desde el router A. Entonces los routers B y D envían la onformación que la red 5 es disponible. Cualquier paquete destinado a la red 5 iría hacia el router A al B y luego retornaría al router A. Este es un routing loop.

- Counting to Infinity: El problema de los routing loop descrito es llamado counting to infinity, y es causado por d}gossip y mala información que se ha comunicado y progado a través de la red. Sin alguna forma de intervención, cada vez que un paquete pase a través de un router, el hop count debería incrementarse indefinidamente.

Una forma de resolver este problema es deefinir un maximo hop count. Distance-vector permite un hop count de hast un valer de 15, cualquier cosa que requiera 16 hops es considerado inalcanzable. En otras palabras, después de un loop de 15 hops, la red 5 sería considerado down. Esto significa que contando a infinito, también conocido como exceeding TTL, mantendría paquetes viajando alrededor deel loop indefnidamente. Los paquetes aún serían attracted deentro deel loop, pero en vez de viajar en un unchecked, ellos solo whirl alrededor por 16 bounces y luego mueren.

- Split Horizon: Otra solución al problema de routing loop es llamado "split horizon," este reduce la información de enrutamiento incorrecta y la cabecera de enrutamiento en una red distance-vector a través de la regla que indica que la información no puede ser enviada de regreso en la misma dirección desde el cual la información fue recibida. Esto debería prevenir al router A de enviar información actualizada que recibió del router B de regreso al mismo router B.

- Route Poisoning: Otra forma de evitar el problema causado por actualizaciones inconsistentes es llamado route poisoning. Cuando la red 5 cae. El router E inicia el route poisoning, ingresando una tabla de entrada para la red 5 como 16 o inalcanzable (algunos veces referido como infinito). Si hacemos inalcanzable la ruta a la red 5, el rouer E no es suceptible a incorrectas actualizaciones de rutas a la red 5. El router E mantendría su información en su tabla hasta que la red 5 se levante otra vez, en ese punto, este dispararía un update para notificar a sus vecinos del evento.

  Route poisoning y triggered updates mejorarían el tiempo de convergencia, ya que los router vecinos no tiene que esperar 30 segundos antes de advertir la ruta hecha inalcanzable (poisoned).

- Hold Down: Este trabaja con rutas poisoning para prevenir mensajes de update regulares que reingresan una ruta que se ha caido. Hold-

down" ayuda a prevenir que las rutas cambien muy rápidamente, permitiendo que las rutas caidas retornen a "up" ó que las redes se estabilizen antes de que cambie a la próxima mejor ruta. "Hold-down" le dice a los routers que restringa por un periodo de tiempo especifico, cualquier cambio que pueda afectar recientemente las rutas retiradas.

"Hold-down" usa "trigger updates", el cual reinicia el "hold-down timer", para permitir que los routers vecinos conozcan los cambios en la red. Hay tres instancias para el cual el "trigger updates" reiniciaría el "hold-down timer":

1. Expira el HD timer
2. El router recibe un procesamiento proporcional al número de enlaces en la red.
3. Otro "update" es recibido indicando que el estado de la red ha cambiado.

"Link-State".- Inversamente, el algoritmo de enrutamiento "link-state" mantiene una tabla mas compleja de información topólogica. Los routers usando "link-state" son previligiados para un completo entendimiento y vista de todos los enlaces de los routers distantes, mejor que como se interconectan ellos. El proceso de enrutamiento "link-state" usa "link-state packets" (LSP) ó " hello packets" para informar a los otros routers de enlaces distantes. Adicionalmente usa base de datos topológicas, el algoritmo "shorest path first" (SPF) y por supuesto una tabla de enrutamiento.

El descubrimiento de la red se hace en forma diferente en "distance-vector" que en "Link-state". Primero, los routers intercambian "hello packets" (LSP) dándole a ellos una vista completa de la red entera. En esta fase inicial, cada router comunica únicamente sus enlaces directamente conectados. Segundo, todos los routers recogen todos los LSPs recibidos desde la red y construyen una base de datos topológica. Después de eso, el SPF calcula como cada red puede ser alcanzado, encontrando ambos, la más corta y más eficiente ruta a cada red "link-state" participante. Cada router crea una estructura de árbol, el cual por si solo representa el "root".

Los resultados son formados dentro de una tabla, completando con un listado de las mejores rutas. Una vez que estas tareas han sido completados, los routers pueden usar la tabla para "packet-switching" del tráfico de datos.

A diferencia de "distance-vector", "link-state" entiende que con la finalidad de que un paquete llegue desde un router A a un D eficientemente, la ruta mas corta es vía el T3. El router sabe esto, por que simplemente no se bazó en la decisión de "hop count", y por que también analiza cosas como disponibilidad de ancho de banda y la cantidad de congestión que existe en el enlace para concluir que es verdaderamente la mejor ruta a un destino determinado.

Los routers link-states también manipulan convergencia de una manera completamente diferente que los routers distance-vector. Cuando la topología cambia, el router o los routers que primero become aware del evento envía información a todos los otros routers participando con el algoritmo link-state. O envia las noticias a un router específico que es designado para consultar las tablas de updates.

- Un router participando en una red link-sate tienen que hacer los siguiente con la finalidad e converger:
- Recordar los nombres d elos vecinos, cuando estan activos o caidos, y el costo de la ruta a ese router.
- Crear un LSP que liste los nombres de sus vecinos y los costos relativos.
- Envia el LSP creado recientemente a todos los otros routers participando en la red link-state.
- Recibir los LSP´s deesde otros router y actualizar su propio base de datos.
- Construir un mapa completo de la topología de la internetwork desde todos los LSP recibidos, luego computar la mejor ruta a cada destino de red.

En cualquier lugar que un router reciba un paquete LSP, este recalcual la mejor ruta y actualiza la tabla de enrutamiento acćordingly.

"Balanced Hybrid".- O enrutamiento balanceado, combina y usa lo mejor de ambos algoritmos "distance-vector" y "link-state".

Aunque la ventaja híbrida que emplea "distance-vector" con conteo de métricas mas precisas que el normal, para determinar la ruta a una "internetwork", este puede converger rápidamente gracias al uso de "trigger link-state". Adicionalmente, el "Balanced hybrid" usa un protocolo "link-state" mas eficiente que ayuda a mitigar el problema de alto ancho de banda, potencia del procesador y necesidades de memoria.

Algunos ejemplos de protocolos son OSI´s IS-IS (Internediate System Routing Protocol).

A continuación explicaremos el funcionamiento de los protocolos de enrutamiento interior.

"Routing Information Protocol" (RIP).- RIP (e IGRP) siempre resumen la información de enrutamiento hacia un número de red mayor. Los llamados "clasfull routing". "Classless" y "prefix routing protocol" permiten un continuo bloque de "hosts", "subnets", o redes, a ser representados por una única ruta. RIP es un protocolo de enrutamiento "classfull" y no soporta prefijos de enrutamiento.

RIP es un protocolo de enrutamiento distance-vector que practica enrutamiento classfull, el cual es usado para descubrir el costo de una ruta dad en terminos de hops y almacena es ainformación en us tabla de enrutamiento.

El router puede luego consultar la tabla seleccionando el menos costoso y mas eficiente ruta a su destino. Este gathers información observando una tabla de enrutamiento que fue broadcasting por otro router y actualiza sus propia tabla de enrutamiento en el evento que un cambio ocurre.

RIP es especificado en el RFC 1058 y actualizazdo con el RFC 1723. Algunas dee las diferencias definidas en RFC 1723 sion adicionados características de seguridad. Los mensajes RIP son ahora permitidos para llevar mas información en sus updates.

- Tablas de Enrutamiento RIP: Las tablas de enrutamiento RIP proveen la siguiente información:
    a. Direccion de destino IP
    b. Una métrica (numerado de 1 a 15) indicativa del costo total, en hops, de una ruta particular a un destino
    c. La dirección IP del próximo router que un datagrama debería alcanzar en la ruta a su deestino.
    d. Un marcador señalizando el reciente cambio a un router

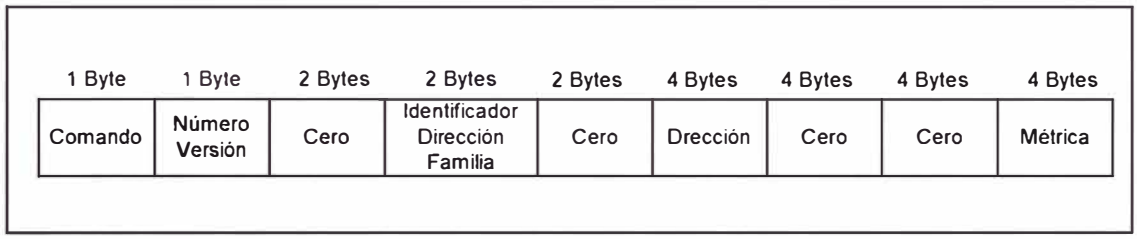
e. "Timers", el cual son usados para regular la performance
f. "Flags", el cual indica si la información acerca del router recientemente ha cambiado.
g. "Hold-down", usado para prevenir los mensajes "update" regulares, al reinstalar una ruta que no es funcionalmente mas grande.
h. "Split-horizon" usado para prevenir lazos.
i. Un "poison revers update" usado para prevenir grandes lazos de enrutamiento.

RIP envía actualizaciones de enrutamiento en intervalos de tiempo regulares y en cualquier lugar que ocurra un cambio de topología.

Cuando un router que esta operando RIP recibe nueva información indicando una mejor ruta a su destino, la nueva información reemplaza a la antigua en su tabla. Por ejemplo, si un router pierde un enlace, este router realiza un nuevo cálculo de las rutas en su propia tabla y luego envía la información revisada a todos los vecinos. Cada router recibiría esta información, actualizaría su tabla en concordancia, y enviaría la información a todos sus vecinos.

- Formato de Paquete RIP: De todas las cosas vistas, podemos decir que RIP puede ser muy usual en enrutamiento dentro de "internetwork" homogéneos de tamaño pequeño ó moderado. Pero, su

pequeño limite de hops count y la única métrica no permitiría realmente mucha flexibilidad en ambientes complejas y en realidad, puede causar un problema o dos. La figura 5-17 muestra un formato de paquete RIP.



1 Byte	1 Byte	2 Bytes	2 Bytes	2 Bytes	4 Bytes	4 Bytes	4 Bytes	4 Bytes
Comando	Número Versión	Cero	Identificador Dirección Familia	Cero	Drección	Cero	Cero	Métrica

Figura 5-17 Formato de paquete RIP.

Los siguientes puntos resumen los campos en un pauete RIP:

a. El campo command indica si el paquete es una solicitud o una respuesta. Una solicitud es un paquete de un router que solicita a otro router enviar todos o parte de su tabla de enrutamiento.
b. El version number especifica que versión de RIP esta siendo implementado. Desde que allí puede haber diferentes versiones de RIP implementado, este número puede actualmente estar especificando imlementacines diferente, potencialmente incompatibles.
c. El address family identifier sigue un campo dee 16 ceros. Este identifica el tipo dee esquema de dirección usado por una dirección destino para el cual la informaciónd eactualización

esta siendo dado o sought en el paquete RIP. El campo mostraría una valor de dos cuando es usado RIP.

d. Otro campo de 16 ceros precede el campo address. Este campo contiene la dirección de un destino, y existe como un update para el recptor del paquete RIP o una solicitud para el enviador del paquete for update informationn about routes to it.
e. El campo metric sigue dos mas, el campo de 32 bits, y especifica el hop count para el destino y addres family y las direcciones fueron dados en el campo precedente. Hasta 25 destinatarios pueden ser listados en un simple paquete RIP. Si mas que 25 entradas necesitan ser enviados, el router enviaría su update tan pronto como sea necesario.

- RIP Timers: RIP usa timer para regular su performancia:
    a. Routing update Timer: Este configura el intervalo (tipicamente de 30 segundos) entre los updates de enrutamiento periódico en el cual el router envía una copia completa dee sus tabla de enrutamiento a todos vecinos.
    b. Route Invalid Timer: Este determina la longitud de tiempo que tiene que expirar (90 seg) antes que un router determine que una ruta has become inválido. Esto conlleva a esta conclusión, si este no ha escuchado cualquier update acerca de euna ruta particular para ese periodo. Cuandoe so ocurre, el router

enviaría updates a todos los vecino letting them know que la ruta es inválida.

c. Route Flash Timer: Este configura el tiempo enttre una ruta becoming inválida y su removal desde la tabla de enrutamiento (240 seg). Antes de que este removido de la tabla, el router notifica a suss vecinos de ese doom impending. El valor ded la ruta inválida timer tiene que ser menos que de la ruta flush timer. La razón para esto es proveer al router con suficiente tiempo para decirle a sus vecinos acerca de la ruta inválida antes que la tabla de enrutamientos sea actualizada.

Interior Gateway Routing Protocol (IGRP).- IGRP es tambien un protocolo de enrutamiento distance-vector que es propietario de cisco. Cisco desarrolló el protocolo IGRP en respuesta al RIP's shortcomings cuando usado en grandes sistemas autónomos. IGRP tiene un huge hop count limit de 255 en vez ded los 15 que tiene RIP.

- Tablas de Enrutamiento IGRP: Para construir la tabla de enrutamiento, IGRP puede usar lo siguiente:
    a. Metric: Estos puededn estar entre 1 y 255; configurados por el administrador para influenciar la selección de ruta.
    b. Delay: La velocidad dedl medio en velocidades de 10 milisegundos. Para 10 Mbps Ethernet, el delay es de 100, o un ms.

c. Bandwidth: Estos valores reflejan las velocidaddes de 1200bps a 10 Gbps.
d. Reliability: Representado en fracciones de 255 (donde 255 es el óptimo)
e. Load: Representa la saturación del enlace en una fracción de 255 (donde 0 equivale a sin carga)

IGRP puede tomar todas estas consideraciones cuando hace desciciones, y los administradores pueden ajustar las configuraciones de IGRP para ayudar a encontrar las necesidades de performancia individual de la red.

Para mejorar la estabilidad de operación IGRP emplea lo siguiente:

1. Multipath routing: Líneas duales de igual ancho de banda pueden correr un simple stream de tráfico en un round-robin fashion. Este adquiere la performancia y la redundancia si es que una linea se cae.
2. Hold-downs: Usado para prevenir mensajes de updates regulares que puedan habilitar líneas caidas. Si una ruta cae durante una convergencia, este prevendría a los router que no hayan escuchado la noticia de la línea caida, a tarvés del engaño que se hace a los otros routers, de que ellos tienen una ruta para esa ruta. Hod-down le dice a los routers que retengan cualquier cambio que podría afectar las rutas por un periodo de tiempo especifico. Este periodo es mas grande que

el periodo de tiempo necesario para actualizar la red entera con un cambio de enrutamiento.

3. Split Horizon: La información nunca es enviado de regreso al router desde el cual llegó, esto para prevenir lazos de enrutamiento. Algunas veces, hold-down debería prevenir efectivamente los lazos de enrutamiento, pero IGRP usa split hrizon para esto. Haciendo eso, provee extra estabilidad del algoritmo.
4. Poison revers updates: Usado para corregir grandes lazos. Los incrementos en las métricas de enrutamiento son generalmente indicativos de lazos de enrutamiento. Poison revers es usado para remover el problema de rutas y ubicarlo en hod-down .

- IGRP Timer: Para controlar la performancia, IGRP incluye timers con configuraciones por defecto para cada uno de los siguiente:
    1. Update timer: Estos especifican como los mensajes de actualizacion de enrutamiento deberían ser enviados frecuentemente. El valor por defecto es de 90 segundos.
    2. Invalid Timers: Este especifica cuanto tiempo un router debería esperar antes de declarar una ruta como inválida, por que no recibió un update específico acerca de este. El valor por defecto es tres veces el periodo de update.

3. Hold-down tiemrs: Este especifica el periodo de hold-dowm . El valor por defecto es tres veces el periodo de update timer, mas 10 segundos.
4. Flush timer: Este indica cuanto tiempo debería pasar antes de que una ruta deberia ser flushed de la tabla de enrutamiento. El valor por defecto es siete veces el periodo de routing update.

- Rutas IGRP: IGRP advierte tres tipos de rutas:
    1. Interior: Estos son rutas entre subnets. Si una red no esta subnetted, entonces IGRP no advierte rutas interiores.
    2. System: Estos son rutas a redes dentro de un sistema autónomo. Ellos son derivados de interfaces directamente conectados, otra ruta IGRP, o acceso a servidores. Ellos no incluyen información de subnet.
    3. Exterior: Estos son rutas a redes fuera de un sistema atónomo. Ellos son considerados al indentificar un gateway ded last resort. El gateway de last resort es elegido desde la lista de rutas exteriores que provee IGRP.

Una distancia administrativa o métrica pueden ser usados para representar el trustworthiness de una fuente de routing update. Cada tipo de ruta y protocolo ded enrutamiento es asignado una distancia administrativa particular. Cuanto mas alto sea el valor, menos verdadero es la fuente.

La tabla 5-3 muestra las actuales distancias administrativas.

RUTAS FUENTES	DISTANCIA POR DEFECTO
Interface Conectado Directamente	0
Rutas estáticas	1
Rutas resumen Enhanced IGRP	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100

Tabla 5-3 Distancias administrativas por defecto.

Notar que el valor por defecto de RIP es 120 y de IGRP es 100. Esto quiere decir que el router creerá en una ruta ingresada por IGRP priorizandola sobre una ruta ingresad por RIP.

Open Shortest Path First (OSPF).- Desde que OSPF esta basado en algoritmos link-state, es conocido como un protocolo de enrútamiento link-state, y que es desarrollado dentro de un sistema autónomo. Cuando el protocolo es OSPF, cada router retiene su propio base de datos describiendo la topología deel sistema autónomo en el que es localizaado.

Esta clase de sistemas es mucho mas flexible y tiene las siguientes ventajas adicinales:

- Los administradores de red son libres de asignar un costo a un enlace particular. El costo total para una ruta dada no necesariamente tiene que tener un límite. Este puede acomodar enormes redes ya que su límite de métrica superior es de 65535. Como cada nodo crea una base de datos de árbol link-state, representando la red como el root del arbol, esta bien equipado para elegir la ruta mas directa a un destino dado. Si mas de una ruta de igual costo existe, los routers OSPF pueden balancear la carga del tráfico de red entre todas las rutas disponibles de igual costo-efectivo.
- Las advertencias de enrutamiento link-state son "broadcasted" con menos frecuencia (únicamente cuando los cambios son detectados) reduciendo el overhead de la red.
- Los paquetes de routing update de link-state pueden efectivamente llevar información para mas de un router. Este tipo de paquete es enviado únicamente a los router adyacente o vecinos, que son seleccionados para intercambiar información de enrutamiento. Este es un arreglo "tell a friend" que contribuye a mejorar la eficiencia de la red.
- Aunque pensar que OSPF es un protocolo de enrutamiento interior, este puede recibir y enviar rutas a otros sistemas autónomos.

Caracteristicas adicionales ofrecidas por OSPF incluyen:

- Type of service routing (TOS)
- Soporte pára una o mas métricas

- Mascara de subred de longitud variable. (VLSM)

Enhanced Interior Gateway Routing Protocol (EIGRP).- IGRP es un protocolo de enrutamiento propietario de Cisco y combina las ventajas de protocolos de enrutamiento link-state con los de distance-vector, de tal manera que es considerado un protocolo de enrutamiento híbrido. Este emplea el distance-vector para determinar la mejor ruta a la red de destino, pero se asemeja a un protocolo link-state, en la manera que este usa cambios topológicos para disparar los updates de la base de datos de enrutamiento.

EIGRP incluye las siguientes características:

- Rápida convergencia
- Mascara de subnet de longitud variable (VLSM)
- Partial-bounded updates
- Soporta multiprotocolo: IPX, IP, Apple Talk

A diferencia de RIP, EIGRP no hace actualizacines periódicas. Cuando un router EIGRP se comunica primero con sus vecinos, este recibe la tabla de enrutamiento completa de ellos. Después de la comunicación inicial, este envía únicamente cambios (o updates parcial). También envía estos cambios únicamente a los routers vecinos que deberían ser afectados por el cambio. Este campo mejora el ancho de banda y aclara la eficiencia de Enhanced IGRP.

5.4.3.- Protocolos de Enrutamiento Exterior

Los protocolos dee enrutamiento exterior fueron diseñados para la comunicación entre diferentes sistemas autónomos (AS). Estos protocolos son mas complejos que el protocolo de enrutameinto interior, debido a que necesitan poseer mas información acerca de grandes números de routers.

Exterior Gateway Protocol.- Aunqie exterior gateway protocol es un protocolo dinámico, usa un simple diseño. Su actualizazcines de enrutamiento especifican que únicamente ciertas redes son accesibles a través de routers específicos. EGP no usa métricas como los protocolos de enrutamiento interior, por lo tanot este no puede detectar o corregir lazos de enrutamiento.

EGP es un protocolo distance-vector que permite a lso AS comunicarse a travé de una red de enrutamiento core que conecta a los As juntos. Estos AS´s tiene únicamente una conexión hacia el core, y pueden conectar a otros únicamente a través del core. La figura 5-18 muestra como este core EGP parece.

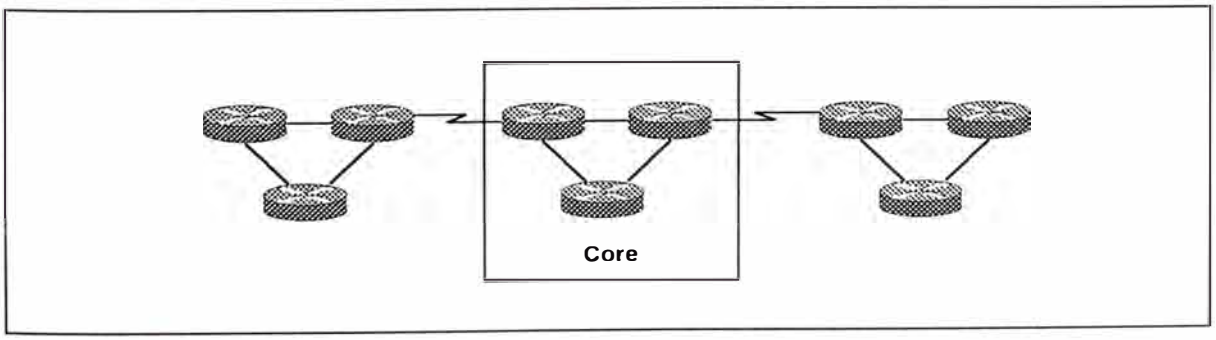


Figura 5-18 Ejemplo de Exterior Gateway Protocol EGP.

- Funciones EGP: EGP tiene tres principales funciones:
    1. Los router EGP establesen un conjunto de vecino con el cual ellos comparten información ded acesibilidad.
    2. Los router EGP polls a sus vecinos para ver, si ellos están vivos.
    3. Los router EGP envian mensajes de actualizaciones conteniendo información de acesibilidad en la red dentro de su istema autónomo.

- Tipos de Mensajes EGP: EGP usa los siguientes tipos de mensajes:
    1. Neighbor acquisition messages para probar si los vecino s estan vivos.
    2. Neighbor reachability messages para determinar cuando un vecino esta caido.
    3. Poll messages para adquirir información de accesibilidad acerca de las redes en el cual los host remotos residen.
    4. Error messages para identificar varias condiciones de error.

Border Gateway Protocol (BGP).- BGP es un protocolo de sistema inter-autónomo creado para usar en el Internet. A diferencia de EGP, BGP puede ser usado entre y dentro de sistemas autónomos, y puedee determinar routing loops. Para que dos vecinos BGP se comuniquen, ellos tienen que estar en la mismo red física.

Los routers dentro de un mismo sistema autónomo aseguran que todos los routers en ese sistema autónomo tenga una vista consistente de ello. La comunicación entre los routers en el AS sirve para determinar el punto de conexíon hacia o desde ciertos sistemas autónomos externos. La figura 5-19 muestra como un BGP puede comunicar entre sistemas atónomos.

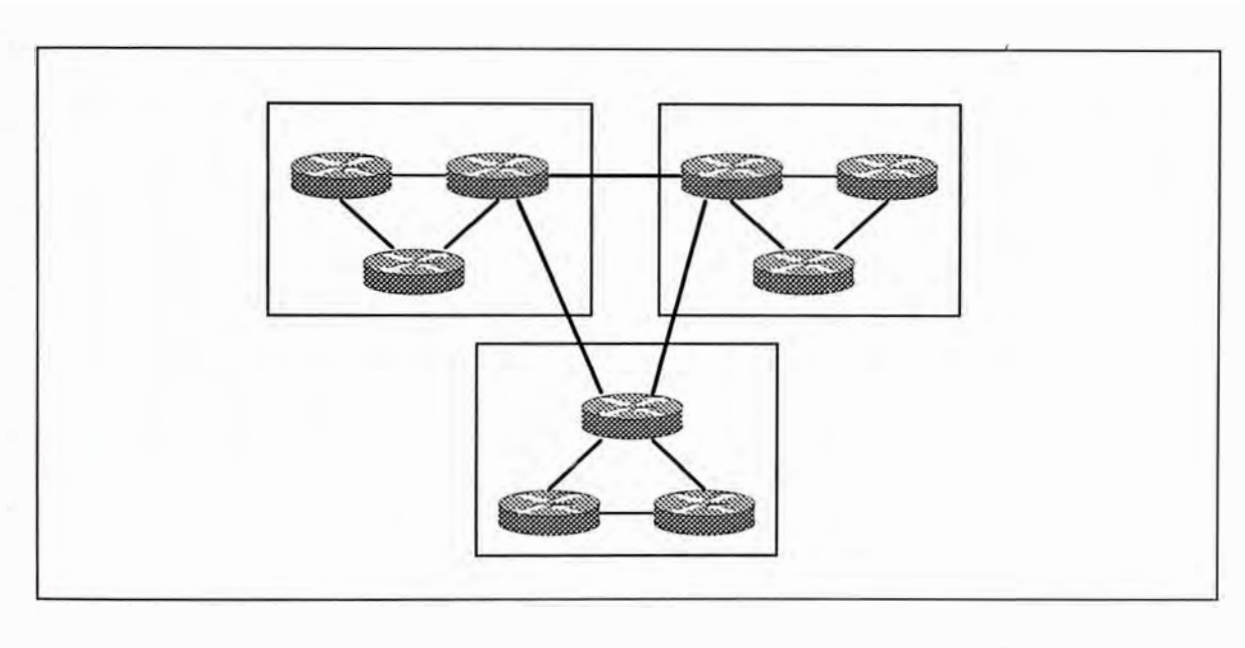


Figura 5-19 Ejemplo de Border Gatyeway Protocol BGP.

BGP no usa un core como EGP por que con BGP, todas las áreas pueden interconectarse entre ellas y comunicarse sin ir a través de un core backcone central.

Cuando un router BGP primero llega online, este recibe una tabla de enrutamiento BGP completa desde sus vecinos.' Si ocurre un cambio, los updates son enviados fuera incrementalmente.

La métrica BGP especifica el grado de preferencia para una ruta particular. Estas preferencias pueden ser basadas en un conteo de sistema autónomo, el tipo de enlace, y otros factores. Las métricas son típicamentes asignados por el administrador de red a través de archivos de onfiguración.

Una característica de BGP es que mantiene el rastreo de todas las posibles rutas hacia un destino, pero advertiría únicamente la ruta que considere que es mejor u óptima en sus mensajes update. Estos mensajes update contiene un número de red y una ruta de sistema autónomo. El latter indica el string ded sistemas autónomos a través del cual las redes especificadas pueden ser alcanzados. En otras palabras BGP lista la ruta al destino. Este precludes la continuidad hacia el infinito y baja los problemas de convergencia asociados con otros protocolos distance-vector.

Adicionalmente a los mensajes update, BGP usa tres tipos de mensajes:

- Open: Este es el primer mensaje enviado después que una conexión en el protocolo de transporte es establecida.
- Notification: Este mensaje es enviado cuando un error es detectado.
- Keepalive: estos mensajes son enviados para mantener el hold timer dedsde expiring.

5.5.- ADMINISTRACION DE TRAFICO CON LISTAS DE ACCESO

Debido a la creciente deemanda ded ancho de banda y por consiguiente el crecimiento paulatino de tráfico, colocaron a los administradores de red en el siguiente dilema: como denegar tráfico norequerido mientras permites el acceso al tráfico apropiado. Aunque otras herramientas tales com el password, equipos callback, y dispositivos de seguridad física son de mucha ayuda, ellos algunas veces lack la expresión flexible y el control específico que la mayoría de los adminitradores de red prefieren.

La lista de acceso ofrece otra poderosa herramienta para controlar la red. Esta lista adiciona la flexibilidad para filtrar el flujo de paquetes hacia o desde las interfaces del router. Tal control puede ayudar a limitar el tráfico de red y restringir redes que usan ciertos usuarios o dispositivos. La lista de acceso diferencia el tráfico de paquetes dentro categorías que permitan o deniegan otras caraterísticas. Las listas deacceso se usan tambien para

- Idedntificar paquetes prioritarios o custom queuing. La priorización te habilita a designar ciertos paquetes a ser procesados por un router antes que otro tráfico, en la base de protocolo. Custom queuing es usado para balancear tráfico basado en protocolos, tipos, y otros propósitos.

- Restringue o reduce el contenido de routing update. Estas restricciones son usados para limitar información acerca de redes específicas que se propagan a través de la red.
- Identifica que paquetes llevaría conexiones de enrutamiento dial-on-demand. Esto asegura que los paquetes que no son vital para las comunicaciones processes no llevarían un enlace WAN.

La lista de acceso también procesan paquetes para otras características de seguridad para

- Provee control de acceso dinámico de tráfico IP con autentificación de usuario mejorado usando la caraterística lock-and-key.
- Identifica paquetes para encriptación
- Identifica acceso Telnet permitido para los terminales virtuales del router.

Como notamos, las lista de acceso puede definir el tipo de tráfico que puede llegar a la WAN . Comparado a la red LAN o Campus, el tráfico que usa enrutamiento dial-on-demand (DDR) es típicamente de bajo volumen y peródico. DDR inicia una llamada WAN hacia un site remoto únicamente cuando hay tráfico para transmitir. Para identificar este tráfico, especificamos los paquetes que el DDR procesa en el router y que interpretaría como tráfico interesante. Por ejemplo la dirección de red de destino, fuente de dirección dee red, e información de servico o de red

podrían ser definidos como tráfico interesante y además estar restringido o permitido en el enlace WAN.

Cuando configuramos DDR tenemos que ingresar los comandos ded configuración que indican que paquetes de protocolo constituyen tráfico interesante para iniciar una llamada. Para configura por iniciación de llamada, ingresa las sentencias de la lista de acceso para identificar la dirección fuente y destino y elige el criterio de selección de protocolo específico para iniciar la llamada.

Luego establecemos la interface donde la llamada DDR puede iniciar. Este paso designa un dialer group. El dialer group asocia los resultados de las especificaciones de paquetes interesantes de la lista de acceso a las interfaces del router para realizar un llamada WAN.

Para DDR al igual que otras aplicaciones, la lista de acceso expresa el conjunto dse reglas que da control adiconal para paquetes que entran en la interfaces, paquetes que relay a través del router, y paquetes que salen de las interfaces del router. La lista de acceso no actúan en paquetes que son originados en el router mismo. En vez de eso, ellos son sentencias que especifican condiciones ded como el router manipularía el flujo de tráfico a través de las interfaces especificadas. La lista de acceso dan controla dicional para procesar los paquetes específicos en un único camino.

Los dos tipos principales de listas de acceso son lista de acceso estándar y extendida.

- Lista de Acceso Estandar: Para IP chequean la dirección fuente de los paquetes que podrían ser ruteados. El resultado permite o deniega la salida para protocolos IP enteros, basado en la dirección de red/subnet(host.
- Lista de Acceso Extendida: Estos chequean la dirección fuente y destino de los paquetes. Ellos también pueden chequear priotocolos especíificos, número de puertos, y otros parámetros, el cual permite a los administradores mas flexibilidad para describir que haría la lista de acceso. Los paquetes pueden ser salidas permitidos o denegados basado en el origen y el destino de los paquetes.

Por ejemplo en la figura 5-20, los paquetes que llegan en el E0 son chequeados por la dirección fuente, dirección destino y protocolo. Si los paquetes belong a un protocolo permitido, dirección fuente y destino, son sacados por S0, el cual es agrupado a la lista de acceso. Si no son dropeados.

La lista de acceso extendida también permite o, deeniega con mas granularidad. Por ejemplo se puede pérmitir tráfico electrónic mail desde E0 al destino S0 específico, mientras deniega los loggimg remotos o transferencia de archivos.

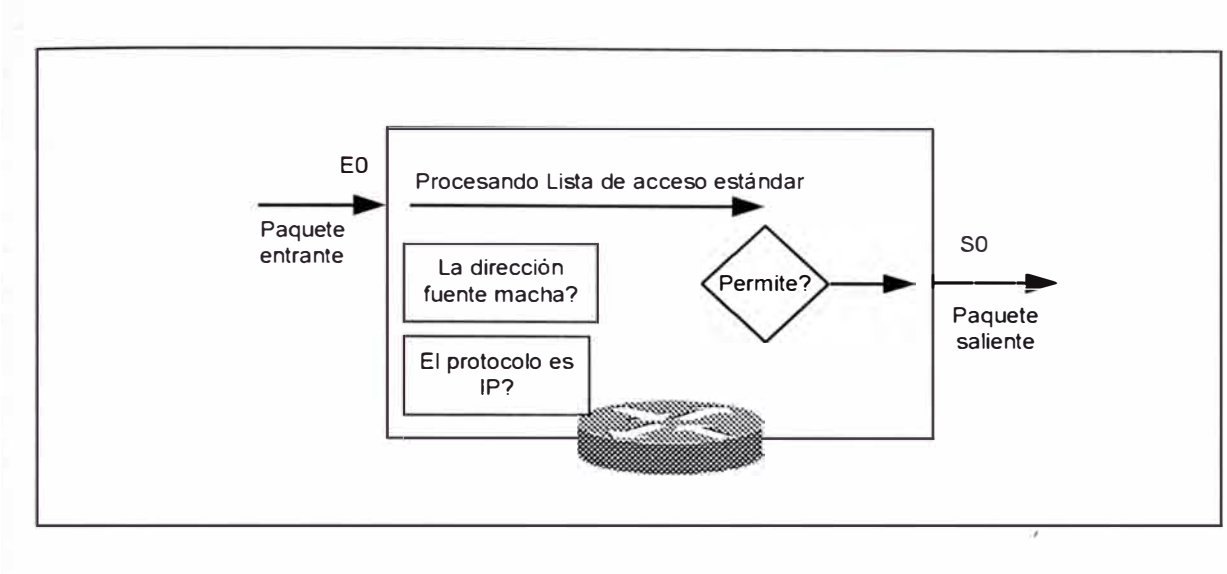


Figura 5-20 Con una lista de acceso extendida, los paquetes que llegan por el E0 son chequeados por la dirección fuente, destino y protocolo.

5.5.1.- Como Trabajan las Listas de Acceso

El principio del proceso es el mismo regardless de si la lista de acceso es usado: Cuando un paquete ingresa a una interface, el router chequea su tabla de enrutamiento para ver si el paquete es ruteable o bridgeable, como mostrado ne la figura 5-21. Si no es ninguna de la s dos cosas, el paquete sería dropeado. Si el paquete es ruteable, una entrada en la tabla de enrutamiento indica una red de destino, alguna métrica de enrutamiento o estado, y la interface a usar para un envío de paquetes.

Luego, el router chequea para ver si la interface de destino es agrupado a una lista dee acceso. Si no es, el paquete puede ser enviado al buffer de salida. Por ejemplo, si el paquete usaría To0 como una interface de destino, y To0 no tiene lista dee acceso en efecto, el paquete usa To0 directamente.

Si la interface de destino del pauete es agrupado a una lista dee acceso, el paquete tiene que ser filtrado a través de esa lista. Por ejemplo, supon que una interface, E0, ha sido agrupado a una lista de acceso extendida. El admistrador usó preciso, expresión lógica para configurar la lista de acceso. Antes de que un paquete pueda proceed a esa interface, este es probado por una combinación de sentencias dee lista de acceso asociados con esa interface.

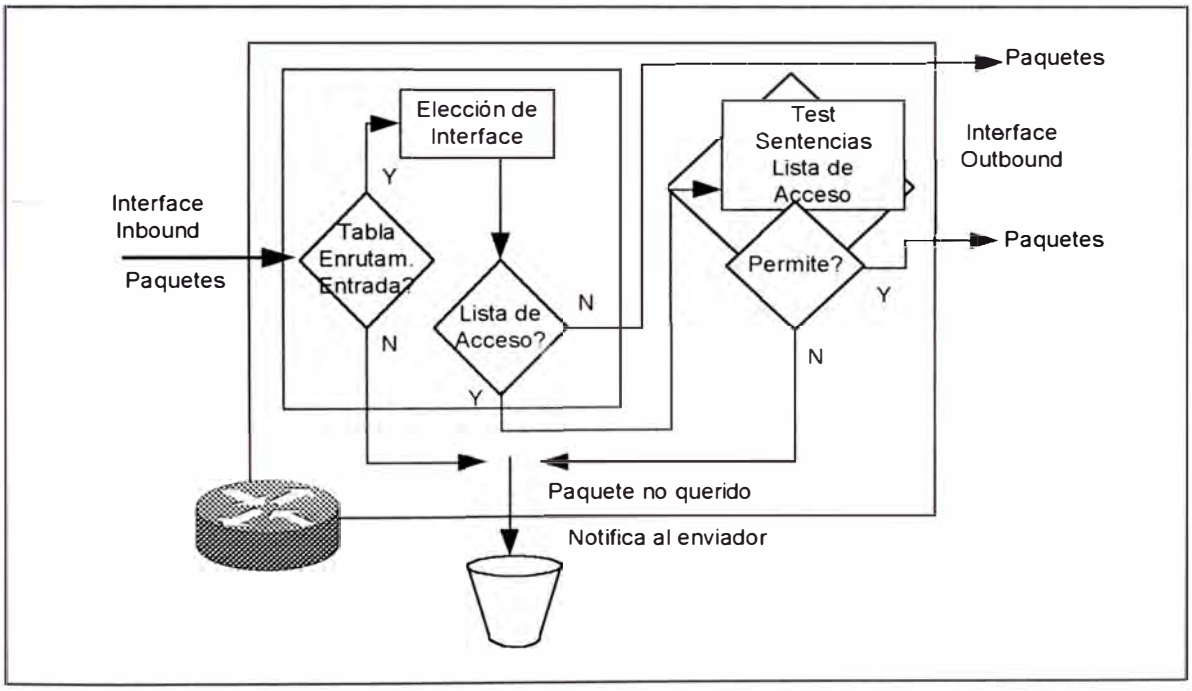


Figura 5-21 Proceso de las Listas de Acceso en un router.

Basado en las pruebas de la lista de acceso extendidas, los paquetes pueden ser permitidos o negados. Denegar los permisos significa dropear el paquete. Cuando descartamos paquetes, algunos protocolos retornan un paquete especial que notifica al enviador del destino inalcanzable. Permitir un paquete quiere decir grant it access a través de la

interface E0. La lista de acceso del router provee control efectivo en denegar el uso de la interface E0.

Notar que E0 en este caso es una lista de acceso de salida. Para listas de salida, el procesos de prueba determina si o no los paquetes son permitidos para accesar a la interface outbound. Para listas inbound, el proceso de pruebas determina si o no el router continúa procesando el paquete después de recibir esto en una interface inbound.

La lista de acceso operan en forma secuencial y lógica. Ellos evalúan los paquetes desde el tope hasta abajo. Si la cabecera del paquete y la sentencia de la lista de acceso concuerdan, el paquete salta el resto de las sentencias. Si una condición que concuerda es verdadera, el paquete es permitido o denegado. Puede haber únicamente una lista de acceso por protocolo o por interface.

En la figura 5-22, si la primera prueba concuerda, un paquete es denegado el acceso a una interface de destino. Este sería descartado y llevado dentro del "bit bucket" o tacho. El paquete no es expuesto a las siguientes pruebas de la lista de acceso que sigue.

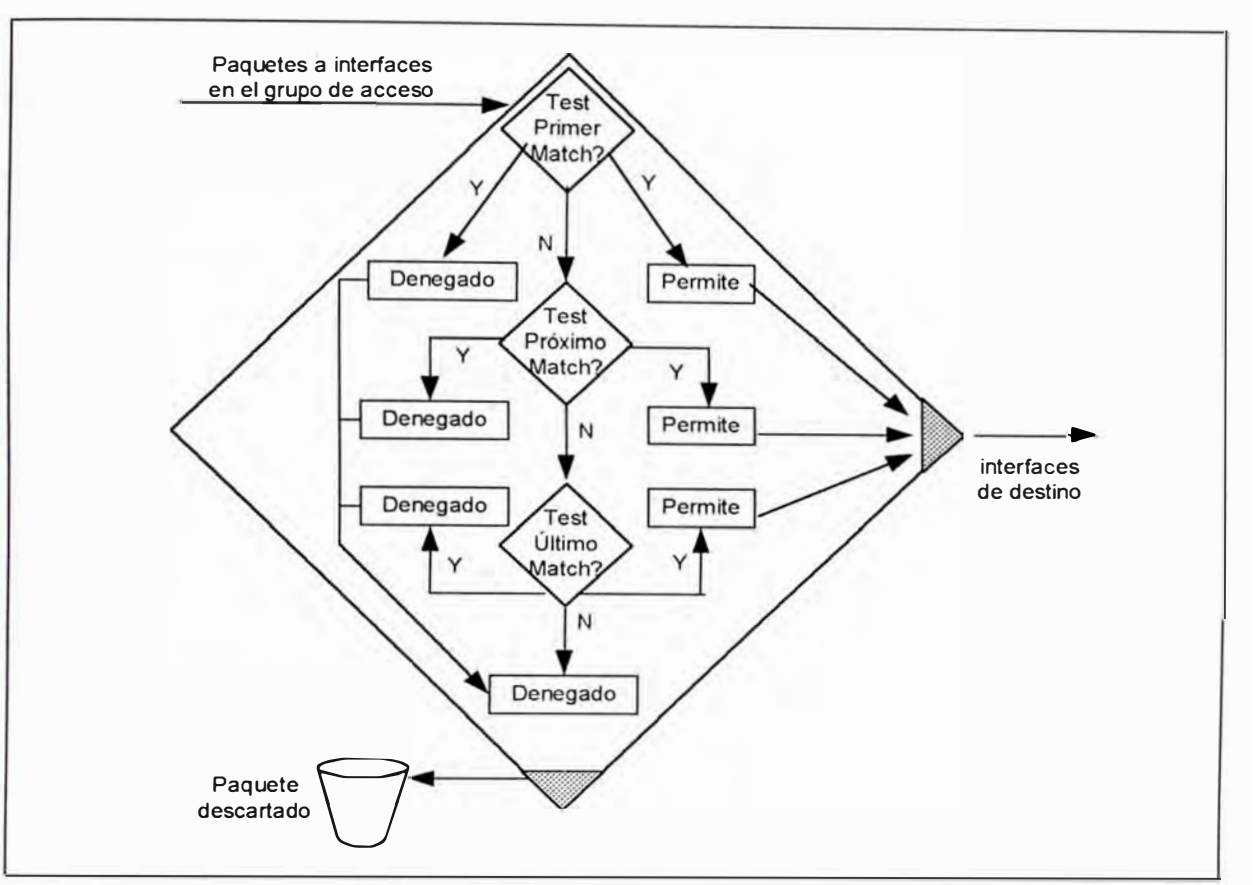


Figura 5-22 Las sentecias de las listas de acceso son colección de sentencias de condición de permite o deniega

Únicamente si el paquete no coincide con las condiciones de la primera prueba, este caería a la siguiente sentencia de la lista de acceso. Si asumimos una sentencia "permit" (faculta al paquete de continuar su camino) para los parámetros de los paquetes que coincidan con la siguiente prueba, el paquete permitido procede a la interface de destino.

Otro paquete que no coincida con la primera ni con la segunda sentencia, pero lo hace con la sentencia de la siguiente línea de la lista de acceso, nos da otra vez un resultado "permit".

La condición de prueba final es un deniega, algunas vecees llamado implicit deny, por que este no aparece actualmente como un linea de codigos de configuración. En vez de proceder en o hacia una interface, todos los paquetes que alcanzan el deny implicita son dropeados.

5.5.2.- Identificando Las Listas de Acceso

Las listas de acceso pueden controlar la mayoria de protocolos en un router cisco. La tabla 5-4 muestra el protoclo y el rango numérico de los tipos de la lista de acceso.

TIPO DE LISTAS DE ACCESO	RANGO NUMERICO / IDENTIFICADOR
IP Estándar Extendido	1 - 99 100 - 199
IPX Estándar Extendido Filtros SAP	800 - 899 900 - 999 1000 - 1099
Apple Talk	600 - 699

Tabla 5-4 Lista de Acceso ded Protocolos y rangos numéricos.

Muchas listas de acceso son posibles para un rpotocolo. Seleccione un número diferente desde un rango de número de protocolo para cada lista de acceso nueva, sin embargo, el administrador puede especificar únicamente una lista de acceso por protocolo y por interface. El rango numérico generalemnte permite 100 diferentes listas de acceso por tipo de protocolo. Cuando un rango ded 100 número s dado designa una

lista dee acceso estándar, la regla es que el siguiente rango de 100 números es para listas de accesos extendidas para este protocolo.

5.5.3.- Lista de Acceso TCP/IP

Para los filtros dee paquetes TCP/IP, la lista de acceso dee Cisco chequea el paquete y la cabecera de capa superior, como mostrado en la figura 5-23 .

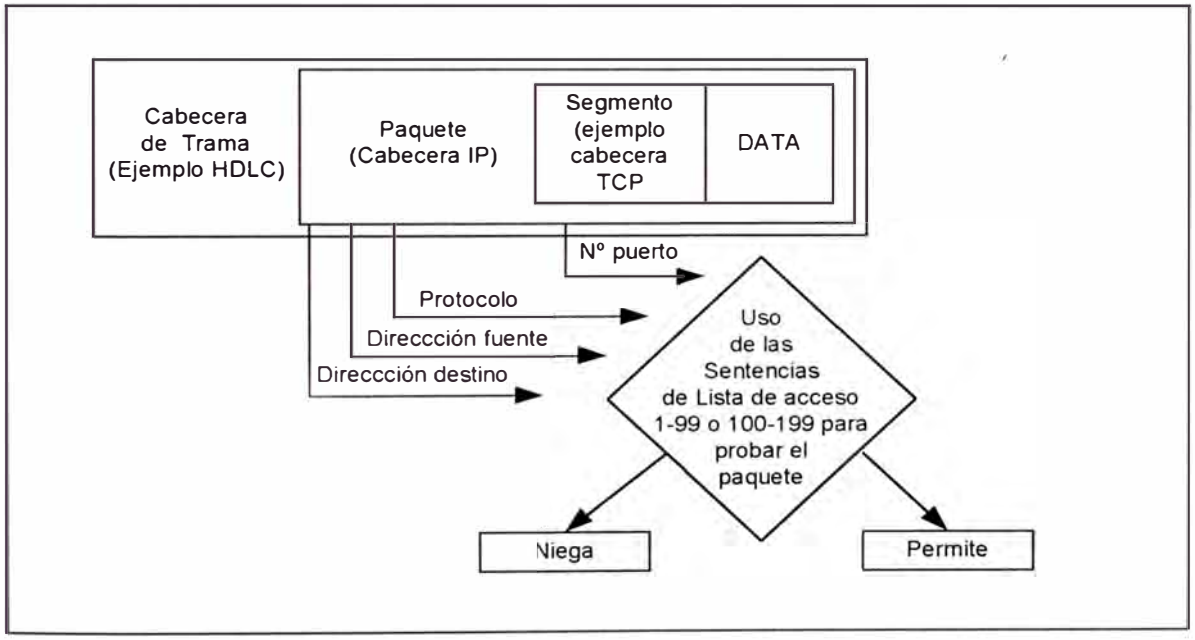


Figura 5-23 Las listas dee acceso pueden chequear la dirección fuente, destino o número de puerto de capa superior de un paquete.

Per ejemplo, las listas ded acceso pueden chequear el paquete:

- Dirección IP fuente, usando lista dee acceso estándar; identifica estos con un número del 1 al 99
- Dirección IP fuente y destino o protocolos específicos, usando lista de acceso extendida; identifica estos con un número de 100 a 199

- Números de puertos UDP o capa superior TCP en adición a las otras pruebas en la lista de acceso extendida; también identifica estos con un número en le rango de 100 a 199

Para todas estas listas ded acceso TCP/IP, deespués que un paquete es chequeado con las sentencias ded la lista de acceso, este puede ser denegado o permitido para usar un número de interface en el grupo de acceso.

Si especificamos una lista de acceso con un númeor de 1 a 99 instruimos al router para aceptar sentencias de lista de acceso IP estándar. Si especificamos un núemro de lista ded acceso de 100 a 199 instruimos al router a aceptar sentencias de lista de acceso extendida.

Selecione que protocolo IP chequear. Cualquier otro protocolo IP no son chequeados. Mas tarde en el procedimiento, el administrador puede también especificar un puerto de destino opcional para mas granularidad.

El filtro de direcciones ocurre usando el wildcard masking, para identificar como chequear o ignorar bits de direcciones IP correspondientes (0=chequea, 1=ignora)

- Wildcard Mask bits: Las listas de acceso IP usan wildcard masking para identificar simples o múltiples direcciones IP para permitir o

denegar pruebas. Un wildcard mask es confrontado con una dirección IP y y usa el número 1 o 0 para identificar como tratar los bits de la dirección IP correspondiente (ver figura 5-24):

1. Un wildcard mask bit 0 significa "chequear el valor dedl bit correspondiente in la dirección IP"
2. Un wildcard mask bit 1 significa"no chequear (ignorar) el valor del bit correspondiente a la dirección IP".

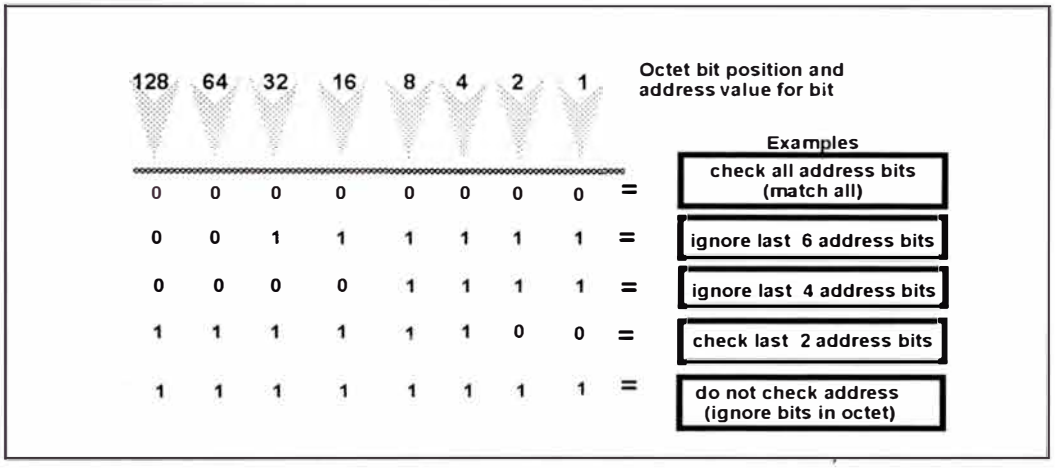


Figura 5-24 Wildcard mask usa unos y ceros para identificar como tratar los bits de las direcciones IP.

Aunque ambos son cantidades de 32 bits, el wildcard mask y la mascara de subnet oiperan de manera diferente. Recordamos que los ceros y unos en una mascara de subnet determina la red, subnet y la porción de host dede la dirección IP correspondiente. Los ceros y unos en un wildcard mask, como lo has notado, determina si los bits correspondientes en la dirección IP deberían ser chequeados o ignorado por la lista de acceso propuesta.

El término wildcard masking es un nickname para access list mask-bit-matching process. Este nickname viene de una analogía de un wildcard que macha con cualquier otro card en un game poker. En la figura 5-24, este proceso de enmascaramiento wilcard es aplicado.

- Matching Cualquier IP Address: Considere un administrador de red que quiere especificar que cualquier dirección de destino sería permitido en la prueba de la lista de acceso, como mostrado en la figura 5-25. Para indicar cualquier dirección IP, el administrador debería ingresar 0.0.0.0; luego indicar que la lista de acceso debería ignorar (permitir sin chequear) cualquier valor, el correspondiente bit wildcard mask para esta dirección debería ser todos unos (es deecir 255.255.255.255). El administrador puede usar la abriviación de varios para comunicar esta misma condición de prueba para el software de la lista de acceso. En vez de tipear 0.0.0.0 255.255.255.255, el administrador puede usar la palabra any por si misma cmo la tecla.

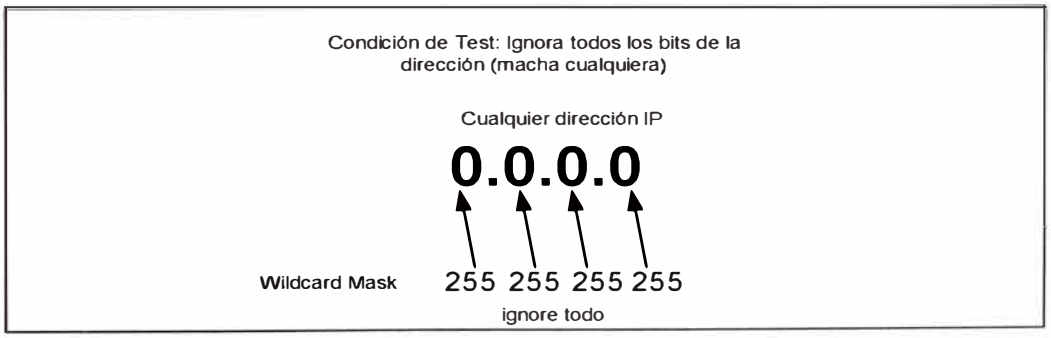


Figura 5-25 Esta abreviación significa ignorar cualquier valor de bit en todas las posiciones de bits.

- Matching una Dirección IP Host Específica: Una segunda condición común en el cual el software cisco permitiría una abreviación en el wildcard mask de la lista de acceso extendida es cuando el administrador quiere machar todos los bits de una dirección IP hsot entera, como mostrado en la figura 5-26 .

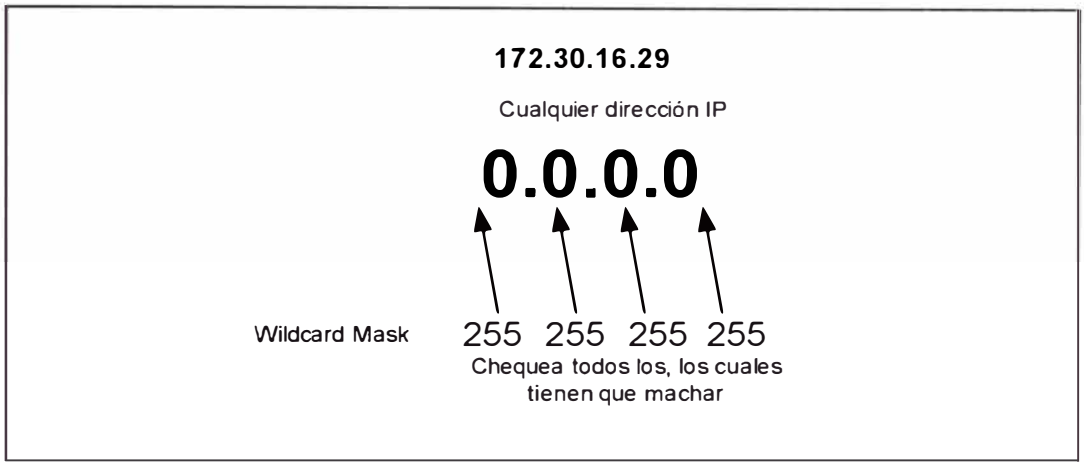


Figura 5-26 Esta abreviación significa ignorar cualquier valor de bit en todas las posiciones de bits, el cual tiene el efecto de machar únicamente la dirección de Host IP especificado.

Considere un administrador de red que quiere especificar que una dirección IP host sería denegado en la prueba de la lsita dee acceso. Para indicar una dirección IP host, el administrador ingresaría la dirección completa, por ejemplo, 172.30.16.29. Luego, para indicar que la lista de acceso debería chequear todos los bits en al dirección, el correspondiente wildcard mask bits para esta dirección IP debería ser todos ceros, es decir 0.0.0.0

El administrador puede usar la abreviación "host" para comunicar la misma condición de prueba. En el ejemplo, en vez de tipear 172.30.16.29 0.0.0.0, el administrador puede usar el "string host" 172.30.16.29

5.5.4.- Donde ubicar las Listas de Acceso

Las listas de acceso son usados para controlar el tráfico a través del filtrado y elimina los paquetes no deseados. Donde el administrador ubica una sentencia de lista de acceso puede reducir tráfico inecesario. El tráfico que sería denegado en el destino remoto no debería usar los recursos de red a lo largo de la ruta al destino.

Supongamos que la política de una red "enterprice" apunte a denegar tráfico "token ring" en el router A para el Ethernet LAN en el puerto E1 del router D, como mostrado en la figura 5-27. A la vez, otro tráfico tiene que ser permitido. Muchas propuestas pueden realizar esta política.

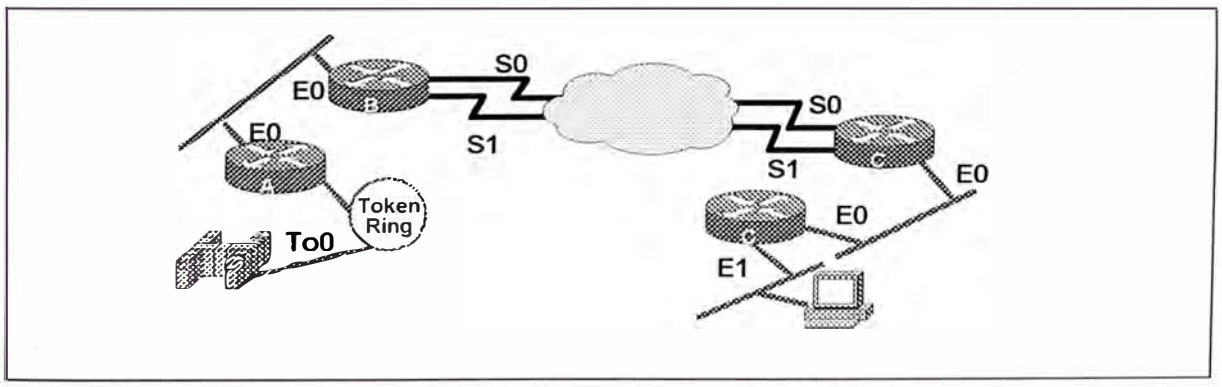


Figura 5-27 Ubica las listas de acceeso estándar cerca al destino. Las listas de acceso extendida son ubicadas próximos a la fuente

El recomendado aproach usa una lista de acceso extendida. Este especifica la dirección fuente y destino. Ubique esta lista de acceso extendida en el router A. Luego los paquetes no cruzaría el Ethernet del router A, no cruzarían la interface serial del routyer B y C, y no entraría la router D. Los tráficos con diferentes direcciones fuente y destino pueden aunser permitidos.

La regla, con lista ded acceso extendida, es poner la lista ded acceso extendida tan próximo como sea posible a la fuente del tráfico denegado.

La lista de acceso estándar no especifican dirección de destino. El administrador debería poner las listas de acceso estándar tan cerca del destino como sea posible. Por ejemplo, en la figura 5-27, ubica una lista de acceso en el E0 delk router D para prevenir tráfico del router A.

CAPÍTULO VI

INTRODUCCION AL DISEÑO DE RED CAMPUS LAN

6.1.- GOALS DEL DISEÑO INTERNETWORK

Una internetwork puede ser generalmente definido como dos o mas redes de área local interconectados por uno o mas dispsitivos de capa 3 (ordinariamente routers). Una internetwork puede estar contenido dentro ded un simple edifico, o puede expandirse en el globo. Aunque hay diferencias específicas entre redes locales e internetworks, en genral hablar la palabra red es usado para rferirse a ambos tipos.

El primer paso para diseñar una internetwork es establecer y documentar los goals del diseño. Estos goals sseríuan particualr para cada organización o situación. Sin embargo, los requerimientos generales tienden a mostrar up en cualquier diseño de red:

- Funcionalidad: La red tiene que trabajar. Es decir, tiene que permitir que los usuarios encuentren sus requerimientos de trabajo individual de tal manera que los requerimientos de los negocios globales de la organización sean encontrados. La red tiene que proveer disponibilidad de aplicaciones end-to-end en algunos niveles

especificados de servicio (definido por el administrador como el compromiso óptimo entre funcionalidad y costo)

- Escalabilidad: La red tien que ser capáz de crecer al igual que la organización crece, y como mas de una organizazción es incluida en la red. Es decir, el diseño inicial debería ser escalable a través de muchos ordenes de magnitud.
- Adaptabilidad: La red debería ser diseñado con un ojo hacia las futuras tecnologías, y no deberían incluir elementos de diseño que limitaría la adopción de nuevas tecnologías como ellos lleguen a ser disponibles.
- Administrabilidad: La red debería ser diseñado para facilitar el monitoreo y administración de red proactivo , con la finalidad de asegurar estabilidad de operación y disponibilidad de recursos.
- Costo effectiveness: Los beneficios de la red a la organización, no obstante cuantificado, tiene igual o costo superior. El costo de implementar el diseño de red tiene que estar dentro de lo presupuestado.

6.1.1.- El Cost Trade – Off

El cost trade-off envuelto en el diseño de red puede ser visto de dos maneras. Primero, el costo podría ser categorizado de acuerdo a la tecnología WAN o LAN. Segundo, el costo podría ser dividido en: Costo fijo (o sunk), y costos que recurren en una base regular (algunas veces mensualmente).

(o sunk), y costos que recurren en una base regular (álgunas veces mensualmente).

En la área WAN, el costo fijo son típicamente para equipos purchase, tal como modems, CSU/DSU, e interfaces router, y para cualquier circuito set-up cost. Los costos recurrentes son los circuitos mensualmente fees del proveedor de servicio.

En el área LAN, los costos fijos otra vez incluyen equipos purchase, tales como routers, switches, y hubs, along con el purchase y costos de instalación del cable de planta físico. Los costos recurrentes son los salarios del staff de administradores de red que atienden diariamente operaciones de red. Las operaciones dia-a-dia incluyen movimientos, adicines, y cambios relacionados a usuarios y estaciones a lo largo con el growth, mantenimiento, y troubleshooting ded la infraestrcutura de red.

Típicamente, los costos recurrentes tienden a predominar en los casos LAN y WAN. Cuando e tradee-off estan siendo weighed, los cambios que ofrecen redución potencial de los costos recurrentes tiene que ser considerados primero.

6.1.2.- Metodologías de Diseño

Existen seis pasos que describen una metodología simple de diseño de red que puede ser usado, la figura pag 1-6 dr muestra estos pasos.

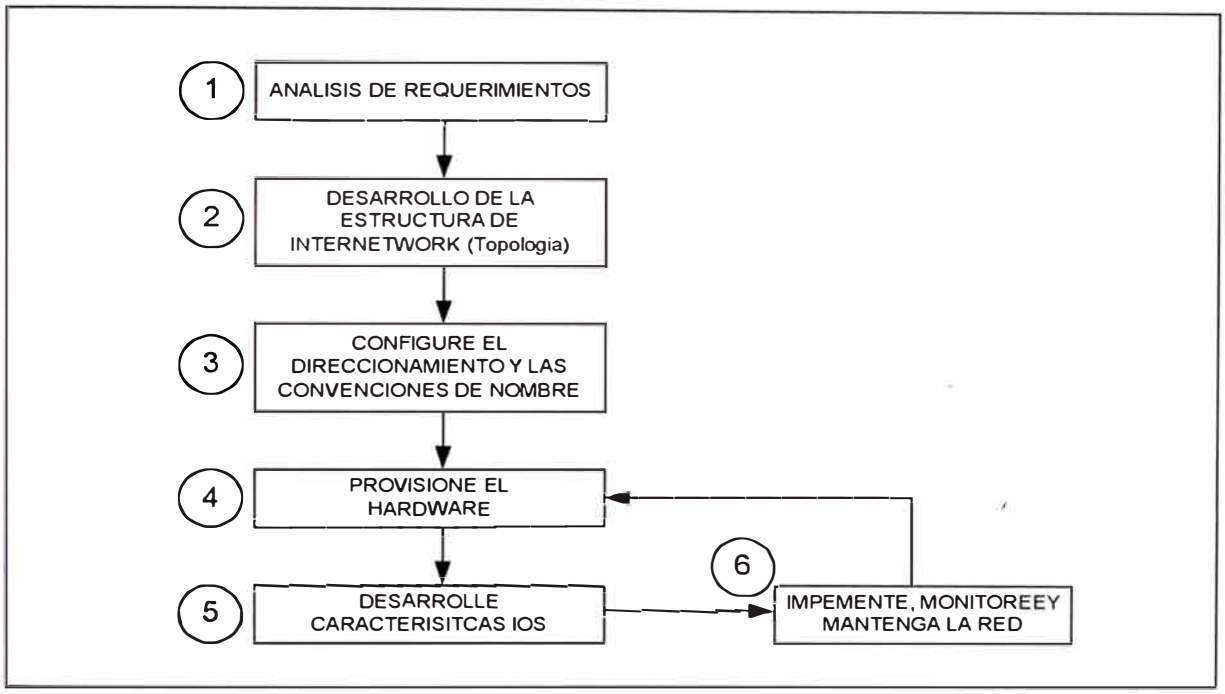


Figura 6-1 Metiodolía de diseño de una Red.

Notar que los tres primeros paso deben ser completados en forma secuencial. El paso inicial de diseñar la topología de red, de devising addressing y convenciones de nombres debería ser completados tempranamente, y no debería requerir mayor revisión después. Los próximos tres pasos son un lazo recurrente que nunca regresa beyond el cuarto paso. Manteniendo el actual código de router, sin embargo, tiene que ser visto como un ongoing task. Como mantenimiento de código, la necesidad de análisis es siempre un esfuerzo ongoing.

Paso 1- Analisis de Requerimiento.- El paso 1 en almetodología es el análisis de requerimiento de la red y de los usuarios. Los usuarios de red necesitan cambios constantemente, en respuesta a los cambios de las condiciones de negocios y en respuesta a los cambios en la trecnología por si misma. Por jemplo, como mas aplicaciones de red basados en voz y video viene a ser disponible, la presión para incrementar el ancho de banda de la red sería intenso. Las necesidadeds de análisi inlcuyen no únicamente el caso dee negocios (análisis costo/beneficio) para adoptar tal aplicación hambrienta de ancho de banda, pero también un análisis detallado de los procedimientos y costos requeridos para actualizar la red para proveer las necesidades de ancho de banda. Similar ejemplo podría incluir el extender la red para incluir oficinas corporativas y regionales, o integrar un sistema telefónico dentro del que fur previamente una red solo de datos.

Paso 2 – Desarrollo de la Estructura de Internetwork.- El paso 2 es la metodología para deesarrollar la topología de toda la red usando un modelo jerarquico. Un buen diseño de internetwork típicamente sigue un modelos jeararquico dee tres capas. En este modelo la red es dividido en capas dee Core, Dsitribución y Acceso. Estas capas describen un conjunto de funciones discretos llevadas a cabo en cada capa, y una topología de red típicamente asociado con cada capa. Cada capa tiene sus propias funciones. Manteniendo las capas separadas, el método de diseño jerarquico produce una red alatamente flexible y escalable.

La capa core primeramente provee el enlace de area amplia entre sites renotos geográficamente tying un número de redes campus juntos en una WAN corporate o enterprice. Raramente hay host en la capa core, los servicios core son tíupicamente leased de un proveedor de servicios de telecomunicaciones (ejemplo, E1, Frame Relay, SMDS, y mas).

La capa de distribución generalmente se refiere a la distribución de los servicios de red para múltiples LANs deentro de un ambiente de red campus. Esta capa es donde la red "backbone campus" eś encontrado y esta típicamente basado en FDDI, fast Ethernet, o ATM. Esta capa es alguna veces donde la política de red es implementado muy bien (como ejemplo, seguridad, convenciones de numero y nombres de red, y mas).

La capa de acceso es usalmente una LAN o un grupo de LANs típicamente Ethernet p Token Ring, que provee a los usuarios con acceso a primera linea de los servicios de red. La cpa de acceso es donde caso todos los host son adjuntados a la red, incluyendo servidores de toda clase como también workstations de usuarios.

La figura 6-2 nos muestra un estructura de red dividido en tres capas.

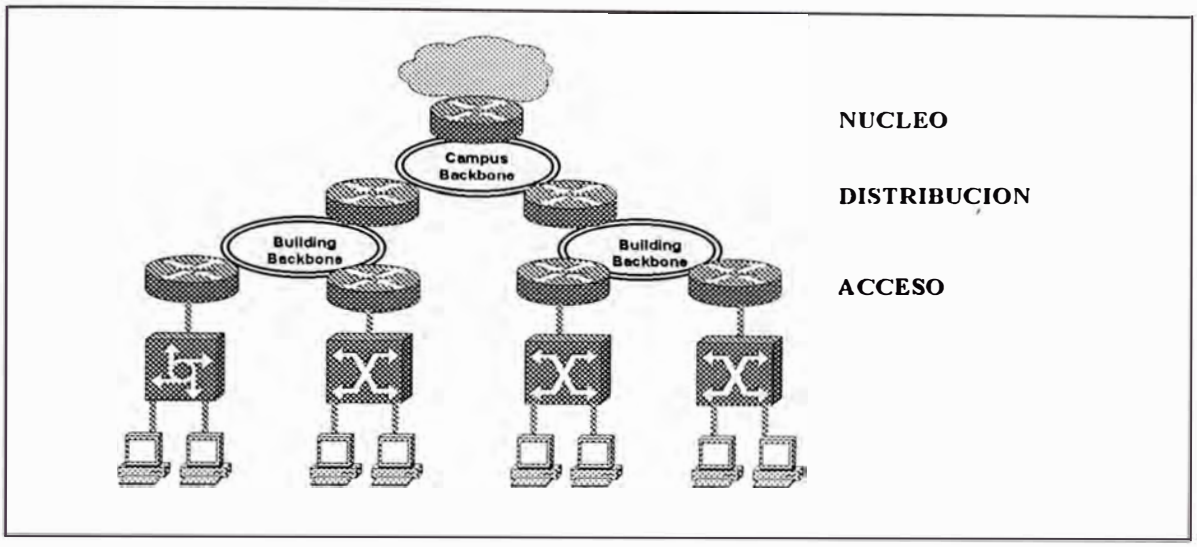


Figura 6-2 Desarrollo de la estructura de la Internetwork.

Paso 3 – Configurando las Convenciones de Nombre y Direcciones.- El paso tres en la metodología es para desarrollar el esquema de direcciones asignando bloques dee direcciones a porciones de la red, así simplificando la administración de direcciones y produciendo un internetwork mas escalable. En la figura 6-3,muestra un ejemplo de TCP/IP , la dirección IP ded 10.0.0.0 con 16 bits dee subneting es usado a través de la organización. Este campus ha sido allocated un bloque continuo de 254 de estas direcciones. La dirección es luego further allocated con cada edificio recibiendo aproximadamente 16 subnets continuos.

Si el protocoo de enrutamiento usado en al internetwork soporta mascarade subnet de longitud variable (VLSM) un verdadero esquema ded dirección jerárquica podría ser desarrollado. En un ejemplo genérico TCP/IP, un subnet de 8 bits de mascara puede estar en uso en al capa de core, una mascara de 16 bits puede estar en uso en la capa de distribución y una

mascara ded 20 bits puede ser aplicado a la capa de acceso. La ubicación cuidadosa dee direcciones en un diseño jerarquico puede resultar en una summarizacion efieciente ded rutas en la tabla dee enrutamiento.

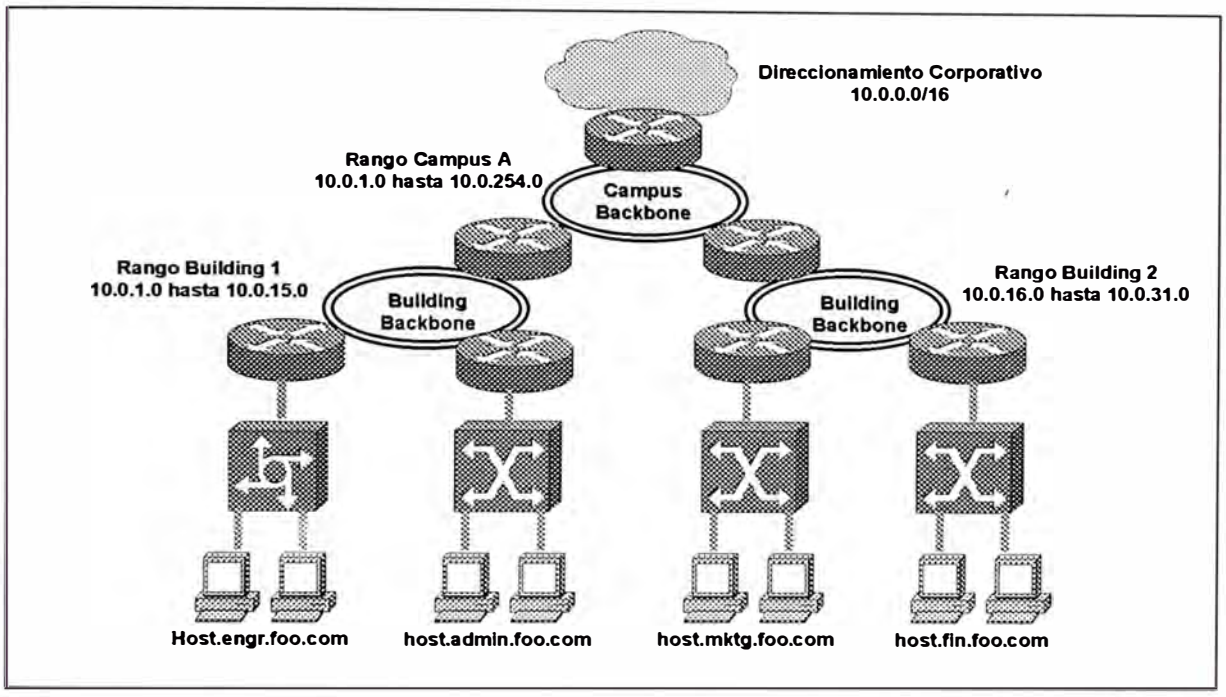


Figura 6-3 Configuración de direccionamiento y convenciones de nombres.

El squema de nombres es también diseñado de una forma sistemática, con prefijos comunes usados para nombrar componentes dentro de una organizazción. La convención sistemática de nombres hace que la red sea mas escalable y fácil de administrar.

Paso 4 – Provisión del Hardware.- El paso cuatro en la metodología es usar la documentación del vendedor para seleccionar los componentes del hardware, incluyendo componentes de conexiones LAN ,y WAN, para implementar el diseño de internetwork. El proceso de selección típicamente incluye consideraciones de funciones y características de un equipo

particular, incluyendo suscapacidades de upgrade y asdministrabilidad. El costo inicial del equipo es siempre parte del proceso de descisión.

Por ejemplo al seleccionar dispositivos LAN tenemos que tomar en cuanta:

- El modelo router
- EL modelo del switch
- El sistema de cableado
- Las conexiones de backbone

Y si quermenos selelcionar dispositivos WAN debemos tomar en cuanta:

- El modelo de routers
- El modelo de modems
- El dispositivo CSU/DSU
- Servidores de acceso remoto.

Cuando queremos provisionar de hardware ded switches y routers, debemos considerar:

- CPU budget
- RAM budget
- BUS budget
- Fordwarding budget

- Tipos de interface y densidad.

Paso 5 – Desarrollo de las Características del Software.- El paso cinco en la metodología es desarrollar características de software apropiadas. Muchos de estas características, tales como lista de acceso, características proxy, queuing, y compresión, son disponibles para soportar administración ded ancho ded banda. Otras características provee soporte para seguridad, administraci´pon de red general, administración de tráfico, y administración de ancho de banda.

El desarrollo inicial de características de software es directamente relacionado a aplicaciones en uso ded máquinas host, las consideraciones para tipo de protocolo es crítico.

Desarrollo adional de caracteríticas estan basados en el modelo jerarquico de tres capas. Los dispositivos de la capa dee acceso, algunas veces emplean deficiones estáticas, serviucios proxy, y filtros first-cut. En la capa de distribución, las características provee compresión, control de congestión, y herramientas de administración.

Paso 6 – Implementar , Monitorear y Administrar la Red.- El últimom paso en la metodología es implementar la red. Si es posible, modelar y probar los nuevos diseños en el laboratorio antes de su completo desarrollo. Durante el desarrollo actual, un aproach paced es recomendado para reeducir el

impacto en las comunidades de usuarios. Llevar a cabo asambleas operacionales continuamente, para que al planear aplicaciones de alto ancho de banda ocurra proactivamente. Desarrollar nuevo hardware y software como son requeridos para soportar nuevas aplicaciones.

6.2.- EL DISEÑO JEARQUICO

6.2.1.- Beneficios del Modelo Jerárquico

Los diseños de red tienden a seguir uno de las dos estrategias de diseño general: malla o jerárquico. En una estructura de malla, la topología de red es plana; todos los routers llevan a cabo esencialmente las mismas funciones, y no hay usualmente una definición clara de donde específicamente una función es llevada acado. La expansión de la red tiende a proceder de una manera arbitraria y fortuita. En una estructura jerarquica, la red es organizada en capas que tienen una o mas funciones específicas. Los beneficios de usar un modelo incluye lo siguiente:

- Escalabilidad : Las redes que siguen el modelo jerarquico pueden crecer mucho mas grande sin sacrificar el control y la administrabilidad, por que la funcionalidad esta localizada y los problemas potenciales pueden ser reconocidos mas fácilmente. Un ejemplo de diseño de red jerarquico a gran escala es la Red Telefónica Pública Switcheada (PSTN).
- Facil Implementación : Un diseño jerarquico asigna funcionalidad clara a cada capa, así hace más fácil la implementación de la red.

- Fácil Troubleshooting : Debido a que las funciones de las capas están bien definidas, el aislamiento de problemas en la red es menos complicada. La segmenrtación temporal de la red para reducir el campo de la red es también fácil.
- Predictibilidad : El comportamiento de una red usando capas funcionales es mucho mas predicible, el cual hace que la capacidad de planear el crecimiento sea mas fácil, este diseño propone también facilidades de modelar la performancia de la red para propósitos analítios.
- Soporte de Protocolos : La mezcla de aplicaciones actuales y futuros y protocolos sería mucho mas fácil en redes que siguen los principios del diseño jerarquico por que la infraestructura precedente está ya organizada localmente.
- Administrabilidad : Todos los beneficios listados contribuyen a la gran administrabilidad de la red.

6.2.2.- Componentes del Modelo de Tres Capas

El modelo de tres capas consiste de una capa Core, Distribución y Acceso, cada uno teniendo funciones específicas:

Capa Core.- Provee un transporte óptimo entre sites geográficamente ubicados en áreas amplias, uniendo un número de redes "campus" en una WAN enterprice o corporate. Los enlaces Core son usualmente punto a

punto y hay raramente un host en esta capa. Los servicios Core son típicamente leased de proveedores de servicos.

Capa de Distribución.- Se refiere a la distribución de los servicios de red para múltiples LANs dedntro de un ambiente de red campus. Esta capa es donde el "backbone campus" es hallado, típicamente basado en FDI, Fast Ethernet, o ATM. En esta capa es donde algunas veces se implementa las políticas de red como seguridad, convenciones de nombres y direcciones, a mas

Capa de Acceso.- La capa de acceso es usalmente una LAN o un grupo de LANs , típicamente Ethernet p Token Ring, que provee a los usuarios con acceso a primera linea de los servicios de red. La cpa de acceso es donde caso todos los host son adjuntados a la red, incluyendo servidores de toda clase como también workstations de usuarios.

Notar que una capa es definida como un punto en la red donde un modelo de referencia OSI de capa 3 boundary ocurre. Las tres capas son bounded y definidos por los dispositivos de capa 3 del modelo de referencia OSI o otros dispositivos que poroveen separación dentro del dominio de broadcast. En el siguiente diagrama, el número de capas en el modelo es determinado por tener un número de saltos (salida de la interface del router) separando dos terminales finales cualesquiera.

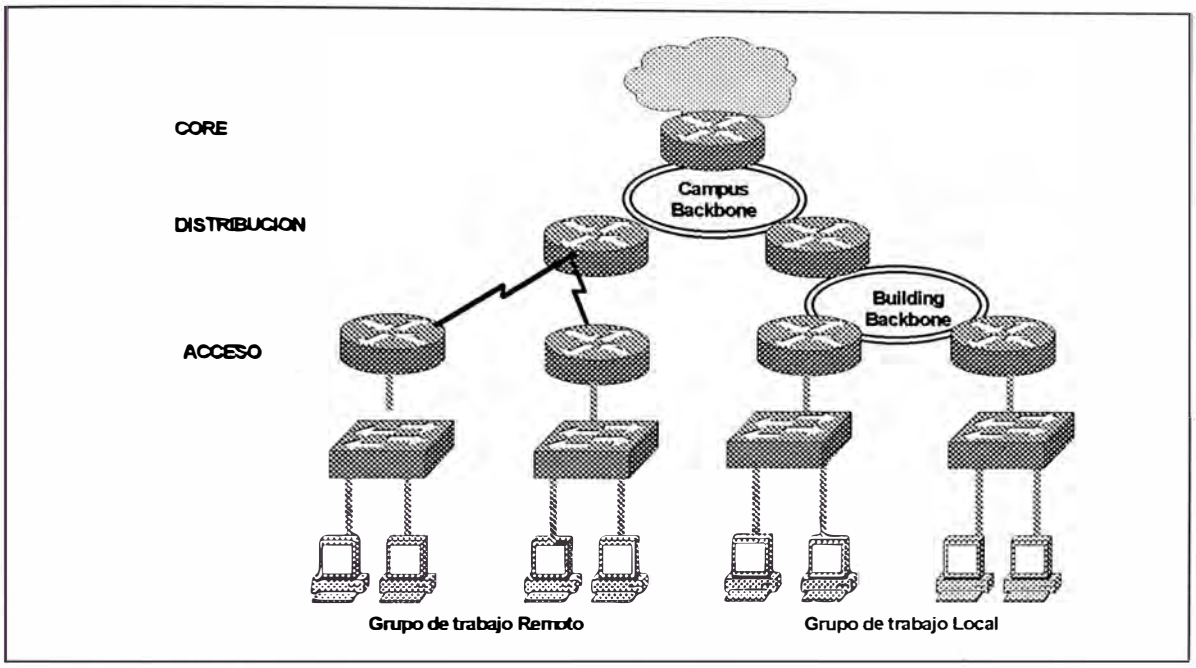


Figura 6-4 Componentes del modelo de tres capas.

Por ejemplo, si dos terminales finales son separados por dos saltos, entonces dos saltos divididos por dos equivale a un modelo dee una capa.

Un modelo de tres capas puede encontrar las necesidades de la mayoría de redes enterprice. Sin embargo, no todos los ambientes requieren un modelo jerarquico completo de tres capas, un diseño de uno o dos capsas puede ser adecuado. Aunque en este caso, una estructura jerarquica debería ser mantenida para permitir que estas redes de una o dos capas puedan expandirse a tres capas a medida que las necesidades lo requiera.

6.2.3.- Funciones de las Capas del Modelo Jerárquico

Funciones de la Capa Core.- La funció de la capa Core es proveer transporte óptimo entre sites remotos. La capa Core es, ademas, usualmente implementado en una Wan. La característia de area amplia deel enlace puede indicar la necesidad para rutas redundantes, para que la red pueda withstand circuitos individuales outage y coninuar funcionando. Compartición de carda y convergencia rápida de protocolos de enrutamiento pueden se características de diseño importantes. Debido a proveedor de tráfico, el eficiente uso de ancho de banda en un Core es siempre un concerní. La eficiencia pued ser alcanzada a través´ del uso de características de software que reducen el consumo de ancho de banda o priorizan tráfico. La figura 6-5 muestra las funciones que deberían ser implementadas en esta capa

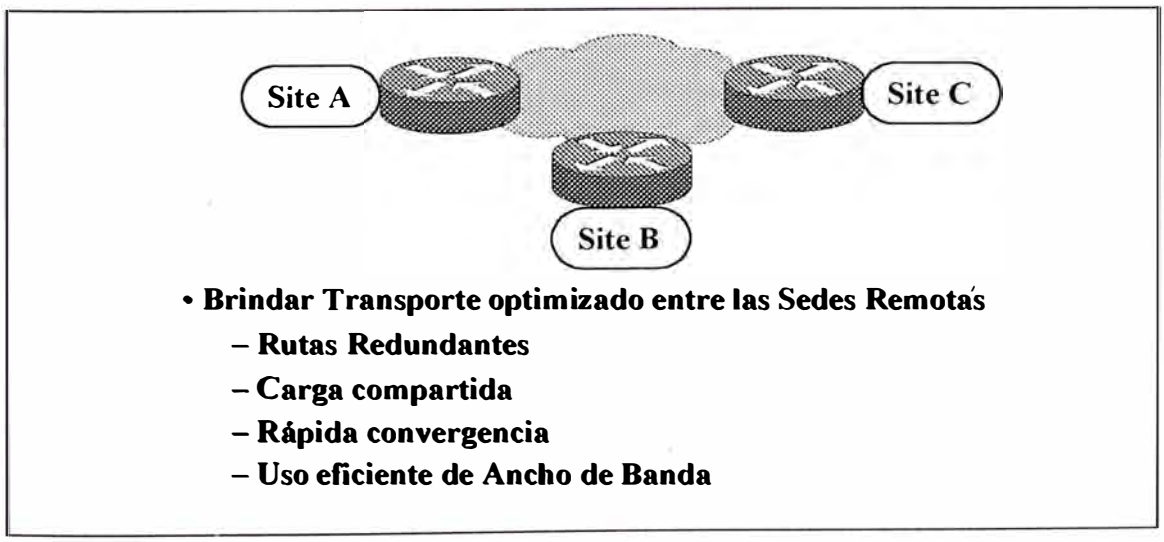


Figura 6-5 Funciones de la capa Core..

Funciones de la Capa de Distribución.- La capa de distribución debería incluir backbione campus con todos sus routers conectados. Debido a que la política es típicamente implementado en este nivel, podemos decir que la capa de distribución provee conectividad basada en políticas. La política en este sentido incluye convenciones de nombres y direcciones, control sobre acceso a servicios, controld e patrones de tráfico a través de definicones de métricas de ruta, y restricciones de advertisements de red por protocolos. Notar que un buen diseño de red no debría poner estaciones (como servidores de red) en el backbone. No poner estaciones en el backbone lo libera para actuar estrictamente como una ruta de tránsito entre workgrups dee edificos diferentes, o de workgrups de servidores campus-wide. La figura 6-6 muestra las funciones que deberían ser implementadas en esta capa

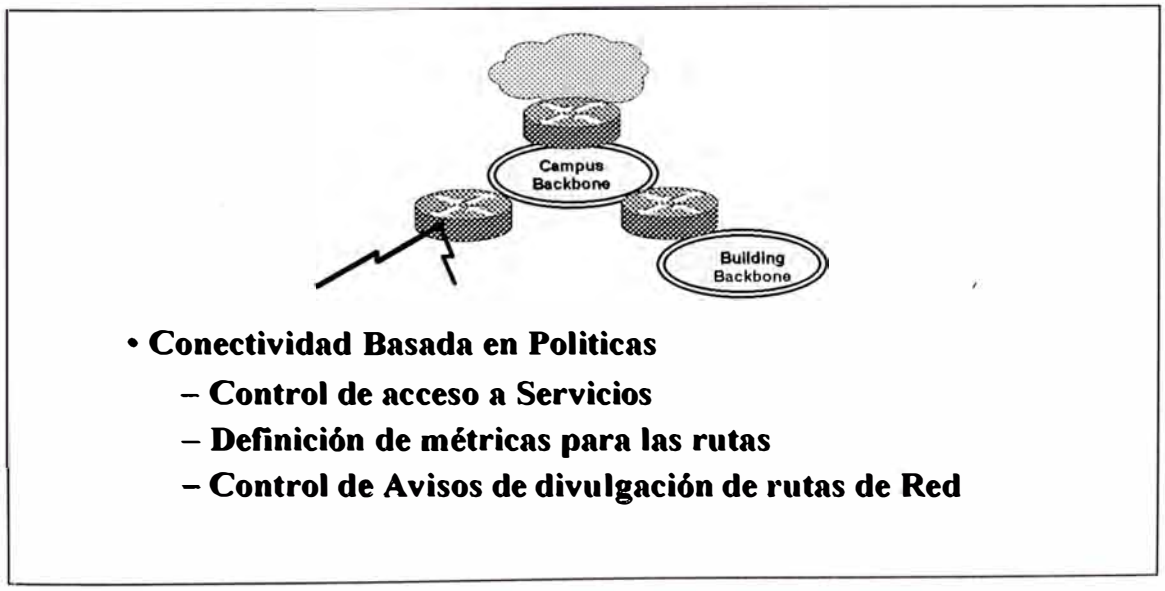


Figura 6-6 Funciones de la capa de Distribución.

Funciones de la Capa de Acceso.- La capa de acceso conecta a los usuarios dentro de las LANs, y las LANs dentro de un backbone campus. Este aproach habilita a los diseñadores a distribuir servicios a través de CPUs de los dispositivos operando en esta capa. La capa de acceso permite la segmentación lógica de la red y el agrupamiento de usuarïos basados en un comunidad de interes. Tradicionalmente, esta segmentación está basada en boundaries organizational como Marketing, administración, o Ingeniería. Sin embargo, la tecnología VLAN permite que tales agrupamientos sea basado en asociaciones ad hoc o asignamiewnto dinámico. Desde una perspectiva de administración y control de red, la principal función de la capa de acceso es aislar el tráfico broadcast al workgrup individual o LAN. Los usuarios remotos (dial up) son también conectados en esta capa de acceso. La figura 6-7 muestra las funciones que deberían ser implementadas en esta capa

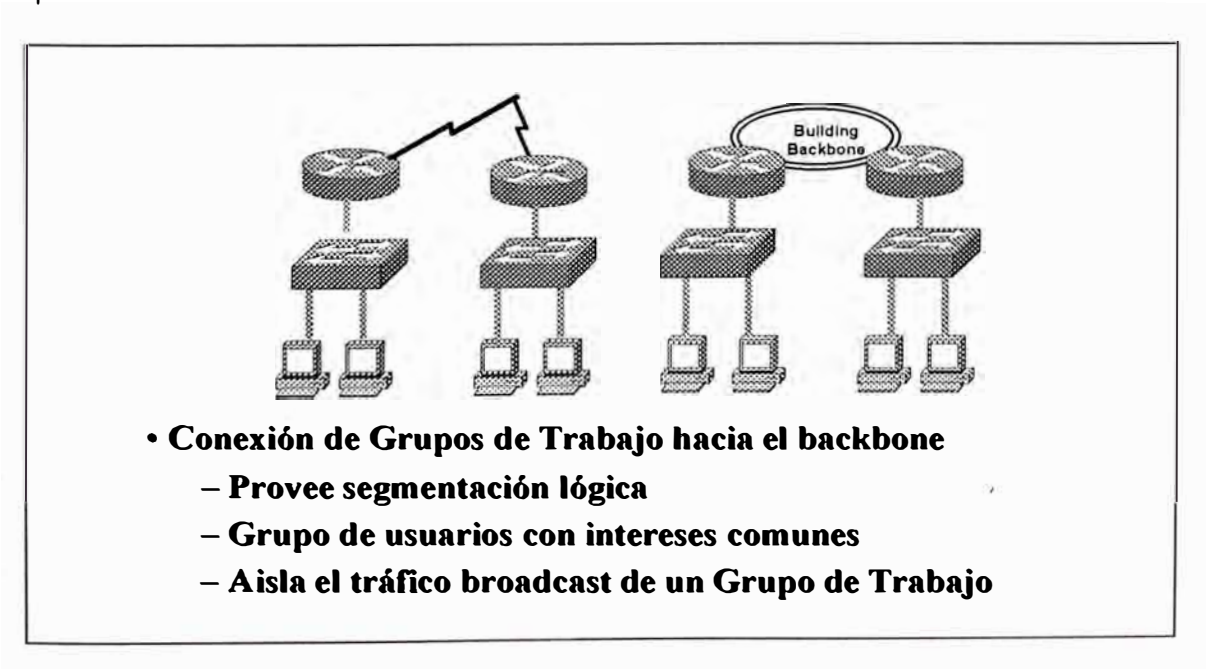


Figura 6-7 Funciones de la capa de Acceso.

Variaciones del Modelo de Tres Capas.- No tadas las redes requieren un jerarquia de tres capas. En realidad un diseño de una capa debería ser suficiente en muchos redes pequeñas. Una descisión de diseño clave viene a ser la ubicación de servidores: Ellos pueden ser distribuidos a través de múltiples LANs, o concentrados en una ubicación "server lam" central. La figura 6-8 muestra un diseño de servidor distribuido cuyo mayor beneficio son survivabilidad y bajos requermientos de ancho de banda entre sites. La desventaja de este diseño, sin embargo es la pérdida de control administrativo aun a un costo de administración muy alto debido a duplicidad de funciones en cada site.

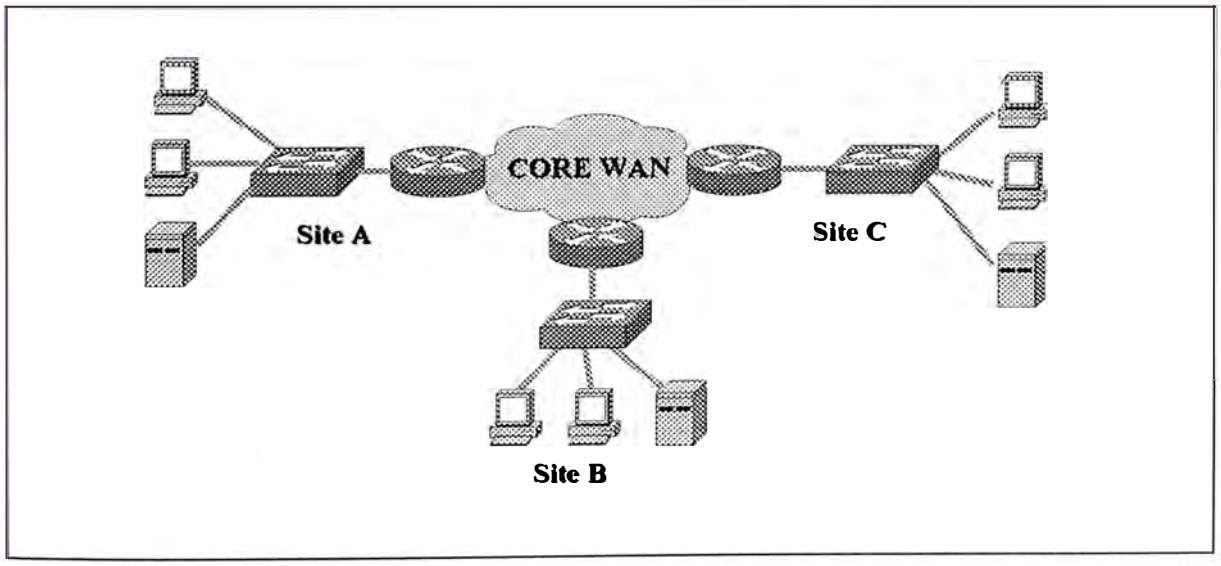


Figura 6-8 Diseño distribuido de un capa.

En el caso donde los servidores son ubicados en un farms central, un diseño hub o spoke sería típicamente desarrollado. Este diseño tiene una ventaja de incrementar el control de administrabilidad, pero puede haber concerní regarding unico punto de falla y ancho de banda agragtion.

En este diseño, el servidor de red farm por si solo hace uso de la tenología LAN de mas alto ancho de banda (por ejemplo FDI, Fast Ethernet).

En un diseño de dos capas, un backbone campus' es usado para interconectar edificos separados. Dentro del edificio una simple red lógica puede ser implementado, o múltiples redes lógicas pueden ser bridged, las VLAN pueden ser implementados para crear redes lógicas separadas redes lógicas sin requerimientos de routers adicionales. La figura 6-9 muestra un diseño de red de dos capas.

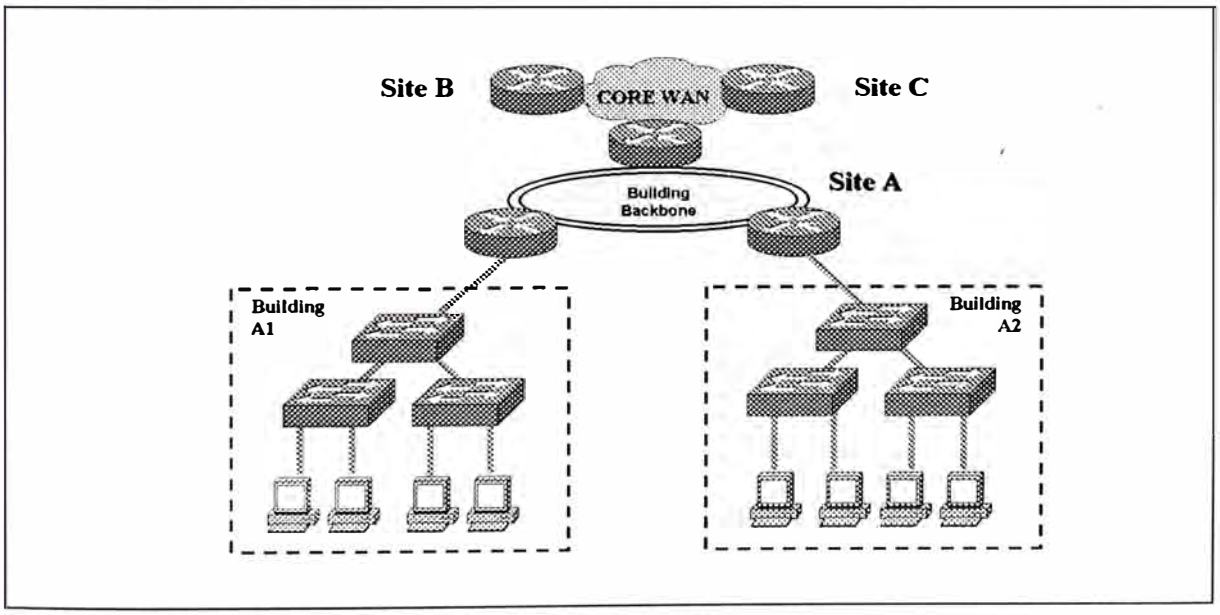


Figura 6-9 Diseño de dos capas.

6.3.- DETERMINANDO LOS REQUERIMIENTOS DE RED

El primer paso para el diseño de red es entender los requerimientos de red. Los dispositivos de red tiene que reflejar los goals, características, y políticas ded la organizacioón en la cual esta opera. Dos principales goals guian el diseño e implementación del internetworking:

- Disponibilidad de Aplicación: Las redes llevan información de aplicación entre computadoras. Si las aplicaciones nos son disponibles a los usuarios de la red, la red no está haciendo su trabajo.
- Costo de ownership: Los budget del sistema de información (IS) ded hoy en día lagunas veces estan en el millon de dolares. Como las grandes organizaciones increasingly rely en data electrónica para las actividades de negocio, los costos asociados en los recursos de computación continuarían creciendo.

Una internetwork bien diseñada puede ayudarte a balancear estos objetivos. Cuando se implementa apropiadamente, la infraestructura de red puede optimizar la disponibilidad de aplicación y permitir el uso cost.efective de recursos de red existentes.

6.3.1.- Optimizando la Disponibilidad y los Costos

En general los problemas de diseño de red consiste de los siguientes tres elementos generales:

- "Environmental givens": Incluye la ubicación de los "hosts", servidores, terminales, y otros nodos; el tráfico proyectado para el ambiente; y el costo proyectado para llevar diferentes niveles de servicio.
- "Performance constraints": Consiste de confiabilidad de la red, "traffic troughput", y velocidades de computadoras de cliente/servidor (por ejemplo, tarjetas de interface de red y velocidades de acceso de disco duro)
- Variables de "internetworking": Incluyen la topología de la red, capacidades de línea y asignamiento de flujo de paquetes.

El objetivo es minimizar los costos basados en estos tres elementos, mientras que la entrega de los servicios no comprometan los requerimientos de disponibilidad establecida. Encarar dos principales consideraciones: disponibilidad y costo. Estos temas están escencialmente sujetos. Cualquier incremento en la disponibilidad tiene que generalmente ser reflejado como un incremento en el costo. Como resultado, tenemos que evaluar la importancia relativa de disponibilidad de recursos y cuidadosamente el costo .

La figura 6-1 muestra que el diseño de la red es una actividad interactiva. Nos muestra las actividades que cuidadosamente debemos considerar cuando diseñamos una implementación de "internetworking".

6.3.2.- Assessing los Requerimientos de Usuario

En general, los usuarios quieren primeramente aplicaciones disponibles en su red. Los componentes chief de disponibilidad de aplicación son: respuesta de tiempo, troughput y confiabilidad.

Respuesta de tiempo es el tiempo entre la entrada ded un comando o keystroke y la ejecución del comando del sistema host o delivery de una respuesta. La satisfacción de los usuarios referente a la respuesta de tiempo generalmente es considerado a ser una función monotónica que sube hasta un límite, en el cual el punto de satisfacción del usuario cae proximamente a cero. Las aplicaciones en la cual la rápida respuesta de tiempo es considerado crítico inlcuye servicios on line interactivos, tales como tellers automatizados y máquinas de puntos dee venta.

Las aplicaciones que ponen alto volumen de tráfico en la red tienen mas efecto en el troughput que las conexiones end-to-end. Las aplicaciones con intensivo throughput generalmente envuelven actividades de transferencia de archivo. Sin embargo estas aplicaciones usualmente también tienen bajos requerimientos de respuesta de tiempo. Indeed, ellos pueden algunas vecees scheduled en el tiempo cuando el tráfico sensible a la respuesta de tiempo es bajo (por ejemplo, después de horas de trabajo normal)

Aunque la confiabilidad es siempre importante, algunas aplicaciones tienen requerimientos genuinos que exceden las necesidades típicas. Las organizaciones que requieren cerca del 100 por ciento up time conducen todas las actividades on line o sobre teléfonos. Los servicios financieros, intercambios de seguridad y las operaciones militares/políticas/emergencia son unois pocos ejemplos. Esta situación implica un requerimientoded un alto nivel de hardware y redundancia topológica. Determinando los costos de cualquier downtime es esencial en determinar la imporatncia de confiabiledad en tu red.

Podemos accesar a los requerimientos de una diversidad de formas. En general, podemos usar los siguientes métodos para obtener esta información:

Perfil de comunidad de Usuario: Trazar en líneas generales cuales son los requerimientos de los diferentes grupos de usuarios. Este es el primer paso en determinar los requerimientos de internetwork. Aunque muchos usuarios tienen los mismos requerimientosm un sistema de mail electrónico, grupos de Ingeniería usando terminales XWindows y workstation Sun en un ambiente NFS tiene diferentes necesaidade s que los usuarios comunes de PC compartiendo impresoras en un departamento de fiinanzas.

Entrevistas, reuniones y visitas: Construye una línea base para implementar una internetwork. Understand that some groups might require access to

common servers. Otros querían poder permitir acceso externo a recursos de computación intyerno específico. Ciertas organizaciones podrían requerir soporte a sistemas IS, para poder ser administrados de una manera particular de acuerdo a algunos estándares externos. El método menos formal de obtener información es conducir entrevistas con los grupos de usuarios. Los Focus groups puede ser usado para recoger información y generar discusión con áreas diferenters y con similar interés. Finalmente, visitas formales pueden ser usados para conseguir estadísticamente lecturas de usuarios válidas para un nivel de servicio particular o una arquitectura de red propuesta.

Pruebas de factores humanos: Este es mayormente aplicable cuando se evalúa requerimientos de respuesta de tiempo. Como un ejempolo, se podría configurar sistemas de trabajo y tener usuarios llevando a cabo operaciones de acceso remoto normal desde el laboratorio. Mediante la evaluación de reacciones de usuarios a variaciones en respuesta de los host, se puede crear un punto de referencia umbral para una performance aceptable.

6.3.3.- Assesing Costos

La Internetwork es un elemento estratégico en la información general del diseño dedl sistema. Como tal, el costo de la internetwork es mucho mas que la suma de las ordenes de embarque de los equipos. Debemos ver esto como un tema a tratar de cost-of-ownership. Hay que considerar el ciclo de vida entera del ambiente internetworking. A

continuación mostramos una breve lista de costos asociados con la internetwork :

- Costos de hardware and software: Coinsiderar que realmente se esta comprando, Cuando se embarca el sistema; los costos deberían incluir el embarque inicial y la instalación, mantenimiento y los costos de upgrade proyectados.
- Costos de tradeoff: Considere los costos ded ir de una respuesta de tiempo de cinco segundos a una respuesta de tiempo de treinta segundos. Tales mejoramientos pueden costar una fortuna en terminos de selección del medio, interfaces de red, nodos de internetworking, modems y servicioes WAN.
- Costos de instalación: Instalando cables físicos de planta en los locales o sedes, puede ser un elemento demasiado caro ded las grandes redes. Los costos incluyen la labor de instalación, modificación de los ambientes, y costos incurridos en asegurar que se cumplan las restricciones ambientales. Otro importante elemento que mantiene los costos a un mínimo incluiría el desarrollo de un diagrama de closet de alambrado bien planeado e implementar convenciones de código de color para tender e instalar los cables.
- Costs de soporte: Complica los costos de las redes, los costos de monitoreo, configuración y mantenimiento. La red no debería mas complicado que necesario, los costos incluyen entrenamiento, labor directa (administradores y gerentes de red), equipos de back-up o

sparing, y los costos ded reemplazo. El costo adicional que debería incluirse son la administración out-of-band, estaciones de administración SNMP, y energía.

- Costos de downtime: Evalúa los costos para cada minuto que el usuario es incapaz de accesar al servidor de archivos a la base de datos centralizado. Si el costo es alto deberías atribuir un alto costo al downtime. Si el costo el suficientemente alto, configuración de redes completamente redundantes debría ser la mejor opción
- Costos de oportunidad: Cada opción que tu haces tiene una alternativa opuesta. Si esa opción es una plataforma de hardware específica, solución topológica, nivel de redundancia o alternativa de integración del sistema, hay siempres muchas opciiones. Los costos de oportunidad son los costos de no recoger una de estas opciones. Los costos de oportunidad de no saltar a nuevas tecnologías y topologías, podría ser una pérdida dee ventaja competitiva, baja productividad una performance bien baja.
- Costos de reemplazo: La inversion hecha en cable de planta existente, routers, concentradores, switches, hosts, y otros equipos son los costos de reemplazo, si este costo es alto, podríamos modificar la red para la red existente pueda ser utilizaado Si estos costos son bajos, sería mas atractivo que significante rediseñar costos.

6.4.- CONSIDERACIONES DE DISEÑO DE RED CAMPUS-LAN

6.4.1.- Consideraciones Técnicas de diseño Campus-LAN

Los issues técnicas en el diseño de LAN campus puede ser agrupado como issues end-station (cliente y servidor), issues de infraestructura de red, y itemas de interés de administración de red.

Cliente end – estaciones.- Los temas a tartar en end-station incluyen el ardware y software.

Los temas de interés de software que recaen en el sistema operativo de la red, incluye los mecanismos de transporte de la red usado, y como este mecanismo recae en broadcast en su operación. Los temas de interés de aplicación incluyen la demanda de ancho de banda anticipada que las aplicaciones presentarían, y garantiza cualquier requerimiento por calidad de servicio (QoS). Aplicaciones de voz y video incrementa la importancia del QoS debido a sus requerimientos de ancho de banda dedicado.

Los temas a tratar de hardware incluyen planes para upgrade mas plataformas poderosas, el cual ubicaría mas ancho de banda en la infraestructura de la red. Otros asuntos incluyen conexiones físicas, tarjetas de interfaces y conectores de cables.

Server end – estacion.- Los asuntos de server end-station son similares a los reuqerimientos para los clientes. Los requerimientos de ancho de banda para los serviodres son altos debido a la ubicación centralizada y de solicitudes de usuarios múltiples y actuales. La necesidad por ancho de banda dedicado via un puerto switch y una via de acceso a un backbone de alta performance, tales como FasEthernet, es reenforzado por los requerimientos de muchas aplicaciones de alto poder.

La figura 6-10 nos muestra los issues de un client end-station.

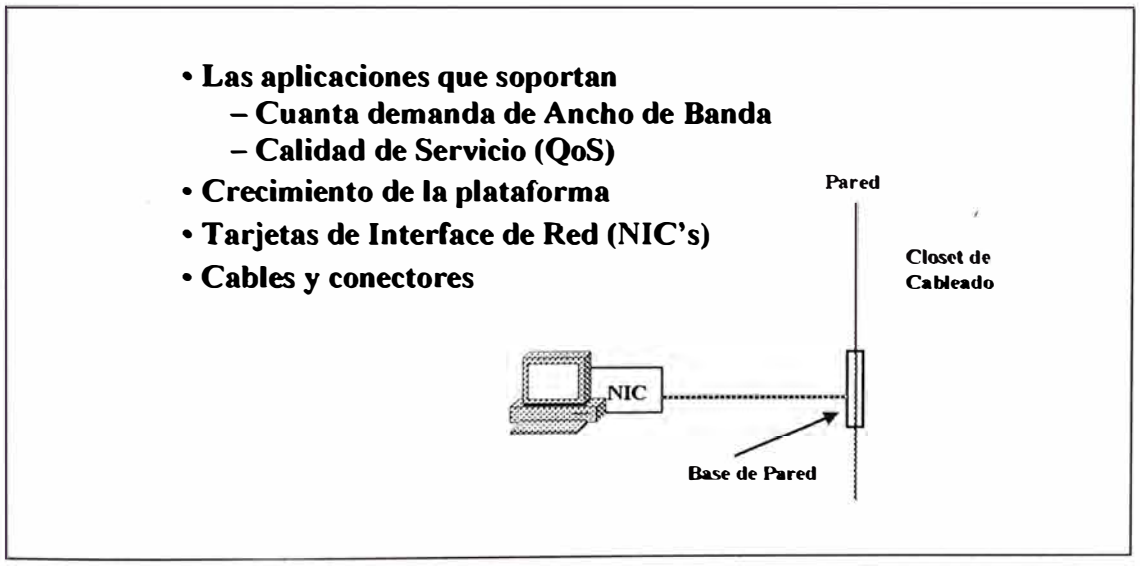


Figura 6-10 Elementos de la Estación-Final del cliente.

La ubicación de servidores, es una consideración crítica debido a la diferentes necesidades del suit de protocolos y aplicacines que se están soportando. Los servidores son requeridos para ser accesisible continuamente, y evitar el circuit outage tales como los enlaces WAN y si

provee un conexión simple o dual debería ser parte de la estrategia de diseño.

La figura 6-11 nos muestra los issues de un server end-station.

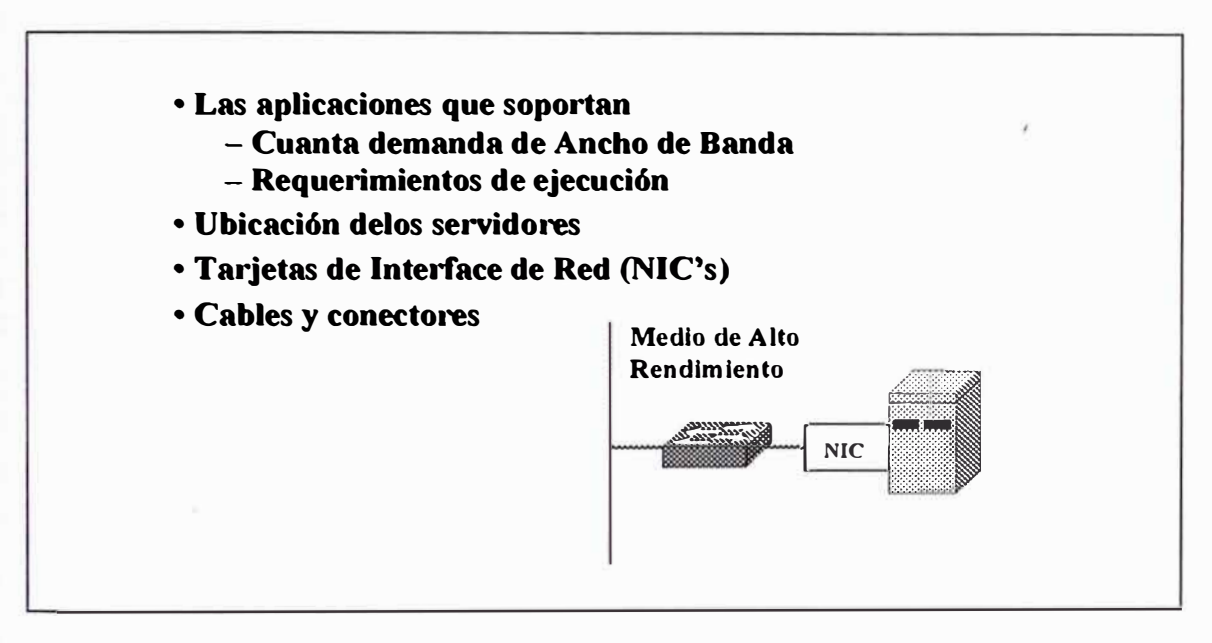


Figura 6-11 Elementos de la Estación-Final del Servidor.

Infraestructura de red.- Los issues de la infraestructura de red incluye si se desarrolla un backbone colapsado o distribuido. Los requerimientos ded ancho de banda del backbone también tiene que ser considerado de la mano con el tipo de tecnología que sería desarrollado. Los costos y beneficios de desarrollar bridging, switching, o routing tienen que ser considerados.

Administración de red.- Los temas de administración incluyen la elección de una plataforma de administración de red y la decisión para administrar la red en un estilo centralizado o distribuido. La mayoría de las administraciones de red de hoy en día están basados en "Simple Network Management Protocol" (SNMP); sin embargo se deben de hacer decisiones referidos a los diferentes tipos de estaciones administradas y herramientas que ellos soportan. También considerar temas generales de administración de usuarios finales, tales como una estratégia para modificar la configuración física (mover, adicionar, y cambiar), como usuarios que se mueven a diferentes ubicaciones y/o la red crezca. EL crecimiento de la red puede incluir una consideración de desarrollar tecnologías LAN virtuales (VLAN).

6.4.2.- Consideraciones de Negocio

Los temas de negocios, incluyen las consideraciones presupuestales, tales como el costo del equipo y el software, el costo de mantenimiento, y los costos y beneficios de preservar la inversión en los componentes de una red existente. Los costos de propiedades alrededor de costos recurrentes, tales como el salario y el entrenamiento de los administradores, tarifas mensuales de circuitos WAN, y otros cargos operativos. Típicamente confrontaría otros temas, como adherir estándares opertivas y de industria, y desarrollar temas para la adopción de tecnologías emergentes. También es importante para el tema de negocios el encontrar los requerimientos de las redes actuales y la planificación para su crecimiento.

CAPÍTULO VII

DISEÑO DE RED CAMPUS-LAN

Tradicionalmente, los diseñadores de LAN recomendaron bridges cuando había la necesiada por segmentar la red. Los diseñadores recomendaron el uso de routers parta manipular internetwork de medio mezclado para evitar problemas relacionado con la fragmentación y direcciones de bit reservados que los routers manipulan mejor que los bridges. Los routers también soportan direcciones ded capa de red jerarquico, provee acceso a la WAN, filtro ded broadcast, ofrece seguridad, provee sumarización de direcciones y administración de flujode tráfico.

7.1.- MODELO DE DISEÑO DEL CABLEADO ESTRUCTURADO

El cable físico de planta es uno de los mas importantes issues a considerar cuando se diseña una red. El issues de diseño incluye el tipo de cable a ser usado (típicamente cobre o fibra) y sobre todo la estructura de la planta de cable. En adición a las limitaciones de distancia, evalua cuidadosamente las strenghs y waknesses de varias topologias de cableado.

En los comienzos de los 80´s la mayoría de las reds LAN consistía de thick y thin cableados Ethernet y token Ring . Al final de los 80´s

la mayopría de compañías adoptaron la regla del diseño de cableados estructurados jerárquicos. La figura muetra un sistema de cableado jerárquico flexible y muy bien diseñado

Existe dos tipos de cableados que pueden ser implementados en un edificio, el cableado horizontal y el vertical.

7.1.1.- Cableado Horizontal

El cableado horizontal, la cual es instalado desde el closet de cableado hasta cada estación de trabajo, y puede ser implementado con cable coaxial o par trensado, en anillo, o estrella. La IEEE 802.3 especifica muchos estándares de cableado para implementar una red Ethernet, los mas importantes son:

- 10Base 5 basado en cable coaxial thick
- 10Base2 basado en cable coaxial dedlgado
- 10BaseT basado en cable ded par trensado sin pantalla (UTP).

Así mismo el cable UTP es rated acorde con su capacidad de llevar la data y son:

- Nivel 1, usado para voz digital y analógica y aplicaciones de baja velocidad
- Nivel 2, usado para ISDN y velocidades medias de datos
- Nivel 3, usado para datos de alta velocidad de hasta 16 Mbps
- Nivel 4, usado para tráfico LAN a grandes distancias hasta 20 Mbps

- Nivel 5, usado para tecnologías UTP dee 100Mbps tales como Ethernet 100-Mbps.
- Nivel 6, usado para tecnologías de 1000Mbps tales como Ethernet Gigabit.

Los componentes activos de la red (hubs, bridges, switches, routers) son típicamente ubicados en los closet de cableado de cada piso, y el centro de datos en la base. El cable de par trensado sin pantalla Categoría 5 debería ser en la mayoría de los casos, usado para enlazar clientes desktop y servidores locales a los equipos activos en los closet de cableado. Un segmento cat 5 UTP es generalmente considerado para ser usado a velocidades de hasta 100Mbps, sobre una distancia máxiam de 100 metros.

7.1.2.- Cableado Vertical o Backbone

El cableado vertical, la cual es instalado desde el Main Distribution Frame (MDF) a los closet de cableado ubicados en cada piso del edificio. La IEEE 802.3 especificó el estándar 10BaseF, basado en cable de fibra óptica multimodo. Adiconalmente es necesario la instalación de fibra óptica monomodo entre pisos para uso futuro.

Las recomendaciones de cableado en general nos guían por fibras tipo riser entre pisos y ductos que típicamente conectan edificios con ambientes campus. La fibra óptica permite que el ancho de banda sea

escalable tan alto como sea necesario mientras provee enlaces confiables que son resistentes a la Interferencia Electromagnética (EMI).

Existe dos tipos de backbone a ser implementado en un diseño de red: Backbone Distribuido y Backbone Colapsado-

Backbone Distribuido.- En el modelo de backone distribuido en edificio cmo mustra la figura 7-1, los routers de cada piso se conectan al backbone en el riser. En este caso el backbone es típicamente un anillo FDDI. El diseño tiene el beneficio de distribuir las conexiones hacia el backbone y asi eliminar cualquier puntode falla.

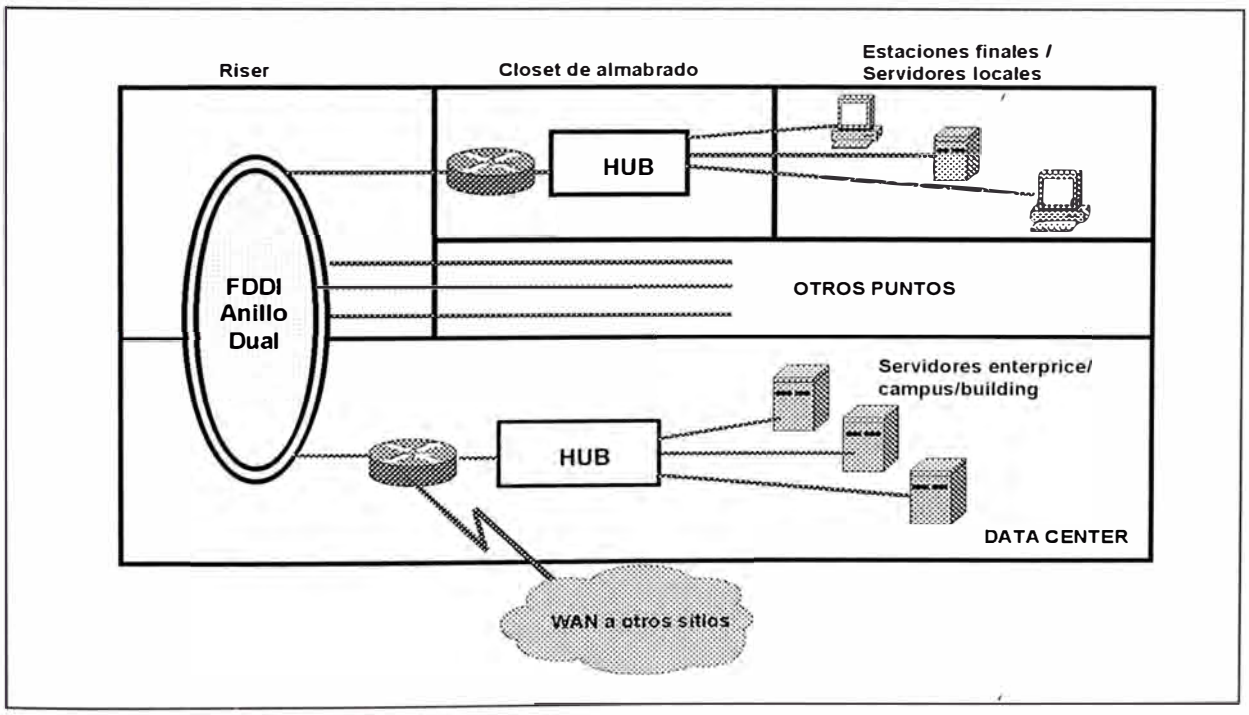


Figura 7-1 Backbone distribuido - Building.

El diseño tiene tambien drawback. Multiples números de red dentro de un edificio reduce la facilidad con el cual el usuario se pueda adicionar, muever y cambiar. Además, este diseño tiendee a ser mas caro y no permite migrar fácilmente a uan red switching.

Notar que en este diseño, no hay estaciones finales adjuntas al backbone. Este es un diseño importante que debemos continuar siguiendo. El backbone únicamente debería ser usado para transitar rutas entre redes locales, y no como una red basado en host por si sola. Este guideline mantiene al backbone mas estable, facilita la administración de tráfico y la capacidad de planeamiento, y mejora la escalabilidad para futuros diseños.

Por otro lado el backbone distribuido en campus es una solución mas eficiente de recursos que el de edificos. Esta solución envuelve un único router por edificio, típicamente localizado en la base (MDF), con una conbinación de hubs y switches proveiendo al usuario acceso throughput al edificio. Con pocas redes lógicas por edificio, la facilidad de adicionar, mover y cambiar usuarios es incrementada. El único drawback es el lack de flexibilidad en conexión con otros edificio en el campus. Los switches fácilmente podrían ser desarrollados en el edificio, pero no a través del campus.

La figura 7-2 nos muestra un ejemplo de backbone campus distribuido.

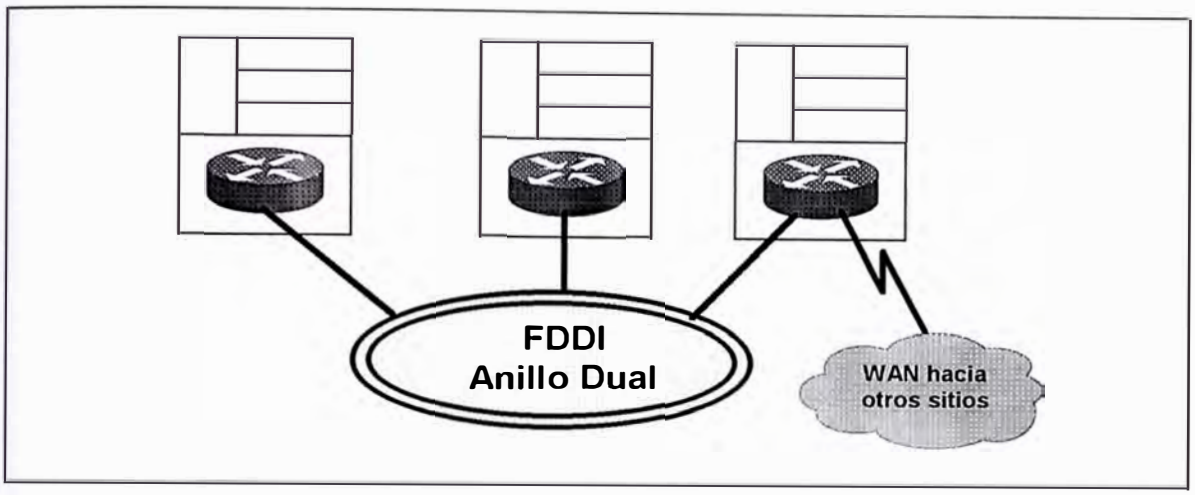


Figura 7-2 Backbone distribuido - Campus.

Backbone Colapsado.- Los backbones colapsados generalmente representan una aproximación mas flexibles y cost-effective para cablear un edificio. En este caso, el anillo tradicional o el bus backbone es colapsado dentro de un único switch o router, haciendo que el back plane del equipo se comporte como una red backbone. Los hubs en cada piso son usados para conectar las estaciones finales en el workgroup, y cada uno se adjunta a una interface LAN separada en el router. Este diseño debería de hacer que los movimientos de usuarios sean mas fáciles que el modelo backbone distribuido, pero la solución no es aún ideal. También, los routers representan un único punto de falla. Esta situación podría ser corregida mediante el desarrollo de un segundo router que se adjunta al hub y usa el protocolo Hot Standby Router. (HSBRP).

La figura 7-3 nos muestra una red backbone colapsado utilizando router y hubs.

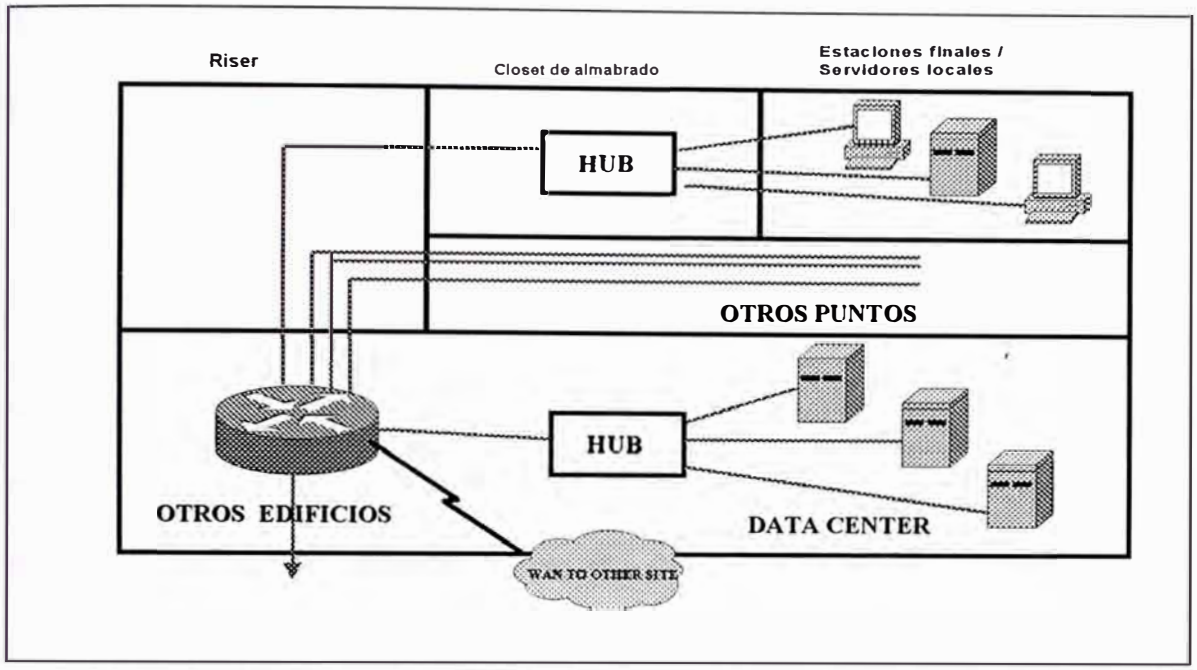


Figura 7-3 Backbone Colapsado – Router/Hub.

El hub en el diseño previo podría ser reemplazado fácilmente con un switch ethernet para proveer mas ancho de banda al workgroup. Sin embargo, el uso de un único router representa un cuello de botella en el flujo de tráfico y un único punto de falla.

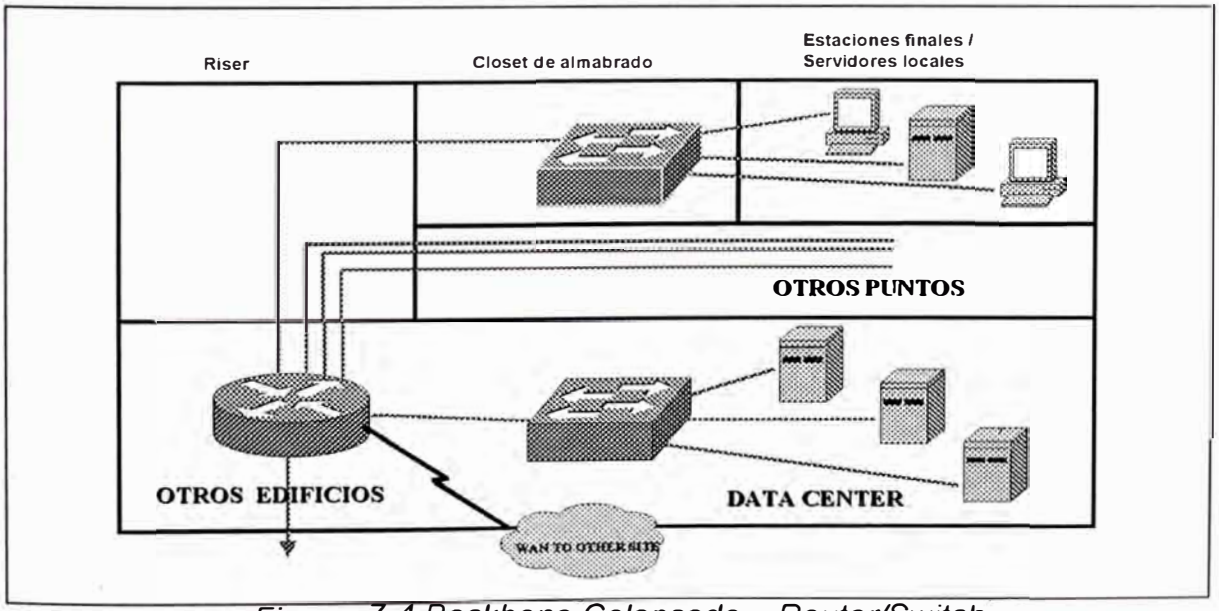


Figura 7-4 Backbone Colapsado – Router/Switch.

La figura 7-4 nos muestra un diseño de red backbone colapsado con router y switches.

El diseño de backbone colapsado puede fácilmente ser extendido para acomodar VLAN´s, simplemente adicionando otro ethernet switch en el data center. El backplane del switch ahora viene a ser el backbone colapsado para el edificio. En este caso el router tiene un puerto ethernet separado para cada VLAN, y las comunicaciones entre VLAN´s ocurren en el router. El router también proveen el límite de punto de conexión para acceder a otros edificos en la red.

La figura 7-5 nos muestra un backbone de red utilizando la tecnología VLAN.

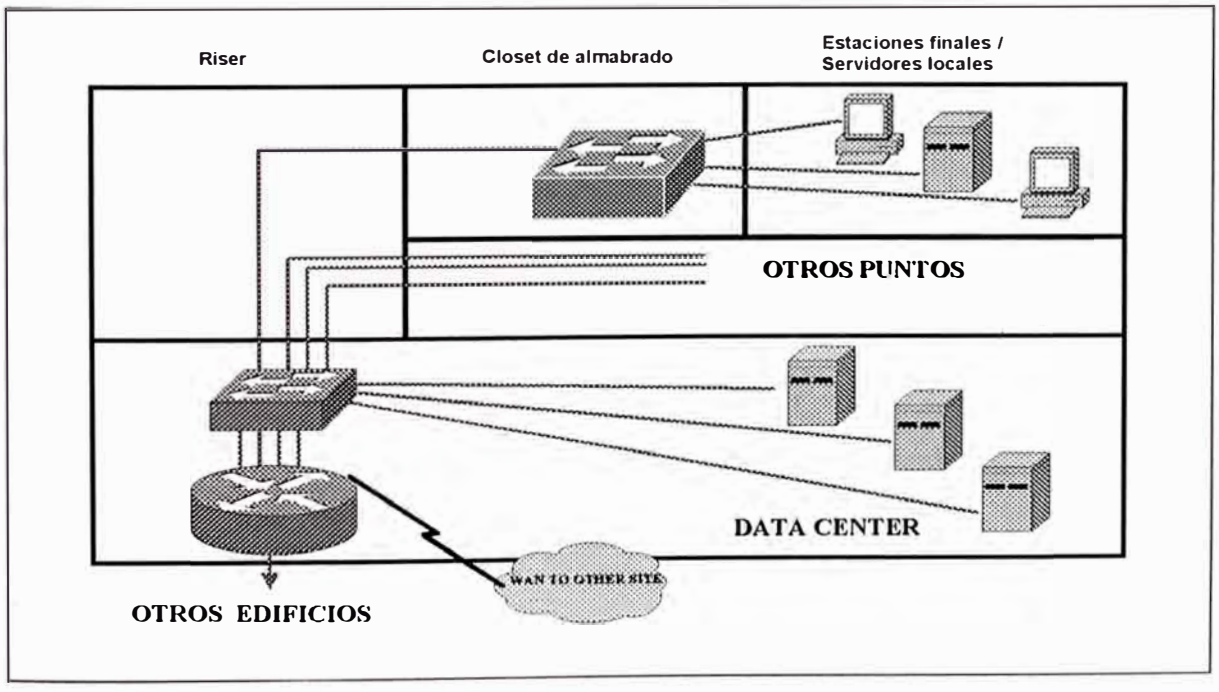


Figura 7-5 Backbone Colapsado – Building VLAN.

7.1.3.- Terminologías de Diseño Campus-LAN

En esta parte explicaremos algunas terminologías que son muy comunmente usados para describir los diseños de red. La discusión comienza con una revisión de la terminología de Intermediate Distribution Frame / Main Distribution Frame (IDF / MDF) que han sido prestado desde la industria telefónica.

Por años, la industria telefónica ha usado el termino Intermediate Distribution Frame (IDF) y Main Distribution Frame (MDF) para referirse a varios elementos del cableado estructurado. Como el cableado estructurado ha crecido en popularidad dentro del círculo de comunicación de datos, esta terminología IDF / MDF también ha llegado a ser común.

La siguiente sección discute algunos de los requerimientos de los switches ubicados en los closets IDF y MDF. Adicionalmente a estos requerimientos especializados, algunas características deberían ser compartidos a través de todos los switches. Para nuevas instalaciones, todos los switches deberían ofrecer una amplia variedad de tipos de medios, que inlcuye varias velocidades Ethernet y ATM. FDDI y Token Ring, que pueden ser importantes cuando se migra antiguas redes. También, debido a la infraestructura de "campus switched" modernos, son tan complejos para la propuesta "plug-it-in-and-forget-it".

IDF.- Los closet de cableado IDF son usados para conectar dispositivos ded estaciones fiunales tales como PCs y terminales a la red. Este cableado horizontal conecta al jack de la pared en un terminal y típicamente consiste de cableado par trenzado sin apantallar (UTP) que forma una estrella hacia el closet ded cableado IDF . Como mostrado en la figura 7-6, cada piso del edifico generalemte contiene uno o mas switches IDF. Cada estación final se conecta al closet de cableado IDF mas cercano. Todos los IDF´s en el edificio generalmente conectan a un par de dispositivos MDF algunas veces ubicados en la base del edificio o bajo tierra.

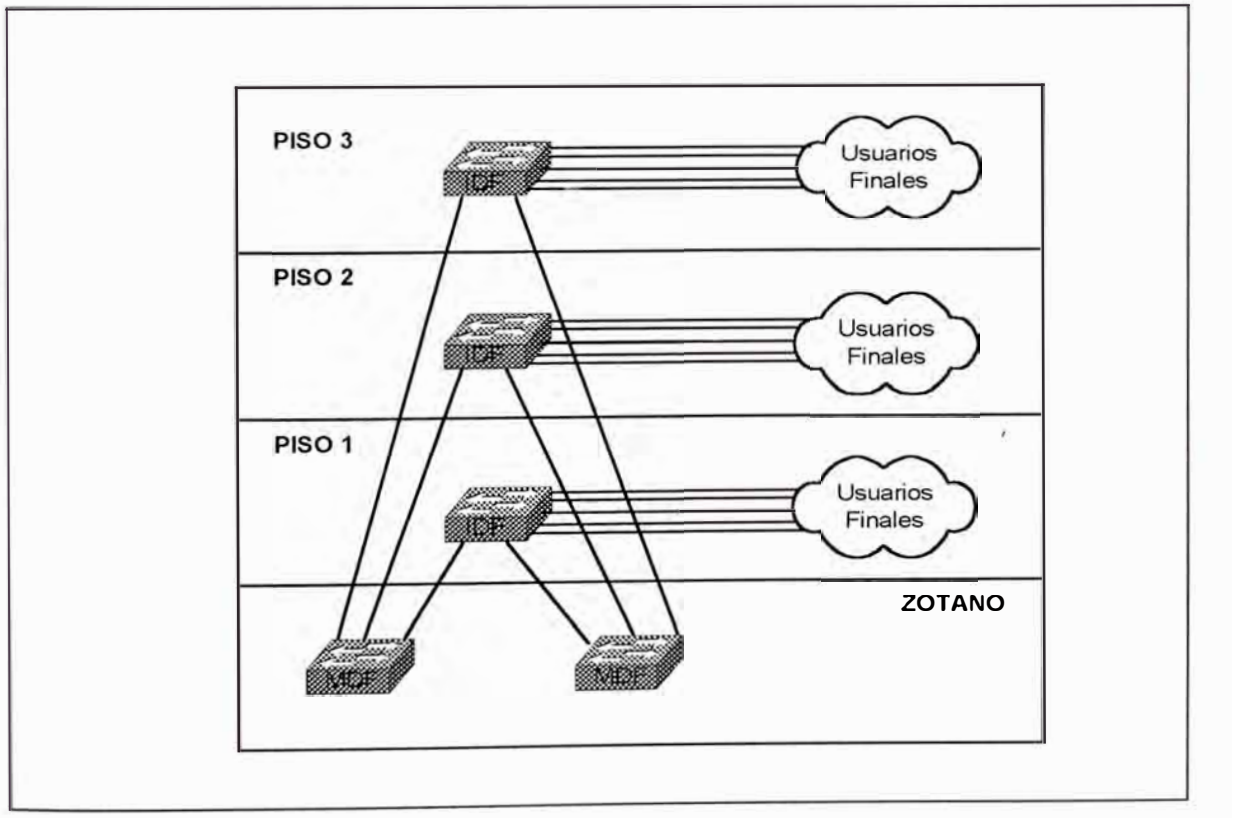


Figura 7-6 Múltiples Closet de Cableado IDF.

Dado el role que ellos llevan a cabo, los closets de cableado IDF tiene muchos requerimientos específicos:

- Densidad de Puertos: Debido a que gran número de estaciones finales necesitan conectarse a cada IDF, debemos tener un densidad de puertos alto.
- Costo Por Puerto: Dado la alta dednsidad de puertos encontrado en un IDF típico, el costo por puerto tiene que ser razonable.
- Redundancia: Debido a que cintos de dispositivos se conectan a cada equipo IDF, una simple falla de un IDF puede crear un significante outage.
- Confiabilidad: Este punto es obviamente relacionado al punto previo, sin embargo este resalta la realidad que un dispositivo IDF es usualmente una estación final que únicamente enlaza al resto del mundo.
- Fácil de Administrar: El alto número de conexiones requiere que la administración por puerto sea mantenido a un mínimo.

Debido a los numerosos usuarios finales, directamente conectados, la redundancia y la confiabilidad son críticas al role del IDF. Como resultado, los IDF´s no únicamente deberían utilizar hardware redundante tal como un power suplí y supervuisores duales, ellos deberían tener múltiples enlaces a los dispositivos MDF´s. Una falla rápida de estos componentes redundantes también es crítico.

La confiablidad del IDF trae un punto interesante acerca de las conexiones de los usuarios finales. Por ejemplo, fuera de los ambientes limitados como el área de finanzas, la relación costo-efecto no es muy buena al tener estaciones finales conectados a mas de un dispositivo IDF. Además, el cableado horizontal sirve como un punto simple de falla para la mayoría de redes. Sin embargo, notar que estas fallas generalmente afectan únicamente a estaciones finales. Este es en gran proporción mucho menos destructivo que perder un switch. Por la importancia de las estaciones finales tales como servidores, los NIC´s de puerto dual de los servidores farm, pueden ser utilizados con múltiples enlaces hacia los switches redundantes.

El dispositivo tradicional para uso en "closets" de cableado IDF es un hub. Debido a que la mayoría de hubs son dispositivos mas simples, el precio por puerto puede ser muy atractivo. Sin embargo, la naturaleza compartida de los hubs obviamente proporciona menos disponibilidad de ancho de banda. Por otro lado, los routers y switches de capa 3 pueden proveer opciones extremadamente inteligentes de compartir anchos de bandas. Como desventaja, estos dispositivos puede ser muy caros y generalmente tienen densidad de puertos limitados.

Para alcanzar un balanceo entre costos, disponibilidad de ancho de banda y densidad de puertos, casi todas las recientes redes "campus" desarrolladas usan switches capa 2 en los IDF´s. Este puede ser una muy

buena forma de cost effective para proveer 500 o mas estaciones finales con acceso a lata velocidad dentro de un backbone campus.

MDF.- Los dispositivos IDF colapsan en uno o mas dispositivos Main Distribution Frame (MDF) en un fashion star-like. Cada IDF usualmente se conecta a dos dispositivos MDF diferentes para proveer adcuada redundancia. Algunas organizaciones ubican ambos dispositivos MDF en el mismo closet físico y rely on disparate routing del cableado vertical por redundancia. Otras organizaciones prefieren ubicar losdispositivos MDFs en closet separados contiguos. La relación entre edificios y MDF no es una regla dura. Cuan mas grande sea el edificio podría tener mas que dos switches MDF, mientras que un par de dispositivos MDF redundantes podría ser capaz de llevar múltiples edificios que son mas pequeños en tamaño.

La figura 7-7 muestra tres edificios con closets MDF. Para encontrar los requerimientos de redundancia, cada edificó generalmente aloja dos dispositivos MDF. Los dispositivos MDF pueden también se usados para interconetar los tres edificios.

Los closets MDF tienen un diferente conjunto de requerimientos y concerns que closets IDF:

- Throutput
- Alta disponibilidad
- Capacidades de enrutamiento

Dado que ellos actuan como puntos de concentraci+ón para tráfico IDF, los dispositivos MDFs tiene que ser capaz de llévar niveles de tráfico extremadamente altos. En el caso de un switch de capa 2, este ancho de banda es inexpensive y readily disponible. Sin embargo, muchas de esta estratégias de alcanzar diseños robustos y escalables requiere enrutamiento en los MDFs. Achieving este nivel de performacia de capa 3 puede requerir algun plan ded cuidado.

Alta disponibilidad es un requerimiento importante para los dispositivos MDF. Aunque la falla de un switch IDF o MDF potencialmente afecta a muchos usuarios, hay una distinción substancial entre estas dos situaciones. Como discutimos en la sección previa, la falla de un dispositivo IDF completamente deshabilita a muchos cientos de estaciones finales. Por otro lado, Debido a que los MDFs son casi siempre desarrollados en pares, las fallas raramente resulta en una inconsecuencia. Por lo contrario, la falla en un MDF afecta a miles de usuarios, mucho mas que con la falla de un IDF. Este requiere tantas características como sea posible para que reenrute el tráfico alrededor del problema MDF.

Adiconalemte, otras características de enrutamiento pueden ser importantes en situaciones MDF. Por ejemplo, el issue de que los protocolos de capa 3 dedl router handles puede ser importante (/IP, IPX, Apple Talk, y mas). El soporte de protocolos de enrutamiento (OSPF, RIP, EIGRP, IS-IS, y

mas) puede tambien ser un factor. Soporte para característica tales como DHCP relay y SEP puede ser críticos.

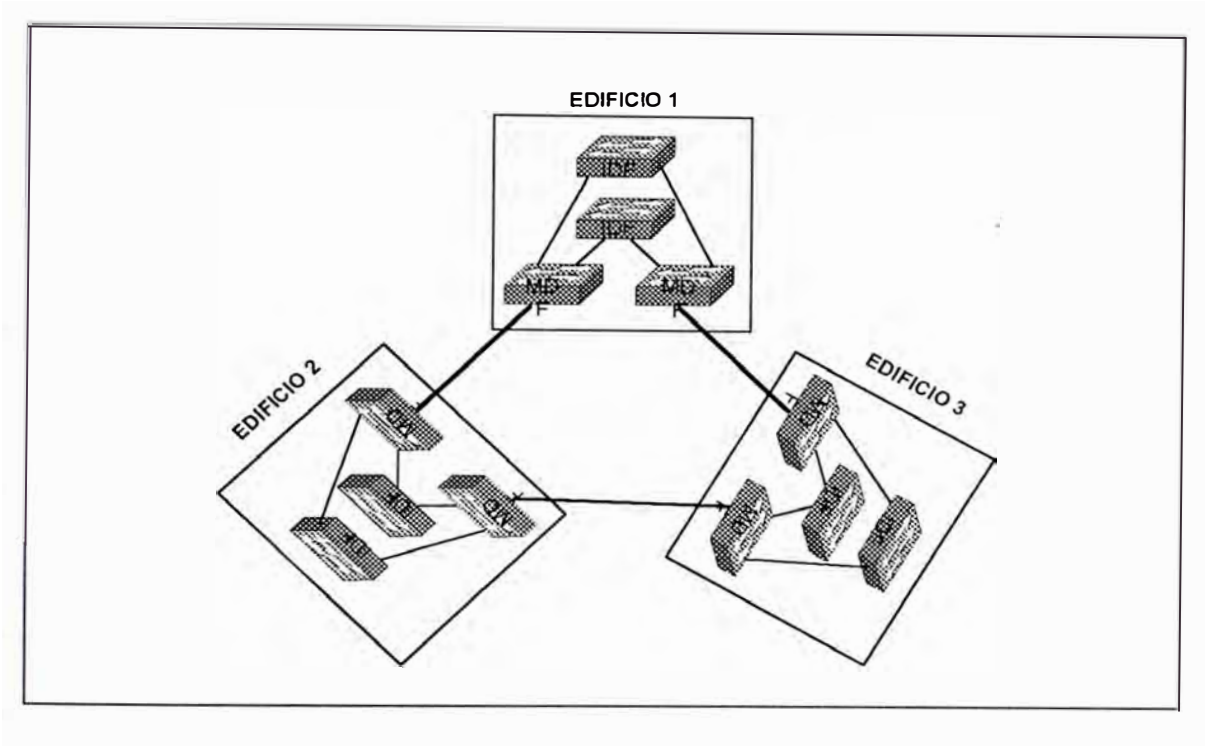


Figura 7-7 Múltiples Closet Principales MDF.

Hay tres tipos de dispositivos que pueden ser utilizados en closets MDF´s:

- Switches de capa 2
- Híbridos "Routing switches" tales como MLS (multilayer switching)
- "Swtiching routers" tales como el Catalyst 8540.

7.2.- MODELOS DE DISEÑO CAMPUS-LAN

Aunque existe un millar de permutaciones y variaciones, la mayoría de diseños campus pueden ser agrupados dedntro dee tres categorías:

- El tradicional modelo router y hubs
- El modelo VLAN campus-wide (también conocido como flat earth and end to end VLAN)
- Modelo multicapas

En esta sección explicaremos en mas detalle cada uno de estos tres diseño de modelo campus.

7.2.1.- Modelo Router y Hub

La figura 7-8 nos iilustra el tradicional modelo router y hub. Este tradicional modelo usa hubs de capa 1 en los IDF / closets de alambrado de acceso. Estos se conectan hacia los puertos únicos ubicados en el MDF/closet de distribución. Muchas opciones son disponibles para el campus core. En un aproach, los routers de la capa de distribución directamentes se interconectan para formar el core/backbone de red. Debido a su confiabilidad y su performance un anillo FDDI tradicionalmente ha sido el medio de elección de estoas conexiones. En otros casos, algunbos diseñadores de red prefieren formar un backbone colapsado con un hub o router.

Hay muchas ventajas del modelo hub y router como también muchas razones por que la mayoría de diseñadores han shied Hawai de este aproach. La tabla 7-1 lista las desventajas y ventajas del modelo router y hub.

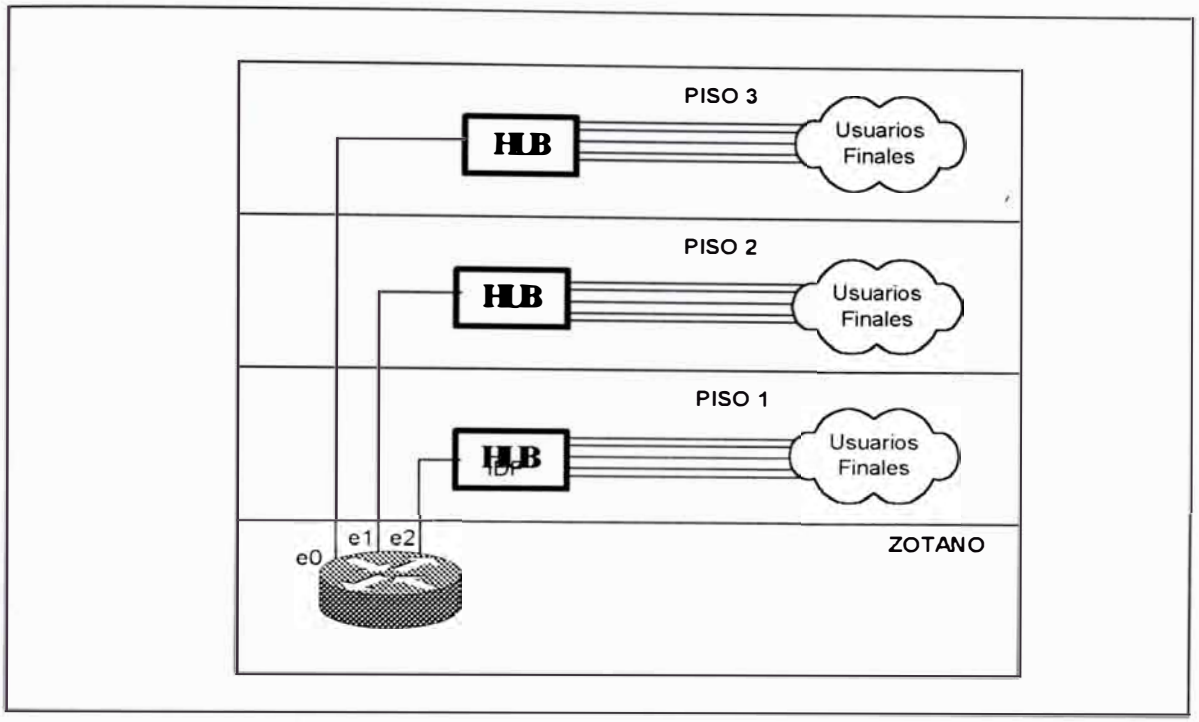


Figura 7-8 Modelo Router y Hub.

VENTAJAS	DESVENTAJAS
Su performance en router hace que el control de multicast y broadcast sean muy buenos.	Los Hubs de medio compartido no ofrecen suficiente ancho de banda para las aplicacines modernas.
Debido a que cada Hub representa un único subnet IP o una red IPX, la adiministración es fuerte y fácil de entender.	Este diseño generálmente usa routers basado en software que no pueden mantener tráfico de niveles crecientes.
dado el nivel moderado de tráfico y servidores departamentales ubicados en el segmento local, el modelo de routers y hubs puede introducir adecuado performance.	Los patrones de tráfico han cambiado, invalidando el supuesto de que el mayor tráfico debería permanecer local. Como resultado, el modelo campus-wide llegó a ser
El hardware para este modelo es disponible y no muy caro.	popular

Tabla 7-1 Ventajas y desventajas del modeelo Router y Hub.

La principal ventaja de este aproach es la simplicidad y la familiaridad que trae al diseño y administración de la red campus. La principal desventaja es el ancho de banda limitado que este medio compartido ofrece. El modedlo de diseño multicapas discutido mas tarde intenta capitalizar en la simplicidad del modelo router y hub mientras completamente evita el ancho de banda limitado a través del uso de tecnología dee conmutación capa 2 y capa 3.

7.2.2.- Modelo VLANs Campus--Wide

Como las personas comienzan a notar que sus redes de router y hub struggling para mantener con la dedmanda de tráfico, ellos buscaron alternativas. Muchas de estas organizaciones decidieron implementar el VLAN campus-wide, también conocido como el flat earth and end-to-end VLAN para el diseño de red.

El VLAN campus-wide strive elimina el uso de routers. Debido a que los router han llegado a ser un significante cuello de botella en redes campus, las personas buscaron formas de minimizar su uso. Como el dominio dee broadcast aun necesito ser held a un tamaño razonable, las VLANs fueron usados para crear barreras lógicas al broadcast. La figura 7-9 ilustra un típico diseño VLAN campus-wide.

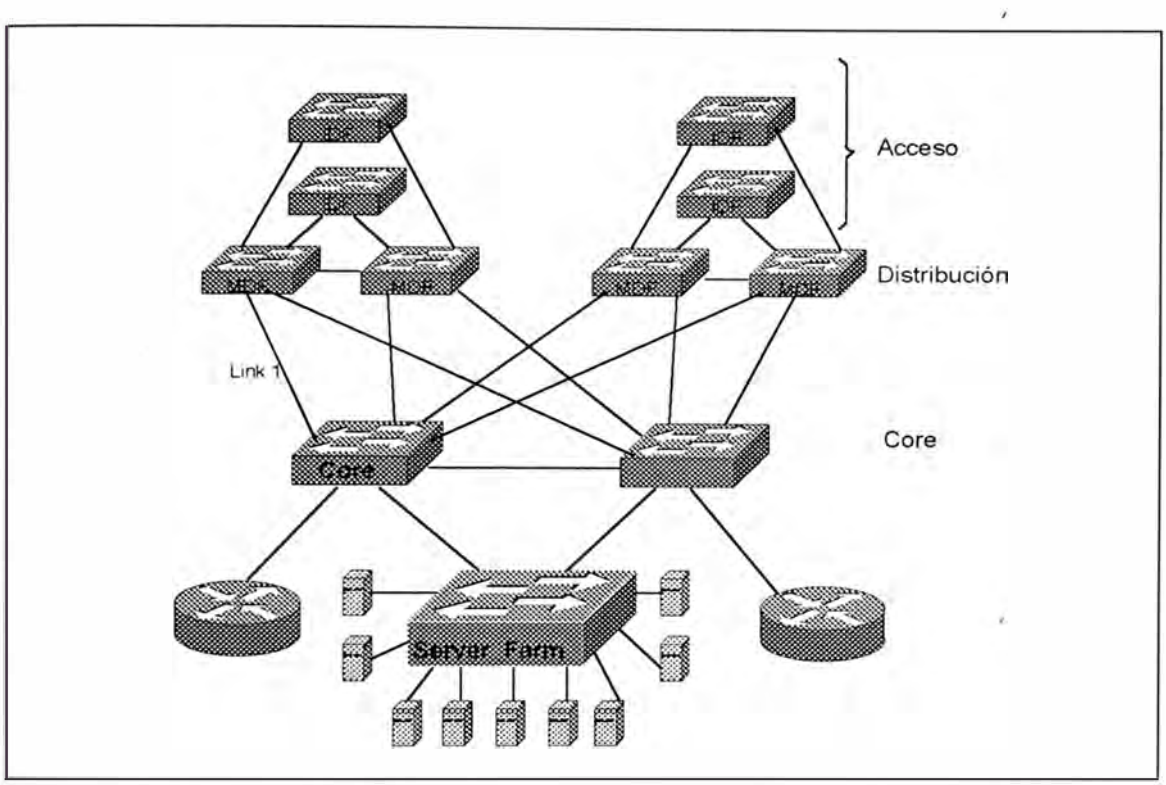


Figura 7-9 Modelo Campus-Wide VLAN

La figura anterior usa switching capa 2 a través de la red entera. Para proveer la comunicación entre las VLANs, dos routers han sido provistos usando la configuración router-on-a-stick

Ventajas del Modelo VLAN Campus-Wide.- Primero, el modelo campus-wide permite que los diseñadores de red crean una ruta capa 2 directa desde las estaciones finales hacia los servidores usados comúnmente. Desarrollando el switching capa 2 en todos las capas (acceso/distribución/core), el VLAN campus-wide dedbería dramáticamente incrementar la disponibilidad del ancho de banda.

La segunda ventaja de este modelo es que las VLANs pueden ser usados para proveer control lógico sobre el dominio de broadcast y además subredes. Algunas plataformas permiten que los switches automáticamente detecten que VLANs en una estación final deberían ser asignados para no requerir administración para adicionar, mover y hacer cambios. Otros esquemas permiten un control mas centralizado sobre asignamientos de VLAN y se esfuerzan para hacer la administración mas fácil como sea posible.

La tercera ventaja es que el tráfico únicamente va a través del router si se necesita atravesar las vecindades de VLANs. Si un usuario de finanzas necesita acceder al servidor de finanzas (ubicado en la misma VLAN) no usa ningun router. Sin embargo, si este usuario necesita ocasionalmente acceder a un servidor en la VLAN de Marketing, un router es usado. Los servidores pueden ser directamente conectados a múltiples VLANs a través del uso de ISL o LANE NICs, reduciendo asi los requerimientos del router. Por ejemplo el servidor en la VLAN de Marketing puede ser fijado con un ISL NIC para permitir un acceso directo de capa 2 a la VLAN de Finanzas.

Finalmente este uso centralizado de enrutamiento puede hacer mucho más fácil configurar listas de acceso y seguridad en la red. Por ejemplo, considere el caso de una red donde dos VLANs existen: estudiantes y profesor. Estas dos VLAN podrían expandirse a docenas de

edificios, pero debido al enrutamiento centralizado típicamente usado con VLANs campus-wide, las listas de acceso podrían ser únicamente necesitados a sser configurados en un par de routers. Por otro lado, si cada edificio en el campus conectado al backbone campus a través de un router, la red podría requerir miles de listas de acceso scattered a través de muchas docenas de routers.

El resultado final, tenemos la velocidad de capa 2, la flexibilidad de VLANs y hemos evitado el slowness del router.

Desventaja del Modelo Campus-Wide.- Algunas desventaja significativas de este modelo se cita a continuación:

- Dificultades de administración
- Lack de estructura lógica
- Dominio de Spanning Tree grande y overlapping
- Es fácil para un problema en una VLAN deplete ancho de banda en todas las VLANs a través de enlaces troncales.
- Muchas redes que usan VLAN Campus-wide tiene que resort para eliminar todas las redundancias para llegar a la estabilidad de la red.
- Lack de Escalabilidad
- La mayoría de tráfico moderno viola la regla "stay in one sbnet" empleado por el modelo VLAN Campus-wide
- Los routers modernos no son un "cuelo de botella".

7.2.3.- Modelo Multicapas

El modelo multicapas strive para proveer la estabilidad y escalabilidad del modelo router y hub mientras que también captura la performancia del modelo VLAN campus-wide. Este aproach toma ventaja completa del enrutamiento basado en hardware. El switching capa 3, para poner el enrutamiento de regreso a su lugar corecto. Sin embargo. Este no ignora el switching capa 2. En realidad, este seeks to strike el balance óptimo. La figura 7-10 ilustra una muestra de red usando el modelo multicapas.

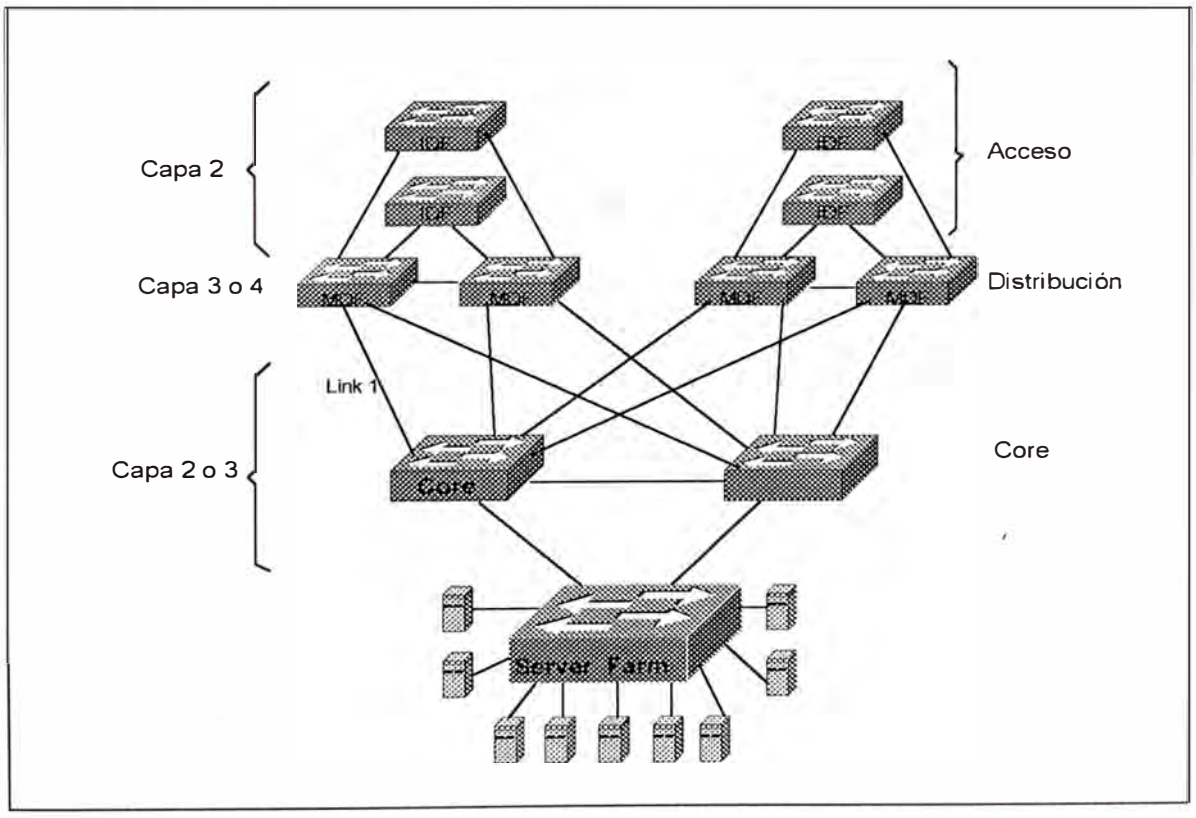


Figura 7-10 Modelo Multicapas.

Cada cluster IDF y MDF forma un módulo separado en el diseño. La figura anterior muestra dos módulos. Los switches IDF de la capa de acceso usa fordwarding capa 2 para proveer gran cantidad de ancho de banda cost-effective. Los switches MDF de la capa de distríbución provee control en la capa 3 que es requerido en todas redes grandes. Estos módulos IDF/MDF se conectan luego a través de una variedad de cores capa 3 o capa 2.

En general el modelo multicapa es recomendado para diseño campus enterprice por muchas razones.

Primero, el uso de routers provee adecuado control de capa 3, En resumen, este permite que todos los beneficios de la ventaja de enrutamiento accrue a tu red.

Segundo, como su nembre sugiere, el modelo multicapas ofrece jerarquia. En las redes jerárquicas, las capas con role específico son definidos para permitir diseños grandes y consistente.

Tercero, este aproach es muy modular. Hay muchos beneficios para un diseño modular, incluyendo lo siguiente:

- Es fácil de crecer en la red.
- El ancho de banda disponible total escala como módulos adicionales son adicionados.

- Las redes modulares son mas fáciles de entender, diagnosticar y mantener.
- Las redes pueden usar configuraciones cookie cutter . Esta consistencia ahorra dolores de cabeza administrativos mientras también reduce los cambios de errores de configuración.
- Es mas fácil migrar a una red modular.
- Las redes modulares permiten patrones dee tráfico´ consistente y deeterminístico.
- Los diseños modulares promueve balanceo de carga y redundancia.
- Es mucho mas fácil proveer rápido failover en un diseño modular y consistente que en diseños menos estructurados. Debido a que la topología es constrained y bien definido, hay una convergencia de capa 2 y capa 3.
- Las redes modulares permiten que las tecnologías sean fácilmente sustituidas por otro. Haciendo esto no únicamente permite a las organizaciones mas libertad en el diseño inicial, esto hace mas fácil actualizar la red en el long run.

7.3.- CONSIDERACIONES PARA EL DISEÑO CAMPUS-LAN

7.3.1.- LAN Virtuales (VLAN´s)

La popularidad de los campus-wide VLAN es debido en gran parte a los beneficios bien publicitados para este aproach. Primero, este puede permitir rutas directas de capa 2 entre todos los dispositivos ubicados en la misma coimunidad de interés. Haciendo esto, podeemos remover

routers desde el la ruta de alto volumen de tráfico tal como el que va a un servidor de archivos departamental. Asumiendo que router basados en software estan en uso, hay potencial para incrementar el ancho de banda disponible.

Segundo, el campus-wide VLAn hace posible el uso de tecnologías como el User Registration Tool (URT) de Cisco por funcionando como una extensión sofisticada al VLAN membership policy server (VMPS). El URT permite que las VLAN placement a ser transparentemente determinado por servidores de autentificación tales como Windows NT Domain Controller y NetWare Directory Services (NDS). Las organizaciones como Universidades han encontrado este características muy appealing poor que ellos puededn crear uno o mas VLAN para profesores y el staff administrativo mientras se crea separados VLAN para estudientes. Consecuentemente, la misma infraestructura de campus físicos puedee ser usado para lógicamente segregar el tráfico dee los estudiantes mientras aún se permite el uso de roving laptops users.

El tercer beneficio de campus-widee VLAn es actualmente implicado por el segundo beneficio, el campus-wide VLAn permite que estos roving users a ser controlados por un conjunto centralizazdo de listas de accesos. Por ejemplo la Universidad usando un campus-wide VLAN podría usar un par dee routers 7500 ubicado en el datacenter para todos los enrutamientos Inter.-VLAN. Como resultado, la lista de acceso entre las

VLAn únicamente necesitan ser configurados en dos lugares. Considere una altrernativa donde los routers (o switches capa 3) podrían ser desarrollado encada edificio en el campus. Para mantener la movilidad de los usuarios, cada unoi de estos routers necesita ser configurado con todas las VLAN y listas de acceso usado a través del campus entero. Esto podría guiar obviamente a una situación donde potencialmente cientos de listas de acceso tendrían que se rmantenidas.

DHCP Para Resolver Problemas de Movilidad del Usuario.- Muchos Ingenieros de redes sienten que un campus-wide VLAN son la única manera ded manipular usuarios móviles y unwittingly saddle themselves con un red plana que requiere alto mantenimiento. Muchos problemas de movilidad de usuario puede ser resuelto con DHCP, Por que DHCP fija bien dentro de un diseño jerárquico que utiliza procecsamiento de capa 3 para escalabilidad, este puede ser una elección muhco mas safer que usar campus-wide VLAN. El uso de DHCP simplemente requier de uno o mas sentencias ip helper address en cada interface del router (o switch de capa 3). Cuando usamos IP helper address para DHCP, considere el uso del comando no ip forward-protocol para deshabilitar el envío de tipos de tráfico no requerido que son habilitados por defecto.

Numeración de VLAN´s.- Aunque la numeración de VLANs es un task muy simple, teniendo un buen plan thought-out puede ayudar a ahcer mas fácil

entender y administrar la red en el long run. En general hay dos aproach para numerar las VLAN:

- Numeración por VLAN globally-unique
- Numeración por VLAN Pattern-based

En la numeración VLAN globally-unique, cada VLAN tiene un único identificador numérico. Por ejemplo, considere la red mostrada en la figura 7-11. Aquí, las VLANs en el edificio 1 usa números del 10 al 13, el edificio 2 usa del 20 al 23, y el edificio 3 usa de 30 a 33.

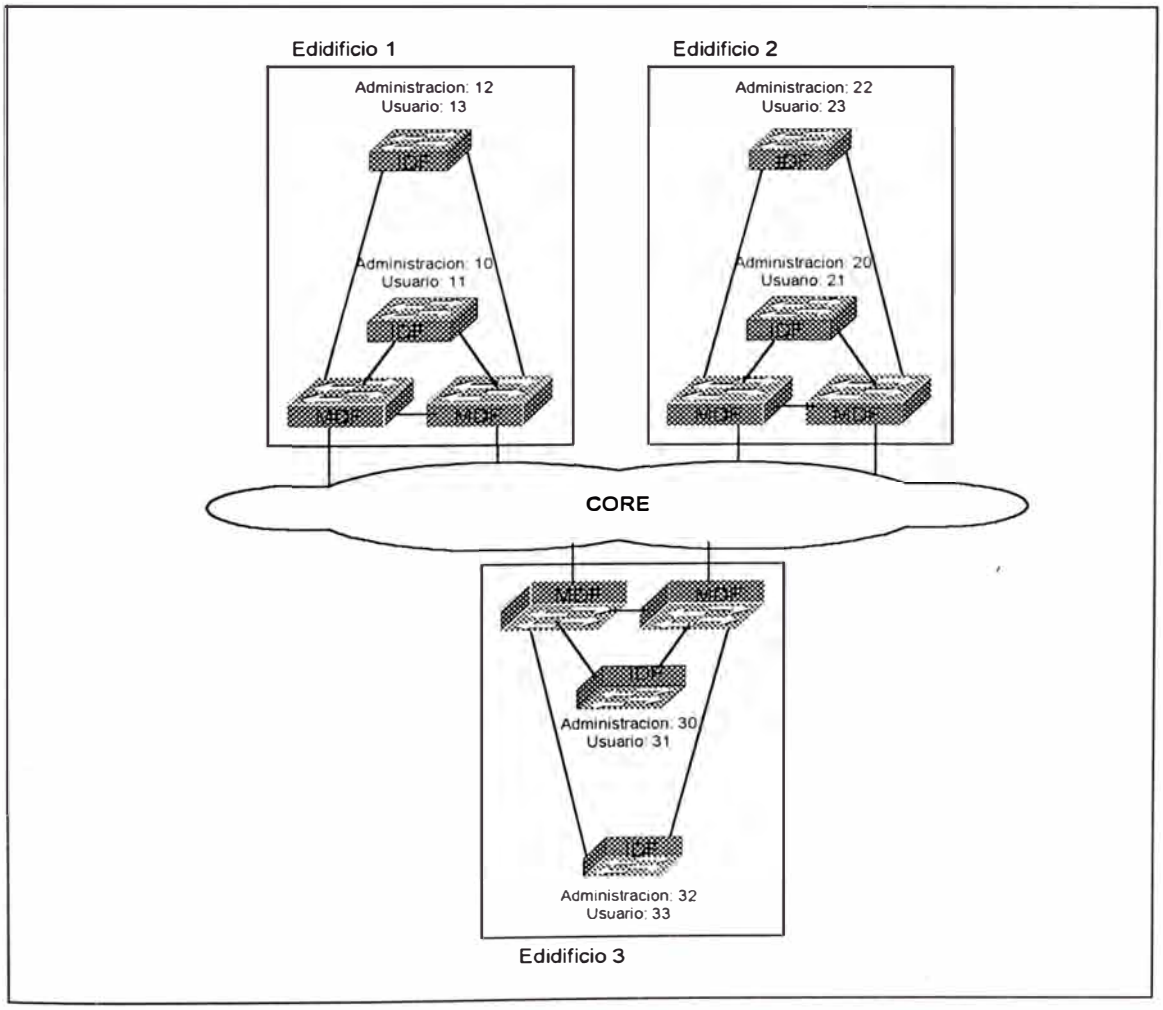


Figura 7-11 VLANs Globalmente únicos

En el caso de numeración VLAN´s pattern-based, el mismo número de VLAN es usado para el mismo propósito en cada edificio. Por ejemplo, en la figura 7-12, muestra uuna red donde el VLAN administrado es siempre 1, el primer VLAN dee usuario final es 2, el segundo VLAN de usuario final es 3, y asi sucesivamente.

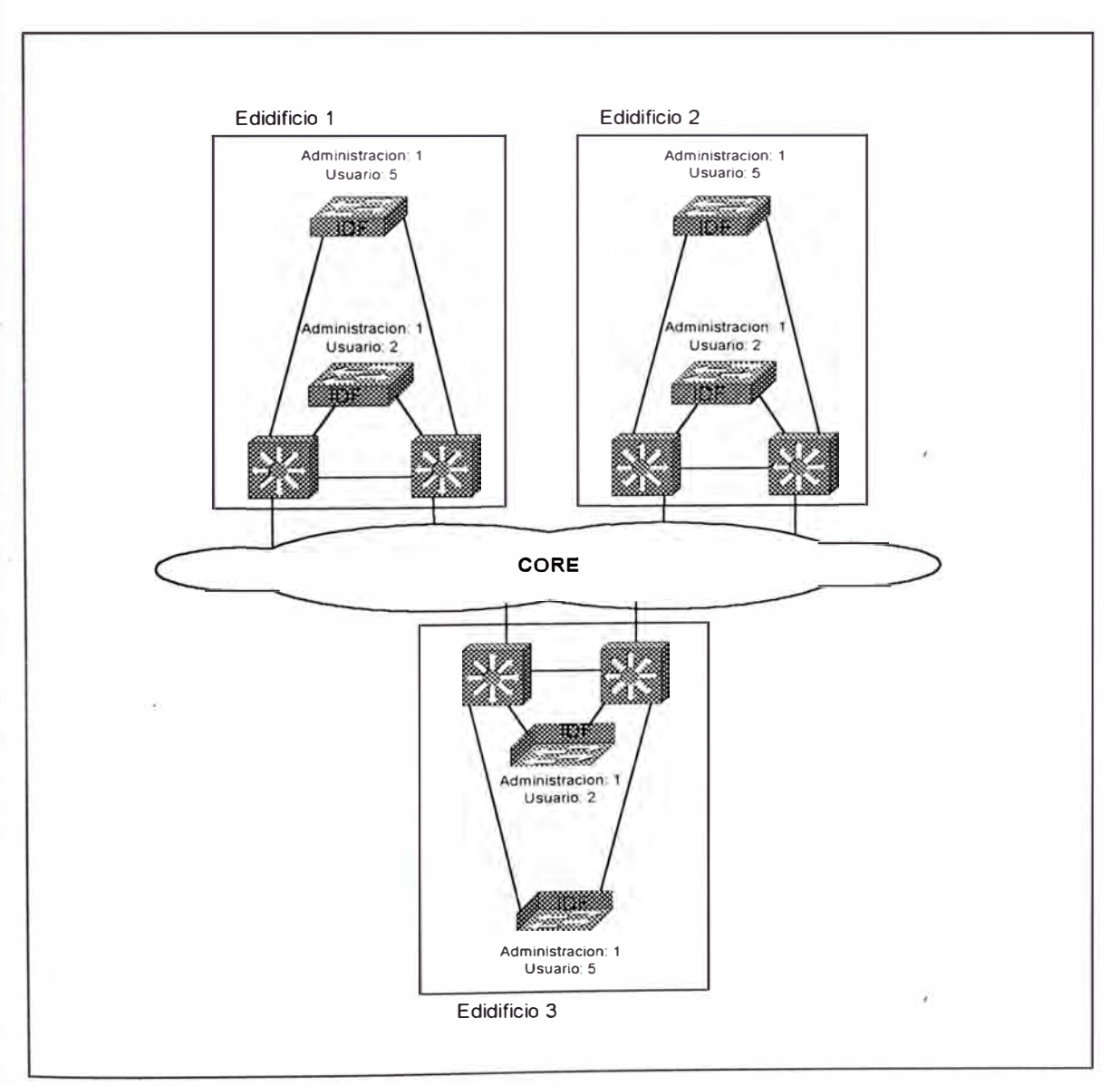


Figura 7-12 VLANs Basado en patrones.

Las propuestas que usaremos es guiado por que tipo de modelo de diseño adoptamos. Si hemos utilizado el modelo campus-wide VLAN, estamos esencialmente forzados a usar numeración globally-unique VLAN. Si estamos usando el modelo multicapas, los dos esquemas de numeración pueden ser adoptados. Debido a que las VLAN son terminados en switches de distribución (MDF´s), no hay requerimientos técnicos mas esenciales del que los números VLAN tienen que corresponder. En realidad, aunque correspondan los números de VLANs, ellos están aún mantenidos como dominios de broadcast separados completamente debido al switching/router de capa 3. Si con la simplicidad de saber que la VLAN administrativa es siempre la VLAN 1, la propuesta "pattern-based" podría ser mas apropiado. Por otro lado, algunas organizaciones prefieren matener cada número de VLAN único justo como cada dirección IP de subnet (esta propuesta une el número de VLAN con el número de subnet, por ejemplo una VALN 25 podría ser una subnet 10.1.25.0/24). En otros caso, una convinación de dos esquemas de numeración pueden trabajan mejor.

- Usar Nombres de VLAN´s Significativos: Aunque el sentido común indica que las VLAN nombrados, claramente sirve como una forma de documentación, las redes son frecuentemente construidos con nombres de VLAN no usuales. Por la teoría de VLAN recordamos que los nombres de VLAN por defecto de un Catalyst son VLAN0002 para la VLAN 2 y VLAN 0003 para la VLAN 3. En otros casos, las organizaciones especifican un nombre de VLAN como un parámetro

para el comando set vlan, pero los nombres son cryptic o poorly mantenidas.

Es usualmente una lejana mejor elección crear nombres de VLAN que actualmente describe la función de ese dominio de broadcast. Este es especialmente cierto cuando usnamos un campus-wide VLAN y una numeración globally-unique VLAN. La naturaleza dinámica y no jerarquica de estas redes hacen que el troubleshooting challenging enough sin tener que gastar tiempo intentando determinar que VLAn envuelve un problema. Teniendo los nombres de VLAn claramente definidos y descritos puede ahorrar tiempo crítico durante un network outage (como tambien evitar la confusión que podría causar un administrador para misconfigure un dispositivo y así crear un network outage).

Aunque los nombre de VLAN son menos importante cuando un modelo dee diseño multcapa esta en uso, los nombres debería al menos diferenciar tráfico de administración y de usuario final. Intentar incluir el nombre del departamento o los closet de la capa de acceso (IDF), donde la VLAN es usado. También algunas organizaciones incluyen el númerode subnet IP en el nombre de la VLAN.

- Usar VLAN´s Administrados Separadamente: Cuando exponemos los VLAN, muchos administradores de red encuentran a estos mucha

confusión, y además deciden adoptar una política de ubicar únicamente una sola VLAN en cada switch. Aunque este tenga una simplicidad muy atractiva, puede seriamente desestabilizar tu red. En resumen tenemos que siempre usar al menos dos VLANs en cada catalyst switch de capa 2. En una configuración mínima tenemos una VLAN para tráfico de administración y una VLAN separada para tráfico de usuario final.

Sin embargo, el tener mas de dos VLAN no es buena idea. Por el contrario, la simplicidad de mantener una única VLAN para usuarios finales (o al menos un número pequeño) puede ser muy benéfico para el mantenimiento de red.

Debido a que el broadcast no son filtrados por el hardware de la tarjeta de interface de red on-board (NIC), cada broadcast es pasado hasta la capa 3 usando un interrupt al CPU. Cuanto mayor parte del tiempo el CPU gasta observando un paquete broadcast no querido, menos tiempo tiene para su tareas usuales.

Los CPUs de los switches catalyst no son diferentes, el CPU tiene que inspeccionar cada paquete broadcast para determinar si un ARP es destinado a su dirección IP ó algún otro paquete broadcast de interés. Sin embargo, si el nivel de tráfico no interesante viene a ser muy alto, ningún daño es causado. Por otro lado, si este

descartas paquetes STP BPDUs, la red entera prodría desestabilizarse.

En realidad, el problema STP es uno de los más comunes en redes "campus" planos. La red está trabajando bien hasta que un "data burst" o "broadcast" en la VLAN administrada causa que el switch se sobrecarge al punto donde este comienza a descartar paquetes. Debido a que algunos de estos paquetes son BPDUs, el switch cae detrás de su información STP e inadvertidamente crea un lazo de capa 2 en la red. En este punto, el "broadcast" en la red va dentro de un completo "feedback loop" .

Si este lazo ocurre en uno o mas VLANs diferentes a la VLAN administrativa, este puede rápidamente abarcar todos los anchos de bandas sobrantes de los "trunks" a través del "campus" entero en una red plana. Sin embargo, los CPUs supervisores son aislados por el "switching VLAN ASIC´s" y continúan operando normalmente.

Por otro lado, si el lazo ocurre en la VLAN administrativa (la VLAN donde el SCO es asignado), el resultado puede ser verdaderamente catastrófico. De repente, cada CPU del switch es golpeada con una oleada de tráfico "broadcast", colisionando completamente con cada switch como un espiral hacia abajo, que virtualmente elimina cualquier cambio de la red, por recobrarse de su

problema. Si una red está utilizando un VLAN campus-wide, este problema puede expandirse por cada switch dentro de unos segundos.

- Decidiendo la Numeración a ser usada para la VLAN de Administración: Una pregunta común del tema de numeración de VLANs es el referente a la VLAN de administración. Para que apropiadamente respondamos a esta pregunta, debemos considerar tres tipos de tráfico que pasan a través de los switches:
    1. Tráfico de control
    2. Tráfico de administración
    3. Tráfico de usuario final

El tráfico de control abarca los protocolos orientados plug and play, tales como DISL/DTP (usado para negociación de estado de trunks), CDP, PagP, y VTP. Estos protocolos siempre usan la VLAN1.

El tráfico de administración incluye protocolos basados en IP y end-to-end, tales como Telnet, SNMP, y VQP (protocolo usado por VMPS). Estos protocolos siempre usan la VLAN asignada para SCO.

El tráfico de usario final es todo el tráfico remanente de tu red. Obviamente, este representa la mayoria de tráfico en la mayoría de redes.

El principio overriding en diseño de VLAN ded administración es nunca mezclar tráfico de usuario final con tráfico de administración y control.

Cuando implementamos este principio, tenemos generalmente que elegir uno de los dos diseños:

1. Usar VLAN 1 para todo tráfico ded administrácion y control mientras ubicamos el tráfico de los usuarios finales en cualquier otra VLAN (del 2 al 1000)
2. Usa VLAN 1 para tráfico de control, otra VLAn (tal como VLAN 2) para tráfico de administración y lo que queda para tráfico de usuario final (tal como VLAN 3 al 1000).

La primera opción combina tráfico de administración y de control en la VLAN 1. La ventaja de esto es la simplicidad ded administración (la configuración por defecto y usa una única VLAN). La primera dedsventaja de esto se centra alrededor del comportamiento por defecto de la VLAN 1, debido a que la VLAN 1 no puede ser actualmente ser removida de lso enlaces trunk, es fácil para esta VLAN llegar a ser extremadamente grande. Por ejemplo, el uso dee enlaces trunk ethernet a través de una red along con MLS switching capa 3 en la capa dee distribución (MDF) resultaría en una VLAN 1 spanning cada enlace y cada switch en el campus, exactamente lo que no quieres para tu VLAN dee administración importante.

Adedmás, ubicar SCO en una VLAN tan grande como plano puede ser riesgoso.

Este riesgo puede ser evitado con una segunda opción donde el tráfico de control y administración son separados. Si el tráfico de control tiene que usar la VLAN 1, el tráfico de administración es ubicado en una VLAN diferente (muchas organizaciones usan la VALN 2, 999, o 1000). Como resultado SCOP y el CPU sería aislado de problemas dee broadcast potenciales en la VLAN 1, Esta optimización puede ser particularmente importante en redes campus extremadamente grandes que estan lacking en la jerarquia ed capa 3.

- Cuidados Cuando se Mueva VLAN SCO´s: Aunque algunos tráficos siempre usan VLAN 1, otros traficos de administración cambian VLANs como SCO es reasignado. Este incluye todos los protocolos end-to-end (opuestos a los protocolos linkby-link que únicamente usan VLAN 1) tales como:

  1.- Telnet

  2.· SNMP

  3.· El VQP protocolo usado por VMPS

  4.· Sylog

  5.· Ping

Para que estos protocolos funcionen SCO tiene que ser asignado a la VLAN correcta con un dirección IP válida y uno o mas gateway por defecto funcionando para alcanzazr el resto de la red. El problema mas común aquí es que loas personas algunas veces mueven el SCO a una VLAN diferente para ́propósitos de troubleshooting y olvidar mover de regreso cuando ellos están hechos. Aunque esto puede ayudar a diagnosticar el problema de einmediato, es casi siempre garantizado para crear mas problemas. Otro problema común es caer en el uso de dirección IP que es apropiado para la VLAN asignado a SCO.

Si reconfiguramos SCO para propósitos de troubleshooting, asegúrate ded regresar esto a su estado original.

- Prune VLAN desde Troncales: Dos tecnologías estan disponibles para crear trunks que comparten múltiples VLANs:

1. Tagging Implícito
2. Tagging Explícito

Cuando usamos tagging implítio, alguna información ya contenida en la trama sirve como un indicador ded VLAN membership. Muchos vendedores han creado equipos que usan direcciones MAC para este propósitos (otros incluyen direcciones ded capa 3, o númerod e puertos de capa4). La desvaentaja es que

tenemos que devise algunas técnicas para compartir algunos de estos tag. Por ejemplo, cundo usamos direcciones MAC, todos los equipos tiene que ser told para que VLAN le ha sido asignado cada dirección MAC. Mantener y sincrinizar esto potencialmente huge las tablas puede ser un problema.

Para evitar estos issues de sincronizazción, cisco ha desarrollado el uso de tagging explícito a través de ISL y 802.1Q. Hay dos ventajas para el tagging explícito: El primero, los membership vienen a ser completamente ambiguos. Segundo, cada switch necesita conocer únicamente el asignamientode VLAN de su puerto directamente conectado (en tagging implícito, las tablas compartidas requieren que cada switch mantenga conocimiento dee cada direcciónMAC de la estación final). Como resultado , la cantidad de información de estado requerido por cada switch es dramáticamente reducida.

Sin embargo hay un hidden downside a la ventaja de cada switch no necesitan saber que las VLAN de otros switches que esten usando tráfico flooded tiene que ser enviados a cada switch en la red de capa 2. En otras palabras, por defecto, una copia de cada broadcast, multicast, y tráfico unicast no conocido es flooded a través de cada enlace trunk en elk dominio de capa 2.

Dos propuestas pueden ser usados para reducir el impacto de este tráfico "flooding". Primero, notar que si estamos usando campus-wide VLAN, este "flooding" tambien viene a ser un problema "campus-wide." Además una de la mas simples y escalables maneras de reducir este flooding es la partición de la red con muchas barreras de capa 3 que utilizan tecnología de enrutamiento (switching capa 3). Esto quiebra la red en pequeñas zonas de capa 2 y limita el flooding en cada zona. Donde los switches de capa 3 no pueden prevenir el flooding innecesario (tales como campus-wide VLAN o dentro de una zona capa 2 creado por switching capa 3), una segunda técnica de VLAN prunning puede ser empleado. Las VLAN no usados pueden ser manualmente "pruned" desde un trunk. Además, cuando un swirtch dado necesita flood una trama, este únicamente lo envía fuera de los puertos de acceso localmente asignados a la fuente VLAN y a los enlaces trunk que no han sido pruned para esta VLAN. Por ejemplo, un switch MDF puede ser configurado para que únicamente "flood" tramas de la VLAN 1 y 2 a un switch IDF dado, si el switch únicamente participa en estos dos VLAN. Para automatizar el proceso de prunning, VTP pruning debe ser usado.

VLAN prunnig en líneas trunk es una de los mas importantes claves para la implementación satisfactoria de una red conteniendo un swtich catalyst de capa 2.

- Haciendo los "Cores" de Capa 2 Libres de Lazo: Cuando usamos un "core" capa 2 asociado a un modelo multicapa, nos esforzamos por eliminar enlaces que crean lazos. Por otro lado, este método suena completamente como un contador intuitivo. Después de todo, la mayoría de los ingenieros de red pasan incontables horas intentando mejorar la resistencia del "core" de la red. Sin embargo, cuidadosamente deshabilitando la red de ciertos enlaces y VLANs, puedes eliminar los retardos de convergencia de "Spanning Tree" mientras aún mantienes un alto grado de redundancia y resistencia. En otras palabras, simplemente ingresando más enlaces y VLANs en un "core" de capa 2 puede eventualmente degradar la confiabilidad de la red debido a la introducción de retardos de Spanning Tree.

Además, hay otra desventaja de usar "cores" de capa 2 libres de lazo. Cuando existe un lazo, "Spanning Tree" automáticamente ubica los puertos en estado "blocking" y además reduce la capacidad para balancear carga a través del "core". Eliminando los lazos y retirando los puertos en estado "blocking" de "Spanning Tree", cada ruta a través del "core" puede ser utilizado para maximizar el ancho de banda disponible en esta área importante de la red.

Por ejemplo considere el "backbone" colapsado de capa 2 ilustrado en la figura 7-13.

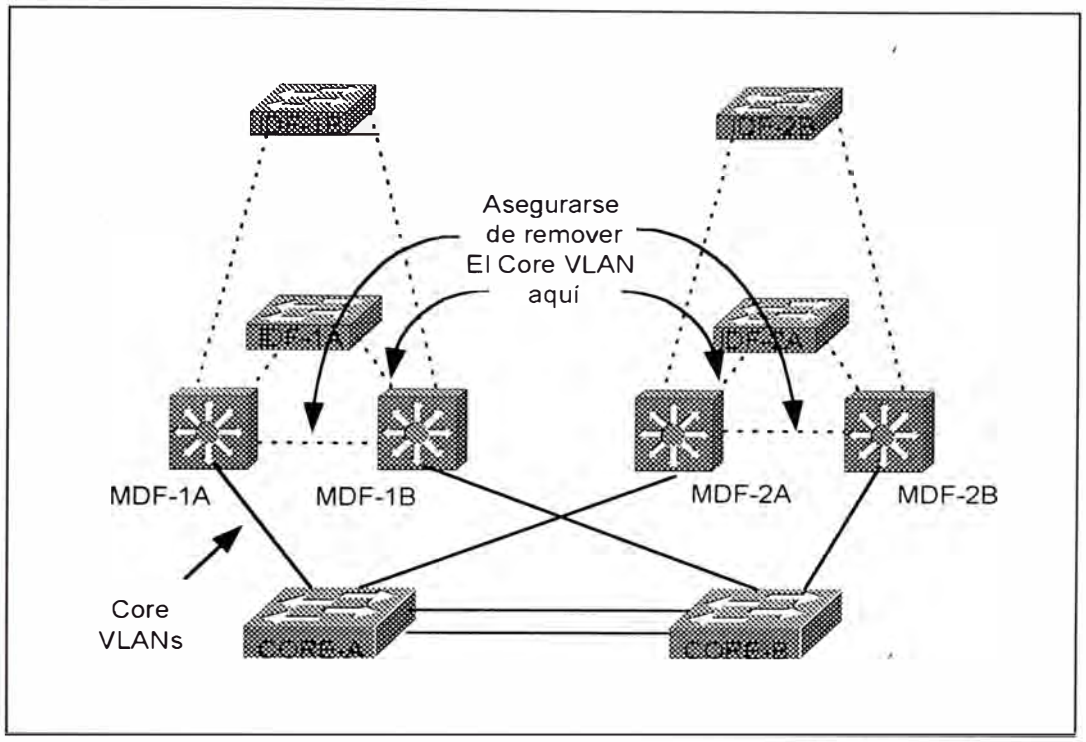


Figura 7-13 Un Core de capa 2 Colapsado libre de Loop.

El core esta formado por un par de switches de capa 2 redundantes, cada uno llevando un único VLAN. Los cuatro switches MDF se conectan a uno de los switches core (coreA y core B), permitiendo que cualquier enlace o switch falle sin causar un permanente outage. Si los cuatro switches MDFs son configurados con catalyst 8540 stilo switching routers, entonces estos automáticamente resulta en un core libre de loop. Por otro lado, el uso ded routers switching de capa 3 (MLS) en dispositivos MDF requiere un planeamiento mas cuidadoso. Especialmente, el core VLAN tierne que ser removido de los enlaces a los switches IDFs como también a los enlaces entre los switches MDF.

Cuando mas grande el core de capa 2 requier un planeamiento mas detallado. Por ejemplo, en la figura 7-14, muestra una red que cubre una gran área geográfica y además usa cuatro switches capa 2 dentro del core. El diseño es algunas veces referido a un core ded capa 2 split.

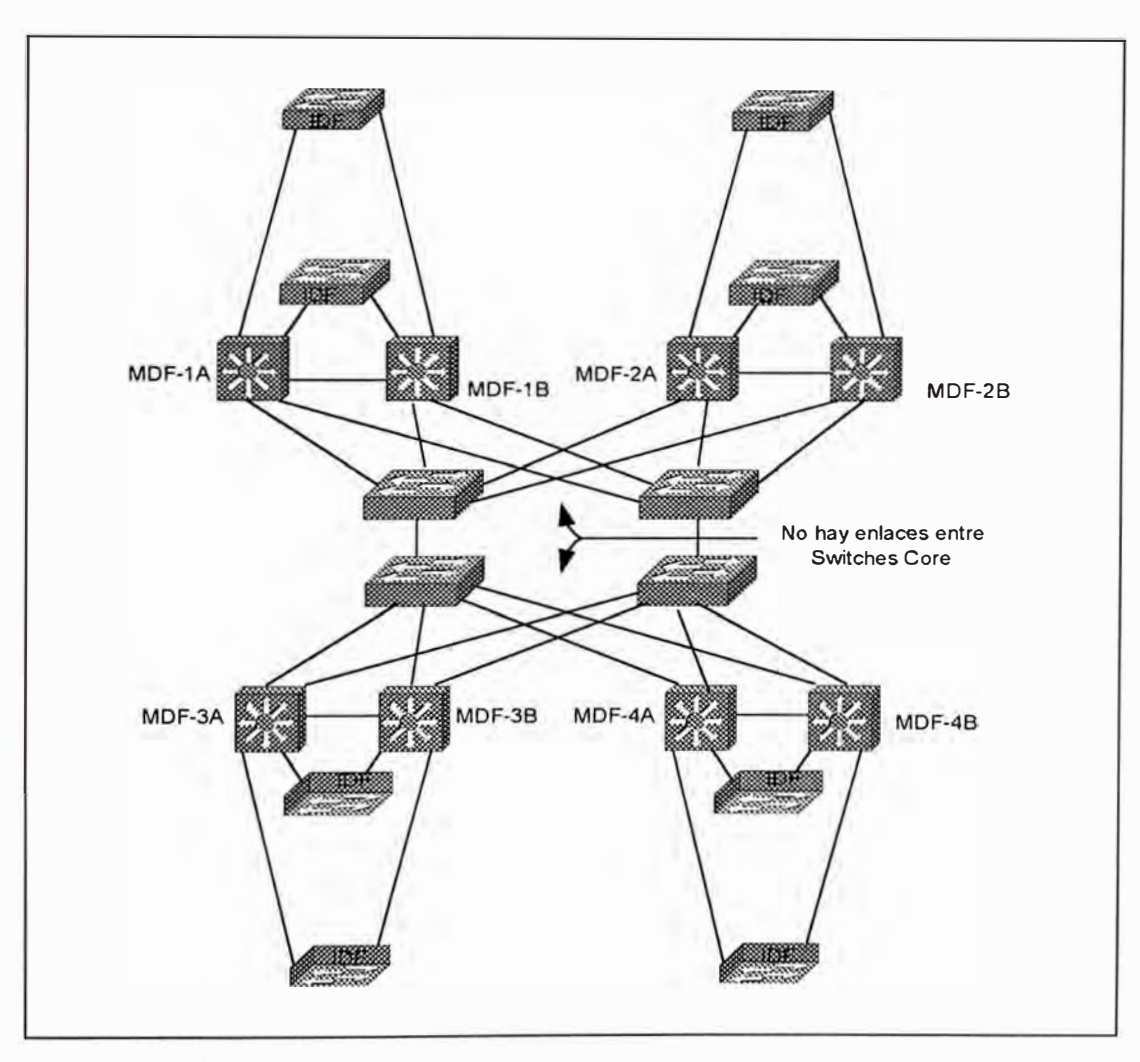


Figura 7-14 Un Core split de capa 2.

En este caso la clave para crear un core de rápida convergencia y resilient es actualmente partir el core dedntro dee dos VLAN separados y no cross-link los switches a cada otro. El primer VLAN core es usado para el par de switches a la iaquierda, y el segundo

VLAN es usado para el par de switches a la derecha. Si los switches "core" en la figura fueron "cross-enlazados" ó completamente conectados, y una única VLAN fue desarrollada, la convergencia "Spanning Tree" y el balanceo de carga debería ser un problema.

Finalmente, notar que crear un "core" libre de lazos requiere el uso de "switching de capa 3" en los "closet MDF" de distribución. Cuando usamos el modelo "VLAN campus-wide", la única manera de lograr un "core" libre de lazos es remover todos los lazos de la red entera, obviamente es un esfuerzo arriesgado si se está preocupado en la redundancia de la red. Finalmente, sigue las sugerencias e intenta usar un modelo "multicapa" y los beneficios de escalabilidad que alcanza el "switching capa 3".

- No Olvides Planificar: Cuando creamos un nuevo diseño o cuando uno o dos intentos de resolver un problema particular falla, rediseña la VLAN usando LANs físicos (PLANs). En otras palabras, toma la topología lógica creada a través del uso de LANs virtuales y rediséñalo usando LAN físicos (PLANs).

PLAN es un término que se inventó para describir un tema muy serio. Por algun motivo, la cabeza de las personas se olvidan del conocimiento de IP subnetting cuando se enfrentan con VLANs. Las personas pasan días observando las trazas del "snnifer" de una cosa

compleja como el trunk ISL y Spanning Tree para únicamente aprender al final que alguien digitó mal una dirección IP.

Para explicar el concepto de PLAN, observemos la figura 7-15, que nos muestra una típica red usando VLANs.

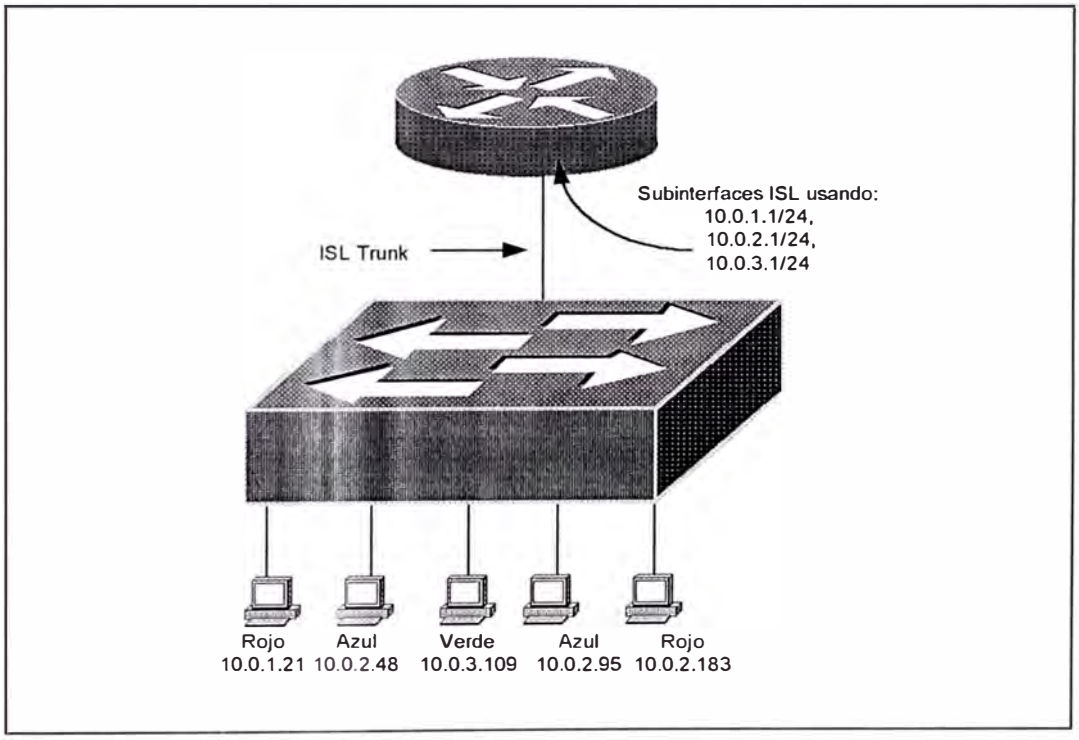


Figura 7-15 LANs virtuales (VLANs).

Cada VLAN en la figura anterior fue redibujado en la figura 7-16 como segmentos conectados a una interface diferente del router. Estos retrata la separación de VLAN con la separación física usado en un tradicional diseño con routers y hubs. Sin embargo, desde una perspectiva de capa 3, ambas redes son idénticas.

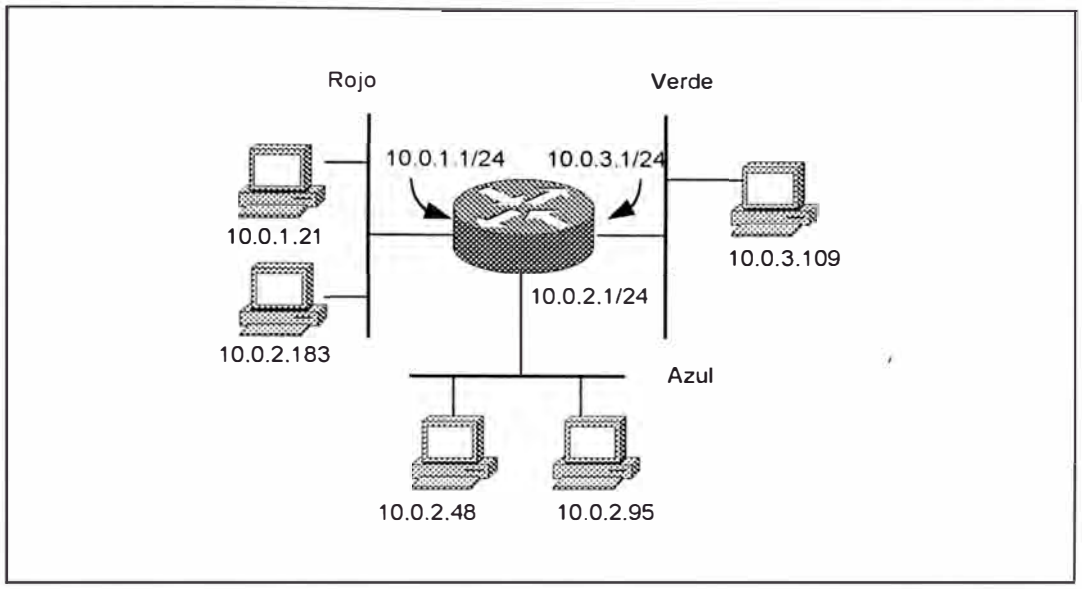


Figura 7-16 LANs Físicos (PVLANs).

Haciendo esto hace que la red sea extremadament efácil de entender. En realidad hace menos doloroso el unicar un problema. El host 10.0.2.183 dee la figura esta ubicado en un segmento errado (debería estar en la VLAN azul)

7.3.2.- Spanning - Tree

El inapropiado uso de VLAN es lo que guia a problemas de Spanning Tren en primer lugar. Uno de los primeros temas desarrollados es que aunque Spanning Tree puede ser tranquilamente manejable cuando se usa en conjunto con switching capa 3, este puede llegar a ser complejo cuando son usados en grandes diseños planos con un como campus-wide VLAN.

Mantener Pequeños Dominios de Spanning-Tree.- Uno de las técnicas mas efectivas para minimizar los problemas de Spanning Tree es mantener dominios de tamaño pequeños . La manera mas fácil de hacer esto es usar el modelo de diseño multicapas. Hay muchos beneficios para constricting Spanning Tree a pequeños pocket dentro de tu red, incluyendo lo siguiente:

- Permite cuidadosamente sintonizar los timers de Spanning Tree.
- Como resultado, la convergencia Spanning Tree puede ser mejorado significativamente.
- Viene a ser muy difícil para los problemas de Spanning Tree en una sección de la red spread a otra sección de la red.
- Cuando se usa switching routers desde un diseño multicapas, el balanceo ded carga Spanning Tree puede ser eliminado. En este caso el tráfcio IDF crea Capa 2 V¨s que son inherentemente libre de loops y además no requier el protocolo Spanning Tree, aunque se recomienda que no se desabilite Spanning Tree.
- Cuando usamos routing switching (MLS) dede un modelo de diseño multicapas. El balanceo ded carga Spanning Tree puede ser dramáticamente simplificado a través del uso de la técina de ubicación del Root bridge. Cuando usamos MLS y el modemlo multicapa, cada IDF y un par de MDFs crea un triángulo capa 2 que, aunque no esta libre de loop, son fácil ded administrar.
- Spanning Tree viene a ser mucho mas simple de diseñar, documentar y entender
- El troubleshooting es mucho mas fácil.

La figura 7-17, ilustra el triángulo de capa 2 creado por MLS (part A) y el Capa 2 V´s creado por los switching-routers. Aunque MLS usa módulos route-switch (RSM), una representación lógica ha sido usada para la parte A.

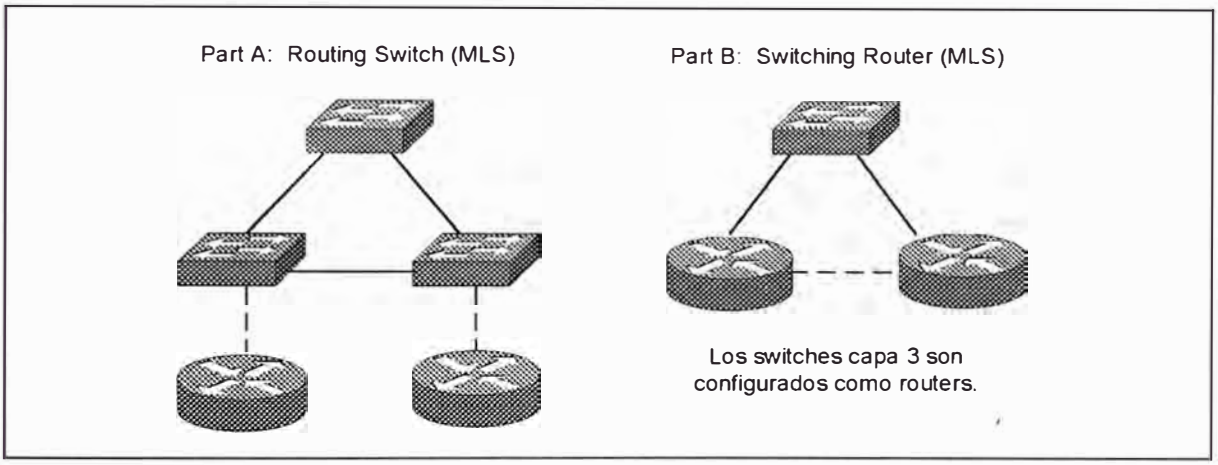


Figura 7-17 Topologías capa 2 bajo Routing swtches (MLS) y Switching routers.

Cuando usamos campus-wide VLAN, es algunas veces posible alcanzaar algunos de los beneficios listados por manualmente prunning VLAn dedsde los trunk seleccionados. Sin embargo, no es posible crear la simplicidad y escalabilidad que son disponibles cuando usamos switching capa 3. También la acción prunning puede algunas veces reducir la redundancia en la red.

El modelo milticapas permite los beneficios listados para ser fácilmente diseñados dentro una red. Cuando usamos routing-switches (MLS)como mostrado en la parte A, este puede ser acomplished por

prunning VLAN seleccionados desde los enlaces trunks (como los enlaces en el core y entre los switches MDFs). Cuando usamos switching-routers como el 8540 como mostrado en la partte B, los benéficos de tener pequeños dominios Spanning Tree accrue por defecto.

No Deshabilitar Spanning-Tree.- En frustación muchas organizaciones desabilitan Spanning Tree protocol para alcanzar la estabilidad de la red (especialmente cuando usamos diseños planos). Sin embargo, cuando estos es hecho en expense de redundancia, esto obviamente introduce un nuevo conjunto de problemas.

Cuando Spanning Tree es deshabilitado, no estamos protegidos ded las configuraciones erradas que crea los loops de capa 2 en la red. Típicamente Spanning Tree es deshabilitado en uno de las tres situaciones:

- Como último recurso para alcanzar la estabilidad de la red bajo el modelo de diseño campus-wide VLANs. Sin embargo, estos también requiere que la redundancia también sea eliminado, esto no es recomendado.
- Cuando usando el switching-router catalyst 8540 en los cosets MDF/distribución. Spanning Tree no es requerido por que los switching-reouter resulatra en una capa 2 V´s libre de loop (como mostrado enla parte B del la figura 7-17). Sin embárgo, los loops pueden ser formados nointencionalmente a través de errores de configuración y cableado en la parte de administrador dee red o

debido a los equipos insatalados de usuarios finales como hubs o switches. Además, un elemento de riesgo se mantiene con este aproach.

- Cuando usamos un backbone LANE. Debido a que automáticamente se crea una topologíua libre de loop dentro de core ATM por si solo, el Spanning Tree puedee ser deshabilitado. En realidad, los vendedores de ATM-centric deshabilitan Spanning Tree para LANE por defecto, sin embargo hay que tener cuidado de no crear loops de capa 2 fuera del backbone LANE.

En general es mejor usar técnicas de diseño escalables y Spanning Tree tunning mejor que deshabilitarlo. Los diseños tales como el modelo milticapa puede alcanzar la estabilidad de la red sin tener resort para deshabilitar Spanning Tree. También, un cuidadoso diseño planeado puede permitir que Spanning Tree sea tunned para una mejor performance.

Evalúa Patrones de Spanning-Tree.- El uso de switching capa 3 y el modeelo de diseño multicapas generalmente resulta en redes que son somprised de muchos triángulos pequeños y "V´s" de conectividad de capa 2

Desde una perspectiva de Spanning Tree, es importante notar que los V´s esten libres dee loops y además no ubicar cualquier puerto en el estado blocking. Como resultado Spanning Tree no impactaría en la performance failover.

A diferemncia del 8540, MLLS nos permiten fácil configurar los triángulos o V´s por defecto, MLS permite que todas las VLAN transitan el switch. Además asume que se ha removido las VLAN dede los usuarios finales de la red core, estaríamos a la izquierda de los triángulos de capa 2 por defecto (Parte A de la figura 7-17). Sin embargo, por prunning una VLAN dad desde el enlace entre los switches MDF/distribución esta VLAN puede fácilmente ser convertidad dentro de una V (parte B de la figura 7-17). En otras palabras, por simplemente prunning la VLAN desde la base del triángulo, esto es convertido dentro ded una "V".

Desde la perspectiva de Spanning Tree, es importante evaluar las diferencias que trae a la red. Si optam,os por usar triángulos, luego Spanning Tree estaría en full efecto. El Root bridge ubica la forma de balanceo de carga y carcterísticas como UplinkFast sería importante. Si optamos por V´s de capa 2, estaríamos a la izquierda con la mismo situación "almost Spanning Tree free" .

Considere Uso de Swtching-Routers Para Virtualmente Eliminar Spanning-Tree .- Debido a que el switching-router catalyst 8540 en los closet MDF/capa de distribución elimina los loops a través de los switch IDF, este resulta en V´s ded capa 2. Además, Spanning Tree puede ser mucho mas simple de diseñar, matener, y diafnosticar. Ekl switch IDF automáticamente se elige por si solo como el root bridge de una red one-bridge /los switches capa 3 previenen que los bridge aprendan acerca de los otros y mantienen el

Spanning Tree separado). Los valores del timer puede ser fairly agresivamente tunned sin riesgo. También el balanceo de carga Spanning Tree no es grandmente necesario.

Notar que los V´s de capa 2 pueden ser creados sin plataformas routing-switch (MLS) por prunning VLAN desde enlaces seleccionados(en este caso la base de los triángulos seleccionados- el enlace MDF a IDF).

Considere Usar Administración de VLAN Libres de Loop.- Asegurar que el diseño de red minimize el riesgo de ocurrencia de broadcast storm en la VLAN de administración. Además, asegurar que la VLAN de administración que por si misma es libre de loop puede proveer una capa adicional de protección. En general, dos técnicas pueden ser usados para crear una VLAN de admnistración libre de loop:

- El uso de Catalyst 8540-stilo switching router en el MDF/capa dee distribución automáticamente crea VLAN de administración libre de loop en el IDF/dispositivos de acceso por defecto. Notar que esto también implica que deberías usar IRB para merge la VLAN dee administración dedntro de una simple VLAN. Aunque esto pueda aparecer para simplificar la administración de la red mediante la ubicación de todos los switches en un simple VLAN, este puede crear problemas de administración en gran término por la adición de loop dentro de la VLAN administrada.

- El campus-wide VLAN algunas veces reequiere el uso de una red de administración fuera dee banda. Por que es muy difícil mantener un loop libre y un ambiente estable cuando el campus-wide VLAN esta en uso, tu algunas veces tienes que resort para correer enlaces Ethernet separados desde los routers a los puertos en cada Catalyst. Luego únicamente asignando este puerto ethernet a la VLAN de administración usado por SCO, una topología lógica libre de loop puede ser creado. Los puertos ME1 (Management Ethernet 1) disponibles en algunos dispositivos ctalyst pueden también ser usados para crear una red de administración fuera de banda.

La figura 7-18, muestra una red típica usando un aproach fuera de banda para crear VLAN de administración liibre de loop. Asumir que por que los switches son desarrollados ded una manera haphazard, no es factible crear VLAN ded administración libres de loop usando la infraestructura existente. En vez dee eso, los enlaces ethernet separados son pulled desde el puerto del router mas cercano disponible. Donde sea posible, los hubs pueden ser usados para reducir el número ded puertos routers requeridos.

Hay que mantener un ojo en la VLAN 1. Aunque pudimos haber usado cuidadosamente los switches capa 3 para crear jerarquía en la red, podemos estar aun en la izquierda con un campus-wide VLAN en la VLAN 1 (especialmente si estamos usando switches de capa 3 MLS).

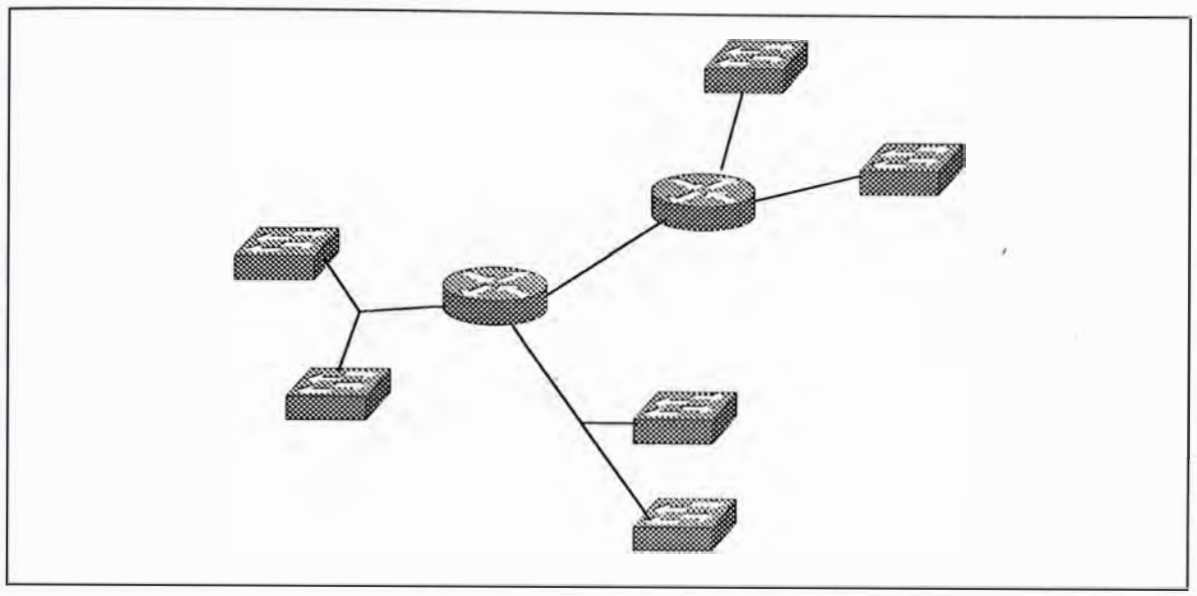


Figura 7-18 Creando Administración de VLANs Loop-free con una Red Out-of-Band.

Notar que esto sería verdad aunque si se hubiese seguido los consejos de prunning VLAN core VLAN desde el trunk del closet dee cableado y las VLANs del closet de cableado desde el core trunk. Debido a que la VLAN 1 es dado como una prioriación especial, por el control de tráfico, un broadcast loop en esta VLAN puede ser devastador para la salud de la red. Para controlar esta situación, las oraganizaciones han usado un o mas de las técnicas siguientes:

- Problablemente la opción mas simple y mas efectiva envuelve el uso de enlaces no-trunk en el core. Asignando cad auno de estos enlaces core a una simple VLAN(no usar VLAN 1 aquí), el core core bloquearía la transmisión de información de VLAN1.
- Usa switches routers tales como el Ctalyst 8540 que no forward VLAN 1 por defecto.

- Una vez que esto es disponible, usa la caraterística upcoming que permitiría a la VLAN 1 ser removido de los enlaces trunk.
- Si estamos usando ATM core, la VLAN 1 puede ser removido desde esta porción de la red.

Siempre Especifica tu Root Bridge.- Anteriormente hemos conversado los problemas que pueden surgir cuando no manualmente especificamos la ubicación del Root Bridge en la red. Es altamente posible que un bridge suboptimo o switch gane la elección del Root. Mejor que dejar que esto cambie, siempre especifica un Root Bridge priemario y secunadrio para cada VLAN. Seleccionando manualmente el Root Bridge, no únicamente podemos optimizar la ruta de datos, pero esto hace a la red mas determinística y mejora su estabilidad, mantenimiento y fácil diagnóstico.

Todos las redes usando grupos de switches capa 2 continuos o bridge transparentes deberían especificar un Root Bridge primario y de respaldo.

intentar Usar el Balanceo de Carga ubicando Root Bridge.- La forma de ubicar el Root Bridge de balanceo de carga Spanning Tree puede ser extremadamente efectivo y fácil de implementar si la topología lo soporta. En la mayoría de redes que utilizan campus-wide VALN y un servidor farm centralizado, es muy dificil obtener cualquier grado de balanceo decarag con esta técnica.

Sin embargo, cuando usamos un modelo multicapa en conjunto con MLS (y otros tipos de routing switches), esta forma de balanceo de carga es altamente recomendado. Debido a que un modelo multicapa y MLS reduce la red a una serie de pequeñas triangulos dee capa 2 que span cada switch y el correspondiente para de switch MDF, la topología de capa 2 es consrained, bien definido y determinístico. Comsecuentemente, es fácil hacer que un switch MDF sea el Root Bridg para aproximadamente la mitad de las VLANs contenidas en ese bloque de distribución, mientras el otro switch es configurado como Root bridge para las VLANs remanentes. (Hay que recordar que un bloque de distribución está compuesta por un par de switches MDF y su colección de switches IDF asociados, tipicamente es contenido dentro de un edificio). Por ejemplo en la figura 7-19, nos muestra un típico bloque de distribución donde el switch MDF-A es el Reoot Bridge para las VLAN odd-numbering y el switch MDF-B es el Root Bridge para las VLAN even-numbering.

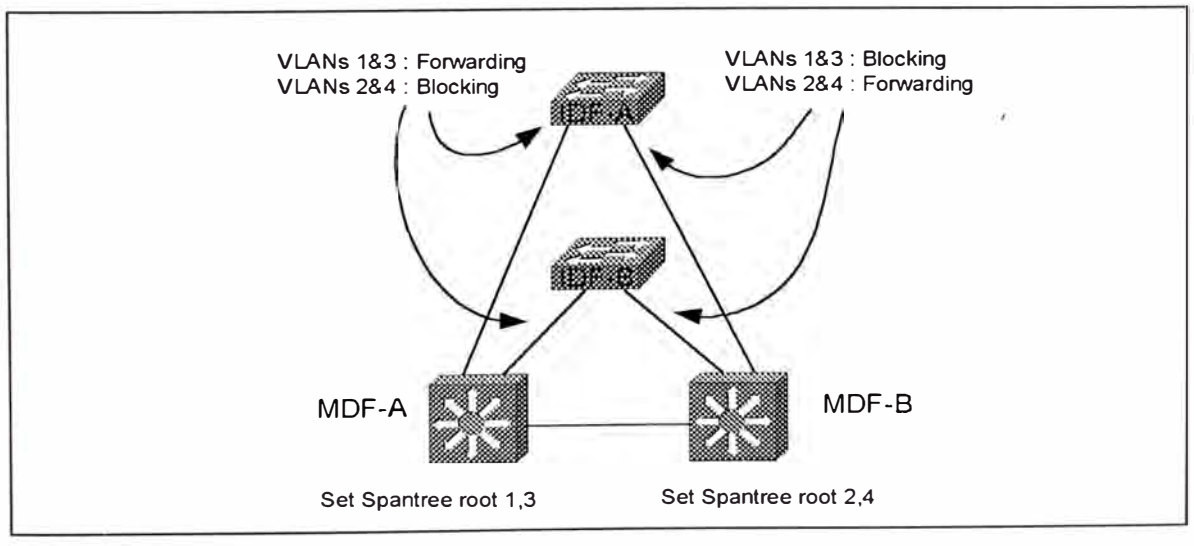


Figura 7-19 Balanceo de carga Spanning Tree con ubicación de Root Birdge.

Esto causa que las VLAN odd usen los enlaces riser de la izquierda (los puertos IDF de la derecha estan en estado blocking para estas VLAN), mientras las VLAN even usan el enlace de la derecha (los puertos IDF de la izquierda están en blocking).

- Consideraciones de Ubicación del Root Bridge: Besides influencing distribución de tráfico a través del balanceo de carga, muchos otros factores deberían ser considerados cuando determinamos donde deberían ser ubicados los Root Bridge. Algunos de las consideraciones mas importantes son mencionados en la lista siguiente:
    1. Ubique el Root Bridge en la ruta del flujo de datos de mas alto ancho de banda
    2. Use un dispositivo que es muy estable, debido a que Spanning Tree es un protocolo que constantemente seeks out el mas atractivo Root Bridge, ubique el Root Bridge en un dispositivo que reboots o falla frecuentemente puede disturb la red entera innecesariamente.
    3. Use un dispositiovo que pueda llevar la carga, debio a que las funiones de un Root Bridge como nodo switching central para todos los branches de Spanning Tree, tiene que ser capaz de manipular la carag agregada altamente potencial.

Cuando implementamos un diseño Spanning Tree, la mayoría delas organizaciones adoptan una o dos estratégias:

1. Root Bridge Distribuidos
2. Root Bridge Centralizados

La ubicaciónd e Root Bridge destribuidos es muy usual en situaciones donde los diseñadores de red quieren spread la carga del switching centralizado sobre mas que un bridge. Debiod al incremento dedl ancho de banda disponible, esta técnica puede también mejorar la estabilidad de la red por no forzando la red entera a depender de uno o dos switches por serivicios de Root Bridge. Sin embargo, los Root Bridge distribuidos pueden significativamente incrementar la complejidad de troubleshooting en la red por creando una topología lógica para cada VLAN.

Los Root Bridge centralizados son muy usuales en situaciones donde el flujo de tráfico son altamente concentrados (tales como en el el caso de un server ferm centralizazdo). Otra ventaja de este aproach es que puede fácilmente diagnosticar mediante la creación de topologías lógicas idénticos en todas las VLAN. Los Root Bridge centralizados son mas comunes.

- Donde Poner el Root Bridge: En general, la mas importante consideración es ubicar el Root Bridge en la ruta del flujo dee datos

de alto ancho de banda, El goal es tener el espejo de la topología Spanning Tree al flujo natural ed tráfico en tu red. Para hacer otherwides implica una ruta ineficiente para el flujo de mayor ancho ded banda-intensivo. La optimización en la mayoría de los caso es alcanzado en una de las dos maneras:

1. Cuando usamos diseños planos tales como campus-wide VALN, el roote bridge debería generalmente ser ubicado en el punto donde los server farms se conectan al campus core. Asumiendo que un par de switches es usado para enlazar el server farm al core, (esto provee redundancia y ancho de banda adicional), el Root Brdige pude ser alternado en un basis per-VLAN.
2. Cuando usamos router-switches (MLS) con modelos multicapas, el Rott Bridge debería ser ubicado en el switch que contiene (o, en caso de un router externo, hacia los enlaces) el peer activo HSRP para una VLAN dada. Adeemás, si un switch MDF está actuando como un HSRP activo peer para las VLAN odd-numbered, este debería también ser el Root Bridge primario para esta VLAN.

Sintonizando el Timer.- La descisión de utilizaar Spanning Tree tiemr tuning debería ser basado en primer lugar en la arquitectura ded campus. Si hemos utilizado el campus-wide VLAN, el timer tuning es casi siempre un ejercicio en futility y frustación. Debido a que el campus-wide VLAN guia a dominios

Spanning Tree muy grandes, el "timer tuning" usualmente resulta en una red plagada por la inestabilidad.

Por otro lado, la barrera de capa 3 creado por el modelo multicapa hace del "timer tuning" una atractiva opción para la mayoría de redes. Cuando llevamos a cabo el "timer tuning", es usualmente mejor usar el macro "set spantree root" . En general los valores de la tabla 7-2, han sido mostrados para ser un buen compromiso entre la estabilidad de la red y la velocidad de convergnecia.

DISEÑO DE RED	DIAMETRO ESPECIFICO	TIEMPO HELLO ESPECIFICO	RESULTADO MAX AGE	RESULTADO FORWARD DELAY
Campus-waide VLAN	N/A	N/A	Defecto (20 seg.)	Defecto (15 seg.)
Multilayer y Routing switches (MLS)	3 hops	2 seg.	12 seg.	9 seg.
Multilayer y Switching routers (8500s)	2 hops	2 seg.	10 seg.	7 seg.

Tabla 7-2 Valores Timer de Spanning Tree recomendados.

Debido a que el "timer tuning" no es recomendado para campus-wide VLAN y debería además no ser especificado en el set spantree root, estos valores han sido omitidos de la tabla . Los valores del routing switch (MLS) y el switching router estan basados en suposiciones bastantes conservadoras acerca de enlaces caidos y la posibilidad de adicionar dispositivos bridging adjuntados a la red.

También, si tu estas listo y capaz de incurrir en la carga extra de BPDUs Spanning Tree, el Hello Time puede ser reducido a 1 segundo para

mejorar el tiempo de convergencia. Sin embargo, notar que esto duplica el ancho de banda consumida por los BPDUs y, lo mas importante, la carga del CPU. Además, si cada dispositivo participa únicamente en un pequeño número de VLANs, el "Hello Time" puede satisfactoriamente mejorar el tiempo de convergencia de "Spanning Tree" con un mínimo impacto en el CPU. Por el contrario, si tus dispositivos participan en un gran número de VLANs, el cambio de "Hello Time" puede sobrecargar tu CPU. Cuando usamos un gran número de VLANs, únicamente baja un poco el "Hello Time" para una subred de VLANs donde necesitan un tiempo de convergencia mejorado como compromiso. Si bajamos el "Hello Time" a un segundo, considere usar los valores especificados en la tabla 7-3.

DISEÑO DE RED	DIAMETRO ESPECIFICO	TIEMPO HELLO ESPECIFICO	RESULTADO MAX AGE	RESULTADO FORWARD DELAY
Multilayer y Routing switches (MLS)	3 hops	1 seg.	7 seg.	5 seg.
Multilayer y Switching routers (8500s)	2 hops	1 seg.	5 seg.	4 seg.

Tabla 7-3 Valores de tiempo de Spanning Tree cuando usamos el tiempo Hello de 1 segundo.

Finalmente, debemos estar seguro del conjunto de valores de tiempo elegidos para el "Root Bridge" principal y "back up". Tener presente que podemos configurar valores en otro switch, pero no tendría efecto.

"Spanning-Tree" y la VLAN de Administración.- El tiempo de aprender la topología lógica "Spanning Tree", no es durante la mitad de una gran red implementada. En vez de eso, es aconsejable crear mapas de las topologías

Spanning Tree principal y backup. La mayoría de organizaciones estan acostunbrados a hacer uso extensivo de diagramas que revelan la topología de capa 3 de su red. Sin embargo, muy pocas de estas mismas organizaciones van a través del buen ejercicio de crear y distribuir mapas de capa 3.

En un mínimo, estos diagramas deberían ilustrar el extent de cada VLAN, la ubicación el Root Bridge, y cuaes puertos switch to switch estan en estado blocking y forwarding. Adicionalmente podría ser muy usual etiquetar los puertos frwarding como los puertos Designados o los puertos Root.

La importancia de tener diagramas de capa 2 es influenciado por, otra vez, la elección del diseño de la red. Ellos son específicamente importantes en el caso de campus-wide VLAN donde la combinación de muchas VLANs y puertos blocking/forwarding pueden llegar a ser muy complejos. Afortunadamente, otro beneficio del modelo multicapas es que reduce la necesidad de diagramas. Primero, la jerarquia de capa 3 creado por este diseño hace que los mapas de capa 3 tradiconales sean muy usuales. Segundo, el triángulo de capa 2 y las "V´s" creadas por este diseño permiten que dos o tres dibujos sean usados para documentar la red de capa 2 entera.

Cuando Usar Up-Lin Fast y Backbone Fast.- Ambos son significant Cisco enhancements para el protocolo Spanning Tree. Es importante conocer cuando usar o no ellos. En general, ninguna característica es particularmente muy usual en una red que contiene fuertes componentes switching de capa 3 . Debido a que tiende a quebrar la red en un gran número de rutas libre de loops, no hay puertos Blocking para que el Uplink fast y Backbone fast lleven a cabo su magia.

Por otro lado ambos pueden ser muy usual en mas diseños orientados a capa 2, tales como campus-wide VLAN y el modelo multicapa con routing switching (MLS). En ambos caso, Uplink fast debería de ser habilitado únicamente en los switches de los closets de cableado IDF mientras el backbone fast es habilitado en el switch en cada dominio Spanning Tree. Aunque ambos protoccolos han sido diseñados para que no completamente desabilitar la red cuando ellos son usados incorrectamente, esto causa una característica de ser completamente inefectivos (como es posible en backbone fast) o invalidar el balanceo de carga y ubicación del Root Bridge (como es posible con Uplink fast).

Cuando Usar Posrt Fast.- Port fast es una herramienta que deserves consideraciones en cada red. Hay dos principales beneficios de usar port fast:

- Las estaciones finales y algunos servidores que eusan NIC tolerante a falla pueden ganar acceso inmediato a la red. En el caso de las estaciones finales, este puede ayudar con protocolos tales como DHCP y servidor inicial o directorio de autentificación. Para servidores que usan NIC tolerante a falla que toggle link-state, el PortFast puede significar la diferencia entre failover transparente y 30-50 segundos dee outage (sin embargo la mayoria de NIC tolerante a fallas no toggle links). Cuando ussamos Portfast conconexiones ded servidor, asegurate de desabilitar PagP en EthernetChannel-capable ports. Otherwise PortFast aun tomaría aproximadamnete 20 segundos en habilitar el enlace.
- Los Ports no envían BPDUs de notificación de cambio de topología (TCN) cuando estan usando PortFast. Debido a que TCN causa que los bridge y switches usen bridge mas corto again periodo, un excesod e estos paquetes puede desestabilizar un gran campus red (especialmente con diseños planos como campus-widede VLAN). Por potencialmente eliminando 10 de miles de TCNs por día en una típica red campus grande, el uso de PortFast puede tener un impacto significativo.

Cuando un Spanning-Tree no es Suficiente.- Aunque muchas personas complain que un Spanning Tree por VLAN es tan complejo para la comprensión humana, hay veces cuando es necesario usar mas que un Spanning Tree por VLAN, mejor que usar usar PVST+ para tunnel múltiples

Spanning Tree a través de una región 802.1Q que únicamente utiliza un simple Spanning Tree, el primer uso de múltiples Spanning Tree por VLAN es para satisfactoriamente integrar bridging y routing entre VLANs. Cuando combinamos bridging y routing, la situación puede arise donde IP subnets llegan a ser particionados y ocurra una pérdida parcial de conectividad. Como se detalló en el capitulo referente a Switching capa 3, la solución es usar dos versiones de protocolo Spanning Tree. Los catlyst de capa 2 únicamente usan la versión IEEE del protocolo Spanning Tree. Sin embargo, los dispositivos basados en IOS tales como los routers y el catalyst 8500 pueden correr la versión DEC del protocolo Spanning Tree o el protocolo Spanning Tree VLAN-Bridge propietario de Cisco. En ambos casos, los BPDUs para estos dos protocolos son tratados como data multicast normal por el catalyst de capa 2 y normalmente flooded. Conversely, los dispositivos basados enIOS swallow el BPDUs IEEE cuando ellos están corriendo una versión diferente de protocolo Spanning Tree.

Consecuentemente los dispositivos basados en IOS particionan el protocolo IEEE dentro de pockets mas pequeños. Dentro de cada pocket, el protocolo Spanning Tree IEEE asegura que la topología lógica esté libre de loop. La versión DEC o VLAN Bridge del protocolo Spanning Tree asegura que la colección de pockets remains libres de loop. El resultado es una red donde ambos protocolos ruteados y no ruteados tengan completa conectividad a través de la red.

7.3.3.- Balanceo de Carga

El balanceo de carga puede ser uno de los telltale signos que indican si una red ha sido cuidadosamente planeado o si esto ha crecido como weeds. Permitiendio enlaces redundantes para efectivamente doblar el ancho de banda disponible, el balanceo de carga es algo que cada red debería strive para implementar.

A continuación detallamos las alternativas disponibles para implementar el balanceo decarga. Además, aunque esta técnica son mayormente referidos con el nombre de blanceo decarga, el nombre dee compartición de carga o distribución de carga podría ser mas apropiado, Sin embargo, no get hung up con intentar alcanzazr un split esacto 50/50 cuando implementas balanceo dee carga sobre un par de enlaces. Solo recuerda que la única forma de balanceo de carga es preferible la operación por defecto en la mayoría de protocolos campus donde una única ruta es ever usado.

Recordar los Requerimientos de Balanceo de Carga.- Antes de entrar a detalle, es necesario hacer una pausa para examinar alguns consideraciones de balanceo de carga. Cuando pensamos acerca de balanceo de carga, primero miremos el número de rutas disponibles. Si tenemos únicamente un conjunto de rutas a través de la red, el balanceco de carga no es posible. La mayoría de diseñadores strive para alcanzazr dos rutas, como visto conectado a un switch IDF/capa de acceso. En algunos

casos, especialmente dentro de un gran campus core, mas de dos rutas podrían ser disponibles.

Otra consideración es la facilidad con la cual se puede configurar, administrar, y diagnosticar un esquema de balanceo de carga particular. Por ejemplo, la forma de ubicación del Root Bridge del balanceo de carga Spanning Tree es muy fácil de implementar y diagnosticar.

También, observar la flexibilidad de cada estilo de balanceo de carga. Por ejemplo, aunque la ubicación del Root Bridge marca muy alto en una escala simple, este puede únicamente ser implementado en topologías seleccionadas (tales como triángulos capa 2 usado en el modelo multicapa). Por el contrario, el método de "portvlancost" del balanceo de carga de Spanning Tree es muy flexible y muy complejo.

Finalmente, considerar la inteligencia del esquema de balanceo de carga. Las consideraciones importantes de balanceo de carga incluye:

- Rutas disponibles
- Facilidad de configuración, administración y diagnóstico
- Flexibilidad
- Inteligencia

Spanning-Tree.- El balanceo de carga Spannig Tree es muy usual dentro de un dominio de capa 2 redundante. Hay cuatro técnicas ded balanceo de carga disponible bajo el protocolo Spanning Tree:

- Ubicación del Root Bridge
- Prioridad e puerto (portvlanpri)
- Prioridad de Bridge
- Costo de puerto (portvlancost)

La ubicación de Root Bridge es la forma mas simple y mas efectiva técnica si el flujo de tráfico de la red lo soporta. Afortunadamente, el modelo multicapa con routing switches (MLS) automáticamente genera una topología donded el Root Bridge puede ser alternado entre switches MDF redundantes dentro de un block de distribusión.

Cuando trabajamos con protocolo Spanning Tree, intentemos no usar la forma de ubicación de Root Bridge del balanceo de carga Spanning Tree.

La ubicación dee Root Bridge es no efectiva en topologías menos constrained tales como campus-wide VLAN. En estos casos, es mejor usar la forma portvlancost de balanceo de carga. Aunque el portvlancost es de uso mas duro que la ubicaciónde Root Bridge, es muy usual en casi cualquier topología redundante.

Cuando trabajamos con protocolo Spanning Tree, usa balanceo de carga portvlancost cuando el uso de ubicación ded Root Bridge no es posible.

Hot Standby Router Protocol (HSRP).- En situaciones donde switching capa 3 esta siendo usado, el HSRP juega un rol muy importante. Cuando usamos switching capa 3 es redes que continen loops ded capa 2 en el bloque dee distribución, tales como con modelos multicapas y routing switches (MLS), Spanning Tree y balanceo de carga HSRP deberíanm ser deesarriollados en un fashion coordinado. Por ejemplo, la red en la figura 7-19 modificó los parámetros de Spanning Tree para forzar a las VLAN odd usar el enlace izquierdo y las VLANs even usar los enlaces derechos. HSRP dedbería ser adisionado a este diseño por haciendo el MDF-A el activo HSRP activo para las VLAN oidd y el MDF-B el peer activo para las VLAN even.

En casos donde el switching router (8500) approach al modelo multicapa está en uso, el HSRP podría ser la única opción diosponible para el balanceod e carga dentro de cada block de distribución. Consecuentemente, dos grupos de HSRP deeberían ser usados para cada subnet.

Use balanceo de carga MHSRP para redes usando tecnología switching router. La figura 7-20 ilustra un ejemplo que provee balanceo decarga para subnet/VLAN en un switch IDF

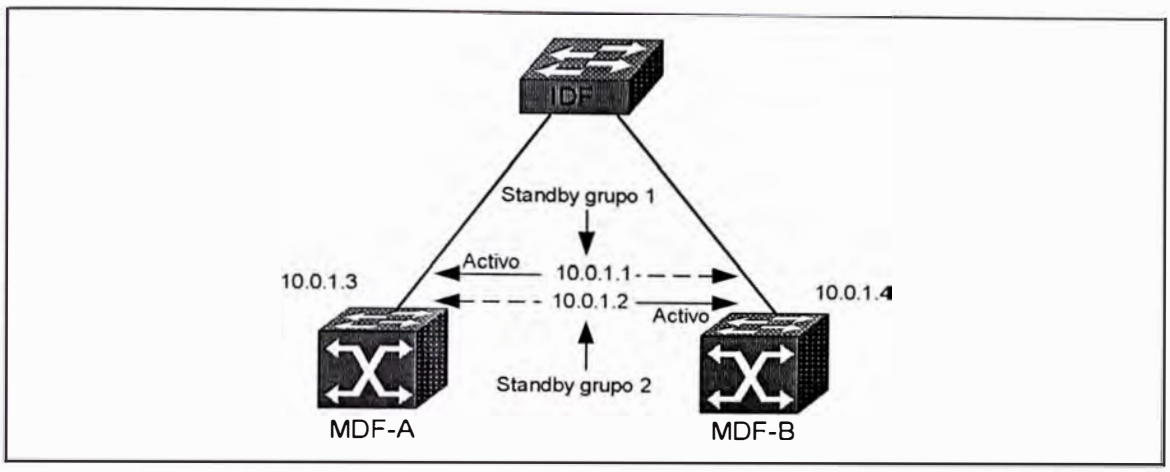


Figura 7-20 Balanceo de carga con MHSRP.

A ambos switches MDF son asignados dos direcciones IP reales 10.0.1.3 y 10.0.1.4 mejor que usar un simple grupo standby (el cual resulta en únicamente un router y un enlace riser activamente llevando tráfico), dos grupos standby son configurados. El primer grupo standby usa una dirección IP de 10.0.1.1 y la prioridad de MDF-A ha sido incrementado para hacer esto un peer activo. El segundo grupo standby usa 10.0.1.2 y tiene MDF B configurado como el peer activo. Si ambos switches MDF estan activos, ambos enlaces riser y ambos dispositivos activamente llevan tráfico. Si cualquiera de los dispositivos MDF fallan, el otro MDF toma el 100 % de la carga.

Enrutamiento IP.- Otra ventaja de usar switches de capa 3 es que los protocolos de enrutamiento IP soportan envío inteligente y mecanismos de determinación de ruta. Sin embargo, esto nos puede llevar a realizar considerables configuraciones para habilitar balanceo de carga sobre dos rutas, usando técnicas como STP load balancing y HSRP, los routers Cisco

automáticamente hacen balanceo de carga hasta seis rutas de igual costo. Loreover, los protocolos dee enrutamiento de capa 3 soportan herramientas de manipulación de ruta extensiva tales como lista distribuida y mapas de rutas.

Dado que un diseño multicapa se enfoca en switching capa 3 en los closet MDF/capa de distribución (y posiblemente el core). El enrutamiento IP puede ser un approach extremadamente efectivo para el balanceo de carga a través de áreas críticas de la red tal comoel core (enlaces WAN caros son otra área).

Asynchronouss Transsfer Mode (ATM) .- Uno de los beneficios en usar ATM en embientes campus es la sofisticación de Private Network-network Interface (PNNI) como un enrutamiento ATM y protocolo de selñalización. Como IP, PNNI autimáticamente hace balanceo de carga sobre múltiples rutas. Sin embargo, a diferencia de IP, PNNI no lleva a cargo enrutamiento en cada unidad ded información que este recibe (celdas). En vez de eso, ATM únicamente enruta el inicial call setup que es usado para construir la conexión ATM. Después que la conexión ha sido establecida, todas la celdas remaining siguen esta única ruta. Sin embargo, otro call entre los mismos dos switches ATM pueden usar un conjunto diferente de rutas a través de una red ATM redundante (además PNNI es dicho a sser un balanceeo dee carga por conexión). De esta manera, todos las rutas dentro de la nube ATM son automáticamente utilizados.

Ether Channel.- Una forma final de balanceo de carga que puede ser usual para redes campus es el EtherChannel. Este puede únicamente ser usado entre un par de switches back to back conetados entre dos y ocho enlaces (aunque algunas plataformas permiten conbinaciones limitadas). Este usa un algoritmo XOR en el orden de bits mas bajo de direcciones MAC o IP para asiganr tramas a enlaces individuales. El 802.3ad commitee de la IEEE trabaja en un protoclo basado en estándar similar al EtherChannel de Cisco.

7.3.4.- Routing / Switching Capa 3

Strive for Modularity.- Uno de los primeros eficios de usar tecnología switching capa 3 es que esto puede crear un alto grado ded modularidad en el diseño. Por instancia, La Figura 7-21 muestra un típico campus de dos edificios usando modelo multicapas.

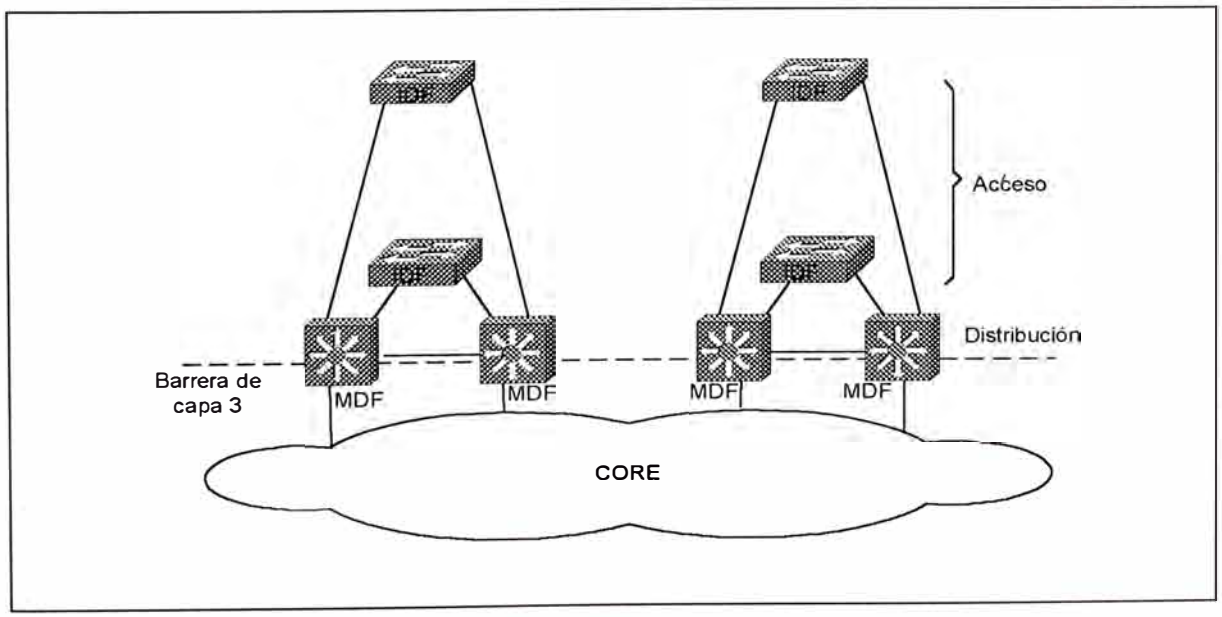


Figura 7-21 Usando barrera de capa 3 para crear un diseño modular.

El arrier de capa 3 creado por la función de enrutamiento emedded en los switches MDF separa cada edificio de Core. Los bneficios primarios de esta técnica son:

La modularidad permite diseños cookie-cutter. Aunque las direcciones IP (como taimen las otras direcciones ded capa 3) camian, cada loque de distriución puede ser implementado con código de router y switches casi idénticos.

- La red es muy fácil de entender y diagnosticar.
- La red es altamente escalale. Como nuevos edificios y servidores farms son adicionados al campus, ellos merely ienen a ser nuevos loques de distriusión off el core.
- La red es muy determinístico. Como los dispositivos o enlaces fallan, el tráfico will failover en formas claramente definidos.

Auinque algunos grados de modularidad pueden ser creados con mas diseños de capa-2 orientado tales como campus-wide VLANs, es mucho mas difícil conseguir la separación requerida por la verdadera modularidad. Sin un arrier de escalailidad de capa 3, los protocolos de capa 2 tienden a ser interwined y tightly coupled. Consecuentemente, esto viene a ser mucho mas difícil crecer y rearreglar la red.

Cuando Usar MLS (y Routing Switches).- La forma routing switch (MLS) del modelo multicapas es mas apropiado cuando queremos mantener un

componente de capa 2 fuerte dentro de cada bloque de distriución. Haciendo eso, el MLS permite que el Catalsyt de capa 2 prospere. Las opciones tales como VTP y PVST pueden ser muy usuales en estos ambientes. También, manteniendo esta orientación de capa 2 fuertemente, podemos fácilmente ubicar una simple VLAN en múltiples switches IDF/closet de capa de acceso. Además, el MLS tiene excelente soporte para enrutamiento multiprotocolo, asi como también combinar enrutamiento y "bridging" dentro de un mismo dispositivo.

Cuando Usar Switching Routers.- Mientras que el MLS mantiene un diseno de capa 2 dentro del bloque de distribusión, los swithing routers van al extremo opuesto. Los switching routers tales como el Catalyst 8540 son mas fáciles de configurar y mantener cuando funcionan como un router puro. Aunque ellos soportan "bridging" a través del uso de IRB y bridges group, el extenso uso de estas características pueden guiar a configuraciones que son difíciles de mantener.

En vez de eso, el uso de estos dispositivos como routers de muy alta velocidad, pueden dramáticamente simplificar el diseño de red. Temas y problemas asociados con Spanning Tree todos desaparecen. El flujo de tráfico viene a ser altamente determinístico. El soporte de personal acostrumbrados a trabajar en el tradicional modelo router y hub, encuentran en el switching router diseños fácil de soportar y diagnosticar. El soporte

superior de tecnología multicas IP en capa 3, provee una excelente ruta de migración hacia el futuro.

Cuando Usar IRB.- En resumen, usa IRB únicamente cuando tengas que usar. No es que IRB sea una mala característica. En realidad, IRB es una tecnología muy flexible para combinar tráfico de capa 2 y capa 3 y esto permite control preciso sobre como ambos tráficos (bridged y routed) es manipulado. El problema es mas diferente a ser uno humano. IRB puedee ser difícil ded entender, soportar y diseñar.

Cuando consideras el uso de IRB, tambiéwn toma en cuenta los siguientes issues:

- Una ventaja de hacer que el IRB en plataformas basados en hardware tales como el Catalyst 8500 es que esto puede ser llevado a cabo a velocidades del alambrado (los routers basados en software son actualmente limitados a velocidades fast-switching).
- Hay un límite al numero dee Interfaces Virtuales Bridges (BVI) que el IOS soporta.
- Algunas características no son soportados en BVIs, por que la lista esta constantemente cambiando.

Cuando decidimos donde usar IRB, intenta únicamente como una herramienta para específicos issues. Por ejemplo, si necesitamos ubicar

muchos servidores conectados directamente dentro de un único VLAN o si hay una VLAN que absolutamente tiene que transitar un switching router.

Limita Innecesario Router Peering.- Caundo usamos router en redes basados en VLAN, este puede ser importante reducir innecesario router peering. Por ejemplo, considere cxasos como los ilustrados en la figura 7-17 y figura 7-20. Asume que estos routers conectan a 30 closets de alambrado VLANs via ISL o trunks 802.1Q . Por defecto, el router formaría 30 adjacencias separadas, gastando memori y procesamiento. Listando todos estos VLANs coio pasivos interfaces para el protocolo de enrutamiento, este puede dramáticamente reducir este innecesario peering. Para las VLANs de closet de alambrado donde ningun routers son localizados, todos los VLANs deberían ser removidos.

Balanceo de Carga.- Como es discutido en la sección de Spanning Tree, el estilo de balanceo ded carga que es necesitado depende primeramente del tipo de switching de capa 3 que esta en uso. Para resumir, el MLS generalmente requiere que una combinación de Spanning Tree y técnica dee balanceo de carga SEP sea usado dentro de un bloque de distribución. Si usamos switching routers, se debería usar MHSRP.

También los switches de capa 3 automáticamente balancean la carga a través del campus core si rutas dee costo igual son disponibles.

Intentar Usar Únicamente Protocolos Ruteables.- A menos que sea absolutamente necesario, intenta pasar únicamente protocolos ruteables a través de tus switches. Es algunas veces mas acomplished relegar protocolos no ruteables a un único VLAN. Si estamos migrando a una nueva infraestructura de red, considere usar el tráfico no ruteable en la infraestructura antigua. El lagging performance de que servidores de red como un incentivo para que los usuarios de protocolos no ruteables upgrade a una aplicación basada en IP.

7.3.5.- Asynchronous Transfer Mode (ATM)

Como los switches capa 3 ha crecido en popularidad, este ha demostrado que ATM no es la única tecnología capable of great speed. Sin embargo, ATM tiene su ubicación en muchas redes campus.

Cuando Usar ATM .- Una de las principales preguntas que el diseñador debería encarar es: Debería el diseño utilizar tecnología ATM. En el pasado, ATM ha sido billed como la solución para cada posible problema de red. Aunque esto podría ser verdad en términos de la capacidad teórica del ATM, no es verdad en términos de cómo la mayoria de organizaciones estan usando ATM. Por ejemplo, en la mitad de 1990 muchos analistas de red foretold de los días venideros donde las redes deberían usar ATM en un basis end to end. En vez de eso, Ethernet ha continuado creciendo en popularidad. Cuando, entonces. Es mejor usar switching basados en celdas?.

Tradicionalmente, ATM ha sido touted por muchos beneficios únicos. El beneficio mas comúnmente mencionado incluye:

- High Bandwidth: Debido a que las celdas usan unidades de tamaño fijado dee data con formatos de cabecera simples y predicibles, es fairly fácil crear equipos switching basados en hardware.
- Sophisticated Bandwith sharing: Las celdas puede ser interleavied para permitir múltiples sesiones de comunicación para compartir un único enlace a través de una forma avanzada de multiplexación estadística. Debido a que las celdas son todos del mismo tamaño, las aplicaciones que usan unidades dee transferencia de datos grandes no crean un efecto log jam que slows down smaller and potentially more tiem-sensitive traffic.,
- Quality of Service (QoS): ATM tiene un complejo y sofisticado mecanismo para permitir contracts de trafico detallado para ser especificado y enforzado.
- Soporta para Voz y Video: La baja latencia de el beneficio de QoS de ATM le da soporte robusto para formas dee tiempo crítico de comunicación tales como voz y video.
- Distancia: A diferencia de la tecnología de campus comun tal como Ethernet, ATM puede funcionar sobre cualquier distancia.
- Interoperatibilidad: Por que ATM es un estándar global, un variedad amplia de dispositivos puede ser purchased desde vendedores diferentes.

Aunque muchos de estos puntos permanecen ciertos, el progreso de la conmutación basado en tramas ha erosionado significativamente los límites del ATM en las siguientes áreas:

- Los Switches Ethernet Gigabit orientados a "campus", ahora corresponden o exceden la velocidad de los switches ATM. Aunque la conmutación de celdas mantiene una ventaja teórica, los switches capa 2 y capa 3 basados en ASIC, han llegado a ser excepcionalmente rápidos. Además, ATM ha continuado para competir en los límites SAR, a las velocidad más rápida que la función de reensamblaje y segmentación ATM pueden ser llevadas a cabo.
- Esquemas QoS basados en Ethernet (o al menos Clase de servicio) han llegado a ser más disponibles, prácticos, y efectivos. Aunque ATM retiene un liderasgo teórico, ATM continúa sufriendo de una carencia de aplicaciones que capitaliza en su capacidad inherentemente superior. Como resultado, los switches Ethernet Gigabit CoS están rápidamente creciendo en popularidad.
- Aunque ATM mantiene una ventaja distintiva en su capacidad de manipular aplicaciones isócronos (tiempo crítico), hay tremendo crecimiento en mecanismos no isócronos para enviar tráfico de voz y video. Esfuerzos como Voz sobre IP (VoIP) y videoconferencia H.323 son ejemplos comunes. Estas tecnologías reducen la necesidad de capacidades únicas de ATM.
- Las distancias de Ethernet Gigabit están creciendo dramáticamente.

- Todas las formas de Ethernet, incluyendo Gigabit Ethernet, han sido percibidos considerablemente como estándares mas interoperables que ATM.

Adicionalmente, la complejidad de ATM ha llegado a ser un issue significante para la mayoría de organizaciones. Cualquier Ethernet es considerado fácil y familiar, ATM es considerado dificultoso y murky.

Donde Usar ATM.- Aunque hay considerables debates de usefullness de ATM en un backbone campus, hay considerable menos debate acerca de donde este es muy usual. Aunque todos los analistas estan deacuerdo que las conexiones desktop serían Ethernet para el futuro foreseeable. Aunque las ventas de Ethernet 10/100 continua to soar, la venta de ATM al desktop ha staggered. Cuando ATM es usado, casi todos acuerdan que ATM es mejor suited al core de la red. En la mayoría de casos, esto significa que un Core LANE conectando a switches ethernet conteniendo módulos uplink LANE.

Aunque este issue ha recibido fairly pequeño debate, un segundo issue ha sido menos clear-cut. El issue concierne el matter de cuan lejos el backbone ATM debería alcanzar. El debate surrounds dos opciones:

Algunos vendedores y diseñadores de red prefieren enlazar únicamente el MDF/dispositivos de capa de disstgribución al core ATM. Los

enlaces Ethernet Gigabit y Fast Ethernet pueden luego ser usados parta conectar a switches IDF como mostrado en la figura 7-22.

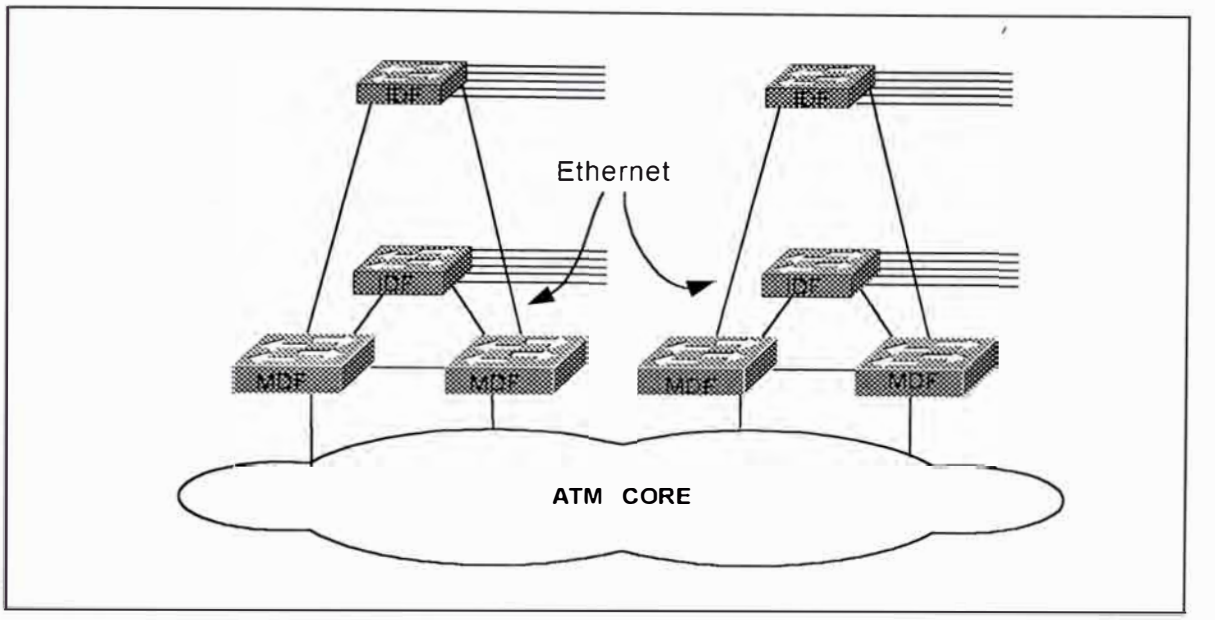


Figura 7-22 Usando enlaces Ethernet en conjunto con un CORE ATM.

La ventaja de este aproach es que este usa tecnología Ethernet de costo efectivo en el número potencialmente grande de closet IDF´s. Este diseño es algunas veces deasarrollado usando el modelo VLAN campus wide para extender la velocidad de ATM a través de enlaces Ethernet. El downside es que esto crea un gran número de loops de capa 2 dondee enlaces redundantes MDF a IDF son usados. Desafortunadamente estos enlaces han sido mostrados para crear Spanning Tree loops que pueden deshabilitar la red campus entera. Además, es muy duro usar características ATM tales como QoS cuando el límite de al red usa Ethernet.

La vista opposing es que el backbone ATM debería extender todos los caminos hacia los closets IDF. Bajo este diseño, la red entera

utiliza ATM excepto para los enlaces que directamente se conectan a dispositivos de usuario final. Este aproach es ilustrado en la figura 7-23

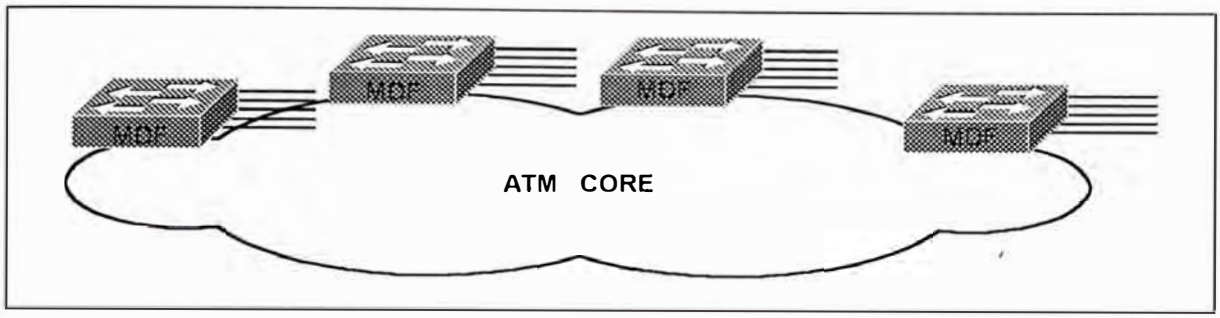


Figura 7-23 Extendiendo el CORE ATM a los switches IDFs.

El downside ded esta alternativa es el costo potencialmente mas alto por que requiere mas upñlink ATM y puertos switches. Sin emabrgo, el major beneficio de este diseño es que elimina los loops de capa 2 formados por los enlaces Ethenret en el aproach previo. Debido a que el LANE inherentemente crea una topología dee capa 2 libre de loop, el riesgo de problemas Spanning Tree es consoderablemente menos.

Habiendo trabajo con implementaciones usando ambos diseños. Se siente que la respuesta debería de ser guiado por el uso de switching de capa 3 (como muchos otros diseños). Si tu estas usando el modelo multicapas para crear barriers de capa 3 duro en el MDF/dispositivos de capa de distribución, los switches MDF pueden ser los puntos de adjunto hacia el core ATM y enlaces Ethernet hacia los dispositivos IDF pueden ser safely usado. Sin embargo, cuando el modelo VLAN campus-wide esta en uso, extendiendo el backbone ATM hacia los IDF´s permite un diseño mas

estable y escalable. Intentando usar el método MDF adjunto con VLANs campus wide, resulta en lazos Spanning Tree y temas de estabilidad de red.

Usando SSRP.- Hasta los mecanismos de redundancia LANE basados en estándares llegan a ser disponibles, el Simple Server Redundancy Protocol (SSRP) retiene una importante característica en casi cualquier core basado en LANE usando switches ATM cisco. Aunque SSRP permite mas que un cunjunto de dispositivos redundantes, la experiencia ha demostrado que este puede guiar a escalar problemas.

Ubicación del BUS.- Siempre intenta ubicar tu LANE Broadcast Unknown Server (BUS) en un Módulo LANE del catalyst. Debido a que el BUS tiene que manipular cada paquete broadcast y multicast en la ELAN, el volumen de tráfico potencial puede ser extremadamente alto. Los módulos LANE del Catalyst 5000 OC-3 y Catalyst 5000/6000 OC-12, ofrecen aproximadamente 130 Kpps y 450 kpps de performancia de BUS respectivamente, considerablemente mas que cualquier otro dispositivo Cisco actualmente ofrecido.

Una decisión encarada por diseñadores de grandes cores implica si un simple BUS o múltiples BUS distribuidos deberían ser usados. La ventaja de un simple BUS es que cada ELAN tiene la misma topología lógica. La desventaja es que el único BUS puede llegar a ser un cuello de botella.

Los BUS distribuidos permiten que cada ELAN tenga un BUS diferente. Aunque este puede ofrecer significativamente troughput dee BUS agragado mas alto, este puede hacer de la red mas duro dee administrar y diagnosticar. Con la introducción de módulos LANE OC-12 y su performancia de BUS extremadamente alto, esto es generalmente advisable a usar un único BUS y capitalizar en la simplicidad de tener una simple topología para cada ELAN.

MPOA.- Multiprotocolo sobre ATM (MPOA) puedee ser una tecnología muy usual para improving performancia dee cpa 3. MPOA, Trunking with Multiprotocolo over ATM, permiten shortcut circuitos virtuales para ser creados y evitar el uso ded routers para flujos extendidos. Cuando consideramos el uso de MPOA, manten los siguientes puntos en mente:

- MPOA puede únicamente crear shortcuts en secciones dee la red que usa ATM. Además, si el dispositivo MDF adjunto a un core ATM pero Ethernet es usado para conectar desde el MDF al switch IDF, MPOA es únicamente usual dentro del core por si solo. Si el core no contine hops de capa 3, MPOA no ofrece ventaja sobre LANE. En general, MPOA es muy usual cuando la nube ATM extiende hacia el IDF/switches de capa de acceso.
- Debido a que MPOA es principalmente diseñado para redes que usan ATM en un basis IDF to IDF, tenemos que intencionalmente construir barriers capa 3 dentro de la red. Sin un plan dee cuidado, MPOA puede guiar a una red flat earth.

- Hasta el presente, las preguntas significativas permanecen sobre la estabilidad y la escalabilidad de MPOA.

7.3.6.- Server Farms

Los servidores juegan un role crítico en las redes modernas. Dado su importancia, ellos deberían estar considerados en los procesos de diseño. A continuación detallaremos algunos temas comunes asociados con diseños de servidores "farms".

Donde Ubicar los Servidores.- La mayoría de las organizaciones están moviéndose hacia servidores "farms" centralizados para permitir mejor soporte y administración de los servidores por si mismos. Dado esto, es generalmente mejor posicionar un servidor "farm" centralizado como otro bloque de distribución adjunto al "core campus". Este concepto es ilustrado en la figura 7-24.

Los servidores en la figura 7-24, pueden estar conectados por una variedad de medios. La figura muestra los servidores directamente conectados al par de switches de capa 3 que enlaza al "core campus". Una alternativa de diseño es usar mas switches de capa 3 dentro de un servidor "farm". Estos dispositivos de capa 2 pueden luego ser conectados a los switches de capa 3 a través de "Ethernet Gigabit" ó "EthernetChannel Gigabit". Aunque algunos servidores pueden conectarse a un único switch, los NICs redundantes proveen una medida de tolerancia a falla.

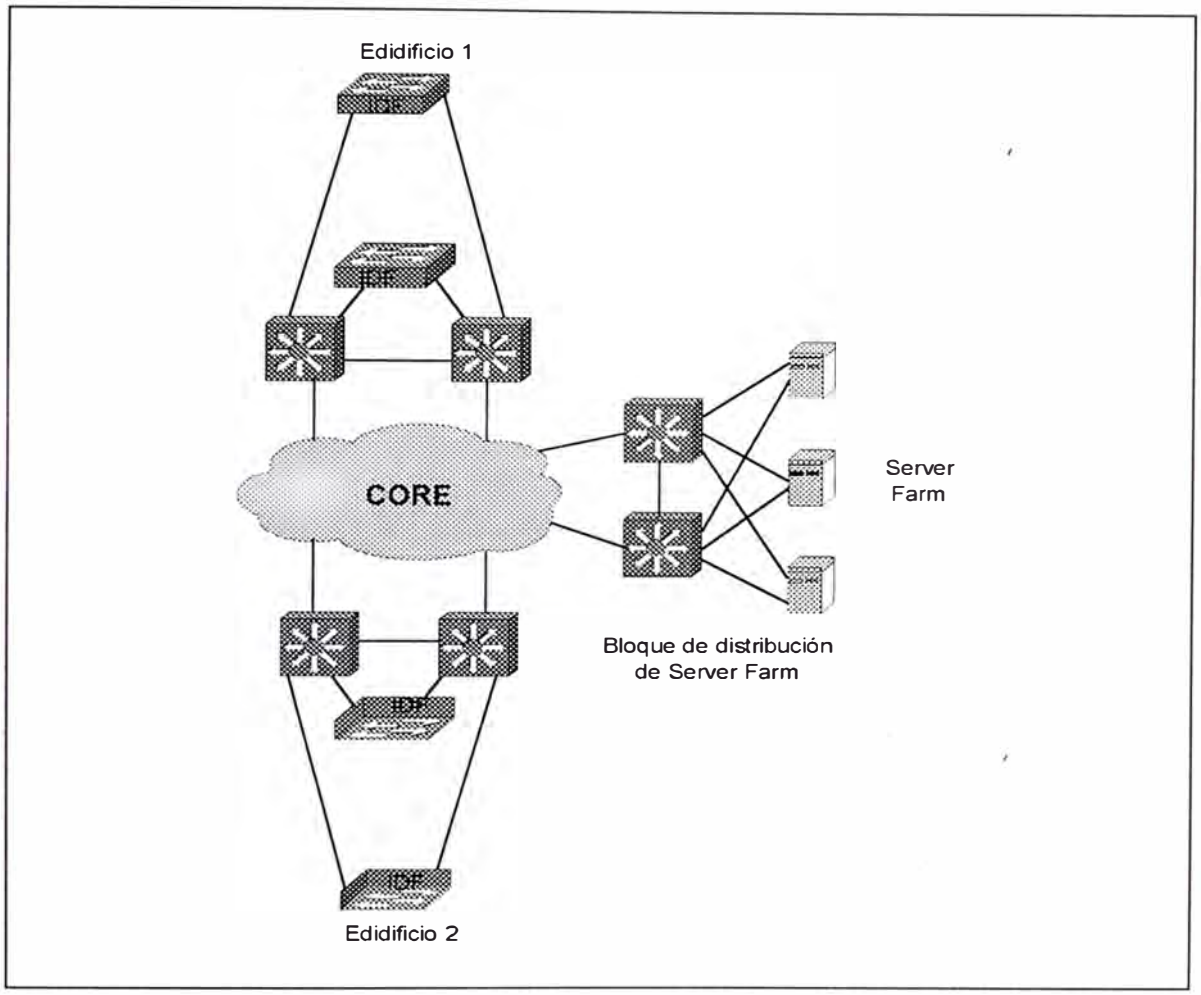


Figura 7-24 Server Farm Cebntralizados.

La clave para este diseño es el barrier ded capa 3 creado por el par de switches de capa 3 que enlaza el server farm al core. No únicamente este insulate el server farm desde el core, pero este también crea un diseño mucho mas modular.

Algunos diseños de redes directamente conectan los servidores al core como muestra la figura 7-25.

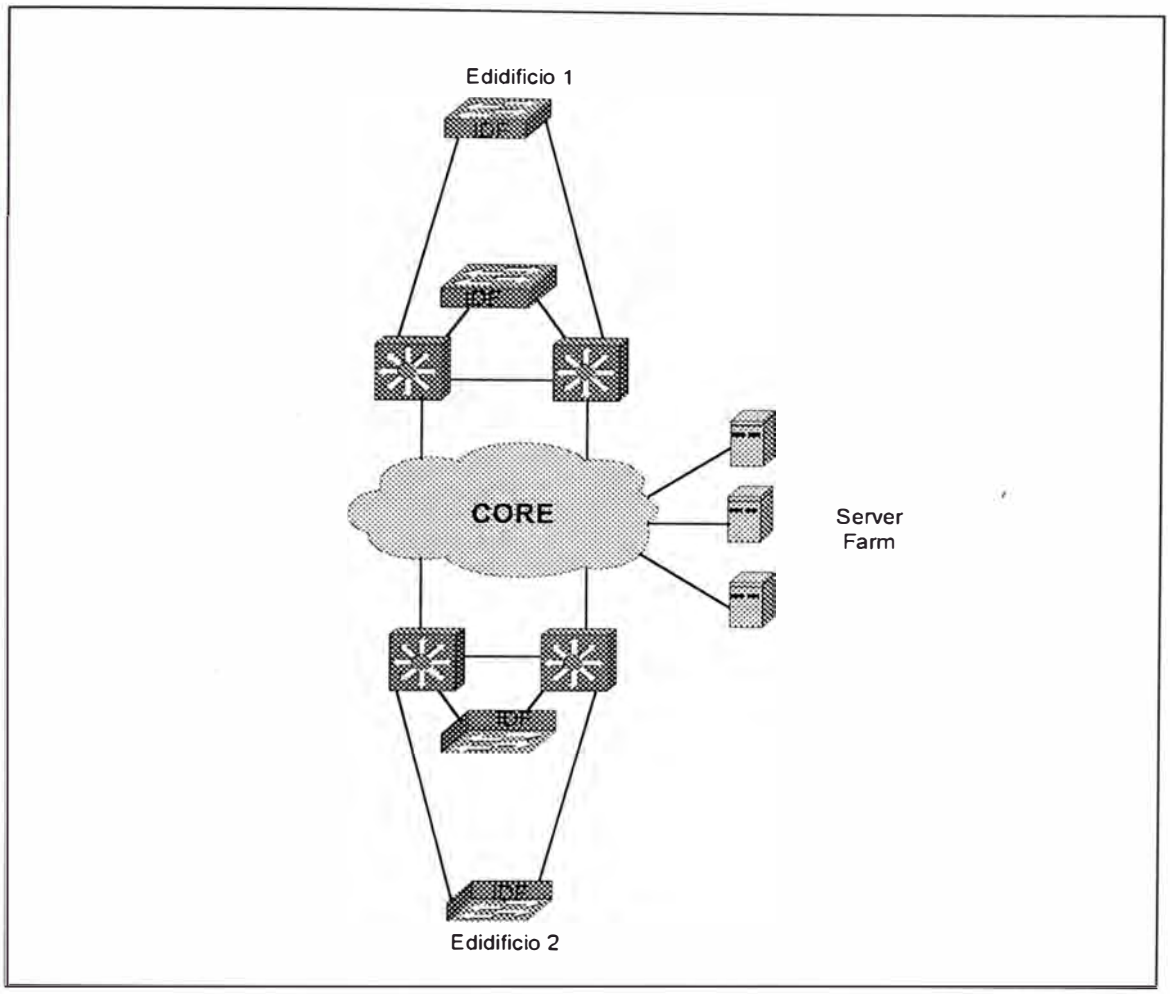


Figura 7-25 Conectando servidores directamente al Core Campus

La figura anterior muestra un popular método usado para servidores adjuntados al core, usando un core ATM. Instalando tarjetas de red (NIC) ATM LANE-capable en los servidores, esllos pueden directamente unir al ELAN usado en el core campus. Un diseño similar podría haber sido construido usando ISL o NIC´s 802.1Q en elos servidores.

La mayoría de las organizaciones corren dentro de uno o dos problemas cuando usan servidores directamente conectados al core campus:

- Flujo ineficiente
- Pobre Performance

El primer problema ocurre con implementaciones dee un modelo multicapa donde los componentes de enrutamiento contenido en el MDF/dispositivos de capa de distribusión puededn guiar a flujos ineficientes. Por ejemplo, considere la figura 7-25, asume que uno de los servidores necesita comunicarse con el usuario final en el edificio 1. Cuando usan tecnología gateway por defecto, los servidores no sabe a cual switch de capa 3 en el MDF enviar los paquetes. Algunos formas de conocimientos de capa 3 es requerido a medida que los paquetes dedjen el server farm. Una forma de alacanzazr esto es correr un protocolo de enrutamiento en los servidores. Sin embargo, este puede limitar la elección de protocolos de enrutamiento a través de remainder de la red , y muchos administradores ded servidor son reluctant para configurar protocolos de enrutamiento en sus servidores. Un clearner aproach es simplemente posicionar el server farm entero detrás de un par de switches capa 3, como mostrado en la figura 7-24.

El segundo problema ocurre con la implementación de VLAN campus wide donde los servidores pueden ser hechos para participar en cada VLAN usado a través del campus (por ejemplo, la mayoría de NIC´s LANE permiten múltiple ELANs a ser configurado),. Aunque esto suene extremadamente atractivo en el papel, estos NIC´s multi-VLAN algunas

veces tienen pobre performance y son sujetos a episodios frecuentes de comportamiento extraño (por ejemplo servidores browsing en redes basados en microsoft).

En general, es la mejor forma de ubicar un servidor farm centralizado detrás de switches capa 3. La cual no únicamente provee forwarding inteligente hacia los switches MDF ubicado a través del resto del campus, pero también provee una variedad de otros beneficios:

- Esta ubicación encourage rápida convergencia.
- Las listas de acceso pueden ser configurados en lkos switches capa 3 para asegurar el server farm.
- El tráfico server-to-server es mantenida off dedl campus core. Este no puede únicamente mejorar la performacia, pero puede también mejorar la seguridad.
- Es altamente escalable
- Los switches ded capa 3 tienen excelente soporte multicast, una consideración importante para campus haciendo uso widespread de tecnología multicast.

Considere Server Farms Distribuidos.- Aunque los servidores farm centralizados estan llegando a ser incrementablemente comun por que ellos simplifican la administración de los servidores, ellos crean problemas desde una perspectiva de administración de ancho de banda, por que ellos agregan razones de data que pueden ser extremadamente alta. Aunque los switches

de capa 3 y 2 de alta velocidad han mitigado estos problemas a un certain extent, los diseñadores de red deberían buscar oportunidades de servidores distribuidos inteligentemente a través de la organización . Aunque este punto es obviamente verdad con regards a enlaces de wide-area, esto tambiéwn puede ser verdad de campus network.

Una ocación donde los servidores pueden fairly fácilmente ser distribuidois en el caso ded servidores departamentales. (servidores que son dedicados a una única unidad organizacional). Estos dispositivos pueden ser directamente conectados al bloque de distribusión de red que ellos sirven. En general, estos servidores son adjuntados en un de dos ubicaciones:

Ellos pueden ser directamente conectados al switch IDF que manipula el departamento dado.

Ellos pueden ser adjuntados a los switches MDF en el edificcio o bloque de distribución. También presenta la oportunidad de crear mini servidores farms en los closets MDF de cada edificio. Los archivosa departamentales y servidores de impresión pueden ser adjuntados aquí donde los servidores enterprice y de alta maintenance pueden ser ubicados en el servidor farm centralizado.

Uso de NICs Tolerante a Fallas.- Muchas organizaciones gastan numerosas horas y millones de dólares creando redes campus altamente redundantes. Sim embargo, mucho de este dinero y esfuerzo pueden irse al tacho a menos que los servidores sean también redundantes por si mismos. Una simple manera de mejorar la redundacia de servidores es instalar algunos tipos de NICs redundantes.

Aunque usando NICs redundantes puede ser tan simple como instalar dos NIC normales en cada servidor, esta propuesta puede guiar a problemas a largo tiempo. Debido a que la mayoría de las redes operando sistemas requieren que cada uno de estos NICs usen una dirección diferente, los clientes necesitan algunos mecanismos para conmutar a la dirección asignada al NIC secundario cuando el primario falle. Esto puede ser arduo de implementar.

En vez de eso, es aconsejable usar NICs especiales que automáticamente soportan conmutación usando una única dirección MAC y dirección de capa 3. En este caso, la conmutación puede ser completamente transparente a las estaciones finales. Una variedad de estos NICs tolerante a fallas son disponibles.

Cuando seleccionamos un NIC tolerante a falla, tambien consideremos que tipo de balanceo de carga este soporta (algunos no soportan balanceo de carga y otros solo en una dirección). Finalmente,

analiza la técnica cercana usado por los NICs para informar al resto de la red que los cambios han ocurrido. Por ejemplo, muchos NICs llevan a cabo un gratuito ARP para forzar un update en los switches vecinos. En algunos casos, este proceso de update puede ser bastante complejo y requiere un compromiso de valores de tiempo. Por ejemplo, cuando usamos NIC ethernet tolerante a fallas en conjunción con un backbone LANE, este no es suficiente para simplificar los update de la tabla CAM de capa 2 y tablas ARP de capa 3. Si módulos LANE redundantes son usados para accesar al server farm, la tabla LANE LE-ARP (conteniendo el mapeo de direcciones MAC a direcciones NSAP ATM) también necesita ser actualizado. Cuando encaramos con este tema, podríamos ser forzados a deshabilitar el PortFast, el cual provocaría que se habilite STP y por consiguiente introducir los retardos que el protocolo trae por defecto. Lo peor de este retardo es que, dispara un mensaje de cambio de topología LANE y fuerza a que las tablas LE-ARP se actualicen. Obviamente, los NICs redundantes deberían ser cuidadosamente planeados y probados antes de que un fallta de red ocurra.

Use VLAN Asegurados en Server Farm.- Cisco está desarrollando un nuevo modelo de VLAN para proveer una simple pero efectiva seguridad para aplicaciones tales como grandes server farms. Bajo esta carácterística, uno o mas puertos son configurados en cada uno de los switches usados para directamente enlazar los servidores a uno o mas gateways por defecto. Estos puertos soportan accesos por dos caminos hacia todos los servers dentro de la VLAN. Sin embargo, otros puertos dentro de la VLAN designada

como acceso o puertos de servidor no pueden comunicarse con cada uno de ellos. Esto crea un ambiente fácil de administrar donde los servidores tienen completa comunicación con el backbone/core de red pero con ningun riesgo de comunicación de los servidores con los otros. Esta característica sería extremadamente usual en situaciones tales como Internet Service Provider (ISP), facilidades de web hosting donde la comunicación entre los servidores de difernetes clientes tienen que estar tightly. Controlados. Generalmente la solución mas temprana envolvió creando cientos de pequeños VLANs y subnets IP,

7.4.- DISEÑO DE RED TCP/IP CAMPUS-LAN

Una red física es definida con referencia a conceptos dee capa 2, algunas veces como un simple dominio de colisión o ancho de banda, mas frecuentemente como un dominio de broadcast.

Una red lógica es definido con referencia a conceptos de capa 3, siempre envolviendo un número de red asignado para o overlaid en una red física. La numeración de la red lógica es por supuesto, protocolo específico.

En general, uno o mas números de red lógicos pueden ser asignados a una red física. La informaciónd e enrutamiento esntre las redes relies en red y nodos seiendo apropiadamente configurados con direcciones de capa 3 inteligible.

7.4.1.- Elección de la Dirección

En este capítulo discutiremos las direcciones jerarquicas, enrutamiento prefijado, direccionamiento classless, y máscara de subred de longitud variable (VLSM). Estos no son conceptos nuevos; Por ejemplo, el sistyema telefónico ha manipulado prefijos ded enrutamiento por muchos años. Un switch telefónico en Lima no necesita saber como alcanzar una línea en Huancayo. Sólo necesita reconocer que la llamada no es local. Un carrier de larga distancia necesita reconocer que el 001 es el código de área de EE.UU., pero no necesita saber el detalle de cómo llegar a la línea específica de los EE.UU.

Este capítulo mostrará que los prefijos de enrutamiento no es nuevo en el ambiente IP. Un router necesita conocer únicamente como llegar al próximo hop. Este no necesita saber el detalle de cómo llegar el nodo final que no es local.

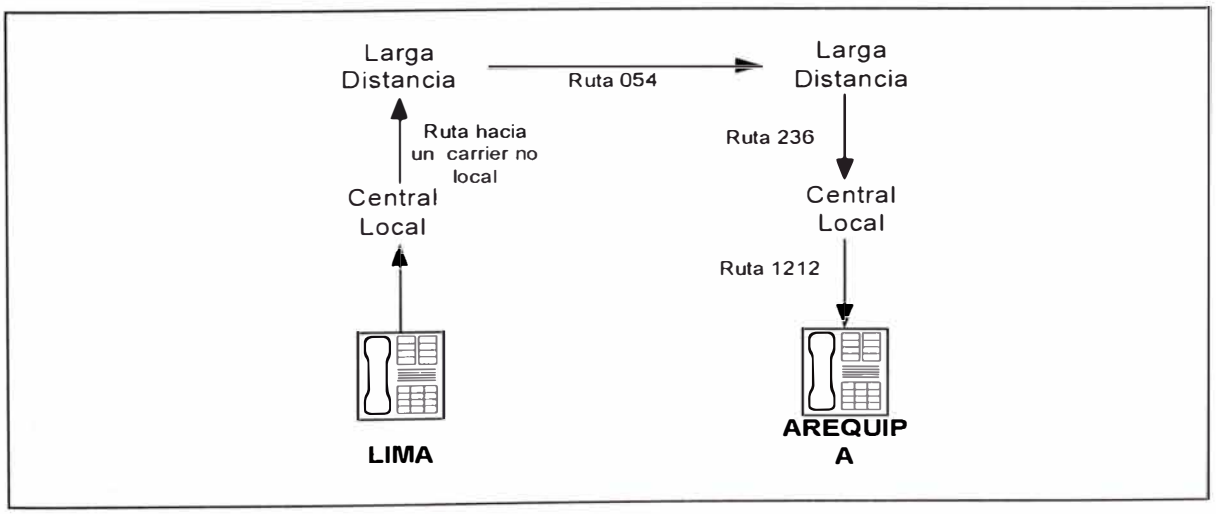


Figura 7-26 Un switch telefónico de Lima no sabe como alcanzar a una línea específica en Arequipa (054 236-1212)

La figura 7-26, muestra un ejemplo de cómo los sistemas telefónicos alcanzan las líneas específicas en Perú. La especificación original IP, RFCC 760, no usó classes. El número de red fue definido como el primer octeto. El primer octeto fue un prefijo. El direccionamiento classsfull fue introducido cuendo mas que 254 redes threatened a colapsar el internet. Direccionamiento Classful es especificado en el RFC 791, el cual es usualmente considerado la especificación IP estándar.

Los tres direcciones IP customary classes define un prefijo dee cierta longitu:

- Una dirección de clase A tiene una longitud de prefijo de 8 bits.
- Una dirección de clase B tiene una longitud de prefijo de 16 bits
- Una dirección de clase C tiene una longitud de prefijo de 24 bits.

Una mascara de subred es simplemente una forma de ubicar n bits de una dirección de 32 bits como identificador de número de red y 32-n es un identificador de número de dispositivo. La longiutud de prefijo variados even antes de la mascara dee subred fueron introducidos. La longitud del prefijo usado para ser determinado por el los pocos primeros bits en una dirección, el cual identifica la clase de dirección son:

- Una dirección de clase A siempre empieza con un patrón de bits 0
- Una dirección de clase B siempre empieza con un patrón de bits 10
- Una dirección de clase A siempre empieza con un patrón de bits 110

Los "host IP" tradicionales conocieron únicamente tres longitudes de prefijos: 8, 16 y 24 bits. Cuando las subredes fueron introducidos, un "host" (o router) podría ser configurado para entender que la longitud del prefijo local fue extendido por el uso de una mascara de subred. En el ejemplo, una red de Clase B (el cual normalmente usa 16 bits para designar el número de red) ha extendido su máscara de subred a un adicional de 7 bits. Esta extensión permite a la red de clase B a ser dividido dentro de 126 subredes individuales. El costo de esta extensión es que el máximo número de nodos en cada una de las subredes es limitado a 510.

Los "Hosts" tienen una limitada habilidad para entender las longitudes prefijadas. Ellos conocen la longitud para las configuraciones locales pero no para las configuraciones remotas. El enrutamiento "classful" tradicional no transmitía ninguna información referente a las longitudes prefijadas, las cuales podrían ser calculadas desde los primeros pocos bits de una dirección "IP classsful". Los protocolos de enrutamiento "classful" como RIP, e IGRP, requieren que una máscara de subred consistente sea desarrollado a través de la red mayor. La máscara seleccionada, obtenida al extender la frontera de la máscara "classful", debería permitir suficientes direcciones de dispositivos "hosts" que reflejan una subred de tamaño promedio. La figura 7-27 mostrada a continuación muestra una red "subneteada" con extensión de prefijos a la derecha.

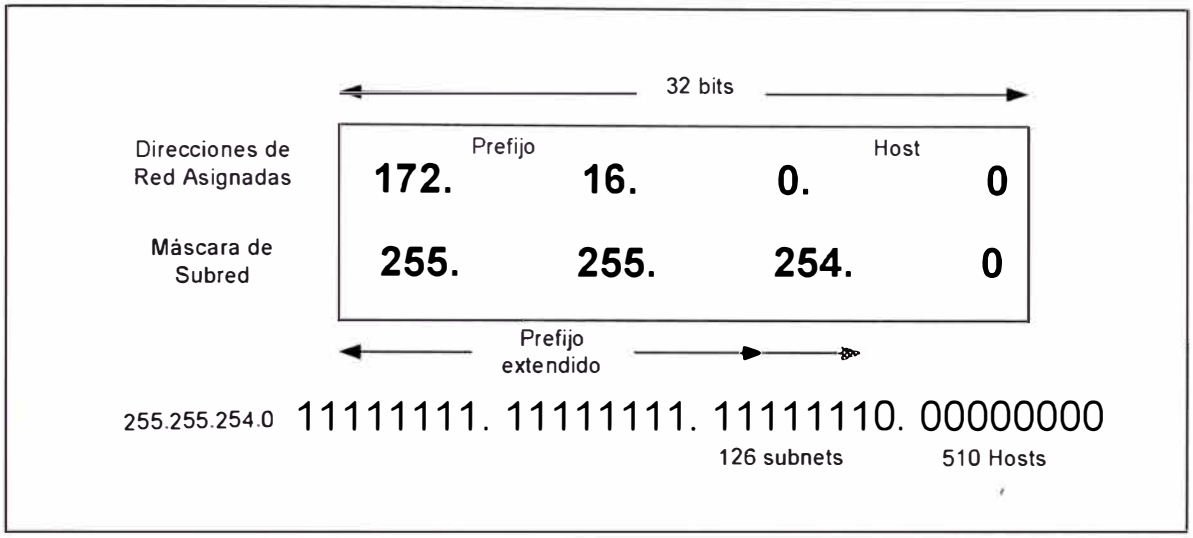


Figura 7-27 El Subnetting extiende el prefijo a la derecha.

Los protocolos de enrutamiento Distan Vector Estándar, tales como RIP e IGRP, no advierten mascara de subred en los updates de protocolo de enrutamiento. Estos protocolos de enrutamiento llevan a cabo sumarización de rutas en la boundary de la red mayor. Si las subredes mayores en una red viene a ser separado por otra red, la característica de sumarización automática causa que las subredes mayores llegara a ser discontinuas. Los dispositivos en la red separando las subredes mayores discontinuas pueden llegar a se confundidas debido a las advertencias de conflicto acerca de la misma red de destino recibida en interfaces diferentes.

Tunneling y direccionamiwento secundario puede efectivamente conectar subredes discontinuas, pero este diseño es ineficiente y negativamente impacta en la performacia. Estas soluciones incrementarías el overhead de la red, degradaría el throughput, y consumirían memoria y los recursos del CPU. La figura 7-28 a continuación nos detalla los conflictos en

una red donde los protocolos dee enrutamiento clasful no advierten prefijos extendidos..

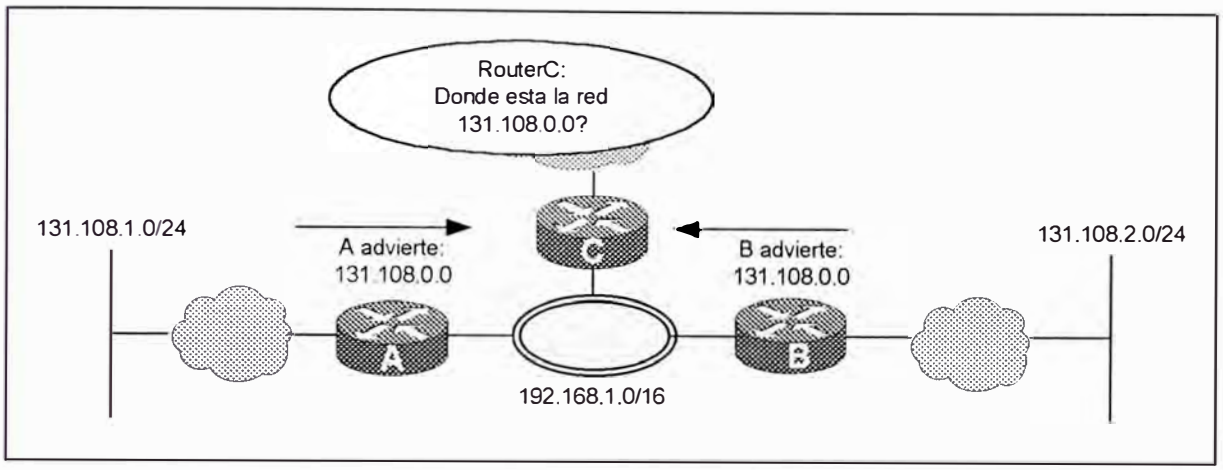


Figura 7-28 Los Protocolos Classful no advierten los prefijos extendidos.

El Protocolo de enrutamiento Link-State e Híbrido advierten máscara de subred cuando sus proceso intercambian información de tabla de enrutamiento. Los protocolos mejorados pueden interpretar las diferencias en mascara de subred; este concepto es conocido como VLSM.

VLSM relies en proveer información de longitud de prefijo explícitamente con cada uso de una dirección. La longitud del prefijo es evaluado independientemente en cada lugar que este es usado. Este método realmente no es diferente que el enrutamiento tradicional, donde una mascara de subred dentro de una red es hidden desde las interredes exteriores.

La habilidad para tener una longitud prefija diferente en diferentes puntos soporta mayor uso eficiente del espacio de la dirección IP

y reduce el tráfico de enrutamiento. La habilidad para usar diferentes mascaras de subred en diferentes ubicaciones en la red le permite al diseñador Taylor la ubicación de direccionamiento hacia la densidad de host requerido para cada subred. Enhanced IGRP, ISO´s, IS-IS, OSPF, y RIPV2 soportan diseño VLSM.

El Protocolo de enrutamiento Link-State e Híbrido manipulan subredes discontinuas mas fácilmente que los protocolos de enrutamiento classful. Enhanced IGRP puedee requerir adicional configuración para soportar subredes discontinuas. Enhanced IGRP por defecto es sumarizado en las boundaries de la red mayor, pero esta característica de auto-sumarize es una característica de protocolo de enrutamiento classless.

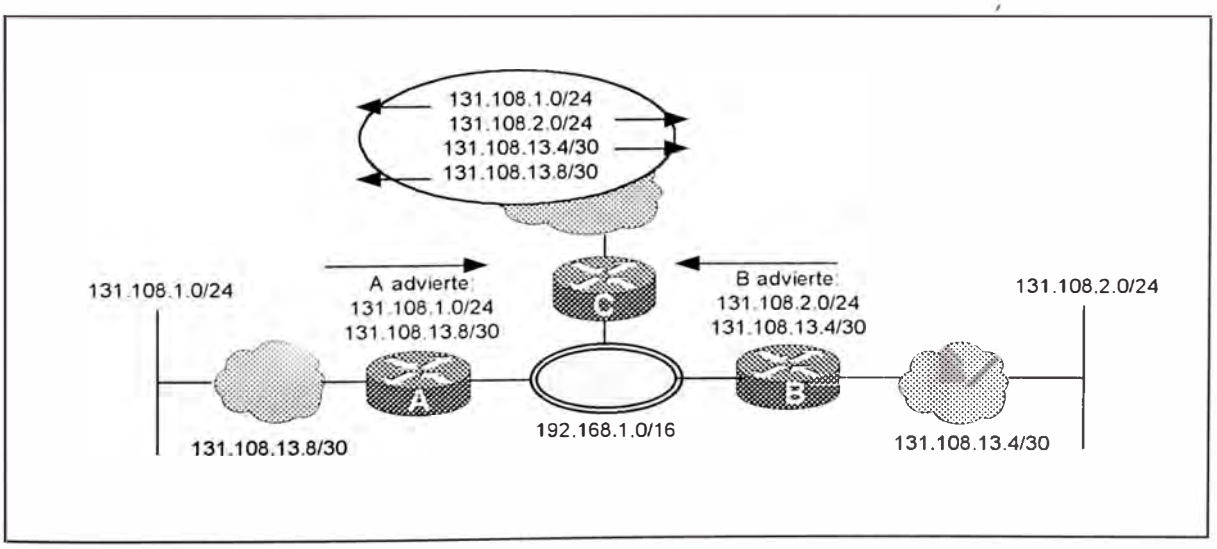


Figura 7-29 Los Protocolos Classless permiten direccionamiento flexible.

VLSM son típicamente usados para numerar líneas seriales. Cada linea serial necesita un numero de subred distinto, aunque cada línea

serial tiene únicamente dos direcciones de host. Este requerimiento gasta números de subred que son muy scarce bajo subnetting classful.

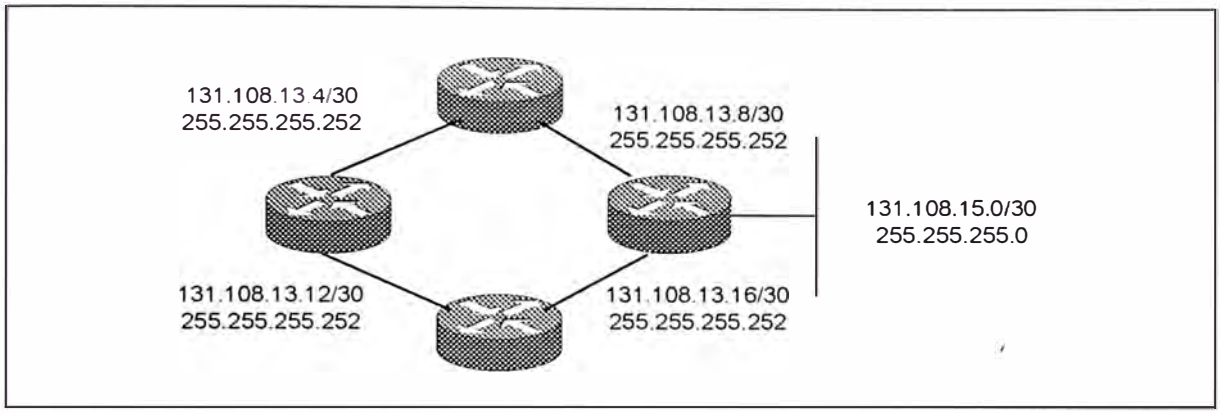


Figura 7-30 VLSM ahorra subnets en una red WAN.

En la grafica, VLSM es usado para numerar todos los enlaces seriales en el core,. Los subnets regulares 131.108.13.0 es further subnetted con seis bits adicionales. Los seis bits de subred adicinales hacen 62 subredes adicionales disponibles, cada uno capaz de soportar hasta dos host. Poir ejemplo, 131.108.13.0 es una subred válido con dos direcciones de host válidos. La ruta agregada para todos las subredes en el core es 131.108.13.0

La sumarización ded ruta es también llamado agregación o supernetting. La sumarizacion de rutas se refiere a ubicar multiples direcciones IP en una forma que permita agregación de multiples redes dentro de un número mas pequeño de tabla de entrada de enrutamiento. La sumarización reduce uso de memoria en routers y tráfico de red en protocolos de enrutamiento. La sumarización es descrito en RFC 1518. El

Classless Interdomain Routing (CIDR) es unoa aplicación de sumarización de rutas.

- Para que la sumarización treabaje correctamente, los siguientes requerimientos tiene que ser encontrados:
- Múltiples direcciones IP tiene que compartir el mismo bits de orden mas alto.
- Las tabla de enrutamiento y protocolos tienen que basar sus descisiones de enrutamientos en una dirección IP de 32 bits con un lungitud prfija que puede ser hasta la longitud entera de 32 bits del campo.
- Los protocolos de enrutamiento tiene que llevar la longitud prefija, la mascara de subred, en un campo separado a lo largo con la dirección IP de 32 bits.

7.4.2.- Administración de Direcciones

Los Cisco routers soportan características de direccionamiento secundario. Esta característica permite que múltiples subredes IP existan fuera del mismo puerto del router. Las direcciones secundarias es mas frecuentemente requerido en un diseño de red flat donded múltiples switches interconectan estaciones finales.

Para reducir el número de task de configuraciones, usa un protocolo de asignamiento de direcciones de host dinámico, por ejemplo, el

protocolo bootstrap (BOOTP) o el protoolo de configuración de host dinámico mas nuevo (DHCP).

El re-ennumeramiento de host IP puede ser necesario para hacer mejor uso de CIDR. Para prepararse para el CIDR y otros futuros cambios de protocolos IP, hay que empezar usando asignamiento de direcciones IP dinámico.

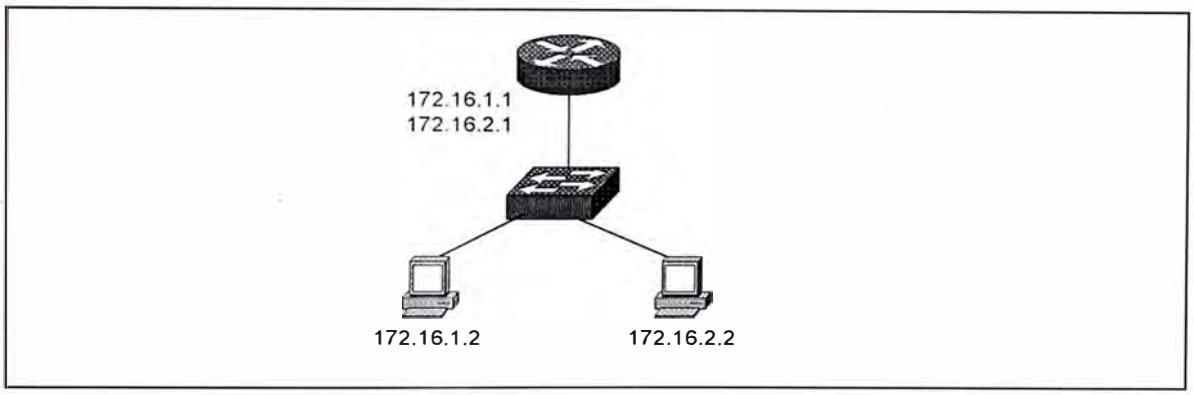


Figura 7-31 Direccionamiento secundario.

Cuando administras direcciones IP en ambientes dinámicos, puede se necesario actualizar el sevidor de nombre de dominio, después que una dirección IP sea asignada. El administrador Cisco DNS/DHCP, cumple con este requerimiento. El software puede ser desarrollado en muchas plataformas incluyendo SUN Solaris, HP-UX, IBM-AIX, Windows NT y Open VMS. El administrador DNS/DHCP es capaz de incluir administración de nombres de dominio y sincronización de direcciones IP. Múltiples subredes lógicas son soportados en la misma interface del router.

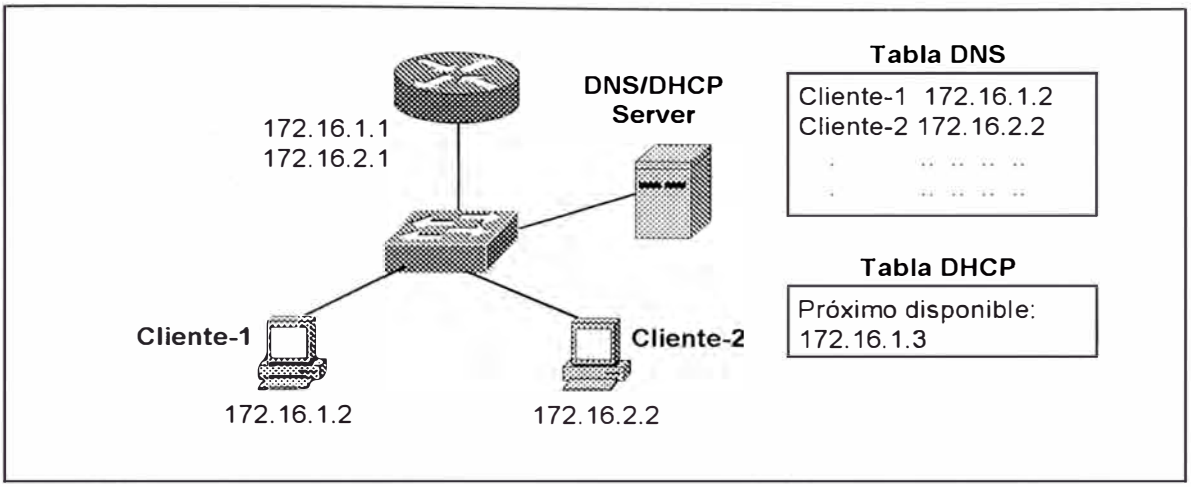


Figura 7-32 Traducción de Nombre-a-Dirección.

El Internet Assigned Numbers Authority (IANA) del InterNIC ha reservado tres bloques de direcciones para redes privadas. Un enterprice que decide usar direcciones IP desde este espacio de dirección, definido en el RFC 1918/RFC 1597, puede hacerlo también sin coordinación con la IANA o un registro de Internet. El espacio de direcciones puede así ser usado por muchas emprezas. Las direcciones dentro de este espacio de direcciones privadas son simplementes únicas dentro de la empresa. Las empresas que usas las direcciones reservadas tienen que encapsular, traducir, o proxy sus direcciones privadas dentro de direcciones únicas registradas antes de acceder a la internet pública.

Las empresas por si mismas también degusta muchos beneficios del uso de espacio de direccines privadas. Ellos gana flexibilidad en el diseño de red por tener mas espacio de direcciones en su disposal que ellos podrían obtener dedsde el pool único global, el cual hace el direcciamiento mas conveniente y habilita smoother growth path.

El Network Address Translation (NAT) es una característica que permite a los host en la red usar un esquema de dirección privada para conectar hacia y a través del Internet sin reenumerar usando un espacio de dirección público registrado. Ordinariamente, todos los host conectados al Internet requiere direcciones IP registrados globalmente únicos. Los dispositivos NAT son capaz de substituir una dirección pública registrada por uno privado no registrado en el campo de dirección fuente de un pauquete IP outbound. Una simple dirección IP registrado puede además servir como un alias para múltiples sesiones entre múltiples host en cada lado del dispositivo NAT. La característica alias permite a las redes que usan un espacio de dirección privado accesar a Internet, y mejora la seguridad de la red a la vez.

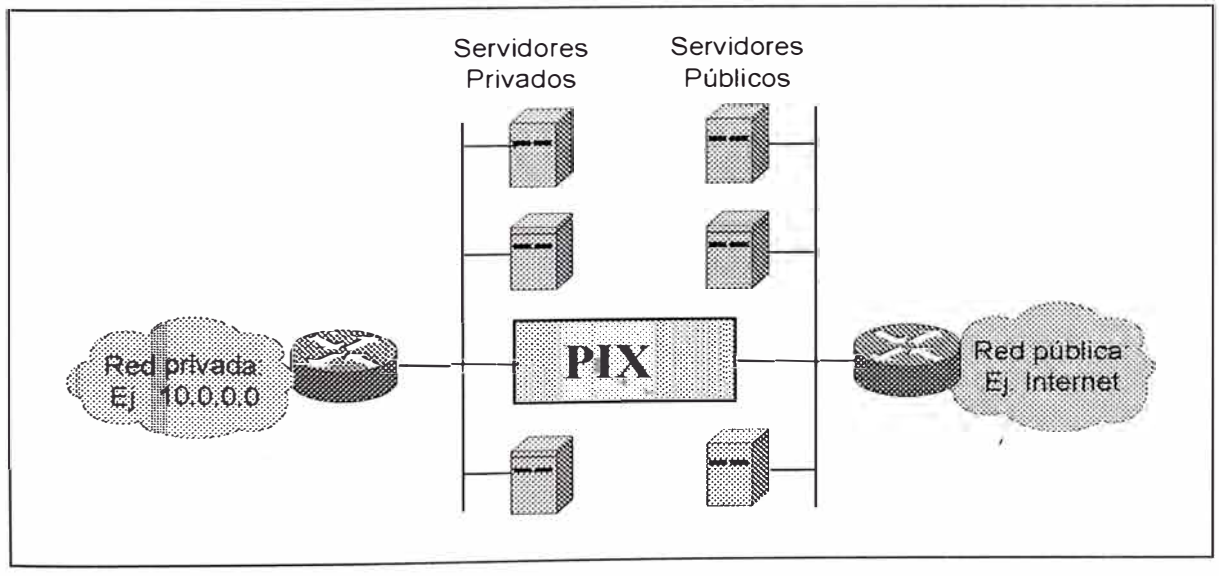


Figura 7-33 Ejemplo de un Private Internet Exchange (PIX)

7.4.3.- Direcciones Multicast

Emergiendo aplicaciones multimedia tale scomo LAN TV, collaborative computing, y dedsktop conferencing depende de la habilidad para comunicarse desde un a muchos o desde muchos a muchos host. El rising necesitado para comunicaciones multipunto presenta un interesante challenge para diseñadores de protocolos. Los protocolos de enrutamiento tradicionalmente han sido diseñado para proveer la ruta óptima desde una red a otra. El enrutamiento multipunto requiere que los routers eficientemente ubiquen la ruta a muchas redes a la vez. Las direcciones clase D es el primer paso hacia la resolución de problemas de accesar a multiples resdes simultáneamente.

Cuando una estación necesita enviar una trama a un grupio IP identificado por la dirección de clase D, la estación toma los 23 bits del orden mas bajo de las dirección de clase D y los intersecta dentro de la dirección ded destino de la capa MAC. Los 9 bits superiores de la dirección de clase D no son usados, incluyendo el 1110 que identifica una dirección como estando en la clase D.

Cuando es necesario un Multicasting en una internetwork, los routers necesitan saber si ellos deberían enviar una trama con dirección de destino dee clase D. Los routers Multicast usan el Internet Group Management Protocol (IGMP) para aprendedr si cualquier host en un segmento dado mas allá de un grupo multicast dado.

7.4.4.- Seguridad TCP/IP

Una red segura toma muchos factores en cuenta, pero en el corazón de un buen diseño es una política de seguridad que es simple y eficiente. Una vez que la política este dirigida a quien, cuando y donde, la implementación va a ser sencilla. El sistema "firewall" en el diagrama esta siendo usado como un genérico item, en vez que una simple solución. Una implementación de seguridad puede incluir productos "firewall", "bastión host", zonas desmilitarizadas, aislamiento de LANs, listas de acceso en routers y asi sucesivamente.

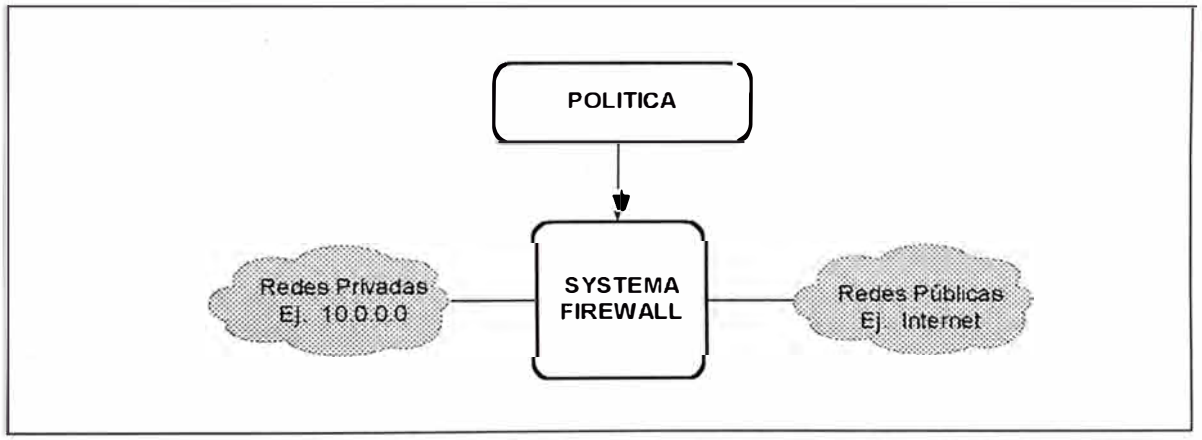


Figura 7-34 Implementando Seguridad en redes IP.

Hay pocos pasos de diseño básico que deberían ser seguidos por los especialistas responsables del diseño: la especificación, la implementación y supervisión de la instalación de sistemas de seguridad.

El primer y mas importante paso de diseño, es determinar la política de nuestra compañía u organización. Cuáles son los objetivos para los sitemas de seguridad?. Debería haber un "firewall" ubicado en el lugar

para explícitamente denegar todos los servicios excepto aquellos que son críticos para la misión de la corporación, ó sólo para auditar los accesos de red?. Hay grados de riesgos entre estas posiciones. La posición final del "firewall" será una decisión de negocios antes que una de ingeniería.

La segunda pregunta que debería ser respondida es: ¿Que monitoreo, redundancia y control se requiere?. Habiendo establecido un nivel de riesgo aceptable al resolver la primera pregunta, podemos formar una lista de qué debería ser monitoreado, permitido y denegado.

El tercer tema es financiero. Es importante intentar cuantificar cualquier propuesta de solución en términos de cuanto costaría comprar ó implementar. Un producto "firewall" completo puede costar entre 100 000.00 dólares como máximo y como mínimo. El "overhead" de la administración del sistema es también una consideración a tomar en cuenta. Es importante construir un sistema que no requiera actualizaciones constantes.

Los "firewalls" usualmente se refieren a configurar listas de control de acceso en los routers. Los "firewall" también se refieren a la topología que reducen el riesgo de accesos no requeridos, tales como el sistema de "firewall" de tres partes.

Los "firewalls" son sólo una parte del diseño de seguridad de la red. La administración de acceso se refiere a controlar los usuarios móviles

asíncronos, branch office y telecomnuter mediante el requerimiento de autorización y técnicas de autentificación. También se refiere a autentificar rutas recibidas desde routers de acceso y otros routers.

La seguridad en hosts se refiere a la seguridad física del host, cuentas de usuarios, uso de software, derechos de acceso a la data, y seguir con respeto las políticas para compartir la data del host. La encriptación puede incluir encriptación de paquetes o encriptación de data, dependiendo de si el riesgo implica hackers haciendo daños a los protocolos, o hackers cambiando la data confidencial.

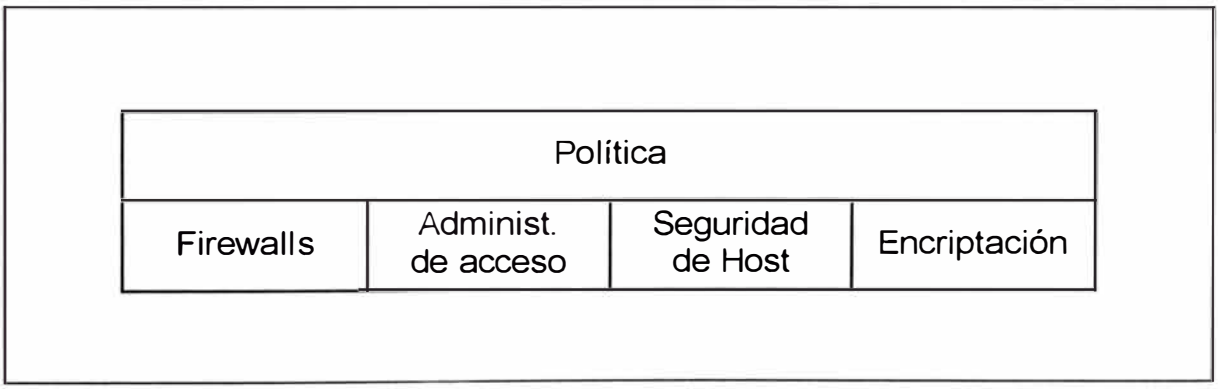


Figura 7-35 Diferentes aspectos de seguridad.

Sistema Firewall.- Dos LANs aislados provee un buffer entre la internetwork corporativa y el mundo fuera. La DMZ tiene un único número de red que es diferente del número de red corporativo . Únicamente la red DMZ es visible al mundo exterior.

Los servicios disponibles en el mundo exterior son ubicados en el DMZ, por ejemplo:

- Servidores FTP anónimos
- Servidores Wide World Web (WWW)
- Domain Name Service (DNS)
- Telnet

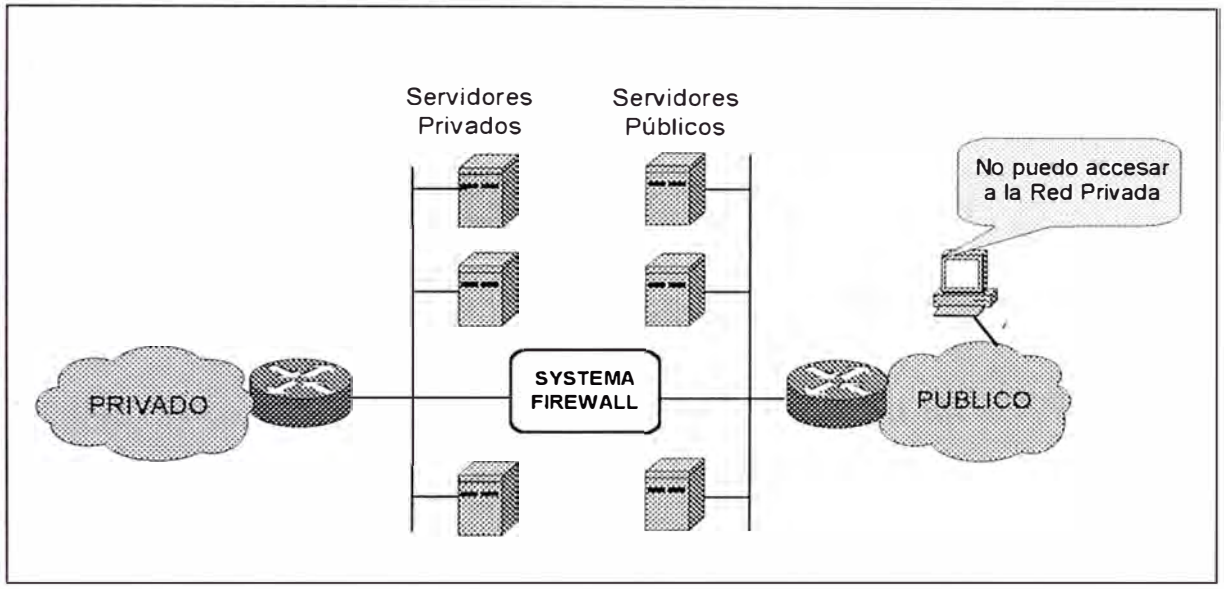


Figura 7-36 Sistemas Firewall con LANs aislados.

Los sistemas firewall varían en sus capacidades. Algunos funcionalidades adicionales buscado en un firewall incluye:

- Traducción de dirección de red: Substituye direcciones públicas por direcciones privadas
- Aplicaciones Proxy: Provee fuente centralizada para acceso de aplicaciones.
- Filtro de paquetes: Examina paquetes para verificar campos de seguridad.
- audit. Trails: Mantiene conteo de estadísticas para uso.

- Login Protección: Provee seguridad adicional con una capa externa de passwords.

Filtrando Protocolos en el Firewall.- El router outside filter sebería ser tan simple como sea posible. No permitir conexiones a este. No habilitar cualquier servicio innecesario:

Una lista de sugerencias para los routers de filtrado exterior incluyen:

- Deshabilitar el acceso a Telnet (nada de terminales virtuales definidos)
- Usar únicamente rutas estáticas
- No hacer de esto un servidor TFTP
- Usar encriptación de password
- Deshabilitar servicios ARP de proxy
- Deshabilitar servicios finger
- Deshabilitar IP redirects
- Deshabilitar IP route caching
- No haccer de esto un aservidor MOP
- No hacer de esto un servidor MacIP

Permitir conexiones exteriores únicamente a servcios específicos en servidores específicos en el DMZ:

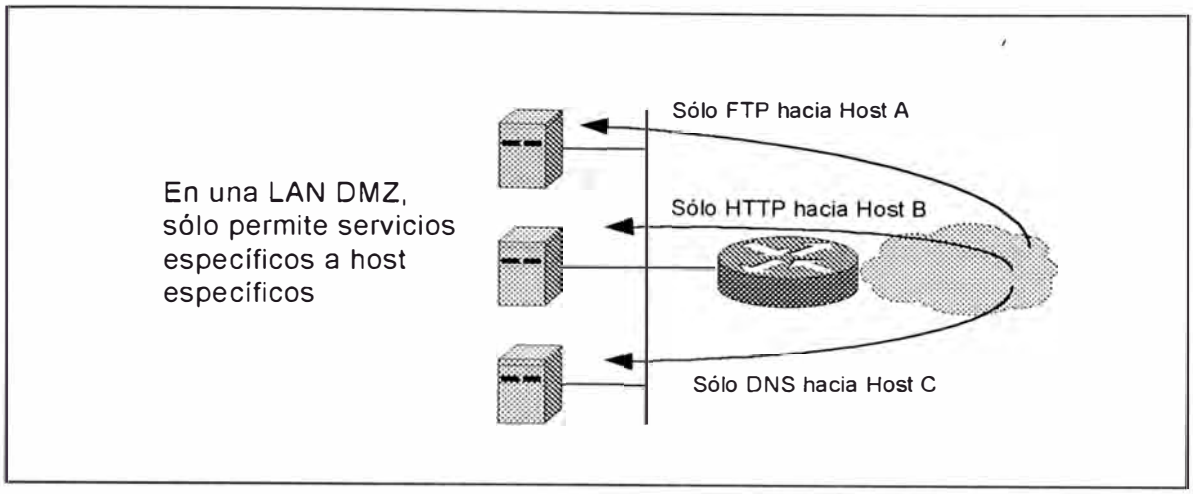


Figura 7-37 Los accesos permitidos deben ser específicos.

APLICACION	PROTOCOLO	TRANSPORTE	Nº PUERTO
E-mail	SMTP	TCP	25
Domain Name System	DNS	UDP o TCP	53
Terminal access	Telnet	TCP	23
Flie transfer	FTP	TCP	21
Flie transfer	TFTP	UDP	69
Mosaic	HTTP	TCP	83

Tabla 7-4 Las conexiones externas solo son permitidos para servicios específicos en servidores específicos en la DMZ.

Los routers firewall y los host no deberían ser automáticamente trusted por cualquier otro sistema. Los routers firewall y los host por si solos son likely a ser jumping-off point para usuarios no autorizados.

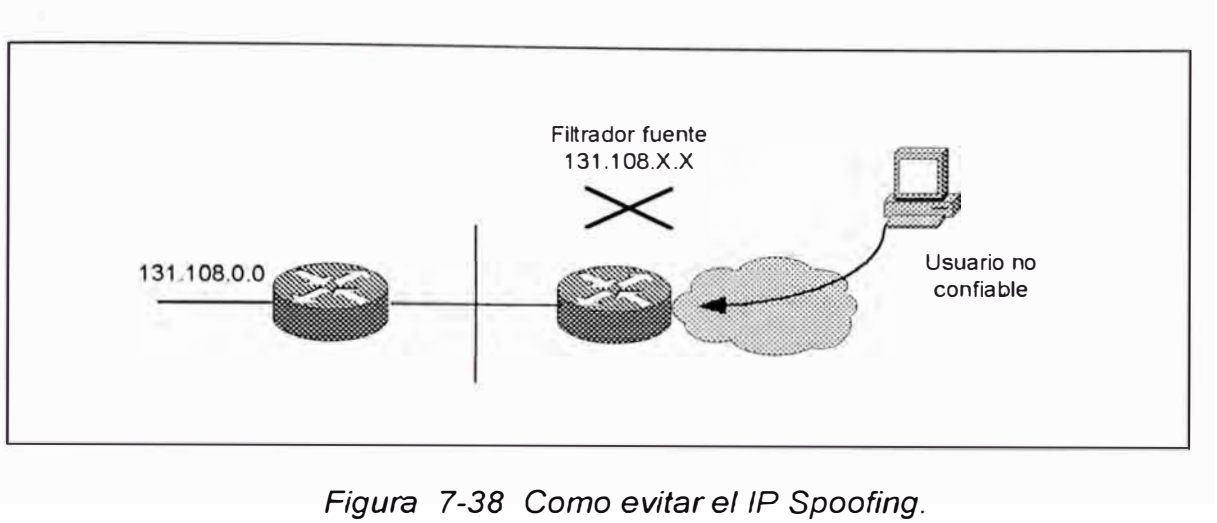


Figura 7-38 Como evitar el IP Spoofing.

La escena de esta defensa es que cualquier paquete llegando desde el exterior que claim a estar desde tu red son dropeados, therby previniendo el estilo ded ataque conocido como "IP Spoofing".

Cuando usamos dirección de fuente IP spoofing, un attacker ilegítimamente usa una dirección IP de una máquina trusted en cunjunción con un mecanismo que hace la autentificación basada en dirección. Por ejemplo, un attacker opodría usar un protocolo UNÍS remoto para spoof un host trusted. Los protocolos UNIX remotos incluyen rsh y rlogin. Estos protocolos permiten a un administrador establecer una lista de host remotos trusted de que usuarios no necesitan abastecer de un password.

Si el filtro no es configurado correctamente en el border del router, entonces los hosts exteriores pueden combinar el IP spoofing con otros métodos hacking y host compromise.

CAPÍTULO VIII

IMPLEMENTANADO LA RED CAMPUS-LAN

8.1.- ESCENARIO DE DISEÑO

HappyHome era una compañía de Telecomunicaciones Americana, que cuentaba con una red de fibra óptica en Lima Metropolitana y el Callao, sobre la cual se implementó la primera plataforma de Red ATM del Perú. En el pasado, HappyHome se ha provisto por si misma en muchas estructuras administradas descentralizadamente. La compañía ha estado dividido en cuatro locales, distribuidos por San Isidro, Miraflores, San Miguel y el Callao; cada una operando de manera autónoma. Posteriormente la Empresa HappyHome fue adquirida por la Multinacional AmericaCom,

AmericaCom es una compañía líder mundial en comunicaciones de voz, video y datos, que sirve a mas 80 millones dee clientes residenciales, corporativos y gubernamenltales. Con ingresos superiores a los US$67.000 millones de dólares y 165,000 empleados, la Compañía desarrolla sus actividades en mas ded 280 países y territorios de todo el mundo.

En Noviembre de 1999, AmericaCom, anunció sus planes dee formar AmericaCom Latin America, fusionando operaciones con Netstream en Brasil, HappyHome en Chile, Colombia y Perú y Keytech en Argentina, una compañía pública de telecomunicaciones de intercambio local competitivo con operaciones en Chile, Colombia y perú. América Com LA tiene su sede en Coral Gables, Florida. En nuestro país, las operaciones de AmericaCoim LA se inicia con la fusión de HapyyHomeSA, con una inversión de 200 millones de dólares.

AmericaCom brinda servicio de voz como son: La Larga Distacia Nacional e Internacional. Medio por el cual un abonado de telefonía fija tiene acceso para realizar sus llamadas de larga distancia nacional e internacional, mediante el portador de larga distancia seleccionado por presuscripción o preselección (contrato de servicios), de acuerdo a la resolución de OSIPTEL; Telefonía Fija. Proveerá a los clientes empresariales que cuentes o tengan acceso a una PBX (central telefónica), el servicio de telefonía local y para el inicio y terminación de las llamadas, el mismo que operarás sobre fibra óptica a través de una única conexión que permite disfrutar a la vez de todas las necesidades de comunicación. Servicios de Transmisión de datos, voz y video – IP Data Servcie – que permite interconectar una empresa con sus sucursales, clientes o proveedores mediante un enlace de fibra óptica que opera sobre una plataforma multiservicios con tecnología ATM (tecnología de conmutación de alta velocidad basada en celdas de longitud fija que permite manejar voz,

datos y video sobre un mismo medio físico). Servicio de Internet como : Acceso dedicado. Es la conexión por la cual la Red Interna de una empresa tiene acceso permanente a Internet (las 24 horas, los 365 días del año), con un costo o tarifa mensual, sin la utilización de una línea o módem telefónico. Los usuarios de líneas dedicadas son básicamente empresas y organizaciones que necesitan conectarse a Internet a altas velocidades. Virtual ISP – Dial Up, provee a los clientes con toda la infraestructura necesaria para que a su vez provean dial up Internet Access a sus clientes..

Ante el crecimiento organizacional de la compañía AmericaCom, la alta dirección descidió que sse debería adquirir una oficina centralizada para una mejor administración. Como resultado de esto, los cuatro locales serían reubicados en una Oficina Central Corporativa ubicado en el distrito de Miraflores.

Actualmente, el campus de AmericaCom consta de un edificio corporativo donde esta ubicada la parte Administrativa y un edificio de datos, donde se encuentran los servidores de red y servidores ISP (Internet Service Provider).

La Sede Corporativa está distribuido a través de 6 pisos y un zótano para el almacenamiento de los equipos de red, temperatura y sistema de tuberías. En el piso 1 se encuentran ubicado la Vicepresidencia de Productos y Servicios y Ventas Ciorporativas; en el piso 2 piso se

encuentran ubicado la Vicepresidencia de Customer Care y Call Center; en el piso 3 esta ubicado la Vicepresidencia de Ingeniería y Recursos Humanos y Seguridad; en el piso 4 se encuentra ubicado la Vicepresidencia de Inromation Technology y Operaciones; en el piso 5 se encuentra la Vicepresidencia de Contratloría , Tesorería y facturación y Logística y Administración y Finanzas, en el piso 6 se encuentra la Vicepresidencia de Legal e Imagen Institucional y Gerencia General.

La Sede Remota de San Isidro está distribuido en dos pisos. El primer piso estan ubicados los servidores de la red corporativa, los servidores ISP y los servidores de Base de Datos; en esta sede esta ubicada la Dirección de Internet Service Provider (ISP).

Adicionalmente, siendo AmericaCom un carrier que cuenta con una Red ATM en Lima Metropolitana, no necesita un proveedor externo para sus comunicaciones WAN. Por lo tanto, las comunicaciones WAN entre las oficinas serán a través de la Red propia de AmericaCom.

8.1.1.- Requerimientos

Los requerimientos técnicos principales son:

- Acceso de alta velocidad a los diversos aplicativos y a los servidores de la red corporativa. Para el caso del Edificio Corporativo, el accesso a los servidores será de tipo local, y para las sede remota, el acceso se realizará a través de la conexión WAN.

- En la tabla 8-1 adjunta detallamos la cantidad de usuarios en cada uno de los pisos, los cuales efectuarán consultas locales a los Servidores con una confiabilidad adecuada.

DEPENDENCIAS DE LA RED CORPORATIVA EDIFICIO COROPORATIVO

ITEM	SITE	DEPENDENCIAS	USUARIOS	DISPONIBILIDAD
1	PISO 6	LEGAL, GER. GENERAL, IMAGEN INSTITUCIONAL	60	100%
2	PISO 5	CONTRALORIA, TESORERIA,FACTURACION, LOGISTICA, ADMINSITRACION, FINANZAS, PRE SELECCIÓN	140	100%
3	PISO 4	OPERACIONES, INFORMATION TECHONOLOGY Y NOC	150	95%
4	PISO 3	SEGURIDAD, RECURSOS HUMANOS, INGENIERA, SALA USO MULTIPLES	75	90%
5	PISO 2	VENTAS, CUSTOMER CARE, CALL CENTER	140	100%
6	PISO 1	PRODUCTOS Y SERVICIOS, VENTAS CORPORATIVAS	120	95%

Tabla 8-1 Distribución de usuarios por piso – Sede Principal

Para el caso de las sede remota con conexión de acceso WAN se muestra también un cuadro que muestra a la cantidad de usuarios y la disponibilidad que deberán tener cada uno de ellos.

ITEM	SITE	DEPENDENCIAS	USUARIOS	DISPONIBILIDAD
1	S. J. MIRAFLORES	TELEFONIA LARGA DISTANCIA INTERNACIONAL, NACIONAL, TRANSMISIONES	40	100%
2	SAN ISDRO	INFORMATION TECHNOLOGIES (IT) E INTERNET SERVICE PROVIDER (ISP)	37	95%

Tabla 8-2 Distribución de usuarios por piso – Sedes Remotas

- El Acceso a los Servidores debe realizarse de manera rápida y confiable, dado que en los mismos se almacenan los recursos de operación y de información de la Compañía. Por lo tanto el requerimiento de acceso a los servidores será diseñado de la manera mas optima, y con la redundancia correspondiente.
- La Videoconferencia entre locales, deberán permitir efectuar sesiones tripartitas y tener acceso a usuarios externos en el futuro.

- La comunicación telefónica entre locales, deberá ser diseñado con los equipos adecuados para el transporte de los canales de comunicación voz.
- Un plan de cableado estructurado de última generación deberá instalarse, para que soporte las trasmisiones de voz, video y datos por el mismo medio y este preparada para las nuevas tecnologías por venir como son Video en completo movimiento, audio digitalizado, imagen de alta definición, etc.
- Todo tráfico ip no es filtrado, por lo que debería de haber una política de seguridad de red para permitir un adecuado desarrollo de las aplicaciones.
- La red deberá presentar un Acceso universal a Internet, una adecuada política de seguridad, una dirección e-mail, una base de datos consistente y una red moderna, simple y que sea capaz de adaptarse a creciemiento futuro.

Los requerimientos administrativos son los que se menciona a continuación:

- Después del trabajo de implementación de la red corporativa, el sistema deberá ser administrado por un mínimo staff de personal.
- Se brindará capacitación al personal a cargo de la administración.
- La expansión global podría crear nuevos temas culturales, de lenguaje y entrenamiento a tratar.
- Una política de seguridad y un manager de seguridad de red es requerido.

- Debido a la estrategia de adquisición agresiva de la compañía, el tamaño de la red podría tomar un tamaño mas grande al asimilar o incorporar otras redes.
- Las actividades de cada área serán desarrolladas dentro de su grupo, es decir, el intercambio de información del área de Administración al área de Ingeniería no deberá efectuarse.

8.1.2.- Descripción Técnica de la Solución LAN y WAN

La solución global contiene los siguientes elementos, que a continuación se describen:

- Debido a que la implementación de la red LAN utilizará tegnologías de punta como Fast Ethernet y Gigabit Ethernet y teniendo presente que la tecnología está continuamente cambiando. Se tomaron las consideraciones pertinentes para el dimensionamiento y selección del medio físico que conectará las estaciones de trabajo, los switches IDF´s y los switches MDF´s, en la sede principal y las sedes Remotas. Es así que se eligió la solución del sistema de cableado estructurado horizontal Categoría 6 "INTEGRITY" de Panduit, como resultado de una licitación. Esta solución Integrity es ideal para uso en altos anchos de banda y aplicaciones compartidas mas alla de los 100MHz. Soporta aplicaciones actuales tales como 4/126 Mbps Token Ring, 10 Base T, 100 Base TX, 100 Base VG AnyLan, 155 ATM y las aplicaciones mas nuevas como 622 ATM y Gigabit Ethernet; Aplicaciones multimedia de pares trensados de línea balanceada

incluye audio analógico, audio digital AES/EBU y control de máquinas RS-442 y video digital con el uso de baluns para convertir de coaxial a formato par trensado. Y la solución del cableado vertical a utilizarse será el tipo "Backbone Colapsado", por la facilidad que tiene esta topología para acomodar y manipular la tecnología VLAN. Se utilizará para el medio físico del cableado vertical la solución IntegrityF que consta con de cables fibra óptica multimodo 62/125 um, las cuales conectaran el MDF con cada uno de los IDF´s ubicadoas en cada piso en la sede principal. Esta solución es ideal para aplicaciones de alta velocidades donde la distancia, el ruido y la seguridad son un tema bastante delicado. Soporta Aplicacines como 4/16 Mbps Token Ring, 10 Base FLK, 100 Base FX, FDDI, ATM, SONET y aplicaciones nuevas como Gigabit Ethernet, y soporta video broadband y baseband.

- De los tres modelos de diseño LAN Campus existentes, se eligió el Modelo Multilayer, por las muchas ventajas que nos proporciona, las cuales han sido explicadas detalladamente en capitulos anteriores. Además por que nos permite gozar de los beneficios del modelo jerárquico como son: La escalabilidad, la implementación fácil, el diagnóstico oportuno, la predictibilidad, el soporte de protocolos y la administrabilidad.

El diseño LAN presenta las siguientes características.

1. Para la implementación de la red Campus LAN se utilizará la tegnología Fast Ethernet y Gigabit Ethernet, incrementando el ancho de banda hasta 100 Mbps usando la tegnología existente CSMA/CD y nuevas tecnologías de switching capa 2 y capa 3 como VLAN´s, MLS y otros. Se tomaron las consideraciones necesarias y pertinentes para el dimensionamiento de los equipos, con datos obtenidos de las proyecciones en crecimiento de las diferentes áreas con un estimado al año siguiente.
2. Teniendo presente el Modelo Multilayer , los swtches a utilizarse en la capa de acceso serán switches capa 2 marca Cisco modelo Serie 3500 de 48 o 24 puertos de acuerdo a la densidad de usuarios por piso. En la capa de distribución serán switches capa 3 marca Cisco modelo Serie 6500 y 8500 con características de Gigabit Ethernet, la cual manipulará todo el enrutamiento VLAN para la red campus; y en la capa core, utilizaremos los switches ATM propios de la Red Metropolitana de AmericaCom.
3. Entre los dos switches capa 3 se habilitará H.S.R.P. que proveerá redundancia a los usuarios VLAN. Aproximadamente una mitad de los subnets (VLANs) sería ruteados por un switch capa 3 y la otra mitad ded los subnets sería ruteado por el otro switch capa 3. Si uno falla, el H.S.R.P. permitiría al otro switch tomar todo el trafico de las VLANs. En operación

normal, la carga de enrutamiento sería fuertemente balanceado entre los dos.

4. El Tráfico de datos será orientado para un manejo local con capacidades de switch hasta el nivel IP. Lo cual permite la facilidad de switching VLANS de dependencias especificas. Este tráfico pesado se manejará en un 80% en la LAN de la RED Campus, logrando que el tráfico de datos externo de entrada o salida sea únicamente para requerimientos WAN, la cual evitará el fenómeno de cuello de botella a la salida, así como también nos brindará protección ante cualquier intento de violación de la privacidad de la Empresa.
5. Los switches IDF´s del backbone en cada piso de las sedes, tendrán enlaces redundantes de 100 Mbps Ethernet hacia el switch MDF. Ciomo regla general, todos los clientesa Ethernet tendrán 10 Mbps al desktop.Además se proveerá de redundancia de switch MDF, para obtener disponibilidad al 100%.
6. Se dispondrá así mismo de dos Routers de Borde en la sede principal, que solo manejará tráfico de requerimiento de acceso WAN. Estos routers serían conectados a los dos swirches capa 3 (8500 y 6500) con enlaces Ethernet.
7. Los servidores serán ubicados en un lugar centralizado llamado "Centralized Server Farm" lo cual permite un mejor soporte y administración. Para el acceso a los Servidores, se

está considerando la utilización de un par de Fibras Oscuras monomodo con su redundancia por rutas distintas desde la sede Principal. Esto nos permite garantizar la operación de los servidores con una confiabilidad del 100%.

8. El Switch ubicado en el Server Farm para efectos de conexión con los servidores de Information Technologies, tendrá conexiones Giga Ethernet en una cantidad máxima de 7. Quedando además disponibles 24 puertos para conexiones 10/100 BaseT. Para un mayor número de conexiones de acceso Giga Ethernet se debe de adquirir adicionalmente un Switch y sus módulos correspondientes.
9. El acceso a Internet será realizado a traves del router 7206, ubicado en el MDF de la sede principal , mediante una conexión PVC al router de borde.

- Para cumplir con los requerimientos, la implementación de la red WAN debe caracterirarze por la confiabilidad del enlace. La WAN es frecuentemente el Backbone de una Red. Los recursos WAN son muy caros, sin embargo, el diseño de la Red WAN será completamente redundante para aumentar la confiabilidad, este costo lo asumimos debido a que se desea una dispónibilidad de los enlaces al 100%. Siendo la Compañía Telecom SA, un carrier en el mercado peruano, con una red WAN instalada en todo Lima Metropolitana y el Callao,

utilizaremos su infraestructura ATM y su red de fibra óptica como Backbone de conexión entre su sede principal y las sedes remotas.

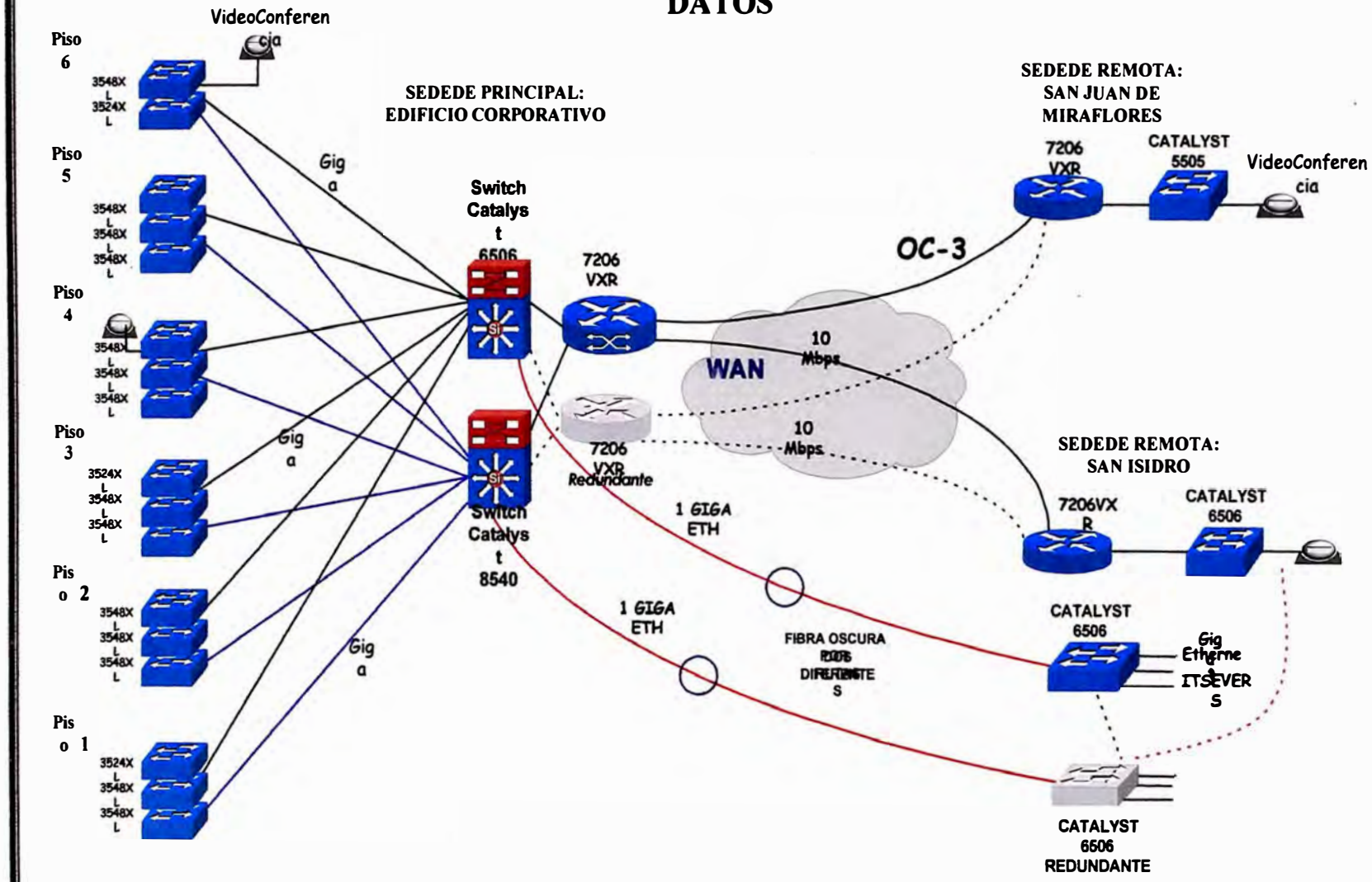
- Cuando se diseñan Redes con routers conectados a Provedores de Servicios ATM, el tema de topología es similar a los utilizados en Frame Relay. Aparecen las dos Topologías principales: NBMA (nonbroadcast multiaccess) y el Hub and Spoke, usando subinterfases. El modelo NBMA requiere pvc's en full mesh para una conectividad completa. El modelo Hub and Spoke tiene la facilidad de conectividad completa con una malla parcial. Para el caso de la Red Corporativa se utilizará la Topología Hub and Spoke, con sub-interfaces para manejar las diferentes Sedes remotas.

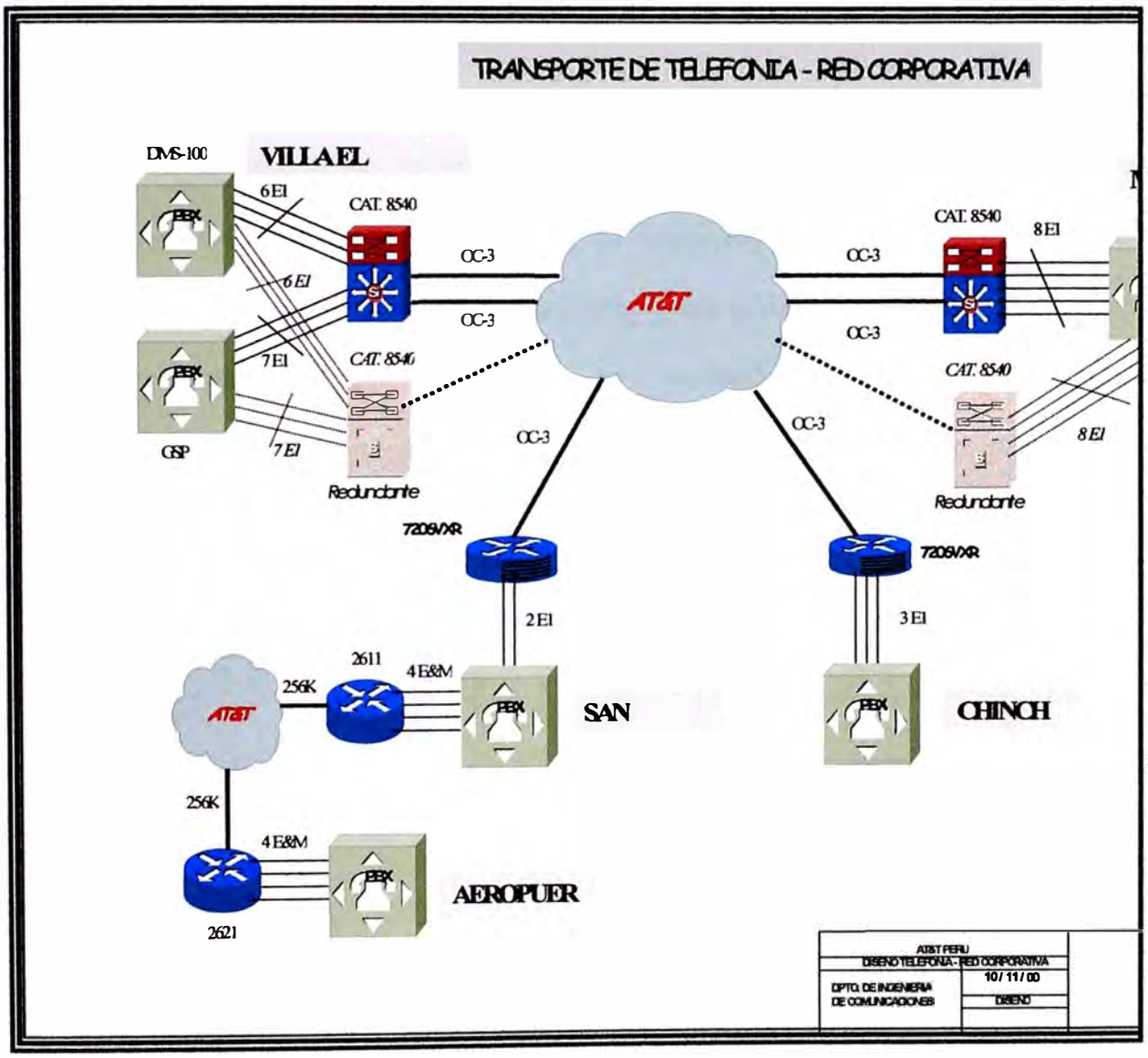
8.1.3.- Descripción Técnica de la Solución de Tlefoníia Local

Para la comunicación telefónica entre locales, debemos diseñar las cantidad de E1 necesarios para que no exista ningun problema de comunicación. Así mismo, estos E1 serán transportados por los switches MDF´s, por lo tanto este equipo a seleccionarse deberá ser capaz de manejar E1´s.

Se instalará una central Meridiam Opción 11 en la Sala de Datos en la sede Principal y la sede de Villa el Salvador, y una central Meridiam Opción 11 en la sede Remota de San Isidro. La Central en la sede Principal será conectada a través de 8 E1´s a la Central de VES. Las Central de San Isidro será conectada a través de 2 E1´s a la Central de VES.

DIAGRAMA DE LA IMPLEMENTACION DE LA RED DE DATOS




TRANSPORTE DE TELEFONIA - RED CORPORATIVA
DMS-100
VILLA EL
6 E1
CAT. 8540
6 E1
7 E1
CAT. 8540
GSP
7 E1
Redundante
OC-3
OC-3
AT&T
OC-3
OC-3
CAT. 8540
8 E1
CAT. 8540
8 E1
Redundante
OC-3
OC-3
7206VXR
7206VXR
2 E1
3 E1
2611
4 E&M
256K
AT&T
SAN
CHINCH
256K
4 E&M
2621
AEROPUER
AT&T PERU
DISEÑO TELEFONIA - RED CORPORATIVA
DPTO. DE INGENIERIA DE COMUNICACIONES
10/ 11/ 00
DISEÑO

8.2.-IMPLEMENTANDO EL SISTEMA DE CABLEADO ESTRUCTURADO

La instalación del sistema de cableado estructurado en la sede Corporativa, se realizará en 6 Plantas, con un aproximado de 880 mts2 y un promedio de 100 personas por piso. La mayoría de las personas se ubicarán en mobiliario modular de oficina. De acuerdo al primer paso de la metodología de diseño de Red, después de concretar varias reuniones con cada uno de las Vicepresidencias de la empresa, se obtuvo las necesidades finales de la cantidad de puntos de Voz, Data y Video para cada uno de las áreas que ellos presiden, las cuales se muestran en la tabla 8-3.

ITEM	PRODUCTO	CANTIDAD DE PUNTOS				TOTAL PUNTOS
		DATOS	VOZ DIG.	VOZ ANAL.	CATV	
1	PLANTA Nº 1	100	100	20	0	220
2	PLANTA Nº 2	117	151	15	2	283
3	PLANTA Nº 3	65	46	10	0	121
4	PLANTA Nº 4	159	91	14	0	264
5	PLANTA Nº 5	114	107	7	0	228
6	PLANTA Nº 6	52	46	15	2	113
					TOTAL	1,229.00

Tabla 8-3 Distribución total de puntos de por piso – Sede Principal

Así mismo se concluyó que el sistema de cableado estructurado para las oficinas se realizará completamente en Categoría 6, siendo ésta la plataforma física que soportaría todos los requermientos de ancho de banda de aplicaciones futuras.

La implementación del sistema de cableado estructurado para la oficina corporativa de AmericaCom, se realizó bajo los estándares

principales de ANSI/TIA/EIA que gobiernan el cableado de telecomunicaciones en edificios y son:

- Estándar ANSI/TIA/EIA-568-A de Alambrado de Telecomunicaciones para Edificios Comerciales, octubre 1995.
- ANSI/TIA/EIA-568-A, Adenda 1, setiembre 1997.
- ANSI/TIA/EIA-568-A, Adenda 2, agosto 1998.
- ANSI/TIA/EIA-568-A, Adenda 3, diciembre 1998.
- ANSI/TIA/EIA-568-A, Adenda 4, noviembre 1999.
- ANSI/TIA/EIA-568-A, Adenda 5, febrero 2000. Especificaciones de Rendimiento de Transmisión Adicionales para Cableado de 4 pares, 100-ohmios Categoría 5 Mejorada, Additional Transmission Performance Specifications for 4-pair 100-ohm Enhanced Category 5 Cabling.
- Estándar ANSI/TIA/EIA-569-A de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales, febrero 1998. (Incluye normativa cortafuego).
- Estándar ANSI/TIA/EIA-598-A, Codificación de Colores de Cableado de Fibra Optica, mayo 1995.
- Estándar ANSI/TIA/EIA-606 de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales, febrero 1993.
- Estándar ANSI/TIA/EIA-607 de Requerimientos de Puesta a Tierra y Puenteado de Telecomunicaciones para Edificios Comerciales, agosto 1994.

- Estándar ANSI/TIA/EIA-758 de Cableado de Planta Externa Perteneciente al Cliente, abril 1999.
- ANSI/TIA/EIA-758-1, Adendo 1, marzo 1999.
- Boletín de Sistemas Técnicos ANSI/TIA/EIA TSB-67, Especificaciones de Rendimiento de Transmisión para la Prueba en el Campo de Sistemas de Cableado de Par Torcido sin Blindaje, octúbre 1995.
- Boletín ANSI/TIA/EIA TSB-72 Guía de Cableado Centralizado de Fibra Optica, octubre 1995.
- Boletín ANSI/TIA/EIA TSB-75 Prácticas Adicionales de Cableado Horizontal para Oficinas Abiertas, agosto 1996.
- P. TIA/EIA-TSB-95, Guía de Rendimiento de Transmisión Adicionales para Cableado de 4 pares, 100-ohmios Categoría 5 Mejorada (Additional Transmission Performance Guidelines for 4-pair 100-ohm Category 5 Cabling), octubre 1999

La implementación del sistema de cableado estructurado obedece al siguiente diseño:

Se reservó espacios en cada piso del edificio, las cuales fueron destinados específicamente para ser utilizado como IDF´s del sistema de cableado estructurado. Así mismo se reservó un espacio en el sótano del edificio para ser utilizado como MDF principal. Las dimensiones de los ambientes a ser utilizado como IDF´s y MDF son los que se muestra en la tabla 8-4 a continuación.

Pisos	Dimensiones de Cuartos de Comunicaciones
Piso 1	1.7 x 2 mts
Piso 2	1.7 x 2.7 mts
Piso 3	1.8 x 2.4 mts
Piso 4	1.7 x 3.5 mts
Piso 5	1.5 x 3.9 mts
Piso 6	1.7 x 2mts
Pisos	**Dimensiones del Cuarto Central de Comunicaciones**
Sótano 1	2.9 x 5.4 mts

Tabla 8-4 Dimensines de los ambientes IDF´s – Sede Principal

Para el subsistema de cableado horizontal, cada usuario tiene como configuración normal, un circuito de voz digital, un circuito de datos, un circuito de voz analógica (sí requerido) y un punto de CATV (si requerido) por cada toma de telecomunicaciones. Tanto los circuitos de voz como la de datos, son proporcionados a través de cables que soporten la categoría 6. Los cables de voz y de datos horizontales se terminarán en los Patch Pannel Categoría 6 para montaje en bastidor de 19". Los circuitos de datos son conectados a los equipos de Telecomunicaciones dentro de cada IDF (Intermadiate Distribution Frame). Los circuitos de voz horizontales son conectados a los Patch Pannel que actúan como espejo del repartidor dentro de cada IDF.

Para el subsistema de cableado vertical, el backbone colapsado resulta en un ahorro de costo y nos da mas flexibilidad. En el backbone de datos se empleó un cable de doce fibras ópticas MM (multimodo) entre el MDF (Main Distribution Frame) y cada IDF ubicado en cada piso, y como

backbone de voz se instaló entre el MDF y cada IDF, la cantidad suficiente de cables multipar Categoría 3 para cubrir las necesidades de cada uno de los IDF. Dentro del MDF y los IDF´s de datos, los cables de fibra óptica se terminaron en bandejas deslizables de una unidad para montaje en bastidor de 19". Dentro del MDF de voz, los cables multipares se terminaron sobre PatchPannel 110 de montaje en pared y en los IDF´s de voz los multipares se terminaron sobre Patch Panel modulares RJ45 CAT 6.

8.2.1.- Instalación del Subsistema de Distribución Horizontal

El subsistema de distribución horizontal Categoría 6 obedecerá o cumplirá con los estándares de la industria tales como la ISO/IEC 11801, ANSI/TIA/EIA 568.A, 568-A-5, 569-A y 606; TIA/EIA TSB67, TSB75 y TSB95; CENELEC 50173 y CSA T529. Este subsistema de distribución horizontal consta de: Cable de distribución horizontal, área de trabajo, Closet de comunicaciones y los cables patch.

Los requisitos de performance de canal propuestos para el cableado estructurado CAT 6, deberán cumplir con los parámetros mostrados en la tabla 8-5, y cuya gráfica para cada una de las carterísticas indicadas en dicha tabla, se detalla en la figura 8-3.

FRECUEN. (MHz)	MAX. ATENUAC. (Db/100M)	MIN. NEXT (dB)	MIN. PSNEXT (dB)	MIN. ACR (dB)	MIN. PSACR (dB)	MIN. RETURN LOSS (dB)	IMPED. DE ENTRADA (ohm)	IMPEDANCIA FIJADA (ohm)	MIN ELFEXT (dB)	MIN. PSELFEXT (dB)
1	1.9	74.3	72.3	70.0	70.0	20.0	100+-12	100+-15	67.8	64.8
4	3.7	65.3	63.3	59.0	59.0	23.0	100+-12	100+-15	55.7	52.7
8	5.3	60.3	58.8	53.0	53.0	24.5	100+-12	100+-15	49.7	46.7
10	5.9	59.3	57.3	51.0	51.0	25.0	100+-12	100+-15	47.8	44.8
16	7.5	56.3	54.3	46.0	46.0	25.0	100+-12	100+-8	43.7	40.7
20	8.4	54.8	52.8	44.0	44.0	25.0	100+-12	100+-8	41.7	38.7
25	9.5	53.4	51.4	42.0	42.0	24.3	100+-15	100+-8	39.8	36.8
31.25	10.6	51.9	49.9	39.0	39.0	23.6	100+-15	100+-8	37.9	34.9
62.5	15.4	47.4	45.4	30.0	30.0	21.5	100+-15	100+-8	31.8	28.8
100	19.8	44.3	42.3	25.0	25.0	21.0	100+-15	100+-8	27.8	24.8
155	25.1	41.5	39.5	14.0	14.0	21.0	100+-15	100+-8	23.9	20.9
200	29.0	39.9	37.9	10.0	10.0	21.0	100+-15	100+-8	21.7	18.7
250	32.8	38.3	36.3	3.0	3.0	18.0	100+-20	100+-8	19.8	16.8
300	35.2	37.2	34.2	0.0	0.0	18.0	100+-20	100+-8	18.2	15.2
310	37.1	36.9	34.9	-	-	18.0	100+-20	100+-8	17.9	14.9
350	39.8	36.2	34.2	-	-	17.0	100+-22	100+-8	16.9	13.9
400	43.0	35.3	33.3	-	-	14.0	100+-32	100+-8	15.7	12.7
500	49.0	33.8	31.8	-	-	14.0	100+-32	100+-8	13.8	10.8

Tabla 8-5 Requisitos de performance de canal del Subsistema de Cableado Estructurado

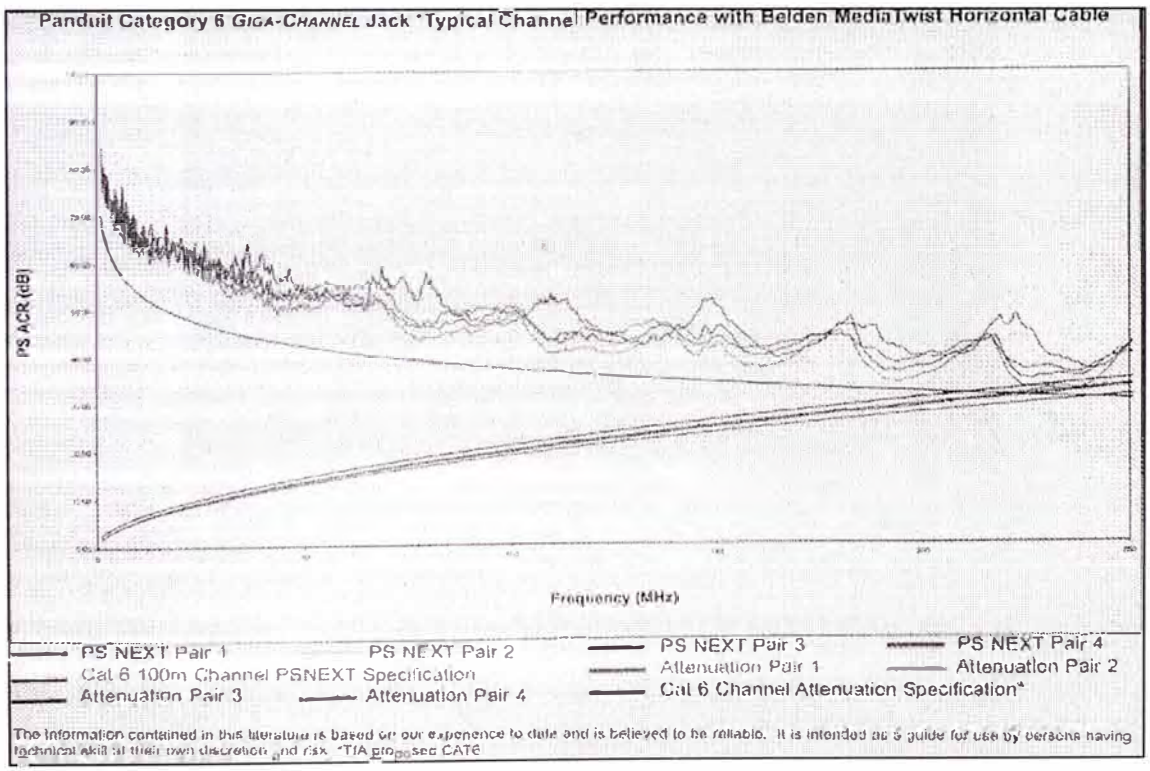


Figura 8-3 Gráfica de los requisitos de performance de canal del Subsistema de Cableado Estructurado

Cable de Distribución Horizontal.- El cable utilizado para la distribución horizontal de los circuitos de datos y voz son de Categoría 6 Media Twist Unshielded Twisted Pair de 4 pares, con número de parte 1874A, de la solución INTEGRITY de Panduit y Belden. El tipo de cable utilizado se muestra en la figura 8-4.

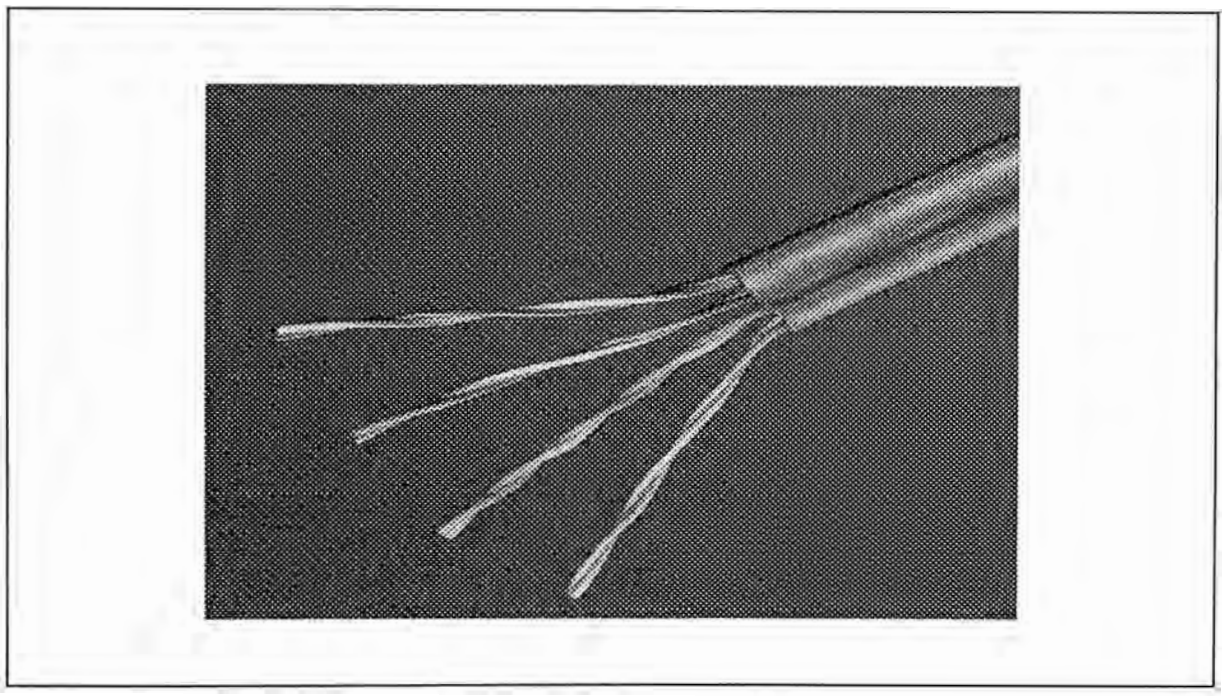


Figura 8-4 Diagrama del cable UTP 1874ª Categoría 6.

- Especificaciones Técnicas del Cable UTP: El cable UTP utilizado en la instalación del cableado horizontal, tiene las siguientes características:

    1. Conductor: 23 AWG,

        Numero de pares 4

        Numero total de conductores: 8

AWG:	23
Stranding:	Sólido
Material del conductor:	BC-Bare Koper
Diámetro del conductor :	0.022 in

2. Aislamiento:

Material de aislamiento:	FEP- Fluorinated Etylene
Diámetro del aislamiento:	0.038 in.

3. Características mecánicas:

Temeperatura de Operación:	-20 a +80 ºC
Peso del cable:	31 lb /1000ft
Tensión de inst. max:	45 lb.
Radio de curvatura min:	0.1 in

4. Características eléctricas:

Capacitancia mut. Nom. A 1KHz:	15.0 pF/ft
Capacitancia max. desbalanceado:	49.2 pF/100m
Velocidad de propagación nom.:	72%
Retardo máximo (ns/100m):	510 a 100MHz
Retardo skew max. (ns/100m):	25
Resistencia DC al conductor max.:	9 ohm/100m
Voltaje de eoperación max – UL:	300 V RMS

5. Las premisas del cable eléctrico se muestra en el cuadro adjunto :

FRECUEN. (MHz)	MAX. ATENUAC. (Db/100M)	MIN. NEXT (dB)	MIN. PSNEXT (dB)	MIN. ACR (dB)	MIN. PSACR (dB)	MIN. RETURN LOSS (dB)
1	1.9	74.3	72.3	70.0	70.0	20.0
4	3.7	65.3	63.3	59.0	59.0	23.0
8	5.3	60.3	58.8	53.0	53.0	24.5
10	5.9	59.3	57.3	51.0	51.0	25.0
16	7.5	56.3	54.3	46.0	46.0	25.0
20	8.4	54.8	52.8	44.0	44.0	25.0
25	9.5	53.4	51.4	42.0	42.0	24.3
31.25	10.6	51.9	49.9	39.0	39.0	23.6
62.5	15.4	47.4	45.4	30.0	30.0	21.5
100	19.8	44.3	42.3	25.0	25.0	21.0
155	25.1	41.5	39.5	14.0	14.0	21.0
200	29.0	39.9	37.9	10.0	10.0	21.0
250	32.8	38.3	36.3	3.0	3.0	18.0
300	35.2	37.2	34.2	0.0	0.0	18.0
310	37.1	36.9	34.9	-	-	18.0
350	39.8	36.2	34.2	-	-	17.0
400	43.0	35.3	33.3	-	-	14.0
500	49.0	33.8	31.8	-	-	14.0

Continuación.

FRECUEN. (MHz)	IMPED. DE ENTRADA (ohm)	IMPEDANCIA FIJADA (ohm)	MIN ELFEXT (dB)	MIN. PSELFEXT (dB)
1	100+-12	100+-15	67.8	64.8
4	100+-12	100+-15	55.7	52.7
8	100+-12	100+-15	49.7	46.7
10	100+-12	100+-15	47.8	44.8
16	100+-12	100+-8	43.7	40.7
20	100+-12	100+-8	41.7	38.7
25	100+-15	100+-8	39.8	36.8
31.25	100+-15	100+-8	37.9	34.9
62.5	100+-15	100+-8	31.8	28.8
100	100+-15	100+-8	27.8	24.8
155	100+-15	100+-8	23.9	20.9
200	100+-15	100+-8	21.7	18.7
250	100+-20	100+-8	19.8	16.8
300	100+-20	100+-8	18.2	15.2
310	100+-20	100+-8	17.9	14.9
350	100+-22	100+-8	16.9	13.9
400	100+-32	100+-8	15.7	12.7
500	100+-32	100+-8	13.8	10.8

- Instalación del Cable de Distribución Horizontal:
    1. El cable se instaló de acuerdo con las recomendaciones del fabricante y las mejores prácticas de instalación de la industria.
    2. Las bandejas no fueron ocupadas con mayor cantidad de cables que los máximos permitidos por el NEC (National Electric Code) para cada tipo particular de bandeja.
    3. Los cables se instalaron en tendidos continuos desde el origen al destino y no se admitió puntos de conexión adicionales intermedios
    4. No se excedieron los radios de curvatura mínimo de los cables ni las máximas tensiones de tendido.
    5. Los cables de distribución horizontales no se agruparon en grupos de más de 40 cables ya que las ataduras de más de 40 cables pueden causar deformación de los cables del centro de la atadura.
    6. No se precintaron cables a las grillas del techo suspendido o a los alambres de soporte de las luminarias.
    7. Cualquier cable dañado o excediendo los parámetros de instalación recomendados durante su tendido fueron reemplazados por la contratista previo a la aceptación final sin costo alguno para el Cliente.
    8. Los cables fueron identificados por una etiqueta autoadhesiva de acuerdo con el estándar de documentación. La etiqueta del

cable se aplicó al cable detrás del faceplate en una sección de cable que pueda ser accedida quitando el Faceplate.

9. Los cables Unshielded Twisted Pair se instalaron de forma tal que no se presenten cambios de dirección que presenten curvaturas menores a cuatro veces el diámetro exterior de los cables (4X O.D. del cable) en ningún punto del recorrido.
10. La tensión de tendido para los cables UTP de 4 pares no excedieron en ningún momento las 25 libras para un solo cable o atadura de cables.

- Diagramas de la Instalación del Cableado Horizontal: Las rutas de instalación del cableado horizontal efectuado en cada uno de los 6 pisos de la sede Principal de la empresa AmericaCom se muestran en el **ANEXO A**.

Toma de Telecomunicaciones.- Cada toma de telecomunicaciones, está compuesta de un cable Categoría 6 para datos y un cable Categoría 6 para voz. Cada cable categoría 6 se terminaron en un conector RJ45 hembra CAT 6 Giga-Channel modular de 8 posiciones/8conductores de a cuerdo al código de colores T568A. Las tomas de telecomunicaciones, se montaron en cajas rectangulares simples.

- Especificaciones Técnicas de los Productos.
    1. Jack Modular Giga-Channel: Los jacks modulares utilizados son el CJ688TIW en conjunto con el face plate y el CJ688TBL

para el lado de Closet. Todos los jacks modulares se conectaron de acuerdo a la asignación de colores T568A, las cuales fueron diseñaron con la mas avanzada tecnología para trasmitir datos a altas velocidades, presenta etiqueta de codificación de colores para T568A y T568B, así mismo el conector tipo 110 acepta conductores sólidos de 22-24 AWG. Los jacks modulares CJ688TIW son compatibles para su uso en cualquier producto de la solución INTEGRITY, ya sea con las tomas de telecomunicaciones, los patch pannels y otros. Los jacks modulares Giga-Channel utilizados en el subsistema de cableado horizontal se muestra a continuación:

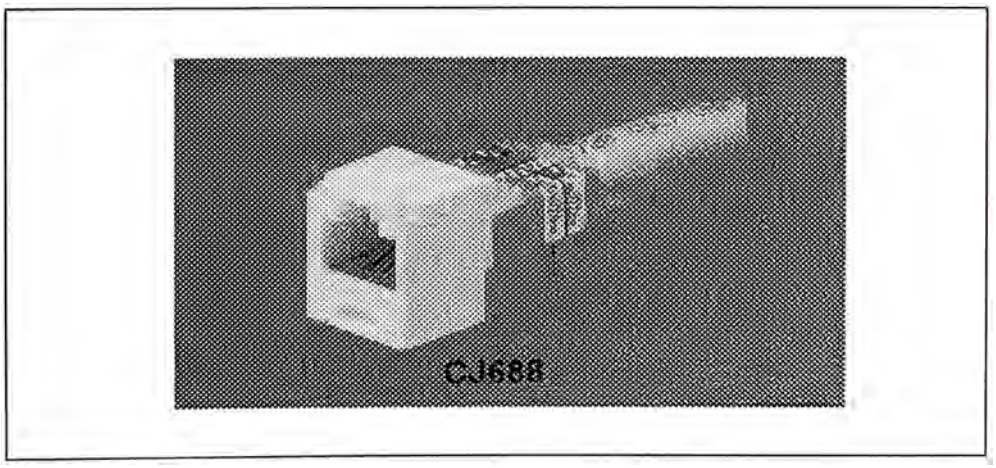


Figura 8-5 Jack Minicom Categoría 6 – Panduit..

Los jacks modulares Giga-Channel exceden todos los requerimientos de los stándares de la industria como se mencionó anteriormente. Adicionalmente, al sér combinados en un canal con cables y paneles Giga-Channel arrojaron

características de performance que superaron las mínimas listadas en la Tabla 8-5.

2. Tomas de oficina: Se utilizó face plates de 4 ports del tipo CFPL4IW, el cual tiene un tamaño de 4.53" X 2.77" X .60". Cada faceplate contendrá dos jacks modulares Giga-Channel, uno para datos y otro para voz. En esta terminaron los cables Media-Twist Categoría 6 para datos y voz; los dos puertos restantes son para una línea analógica o reservado para uso futuro. A cada port se le proporcionó un icono para indicar su función. Los face-plate utilizados en el subsistema de cableado horizontal se muestra a continuación

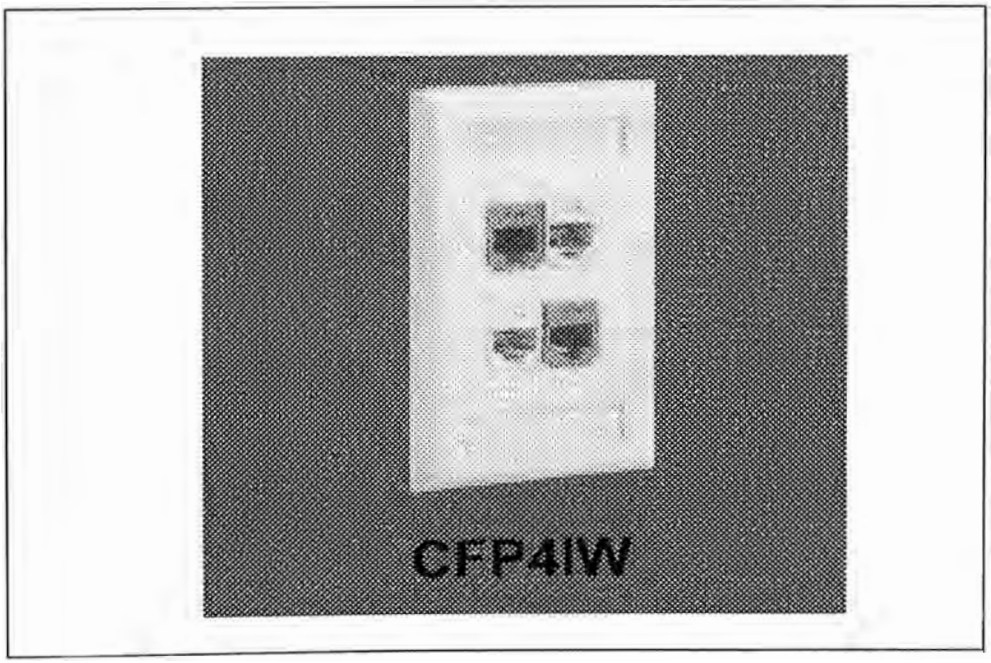


Figura 8-6 Face Plate Categoría 6 – Panduit..

- Instalación de la Toma de Telecomunicaciones: Todas las tomas de telecomunicaciones se instalarán de la manera siguiente: El exceso de cable se enrolló en las cajas de distribución o en las cajas de montaje superficial teniendo presente que al alojar el rollo del cable no se excedió los radios de curvatura del fabricante.

  Además, cada tipo del cable se terminó tal como se indica a continuación :

  1. Los cables se terminaron de acuerdo con las recomendaciones hechas en la TIA/EIA-568-A
  2. El destrenzado de los pares de los cables Media-Twist en el área de terminación fueron el mínimo posible y en ningún caso fué superior a media pulgada.
  3. Los radios de curvatura de los cables en el área de realización de la terminación no fueron menor a 4 veces el diámetro externo del cable.
  4. La vaina del cable se mantuvo tan cerca como posible del punto de terminación.
  5. Los jacks modulares RJ45 de voz, se ubicaron en las posición de abajo de cada faceplate. Los jacks modulares de voz ubicados en faceplates orientados en forma horizontal
  6. Los jacks modulares RJ45 de datos ocuparon las posiciones superiores del faceplates. Los jacks modulares de datos ubicados en faceplates orientados en forma horizontal

- Diagrama de la Instalación de un Face-Plate: A continuación mostramos la instalación típica de un face-plate en un subsistema de cableado horizontal instalado en cada uno de los 6 pisos de la sede Principal de la empresa AmericaCom.

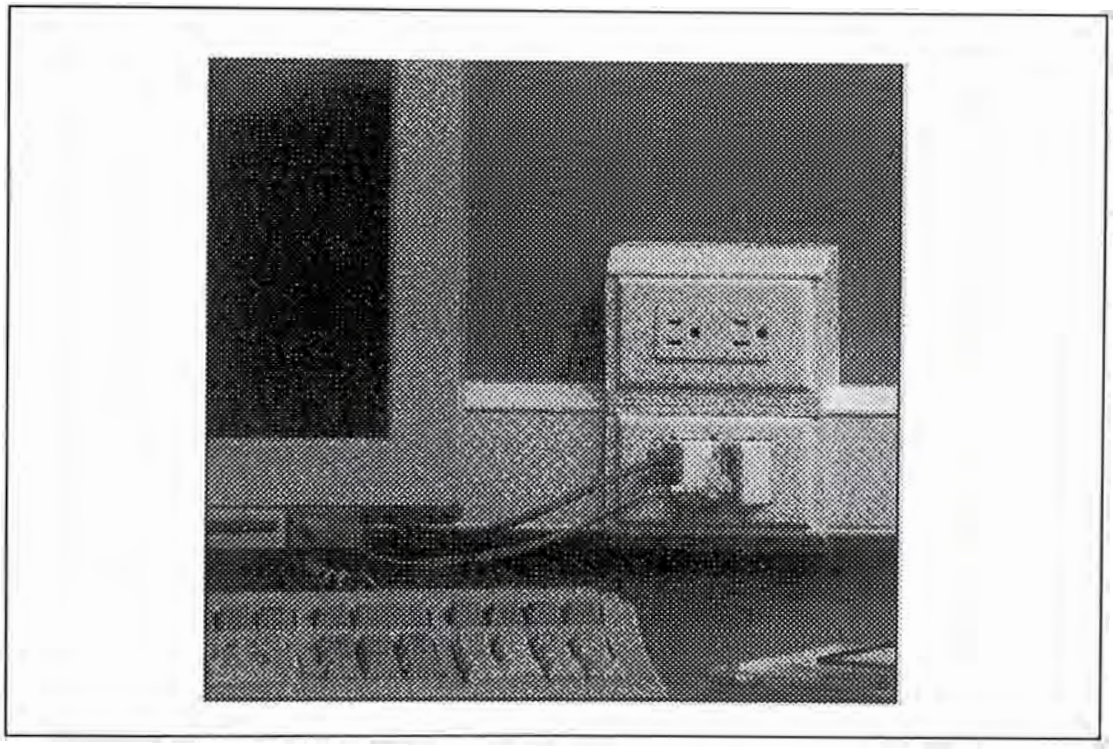


Figura 8-7 Típico toma de telecoimunicaciones Categoría 6 – Panduit,. en un área de trabajo

Hardware de Terminación de Cross-Connect.- El Hardware de terminación de Cross-Connect se expolica a continuación.

- Cross-Connect del Sistema de Datos: Las cruzadas para los circuitos de datos se realizaron mediante Patch Cords Giga-Channel desde los Patch Panels Giga-Channel del tendido horizontal de datos hacia los switches IDFD´s capa 2 dentro del mismo rack o hacia bastidores contiguos. El hardware de conexionado horizontal de datos se

dispuso en racks abiertos. Todos los racks se equiparon con el hardware de administración, horizontal y vertical, frontal y trasero de la línea Panduit. Todos los patch panel instalados son de 1“ de alto y del tipo CP24BL (Patch-panel modular de 24 puertos Metal.), la cual nos proporcionó 24 ports modulares RJ45, conexionados según la asignación de colores T568A. Los patch panels utilizados fueron de color negro al igual quie los jacks modulares RJ45. Asimismo fueron configurados con 6 módulos de 4-port cada uno, reemplazables, con etiquetas universales con capacidad de codificación T568A y B. El frente de cada módulo fue etiquetado con etiquetas de 9mm a 12mm.

Los patch panels Giga-Channel cuando se combinan en un canal con un cable UTP Media-Twist y jacks Giga-Channel deben proporcionar las características de performance mínimas detalladas el la Tabla 8-5.

- Cross-Connect del Sistema de Voz: Las cruzadas para los circuitos de voz se realizaron mediante Patch Cords Giga-Channel desde los Patch Panels Giga-Channel del tendido horizontal hacia los Patch Panels que oficiaron como espejo del repartidor telefónico dentro del mismo rack. El hardware de conexionado horizontal de voz se dispondrá en racks abiertos. Todos los racks se equiparon con el hardware de administración, horizontal y vertical, frontal y trasero de la línea Panduit. Todos los patch panel instalados son de 1“ de alto y

del tipo CP24BL (Patch-panel modular de 24 puertos Metal.), la cual nos proporcionó 24 ports modulares RJ45, conexionados según la asignación de colores T568A. Los patch panels utilizados fueron de color negro al igual que los jacks modulares RJ45. Asimismo fueron configurados con 6 módulos de 4-port cada uno, reemplazables, con etiquetas universales con capacidad de codificación T568A y B. El frente de cada módulo fue etiquetado con etiquetas de 9mm a 12mm. Los requisitos de los patch panels Giga-Channel fueron detallados en el item anterior.

Los patch panels Giga-Channel cuando se combinen en un canal con cable Media-Twist y jacks Giga-Channel deben proporcionar las características de la performance mínimas detalladas en la Tabla 8.5.

Los patch panel que oficiaron de espejo del repartidor telefónico fueron de 3.5" de alto, nos proporcionó 48 ports modulares RJ45, conexionados según la asignación de colores T568A, en la cual se realizó la terminación de los cables multipares provenientes de la central telefónica. Los patch panels utilizados fueron de ecolor negro con numeración de color blanco y configurados con 8 módulos de 6-port reemplazables, con etiquetas universales con capacidad de codificación T568A y B. . El frente de cada módulo fue etiquetado con etiquetas de 9mm a 12mm.

- Instalación de Cross-Connect Horizontal: El hardware de terminación de cobre y el hardware de management de cables se instalaron de la siguiente manera:

    1. Se acomodaron y se terminaron los cables de acuerdo con las recomendaciones hechas en la TIA/EIA-568-A.
    2. El destrenzado de los pares de los cables Media-Twist en el área de terminación fué el mínimo posible y en ningún caso fue superior a media pulgada.
    3. Los radios de curvatura de los cables en el área de realización de la terminación no fueron menor a 4 veces el diámetro externo del cable.
    4. La vaina del cable se mantuvo tan cerca como fue posible del punto de terminación.
    5. Los mazos de cables se precintaron y acomodaron en forma prolija a sus respectivos patch panels. Cada patch panel fue alimentado por un mazo de cables individualmente separado, acomodado y precintado hasta el punto de entrada al rack.
    6. Cada cable se etiquetó claramente en la vaina, detrás del patch panel en una ubicación que pueda verse sin quitar los precintos de sujeción del mazo.

El hardware de terminación de fibra óptica se instaló de la manera siguiente:

1. El exceso de cable de fibra óptica se enrolló en forma prolija en los anillos organizadores que se encuentran dentro de los Patch Panel deslizables de fibra óptica. Se tuvo presente que al alojar el rollo del cable no se excedió los radios de curvatura mínimos recomendados.
2. Cada cable se precintó en forma individual dentro del hardware de terminación respectivo. El o los "strength members" de los cables de fibra óptica se sujetaron a los accesorios internos del hardware de terminación dispuestos internamente para tal fin.
3. A cada cable de fibra se despojó de su vaina al entrar en el hardware de terminación y se ruteó cada una de las fibras en forma individual hacia los acopladores ópticos.
4. Cada cable se etiquetó claramente a la entrada del hardware de terminación.
5. Los protectores de polvo se dejaron instalados en todo momento en los conectores y acopladores, a menos que se hallen físicamente conectados.

- Diagrama de Instalación del Cross-Connect Horizontal: A continuación mostramos el modo de instalación del cross-connect horizontal en cada uno de los pisos de la compañía AmericaCom.

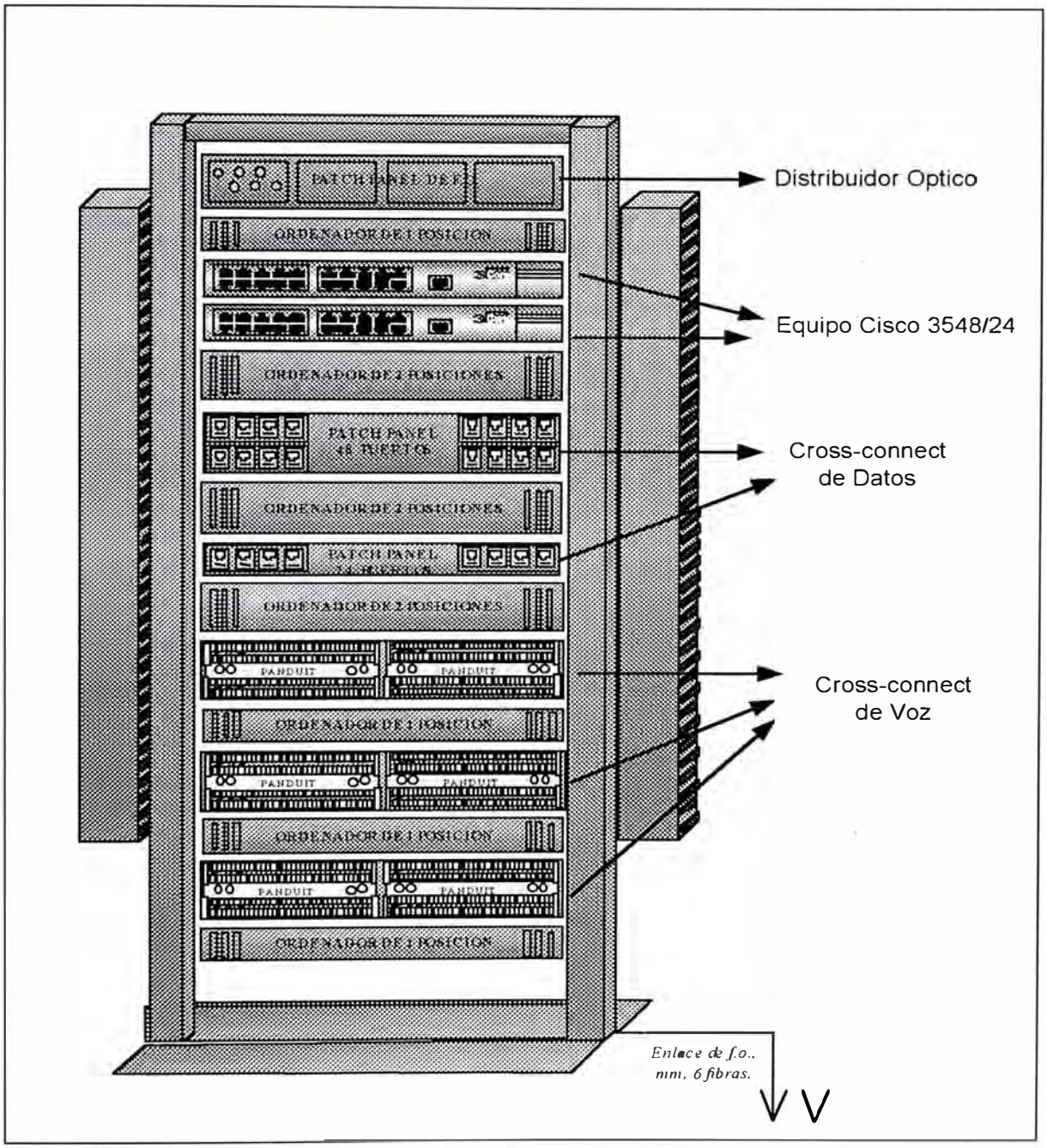


Figura 8-8 Diagrama de la instalación de Cross-Connexión en cada uno de los closet de telecomunicaciones de los 6 pisos correspondientes a la Sede Principal o Corporativa, en la cual se muestra la terminación de fibra óptica, la terminación del cableado horinzal de voz y data y los equipos de comunicación de red.

8.2.2.- Instalación del Backbone

Para la parte de Voz, se instaló cables multipar de Categoría 3 de 24 AWG en el backbone, para extender los teléfonos de cada piso con la central ubicada en el Cuarto de la central PBX, ubicada en el Sótano del Edificio. El cable utilizado para este propósito fue un multipar de 100 pares. Dentro del mazo de cables se instaló un conductor que se conectó a tierra en cada extremo.

Para abastecer las necesidades de voz para cada piso, se tendió:

- Piso 6 : 140 pares de cobre
- Piso 7 : 200 pares de cobre
- Piso 8 : 140 pares de cobre
- Piso 9 : 140 pares de cobre
- Piso 10 : 140 pares de cobre
- Piso 11 : 140 pares de cobre

Este cableado se realizó entre el ambiente de Comunicaciones de cada Piso (IDF´s) y la sala de datos principal (MDF) ubicado en el Sótano, posteriormente se cableó multipar entre el MDF y la central telefónica, debido a que la central y la sala de Datos se encuentran en mabientes separados.

Para la parte de Datos se utilizó un cable de doce fibras ópticas multimodo para proporcionar conectividad a nivel backbone entre el MDF de

datos y cada IDF de datos en los pisos. El cable instalado en el backbone fue apropiada para el uso en montantes. El cable de fibra óptica fue de 12 fibras multimodo de 62/125 micrones y con un diámetro externo de 7.10 mm. El cable proporcionó una atenuación máximo de 3.5 dB/km @ 850 nm y 1.5 dB/km @ 1300 nm. (2.6/1.1 dB/km de atenuación típica). Los anchos de banda del cable fueron 500 MHz/km @ 850 nm y 500 MHz/km @ 1300 nm de acuerdo a las especificaciones del fabricante. Las fibras ópticas estan cubiertas con un buffer primario de 900 micrones con codificación de colores standard. Estas fibras estan recubiertas con un miembro fuerte de fibras de aramida y una vaina exterior de PVC .

De acuerdo al los requerimientos dee diseño mencionado anteriormente, el tipo de backbone utilizado fue el "Backbone Colapsado" la cual se muestra en la figura 8-3.

Instalación del Cable Backbone.- Todos los cables del Backbone se instalaron de la manera siguiente:

- Los cables del backbone se instalaron en forma separada de los cables de la distribución horizontal.
- Se utilizaron ductos separados a través de la montante del edificio, para el transporte de cables de fibra óptica y cables multipar a cada piso del edificio.
- Se utilizaron dos cables de 6 hilos de fibra óptica para obtener protección redundante ante posibles cortes.

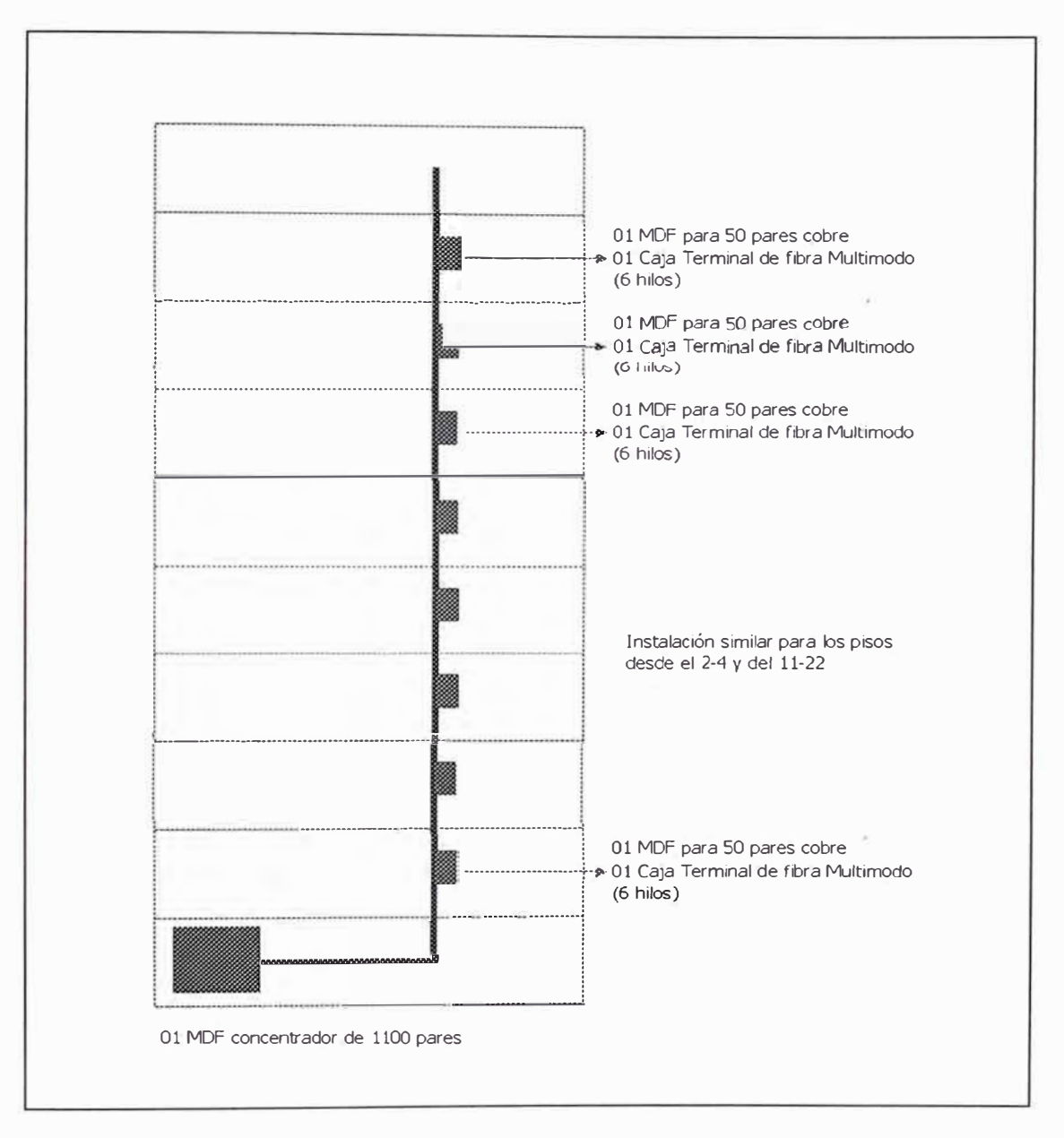


Figura 8-9 Diagrama de distribución física dedl backbone de Voz y Datos para el sistema de cableado Estructurado de la Red Corporativa.

Hardware de Terminación Backbone.- Para la parte de Datos, cada cable de fibra óptica se terminó en el MDF de datos y en cada uno de los IDF´s de datos, en bandejas deslizables, para montaje en bastidores de 19". Utilizamos el producto Opticom de 24 y 48 ports de Panduit, los que son las encargadas de proporcionar protección a las fibras terminadas. En los

ambientes IDF´s se utilizaron Opticom de 24 puertos para terminación de fibra, la cual tiene una altura de 9.0 cm. En los ambientes MDF se utilizaron Opticom de 48 puertos, la cual tiene una altura de 13.5 cm. Las bandejas son de color negro e incluirán los acopladores SC Multimodo Duplex montados, son del tipo deslizable y poseen en su interior los ruteadores y fijaciones para una correcta instalación de los cables de acuerdo a los estándares de la industria. Los distribuidores ópticos de 24 y 48 puertos utilizados en el cableado del backbone se muestran en la figura 8-4.

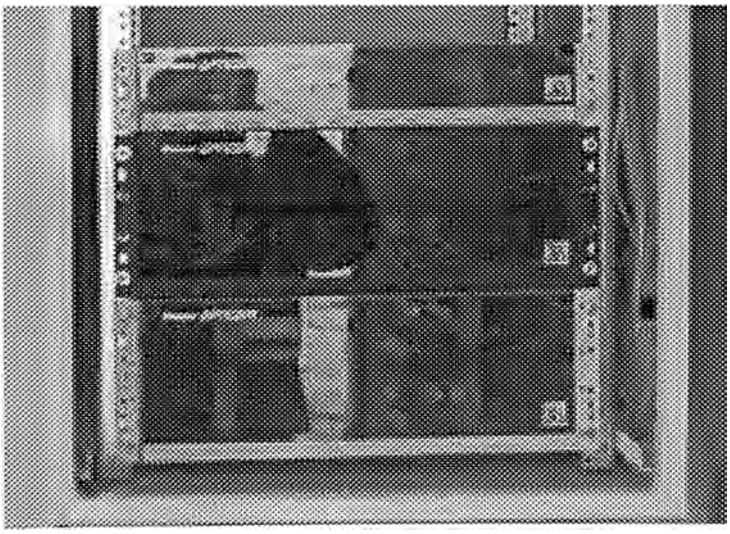
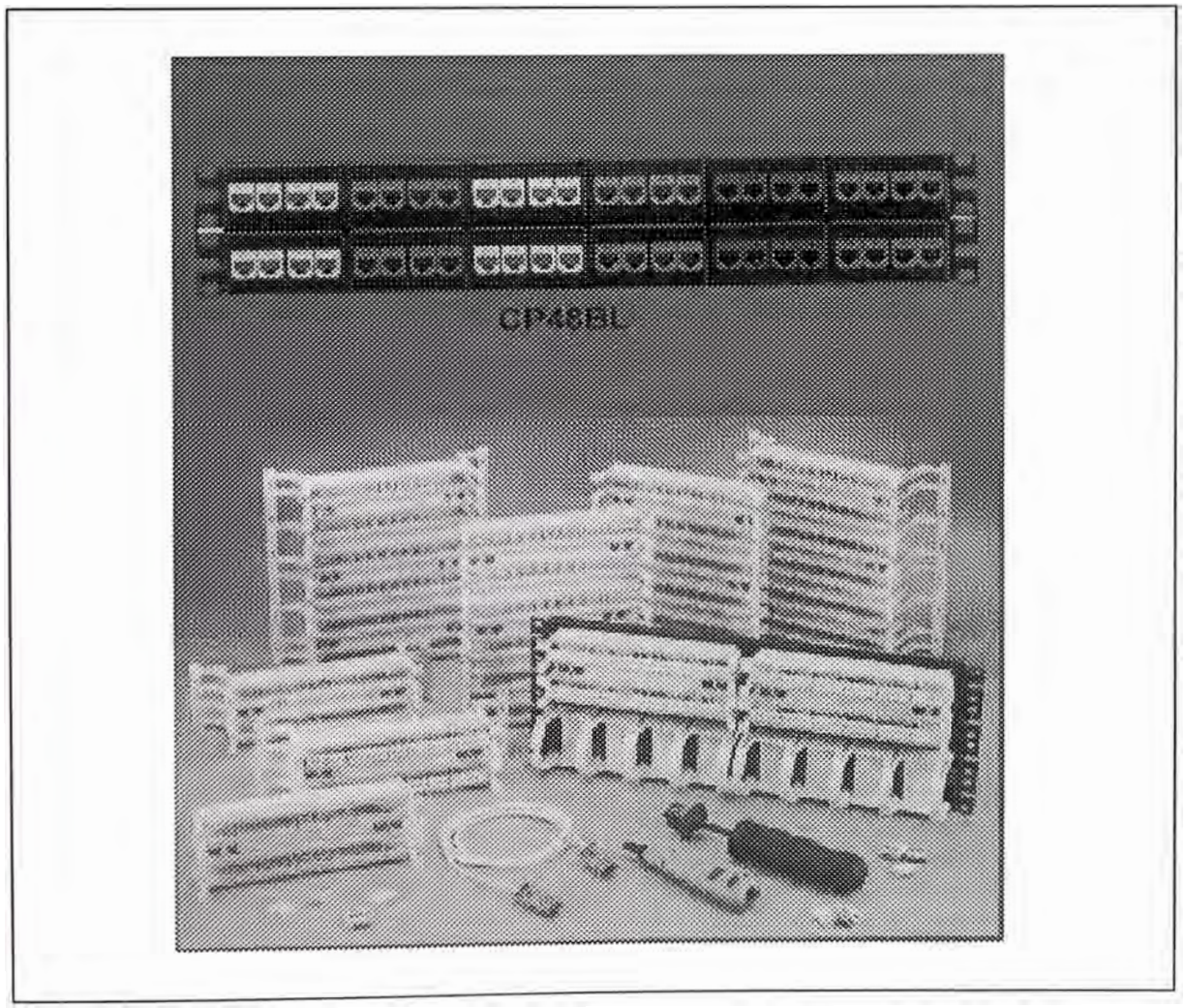


Figura 8-10 Distribuidores ópticas de 24 y 48 fibras respectivamente utilizados en los closet´s IDF y MDF..

Para la parte de Voz, los cables de cobre del backbone se terminaron en el área del MDF en bloques 110 de montaje en pared. Los bloques de montaje en pared son kits 110ConnectXC de terminación en campo, que incluyen blocks, bloques de conexionado y los plásticos

transparentes para la ubicación y protección de las etiquetas, asimismo fueron provistos de las guías de organización horizontal. En los ambientes IDF´s, los cables de cobre se terminaron en pach panel 110 Categoría 3 de 48 puertos, la cuales constituyen el punto de interconexión con el cableado horizontal. Así mismo se tendió igual cantidad de pares de cobre entre el ambiente de la central telefónica y la sala de datos principal o MDF, para habilitar los anexos de voz en cada uno de los pisos de la Empresa.



. Figura 8-11 Patch Panel y módulos cross-conexión instalados en los closet dee comunicaciones IDF´s y MDF..

8.2.3.- Armarios de Telecomunicaciones : MDF´ss –IDF´s

Los armarios de telecomunicaciones alojan a los racks, los campos de terminación de voz y datos y el hardware para la realización de la administración de los cables.

El ambiente del MDF se implementó de la manera siguiente: Se instalaron un gabinete para la ubicación del switch capa 3 principal y el router de borde principal, otro gabinete en la cual se instalaron los equipos de respaldo tanto switch como router, y un tercer gabinete para la terminación tanto de fibra óptica para el servicio de datos y los cables de cobre para el servicio de telefonía. Así mismo se diseñó los espacios para futuros gabinetes para un crecimiento posterior si es necesario. El diagrama del MDF principal se muestra la figura 8-12.

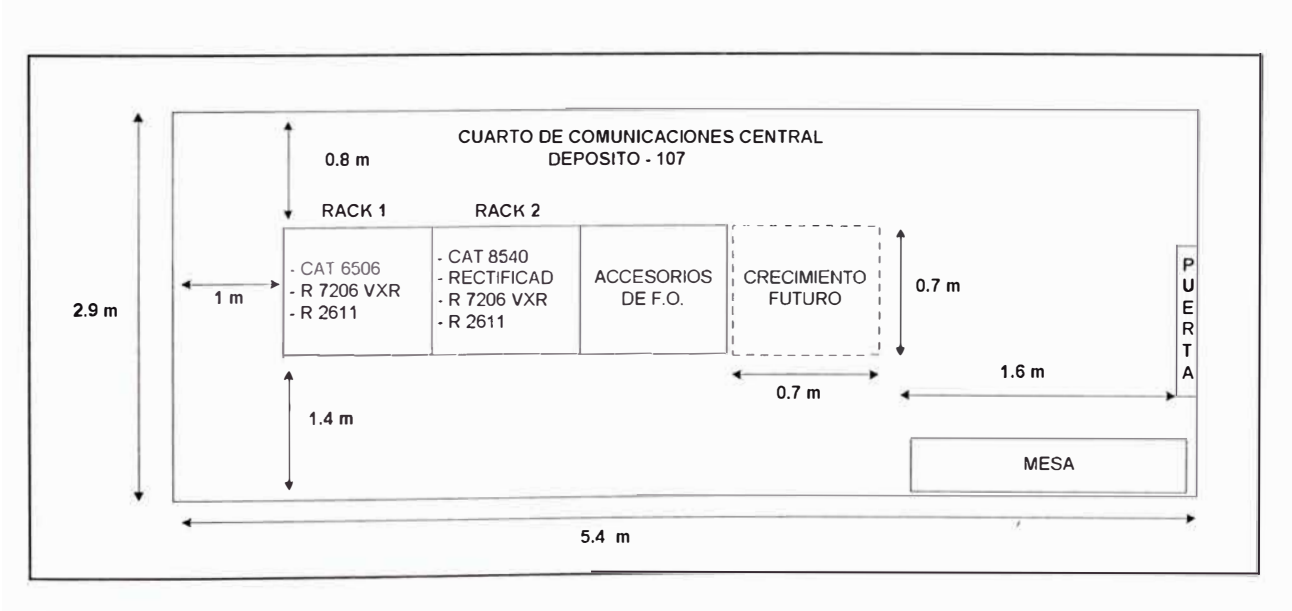


Figura 8-12 Diagrama de distribución de racks y equipos de comunicación en el Closet principal de Telecomunicación (MDF) para la Red Corporativa.

Los ambientes IDF´s se implementaron todos de una manera similar: Se instalaron dos racks autosoportados, un rack para la terminación de voz y el hardware para la realización de la administración de los cables y el otro rack para la instalación de los switches IDF´s y la terminación de los puntos de datos. Los racks fueron dispuestos para permitir un mínimo de 0.80 metros de claridad desde las superficies de montaje delanteras y traseras y de uno de los lados. Se instaló un bastidor en forma contigua para que nos proporcione el hardware de administración vertical intermedio suficiente para albergar la totalidad de cables de ambos bastidores. Las dimensiones de cada closet IDF se muestran en la tabla 8-4.

Especificaciones técnicas de la Energía.- Tanto los Closets de distribución (IDF´s) como el closet principal (MDF) fueron provistos con la energía necesaria correspondiente, para el buen funcionamiento y la mejor performance de los equipos. De esta manera podemos encontrar lo siguiente :

- De los Closet´s de Comunicaciones (IDF´s Pisos 6-11): La Energía Eléctrica instalada fue de 220 VAC con un consumo de 3A. Además, se Instalaron 2 regletas de 220VAC en la cual cada una fue conectada a una llave térmica independiente en el Tablero AC del Cuarto de Comunicaciones de cada Piso. La energía en cada IDF fue estabilizada, la cual fué respaldada por un UPS con características de protección de Sobre Picos y corrientes Armónicas. Se instalaron energía 220VAC con punto a neutro, es decir de las 2 líneas activas, en la cual una media 0Volt respecto a Tierra.
- Del Closet de Comunicación Central (MDF): Se instaló un Rectificador de 48VDC con capacidad de abastecimiento de 40 Amp como mínimo, el cual fue instalado en el Rack No 2. Se asumió que el rectificador que abastece los 40 A / 48VDC requerirá una carga de energía de 10A / 220VAC. El requerimiento total de energía para el cuarto de comunicaciones fue de 26Amp / 220 VAC. Se asume que la carga de 40A /48VDC será suministrada de la carga que consumirá el Rectificador. Se instalaron 2 regletas de 220VAC en los Rack 1, 2 y 3 en la cual, cada una fue conectada a una llave térmica independiente en el Tablero AC. La energía instalada es estabilizada, la cual esta

respaldada por UPS con características de protección de Sobre Picos y corrientes Armónicas. Se cuenta con energía 220VAC con punto a neutro, es decir de las 2 líneas activas, una mide 0Volt respecto a Tierra. Los equipos Catalyst 6506 , Catalyst 8540 fueron conectados directamente al tablero AC/DC según corresponda, utilizando para cada una de sus fuentes (2 fuentes por equipo) una llave térmica independiente. Se consideró que los demás equipos se conectarán a ambas regletas en forma separada.

Especificaciones técnicas del Pozo de tierra.- Se contó con un pozo a tierra en AC, la cual se utilizó para los equipos de comunicaciones que operan en AC, así como para anclar los rack a tierra. Se contó con un pozo de tierra en DC (Tierra Electrónica) , la cual se utilizó para formar la carga de –48VDC y se utilizó para los equipos de transporte para los enlaces de Voz. La tierra DC es la misma tanto para el uso de la central telefónica como para los equipos encargados del transporte de los enlaces de Voz. El valor típico de los pozos de tierra deberá ser menor a 5 Ohm.

Especificaciones técnicas de las condiciones ambientales- El ambiente se preparó a una temperatura adecuada, para el funcionamiento correcto de los equipos, ded esa manera fue necesario el uso de equipos de aire acondicionado para mantener una temperatura promedio de 20 Grados Centígrados. Se Mantiene los valores de Humedad Relativa dentro del rango

de 10 a 90%, no –condensado. Se adjunta la tabla 8-6 que nos muestra el cuadro de disipación calorífica por Piso:

No Piso	Equipo Comunicaciones	Cant.	Disipación de energía	Temperatura de operación	Disipación de energía (Total)
Cuartos de Comunicaciones					
1	Catalyst 3548XL	3	600 BTU/h	De 0 hasta 45° C	1,800 BTU/h
2	Catalyst 3548XL	3	600 BTU/h	De 0 hasta 45° C	1,800 BTU/h
3	Catalyst 3548XL	3	600 BTU/h	De 0 hasta 45° C	1,800 BTU/h
4	Catalyst 3548XL	3	600 BTU/h	De 0 hasta 45° C	1,800 BTU/h
5	Catalyst 3548XL	3	600 BTU/h	De 0 hasta 45° C	1,800 BTU/h
6	Catalyst 3548XL	3	600 BTU/h	De 0 hasta 45° C	1,800 BTU/h
Cuarto Principal de Comunicaciones					
	Catalyst 6506/8540	2	6140 BTU/h	De 0 hasta 40° C	12,280 BTU/h
	Router 2611	2	245 BTU/h	De 0 hasta 45° C	490 BTU/h
	Rectificad 16Amp	1	1500 BTU/h	De 0 hasta 45° C	1500 BTU/h
	Router 7206	2	1265 BTU/h	De 0 hasta 40° C	2530 BTU/h
					16,800 BTU/h

EQUIPO	CANTIIDAD	REQUERIMIENTO ENERGIA	REQUERIMIENTO AIRE ACONDICIONADO
LOCAL : CUARTO DE COMUNICACIONES PRINCIPAL			
RACK 1:			
CATALYST 6506 **(2 Llaves de 8A)**	1	8 A / 220 VAC	6140 BTU
ROUTER 7206 VXR **(Directo a 2 Regletas)**	1	2.5 A / 220VAC	1265 BTU
ROUTER 2611 **(Directo a 1 Regleta)**	1	1.5 A / 220VAC	72 W (245 BTU)
TOTAL RACK 1		**12 A / 220VAC**	**7650 BTU**
RACK 2:			
CATALYST 8540 **(2 Llaves de 40A)**	1	40 A / 48 VDC	6140 BTU
RECTIFICADOR 48 VDC **(Llave Independiente)**	1	10 A / 220 VAC	1500 BTU
ROUTER 7206 VXR **(Directo a 2 Regletas)**	1	2.5 A / 220VAC	1265 BTU
ROUTER 2611 **(Directo a 1 Regleta)**	1	1.5 A / 220VAC	72 W (245 BTU)
TOTAL RACK 2		**14 A / 220VAC**	**9150 BTU**
TOTAL CARGA	AC	26 A / 220VAC	16800 BTU
	DC	40 A / 48VDC	
LOCAL : CUARTO DE COMUNICACIONES (POR PISO)			
CATALYST 3548XL **(Directo a 2 Regletas)**	3	1A / 220 VAC	600 BTU
TOTAL X PISO		**3 A / 220 VAC**	**1800 BTU**

Tabla 8-6 Requerimientos técnicos de la energía eléctrica instalada en los IDF´s y el MDF

8.2.4.- Pruebas y Mediciones del Sistema de Cableado Estructurado.

Todos los cables y materiales de terminación fueron 100% probados contra defectos de instalación y verificamos la performance del cable bajo las condiciones de instalación. Todos los conductores de cada cable instalado fueron certificados por la contratista previo a la aceptación del sistema. Cualquier defecto en el sistema fue reparado o cambiado para asegurar un 100% de utilidad de todos los conductores de todos los cables instalados. Las pruebas realizadas cumple con los estándares para cada característica de acuerdo a lo establecido por la EIA/TIA.- TSB 67

Mediciones del Cable de Cobre.- En cada cable se verificó la continuidad en todos sus pares y conductores. Así como también pares reversos, cortos y extremos abiertos utilizando un tester tipo secuenciador. Además del testeo anteriormente citado estos cables se verificaron utilizando un analizador de cables Clase II.

Como los medios de cable de cobre pueden ser dramáticamente influenciados por muchos problemas típicos y características del cable, las pruebas a que fueron sometidos después de la instalación incluyeron:

- Wired MAP
- Ruidos eléctricos
- Crosstalk NEXT
- Power Sum NEXT

- FELXT y ELFEXT
- Atenuación
- Razón de Atenuación a Crosstalk (ACR)
- Capacitancia
- Impedancia
- Resistencia DC
- Continuidad y polaridad
- Longitud del cable
- Retardo
- Retardo Skew

El resultado de las pruebas fueron evaluados en forma automática por el probador, utilizando el último criterio de la Categoría 6 ISO/IEC y el resultado mostrado fue del tipo pass/fail. El resultado fue bajado directamente desde el tester hacia un archivo, utilizando la aplicación del fabricante. Dicho resultado incluyen todos los parámetros de pruebas indicados y se muestra a continuación. Las mediciones de los cables de cobre UTP CAT de voz y datos para cada uno de los seis pisos de la Red Corporativa, se encuentran detallados en el **ANEXO B**. Debido a que existen mas de 1000 mediciones, sólo se incluirá las mediciones correspondientes a un punto de voz y uno de datos para cada piso de la sede Corporativa.

Mediciones del Cable de Fibra Óptica_.- Todas las terminaciones de fibra óptica se inspeccionaron visualmente, para asegurar que no tengan imperfecciones luego de haberse concluido el proceso de instalación. Además, para cada hilo de fibra se midió la atenuación con un Optical Power Meter y una Optical Ligth Source. La longitud del cable y la atenuación de los empalmes se verificaron utilizando un OTDR.

- Atenuación: Los cables de fibra multimodo del backbone fueron medidos en longitud de onda dee 850 nm en solo una dirección. El método de setup del equipo y la medición de performance fueron realizadas de acuerdo con el estándar ANSI/EIA/TIA-526-14, método B. El mismo indica que debe usarse un patch cord de 2 metros como referencia y 2 patch cords de 2 metros para realizar la medición del link. Este método de testeo utiliza un patch cord de referencia, y dos patch cord para realizar la medición de la perdida del link mas la de dos conectores. Esta medición es coherente con la perdida en el cual el equipo de red será instalado y utilizado. El test de evaluación de panel a panel (backbone) estará basado en los valores establecidos en la EIA/TIA-568-A Anexo H, Optical Fiber Link Performance Testing. Para la conexión WAN, la atenuación de la fibra monomodo fue medida a 1310 y 1550 nanómetros utilizando una fuente de emisión láser y un Power Meter. El testeo fue medido en ambas longitudes de onda en una dirección en cada hilo de fibra. La medición se realizó de acuerdo con el standard EIA/TIA-526-7, método 1A . Un Patch cord

de 2 metros debe ser utilizado como referencia y testeo. Este método utiliza un patch cord de referencia, dos patch cord de testeo para estimar la perdida del link más dos patch cords. Los resultados esperados para cada cable (o grupo de cables de igual longitud) fueron calculados antes de comenzar la medición y documentados. Luego cada valor obtenido se evaluó contra este número prefijado. Todas las fibras que excedan este valor fueron reparadas o recambiadas.

- Pérdida por Distancias y Empalmes: El cable fue probado con un OTDR (Optical Time Domain Reflectometer) para verificar su longitud y la perdida de los empalmes. La medición de longitud con el OTDR se realizó de acuerdo al standard EIA/TIA-455-60. Estos testeos fueron realizados para comprobar si existen empalmes en el tramo, verificar la longitud del cable, ya que fueron sometidos a tensiones en el momento de la instalación.

8.2.5.- Presupuesto del Sistema de Cableado Estructurado

Para la instalación del cableado estructurado Categoría 6 en el edificio Corporativo, se realizó una licitación de precios y materiales entre los distintos proveedores del medio local, en coordinación con estos y las áreas responsables del proyecto, concluyeron en la elección del proveedor, los costos y beneficios que brindarían post la instalación.

A continuación presentamos una tabla 8-7 en la cual nos muestra los montos que se requirió invertir para este proyecto de instalación de cableado estructurado Categoría 6, siendo la empresa AmericaCom una de las pocas en el medio con este tipo de sistemas en el Perú.

OFICINAS DEL EDIFICIO CORPORATIVO	COSTO DE MATERIALES ($)	COSTO DE MANO DE OBRA ($)	COSTO TOTAL SIN IGV ($)	IMPUESTO ($)	COSTO TOTAL ($)
PRIME PISO	12,636.69	3,300.00	**15,936.69**	2868.60	**18,805.29**
SEGUNDO PISO	15,978.84	4,245.00	**20,223.84**	3640.29	**23,864.13**
TERCER PISO	8,466.20	1,815.00	**10,281.20**	1850.62	**12,131.82**
CUARTO PISO	14,768.65	3,960.00	**18,728.65**	3371.16	**22,099.81**
QUINTO PISO	12,482.87	3,420.00	**15,902.87**	2862.52	**18,765.39**
SEXTO PISO	8,595.16	1,845.00	**10,440.16**	1879.23	**12,319.39**
				TOTAL GENERAL $	107,985.82

Tabla 8-7 Inversión total requerida para la implementación del Sistema de Cableado Estructurado CAT 6 de la Sede Principal del Edificio Corporativo.

Los costos de materiales y mano de obra para el cableado estructurado horizontal efectuado en cada uno de los 6 pisos de la sede Principal de la empresa AmericaCom se muestran en forma detallada en el **ANEXO C**.

8.3.- IMPLEMENTANDO SWITCHING Y ROUTING EN LA RED CAMPUS-LAN CORPORATIVA

De acuerdo al diseño mencionado anteriormente, el cual nos manifiesta la utilidad de implementar un modelo Multilayer, y de las muchas ventajas que esta nos proporciona, explicadas en capítulos anteriores, utilizaremos equipos switches capa 2, switches capa 3 y routers, en la implementación del hardware y software del sistema. Es necesario mencionar que los switches capa 3 es usado para control, mientras los switches capa 2 es usado para fordwarding data con un cost-effective.

Haremos referencia a los requerimientos que en su momento se solicitaron, así como también las características físicas del medio como producto del diseño e implementación del sistema de cableado estructurado. En esta representación se hace referencia a los equipos que fueron elegidos. Así tambien mostramos las conexiones con las dos sedes remotas restantes y la conexión a Internet.

A continuación mostramos en la figura 8-13 detalladamente el diagrama esquemático real de la configuración de los equipos Cisco (switches y routers), implementados en la sede Principal de la red Corporativa.

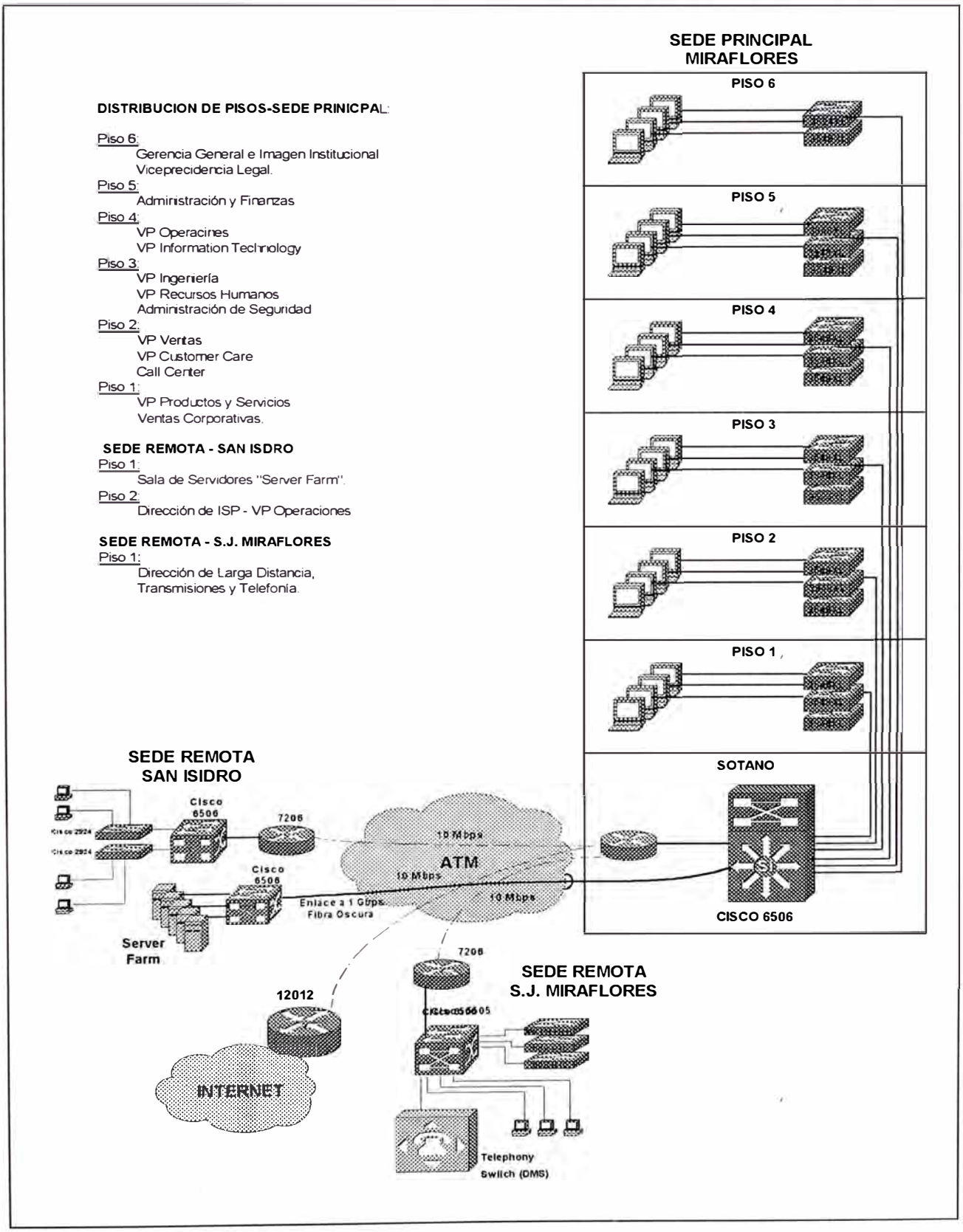


Figura 8-13 Diagrama de distribución de equipos y conexiones de la red Corporativa de America Com.

8.3.1.- Selección del Hardware

Para seleccionar los switches IDF´s, dado de que el switch estará conectado a los usuarios finales a través del subsistema de cableado estructurado horizontal categoría 6, a la velocidad de 100 Mbps y además que la conexión a los switches MDF´s será a través del backbone de fibra óptica multimodo a la velocidad de 1 Gigabps, el switch deberá tener la característica de soportar alta densidad de puertos 10/100 Base T y dos puertos Gigabit Ethernet (una principal y otra de respaldo) para la conexión a los switch MDF´s a través de rutas redundantes.

De las características mencionadas líneas arriba, se seleccionó el switch capa 2 modelo Cisco 3548XL y el Cisco 3524XL, las cuales serán instalados en los closets IDF´s de cada piso de la sede Corporativa. En la figura 8-14, se muestra las características físicas de los equipos.

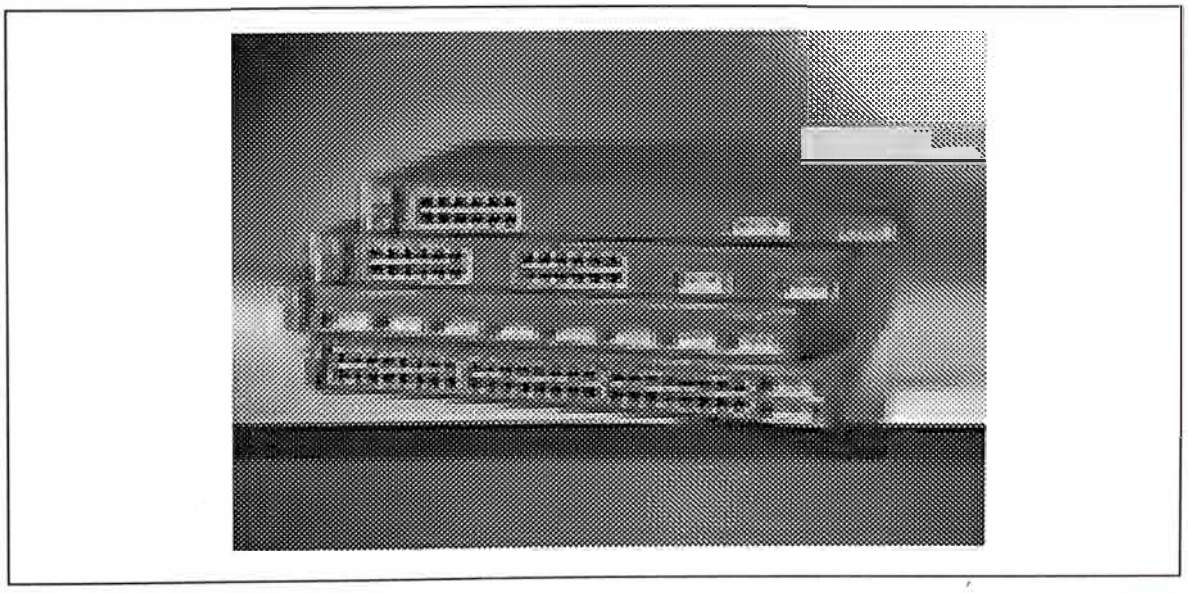


Figura 8-14 Características físicas de los equipos Cisco 3548XL y 3524XL..

Las características técnicas, la descripción del panel frontal y posterior, así como también las opciones de administración de los equipos Cisco Serie 3500 se muestran en el **ANEXO D.**

Para seleccionar los switches MDF´s, dado de que el switch estará conectado a los switches IDF´s a través del backbone de fibra óptica multimodo a la velocidad de un Gigabps, el switch deberá tener la característica de soportar puertos 1000 Base FL ó Giga Bit Ethernet de fibra óptica multimodo y dos puertos Fast Ethernet (una principal y otra de respaldo) para la conexión a los routers de borde, a través de rutas redundantes. Además es necesario adicionar que de acuerdo al diseño y requerimiento del servicio de Voz, uno de estos equipo deberá transportar los E1´s a través de la red WAN ATM, hacia la central de interconexión Local e Internacional ubicada en San Juan de Miraflores; es decir, el equipo debe proveer capacidad de switching en Ethernet y ATM.

De las características mencionadas líneas arriba, se seleccionó el routing switch capa 3 modelo Cisco Catalyst 6506s y el switching router Cisco Catalyst 8540 para redundancia de datos y el transporte de voz, así mismo se instaló un router 2611 el cual se conecta ala red PSTN local para poder tener acceso remoto. Estos equipos se instalaron en el closet MDF ubicado en el sótano de la empresa Corporativa. En la sede remota de San Isidro se se encuntra operando un Cisco Catalyst 6506 y para la sede

remota de San Juan de Miraflores un Cisco 5509´s, las cuales ya se encuentran operativos.

Debido a que el diseño incluye la habilitación de un ambiente de ubicación de servidores llamado "server farm", la cual será instalada en la sede remota de San Isidro y que la conexión de dichos servidores hacia los switches MDF en la sede Principal será a través un par de fibras oscuras de tipo monomodo con redundancia de rutas y switches de acceso..Se seleccionó dos switches Cisco Catalyst 6506 para proveer accesibilidad de los usuarios a los servidores y protección a través conexiones redundantes a los dos switches MDF diferentes ubicados en la sede Principal, además por que nos provee conexiones Giga Bit Ethernet de fibra monomodo (hacia los switches MDF de la sede Principal) y multimodo (hacia los servidores).

A continuación en la figura 8-15 y 8-16, se muestran las características físicas de los equipos que estan operando en la capa de distribución, conjuntamente con las tarjetas correspondientes al diseño anteriormente analizado, tales como el módulo Gigabit Ethernet, módulos Fast Ethernet y módulos 10/100 para la densidad de puertos

Las características técnicas, la descripción del panel frontal y posterior, así como también las opciones de administración de los equipos y los módulos respectivos de los equipos Catalyst Cisco 6500 y Cisco 8540, se muestran en el **ANEXO E.**

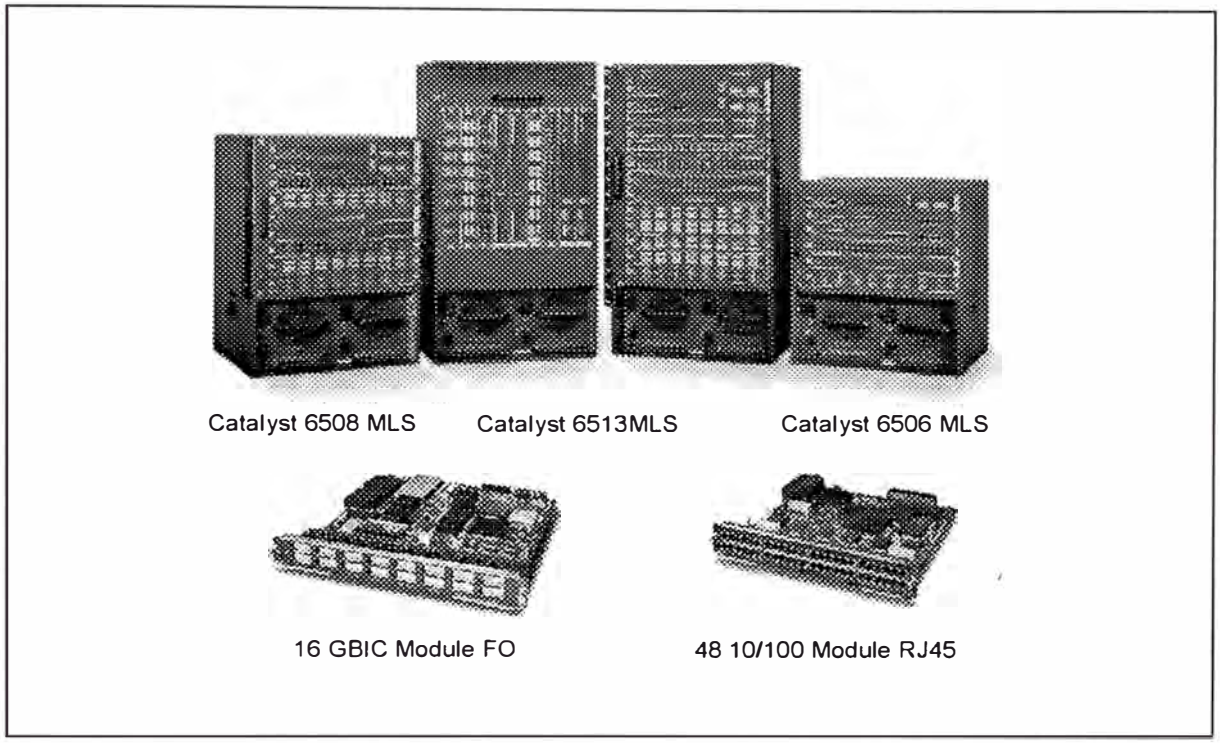


Figura 8-15 Catalyst 6500 Multilayer Switches y los múdulos GigaBit y 10/100 Ethernet.

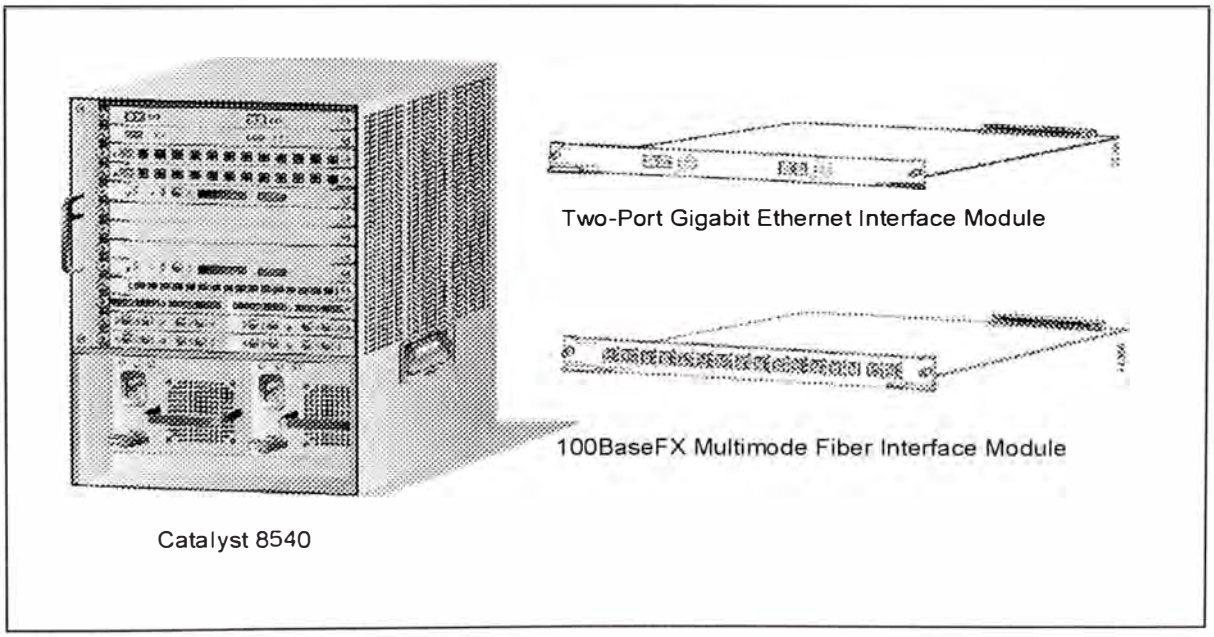


Figura 8-16 Catalyst 8500 Switching Router y los múdulos GigaBit y 10/100 Ethernet.

Finalmente, el equipo seleccionado para realizar las funciones dee ruteo, de protección y de conexión con las demás sedes de la red Corporativa fue un router Cisco 7206, quien conectado a los Switches de distribución a través de enlaces Fast Ethernet, enruta el tráfico saliente. Adicionalmente, la conexión a la WAN ATM fue realizada mediante un enlace OC-3 en la que se configuró PVC´s para las conexiones con las demás sedes remotas y PVC´s para la conexión al router de Borde de Internet Cisco 12012, para guiar todo el tráfico de Internet. En la figura 8-17, mostramos las característica físicas dedl router 7206 , instalado en la sede principal de la Red Corporativa.

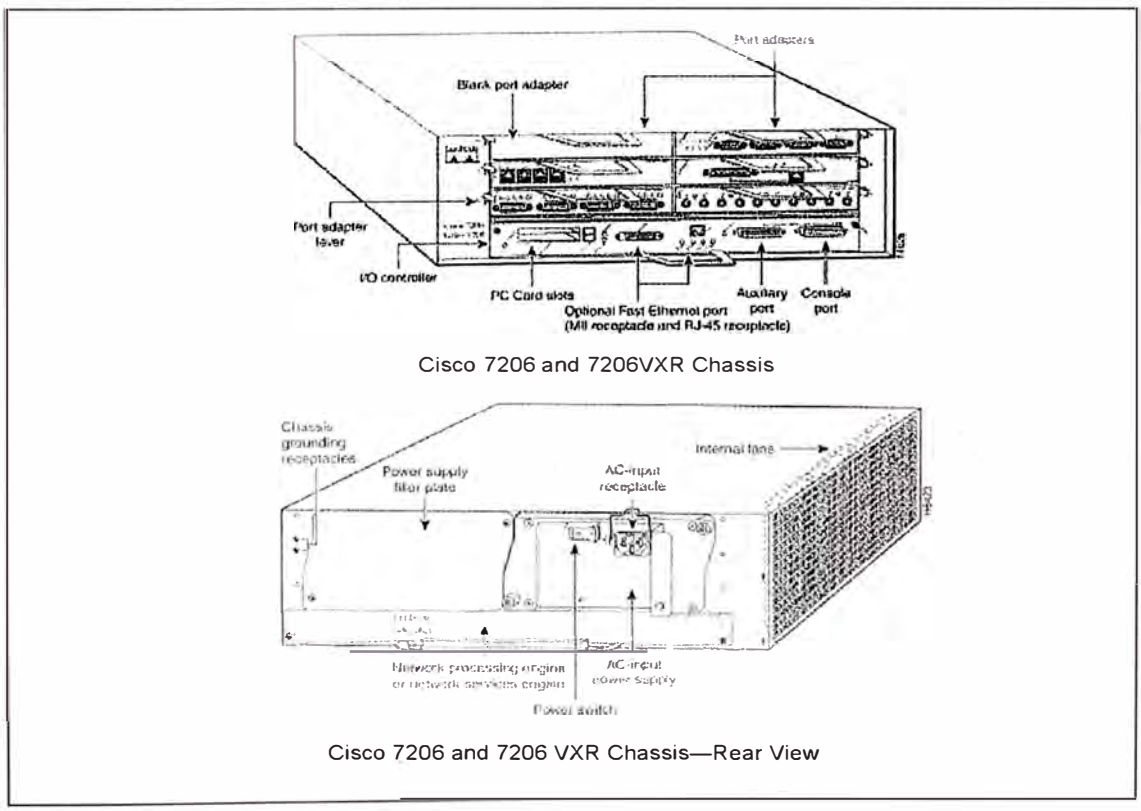


Figura 8-17 Router 7206 VXR vista frontal y posterior.

Las características técnicas, la descripción del equipo, así como también las opciones de administración del router 7206, se muestran en el **ANEXO F.**

8.3.2.- Orientación del Diseño

Asignando las VLANs.- El diseño utiliza 11 VLAN´s en el edificio Corporativo, dos VLAN´s en la sede Remota de San Isidro y dos VLAN´s en la sede Remota de San Juan de Miraflores. La primera VLAN en cada sede fue reservado para administración de VLAN´s y las otras 10 VLAN´s fueron usados por los usuarios finales como Ventas, Productos, Customer care y Call Center, Seguridad, Recursos Humanos, Ingeniería, Operaciones, Contraloría, Administración y Finanzas, Legal y Gerencia General. La tabla 8-8, nos presenta los nombres de lasVLAN´s y los valores asignados..

En dicha tabla, se diseñó una codificación de las números para representar de manera adecuada los departamentos dentro de cada oficina de la red Corporativa, ya sea Principal o las Remotas. Es así que el primer dígito del número de la VLAN especifica la sede a la que pertenece (1 Sede Principal, 2 Seded Remota S. Isidro y 3 Sede remota S.J. Miraflores), y los últimos dos dígitos especifica la VLAN dentro de dicha sede.

ITEM	SITE	NOMBRE DE LAS AREAS EN LA RED CORPORATIVA	NUMERO VLAN	SUBNET
I.0 SEDE PRINICPAL: MIRAFLORES				
1	Piso 6	Gerencia General, Imagen Institucional y Legal	102	10.1.102.0
2	Piso 5	Administración y Finanzas	103	10.1.103.0
3	Piso 4	Operaciones - NOC, Mantenimiento e Instalaciones	104	10.1.104.0
4		Information Technology	105	10.1.105.0
5	Piso 3	Ingeniería	106	10.1.106.0
6		Recursos Humanos	107	10.1.107.0
7		Administración de Seguridad	108	10.1.108.0
8	Piso 2	Ventas y Ventas Corporativas	109	10.1.109.0
9		Customer Care y Call Center	110	10.1.110.0
10	Piso 1	Productos y Servicios	111	10.1.111.0
11		Management	101	10.1.101.0
II.0 SEDE REMOTA: SAN ISIDRO				
12	Piso 2	Operaciones - Internet Service Provider	204	10.2.204.0
		Server Farm	100	10.1.100.0
13		Management	201	10.2.201.0
III.0 SEDE REMOTA: S. J. MIRAFLORES				
14	Piso 1	Operaciones - Telefonía y Transmisiones	304	10.3.304.0
15		Management	301	10.3.301.0

Tabla 8-8 Asignamiento y distribución de VLAN´s a las áreas respectivas, dentro de la Red Corporativa de AmericaCom.

Es necesario notar aquí que implementando las VLAN´s de esa manera separa el tráfico de administración y el tráfico de usuario final. Esto es hecho para aislar el CPU del Cátalyst del tráfico broadcast que prodría ser presentado en las VLANs´s de los usuarios finales. De esta manera se mejora la estabilidad de la red.

Asignación de Dirfecciones IP.- Cada VLAN utiliza un único subnet IP. Para el caso de AmericaCom utilizamos la red 10.0.0.0 con Network Address Translation (NAT) para llegar a Internet. El patrón de asignación se muestra en el siguiente esquema dirección IP

IP Address : 10 . Sede . VLAN . Usuario
Subnet Mask: 255 . 255 . 255 . 0

Debido a que se estaría utilizando la tecnología HSRP (descrito anteriormente), tres direcciones de nodos son reservados para los routers en cada subnet. La dirección .1 será reservado para dirección HSRP compartido, mientras que el .2 y el .3 serán usados para las direcciones reales asociadas con cada router. A ntinuación mostramos en la tabla 8-9 un esquema, en la cual presentamos las direcciones subnet IP de la red.

ITEM	SITE	NOMBRE DE LAS AREAS EN LA RED CORPORATIVA	NUMERO VLAN	SUBNET
I.0 SEDE PRINICPAL: MIRAFLORES				
1	Piso 6	Gerencia General, Imagen Institucional y Legal	102	10.1.102.0
2	Piso 5	Administración y Finanzas	103	10.1.103.0
3	Piso 4	Operaciones - NOC, Mantenimiento e Instalaciones	104	10.1.104.0
4		Information Technology	105	10.1.105.0
5	Piso 3	Ingeniería	106	10.1.106.0
6		Recursos Humanos	107	10.1.107.0
7		Administración de Seguridad	108	10.1.108.0
8	Piso 2	Ventas y Ventas Corporativas	109	10.1.109.0
9		Customer Care y Call Center	110	10.1.110.0
10	Piso 1	Productos y Servicios	111	10.1.111.0
11		Management	101	10.1.101.0
II.0 SEDE REMOTA: SAN ISIDRO				
12	Piso 2	Operaciones - Internet Service Provider	204	10.2.204.0
		Server Farm	100	10.100.100.0
13		Management	201	10.2.201.0
III.0 SEDE REMOTA: S. J. MIRAFLORES				
14	Piso 1	Operaciones - Telefonía y Transmisiones	304	10.3.304.0
15		Management	301	10.3.301.0

Tabla 8-9 Asignamiento y distribución de Subnets IP a las áreas respectivas, dentro de la Red Corporativa de AmericaCom.

Adicionalmente se ha considerado el uso de DHCP en la red. Las primeras 20 direcciones en cada segmento fueron reservados para dispositivos que no utilizan DHCP tales como impresoras, servidores y direcciones de routers. Las direcciones en cada subnet se dividieron entre un par de servidores DHCP para redundancia. Esto nos permite que si en caso un servidor falla, el otro tendría su propio bloque de direcciones para cada subnet.

Definiendo el Nombre de Dominio VTP.- Para maximizar la orientación del diseño a capa-2, usamos VTP modo server. Sin embargo, como el diseño solo muestra una sede compleja, usamos un único dominio de VTP en la sede Principal. Debido a que el cátalyst únicamente intercambia información VTP si los dominios VTP comparados coinciden, este crea una barrera VTP. Es así que nominaremos como dominio VTP a la sede Principal el nombre dee AmericaCom-B1.

Definiendo los Trunks.- Para mejorar la estabilidad y escalabilidad de la red, el diseño llama para muchas optimizaciones en los enlaces trunk. Primero, es recomendado que las configuraciones manuales sean usados para sobrellevar todos los protocolos de negociación de velocidad, duplex y trunk. Relyin en autonegociación de velocidades Ethernet 10/100 podría crear horas de frustación en el diagnostico del problema. Para evitar esto, es importante que los trunk y los enlaces a servidores sean Hard-coded. Las estaciones finales generalmente continuan el uso de protocolos de

autonegociación para maximizar la libertad de movimiento en el desarrollo de la PC. Similarmente, los enlaces trunks tienen información de estado del trunk hard-coded.

Segundo, el diseño recomienda que los enlaces trunk sean pruned de innecesario VLAN´s, por que esto puede construir innecesario broadcast flooding, la cual puede ser una importante optimización en redes orientadas a capa 2.

De esta manera, los enlaces Gigabit Ethernet desde los switches de acceso 3500XL instalados en cada piso de la Sede Principal hacia los switches de distribución Catalyst 6506 y 8540 fueron configurados como Trunks.

Definiendo el Balanceo de Carga.- Debido a la orientación a capa-2 del diseño, el balanceo de carga Spanning Tree tiene que ser empleado. La forma y ubicación del Root Bridge deel Spanning Tree es efectivo y simple de configurar y mantener. Una de las ventajas dee tener un triángulo de capa 2 empleado por el diseño es que facilita esta forma de balanceo ded carga. Es así que hacemos que el Catalyst Cat-B1-0A sea el Root Bridge para la VLAN 21, el tráfico de la VLAN de Ventas automáticamente usa el enlace de subidad izquierdo. Del diseño hacemos que el switch capa 3 o MDF´s (Cat-B1-0A) actue como Root Bridge para el tráfico de las VLAN

numeradas impares, mientras que el switch-capa 3 de la derecha (Cat-B1-0B) manipule el tráfico de las VLANs nuneradas pares.

Adicionalmente, para crear un sistema de balanceo de carga, la ubicación del Root Bridge del Spanning Tree debería ser coordinado con el HSRP. Esto se realizará con el comando HSRP priority, lo cual nos permite alternar el activo HSRP peer para VLANs pares e impares.

Definiendo Spanning-Tree.- Adicional a la ubicación del Root Bridge, otros parámetros de Spanning Tree debería ser modificado en el diseño. Debido a que la barrera capa-3 del diseño limita la conectividad de capa 2 a pequeños triángulos, el número máximo de bridges que puedes existir entre dos estaciones finales es tres hops (saltos).

Además, los parámetros Fordware Delay y Max Age puede ser cuidadosamente reducida a 12 y 9 segundos, respectivamente (asumiendo el valor por defecto dedl Hello Time de 2 segundos). La forma mas simple y cuidadosa de cumplir con esto es modificar los parámetros Spanning Tree a traves de los comandos respectivos. Como resultado, el tiempo dee convergencia puede ser reducida de un valor ded 30-50 segundos a 18-30 segundos.

8.3.3.- Configuraión de los Equipos en la Red Corporativa

Para el proceso de configuración de los equipos Switches, Catalyst y Routers, nosotros usamos los siguientes softwares ó sistemas operativos:

Catalyst 3524XL switch running Cisco IOS® 12.0(5)WC7
Catalyst 5500 switch running Catalyst OS 6.4(2) software

Las configuraciones en este documento fueron implementadas asegurando que todas sean claras, y así mismo entender el impacto que cualquier configuración o comando producirá en la red antes de usarlo.

Configuración de los Switches Catalyst 3500XL.- Los Switches 3500XL fueron instalados en la capa de Acceso del modelo herárquico. Este equipo concentrará a todos los usuarios de la Sede Principal. Las configuraciones para cada switch se describen a continuación:

- Configurando el nombre a los switches: Esto nos permite darle una identificación a cada switch instalado. De esta manera poder administrarlo mejor e identificarlo dee los demás equipos en la red. A continuación se detalla los pasos de configuración realizada para al fin.

```
IOSSwitch#config terminal
IOSSwitch(config)#hostname Switch_Piso1_1
Switch_Piso1_1#

IOSSwitch#config terminal
IOSSwitch(config)#hostname Switch_Piso1_3
Switch_Piso1_3#

IOSSwitch#config terminal
IOSSwitch(config)#hostname Switch_Piso1_2
Switch_Piso1_2#

.
.
.
.
.

OSSwitch#config terminal
IOSSwitch(config)#hostname Switch_Piso 6_1
Switch_Piso6_1#

IOSSwitch#config terminal
IOSSwitch(config)#hostname Switch_Piso6_2
Switch_Piso6_2#
```

- Asignamiento manual de información IP del Switch: Manualmente asignamos una dirección IP y un default gateway a los switches. La mask identifica los bits que denota el número de subnet en la dirección IP. Las direcciones broadcast fueron reservados para enviar mensajes a todos los hosts. Así mismo el CPU envía mensajes a una dirección no concida a través de un default gateway. A continuación se detalla los pasos de configuración realizada para al fin.

```
Switch_Piso1_1# config terminal
Switch_Piso1_1(config) # interface VLAN 101
Switch_Piso1_1(config-if) # ip adddress 10.1.101.21 255.255.255.0
Switch_Piso1_1(config-if) #  exit
Switch_Piso1_1(config) # ip default-gateway 10.1.101.3
Switch_Piso1_1(config) # end
Switch_Piso1_1#

Switch_Piso2_1# config terminal
Switch_Piso2_1(config) # interface VLAN 101
Switch_Piso2_1(config-if) # ip adddress 10.1.101.24 255.255.255.0
Switch_Piso2_1(config-if) #  exit
Switch_Piso2_1(config) # ip default-gateway 10.1.101.3
Switch_Piso2_1(config) # end
Switch_Piso2_1#
                .
                .
                .
                .
                .

Switch_Piso5_1# config terminal
Switch_Piso5_1(config) # interface VLAN 101
Switch_Piso5_1(config-if) # ip adddress 10.1.101.33 255.255.255.0
Switch_Piso5_1(config-if) #  exit
Switch_Piso5_1(config) # ip default-gateway 10.1.101.3
Switch_Piso5_1(config) # end
Switch_Piso5_1#

Switch_Piso6_2# config terminal
Switch_Piso6_2(config) # interface VLAN 101
Switch_Piso6_2(config-if) # ip adddress 10.1.101.37 255.255.255.0
Switch_Piso6_2(config-if) #  exit
Switch_Piso6_2(config) # ip default-gateway 10.1.101.3
Switch_Piso6_2(config) # end
Switch_Piso6_2#
```

- Configurando VLAN Trunking Protocol: VTP is a protocolo de mesagería de capa 2, que mantiene las configuraciones de VLAN de manera consistente, mediante la administración, adición, borrado y renombramiento de VLANs en la Red corporativa. VTP minimiza los errores de configuración o las inconsistencias causadas por muchos problemas, tales como nombres de VLAN duplicados, tipo de VLAN incorrecto y violaciones a la seguridad. A continuación se detalla los pasos de configuración realizada para al fin.

```
Switch_Piso1_1# vlan database
Switch_Piso1_1(vlan) # vtp client
Switch_Piso1_1(vlan) # vtp domaing AmericaCom-B1
Switch_Piso1_1(vlan) # vtp password AmericaCom
Switch_Piso1_1(vlan) #  exit
Switch_Piso1_1#
        .
        .
        .
        .
        .

Switch_Piso6_2# vlan database
Switch_Piso6_2(vlan) # vtp client
Switch_Piso6_2(vlan) # vtp domaing AmericaCom-B1
Switch_Piso6_2(vlan) # vtp password AmericaCom
Switch_Piso6_2(vlan) #  exit
Switch_Piso6_2#
```

- Creando VLAN y asignamiento de ports: Cada VLAN tiene un único ID de 4 dígitos, que puededn ser números deel 1 al 1001. Para adicionar una VLAN a una base de datos VLAN, asigna números y nombres a la VLAN. Por defecto, todos los puertos son static-access asignados a la VLAN 1. Si asignamos un puerto a un switch miembro de un clusterr a una VLAN, primero nos registramos en un switch miembro, mediante el uso del comando *rcommand* en el modo privileged EXEC. A continuación se detalla los pasos de configuración realizada para tal fin.

```
Switch_Piso1_1# vlan database
Switch_Piso1_1(vlan) # vlan 101 name management
Vlan 101 configuration successful
Switch_Piso1_1(vlan) # vlan 111 name Productos&Servicios
Vlan 111 configuration successful
Switch_Piso1_1(vlan) # vlan 109 name Ventas&Corporativas
Vlan 109 configuration successful
Switch_Piso1_1(vlan) #  exit
Switch_Piso1_1#

Switch_Piso2_1# vlan database
Switch_Piso2_1(vlan) # vlan 101 name management
Vlan 101 configuration successful
Switch_Piso2_1(vlan) # vlan 109 name Ventas
Vlan 109 configuration successful
Switch_Piso2_1(vlan) # vlan 110 name CustomerCare&CallCenter
Vlan 110 configuration successful
Switch_Piso2_1(vlan) #  exit
Switch_Piso2_1#

Switch_Piso3_1# vlan database
Switch_Piso3_1(vlan) # vlan 101 name management
Vlan 101 configuration successful
Switch_Piso3_1(vlan) # vlan 106 name Ingenieria
Vlan 106 configuration successful
Switch_Piso3_1(vlan) # vlan 107 name RecursoHumanos
Vlan 107 configuration successful
Switch_Piso3_1(vlan) # vlan 108 name Seguridad
Vlan 108 configuration successful
Switch_Piso3_1(vlan) #  exit
Switch_Piso3_1#
          .
          .
          .
          .
          .

Switch_Piso6_1# vlan database
Switch_Piso6_1(vlan) # vlan 101 name management
Vlan 101 configuration successful
Switch_Piso6_1(vlan) # vlan 102 name GGeneral&Legal
Vlan 102 configuration successful
Switch_Piso6_1(vlan) #  exit
Switch_Piso6_1#
```

Podemos adicionar los ports (interfaces) en una VLAN nueva creada, ingresando al modo de configuración de interface para cada una de las interfaces que se quiere adicionar a la nueva VLAN Usa mos los siguientes conjuntos de comandos en el modos previligiado para adicionar uan interface particular en la VLAN creada.

```
Switch_Piso1_1# config terminal
Switch_Piso1_1(config) # interface fastEthernet 0/3
Switch_Piso1_1(config-if) # switchport access vlan 111
Switch_Piso1_1(config-if) #  exit

!-- Assigning interface fa0/3 to vlan 111

Switch_Piso1_1(config) # interface fastEthernet 0/45
Switch_Piso1_1(config-if) # switchport access vlan 108
Switch_Piso1_1(config) # end
Switch_Piso1_1#

!-- Assigning interface fa0/45 to vlan 108

Switch_Piso2_1# config terminal
Switch_Piso2_1(config) # interface fastEthernet 0/10
Switch_Piso2_1(config-if) # switchport access vlan 110
Switch_Piso2_1(config-if) #  exit

!-- Assigning interface fa0/10 to vlan 110
                .
                .
                .
                .
                .

Switch_Piso5_1(config) # interface fastEthernet 0/24
Switch_Piso5_1(config-if) # switchport access vlan 103
Switch_Piso5_1(config) # end
Switch_Piso5_1#

!-- Assigning interface fa0/24 to vlan 103

Switch_Piso6_1# config terminal
Switch_Piso6_1(config) # interface fastEthernet 0/13
Switch_Piso6_1(config-if) # switchport access vlan 102
Switch_Piso6_1(config-if) #  exit

!-- Assigning interface fa0/13 to vlan 102
```

- Configurando Trunking LAN ISL: Trunking es una forma de llevar tráfico de muchos VLAN´s sobre un enlace punto a punto entre dos dispositivos. Existe dos formas en la que Ethernet trunking puede ser implementado: ISL (Cisco proprietary InterSwitch Link protocol) y 802.1q (Institute of Electrical and Electronics Engineers (IEEE) standard). Nosotros creamos Trunks que llevan tráfico de VLAN´s a través de los enlaces entre el Catalyst 3500 y un Catalyst 6500

switch. A continuación se detalla los pasos de configuración realizada para tal fin.

```
Switch_Piso1_1# config terminal
Switch_Piso1_1(config) # interface GigabitEthernet 0/1
Switch_Piso1_1(config-if) # switchport mode trunk
Switch_Piso1_1(config-if) # switchport trunk encapsulation isl
Switch_Piso1_1(config-if) # exit

!-- Assigning interface Gbit 0/1 with trunk mode

Switch_Piso1_3 # config terminal
Switch_Piso1_3(config) # interface GigabitEthernet 0/1
Switch_Piso1_3(config-if) # switchport mode trunk
Switch_Piso1_3(config-if) # switchport trunk encapsulation isl
Switch_Piso1_3(config-if) # exit

!-- Assigning interface Gbit 0/1 with trunk mode

Switch_Piso2_1# config terminal
Switch_Piso2_1(config) # interface GigabitEthernet 0/1
Switch_Piso2_1(config-if) # switchport mode trunk
Switch_Piso2_1(config-if) # switchport trunk encapsulation isl
Switch_Piso2_1(config-if) # exit

!-- Assigning interface Gbit 0/1 with trunk mode

Switch_Piso2_3 # config terminal
Switch_Piso2_3(config) # interface GigabitEthernet 0/1
Switch_Piso2_3(config-if) # switchport mode trunk
Switch_Piso2_3(config-if) # switchport trunk encapsulation isl
Switch_Piso2_3(config-if) # exit

!-- Assigning interface Gbit 0/1 with trunk mode
                .
                .
                .
                .
                .

Switch_Piso6_1 # config terminal
Switch_Piso6_1(config) # interface GigabitEthernet 0/1
Switch_Piso6_1(config-if) # switchport mode trunk
Switch_Piso6_1(config-if) # switchport trunk encapsulation isl
Switch_Piso6_1(config-if) # exit

!-- Assigning interface Gbit 0/1 with trunk mode

Switch_Piso6_2 # config terminal
Switch_Piso6_2(config) # interface GigabitEthernet 0/1
Switch_Piso6_2(config-if) # switchport mode trunk
Switch_Piso6_2(config-if) # switchport trunk encapsulation isl
Switch_Piso6_2(config-if) # end
Switch_Piso6_2 #

!-- Assigning interface Gbit 0/1 with trunk mode
```

- Configurando Spanning Tree Proptocol (STP): STP provee rutas redundantes mientras prevenimos de loops indeseados en la red. únicamente una ruta activa puede existir entre dos estaciones. STP calcula la mejor ruta loop-free a través de la red. Los Catalyst 3500 XL switches supportan 64 STP instances y 250 VLANs. Cross-stack UplinkFast (CSUF) provee una transiución spanning-tree muy rápido (ráopida convergencia en menos de 2 segundos bajo condiciones normales ded red) a través dee un stack de switches que usan el GigaStack GBICs conectados en configuración compartida en cascada (multidrop backbone).CSUF no podría proveer una rápida transición todos las veces, en estos casos, ocurre una normal transición STP, que se completa en 30 a 40 segundos. A continuación desarrollamos un esquema de switches configurados en modo stack.

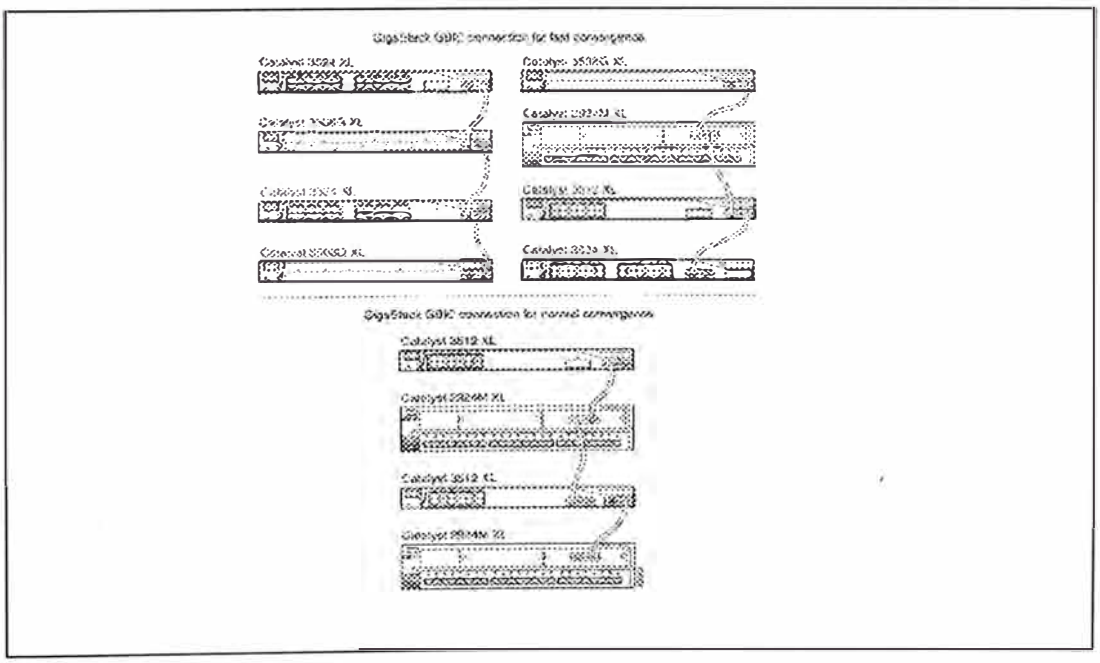


Figura 8-18 Switches 3500 XL coinfigurados en modo stack a través de los enlaces GBIC.

A continuación se detalla los pasos de configuración realizada para tal fin.

```
Switch_Piso1_1# config terminal
Switch_Piso1_1(config) # spanning-tree vlan 111,109
Switch_Piso1_1(config) # interface GigabitEthernet 0/2
Switch_Piso1_1(config-if) # spanning-tree stack-port
Switch_Piso1_1(config-if) # exit

!-- Assign vlan stp list in last two another switches

Switch_Piso2_1# config terminal
Switch_Piso2_1(config) # spanning-tree vlan 109,110
Switch_Piso2_1(config) # interface GigabitEthernet 0/2
Switch_Piso2_1(config-if) # spanning-tree stack-port
Switch_Piso2_1(config-if) # exit

!-- Assign vlan stp list in last two another switches

Switch_Piso3_1# config terminal
Switch_Piso3_1(config) # spanning-tree vlan 106,107,108
Switch_Piso3_1(config) # interface GigabitEthernet 0/2
Switch_Piso3_1(config-if) # spanning-tree stack-port
Switch_Piso3_1(config-if) # exit

!-- Assign vlan stp list in last two another switches
                .
                .
                .
                .
                .

Switch_Piso5_1 # config terminal
Switch_Piso5_1(config) # spanning-tree vlan 103
Switch_Piso5_1(config) # interface GigabitEthernet 0/2
Switch_Piso5_1(config-if) # spanning-tree stack-port
Switch_Piso5_1(config-if) # exit

!-- Assign vlan stp list in last two another switches

Switch_Piso6_1 # config terminal
Switch_Piso6_1(config) # spanning-tree vlan 102
Switch_Piso6_1(config) # interface GigabitEthernet 0/2
Switch_Piso6_1(config-if) # spanning-tree stack-port
Switch_Piso6_1(config-if) # exit

!-- Assign vlan stp list in last another switches
```

- Balanceo de carga usando STP: El balanceo de carga divide the bandwidth que tenemos por trunks paralelos que conectan los switches. Para evitar Loops, STP normalmente bloquea todos pero menos un enlace paralelo entre los switches. Con balanceo de carga,

dividimos el tráfico entre los enlaces de acuerdo a que tráfico de VLAnN es generado. Se configura balanceo de carga en trunk ports usando port priorities o STP path costs. Para balanceo de carga usando STP path costs, cada enlace load-sharing puede ser conectada al mismo switch o a dos switches diferentes.

```
Switch_Piso1_1# config terminal
Switch_Piso1_1(config) # interface GigabitEthernet 0/1
Switch_Piso1_1(config-if) # spanning-tree vlan 109 cost 30
Switch_Piso1_1(config-if) # exit

!-- Assign cost 30 to vlan 109. vlan 111 defasult cost 19

Switch_Piso1_3# config terminal
Switch_Piso1_3(config) # interface GigabitEthernet 0/1
Switch_Piso1_3(config-if) # spanning-tree vlan 111 cost 30
Switch_Piso1_3(config-if) # exit

!-- Assign cost 30 to vlan 111. vlan 109 defasult cost 19

Switch_Piso3_1# config terminal
Switch_Piso3_1(config) # interface GigabitEthernet 0/1
Switch_Piso3_1(config-if) # spanning-tree vlan 106,107 cost 30
Switch_Piso3_1(config-if) # exit

!-- Assign cost 30 to vlan 106,107. vlan 108 defasult cost 19

Switch_Piso3_3# config terminal
Switch_Piso3_3(config) # interface GigabitEthernet 0/1
Switch_Piso3_3(config-if) # spanning-tree vlan 108 cost 30
Switch_Piso3_3(config-if) # exit

!-- Assign cost 30 to vlan 108. vlan 106,107 defasult cost 19

.
.
.
.
.

Switch_Piso6_1# config terminal
Switch_Piso6_1(config) # interface GigabitEthernet 0/1
Switch_Piso6_1(config-if) # spanning-tree vlan 102 cost 19
Switch_Piso6_1(config-if) # exit

!-- Assign cost 19 to vlan 102.

Switch_Piso6_2# config terminal
Switch_Piso6_2(config) # interface GigabitEthernet 0/1
Switch_Piso6_2(config-if) # spanning-tree vlan 102 cost 30
Switch_Piso6_2(config-if) # exit

!-- Assign cost 30 to vlan 102.
```

Configuración de los Switches Catalyst 6500.- Los Switches 6500 fueron instalados en la capa de Distribución del modelo jerárquico. Este equipo concentrará a todos los trunks creados en los switches de acceso para cada uno de los pisos en la Sede Principal. Las configuraciones para cada switch se describen a continuación:

- Configurando el nombre a los switches: Esto nos permite darle una identificación a cada switch instalado. De esta manera poder administrarlo mejor e identificarlo de los demás equipos en la red.

```
CatosSwitch> (enable)  set system name Cat-B1
Cat-B1 > (enable)  set vtp domain AmericaCom-B1
VTP domain AmericaCom-B1 modified
Cat-B1 > (enable)  set vtp mode server
VTP domain AmericaCom-B1 modifie
Cat-B1 > (enable)  set interface sc0 101 10.1.101.38 255.255.255.0
Interface sc0 vlan set, IP address and mask set
Cat-B1 > (enable)  set ip route default 10.1.101.3
Route added.

CatosSwitch> (enable)  set system name Cat-B2
Cat-B2 > (enable)  set vtp domain AmericaCom-B1
VTP domain AmericaCom-B1 modified
Cat-B2 > (enable)  set vtp mode server
VTP domain AmericaCom-B1 modifie
Cat-B2 > (enable)  set interface sc0 101 10.1.101.39 255.255.255.0
Interface sc0 vlan set, IP address and mask set
Cat-B2 > (enable)  set ip route default 10.1.101.3
Route added.
```

- Para implementar balanceo de carga, los switches MDF requiere mas configuración de Spanning Tree que los switches IDF. El comando set spantree root configura que el switch Cat-B1 sea el root bridge para las VLAN's 111,110,106,107,104,103 y 102 , mientras que el switch Cat-B2 sea el root bridge para las VLAN´s 109,108,105, 03 y 102.

```
Cat-B1 > (enable)  set spantree root 111 dia 3 hello 2
VLAN 111 bridge priority set to 8192
VLAN 111 bridge max aging time set to 12
VLAN 111 bridge helo time set to 2
VLAN 111 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root secondary 109 dia 3 hello 2
VLAN 109 bridge priority set to 16384
VLAN 109 bridge max aging time set to 12
VLAN 109 bridge helo time set to 2
VLAN 109 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root 110 dia 3 hello 2
VLAN 110 bridge priority set to 8192
VLAN 110 bridge max aging time set to 12
VLAN 110 bridge helo time set to 2
VLAN 110 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root 106,107 dia 3 hello 2
VLAN 106,107 bridge priority set to 8192
VLAN 106,107 bridge max aging time set to 12
VLAN 106,107 bridge helo time set to 2
VLAN 106,107 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root secondary 108 dia 3 hello 2
VLAN 108 bridge priority set to 16384
VLAN 108 bridge max aging time set to 12
VLAN 108 bridge helo time set to 2
VLAN 108 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root 104 dia 3 hello 2
VLAN 104 bridge priority set to 8192
VLAN 104 bridge max aging time set to 12
VLAN 104 bridge helo time set to 2
VLAN 104 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root secondary 105 dia 3 hello 2
VLAN 105 bridge priority set to 16384
VLAN 105 bridge max aging time set to 12
VLAN 105 bridge helo time set to 2
VLAN 105 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B1 > (enable)  set spantree root 103 dia 3 hello 2
VLAN 103 bridge priority set to 8192
VLAN 103 bridge max aging time set to 12
VLAN 103 bridge helo time set to 2
VLAN 103 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B2 > (enable)  set spantree root secondary 103 dia 3 hello 2
VLAN 103 bridge priority set to 16384
VLAN 103 bridge max aging time set to 12
VLAN 103 bridge helo time set to 2
VLAN 103 bridge forward delay set to 9
Cat-B2 > (enable)
Cat-B1 > (enable)  set spantree root 102 dia 3 hello 2
VLAN 102 bridge priority set to 8192
VLAN 102 bridge max aging time set to 12
VLAN 102 bridge helo time set to 2
VLAN 102 bridge forward delay set to 9
Cat-B1 > (enable)
Cat-B2 > (enable)  set spantree root secondary 102 dia 3 hello 2
VLAN 102 bridge priority set to 16384
VLAN 102 bridge max aging time set to 12
VLAN 102 bridge helo time set to 2
VLAN 102 bridge forward delay set to 9
Cat-B2 > (enable)
```

- En esta parte, al igual que en los switches IDF, configuramos los nombres de los enlaces y hard-coded a ser una trunk ISL. Y también los enlaces trunk Gigabit Ethernet desde los switches MDF hacia los switches IIDF´s. Se borró las deemás VLAN´s para cada trunk, debido a que no estan operativas. Sin embargo es importante mencionar que aunque en un plan a primera etapa las áreas de Ventas y Customer Care comparten el mismo piso, la compañía conoce que habrá una gran cantidad de movimiento entr los pisos.

```
Cat-B1 > (enable) set port name 2/1 Gigabit link to Switch_Piso1_1
Port 2/1 name set
Cat-B1 > (enable) set port name 2/2 Gigabit link to Switch_Piso2_1
Port 2/2 name set
Cat-B1 > (enable) set port name 2/3 Gigabit link to Switch_Piso3_1
Port 2/3 name set
Cat-B1 > (enable) set port name 2/4 Gigabit link to Switch_Piso4_1
Port 2/4 name set
Cat-B1 > (enable) set port name 2/5 Gigabit link to Switch_Piso5_1
Port 2/1 name set
Cat-B1 > (enable) set port name 2/6 Gigabit link to Switch_Piso6_1
Port 2/6 name set
Cat-B1 > (enable) set trunk 2/1 on isl
Port(s) 2/1 trunk mode set to on.
Port(s) 2/1 trunk type set to isl
Cat-B1 > (enable) clear trunk 2/1 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port 2/1 allowed vlans modified to 1,101-111.
Cat-B1 > (enable) set trunk 2/2 on isl
Port(s) 2/2 trunk mode set to on.
Port(s) 2/2 trunk type set to isl
Cat-B1 > (enable) clear trunk 2/2 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port 2/2 allowed vlans modified to 1,101-111.
Cat-B1 > (enable) set trunk 2/3 on isl
Port(s) 2/3 trunk mode set to on.
Port(s) 2/3 trunk type set to isl
Cat-B1 > (enable) clear trunk 2/3 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port 2/3 allowed vlans modified to 1,101-111.
Cat-B1 > (enable) set trunk 2/4 on isl
Port(s) 2/4 trunk mode set to on.
Port(s) 2/4 trunk type set to isl
Cat-B1 > (enable) clear trunk 2/4 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port 2/4 allowed vlans modified to 1,101-111.
```

```
Cat-B1 > (enable)  set trunk 2/5 on isl
Port(s)  2/5 trunk mode set to on.
Port(s)  2/5 trunk type set to isl
Cat-B1 > (enable)  clear trunk 2/5 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port  2/5 allowed vlans modified to 1,101-111.
Cat-B1 > (enable)  set trunk 2/6 on isl
Port(s)  2/6 trunk mode set to on.
Port(s)  2/6 trunk type set to isl
Cat-B1 > (enable)  clear trunk 2/6 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port  2/6 allowed vlans modified to 1,101-111.
```

- Adicionalmente, podemos configurar Password, Banners, System Information, DNS, IP Permit List, IGMP, Snooping, SNMP y Syslog, las cuales son mostradas a continuación:

```
Cat-B1 > (enable)  set password
Enter old password: Cisco
Enter new password: AmericaCom-B1
Retype new password: AmericaCom-B1
Password changed
Cat-B1 > (enable)
Cat-B1 > (enable)  set enabled
Enter old password: Cisco
Enter new password: AmericaCom-B1
Retype new password: AmericaCom-B1
Password changed
Cat-B1 > (enable)
Cat-B1 > (enable)  set banner motd - RED PRIVADA - DO NOT ENTER!-
Cat-B1 > (enable)  set system location  Sede Principal MDF
Cat-B1 > (enable)  set ip dns enabled
Cat-B1 > (enable)  set ip dns domain AmericaCom.com
Cat-B1 > (enable)  set ip dns server 10.1.40.42
Cat-B1 > (enable)  set ip dns server 10.1.40.68
Cat-B1 > (enable)  set ip permit enabled
Cat-B1 > (enable)  set ip igmp enabled
Cat-B1 > (enable)  set ip snmp community read-only lesspublic
Cat-B1 > (enable)  set ip snmp community read-write moreprivate
Cat-B1 > (enable)  set snmp trap 10.1.40.20 trapped
Cat-B1 > (enable)  set snmp trap enabled module
Cat-B1 > (enable)  set snmp trap enabled chassis
Cat-B1 > (enable)  set snmp trap enabled bridge
Cat-B1 > (enable)  set snmp trap enabled auth
Cat-B1 > (enable)  set snmp trap enabled config
Cat-B1 > (enable)  set logging server enabled
Cat-B1 > (enable)  set logging server 10.1.40.20
Cat-B1 > (enable)  set logging server enabled
Cat-B1 > (enable)
```

- Finalmente, mostramos las configuraciones realizadas para el routing entre las VLAN´s, llevada a cabo en en el router 7206, permitiendo que las VLAN´s configuradas puedan comunicarse entre ellos y además implementamos Hot Standby Router Protocol (HRSP) para obtener rutas redundantes. Así la configuración en el Cat-B1 para una insterface Fast Ethernet conectada al router será:

```
Cat-B1 > (enable)  set trunk 3/1 on isl
Port(s)  3/1 trunk mode set to on.
Port(s)  3/1 trunk type set to isl
Cat-B1 > (enable)  clear trunk 3/1 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port  3/1 allowed vlans modified to 1,101-111.
Cat-B1 > (enable)
Cat-B2 > (enable)  set trunk 3/1 on isl
Port(s)  3/1 trunk mode set to on.
Port(s)  3/1 trunk type set to isl
Cat-B2 > (enable)  clear trunk 3/1 2-100,112-1005
Removing Vlan(s) 2-100,112-1005 from allowed list
Port  3/1 allowed vlans modified to 1,101-111.
```

Adicionalmente, mostramos las configuraciones realizadas para las conexiones al site dee servidores ubicado en San Isdro, llamdo Server Farm.

```
Cat-B1 > (enable)  set port name  2/7 Gigabit link to Switch_Servers_1
Port 2/7 name set
Cat-B1 > (enable)  set trunk 2/7 on isl
Port(s)  2/7 trunk mode set to on.
Port(s)  2/7 trunk type set to isl
Cat-B1 > (enable)  clear trunk 2/1 2-99,112-1005
Removing Vlan(s) 2-99,112-1005 from allowed list
Port  2/7 allowed vlans modified to 1,101-111.

Cat-B2 > (enable)  set port name  2/7 Gigabit link to Switch_Servers_1
Port 2/7 name set
Cat-B1 > (enable)  set trunk 2/7 on isl
Port(s)  2/7 trunk mode set to on.
Port(s)  2/7 trunk type set to isl
Cat-B2 > (enable)  clear trunk 2/1 2-99,112-1005
Removing Vlan(s) 2-99,112-1005 from allowed list
Port  2/7 allowed vlans modified to 1,101-111.
```

Configuración de los Routers 7206.- Los Routers 7206 fueron instalados en la capa de Distribución del modelo jerárquico para formar una barrera de capa 3 en la Sede Principal de la Red Corporativa. Estos equipo permitiran un balanceo de carga para los usuarios pertenecientes a cada VLAN en la red, donde algunos usuarios pertenecientes uan una VLAN van a tomar un router como su defaultr gateway y a otros tomaran el otros router como su default gateway.

- Configurando el nombre a los routers: Esto nos permite darle una identificación a cada router instalado. De esta manera poder administrarlo mejor e identificarlo de los demás equipos en la red.

```
Cisco7206 # config  terminal
Cisco7206(conf) # hostname americacom-R1
americacom-R1 #
Cisco7206 # config  terminal
Cisco7206(conf) # hostname americacom-R2
americacom-R2 #

americacom-R1 # config terminal
americacom-R1(config) # line console 0
americacom-R1(config-line) # login password americacomr1
americacom-R1(config-line) # exit
americacom-R1(config) # line vty 0 4
americacom-R1(config-line) # login password americacomr1
americacom-R1(config-line) # enabled password americacomr1
americacom-R1(config-line) # end

americacom-R2 # config terminal
americacom-R2(config) # line console 0
americacom-R2(config-line) # login password americacomr1
americacom-R2(config-line) # exit
americacom-R2(config) # line vty 0 4
americacom-R2(config-line) # login password americacomr1
americacom-R2(config-line) # enabled password americacomr1
americacom-R1(config-line) # end
```

- Configurando balanceo de carga con HSRP:: Hot Standby Router Protocol, es un técnica empleada para brindar balanceo de carga y ruta redundante a una red campus. Para nuestro caso, se confurara los routers de tal manera que el router1 será el activo HSRP peer para alguna VALN´s y el router2 lo será para otras.,

```
americacom-R1 # config terminal
americacom-R1(config) # interface FastEthernet 0/0/0
americacom-R1(config-if) # description Enlace al Switch -B1
americacom-R1(config-if) # no ip addressst
americacom-R1(config-if) # exit
!
americacom-R1(config) # interface FastEthernet 0/0/0.1
americacom-R1(config-if) # encapsulation isl 100
americacom-R1(config-if) # ip address 10.1.100.2 255.255.255.0
americacom-R1(config-if) # standby 1 priority 110
americacom-R1(config-if) # standby 1 prempt
americacom-R1(config-if) # standby 1 ip 10.1.100.1
americacom-R1(config-if) # standby 1 track ATM 6/0 15
!
americacom-R1(config) # interface FastEthernet 0/0/0.2
americacom-R1(config-if) # encapsulation isl 101
americacom-R1(config-if) # ip address 10.1.101.2 255.255.255.0
americacom-R1(config-if) # standby 2 priority 100
americacom-R1(config-if) # standby 2 prempt
americacom-R1(config-if) # standby 2 ip 10.1.102.1
!
americacom-R1(config) # interface FastEthernet 0/0/0.3
americacom-R1(config-if) # encapsulation isl 102
americacom-R1(config-if) # ip address 10.1.102.2 255.255.255.0
americacom-R1(config-if) # standby 3 priority 110
americacom-R1(config-if) # standby 3 prempt
americacom-R1(config-if) # standby 3 ip 10.1.102.1.
americacom-R1(config-if) # standby 3 track ATM 6/0  15
!
americacom-R1(config) # interface FastEthernet 0/0/0.4
americacom-R1(config-if) # encapsulation isl 103
americacom-R1(config-if) # ip address 10.1.103.2 255.255.255.0
americacom-R1(config-if) # standby 4 priority 100
americacom-R1(config-if) # standby 4 prempt
americacom-R1(config-if) # standby 4 ip 10.1.103.1
!
.
.
.
.
.
!
americacom-R1(config) # interface FastEthernet 0/0/0.12
americacom-R1(config-if) # encapsulation isl 111
americacom-R1(config-if) # ip address 10.1.111.2  255.255.255.0
americacom-R1(config-if) # standby 12 priority 100
americacom-R1(config-if) # standby 12 prempt
americacom-R1(config-if) # standby 12 ip 10.1.111.1
!
```

De la misma manera se realiza las configuraciones para el router2, las cuales se muestran a continuación.

```
americacom-R2 # config terminal
americacom-R2(config) # interface FastEthernet 0/0/0
americacom-R2(config-if) # description Enlace al Switch -B1
americacom-R2(config-if) # no ip addressst
americacom-R2(config-if) # exit
!
americacom-R2(config) # interface FastEthernet 0/0/0.1
americacom-R2(config-if) # encapsulation isl 100
americacom-R2(config-if) # ip address 10.1.100.3 255.255.255.0
americacom-R2(config-if) # standby 1 priority 100
americacom-R2(config-if) # standby 1 prempt
americacom-R2(config-if) # standby 1 ip 10.1.100.1
!
americacom-R2(config) # interface FastEthernet 0/0/0.2
americacom-R2(config-if) # encapsulation isl 101
americacom-R2(config-if) # ip address 10.1.101.3 255.255.255.0
americacom-R2(config-if) # standby 2 priority 110
americacom-R2(config-if) # standby 2 prempt
americacom-R2(config-if) # standby 2 ip 10.1.101.1
americacom-R2(config-if) # standby 2 track ATM 6/0 15
!
americacom-R2(config) # interface FastEthernet 0/0/0.3
americacom-R2(config-if) # encapsulation isl 102
americacom-R2(config-if) # ip address 10.1.102.3 255.255.255.0
americacom-R2(config-if) # standby 3 priority 100
americacom-R2(config-if) # standby 3 prempt
americacom-R2(config-if) # standby 3 ip 10.1.102.1.
!
americacom-R2(config) # interface FastEthernet 0/0/0.4
americacom-R2(config-if) # encapsulation isl 103
americacom-R2(config-if) # ip address 10.1.103.3 255.255.255.0
americacom-R2(config-if) # standby 4 priority 110
americacom-R2(config-if) # standby 4 prempt
americacom-R1(config-if) # standby 4 ip 10.1.103.1
americacom-R2(config-if) # standby 4 track ATM 6/0  15
!
.
.
.
.
.
!
americacom-R2(config) # interface FastEthernet 0/0/0.12
americacom-R2(config-if) # encapsulation isl 111
americacom-R2(config-if) # ip address 10.1.111.3 255.255.255.0
americacom-R2(config-if) # standby 12 priority 110
americacom-R2(config-if) # standby 12 prempt
americacom-R2(config-if) # standby 12 ip 10.1.111.1
americacom-R2(config-if) # standby 12 track ATM 6/0  15
!
```

- Configurando PVC´s para el enlace a Internet: El router tiene una conexión OC-3 para su enlace con la WAN de AmericaCom. El acceso Internet será provisto desde una PVC configura hace el router de Border ubicado en San Juan de Miraflores.

```
interface ATM6/0.8 point-to-point
 description CID 20179 INTERNET Redundante - AR01
 bandwidth 2000
 ip address 200.62.129.222 255.255.255.252
 delay 20
 pvc Enl_AR01 0/108
  abr 4523 4523
  oam-pvc manage
  encapsulation aal5snap
!
interface ATM6/0.9 point-to-point
 description CID 20179 INTERNET Enlace Principal POP rlSPChinchon
 bandwidth 2000
 ip address 216.244.137.98 255.255.255.252
 delay 10
 pvc Enl_rlSPChincho 0/109
  abr 4523 4523
  oam-pvc manage
  encapsulation aal5snap
```

- Configuración del Protocolo de enrutamiento interior: Para este caso, teniendo en cuenta que los equipos son Cisco y dada las características de convergencia y flexibilidad de su manejo con otros protocolos, elegimos configurar el protocolo EIGRP para la red de Americacom. Este protocolo permite que el router de las sede Principal converse e intercambie rutas a través de su Routing Table con los routers de las sedes remotas de San Isidro y S. J. De Miraflores, y proveen además seguridad a la red corporativa. Es necesario recalcar que los enlaces Wan son conexiones ATM a los switches ATM lightstream BPX que trabajan en la cpa 2 del modelo OSI.

```
router eigrp 200
  passive-interface Ethernet2/1
  passive-interface Ethernet2/2
  passive-interface Ethernet2/3
  passive-interface Ethernet2/4
  passive-interface Ethernet2/5
  passive-interface Ethernet2/6
  passive-interface Ethernet2/7
  passive-interface ATM6/0.400
  passive-interface BVI1
  network 10.9.27.192 0.0.0.7
  network 10.1..100.0 0.0.0.255
  network 10.1..101.0 0.0.0.255
  network 10.1..102.0 0.0.0.255
  network 10.1..103.0 0.0.0.255
  network 10.1..104.0 0.0.0.255
  network 10.1..105.0 0.0.0.255
  network 10.1..107.0 0.0.0.255
  network 10.1..108.0 0.0.0.255
  network 10.1..109.0 0.0.0.255
  network 10.1..110.0 0.0.0.255
  network 10.1..111.0 0.0.0.255
  network 10.2..201.0 0.0.0.255
  network 10.2..204.0 0.0.0.255
  network 10.3..301.0 0.0.0.255
  network 10.3..304.0 0.0.0.255
  network 10.128.120.0 0.0.0.255
  network 10.128.123.4 0.0.0.3
  network 10.128.248.224 0.0.0.3
  network 10.129.251.224 0.0.0.3
  no auto-summary
  no eigrp log-neighbor-changes
```

8.3.4.- Presupuesto de Equipos Cisco

A continuación presentamos un cionjunto de tablas en las cuales nos muestran los precioss sin que se requirió para la instalación de switches y routers en este proyecto de implementación de la red Corporativa, siendo la empresa AmericaCom una de las pocas con este tipo de sistemas en el Perú. Es importante mencionar que, siendo AmericaCom una carrier en el mercado Peruano, la disponibilidad de equipos swithers y routers son a corto plazo.

AT&T

RESUMEN DE COSTOS DE LA RED CORPORATIVA

Resumen de Costos (Al 37% Descto. - CISCO)

1. **EQUIPOS EDIFICIO CORPORATIVO MARRIOT**

Nº	Ambiente	Equipo	Costo Unitario	Cantidad	Total
	Sótano	Catalyst 6506	31.495	1	31.495
		Router 2611	18.590	1	18.590
		(*) Router 7206VXR	0	1	0
	Piso 1	Catalyst 3524	3.745	1	3.745
		Catalyst 3548	5.745	1	5.745
		Catalyst 3548	5.495	1	5.495
	Piso 2	Catalyst 3548	5.745	2	11.490
		Catalyst 3548	5.495	1	5.495
	Piso 3	Catalyst 3524	3.995	1	3.995
		Catalyst 3548	5.745	2	11.490
	Piso 4	Catalyst 3548	5.495	1	5.495
		Catalyst 3548	5.745	2	11.490
	Piso 5	Catalyst 3548	5.495	1	5.495
		Catalyst 3548	5.745	2	11.490
	Piso 6	Catalyst 3548	5.745	1	5.745
		Catalyst 3524	3.745	1	3.745
				SUB-TOTAL	**141.000**
				37% DESCUENTO	**52.170**
				TOTAL	**88.830**

(*) Se utilizarán los equipos 7206VXR de Almacén.

1.2	SPARE				Total
	RESPUESTOS PARA EQUIPOS CISCO				**53.815**
				Subtotal	**53.815**
				37% DESCUENTO	**19.912**
				TOTAL	**33.903**

SUB-TOTAL 1 - FOB **122.733**

2. **EQUIPOS PARA OTROS LOCALES**

2.1 AEROPUERTO

Nº	Ambiente	Equipo	Costo Unitario	Cantidad	Total
1	Router de Acceso Wan	Router 2621	7.695	1	7.695
2	Equipo de LAN Switch	Catalyst 3524	3.995	1	3.995
				SUB-TOTAL	**11.690**
				37% DESCUENTO	**4.325**
				TOTAL	**7.365**

2.2 VILLA EL SALVADOR

Nº	Ambiente	Equipo	Costo Unitario	Cantidad	Total
1	Router de Acceso Wan	Router 7206VXR	0	1	0
2	Equipo de LAN Swich	Catalyst 5505	26.730	1	26.730
				SUB-TOTAL	**26.730**
				37% DESCUENTO	**9.890**
				TOTAL	**16.840**

2.3 CHINCHON

Nº	Descripción	Equipo	Costo Unitario	Cantidad	Total
1	Router de Acceso Wan	Router 7206VXR	0	1	0
2	Equipo de LAN Switch	Catalyst 6506	21.490	1	21.490
				SUB-TOTAL	**21.490**
				37% DESCUENTO	**7.951**
				TOTAL	**13.539**

2.4 SAN MIGUEL

Nº	Descripción	Equipo	Costo Unitario	Cantidad	Total
1	Router de Acceso Wan	Router 7206VXR	0	1	0
2	Equipo de LAN Switch	Catalyst 5505	36.720	1	36.720
				SUB-TOTAL	**36.720**
				37% DESCUENTO	**13.586**
				TOTAL	**23.134**

SUB-TOTAL 2 - PRECIO - FOB **60.877**

3 EQUIPOS PARA TRASLADO DE SERVIDORES

3.1	Descripción	Equipo	Costo Unitario	Cantidad	Total
3	Equipo de LAN Switch	Catalyst 6506	28.490	1	28.490
				SUB-TOTAL	**28.490**
				37% DESCUENTO	**10.541**
				TOTAL	**17.949**

SUB-TOTAL 3 - PRECIO - FOB **17.949**

4. OTROS - COSTOS ADICIONALES

4.1	ACCESORIOS ADICIONALES				Total
	RACK, ACCESORIOS DE F.O.				3.250
				Subtotal	**3.250**

SUB-TOTAL 4 - COSTO LOCAL **3.250**

5. REDUNDANCIA

5.1 RED DE DATOS Y TELEFONIA

Nº	Ambiente	Equipo	Costo Unitario	Cantidad	Total
1	Router de Acceso Wan (*)	Router 7206VXR	0	1	0
2	Equipo de LAN Switch	Catalyst 8540	145.735	1	145.735
				Subtotal	**145.735**
				37% DESCUENTO	**53.922**
				TOTAL	**91.813**

(*) Se utilizarán los equipos 7206VXR de Almacén.

SUB-TOTAL 5 - PRECIO FOB **91.813**

RESUMEN GLOBAL AL 37%

SUB-TOTAL 1 - FOB =	***122.733***
SUB-TOTAL 2 - FOB =	***60.877***
SUBTOTAL EQUIPOS =	***183. 610***
SUB-TOTAL 3 - SERVIDORES FOB =	***17.949***
SUB-TOTAL 4 - COSTO LOCAL=	***3.250***
SUB-TOTAL 5 - REDUNDANCIA PRECIO FOB=	***91.813***

		FOB
RED CON REDUNDANCIA SIN TRASLADO DE SERVIDORES - FOB	TOTAL ($) -	278.673
RED CON REDUNDANCIA CON TRASLADO DE SERVIDORES - FOB	TOTAL ($) -	296.622

CONCLUSIONES

1. Si bien es cierto que las compañías se enfocan en acortar las distancias geográficas mediante nuevas tecnologías, para obtener una comunicación mucho mas rápida, un intercambio de información global, y acceder a las fuentes de información mundial desde cualquier lugar del planeta, Las redes de área local de hoy en día se se encuentran prácticamente interconectadas entre sí, no existe red en el mundo que no esté conectada a la gigantesca red mundial como es el internet.

2. Desde finales del siglo XX, la red de área local fue una de las tecnología que se desarroló rápidamente, surgiendo de los laboratorios y otros lugares de investigación, nuevas caracteríscas tales como velocidades del orden de los Gigabit (actualmente ya se cuenta con velocidades de 10 Gigabit), Virtual LAN (VLAN), Spaning-Tree Protocol (STP), VLAN Trunking Protocol (VTP) y lo último Multilayer Switching (MLS) y mas.

3. Debido al avance de la tecnología, y al avaratamiento de los costos, se hizo mas accesible la utilización de medios físicos de mas calidad y performance. Es así que se pudo acceder a la fibra óptica, que en la actualidad ya es muy común ver instalaciones de área local con este tipo de medio y equipos soportan estos.

4. Debido a la utilización de fibra óptica y al avance de la tecnología, los medios de cobre también se desarrollaron. Se empezó con medios de cobre sin categoría, continuando con los cables de Cat3 (soporta 10Mbps), luego con cables Cat 5 y Cat 5E (soporta hasta 100 Mbps), después con cables Cat 6 (soprta hasta 1Gbps, comunicaciones ATM, video) y finalmente ya se encuentran en pruebas el cable Cat 7

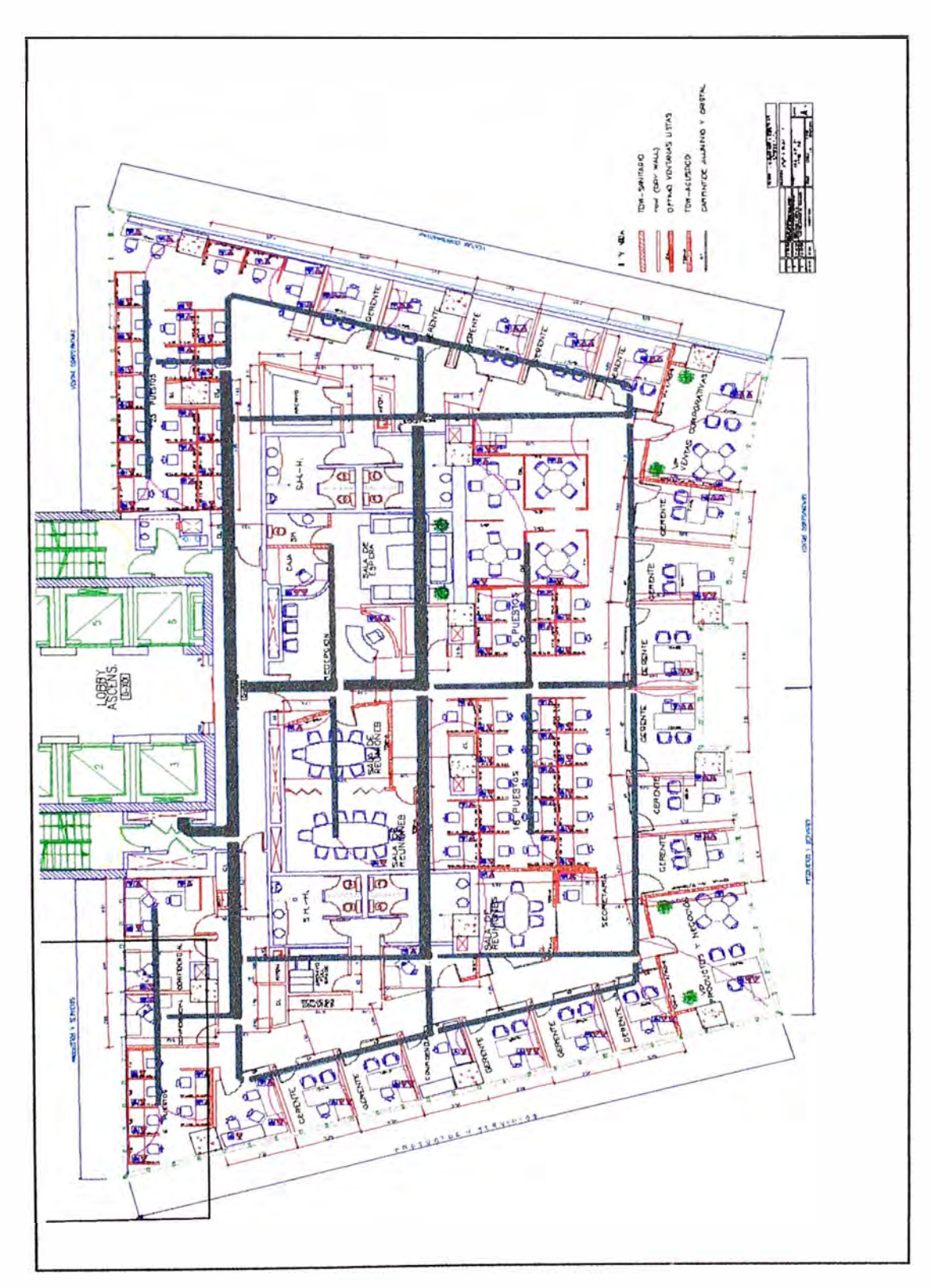
5. El diseño de red en una compañía, obedece a un análisi detallado de los requerimientos técnicos y administrativos de los usuarios y los leaders. El requerimiento técnico esta referido a las necesidades que cada usuario, director, Vicepresidente y el Presidente presenta, para obtener la mejor performance en sus respectivos trabajos y funciones. El requermiento administrativo esta referenciado al presupuesto que la compañía está capacitado en invertir.

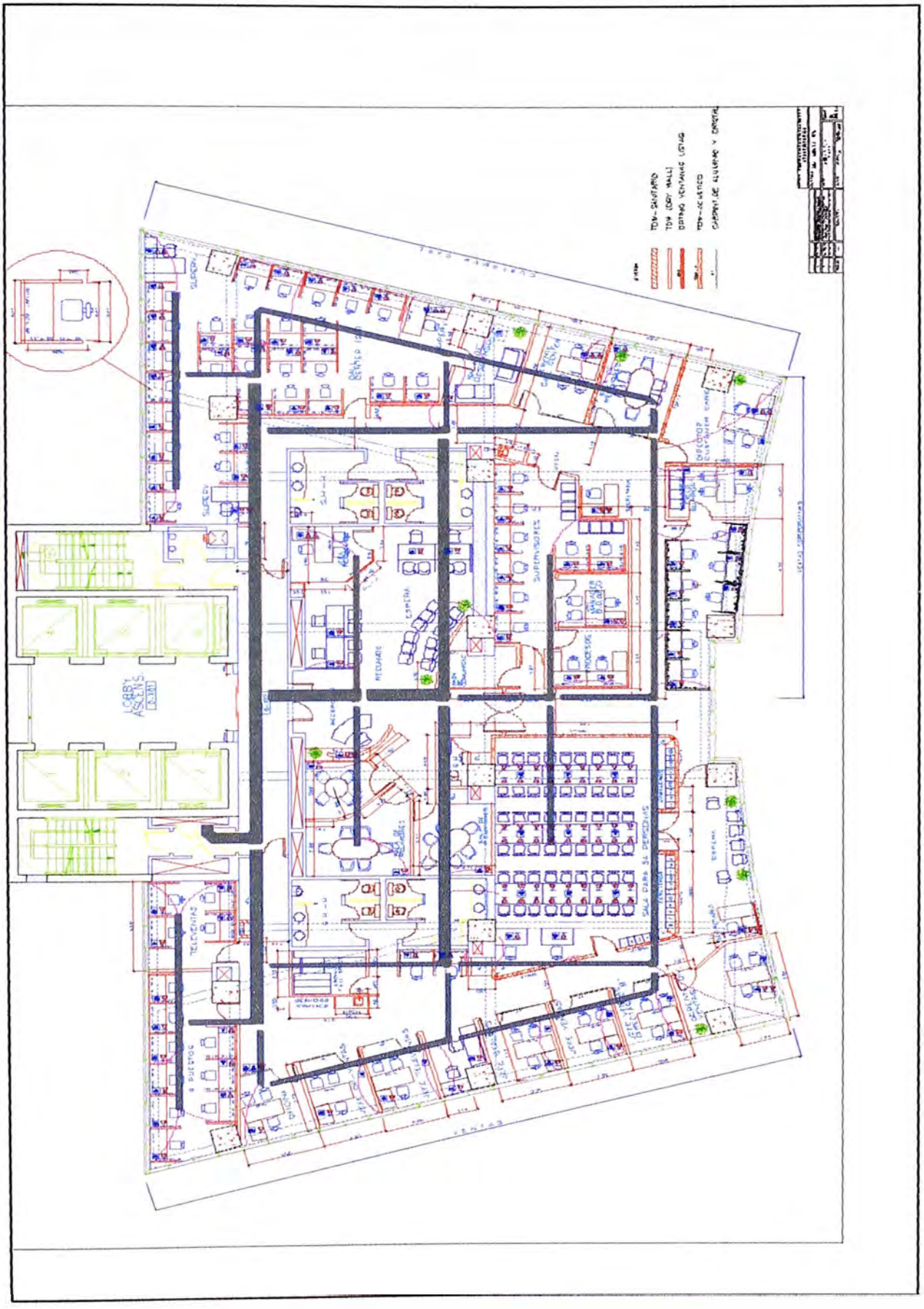
6. El diseño e implementación de una internetwork , está asociado a la correcta elección de todos los euipos que serán instalados, la correcta tecnología que será implementada, las carcaterísticas particulares

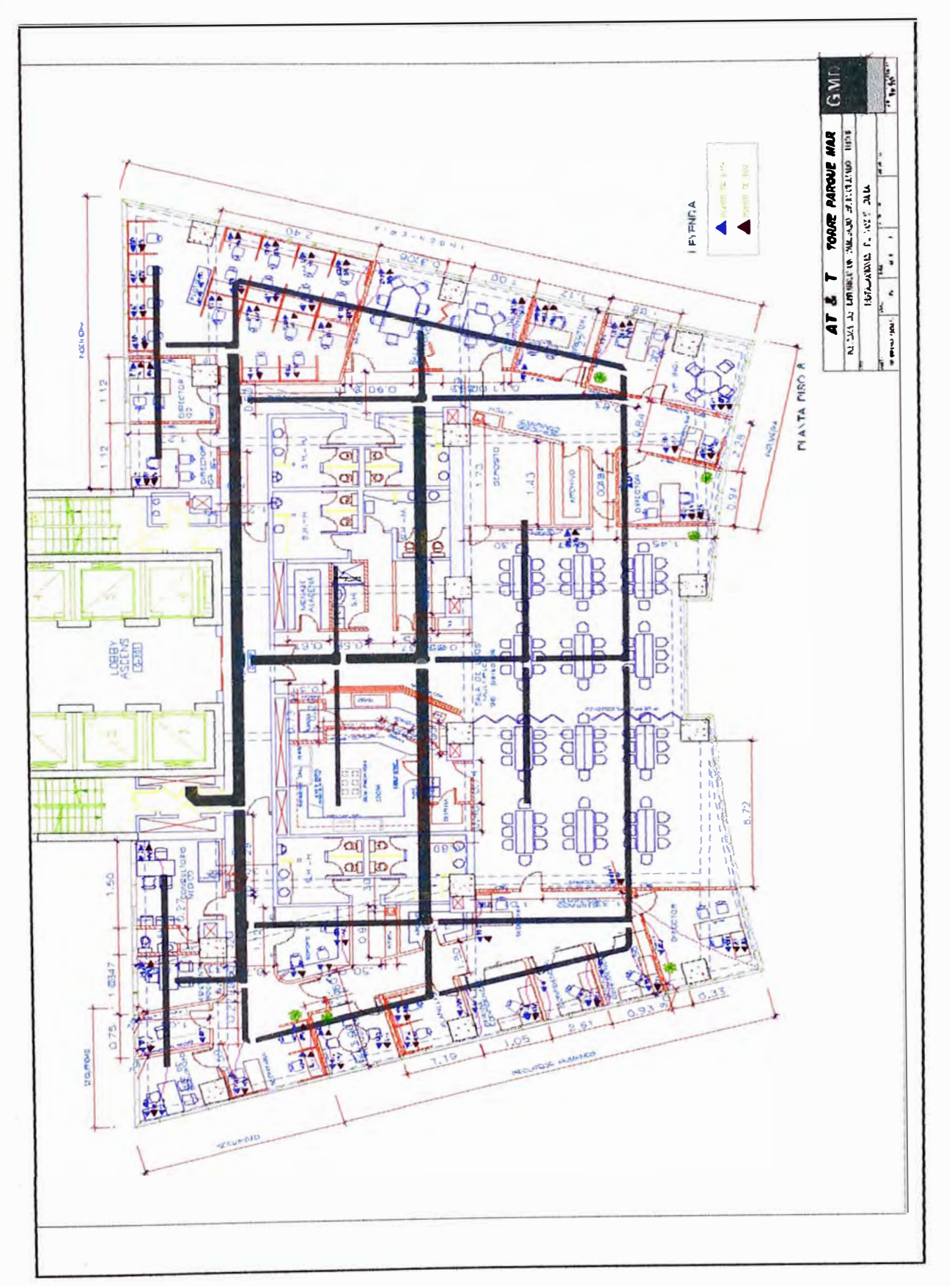
que se habilitarán para la tecnología elegida y el medio físico que será utilizado como plataforma de soporte de la tecnología elegída, Es importante conjugar todas estos cuatro items , por que si uno de ellos no cumple con los requerimientos , todo será reflejado en la performance de la red y finalmente en cada usuario final. Es decir si aplicamos tecnología de última generación (Fast y Giga Ethernet) y la plataforma física que soprta dicha tecnología no es la adecuada (cableado de cobre Cat 3), la red tendrá una baja performance. De la misma manera si se habilita características innecesarias o no se habilita las adecuadas, en los equipos (switches y routers) de red, puede traer como consecuencia infiltraciones de agentes externos (Hackers), pérdida de información y lo que es peor que la red no funcione. El no funcionamiento de la red es sinónimos de pérdida de horas de trabajo y esta finalmente se traduce en pérdida del revenue para la compañía.

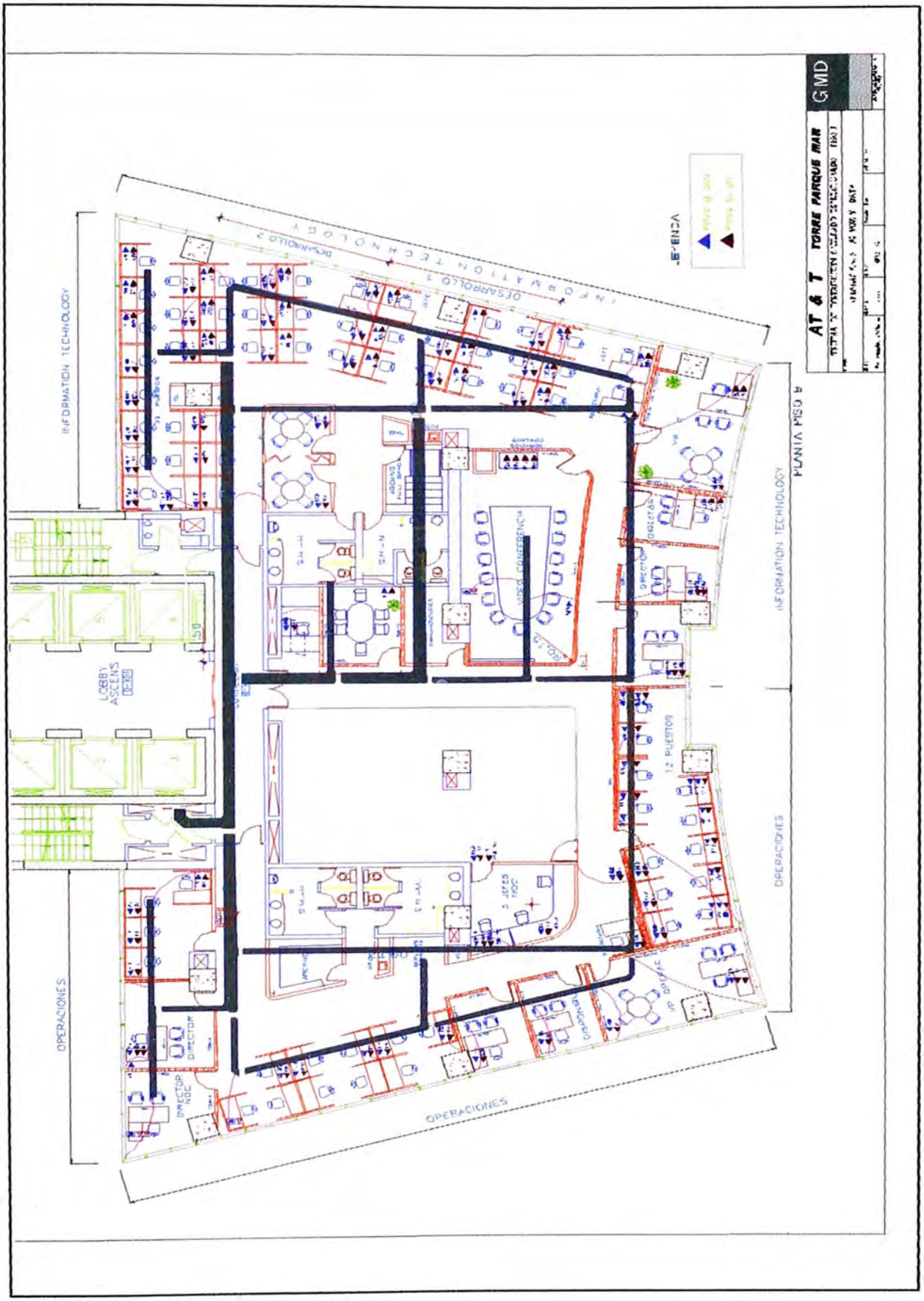
ANEXOS

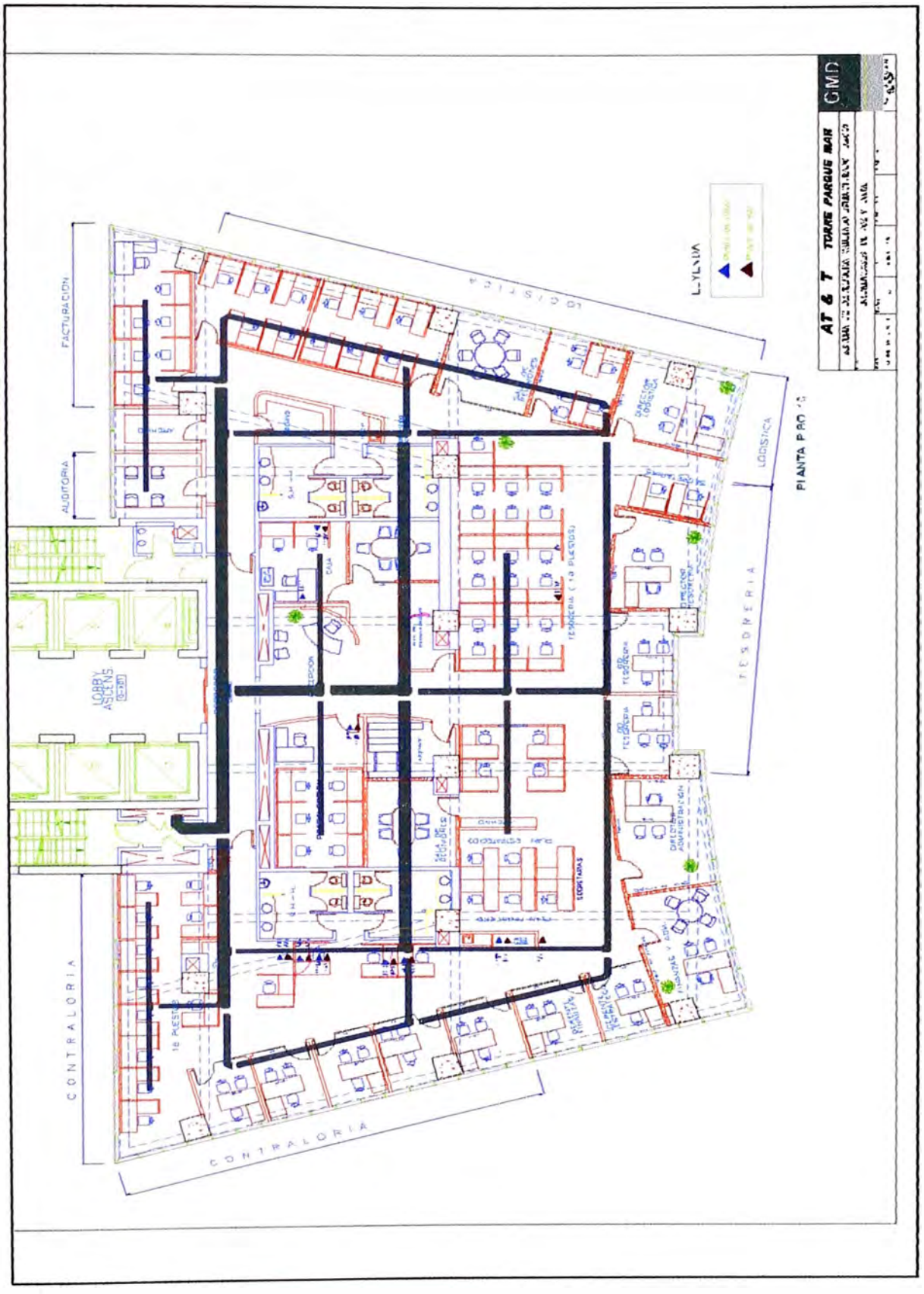
ANEXO A. DIAGRAMA DE INSTALACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO PISO 1 - 6.

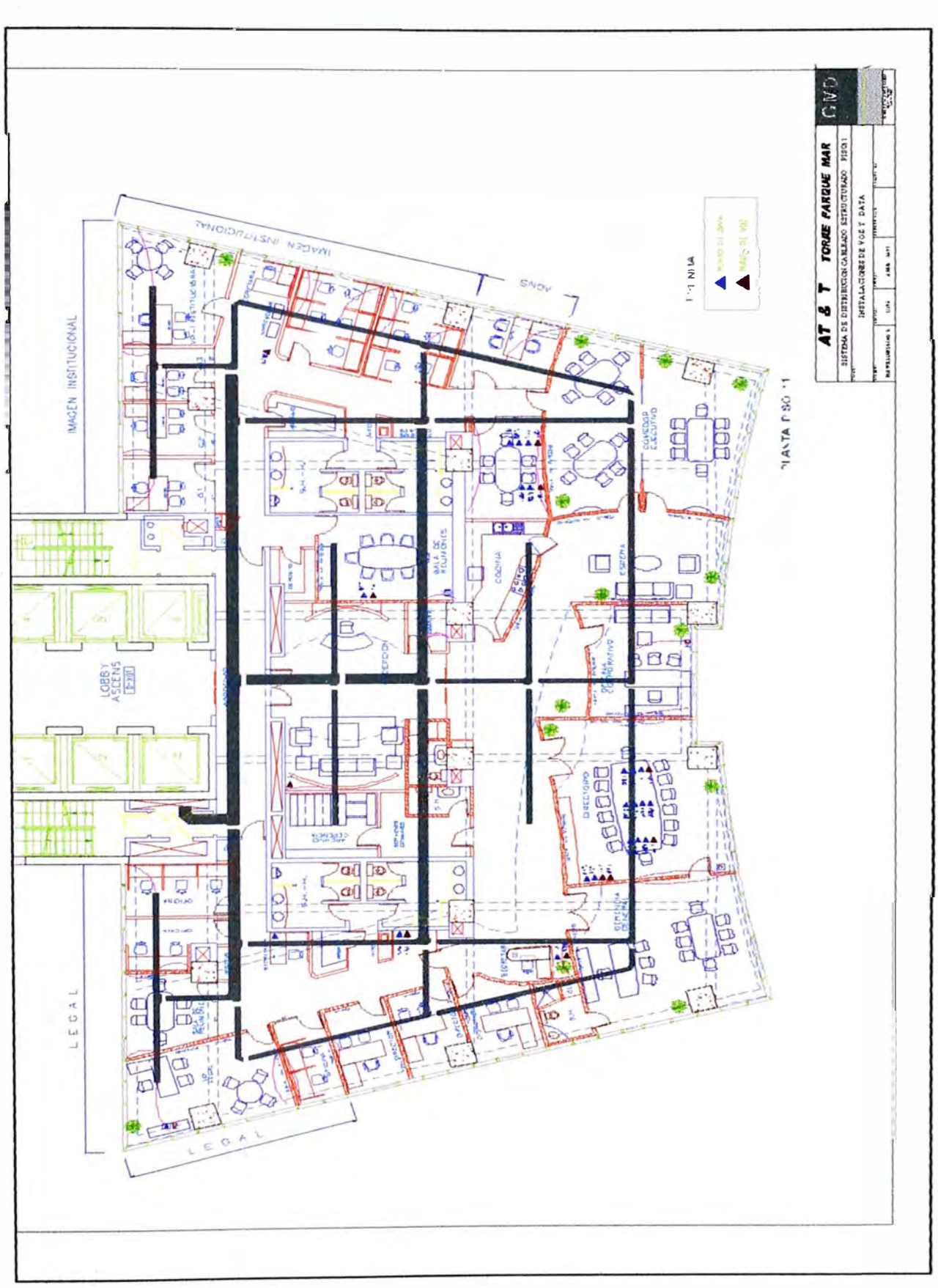





AT & T TORRE PARQUE MAR
GMD
PLANTA PISO A
LOBBY ASCENSORES
LEYENDA


AT & T
TORRE PARQUE MAR
GMD
PLANTA PISO 8
INFORMATION TECHNOLOGY
OPERACIONES
LOBBY ASCENS
SALA CONFERENCIA
DIRECTOR
12 PUESTOS
3 JEFES TROC
DESARROLLO
INFORMATION TECHNOLOGY


AT & T
TORRE PARQUE MAR
GMD
PLANTA PRIMER PISO
LOGISTICA
TESORERIA
CONTRALORIA
AUDITORIA
FACTURACION
LOBBY ASCENSORES
LLAVERIA


AT & T TORRE PARQUE MAR
SISTEMA DE DISTRIBUCION CABLEADO ESTRUCTURADO PISO 1
INSTALACIONES DE VOZ Y DATA
IMAGEN INSTITUCIONAL
LEGAL
LOBBY ASCENSORES
SALA DE REUNIONES
COCINA
COMEDOR EJECUTIVO
DIRECTORIO
ESPERA
RECEPCION

ANEXO B. RESULTADO DE LAS PRUEBAS DE CERTIFICACIÓN CAT 6 DE LOS PUNTOS DE VOZ Y DATOS PISOS 1 - 6.

GMD

BIEN

OMNIScanner2 Informe de certificación

		OMNIScanner		OMNIRemote
ID de circuito:	Piso-05-001			
Proyecto:	ATT-P6VOZ	50D00I100463	SW: V04.01	50E00GC0024
Propietario:	OmniScanner	Adapd.		Adapd.
Autotest:	*Panduit Cat 6*	MT CAT6 SSTP		MT CAT6 SSTP
Cable:	BELDEN1872A			
NVP:	70			
Ubicación:	---			
Edificio:	---			
Piso:	---			
Anuario:	---			

	Límite	12	36	45	78
Longitud (ft	(100.5)	27.7	38.7	38.0	38.3
Retraso (ns):	(545)	177	182	179	180
Resistencia (Ohms):	(---)	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 5
Remote:	12345678	12345678	Ancho de banda (MHz):	---

Atenuación — Valor general de margen (dB)* 20.2

Pares	dB	Margen	MHz
12	9.7	20.9	199.3
36	10.2	20.4	199.8
45	10.2	20.2	197.5
78	10.1	20.5	198.4

Pérdida — Valor general de margen (dB)* 6.7

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	24.6	11.8	80.5	25.1	9.6	45.3
36	16.9	7.5	182.2	16.3	6.7	175.9
45	23.8	9.0	53.6	22.7	8.0	53.6
78	29.5	13.4	39.0	23.4	12.8	139.9

NEXT — Valor general de margen (dB)* 7.9

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	55.7	7.4	31.8	69.9	9.8	6.1
12/45	69.4	9.6	6.4	68.4	8.6	6.4
12/78	40.3	2.9	141.7	64.6	7.0	9.7
36/45	55.1	10.6	53.8	66.3	13.3	1.0
36/78	46.6	11.2	180.9	49.3	13.7	181.3
45/78	67.4	17.8	26.6	62.4	18.5	174.1

ACR — Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT — Valor general de margen (dB)* 10.3

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	73.9	10.3	1.0	72.9	11.1	1.2
12/45	78.7	18.3	1.4	81.7	16.1	1.0
12/78	41.5	23.1	174.6	40.2	22.0	178.2
36/12	73.0	11.2	1.2	73.9	10.2	1.0
36/45	78.3	14.8	1.0	78.6	14.8	1.2
36/78	40.2	21.0	169.7	43.3	22.9	139.9
45/12	81.7	18.2	1.0	79.6	18.3	1.4
45/36	78.5	14.7	1.2	78.3	14.7	1.0
45/78	66.4	36.4	57.9	63.4	37.7	76.0
78/12	40.5	22.2	178.2	41.7	23.3	175.0
78/36	56.2	22.9	31.3	38.8	26.7	160.7
78/45	63.3	37.7	76.0	66.3	38.3	57.9

PSNEXT — Valor general de margen (dB)* 5.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	39.6	5.1	141.7	64.7	7.2	6.1
36	55.0	9.4	31.8	62.4	11.4	15.1
45	66.4	11.1	6.4	67.8	10.5	6.4
78	40.0	5.5	141.3	54.3	10.5	10.6

PSELFEXT — Valor general de margen (dB)* 12.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	74.1	13.5	1.0	73.4	12.8	1.0
36	72.7	12.1	1.0	73.2	12.8	1.0
45	73.0	16.5	1.4	73.8	16.5	1.4
78	38.7	22.6	162.4	38.3	23.1	178.2

PSACR — Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remote

MICROTEST

Date: 3/Feb/01 11:36:00 AM Página 1

GMD

BIEN

OMNIScanner2 Informe de certificación

		OMNIScanner		OMNIRemote
ID de circuito:	Piso 06-001			
Proyecto:	AAT-DATOS PB	50D00H00101	SW: V04.01	50E00H00133
Propietario:	OmniScanner	Adapd.		Adapd.
Autotest:	*Panduit Cat 6*	MT CAT6 SSTP		MT CAT6 SSTP
Cable:	BELDEN 1872A			
NVP:	70			
Ubicación:	---			
Edificio:	---			
Piso:	---			
Armario:	---			

	Límite	12	36	45	78
Longitud ft	(100 5)	35 4	37 2	36 8	36 8
Retraso (ns):	(546)	171	175	173	173
Resistencia (Ohms):	(---)	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 4
Remote:	12345678	12345678	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 20.2

Pares	dB	Margen	MHz
12	9.4	21.1	199.8
36	10.0	20.4	198.9
45	10.3	20.3	199.6
78	10.3	20.2	199.3

Pérdida

Valor general de margen (dB)* 6.8

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	22.9	11.6	125.1	25.9	10.5	44.1
36	22.0	7.1	52.0	17.2	7.5	171.8
45	20.7	6.8	65.1	20.4	6.6	95.1
78	25.7	10.1	43.9	24.3	7.7	34.9

NEXT

Valor general de margen (dB)* 6.9

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	43.2	7.0	166.5	51.6	6.9	50.9
12/45	58.1	13.9	58.5	64.3	15.3	20.1
12/78	53.4	10.6	16.9	45.2	9.3	171.4
36/45	52.0	11.7	95.3	56.5	12.4	56.7
36/78	44.2	9.3	196.6	47.4	11.6	100.0
45/78	50.2	15.4	197.5	63.2	16.3	194.4

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 12.4

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	73.2	12.9	1.4	76.5	12.4	1.6
12/45	49.5	16.9	37.4	51.4	17.2	23.4
12/78	60.9	28.2	33.8	66.0	29.8	56.3
36/12	75.0	12.4	1.6	73.2	12.9	1.4
36/45	49.0	16.3	33.8	48.0	16.1	37.2
36/78	47.0	26.0	125.6	43.8	23.9	148.0
45/12	79.0	17.2	1.2	80.1	17.0	32.4
45/36	48.0	16.2	37.2	49.0	16.2	33.8
45/78	95.0	36.0	1.6	94.2	35.2	1.6
78/12	58.3	30.0	36.3	61.1	29.5	33.6
78/36	43.6	24.2	157.5	48.0	25.3	110.6
78/45	94.2	36.2	1.6	95.1	36.0	1.6

PSNEXT

Valor general de margen (dB)* 8.5

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	42.5	9.2	166.5	46.5	8.8	70.7
36	41.8	8.5	166.5	51.6	9.4	30.7
45	54.7	13.3	56.5	55.8	14.4	56.7
78	43.1	11.1	187.4	43.7	10.8	171.0

PSELFEXT

Valor general de margen (dB)* 14.4

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	79.0	14.4	1.0	79.6	14.6	1.0
36	44.2	14.5	33.8	75.3	14.7	1.0
45	46.4	16.7	33.8	48.0	16.9	25.6
78	36.3	28.5	129.6	43.5	28.2	148.6

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general [illegible] del peor par [illegible]

MICROTEST

Date: 5/Feb/01 1:24:00 PM Página 1

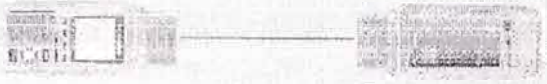
GMD

OMNIScanner2 Informe de certificación

ID de circuito:	P7V-01
Proyecto:	ATT-Piso7-V
Propietario:	GMD
Auditor:	Randall Carroll
Cable:	SELOSEN1873A
NVP:	70
Ubicación:	---
Edificio:	---
Piso:	---
Armario:	---

OMNIScanner 50000H00101 SW: V04.01 Adapt. MT CAT6 SSTP

OMNIRemote 50E00H00133 Adapt. MT CAT6 SSTP



	Límite	12	36	45	78
Longitud ft	(100.0)	30.4	36.6	36.4	36.6
Retraso (ns):	(545)	171	173	171	172
Resistencia (Ohms):	(----)	---	---	---	---

Gráfico de calibrado	Estimación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 2
Remoto:	12345678	12345678	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 20.6

Pares	dB	Margen	MHz
12	9.2	21.2	198.9
36	9.7	20.8	199.3
45	9.6	20.9	199.3
78	9.5	21.0	199.3

Pérdida

Valor general de margen (dB)* 6.4

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	26.2	11.6	56.6	27.5	13.0	56.7
36	21.0	6.4	56.6	22.3	7.7	56.6
45	20.8	6.9	155.5	20.2	9.2	125.5
78	24.7	11.2	72.9	25.8	14.6	119.7

NEXT

Valor general de margen (dB)* 8.4

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	74.0	9.6	3.4	69.6	9.4	9.3
12/45	80.0	9.6	99.1	97.5	11.4	43.0
12/78	49.7	11.3	136.4	52.5	9.5	65.7
36/45	47.2	8.4	116.6	48.4	10.5	132.3
36/78	56.9	12.1	46.3	50.1	11.3	113.4
45/78	46.8	11.3	199.3	50.3	16.3	166.2

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 12.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	74.2	12.5	1.2	79.6	12.6	1.0
12/45	41.0	17.7	99.2	78.3	17.5	1.2
12/78	40.9	23.1	199.3	40.2	22.9	197.5
36/12	75.7	12.1	1.0	74.3	12.5	1.2
36/45	53.1	18.3	20.4	68.0	18.0	35.9
36/78	42.0	21.7	139.9	40.2	30.5	160.3
45/12	78.3	17.5	1.2	41.3	17.8	97.9
45/36	53.0	16.0	25.9	52.2	18.2	29.1
45/78	90.7	28.9	1.2	87.2	26.9	1.4
78/12	40.4	20.2	198.9	40.6	23.4	199.3
78/36	35.9	20.2	150.5	40.5	21.6	166.0
78/45	87.2	26.9	1.4	90.7	28.9	1.3

PSNEXT

Valor general de margen (dB)* 9.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	52.7	10.3	49.1	42.0	10.0	197.1
36	49.1	10.3	136.3	72.6	10.4	3.2
45	41.0	9.0	102.5	43.3	11.3	197.5
78	56.2	11.4	35.8	46.9	11.1	119.7

PSELFEXT

Valor general de margen (dB)* 14.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	72.8	14.1	1.2	71.8	14.5	1.4
36	48.2	14.2	25.9	48.1	14.2	29.2
45	50.2	18.4	20.4	70.9	18.1	1.2
78	40.1	22.7	139.9	38.0	21.7	166.3

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remoto

GMD

OMNiScanner2 Informe de certificación

		OMNIScanner		OMNIRemote
ID de circuito:	P7D-01			
Proyecto:	ATT-Piso7-D	50D0CH00101	SW: V04.01	50E00H001B3
Propietario:	GMD	Adapd.		Adapd.
Autocal.	Fallido Cat 6	MT CAT6 SSTP		MT CAT6 SSTP
Cable:	BELDEN1872A			
NVP.	70			
Ubicación.	---			
Edificio:	---			
Piso:	---			
Armario:	---			

	Límite	12	36	45	78
Longitud (ft	(1005)	35.5	36.2	36.2	36.2
Retraso (ns):	(545)	168	170	170	170
Resistencia (Ohms):	(---)	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	12345678	12345678	**Sesgo (ns):**	(45) 2
Remote:	12345678	12345678	**Ancho de banda (MHz):**	---

Atenuación

Valor general de margen (dB)* 20.9

Pares	dB	Margen	MHz
12	9.0	21.5	168.0
36	9.6	20.9	198.9
45	9.5	21.0	199.3
78	9.4	21.1	196.9

Pérdida

Valor general de margen (dB)* 6.2

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	27.0	12.3	54.7	27.5	12.8	54.7
36	21.0	6.2	53.4	21.7	6.9	53.6
45	25.2	9.9	46.5	22.6	9.2	69.8
78	25.1	10.9	58.8	27.5	13.8	88.0

NEXT

Valor general de margen (dB)* 6.8

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	46.7	11.7	193.5	53.1	11.5	1.2
12/45	62.3	10.8	20.5	51.9	11.5	94.5
12/78	48.4	12.8	160.9	51.1	11.5	152.6
36/45	44.3	9.5	188.5	61.7	12.3	31.3
36/78	42.0	10.9	145.8	53.1	12.9	145.8
45/78	41.6	8.8	168.9	63.1	14.6	30.9

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 11.9

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	74.1	12.3	1.2	75.9	11.9	1.0
12/45	49.5	18.2	31.3	76.4	16.1	1.4
12/78	69.7	23.1	1.0	65.4	27.3	180.4
36/12	75.9	11.9	1.0	74.1	12.4	1.2
36/45	53.4	16.8	27.1	79.3	19.0	1.4
36/78	48.0	26.5	154.3	48.1	26.7	155.7
45/12	76.4	16.1	1.4	78.1	16.3	1.2
45/36	79.3	19.0	1.4	53.3	18.7	27.1
45/78	92.1	31.8	1.4	66.5	39.7	1.2
78/12	45.7	27.6	180.4	89.7	26.2	1.0
78/36	45.6	26.2	195.6	47.5	38.1	180.1
78/45	36.5	33.7	1.2	62.1	31.8	1.4

PSNEXT

Valor general de margen (dB)* 8.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	42.8	10.8	197.5	43.4	11.4	197.1
36	42.0	10.4	193.6	52.1	13.0	1.2
45	39.9	8.0	199.4	57.4	11.6	30.9
78	40.0	8.1	199.3	45.7	11.4	145.8

PSELFEXT

Valor general de margen (dB)* 13.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	72.9	13.6	1.2	73.7	14.0	1.2
36	78.0	14.7	1.4	74.5	14.5	1.0
45	48.5	17.6	28.2	74.0	17.3	1.4
78	69.5	27.9	1.0	41.9	27.7	159.8

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remote

MICROTEST

Date: 8/May/01 12:48:00 AM Página 1

GMD

BIEN

OMNIScanner2 Informe de certificatión

		OMNIScanner		OMNIRemote
ID de circuito:	Piso-08-001			
Proyecto:	ATT-P8VOZ	SCD0CH00463	SW: V04.01	60E00G00024
Propietario:	OmniScanner	Adapd.		Adapd.
Autotest:	*Pandult Cat 6*	MT CAT6 SSTP		----
Cable:	BELDEN1872A			
NVP:	70			
Ubicacion:	---			
Edificio:	---			
Piso:	---			
Armario:	---			

	Limite	12	36	45	78
Longitud ft	(100.0)	42.7	43.9	43.1	43.3
Retraso (ns):	(545)	201	207	203	204
Resistencia (Ohms):	(---)	---	---	---	---

Gráfico de cableado	Refinación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 6
Remote:	12345678	12345678	Ancho de banda (MHz):	----

Atenuación

Valor general de margen (dB)* 18.6

Pares	dB	Margen	MHz
12	11.5	19.1	199.3
36	11.9	18.7	199.8
45	11.8	18.6	199.8
78	11.9	18.6	199.8

Pérdida

Valor general de margen (dB)* 6.6

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	26.9	11.9	49.8	24.6	9.5	49.8
36	17.2	7.2	161.5	18.1	6.6	112.9
45	18.6	9.7	164.2	20.1	9.2	120.1
78	28.8	12.8	41.7	25.0	9.2	41.7

NEXT

Valor general de margen (dB)* 4.7

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	58.3	6.1	18.5	55.9	4.7	21.2
12/45	56.9	11.3	46.4	53.6	13.0	46.6
12/78	44.1	6.0	182.1	66.1	10.7	12.0
36/45	55.1	12.8	72.9	59.8	16.5	63.3
36/78	70.9	12.6	7.9	70.9	12.7	7.9
45/78	58.3	15.7	69.8	53.0	17.2	175.9

ACR

Valor general de margen (dB)* ----

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	----	----	----	----	----	----
12/45	----	----	----	----	----	----
12/78	----	----	----	----	----	----
36/45	----	----	----	----	----	----
36/78	----	----	----	----	----	----
45/78	----	----	----	----	----	----

ELFEXT

Valor general de margen (dB)* 10.7

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	44.0	11.0	32.4	45.6	10.7	26.4
12/45	39.5	16.9	160.7	45.6	19.1	99.8
12/78	61.3	27.7	1.0	91.3	28.3	1.0
36/12	45.7	10.6	26.4	72.9	11.1	1.2
36/45	36.3	15.0	199.8	36.6	19.4	199.8
36/78	41.1	21.2	147.1	44.6	21.0	96.1
45/12	45.2	19.5	69.8	48.1	20.2	68.6
45/36	36.5	19.3	199.8	36.2	19.0	199.8
45/78	96.6	34.6	1.2	94.5	32.8	1.2
78/12	61.9	28.3	1.0	91.3	27.7	1.0
78/36	44.6	21.0	96.1	40.9	21.2	150.3
78/45	94.5	32.8	1.2	96.4	34.6	1.2

PSNEXT

Valor general de margen (dB)* 6.9

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	58.2	7.2	18.5	55.5	6.9	21.2
36	53.0	8.1	35.1	56.6	7.9	21.2
45	55.1	12.6	49.8	47.1	15.2	198.9
78	42.9	10.7	192.1	62.6	12.7	17.8

PSELFEXT

Valor general de margen (dB)* 13.5

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	46.4	13.5	26.4	72.9	13.7	1.2
36	43.8	13.7	32.2	45.3	13.5	26.4
45	34.9	20.6	198.9	35.2	21.0	199.8
78	40.8	24.0	148.8	44.6	23.9	96.1

PSACR

Valor general de margen (dB)* ----

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	----	----	----	----	----	----
36	----	----	----	----	----	----
45	----	----	----	----	----	----
78	----	----	----	----	----	----

* El valor general de margen es el peor margen del OMNI y el Remote.

GMD

BIEN

OMNIScanner2 Informe de certificatión

		OMNIScanner		OMNIRemote
ID de circuito:	Piso-08-001			
Proyecto:	All-DATOS-P8	50D00H00101	SW: V04.01	50E00H00133
Propietario:	OmniScanner	Adapd.		Adapd.
Anotest:	*Panduit Cat 6*	GIG-CHNL TX6		GIG-CHNL TX6
Cable:	BELDEN1872A			
NVP:	70			
Ubicación:	---			
Edificio:	---			
Piso:	---			
Armario:	---			

	Límite	12	36	45	78
Longitud ft	(100.5)	42.9	43.9	43.7	43.9
Retraso (ns):	(645)	202	207	206	207
Resistencia (Ohms):	(----)	----	----	----	----

Gráfico de cableado	Estimación	Real		
OMNI:	[illegible]	[illegible]	Sesgo (ns):	(45) 5
Remote:	[illegible]	[illegible]	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 18.5

Pares	dB	Margen	MHz
12	11.3	18.3	199.5
36	11.4	18.0	198.3
45	11.6	18.6	198.0
78	12.5	18.5	198.4

Pérdida

Valor general de margen (dB)* 7.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	25.6	9.3	37.6	27.1	11.8	47.5
36	16.6	8.7	161.5	19.2	9.3	161.1
45	22.4	11.1	116.5	22.2	10.6	111.6
78	24.7	7.0	28.8	27.0	9.2	25.6

NEXT

Valor general de margen (dB)* 6.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	65.8	10.8	12.9	67.6	12.9	13.1
12/45	48.6	13.4	139.4	48.2	12.8	184.9
12/78	56.7	11.7	49.8	45.7	9.5	184.7
36/45	56.8	6.1	22.8	58.4	7.6	23.8
36/78	45.5	10.2	189.5	46.8	10.9	170.5
45/78	50.4	9.7	90.9	84.4	15.1	1.6

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 10.9

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	74.7	17.1	1.0	72.9	10.9	1.2
12/45	92.0	18.6	1.0	80.1	18.3	1.2
12/78	46.1	24.6	121.5	51.5	25.1	69.8
36/12	72.7	10.9	1.2	74.8	11.0	1.0
36/45	52.0	17.9	26.0	48.0	16.0	45.9
36/78	43.4	23.6	149.8	43.0	23.8	160.2
45/12	80.1	18.3	1.2	82.0	15.4	1.0
45/36	47.9	17.9	45.9	52.0	17.8	20.0
45/78	50.3	32.8	188.5	53.1	34.1	163.3
78/12	61.8	25.4	60.5	60.8	25.0	74.3
78/36	43.1	23.9	160.2	43.3	23.8	157.5
78/45	53.2	34.2	163.3	50.9	33.1	156.7

PSNEXT

Valor general de margen (dB)* 7.6

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	44.4	12.5	198.4	43.9	10.6	164.7
36	58.4	8.4	23.0	41.7	9.6	195.3
45	56.6	7.5	22.8	57.7	9.6	22.8
78	45.3	10.2	131.4	43.5	10.3	166.3

PSELFEXT

Valor general de margen (dB)* 13.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	71.9	13.1	1.2	73.9	13.3	1.0
36	73.6	13.3	1.0	71.0	13.1	1.2
45	78.5	18.3	1.0	77.5	18.7	1.2
78	41.3	25.0	157.5	45.2	24.7	97.9

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remote.

MICROTEST

Date: 22/Feb/00 6:23:00 AM Página 1

GMD

BIEN

OMNIScanner2 Informe de certificatión

		OMNIScanner		OMNIRemote
ID de circuito:	Piso-05-001			
Proyecto:	ATT P8VOZ	50D00H00463	SW: V04.01	50E05G30024
Propietario:	GMD	Adapd.		Adapd.
Autotest:	*Pantuh Cat 6*	MT CAT6 SSTP		MT CAT6 SSTP
Cable:	BELDEN1872A			
NVP:	70			
Ubicación:	---			
Edificio:	---			
Piso:	---			
Armario:	---			

	Límite	12	36	45	78
Longitud ft	(100.0)	50.0	61.5	60.7	50.5
Retraso (ns):	(545)	286	348	339	338
Resistencia (Ohms):	(----)	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 7
Remoto:	12345678	12345678	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 16.9

Pares	dB	Margen	MHz
12	13.0	17.5	196.3
36	13.5	17.0	199.8
45	13.5	16.9	198.4
78	13.7	16.9	199.6

Pérdida

Valor general de margen (dB)* 5.5

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	29.1	10.7	23.5	27.1	11.8	47.1
36	20.1	6.4	67.6	21.9	7.5	50.8
45	24.1	5.5	21.9	34.8	6.1	31.9
78	26.8	7.0	21.0	20.4	12.3	31.3

NEXT

Valor general de margen (dB)* 8.3

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	53.3	8.3	50.0	76.1	9.8	2.5
12/45	50.7	14.7	171.9	49.8	13.1	172.3
12/78	56.1	9.0	9.2	66.5	9.1	9.1
36/45	43.7	8.5	196.3	52.9	10.9	40.4
36/78	54.9	13.8	85.2	50.4	12.9	40.8
45/78	55.9	16.0	25.5	44.0	9.8	192.6

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 12.7

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	31.3	12.7	171.4	31.3	12.9	173.7
12/45	40.3	21.6	167.8	40.9	20.8	71.4
12/78	40.7	20.9	166.9	50.5	31.7	166.5
36/12	31.7	13.3	175.7	31.8	13.2	171.4
36/45	34.0	16.9	181.3	34.8	16.6	178.2
36/78	51.1	27.1	92.5	47.4	27.4	145.3
45/12	47.2	21.0	71.4	40.6	22.1	167.8
45/36	34.8	16.8	177.7	35.0	17.0	181.3
45/78	56.5	31.5	89.1	56.3	31.8	89.1
78/12	50.8	32.0	166.5	50.0	31.7	166.9
78/36	47.5	27.5	145.3	51.1	27.2	92.5
78/45	58.2	31.8	89.1	56.5	31.5	65.1

PSNEXT

Valor general de margen (dB)* 9.8

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	64.4	9.8	9.2	64.6	9.9	9.1
36	51.5	10.0	54.9	59.1	10.4	20.1
45	43.2	10.9	150.3	42.8	10.6	192.6
78	65.1	10.5	9.3	64.6	9.9	9.1

PSELFEXT

Valor general de margen (dB)* 14.6

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	31.6	16.1	173.7	31.4	15.8	171.4
36	30.1	14.6	71.4	30.0	14.6	173.7
45	33.9	18.0	181.3	50.3	18.8	27.5
78	49.2	29.1	160.3	46.5	29.5	146.3

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remoto.

MICROTEST

Data: 1/Feb/00 12:46:00 AM Página 1

GMD

BIEN

OMNIScanner2 Informe de certificatión

ID de circuito:	Pas 09-051
Proyecto:	All-DATOS-P9
Propietario:	GMD
Autotest:	*Panduit Cat 6*
Cable:	BELDEN1872A
NVP:	78
Ubicación:	---
Edificio:	---
Piso:	---
Armario:	---

	OMNIScanner		OMNIRemote
	50D50H00101	SW: V04.01	50E50H00133
	Adapd.		Adapd.
	GIG-CHNL TX6		GIG-CHNL TX6

	Límite	12	36	45	78
Longitud ft	(100 5)	51 3	52 1	51.3	51.5
Retraso (ns):	(545)	242	246	242	243
Resistencia (Ohms):	(----)	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	1,2,3,6,7,8	1,2,3,6,7,8	Sesgo (ns):	(45) 4
Remote:	1,2,3,6,7,8	1,2,3,6,7,8	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 16.7

Pares	dB	Margen	MHz
12	13.3	17.5	199.8
36	13.8	16.7	199.6
45	13.6	17.0	199.8
78	13.8	16.7	199.3

Pérdida

Valor general de margen (dB)* 7.7

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12	26.2	11.1	48.4	24.0	8.9	48.4
36	18.9	9.5	162.2	22.9	7.7	47.3
45	27.4	9.1	23.7	23.1	8.1	50.7
78	27.6	9.1	22.8	26.6	8.1	22.8

NEXT

Valor general de margen (dB)* 7.1

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12/36	47.4	11.2	165.5	60.1	7.1	35.7
12/45	45.3	7.4	130.9	47.6	11.4	166.5
12/78	72.1	9.2	4.1	73.3	10.4	4.1
36/45	50.6	10.1	92.9	44.2	9.0	199.3
36/78	48.5	11.1	184.9	45.1	9.8	187.8
45/78	51.8	16.8	199.3	52.6	17.1	187.8

ACR

Valor general de margen (dB)* ----

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 13.6

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12/36	71.6	12.6	1.6	72.8	12.5	1.4
12/45	64.3	23.0	1.2	64.2	22.9	54.7
12/78	62.7	29.1	1.0	59.3	29.6	54.7
36/12	72.8	12.6	1.4	71.6	12.6	1.6
36/45	36.1	17.9	179.5	35.7	17.5	178.2
36/78	45.3	26.7	171.0	44.3	25.4	164.2
45/12	46.5	23.0	99.7	64.6	22.8	1.2
45/36	35.3	17.0	178.2	35.7	17.6	179.5
45/78	58.8	38.3	1.0	40.5	33.1	194.8
78/12	85.0	29.9	25.7	92.7	29.1	1.0
78/36	43.9	24.5	164.2	14.9	25.3	171.0
78/45	59.8	33.4	194.4	58.9	15.9	1.0

PSNEXT

Valor general de margen (dB)* 8.5

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12	44.2	9.1	130.9	50.6	9.3	16.7
36	43.4	10.0	162.3	49.9	8.5	187.6
45	41.3	8.6	187.6	43.4	10.9	184.9
78	72.0	11.8	4.1	43.3	11.2	193.5

PSELFEXT

Valor general de margen (dB)* 14.9

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12	72.5	16.2	1.4	71.3	15.3	1.6
36	70.9	14.9	1.6	71.2	16.2	1.6
45	35.7	20.6	179.5	35.8	19.9	165.5
78	44.9	26.9	171.0	44.1	27.8	157.0

PSACR

Valor general de margen (dB)* ----

Pares	OMNIScanner dB	OMNIScanner Margen	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margen	OMNIRemote MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remote.

MICROTEST

Date: 25/Feb/00 11:32:00 PM Página 1

GMD

BIEN

OMNIScanner2 Informe de certificatión

		OMNIScanner		OMNIRemote
ID de circuito:	[illegible]			
Proyecto:	ATT-PISO10 VOZ	SOBC0100463	SW: V04.01	50B0C000024
Propietario:	OmniScanner	Adapd.		Adapd.
Autotest:	*Panduit Cat 6*	MT CAT6 SSTP		MT CAT6 SSTP
Cable:	BELDEN1872A			
NVP:	70			
Ubicación:	---			
Edificio:	---			
Piso:	---			
Armario:	---			

	Límite	12	36	45	78
Longitud ft	(100.0)	41.8	42.7	42.0	42.5
Retraso (ns):	(545)	197	201	198	200
Resistencia (Ohms):	(----)	---	---	---	---

Gráfico de cableado — Estimación — Real

OMNI: [illegible]

Remote: [illegible]

Sesgo (ns) (45): 4

Ancho de banda (MHz): ---

Atenuación

Valor general de margen (dB)*: 19.2

Pares	dB	Margen	MHz
12	10.8	19.7	199.9
36	11.3	19.2	199.8
45	11.3	19.2	199.8
78	11.3	19.2	199.8

Pérdida

Valor general de margen (dB)*: 7.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	25.2	11.5	66.0	25.3	11.6	66.5
36	18.2	7.1	124.2	18.7	7.7	124.2
45	22.4	9.1	74.7	22.7	8.9	66.6
78	29.0	12.1	32.9	30.4	13.6	33.1

NEXT

Valor general de margen (dB)*: 7.2

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	64.8	8.7	10.9	63.5	9.6	14.0
12/45	52.2	11.0	84.8	47.9	11.6	183.3
12/78	52.0	9.3	69.3	52.8	10.2	69.3
36/45	44.6	3.9	171.0	42.8	7.2	179.5
36/78	51.0	14.0	185.5	47.0	12.6	196.2
45/78	59.3	14.1	42.9	56.0	17.5	1.4

ACR

Valor general de margen (dB)*: ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)*: 12.4

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	74.2	12.4	1.0	26.1	12.6	1.0
12/45	39.6	19.6	147.1	50.7	18.9	1.2
12/78	43.9	20.8	151.8	44.7	27.3	197.1
36/12	75.2	12.0	1.0	74.2	12.4	1.2
36/45	53.0	17.8	25.3	51.4	17.9	30.6
36/78	41.8	22.3	154.3	40.9	23.0	196.4
45/12	80.7	18.9	1.2	83.4	19.9	1.0
45/36	54.3	17.8	30.6	53.0	17.8	25.2
45/78	52.9	25.4	190.6	56.2	38.0	190.3
78/12	46.5	27.6	183.6	44.2	26.2	181.8
78/36	41.0	21.7	126.4	41.6	22.1	154.3
78/45	56.3	28.6	190.3	53.1	35.6	152.6

PSNEXT

Valor general de margen (dB)*: 6.8

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	60.4	8.8	14.0	60.2	8.1	14.0
36	62.1	9.7	10.9	42.6	8.8	170.5
45	43.3	10.2	171.0	42.3	6.5	179.5
78	51.2	11.4	69.3	43.2	11.4	198.9

PSELFEXT

Valor general de margen (dB)*: 14.5

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	79.4	14.8	1.0	75.5	14.7	1.2
36	75.3	14.5	1.2	75.3	14.5	1.2
45	77.7	18.9	1.2	49.2	18.9	31.3
78	40.8	24.2	154.3	39.6	25.3	198.4

PSACR

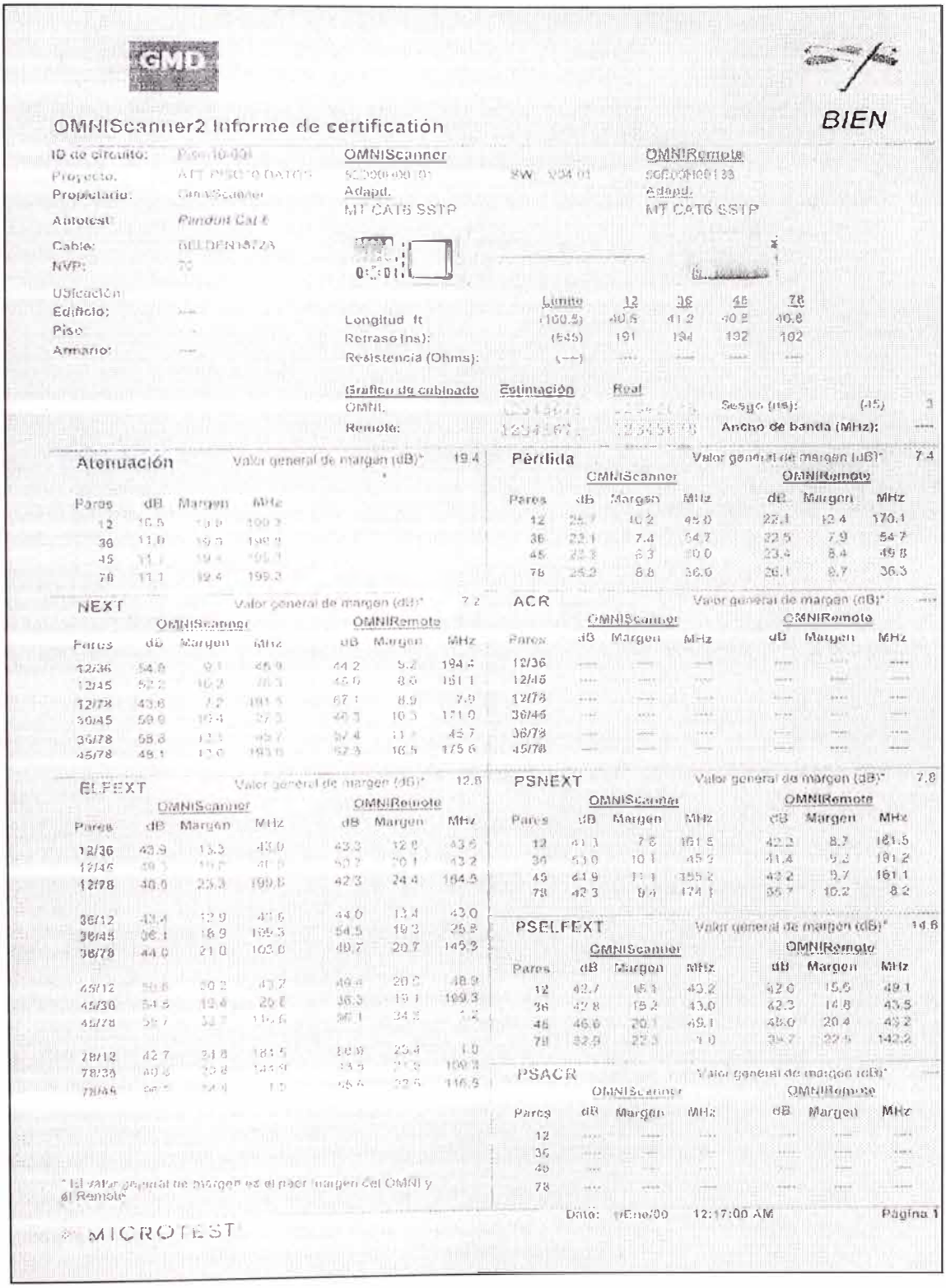
Valor general de margen (dB)*: ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remoto.

Date: 1/Ene/00 12:24:00 AM Página 1

MICROTEST



GMD

BIEN

OMNIScanner2 Informe de certificatión

ID de circuito: Piso10-001
Proyecto: ATT PISO 10 DATOS
Propietario: OmniScanner
Autotest: Pandun Cat 6
Cable: BELDEN1872A
NVP: 72
Ubicación
Edificio: ---
Piso: -
Armario: ---

OMNIScanner
SC000600 01
Adapd.
MT CAT6 SSTP

SW: V34.01

OMNIRemote
SCE000100139
Adapd.
MT CAT6 SSTP

	Limite	12	36	45	78
Longitud ft	(100.0)	40.6	41.2	40.2	40.8
Retraso (ns):	(545)	191	194	192	192
Resistencia (Ohms):	(---)	----	----	----	----

Grafico de cableado	Estimación	Real
OMNI:		
Remote:	12345678	12345678

Sesgo (ns): (45) 3
Ancho de banda (MHz): ----

Atenuación

Valor general de margen (dB)* 19.4

Pares	dB	Margen	MHz
12	16.5	19.4	100.0
36	17.0	19.5	100.0
45	17.1	19.4	100.0
78	17.1	19.4	100.0

Pérdida

Valor general de margen (dB)* 7.4

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	25.7	10.2	45.0	22.1	12.4	170.1
36	22.1	7.4	54.7	22.5	7.9	54.7
45	22.8	8.3	80.0	23.4	8.4	49.8
78	25.2	8.8	36.6	26.1	8.7	36.3

NEXT

Valor general de margen (dB)* 7.2

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	54.8	9.1	45.9	44.2	9.2	194.4
12/45	52.2	10.2	80.3	46.6	8.6	161.1
12/78	43.6	7.2	191.5	67.1	8.9	7.9
36/45	59.9	16.4	37.3	46.3	10.3	171.0
36/78	58.8	13.1	45.7	57.4	11.7	45.7
45/78	48.1	12.0	193.6	52.3	16.5	175.6

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	----	----	----	----	----	----
12/45	----	----	----	----	----	----
12/78	----	----	----	----	----	----
36/45	----	----	----	----	----	----
36/78	----	----	----	----	----	----
45/78	----	----	----	----	----	----

ELFEXT

Valor general de margen (dB)* 12.8

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	43.9	15.3	43.0	43.3	12.8	43.6
12/45	39.3	10.7	46.8	50.2	20.1	43.2
12/78	40.6	25.3	190.6	42.3	24.4	164.5
36/12	43.4	12.9	47.6	44.0	13.4	43.0
36/45	36.1	18.9	199.3	54.5	19.3	25.8
36/78	44.0	21.0	103.6	48.7	20.7	145.3
45/12	50.6	20.2	43.7	49.4	20.2	48.9
45/36	54.5	19.4	20.2	36.3	19.1	199.3
45/78	36.7	33.7	116.6	36.1	34.2	1.0
78/12	42.7	34.8	181.5	50.9	25.4	1.0
78/36	40.6	23.8	144.9	34.5	21.9	199.3
78/45	36.5	34.9	1.0	45.6	22.5	116.5

PSNEXT

Valor general de margen (dB)* 7.8

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	41.3	7.8	161.5	42.2	8.7	161.5
36	53.0	10.1	45.2	41.4	9.2	191.2
45	41.9	11.1	155.2	43.2	9.7	161.1
78	42.3	9.6	174.1	35.7	10.2	8.2

PSELFEXT

Valor general de margen (dB)* 14.6

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	42.7	15.1	43.2	42.0	15.6	49.1
36	42.8	15.2	43.0	42.2	14.8	43.5
45	46.6	20.1	49.1	45.0	20.4	49.2
78	32.9	22.3	1.0	39.7	22.6	142.2

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	----	----	----	----	----	----
36	----	----	----	----	----	----
45	----	----	----	----	----	----
78	----	----	----	----	----	----

* El valor general de margen es el peor margen del OMNI y el Remote

Date: 9/Ene/00 12:17:00 AM Página 1

MICROTEST

GMD

BIEN

OMNIScanner2 Informe de certificación

		OMNIScanner		OMNIRemote
ID de circuito:	Proc 11-001			
Proyecto:	ATT-VOZ-P11	60D30H00463	SW: V04.01	98E00G00024
Propietario:	OmniScanner	Adapd.		Adapd.
Autotest:	*Panduit Cat 6*	MT CAT6 SSTP		MT CAT6 SSTP
Cable:	BELDEN1872A			
NVP:	70			
Ubicación:	----			
Edificio:				
Piso:	----			
Armario:	----			

	Límite	12	36	45	78
Longitud (ft)	(100.5)	38.0	38.9	38.6	38.7
Retraso (ns):	(548)	179	183	181	182
Resistencia (Ohms):	(----)	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 4
Remote:	12345678	12345678	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 20.0

Pares	dB	Margen	MHz
12	9.9	20.6	199.3
36	10.5	20.0	195.8
45	10.4	20.1	180.3
78	10.5	20.0	198.3

Pérdida

Valor general de margen (dB)* 6.5

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	28.9	12.5	58.8	24.6	9.7	47.5
36	17.6	8.0	174.6	18.1	6.5	110.2
45	24.4	10.2	61.9	22.6	8.9	61.9
78	26.7	12.2	39.8	25.7	10.2	35.6

NEXT

Valor general de margen (dB)* 2.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	55.4	4.3	21.7	45.9	2.4	61.5
12/45	61.6	16.2	48.0	54.1	17.1	140.8
12/78	59.3	12.1	37.2	59.0	8.4	23.2
36/45	57.8	2.1	179.1	64.6	8.7	11.3
36/78	48.1	11.9	164.7	55.1	14.7	94.3
45/78	47.2	17.3	196.6	48.6	14.7	139.3

ACR

Valor general de margen (dB)* ----

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	----	----	----	----	----	----
12/45	----	----	----	----	----	----
12/78	----	----	----	----	----	----
36/45	----	----	----	----	----	----
36/78	----	----	----	----	----	----
45/78	----	----	----	----	----	----

ELFEXT

Valor general de margen (dB)* 1.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	43.0	11.0	36.5	43.5	11.5	36.5
12/45	47.2	19.4	52.9	43.8	18.2	76.0
12/78	47.7	29.5	176.2	63.9	27.9	23.0
36/12	43.7	11.6	36.5	43.1	11.1	36.5
36/45	78.0	15.6	1.4	77.3	15.5	1.2
36/78	41.6	22.2	156.1	40.2	22.0	89.8
45/12	44.1	18.4	75.0	80.2	18.5	1.2
45/36	77.3	15.5	1.2	76.0	15.7	1.4
45/78	94.2	30.6	1.0	93.4	31.6	1.2
78/12	64.0	27.9	23.6	46.0	29.7	178.2
78/36	46.2	22.0	89.8	41.6	22.1	155.2
78/45	93.4	31.6	1.2	94.2	30.5	1.0

PSNEXT

Valor general de margen (dB)* 4.2

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	56.1	6.7	21.7	45.9	5.2	61.5
36	44.9	4.9	61.9	46.6	4.9	61.5
45	37.6	4.8	178.8	34.3	11.1	11.3
78	44.4	11.1	194.7	38.0	11.9	23.2

PSELFEXT

Valor general de margen (dB)* 12.0

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	43.1	14.0	36.5	42.5	13.5	36.5
36	41.9	12.8	36.8	43.9	13.1	30.0
45	74.3	17.0	1.4	75.9	17.2	1.2
78	41.2	24.7	155.2	46.2	25.0	89.8

PSACR

Valor general de margen (dB)* ----

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	----	----	----	----	----	----
36	----	----	----	----	----	----
45	----	----	----	----	----	----
78	----	----	----	----	----	----

* El valor general de margen es el peor margen del OMNI y el Remote.

MICROTEST

GMD

BIEN

OMNIScanner2 Informe de certificación

		OMNIScanner		OMNIRemote	
ID de circuito:	Piso-11-001				
Proyecto:	ATT-Parquemar	50D00H00101	SW: V04.01	50E00H00132	
Propietario:	OmniScanner	Adapd.		Adapd.	
Autotest:	*Panduit Cat 6*	MT CAT6 SSTP		MT CAT6 SSTP	
Cable:	BELDEN1872A				
NVP:	70				
Ubicación:	---				
Edificio:	---				
Piso:	---				
Armario:	---				

	Límite	12	36	45	78
Longitud ft	(100.0)	38.9	39.5	39.1	39.3
Retraso (ns)	(548)	193	196	194	195
Resistencia (Ohms):	[---]	---	---	---	---

Gráfico de cableado	Estimación	Real		
OMNI:	12345678	12345678	Sesgo (ns):	(45) 3
Remoto:	12345678	12345678	Ancho de banda (MHz):	---

Atenuación

Valor general de margen (dB)* 20.0

Pares	dB	Margen	MHz
12	9.9	20.0	195.0
36	10.5	20.0	196.9
45	10.3	20.2	190.3
78	10.3	20.1	190.9

Pérdida

Valor general de margen (dB)* 7.2

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	25.5	10.4	49.5	27.6	12.5	48.1
36	16.6	7.2	114.3	15.4	7.3	123.5
45	23.0	8.2	60.9	22.4	8.0	66.6
78	25.6	10.6	48.9	26.1	13.9	54.6

NEXT

Valor general de margen (dB)* 1.9

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	41.0	6.1	197.1	42.2	4.6	138.6
12/45	56.0	13.1	77.4	65.1	14.2	68.2
12/78	42.9	1.9	76.6	54.6	6.5	32.9
36/45	42.4	5.3	150.1	50.1	6.6	15.4
36/78	49.6	10.6	114.7	47.8	11.0	163.4
45/78	50.7	15.7	196.2	52.9	17.6	134.0

ACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Valor general de margen (dB)* 12.7

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12/36	73.4	13.1	1.4	67.8	12.7	25.3
12/45	38.1	19.1	164.2	54.4	19.2	25.3
12/78	40.3	21.3	75.4	56.6	21.2	28.0
36/12	74.0	12.8	1.2	73.4	13.1	1.4
36/45	50.5	17.6	28.1	51.3	17.7	30.2
36/78	47.2	26.5	151.4	43.0	25.6	198.6
45/12	74.5	19.3	25.3	81.0	19.2	1.2
45/36	51.3	17.6	30.2	52.4	17.8	27.1
45/78	53.0	29.4	1.0	64.4	30.8	1.0
78/12	55.1	21.4	25.3	56.5	21.5	28.0
78/36	45.1	29.7	149.4	47.1	26.7	151.4
78/45	64.4	30.8	1.0	63.9	29.4	1.0

PSNEXT

Valor general de margen (dB)* 4.1

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	43.4	4.1	74.9	46.6	6.9	71.1
36	38.3	6.3	196.6	39.6	6.7	190.4
45	43.7	7.9	119.9	50.8	8.9	18.4
78	43.7	4.6	75.4	54.1	8.7	32.9

PSELFEXT

Valor general de margen (dB)* 14.5

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	40.8	14.6	28.3	72.2	14.9	1.4
36	45.7	15.1	30.4	46.7	14.5	25.3
45	50.2	16.7	27.7	49.0	16.5	28.2
78	41.5	23.2	136.1	46.5	20.7	53.1

PSACR

Valor general de margen (dB)* ---

	OMNIScanner			OMNIRemote		
Pares	dB	Margen	MHz	dB	Margen	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

* El valor general de margen es el peor margen del OMNI y el Remote.

MICROTEST

Date: 2/Feb/01 6:19:00 PM Página 1

ANEXO C. PRESUPUESTO DEL SISTEMA DE CABLEADO ESTRUCTURADO HORIZONTAL CAT 6 PISOS 1 - 6.

ITEM	DESCRIPCION	Unid.	CANT.	COSTO EN $	
				COSTO MATERIALES ($)	SUB TOTAL ($)
1	Rollo de cable UTP, 350 Mhz. Nivel 6, Belden	Cajas	39	105.12	4099.68
2	Face Plate de 2 puertos, Panduit	U.	8	2.26	18.08
3	Face Plate de 4 puertos, Panduit	U.	100	2.38	238
4	Mini Jack RJ-45 Nivel 6, Panduit	U.	220	5.3	1166
5	Modulo Blank Panduit	U.	200	0.5	100
6	Patch Pannel modular 24 RJ-45 Nivel 6, Panduit c /Jacks	U.	10	147.72	1477.2
7	Patch Pannel modular/IDC 24 RJ-45 Nivel 6,Panduit c /Jacks	U.	6	142.5	855
8	Organizador Horizontal 2ur. frontal, Panduit	U	15	40.05	600.75
9	Organizador Vertical frontal posterior Panduit	U.	8	84	672
10	Organizador Horizontal 1ur. frontal Panduit	U.	4	37.8	151.2
11	Rack Autosoportado 7' x 19", Rack Tecnologies	U.	2	210	420
12	Cinta tipo Velcro	U.	2	22.56	45.12
13	Rollo de tubo flexible 3/4"	mts	1	14	14
14	Rollo de tubo flexible 1"	mts	1	17	17
15	Patch cord 4', nivel 6 Panduit	U.	170	5.61	953.7
16	Patch Cord 6', nivel 6 Panduit	U.	70	5.98	418.6
17	Etiqueta para Patch Pannel	U.	2	70	140
18	Canaleta T-70 Panduit (base tapa y divisor)	U.	8	46.85	374.8
19	Base de union para canaleta T-70	U.	6	4.71	28.26
20	Tapa de union para canaleta T-70	U.	6	2.3	13.8
21	Esquinero interior para canaleta T-70	U.	0	12.5	0
22	Esquinero exterior para canaleta T-70	U.	4	15.48	61.92
23	Angulo Recto para canaleta	U.	6	18.79	112.74
24	Terminacion para canaleta T-70	U.	8	5.57	44.56
25	Soporte de Face Plate para canaleta T-70	U.	10	3.49	34.9
26	Cable Coaxial RG6	Cja.	0	0	0
27	Conectores RG6	U.	0	0	0
28	Spliter CATV RG6	U.	0	0	0
29	Falso Piso	U.	1	220	220
30	Escalerilla de Metal	U.	1	129.38	129.38
31	Materiales Varios	U.	1	230	230
32	Mano de obra	U.	220	15	3300
	NOTA : TODOS LOS PRECIOS NO INCLUYEN IGV.			TOTAL PARCIAL ($)	15,936.69

PISO 2

ITEM	DESCRIPCION	Unid.	CANT.	COSTO EN $	
				COSTO MATERIALES ($)	SUB TOTAL ($)
1	Rollo de cable UTP, 350 Mhz. Nivel 6, Belden	Cja	52	105.12	5466.24
2	Face Plate de 2 puertos, Panduit	U.	10	2.26	22.6
3	Face Plate de 4 puertos, Panduit	U.	144	2.38	342.72
4	Mini Jack RJ-45 Nivel 6, Panduit	U.	290	5.3	1537
5	Modulo Blank Panduit	U.	190	0.5	95
6	Patch Pannel modular 24 RJ-45 Nivel 6, Panduit c /Jacks	U.	13	147.72	1920.36
7	Patch Pannel modular/IDC 24 RJ-45 Nivel 6,Panduit c /Jacks	U.	8	142.5	1140
8	Organizador Horizontal 2ur frontal, Panduit	U	18	40.05	720.9
9	Organizador Vertical frontal posterior Panduit	U.	8	84	672
10	Organizador Horizontal 1ur, frontal Panduit	U.	6	37.8	226.8
11	Rack Autosoportado 7´ x 19", Rack Tecnologies	U.	2	210	420
12	Cinta tipo Velcro Panduit	U.	2	22.56	45.12
13	Rollo de tubo flexible 3/4"	Rollo	1	14	14
14	Rollo de tubo flexible 1"	Rollo	1	17	17
15	Patch cord 4´, nivel 6 Panduit	U.	180	5.61	1009.8
16	Patch Cord 6´, nivel 6 Panduit	U.	115	5.98	687.7
17	Etiqueta para Patch Pannel	U.	3	70	210
18	Canaleta T-70 Panduit (base tapa y divisor)	U.	10	46.85	468.5
19	Base de union para canaleta T-70	U.	8	´4.71	37.68
20	Tapa de union para canaleta T-70	U.	8	2.3	18.4
21	Esquinero interior para canaleta T-70	U.	0	12.5	0
22	Esquinero exterior para canaleta T-70	U.	0	15.48	0
23	Angulo Recto para canaleta	U.	6	18.79	112.74
24	Terminacion para canaleta T-70	U.	8	5.57	44.56
25	Soporte de Face Plate para canaleta T-70	U.	6	3.49	20.94
26	Cable Coaxial RG6	Cja.	1	103	103
27	Conectores RG6	U.	6	6.4	38.4
28	Spliter CATV RG6	U.	1	8	8
29	Falso Piso	U.	1	220	220
30	Escalerilla de Metal	U.	1	129.38	129.38
31	Materiales Varios	U.	1	230	230
32	Mano de obra	U.	283	15	4245
			TOTAL PARCIAL ($)		20,223.84

NOTA : TODOS LOS PRECIOS NO INCLUYEN IGV

PISO 3

ITEM	DESCRIPCION	Unid.	CANT.	COSTO EN $	
				COSTO MATERIALES ($)	SUB TOTAL ($)
1	Rollo de cable UTP, 350 Mhz. Nivel 6 , Belden	Cja	24	105.12	2522.88
2	Face Plate de 2 puertos, Panduit	U.	8	2.26	18.08
3	Face Plate de 4 puertos, Panduit	U.	65	2.38	154.7
4	Mini Jack RJ-45 Nivel 6, Panduit	U.	125	5.3	662.5
5	Modulo Blank Panduit	U.	100	0.5	50
6	Patch Pannel modular 24 RJ-45 Nivel 6, Panduit c /Jacks	U.	6	147.72	886.32
7	Patch Pannel modularMDC 24 RJ-45 Nivel 6,Panduit c /Jacks	U.	3	142.5	427.5
8	Organizador Horizontal 2ur, frontal, Panduit	U	6	40.05	240.3
9	Organizador Vertical frontal posterior Panduit	U.	8	84	672
10	Organizador Horizontal 1ur, frontal Panduit	U.	3	37.8	113.4
11	Rack Autosoportado 7' x 19" , Rack Tecnologies	U.	2	210	420
12	Cinta tipo Velcro Panduit	U.	2	22.56	45.12
13	Rollo de tubo flexible 3/4"	Rollo	1	14	14
14	Rollo de tubo flexible 1"	Rollo	1	17	17
15	Patch cord 4', nivel 6 Panduit	U.	100	5.61	561
16	Patch Cord 6', nivel 6 Panduit	U.	40	5.98	239.2
17	Etiqueta para Patch Pannel	U.	2	70	140
18	Canaleta T-70 Panduit (base tapa y divisor)	U.	10	46.85	468.5
19	Base de union para canaleta T-70	U.	8	4.71	37.68
20	Tapa de union para canaleta T-70	U.	8	2.3	18.4
21	Esquinero interior para canaleta T-70	U.		12.5	0
22	Esquinero exterior para canaleta T-70	U.		15.48	0
23	Angulo Recto para canaleta	U.	6	18.79	112.74
24	Terminacion para canaleta T-70	U.	8	5.57	44.56
25	Soporte de Face Plate para canaleta T-70	U.	6	3.49	20.94
26	Cable Coaxial RG6	Cja.	0	103	0
27	Conectores RG6	U.	0	6.4	0
28	Spliter CATV RG6	U.	0	8	0
29	Falso Piso	U.	1	220	220
30	Escalerilla de Metal	U.	1	129.38	129.38
31	Materiales Varios	U.	1	230	230
32	Mano de obra	U.	121	15	1815
				TOTAL PARCIAL ($)	10,281.20

NOTA : TODOS LOS PRECIOS NO INCLUYEN IGV.

PISO 4

ITEM	DESCRIPCION	Unid.	CANT.	COSTO EN $	
				COSTO MATERIALES ($)	SUB TOTAL ($)
1	Rollo de cable UTP, 350 Mhz Nivel 6 , Belden	Cja	48	105.12	5045.76
2	Face Plate de 2 puertos, Panduit	U.	10	2.26	22.6
3	Face Plate de 4 puertos, Panduit	U.	264	2.38	628.32
4	Mini Jack RJ-45 Nivel 6, Panduit	U.	270	5.3	1431
5	Modulo Blank Panduit	U.	260	0.5	130
6	Patch Pannel modular 24 RJ-45 Nivel 6, Panduit c /Jacks	U.	13	147.72	1920.36
7	Patch Pannel modular/IDC 24 RJ-45 Nivel 6,Panduit c /Jacks	U.	5	142.5	712.5
8	Organizador Horizontal 2ur, frontal, Panduit	U	14	40.05	560.7
9	Organizador Vertical frontal posterior Panduit	U.	8	84	672
10	Organizador Horizontal 1ur, frontal Panduit	U.	6	37.8	226.8
11	Rack Autosoportado 7' x 19", Rack Tecnologies	U.	2	210	420
12	Cinta tipo Velcro Panduit	U.	2	22.56	45.12
13	Rollo de tubo flexible 3/4"	Rollo	1	14	14
14	Rollo de tubo flexible 1"	Rollo	1	17	17
15	Patch cord 4', nivel 6 Panduit	U.	175	5.61	981.75
16	Patch Cord 6', nivel 6 Panduit	U.	100	5.98	598
17	Etiqueta para Patch Pannel	U.	3	70	210
18	Canaleta T-70 Panduit (base tapa y divisor)	U.	8	46.85	374.8
19	Base de union para canaleta T-70	U.	6	4.71	28.26
20	Tapa de union para canaleta T-70	U.	6	2.3	13.8
21	Esquinero interior para canaleta T-70	U.	0	12.5	0
22	Esquinero exterior para canaleta T-70	U.	0	15.48	0
23	Angulo Recto para canaleta	U.	4	18.79	75.16
24	Terminacion para canaleta T-70	U.	6	5.57	33.42
25	Soporte de Face Plate para canaleta T-70	U.	8	3.49	27.92
26	Cable Coaxial RG6	Cja.	0	103	0
27	Conectores RG6	U.	0	6.4	0
28	Spliter CATV RG6	U.	0	8	0
29		U.	0	0	0
30		U.	0	0	0
31	Falso Piso	U.	1	220	220
32	Escalerilla de Metal	U.	1	129.38	129.38
33	Materiales Varios	U.	1	230	230
34	Mano de obra	U.	264	15	3960
			TOTAL PARCIAL ($)		18,728.65

PISO 5

ITEM	DESCRIPCION	Unid.	CANT.	COSTO EN $	
				COSTO MATERIALES ($)	SUB TOTAL ($)
1	Rollo de cable UTP, 350 Mhz. Nivel 6 , Belden	Cja	42	105.12	4415.04
2	Face Plate de 2 puertos, Panduit	U.	7	2.26	15.82
3	Face Plate de 4 puertos, Panduit	U.	110	2.38	261.8
4	Mini Jack RJ-45 Nivel 6, Panduit	U.	235	5.3	1245.5
5	Modulo Blank Panduit	U.	210	0.5	105
6	Patch Pannel modular 24 RJ-45 Nivel 6, Panduit c /Jacks	U.	10	147.72	1477.2
7	Patch Pannel modular/IDC 24 RJ-45 Nivel 6,Panduit c /Jacks	U.	5	142.5	712.5
8	Organizador Horizontal 2ur, frontal, Panduit	U	8	40.05	320.4
9	Organizador Vertical frontal posterior Panduit	U.	8	84	672
10	Organizador Horizontal 1ur frontal Panduit	U.	5	37.8	189
11	Rack Autosoportado 7' x 19" , Rack Tecnologies	U.	2	210	420
12	Cinta tipo Velcro Panduit	U.	2	22.56	45.12
13	Rollo de tubo flexible 3/4"	Rollo	1	14	14
14	Rollo de tubo flexible 1"	Rollo	1	17	17
15	Patch cord 4', nivel 6 Panduit	U.	170	5.61	953.7
16	Patch Cord 6', nivel 6 Panduit	U.	70	5.98	418.6
17	Etiqueta para Patch Pannel	U.	3	70	210
18	Canaleta T-70 Panduit (base tapa y divisor)	U.	6	46.85	281.1
19	Base de union para canaleta T-70	U.	4	4.71	18.84
20	Tapa de union para canaleta T-70	U.	4	2.3	9.2
21	Esquinero interior para canaleta T-70	U.	0	12.5	0
22	Esquinero exterior para canaleta T-70	U.	0	15.48	0
23	Angulo Recto para canaleta	U.	3	18.79	56.37
24	Terminacion para canaleta T-70	U.	5	5.57	27.85
25	Soporte de Face Plate para canaleta T-70	U.	5	3.49	17.45
26	Cable Coaxial RG6	Cja.	0	103	0
27	Conectores RG6	U.	0	6.4	0
28	Spliter CATV RG6	U.	0	8	0
29	Falso Piso	U.	1	220	220
30	Escalerilla de Metal	U.	1	129.38	129.38
31	Materiales Varios	U.	1	230	230
32	Mano de obra	U.	228	15	3420
				TOTAL PARCIAL ($)	15,902.87

NOTA : TODOS LOS PRECIOS NO INCLUYEN IGV.

PISO 6

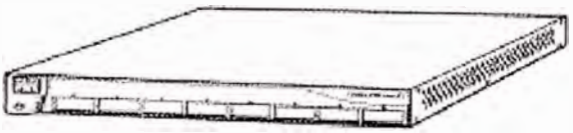
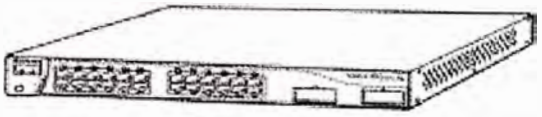
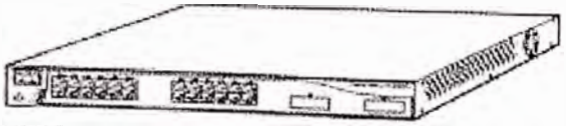
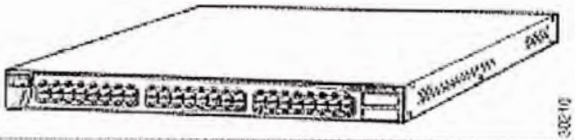
ITEM	DESCRIPCION	Unid.	CANT.	COSTO EN $	
				COSTO MATERIALES ($)	SUB TOTAL ($)
1	Rollo de cable UTP, 350 Mhz. Nivel 6 , Belden	Cja	23	105.12	2417.76
2	Face Plate de 2 puertos, Panduit	U.	5	2.26	11.3
3	Face Plate de 4 puertos, Panduit	U.	120	2.38	285.6
4	Mini Jack RJ-45 Nivel 6, Panduit	U.	130	5.3	689
5	Modulo Blank Panduit	U.	110	0.5	55
6	Patch Pannel modular 24 RJ-45 Nivel 6, Panduit c /Jacks	U.	6	147.72	886.32
7	Patch Pannel modular/IDC 24 RJ-45 Nivel 6,Panduit c /Jacks	U.	3	142.5	427.5
8	Organizador Horizontal 2ur, frontal, Panduit	U	6	40.05	240.3
9	Organizador Vertical frontal posterior Panduit	U.	8	84	672
10	Organizador Horizontal 1ur, frontal Panduit	U.	3	37.8	113.4
11	Rack Autosoportado 7' x 19" , Rack Tecnologies	U.	2	210	420
12	Cinta tipo Velcro Panduit	U.	2	22.56	45.12
13	Rollo de tubo flexible 3/4"	Rollo	1	14	14
14	Rollo de tubo flexible 1"	Rollo	1	17	17
15	Patch cord 4', nivel 6 Panduit	U.	100	5.61	561
16	Patch Cord 6', nivel 6 Panduit	U.	30	5.98	179.4
17	Etiqueta para Patch Pannel	U.	2	70	140
18	Canaleta T-70 Panduit (base tapa y divisor)	U.	10	46.85	468.5
19	Base de union para canaleta T-70	U.	8	4.71	37.68
20	Tapa de union para canaleta T-70	U.	8	2.3	18.4
21	Esquinero interior para canaleta T-70	U.	0	12.5	0
22	Esquinero exterior para canaleta T-70	U.	0	15.48	0
23	Angulo Recto para canaleta	U.	6	18.79	112.74
24	Terminacion para canaleta T-70	U.	6	5.57	33.42
25	Soporte de Face Plate para canaleta T-70	U.	6	3.49	20.94
26	Cable Coaxial RG6	Cja.	1	103	103
27	Conectores RG6	U.	6	6.4	38.4
28	Spliter CATV RG6	U.	1	8	8
29		U.	0	0	0
30		U.	0	0	0
31	Falso Piso	U.	1	220	220
32	Escalerilla de Metal	U.	1	129.38	129.38
33	Materiales Varios	U.	1	230	230
34	Mano de obra	U.	123	15	1845
				TOTAL PARCIAL ($)	10,440.16

NOTA : TODOS LOS PRECIOS NO INCLUYEN IGV.

ANEXO D. CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS CISCO – 3500XL SWITCHES

Features

The Catalyst 3500 series XL switches---also referred to as Catalyst 3500 XL switches---are stackable 10/100 Ethernet switches to which you can connect workstations and Cisco IP Phones and other network devices such as servers, routers, and other switches. These switches also can be deployed as backbone switches, aggregating 10/100 and Gigabit Ethernet traffic from other network devices. A feature specific to the Catalyst 3524-PWR XL switch is its ability to provide inline power to Cisco IP Phones. (Phone adapters are not required when connecting to the Catalyst 3524-PWR XL 10/100 switch ports.)

Switch	Description	
WS-C3508G-XL	8 GBIC[1]-based gigabit module slots	
WS-C3512-XL	12 autosensing 10/100 Ethernet ports 2 GBIC-based gigabit module slots	
WS-C3524-XL	24 autosensing 10/100 Ethernet ports 2 fixed GBIC-based gigabit module slots	
WS-C3524-PWR-XL	24 autosensing 10/100 inline-power Ethernet ports 2 GBIC-based gigabit module slots	
WS-C3548-XL	48 autosensing 10/100 Ethernet ports 2 GBIC-based gigabit module slots	

1. GBIC = Gigabit Interface Converter

Table 1-2: Catalyst 3512, 3524, 3524-PWR, and 3548 XL Features

Feature	Description
Performance and Configuration	• Autonegotiation of speed and duplex operation on 10/100 Ethernet ports • 12, 24, or 48 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet slots • Support for up to 250 port-based VLANs • ISL and IEEE 802.1Q trunking support on all ports • Support for voice VLAN ID (VVID) • High-speed EtherChannel connections between switches and servers • 8192 MAC addresses • IEEE 802.1p capable • CGMP to limit the flooding of IP multicast traffic • Broadcast storm control to prevent performance degradation from broadcast storms • SPAN port monitoring on any port • Support for command switch redundancy • Support for Cisco GBIC modules o GigaStack GBIC o 1000BaseSX GBIC module o 1000BaseLX/LH GBIC module o 1000BaseZX GBIC module
Management	• Cisco IOS CLI through the console port or Telnet • CiscoView device-management application • Cluster Management Suite, a web-based tool for managing switch clusters or an individual switch through a single IP

	address • SNMP
Power Redundancy	• Connection for optional Cisco RPS 600 that operates on AC input and supplies DC output to the Catalyst 3512, 3524, and 3548 XL switches • Connection for optional Cisco RPS 300 that operates on AC input and supplies DC output to the Catalyst 3524-PWR XL switch
Inline Power (Catalyst 3524-PWR XL switch only)	• Ability to provide inline power for Cisco IP Phones from all 24 10/100 Ethernet ports • Auto-detection and control of inline phone power on a per-port basis on all 10/100 ports • Support for fan-fault and over-temperature detection through Visual Switch Manager (VSM)

Front-Panel Description

The front panel of the Catalyst 3508G XL switch (Figure 1-2) has eight 1000BaseX GBIC module slots but no 10/100 ports. The front panel of the Catalyst 3512, 3524, 3524-PWR and 3548 XL switches (Figure 1-3, Figure 1-4, Figure 1-5, and Figure 1-6) have **10/100 RJ-45 ports and two 1000BaseX GBIC module slots. All Catalyst 3500 XL switches have a set of LEDs and a Mode button. (The Catalyst 3548 XL switch has a Mode label that you press.) These front-panel components are described in this section.**

Figure 1-2: Catalyst 3508G XL Switch

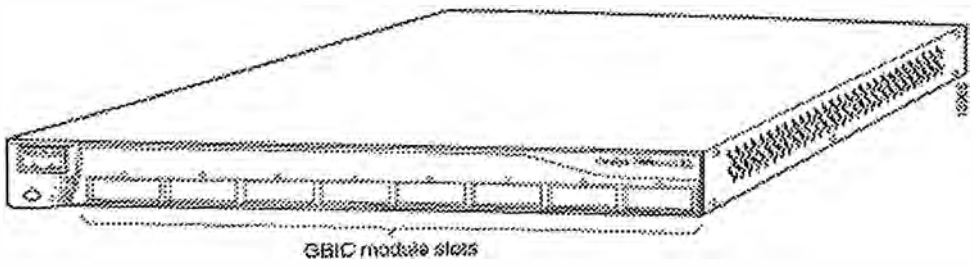


Figure 1-3: Catalyst 3512 XL Switch

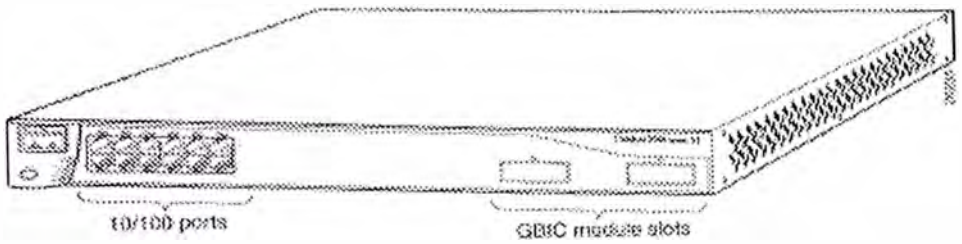


Figure 1-4: Catalyst 3524 XL Switch

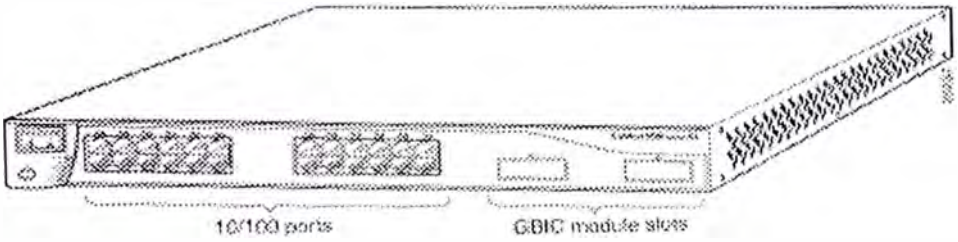


Figure 1-5: Catalyst 3524-PWR XL Switch

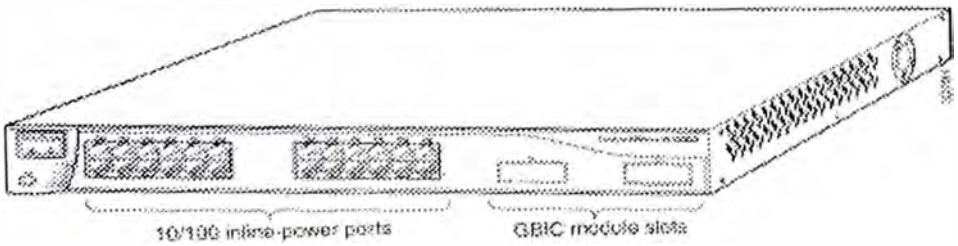
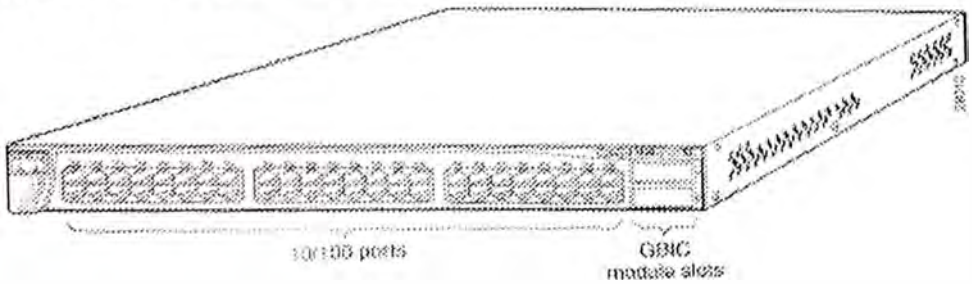


Figure 1-6: Catalyst 3548 XL Switch



10/100 Ports

The 10/100 ports on the Catalyst 3512, 3524, 3524-PWR, and 3548 XL switches are grouped in pairs. For example, in Figure 1-3, Figure 1-4, Figure 1-5, and Figure 1-6, ports 1 and 2 are the left-most pair. The first member of the pair (port 1) is above the second member (port 2). Port 3 is above port 4, and so on.

The 10/100 switch ports can connect, up to a distance of 100 meters, to any compatible network device:

- 10BaseT-compatible devices such as workstations, Cisco IP Phones, and hubs through standard RJ-45 connectors and Category 3, 4, or 5 cabling

- 100BaseTX-compatible devices such as high-speed workstations, Cisco IP Phones, servers, hubs, routers, and other switches through standard RJ-45 connectors and Category 5 cabling

The 10/100 switch ports can be explicitly set to operate in any combination of half duplex, full duplex, 10 Mbps, or 100 Mbps. These ports also can be set for speed and duplex autonegotiation, compliant with IEEE 802.3u. When set for autonegotiation, the port can sense the speed and duplex settings of the attached device and advertises its own capabilities. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission, if the attached device supports it) and configures itself accordingly.

The 10/100 ports on the Catalyst 3512, 3524, 3524-PWR, and 3548 XL switches provide protocol support for Cisco IP Phones. The Catalyst 3548 and 3524-PWR XL switches also support per-port priority override. Refer to the *Cisco IOS Desktop Switching Software Configuration Guide* for more information about these features.

GBIC Module Slots

The Cisco Gigabit Interface Converter (GBIC) module slots support the following modules to provide flexibility in media and distance options:

- 1000BaseSX GBIC module for fiber connections of up to 550 meters.
- 1000BaseLX/LH GBIC module for fiber connections of up to 10 kilometers.
- 1000BaseZX GBIC module for fiber connections of up to 100 kilometers.
- GigaStack GBIC module for creating a 1-Gbps stack configuration of up to nine Catalyst 3500 XL switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to nine half-duplex links (in a stack configuration) to other Gigabit Ethernet devices. Using the required Cisco proprietary signaling and cabling, the maximum distance for a GigaStack GBIC-to-GigaStack GBIC connection is 1 meter.

You can install up to two GBICs in the Catalyst 3512, 3524, 3524-PWR and 3548 XL switches and up to eight GBICs in the Catalyst 3508G XL switch.

Figure 1-7 and Figure 1-8 show how a GBIC module is inserted into a GBIC module slot on the switch. Refer to the documentation that came with your GBIC module for complete GBIC module information.

Figure 1-7: Installing a 1000BaseX GBIC Module in the Switch

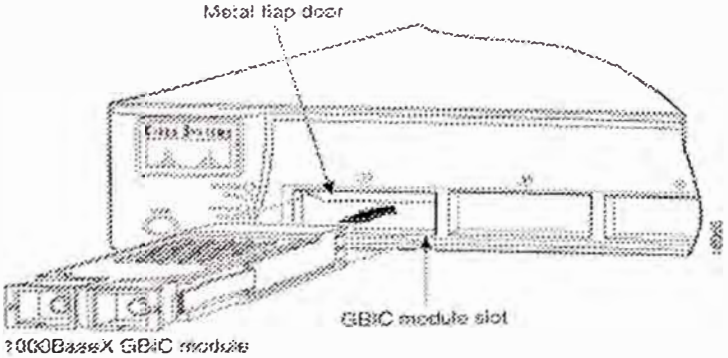
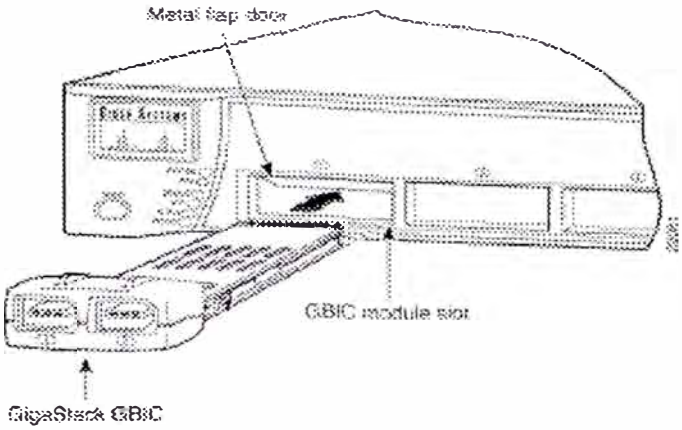


Figure 1-8: Installing a GigaStack GBIC Module in the Switch



LEDs

You can use the switch LEDs described in this section to monitor switch activity and its performance. Figure 1-9, Figure 1-10, Figure 1-11, and Figure 1-12 show the location of the LEDs and the Mode button that you use to select one of the port modes.

All of the LEDs described in this section except the utilization meter (UTL) are visible on the VSM home page and Cluster Manager page. The *Cisco IOS Desktop Switching Software Configuration Guide* describes how to use the Cluster Management Suite to monitor individual switches and how to use cluster management software to monitor all the switches in a cluster.

Figure 1-9: Catalyst 3508G XL LEDs

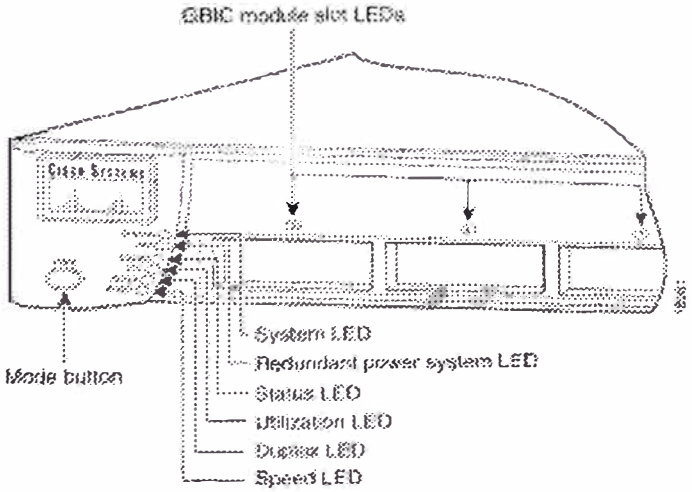


Figure 1-10: Catalyst 3512 and 3524 XL LEDs

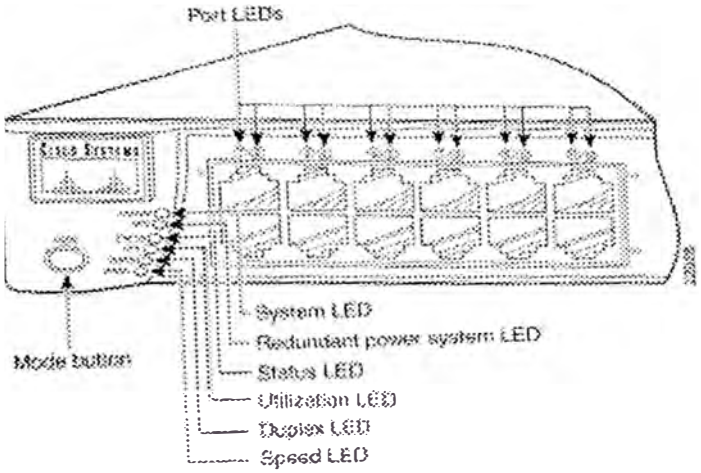


Figure 1-11: Catalyst 3524-PWR XL LEDs

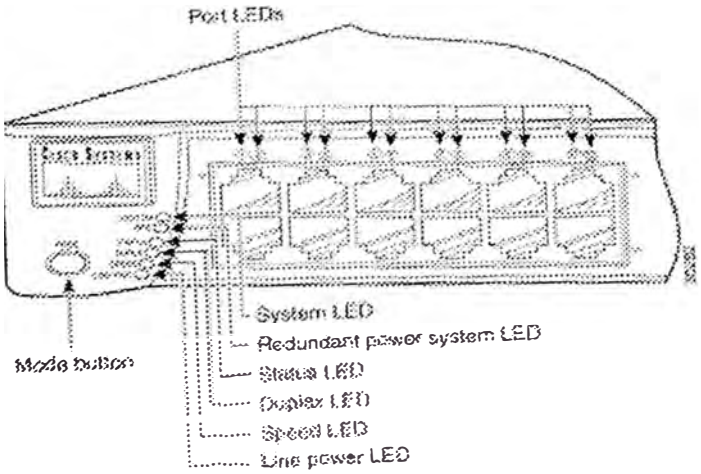
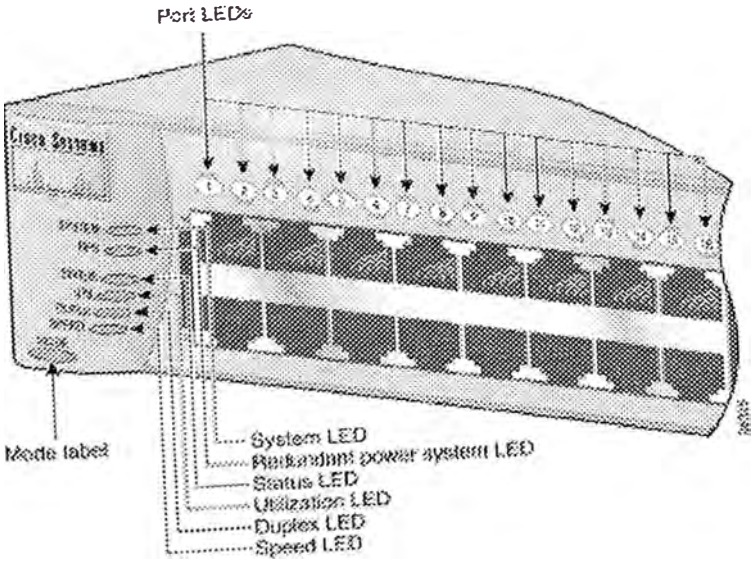


Figure 1-12: Catalyst 3548 XL LEDs



System LED

The System LED shows whether the system is receiving power and is functioning properly. Table 1-3 lists the LED colors and their meanings.

Table 1-3: System LED

Color	System Status
Off	System is not powered on.
Green	System is operating normally.
Amber	System is receiving power but is not functioning properly.

For information on the System LED colors during POST, see the "Powering On the Switch and Running POST" section.

RPS LED

The Redundant Power System (RPS) LED shows the RPS status. Table 1-4 and Table 1-5 list the LED colors and their meanings.

Note The Cisco RPS 600 (model PWR600-AC-RPS) supports the Catalyst 3512, 3524, 3548, and 3508 XL switches.

Table 1-4: RPS LED for the Catalyst 3508, 3512, 3524, and 3548 XL Switches

Color	RPS Status
Off	RPS is off or is not installed.
Solid green	RPS is operational.
Blinking green	RPS and the switch AC power supply are both powered on. If the switch power supply fails, the switch powers down and restarts after 15 seconds, using power from the RPS. The switch goes through its normal boot sequence when it restarts.

	Note This is not a recommended configuration. For more information see the "RPS Connector on the Catalyst 3508, 3512, 3524, and 3548 XL Switches" section.
Amber	RPS is connected but not functioning properly. One of the power supplies in the RPS could be powered down, or a fan on the RPS could have failed. **Note** If you are using an RPS with a revision level lower than Z3 with a Catalyst 3508G XL or a Catalyst 3548 XL switch, the switch RPS LED might display amber (normally indicating an RPS malfunction) even when the RPS is functioning properly. The LEDs display correctly for RPS revision level Z3 or later. The label on the bottom of the RPS shows the revision level.

Note The Cisco RPS 300 (model PWR300-AC-RPS) supports the Catalyst 3524-PWR XL switch.

Table 1-5: RPS LED for the Catalyst 3524-PWR XL Switch

Color	RPS Status
Off	RPS is off or is not installed.
Solid green	RPS is connected and operational.
Blinking green	RPS is backing up another switch in the stack.
Solid amber	RPS is connected but not functioning properly. One of the power supplies in the RPS could be powered down, or a fan on the RPS could have failed.
Blinking amber	Internal power supply of the switch is down, and redundancy is lost. The switch is operating on the RPS.

For more information about the failure conditions on the Cisco RPS 300, refer to the *Cisco Redundant Power System 300 Hardware Installation Guide*.

Port LEDs and Modes

Each 10/100 port and module slot has a port LED. These port LEDs, as a group or individually, display information about the switch and about the individual ports. The port modes (Table 1-6) determine the type of information displayed through the port LEDs.

To select or change a mode, press the Mode button until the desired mode is highlighted. When you change port modes, the meaning of the port LED colors also changes. Table 1-7 and Table 1-8 explain how to interpret the port LED colors after you change the port mode.

Note To change the port mode in the Catalyst 3548 XL switch, press the Mode label.

Table 1-6: Port Mode LEDs

Mode LED	Port Mode	Description
STAT	Port status	The port status. This is the default mode.
UTL	Switch utilization	The current bandwidth in use by the switch.
DUPLX	Port duplex mode	The port duplex mode: full duplex or half duplex.
SPEED	Port speed	The port operating speed: 10, 100, or 1000 Mbps.
LINE PWR	Port inline power	The inline power status: on or off.

Table 1-7: Meaning of LED Colors in Different Modes on the Catalyst 3508, 3512, 3524, and 3548 XL Switches

Port Mode	LED Color	Meaning
STATUS (port status)	Off	No link.
	Solid green	Link present.

	Flashing green	Activity Port is transmitting or receiving data
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Solid amber	Port is not forwarding. Port was disabled by management or an address violation or was blocked by Spanning Tree Protocol (STP). **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
UTL (utilization)	Green	The LEDs display backplane utilization on a logarithmic scale. If all port LEDs are green, the switch is using 50 percent or more of its total bandwidth capacity. If the right-most LED is amber, the switch is using less than 50 percent of its total bandwidth. If the LED to the left of the right-most LED is amber, the switch is using less than 25 percent of its total capacity, and so on. See Figure 1-13, Figure 1-15, and Figure 1-16 for details.
DUPLEX	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
SPEED (speed)	**10/100 ports**	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	1000BaseX ports	
	Off	Port is not operating.
	Green	Port is operating at 1000 Mbps.

Table 1-8: Meaning of LED Colors in Different Modes on the Catalyst 3524-PWR XL Switch

Port Mode	LED Color	Meaning
STATUS (port status)	Off	No link.
	Solid green	Link present.
	Flashing green	Activity. Port is transmitting or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Solid amber	Port is not forwarding. Port was disabled by management or an address violation or was blocked by Spanning Tree Protocol (STP). **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
DUPLEX	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
SPEED (speed)	**10/100 ports**	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	1000BaseX ports	

	Off	Port is not operating.
	Green	Port is operating at 1000 Mbps.
LINE PWR (inline power)	Off	Inline power is off.
	Green	Inline power is on. If the Cisco IP Phone is receiving power from an AC power source, the port LED is off even if the IP phone is connected to the switch port. The LED turns green only when the switch port is providing power.

Figure 1-13, Figure 1-14, Figure 1-15, and Figure 1-16 show the bandwidth utilization percentages displayed by the right-most LEDs.

Note The port LEDs on the Catalyst 3524-PWR XL switch do not show bandwidth utilization. To find out the switch bandwidth usage, use the Device Bandwidth Graph on VSM.

Figure 1-13: Bandwidth Utilization for the Catalyst 3508G XL Switch

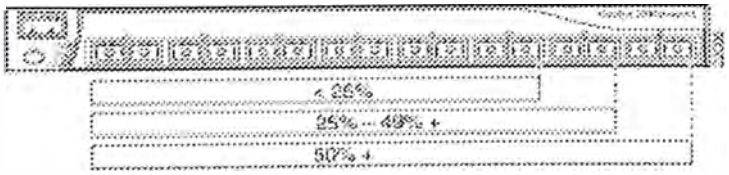


Figure 1-14: Bandwidth Utilization for the Catalyst 3512 XL Switch

Figure 1-15: Bandwidth Utilization for the Catalyst 3524 XL Switch

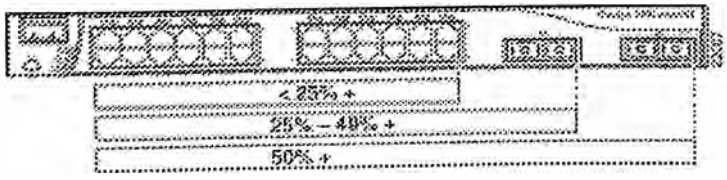
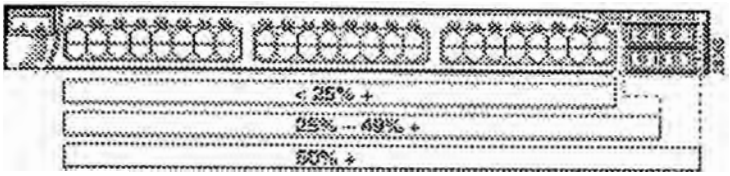


Figure 1-16: Bandwidth Utilization for the Catalyst 3548 XL Switch



If all port LEDs on the Catalyst 3548 XL switch are green, the switch is using 50 percent or more of its total bandwidth capacity. If all 10/100 port LEDs are green and the lower GBIC LED is amber, the switch is using between 25 and 50 percent of its total bandwidth. If all 10/100 port LEDs are green and if both the GBIC LEDs are amber, the switch is using less than 25 percent of its total capacity, and so on.

Rear-Panel Description

Switch rear panels have an AC power connector, an RPS connector, and an RJ-45 console port (see Figure 1-17, Figure 1-19, Figure 1-18, and Figure 1-20), which are described in this section.

Figure 1-17: Catalyst 3508G XL Rear Panel

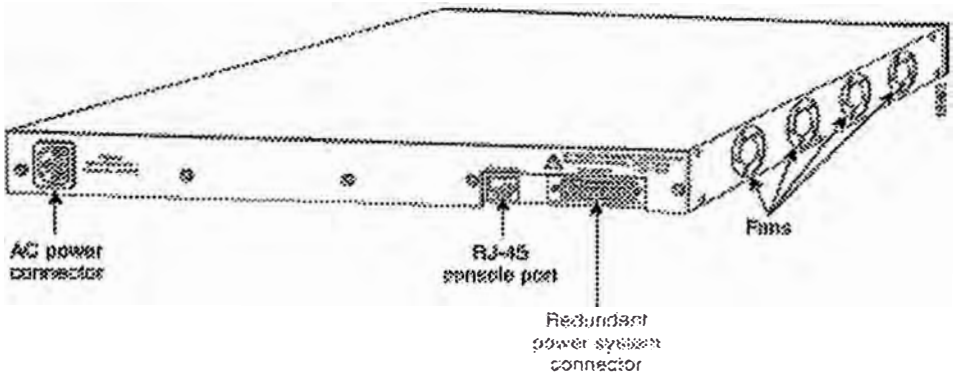


Figure 1-18: Catalyst 3512 and 3524 XL Rear Panel

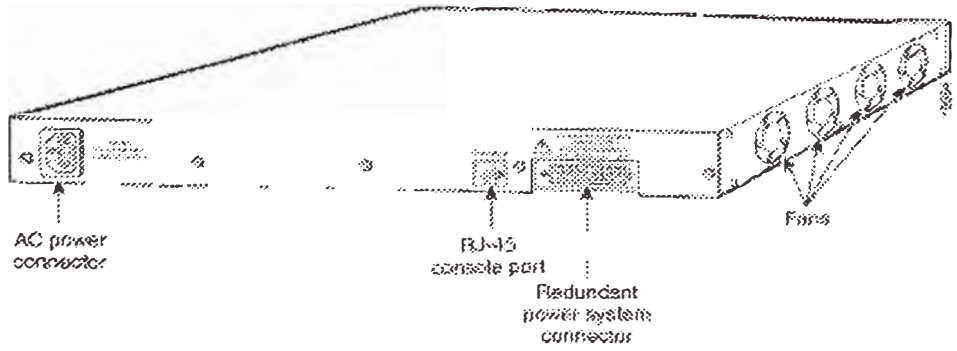


Figure 1-19: Catalyst 3524-PWR XL Rear Panel

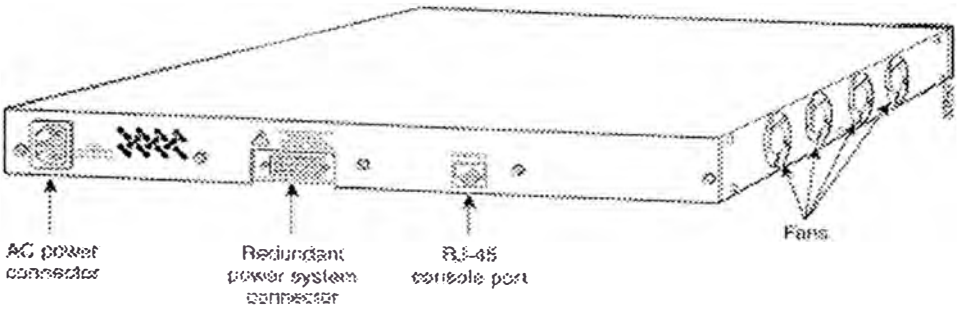
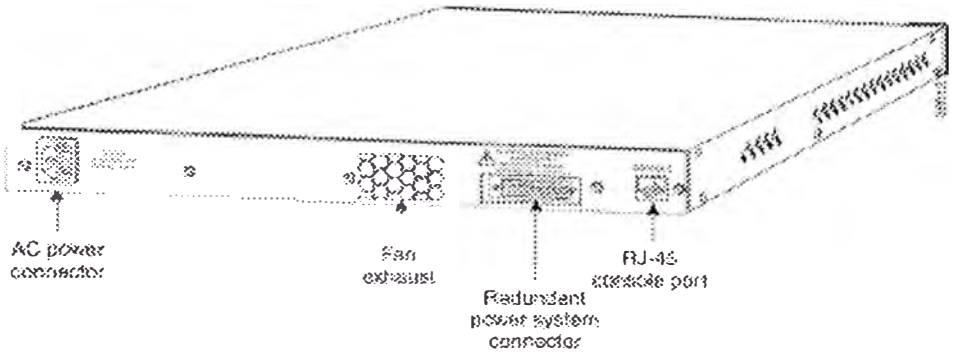


Figure 1-20: Catalyst 3548 XL Rear Panel



Power Connectors

You can provide power to the switch either through the internal power supply or through the Cisco RPS.

Internal Power Supply Connector

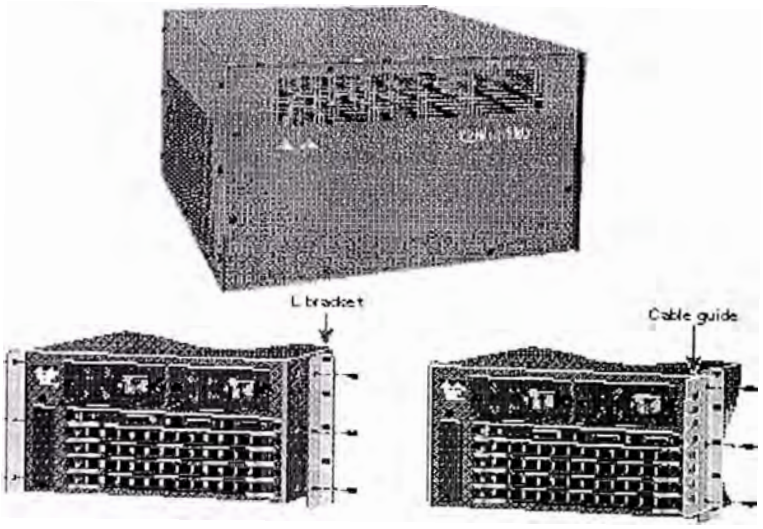
The internal power supply is an autoranging unit that supports input voltages between 100 and 240 VAC. If you plan to use the internal power supply, use the supplied AC power cord to connect the AC power connector to an AC power outlet.

Cisco RPS Connector

Specific Cisco RPS models support specific Catalyst 3500 XL switches:

- Cisco RPS 600 (model PWR600-AC-RPS)---Supports the Catalyst 3512, 3524, 3548, and 3508 XL switches
- Cisco RPS 300 (model PWR300-AC-RPS)---Supports the Catalyst 3524-PWR XL switch

ANEXO E. CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS CISCO – CATALYST 6500 SWITCHES.



Power Requirements

- 8.0A @ 100 VAC 60 Hz
- KVA rating: 0.8 KVA
- 4.0A 200 VAC 50 Hz
- Power consumption: 376 watts

Environmental Conditions

- Operating temperature: 32 to 104° F (0 to 40° C)
- Storage temperature: -40 to 167° F (-40 to 75° C)
- Relative humidity: 10% to 90%, noncondensing
- Operating altitude: -60 to 4000 m
- Mean time between failures (MTBF): seven years for system configuration

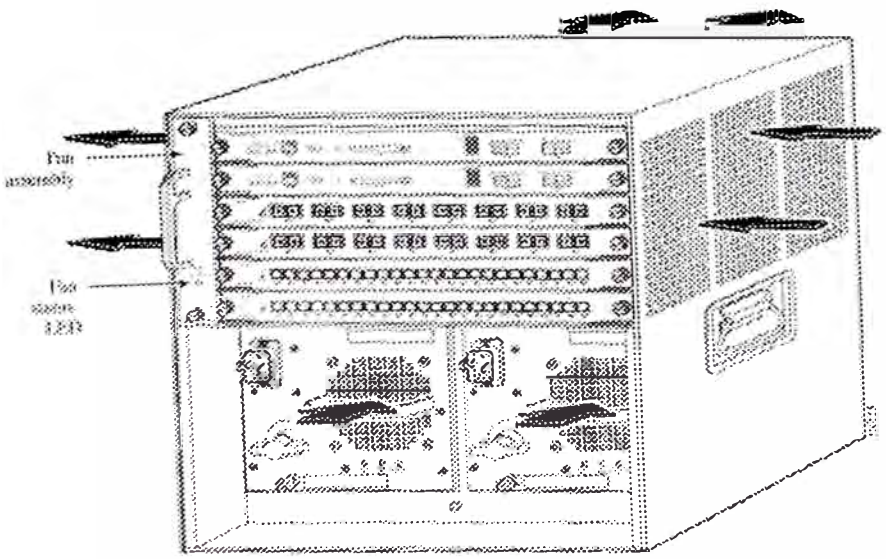
Regulatory Compliance

Safety Certifications

- UL 1950
- EN 60950
- CSA-C22.2 no. 950
- IEC 950

Electromagnetic Emissions Certifications

- FCC 15J Class A
- VCCI CE II
- CE Mark
- EN 55022 Class B
- CISPR 22 Class B



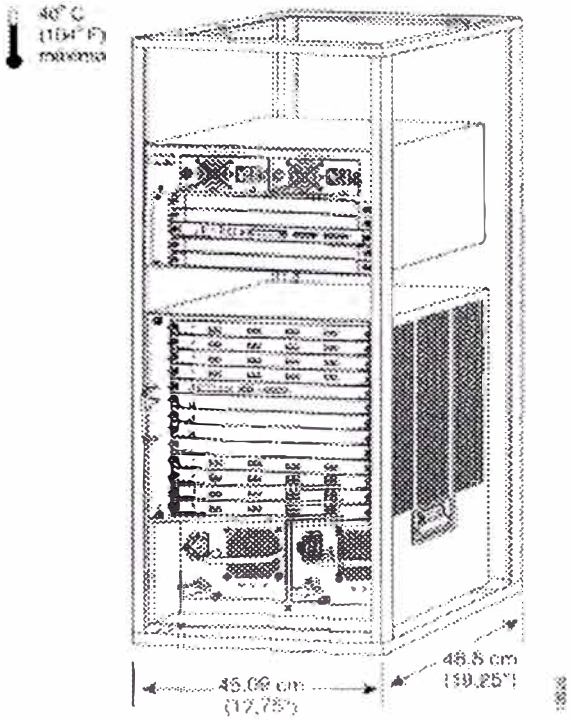


Table 21-51: Power Requirements for Catalyst 6000 Series and 6500 Series

Description	Specification
AC Input Current	17.6A max. @ 100VAC 8.8A max. @ 200VAC
DC Input current	-38A @ 48VDC -30A @ 60VDC
KVA rating	.8KVA
AC Output power	1300W max.
DC Output power	1360W
Heat Dissipation	6140 BTU/hr max.

Table 21-52: Physical and Environmental Specifications for Catalyst 6000 Series and 6500 Series

Description	Specification
Dimensions (H x W x D)	Catalyst 6006 and 6506 switches: 20.1 x 17.2 x 18.1 in. (49.7 x 42.5 x 44.7 cm) Catalyst 6009 and 6509 switches: 25.2 x 17.2 x 18.1 in. (62.3 x 42.5 x 44.7 cm)
Minimum weight	65 lb (29.4 kg)
Maximum weight	150 lb (67.9 kg)
Mounting	19 in. (48.26 cm) rack-compatible (rack and cable guide hardware included)
Operating temperature	32 to 104°F (0 to 40°C)
Storage	-60 to 4000 m
Mean time between temperature	-40 to 167°F (-40 to 75°C)
Relative humidity	10 to 90%, noncondensing
Operating altitude failures (MTBF)	Seven years for system configuration

Table 21-53: Regulatory Approvals for Catalyst 6000 Series and 6500 Series

Description	Specification
Safety Certifications	UL 1950 EN 60950 CSA-C22.2 no. 950 IEC 950
Electromagnetic Emissions Certifications	FCC 15J Class A VCCI CE II EN 55022 Class B CISPR 22 Class B

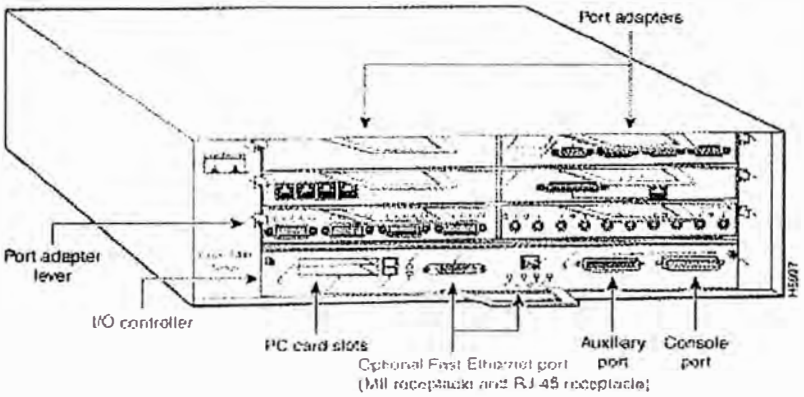
ANEXO F. CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS CISCO – ROUTERS 7200 .

Physical Description

The front of the Cisco 7206 provides access to an I/O controller and up to six network interface port adapters (see Figure 1-1). The I/O controller contains the following: a local console port for connecting a data terminal (or data terminal equipment [DTE]) and an auxiliary port for connecting a modem (or other data communications equipment [DCE]) or other devices for configuring and managing the router; two PC Card slots for Flash memory cards; an optional Fast Ethernet port. The Fast Ethernet port provides a 100-Mbps connection to the network.

✎ **Note** The I/O controller is available with or without a Fast Ethernet port. The I/O controller with a Fast Ethernet port is equipped with either a single MII port or an MII port and an RJ-45 port (only one port can be used at a time). Although still supported by Cisco Systems, the I/O controller equipped with the single MII port was discontinued as an orderable product in May 1998.

Figure 1-1 Cisco 7206 Router—Front View



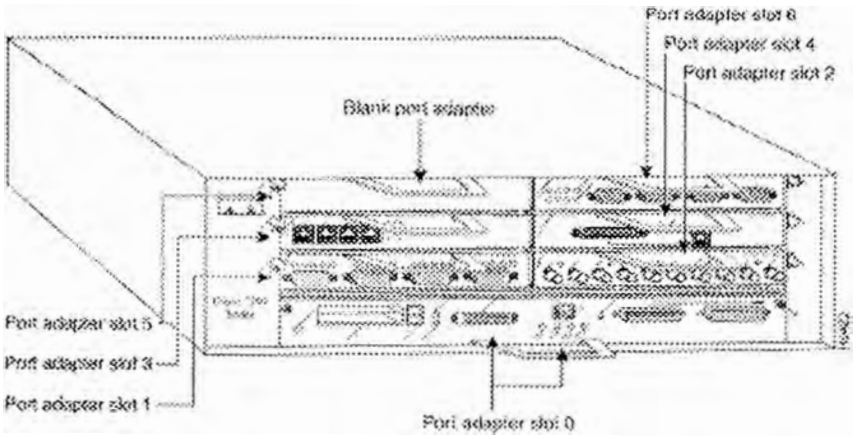
The port adapters installed in the Cisco 7206 are of the same type as those installed on the second-generation Versatile Interface Processors (VIP2s) in the Cisco 7500 series routers, in Cisco 7000 series routers using the 7000 Series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI), and in the Cisco uBR7200 series routers. The port adapters installed in the Cisco 7206 support OIR. For an explanation of OIR, refer to the "Online Insertion and Removal" section later in this chapter.

✎ **Note** The I/O controller does not support OIR. You must power down the Cisco 7206 before removing the I/O controller from the router.

Port adapter slots in the Cisco 7206 router are numbered from left to right, beginning with port adapter slot 1 and continuing through port adapter slot 6. Port adapter slot 0 is the Fast Ethernet port on the I/O controller (refer to Figure 1-2).

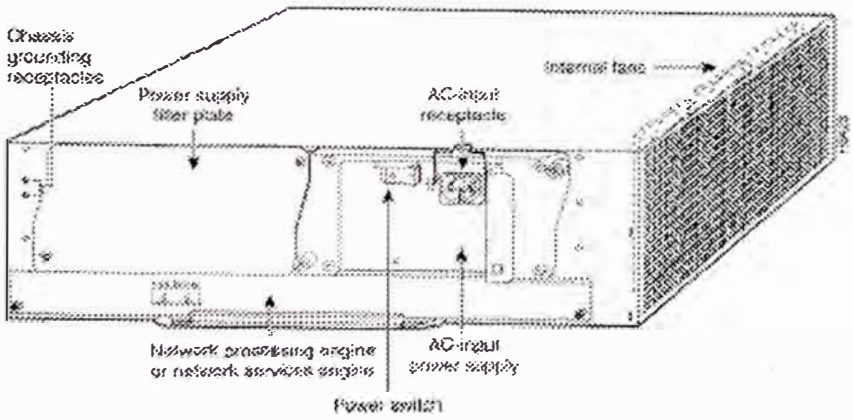
✎ **Note** In Figure 1-1 and Figure 1-2, a blank port adapter is installed in slot 5. To ensure adequate airflow across the port adapters, each port adapter slot must be filled with either a port adapter or a blank port adapter.

Figure 1-2 Port Adapter Slot Numbering



The rear of the Cisco 7206 router provides access to the network processing engine and up to two power supplies (refer to Figure 1-3).

Figure 1-3 Cisco 7206 Router—Rear View



Note The network processing engine does not support OIR. You must power down the Cisco 7206 before removing the network processing engine from the router.

The network processing engine has no external connectors or LEDs. There is a handle for removing and installing the network processing engine and two captive installation screws for securing it to the chassis.

The Cisco 7206 router comes equipped with one 280W AC-input or one 280W DC-input power supply. A fully configured Cisco 7206 router operates with only one installed power supply; however, a second, optional power supply of the same type provides hot-swappable, load-sharing, redundant power. Figure 1-3 shows the rear of a Cisco 7206 router configured with a single AC-input power supply. (A power supply filler plate is installed over the second power supply bay.)

Caution Do not mix power supplies in the Cisco 7206. In dual power supply router configurations, both power supplies *must* be of the same type (two AC-input power supplies or two DC-input power supplies).

The power supply has the router's main power switch and either an AC-input power receptacle or a hardwired DC-input power cable (depending on the type of installed power supply).

Adjacent to the power supply bays are two chassis grounding receptacles that provide a chassis ground connection for ESD equipment or a two-hole grounding lug (refer to Figure 1-3).

Three internal fans draw cooling air into the chassis and across internal components to maintain an acceptable operating temperature. (Refer to Figure 1-3.) The three fans are enclosed in a tray that is located in the subchassis.

Caution To ensure the proper flow of cooling air across the internal components, make sure blank port adapters are installed in unoccupied port adapter slots, and power supply filler plates are installed in unoccupied power supply bays.

The I/O controller, port adapters, power supplies, and network processing engine slide into their respective chassis slots and connect directly to the router midplane; there are no internal cables to connect. The midplane distributes DC power from the power supplies to the I/O controller, port adapters, fan tray, and network processing engine.

The midplane also senses OIR of the port adapters, bridges the PCI buses from the port adapters to packet static random-access memory (SRAM) on the network processing engine, arbitrates traffic across the PCI buses, and generates the clock signals for the port adapters on each PCI bus.

The Cisco 7206 operates as either a tabletop or rack-mounted unit. A rack-mount kit is standard equipment included with all Cisco 7206 routers when they are shipped from the factory. The kit provides the hardware needed to mount the router in a standard 19-inch equipment rack or a telco rack. Steps for installing the Cisco 7206 router in an equipment rack are explained in "Installing the Cisco 7206," the "Rack-Mounting the Cisco 7206" section. If you are not rack-mounting your Cisco 7206, place it on a sturdy tabletop or platform.

A fully configured Cisco 7206, with two installed power supplies and all chassis slots filled, weighs approximately 50 pounds (22.7 kilograms [kg]). For clearance requirements and rack-mount installation considerations, refer to "Preparing for Installation," the "Site Requirements" section.

System Specifications

Table 1-1 lists the Cisco 7206 router physical specifications and power requirements.

Table 1-1 Cisco 7206 Physical Specifications

Description	Specification
Midplane	Two primary PCI buses and one secondary PCI bus with an aggregate bandwidth of 600 Mbps[1]
Dimensions (H x W x D)	5.25 in. x 16.8 in. x 17 in. (13.34 cm x 42.67 cm x 43.18 cm)
Weight	Chassis fully configured with a network processing engine, I/O controller, 6 port adapters, 2 power supplies, and a fan tray: ~ 50 lb (22.7 kg)
Heat dissipation	370W (1262 Btu[2])
AC-input voltage rating	100-240 VAC[3] wide input with power factor correction
AC-input current rating	5A[4] at 100-240 VAC with the chassis fully configured

AC-input frequency rating	50/60 Hz[5]
AC-input cable	18 AWG[6] three-wire cable, with a three-lead IEC-320 receptacle on the power supply end, and a country-dependent plug on the power source end
DC-output power	280W maximum (with either a single or a dual power supply configuration)
DC-input voltage rating	-48 VDC[7] nominal in North America -60 VDC nominal in the European Union
DC-input current rating	13A at -48 VDC (370W/-48 VDC = 7.7A typical draw) 8A at -60 VDC (370W/-60 VDC = 6.2A typical draw)
DC voltages supplied and maximum, steady-state current ratings	+5.2V @ 30A +12.2V @ 9A -12.0V @ 1.5A +3.5V @ 13A
DC-input cable	In accordance with local and national wiring regulations
Airflow	~80 cfm[8]
Temperature	32 to 104° F (0 to 40° C) operating; -4 to 149° F (-20 to 65° C) nonoperating
Humidity	10 to 90% noncondensing
Recommended minimum software requirements[9]	Cisco IOS Release 11.1(17)CA or a later release of Cisco IOS 11.1 CA Cisco IOS Release 11.2(12)P or a later release of Cisco IOS 11.2 P Cisco IOS Release 11.3(2)T or a later release of Cisco IOS 11.3 T Cisco IOS Release 12.0(3)T or a later release of Cisco IOS 12.0 T
Standards compliance • Compliance • Safety • EMC •	CE marking UL 1950, CSA 22.2 No. 950, EN60950, ACA TS001, AS/NZS 3260, IEC 950 FCC Class A (47 CFR, Part 15), CSA Class A, EN55022 Class B, CISPR22 Class B, VCCI Class B, AS/NRZ 3590 Class B

	Class B GR-1089-CORE, GR-63-CORE IEC-1000-4-2, IEC-1000-4-3, IEC-1000-4-4, IEC-1000-4-5, IEC-1000-4-6, IEC-1000-4-11, IEC 1000-3-2, EN50082-1, EN50082-2

1 Mbps = megabits per second.

2 Btu = British thermal units.

3 VAC = volts alternating current.

4 A = amperes.

5 Hz = hertz.

6 AWG = American Wire Gauge.

7 VDC = volts direct current.

8 cfm = cubic feet per minute.

9 Refer to the Cisco AS5800 Universal Access Server documentation listed in the "Related Documentation" section for Cisco IOS release requirements for the Cisco AS5800 Universal Access Server.

Note For a chassis footprint, additional dimensions, and clearance requirements for the Cisco 7206 perimeter, refer to "Preparing for Installation," the "Site Requirements" section.

Field-Replaceable Units

The Cisco 7206 router is easy to service; all its major components are field replaceable units (FRUs). The following sections describe Cisco 7206 FRUs:

- Network Processing Engine
- Input/Output Controller
- LED Descriptions
- Port Adapters and Service Adapters
- Power Supplies
- Chassis
- Flash Disks and Flash Memory Cards
- Rack-Mount and Cable-Management Kit

Note Instructions for removing and replacing FRUs are contained in separate documents. For example, if you need to replace the network processing engine (NPE) in your Cisco 7206 router, refer to the Network Processing Engine and Network Services Engine Installation and Configuration document that accompanies every NPE shipped from the factory as a FRU. The document is also available on the Documentation CD-ROM and on Cisco.com (formerly Cisco Connection Online [CCO]).

For ordering information, contact a customer service representative.

Network Processing Engine

The network processing engine maintains and executes the system management functions for the Cisco 7206 router. The network processing engine also shares the system memory and environmental monitoring functions with the I/O controller.

Note Detailed instructions for removing and replacing the network processing engine are contained in the document Network Processing Engine and Network Services Engine Installation and Configuration. This document accompanies every network processing engine that is shipped from the factory as a FRU. It is also available on the Documentation CD-ROM and on Cisco.com (formerly Cisco Connection Online [CCO]).

Cisco 7206 routers support five versions of the network processing engine: NPE-100, NPE-150, NPE-175, NPE-200, and NPE-225. These network processing engines have the same functionality; however, the performance differs because of the microprocessor type and the type of memory for packet data (SRAM and DRAM, or SDRAM) each network processing engine provides.

The NPE-175 and NPE-225 consist of two modular boards: the processor engine board and the network controller board. SRAM is not included in the NPE-175 or NPE-225.

Note The NPE-100, although still supported, is no longer an orderable product as of May 1999.

Note The Cisco 7206 as a router shelf in a Cisco AS5800 Universal Access Server only supports the NPE-200.

The network processing engines consist of the following components:

- Reduced instruction set computing (RISC) microprocessor
  - The NPE-100 and NPE-150 have an R4700 microprocessor that operates at an internal clock speed of 150 MHz.
  - The NPE-175 has an RM5270 microprocessor that operates at an internal clock speed of 200 MHz.
  - The NPE-200 has an R5000 microprocessor that operates at an internal clock speed of 200 MHz.
  - The NPE-225 has an RM5271 microprocessor that operates at an internal clock speed of 262 MHz.
- System controller
  - The NPE-100, NPE-150, and NPE-200 have a system controller that uses direct memory access (DMA) to transfer data between DRAM and packet SRAM on the network processing engine.
  - The NPE-175 and NPE-225 have one system controller that provides processor access to the two midplane and single I/O controller PCI buses. The system controller also allows port adapters on either of the two midplane PCI buses to access SDRAM.
- Upgradable memory modules
  - The NPE-100, NPE-150, and NPE-200 use DRAM for storing routing tables, network accounting applications, packets of information in preparation for process switching, and packet buffering for SRAM overflow (except in the NPE-100, which contains no packet SRAM). The standard configuration is 32 MB, with up to 128 MB available through single in-line memory module (SIMM) upgrades.
  - The NPE-175 and NPE-225 use SDRAM for providing code, data, and packet storage.

- Packet SRAM for storing packets of information in preparation for fast switching
  -
    - The NPE-100 does not have packet SRAM.
    - The NPE-150 has 1 MB of SRAM.
    - The NPE-175 does not have packet SRAM.
    - The NPE-200 has 4 MB of SRAM.
    - The NPE-225 does not have packet SRAM.
- Cache memory
  -
    - The NPE-100, NPE-150, and NPE-200 have unified cache SRAM that functions as the secondary cache for the microprocessor. (The primary cache is within the microprocessor.)
    - The NPE-175 and NPE-225 have two levels of cache: a primary that is internal to the processor and a secondary, 2-MB external cache that provides additional high-speed storage for data and instructions.
- Two environmental sensors for monitoring the cooling air as it leaves the chassis
- Boot ROM for storing sufficient code for booting the Cisco IOS software; the NPE-175, NPE-200, and NPE-225 have a boot ROM

The network processing engines perform the following system management functions:

- Sending and receiving routing protocol updates
- Managing tables, caches, and buffers
- Monitoring interface and environmental status
- Providing Simple Network Management Protocol (SNMP) management through the console and Telnet interface
- Accounting for and switching of data traffic
- Booting and reloading images
- Managing port adapters (recognition and initialization during online insertion and removal)

Figure 1-4 shows the NPE-100, Figure 1-5 shows the NPE-150, Figure 1-6 shows the NPE-175, Figure 1-7 shows the NPE-200, and Figure 1-8 shows the NPE-225.

Figure 1-4 NPE-100

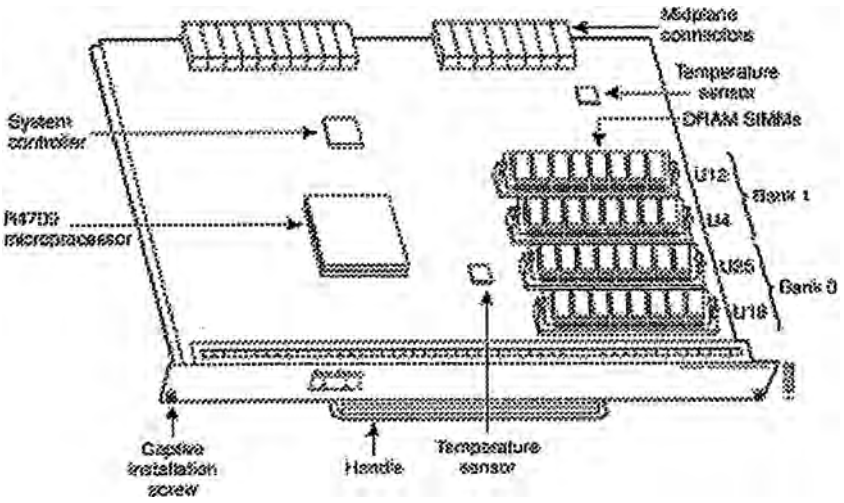


Figure 1-5 NPE-150

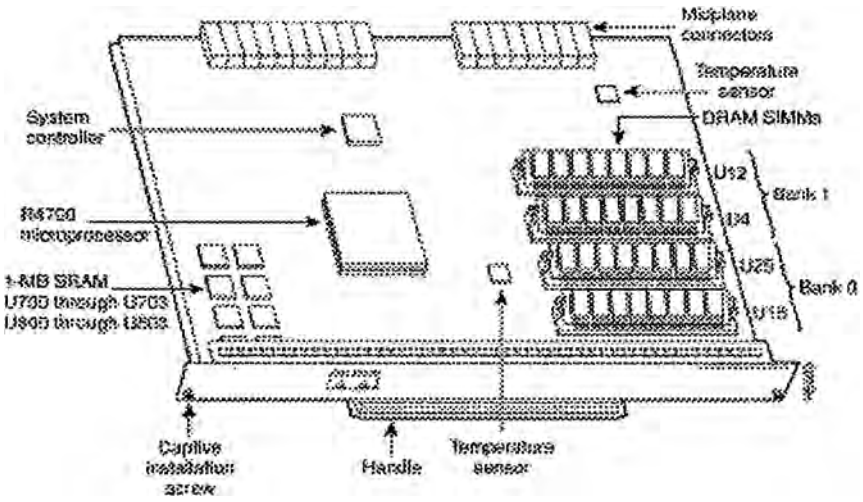


Figure 1-6 NPE-175

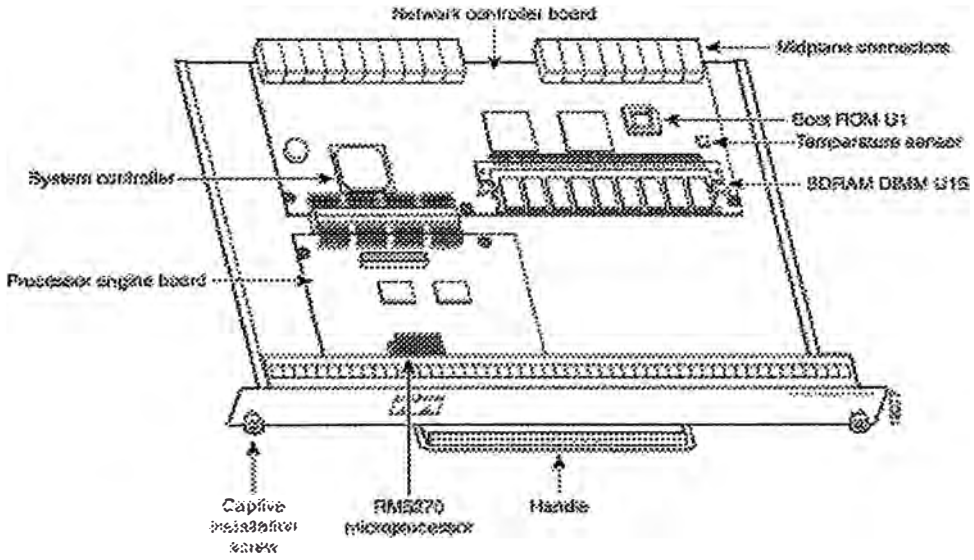


Figure 1-7 NPE-200

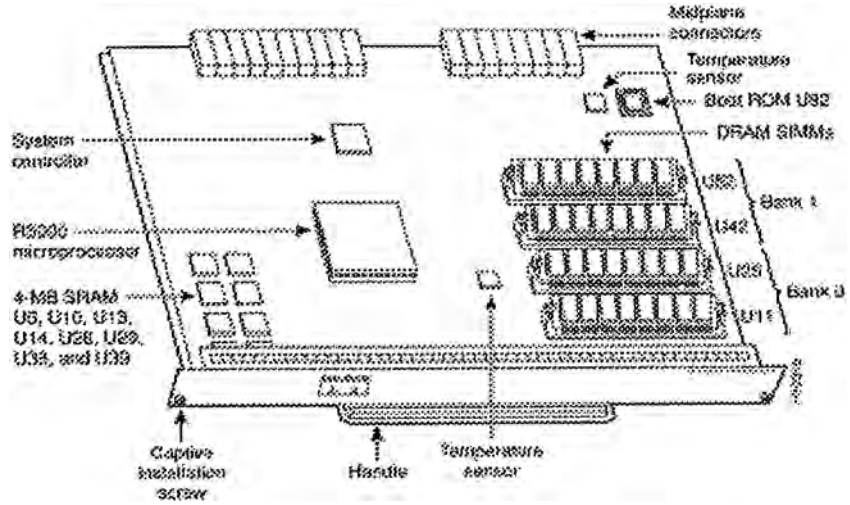


Figure 1-8 NPE-225

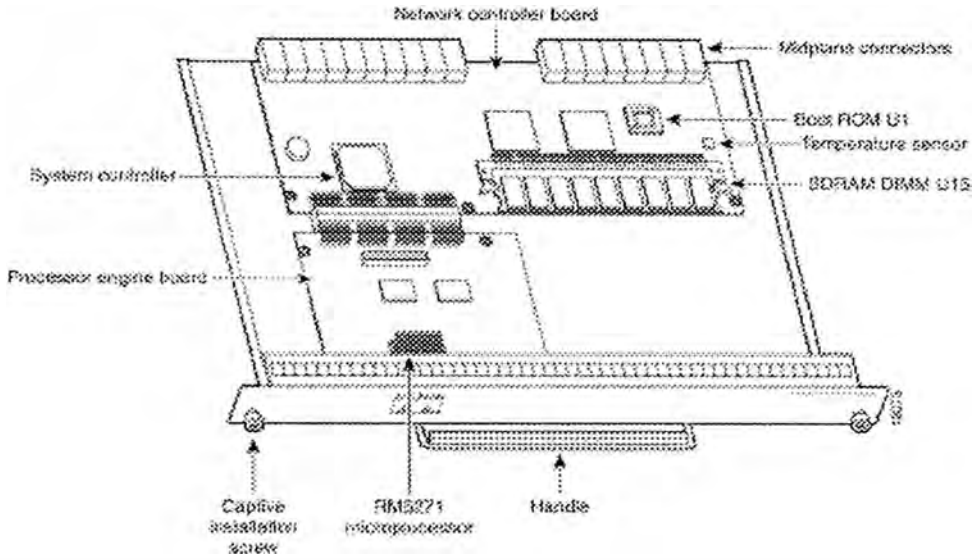


Table 1-2 lists the NPE-100, NPE-150, and NPE-200 network processing engine memory specifications.

Table 1-2 Network Processing Engine Memory Specifications (NPE-100, NPE-150, and NPE-200)

Memory Type	Size	Quantity	Description	Location
DRAM	32 to 128 MB	2 to 4	16- or 32-MB SIMMs (based on maximum DRAM required)	Bank 0: U18 and U25 or U11 and U25[1] Bank 1: U4 and U12 or U42 and U52[2]
SRAM NPE-150	1 MB	8	8 chips, each being 128K words x 9 bits wide	U700 through U703 U800 through U803
NPE-200	4 MB	8	8 chips, each being 512K words x 8 bits wide	U6, U10, U13, U14, U28, U29, U38, and U39
Boot ROM[3] NPE-200	256 KB	1	EPROM for the ROM monitor program	U92
Primary cache	—	—	R4700 processor, internal cache R5000 processor, internal cache	NPE-100, NPE-150: U201 NPE-200: U44
Secondary cache	512 KB	4	R4700, unified external cache	NPE-100 and NPE-150: U2, U10, U14, and U26

cache	KB			U26
			R5000 unified, external cache	NPE-200: U16, U9, U109, and U107

1 The sockets for bank 0 on the NPE-100 and the NPE-150 are numbered U18 and U25. The same sockets on the NPE-200 are numbered U11 and U25.

2 The sockets for bank 1 on the NPE-100 and the NPE-150 are numbered U4 and U12. The same sockets on the NPE-200 are numbered U42 and U52.

3 ROM = read-only memory. The NPE-100 and NPE-150 use the boot ROM present on the I/O controller.

Note To prevent DRAM errors in the NPE-100, NPE-150, or NPE-200, and to ensure that your system initializes correctly at startup, DRAM bank 0 (socket U18 and U25, or U11 and U25) must contain no fewer than two SIMMs of the same type. You may also install two SIMMs of the same type in bank 1 (socket U4 and U12, or U42 and U52); however, bank 0 must always contain the two largest SIMMs.

Table 1-3 lists the NPE-175 and NPE-225 memory specifications.

Table 1-3 NPE-175 and NPE-225 Memory Specifications

Memory Type	Size	Quantity	Description	Location[1]
SDRAM	64 or 128 MB	1 configurable bank with 1 SDRAM slot	DIMM	U15
Boot ROM	512 KB	—	One-time programmable ROM	U1
Primary cache	16 KB (instruction), 16 KB (data)	—	R527x processor primary internal cache	U4
	32 KB (instruction), 32 KB (data)	—	R527x processor primary internal cache	U4
Secondary cache	2 MB	4 chips, each 512K by 8 bits wide	R527x unified external cache	U5, U6, U7, U8

1 Located on processor engine board. (See Figure 1-6 or Figure 1-8.)

Table 1-4 lists the NPE-100, NPE-150, and NPE-200 factory-installed DRAM configurations and their product numbers.

Table 1-4 DRAM SIMM Configurations (NPE-100, NPE-150, and NPE-200)

Total DRAM[1]	DRAM Bank 0	Quantity	DRAM Bank 1	Quantity	Product Number
32 MB	U18 and U25 or U11 and U25	2 16-MB SIMMs	U4 and U12 or U42 and U52	—	MEM-NPE-32MB[2]
64 MB	U18 and U25 or U11 and U25	2 32-MB SIMMS	U4 and U12 or U42 and U52	—	MEM-NPE-64MB[2]
128 MB	U18 and U25 or U11 and U25	2 32-MB SIMMs	U4 and U12 or U42 and U52	2 32-MB SIMMs	MEM-NPE-128MB[2]

1 Refer to the Cisco AS5800 Universal Access Server documentation listed in the Preface, "Related Documentation" section, for Cisco AS5800 Universal Access Server DRAM options.

2 These products are also available as DRAM upgrades. For example, to upgrade a network processing engine from 32 MB to 64 MB of DRAM, order Product Number MEM-NPE-64MB=.

Table 1-5 lists the NPE-175 and NPE-225 SDRAM DIMM configurations.

Table 1-5 NPE-175 and NPE-225 SDRAM DIMM Configurations

Total DRAM	DRAM Bank	Quantity	Product Number
64 MB	U15	1 64-MB DIMM	MEM-SD-NPE-64MB
128 MB	U15	1 128-MB DIMM	MEM-SD-NPE-128MB

Input/Output Controller

The I/O controller shares the system memory functions and the environmental monitoring functions for the Cisco 7206 router with the network processing engine. It contains the following components:

- Flash memory for storing the boot helper image
- Two PC Card slots for Flash Disks or Flash memory cards, which contain the default Cisco IOS software image
- Boot ROM for storing sufficient code for booting the Cisco IOS software
- Two environmental sensors for monitoring the cooling air as it enters and leaves the Cisco 7206 chassis

Note Detailed instructions for removing and replacing the I/O controller are contained in the Input/Output Controller Replacement Instructions document. This document accompanies every I/O controller that is shipped from the factory as a FRU and is also available on the Documentation CD-ROM and on Cisco.com (formerly Cisco Connection Online [CCO]).

The I/O controller is available in these versions: C7200-I/O-FE-MII, C7200-I/O-FE=.

- The C7200-I/O-FE-MII and C7200-I/O-FE= I/O controllers consists of the following components:
  -
  - Dual EIA/TIA-232 channels for local console and auxiliary ports. The console port has full DCE functionality and a DB-25 port. The auxiliary port has full DTE functionality and a DB-25 plug.
  - An optional Fast Ethernet port that is configurable for use at 100 megabits per second (Mbps) full-duplex or half-duplex (half-duplex is the default). The Fast Ethernet port is equipped with either an MII port and an RJ-45 port (C7200-I/O-FE=) (see Figure 1-9), or a single MII port (C7200-I/O-FE-MII=) (see Figure 1-11). Although still supported by Cisco Systems, the I/O controller equipped with the single MII port (C7200-I/O-FE-MII=) is no longer an orderable product as of May 1998. The I/O controller without the Fast Ethernet port (C7200-I/O=) is shown in Figure 1-10.

Note The I/O controller with the Product Number C7200-I/O-FE-MII= has a single MII Fast Ethernet port only. The Product Number for the I/O controller with two Fast Ethernet ports, C7200-I/O-FE=, does not specify MII because both an MII and an RJ-45 port are included.

Note When you use the I/O controller that is equipped with an MII port and an RJ-45 port (C7200-I/O-FE=), only one port can be configured for use at a time.

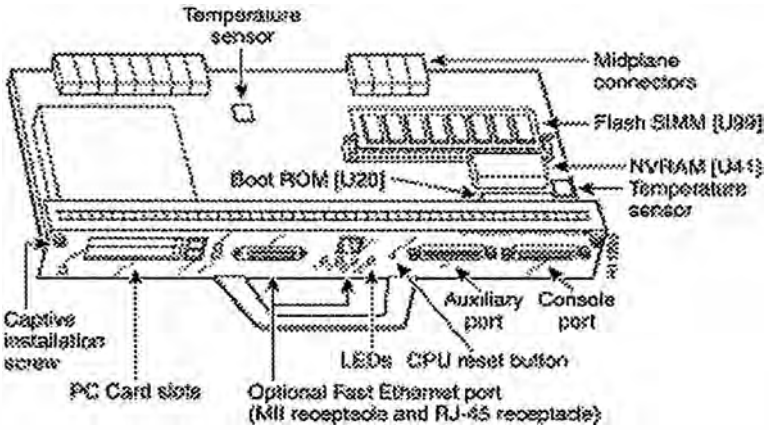
You can install an I/O controller with or without a Fast Ethernet port in all Cisco 7200 series routers (including the Cisco 7206 and Cisco 7206VXR as router shelves in a Cisco AS5800 Universal Access Server).

- Nonvolatile random-access memory (NVRAM) for storing the system configuration and environmental monitoring logs.

Note NVRAM uses lithium batteries to maintain its contents when disconnected from power. Some I/O controllers use an SRAM component with an external lithium battery to provide the same functionality as the NVRAM. (See the second illustration in Figure 1-9 and Figure 1-10.)

Note Your I/O controller with the Fast Ethernet port that has MII and RJ-45 ports (C7200-I/O-FE=) might look like the first illustration in Figure 1-9, or it might look like the second illustration in Figure 1-9. There is no functional difference between these two I/O controllers with the Fast Ethernet port.

Figure 1-9 C7200-I/O-FE=—with MII and RJ-45 Fast Ethernet Ports



Note Your I/O controller without the Fast Ethernet port (C7200-I/O=) might look like the first illustration in Figure 1-10, or it might look like the second illustration in Figure 1-10. There is no functional difference between these two I/O controllers without the Fast Ethernet port.

Figure 1-10 C7200-I/O=—Without Fast Ethernet Port

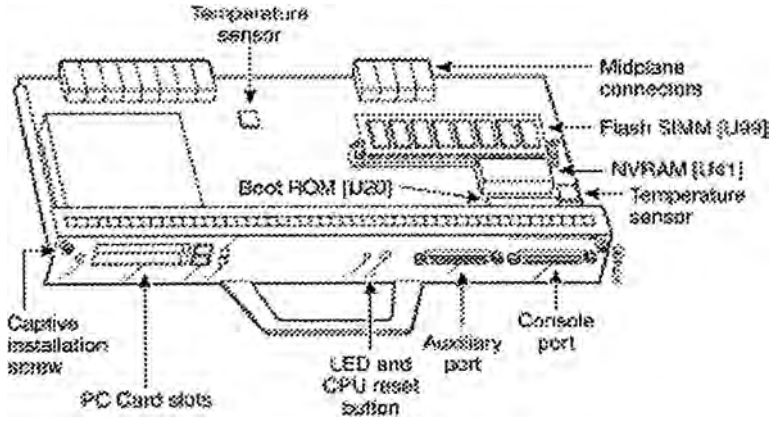


Figure 1-11 C7200-I/O-FE-MII=—with Single MII Fast Ethernet Port

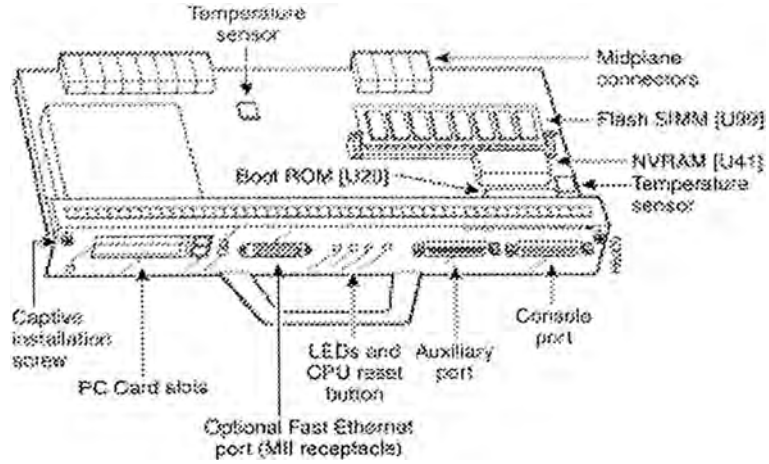


Table 1-6 lists the I/O controller memory components.

Table 1-6 I/O Controller Memory Components

Memory Type	Size	Quantity	Description	Model	Location
Boot ROM	256 KB	1	32-pin DIP-type	C7200-I/O-FE-MII	U20
			32-pin DIP-type or 32-pin PLCC-type	C7200-I/O-FE, C7200-I/O	U20 or U4
Flash memory	4 MB	1	Contains the default boot helper image	C7200-I/O-FE-MII	U99
				C7200-I/O-FE, C7200-I/O	U99 or U10, U11, U12, and U13 (soldered[1])
Flash memory card	20 MB	Up to 2	Contains the default Cisco IOS image	All models	PC Card slot 0 and slot 1
Flash Disk	48 to 128 MB	Up to 2			
NVRAM[2]	128 KB	1	Nonvolatile EPROM for the system configuration file	C7200-I/O-FE-MII	U41
				C7200-I/O-FE, C7200-I/O	U41 or U14 (soldered)[2]

1 Some I/O controllers have no Flash SIMM but use a permanently fixed 4-MB Flash chip instead. (See Figure 1-9.)

2 The NVRAM on some I/O controllers is replaced by a 32-pin nonsocketed SRAM component that is soldered onto the card. The SRAM component is made to act like the NVRAM by the addition of some external components, one of which is a 1-inch (2.54-cm) button-type lithium battery.

LED Descriptions

Figure 1-12 shows the LEDs on the I/O controller with the Fast Ethernet port that is equipped with an MII port and an RJ-45 port. Figure 1-13 shows the LEDs on the I/O controller without the Fast Ethernet port. Figure 1-14 shows the LEDs on the I/O controller with the Fast Ethernet port that is equipped with a single MII port.

Table 1-7 lists I/O controller LEDs and their functions. To use the LEDs for troubleshooting the I/O controller, refer to "Troubleshooting the Installation," the "Troubleshooting the I/O Controller" section.

A CPU reset button is located next to the IO power OK LED or the auxiliary port on the I/O controller faceplate. The CPU reset button resets the entire system.

Caution To prevent system errors and problems, use the CPU reset button only at the direction of your service representative.

Figure 1-12 C7200-I/O-FE=—LEDs and CPU Reset Button—with Fast Ethernet Port (MII and RJ-45 Ports)

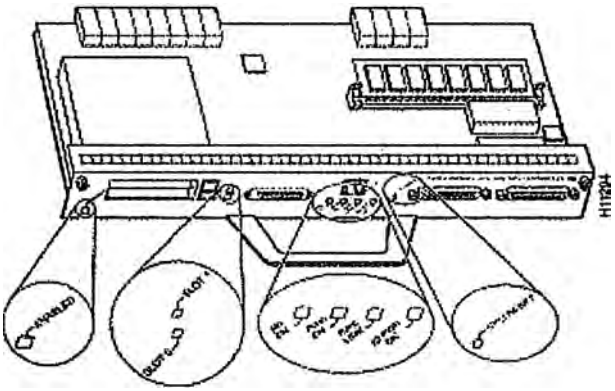


Figure 1-13 C7200-I/O=—LEDs and CPU Reset Button—without Fast Ethernet Port

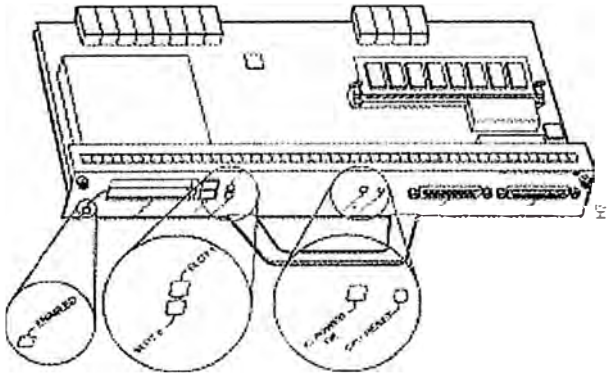
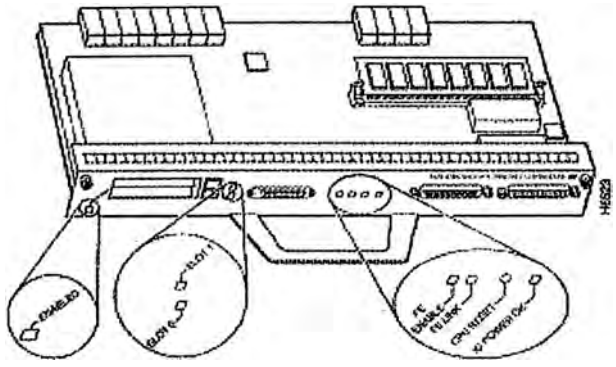


Figure 1-14 C7200-I/O-FE=—LEDs and CPU Reset Button—with Fast Ethernet Port (Single MII Port)



LEDs are either on or off. The LED state (on or off), not the color, determines the status of connection as described in Table 1-7. However, most LEDs are green when on, with the exception of the IO POWER OK LED, which is orange when in the on state.

Table 1-7 I/O Controller LEDs

LED	Color	Function
ENABLED	Green	Indicates that the network processing engine and the I/O controller are enabled for operation by the system; however, it does not mean that the Fast Ethernet port on the I/O controller is functional or enabled. This LED comes on during a successful router boot and remains on during normal operation of the router.
IO POWER OK	Orange	Indicates that the I/O controller is on and receiving DC power from the router midplane. This LED comes on during a successful router boot and remains on during normal operation of the router.
FE ENABLE	Green	Indicates that the Fast Ethernet port is initialized and enabled for operation by the system. This LED comes on after the I/O controller has been enabled and remains on during normal operation of the router.
FE LINK [1]	Green	Indicates that the Fast Ethernet port has established a valid link with the network. This LED remains off during normal operation of the router, unless there is an incoming carrier signal.
MII EN	Green	Indicates that the Fast Ethernet MII port is initialized and enabled by the system, and is configured for operation. This LED comes on after the I/O controller has been enabled and the MII port has been configured as the media type for the Fast Ethernet port (the RJ-45 port is the default media type for the Fast Ethernet port). This LED remains on during normal operation of the router.
RJ45 EN	Green	Indicates that the Fast Ethernet RJ-45 port (the default media type for the Fast Ethernet port) is initialized and enabled by the system. This LED comes on after the I/O controller has been enabled and remains on during normal operation of the router.
RJ45 LINK	Green	Indicates that the Ethernet or Fast Ethernet RJ-45 port has established a valid link with the network. This LED remains off during normal operation of the router, unless there is an incoming carrier signal.
SLOT 0 SLOT 1	Green	Goes on to indicate which PC Card slot is in use by coming on when either slot is being accessed by the system. These LEDs remain off during normal operation of the router.

1 The FE LINK LED is only found on the I/O controller with the single MII port.

ANEXO G. PRESUPUESTO DE IMPLEMENTACION DE LA RED CORPORATIVA CON EQUIPOS CISCO.

I EQUIPOS EDIFICIO CORPORATIVO

SOTANO

CATALYST 6506

Item	Product	Description	Quantity	Price List	Total
	WS-C6506	Catalyst 6506 Chassis			
	WS-CAC-1300W	Catalyst 6000 1300W AC Power Supply			
	CAB-7513AC	AC POWER CORD NORTH AMERICA			
	SC6K-SUPCV-5 4 2	Cat6K Supervisor Flash Image w/CiscoView, Release 5 4(2)			
1	WS-X6K-SUP1A-MSFC	Catalyst 6000 Supervisor Engine1-A, 2GE, plus MSFC & PFC	1	29.995,00	29995
2	SC6MSFCC-12101E	Catalyst 6000 MSFC IOS IP	1	0	0
	WS-X6348-RJ-45	Catalyst 6000 48-port 10/100, Upgradable to Voice, Enh QoS			
	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)			
3	WS-G5486	1000BASE-LX/LH 'long haul' GBIC (singlemode or multimode)	1	1500	1500
				SUB-TOTAL	31495

ROUTERS 2611 PARA ACCESO DIAL

Item	Product	Description	Quantity	Price List	Total
1	CISCO2611	Dual Ethernet Modular Router w/ Cisco IOS IP Software	2	2.495,00	4990
2	CAB-AC	Power Cord, 110V	2	0,00	0
3	S26CP-12103T	Cisco 2600 Series IOS IP PLUS	2	700,00	1400
4	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series	2	1000	2000
5	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series	2	700,00	1400
6	NM-16AM	16 Port Analog Modem Network Module	2	4400	8800
				SUB-TOTAL	18590

CISCO 7206VXR

Item	Product	Description	Quantity	Price List	Total
1	CISCO7206VXR	Cisco 7206VXR, 6-slot chassis, 1 AC Supply w/IP Software	1		0
2	PWR-7200	Cisco 7200 AC Power Supply Option	1		0
3	CAB-ACE	Power Cord Europe	1		0
4	E-72VXR	S72A - ENTERPRISE	1		0
5	S72A-12 0.7XE	Cisco 7200 Series IOS ENTERPRISE	1		0
6	FR-CES72	CES software license for ATM CES PA*	1		0
7	C7200-I/O-FE	Cisco 7200 Input/Output Controller with Fast Ethernet Port	1		0
8	MEM-I/O-FLC20M	Cisco 7200 I/O PCMCIA Flash Memory, 20 MB Option	1		0
9	NPE-300	7200VXR NPE-300 w/ 32MB base mem + 32 MB extra mem	1		0
10	MEM-SD-NPE-64MB	64MB Memory for NPE-300/NPE-225/NPE-175 in 7200 Series	1		0
11	PA-A2-4E1XC-OC3SM	CES OC3 Port Adapter 4E1 Ports 120ohms	1		0
				SUB-TOTAL	0

PISO 1(120)

CATALYST 3524

Item	Product	Description	Quantity	Price List	Total
1	WS-C3524-XL-EN	Catalyst 3524 XL Enterprise Edition	1	2.995,00	2995
2	CAB-AC	Power Cord,110V	1	0	0
3	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
4	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
				SUB-TOTAL	3745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	2	250,00	500
3	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5495

PISO 2 (140)

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
4	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	2	250,00	500
3	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5495

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

PISO 3 (75)

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

CATALYST 3524 (NOC)

Item	Product	Description	Quantity	Price List	Total
1	WS-C3524-XL-EN	Catalyst 3524 XL Enterprise Edition	1	2.995,00	2995
2	CAB-AC	Power Cord,110V	1	0	0
3	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	2	500,00	1000
				SUB-TOTAL	3995

PISO 4 (150)

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
4	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	2	250,00	500
3	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5495

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

PISO 5 (140)

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
4	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	2	250,00	500
3	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5495

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

PISO 6 (60)

CATALYST 3524

Item	Product	Description	Quantity	Price List	Total
1	WS-C3524-XL-EN	Catalyst 3524 XL Enterprise Edition	1	2.995,00	2995
2	CAB-AC	Power Cord,110V	1	0	0
3	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
4	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
				SUB-TOTAL	3745

CATALYST 3548

Item	Product	Description	Quantity	Price List	Total
1	WS-C3548-XL-EN	Catalyst 3548 XL Enterprise Edition	1	4.995,00	4995
2	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	1	500,00	500
3	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1	250,00	250
4	CAB-AC	Power Cord,110V	1	0	0
				SUB-TOTAL	5745

III EQUIPOS PARA TRASLADO DE SERVIDORES

CISCO 6506

Item	Product	Description	Quantity	Price List	Total
1	WS-C6506	Catalyst 6506 Chassis	1	0	0
2	WS-CAC-1300W	Catalyst 6000 1300W AC Power Supply	1	0	0
3	WS-CAC-1300W/2	Catalyst 6000 Second 1300W AC Power Supply	1	0	0
4	CAB-7513AC	AC POWER CORD NORTH AMERICA	2	0	0
5	SC6K-SUP-6.1.1	Catalyst 6000 Supervisor 1 Flash Image, Release 6.1.1	1	0	0
6	WS-X6K-SUP1A-2GE	Catalyst 6000 Supervisor Engine1A, Enhanced QoS, 2GE	1	0	0
7	MEM-C6K-FLC24M	Catalyst 6000 Supervisor PCMCIA Flash Mem Card, 24MB Option	1	0	0
8	WS-X6408-GBIC	Catalyst 6000 8-port Gigabit Ethernet Module (Req. GBICs)	1	9995	9995
9	WS-X6248-RJ-45	Catalyst 6000 48-port 10/100 RJ-45 Module	1	12995	12995
10	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	8	500	4000
11	WS-G5486	1000BASE-LX/LH 'long haul' GBIC (singlemode or multimode)	1	1500	1500
12	WS-G5487	1000Base-ZX extended reach GBIC(singlemode)	0	7495	0
				SUB-TOTAL	28.490

IV OTROS - COSTOS ADICIONALES

ACCESORIOS ADICIONALES

Item	Product	Description	Quantity	Price List	Total
1	Rack	Rack de Piso de 19"	1		
2	Escalerilla	Estalerilla Metálica / metro	10	25,00	250
3	Jumper F.O.	Jumpers de Fibra Optica	25	120,00	3000
				SUB-TOTAL EN LIMA	3.250,00

V REDUNDANCIA

RED DE DATOS Y TELEFONIA

CISCO 7206VXR

Item	Product	Description	Quantity	Price List	Total
1	CISCO7206VXR	Cisco 7206VXR, 6-slot chassis, 1 AC Supply w/IP Software	1		0
2	PWR-7200	Cisco 7200 AC Power Supply Option	1		0
3	CAB-ACE	Power Cord Europe	1		0
4	E-72VXR	S72A - ENTERPRISE	1		0
5	S72A-12.0.7XE	Cisco 7200 Series IOS ENTERPRISE	1		0
6	FR-CES72	CES software license for ATM CES PA*	1		0
7	C7200-I/O-FE	Cisco 7200 Input/Output Controller with Fast Ethernet Port	1		0
8	MEM-I/O-FLC20M	Cisco 7200 I/O PCMCIA Flash Memory, 20 MB Option	1		0
9	NPE-300	7200VXR NPE-300 w/ 32MB base mem + 32 MB extra mem	1		0
10	MEM-SD-NPE-64MB	64MB Memory for NPE-300/NPE-225/NPE-175 in 7200 Series	1		0
11	PA-A2-4E1XC-OC3SM	CES OC3 Port Adapter 4E1 Ports 120ohms	1		0
				SUB-TOTAL	0

CATALYST 8540

Item	Product	Description	Quantity	Price List	Total
1	C8540MSR-SKIT-DC	C8540 MSR Starter Kit w/ Stratum 4 Clock Module - DC Power	1	40000	40000
2	C8540-PWR-DC/2	C8540 Redundant Power Supply - DC	1	8500	8500
3	C8546MSR-MSP-FCL/2	C8540 Redundant MSR Switch Processor with ATM FC	1	20000	20000
4	S854R2-12.0.7W	Catalyst 8540 Integrated ATM and Layer 3 feature set	1	2500	2500
5	C85FE-16T-16K	C8540 16-port 10/100 RJ-45 16K	1	9995	9995
6	C85GE-8X-64K	C8540 8 port GE Module 64K	1	12995	12995
7	WS-G5484	1000BASE-SX 'Short Wavelength' GBIC (Multimode only)	7	500	3500
8	WS-G5487	1000Base-ZX extended reach GBIC(singlemode)	1	7495	7495
9	C85MS-SCAM-2P	C8540 SuperCAM for Port Adapter Modules (PAMs)	3	1500	4500
10	WAI-E1C-4RJ48	4 Port E1 (circuit emulation) RJ-48 PAM	5	4950	24750
11	WAI-OC3-4SS	4 Port OC-3c/STM-1 SMF-IR PAM	1	11500	11500
				SUB-TOTAL	145735

GLOSARIO

AP-access point

ANSI – American National Standard Institute

ATM – Asyncrhonous Transfer Mode

ARP – Address Resolution Protocol

BPDU – bridge Protocol Data Unit

BPSK - Binary Phase Shift Keying

BSS - Basic Service Set

CCITT – Consultative Committee for International Telegraph and Telephone

CDP – Cisco discovery protocol

CLI – Command Line interface

COFDM or OFDM (coded orthogonal frequency division multiplexing)

CRC - cyclic redundancy check

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

CTS - Clear to Send

DCE – Data Communications equipment

DCF - Distribution Coordination Function

DNS – Domain name System

DHCP - Dynamic Host Configuration Protocol

DS - Dstribution system

EIGRP – Enhanced

EIA– Electronics Industries Association

EIA/TIA-568 – Estándar que describe las características para cableado UTP

ESS - Extended Service Set

ETSI – European Telecommunication Standard Institute

FCC - Federal Communications Commission (USA)

GB – Gigabyte Aproximadamente 1000,000,000 bytes

GBps – Gigabytes por segundo

Gbps – Gigabit por segundo

FHSS - Frequency Hopping Spread Spectrum

HSRP – Hot Standby Router protocol

IANA – Internet Assigned Numbres Authoriy

IBSS - Independent Basic Service Set

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IP - Internet Protocol

IDF – Intermediate Distributiion Frame

IGMP – Internet Group Management Protocol

INTERFACE – Conexión entre dos sistemas o dispositivos

IPSec - Internet Protocol security

IP Address – Dirección de 32 bits asignados a Hosts usando TCP/IP

ISL – Inter-Switch Link

ISM - Industry, Scientific, and Medical

ISO - International Organization for Standardization

ISP – Internet Service Provider

LLC - Logical Link Control

MAC - Media Access Control

MDF -. Main Distributiojn Frame

MIB - management information base

MTU – Maximum Transmission Unit

NAT – Network Address Translation

NIC - network interface card

NOS - network operating system

OSI – Open System Interconnection

PCF - Point Coordination Function

PCI - Peripheral Component Interconnect

PING – Packet InterNet Groper

PROTOCOL – Descripción formal de un conjunto de reglas y convenciones.

PSTN – Public Switch Telephone Network

QPSK - Quadrature Phase Shift Keying

RC4 - Ron's Code or Rivest's Cipher

RFC – Reqest for Coments

RTP – Routing Table Protocol

RTS - Request to Send

SNMP - Simple Network Management Protocol

STP – Spanning Tree protocol

SWITCHED LAN – LAN implementado con LAN switches

TELNET – Protocolo estándard de TCP/IP para servicio de terminal remota

TRUNK – Conexión lógica y física entre dos switches.

TCP/IP - Transmission Control Protocol/Internet Protocol

TIA – Telecomunications Industry Association

UTP – Unshielded Twisted Pair

VLSM – Variable Length Subnet Mask

VLAN – Virtual LAN internetwork

WECA - Wireless Ethernet Compatibility Alliance

WEP - Wired Equivalent Privacy

WLAN - wireless local area network

WLANA - Wireless LAN Alliance

WWW – World Wide Web

BIBLIOGRAFIA

1. CISCO SYSTEM INC.

   2000 Cisco Internetwork Design. Student Guide. Revision 3.0. USA

   En: Introduction to Internetwork Design; Campus LAN Design; TCP/IP Network Design. 1 v.

2. LAMMLE, Todd y PORTER, Donald.

   1999 Cisco Certified Network Associate. Student Guide. USA; Cisco Press.

3. CHAPPELL, Laura

   1999 Introduction to Cisco Router Configuration. USA; Macmillan Technical Publishing.

4. CLARK, Kennedy y HAMILTON, Kevin

   1999 Cisco LAN Switching. USA; Cisco Press.

5. INSTITUTO PERUANO DE INFORMATICA Y TECNOLOGIA – TELEMATIC

   2000 Interconnecting Cisco Network Devices. Lima: Telematic

6. INSTITUTO PERUANO DE INFORMATICA Y TECNOLOGIA – TELEMATIC

   2000 Building Scalable Cisco Networks. Lima: Telematic

7. UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

2000 Introduction to Local Area Networks. Conceptos sobre TCP/IP. Lima: UPC.

8. BELDEN ELECTRONICS DIVISION AND PANDUIT NETWORK CONNECTIVITY GROUP.

2001 Structured Cabling Solutions – Integrity; The New Standard for Interconnectivity; Panduit Comunication Products; Category 6 Solution. USA.

9. JOHNSTON, Mark

2000 Physical Layer Test, pp . 16 - 40

En: Field Testing of High Performance Premise Cabling, USA

10. DATA – COM

2002 Specifier Tools, Revision 1.1. Lima.: Data - Com

11. COMMUNICATION PRODUCTS

2002 Interactive Digital Catalog USA.: Communication Products

12. CISCO CISTEM INC.

2003a *http://www.cisco.com/en/US/partner/products/hw/switches/*

2003b *http://www.cisco.com/en/US/partner/products/hw/switches/ps637/products_installation_guide_chapter09186a00801ab94d.html*

2003c *http://www.cisco.com/warp/customer/cc/pd/si/casi/ca3500xl/prodlit/c3524_ds.htm*

2003d http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_data_sheet09186a008014c49f.html

2003d http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_white_paper09186a0080092397.shtml

2003e http://www.cisco.com/en/US/partner/tech/tk389/tk390/technologies_configuration_example09186a008009441a.shtml

13. PANDUIT NETWORK CONNECTIVITY

2003 http://bwccat.belden.com/ecat/jsp/Index.jsp?&P1=null&P2=null&P3=*null&P4=null&P5=null&P6=null*

2003 *www.panduit .com*

14 CISCO SYSTEM INC..

2000 Compilación de diapositivas de Introduction to Cisco Routing Coinfiguration (ICRC. Lima: Cisco

15. CISCO SYSTEM INC..

2000 Compilación de diapositivas de Estándares del Cableado Estructurado. Lima: Cisco