DISEÑO DE LA RED LAN PARA EL COLEGIO MILITAR JOSE ANTONIO GALAN

YISETH CONTRERAS

JACKSON MARTINEZ M.

ALEJANDRO BUSTOS R.

UNITEC, CORPORACIÓN UNIVERSITARIA.

SANTA FE DE BOGOTA

C.P.G.

DISEÑO DE LA RED LAN PARA EL COLEGIO MILITAR JOSE ANTONIO GALAN

YISETH CONTRERAS

JACKSON MARTINEZ M.

ALEJANDRO BUSTOS R.

DIPLOMADO

EN DISEÑO E IMPLEMENTACION DE REDES LAN Y WAN

INGENIERA

MONICA EDITH GONZALES

Ingeniero de Sistemas - CCNA

UNITEC, CORPORACIÓN UNIVERSITARIA.

SANTA FE DE BOGOTA

C.P.G.

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

TABLA DE CONTENIDO

INTRODUCCION

En un mundo que evoluciona a cada instante, y si nos enfocamos en el campo de la electrónica, vemos que es un factor que incide en la vida diaria de cada ser humano; pues siempre que hay una necesidad aparecerá la electrónica tratándola de satisfacer. Esto nos ha facilitado muchas cosas, nos ha brindado comodidad, seguridad y mayor eficiencia en el desarrollo de actividades tales como, las telecomunicaciones.

Las tecnologías en el ámbito de comunicación interactiva, constituyen la evolución de las telecomunicaciones convencionales. Se transforma la imagen, el audio y los datos en información digital, es decir, en bits (0,1). Al tratarse de una transmisión digital o numérica, se pueden aplicar procesos de compresión y corrección de errores, lo que, por ejemplo, nos permitiría ver una mayor calidad tanto de imagen como de sonido. Facilitando también la transmisión de otros servicios interactivos.

La comunicación en si es un proceso de transmisión y recepción de ideas, información y mensajes. En los últimos 150 años, y en especial en las dos últimas décadas, la reducción de los tiempos de transmisión de la información a distancia y de acceso a la información ha supuesto uno de los retos esenciales de nuestra sociedad. Las nuevas tecnologías de la información basadas en la microelectrónica, junto con otras innovaciones, como la fibra óptica, permiten enormes aumentos de potencia y reducción de costo en toda clase de actividades de procesado de información (el término "procesado de información" cubre la generación, almacenamiento, transmisión, manipulación y visualización de información, que incluye datos numéricos, de texto, de sonido o de vídeo).

Siendo este tema de interés, es el cual se trata a lo largo de este proyecto esencialmente en el ámbito de generar conocimiento en redes LAN pero sin dejar de lado su debida extrapolación para aplicaciones de más profundidad y detalle.

El proyecto tiene por objeto el estudio y análisis de temas relacionados con el diseño de la red LAN para el **colegio militar José Antonio galán**, tales como: Recolección de información, diseño de planos e instalaciones físicas, centros de cableado, topología física y lógica, equipos de Networking, protocolos de comunicación y recomendaciones para el mejor rendimiento de la red.

OBJETIVOS

OBJETIVO GENERAL.

Ofrecer una propuesta que se adapte a las necesidades del colegio militar **José Antonio galán** basándonos en el diseño y análisis de dicha red. Incluyendo aspectos de diseño físico, lógico y niveles de seguridad. Tecnología que se es brindada por la academia de Networking de CCNA Cisco Redes.

OBJETIVOS ESPECIFICOS.

- ✓ Recolectar información sobre las necesidades del colegio, para identificar y definir cualquier problema que pueda tratarse y presentar soluciones para suplirlo.
- ✓ Evaluar la estructura física y lógica de la red.
- ✓ Diseñar el cableado estructurado, ajustándose a los estándares mundiales como: IEEE, EIA/TIA y demás entidades que regulan la convergencia y desarrollo de las redes.
- ✓ Diseñar el esquema de una Red LAN que optimice el nivel de rendimiento en la comunicación de datos e implemente nuevas posibilidades para su crecimiento.
- ✓ Establecer si el rendimiento de la red satisface las necesidades de todos los usuarios.

JUSTIFICACION

El **COLEGIO MILITAR JOSE ANTONIO GALAN** es una institución educativa que presta un servicio a la comunidad del sector de fontibon, por lo cual requiere que se encuentre en capacidad a nivel tecnológico tanto para el aprendizaje de sus alumnos como para desarrollar su propia base de datos.

FACTIBILIDAD

El cambio mas importante propuesto en nuestro proyecto para el **Colegio Militar JOSE ANTONIO GALAN** es la construcción e implementación de una red LAN. Basándonos en el uso del modelo de referencia OSI como estructura jerárquica para el diseño de redes. Junto con la organización, documentación, aplicación de normas en el diseño de la red, podremos gestionar y maximizar el funcionamiento de esta.

Actualmente, en cuanto al estudio y presentación de proyecto no genera costos para la empresa por tratarse de un proyecto de grado.

Podemos decir entonces que la factibilidad de llevar este proyecto a cabo es satisfactorio, ya que la necesidad del colegio por solucionar el problema de comunicación entre dependencias es una necesidad de la institución.

TECNICA: la implementación de una red LAN para el Colegio Militar JOSE ANTONIO GALAN esta basada en el modelo de referencia OSI.

FINANCIERA: podemos utilizar una tecnología inalámbrica que es la Ethernet 802.11 wireless o la Ethernet 802.3 que es la alambrica.

- ✓ La implementación de la primera tecnología la 802.11 es muy costosa ya que toda la red seria inalámbrica pero tendría mucha ventaja referente a la 802.3 ya que no utilizamos cableado y los anchos de banda serian enormes.

- ✓ La implementación de la segunda tecnología la 802.3 como lo dijimos anteriormente es alambrica entonces tendría un ancho de banda limitado pero para un colegio es mas que suficiente

Detodas maneras La inversión que genera la solución propuesta, es grande en lo que a equipos y recurso físico se refiere; ya que actualmente el colegio no cuenta con ningún tipo de red.

CULTURAL: la propuesta de la red LAN del colegio se verían reflejados básicamente en el rendimiento, solidez y estabilidad de la red, generando así una administración, crecimiento y sostenimiento mas fácil, por consiguiente esto implica grandes cambios a nivel de software y hardware para los usuarios, lo cual incurriría en gastos de capacitación de personal. Vemos entonces una buena factibilidad para la implementación de esta propuesta.

PLANTEAMIENTO DEL PROBLEMA

El **Colegio Militar JOSÉ ANTONIO GALÁN**, actualmente es una instalación compuesta físicamente por dos edificios, cada uno de cuatro pisos, cuenta con 35 host, los cuales están repartidos de la siguiente manera:

En el edificio A, esta repartido de la siguiente manera; en el segundo piso la secretaria, la sala de profesores, y la sala de los oficiales en el tercer piso se encuentra la oficina del rector y la del vicerrector. Actualmente solo cuenta con dos host y esta repartido así; para el rector y la secretaria pero para el siguiente año van a colocar host en la sala de profesores, para el vicerrector y también para la sala de los oficiales.

El edificio B, esta organizado de la siguiente manera; el primer piso se encuentra la biblioteca, el segundo piso el régimen interno, la dirección militar y la coordinación académica, cada uno de estas contando con un solo host. El tercer piso se encuentra una sala de sistemas con 16 host, el cuarto piso la otra sala de sistemas contando actualmente con 15 host pero para el siguiente año va a contar con 40 host.

Los alumnos no tienen acceso a Internet de ninguna forma, solo en los host manejan los programas básicos como Windows 98, Excel, Power Point y Word. El único host que cuenta con Internet es el de la secretaria.

Quisimos hacer un estudio a los computadores y a la gran mayoría no les sirve la unidad de CD, la cual es muy necesaria, ya que utilizamos un programa llamado Sandra, que nos brindaría la información correspondiente de cada host.

RESEÑA HISTORICA

El **COLEGIO MILITAR JOSE ANTONIO GALAN** es una institución académica con énfasis en la formación y orientación militar, desde el curso primero elemental hasta el curso once. Para lograr su desarrollo se vale de metas a corto, mediano y largo plazo.

El colegio tiene como prioridad formar hombres capaces de tomar determinaciones respetuosas, responsables, racionales y justas para que puedan enfrentar la realidad actual con acierto, y practicar la democracia.

El alumno galanista va adquiriendo a través de la educación recibida en la institución su sentido crítico, analítico, capaz de aceptar y seleccionar todo lo que contribuya a fortalecer su voluntad, enriquecer su entendimiento y alcanzar su realización personal y social.

La formación militar y académica capacitan al cadete para desempeñarse como combatiente individuales, regulares e irregulares, formando parte de una escuadra, un pelotón o de una unidad fundamental, para participar activamente en la conservación de las instituciones tradicionales de **COLOMBIA** como es el sistema democrático.

A nivel académico, hombres que aprecien y defienda valores culturales, científicos, tecnológicos, capaces de transformar y desarrollar nuevos proyectos académicos que le permitan ingresar a los estudios superiores, para tener como meta ser buenos cristianos, y honestos ciudadanos, para transformar y contribuir al desarrollo de nuestra patria.

MARCO TEORICO

Los profundos cambios que últimamente se han producido como efecto de los avances tecnológicos, han permitido comprobar la importancia de las telecomunicaciones en procesos tan interesantes y necesarios como el diseño, implementación y mantenimiento de redes, las cuales se han convertidos en puntos fundamentales para responder a las necesidades y problemas del mundo real. Es así, interesante resaltar los beneficios de este campo que de una u otra forma presentan una retroalimentación a las necesidades básicas, que son el común denominador de una sociedad que día a día experimenta nuevas cosas y se cataloga como una herramienta, a la visión futura de lo que ya esta creado. Por tanto, empresas y otras organizaciones han decidido acoger estos procesos con la intención de mejorar la eficacia, la rentabilidad y la calidad en la productividad y todo aquello que le permita implementar sus nuevas capacidades, así como la demanda de las mismas. Con lo cual, es factible reconocer que son diversos los medios, protocolos estándares y otros que convergen en uno o varios entornos para reducir los problemas asociados al crecimiento de una red en desarrollo, estableciendo el modelo OSI, como una guía para facilitar dichos cambios.

Determinando al final, las ventajas de las redes, especialmente en el ámbito de generar bases para su aplicación, en este caso a un Proyecto de Diseño de una Red LAN para el **Colegio Militar JOSÉ ANTONIO GALÁN**, que tiene por objeto el análisis y estudio de diferentes factores como: recolección de información, diseño de planos e instalaciones físicas, centro de cableado, topología física y lógica, equipos de networking, protocolos de comunicaciones y recomendaciones para el mejor rendimiento de la red.

GRUPOS DE TRABAJO Y CANTIDAD DE USUARIOS

lista de usuarios		
dependencia	**N° de equipos**	**futuro**
rector	1	1
subdirector	0	1
secretaria	1	1
sala de profesores	0	5
sala de oficiales	0	3
régimen interno	1	1
director militar	0	1
coordinación académica	1	1
biblioteca	0	4
sala de sistemas uno	16	16
sala de sistemas dos	15	40
auditorio	0	1
laboratorios	0	4
audiovisuales	0	1
total	**35**	**80**

RECOPILACION DE INFORMACIÓN

Para la recopilación de la información tomamos en cuenta los siguientes aspectos importantes:

Hardware y Software que manejan cada uno de los equipos.

Rendimiento y desempeño de los recursos con los que cuenta actualmente el sistema.

Jerarquización de tipo información según manejo del usuario.

La anterior información fue hecha por medio de una encuesta, la cual fue formulada a cada usuario (profesores).

Para la recopilación de información referente al Hardware y Software de equipos, usamos un formato que contenía ítems básicos y precisos; tales como la velocidad de procesador, marca, sistema operativo, aplicaciones, MODEM entre otras.

Se utilizo el programa SANDRA, el cual facilitó la obtención de la información de una manera más exacta evitando así el margen de error.

EQUIPOS COL MILITAR JOSÉ ANTONIO GALÁN

RECOPILACIÓN DE INFORMACIÓN

COMPUTER SYSTEM.

- ✓ **Name:** Servidor
- ✓ **User Name:** CMJAG
- ✓ **Logon Domain:** Servidor

PROCESSOR.

- ✓ **Model:** Intel (R) Pentium (R) 3 CPU 1.706 HZ
- ✓ **Speed:** 1.170 GHZ

WINDOWS MEMORY INFORMATION.

- ✓ **Total System Memory:** 769 MB
- ✓ **Free System Memory:** 510 MB, 66%
- ✓ **Total Physical Memory:** 224 MB
- ✓ **Free Physical Memory:** 115 MB, 51%
- ✓ **Maximum Page File:** 546 MB
- ✓ **Currentpage File:** 322 MB
- ✓ **Free Page File:** 396 MB, 72 **%**

PORTS INFORMATION.

- ✓ **Model:** HSP 56 Mr

REQUERIMIENTOS

- ✓ Acceso a Internet.
- ✓ Implementación de servidores para las áreas administrativas.
- ✓ Implementación de VLANS.
- ✓ Ancho de banda inicial de 10 MB para cualquier host en la red. Ancho de banda inicial de 100 MB para cualquier servidor de la red.
- ✓ Interconexión con todos los salones y áreas administrativas.
- ✓ Cableado horizontal UTP CAT 5e, o CAT 6.
- ✓ Debe cumplir con los estándares **TIA/EIA.**
- ✓ Debe contemplar seguridad basada en la conmutación LAN Ethernet.
- ✓ Debe contemplar un MDF, los IDF necesarios y POP con capacidad de conexión WAN.
- ✓ El diseño debe ser en estrella extendida o en cascada.
- ✓ Un esquema jerárquico donde se conecte el servidor DNS y de correo electrónico con todos los servicios ubicados en el servidor maestro.
- ✓ Conexión de un servicio administrativo, el servidor de biblioteca, servidor de aplicaciones, y otros servidores.
- ✓ Esquema de convención de nombres y un esquema de direccionamiento TCP/IP con subneting, NAT y números de redes privadas.
- ✓ Direccionamiento estático en las áreas administrativas y DHCP en el currículo.
- ✓ Uno o varios host maestro para la administración.

TOPOLOGIA FISICA DE LA RED.

Una topología de red define como están conectadas las computadoras, impresoras, dispositivos de red y otros. En otras palabras, una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos.

Las redes pueden tener una topología física y una topología lógica.

La topología física se refiere a la disposición física de los dispositivos y los medios. Las topologías físicas más comunes son las siguientes:

Topología de Bus: Utiliza un único segmento Backbone (longitud del cable) al que todos los host se conectan de forma directa.

Topología de Anillo: Conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

Topología en Estrella: Conecta todos los cables con un punto central de concentración. Por lo general, este punto es un Hub o un switch.

Topología en Estrella Extendida: Esta topología conecta estrellas individuales conectando los Hub / switch. Esto, permite extender la longitud y el tamaño de la red.

Topología Jerárquica: Se desarrolla de forma similar a la topología en estrella extendida pero, en lugar de conectar los Hub / switch entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

Topología en Malla: Se utiliza cuando no puede existir absolutamente ninguna interrupción en las comunicaciones. De modo que, cada host tiene sus propias conexiones con los demás host.

La topología lógica define como acceden los host a los medios para enviar datos.

CENTROS DE CABLEADO

Los centros de cableado es donde se encuentran instalados la mayoría de cables y dispositivos de Networking. Los servicios de distribución principal se denominan MDF (Main Distribution Facility), es decir; la habitación de comunicaciones principal de un edificio.

Cuando los host de redes grandes están fuera de la limitación de 100 metros del cable UTP categoría 5, es habitual que halla más de un recinto de cableado al crear múltiples recintos de cableado, se crean múltiples zonas de captación.

Los recintos de cableado secundarios se denominan IDF (intermediate Distribution Facility). Existen estándares que rigen los MDF y los IDF, por ejemplo: Los estándares TIA / EIA especifican que los IDF deben estar conectados al MDF por medio del cableado vertical también llamado cableado Backbone.

CONEXIÓN A TIERRA.

Para proteger los dispositivos conectados a la red y a las personas que trabajan con ellos de las descargas eléctricas, es necesario contar con una buena instalación de polos a tierra.

La tierra en su conjunto se clasifica propiamente como un conductor y por conveniencia se supone su potencial como cero. Basándose en la composición de la tierra, la resistencia de la misma puede variar dentro de un rango muy amplio de un lugar a otro. Cuando un objeto metálico se conecta a tierra por medio de un electrodo de aterrizamiento o un conector a tierra del equipo, se forja a tener el mismo potencial cero de tierra. Cualquier intento de bajar o elevar el potencial del objeto con respecto a tierra da como resultado la circulación de una corriente que pasa a través de una conexión a tierra hasta que el potencial del objeto y de la tierra se iguale.

La temperatura del suelo y del contenido de humedad son otros factores que tienen una gran influencia en la resistencia del suelo.

Se deben conectar los circuitos y sistemas a tierra para limitar los voltajes excesivos por ondas entrantes en la línea o por efectos de las descargas atmosféricas. También para proporcionar potencial cero a tierra para los gabinetes, bastidores y equipos no conductores.

En forma ideal, la resistencia de un sistema a tierra debería ser cero ohmios para reducir cualquier voltaje, debido a las corrientes de fuga esta resistencia es prácticamente imposible.

CABLEADO ESTRUCTURADO.

Existen diferentes tipos de medios para Networking usados en la capa física, incluyendo el cable de par trenzado blindado, el cable de par trenzado no blindado, el cable coaxial y el cable de fibra óptica, además las especificaciones de estos medios junto con los dispositivos de red, topología de red, colisiones y dominios de colisión, pueden ayudar a determinar cosas tales como la cantidad de datos que pueden viajar a través de la red y a que velocidad.

El cobre es el medio más común para el cableado de la señal. Los hilos de cobre son los componentes de un cable que transporta las señales desde una computadora de origen hasta una computadora destino. El cobre tiene algunas propiedades que le son muy adecuados para el cableado electrónico.

Conductividad. El cobre es, quizás el mejor conductor de corriente eléctrica que conocemos. También es un excelente conductor de calor. Esta propiedad le hace muy útil para utensilios de cocina, radiadores y frigoríficos.

Resistencia a la Corrosión. El cobre no se oxida y es bastante resistente a la corrosión; el cobre se corroe como oxido cobrizo de forma más lenta que otros metales.

Ductilidad. El cobre posee una gran ductilidad, la capacidad de dividirse en finos hilos sin romperse. Por ejemplo, una barra de cobre de un centímetro de diámetro puede calentarse, enrollarse y dividirse en hilos más finos que un pelo humano.

Maleabilidad. El cobre puro es altamente maleable. No se agrieta al golpearlo, estamparlo, forjarlo o tornearlo con formas inusuales. Puede trabajarse cuando esta caliente o frío.

Fuerza. El cobre enrollado frío tiene una fuerza tensora de entre 3500 y 4900 kilogramos por centímetro cuadrado. El cobre mantiene su fuerza y su dureza hasta cerca de los 204 centígrados.

Aquí nos centraremos en dos tipos de cable de cobre utilizado para las redes:

Par trenzado. Los cables de par trenzado están compuestos por uno o más pares de hilos de cobre. La mayoría de redes de voz y datos utilizan cableado de par trenzado.

Coaxial. El cable coaxial tiene un conductor central compuesto por un hilo de cobre sólido o un manojo de hilos. El cable coaxial, es una de las opciones para el cableado de redes de área local (LAN), se utiliza ahora principalmente para las conexiones de video, conexiones de alta velocidad como las líneas T3 y la televisión por cable.

CABLE DE PAR TRENZADO.

El cable de par trenzado es un tipo de cable que se utiliza para las comunicaciones telefónicas y la mayoría de redes Ethernet modernas. Un par de cables forman un circuito que puede transmitir datos. Los pares están trenzados para proporcionar protección contra la diafonía, el ruido generado por pares adyacentes.

Estos hilos están trenzados por dos razones:

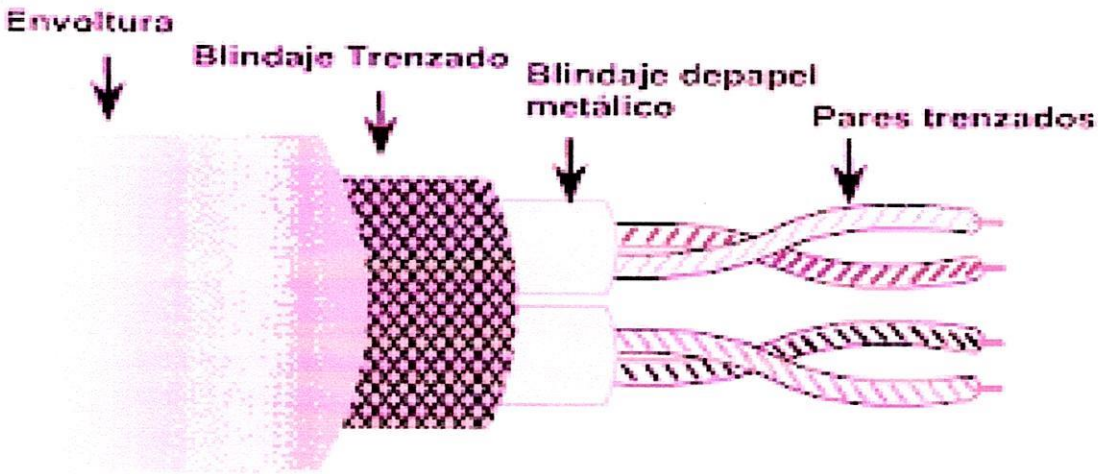
Cuando un hilo esta transportando corriente, crea un campo magnético alrededor del hilo este campo puede interferir con señales o hilos cercanos, para combatirlos, los pares de hilos transportan señales en direcciones opuestas y se neutralizan. Este proceso se denomina cancelación.

Los datos de la red se envían utilizando dos hilos en un par trenzado. Por cada uno de los hilos se envía una copia de los datos, siendo las dos copias imágenes espejo, estas señales se denominan señales diferenciales. De este modo, el receptor puede filtrar el ruido porque las señales de ruido se cancelan entre si.

Hay dos tipos básicos de cable de par trenzado blindado (STP) y par trenzado sin apantallar (UTP).

CABLE DE PAR TRENZADO BLINDADO.

El cable de par trenzado blindado (STP) contiene cuatro pares de hilos de cobre finos cubiertos por unos aislantes plásticos codificados por colores y trenzados conjuntamente. Cada par esta envuelto en una fina lamina metálica, y los cuatro pares envueltos colectivamente con otra capa metálica. Esta última se recubre con una cubierta plástica exterior.



El cable de par trenzado apantallado (ScTP) es una variante del STP. La diferencia entre estos dos tipos de cableado es que ScTP solo tiene una capa de blindaje alrededor del conjunto de cuatro pares de hilos.

El blindaje en ambos tipos reduce el ruido eléctrico indeseado. Esta reducción de ruido proporciona una ventaja mayor del STP frente al cable sin apantallar.

A continuación tiene un resumen de las características del cable STP.

Velocidad y rendimiento de transferencia 10 a 100 Mbps.

Coste medio por nodo. Ligeramente caro.

Tamaño del medio y conector. Medio a grande.

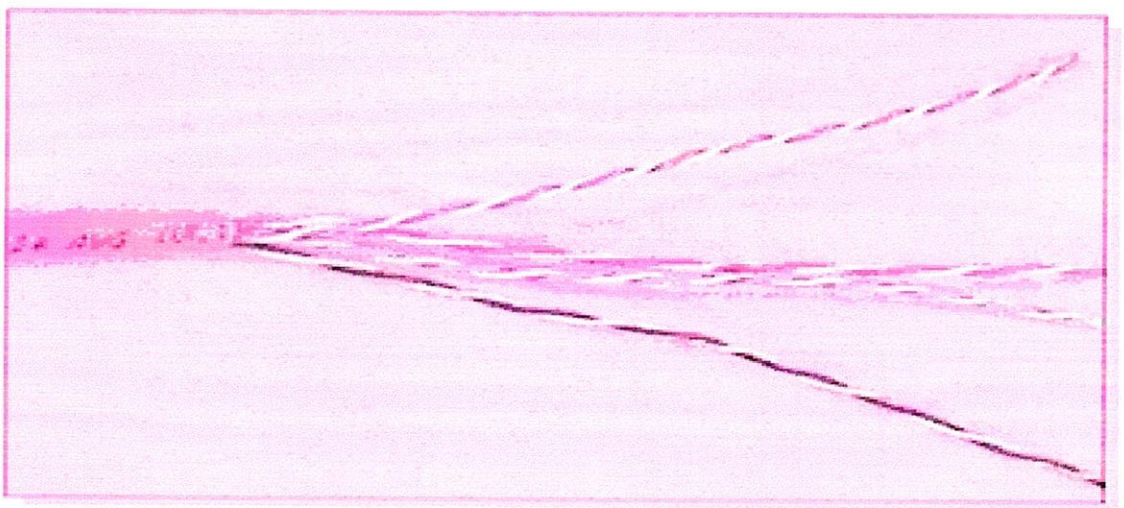
Longitud máxima del cable. 100 metros.

La instalación del cable blindado o apantallado es más compleja que la del cable sin apantallar porque los blindajes metálicos deben estar conectados a tierra. Si la instalación no es correcta la red será muy susceptible al ruido ya que un blindaje sin conexión a tierra actúa como una antena tomando señales indeseadas.

CABLE DE PAR TRENZADO SIN APANTALLAR.

El cable de par trenzado sin apantallar (UTP) es un medio de red común. Esta compuesto por cuatro pares de hilos de cobre finos cubiertos por unos aislantes plásticos codificados por colores y trenzados en conjunto, los pares de hilos están cubiertos por una carcasa plástica exterior.

El cable UTP tiene muchas ventajas. Tiene un diámetro pequeño y no requiere conexión a tierra. Por lo que lo hace mas sencillo para instalar, también es el medio de red mas barato y soporta las mismas velocidades de datos que otros medios de cobre.



A continuación tiene un resumen de las características del cable UTP.

Velocidad y rendimiento de transferencia. 10 a 100 Mbps.

Coste medio por nodo. Ligeramente caro.

Tamaño del medio y el conector. Pequeño.

Longitud máxima del cable. 100 metros.

La principal desventaja del UTP es que es más susceptible al ruido eléctrico y las interferencias de otros medios de red. Lógicamente por lo que no es blindado.

Los tipos de cable UTP mas utilizados son los siguientes:

Categoría 1(CAT1). Se utiliza para comunicaciones telefónicas. No es adecuado para la transmisión de datos.

Categoría 2 (CAT2). Capaz de transmitir datos a velocidades superiores a 4 Mbps.

Categoría 3 (CAT3). Se utiliza en redes Ethernet 10BASET. Puede transmitir datos a velocidades de hasta 10Mbps.

Categoría 4 (CAT4). Se utiliza en las redes Token Ring. Puede transmitir datos a velocidades de hasta 16Mbps.

Categoría 5 (CAT5). Puede transmitir datos a velocidades de hasta 100Mbps se utiliza en redes Fast Ethernet.

Categoría 5e (CAT5e). Se utiliza en redes con velocidades de hasta 1000Mbps. Se utiliza en redes Gigabit Ethernet.

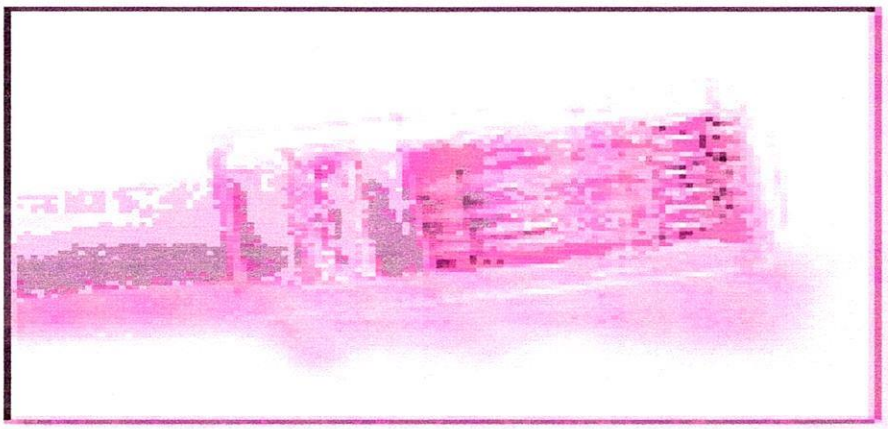
Categoría 6 (CAT6). Las especificaciones para la CAT 6 es nueva, se utiliza en redes Gigabit Ethernet.

Normalmente los cables de red de categoría 5 y superiores están compuestos por cuatro pares de hilos de cobre 24 AWG multitrenzados. Las instalaciones de cableado más antiguas utilizaban CAT 3 para la voz y CAT 5 para datos. Las instalaciones mas modernas utilizan, como mínimo, CAT 5e para la voz y los datos. Aunque el coste de CAT 5e es ligeramente superior, a la larga merece la pena.

Tenga en cuenta lo siguiente al comprar el UTP con el STP:

- ✓ La velocidad de ambos tipos de cable es normalmente satisfactoria para las distancias del área local.
- ✓ Son los medios más baratos para la comunicación de datos. El cable UTP es mas barato que el cable STP.
- ✓ Debe asegurarse de que el nivel de categoría del cable es adecuado para manipular el ancho de banda deseado.

El conector utilizado en los anteriores cables se denomina conector RJ-45.

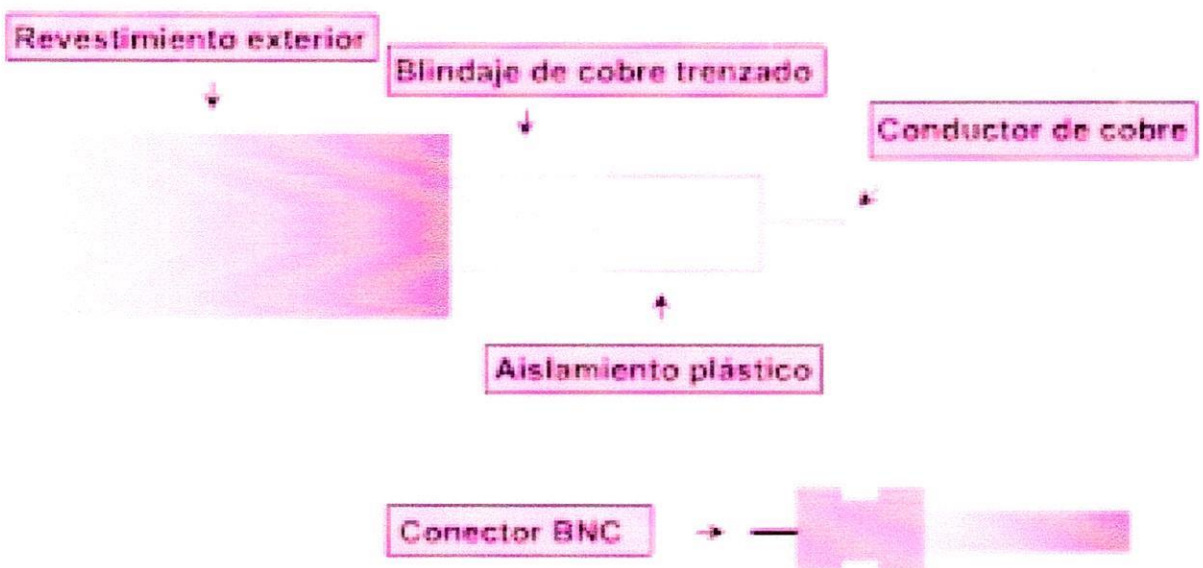


CABLE COAXIAL.

El cable coaxial consta de cuatro partes principales.

- ✓ Conductor de cobre.
- ✓ Aislante plástico.
- ✓ Pantalla de cobre trenzada.
- ✓ Cubierta exterior.

En el centro del cable hay un conductor sólido de cobre. Le rodea una capa aislante plástica flexible. Sobre este material aislante, un tejido trenzado de cobre o papel metálico que actúa como el segundo de los dos hilos de cable. A la vez actúa como blindaje para el conductor interno y ayuda a reducir la cantidad de interferencia exterior.



El conector utilizado en el cable coaxial es el denominado BNC, (conector naval británico).

Aunque muchas redes con topología en bus todavía utilizan cable coaxial en todo el mundo, el IEEE ya no recomienda este cable o topología como estándar con Ethernet. Casi todas las LAN nuevas utilizan la topología Ethernet en estrella extendida y una combinación de UTP con fibra óptica.

A continuación tiene un resumen de las características del cable coaxial.

Velocidad y rendimiento de transferencia. 10 a 100 Mbps.

Coste medio por nodo. Barato.

Tamaño del medio y conector. Medio.

Longitud máxima del cable. 500 metros.

REQUERIMIENTOS DE SEGURIDAD

Una de las primeras decisiones que debe tomar al planificar su red es la colocación de los centro(s) de cableado, ya que es allí donde deberá instalar la mayoría de los cables y los dispositivos de networking. La decisión más importante es la selección del (de los) servicio(s) de distribución principal (MDF). Existen estándares que rigen los MDF e IDF.

El estándar TIA/EIA-568-A especifica que en una LAN Ethernet, el tendido del cableado horizontal debe estar conectado a un punto central en una topología en estrella.

El punto central es el centro de cableado y es allí donde se deben instalar el panel de conexión y el hub. El centro de cableado debe ser lo suficientemente espacioso como para alojar todo el equipo y el cableado que allí se colocará, y se debe incluir espacio adicional para adaptarse al futuro crecimiento. Naturalmente, el tamaño del centro va a variar según el tamaño de la LAN y el tipo de equipo necesario para su operación. Una LAN pequeña necesita solamente un espacio del tamaño de un archivador grande, mientras que una LAN de gran tamaño necesita una habitación completa.

El estándar TIA/EIA-569 especifica que cada piso deberá tener por lo menos un centro de cableado y que por cada 1000 m^2 se deberá agregar un centro de cableado adicional, cuando el área del piso cubierto por la red supere los 1000 m^2 o cuando la distancia del cableado horizontal supere los 90 m.

Cualquier ubicación que se seleccione para instalar el centro de cableado debe satisfacer ciertos requisitos ambientales, que incluyen, pero no se limitan al, suministro de alimentación eléctrica y aspectos relacionados con los sistemas de calefacción / ventilación / aire / acondicionado (*HVAC*). Además, el centro debe protegerse contra el acceso no autorizado y debe cumplir con todos los códigos de construcción y de seguridad aplicables.

Cualquier habitación o centro que se elija para servir de centro de cableado debe cumplir con las pautas que rigen aspectos tales como las siguientes:

- ✓ Materiales para paredes, pisos y techos.
- ✓ Temperatura y humedad.
- ✓ Ubicaciones y tipo de iluminación.
- ✓ Tomacorrientes.

- ✓ Acceso a la habitación y al equipamiento.
- ✓ Acceso a los cables y facilidad de mantenimiento.

PAREDES PISOS Y TECHOS.

Si existe sólo un centro de cableado en un edificio o si el centro de cableado sirve como MDF, entonces, el piso sobre el cual se encuentra ubicado debe poder soportar la carga especificada en las instrucciones de instalación que se incluyen con el equipo requerido, con una capacidad mínima de 4.8 kPA (100 lb/ft²). Cuando el centro de cableado sirve como 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 elevado a fin de poder instalar los cables horizontales entrantes que provienen de las áreas de trabajo. Si esto no fuera posible, deberá instalarse un bastidor de escalera de 30,5 cm. 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.

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. Si el centro de cableado sirve de MDF para el edificio, entonces el **punto de presencia (POP)** telefónico se puede ubicar dentro de la habitación. En tal caso, las paredes internas del sitio POP, detrás del PBX, se deben recubrir del piso al techo con madera terciada de 20mm, dejando como mínimo 4,6 m. de espacio de pared destinado a las terminaciones y equipo relacionado.

Además se deben usar materiales de prevención de incendios que cumplan con todos los códigos aplicables (por Ej., madera terciada resistente al fuego, pintura retardarte 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 no se puede garantizar la seguridad de las instalaciones, ya que esto haría posible el acceso no autorizado. Si no se cumple con esta especificación no se puede garantizar la seguridad de las instalaciones, ya que esto haría posible el acceso no autorizado.

TEMPERATURA Y HUMEDAD.

El centro de cableado deberá incluir suficiente calefacción / ventilación / aire acondicionado como para mantener una temperatura ambiente de aproximadamente 21°C cuando el equipo completo de la LAN esté funcionando a pleno. No deberá haber 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%. El incumplimiento de estas especificaciones podría causar corrosión severa de los hilos de cobre que se encuentran dentro de los UTP y STP. Esta corrosión reduce la eficiencia del funcionamiento de la red.

DISPOSITIVOS DE ILUMINACIÓN Y TOMA CORRIENTES.

Si existe sólo un centro de cableado en el edificio o si el centro sirve como MDF, debe tener como mínimo dos receptáculos para tomacorrientes dúplex de CA, dedicados, no conmutados, ubicados cada uno en circuitos separados. También debe contar con por lo menos un tomacorrientes dúplex ubicado cada 1,8 m a lo largo de cada pared de la habitación, que debe estar ubicado a 150 Mm. 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.

Aunque se debe evitar el uso de iluminación fluorescente en el recorrido del cable debido a la interferencia externa que genera, sin embargo 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.

ACCESO A LA HABITACIÓN Y AL EQUIPAMIENTO.

La puerta de un centro de cableado deberá tener por lo menos 0,9 m. de ancho, y deberá abrirse hacia afuera de la habitación, permitiendo de esta manera que los trabajadores puedan salir con facilidad. La cerradura deberá ubicarse en la parte externa de la puerta, pero se debe permitir que cualquier persona que se encuentre dentro de la habitación pueda salir en cualquier momento.

Se podrá montar un hub de cableado y un panel de conexión contra una pared mediante una consola de pared con bisagra o un bastidor de distribución. Si elige colocar una consola de pared con bisagra, la consola deberá fijarse a la madera terciada que recubre la superficie de la pared subyacente. El propósito de la bisagra es permitir que el conjunto se pueda mover hacia afuera, de manera que los trabajadores y el personal del servicio de reparaciones puedan acceder con facilidad a la parte trasera de la pared. Se debe tener cuidado, sin embargo, para que el panel pueda girar hacia fuera de la pared unos 48 cm. Si se prefiere un bastidor de distribución, se deberá dejar un espacio mínimo de 15,2 cm. entre el bastidor y la pared, para la ubicación del equipamiento, además de otros 30,5-45,5 cm. para el acceso físico de los trabajadores y del personal del servicio de reparaciones. Una placa para piso de 55,9 cm., utilizada para montar el bastidor de distribución, permitirá mantener la estabilidad y determinará la distancia mínima para su posición final.

Si el panel de conexión, el hub y los demás equipos se montan en un gabinete para equipamiento completo, se necesitará un espacio libre de por lo menos 76,2 cm. frente a él para que la puerta se pueda abrir. Generalmente, los gabinetes de estos equipos son de 1,8 m de alto x 0,74 m de ancho x 0,66 m de profundidad.

ACCESO A LOS CABLES Y MANTENIMIENTO.

Si un centro de cableado sirve como MDF, todos los cables que se tiendan a partir de este, hacia las IDF, computadores y habitaciones de comunicación ubicadas en otros pisos del mismo edificio, se deben proteger con un conducto o corazas de 10,2 cm.

Asimismo, todos los cables que entren en los IDF deberán tenderse a través de los mismos conductos o corazas de 10,2 cm. La cantidad exacta de conductos que se requiere se determina a partir de la cantidad de cables de fibra óptica, UTP y STP que cada centro de cableado, computador o sala de comunicaciones puede aceptar. Se debe tener la precaución de incluir longitudes adicionales de conducto para adaptarse al futuro crecimiento.

Para cumplir con esta especificación, se necesitan como mínimo dos corazas revestidas o conductos adicionales en cada centro de cableado. Cuando la construcción así lo permita, todos los conductos y corazas revestidas deberán mantenerse dentro de una distancia de 15,2 cm. de las paredes.

Todo el cableado horizontal desde las áreas de trabajo hacia un centro de cableado se debe tender debajo de un piso falso. Cuando esto no sea posible, el cableado se debe tender mediante conductos de 10,2 cm. ubicados por encima del nivel de la puerta. Para asegurar un soporte adecuado, el cable deberá tenderse desde el conducto directamente hasta una escalerilla de 30,5 cm. que se encuentre dentro de la habitación. Cuando se usa de esta forma, como soporte del cable, la escalerilla se debe instalar en una configuración que soporte la disposición del equipo.

Finalmente, cualquier otra apertura de pared / techo que permita el acceso del conducto o del núcleo revestido, se debe sellar con materiales retardadores de humo y llamas que cumplan todos los códigos aplicables.

SELECCIONES DE UBICACIONES POTENCIALES.

Una buena manera de empezar a buscar una ubicación para el centro de cableado consiste en identificar ubicaciones seguras situadas cerca del POP. La ubicación seleccionada puede servir como centro de cableado único o como MDF, en caso de que se requieran IDF. El POP es donde los servicios de telecomunicaciones, proporcionados por la compañía telefónica, se conectan con las instalaciones de comunicación del edificio. Resulta esencial que el hub se encuentre ubicado a corta distancia, a fin de facilitar una networking de área amplia y la conexión a Internet.

DETERMINACIÓN DE LA CANTIDAD DE CENTROS DE CABLEADO.

Después de incorporar en el diseño todos los dispositivos que se conectarán a la red en un plano de piso, el siguiente paso es determinar cuántos centros de cableado necesitará para brindar servicio al área que abarca la red. Tendrá que usar su mapa del sitio para hacerlo.

Use un compás para trazar círculos que representen un radio de 50 m. a partir de cada ubicación de hub potencial. Cada uno de los dispositivos de red que dibuje en su plano deberá quedar dentro de uno de estos círculos. Sin embargo, si cada tendido de cableado horizontal sólo puede tener una longitud de 90 m., ¿sabe por qué se deben usar círculos con un radio de sólo 50 m.?

Después de trazar los círculos, vuelva a consultar el plano de piso. ¿Existen ubicaciones de hub potenciales cuyas áreas de captación se superpongan sustancialmente? De ser así, podría seguramente eliminar una de las ubicaciones de hub.

¿Existen ubicaciones de hub potenciales cuyas áreas de captación puedan contener todos los dispositivos que se deban conectar a la red? De ser así, una de ellas puede servir de centro de cableado de todo el edificio. Si necesita más de un hub para brindar cobertura adecuada para todos los dispositivos que se conectarán a la red, verifique si alguno de ellos está más cerca del POP que los otros. De ser así, probablemente represente la mejor opción para funcionar como MDF.

NORMATIVIDAD DEL CABLEADO

Existen en la actualidad varias organizaciones en el ámbito mundial, dedicadas a la Implementación de estándares para los medios de Networking. Estas especificaciones o normas son conjuntos de reglas o procedimientos ampliamente utilizados que sirven como método aceptado de hacer una tarea.

El instituto de ingenieros eléctricos y electrónicos (IEEE) ha diseñado unas especificaciones para el cableado de las LAN. El IEEE 802.3 es una norma para las redes. Ethernet y el IEEE 802.5 otra norma para las redes Token Ring.

La asociación de la industria de las telecomunicaciones (TIA) y a asociación de industrias electrónicas (EIA) han emitido conjuntamente varias normas sobre el cableado, denominadas normas TIA / EIA. La siguiente lista describe algunas de ellas:

TIA/EIA-568-B. Norma para el cableado de telecomunicaciones en un edificio comercial.

TIA/EIA-569-B. Antiguamente era la norma TIA / EIA-568-A. Es una norma de edificios comerciales para caminos y espacios de telecomunicaciones.

TIA/EIA-570-A. Norma de cableado de telecomunicaciones comercial ligera y residencial.

TIA/EIA-606. Norma de administración para la infraestructura de telecomunicaciones de edificios comerciales.

TIA/EIA-607. Para edificios comerciales conectados a tierra y con requisitos de enlace para telecomunicaciones.

Las especificaciones creadas por esta organización han tenido un gran impacto en las normas referidas a medios de red e incluyen normas para el cableado horizontal y backbone (vertical), recintos de cableado y salas de equipamiento, áreas de trabajo y servicios de entrada.

La norma TIA/EIA-568-B se centra en el cableado horizontal, que es el cableado que se extiende desde un enchufe en la pared del área de trabajo hasta un recinto de cableado. Las CAT 3, CAT 4 y CAT 5 reúnen la norma TIA-EIA-568-B. El cable de categoría 5 es el más instalado.

La TIA7EIA-568-B requiere dos cables para cada enchufe del área de trabajo:

- ✓ Un cable telefónico para la voz.
- ✓ Un cable de red para los datos.

El cable para la voz debe ser un cable UTP de dos pares con sus conectores correctos, o terminadores. El cable de red debe ser uno de lo9s siguientes y debe incluir los conectores o terminadores correctos

- ✓ Cable STP de 2 pares y 150 ohms (LAN Token Ring).
- ✓ Cable UTP de cuatro pares y 100 ohm (LAN Ethernet).
- ✓ Cable de fibra óptica de 62.5 / 125u (LAN Ethernet).
- ✓ Cable coaxial raramente utilizado en las nuevas instalaciones y que se espera sea eliminado de esta lista.

Aunque no forma parte de la norma, un cable coaxial RG-6 de 75 ohm también puede utilizarse para la conexión de TV por cable, así como para un mínimo de conexiones de voz y datos si lo desea.

La norma también especifica la longitud máxima de cada recorrido de cable UTP desde el enchufe de la pared hasta las conexiones del recinto de cableado. También aparece especificado un alargador de 3 metros desde la estación de trabajo hasta el enchufe de la pared. Esta permitido un recorrido de cable de 90 metros desde el enchufe de la pared hasta el patch panel del recinto de cableado.

Esta permitido un alargador de 6 metros desde el patch panel hasta la conexión cruzada horizontal en el recinto de cableado. Estas normas aseguran que todo el recorrido del cable no excede de 100 metros.

Backbone: Suele ser el cable principal (o el enlace troncal) al que acceden todos los nodos y dispositivos. Actualmente debido a sus características eléctricas, como la inmunidad ante problemas de ruido y masa, la fibra óptica es el medio mas utilizado para el cableado Backbone por delante del cable coaxial y el par trenzado sin apantallar (UTP).

CANALETAS.

La canaleta es un canal montado sobre la pared con una cubierta móvil. Existen dos tipos de canaletas.

- ✓ **Canaleta Decorativa:** La canaleta decorativa se utiliza para colocar un cable sobre la pared de una habitación, donde quedaría visible de otra manera.
- ✓ **Canal:** Su principal ventaja, es que es lo suficientemente grande como para contener varios cables. Generalmente, el uso del canal se ve restringido a espacios como áticos y el espacio sobre un techo falso.

La canaleta puede ser de plástico o de metal y se puede montar con adhesivo o con tornillos.

PATCH PANEL.

Los Patch Panel son jacks RJ-45 agrupados de una forma conveniente. Generalmente son de 12, 24 ó 48 puertos y normalmente están montados en un bastidor. Las partes delanteras son jacks RJ-45, y las partes traseras son bloques de punción que proporcionan conectividad.

Un Patch Panel es un dispositivo de interconexión a través del cual los tendidos de cableado horizontal se pueden conectar con otros dispositivos de red como, por ejemplo, Hubs y repetidores. El Patch Panel actúa como un conmutador, donde los cables horizontales que provienen de las estaciones de trabajo se pueden conectar a otras estaciones de trabajo.

Puede montar los paneles de conexión en las paredes (con la ayuda de soportes), colocarlos parados en bastidores o colocarlos en gabinetes (equipados con bastidores interiores y puertas).

La ventaja del bastidor de distribución es que permite acceder fácilmente tanto a la parte delantera como a la parte trasera del equipo.

ROTULACIÓN.

Cada unidad de terminación de hardware debe tener algún tipo de identificador exclusivo. Este identificador debe estar marcado en cada unidad de terminación de hardware o en su rótulo. Cuando se utilizan identificadores en áreas de trabajo, las terminaciones de estaciones deben tener un rótulo en la placa, el bastidor o el conector mismo.

Todos los rótulos, ya sean adhesivos o insertables, deben cumplir con los requisitos de legibilidad, protección contra el deterioro y adhesión.

Se deben usar rótulos que sean comprensibles para alguien que deba trabajar en el sistema muchos años después.

La mayoría de los administradores de red incorporan números de habitaciones a la información rotulada. Asignan letras a cada cable que llega hasta una habitación. Algunos sistemas de rotulado, especialmente en redes muy grandes, también incorporan una codificación con color. Se deben colocar las conexiones de manera tal que los rótulos queden ordenados de forma ascendente. Esto facilita el diagnóstico y ubicación de los problemas cuando se presenten en el futuro. Finalmente, rotule los cables en cada extremo.

TIPO DE RED.

La capa de enlace de datos hace posible la transmisión confiable de datos a través de un enlace físico mediante el uso de las direcciones de control de acceso al medio (MAC). Algunas tecnologías LAN de capa 2 como Ethernet, interfaz de datos distribuida por fibra (FDDI) y Token Ring son tecnologías de uso muy difundido que se emplean virtualmente en todas las LAN existentes.

Token Ring: Token Ring es la tecnología de LAN principal de IBM, y en el ámbito de implementación LAN ocupa el segundo lugar después de Ethernet (IEEE 802.3). La especificación IEEE 802.5, se basó en el Token Ring de IBM y ha venido evolucionando en paralelo con este estándar.

Los Token tienen una longitud de 3 bytes y están formados por un delimitador de inicio de un byte de control de acceso y un delimitador de fin. Esta pequeña trama o Token es transportada a través de la red.

La posesión del Token otorga el derecho de transmitir datos, si el nodo que recibe el Token no tiene información para enviar, transfiere el Token a la siguiente estación terminal; si no hay ningún Token en la red mientras la trama de información gira alrededor del anillo, las otras estaciones no pueden realizar transmisiones hasta que el Token este disponible. Las redes Token Ring pueden calcular el tiempo máximo que transcurrirá antes que cualquier estación Terminal pueda realizar una transmisión, ésta y varias características de confiabilidad hacen que estas redes sean ideales para un funcionamiento sólido.

FDDI (interfaz de datos distribuida por fibra): A mediados de los años 80, las estaciones de trabajo de alta velocidad para uso en ingeniería habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades; para solucionar éste problema la comisión normalizadora ANSI X3T9.5 creó FDDI, luego el ANSI envió el FDDI a la ISO la cual creó entonces una versión internacional de dicha interfaz, compatible con la versión del ANSI.

Aunque en la actualidad las implementaciones de la FDDI no son tan comunes como Ethernet y Token Ring, la FDDI se usa con frecuencia como una tecnología Backbone y para conectar los computadores de alta velocidad en una LAN, FDDI utiliza una estrategia de transmisión de tokens similar a la de Token Ring.

ETHERNET: Ethernet es una tecnología de red de área local (LAN) de uso más generalizado. El diseño original de Ethernet representaba un punto medio entre las redes de larga distancia y baja velocidad y las redes especializadas de las salas de computadores que transportaban datos a altas velocidades y a distancias muy limitadas Ethernet se adecua bien a las aplicaciones en las que un medio de comunicación local debe transportar trafico esporádico y ocasionalmente pesado a velocidades muy elevadas.

El método de acceso utilizado por Ethernet es el CSMA/CD (acceso múltiple con detección de portadora y detección de colisiones).

Las estaciones de una LAN tipo CSMA/CD pueden acceder a la red en cualquier momento, antes de enviar datos las estaciones CSMA/CD escuchan a la red para determinar si se encuentra en uso. Si lo está, entonces esperan. Si la red no está en uso las estaciones transmiten.

En una colisión, o sea cuando 2 estaciones entran a transmitir en forma simultánea, ambas transmisiones se dañan y las estaciones deben transmitir más tarde Tanto las LAN Ethernet como las LAN IEEE 802.5 son redes broadcast, o sea que cada estación puede ver todas las tramas, cada estación debe examinar las tramas que recibe para determinar si corresponde al destino.

SEGMENTACION.

Una red se puede dividir en unidades más pequeñas llamadas segmentos. Cada segmento utiliza el método de acceso CSMA/CD y mantiene el tráfico entre los usuarios del segmento. Al usar segmentos en una red, menos usuarios / dispositivos comparten los mismos 10 Mbps al comunicarse entre sí en el segmento. Cada segmento es su propio dominio de colisión, aparte un administrador de red puede reducir la congestión de cada segmento.

Segmentación con Puentes:

Las LAN Ethernet que utilizan un puente (dispositivo capa 2) para segmentar la LAN proporcionan más ancho de banda por usuario, ya que hay menos usuarios en cada segmento. Los puentes "aprenden" la segmentación de una red construyendo tablas de direcciones que contienen la dirección de cada dispositivo de red y que le permiten que segmento utilizar para alcanzar ese dispositivo.

Los puentes incrementan la latencia de una red de un 10 a un 30%, esto se debe a la toma de decisiones (almacenamiento y reenvío basado en direcciones MAC) para que el puente o los puentes transmitan datos.

Segmentación con Routers:

Los routers están mas avanzados que los típicos puentes. Un router funciona en la capa de red y basa todas sus decisiones acerca del reenvío entre segmentos en la dirección del protocolo de capa de red.

Un router toma decisiones de reenvío con respecto a los segmentos examinando la dirección de destino del paquete de datos y examinando su tabla de enrutamiento para decidir las instrucciones de reenvío.

Segmentación con Switches LAN:

Un switch puede segmentar una LAN en microsegmentos, que son segmentos de un solo host. El switch LAN elimina los dominios de colisión, todos los hosts que estén conectados al switch seguirán estando en el mismo dominio de difusión. Un switch LAN es un puente multipuerto de muy alta velocidad provisto de un puerto en cada nodo o segmento de la LAN.

Los switches también pueden tomar decisiones de reenvío construyendo una tabla de direcciones MAC de los host que estén unidos a cada puerto.

Una computadora que este directamente conectada a un switch Ethernet es su propio dominio de colisión y accede a la totalidad de los 10Mbps.

DIRECCIONAMIENTO IP

Para acomodar las redes de distintos tamaños y ayudar a su clasificación, las direcciones IP están divididas en grupos denominados clases. Es lo que se llama direccionamiento con clase. Cada dirección IP con 32 bits completa se divide en una parte de red y una parte de host, un bit o una secuencia de bits al principio de cada dirección determina la clase de la misma hay cinco clases de direccionamiento IP.

RED		HOST	
172	16	122	204
8 BITS	8 BITS	8 BITS	8 BITS
1 BITE	1 BITE	1 BITE	1 BITE

Las direcciones de clase A se diseñaron para dar soporte a redes extremadamente grandes. Una dirección IP de clase A solo utiliza el primer octeto para indicar la dirección de red. Los tres octetos restantes se utilizan como parte del host.

Las direcciones de clase B se diseñaron para dar soporte a las necesidades de redes de tamaño moderado a grande. Una dirección de clase B utiliza dos de los cuatro octetos para indicar la dirección de red. Los otros dos octetos especifican las direcciones de host.

Las direcciones de clase C son las más utilizadas. Este espacio de direcciones se pensó para dar soporte a un montón de redes pequeñas. Una dirección de clase C utiliza para indicar la dirección de red y el otro octeto especifica las direcciones de host.

Las direcciones de clase D se utilizan para grupos de difusión (broadcast). No es necesario asignar octetos o bits para separar las direcciones de red y host.

Las direcciones de clase E están reservadas únicamente para investigación.

Direccionamiento Estático.

Cuando las direcciones IP se asignan estáticamente, cada dispositivo debe configurarse con una dirección IP. Cada sistema operativo tiene su propia forma de configurar TCP / IP. Este método requiere guardar registros de las asignaciones de direcciones, porque podría haber problemas en una red en caso de utilizar direcciones IP duplicadas. Algunos sistemas operativos, como Windows 95 Windows NT, envían una petición ARP para comprobar direcciones IP duplicadas al intentar inicializar TCP / IP. Si se descubre una duplicidad, el sistema operativo no inicializa y genera un mensaje de error. No todos los sistemas operativos identifican las direcciones IP duplicadas. Esto enfatiza la necesidad de un buen mantenimiento de registros.

Direccionamiento Dinámico.

Hay varios métodos distintos que se pueden usar para asignar direcciones IP de forma dinámica. Ejemplos de estos métodos son:

Protocolo de Resolución de Dirección Inversa (RARP):

El protocolo de resolución inversa de direcciones (RARP) une las direcciones MAC con las direcciones IP. Esta unión permite que los dispositivos de red encapsulen los datos antes de enviarlos a la red. Un dispositivo de red o estación de trabajo puede conocer su dirección MAC, pero no su dirección IP.

Los dispositivos que utilizan RARP necesitan un servidor RARP en la red para responder a las peticiones RARP.

Las distintas partes de una estructura de cabecera RARP son las siguientes:

Tipo de hardware. Especifica un tipo de interfaz hardware para la que el emisor requiere una respuesta.

Tipo de protocolo. Especifica el tipo de dirección de protocolo de alto nivel que el emisor ha suministrado.

LongH. Longitud de la dirección hardware.

LongP. Longitud de la dirección de protocolo.

Funcionamiento. Sus valores son los siguientes.

Petición ARP.

Respuesta ARP.

Petición RARP.

Petición RARP.

Petición RARP dinamita.

Respuesta RARP dinámica.

Error RARP dinámico.

Petición InARP.

Respuesta InARP.

Dirección hardware (HA) del emisor. LongH bytes de longitud.

Dirección de protocolo (PA) del emisor. LongP bytes de longitud.

Dirección hardware (HA) del destino. LongH bytes de longitud.

Dirección de protocolo (PA) del destino. LongP bytes de longitud.

Protocolo Bootstrap (BOOTP):

Al igual que RARP, BOOTP funciona en un entorno cliente / servidor y requiere solo el intercambio de un único paquete para obtener la información IP. Sin embargo, a diferencia de RARP, que devuelve solo direcciones IP de cuatro octetos, los paquetes BOOTP pueden incluir la dirección IP, la dirección de un router (gateway predeterminado), la dirección de un servidor e información especifica del fabricante.

Protocolo de Configuración Dinámica del Host (DHCP):

El protocolo de configuración dinámica del host DHCP es el sucesor de BOOTP. A diferencia de BOOTP, DHCP permite al host obtener una dirección IP dinámicamente sin que el administrador de la red tenga que configurar un perfil individual para esa maquina.

Todo lo que necesita para utilizar DHCP es un rango de direcciones definidos IP en un servidor DHCP. Al quedar los host online, contactan con el servidor DHCP y piden una dirección. El servidor DHCP selecciona una dirección y la asigna a ese host. Con DHCP se puede obtener la configuración TCP / IP completa de una computadora en un mensaje; esto incluye todos los datos suministrados por el mensaje BOOTP, además de una dirección IP alquilada y una mascara de subred.

VLAN

Las VLAN son una forma muy eficaz de agrupar usuarios en grupos de trabajo virtuales, independientemente de su ubicación física en la red, funciona en la capa dos y tres del modelo OSI, la comunicación entre VLAN la proporciona en enlace de capa tres ofrece además un control en las difusiones de la red.

Por seguridad el administrador de red asigna usuarios a una VLAN. Los usuarios conectados en un grupo de trabajo se definen lógicamente por ser compañeros del mismo departamento, un equipo de producto multidisciplinar, distintos grupos de usuarios que comparten la misma aplicación o software. Las soluciones para el agrupamiento lógico de los usuarios en VLAN distintas son el filtrado de trama y la identificación de trama, funciones del Switch al recibir o reenviar una trama.

Las VLAN de puerto central asignan el mismo identificador a los puertos conectados a la VLAN, los usuarios son asignados por puertos, son más fáciles de administrar y ofrece mayor seguridad entre las VLAN. Las VLAN estáticas son puertos de un Switch que se asignan estáticamente a una VLAN, estos puertos mantiene su configuración hasta que el administrador realice los cambios pertinentes, son seguras, fáciles de configurar y controlar.

Las VLAN dinámicas son puertos de un Switch que determinan automáticamente sus tareas, estas funciones se basan en el direccionamiento lógico, tipo de protocolo de los paquetes de datos o direccionamiento MAC; Las ventajas de esta VLAN son ofrecer una menor administración de la red.

Las ventajas globales de las VLAN son proporcionar una actividad de difusión controlada, seguridad de grupo de trabajo y de red, reducir costos relacionados con la solución de problemas asociados con traslados, adiciones o cambios, además supone un ahorro de dinero al usar los equipos existentes. Para administrar e incrementar la seguridad en una VLAN se puede segmentar la red en múltiples grupos de difusión, esto le permite el administrador de red: Restringir el numero de usuarios de un grupo VLAN, configurar los puertos que no se utilicen a una VLAN predeterminada de poco servicio, prohibir a otros usuarios que se conecten a la VLAN sin previa autorización del administrador. En toda arquitectura VLAN es importante la capacidad de transportar información VLAN entre Switches y Routers interconectados los cuales residen en el Backbone.

LISTAS DE CONTROL DE ACCESO

Los administradores de redes deben ser capaces de denegar el acceso no deseado a la red, a la vez que permiten el acceso si deseado. Aunque las herramientas de seguridad como contraseñas, equipos callback y dispositivos físicos de seguridad son útiles, a menudo carecen de la flexibilidad del filtrado básico del tráfico y de los controles específicos que prefieren la mayoría de los administradores.

Las ACL se pueden usar para:

Limitar el tráfico de red y mejorar el rendimiento de la red. Las ACL pueden designar ciertos paquetes para que un router los procese antes de procesar otro tipo de tráfico, según el protocolo.

Brindar control de flujo de tráfico. Las ACL pueden restringir o reducir el contenido de las actualizaciones de enrutamiento. Estas restricciones se usan para limitar la propagación de la información acerca de redes específicas por toda la red.

Proporcionar un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le deniega el acceso a dicha red.

Si no se configuran ACL en el router, todos los paquetes que pasan a través del router supuestamente tendrían acceso permitido a todas las partes de la red.

Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Por ejemplo, se puede permitir que se enrute el tráfico de correo electrónico, pero bloquear al mismo tiempo todo el tráfico de Telnet.

ACL ESTANDAR.

Estas comprueban la dirección de origen de los paquetes IP enrutados y los comparan con las sentencias que definen las ACL. Las ACL estándar permiten o designan el acceso para un conjunto entero de protocolos como IP en función de las direcciones de red subred y host.

ACL EXTENDIDA.

Las ACL extendidas se utilizan más que las ACL estándar porque proporcionan más flexibilidad y control. Las ACL extendidas comprueban las direcciones IP de origen y destino también pueden comprobar los protocolos y los números de puerto TCP y UDP.

SEGURIDAD DE RED.

La seguridad de red involucra dos componentes principales: El primero es proteger la red contra el acceso no autorizado y el segundo es la habilidad para recuperar datos ante eventos catastróficos. La primera parte, Implica hacer que la red esté lo más protegida posible contra el acceso no autorizado. Esto se lleva a cabo estableciendo políticas de seguridad, tales como: longitud mínima de la contraseña, antigüedad máxima de la contraseña, contraseñas exclusivas (no se permite que la misma contraseña se repita) y permitir que el usuario se conecte a la red sólo en momentos determinados del día o en ciertos días de la semana. Estos parámetros pueden ser controlados directamente por el administrador de red y el sistema operativo de la red los hará cumplir. La segunda parte de la seguridad de red, implica proteger los datos ante pérdidas. Por lo general, hay más de un método en uso al mismo tiempo para proteger los datos. Tres de los métodos populares para la protección de datos son: la copia de respaldo de los datos en cinta, las configuraciones de disco a prueba de fallas y el uso de sistemas de alimentación ininterrumpida (UPS) para evitar que el equipo deje de funcionar cuando se producen interrupciones del suministro eléctrico.

ADMINISTRACIÓN EN REDES

La administración de red incluye varias responsabilidades, incluyendo el análisis de costos. Esto implica la determinación no sólo del costo del diseño e implementación de la red, sino también el costo del mantenimiento, actualización y monitoreo de la red. La determinación del costo de instalación de la red no es una tarea particularmente difícil para la mayoría de los administradores de red. Las listas y costos de los equipos se pueden establecer fácilmente; los costos laborales se pueden calcular mediante porcentajes fijos. Desafortunadamente, el costo del desarrollo de la red es tan sólo el principio.

Estos son algunos de los demás factores de costos que se deben tener en cuenta: El crecimiento de la red con el tiempo; la capacitación de técnicos y usuarios; reparaciones y distribución de software. Estos costos son mucho más difíciles de proyectar que el costo de desarrollo de la red. El administrador de red debe estar capacitado para analizar las tendencias históricas y de crecimiento de la empresa para proyectar el costo del crecimiento en la red. Un administrador debe examinar el nuevo software y hardware para determinar si la empresa necesitará implementarlo y cuándo, así como las necesidades de capacitación del personal para brindar soporte a estas nuevas tecnologías.

El costo del equipo redundante para operaciones críticas también se debe agregar al costo del mantenimiento de la red. Considere lo que ocurriría en una empresa cuya actividad se basa en Internet y que usa un solo router para conectarse a Internet. Si ese router falla, la empresa no podrá funcionar hasta que el router sea reemplazado, lo que podría costarle a la empresa miles de dólares en ventas perdidas.

Un administrador de red que conozca bien su trabajo debe tener un router de repuesto disponible para reducir al mínimo el tiempo durante el cual la empresa queda fuera de línea.

La efectiva administración de red requiere documentación completa, de manera que, en caso de problemas, se debe elaborar algún tipo de documentación de los errores. Esta documentación se utiliza para reunir la información básica necesaria para identificar y asignar un problema de red, y también ofrece una manera para hacer un seguimiento del progreso y eventual solución del problema. Los informes de problema pueden ofrecer los motivos que justifiquen la contratación de nuevo personal, adquisición de equipos y capacitación adicional por parte de la gerencia de nivel superior. Esta documentación también brinda soluciones para problemas recurrentes que ya han sido resueltos.

PORQUE ES NECESARIO MONITOREAR LA RED.

Aunque hay varias razones para el monitoreo de la red, los dos motivos principales son la predicción de los cambios para el crecimiento futuro y la detección de cambios inesperados en el estado de la red. Entre los cambios inesperados se pueden incluir cosas tales como la falla de un router o un switch, un "hacker" que intenta obtener acceso ilegal a la red, o una falla de enlaces de comunicación. Si no tiene la capacidad para monitorear la red, un administrador sólo puede reaccionar a los problemas a medida que ocurren, en lugar de prevenir estos problemas antes de que se produzcan.

El monitoreo de una red de área amplia involucra varias de las mismas técnicas básicas de administración que se aplican para una red de área local.

Una de las diferencias principales que surgen de una comparación entre WAN y LAN es la ubicación física del equipo. La ubicación y uso de las herramientas de monitoreo es fundamental para la operación ininterrumpida de la red de área amplia.

MONITOREO DE LAS CONEXIONES.

Una de las formas más básicas de monitoreo de las conexiones se produce diariamente en una red. El proceso de conexión de los usuarios a la red verifica si las conexiones funcionan correctamente; de lo contrario, el departamento de networking será contactado de inmediato. Este no es el método más eficiente o preferible para monitorear las conexiones. Existen programas simples que permiten que el administrador ingrese una lista de direcciones IP de hosts, y se hace ping a estas direcciones de forma periódica. Si hay un problema de conexión, el programa advierte al administrador con el resultado del ping. Esta es una forma muy ineficiente y primitiva de monitorear la red, pero siempre es mejor que no hacer nada. Otro aspecto de este tipo de monitoreo es que sólo determina si en algún lugar entre la estación de control y el dispositivo objetivo hay una ruptura de las comunicaciones. El problema puede ser un router, switch o segmento de red defectuoso, o que el host propiamente dicho esté desactivado. La prueba de ping sólo indica que la conexión está desactivada, pero no indica dónde lo está.

La verificación de todos los hosts en una WAN mediante este tipo de monitoreo utiliza muchos recursos. Si la red tiene 3000 hosts, hacer ping a todos los dispositivos de la red y hosts puede utilizar demasiados recursos del sistema.

Un método más adecuado es hacer ping a sólo algunos de los hosts, servidores, routers y switches importantes para verificar su conectividad. Las pruebas de ping no ofrecen datos verdaderos, a menos que las estaciones de trabajo siempre estén encendidas. Nuevamente, este método de monitoreo se debe usar sólo si no hay otro método disponible.

MONITOREO DEL TRÁFICO.

El monitoreo del tráfico es un método mucho más sofisticado de monitoreo de la red. Analiza el tráfico real de paquetes en la red y genera informes basados en el tráfico de la red. Los programas como el Monitor de red de Microsoft Windows NT y el Network Analyzer de Fluke son ejemplos de este tipo de software. Estos programas no sólo detectan el equipo defectuoso sino que también determinan si un componente se encuentra sobrecargado o mal configurado.

La desventaja de este tipo de programa es que normalmente funciona en un solo segmento por vez. Si es necesario reunir datos de otros segmentos, el software de monitoreo se debe trasladar a ese segmento. Esto se puede resolver mediante el uso de agentes en los segmentos remotos de red.

Equipos como los switches y los routers tienen la capacidad de generar y transmitir estadísticas de tráfico como parte de su sistema operativo. Entonces, ¿cómo se reúnen y organizan los datos en una ubicación central para que sean útiles para el administrador de red? La respuesta es: Protocolo simple de administración de red.

PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED.

SNMP es un protocolo que permite que la administración transmita datos estadísticos a través de la red a una consola de administración central. **SNMP** es un componente de la Arquitectura de administración de red. La Arquitectura de administración de red está formada por cuatro componentes principales

1. Estación de administración:

La estación de administración es la interfaz del administrador de red al sistema de red. Posee los programas para manipular los datos y controlar la red. La estación de administración también mantiene una base de datos de información de administración (MIB) extraída de los dispositivos bajo su administración.

2. Agente de administración:

El agente de administración es el componente incluido en los dispositivos que se deben administrar. Puentes, routers, hubs y switches pueden contener agentes SNMP que les permitan ser controlados por la estación de administración. El agente de administración responde a la estación de administración de dos maneras. En primer lugar, mediante sondeo, la estación de administración requiere datos desde el agente y el agente responde con los datos solicitados. Trapping es un método de recopilación de datos diseñado para reducir el tráfico en la red y el procesamiento en los dispositivos que se controlan. En lugar de que la estación de administración haga un sondeo a los agentes a intervalos específicos, se establecen umbrales (límites superiores o inferiores) en el dispositivo administrado. Si se supera este umbral en el dispositivo, el dispositivo administrado envía un mensaje de alerta a la estación de administración.

Esto elimina la necesidad de realizar sondeos continuos de todos los dispositivos administrados en la red. El trapping es muy ventajoso en las redes que incluyen una gran cantidad de dispositivos que necesitan administrarse. Reduce la cantidad de tráfico SNMP en la red para proporcionar mayor ancho de banda para la transferencia de datos.

3. Base de información de administración:

La base de información de administración tiene una estructura de base de datos y reside en cada dispositivo administrado. La base de datos contiene una serie de objetos, que son datos sobre recursos reunidos en el dispositivo administrado. Algunas de las categorías en el MIB incluyen datos de interfaz de puerto, datos de TCP y datos de ICMP.

4. Protocolo de administración de red:

El protocolo de administración de red utilizado es SNMP. SNMP es un protocolo de capa de aplicación diseñado para comunicar datos entre la consola de administración y el agente de administración. Tiene tres capacidades clave. La capacidad para OBTENER, que implica que la consola de administración recupera datos del agente, COLOCAR, que implica que la consola de administración establece los valores de los objetos en el agente, y TRAP, que implica que el agente notifica a la consola de administración acerca de los sucesos de importancia.

La palabra clave que se debe recordar con respecto al Protocolo simple de administración de red es "Simple". En el momento en que se desarrolló SNMP, se diseñó para ser un sistema a corto plazo que eventualmente se reemplazaría. Pero, al igual que TCP/IP, se ha transformado en uno de los estándares principales en las configuraciones de administración de Internet-redes internas.

En los últimos años, se han agregado mejoras a SNMP, a fin de expandir sus capacidades de monitoreo y administración. Una de las mejoras principales de SNMP se denomina Monitoreo remoto (**RMON**). Las extensiones de RMON a SNMP brindan la capacidad para observar la red como un todo, en contraste con el análisis de dispositivos individuales.

SOLUCIÓN DE PROBLEMAS.

¡Los problemas son inevitables! Aunque la red se monitoree constantemente, el equipo sea confiable y los usuarios sean cuidadosos, las cosas pueden salir mal. La capacidad de un buen administrador se demuestra a través de su habilidad para analizar, diagnosticar las fallas y corregir los problemas de la red trabajando bajo presión, cuando se produce una falla que hace que la empresa pierda horas de trabajo. Las buenas técnicas de administración de red son las que salen a relucir. Las siguientes sugerencias analizan estas técnicas, al igual que otras herramientas para diagnosticar las fallas de una red. Lo siguiente es un repaso de algunas técnicas ya conocidas y otras adicionales para diagnosticar las fallas de una red. Estas técnicas, como se explicó anteriormente, pueden ser las mejores herramientas para resolver los problemas de las redes.

Lo primero y lo más importante es el uso del diario de ingeniería y las notas. La toma de notas puede representar la mejor manera de diagnosticar un problema. Las notas describen las alternativas que ya se han probado y qué efecto tuvieron sobre el problema. Esto puede ser sumamente valioso para el técnico, ya que de esta manera lo que se intentó con anterioridad no vuelve a utilizarse inútilmente para resolver el problema tiempo después.

La toma de notas también es muy valiosa si el problema se deriva a otro técnico, para evitar que el nuevo técnico tenga que volver a hacer todo lo que ya se hizo anteriormente. Se debe incluir una copia de estas notas junto con los documentos de solución del problema cuando se complete el informe de problemas sobre esta tarea en particular. Esto puede proporcionar material de consulta si se presentan otros problemas similares relacionados con este problema en particular.

Otro de los elementos esenciales del diagnóstico preventivo de fallas es la rotulación. Se debe rotular todo, incluyendo ambos extremos de un tendido de cable horizontal. La rotulación debe incluir no sólo el número del cable sino también donde se ubica el otro extremo y el uso del cable, por ejemplo, voz, datos o vídeo. Este tipo de rótulo puede ser aun más valioso que un plan de distribución de cableado para realizar el diagnóstico de fallas, porque se ubica donde está la unidad misma y no en un cajón en alguna parte. Junto con los rótulos de cables, la rotulación de cada puerto en un hub, switch o router en lo que se refiere a la ubicación, propósito y punto de conexión mejorará enormemente las posibilidades de resolver problemas. Por último, todos los demás componentes conectados a la red también se deben rotular, incluyendo en el rótulo su ubicación y propósito. Con este tipo de rótulo, todos los componentes pueden ubicarse y su propósito en la red es fácilmente definido. La rotulación correcta, en conjunto con la documentación de la red que se prepara en el momento de su desarrollo y actualización, ofrece un panorama completo de la red y sus relaciones. Otra cosa importante que debe recordar es que la documentación sólo sirve si está actualizada. Todos los cambios realizados en la red deben documentarse, tanto en los dispositivos o cables que se cambian como en los documentos en papel utilizados para definir toda la red.

El primer paso en el diagnóstico de fallas de la red es la definición del problema. Esta definición puede unir la información proveniente de distintas fuentes. Una de las fuentes puede ser un informe de problema o informe de la mesa de ayuda, que identifica inicialmente el problema. Otra fuente puede ser una conversación telefónica con el usuario que tiene el problema, para reunir más información acerca del problema. Las herramientas de monitoreo de la red pueden proporcionar una noción más completa acerca del problema específico que debe resolverse. También se puede obtener información de otros usuarios y las observaciones propias. La evaluación de toda esta información brinda al técnico una base para resolver el problema mucho más clara que si se utiliza una sola de cualquiera de estas fuentes.

HERRAMIENTAS DE SOFTWARE.

Junto con los procesos que se describen anteriormente, hay herramientas de software disponibles para que el administrador de red pueda resolver los problemas de conectividad de la red. Estas herramientas pueden ayudar en el diagnóstico de fallas de las redes de área local, pero son especialmente útiles para resolver los problemas de las redes de área amplia.

Analizaremos los comandos disponibles para un administrador de red en la mayoría de los paquetes de software cliente. Entre estos comandos se incluyen `Ping`, `Tracert (Traceroute)`, `Telnet`, `Netstat`, `ARP` y `IPconfig (WinIPcfg)`.

Ping

Envía paquetes de eco ICMP para verificar las conexiones a un host remoto. El resultado muestra si el ping fue exitoso. El resultado muestra la cantidad de paquetes a los que se respondió y el tiempo de retorno del eco.

```
Ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-r
count] destination
```

`-t`	ping hasta interrumpirse
`-a`	resuelve nombre de host y dirección de ping
`-n`	resuelve nombre de host y dirección de ping
`-l`	longitud - enviar paquetes de eco de un tamaño especificado
`-f`	comando NO FRAGMENTAR enviado a los gateways
`-i`	ttl establece el campo TTL
`-r`	el recuento registra la ruta de los paquetes que salen y que vuelven
`destination`	especifica el host remoto al que se debe hacer ping, por nombre de dominio o por dirección IP

Tracert(Traceroute)

Esta utilidad muestra la ruta que siguió un paquete para alcanzar su destino. El resultado siguiente muestra el comando `trace`.

```
Tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
target_name
```

`-d` especifica las direcciones IP que no se deben resolver a nombres de host

`-h` max_hops Cantidad máxima de saltos buscados

`-j` lista de host especifica la ruta origen suelto

`-w` el tiempo de espera determina la cantidad de milisegundos especificados para cada respuesta

Telnet

Este es un programa de emulación de terminal que le permitirá ejecutar comandos interactivos en el servidor telnet. Hasta que se establece una conexión, no pasa ningún dato, y si la conexión se interrumpe, telnet lo informa.

Es bueno para probar los parámetros de configuración de conexión a un host remoto. Telnet [destino (IP o nombre DNS)]

Netstat Muestra estadísticas de protocolo y conexiones de red TCP/IP actuales.

```
Netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

-a	Muestra todas las conexiones y puertos que escuchan. (Las conexiones del lado del servidor normalmente no se muestran).
-e	Muestra estadísticas de Ethernet. Esto se puede combinar con la opción -s.
-n	Muestra direcciones y números de puerto en forma numérica.
-p proto	Muestra conexiones para el protocolo especificadas por protocolo. El protocolo puede ser tcp o udp. Si se usa con la opción -s para mostrar estadísticas por protocolo, el protocolo puede ser tcp, udp o ip.
-r	Muestra el contenido de la tabla de enrutamiento.
-s	Muestra estadísticas por protocolo. Por defecto, se muestran las estadísticas para TCP, UDP e IP. La opción -p se puede usar para especificar un subconjunto de las opciones por defecto.
interval	Vuelve a mostrar estadísticas seleccionadas, con segundos de intervalo entre cada visualización. Presione CONTROL+C para detener la nueva visualización de las estadísticas. Si se omite, Netstat imprime la información de configuración actual una vez.

ARP

Se usa para reunir direcciones de hardware para los hosts locales y el gateway por defecto, se puede ver el caché ARP y verificar la existencia de entradas no válidas o duplicadas

```
arp -a [inet_addr] [-N [if_addr]]
arp -d inet_addr [if_addr]
arp -s inet_addr ether_addr [if_addr]
```

`-a o -g` Muestra el contenido actual del caché arp

`-d` Elimina la entrada especificada por inet_addr

`-s` Agrega una entrada estática al caché

`-N` Muestra las entradas arp para la dirección física especificada

`inet_addr` dirección IP, en el formato decimal separado por puntos

`if_addr` Dirección IP cuyo caché debe modificarse

`ether_addr` Dirección MAC en formato hexadecimal separado por guiones

IPconfig (Windows NT)/WinIPcfg (Windows 95-98) Estas utilidades Windows muestran información de direccionamiento IP para el adaptador(es) de red local o una NIC especificada.

```
IPconfig [/all | /renew [adapter] | /release [adapter]]
```

`/all` toda la información acerca del adaptador(es)

`/renew` renovar la información de arrendamiento de DHCP para todos los adaptadores locales si no se nombra ninguno

`/release` liberar información de arrendamiento DHCP inhabilitando TCP/IP en este adaptador

Estas son las herramientas que permiten que un administrador de red monitoree y controle la red de forma remota. Es importante implementar las medidas de seguridad correctas al utilizar SNMP y RMON para que no haya violaciones a la seguridad de la red.

Herramientas de administración y monitorización

La interfaz de administración del servidor NOS proporciona las herramientas para la monitorización del servidor y la administración de clientes, ficheros, impresoras y almacenamiento de disco. También ofrece formas para la instalación de nuevos servicios y su configuración. Además, los servidores precisan de una monitorización y ajustes regulares.

SEGURIDAD.

Un NOS debe proteger los recursos compartidos que están bajo su control. La seguridad incluye la autenticación de los usuarios que pretenden acceder a los servicios para prevenir acceso no autorizado a los mismos. También se encarga de encriptar la información que viaja entre los clientes y los servidores.

ESCALABILIDAD.

Es la capacidad del NOS para crecer sin degradar su rendimiento. Debe ser capas de mantener su rendimiento cuando se incorporen nuevos usuarios a la red y al añadir nuevos servidores capaces de soportarlos.

ROBUSTEZ / TOLERANCIA A LOS FALLOS.

Un indicador de robustez es la capacidad de ofrecer servicios NOS de forma consistente bajo condiciones de carga extrema y de mantener dichos servicios cuando algún componente o proceso falla.

La siguiente sección trata de los distintos NOS que ofrece Microsoft.

WINDOWS 2000.

Windows 2000 Professional es el sistema operativo de Microsoft mas reciente orientado a computadoras de escritorio corporativas. Al igual que los productos Windows 2000 Server, Windows 2000 esta basado en el **kernel** NT e incluye muchas características avanzadas. Por Ej. Ofrece un alto nivel de seguridad y estabilidad para tareas criticas.

La siguiente es una lista de ventajas que Windows 2000 Professional tiene como sistema operativo de escritorio y como cliente de red.

- ✓ Ofrece soporte a usuarios móviles a través de APM (gestión avanzada de energía) y ACPI (interfaz de energía y configuración avanzada) Windows NT no soporta ACPI.
- ✓ Ofrece una VPN (red privada virtual) mas segura a través de L2TP (protocolo de tunneling de capa 2) e IPSec (seguridad IP). Las primeras versiones de Windows solo soportaban PPTP (protocolo de tunneling punta a punto) para las VPN.

- ✓ La característica de carpeta sin conexión permite a los usuarios copiar y sincronizar documentos desde la red al sistema local para que estos estén accesibles cuando la computadora este desconectada de la red.
- ✓ El IPP (protocolo de impresión Internet) permite a los usuarios imprimir una URL (localizador universal de recursos) y administrar impresoras a través de un navegador Web.
- ✓ Los desfragmentadores de disco integrados y otras herramientas y utilidades ayudan a los usuarios a mantener y administrar el sistema operativo. Estas herramientas debe adquirirse por separado a terceras partes para Windows NT.
- ✓ Soporta seguridad **Kerberos** (desarrollando una norma para autenticar a los usuarios de red) y las características de un dominio Windows 2000 como un cliente active directory.
- ✓ Ofrece una administración de cuentas más fácil y eficaz.

WINDOWS 2000 SERVER.

Es una opción ideal para redes de pequeño y mediano tamaño e incluye muchas funciones específicas de servidor, como ficheros, impresión y servicios Web, así como servicios de servidor de aplicaciones. Lo que lo diferencia a las demás versiones de servidores previas de Microsoft es un completo conjunto de funciones de infraestructura basadas en el servicio Active Directory.

WINDOWS 2000 ADVANCED SERVER.

El Server y advanced Server son lo mismo acepto que el segundo proporciona soporte para el hardware y el software que un administrador de sistemas necesita en una red empresarial. Advanced Server es un sistema operativo de servidor mas potente, departamental y de servidor de aplicaciones que incluye todas las funciones de Windows 2000 Server y añade la alta disponibilidad avanzada y la escalabilidad mejorada que es necesaria para redes más grandes.

WINDOWS .NET SERVER.

Microsoft ha desarrollado Windows . NET Server con la intención de ofrecer un sistema fiable y seguro para ejecutar sitios Web de empresas y FTP que pueda compartir con **Linux** y **UNIX.** Sin embargo, Windows . NET Server proporciona características únicas. Por Ej. Con la explosión del comercio electrónico y las empresas basadas en Web y las compañías que están expandiendo sus servicios de Internet, existe una importante demanda del sistema operativo capaz de proporcionar servicios Web y de FTP fiables.

UNIX Y LINUX.

Aunque similares, tienen algunas importantes diferencias entre ellas:

UNIX.

Es un grupo de sistemas operativos que tienen su origen hacia 1969 en Bell Lab. Fue diseñado para soportar múltiples usuarios y multitarea, y también fue uno de los primeros sistemas operativos en incluir soporte para protocolos de red de Internet.

Cuando comenzó a comercializarse por los años 80 fue utilizado en potentes servidores de red y no en computadoras de escritorio. En la actualidad, existen una gran cantidad de distintas versiones de UNIX:

- ✓ HP – UX (UNIX de hewlett Packard).
- ✓ Berkeley software design, inc., (BSD UNIX, del cual se a derivado otras versiones como FreeBSD).
- ✓ Santa Cruz operation (SCO) UNIX.
- ✓ Sun Solares.
- ✓ AIX (UNIXZ de IBM).

En general, UNIX y todas sus variantes continúan siendo la elección principal como sistema operativo fiable y seguro para aquellas aplicaciones cruciales en la operativa de la empresa o el negocio. Además, esta firmemente integrado con TCP / IP, el cual creció gracias a UNIX debido a las necesidades de comunicaciones LAN y WAN. A pesar de la popularidad de Microsoft Windows en las LAN corporativas, una gran parte de Internet funciona en sistemas UNIX. Aunque este sistema operativo esta asociado a hardware de alto coste y esta considerado como "poco amigable para el usuario" desarrollos mas recientes como Linux están cambiando esta imagen.

LINUX.

Al igual que UNIX, Linux dispone de numerosas versiones. Algunas son gratuitas y pueden descargarse desde la Web, y otras son de pago a continuación puede ver una lista de las versiones mas populares.

- ✓ RedHat Linux, distribuida por RedHat software.
- ✓ SCOLinux, distribuida por SCO.
- ✓ Xandros Linux.
- ✓ Slackware.
- ✓ Debian GNU / Linux.
- ✓ SuSE Linux.

Linux es uno de los sistemas operativos más fiables y potentes del mundo. Gracias a ello, ha invadido las computadoras de usuarios ansiosos de más potencia y el entorno de los servidores de empresa. Sin embargo, su aceptación como sistema operativo de computadoras de escritorio corporativas es menor.

Cuando Linux esta implementando en un sistema de escritorio, hay que tener muy en cuenta que el número de aplicaciones existentes es considerablemente menor que para Windows. Sin embargo, algunos fabricantes ofrecen software de emulación de Windows (como WABI y WINE) que permite que muchas aplicaciones Windows se ejecuten en linux. Además, empresas como Corel están preparando versiones Linux de sus paquetes de software mas conocidos.

DIRECCIONAMIENTO LÓGICO

- ✓ **Servidor DNS.**
- ✓ **Servidor E-mail.**
- ✓ **Servidor administrativo.**
- ✓ **Servidor aplicaciones.**
- ✓ **Profesores.**
- ✓ **Personal administrativo.**
- ✓ **Biblioteca.**
- ✓ **Laboratorios.**
- ✓ **Alumnos.**
- ✓ **Internet.**

TOPOLOGÍA

IP 192.168.0.0

DIRECCIONAMIENTO DE REDES					
# de subred	**subdirección de red**		**descripción**	**rango de host**	**host**
1	192,168,2,16/28		Administrativo	192,168,2,0 - 192,168,2,15	14
2	192,168,2,32/28		Profesores	192,168,2,16 - 192,168,2,32	14
3	192,168,2,64/28	192,168,2,64/29	Militar	192,168,2,64 - 192,168,2,71	6
4		192,168,2,72/29	Servidor	192,168,2,72 - 192,168,2,79	6
5		192,168,2,80/29	Audiovisuales	192,168,2,80 - 192,168,2,87	6
6	192,168,3,0/24		Alumnos	192,168,3,0 - 192,168,3,254	126

SERVIDORES:

DNS : 192.168.2.72/30

Administrativo : 192.168.2.76/30

E-mail : 192.168.2.80/30

Aplicaciones : 192.168.2.84/30

Notas : 192.168.2.88/30

Internet : 192.168.2.92/30

LISTA DE ACCESO

ROUTER	INTERFAZ	# ACL	SERVICIO PERMITIDO
	192,168,2,16/28 Vlan_ Administrativo	101	Servicio Administrativo, DNS, Internet, Aplicaciones, E-mail
	192,168,2,32/28 Vlan_ Profesores	102	Servicio Administrativo, DNS, Notas Internet, Aplicaciones, E-mail
	192,168,2.64/28 Vlan_ Militar	103	DNS, Administrativo, Aplicaciones, E-mail, Internet
	192,168,2.72/29	104	DNS, Administrativo, Aplicaciones,
	Vlan_ Servidores		E-mail, Internet
	192,168,2.80/29	105	DNS, Administrativo, Aplicaciones,
	Vlan_ Audiovisuales		E-mail, Internet
	192,168,3.0/24	106	DNS, Aplicaciones, E-mail, Internet
	Vlan_ Alumnos		

La red alumnos debe acceder DNS, Correos, Aplicaciones e Internet.

Access – List 106 Permit IP 192.168.3.0 0.0.0.255 host 192.168.2.72 0.0.0.3

Access – List 106 Permit IP 192.168.3.0 0.0.0.255 host 192.168.2.80 0.0.0.3

Access – List 106 Permit IP 192.168.3.0 0.0.0.255 host 192.168.2.84 0.0.0.3

Access – List 106 Permit IP 192.168.3.0 0.0.0.255 host 192.168.2.92 0.0.0.3

La red alumnos no debe acceder a ninguna nomina de la red administrativa.

Access_list 106 Deny 192.168.3.0 0.0.0.255 192.168.2.16 0.0.0.15

La red alumnos no debe acceder al servidor administrativo.

Access_list 106 Deny 192.168.3.0 0.0.0.255 192.168.2.76 0.0.0.15

La red alumnos no debe acceder al servidor de notas.

Access_list 106 Deny 192.168.3.0 0.0.0.255 192.168.2.88 0.0.0.15

La red de alumnos no debe acceder a la red militar.

Access_list 104 Deny 192.168.3.0 0.0.0.255 192.168.2.64 0.0.0.15

Acceso a la red servidores 192.168.6.0 para todos los usuarios del colegio.

Access_list 101 Permit IP 192.168.2.16 0.0.0.249 192.168.2.96 0.0.0.255

La red de profesores debe acceder a servidores de notas, aplicaciones, DNS, correo, e Internet.

Access_list 102 Permit IP 192.168.2.32 0.0.0.15 192.168.2.88 0.0.0.3

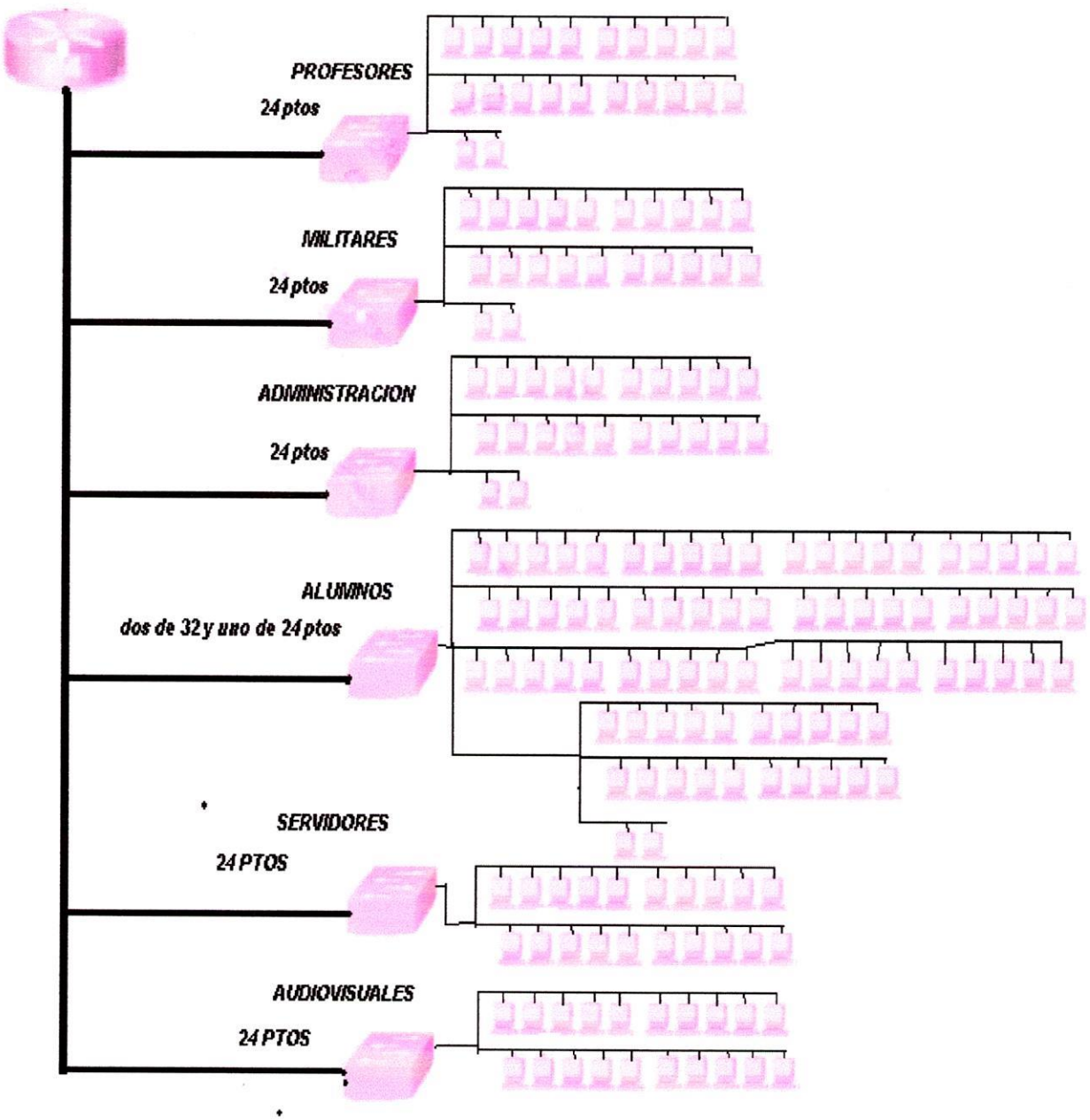
Access_list 102 Permit IP 192.168.2.32 0.0.0.15 192.168.2.84 0.0.0.3

Access_list 102 Permit IP 192.168.2.32 0.0.0.15 192.168.2.72 0.0.0.3

Access_list 102 Permit IP 192.168.2.32 0.0.0.15 192.168.2.80 0.0.0.3

Access_list 102 Permit IP 192.168.2.32 0.0.0.15 192.168.2.92 0.0.0.3

TOPOLOGÍA LÓGICA



CONEXIÓN	SALÓN	CONEXIÓN CRUZADA		ESTADO
		CABLE	# DE PUERTO	
IDF 1 A	SALA PROFESORES	HCCI	3	ACTIVO
IDF 1 A	SALA PROFESORES	HCCI	4	ACTIVO
IDF 1 A	SALA PROFESORES	HCCI	5	ACTIVO
IDF 1 A	SALA PROFESORES	HCCI	6	ACTIVO
IDF 1 A	SALA PROFESORES	HCCI	7	ACTIVO
IDF 1 A	SALA PROFESORES	HCCI	8	INACTIVO
IDF 1 A	SALA PROFESORES	HCCI	9	INACTIVO
IDF 1 A	SALA PROFESORES	HCCI	10	INACTIVO
IDF 1 A	SALA PROFESORES	HCCI	11	INACTIVO
IDF 1 A	SALA PROFESORES	HCCI	12	INACTIVO
IDF 1 A	BIBLIOTECA	HCCI	13	ACTIVO
IDF 1 A	BIBLIOTECA	HCCI	14	ACTIVO
IDF 1 A	BIBLIOTECA	HCCI	15	ACTIVO
IDF 1 A	BIBLIOTECA	HCCI	16	ACTIVO
IDF 1 A	SALON 201	HCCI	17	ACTIVO
IDF 1 A		HCCI	18	INACTIVO
IDF 1 A	SALON 202	HCCI	19	ACTIVO
IDF 1 A		HCCI	20	INACTIVO
IDF 1 A	AUDIOVISUALES	HCCI	21	ACTIVO
IDF 1 A		HCCI	22	INACTIVO
IDF 1 A	SALON 301	HCCI	23	ACTIVO
IDF 1 A		HCCI	24	INACTIVO
IDF 1 B	O. MILITARES	HCCI	3	ACTIVO
IDF 1 B	O. MILITARES	HCCI	4	ACTIVO
IDF 1 B	O. MILITARES	HCCI	5	ACTIVO
IDF 1 B	O. MILITARES	HCCI	6	ACTIVO
IDF 1 B	O. MILITARES	HCCI	7	ACTIVO
IDF 1 B	O. MILITARES	HCCI	8	ACTIVO
IDF 1 B	R. INTERNO	HCCI	9	ACTIVO
IDF 1 B		HCCI	10	INACTIVO
IDF 1 B	D. MILITAR	HCCI	11	ACTIVO
IDF 1 B		HCCI	12	INACTIVO
IDF 1 B	SALONES 203	HCCI	13	ACTIVO
IDF 1 B	SALONES 203	HCCI	14	INACTIVO
IDF 1 B	SALONES 204	HCCI	15	ACTIVO
IDF 1 B	SALONES 204	HCCI	16	INACTIVO
IDF 1 B	SALONES 205	HCCI	17	ACTIVO
IDF 1 B	SALONES 205	HCCI	18	INACTIVO
IDF 1 B	SALONES 206	HCCI	19	ACTIVO
IDF 1 B	SALONES 206	HCCI	20	INACTIVO
IDF 1 B	SALONES 207	HCCI	21	ACTIVO
IDF 1 B	SALONES 207	HCCI	22	INACTIVO
IDF 1 B	SALONES 208	HCCI	23	ACTIVO
IDF 1 B	SALONES 208	HCCI	24	INACTIVO

CONEXIÓN	SALÓN	CONEXIÓN CRUZADA		ESTADO
		CABLE	# DE PUERTO	
IDF 2 A	RECTOR	HCCI	3	ACTIVO
IDF 2 A		HCCI	4	INACTIVO
IDF 2 A	SUBDIRECTOR	HCCI	5	ACTIVO
IDF 2 A		HCCI	6	INACTIVO
IDF 2 A	SECRETARIA	HCCI	7	ACTIVO
IDF 2 A		HCCI	8	ACTIVO
IDF 2 A	C. ACADEMICA	HCCI	9	ACTIVO
IDF 2 A		HCCI	10	INACTIVO
IDF 2 A	SALON 303	HCCI	11	ACTIVO
IDF 2 A	SALON 303	HCCI	12	INACTIVO
IDF 2 A	SALON 304	HCCI	13	ACTIVO
IDF 2 A	SALON 304	HCCI	14	INACTIVO
IDF 2 A	SALON 305	HCCI	15	ACTIVO
IDF 2 A	SALON 305	HCCI	16	INACTIVO
IDF 2 A	SALON 306	HCCI	17	ACTIVO
IDF 2 A	SALON 306	HCCI	18	INACTIVO
IDF 2 A	SALON 307	HCCI	19	ACTIVO
IDF 2 A	SALON 307	HCCI	20	INACTIVO
IDF 2 A	SALON 308	HCCI	21	ACTIVO
IDF 2 A	SALON 308	HCCI	22	INACTIVO
IDF 2 A	SALON 309	HCCI	23	ACTIVO
IDF 2 A	SALON 309	HCCI	24	INACTIVO
IDF 2 B	SALON 302	HCCI	3	ACTIVO
IDF 2 B	SALON 302	HCCI	4	INACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	5	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	6	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	7	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	8	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	9	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	10	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	11	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	12	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	13	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	14	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	15	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	16	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	17	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	18	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	19	ACTIVO
IDF 2 B	S. SISTEMAS 3	HCCI	20	ACTIVO
IDF 2 B	LAB. FISICA	HCCI	21	ACTIVO
IDF 2 B		HCCI	22	INACTIVO
IDF 2 B	LAB. QUIMICA	HCCI	23	ACTIVO
IDF 2 B		HCCI	24	INACTIVO

conexión	salón	conexión cruzada		estado
		cable	# de puerto	
IDF 3 A	S. SISTEMAS 4	HCCI	3	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	4	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	5	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	6	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	7	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	8	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	9	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	10	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	11	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	12	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	13	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	14	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	15	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	16	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	17	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	18	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	19	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	20	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	21	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	22	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	23	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	24	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	25	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	26	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	27	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	28	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	29	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	30	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	31	ACTIVO
IDF 3 A	S. SISTEMAS 4	HCCI	32	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	3	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	4	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	5	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	6	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	7	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	8	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	9	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	10	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	11	ACTIVO
IDF 3 B	S. SISTEMAS 4	HCCI	12	ACTIVO
IDF 3 B	SALON 401	HCCI	13	ACTIVO
IDF 3 B	SALON 401	HCCI	14	INACTIVO
IDF 3 B	SALON 402	HCCI	15	ACTIVO
IDF 3 B	SALON 402	HCCI	16	INACTIVO

IDF 3 B	SALON 403	HCCI	17	ACTIVO
IDF 3 B	SALON 403	HCCI	18	INACTIVO
IDF 3 B	SALON 404	HCCI	19	ACTIVO
IDF 3 B	SALON 404	HCCI	20	INACTIVO
IDF 3 B	SALON 405	HCCI	21	ACTIVO
IDF 3 B	SALON 405	HCCI	22	INACTIVO
IDF 3 B	SALON 406	HCCI	23	ACTIVO
IDF 3 B	SALON 406	HCCI	24	INACTIVO
IDF 3 B	AUDITORIO	HCCI	25	ACTIVO
IDF 3 B	AUDITORIO	HCCI	26	INACTIVO

CRONOGRAMA DE ACTIVIDADES					
ACTIVIDAD	**DESCRIPCIÓN**	**LUGAR**	**DURACIÓN**		**FECHA**
			HORAS	**DÍAS**	
Reunión grupo de trabajo	Aclarar puntos	Unitec	tres	uno	Sep. 15 / 04
Toma de la información	Equipos del Colegio	Colegio	una	dos	Sep. 22 y 23 / 04
Análisis de la información	Equipos del Colegio	Unitec	tres	uno	Sep. 27 / 04
Encuesta profesores	Encuesta	Colegio	dos	uno	Sep. 30 / 04
Reunión grupo de trabajo	Inicio del proyecto	Unitec	cuatro	uno	Oct. 7 / 04
Reunión grupo de trabajo	Costos del proyecto	Unilago	dos	uno	Oct. 11 / 04
Reunión grupo de trabajo	Proveedores de Internet	Múltiples	una	tres	Oct. 13, AL 15 / 04
Reunión grupo de trabajo	Adelantos del proyecto	Unitec	una	dos	Oct. 21 y 22 / 04
Reunión grupo de trabajo	Preentrega del proyecto	Unitec	una	uno	Oct. 29 / 04
Reunión grupo de trabajo	Arreglos al Proyecto	Unitec	tres	uno	Nov. 3 / 04
Reunión grupo de trabajo	Preentrega del proyecto	Unitec	una	uno	Nov. 16 / 04
Reunión grupo de trabajo	Arreglos al Proyecto	Unitec	dos	cuatro	Nov. 22 al 25 / 04
Reunión grupo de trabajo	Preentrega del proyecto	Unitec	una	uno	Nov. 29 / 04
Reunión grupo de trabajo	Arreglos al Proyecto	Unitec	dos	tres	Dic. 1, 2, 3 / 04
Reunión grupo de trabajo	Preentrega del proyecto	Unitec	tres	uno	Dic. 6 / 04
Presentación publica	Exposición	Unitec	tres	uno	Dic. 15 / 04

COSTOS DE ESTUCIO DEL PROYECTO

Materiales	**Justificación**	**Valor**
Arquitecto.	Planos de la red	$135000
Ingeniero.	Diseño	$150000
Metro.	Toma de medidas.	$20.000
	total	$305000

PROVEEDORES DE INTERNET						
Proveedor / Plan	**Tecnología**	**Velocidad**	**Tarifa mensual**	**Otros costos**	**Valores agregados**	**Ciudades**
ETB / Internet Extremo	ADSL	128 Kbps	78.000 pesos	Conexión: desde 30.000 hasta 150.000; módem en comodato, o 250.000 sin contrato anual	Cinco cuentas de correo de 15 MB, portal de banda ancha	Bogotá
		256 Kbps	116.000			
EPM.Net / Banda Ancha Residencial	ADSL	128 Kbps	95.000	Conexión: 114.000		
		256 Kbps	120.000	Conexión: 170.000		Medellín, Bogotá, Manizales, Pereira
		384 Kbps	180.000	Conexión: 255.000	3-4 cuentas de correo de 60 MB	
Emcali	ADSL	128 Kbps	119.000	Conexión: 200.000;		
		256 Kbps	174.000			
		384 Kbps	297.000	módem: 220.000		
		512 Kbps	428.000			
Cablenet	Cable	64 Kbps	88.000			
		128 Kbps	135.000			Bogotá
		256 Kbps	160.000			
Supercable	Cable	90 Kbps	80.000			
		128 Kbps	98.000			Bogotá
		256 Kbps	145.000			
Axesat	Satelital	64 Kbps	780.000	Conexión: desde 700.000		Todo el país (incluidas zonas rurales)

Nota:

- Precios en pesos. No incluyen IVA.
- La tabla no incluye promociones especiales.
- Los operadores de cable tienen precios especiales para usuarios de su servicio de televisión.

GEONET S.A.

Es una sociedad anónima creada con capital privado que se gestó a mediados de 1997, cuando un grupo de profesionales de diferentes áreas empezó a realizar un proyecto de inversión cuyo objetivo era crear una empresa Proveedora de Servicios de Internet. Después de realizar algunos estudios de carácter técnico, comercial, administrativo, legal y financiero, se cristalizó la idea y en mes de abril de 1998 se dio vía libre para su ejecución.

Su objeto es la prestación de servicios de valor agregado de telecomunicaciones, acceso personal e inalámbrico a Internet y la unidad de Negocios Web encargada del desarrollo de un sitio Web rentable de contenido local, que satisface todas las necesidades de información que el visitante tenga.

Es la conexión de un equipo o una comunidad de equipos ubicados en una misma área, permitiendo compartir el recurso de Internet entre ellos. El servicio dedicado de Internet es prestado a través de últimas millas diferentes a las utilizadas por los servicios de telefonía básica conmutada, es decir inalámbrico, satélite, cable MODEM, tecnologías xDSL o fibra.

Valor Agregado

Con un canal dedicado a Internet el usuario tiene el servicio siempre disponible (las 24 horas del días) y solo tiene que utilizar el explorador de su PC, para disfrutar e los diferentes servicios de Internet. En los servicios dedicados no hay cargos adicionales proporcionales al consumo, es un cargo básico mensual.

PLANES:

SPEED CORPORATE

Este servicio está dirigido a medianas y grandes empresas, que requieran acceso a Internet de alta velocidad (Acceso de banda ancha).
El servicio es entregado al cliente bajo las configuraciones pre-establecidas por GeoNet.
Se instala una antena para cada una de las sedes del cliente, ubicadas en el área de cobertura.

Características

Ancho de banda desde **128 Kbps** hasta **3 Mbps** en condiciones normales y 6 en condiciones especiales.

Venta o arriendo de Enrutador.

20 Buzones de correo de 40 MB cada uno, **Webmail**.

Capacitaciones especializadas en Internet.

Asistencia Técnica Telefónica las 24 horas del día en el 44 44 555 en Medellín y 01 8000 120111 en el resto del país.

Servicios en línea.

Hospedaje de 20 MB para su página.

Dominio propio www.empresa.com

IP Pública fija.

Beneficios

Los tiempos de Uploads y Download pasarán de Minutos a Segundos.

No hay tiempos de espera.

No necesitará otra línea telefónica.

No hay cargos por tiempos de conexión.

Libere su línea telefónica para hacer negocios.

Rápidos tiempos de instalación.

Monitoreo permanente de sus servicios

Router propio o arrendado

Niveles de Servicio Garantizados.

Servicio Ilimitado.

TV CABLE - CABLE NET

Cable net negocios - 400 kbps. up 200 kbps

Correo de 250 Mb

Cable net negocios - 800 kbps. up 400 kbps

Correo de 500 Mb

Cable net negocios - 1200 kbps. up 500 kbps

Correo de 750 Mb

Cable net negocios - 1800 kbps. up 600 kbps, Correo de 1000 Mb

IMPACTO AMBIENTAL

ARTÍCULO 49. Modificado Decreto 1122 de 1999, Art. 89. Modificado Estatuto Antitramitologia, Art. 49. **Licencia ambiental.** Requerirán Licencia ambiental para su ejecución los proyectos, obras o actividades, que puedan generar deterioro grave al medio ambiente, a los recursos naturales renovables o al paisaje, de conformidad con el artículo siguiente.

ARTÍCULO 50. De la licencia ambiental. Se entiende por licencia ambiental la autorización que otorga la autoridad ambiental competente para la ejecución de una obra o actividad, sujeta al cumplimiento por el beneficiario de la licencia de los requisitos que la misma establezca en relación con la prevención, mitigación, corrección, compensación y manejo de los efectos ambientales de la obra o actividad autorizada.

ARTÍCULO 51. Competencia. Las licencias ambientales serán otorgadas por el Ministerio del Medio Ambiente, las corporaciones autónomas regionales y algunos municipios y distritos, de conformidad con lo previsto en esta ley.

En la expedición de las licencias ambientales y para el otorgamiento de los permisos, concesiones y autorizaciones se acatarán las disposiciones relativas al medio ambiente y al control, la preservación y la defensa del patrimonio ecológico, expedidas por las entidades territoriales de la jurisdicción respectiva.

ARTÍCULO 52. Modificado Decreto 1122 de 1999, Art. 90, Modificado Estatuto Antitramitologia, Art. 50 . **De la exigencia de licencia ambiental**.

El Ministerio del Medio Ambiente otorgará licencia ambiental respecto de las siguientes actividades:

- ✓ Explotación, transporte, conducción y depósito de hidrocarburos, y construcción de refinerías.
- ✓ Proyectos de gran minería.
- ✓ Proyectos de generación y transmisión de energía eléctrica de orden nacional.
- ✓ Proyectos de infraestructura vial, fluvial y ferroviaria nacional; infraestructura aeroportuaria de carácter internacional; proyectos portuarios de gran calado.
- ✓ Producción e importación de plaguicidas.
- ✓ Importación, tratamiento, disposición y eliminación de sustancias, productos o materiales regulados por Tratados, Convenios y Protocolos Internacionales de carácter ambiental.
- ✓ Proyectos en áreas del Sistema de Parques Nacionales Naturales.
- ✓ Proyectos que requieran licencia ambiental y que adelanten las Corporaciones Autónomas Regionales y de Desarrollo Sostenible o los grandes centros urbanos.
- ✓ Generación de energía nuclear.
- ✓ Introducción de especies foráneas de fauna y flora silvestre y microorganismos.
- ✓ Transvases de una cuenca a otra de corrientes de agua que excedan de 2 mt3/segundo durante los períodos de mínimo caudal.

PARAGRAFO 1. La facultad de otorgar licencias ambientales para la construcción de puertos se hará sin perjuicio de la competencia legal de la Superintendencia General de Puertos y Transporte de otorgar concesiones portuarias. No obstante la licencia ambiental es prerrequisito para el otorgamiento de concesiones portuarias.

PARAGRAFO 2. El Ministerio del Medio Ambiente podrá definir mecanismos e instrumentos administrativos de prevención, control y seguimiento ambiental para la ejecución de proyectos, obras o actividades que no generen impactos significativos al medio ambiente, los recursos naturales renovables o al paisaje

ARTÍCULO 52 BIS Adicionado Decreto 1122 de 1999, Art. 91.**Mecanismos de prevención, control y seguimiento ambiental**. El Ministerio del Medio Ambiente podrá definir y regular mecanismos e instrumentos administrativos de prevención, control y seguimiento ambiental para la ejecución de proyectos, obras o actividades que no generen impactos significativos al medio ambiente, los recursos naturales renovables o al paisaje

ARTÍCULO 53. De la facultad de las corporaciones autónomas regionales para otorgar licencias ambientales. El Gobierno Nacional por medio de reglamento establecerá los casos en que las corporaciones autónomas regionales otorgarán licencias ambientales y aquellos en que se requiera estudio de impacto ambiental y diagnóstico ambiental de alternativas.

ARTÍCULO 54. Delegación. Las corporaciones autónomas regionales podrán delegar en las entidades territoriales el otorgamiento de licencias, concesiones, permisos y autorizaciones que les corresponda expedir, salvo para la realización de obras o el desarrollo de actividades por parte de la misma entidad territorial.

ARTÍCULO 55. De las competencias de las grandes ciudades. Los municipios, distritos y áreas metropolitanas cuya población urbana sea superior a 1.000.000 de habitantes serán competentes, dentro de su perímetro urbano, para el otorgamiento de licencias ambientales, permisos, concesiones y autorizaciones cuya expedición no este atribuida al Ministerio del Medio Ambiente.

ARTÍCULO 56. Modificado Decreto 1122 de 1999, Art. 92. Modificado Estatuto Antitramitologia, Art. 51 **Del diagnóstico ambiental de alternativas**.

En los proyectos que requieran de licencia ambiental, el interesado deberá solicitar en la etapa de factibilidad a la autoridad ambiental competente que ésta se pronuncie sobre la necesidad de presentar o no un diagnóstico ambiental de alternativas. Con base en la información suministrada la autoridad ambiental fijará en un término no mayor de 30 días hábiles, los términos de referencia para la elaboración del Diagnóstico Ambiental de Alternativas, salvo que los términos de referencia hayan sido definidos de manera genérica para la actividad por la autoridad ambiental.

El Diagnóstico Ambiental de Alternativas incluirá información sobre la localización y características del entorno geográfico, de las alternativas del proyecto, además de un análisis comparativo de los riesgos inherentes al proyecto sobre el medio ambiente y los recursos naturales. Con base en el Diagnóstico Ambiental de Alternativas presentado, la autoridad ambiental elegirá en un plazo no mayor a treinta (30) días, la alternativa o las alternativas sobre las cuales deberá elaborarse el correspondiente Estudio de Impacto Ambiental, antes de otorgarse la respectiva licencia. En el evento que la información o documentos que proporcione el interesado no sean suficientes para decidir, la autoridad ambiental le requerirá, por una sola vez, el aporte de lo que haga falta. Este requerimiento interrumpirá el término con que cuenta la autoridad para la elección de la alternativa.

PARÁGRAFO. Adicionado. Decreto 2150 de 1995, Art. 133. El Gobierno Nacional reglamentará los casos en los cuales la autoridad ambiental podrá prescindir de la exigencia del diagnóstico ambiental de alternativas.

ARTÍCULO 57. Modificado Decreto 1122 de 1999, Art. 93. Modificado Estatuto Antitramitologia, Art. 52 **Del estudio de impacto ambiental**. Se entiende por estudio de impacto ambiental el conjunto de la información, que deberá presentar ante la autoridad ambiental competente, el peticionario de una licencia ambiental.

El estudio de impacto ambiental contendrá información sobre la localización del proyecto y los elementos abióticos, bióticos y socioeconómicos del medio que puedan sufrir deterioro por el respectivo proyecto obra o actividad, para cuya ejecución se pide la licencia y la evaluación de los impactos que puedan producirse. Además, incluirá el diseño de los planes de manejo ambiental respectivos.

La autoridad ambiental competente para otorgar la licencia ambiental fijará los términos de referencia de los estudios de impacto ambiental en un término que no podrá exceder de treinta (30) días hábiles, contados a partir de la solicitud por parte del interesado, salvo que los términos de referencia hayan sido definidos de manera genérica para la actividad por la autoridad ambiental.

ARTÍCULO 58. Modificado Decreto 1122 de 1999, Art. 94. Modificado Estatuto Antitramitologia, Art. 53 El interesado en el otorgamiento de una licencia ambiental presentará ante la autoridad ambiental competente la solicitud acompañada del Estudio de Impacto Ambiental correspondiente para su evaluación. La autoridad competente dispondrá de quince (15) días hábiles para solicitar a otras entidades o autoridades los conceptos técnicos o informaciones pertinentes que deberán serle remitidos en un plazo no mayor a treinta (30) días hábiles.

Allegada la información y los conceptos técnicos requeridos, la autoridad competente dispondrá de quince (15) días hábiles para solicitar información adicional al interesado, en caso de requerirse. Recibida la información o vencido el término del requerimiento de informaciones adicionales, la autoridad ambiental decidirá mediante resolución motivada sobre la viabilidad ambiental del proyecto o actividad y otorgará o negará la respectiva licencia ambiental en un término que no podrá exceder de sesenta (60) días hábiles.

ARTÍCULO 59. De la licencia ambiental única. A solicitud del peticionario, la autoridad ambiental competente incluirá en la licencia ambiental, los permisos, concesiones y autorizaciones necesarias para adelantar la obra o actividad.

En los casos en que el Ministerio del Medio Ambiente sea competente para otorgar la licencia ambiental, los permisos, concesiones y autorizaciones relacionadas con la obra o actividad para cuya ejecución se pide la licencia, serán otorgados por el Ministerio del Medio Ambiente, teniendo en cuenta la información técnica suministrada por las corporaciones autónomas regionales, las entidades territoriales correspondientes y demás entidades del sistema nacional del ambiente.

ARTÍCULO 60. En la explotación minera a cielo abierto se exigirá, la restauración o la sustitución morfológica y ambiental de todo el suelo intervenido con la explotación por cuenta del concesionario o beneficiario del título minero, quien la garantizará con una póliza de cumplimiento o con garantía bancaria. El gobierno reglamentará el procedimiento para extender la póliza de cumplimiento o la garantía bancaria.

ARTÍCULO 61. Declarase la sabana de Bogotá, sus páramos, aguas, valles aledaños, cerros circundantes y sistemas montañosos como de interés ecológico nacional, cuya destinación prioritaria será la agropecuaria y forestal.

El Ministerio del Medio Ambiente determinará las zonas en las cuales exista compatibilidad con las explotaciones mineras, con base en esta determinación, la corporación autónoma regional de Cundinamarca, CAR, otorgará o negará las correspondientes licencias ambientales.

Los municipios y el Distrito Capital, expedirán la reglamentación de los usos del suelo, teniendo en cuenta las disposiciones de que trata este artículo y las que a nivel nacional expida el Ministerio del Medio Ambiente.

ARTÍCULO 62. De la revocatoria y suspensión de las licencias ambientales. La autoridad ambiental, salvo los casos de emergencia, podrá mediante resolución motivada, sustentada en concepto técnico, revocar o suspender la licencia ambiental, los permisos, autorizaciones o concesiones para el uso o aprovechamiento de los recursos naturales y del medio ambiente, cuando quiera que las condiciones y exigencias por ella establecidas no se estén cumpliendo conforme a los términos definidos en el acto de su expedición.

La revocatoria o suspensión de una licencia ambiental no requerirá consentimiento expreso o escrito del beneficiario de la misma.

La suspensión de obras por razones ambientales, en los casos en que lo autoriza la ley, deberá ser motivada y se ordenará cuando no exista licencia o cuando, previa verificación del incumplimiento, no se cumplan los requisitos exigidos en la licencia ambiental correspondiente.

COSTOS PROYECTO

COSTOS CAT 5				
PARTE	**DESCRIPCION**	**VALOR UNIDAD**	**CANTIDAD**	**VALOR**
Cable UTP	Metro	$ 500	400 M.	$ 175.250
Conectores	RJ 45	$ 500	136	$ 67.500
Caja Patch Cord	1 metro	$ 130.000	1	$ 130.000
Accesorios	Unidad	$ 13.900		$ 13.900
	30 cm. de alto,			
Bastidor	50 cm. de frente	$ 130.000	1	$ 130.000
	60 cm. de profundidad			
Canaletas	plástica con división metro	$ 19.500	400 M.	$ 7.800.000
Rótulos	100 Unidades	$ 19.000	1 CAJA	$ 19.000
Toma de Datos sencilla	Unidad	$ 11.000	140	$ 1.540.000
Toma de Datos dobles	Unidad	$ 18.000	70	$ 1.260.000
Toma Eléctrica Sencilla	Unidad	$ 5.000	140	$ 700.000
Toma Eléctrica Dobles	Unidad	$ 7.000	70	$ 490.000
tarjeta de red	10/100	$ 45.000	85	$ 3.825.000
SWITCH	TREDNET 32 PTOS	$ 945.000	1	$ 945.000
SWITCH	TREDNET 24 PTOS	$ 400.000	5	$ 2.000.000
ROUTER CISCO	1751	$ 4.180.000	1	$ 4.180.000
TOTAL				$ 23.275.650

COSTOS CAT 6				
PARTE	**DESCRIPCION**	**VALOR UNIDAD**	**CANTIDAD**	**VALOR**
Cable UTP	Metro	$ 1.200	400 M.	$ 480.000
Conectores	RJ45	$ 2.500	136	$ 340.000
Caja Patch Cord	1 metro	$ 250.000	1	$ 250.000
Accesorios	Unidad	$ 13.900		$ 13.900
	30 cm. de alto,			
Bastidor	50 cm. de frente	$ 130.000	1	130000
	60 cm. de profundidad			
Canaletas	plástica con división metro	$ 19.500	400 M.	$ 7.800.000
Rótulos	100 Unidades	$ 19.000	1 CAJA	$ 19.000
Toma de Datos sencilla	Unidad	$ 11.000	140	$ 1.540.000
Toma de Datos dobles	Unidad	$ 18.000	70	$ 1.260.000
Toma Eléctricas Sencilla	Unidad	$ 5.000	140	$ 700.000
Tomas Eléctricas Dobles	Unidad	$ 7.000	70	$ 490.000
tarjeta de red	10/100/1000	$ 75.000	85	$ 3.825.000
SWITCH	TREDNET 24 PTOS	$ 2.910.000	5	$ 14.550.000
SWITCH	TREDNET 32 PTOS	$ 3.500.000	1	$ 3.500.000
ROUTER CISCO	1751	$ 4.180.000	1	$ 4.180.000
TOTAL				$ 39.077.900

CONCLUSIONES

- ✓ Se hace necesario seguir las normas establecidas internacionalmente como la ANSI, TIA-EIA para tender el cableado estructurado de una red.
- ✓ Las aplicaciones más utilizadas en las áreas de trabajo es el paquete Office.
- ✓ Las instalaciones del colegio facilitan la adecuación de uno o varios IDF por cada piso para cumplir con el estándar, sobre la máxima distancia que requiere el cableado horizontal.
- ✓ Con la Implementación de las VLAN en el colegio se proporcionara una escalabilidad a ésta red LAN.
- ✓ La topología física que se estableció para el colegio es de tipo estrella extendida.
- ✓ La información recopilada el sistema operativo más común es Windows 98.
- ✓ Los equipos no se encuentran expuestos a descargas eléctricas, debido a una buena puesta a tierra.

RECOMENDACIONES

- ✓ Se le recomienda al colegio cambiar su Windows operativo a uno mas avanzado como Windows XP.
- ✓ Adquirir una UPS.
- ✓ Para la seguridad de la red y los equipos se hace necesario:
  - ❖ No entrar a los salones de sistemas con comida o bebidas.
  - ❖ Tener un administrador de red.
  - ❖ Donde se encuentra ubicado el MDF tenerlo siempre con llave y que solo entre personal autorizado.

SIGLAS

ANSI	American National Standard Institute. Instituto Nacional Americano de Estándares.
ASP	Active Server Pages. Servidor de Páginas Activas.
CSMA/CD	(Carrier Sense Multiple Access with Collision Detection) Acceso Múltiple con Detección de Portadora y Detección de Colisiones
DHCP	Dynamic Host Configuration Protocol Protocolo de Configuración Dinámica de Host
DNS	Domain Naming Service Servicio de Dominio de Nombres
EIA	Electronic Industries Associate Asociación de Industrias Electrónicas
FDDI	Fiber Distributed Data Interconnect Interconexión de Datos Distribuidos pos Fibra
FTP	File Transfer Protocol Protocolo de Transferencia de Archivos
HTTP	Hyper Text Transfer Protocol Protocolo para la Transferencia de Hiper Texto

IDF	Intermediate Distribution Facility
	Servicio de Distribución Intermedia
IEEE	Institute of Electrical and Electronics Engineers
	Instituto de Ingenieros Eléctricos y Electrónicos
IP	Internet Protocol
	Protocolo de Internet
ISO	International Standards Organizations
	Organización Internacional de Estándares
ISP	Internet Service Provider
	Proveedor de Servicios de Internet
LAN	Local Area Network
	Red Area Local
MAC	Media Access Control
	Control de Acceso al Medio
MDF	Main Distribution Facility
	Bastidor de Distribución Principal
NFS	Network File System
	Sistemas de Archivos de Red
NIC	Network Interface Card
	Tarjeta de Interfaz de Red

OSI	Open System Interconnection
	Interconexión de Sistemas Abiertos
PBX	Private Branch Exchange
	Intercambio de Ramales Privado
POP	Point of Presence
	Punto de Presencia
SNMP	Simple Network Manager Protocol
	Protocolo de Administración de Red Simple
SMTP	Simple Mail Transfer Protocol
	Protocolo de Transferencia de Correos Simple
TCP	Transfer Control Protocol
	Protocolo de Control de Transferencia
TCP/IP	Transfer Control Protocol / Internet Protocol
	Protocol de Control de Transferencia / Protocol Internet
TIA	Telecommunications Industry Association
	Asociación de Industrias de Telecomunicaciones
UTP	Unshielded Twisted Pair
	Par Trenzado No Blindado

GLOSARIO

ADMINISTRADOR DE RED: Persona encargada del mantenimiento, funcionamiento y administración de una red.

ANCHO DE BANDA: Diferencia entre las frecuencias superior e inferior disponibles para las señales de red.

ARMARIO DE TELECOMUNICACIONES: Espacio cerrado para alojar equipos de telecomunicaciones, este armario es el sitio reconocido de conexión cruzada entre el sistema principal de cableado y el sistema horizontal.

ANILLO: Conexión de dos o más estaciones en una topología circular lógica, la información pasa de forma secuencial entre estaciones activas.

APLICACIÓN: Programa que realiza una función directamente para un usuario.

APPLETALK: Conjunto de protocolos de comunicación diseñados por Apple Talk, el cual consta de dos fases.

AREA DE CAPACITACION: Zona en la que recae un área a la que puede servir un dispositivo de internetworking.

ARP: Protocolo de Internet que sirve para asignar una dirección IP a una dirección MAC.

ATM: Estándar internacional para la distribución de celdas en el que múltiples tipos de servicios son transportados en celdas de longitud fijas.

BACKBONE: Núcleo estructural de la red, conecta todo los componentes de la red de forma que se lleve a cabo la comunicación.

BASTIDOR: Estructura con terminaciones para conectar el cableado permanente de una instalación, facilita las interconexiones o conexiones cruzadas

BROADCAST: Paquetes de datos enviados a todos los nodos de una red, identificados con una dirección de broadcast.

CABLE: Conjunto de dos a más conductores dentro de una chaqueta, permite el uso de estos conductores en grupo o por separado.

CABLE COAXIAL: Cable formado por un conductor cilíndrico externo que rodea a un solo conductor de cable interno.

CABLEADO CAT 5: Uno de los cinco grados del cableado UTP, pude transmitir datos a velocidades de 100 Mbps.

COLISION: En Ethernet es el resultado de dos nodos transmitiendo a la vez, las tramas colisionan y se dañan.

CONSOLA: Un DTE a través del cual se introducen comandos al Host

CSMA/CD: Mecanismo de acceso al medio en el cual los dispositivos listos para transmitir datos comprueban el canal para ver si hay una portadora, si no detecta un carrier en un lapso, el host empieza la transmisión.

DATAGRAMA: Agrupamiento lógico de información enviado como unidad de la capa de red sobre un medio de transmisión sin establecer antes un circuito virtual.

DCE: Dispositivo que se usa para convertir los datos de usuarios desde un DTE a una forma aceptada para la red.

DHCP: Protocolo que se usa para asignar direcciones IP de una forma dinámica.

DIFUSIÓN: Paquetes de datos que se envía a todos los host de la red.

DIRECCIÓN DE RED: Dirección de capa de red que hace referencia a un dispositivo de red lógico.

DIRECCIÓN IP: Dirección de 32 bits que se asigna a los host por medio de TCP/IP, cada dirección consta de un número de red, subred y de host.

DIRECCIÓN MAC: Dirección de capa de enlace de datos necesaria en todo puerto o dispositivo que se conecte a una LAN.

DTE: Dispositivo ubicado en el extremo de una interfaz de usuario a red que sirve como origen de datos, destino de datos o ambos.

ENLACE: Un canal de comunicación de red que consta de un circuito o ruta de transmisión y de todo equipo necesario entre un remitente y receptor.

ENRUTAMIENTO DINAMICO: Enrutamiento que se ajusta automáticamente a la topología de una red o a los cambios de tráfico.

ENRUTAMIENTO ESTATICO: Enrutamiento que se configura e introduce explícitamente en la tabla de enrutamiento.

ESTANDAR: Conjunto de reglas o procedimientos los cuales son muy utilizados o están especificados de forma oficial.

ETHERNET: Una especificación LAN de banda de base, esta red utilizan CSMA / CD.

FAST ETHERNET: Cualquiera de las especificaciones Ethernet de 100 Mbps.

FDDI: Estándar LAN que especifica una red de transmisión de testigos de 100 Mbps.

FIREWALL: Router de un servidor de acceso o varios router que están designados como un buffer entre una red pública conectada y una red privada.

FRAME RELAY: Estándar de la industria que consiste en un protocolo de datos de capa de enlace conmutado que maneja múltiples circuitos virtuales usando la encapsulación DIC entre dispositivos conectados.

FTP: Protocolo de aplicación, de la pila TCP/IP el cual se usa para transmitir archivos de nodos de red.

GATEWAY: Término que se refiere a un dispositivo de enrutamiento, los router actualmente se usa para describir los nodos que llevan a cabo ésta función.

HTML: Lenguaje sencillo de formateo de documentos de hipertexto que utiliza etiquetas.

HTTP: Protocolo que usa los Navegadores Web y servidores Web para transferir archivos.

HUB: Dispositivo que sirve como centro de una red de topología en estrella, llamado también repetidor multipuerto.

IDF: Habitación de comunicación secundaria de un edificio que usa topología en estrella.

NSTALACIÓN DE TIERRAS: Conjunto formado por electrodos y líneas de tierra de una instalación eléctrica.

INTEROPERABILIDAD: Capacidad de un equipo de conmutación creado por distintos fabricantes se puede comunicar con otros de una red.

INTRANET: Una red interna a la que acceden los usuarios que tenga acceso a la LAN interna de una organización.

IP: Un protocolo de capa de red de la pila TCP/IP que ofrece un servicio Internetwork sin conexión.

IPX: Intercambio de paquetes entre redes, un protocolo netware de capa de red que se emplea para transferir datos desde servidores hasta estaciones de trabajo.

ISO: Organización internacional encargada de una amplia gama de estándares.

LAN: Red de área local, que cubre una área geográfica relativamente pequeña.

LATENCIA: Retraso entre el tiempo que tarda un dispositivo en solicitar acceso a una red y el momento que se le permite transmitir.

MAC: Control de acceso al medio, la parte de capa dos que incluye la dirección de 6 bytes del origen y del destino.

MAN: Red de área metropolitana que abarca un área geográficamente más pequeña que la de una Wan.

MENSAJE: Un agrupamiento de información lógico de capa de aplicación.

MTU: Tamaño máximo de un paquete en bytes que puede manejar una determinada interfaz.

NETBEUI: Versión mejorada del protocolo Netbios que utiliza los sistemas operativos de red como Lan manager, Lan Server, Windows para grupos de trabajo y Windows NT.

NIC: Tarjeta que proporciona soluciones de comunicación de red en un sistema de computación.

NODO: Punto final de una conexión de red o una confluencia común a dos o más líneas de una red.

NUMERO HOST: Parte de una dirección IP que designa a que nueva subred nos estamos dirigiendo.

NUMERO RED: Parte de una dirección IP de una red que especifica a la que especifica el host.

OUI: identificador organizativo único, son tres octetos que designa la IEEE en un bloque de direcciones Lan de 48 bits.

PAQUETE: Agrupamiento Lógico de información que incluye una cabecera que contiene información de control y datos de usuario.

PATCH PANEL: Un conjunto de ubicaciones de ping y puertos que se puede montar en una estantería o rodapié en un recinto de cableado.

PBX: Intercambio de ramas, una centralita de líneas telefónicas digitales o analógicas ubicada en las oficinas del abonado y que se usa para conectar redes telefónicas y públicas.

PDU: Unidad de datos del protocolo.

POP: Punto de presencia, punto de interconexión entre las utilidades de comunicación que proporciona la compañía telefónica y el armario de distribución principal del edificio.

PPP: Protocolo punto a punto que proporciona conexiones de router a router y de host a red sobre circuitos síncronos y asíncronos.

PROTOCOLO: Descripción formal de una serie de reglas y convenciones que rigen como los dispositivos de una red intercambia información.

PUENTE: Dispositivo que conecta y pasa paquetes entre dos segmentos de red que usa el mismo protocolo de comunicaciones.

PUERTO: Interfaz de un dispositivo de Internetworking en terminología IP es un proceso de capa superior que recibe información de las capas superiores los puertos están enamorados y muchos están asociados con un proceso especifico.

RED: Una conexión de computadoras, impresoras, rotures, Switches y otros dispositivos que son capaces de comunicarse entre sí a través de un medio de transmisión.

ROUTER: Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta optima por la que hay que reenviar el tráfico de la red.

SALTO: El pasó de un paquete de datos entre dos nodos de red.

SEGMENTACIÓN: El proceso de dividir un solo dominio de colisión en dos o más dominios de colisión con el fin de reducir el dominio de colisiones y la cogestión de la red.

SEGMENTO: Una sección de red limitada por puentes, routers o Switches. En la especificación TCP, una sola unidad información de la capa de transporte.

SERVIDOR DE EMPRESA: Servidor que da cobertura a todos los usuarios de una red ofreciendo servicios como el correo electrónico o el sistema de denominación de dominio (DNS).

SERVIDOR GRUPO DE TRABAJO: Es un servidor que da cobertura a una serie concreta de usuarios y que ofrece servicios como procesamiento de textos y la opción de compartir archivos.

SERVIDOR: Un nodo o programa de software que proporciona servicios a los clientes.

STP: Medio de cableado de dos pares que se emplean en una serie de implementaciones de red, tiene una capa de aislamiento para reducir las EMI.

SWITCH: Dispositivo de red que filtra, reenvía e inunda tramas con base a la dirección de destino de cada trama.

TCP: Un protocolo de capa de transporte orientado a la conexión que proporciona a la transmisión de datos duplex fiable.

TCP/IP: Un nombre común para el conjunto de protocolos desarrollado por el DOD de los EE.UU.

TOKEN RING: Una Lan de paso de testigo desarrollada y mantenida por IBM. Token Ring se ejecuta a 4 o 16 Mbps sobre una topología en anillo.

TOPOLOGIA: Una organización física de nodos de red y medios en una estructura de Networking empresarial.

TRAMA: Un agrupamiento lógico de información que se envía como unidad de capa de enlace de datos por un medio de transmisión.

UDP: Un protocolo de capa de transporte sin conexión, sencillo que intercambia data gramas sin acuse de recibo ni entrega garantizada.

UPS: Sistema de alimentación ininterrumpida, un dispositivo de respaldo.

VLAN: Lan virtual, un grupo de dispositivos de una Lan que están configurados (con software de administración) de forma que se pueden comunicar como si estuvieran conectados al mismo cable.

WAN: Red de área amplia que presta servicios a los usuarios en una zona geográficamente extensa.

X.25: Un estándar ITU-T que define como se mantiene las conexiones entre los DTE y los DCE en el acceso de terminal remoto y en las comunicaciones computacionales de las redes publicas.

BIBLIOGRAFIA

CYSCO SYSTEM, 2002 Guía del Segundo Año. Tercera Edición

http//www.yahoo.com

http//www.altavista.com

http//www.trendnet.com

http//www.3com.es

http//www.netgear.com

http//www.google.com

Biblioteca de consulta Encarta.