

**TÉCNICAS DE MEJORAMIENTO DE ANCHO DE BANDA Y OPERACIÓN
CONTINUA EN REDES DE AREA LOCAL**

JAVIER CAMPILLO JIMENEZ
EDGAR CASTILLA CHAVARRIAGA

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y
MECATRÓNICA

CARTAGENA DE INDIAS

2003

**TÉCNICAS DE MEJORAMIENTO DE ANCHO DE BANDA Y OPERACIÓN
CONTINUA EN REDES DE AREA LOCAL**

JAVIER CAMPILLO JIMENEZ
EDGAR CASTILLA CHAVARRIAGA

Monografía presentada como requisito para optar al título de Ingeniero Electrónico

Director:

JESÚS CAMPILLO MARIN

Ingeniero Electrónico y Telecomunicaciones

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
DEPARTAMENTO DE INGENIARÍA ELÉCTRICA, ELECTRÓNICA Y
MECATRÓNICA

CARTAGENA DE INDIAS

2003

Cartagena de Indias D.T y C. Mayo 15 del 2003

Señores:

Comité Evaluador

Departamento de Ingeniería Eléctrica, Electrónica y Mecatrónica

Apreciados señores:

Por medio de la presente me permito informarles que la monografía titulada **“TÉCNICAS DE MEJORAMIENTO DE ANCHO DE BANDA Y OPERACIÓN CONTINUA EN REDES DE AREA LOCAL”** ha sido desarrollado de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

Javier E. Campillo Jiménez.

Edgar V. Castilla Chavarriaga.

Cartagena de Indias D.T y C. Mayo 15 del 2003

Señores:

Comité Evaluador

Departamento de Ingeniería Eléctrica, Electrónica y Mecatrónica

Apreciados señores

Por medio de la presente me permito informarles que la monografía titulada **“TÉCNICAS DE MEJORAMIENTO DE ANCHO DE BANDA Y OPERACIÓN CONTINUA EN REDES DE AREA LOCAL”** ha sido desarrollado de acuerdo a los objetivos establecidos.

Como director del proyecto considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

Ing. Jesús Campillo Marín.

Nota de aceptación

Jurado

Jurado

TABLA DE CONTENIDO

1. INTRODUCCION	10
2. MEJORAMIENTO DE ANCHO DE BANDA	12
2.1. CAPA FISICA	13
2.1.1. SUBSISTEMAS DE CABLEADO HORIZONTAL	15
2.1.1.1. Protección contra Interferencias Electromagnéticas	18
2.1.1.2. Protección contra la Diafonía	19
2.1.1.3. Protección contra la atenuación	19
2.1.1.4. Elaboración de los Patch Cords	20
2.1.1.5. Canalizaciones y Ductos	22
2.1.2. CABLEADO DE BACKBONE O VERTICAL	23
2.1.2.1. Distancias Máximas	25
2.1.2.2. Conductos, Pasos y Espacios para Cableado Vertical	25
2.1.2.3. Prevención de Deformaciones en la Fibra	26
2.1.2.4. Empalmes	29
2.2. CAPA DE ENLACE DE DATOS	30
2.2.1. TARJETA INTERFAZ DE RED	30
2.2.1.1. Funciones de la NIC	31
2.2.1.2. Consideraciones para la selección de una NIC	31
2.2.2. BRIDGES (PUENTES)	34

2.2.3. SWITCHES	37
2.2.3.1. Modo de operación	38
2.2.3.2. Ventajas	40
2.2.3.3. Desventajas	41
2.2.3.4. Segmentación con Switches	41
2.3. BROADCAST. DEFINICION Y CONSIDERACIONES	43
2.3.1. MULTICAST	44
2.3.2. UNICAST	44
2.3.3. VLANs	45
2.3.3.1. Características	46
2.3.3.2. Funcionamiento de VLAN	48
2.3.3.3. Clases de VLANs	49
2.4. SOLUCIÓN DE ANCHODE BANDA EN BACKBONES	51
2.4.1. MIGRACIÓN A OTRAS TECNOLOGÍAS	51
2.4.1.1. Fast Ethernet.	51
2.4.1.2. Gigabit Ethernet.	53
2.4.2. REDES HIBRIDAS. LAN EMULATION Y EMULATED LAN	56
2.4.2.1. ATM	56
2.4.2.2. LANE (LAN Emulation)	59
2.4.3. TRUNKING	62
2.4.4. BALANCEO DE CARGAS. SOLUCIÓN EN SERVIDORES	66
2.5. CONFIGURACIÓN DE SWITCHES	68
2.5.1. IDENTIFICACIÓN DE UN SWITCH	70

2.5.2. SEGURIDAD Y PASSWORDS	71
2.5.3. COMUNICACIÓN ENTRE SWITCHES	71
2.5.4. CONFIGURACIÓN DE PUERTOS	72
2.5.4.1. Descripción de un Puerto Ethernet.	72
2.5.4.2. Velocidad de los Puertos Ethernet	73
2.5.4.3. Configuración del enlace Ethernet.	73
2.5.4.4. Configuración de Puertos Token Ring	74
2.5.5. CONFIGURACIÓN DE VLAN'S	74
3. OPERACIÓN CONTINUA	78
3.1. SELECCIÓN DEL CENTRO DE CABLEADO	80
3.1.1. TAMAÑO	82
3.1.2. MATERIALES PARA PAREDES, PISOS Y TECHOS	83
3.1.3. TEMPERATURA Y HUMEDAD	84
3.1.4. PREVENCIÓN DE INUNDACIONES	85
3.1.5. ILUMINACIÓN Y TOMACORRIENTES	85
3.1.6. SEGURIDAD	86
3.2. CONSIDERACIONES ELÉCTRICAS	86
3.2.1. CONEXIÓN A TIERRA	89
3.2.2. SOLUCIÓN PARA PROBLEMAS DE SOBREVOLTAGES	91
3.2.3. SOLUCIÓN A LOS CORTES Y BAJAS DE TENSIÓN	94
3.2.4. SOLUCIÓN PARA LAS OSCILACIONES	95
3.2.5. PROTECCIÓN CONTRA RAYOS	96

3.3. REDUNDANCIA EN REDES	97
3.3.1. REDUNDANCIA DE EQUIPOS	97
3.3.2. REDUNDANCIA DE ENLACES	98
<u>4. CONCLUSIONES Y RECOMENDACIONES</u>	<u>101</u>
<u>5. GLOSARIO DE TERMINOS</u>	<u>104</u>
<u>BIBLIOGRAFÍA</u>	<u>123</u>

1. INTRODUCCION

Las redes de área local LAN (Local Area Network) se han convertido en un estándar en las empresas, presionando inclusive la interconexión de redes locales y remotas. Por otro lado han surgido nuevas aplicaciones tales como CAD (Computer Aided Design), CAM (Computer Aided Manufacturing) y grandes bases de datos, que junto con las aplicaciones en tiempo real, tales como video y multimedia, constituyen grandes consumidores de recursos de comunicaciones.

Como consecuencia de estos nuevos servicios, la demanda por tecnologías de mayor ancho de banda y velocidades de transmisión más altas ha crecido.

La meta de las telecomunicaciones actualmente es integrar servicios de voz, datos y video en una gran red de alta velocidad. Esta red debe ser capaz de transferir toda clase de información independientemente del ancho de banda requerido y de enviarla a través de la red en forma tan simple como sea posible. Para esto, muchas tecnologías han sido desarrolladas, incluyendo ATM (Asynchronous Transfer Mode), Cableado con fibra óptica, y Gigabit Ethernet.

Por ello estudiaremos las técnicas que permitan el máximo aprovechamiento del medio físico y de los equipos activos de la red, garantizando una velocidad de operación cercana a la teórica brindada por cada tecnología (Throughput).

Un inconveniente que trae consigo la integración de todos los servicios en una sola red, es la operación continua de la misma, ya que una falla provocaría un colapso total de todos los servicios que soporta. En consecuencia se hace necesario e indispensable estudiar técnicas que permitan evitar fallos a como de lugar. Algunas de estas técnicas son la redundancia, balanceo de cargas, mantenimiento preventivo, disponibilidad eléctrica y otros que mencionaremos mas adelante.

A partir de estas premisas filosóficas, se estudiarán las conocidas tecnologías, donde la tecnología Ethernet ha desempeñado un excelente papel gracias a todas sus mejoras. Esta tecnología ha sido un sobreviviente de las velocidades, brindando a sus usuarios velocidades aún mayores, con ligeros cambios en su estructura y a un bajo costo, pasando de 10Mbps a Fast Ethernet 100Mbps, y el gigante de Gigabit Ethernet 1000Mbps. Al mismo tiempo permite la realización de redes híbridas, atravesando de conmutación de paquetes a conmutación de celdas de la tecnología ATM, las conocidas LAN Emulation y Emulated LAN, creando toda una autopista de la información.

2. MEJORAMIENTO DE ANCHO DE BANDA

El ancho de banda esta relacionado con la capacidad máxima de datos que se pueden transmitir desde un punto a otro en una red, para ello las técnicas de mejoramiento de la misma que se describen en la presente monografía han sido clasificadas por grupos, por ejemplo la capa física, donde se estudian las características de los medios de transmisión, así como los métodos adecuados de instalación, problemas del cableado y la escalabilidad de los mismos.

Otro aspecto significativo en el mejoramiento de ancho de banda, es el proceso de transmisión de tramas a alta velocidad. En ello se deben tener presentes las especificaciones precisas a la hora de elegir los elementos de conectividad y de conmutación de la red.

En el entorno de redes LAN, Ethernet ha sido la tecnología que mayor desarrollo ha alcanzado, desafortunadamente posee el inconveniente del dominio de colisiones compartido y el empleo de señales de broadcast. En consecuencia se estudian los mecanismos que permitan la solución de estos problemas y se presenta como la mejor opción el empleo de VLAN's, adicionalmente se describen las ventajas que ofrecen el uso de las mismas.

2.1. CAPA FISICA

A pesar de que existen otros factores que afectan el rendimiento de una red (NIC's, switches, routers, etc) como hablaremos mas adelante, es inútil invertir en tecnologías de capas superiores cuando se esta trabajando sobre una infraestructura pobre de cableado.

A continuación haremos referencia a situaciones que reafirman la importancia del cableado en una red.

- ❑ El 50 % de los problemas en la red son causados por el 4 % de su inversión en Tecnología de Información (TI).
- ❑ Por menos \$ 10 usd al año por nodo puede asegurar una alta productividad.
- ❑ El 40 % del tiempo de los Administradores de red está dedicado a resolver problemas en la red.
- ❑ Cumplir sólo con los estándares asegura un desempeño mínimo en su red.
- ❑ Tener un Sistema Totalmente Integrado de Cableado incrementa el desempeño de su red.

Para resolver los problemas derivados de lo anterior surge el Cableado Estructurado, definido por los estándares ANSI/TIA/EIA-568 que especifica un cableado genérico y permite la transmisión de cualquier servicio de comunicación sobre él en forma independiente a las aplicaciones, estableciendo requisitos de

desempeño, distancias máximas del cableado y configuración de los conectores. Todo bajo una topología física en estrella.

Estos estándares garantizan un alto rendimiento en la instalación del cableado de la red, evitando caer en problemas como la diafonía, la atenuación, la interferencia electromagnética, entre otros expuestos mas adelante.

El desarrollo de las redes ha hecho que hoy los Sistemas de Cableado Estructurado jueguen un papel determinante en el desempeño de las mismas. Al observar algunos elementos que afectan el rendimiento de las redes podemos notar claramente por qué es tan importante hacer la mejor selección del sistema de cableado, el “asfalto de la súper carretera de la información” .

El cableado estructurado divide su instalación en subsistemas, tomando en cuenta las prestaciones del cableado a emplear y la aplicación del mismo, a continuación se hace una descripción de estos subsistemas, tomando en cuenta su topología, tipo de cableado empleado, y condiciones de instalación para garantizar el máximo rendimiento.

2.1.1. SUBSISTEMAS DE CABLEADO HORIZONTAL

El cableado horizontal se extiende desde el área de trabajo hasta el cuarto de telecomunicaciones. Incluye cajas, placas y conectores en el área de los usuarios; cables y conectores de transición instalados entre las salidas de los usuarios y el cuarto de telecomunicaciones, y paneles y cables de empate utilizados para configurar las conexiones del cableado horizontal en dicho cuarto.

El cableado se basa en una topología de estrella, con el fin de tener todos los nodos concentrados en un cuarto principal.

Para el diseño del subsistema de cableado horizontal se pueden emplear el cableado UTP (Unshielded Twisted Pair), Fibra Óptica y STP (Shielded Twisted Pair). Sin embargo solo mencionaremos las prestaciones del primero pues no recomendamos el empleo del cableado STP debido a que ha ido saliendo del mercado, a causa de que es un cableado difícil de maniobrar y requiere de una compleja instalación de puesta a tierra. De igual forma el empleo del cableado STP se ha visto afectado por las ventajas que ofrece la instalación empleando cableado UTP Cat-6 y la reducción en el costo de la fibra óptica durante los últimos años. El cableado de fibra óptica será mencionado mas adelante en el cableado vertical o de backbone porque es en este subsistema donde encuentra su mejor aplicación, a pesar de que puede emplearse en el subsistema horizontal, actualmente sigue siendo una opción muy costosa en el mismo.

El cableado UTP es el soporte físico más empleado en las redes LAN, pues es barato y su instalación es sencilla. Consiste en un conjunto de conductores de cobre (protegidos cada uno por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la diafonía.

Este cableado ha evolucionado en categorías según sus prestaciones, en redes de comunicación de datos se han empleado las categorías 4, 5, 5e y 6, pero actualmente se recomienda iniciar las nuevas instalaciones empleando cableado cat-6 que fue estandarizado en junio de 2002. Las razones que soportan tal afirmación se mencionan a continuación.

- ❑ GigaSPEED
- ❑ Ethernet a 1 Gbps y ATM a 1.2 Gbps y 2.4 Gbps
- ❑ Soporta los 77 canales (550 Mhz) de vídeo analógico de banda ancha
- ❑ Frecuencia de operación hasta 250 Mhz

En caso de tener una red previamente instalada con cat-5e se pueden alcanzar las velocidades que en este momento maneja el cat-6 (1000Mbps @ 100MHz) con el costo de una electrónica compleja en las tarjetas de red, negándole la posibilidad de escalabilidad y presionándolo a una futura migración a cat-6 o fibra óptica.

La selección del cableado a instalar debe escogerse de una compañía que distribuya el cableado certificado de categoría 6. Las especificaciones técnicas que se deben cumplir se muestran a continuación:

ATENUACION	250 MHz (dB)
Cable	19.8
Conector	0.2
Canal	21.3
NEXT	
Cable	44.3
Conector	54.0
Canal	39.9
ELF EXT	
Cable	27.8
Conector	43.1
Canal	23.3
PERDIDA DE RETORNO	
Cable	20.1
Conector	24.0
Canal	12.0

Una vez se selecciona el cableado certificado deben tomar en cuenta ciertas medidas en el momento de la instalación con el fin de mantener al mínimo las condiciones que afectan el rendimiento del ancho de banda del mismo.

2.1.1.1. Protección contra Interferencias Electromagnéticas

A la hora de establecer la ruta del cableado de los centros de comunicaciones a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos:

- ❑ Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
- ❑ Cables de corriente alterna
 - Mínimo 13 cm. para cables con 2KVA o menos
 - Mínimo 30 cm. para cables de 2KVA a 5KVA
 - Mínimo 91cm. para cables con mas de 5KVA
- ❑ Luces fluorescentes y balastos (mínimo 12 centímetros). El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- ❑ Intercomunicadores (mínimo 12 cms.)
- ❑ Equipo de soldadura (Mínimo 2 metros)
- ❑ Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
- ❑ Otras fuentes de interferencia electromagnética y de radio frecuencia.

2.1.1.2. Protección contra la Diafonía

La diafonía es una transferencia indeseada de energía desde un circuito a otro usualmente adyacente; ocurre en el extremo del enlace de transmisión donde la fuente de señal está ubicada; la energía absorbida se propaga hacia el otro extremo del circuito afectado. Es causada por altas frecuencias, señales no balanceadas o insuficiente aislamiento.

Con el fin de evitar esta perturbación, es necesario tomar en cuenta ciertas precauciones a la hora de manipular el cableado.

- El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 7mm para cables UTP categoría 6.
- El radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable. Para par trenzado de cuatro pares categoría 6 el radio mínimo de doblado es de 3 cm.

2.1.1.3. Protección contra la atenuación

La atenuación es la pérdida de potencia que se tiene a lo largo del medio de transmisión, esta es absorbida por el mismo.

Con el fin de no sobrepasar las condiciones de atenuación admisibles por la norma que garanticen al máximo throughput a través del cableado, deben establecerse las siguientes medidas como las máximas permitidas

La distancia horizontal máxima es de 90 metros, esta es la distancia desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones. Al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la distancia combinada de cables de empate (3 metros) y cables utilizados para conectar equipo en el área de trabajo de telecomunicaciones y el centro de cableado.

2.1.1.4. Elaboración de los Patch Cords

Las longitudes cortas de las conexiones modulares al final de los cables que conectan las PC a las salidas de pared e interconectan los switches, los patch cords, pueden causar grandes problemas en el desempeño y en la transmisión de datos para las redes.

Los patch cords son el elemento que introduce la conexión básica al canal. Son inherentemente difíciles de manufacturar con consistencia, difíciles de probar y contribuyen al desempeño degradado en la red, además son los componentes del canal más baratos de reemplazar.

Algunas firmas utilizan cable de mala calidad, mientras que algunos utilizan conectores malos y técnicas de ensamblado defectuosas. Los patch cords inclusive pueden diferir en desempeño de un punto al otro.

Evitar el uso de estos productos de calidad marginal es crucial para obtener el desempeño más alto de su red. Los patch cords de dudosa calidad pueden reducir el índice de transmisión de datos, al reducir el ancho de banda general, y eso sigue siendo cierto sin importar qué tan grandes se supone que son las conexiones de cable.

Al instalar una red nueva, asegúrese de hacer coincidir el tipo de patch cord con el cable horizontal instalado en el canal. El hacerlo resultará en una mejor impedancia, la cual hará coincidir el desempeño en todo el canal. Las reflexiones eléctricas o pérdida de retorno debidos a unos que no coinciden, se minimizan. En otras palabras, cuando usted utiliza patch cords, cables y conectores diseñados por el mismo fabricante, se obtienen mejores resultados.

De una manera similar, verifique que los conectores de terminadores modulares en el patch cord estén diseñados para ser utilizados con el contacto modular con el cual se complementa. Muy a menudo, los fabricantes de conectividad afinan óptimamente sus sistemas para lograr lo mejor con sus propios componentes.

Cuando hay patch cords con conectores RJ-45 o patch panels de diferentes compañías, el desempeño no es tan bueno porque el fabricante de componentes a menudo tiene procedimientos de ensamblado muy precisos para asegurarse que el contacto es terminado consistentemente en el patch cord.

2.1.1.5. Canalizaciones y Ductos

Otro de los factores que puede afectar el rendimiento del cableado horizontal, es la forma en la cual el mismo es canalizado y distribuido hasta los puntos de trabajo, a continuación se mencionan algunas precauciones que se deben tener cuando se realiza esta operación.

- Los cables UTP pueden circular por bandeja compartida con cables de energía respetando el paralelismo a una distancia mínima de 10 cm. En el caso de existir una división metálica puesta a tierra, esta distancia se puede reducir a 7 cm.

- En el caso de pisoductos o caños metálicos, la circulación puede ser en conductos contiguos.

- Si es inevitable cruzar un gabinete de distribución con energía, no debe circularse paralelamente a más de un lateral.

- De usarse cañerías plásticas, debe lubricar los cables (talco industrial, vaselina, etc) para reducir la fricción entre los cables y las paredes de los caños ya que esta genera un incremento de la temperatura que aumenta la adherencia.

- El radio de las curvas no debe ser inferior a 2".

- Las canalizaciones no deben superar los 20 metros o tener más de 2 cambios de dirección sin cajas de paso .

- Al utilizar fijaciones (grapas, cordones o zunchos) no debe excederse en la presión aplicada (no arrugar la cubierta), pues puede afectar a los conductores internos.

2.1.2. CABLEADO DE BACKBONE O VERTICAL

Es un elemento básico del cableado estructurado. Su función es proporcionar interconexiones entre cuartos de entrada a servicios de edificio, cuartos de equipo y de telecomunicaciones. El cableado de backbone incluye la conexión vertical entre edificios de varios pisos.

Los requerimientos de diseño que se deben tener en cuenta para el cableado horizontal son los siguientes:

- ❑ Topología en Estrella
- ❑ No mas de 2 niveles jerárquicos de conexiones
- ❑ No se permiten derivaciones en puente
- ❑ No estar en cercanías de fuentes de interferencia electromagnética (Para el cable UTP).

La norma especifica que el cableado de backbone puede ser en UTP o en fibra óptica, sin embargo con el propósito de garantizar el cumplimiento de los requerimientos de ancho de banda que requiera la red en los próximos años es altamente recomendado el empleo de fibra óptica monomodo.

La Fibra óptica es un medio muy flexible y fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por varias fibras muy finas de cristal o plástico, cada fibra está rodeada de su propio revestimiento con diferentes propiedades ópticas distintas a las del núcleo. Posteriormente, está la cubierta que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etcétera.

Algunos de sus beneficios en relación con los pares trenzados (UTP) son el mayor ancho de banda, menor peso y tamaño, menor atenuación, aislamiento electromagnético y mayor separación entre repetidores, entre otros.

Con el fin de garantizar la correcta operación de la instalación del cableado de fibra óptica de backbone se deben tomar en cuenta ciertas consideraciones que serán mencionadas a continuación:

2.1.2.1. Distancias Máximas

- ❑ Dentro del Edificio se puede realizar un tendido de fibra óptica hasta 500 mts.
- ❑ Entre Edificios se permiten distancias hasta 2Km en Fibra Óptica Multimodo y hasta 3Km en Fibra Óptica Monomodo.

2.1.2.2. Conductos, Pasos y Espacios para Cableado Vertical

- ❑ Utilización de tuberías de 4" de metal rígido para exteriores, galvanizadas para interiores.

- Debe instalarse una tubería mínimo desde el cuarto de equipos hasta cada cuarto de telecomunicaciones.
- Las bocas de las tuberías deben tener anillos de protección para los cables.
- Las aberturas alrededor de las tuberías deben estar selladas con concreto o barreras contra fuego.

2.1.2.3. Prevención de Deformaciones en la Fibra

Es necesario disponer de cubiertas y protecciones de calidad capaces de proteger la fibra. Para alcanzar tal objetivo hay que tener en cuenta su sensibilidad a la macrocurvatura y microcurvatura, la resistencia mecánica y las características de envejecimiento.

Las fuerzas laterales localizadas a lo largo de la fibra dan origen a lo que se conoce como microcurvaturas. El fenómeno puede ser provocado por esfuerzos durante la manufactura e instalación y también por variaciones dimensionales de los materiales del cable debidos a cambios de temperatura. La sensibilidad a la microcurvatura es función de la diferencia del índice de refracción, así como de los diámetros del núcleo y del revestimiento. Es evidente que la microcurvaturas incrementan las pérdidas ópticas.



Figura 1. Microcurvaturas, la desviación es inferior a un par de micrones

Las pérdidas por microcurvaturas afectan el cableado de fibra multimodo independientemente de la longitud de onda de la señal, a diferencia de la fibra monomodo en la cual si se depende de este factor para determinar las pérdidas.

Los esfuerzos que provoca la torcedura de las fibras son básicamente una fuerza transversal y un esfuerzo longitudinal. El esfuerzo longitudinal no provoca torcedura cuando trabaja para alargar la fibra, no hay cambio en las pérdidas ópticas. Sin embargo, cuando trabaja para contraer la fibra, este esfuerzo provoca que la fibra forme bucles y se curve, de tal manera que la pérdida óptica se incrementa. Por lo tanto, al evaluar los diseños de los cables se debe poner especial atención en:

- La carga transversal que trabaja en la fibra durante el cableado, instalación y utilización.
- El esfuerzo de contracción que ocurre a bajas temperaturas debido al encogimiento de los elementos del cable.

Además el eje de la fibra puede curvarse severamente (macrocurvaturas) causando grandes incrementos en las pérdidas ópticas. Para prevenir esta situación se tienen en cuenta las siguientes consideraciones:

- Mantener un radio de curvatura determinado, seleccionando el radio y la longitud del cableado, no se debe realizar un curvado de radio inferior a 7 veces el diámetro interno de la fibra.
- Reducir variaciones técnicas de las fibras protegidas con pequeños coeficientes de expansión térmica disponiéndolas alrededor de un elemento con buenas propiedades térmicas.

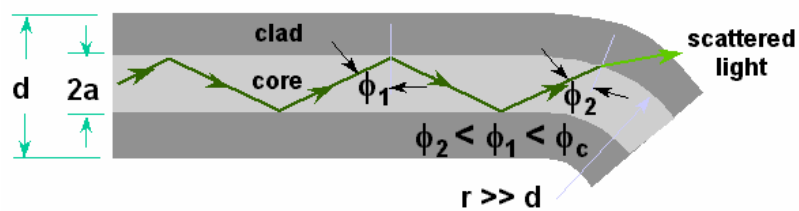


Figura 2. Macrocurvaturas

En las macrocurvaturas, las pérdidas dependen de la longitud de onda empleada en la señal.

2.1.2.4. Empalmes

Cuando se realizan enlaces con Fibra óptica, es necesario empalmar segmentos de la misma, estos empalmes pueden ser de tipo mecánico, o de fusión. El más común debido a su bajo costo es el empalme mecánico pero ofrece la desventaja de producir 10 veces más pérdidas que los empalmes de fusión. Esto puede ocasionar problemas en enlaces de F.O. muy extensos, sin embargo, si tomamos en cuenta que estamos realizando enlaces en redes de área local, esto no representa un problema.

El manejo de la F.O. en redes LAN es igual al manejo que se hace con el cableado UTP, se hacen conectores en los extremos de la fibra y en el patch panel de fibra, la conexión entre los mismos se hace a través de patch cords de fibra.

Las pérdidas típicas en empalmes mecánicos son de aproximadamente 2dB, no obstante, hacer un empalme eficiente requiere del empleo de técnicas que aunque sencillas son muy importantes.

- Deben emplearse conectores certificados que garanticen la eficiencia del empalme.
- En los patch panels de fibra se deben dejar fibra suficiente para permitir hacer al menos 8 bucles dentro del patch panel.

- Se recomienda el empleo de un pulidor automatizado para la finalización del empalme, el cual, además de reducir el tiempo de pulido de la fibra en un 66%, la pérdida de inserción disminuye a 0.2dB o menos.
- Al finalizar cada empalme se debe verificar la condición del extremo de la fibra con un microscopio para fibra.
- En el patch panel se debe colocar un anillo protector giratorio que facilite la distribución y minimice la tensión de curvatura cuando se utilizan bandejas deslizantes.

2.2. CAPA DE ENLACE DE DATOS

Para justificar la inversión y las precauciones tomadas en la instalación del cableado estructurado, conviene realizar una eficiente selección de los equipos que se conectan al cableado, los equipos de la capa de enlace de datos. La función de esta capa es la controlar el acceso al medio, de allí la importancia que cobran en el rendimiento del ancho de banda general de la red.

2.2.1. TARJETA INTERFAZ DE RED

Una tarjeta de red es una interfase que proporciona la electrónica necesaria al computador para que se comunique con otros dispositivos. Existen varios tipos de

tarjetas de red, en función de la topología de la LAN. Pueden ser Ethernet, Token Ring, FDDI, etc.

2.2.1.1. Funciones de la NIC

Algunas de las funciones de las tarjetas de red o NIC son las siguientes:

- *Control de enlace lógico*: Se comunica con las capas superiores del computador
- *Denominación*: Proporciona un identificador exclusivo.
- *Entramado*: Parte del proceso de encapsulamiento, empaqueta los bits para transportarlos
- *Control de acceso al medio (MAC)*: Proporciona un acceso estructurado a los medios de acceso compartido.
- *Señalización*: Crea señales y realiza interfaz con los medios usando transceivers incorporados.

2.2.1.2. Consideraciones para la selección de una NIC

Al elegir una tarjeta de red, se deben tener presente los siguientes factores:

1. El tipo de red, es decir, si es Ethernet, Token Ring, FDDI, entre otras.

2. El tipo de medio, por ejemplo si es par trenzado, cable coaxial, Fibra óptica, etc.
3. El tipo de Bus del sistema, si es PCI, ISA, etc.
4. Características de trabajo, velocidad, Gestión automática de Interrupción, Agente SNMP.

El indicativo tres es muy importante, este evita incurrir en gastos innecesarios al seleccionar una tarjeta con la que no se va a obtener el mejor rendimiento, porque se verá limitada por la velocidad del bus de datos del sistema, de los procesadores, entre otras. Con el propósito de ilustrar este fenómeno, imagine un PC con un procesador Pentium @ 66MHz y una tarjeta de red de 100Mbps Full Duplex conectada en uno de sus puertos ISA, ¿Como sería posible que este fuese capaz de transmitir datos a una velocidad superior a su velocidad de procesamiento? La respuesta es sencilla, no es posible, simplemente transmite a la máxima velocidad permitida por el procesador y el bus de datos, desaprovechando así las capacidades de la NIC.

A continuación se muestra una tabla que realiza una comparación entre los anchos de banda teóricos y reales de los buses de datos mas empleados en la conexión de NIC's.

	ISA	PCMCIA	EISA	MCA	PCI
Ancho de banda del Bus (teórico)	66Mbps	66Mbps	264Mbps	320Mbps	1056Mbps
Ancho de banda del Bus (Real)	10-20Mbps	10-20Mbps	64Mbps	80Mbps	264Mbps

Tabla 1. Velocidad del Bus de datos del sistema.

Como se puede observar en la tabla 1, no se puede implementar la tecnología Fast Ethernet en todas las arquitecturas de nodos, para la arquitectura ISA es más rentable tener tarjetas de 10Mbps.

Una opción interesante para soluciones en estaciones de trabajo que demanden alto ancho de banda (Multimedia) y servidores, es el uso de tarjetas escalables en velocidades. En el mercado encontramos tarjetas escalables de 10 a 1000Mbps, sobre infraestructura de cable de cobre UTP Cat. 5e y 6. El medio es de gran ayuda para la electrónica de componentes en las tarjetas, si el cable tiene mejoras se pueden evitar componentes adicionales (Chips DSP) que resultan costosos, encareciendo el precio de la tarjeta.

Una de las características importantes en las tarjetas es el hecho que sea Full duplex, aumentando de esta forma el ancho de banda, al mismo tiempo que sea auto negociable en las velocidades y tenga gestión de interrupción inteligente en

caso de que se este utilizando tráfico troncalizado (Ej. En servidores), además que posea soporte para VLAN's y encolamiento de prioridades de nivel 2.

Además existen tarjetas con protección Firewall, con gestion SNMP, con conectores para fibra, diagnóstico de fallas, entre otras categorías.

Ahorrarse unos pesos en la tarjeta de red pueden resultar en Miles en corto plazo, si se desea justificar la inversión, se debe escoger una buena NIC.

Sin embargo, se debe tener en cuenta cual va ser su funcionalidad, no se debe olvidar que, tener una tarjeta rápida no implica de que la red lo sea, la velocidad depende de otros factores como la arquitectura interna del bus de datos en un nodo, si es de entorno compartido o conmutado, de las tramas a transmitir, de los buffers de almacenamiento y de la negociación en los switches para las velocidades.

2.2.2. BRIDGES (PUENTES)

Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando tráfico de las interconexiones.

El puente escucha la red y además aprende la ubicación de cada uno de los terminales. Este dispositivo genera una tabla con direcciones MAC.

Si ve que alguien quiere enviar algo a otro participante del mismo segmento, hace que rebote la señal. Si es de otro segmento emite la señal y lo conecta con el otro participante, o repite la señal hasta que establezca la conexión correctamente.

También se usa para unir varios segmentos del mismo tipo (Ethernet por ejemplo) con el fin de obtener mayor privacidad, o de cualquier otra tecnología como Token Ring. El tráfico local de cada segmento no será enviado a otros, sólo se envían los que tengan dirección destino en otro segmento.



Figura 3. Bridge

Los puentes son dispositivos de intercomunicación que se pueden usar para reducir los dominios de colisión de gran tamaño. Logran esto dividiendo la red en segmentos más pequeños y reduciendo la cantidad de tráfico que debe pasar entre los segmentos. Los puentes trabajan mejor cuando no hay demasiado tráfico entre un segmento de la red y los demás segmentos.

Cuando el tráfico entre los segmentos de red aumenta, se puede producir un cuello de botella en el puente y la comunicación puede tornarse más lenta. Existe

otro problema cuando se usa un puente, éstos difunden el broadcast, estos paquetes de datos aparecen cuando un dispositivo de la red desea comunicarse con otro dispositivo, pero no conoce la dirección destino del mismo. Cuando esto ocurre, con frecuencia el origen envía una señal de *broadcast* a todos los dispositivos de la red.

Mediante un sencillo ejemplo, se explicará el principio de funcionamiento de los puentes y las ventajas que le ofrecen a la red.

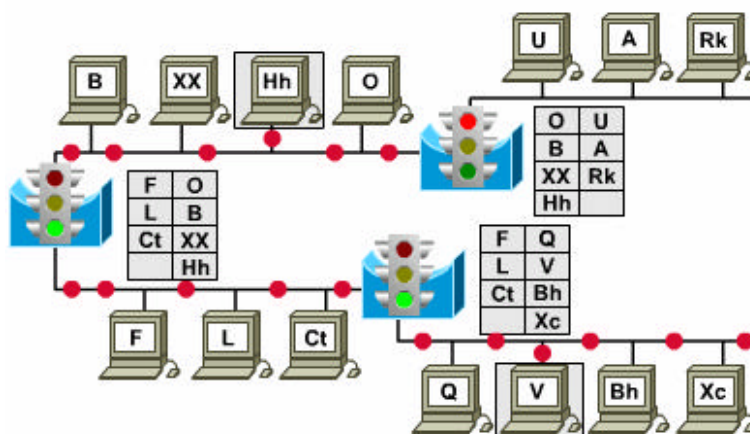


Figura 4. Funcionamiento

1. Se origina un paquete de datos desde el computador V con destino el PC Hh.
2. El paquete viaja por todos los nodos del segmento origen del computador V.

3. El puente verifica la tabla de direcciones MAC para determinar si el paquete debe viajar a los demás segmentos de la red. El mismo proceso se ve en los demás puentes.
4. El paquete de datos llega a su destino final.

El puente está saliendo del mercado LAN, ya que ha sido reemplazado por el switch, que detallaremos más adelante en este estudio, no tiene caso realizar diseños con Puentes ya que el switch realiza las mismas funciones del Bridge y muchas más labores de gestión, además los tiempos de latencia en un switch oscilan entre 70 y 80uS, mientras que en el bridge vemos retardos del orden de los 30mS.

2.2.3. SWITCHES

El switch toma decisiones de envío sencillas basándose en la dirección MAC de destino contenida en cada paquete y, generalmente, sin tomar en consideración otros datos incluidos en éste.

La tecnología de switching permite incrementar el ancho de banda tanto en segmentos de LAN compartidos como dedicados y elimina los cuellos de botella entre varias LAN. En la actualidad los productos de switching se encuentran

disponibles para todas las tecnologías (Familia Ethernet, FDDI, ATM y Token Ring).

2.2.3.1. Modo de operación

La conmutación Ethernet aumenta el ancho de banda disponible en una red. Esto se hace creando segmentos de red dedicada, o conexiones punto a punto, y conectando estos segmentos en una red virtual dentro del switch. Este circuito de red virtual existe solamente cuando dos nodos necesitan comunicarse.

Aunque el switch LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch pertenecen al mismo dominio de broadcast. Por lo tanto, un broadcast emitido de un nodo lo percibirán todos los demás conectados a través del switch LAN

Los switches poseen 2 modos de operación, cut-through y store and Forward que se describen a continuación.

Cut-Through

Inician el proceso de reenvío antes de haber recibido la trama completa.

Dado que el switch sólo tiene que leer la dirección MAC para poder reenviar la trama, los paquetes se procesan con mayor rapidez y la latencia es la misma para paquetes grandes y pequeños. La mayor desventaja es que las tramas dañadas o paquetes truncados también se envían de forma inmediata.



Figura 5. Switch 3COM 4005

Esta modalidad de reenvío puede utilizarse cuando el tráfico se conmuta entre puertos de LAN con la misma velocidad pues de no ser así tendrá que quedar almacenado en el buffer antes del reenvío.

Store-and-forward

Leen y validan el paquete entero antes de iniciar el proceso de reenvío.

Esto permite eliminar los paquetes dañados y ofrece al administrador de la red la posibilidad de definir los filtros de paquetes más adecuados para controlar el flujo

de tráfico que pasa por el switch. La desventaja de esta última modalidad es que la latencia se incrementa proporcionalmente al tamaño del paquete.

Un switch es un dispositivo especialmente diseñado para resolver los problemas de rendimiento de la LAN provocados por las reducciones del ancho de banda y los cuellos de botella. La solución aportada por los switches consiste en proporcionar gran cantidad de ancho de banda agregado y una velocidad de proceso de paquetes muy elevada y baja latencia.

Los switches no están diseñados con el objetivo de proporcionar un control completo sobre la red, sino que deben considerarse como "suministradores" de ancho de banda, no como la fuente última de seguridad, redundancia, control o gestión de red

2.2.3.2. Ventajas

Además de las ventajas que ya han sido mencionadas, podemos destacar:

- Reducción de las colisiones, elimina el dominio de colisiones y reenvía tramas. Métodos de almacenamiento Store and Forward.
- Múltiples comunicaciones simultáneas e incremento del ancho de banda por segmento.
- Enlaces superiores de alta velocidad y baja latencia. Los switches son más veloces porque realizan la conmutación por hardware, mientras que

los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch

- Respuesta de red mejorada ayudando al aumento de la productividad del usuario.

2.2.3.3. Desventajas

- Para la segmentación LAN adecuada deben ser gestionables y configurables.
- No todos permiten Monitoreo de la red. Deben Manejar SNMP.
- Sin la configuración adecuada pueden ser puntos de colapso en la red.

2.2.3.4. Segmentación con Switches

Una LAN que usa una topología Ethernet de conmutación crea una red que funciona como si sólo tuviera dos nodos; el nodo emisor y el nodo receptor. Estos dos nodos comparten el ancho de banda.

Un computador conectado directamente a un switch Ethernet está en su propio dominio de colisión y tiene acceso al ancho de banda disponible en la red. Cuando una trama entra a un switch, se lee para obtener la dirección origen o destino.

Luego, el switch determina cuál es la acción de conmutación que se llevará a cabo basándose en lo que sabe a partir de la información que ha leído en la trama. Si la dirección destino se encuentra ubicada en otro segmento, la trama se conmuta a su destino.

La segmentación de los dominios de colisiones también se pueden llevar a cabo con Routers, pero esta alternativa es muy costosa, ya que el precio por puerto de un router se encuentra en los \$1000 dólares, mientras que el precio por puerto de un switch está alrededor de los \$150 dólares y realizarán la misma labor a este nivel. Para este tipo de segmentación se utilizan switches, el router tiene mayor aplicabilidad para la segmentación de los dominios de Broadcast; No obstante, el switch también puede tener partido en la segmentación de Broadcast con el uso de VLANs, que serán expuestas más adelante.

El switch se constituye el protagonista de la capa de enlace de datos. Si en la red existente se tienen Hubs, para mejorar su funcionamiento, en lo posible se deben cambiar por Switches, o colocarlos como concentradores de estaciones de trabajo que requieran bajo ancho de banda, como procesadores de texto, hojas de cálculos, impresoras compartidas entre otros, si se está diseñando una nueva red por ningún motivo se deben emplear hubs.

2.3. BROADCAST. DEFINICION Y CONSIDERACIONES

Es un paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican mediante una dirección específica. Esta técnica de enrutamiento permite que el tráfico de IP se propague desde un origen hasta una serie de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, un paquete se envía a un grupo de broadcast identificado a través de una sola dirección IP de grupo de destino.

La dirección IP del Broadcast está compuesta por la dirección de red, seguida de 255 en la parte de Host, indicando que es para todos.

Ejemplo: Dirección de red 10.0.0.0, el Broadcast para esta dirección será 10.255.255.255.

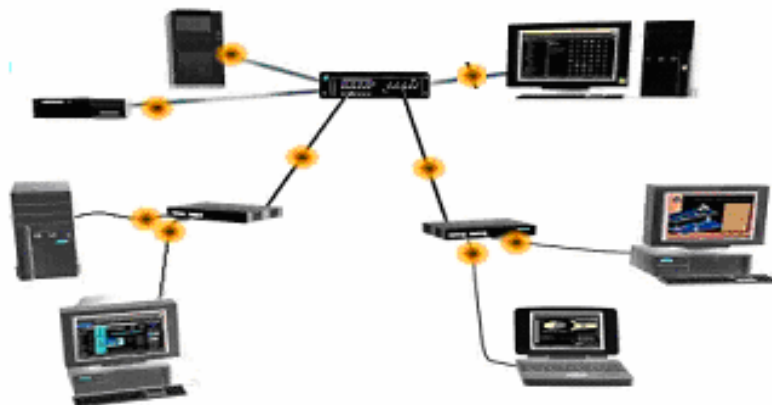


Figura 6. Broadcast

Existen varios tipos de Broadcast.

2.3.1. MULTICAST

consiste en el envío de paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de direcciones de destino.



Figura 7. Multicast

2.3.2. UNICAST

Es un mensaje que se envía específicamente a un Nodo de la red.

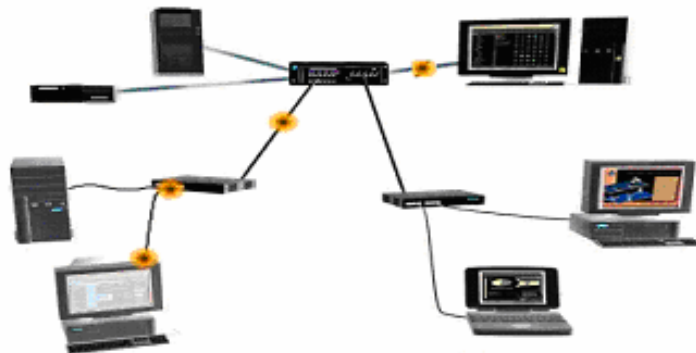


Figura 8. Unicast

El Broadcast se ve irrigado por elementos de red como Hub y Switches que no posean configuración VLAN. El Router trabaja con direcciones IP y no permite que se difundan estas tramas entre segmentos. Cuando un Host no conoce la dirección IP destino o desconoce la MAC de otro, irriga un paquete a todos preguntando su IP o la MAC (Protocolos RARP y ARP), cuando este llega al router, el responde con su propia IP o con la MAC negando al origen el acceso a otro segmento, y envía un paquete hacia el origen que será almacenado e identificado. El host origen entenderá alcanza su destino a través del router.

El router es la solución de capa 3 para el broadcast, también existen Switches de Capa 3 o Switches de enrutamiento a alta velocidad que realizan esta función, el ligero problema radica en el costo de ambos, sin embargo, el broadcast puede ser controlado con la configuración de VLANs en switches de capa 2 gestionables.

2.3.3. VLANs

Una VLAN es una agrupación lógica de dispositivos o usuarios que se pueden congrega por función, departamento o aplicación, sin importar la ubicación física del segmento. Una VLAN crea un dominio de broadcast único que no se restringe a un segmento físico y se considera como una subred. La configuración de la VLAN se realiza en el switch por software.

La creación de VLANs se puede basar en el ID de puerto, dirección MAC, protocolo o aplicación, creando un grupo de usuarios que comparten el mismo dominio de broadcast, rotulando en la trama un identificador o ID de VLAN.

Generalmente su creación se ve reflejada en los switches y en el software de administración de la LAN.

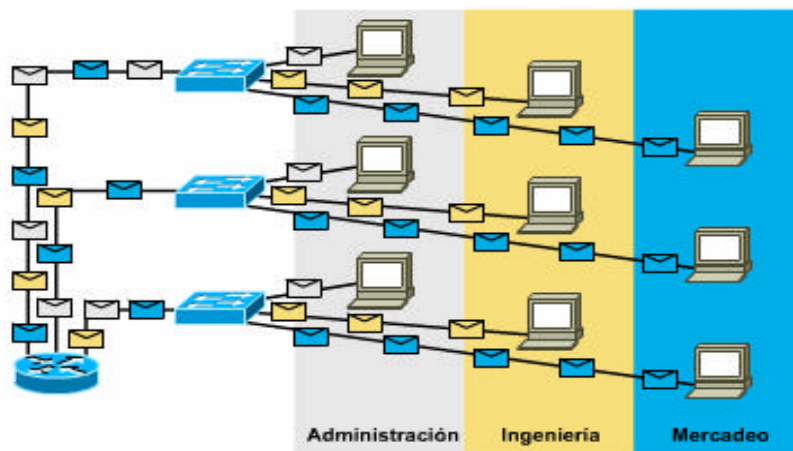


Figura 9. Funcionamiento de VLAN

2.3.3.1. Características

- ❑ Las VLAN funcionan a nivel de Capa 2 y Capa 3 del modelo de referencia OSI.
- ❑ La comunicación entre las VLAN es implementada por el enrutamiento de Capa 3.
- ❑ Las VLAN proporcionan un método para controlar los broadcasts de red.
- ❑ El administrador de la red asigna usuarios a una VLAN.

- Las VLAN pueden aumentar la seguridad de la red, definiendo cuáles son los nodos de red que se pueden comunicar entre sí.

Mediante la tecnología VLAN, se pueden agrupar los puertos de switch y sus usuarios conectados en grupos de trabajo lógicamente definidos, como los siguientes:

- Compañeros de trabajo en el mismo departamento
- Un equipo de producción interfuncional
- Diferentes grupos de usuarios que comparten la misma aplicación de red o software

Se pueden agrupar estos puertos y usuarios en grupos de trabajo con un solo switch o switches conectados. Al agrupar los puertos y los usuarios a través de múltiples switches, las VLAN pueden abarcar infraestructuras contenidas en un solo edificio, edificios conectados entre sí o aun redes de área amplia (WAN).

En la configuración de VLANs se debe tener presente el backbone de la red, prácticamente el proceso de LAN virtual se da entre switches, para el usuario final es transparente este proceso.

2.3.3.2. Funcionamiento de VLAN

Las VLANs adjuntan a la trama común un identificador único en el encabezado a medida que se envía por todo el backbone de la red. Un identificador está asociado al número de VLAN y la dirección MAC. El identificador es comprendido y examinado por cada switch antes de enviar cualquier broadcast o transmisión a otros switches, routers o dispositivos de estación final. Cuando la trama sale del backbone de la red, el switch elimina el identificador antes de que la trama se transmita a la estación final. La identificación de trama funciona a nivel de Capa 2 y requiere poco procesamiento o sobrecarga administrativa.

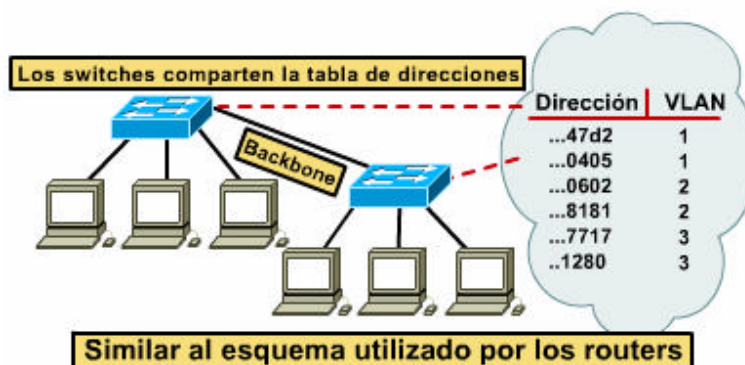


Figura 10. Esquema de VLAN

2.3.3.3. Clases de VLANs

Estáticas

Las VLAN estáticas son puertos en un switch que se asignan estáticamente a una VLAN. Estos puertos mantienen sus configuraciones de VLAN asignadas hasta que se cambien. No obstante las VLAN estáticas requieren que el administrador haga los cambios, este tipo de red es segura, de fácil configuración y monitoreo. Las VLAN estáticas funcionan bien en las redes en las que el movimiento se encuentra controlado y administrado.



Figura 11. VLAN Estática

Dinámicas

Las VLAN dinámicas son puertos en un switch que pueden determinar automáticamente sus asignaciones de VLAN. Las funciones de las VLAN dinámicas se basan en las direcciones MAC, direccionamiento lógico o tipo de protocolo de los paquetes de datos. Cuando una estación se encuentra inicialmente conectada a un puerto de switch no asignado, el switch

correspondiente verifica la entrada de direcciones MAC en la base de datos de administración de la VLAN y configura dinámicamente el puerto con la configuración de VLAN correspondiente. Los principales beneficios de este enfoque son una necesidad de menor administración en el centro de cableado, cuando se agrega o desplaza un usuario y la notificación centralizada cuando se agrega un usuario no reconocido en la red. Normalmente, se necesita una mayor cantidad de administración en un primer momento para configurar la base de datos dentro del software de administración de la VLAN y para mantener una base de datos exacta de todos los usuarios de la red.

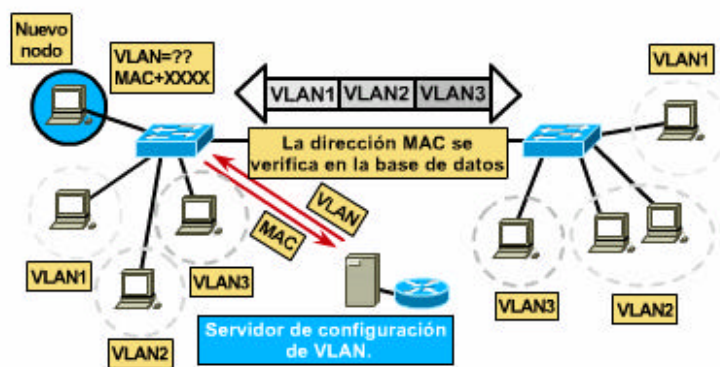


Figura 12. VLANs Dinámicas

Ya sea que usted necesite seguridad o flexibilidad, puede configurar su red con VLANs estáticas o dinámicas.

2.4. SOLUCIÓN DE ANCHO DE BANDA EN BACKBONES

Como es común verse, los backbones entre switches, routers y servidores, son los que se ven afectados por el alto tráfico, es decir, colapsados. Asimismo los backbones son los que definen el verdadero ancho de banda disponible para cualquier tipo de aplicación que se desea correr en la red.

A continuación explicaremos técnicas que ayudan al ancho de banda, como migración a otras tecnologías, Trunking, entre otras.

2.4.1. MIGRACIÓN A OTRAS TECNOLOGÍAS

La tecnología Ethernet es la más versátil en este aspecto, pues pertenece a un número de familias que brindan mayor ancho de banda con ligeros cambios en la estructura en la red.

2.4.1.1. Fast Ethernet.

Fast Ethernet es la Ethernet que se ha actualizado a 100 Mbps. Este tipo utiliza la topología de bus lógica orientada a broadcast Ethernet estándar de 10BASE-T, junto con el método familiar CSMA/CD para el Control de acceso al medio (MAC).

El estándar Fast Ethernet en realidad se compone de varios estándares distintos basados en cable de par de cobre (100BASE-TX) y en cable de fibra óptica (100BASE-FX), y se utiliza para conectar el distribuidores.

Eventualmente Fast Ethernet se puede utilizar entre switches de un mismo nivel, además, a estos se les puede configurar la velocidad por puerto. Generalmente los switches son 10/100, con puertos Uplink o downlink, de salida o de entrada a conexión con otros switches respectivamente.

La migración a esta tecnología se realiza únicamente con el cambio de tarjetas de 10Mbps a 100Mbps, la diferencia de precio entre ellas es de US\$15, siendo una excelente opción para estaciones de trabajo. Asimismo se debe migrar a switches que soporten enlaces 10/100/1000, con puertos de expansión en Fibra.

Fast Ethernet Full Duplex

Así como una Ethernet tradicional, la progresión natural en las tecnologías es utilizar Full duplex. Fast Ethernet puede proveer 100Mbps en cada dirección obteniendo un throughput total de 200Mbps. El máximo caudal de bits es posible sólo si la estación de trabajo está directamente conectada a un switch y este es full duplex.

En algunas tarjetas de red y switches estas velocidades de 10/100Mbps son autonegociables, si la tarjeta observa que el puerto del switch al que está conectada es de 100Mbps segmentados, ella automáticamente cambia su caudal de bits a 100Mbps, y lo hace a 200Mbps cuando identifica que es full duplex.

Sin embargo en los Switches se pueden especificar prioridades de autonegociación por puertos, como se ilustra en la siguiente tabla.

Prioridad	Modo Ethernet
7	100BaseT2(Full duplex)
6	100BaseT2(Half duplex)
5	100BaseTx(full duplex)
4	100BaseT4
3	100BaseTx
2	10BaseT(full duplex)
1	10BaseT(half duplex)

Tabla 2. Especificación Fast Ethernet

2.4.1.2. Gigabit Ethernet.

El estándar Fast Ethernet se puede llevar a 1000Mbps o Gigabit Ethernet, migrando hacia tasas de transferencias mucho más altas entre los backbones con

una inversión adicional mínima, sin necesidad de reformar los administradores de la red o los usuarios, gracias a que las tres tecnologías son compatibles entre si.

El estándar Gigabit Ethernet fue establecido en 1998 bajo el IEEE 803.z, (1000BaseLX/SX) con comunicación full duplex sobre cableado de fibra. En 1999 se estableció la IEEE 803.ab, que especifica Gigabit sobre cable de cobre UTP Cat. 5E y 6 facilitando transmitir Gigabit Ethernet sobre el cable existente.

Migrar hacia Ethernet 1000BaseTX, sobre cable de cobre se convierte en la opción más económica de mejoramiento de ancho de banda, debido a que es sobre la infraestructura del cableado existente.

Para Distancias cortas no superiores a los 100m se puede utilizar 1000BaseT, sobre UTP Cat 5. Sin embargo, las tarjetas 1000BaseT sobre cable categoría 6 son más económicas, por ello se recomienda utilizar cable UTP Cat. 6 para las nuevas implementaciones dentro de la red.

Para distancias superiores se debe utilizar fibra óptica. Algunas de las especificaciones se encuentran en la siguiente tabla.

GE Type	Wiring Type	Pairs	Cable Length
1000BaseCX	Shielded Twisted Pair (STP)	1	25 m
1000BaseT	EIA/TIA Category 5 UTP	4	100 m
1000BaseSX	Multimode fiber (MMF) with 62.5 micron core; 850 nm laser	1	275 m
	MMF with 50 micron core; 1300 nm laser	1	550 m
1000BaseLX/LH	MMF with 62.5 micron core; 1300 nm laser	1	550 m
	Single-mode fiber (SMF) with 50 micron core; 1300 nm laser	1	550 m
	SMF with 9 micron core; 1300 nm laser	1	10 km
1000BaseZX	SMF with 9 micron core; 1550 nm laser	1	70 km
	SMF with 8 micron core; 1550 nm laser	1	100 km

Tabla 3. Especificaciones Gigabit Ethernet

La L representa onda larga o de 1270 nanómetros, y la S representa onda corta de 850 nanómetros. Generalmente se implementan sobre conectores SC.

Ventajas principales de Gigabit

- Incremento substancial en el ancho de banda, Las aplicaciones de multimedia operan sin problemas, además elimina los cuellos de botella en el servidor.
- Transmite bi-direccionalmente sobre 4 pares para lograr comunicación full-duplex (500 Mbps por cada par) @ 250 Mhz brindando un throughput de 2000Mbps.
- Compatibilidad total con LANs Ethernet y Fast Ethernet

- ❑ Sólo es necesario migrar unas partes de la red (red troncal, conexiones del servidor).
- ❑ Se puede aprovechar el cableado existente.
- ❑ Calidad de servicio (QoS) asegura que bs paquetes de información se entregan según su nivel de prioridad
- ❑ El soporte VLAN reduce el tráfico en la red
- ❑ Utiliza tecnología de procesamiento digital de señales para: Supresión de ruido, Cancelación de Eco, Cancelación de Interferencia Cruzada Cercana y Lejana (Near End Cross Talk & Far End Cross Talk)
- ❑ Aprovecha las nuevas tecnologías de chips de alta densidad y alta velocidad.
- ❑ Utiliza modulación por amplitud con 4 niveles de amplitud y codificación digital trellis.

2.4.2. REDES HIBRIDAS. LAN EMULATION Y EMULATED LAN

Con la incursión de ATM surgen dos conceptos en redes Ethernet que son, LANE (LAN emulation) y ELAN (Emulated LAN).

2.4.2.1. ATM

La tecnología ATM envía unos paquetes de 53 bytes denominados celdas. El pequeño tamaño de los paquetes garantiza un mínimo retardo aunque supone un

incremento del overhead: cuanto más pequeño es el paquete, más proporción hay de cabeceras y más pérdida de ancho de banda. Las ventajas obtenidas es una baja latencia que permite transportar datos isocrónicos (vídeo y Voz) y una eficiente conmutación en hardware gracias al tamaño constante de los paquetes.

Arquitectura

ATM puede ser considerado como una tecnología de conmutación de paquetes a alta velocidad con las siguientes características:

- ❑ Los paquetes son pequeños y de tamaño constante (53 bytes).
- ❑ Es una tecnología de naturaleza conmutada y orientada a la conexión.
- ❑ Los nodos que componen la red no tienen mecanismos para el control de errores o control de flujo.
- ❑ El header de las celdas tiene una funcionalidad limitada.
- ❑ Múltiples conexiones inter-switch para balanceo de cargas.

Simplificando al máximo podemos ver que una red ATM está compuesta por nodos de conmutación, elementos de transmisión y equipos terminales de usuarios. Los nodos son capaces de encaminar la información empaquetada en celdas a través de unos caminos conocidos como Conexiones de Canal Virtual. El routing, en los nodos conmutadores de celdas, es un proceso hardware mientras

que el establecimiento de conexiones y el empaquetamiento/desempaquetamiento de las celdas son procesos por software.

Ventajas

Las ventajas que ofrece la tecnología **ATM** respecto a otras son las siguientes:

- Integración de todo tipo de red : LAN, MAN y WAN
- Manejo uniforme de todos los servicios de una red, incluidos vídeo, imagen, datos y voz.
- Asignación dinámica de ancho de banda para que los servicios sólo utilicen lo que necesiten y para que puedan coexistir distintos servicios en el mismo enlace o línea.
- Tecnología basada en celdas que permite a los clientes "pagar lo que se use" para obtener servicios más baratos.

Desventajas

- La principal desventaja de ATM es que requiere de una infraestructura costosa, dificultando su implementación a corto plazo.

2.4.2.2. LANE (LAN Emulation)

LANE hace que las tramas de Ethernet se vean como celdas de ATM, creando un soporte de Ethernet sobre ATM. Esta solución no influye excesivamente en la infraestructura de la red LAN existente, no requiere el cambio de Hubs, switches ó Routers, Creando redes virtuales y lógicas con cada conexión ATM.

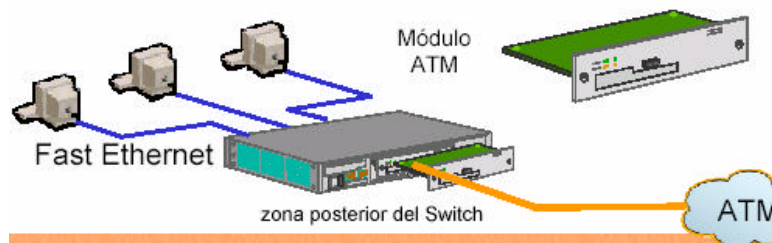


Figura 13. Migración Ethernet a ATM

Esta solución convierte a los backbones principales en backbones ATM, soportando tecnologías mezcladas, asimismo, genera prestaciones ATM a las conexiones en servidores, disponibilidad de enlaces ATM a estaciones de trabajo como se ve en el switch del tercer piso de la figura 14, velocidades de 155Mbps OC-3 (3 hilos troncales) y de 622Mbps OC-12 (12 hilos troncales), aunque Gigabit Ethernet trabaja a 1000Mbps, las prestaciones ATM como QoS (calidad del servicio), conmutación de celdas, establecimiento de circuitos virtuales y ser orientado a conexión descongestionan indudablemente los backbones de la red.

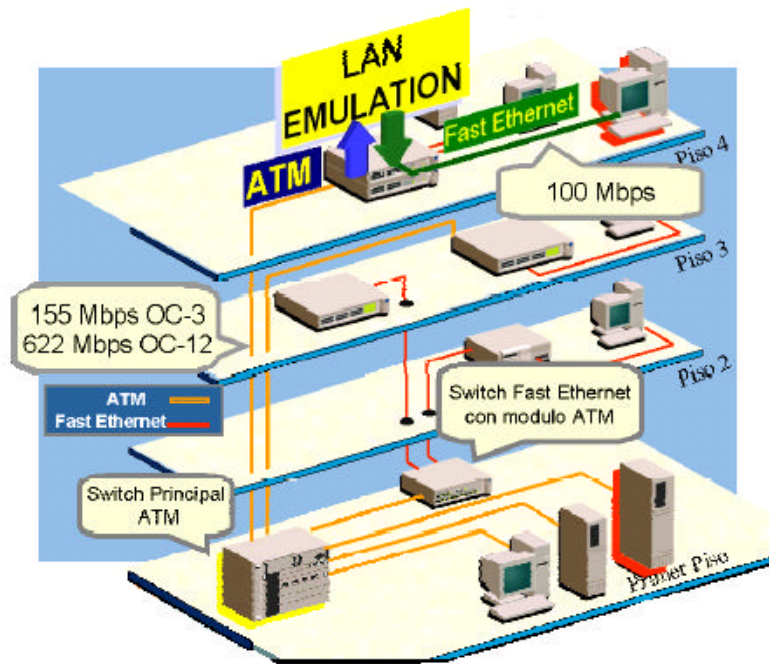


Figura 14. LAN Emulation.

Para migrar se requieren de módulos ATM (NIC's ATM), Switches ATM y que los switches Ethernet sean Stackable y tengan ranuras de expansión para los mismos.

Elementos de una LAN Emulation

Para construir una red híbrida con soporte ATM (LANE) es necesario que esta posea los siguientes elementos:

1. LAN Emulation Client (LEC)

Es la entidad en un sistema terminal que se encarga de la transmisión de datos, la resolución de direcciones, y otras funciones de control en cada ELAN (LAN Emulada). Un LEC también provee una interfase estándar de servicio de LAN para cualquier entidad de las capas superiores. Además provee servicio IEEE 802.3 y IEEE 802.5.

Una NIC ATM o switch LAN soporta un solo LEC por cada ELAN al cual está conectado.

2. LAN Emulation Server (LES)

El LES implementa las funciones de control para una ELAN en particular. Hay solamente un LES lógico por ELAN. Cada LES es identificado por una única dirección ATM.

3. Broadcast and Unknown Server (BUS)

El BUS es un servidor multiemisor (multicast) que es utilizado para fluir el tráfico de las direcciones destino desconocidas y reenviar el tráfico de los emisores y multiemisores a los clientes en una ELAN en particular. Cada LEC es asociado a un solo BUS por ELAN.

4. LAN Emulation Configuration Server (LECS)

Los LECS es una entidad que asigna individualmente a los clientes LANE a una ELAN en particular, direccionándolos hacia el LES que corresponde a una ELAN específica. Lógicamente hay un LECS por dominio administrativo y éste sirve a todas las ELAN's dentro del dominio.

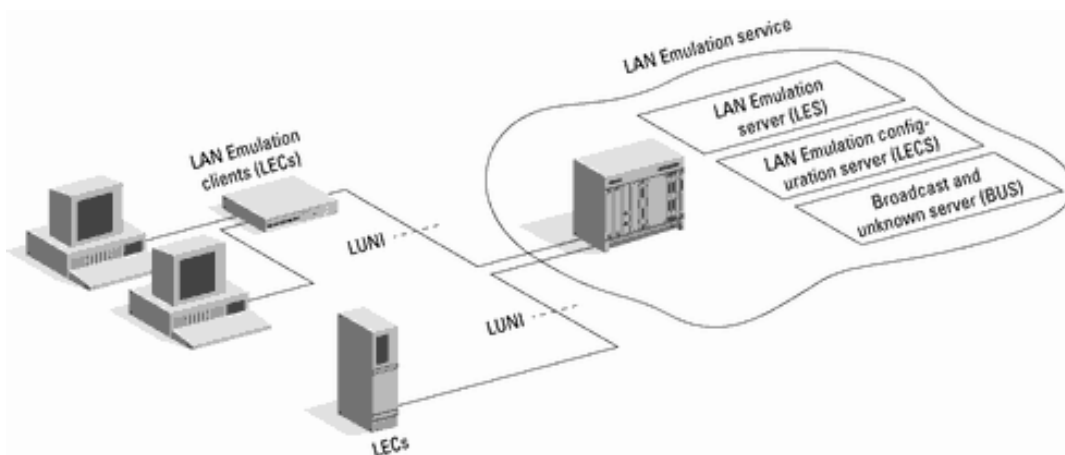


Figura 15. Elementos de una LANE con Ethernet

2.4.3. TRUNKING

Mediante la función de Trunking, el flujo de datos entre dos switches puede ser multiplicado, transmitiendo en paralelo por varios puertos el mismo flujo de datos, pero particionado, logrando un canal de comunicación mucho más amplio. Los puertos conectados de esta forma crean un único enlace lógico. El método Trunking fue establecido por el Instituto de Ingeniería Eléctrica y Electrónica IEEE 803.ad Link Aggregation.

Características

- Permite escalar gradualmente a medida que lo requiere.
- Permite combinar múltiples enlaces físicos (Fast Ethernet, GEthernet, ATM) en un solo enlace lógico.
- Un algoritmo Hashing distribuye el tráfico entre los enlaces.

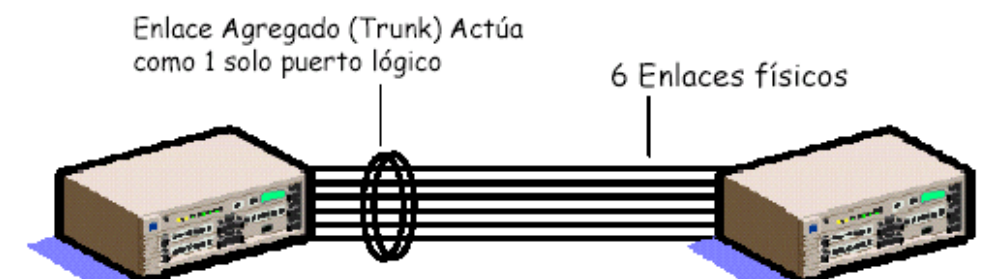


Figura 16. *Trunking*

Incrementa el ancho de banda punto a punto sin necesidad de cambiar los dispositivos existentes o el cableado. Incrementa la disponibilidad de la red, si un puerto falla, el tráfico se redistribuye entre el conjunto de puertos que continúan operando.

Consideraciones

Todos los enlaces de un grupo troncal deben ser de la misma tecnología, no se puede combinar enlaces Fast Ethernet con Gigabit Ethernet en un mismo enlace agregado.

El caudal de datos (Throughput) de un enlace agregado es igual al ancho de banda total obtenido al sumar los anchos de banda de cada uno de los enlaces individuales. Por ejemplo: La agregación (Trunking) de 2 enlaces de 1000 Mbps c/u provee un enlace de 2000 Mbps.

La técnica Trunking reparte los canales que han sido troncalizados al número de estaciones que están conectados al switch, este los asocia con las MAC, en el caso de crear un enlace lógico con 6 troncales y 6 PCs conectados al switch directamente, se le asigna un canal a cada PC, respetando el ancho de banda disponible por canal, si un enlace falle, se realiza una nueva asignación de los mismos, ayudando a la operación continua.

La comunicación entre dos direcciones MAC específicas se le asigna a solo uno de los puertos del enlace trunking. Por lo tanto es importante saber que el Trunking no brinda beneficios directos a cierto tipo de aplicaciones como por ejemplo al Backup entre servidores.

Las ventajas del enlace Trunking se obtienen en el tráfico Any-to-Any debido a la simultaneidad. Estas se pueden apreciar cuando un grupo grande de usuarios envía tráfico sobre el enlace agregado, los resultados en rendimiento son excelentes.

Cabe anotar que la técnica Trunking resulta atractiva a los diseñadores de redes, pues no interviene directamente ni en los equipos, ni con el medio, pero mirando que el valor de un Switch oscila en los US\$150/Puerto, para un enlace sencillo se necesitan mínimo 2 switches, si se realiza un enlace lógico de 6 troncales, el gasto ($us\$150 \cdot 6 \cdot 2 \text{switch}$) está alrededor de us\$1800, se utilizaron 12 puertos que equivalen a otro dispositivo.

Hay que analizar donde es funcional un enlace Trunking, pues resulta más conveniente invertir en Switches con módulos de fibra a 1000Mbps, y comprar 2 tarjetas para fibra que oscilan alrededor de unos US\$200; esta solución se encuentra en el mismo valor que la solución troncalizada pero posee mejores prestaciones. Para este caso el trunking no es funcional, es recomendable migrar su red hacia módulos con fibra.

Las aplicaciones Trunking van mejor acompañadas del balanceo de cargas en servidores, además también se pueden troncalizar enlaces de Gigabit, llegando a obtener velocidades de 6Gbps Full duplex.

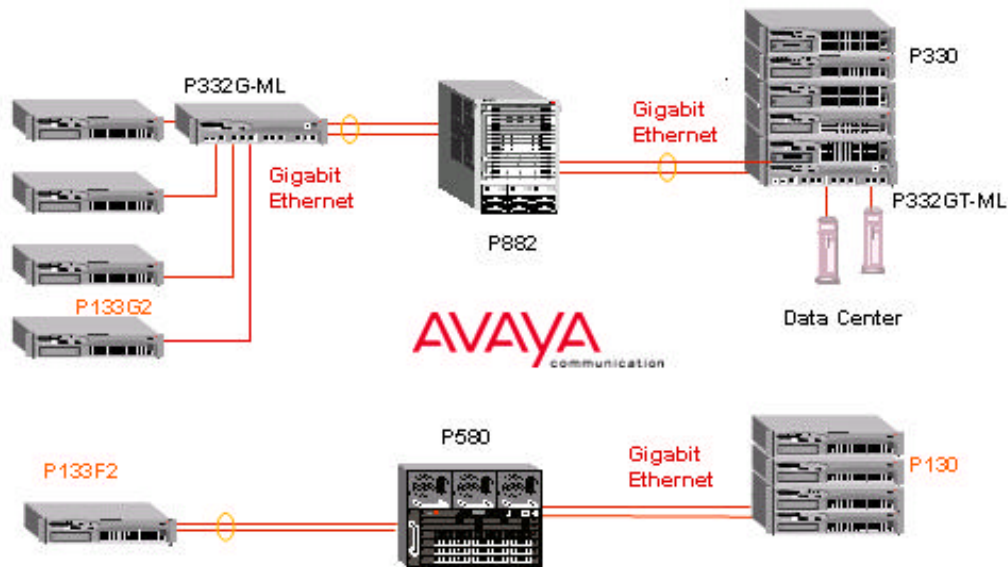


Figura 17. Solución AVAYA

Capacidad de Troncales con Switches AVAYA

- 8 Troncales 10/100 Mbps (full duplex)
- 2 Troncales 100BaseFX (full duplex)
- 2 Troncales 1000BaseSX/LX (full Duplex)

2.4.4. BALANCEO DE CARGAS. SOLUCIÓN EN SERVIDORES

Dentro de los puntos de colapso en una red LAN encontramos los servidores. Estos al igual que los switches se ven agobiados por el exceso de tráfico; una solución al tráfico excesivo en servidores, es tener servidores de respaldo, lógicamente esta solución incurre en gastos tan grandes como la capacidad de los

servidores, vale la pena mirar cual es la importancia que cobra la información que se va a proteger.

El balanceo de carga es una técnica que ayuda a mitigar el tráfico en servidores, además de garantizar la operación continua en los mismos, también esta se puede realizar en caliente, transparente a los usuarios, ellos sólo verán una red con mejor rendimiento.

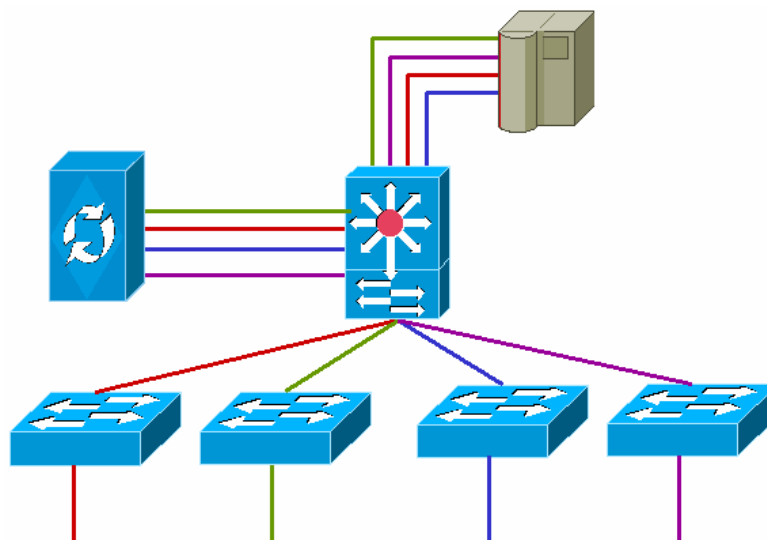


Figura 18. Balanceo de carga en servidores.

AVAYA al igual que CISCO y 3COM han incursionado en switches con balanceo de carga y puertos de expansión para el mismo efecto.

Estos generalmente se utilizan en conexiones con servidores de transporte TCP o UDP, como HTTP, FTP, DNS. Estos switches también distribuyen tráfico entre servidores de respaldo.

Los servidores con balanceo de cargas utilizan varias NIC con Drivers especializados SDH (Autodetección de fallas y gestión de interrupción automática), en caso de una falla en una de ellas, el tráfico se redistribuye entre las demás tarjetas.

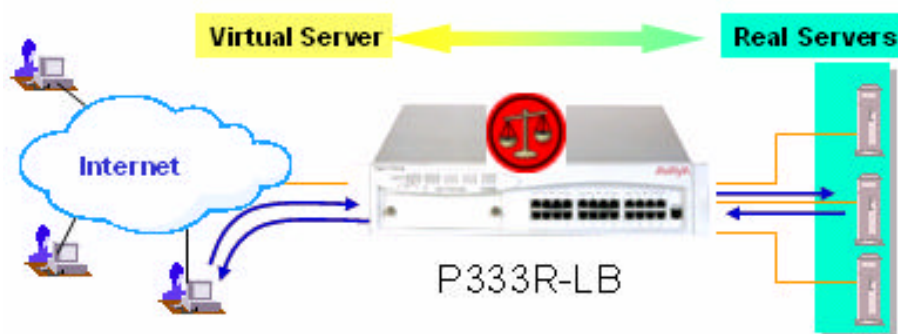


Figura 19. Referencia de Switch AVAYA y servidores de respaldo

Es necesario el balanceo de cargas en servidores, con canales troncales hacia él, que las tarjetas que posee tengan gestión inteligente de interrupción, asimismo se debe configurar el switch con la debida distribución del tráfico por puerto. Para esta solución el switch debe estar configurado como Store and Forward.

2.5. CONFIGURACIÓN DE SWITCHES

La Siguiete guía de configuración se aplica a los Switches Catalyst 1900 en adelante de Cisco.

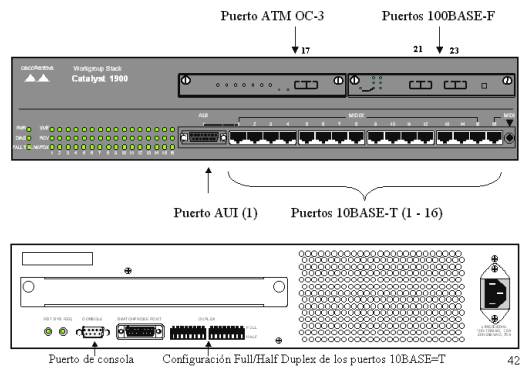


Figura 20. Switch Catalyst 1900

Todos los Switches vienen de fábrica con una configuración por defecto y con un nombre de sistema por defecto o Prompt.

Al iniciar el Switch, se mostrará la siguiente pantalla, donde podrá optar por trabajar con menús o por medio de línea de comandos de consola (CLI)

```

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address:      00-30-80-C7-BE-C0

PCA Number:           73-3122-04
PCA Serial Number:    FAB033723WJ
Model Number:         WS-C1912-A
System Serial Number: FAB0338S10A
Power Supply S/N:     APQ032404SA
PCB Serial Number:    FAB033723WJ,73-3122-04
-----

1 user(s) now active on Management Console.

      User Interface Menu

      [M] Menus
      [K] Command Line

Enter Selection:

```

Para Ingresar al modo CLI (command line interface) del Switch se presiona la letra "K", con lo que obtendrá el siguiente mensaje seguido por el respectivo Prompt

```
CLI session with the switch is open.  
To end the CLI session, enter [Exit].  
>
```

Del mismo modo que en los Routers 2500/2600, Ingrese al modo Enable y Luego al modo de configuración global.

```
>enable
```

Aparecerá el Prompt de modo privilegiado, "#"

Luego se ejecuta Configure Terminal para ingresar al modo de configuración global.

```
#Configure Terminal  
(config)#
```

2.5.1. IDENTIFICACIÓN DE UN SWITCH

Con el comando Hostname seguido del nombre que se desea dar, se identifica el switch.

```
Switch(config)# hostname simulador  
Simulador(config)#
```

2.5.2. SEGURIDAD Y PASSWORDS

Las contraseñas o Passwords en un switch pueden variar desde 1 hasta 15 niveles, la configuración de ellas se puede definir.

```
Simulador(config)# enable password level 1 password1
Simulador(config)# enable password level 2 password2
.
.
Simulador(config)# enable password level 15 password15
```

Para remover un Password, se ejecuta, no enable password, desde el comando de nivel de password.

```
Password changed.
```

2.5.3. COMUNICACIÓN ENTRE SWITCHES

Para que exista comunicación entre Switches, Cisco ha desarrollado el CDP (CISCO Discover Protocol). Este protocolo brinda información de la configuración de los vecinos, velocidad de puertos, identificación de VLANS, entre otras. Los Switches CISCO ya tienen activado el CDP por defecto, sin embargo se puede activar o desactivar con la siguiente línea.

```
Switch(config-if)# cdp enable
Switch(config-if)# no cdp enable
```

El CDP es necesario de manera que ayuda a identificar a los equipos vecinos de la red. Más que todo es un protocolo que ayuda a la gestión e identificación de la condición de una red.

Para observar la información recuperada por el CDP se puede escribir la siguiente línea:

```
Switch# show cdp interface [ type module/port ]  
Switch# show cdp neighbors [ type module/port ] [detail]
```

La primera línea de comandos muestra información de una interfase específica, la segunda muestra información de los vecinos CISCO en la red.

2.5.4. CONFIGURACIÓN DE PUERTOS

Un parámetro importante en la configuración de Switches es la configuración de puertos, es aquí donde se define la tecnología que se desea utilizar, si es Ethernet, Fast Ethernet, Gigabit Ethernet o Token Ring.

En ocasiones se poseen Switches, pero no se les saca provecho por el desconocimiento de las habilidades que este posee.

2.5.4.1. Descripción de un Puerto Ethernet.

En el modo de configuración global se accede a una interfaz específica.


```
Switch# Configure terminal
Switch (config)# FastEthernet 0/1
Switch(config-if)#
```

El cero indica al modulo que pertenece dicha interfaz y el 1 el número del puerto de ese módulo.

Luego se ejecuta el comando *description* seguido del nombre que desea asignar a esa interfaz.

```
Switch(config-if)# description Red Lan
```

2.5.4.2. Velocidad de los Puertos Ethernet

La velocidad de los puertos se puede configurar en 10, 100 o Auto para el modo negociable. Este último comercializa directamente con la tarjeta de red identificando su velocidad o máxima tasa de bits, trabajando a dicha velocidad.

```
Switch(config-if)# speed {10 | 100 | auto}
```

2.5.4.3. Configuración del enlace Ethernet.

Los enlaces tienen configuración Half duplex, full duplex y auto. Veamos la siguiente línea de comandos:

```
Switch(config-if)# duplex {auto | full | half}
```

2.5.4.4. Configuración de Puertos Token Ring

Token Ring es una tecnología que ayuda a la operación continua en redes, por ser una red determinista. Por ello algunas empresas que manejan procesos críticos utilizan esta tecnología.

Tiene varios modos:

- Half-duplex Puerto concentrador. Nomenclatura de Switch (hdxcpport)
- Half-duplex Emulación de Estación. Nomenclatura de Switch (hdxstation)
- Full-duplex Puerto concentrador. Nomenclatura de Switch (fdxcport)
- Full-duplex Emulación de Estación. Nomenclatura de Switch (fdxstation)
- Autosensing (auto)

Desde el CLI (Command Line Interface):

```
Switch(enable) set tokenring portmode module/number {auto |  
fdxcport | hdxcpport |  
fdxstation | hdxstation}
```

2.5.5. CONFIGURACIÓN DE VLAN'S

Para Crear VLANs, deberá seguir los siguientes pasos:

Desde el modo privilegiado acceda a una base de datos donde se registran las VLANs.

```
Switch# vlan database
Switch(vlan)#
```

Como se ve el prompt cambió al modo de configuración de VLANs. Luego nos disponemos a identificar a las VLANs por número y por nombres.

```
Switch(vlan)# vlan 2 name Mercadeo
Switch(vlan)# vlan 3 name Contabilidad
Switch(vlan)# vlan 4 name Gerencia
Switch(vlan)# exit
```

Los números 2, 3, y 4, identifican el número de la VLAN, la VLAN 1 es la VLAN por defecto que posee el Switch y se utiliza para la configuración de accesos remotos. Las VLAN's se reconocen por el nombre que desee asignar, en nuestro caso serán Mercadeo, contabilidad y Gerencia.

Si desea observar las VLANs creadas, ejecute el comando Show VLAN.

```
Switch(vlan)# Show
```

Para asignar puertos a una VLAN deberá realizar el siguiente procedimiento:

Desde el modo de configuración Global, ingresar a la interfaz deseada (ejemplo int FastEthernet 0/1).

```
Switch(config)#int FastEthernet 0/3
Switch(config-if)#
```

Indicamos el modo de acceso al puerto del switch.

```
Switch(config-if)# switchport mode access
```

De la misma forma se asigna el número de VLAN a este puerto.

```
Switch(config-if)# switchport access vlan 3
Switch(config-if)# end
```

En caso de compartir VLAN's entre Switches se debe establecer una conexión entre éstos por medio de los puertos Fast Ethernet o Gigabit troncalizados, debido al alto tráfico que poseen los puertos. Para ello se utilizan los siguientes comandos para crear VLANs troncalizadas.

```
Switch(config)# interface FastEthernet 0/12
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation {isl | dot1q}
Switch(config-if)# switchport trunk allowed vlan remove vlan-list
Switch(config-if)# switchport trunk allowed vlan add vlan-list
```

La primera línea indica el acceso al puerto que se desea troncalizar, una vez, estando en el modo de configuración del puerto, se activa el modo troncal. El Trunking agrega a la trama un encabezado que lo identifica. Este encapsulamiento se puede dar de dos formas ISL (Inter.-Switch Link Protocol) o el dot1Q (IEEE 802.1Q). EL ISL es un protocolo propietario de CISCO que permite la comunicación de VLANs troncalizada, únicamente con dispositivos de dicha compañía. El dot1Q es referente a la estandarización de VLANs troncalizadas entre dispositivos de diferentes vendedores, establecido por la IEEE.

Generalmente en los Switches CISCO 1900 en adelante, las VLANs vienen troncalizadas en una lista de (1 -1005), por ello se borra dicha lista y se agregan las VLANs que se desean troncalizar. Esto se realiza con las dos últimas líneas de

comando. Si se desean más troncales se puede repetir este proceso cambiando el puerto.

El número de puertos configurados como troncales está limitado por la tecnología del Switch, generalmente se pueden configurar 6 puertos troncalizados a 100Mbps full duplex y 2 a 1000Gbps.

Otras compañías como 3COM y AVAYA poseen una interfaz de configuración mucho más amable y sencilla, incluso en formato de WEB. Sin embargo, esta configuración por líneas de comandos genera mayor seguridad a intromisión.

Nota:

Dado que las VLANs es un método de segmentación de broadcast, estas no se ven entre sí, para lograr conectividad entre las VLANS se debe utilizar uno o más Routers (según la cantidad de Puertos Ethernet que estos posean, la cual debe ser la misma que la cantidad de VLANs, y cada uno de éstos debe estar asignado a una de las VLANs).

3. OPERACIÓN CONTINUA

El termino de operación continua en redes cobra cada vez más importancia entre los inversionistas y diseñadores de red. Algunas empresas y negocios han decidido tener una infraestructura conjunta, integrando voz y datos, es por ello que se requiere de una disponibilidad de red normal las 24 horas del día, los 31 días del mes, los 12 meses del año, para que esta idea integral de servicios tenga sentido.

Algunas personas piensan que una disponibilidad del 99% en su red, es demasiado alta e imposible de alcanzar, que con un 90% está bien; pero, si vemos, una disponibilidad del 99%, nos deja fuera por lo menos 3.65 días del año. Si esta empresa es un banco, una planta de procesos críticos, un servidor de la bolsa de valores, entre otras aplicaciones, esta meta de disponibilidad puede resultar ineficiente y peligrosa, ya que se pueden perder transacciones, el control de algún reactor e incluso el dinero de un personal. Esto nos lleva a establecer metas más claras en la disponibilidad de nuestra red y mirar cuales deben ser las condiciones para poder lograrlo.

Veamos una tabla de disponibilidades.

Disponibilidad(%)	Referencia	Tiempo promedio fuera de servicio por año.
90.000	Un-9	876H (36.5D)
99.000	Dos-9s	87.6H (3.65D)
99.900	Tres-9s	8.76H
99.990	Cuatro-9s	52.56M (< 1H)
99.999	Cinco-9s	5.25M

Tabla 4. Disponibilidad de una red

Una disponibilidad de 99.99% se traduce en 52.56 minutos fuera de servicio en promedio en el año.

Teniendo en mente el criterio de disponibilidad y el objetivo de los cuatro 9s (99.99%), se deben realizar inversiones en equipos de red con características tales como:

- ❑ Fuentes de poder redundantes
- ❑ Módulos de administración (Software de Monitoreo y accesos remotos)
- ❑ Módulos Hot-Swappable (cambios en Caliente)
- ❑ Sistema de monitoreo y administración de temperatura interna
- ❑ Sistema de reporte de fallos
- ❑ Administración distribuida

- Redundancia Física, Equipos y Enlaces.

Algunas de las técnicas importantes de operación continua han sido estudiadas, por medio del Trunking si un medio físico falla, se redistribuyen las estaciones de trabajo a los medios que quedaron activos sin la interrupción de la comunicación entre segmentos; el balanceo de cargas en servidores, también ayuda a la operación continua del mismo, en dicho caso que alguna tarjeta de red falle, este servidor no quedará por fuera de la misma.

Estos servidores utilizan dos o más tarjetas de red (NIC). Una de ellas opera como primaria y la otra como Standby o Trunking. Estas tarjetas utilizan drivers SHDs (Self Healing Drivers). Cuando el SHDs detecta una condición de falla, la NIC en standby asume el perfil de configuración y el tráfico de red de la NIC que ha fallado. El evento toma menos de un segundo y es transparente al usuario.

3.1. SELECCIÓN DEL CENTRO DE CABLEADO

Una de las primeras decisiones que se debe tomar al planificar una red es la ubicación del centro de cableado, pues es allí donde se instalan la mayoría de los cables y los dispositivos de red.

Por ello el estándar ANSI/TIA/EIA-569-A define algunas variables que serán expuestas mas adelante, estas le ayudarán a elegir el mejor sitio para su centro de cableado.

Un centro de cableado bien organizado y ubicado, ayuda de gran manera a la gestión, administración de equipos y al mantenimiento preventivo, dichos conceptos pertenecen a los criterios de operación continua.

La administración de equipos permite el cambio de equipos o módulos que han tenido fallas, por otros que se encontraban en reservas. El mantenimiento preventivo como su nombre lo indica previene futuras fallas, algunas LAN's le restan importancia viéndose en la necesidad de reestructurar su closet de comunicaciones por desorden y falla en los equipos.

Se recomienda establecer varios centros de cableado en un campus amplio, aunque parezca irónico, con la caída de las torres gemelas, muchos pensaron que el sistema se reanudaría en un mes quizá, pero al tercer día ya estaba en operación, pues ellos poseían redundancia física de equipos, es decir que la información que se manejaba en los servidores de la bolsa de New York simultáneamente se procesaba en diferentes sitios de la ciudad. La inversión en el centro de cableado depende del valor de la información que usted desea proteger, tan valiosa como sea su información, será su inversión.

3.1.1. TAMAÑO

El área debe ser lo suficientemente espaciosa como para alojar todo el equipo y el cableado que allí se colocará, se debe incluir espacio adicional para adaptarse al futuro crecimiento, pues es el punto central donde llega el tendido horizontal del cableado estructurado. Una LAN pequeña necesita solamente un espacio del tamaño de un archivador grande, mientras que una LAN de gran tamaño necesita una habitación completa.

Tamaño recomendado para el armario para cableado (basado en 1 estación de trabajo por 10 metros cuadrados)			
Área de servicio		Tamaño del armario para cableado	
(m)²	(ft)²	(m)²	(ft)²
1000	10000	3.0 x 3.4	10 x 11
800	8000	3.0 x 2.8	10 x 9
500	5000	3.0 x 2.2	10 x 7

Tabla 5. Tamaño del Centro de cableado

El estándar TIA/EIA-569 especifica que cada piso deberá tener por lo menos un centro de cableado y que por cada 1000 m² se deberá agregar un centro de cableado adicional, cuando el área del piso cubierto por la red supere los 1000 m² o cuando la distancia del cableado horizontal supere los 90 m.

Un centro de cableado espacioso ayuda a los técnicos de mantenimiento a detectar más rápidamente problemas en la red y de esta forma tomar las medidas adecuadas. Asimismo permite orden en los cables hacia los equipos, se pueden determinar las distancias del cable por conductos o cable libre como se le conoce, previendo futuras ampliaciones.

3.1.2. MATERIALES PARA PAREDES, PISOS Y TECHOS

El piso debe soportar la carga mínima especificada de 4.8 kPA (100 lb/ft²), en caso de que sea un Distribuidor principal (MDF), si es un Distribuidor intermedio (IDF) el piso debe poder soportar una carga mínima de 2.4 kPA (50 lb/ft²).

Siempre que sea posible, la habitación deberá tener el piso falso a fin de poder instalar los cables horizontales entrantes que provienen de las áreas de trabajo. Si esto no fuera posible, deberá instalarse una bandeja portacables de 30,5 cm de ancho en una configuración diseñada para soportar todo el equipamiento y el cableado propuesto. El piso deberá estar revestido de cerámica o de cualquier otro tipo de superficie acabada. Esto ayuda a controlar el polvo y protege al equipo de la electricidad estática. En los centros de cableado se debe aspirar en lugar de barrer, para evitar poner en suspensión partículas de polvo que caerán en los equipos evitando su correcto funcionamiento.

Un mínimo de dos paredes se debe cubrir con madera terciada A-C de 20mm que tenga por lo menos 2,4 m de alto. Además se deben usar materiales de prevención de incendios que cumplan con todos los códigos aplicables (por ej., madera terciada resistente al fuego, pintura retardante contra incendios en todas las paredes interiores, etc.) en la construcción del centro de cableado.

Los techos de las habitaciones no deben ser techos falsos. Si no se cumple con esta especificación se debe proceder a instalar una malla o verja metálica para prevenir la entrada a intrusos y ladrones, previendo la seguridad en caso que sea necesario.

3.1.3. TEMPERATURA Y HUMEDAD

El centro de cableado deberá incluir suficiente, ventilación o aire acondicionado como para mantener una temperatura ambiente de aproximadamente 21°C cuando el equipo completo de la LAN esté funcionando a plena carga.

No deben existir cañerías de agua ni de vapor que atraviesen o pasen por encima de la habitación, salvo un sistema de rociadores, en caso de que los códigos locales de seguridad contra incendios así lo exijan. Se deberá mantener una humedad relativa a un nivel entre 30% y -50%, en zonas con altos niveles de humedad se emplean sistemas de refrigeración para la reducción de la misma.

Si no se cumplen estas especificaciones se pueden corroer los hilos del cableado UTP y de los equipos activos, reduciendo la eficiencia del funcionamiento de la red.

3.1.4. PREVENCIÓN DE INUNDACIONES

Los closets de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe existir riesgo de ingreso de agua, por esto deben estar alejados de regaderas o tuberías, en caso de existir algún peligro de inundación, se debe proporcionar drenaje de piso. De haber regaderas contra incendio, estas deben ser de espuma o de CO₂, con el fin de prevenir el incendio y la integridad del equipo.

3.1.5. ILUMINACIÓN Y TOMACORRIENTES

Se debe tener como mínimo dos receptáculos para tomacorrientes dúplex de CA, dedicados, no conmutados, ubicados cada uno en circuitos separados. También se debe contar por lo menos con un tomacorriente dúplex ubicado cada 1,8 m a lo largo de cada pared de la habitación, debe estar ubicado a 15cm por encima del piso. Se deberá colocar un interruptor de pared que controle la iluminación principal de la habitación en la parte interna, cerca de la puerta.

Se debe evitar el uso de iluminación fluorescente en el recorrido del cable debido a la interferencia externa que genera, pero se puede utilizar en centros de cableado si la instalación es adecuada. Los requisitos de iluminación para un centro de telecomunicaciones especifican un mínimo de 500 lx (brillo de la luz equivalente a 50 bujías-pie) y que los dispositivos de iluminación se eleven a un mínimo de 2,6 m por encima del nivel del piso.

3.1.6. SEGURIDAD

- ❑ Mantener el cuarto de telecomunicaciones con llave en todo momento.
- ❑ Asignar llaves a personal que esté en el edificio durante las horas de operación.
- ❑ Es necesario proveer extintores de fuego portátiles y hacerles mantenimiento periódicamente. Estos deben ser instalados tan cerca a la puerta como sea posible.

3.2. CONSIDERACIONES ELÉCTRICAS

Una gran preocupación es la continuidad del fluido eléctrico y la calidad del mismo. Gran parte de la condición de operación continua sobrecarga en la

disponibilidad eléctrica, pues ha sido el gran temor de todos a la hora de integrar la voz por el sistema estructurado de los datos, la penuria parte de la premisa, Si falla el fluido eléctrico en una red LAN integrada, ¿Cómo nos comunicamos?

En el diseño de redes de operación continua este punto es el de mayor interés, de aquí depende toda la infraestructura de la LAN, pues sino hay energía, no hay redundancia, trunking o centro de cableado que trabaje.

Es necesario que toda red de área local posea una fuente de alimentación ininterrumpida (UPS) ya que no sólo garantiza la operación continua de los sistemas, sino que, también elimina otros problemas como lo son los sobrevoltajes, picos y transitorios.

Uno de los factores que hay que cuidar en las redes, es la calidad de la energía, esta se encuentra estrictamente ligada con el problema de los armónicos y el ruido.

Los armónicos degeneran la señal de alimentación que llega a nuestros hogares o centros de trabajo, agregando componentes en frecuencias armónicas de la señal.

Surgen como consecuencia del alto uso de elementos activos (semiconductores) de potencia como Transistores, Tiristores, entre otros dispositivos que manejan el flujo de la señal de alimentación. Estos dispositivos son usualmente utilizados en

plantas de control de procesos industriales, donde se necesita accionar elementos de alto consumo de corriente, como es el caso del arranque de motores o generadores. A su vez, el uso de cargas Inductivas en la red, degeneran el factor de potencia de la misma. Una recomendación vital es separar los hilos de alimentación de las cargas de este tipo, de las líneas de alimentación de los equipos de red.

El ruido de la línea de alimentación de CA, agrega voltajes no deseados a las señales deseadas e impide que las compuertas lógicas de un computador por ejemplo, no puedan detectar los bordes anterior y posterior de las ondas rectangulares de la señal generando problemas en la información.

En definitiva, el encendido abrupto de los motores de una planta ó del aire acondicionado por ejemplo, degrada la vida útil de los switches, PC's y demás dispositivos. En efecto se hace necesario, el uso de UPS, poseer protección a sobrevoltaje, Sobre corrientes y una adecuada puesta a tierra para evitar fluctuaciones en la señal de alimentación alterna.

Otro de los grandes problemas en el entorno eléctrico de las redes, son las descargas electroestáticas, estas pueden destruir semiconductores y datos al azar, a medida que el computador recibe los impactos eléctricos.

3.2.1. CONEXIÓN A TIERRA

La conexión a tierra constituye el voltaje de referencia, o sea, cero voltios. Todos los voltajes son mediciones de potenciales eléctricos, desde un punto con respecto a otro; normalmente son con respecto a la tierra.

El propósito de la conexión a tierra es más por razones de seguridad, que por motivos de referencia de potencial, la idea es impedir que las partes metálicas de los equipos informáticos se carguen con voltaje y lo descarguen a través de una persona o dispositivos electrónicos.

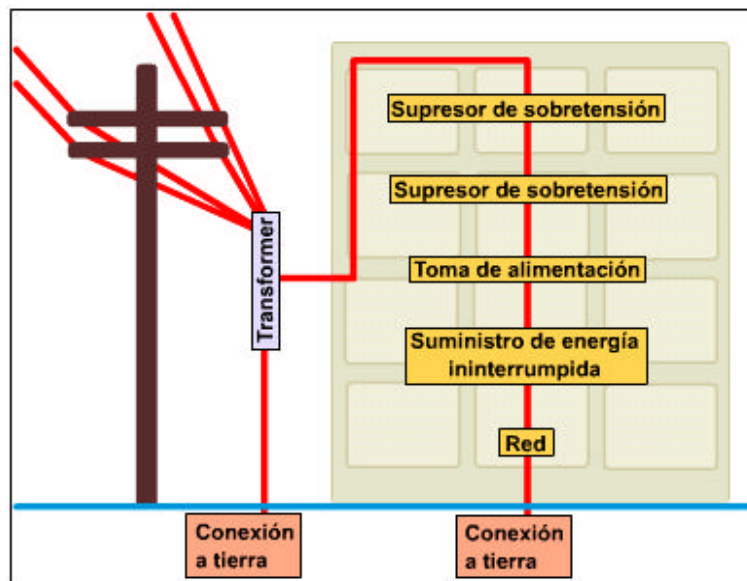


Figura 21. Conexión a Tierra de un equipo de Red

En la figura 17 se ilustra como debe ser la conexión de alimentación dentro de una red LAN, destacando las conexiones a tierra y las protecciones (serán detalladas más adelante).

En edificios distantes involucrados en la red, generalmente se necesitan más de una conexión a tierra, pero se requiere que estas conexiones a tierra se encuentren unificadas. Infortunadamente, la conexión a tierra entre varios campos casi nunca es igual. Las conexiones a tierra separadas dentro de un mismo lugar también pueden variar por las condiciones del terreno.

Esta diferencia de potencial puede producir un flujo de corriente entre las distintas conexiones a tierras, dañando los dispositivos y poniendo en riesgo la vida de los usuarios de la red.

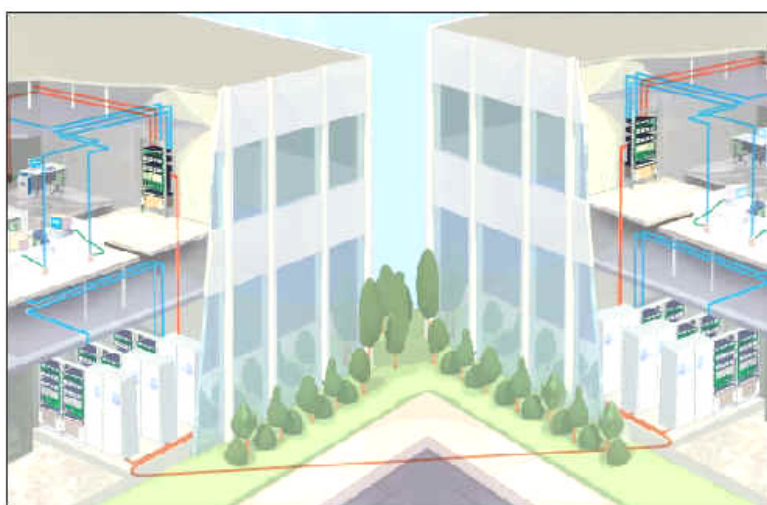


Figura 22. Cable de Fibra Óptica como Backbone entre edificios

Las especificaciones del estándar TIA/EIA-568-A para el cableado backbone permiten el uso de cable de fibra óptica así como de cable UTP.

Como el vidrio es un aislador, más que un conductor, la electricidad no viaja a través de los cables de fibra óptica. Por lo tanto, cuando se va a realizar la conexión en red de múltiples edificios o en circunstancias donde se tienen problemas con la conexión a tierra, se aconseja enfáticamente usar cable de fibra óptica para los enlaces.

A menudo se le resta importancia a las conexiones a tierra, pero la seguridad de una red depende de ella, por eso es ineludible realizar un buen diseño e implementación, sin escatimar en gastos, recuerde que se están protegiendo elementos costosos y la disponibilidad de un servicio, cuyo valor no se puede estimar.

Antes de implementar, se deben estudiar las condiciones del terreno y explorar los cambios que pueden resultar en un determinado tiempo. La conexión a tierra no es una simple varilla de cobre, en ocasiones se hace necesario colocar una estructura en malla de cobre y adecuar el terreno para una buena conexión a tierra cuya resistencia no sea superior a los 5Ω .

3.2.2. SOLUCIÓN PARA PROBLEMAS DE SOBREVOLTAGES

Un sobrevoltaje es el aumento en el voltaje por encima del 110% del normal transportado por la línea de alimentación eléctrica. Generalmente, estos incidentes

duran sólo unos pocos segundos, sin embargo, este tipo de disturbio eléctrico es responsable de casi todos los daños en elementos activos.

Los suministros de energía eléctrica de los equipos de red que operan a 120 V no están preparados para manejar 260 V ni siquiera por periodos instantáneos de tiempo. Los hubs son particularmente vulnerables a los sobrevoltajes debido a sus líneas de datos de bajo voltaje, que son sumamente sensibles.

En condiciones de sobrevoltaje es común encontrar otro tipo de perturbación conocida como pico. Un pico es un impulso que genera una sobrecarga de voltaje en la línea de alimentación eléctrica. Habitualmente, los picos duran entre 0,5 y 100 microsegundos. Existen numerosas fuentes de picos, la más común son los rayos.

De la misma forma, las operaciones de conmutación realizadas por la compañía local de energía eléctrica también pueden provocarlos. Otras fuentes pueden ser, los ciclos de equipamientos como ascensores, fotocopiadoras y aparatos de aire acondicionado.

Las consecuencias pueden ser graves. Entre las que podemos mencionar las siguientes:

- Bloqueos

- ❑ Pérdida de memoria
- ❑ Problemas para recuperar los datos
- ❑ Datos alterados
- ❑ Datos dañados o "basura"

Una solución común es el uso de *supresores de sobrevoltaje*. Este tipo de supresor posee un sistema de circuitos diseñados basados en un dispositivo llamado *varistor de metal-óxido (MOV)*. Un MOV protege los dispositivos de red dirigiendo los voltajes excesivos, que se producen durante los sobrevoltajes y los picos de voltaje, hacia una conexión a tierra.

Los supresores de sobrevoltaje se utilizan para conectar aquellos equipos o estaciones de trabajo de la red cuya operación continua no es crítica y no se poseen los recursos para protegerlos con una UPS.



Figura 23. Supresor de Picos y Sobrevoltajes

Desafortunadamente, un MOV puede no resultar un medio efectivo para proteger los dispositivos conectados a él. La descarga de voltajes excesivos en la línea de alimentación eléctrica cercana al PC puede provocar una elevación del potencial de conexión a tierra. Las diferencias resultantes en los voltajes de conexión a tierra pueden hacer que la corriente eléctrica fluya por el circuito de conexión a tierra. El flujo de corriente en una malla de tierra puede dañar los dispositivos no protegidos; por lo tanto, en cualquier instalación de LAN, una buena regla a seguir es proteger todos los dispositivos de red.

3.2.3. SOLUCIÓN A LOS CORTES Y BAJAS DE TENSIÓN

Una baja de voltaje es un corte parcial que dura menos de un segundo. Estos incidentes ocurren cuando el voltaje de la línea de alimentación eléctrica cae por debajo del 80% del voltaje normal. A veces son provocadas por circuitos sobrecargados. Los cortes de la tensión pueden ocurrir por mantenimiento de la empresa prestadora de estos servicios o problemas de la alimentación eléctrica del edificio.

La solución a este tipo de problema es proveer a la red LAN de un sistema continuo de alimentación o UPS. Un UPS se compone de una serie de baterías, un cargador de batería y un inversor de energía eléctrica (de CC a CA).

En una UPS continua el inversor de voltaje (Convertor DC-AC) funciona todo el tiempo mientras el circuito cargador mantiene cargada la batería, esto le brinda la ventaja al sistema de que no recibe la alimentación del suministro externo, protegiendo así el dispositivo de los picos, sobrevoltajes y bajas de tensión.

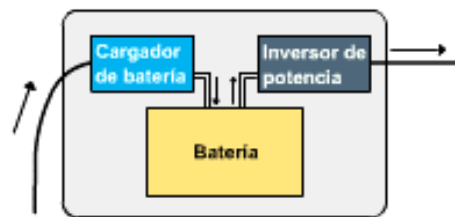


Figura 24. UPS Continua

Como mínimo, cada servidor de archivo de red debe tener una fuente de energía UPS de respaldo. En redes con topología en estrella extendida, donde se utilizan dispositivos de red tales como Switches y Routers, se debe garantizar de igual manera el fluido eléctrico a fin de evitar fallas en el sistema. En lo posible, se debe respaldar a todas las áreas de trabajo, como bien saben los administradores de red, no sirve de nada tener un servidor operacional y un buen sistema de cableado, si no se puede garantizar el flujo continuo de los datos.

3.2.4. SOLUCIÓN PARA LAS OSCILACIONES

Las oscilaciones son generalmente causadas por un tendido de cableado eléctrico demasiado largo, lo que crea un efecto de antena captando señales de radio frecuencia.

La mejor forma de tratar el problema de las oscilaciones es realizando un nuevo cableado. A pesar de que esta solución puede parecer extrema y costosa, probablemente es la única forma confiable de garantizar conexiones a tierra y de alimentación eléctrica totalmente limpia y directa.

3.2.5. PROTECCIÓN CONTRA RAYOS

Como ya se ha estudiado, los rayos representan una de las fuentes primarias de los disturbios eléctricos, es por eso que se hace necesario que toda red LAN posea este tipo de protección.

Los tipos de pararrayos más comunes son los de tipo de punta de Franklin, ionizados y Radioactivos. Estos últimos se encuentran prohibidos por leyes de protección ambiental.

Los pararrayos ionizados operan ionizando el medio circundante, facilitando de esta forma la descarga de rayos con voltajes que la conexión a tierra pueda manejar. Por esta razón se recomiendan su uso por encima que los de punta de Franklin a pesar de ser más costosos.

3.3. REDUNDANCIA EN REDES

En el contexto de las redes, la redundancia se refiere a la capacidad que tiene la misma para enfrentar cualquier falla que se presente en el sistema, con el uso duplicado de equipos y enlaces sin afectar la operación continua. Esta puede ser tanto física como lógica (en el caso del Resilient), a continuación realizaremos un análisis de las técnicas utilizadas para llevar a cabo este diseño.

3.3.1. REDUNDANCIA DE EQUIPOS

Tener equipos redundantes implica poseer una copia en standby del equipo que se desea reemplazar en caso de que este se averíe. Los equipos que comúnmente son redundados son los elementos core de la red (nucleo), como servidores, switches y routers.

Se debe poseer un stock de equipos en el sitio de trabajo (Closet de Comunicaciones). Esta modalidad es conocida como redundancia *in situ* y ofrece la ventaja de disponibilidad inmediata en caso necesario de reemplazar al equipo defectuoso. Muchos proveedores ofrecen esta característica como parte de sus paquetes de suministro de equipos. Este servicio incluye (en la mayoría de la empresas) la reposición del equipo utilizado en un plazo menor a 24 horas.

3.3.2. REDUNDANCIA DE ENLACES

En una red deben ser redundados los enlaces, este principio fue adoptado de Internet, pues, la idea de esta red global es conectar dos puntos independientemente de la ruta que se tome. Se emplean dos modalidades, el uso de enlaces en reserva (Resilient) y la agregación de enlaces (Trunking). [2.4.3]

Existen tres puntos críticos a fallas en la red, los nodos, las conexiones de los servidores y el cableado vertical.

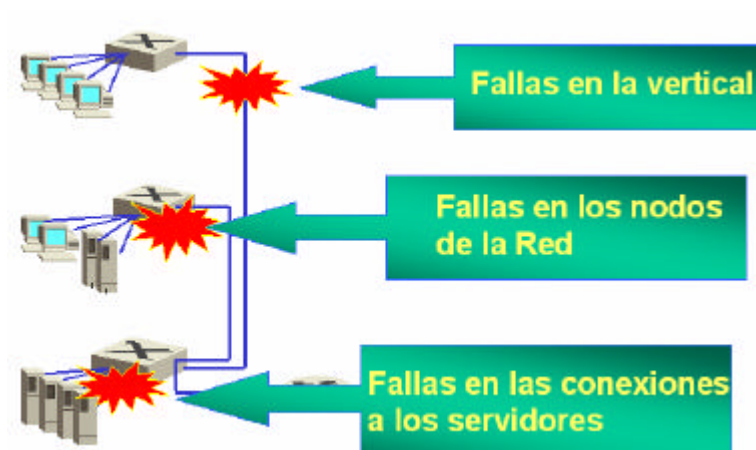


Figura 25. Fallas comunes en los enlaces de la red

El resilient es la técnica mediante la cual se configuran dos enlaces redundantes, el tráfico se mantiene fluyendo a través del enlace activo, mientras el segundo enlace permanece como backup. Cuando ocurre una falla en el enlace principal, el enlace preconfigurado como backup, se activa y acomoda todo el flujo de tráfico.



Figura 26. Enlaces Resilient entre switches

Los enlaces resilient en Switches protegen la red contra la falla de un enlace individual, previendo un enlace secundario que permanece inactivo hasta que sea requerido. El tiempo de transferencia del enlace toma menos de 1 segundo.

Bajo condiciones normales de operación el enlace principal transporta los datos, el Switch monitorea constantemente la señal Test Pulse en al caso de UTP o la señal Receive Idle en el caso de la fibra óptica. Si se detecta la pérdida de la señal, el software interno del Switch habilita inmediatamente el segundo enlace o enlace Standby, el cual se encarga de los datos, adicionalmente el Switch envía una alerta a la estación de monitoreo de la red.

Existen dos tipos de configuración de los enlaces resilient Single-Home y Dual-Homed.

En el single-Homed se tiene el enlace principal y el redundante conectado al mismo Switch. Este modo de operación garantiza el funcionamiento continuo de la red con fallas en el medio únicamente.

El método Dual-Homed el enlace principal y el redundante están conectados a Switches diferentes, protegiendo la red contra fallas en el enlace y en el Switch.

El mismo esquema se aplica para enlaces resilients en servidores. Como se puede apreciar en la Figura 27.

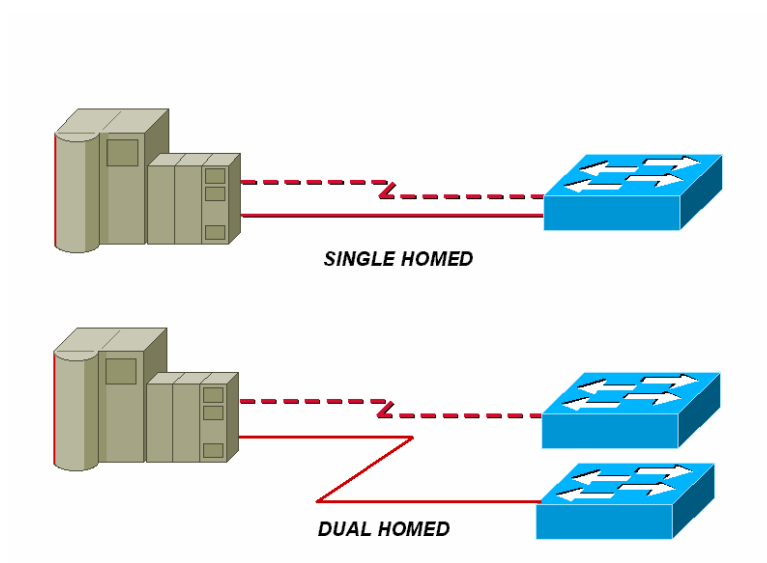


Figura 27. Enlaces Dual-Homed y Single Homed en Servidores

4. CONCLUSIONES Y RECOMENDACIONES

En el presente trabajo se desarrollaron las técnicas necesarias que mejoran el rendimiento del ancho de banda en una red de área local, técnicas establecidas de acuerdo a las consideraciones y estándares promovidos por entidades como IEEE, ANSI, EIA y TIA. Es necesario que nuestra red LAN posea una alta escalabilidad a futuras tecnologías, con una inversión ligera y pocos cambios en la infraestructura existente.

El medio físico es una de las variables que define la vida útil de la red, pues, la evolución en las tecnologías parte de la premisa de tener un cable cada vez más fiable y que brinde mejores prestaciones. El UTP ha desarrollado categorías, donde la CAT. 6 ha dejado atrás a la ya olvidada CAT. 5. La CAT. 5E sin embargo, se encuentra irrigada en el medio comercial, pero una fuerte recomendación es prever en futuros diseños e implementaciones el uso de CAT.6 y de fibra óptica. El progreso de estos medios ha eliminado en un alto porcentaje los problemas de diafonía y el ruido, teniendo un impacto positivo sobre el precio de las tarjetas, haciendo que estas posean una electrónica de componentes menos robustas y con mejores tributos de gestión.

La ejecución de cableado estructurado certificado es crucial para definir el rendimiento LAN, la excelente realización de los patch cords, la ubicación del

cableado y las recomendaciones de distancia constituidas por los estándares, ayudan de gran forma a que su red no tenga problemas de colapsos.

Otro aspecto significativo en el mejoramiento del ancho de banda, es elegir los mejores elementos comprometidos con las técnicas de control de acceso al medio. La buena selección de la tarjeta de red evita que se incurra en gastos innecesarios pensando que una tarjeta de mayor velocidad va tener un efecto significativo en la red. Para esto, se tiene que ver cual va ser su aplicación y su necesidad en la terminal donde se va a colocar, pues las velocidades por segmentos de la red no sólo dependen de la tarjeta, sino de un conjunto de elementos activos como el caso de los switches y si estos son configurables.

No sólo se debe garantizar que una red trabaje a su wirespeed o máximo caudal de bits permitidos, también se debe asegurar que no se tengan interrupciones por fallas en los dispositivos o colapsos en los backbones.

Por esta consideración surgen técnicas como el Trunking que descongestionan y aumentan el rendimiento del canal, tanto como su dinero y su necesidad lo demande. Además ayuda a la operación continua y evita posibles colapsos en servidores, eliminando los comúnmente conocidos cuellos de botella.

La redundancia a su vez garantiza la operación continua de los enlaces críticos de la red tales como los enlaces resilient.

En últimas el presente documento muestra que el montaje de una red no sólo depende de la adquisición de equipos costosos y el uso de un buen cableado, sino que requiere el empleo de técnicas específicas con el fin de aprovechar al máximo los recursos de la red y ofrecer un excelente ancho de banda, a la vez que se garantiza una disponibilidad cercana al 100%.

Cabe anotar que el mejoramiento de ancho de banda sobre cae principalmente en las capas 1 y 2 del modelo OSI, podemos decir que de la capa 3 en adelante las decisiones que se establecen pertenecen mas a criterios de software. Sin embargo estableciendo buenas políticas de enrutamiento, sistemas de transporte, mejorando el formato de los archivos y las técnicas de compresión, se puede obtener un mejor rendimiento y aprovechamiento de los recursos que se poseen en la red. Esta premisa deja abierta la expectativa de ahondar en otras técnicas de mejoramiento del ancho de banda en capas superiores, así como, la redundancia de enlaces inalámbricos, Switches de enrutamiento a alta velocidad, mejoras en los códigos de programación y el empaquetamiento de datos, teniendo como finalidad el descongestionamiento del tráfico en la red de manera más lógica que física.

Es necesario para el buen provecho de esta investigación poseer conocimientos en diseño de redes LAN, de no ser así, es indispensable que utilice la ayuda del glosario y del índice general. Si desea más información puede profundizar con la bibliografía citada o consultar sitios WEB.

5. GLOSARIO DE TERMINOS

Almacenamiento y envío

Técnica de conmutación de paquetes en la que las tramas se procesan completamente antes de enviarse al puerto apropiado. Este procesamiento incluye calcular el CRC y verificar la dirección destino. Además, las tramas se deben almacenar temporalmente hasta que los recursos de la red (como un enlace no utilizado) estén disponibles para enviar el mensaje.

Ancho de banda

Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

Aprendizaje de la dirección MAC

Servicio que caracteriza a un switch de aprendizaje en el que se guarda la dirección MAC origen de cada paquete recibido, de modo que los paquetes que se envían en el futuro a esa dirección se pueden enviar solamente a la interfaz de switch en la que está ubicada esa dirección. Los paquetes cuyo destino son direcciones de broadcast o multicast no reconocidas se envían desde cada interfaz de switch salvo la de origen. Este esquema ayuda a reducir el tráfico en

las LAN conectadas. El aprendizaje de las direcciones MAC se define en el estándar IEEE 802.1.

ARP (Protocolo de Resolución de Direcciones)

Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826. Comparar con RARP.

Atenuación

Pérdida de energía de la señal de comunicación

Backbone

Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Balanceo de la carga

En el enrutamiento, la capacidad de un router para distribuir el tráfico a lo largo de todos sus puertos de red que están a la misma distancia desde la dirección destino. Los buenos algoritmos de balanceo de carga usan velocidad de línea e información de confiabilidad. El balanceo de carga aumenta el uso de segmentos de red, aumentando así el ancho de banda efectivo de la red. El mismo principio es aplicado en servidores y switches programables.

Banda ancha

Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

Bit

Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno.

Broadcast

Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast.

Búfer de memoria

área de la memoria donde el switch almacena los datos destino y de transmisión.

Cable de fibra óptica

Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

Cableado backbone

Cableado que brinda interconexiones entre los armarios de cableado, entre los armarios de cableado y el POP, y entre edificios que forman parte de la misma LAN

Capa de enlace de datos

Capa 2 del modelo de referencia . Esta capa proporciona un tránsito de datos confiable a través de un enlace físico. La capa de enlace de datos se ocupa del direccionamiento físico, topología de red, disciplina de línea, notificación de errores, entrega ordenada de las tramas y control de flujo. IEEE dividió esta capa en dos subcapas la subcapa MAC y la subcapa LLC. A veces se denomina simplemente capa de enlace. Corresponde aproximadamente a la capa de control de enlace de datos del modelo SNA.

Capa de red

Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es la capa en la que se produce el enrutamiento. Equivale aproximadamente a la capa de control de ruta del modelo SNA.

Capa física

Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Corresponde a la capa de control físico del modelo SNA.

Carga

Cantidad de actividad de un recurso de la red, como por ejemplo un router o un enlace.

Colisión

En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Conexión a tierra de referencia de señal

Punto de referencia que usan los dispositivos informáticos para medir y comparar las señales digitales entrantes. Punto de referencia que usan los dispositivos informáticos para medir y comparar las señales digitales entrantes.

Conexión punto a multipunto

Uno de dos tipos fundamentales de conexión. En ATM, una conexión punto a multipunto es una conexión unidireccional en la cual un solo sistema final de

origen (denominado nodo raíz) se conecta a múltiples sistemas finales de destino (denominados hojas). Comparar con conexión punto a punto.

Conexión punto a punto

Uno de dos tipos fundamentales de conexión. En ATM, una conexión punto a punto puede ser una conexión unidireccional o bidireccional entre dos sistemas finales ATM. Comparar con conexión punto a multipunto.

Congestión

Tráfico que supera la capacidad de la red.

Conmutación

Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

CSMA/CD (Acceso múltiple con detección de portadora y detección de colisiones)

Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos

dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

Dirección broadcast

Dirección especial reservada para enviar un mensaje para todas las estaciones. Por lo general, una dirección broadcast es una dirección destino MAC compuesta exclusivamente por números uno. Comparar con dirección multicast y dirección unicast.

Dirección de red

Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo

Dirección IP

Dirección de 32 bits asignada a los hosts mediante TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet (dirección IP)

Dirección MAC (Control de Acceso al Medio)

Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

Dominio de broadcast

Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo dentro de ese conjunto. Los dominios de broadcast normalmente se encuentran limitados por routers porque los routers no envían tramas de broadcast.

Dominio de colisión

En Ethernet, el área de la red en la que las tramas que colisionan se propagan. Los repetidores y los hubs propagan las colisiones, mientras que los switches de LAN, puentes y routers no lo hacen..

EIA/TIA568

Estándar que describe las características y aplicaciones para diversos grados de cableado UTP.

Encapsular

Colocar un encabezado de protocolo en particular a los datos. Por ejemplo, a los datos de Ethernet se les agrega un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red simplemente se coloca en el encabezado utilizado por el protocolo de enlace de datos de la otra red.

Escalabilidad

Capacidad de una red para aumentar de tamaño sin que sea necesario realizar cambios importantes en el diseño general.

Ethernet

El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

Fast Ethernet

Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de

administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

Fibra óptica

Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda electromagnética generada por un láser.

Full dúplex

Capacidad para la transmisión simultánea de datos entre la estación emisora y la estación receptora. Comparar con semidúplex y unidireccional.

Host

Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

Hub

1. En general, dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto.
2. Dispositivo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Los hubs pueden ser

activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

Interfaz

1. Conexión entre dos sistemas o dispositivos.
2. En terminología de enrutamiento, una conexión de red.
3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas.
4. Límite entre capas adyacentes del modelo de referencia OSI.

Internetwork

Industria dedicada a la conexión de redes entre sí. Este término se refiere a productos, procedimientos y tecnologías.

LAN (red de área local)

Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos

del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas. Comparar con MAN y WAN.

Latencia

Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

Máximo esfuerzo de entrega

Entrega que se produce cuando un sistema de red no usa un sistema sofisticado de acuse de recibo para garantizar la entrega confiable de la información.

Multicast

Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

Networking

Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres y CD-ROM) y otros dispositivos.

NIC (tarjeta de interfaz de red)

Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

No orientado a conexión

Transferencia de datos sin un circuito virtual. Comparar con orientado a conexión.

Orientado a conexión

Transferencia de datos que requiere que se establezca un circuito virtual.

Paquete

Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

QoS (calidad de servicio)

Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

Red

Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red híbrida

Internetwork de redes compuesta por más de un tipo de tecnología de red, incluyendo LAN y WAN.

Redundancia

1. En internetwork, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla.
2. En telefonía, la porción de la información total contenida en un mensaje que se puede eliminar sin sufrir pérdidas de información o significado esencial.

Retardo

Tiempo entre la iniciación de una transacción por parte del emisor y la primera respuesta recibida por éste. Asimismo, el tiempo requerido para mover un paquete desde el origen hasta el destino en una ruta dada.

Router

Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

Segmentación

Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

Segmento

Sección de una red que está rodeada de puentes, routers o switches 2. En una LAN que usa topología de bus, un circuito eléctrico continuo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Servidor

Nodo o programa de software que suministra servicios a los clientes.

Spanning tree

Subconjunto sin bucles de una topología de red de Capa 2 (conmutada).

Switch

Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

Los switches son más “inteligentes” que los “Hubs” y ofrecen un ancho de banda más dedicado para los usuarios o grupos de usuarios. Un switch envía los paquetes de datos solamente a la computadora correspondiente, con base en la información que cada paquete contiene. Para aislar la transmisión de una computadora a otra, los switches establecen una conexión temporal entre la fuente y el destino, y la conexión termina una vez que la conversación se termina.

Switch de LAN

Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches de LAN envían tráfico basándose en las direcciones MAC. Los switches de LAN a menudo se clasifican según el método utilizado para enviar tráfico: conmutación de paquetes por método de corte o conmutación de paquetes por almacenamiento y envío. Un ejemplo de switch de LAN es el Cisco Catalyst 5000.

TCP/IP (Protocolo de Control de Transmisión /Protocolo Internet)

Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años '70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Topología en estrella

Topología de LAN en la que los puntos finales de una red se encuentran conectados a un switch central común mediante enlaces punto a punto. Una topología de anillo que se organiza en forma de estrella implementa una estrella de bucle cerrado unidireccional, en lugar de enlaces punto a punto. Comparar con topología de bus, topología de anillo y topología en árbol.

Tormenta de broadcast

Suceso de red no deseado, en el que se envían varios broadcasts simultáneamente a todos los segmentos de red. Una tormenta de broadcast usa una parte considerable del ancho de banda de la red y normalmente hace que se agoten los tiempos de espera de la red.

Trama

Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama,

mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Unicast

Mensaje que se envía a un solo destino de red.

UTP (par trenzado no blindado)

Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hay cinco tipos de cableado UTP de uso común cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Comparar con STP.

Velocidad asegurada

Rendimiento de datos a largo plazo, en bits o celdas por segundo, que una red ATM puede proporcionar bajo condiciones normales de la red. La velocidad asegurada se encuentra asignada en un 100 por ciento. Se deduce en su totalidad del ancho de banda troncal a lo largo de la ruta del circuito. Comparar con velocidad excesiva y velocidad máxima.

VLAN (LAN virtual)

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

BIBLIOGRAFÍA

- [1]. CISCO SYSTEMS INC. Academia de Networking de Cisco Systems. Guía del Primer Año. Segunda Edición.
- [2]. CISCO SYSTEMS INC. Academia de Networking de Cisco Systems. Guía del Segundo Año. Segunda Edición.
- [3]. DAGA S.A. Tecnología en Redes y Comunicaciones. Catálogo 2002.
- [4]. PANDUIT. Network Connectivity Group. Power Sum ACR.
- [5]. ERICSSON TELECOM AB. ENGINE Access Ramp. Next Generation Network Solutions.
- [6]. ALCATEL. 1000 Softswitch Datasheet.
- [7]. ANIXTER. Whitepaper. “Es el momento de migrar a un cableado de categoría 6/Clase E?”.
- [8]. AVAYA COMMUNICATIONS. Whitepaper. “La Elección del Cableado Estructurado: Una decision Clave Para El Futuro de Cualquier Empresa”.