UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

Carrera:

INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema:

DISEÑO DE UN SISTEMA DE ALARMAS INALÁMBRICAS IP PARA LA BRIGADA DE CABALLERÍA BLINDADA No 11 "GALÁPAGOS" EN LA CIUDAD DE RIOBAMBA

Proyecto de Pasantía de grado previo a la obtención del Título de Ingeniero en Electrónica y Comunicaciones.

Autor:

Lasluisa Chacha Fernando Gabriel

Tutor:

Ing. Geovanni Brito

Ambato – Ecuador

JUNIO / 2008

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación sobre el tema: "DISEÑO DE UN SISTEMA DE ALARMAS INALÁMBRICAS IP PARA LA BRIGADA DE CABALLERÍA BLINDADA No 11 "GALÁPAGOS" EN LA CIUDAD DE RIOBAMBA" de Lasluisa Chacha Fernando Gabriel, estudiante de la Carrera de Ingeniería Electrónica y Comunicaciones, de la Facultada de Ingeniería en Sistemas, Electrónica e Industrial, Universidad Técnica de Ambato, considero que dicho informe investigativo reúne los requisitos y meritos suficientes para ser sometidos a la evaluación de conformidad con el artículo 68 del capítulo sexto, del reglamento de graduación de pregrado de la Universidad Técnica de Ambato

Ambato, Junio 2008

El TUTOR

……..

Ing. Geovanni Brito

AUTORÍA

El presente trabajo de investigación "DISEÑO DE UN SISTEMA DE ALARMAS INALÁMBRICAS IP PARA LA BRIGADA DE CABALLERÍA BLINDADA No 11 "GALÁPAGOS" EN LA CIUDAD DE RIOBAMBA", es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se pretenden del mismo son exclusivamente responsabilidad del autor.

Ambato, Junio 2008

…….

Lasluisa Fernando

180360973-2

DEDICATORIA

A mis padres Amador y Marta, a mis hermanos Diana, Belén, Andrés por el gran apoyo que me brindaron para la realización de este trabajo

AGRADECIMIENTO

A Dios por darme fortaleza y templanza para la realización del trabajo.

A mis padres por su incondicional y permanente apoyo en mis estudios.

A la Facultad por brindarme los recursos necesarios para realizarme como profesional y como persona

A todos los profesores que me brindaron los conocimientos necesarios en el transcurso de la carrera, al Ing. Javier Sánchez y especialmente a mi Tutor Ing. Geovanni Brito.

AL personal de EC-11 por la acogida y apoyo brindado durante el proceso de poner en práctica los conocimientos adquiridos en la Universidad.

ÍNDICE DE CONTENIDOS

RESUMEN EJECUTIVOS

La Brigada de Caballería Blindada No. 11 "GALÁPAGOS " perteneciente a las FF.AA del Ecuador, ubicada al Norte de la Ciudad de Riobamba en la Av. De los Héroes S/N. Cuenta con de 7 grupos de operaciones; 5 de Caballería y 2 de Artillería; una Compañía de Ingenieros, una Compañía de morteros, un Comando de apoyo logístico y una Compañía de Comunicaciones, lugar donde se realizará la pasantía.

El Escuadrón de Comunicaciones No. 11 “RUMUÑAHUI” lugar de la pasantía debe iniciarse identificando la visión de los cuadros de los directivos, junto con su misión, los objetivos y los propósitos, para saber que fortalezas y debilidades que presenta y evaluarlos, según las nuevas tendencias actuales, ya sean sociales, tecnológicas, económicas, y políticas.

La Brigada Blindada No. 11 "GALÁPAGOS", como subsistema de la Fuerza Terrestre, tiene que interactuar con las políticas generales del comando, para alcanzar en forma sincronizada los objetivos propuestos y en el marco de la Planificación Estratégica Institucional.

De la convención del Arma se pudieron establecer la realidad de las diferentes Unidades y se establecieron objetivos a alcanzar a través de coherentes políticas.

La 11-BCB se encuentra preocupada de su fortalecimiento y de incrementar su capacidad operativa encaminada al cumplimiento de sus misiones tanto para Defensa Externa, Defensa Interna y de Apoyo al Desarrollo en sus respectivos sectores de responsabilidad.

INTRODUCCIÓN

Los tipos de alarmas y sensores entre los que podremos elegir son muy variados, y los avances tecnológicos en este campo son continuos. Hoy en día la conexión con la Central de Alarmas puede hacerse vía Internet por lo que la comunicación es continua y bidireccional, un sistema mucho más sofisticado y seguro que aquellos basados exclusivamente en una llamada telefónica automática a la Central en cuanto se detectaba la intrusión. Complicamos al posible intruso la tarea de saltarse la alarma. En este sentido, el enlace vía TCP/IP, es decir a través de la Red, con la Central de Alarmas permite también la transmisión de vídeo a tiempo real, e incluso una comunicación verbal con la vivienda en el mismo momento en que se produce la incidencia para tratar de disuadir a los intrusos. Por otra parte, hoy en día las alarmas enlazadas con la Central mediante línea telefónica suelen recurrir al uso de tecnología móvil, GSM o GPRS, para evitar que alguien pueda cortar la línea desde el exterior anulando así la alarma.

El Escuadrón de Comunicaciones No. 11 "RUMUÑAHUI" lugar de la pasantía debe iniciarse identificando la visión de los cuadros de los directivos, junto con su misión, los objetivos y los propósitos, para saber que fortalezas y debilidades que presenta y evaluarlos, según las nuevas tendencias actuales, ya sean sociales, tecnológicas, económicas, y políticas.

Con el conocimiento de los avances tecnológicos en el área de sistemas de seguridad y la necesidad de actualizar el sistema de seguridad se procedió a realizar un diseño, el cual abarcando las siguientes actividades:

- Análisis y reconocimiento visual de áreas críticas.
- Definir las áreas a ser protegidas
- Analizar la tecnología a utilizar
- Costo
- Ubicación de la central de monitoreo
- Diseño del sistema de alarmas y sistema de monitoreo.

CAPITULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema:

Diseño de un sistema de alarmas inalámbricas IP para la Brigada de Caballería Blindada No 11 “Galápagos” en la ciudad de Riobamba.

1.2 Planteamiento del problema

La Política de Defensa Nacional es una Política de Estado y como tal trasciende a un Gobierno y perdura como resultado de la legitimidad que ha alcanzado. Es flexible y dinámica, debe ser actualizada conforme a los requerimientos de seguridad del país, y su necesario reajuste responde a los cambios más trascendentes en el ámbito de la defensa, tanto en nuestro país como en el resto del sistema internacional.

No obstante la adopción de medidas preventivas y prioritarias, está pendiente la Reestructuración de Fuerzas Armadas como paso previo a la Transformación de la Defensa, que comprende la actualización del marco legal, el fortalecimiento de la organización y de la capacidad operativa y la adaptación de los recursos a los diferentes escenarios.

Los cambios estratégicos y geopolíticos que han ocurrido a inicios del siglo XXI han producido importantes transformaciones en la situación mundial, regional y nacional, lo cual obliga al país y sus instituciones a encuadrarse en esa realidad política estratégica.

En ese ambiente de incertidumbre, con escenarios permanentemente cambiantes, los avances de la ciencia y tecnología exigen la reestructuración y transformación de las Fuerzas Armadas.

Es importante considerar que en la actualidad se destacan los valores de democracia y los derechos humanos como elementos sustantivos en la conducta de los Estados, así como la institucionalización de la diplomacia de cumbres en los diferentes niveles y el surgimiento de una nueva agenda de seguridad y defensa.

En el ámbito hemisférico se inició la construcción de una nueva concepción de seguridad definiéndose el enfoque "multidimensional", que incorpora amenazas nuevas y tradicionales; incorpora las prioridades de cada Estado; contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social; se basa en valores democráticos, el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional. Esta nueva dimensión de la seguridad, que se fundamenta en el bienestar del individuo, conocida como seguridad humana, tiene como meta la protección del ser humano y se fundamenta en la gobernabilidad y el desarrollo.

El conflicto interno que vive Colombia data de mediados del siglo pasado; en la actualidad es el aspecto de mayor relevancia para la paz, seguridad y estabilidad para el Ecuador; desafortunadamente, en los últimos años se ha incrementado y los efectos se sienten con gran intensidad en el Ecuador por su condición de país vecino. Las principales repercusiones para nuestro país se relacionan con el incremento de desplazados y refugiados, de contrabando e infiltraciones de grupos ilegales armados colombianos, generación de violencia en la zona fronteriza con Colombia, la presencia de grupos ilegales armados y el crimen organizado internacional en el área; el alto costo de la vigilancia y protección del territorio en la zona de frontera, y la necesidad de participación de todas las instituciones y órganos de seguridad del Estado.

Otro de los puntos que se debe tomar en cuenta es la seguridad en las Bases militares del país las cuales son puntos estratégicos de ataques en un posible conflicto armado que se produzca. Un sistema de alarmas debe ser lo suficiente mente eficaz para dar diferentes tipos de alertas contra todos los posibles ataques que pudieran sufrir estas bases militares.

El siguiente estudio se realizará para la empresa BCB No 11 "GALÁPAGOS" en la cuidad de Riobamba por el periodo OCTUBRE 2007 – ENERO 2008

1.3 Justificación

La BCB No 11 Galápagos es una entidad estatal que brinda seguridad al pueblo ecuatoriano por esta razón se encuentra dotado de armamento bélico para cumplir con este objetivo.

El día 20 de noviembre del 2002 en la BCB No. 11 "Galápagos" se produjo una explosión de uno de los polvorines causando perdidas materiales en los alrededores del siniestro.

El sistema de alarmas instalada en la BCB No 11 "Galápagos" colapso quedando obsoleto, en la actualidad BCB No 11 "Galápagos" no se cuenta con sistema de alarmas por lo que se vio la necesidad de diseñar un nuevo sistemas de seguridad interna y externa.

1.4 Objetivos

General

Diseñar un sistema de seguridad de alarmas IP inalámbricas para la BCB No 11 "Galápagos" en la ciudad de Riobamba.

Específicos

- Determinar los puntos estratégicos en donde se colocaran los dispositivos que accionaran el sistema de seguridad.

- Diseñar un sistemas de altavoces para alertar al personal de la Brigada cuando se detecte la activación de una de las alarmas
- Diseñar un sistema de gestión y administración para el control de trafico TCP/IP de las alarmas.
- Seleccionar los equipos adecuados a ser implementados en la BCB No 11 “Galápagos”.
- Capacitar al personal en la administración del sistema de seguridad.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes investigativos

Revisado los temas de tesis y perfiles no se a encontró ningún tema relacionado con el proyecto que se va a desarrollar.

2.2 Fundamento legal

La Brigada de Caballería Blindada No. 11 "GALÁPAGOS " perteneciente a las FF.AA del Ecuador, ubicada al Norte de la Ciudad de Riobamba en la Av. De los Héroes S/N. Cuenta con de 7 grupos de operaciones; 5 de Caballería y 2 de Artillería; una Compañía de Ingenieros, una Compañía de morteros, un Comando de apoyo logístico y una Compañía de Comunicaciones, lugar donde se realizará la pasantía.

El Escuadrón de Comunicaciones No. 11 “RUMUÑAHUI” lugar de la pasantía debe iniciarse identificando la visión de los cuadros de los directivos, junto con su misión, los objetivos y los propósitos, para saber que fortalezas y debilidades que presenta y evaluarlos, según las nuevas tendencias actuales, ya sean sociales, tecnológicas, económicas, y políticas.

La historia es un relato de los hechos verídicos y documentados de la vida de un pueblo, los mismos que forman su personalidad contemplado el pasado, junto al presente en busca del futuro, para llevar adelante el porvenir dinámico y positivo.

Es por eso que hemos creído “Hacer la historia de la Brigada de Caballería Blindada N°. 11 “Galápagos”, para poder ver en perspectiva lo que habremos de “Heredar”, cuanto de ello podemos aprovechar, perder o superar; que es lo que podemos construir con la herencia recibida, para trasmitirlo a las futuras generaciones.

Según orden de Comando N°004-III-C-974 del 27 de marzo del año de 1974, se ordena la creación de la Brigada Blindada N° 11 “Galápagos” con sede en San Pedro de Riobamba, basada en el decreto N° 246 del 18 de febrero de 1974 luego de la aprobación del reglamento orgánico del ejército, es así, que entre los meses de agosto y octubre de 1974, se traslada la unidad al campamento “San Nicolás” de la ciudad de Riobamba, siendo su primer Comandante el Sr. Crnl. Américo Alaba , y del escuadrón de reconocimiento blindado el Tnte. Crnl. René Silva, jugando un papel importante la cooperación del personal de tropa y la iniciativa de los oficiales.

Desde entonces, la lealtad, el compañerismo, el espíritu de cuerpo, son sentimientos presentes en el soldado de Caballería Blindada y constituyen los pilares fundamentales sobre los que se asienta la institución armada, que con esfuerzo, sacrificio y auto superación, se esfuerzan por alcanzar la meta de ser un excelente profesional militar, líder y conductor.

A los veintinueve días del mes de agosto de 1985, según orden de Comando N° 011-985, el Comando General del ejército, dispone la fusión de las armas de Caballería y Fuerzas Blindadas, bajo el denominativo “Caballería Blindada”.

En abril de 1989, según la resolución ministerial No. 027, en su articulo 7º, se autoriza el funcionamiento integrado de las actuales armas de caballería y fuerzas blindadas del ejército, con esta última disposición definitiva, basada en la ya emitida en el año de 1985, y en consideración, al orgánico para los años 1987-

1982, en el cual se considera una nueva organización de los pelotones de tanques, y ante la iniciativa e interés del Comando de la 11-BCB “GALAPAGOS”, renace la idea de materializar a los grupos de Caballería Blindada.

Con este concepto, la institución militar forja conductores capaces de enfrentar el desarrollo tecnológico y los nuevos desafíos, empleando sus conocimientos para fortalecer el desarrollo institucional logrando el mejor desempeño profesional en sus funciones.

La gesta del 21 de abril, gloria inmortal de nuestros héroes, se vio vivificada y renovada por el espíritu de solidaridad nacional y el ímpetu combativo de nuestros soldados, quienes reeditaron la campaña de Tapi y se cubrieron de honor y gloria en una magistral batalla por la dignidad, soberanía y derechos de la patria.

Jamás olvidemos a nuestros antepasados, verdaderos héroes innatos y quizá olvidados; que no subestimemos lo mejor de nuestra vida cual es, el honor y la dignidad.

ESCUADRON DE COMUNICACIONES No. 11

VISION DE FUTURO

Modernizar, automatizar los sistemas de comunicaciones a fin de brindar apoyo de comunicaciones y enlaces seguros, confiables, oportunos, tanto en tiempo de paz como en operaciones.

Especializar, capacitar al personal del Escuadrón para el manejo, explotación y mantenimiento de los sistemas.

MISION

El Escuadrón de Comunicaciones N.-11 organizará, instalará, explotará y mantendrá el Sistema General de Comunicaciones de la 11- BCB, desde ya hasta el término de las operaciones, para permitir al comando de la Brigada ejercer el mando y control de las operaciones.

MISION.- DEL EC-11 PARA DEFENSA EXTERNA

El EC-11 instalará, explotará y mantendrá el Sistema General de Comunicaciones desde ya hasta el término de las operaciones, desde Riobamba, en la ruta de marcha, en la ocupación de las ZR., ARA., y durante la ejecución de operaciones ofensivas, para permitir a la 11-BCB ejercer el mando y el control de las operaciones, a fin de colaborar con el EJEOP en el debilitamiento de la capacidad ofensiva del enemigo.

MISION.- DEL EC-11 PARA DEFENSA INTERNA

El Escuadrón de Comunicaciones No. 11, instalará, explorará y mantendrá el sistema general de Comunicaciones desde ya, hasta la total pacificación y normalización de las actividades, en la SZD-C, para permitir el mantenimiento de la paz, el orden público, proteger, la población, los recursos, neutralizar fuerzas oponentes y garantizar el ordenamiento jurídico, a fin de colaborar en el cumplimiento de la misión de la FTC-1.

POLITICAS

- Optimizar el empleo de los recursos humanos y materiales.
- Promover y facilitar el entrenamiento y perfeccionamiento del personal.
- Optimizar el funcionamiento y operatividad de los equipos de comunicaciones e informática.
- Evaluar el funcionamiento y operatividad de los sistemas.
- Alcanzar la compatibilidad de los medios disponibles.

- Capacitar al personal en forma sistemática y progresiva, propendiendo a la preparación técnica especializada.
- Propender a la renovación parcial del material, incorporando tecnología de punta para permitir el mejor empleo de los sistemas.
- Fomentar las relaciones con los Organismos afines a las comunicaciones e informática, tanto en las entidades publicas como privadas.
- D esarrollar la capacidad profesional Fortalecer los valores humanos y profesionales.

2.3 Categorías fundamentales

Sistemas de alarmas

Los sistemas de alarmas están constituidos por instalaciones destinadas a avisar al personal en caso de siniestro. Toda escuela, hospital, jardín infante, casa de anciano, edificios, oficinas, hotel, fábrica, departamento, etc., deben contar con una protección adecuada. Las alarmas pueden ser:

Alarmas manuales: consta de estaciones de aviso distribuidas por todo el establecimiento. Estas estaciones consisten en llaves o botones cuyo accionamiento hace sonar la alarma. Con el objetivo de impedir que alguien las oprima inadvertidamente están protegidas por vidrios. Deben estar colocadas al alcance de los operarios de manera que no sean necesarios a estos recorrer más de 30 metros para encontrar una.

Alarmas automáticas: estas pueden accionarse por dos mecanismos. Uno es un detector que indican un aumento de la temperatura ambiente sobre un cierto límite: tipo de temperatura fija. Y el otro es un detector sensible a una variedad brusca de la temperatura ambiental: tipo de rapidez de aumento.

Existen diversos tipos de señales: auditivas ó luminosas; ambas deben ser seguras, ser características, y llegar a todos los operarios. Estar combinadas con

una llamada de auxilio a los bomberos con el objeto de asegurar su funcionamiento a los sistemas de alarmas debe estar alimentado eléctricamente por fuentes de energía independiente de las maquinarias o el alumbrado.

La sirena de alarma debe ser característica para cada tipo de alarma instalada, sin lugar a dudas o confusiones. Debe ser audible para todos las persona y en todos los rincones del establecimiento (talleres, comedores, vestuarios, baños, depósitos, dormitorios, etc.)

Tipos de alarmas

Alarma de compaginado: sirve para concretar al personal clave, incluso los petitos de seguridad, de empleados de primeros auxilios, etc., cerca de su oficina centralita de teléfono. Indispensable en los casos de emergencia.

Alarma contra ladrones: de protección en todos los puntos de entrada de la planta.

Señales de comienzo y término de jornada: también para los cambios de turno.

Señales periódicas: que indican las pausas de descanso en la mañana o por la tarde, ó al mediodía; que marcan los exámenes que se llevan acaso cotidianamente.

Indicadores de peligro: montados sobre tableros indican cuando surge un problema con el equipo. Por ejemplo una señal suena actuada por un termostato cuando se recalienta un cojinete.

Indicadores de advertencia: la señal suena cuando ciertas personas ó vehículos penetran el algún sitio del establecimiento. Las señales cerca de las bombas de gasolina, etc.

Indicadores para el teléfono: en las secciones ruidosas de la planta donde el sonido del teléfono seria inaudible, se monta una campanilla, zumbador ó bocina con mayor intensidad.

Tipos de señales audibles

Existen varios tipos de señales audibles que se pueden aplicar según los requisitos de distintas plantas ó sistemas de señales. Estas pueden ser:

Bocinas: es casi el aparato más usado. Emite tonos claros, definidos, elevados y agudos. Su gran escala de volúmenes les permite una aplicación infinita en las instituciones comerciales e industriales. Normalmente se emplean para señales de alarma, de iniciación ó término de la jornada y para un código general de trabajo de compaginación. Los hay para montaje convencional ó desmontables; para el interior o al aire libre; operado por aire, electricidad ó manualmente.

Sirenas: son las más poderosas y llamativas de todas las señales, por lo que se emplean en ambulancias, camiones de bombero, policía, etc. Su radio de alcance es mayor (1Km en condiciones favorables) y sus tonos elevados horadan prácticamente cualquier otro sonido exterior. Convenientemente para las señales de emergencia, de comienzo y fin de jornadas en las fábricas, fundiciones, aeropuertos, etc.

Campanillas: sin duda alguno es la más versátil de las señales. Se prestan para cualquier tipo de señal concebible los modelos grandes se emplean para alarma contra ladrones o incendio, para compaginación de códigos y señales de horario. El tono varía del moderado y apacible hasta la estridente insistencia. Disponibles con soportes convencionales o intercambiadores; de campaneo continuo por vibración o de golpes individuales.

Zumbadores: hay muchos problemas de señales que solo un zumbador o "abejorro" puede resolver. Son populares para las señales en general, sobre todo para las alarmas en los edificios públicos, hospitales, escuelas y otros sitios

donde la señal más estridente no conviene. En las industrias, oficinas y edificios comerciales se emplean para señales de compaginación.

Carillón: son de sonido agradable, sin embargo muy efectivo en la práctica. Los carillones se recomiendan para las plantas de un nivel de ruidos moderados, tales como bancos, tiendas de comercios, hospitales y oficinas en general. De volumen audible, sus tonos musicales y maduros les hacen tolerables.

Anunciadores: en realidad estos son anunciadores visuales antes que señales sonoras. En la industria se emplean para localizar un punto crítico (recalentamiento de un cojinete) en una máquina automática o que se opera por baterías. Estas señales visuales, que se combina con otras sonoras, se expenden varios tamaños y tipos.

REDES DE DATOS

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. Por aquel entonces, los microcomputadores no estaban conectados entre sí como sí lo estaban las terminales de computadores mainframe, por lo cual no había una manera eficaz de compartir datos entre varios computadores. Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial. La red a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos
- Cómo comunicarse con eficiencia
- Cómo configurar y administrar una red

Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones fue la creación de los estándares de Red de área local (LAN - Local Área Network, en inglés). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN

Red Inalámbrica de Área Local (WLAN)

WLAN (Wireless Local Área Network) es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para

manufactura, en los que se transmite la información en tiempo real a una Terminal central.

Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas con licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación, pues éstas requieren de un importante desembolso económico previo por parte de los operadores del servicio, ello también obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico de dominio público disponible.

Los pioneros en el uso de redes inalámbricas han sido los radioaficionados mediante sus emisoras, que ofrecen una velocidad de 9600 bps. Pero si hablamos propiamente de redes inalámbricas debemos remontarnos al año 1997, en el que el organismo regulador IEEE publicó el estándar 802.11 dedicado a redes LAN inalámbricas. Dentro de este mismo campo y anteriormente, en el año 1995, tenemos la aparición de Bluetooth, una tecnología de Ericsson con el objetivo de conectar mediante ondas de radio los teléfonos móviles con diversos accesorios. Al poco tiempo se generó un grupo de estudio formado por fabricantes que estaban interesados en esta tecnología para aplicarla a otros dispositivos, como PDAs, terminales móviles o incluso electrodomésticos.

El futuro de la tecnología WLAN pasa necesariamente por la resolución de cuestiones muy importantes sobre seguridad e interoperabilidad, en donde se centran actualmente la mayor parte de los esfuerzos. Sin embargo, desde el punto de vista de los usuarios, también es importante reducir la actual confusión motivada por la gran variedad de estándares existentes.

Principios de las redes WLAN

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos

normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

Estándares de redes WLAN

El estándar IEEE 802.11 fue adoptado finalmente en 1997. Todos los equipos que implementan esta tecnología (tarjetas de red, puntos de acceso, etc.) se basan en una estructura de capas de acuerdo con el modelo de referencia OSI.

IEEE 802.11

Las tasas de transmisión que permite el estándar IEEE 802.11 son de 1 y 2 Mbit/s. El esquema de modulación propuesto para velocidades de 1 Mbit/s es BPSK, mientras que para 2 Mbit/s es QPSK. Sin embargo, estas velocidades

significativamente inferiores a las de las redes de área local cableadas (10 y 100 Mbit/s) redujeron inicialmente el interés por estos sistemas.

IEEE 802.11a

La banda de 5 GHz constituye otra alternativa viable para el desarrollo de soluciones WLAN, resultando especialmente interesante conforme la banda de 2,4 GHz se va encontrando cada vez más congestionada. En esta zona del espectro existe una mayor cantidad de ancho de banda disponible, el cual se encuentra dividido en varias sub-bandas dependiendo de la región. Cambia su modulación, depende de la Vtx. 5.2 sub portadoras= 2.4-5GHz. Vtx= 54Mbps, dependiendo de su cobertura disminuye su velocidad.

IEEE 802.11b

También llamado a veces Ethernet inalámbrico de alta velocidad o Wi-Fi (Wireless Fidelity). La diferencia sustancial respecto a su predecesor es que 802.11b ofrece una tasa de transmisión de hasta 11 Mbit/s, que puede llegar a compartirse entre doce conexiones de un mismo punto de acceso. Además, en una misma zona de cobertura pueden trabajar simultáneamente tres puntos de acceso, cada uno de ellos con un alcance para interiores de unos 90 m a 1 Mbit/s y de unos 30 m a la tasa máxima de 11 Mbit/s. La tasa de transmisión puede seleccionarse entre 1, 2, 5,5 y 11 Mbit/s, característica denominada DRS (Dynamic Rate Shifting), lo cual permite a los adaptadores de red inalámbricos reducir las velocidades para compensar los posibles problemas de recepción que puedan generarse por las distancias o los materiales que deba atravesar la señal (paredes, tabiques, ventanas, etc.), especialmente en el caso de interiores. En el caso de espacios abiertos, los alcances pueden aumentar hasta 120 m (a 11 Mbit/s) y 460 m (a 1 Mbit/s). La técnica de modulación empleada es CCK (Complementary Code Keying), codificando cada símbolo con 4 bits a velocidades de 1,375 MBd. Dado que CCK es una técnica DSSS, existe compatibilidad con los

productos 802.11 originales simplemente reduciendo las velocidades de funcionamiento a 1 ó 2 Mbit/s. Posteriormente, un segundo esquema de codificación llamado PBCC (Packet Binary Convolutional Code) fue incluido para mejorar el alcance en el caso de tasas de 5,5 y 11 Mbit/s, ya que proporciona una ganancia de codificación de 3 dB.

IEEE 802.11g

El estándar 802.11g utiliza tecnología OFDM, implementando al mismo tiempo las modalidades 802.11b y, de manera opcional, CCK-OFDM y PBCC-22. Consigue tasas de funcionamiento de hasta 54 Mbit/s como en 802.11a pero en la banda de 2,4 GHz, manteniendo de este modo la compatibilidad con el equipamiento 802.11b. Luego en términos de velocidad y alcance, las prestaciones del estándar 802.11g son mejores que las de cualquiera de las alternativas comentadas.

Otros estándares

Dentro del grupo 802.11, existen también otros estándares dignos de mención por su importancia en la mejora y evolución de las normas básicas o por cubrir algunos aspectos no contemplados en dichas normas, los cuales se comentan a continuación.

IEEE 802.11e: implementa características de QoS y multimedia para las redes 802.11b, aunque también será aplicable a 802.11a.

IEEE 802.11f: se trata básicamente de una especificación que funciona bajo el estándar 802.11g y que se aplica a la intercomunicación entre puntos de acceso de distintos fabricantes, permitiendo el roaming de clientes.

IEEE 802.11h: consiste en una evolución de 802.11a que permite la asignación dinámica de canales y el control automático de potencia para minimizar los efectos de posibles interferencias.

IEEE 802.11i: su objetivo principal es ofrecer una forma interoperable y estándar de asegurar datos inalámbricos. Si bien 802.11i puede aplicarse a cualquier

tecnología 802.11 inalámbrica, realmente se está considerando sólo como la solución de seguridad de 802.11a.

Como resumen final, en la tabla siguiente se detallan las características más significativas de cada uno de los estándares WLAN analizadas, en comparación con otras tecnologías inalámbricas como Bluetooth o UWB.

Estándar	802.11b	802.11a	802.11g	HiperLAN/2	Bluetooth	802.15.3a
Organismo	IEEE	IEEE	IEEE	ETSI	Bluetooth SIG	IEEE
Finalización	1999	2002	2003	2003	2002	-
Banda de frecuencias	2,4 GHz	5 GHz	2,4 GHz	5 GHz	2,4 GHz	3,1-10,6 GHz
Tasa máxima	11 Mbit/s	54 Mbit/s	54 Mbit/s	54 Mbit/s	1 Mbit/s	480 Mbit/s
Interfaz aire	DSSS/FHSS	OFDM	OFDM	OFDM	DSSS/FHSS	Códigos PN

2.4 Hipótesis

El diseño del sistema de seguridad proporcionara integridad y confiabilidad para el personal de la BCB No 11 “Galápagos” en la ciudad de Riobamba.

2.5 Señalamiento de las variables

Variable dependiente

BCB No 11 “Galápagos”

Variable Independiente

Sistema de alarmas

CAPITULO III

METODOLOGIA

3.1 Modalidad Básica de Investigación

La presente investigación se contextualiza en la modalidad de investigación de campo y bibliográfica, debido a que los hechos fueron estudiados en primera instancia en base a normas legales que se encuentran tipificadas en diversos códigos, leyes, reglamentos, etc. Además se realizó la visita a la BCB No 11 "Galápagos" Escuadrón de Comunicaciones (EC -11) en la ciudad de Riobamba, lo cual fue de gran ayuda para obtener elementos de juicio necesarios para la configuración de esta investigación.

3.2 Tipos de Investigación

La investigación abarcó el nivel exploratorio pues reconoció las variables que nos competen, el nivel descriptivo permitió caracterizar la realidad investigada, el nivel correlacional dilucidó el grado de relación entre las variables en estudio y finalmente el nivel explicativo detectó las causas de determinados comportamientos y canalizó la estructuración de propuestas de solución a la problemática analizada.

3.3 Técnicas e instrumentos de investigación

Las Técnicas empleadas en la presente investigación fueron: la entrevista y la observación. La entrevista fue empleada para obtener datos significativos referentes al sistema de alarma que tenían instalados antes de la explosión.

La técnica de la observación fue de gran valor en la apreciación directa circunstancias que permitieron confrontar los hechos con palabras, elementos medulares para imprimir un sello de transparencia e imparcialidad en la investigación.

3.4 Recolección de información

Para la recolección eficaz de la información de campo, se recurrió a las siguientes estrategias:
Diseño y elaboración de los instrumentos de recolección de información a partir de la matriz operacional de las variables.

3.5 Procesamiento de la formación

Una vez aplicados los instrumentos y analizada la validez, se procedió a la tabulación de datos. Acto seguido se procedió al análisis integral, enriquecido gracias a los elementos de juicio desprendidos del marco teórico, objetivos y variables de la investigación.

A continuación se efectuó la estructuración de conclusiones y recomendaciones que organizadas en una propuesta lógica y factible, permitirán participar proactivamente en la solución o minimización de la problemática planteada.

Finalmente, como parte medular de la investigación crítica propositiva, se estructura una propuesta pertinente al tema de investigación que nos compete, enfocada a optimizar de los recursos existentes, fiabilidad, confiabilidad y desempeño del sistema de alarmas.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Estamos en la era de la tecnología de las comunicaciones, y no podía ser menos para las centrales de alarma. Las tecnologías de conexión a Internet están abriendo una nueva vía de comunicación rápida, fiable y económica.

Hoy en día el 34% (5,4 millones) de hogares y el 90% de la empresas están conectadas a Internet de alguna forma: DSL, Cable, satélite etc.... Esto supone que la mayor parte de las empresas y muchos hogares están preparados para las conexiones TCP/IP.

Ventajas de las comunicaciones por TCP/IP

Las conexiones TCP/IP brinda una serie de ventajas muy claras frente a la transmisión de señales tipo DTMF, Contact-ID y Radionics (4x2) o similares.

- Costo cero de las comunicaciones con las receptoras.
- Mayor seguridad para el cliente.
- Mayor seguridad de las comunicaciones.
- Liberación de la línea telefónica.
- Fin de los problemas propios de líneas saturadas u ocupadas.

El costo de las llamadas hoy en día ya no es un problema económico serio para el cliente, pero el simple hecho de ahorro es un argumento válido.
El incremento de la seguridad para los clientes viene dado por la velocidad y el nulo costo de las comunicaciones. Con un sistema TCP/IP bien diseñado, podemos mantener un “Test” con la central de segundos o minutos.

Las limitaciones propias de las comunicaciones por medio de líneas telefónicas nos impiden tener una comunicación rápida con la Central. Una llamada telefónica tiene una serie de pasos que en general son relativamente lentos.

- Descuelgue y detección de línea
- Marcado del número (tonos DTMF)
- Tiempo propio del enrutado de la llamada.
- Detección de la llamada en el otro extremo de la línea.
- Establecimiento de la conexión.
- Intercambio de protocolo de comunicaciones.
- Envío de la secuencia DTMF.
- ACK de la comunicación.

Cualquier fallo de alguno de los pasos provoca que tengamos que repetir todos los pasos. Teniendo en cuenta que una comunicación de este tipo tarda de un mínimo de 20-30 segundos en el mejor de los casos, Además para cada comunicación debemos iniciar una llamada, lo que suma más tiempo.

Los tiempos para establecer múltiples comunicaciones consecutivas se vuelven delicados hablando en términos de seguridad. Ni que decir tiene que mantener la comunicación abierta resulta no viable, por costos de llamada, costos de líneas dedicadas en ambos lados de la comunicación.

En las comunicaciones TCP/IP los tiempos son de milisegundos, por lo que podemos hacer múltiples reintentos en un tiempo muy breve. Además si fuera necesario podríamos mantener abierta la comunicación permanentemente.

Eficacia de la transmisión

La transmisión telefónica tiene varios puntos débiles a veces inherentes a la propia instalación. Múltiples factores pueden influir en la transmisión. Podemos encontrarnos con:

- Una instalación deficiente que permite que se ocupe la línea que utiliza la Central de alarmas
- Calidad de la línea telefónica inestable. Exceso de ruido en la comunicación en cualquiera de los lados de la comunicación, que impide que las señales DTMF sean transmitidas.

Seguridad en la transmisión

La seguridad propia de los datos transmitidos durante la comunicación telefónica es bastante frágil por el propio sistema usado. Los protocolos son conocidos porque se ha tendido a la estandarización total. Hoy en día sería relativamente sencillo emular una comunicación de TEST de la Central, colocando un MODEM y un PC o similar en un extremo de la línea. La señal no está encriptada y solo se identifica con el número de abonado. Es decir son datos que pueden conocerse con relativa facilidad.

Un protocolo de comunicación que tenga como transporte redes TCP/IP puede protegerse de forma muy eficaz a la vez que sencilla.

Es fundamental poder asegurar los datos durante la conexión sin complicar para ninguna de las partes la instalación, programación o control. Con estas premisas se ha construido una Central en la que la transmisión en primer lugar tiene un origen conocido y único. El origen es una Central de alarmas que se identifica

ante la Receptora. Por otra parte la receptora también se identifica ante la Central de manera que no podamos enganchar la Central con otra receptora.

Una vez identificados y asegurados el origen y destino debíamos de protegernos contra snifing, escucha de los datos transmitidos por la red TCP/IP. Estas técnicas de escucha de datos transmitidos por las redes podría ser realmente peligrosa, equivaldría a escuchar la línea telefónica en las transmisiones DTMF.

Escuchar líneas telefónicas convencionales es relativamente fácil. Escuchar líneas de datos es mas complicado pero también es posible, por lo que se decidió que si lograban escucharnos al menos que no se enteraran de nada. Los paquetes TCP/IP van encriptados de manera que lo "oído" no sirve para gran cosa.
Aún así los equipos informáticos permiten ejecutar muchos miles de operaciones por segundo, por lo que se podría intentar desencriptar la señal por fuerza bruta, a base de prueba error y comparación. De manera que se ha añadido un código variable que la receptora espera escuchar en la próxima transmisión para validar la comunicación.
En resumen todos estos elementos son:

- Identificar el lado de la Central.
- Identificar el lado de la Receptora.
- Encriptar la señal para que no se pueda entender.
- Variar la encriptación para que quien escuche no pueda aprender el idioma.

Conversores DTMF a TCP/IP

A nivel técnico estamos encontrando en el mercado múltiples sistemas de conexión de Centrales de alarma por TCP/IP. La solución provisional, ante la falta de Centrales TCP/IP nativas, que han ido dando en general los fabricantes, ha sido instalar conversores de señales DTMF a TCP/IP.

Estos sistemas son una manera de convertir las Centrales convencionales a TCP/IP pero en general estas Centrales no hacen todo lo que una Central nativa TCP/IP puede ser. Por otra parte nos encontramos con la imposibilidad de establecer una comunicación bi-direccional con la Central.

Esto es un grave inconveniente para los instaladores y receptoras de alarma. Esto les obliga a seguir con las comunicaciones bi-direccionales vía MODEM telefónico, con los consabidos problemas.

Los conversores no son una parte de la Central. Solo son traductores de un lenguaje de comunicación a otro. Por otra parte un aparato más supone una posibilidad de avería más.

Nos encontramos que muchos de estos sistemas tienen “test”, pero realmente este “test” controla que el conversor está operativo. No se está hablando con la Central, se está hablando con su traductor. Si queremos seguridad en el “test” debemos hablar directamente con la Central.

Además si el comunicador está integrado podremos hacer que las comunicaciones sean más rápidas, y sobre todo, al ser parte de la Central, está controlado por la Central y cualquier suceso es registrado y tratado como un verdadero elemento de seguridad.

CAPITULO V

PROPUESTA

BRIGADA DE CABALLERIA BLINDADA N° 11 “GALAPAGOS

5.1 ORGANIZACIÓN DE LA 11-BCB “GALAPAGOS”

La Brigada de Caballería Blindada No. 11 "GALÁPAGOS " perteneciente a las FF.AA del Ecuador, ubicada al Norte de la Ciudad de Riobamba en la Av. De los Héroes S/N. Cuenta con de 7 grupos de operaciones; 5 de Caballería y 2 de Artillería; una Compañía de Ingenieros, una Compañía de morteros, un Comando de apoyo logístico y una Compañía de Comunicaciones, lugar donde se realizará la pasantía.

- Comando y Estado Mayor.
- Grupo de Caballería Blindada No.30 “RIOBAMBA”.
- Grupo Escuela de Caballería Blindada No.31 “MACHALA”.
- Grupo de Caballería Blindada No. 32 “AZUAY”.
- Grupo de Caballería Blindada No. 33 “SARAGURO”.
- Grupo de Caballería Blindada No. 34 “EPICLACHIMA”.
- Grupo de Artillería Auto-Propulsado “TNTE. RODRIGUEZ”
- Grupo de Artillería No.12 “CABO QUIROZ”
- Batería de Artillería AM.-11 “AMAZONAS”
- Escuadrón Blindado de Morteros 120mm. No.11.
- Comando de Apoyo Logístico No.11 “CALUCUCHIMA”
- Escuadrón de Comunicaciones No. 11
- Escuadrón de Ingenieros Blindados No. 11

- Escuadrón Policía Militar No. 11
- Pelotón Banda de Músicos
- Escuadrón de Apoyo Cívico y Forestación No. 11 y 12
- Hospital de Brigada No.11
- Colegio Militar “COMBATIENTES DE TAPI”

Objetivos Generales de la 11-BCB "GALÁPAGOS"

- ✓ Reestructurar orgánica y funcionalmente a la 11-BCB " GALÁPAGOS".
- ✓ Mantener la capacidad operativa de la 11-BCB " GALÁPAGOS".
- ✓ Establecer un sistema de planificación que armonice con el Plan de Desarrollo de la Fuerza Terrestre.
- ✓ Fomentar como principio básico de comportamiento militar, la práctica permanente del liderazgo y de los valores éticos y morales.
- ✓ Elevar y mantener la moral y el bienestar del personal de la brigada.
- ✓ Fomentar y practicar la austeridad como un principio en la Fuerza Terrestre en general y en la Brigada en forma particular.
- ✓ Dirigir la integración con las otras unidades del Arma, con el propósito de armonizar recursos, establecer doctrina, mantener la unidad de acción, optimizar los recursos particularmente para el mantenimiento del material blindado.
- ✓ Optimizar la administración de recursos humanos, materiales y financieros, en todas las actividades que tienen que ver con el cumplimiento de las misiones encomendadas a la brigada.
- ✓ Conservar el material Bélico disponible, capaz que cuando se lo requiera se encuentre en las mejores condiciones.

5.2 Sistema de Alarmas

Introducción

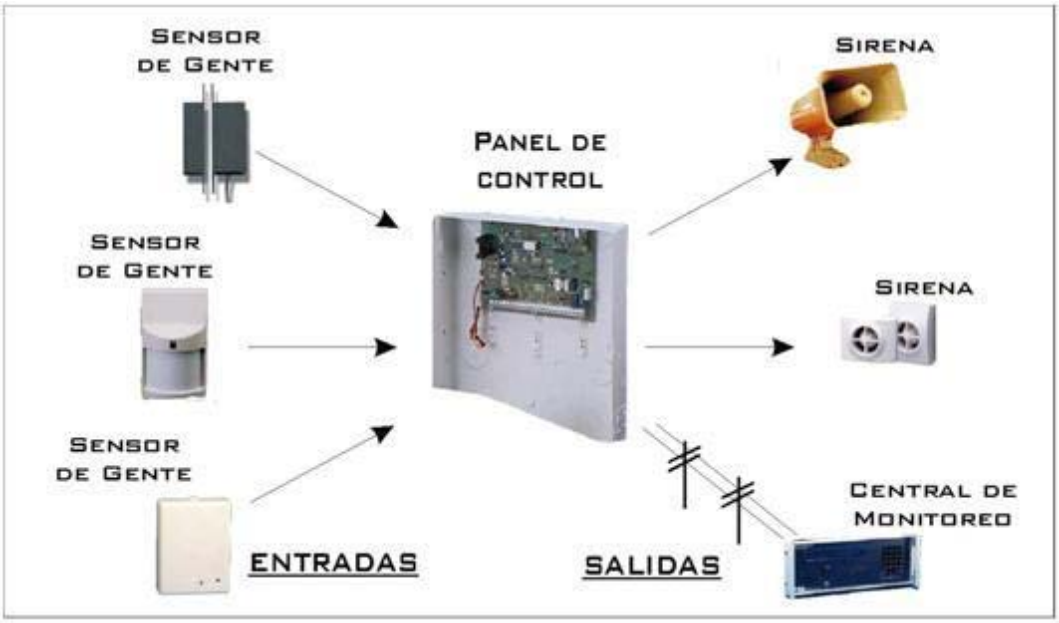
La necesidad de controlar el ingreso de personas no autorizadas en algún lugar determinado es la base de la existencia de estos equipos, los cuales mantienen la seguridad en comercios, oficinas, industrias, almacenes, áreas de diseño o desarrollo, laboratorios, etcétera.

La instalación de los sistemas de alarmas contra intrusos ha contribuido a reducir la cantidad de robos y hurtos producidos en los hogares, establecimientos publico o privados de todo el mundo, presentando no sólo la ventaja directa de la seguridad que brinda a las personas y sus bienes, sino también permitiendo reducir los montos de las primas de los seguros de las empresas, comercios y viviendas.

Sin embargo, como su uso aún no está debidamente generalizado, cada año continúan produciéndose numerosos incidentes, con daños humanos y materiales causados por la falta de una oportuna detección.
Estos sistemas de alarmas pueden contener los siguientes elementos:

- ✓ Central de alarma
- ✓ Batería y cargador
- ✓ Consola de activación/desactivación
- ✓ Cableado o vinculación inalámbrica
- ✓ Alarma
- ✓ Avisador telefónico
- ✓ Pulsadores de pánico/asalto
- ✓ Detectores

En ciertos modelos comerciales, algunos de estos elementos se encuentran debidamente integrados dentro de la central de alarma.



Central de alarma

La central de alarma es la parte medular del equipamiento, ya que es el elemento que se encarga de controlar automáticamente el funcionamiento general del sistema de alarma, recogiendo información del estado de los distintos detectores y accionando eventualmente los sistemas de aviso de la presencia de intrusos en el área protegida.

La central en sí es una tarjeta electrónica con sus distintas entradas y salidas, que se encuentra resguardada en un gabinete con protección antidesarme, el que generalmente también incluye la batería y su cargador.

Las centrales se clasifican de acuerdo a la cantidad de zonas independientes a

proteger, por lo que podemos encontrar productos de 2 zonas, 6 zonas, 16 zonas, etcétera.

Cada zona puede ser activada y desactivada en forma individual, lo que permite en hogares con muchas dependencias, proteger las áreas que no tienen presencia humana prevista y deshabilitar la protección en aquellas zonas ocupadas por los dueños de casa.

Asimismo, se suele incorporar un retardo de activación de la alarma en al menos una zona (zona temporizada), para dar tiempo a que pueda desactivarse el sistema, al ingresar los dueños al domicilio protegido. Sin embargo, esto no es necesario en los casos en que se dispone de un control remoto por ondas de radio.

Batería y cargador

Estos elementos sirven para proveer un sistema de alimentación eléctrica ininterrumpida (UPS), de manera que ante una falta del suministro eléctrico de red (normal o provocado por un ladrón), el sistema de alarma contra intrusos continúe brindando protección en forma absolutamente normal.

Consola de activación/desactivación

Esta consola habitualmente contiene un teclado que permite programar todas las funciones del sistema. Esta interface de control cuenta con teclas alfanuméricas, como también otras funciones de señalización de estados, por lo que constituye una pieza importante para el usuario del sistema. Existen señalizadores de dos tipos, los de led o luces, y también los de pantalla de cuarzo líquido. En ambos casos brindan información de cada una de las zonas

que están conectadas (áreas de protección exterior, puertas, ventanas, áreas interiores, etcétera).
En algunos modelos, la consola de activación/desactivación se encuentra montada en el frente de la central de alarma, aunque esto tiende a caer en desuso.

También existen modelos en que se dispone un control remoto por ondas de radio codificado, que permite la activación/desactivación de la central, y eventualmente puede accionar las sirenas y hacer llamados telefónicos en caso de asaltos.

Cableado o vinculación inalámbrica

Como su nombre lo indica, sirve para vincular los distintos componentes del sistema de alarma contra intrusos, ya sea por medio de cables o en forma inalámbrica. En el caso de redes cableadas, generalmente se utilizan dos conductores para alimentación de 12 V y dos conductores para las señales (circuito serie de NC).

Alarma

El elemento de alarma está formado generalmente por una sirena (o campana) que advierte de la ocurrencia de una intrusión detectada por el sistema, mediante una señal sonora de alto nivel. En algunos casos, también puede incluir algún tipo de señalización visual, como balizas y destelladores (flash), para aquellas personas que tienen problemas de audición o cuando existe un alto nivel de ruido ambiente.

La sirena exterior se coloca dentro de un gabinete para su protección, y se instala en la fachada de la casa, comercio o industria a proteger. Además de su función

de alertar en los casos en que se ha detectado un intruso, la sirena exterior es un elemento disuasivo de por sí, ya que advierte de la existencia de un sistema de alarma instalado en el domicilio.

Por otro lado, la sirena interior sirve para actuar como auxiliar de la exterior, de manera que las dos sirenas suenen al mismo tiempo. Si el intruso destruye la sirena exterior, queda funcionando la sirena interior dentro del lugar a proteger.

En todos los casos, estas sirenas emiten un sonido de unos 120 decibeles (equiparable al sonido de una ambulancia) y tienen una protección antidesarme que envía una señal a la central, en los casos en que se pretenda sabotear su correcto funcionamiento.

Para determinar el tipo de alarma a instalar debe tenerse en cuenta algunos factores como el nivel de ruido ambiental, el tipo y calidad del sonido ambiental, la duración de la señal requerida, el nivel acústico deseado y la alimentación eléctrica disponible.

Por ello, para su correcta instalación hay que tener en cuenta la presencia de fuentes de sonido en los locales a proteger, como por ejemplo equipos de aire acondicionado, sistemas estereofónicos, televisores, etcétera, que eventualmente impidan la audición de las sirenas de alarma.

Por otro lado, el entorno en el cual un señalizador luminoso debe ser instalado es lo que determina tanto el tipo de producto como la intensidad luminosa necesaria para cada aplicación. Por ello, un avisador luminoso diseñado para uso industrial, que incorpora una gran salida luminosa nunca podrá ser adecuado para un domicilio y viceversa

Avisador telefónico

En los sistemas de alarma más modernos, 33ateway se suele instalar un elemento que ante la ocurrencia de una anormalidad, efectúa un llamado al número telefónico programado previamente. Este llamado puede incluir un mensaje de voz grabado en una memoria no volátil o ser simplemente una secuencia de tonos característicos (bip-bip).

Pulsadores de pánico/asalto

Estos dispositivos de seguridad contra asalto deben ser colocados estratégicamente, para enviar una señal a la central de alarma, que ordene una acción de respuesta silenciosa, como por ejemplo la ejecución de un llamado telefónico, la activación de una señal luminosa o sonora en el puesto central de vigilancia.

Detectores

Los detectores se fabrican con diversas técnicas que operan bajo principios de funcionamiento diferentes.

En la mayoría de los casos se dispone un elemento sensor que analiza la

alteración de alguna magnitud física. Esta alteración es detectada por un circuito electrónico asociado que opera un contacto normalmente cerrado, que al abrirse envía la información de su estado a la central, la que acciona la alarma acústica y/o lumínica del sistema, para advertir la presencia de intrusos en el ambiente en que se halla instalado.

Estos detectores deben ser cuidadosamente seleccionados en función del tipo de alteración a identificar, para evitar falsas alarmas.

Por lo general, el detector está concebido para dar una rápida advertencia a un costo razonable, de manera de brindar un oportuno preaviso. Esta advertencia sólo es posible si el detector está correctamente localizado, instalado y mantenido.

Tipos de detectores

Magnético

- Son los dispositivos más comunes y utilizados en sistemas €.
- El propósito de éstos es disparar una alarma cuando se abra una puerta o ventana.
- S on montables en cualquier tipo de superficie.

Audio Detectores.

- Este tipo de sensores detectan la frecuencia de un vidrio al quebrarse, y reducen una alarma.

Detectores de ruptura de cristal

- Este tipo de detectores de ruptura de cristal es activado por dos frecuencias de audio
- Lo hacen más seguro y confiable para sistemas residenciales

Detectores de vibración

- Este tipo de detectores captan la vibración que produce un golpe en una pared.
- Se recomienda para zonas de respuesta rápida

Detectores de Impacto

- Este tipo de detectores van pegados sobre el vidrio
- Al impactarse algún objeto sobre el cristal se produce una alarma.

Sensores de Movimiento

- Pasivo Infrarrojo. Detecta la emanación de calor y su desplazamiento dentro del área seleccionada; si el desplazamiento de calor es muy rápido esto produce una alarma.

Detectores de Humo

- Iónico: Utilizan una pequeña cantidad de material radioactivo localizado dentro de la cápsula que contiene electrodos positivos y negativos. Bajo condiciones normales el material radioactivo permite a los electrones fluir dentro de la cápsula, pero cuando pequeñas partículas de humo entran en la cápsula, interfieren con la fluidez; esto provoca una alarma.
- Fotoeléctrico. Utilizan un emisor de luz, usualmente infrarrojo, y un detector fotoeléctrico. Estos elementos son distribuidos dentro de la cápsula de tal forma que en condiciones normales el detector fotoeléctrico no ve la luz enviada por la fuente emisora. Cuando grandes partículas de humo entran en la cápsula, éstas reflejan la luz en el detector fotoeléctrico el cual causa que se active la alarma.

5.3 MODULO DE COMUNICACIÓN IP "mIP"

Introducción

El *m***IP** (**M**odulo para **P**rotocolos **I**nternet) es un módulo adaptable para paneles de alarmas diseñado para enviar cualquier tipo de alarma o señal generada por el panel a través de redes de datos como Internet. Compatible con cualquier panel de alarmas que haga uso del protocolo Contact-ID, el mIP permite transmisiones de alarmas con una mayor velocidad de transmisión y con mayor seguridad a las Centrales Receptoras de Alarmas.

mIP

El módulo IP (MIP) es un sencillo dispositivo de comunicaciones que conectado a un panel de alarmas de seguridad realiza dos tareas básicas:

- El envío por una red IP de la información de alarmas que envía el panel de alarmas al que se conecta.
- La comprobación de la conectividad entre el panel de alarmas y el centro de recepción de alarmas.

El mIP está especialmente diseñado para operar con la mayoría de los paneles de alarmas instalados en el mercado actualmente y para permitir una transmisión de alarmas más rápida y económica mejorando los tiempos de respuesta, reduciendo los costes y proporcionando funcionalidades de valor añadido que permiten a la central receptora de alarmas supervisar los paneles de alarmas.

El mIP opera en conjunción con el VisorALARM, ubicado en el centro de recepción de alarmas, que se comporta como una receptora de alarmas que recibe las mismas por una red IP (en lugar de la clásica red telefónica pública) y las envía por un puerto serie a un software de automatización para su procesado. Además se encarga de recibir los mensajes de supervisión de

múltiples mIP y generar la correspondiente alarma en caso de que falle la comunicación con alguno de éstos.

Conexión telefónica del P.A.....
A teléfonos de la instalación.....
Línea telefónica.....
Conexión telefónica al P.A.....
Salida de relé .....
Entrada de alarma.....
Entrada de tamper.....
Alimentación (12Vdc).....
A la red de datos.....

FUNCIONALIDADES

Compatibilidad: Permite que cualquier panel de alarmas que soporte el protocolo Contact-ID transmita alarmas sobre redes IP.

Rapidez: El mIP permite la transmisión de alarmas en menos de un segundo a través de la red IP mejorando los tiempos de respuesta ante un evento.

Opera sobre cualquier tipo de red IP, tanto intranets como a través de Internet.

No requiere de una dirección IP pública y hace uso de un cliente DHCP para la configuración automática de la configuración IP.

Soporte de configuraciones en alta disponibilidad: Todas las alarmas se pueden enviar automáticamente a una receptora de respaldo en caso de pérdida de conectividad con la primera.

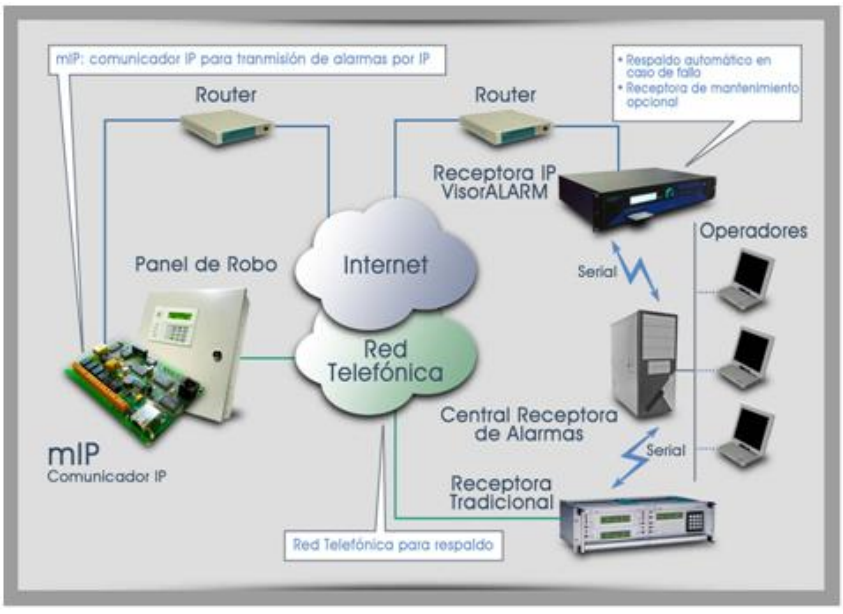
Puertos de transmisión configurables para permitir la compatibilidad de los mIP con los firewalls y proxies de la red.

Back up telefónico: Si mantiene la línea telefónica conectada al mIP, éste, en caso de indisponibilidad de las receptoras principal y de respaldo realizará un tercer nivel de respaldo a través de la línea telefónica como en un escenario tradicional.

Cifrado (AES 512 bits): Todas las alarmas y tramas de sondeo son enviadas a la receptora cifradas con un algoritmo AES de hasta 512 bits.

Bajo consumo: Con un consumo inferior a 200 mA en estado de reposo y de 240 mA durante la transmisión de una alarma.

Fácil instalación: El mIP puede instalarse dentro delpanel de alarmas o en su propia caja.



VisorALARM

La receptora VisorALARM es una receptora IP diseñada para recibir alarmas desde cualquiera de los módulos mIP instalados dentro de los paneles de alarmas convencionales. Desde el punto de vista de una Central Receptora de Alarmas, el VisorALARM funciona exactamente igual que cualquiera de las receptoras convencionales actualmente existentes en la CRA (Central receptora de Alarmar).

La receptora IP VisorALARM gestiona y recibe alarmas de paneles de robo y/o incendio equipados con un comunicador IP – mIP. Cada receptora VisorALARM es capaz de gestionar, simultáneamente, hasta 3.000 paneles de alarmas y proporciona el conjunto de funcionalidades más avanzado de la industria incluyendo supervisión de línea, 512 bits de cifrado y dos niveles de redundancia que garantiza el máximo nivel de disponibilidad y fiabilidad.

La integración con el software de gestión de la central receptora es casi inmediata. La receptora VisorALARM es capaz de emular los protocolos más utilizados del mercado. La comunicación entre la receptora IP y el software de automatización de la receptora se realiza a través de una conexión serie.

FUNCIONALIDADES

Escalabilidad: Gestión simultánea de hasta 3.000 mIPs.

Monitorización de línea: Monitorice el estado de la conectividad de todos los dispositivos registrados generando alarmas técnicas en caso de pérdida y/o restauración de la conectividad.

Monitorización de la red: Monitorice el estado de la red de acceso de central para evitar generar falsas alarmas en caso de fallo de la línea de datos central.

Soporte de direcciones IP dinámicas para los equipos remotos mIP.

Cifrado: Hace uso de algoritmos de cifrado AES de hasta 512 bits para cada uno de los dispositivos conectados con la receptora.

Comunicación de alarmas al software de control a través de un puerto serie haciendo uso del protocolo Contact-ID y emulando protocolos Surgard, Radionics o Ademco.

Smart card: Almacene toda la configuración de la receptora y la información de las cuentas en una tarjeta inteligente externa que puede ser usada para reemplazar inmediatamente la receptora por otra en caso de fallo físico.

Receptora de respaldo: Se pueden establecer dos receptoras VisorALARM en modo principal y respaldo para escenarios de alta disponibilidad. Los mIP son capaces, en tiempo real, de conectar con la receptora principal o de respaldo de forma transparente.

Sincronización automática: Las receptoras principal y de respaldo son capaces de sincronizarse las configuraciones y datos de cuentas.

Herramientas de gestión local y remota: La configuración local puede realizarse a través de una consola serie. La gestión remota a través de un software de gestión o de una sesión telnet.

Sistema operativo de tiempo real 24x7 para proporcionar rendimiento y protección frente a virus y ataques

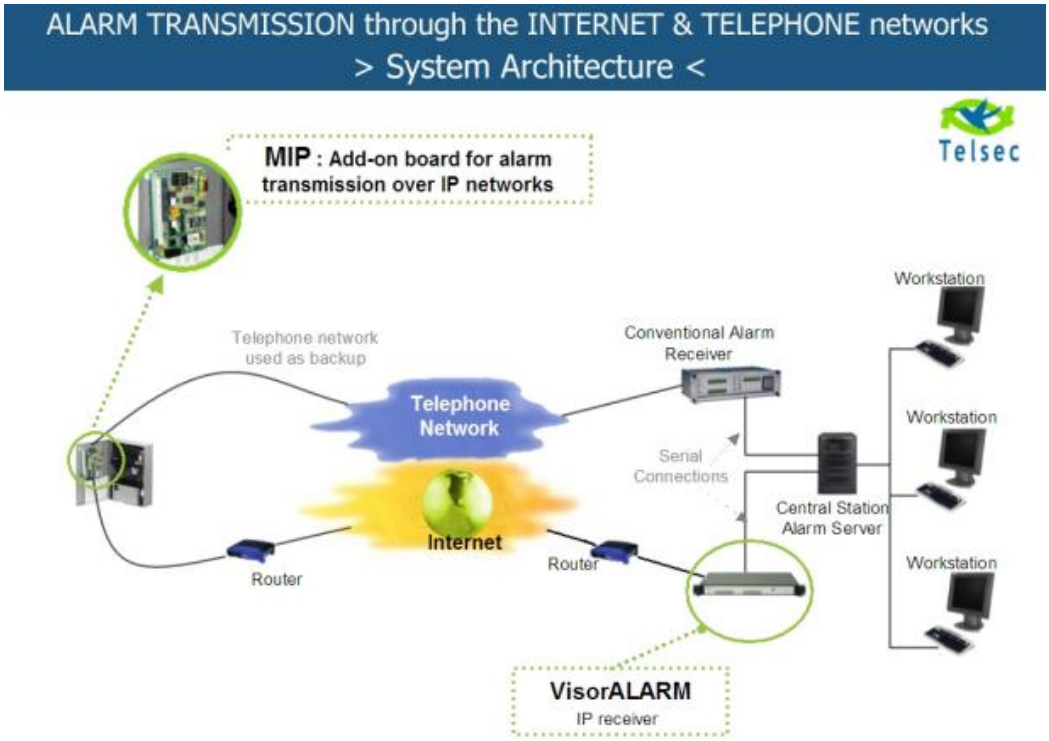
Cuando se genera una alarma en cualquiera de los paneles equipados con un módulo mIP, el proceso de transmisión de la alarma se lleva a cabo entre el mIP y la receptora VisorALARM. Este proceso se realiza con mayor velocidad y efectividad:

1. Se genera una alarma en uno de los paneles de alarmas (via activación de uno de sus sensores).
2. El panel de alarmas trata de llamar por RTC al número de teléfono de la receptora RTC configurada en el panel de alarmas.
3. El módulo mIP "intercepta" la llamada, obtiene la información del panel de alarmas y la encapsula en paquetes IP para ser mandados a través de la red de datos.
4. El mIP envía la alarma a través de Internet y con destino la receptora IP, el VisorALARM unit.
5. En menos de un segundo, el VisorALARM dispone de la alarma y comenzará con el proceso de transferencia de la misma hacia el software de automatización / monitorización haciendo uso de una conexión por puerto serie entre ella misma y el PC que corre el servidor de alarmas.
6. Una vez que la alarma ha llegado correctamente al software y que ha sido procesada, el VisorALARM enviará un "handshake" al mIP que provocará que éste retorne una señal de "kiss-off" al panel de alarmas lo que le indicará que el proceso se ha completado satisfactoriamente.

Que pasa si Internet está caída o por cualquier razón la alarma no llega a la receptora VisorALARM? En este caso, el comportamiento del MIP es el siguiente:

Si el mIP no es capaz de comunicarse con el VisorALARM o si el mIP no recibe el ACK de que la alarma se ha procesado entonces el mIP no proporcionará el kiss-off al panel de alarmas lo que provocará que el panel de alarmas reintente la transmisión de la alarma hacia la Central Receptora de Alarmas por RTC.

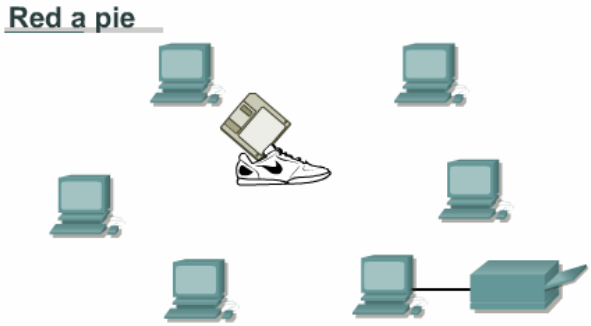
En esta segunda ocasión, el mIP no interceptará la llamada permitiendo que el panel de alarmas conecte con la receptora convencional de RTC mediante los mecanismos tradicionales de llamada telefónica



5.4 REDES DE DATOS

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. Por aquel entonces, los microcomputadores no estaban conectados entre sí como sí lo estaban las terminales de computadores mainframe, por lo cual no había una manera eficaz de compartir datos entre varios computadores. Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial. La red a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos
- Cómo comunicarse con eficiencia
- Cómo configurar y administrar una red

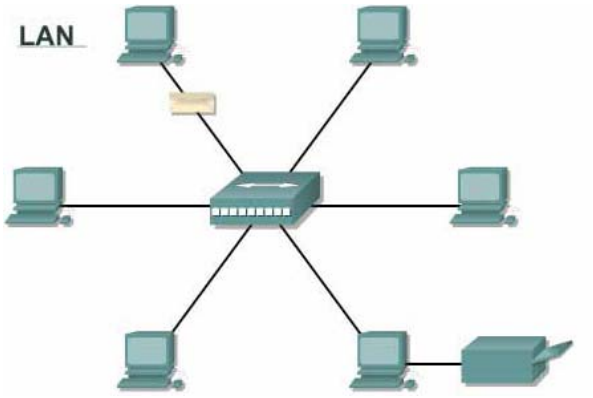


Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

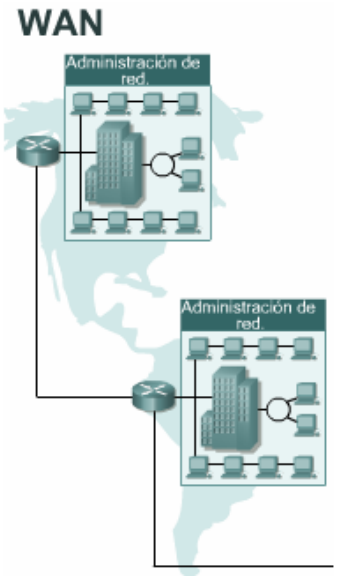
Una de las primeras soluciones fue la creación de los estándares de Red de área local (LAN – Local Area Network, en inglés). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN.

En un sistema LAN, cada departamento de la empresa era una especie de isla electrónica. A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes.



Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino también de una empresa a otra. La solución fue la creación de redes de área

metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias. La Figura resume las dimensiones relativas de las LAN y las WAN.



Distancia entre las CPU	Ubicación de las CPU	Nombre
0.1 m	Placa de circuito impreso/Asistente personal de datos	Motherboard Red de área personal (PAN)
1.0 m	Milímetro Mainframe	Red del sistema de la computadora
10 m	Habitación	Red de área local (LAN) Su aula
100 m	Edificio	Red de área local (LAN) Su escuela
1000 m = 1 km	Campus	Red de área local (LAN) Universidad de Stanford
100,000 m = 100 km	País	Red de área amplia (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continente	Red de área amplia (WAN) África
10,000,000 m = 10,000 km	Planeta	Wide Area Network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Red de área amplia (WAN) Tierra y satélites artificiales

HISTORIA DE LAS REDES INFORMATICOS

La historia de networking informática es compleja. Participaron en ella muchas personas de todo el mundo a lo largo de los últimos 35 años. Presentamos aquí una versión simplificada de la evolución de la Internet. Los procesos de creación y comercialización son mucho más complicados, pero es útil analizar el desarrollo fundamental.

En la década de 1940, los computadores eran enormes dispositivos electromecánicos que eran propensos a sufrir fallas. En 1947, la invención del transistor semiconductor permitió la creación de computadores más pequeños y confiables. En la década de 1950 los computadores mainframe, que funcionaban con programas en tarjetas perforadas, comenzaron a ser utilizados habitualmente por las grandes instituciones. A fines de esta década, se creó el circuito integrado, que combinaba muchos y, en la actualidad, millones de transistores en un pequeño semiconductor. En la década de 1960, los mainframes con terminales eran comunes, y los circuitos integrados comenzaron a ser utilizados de forma generalizada.

Hacia fines de la década de 1960 y durante la década de 1970, se inventaron computadores más pequeños, denominados minicomputadores. Sin embargo, estos minicomputadores seguían siendo muy voluminosos en comparación con los estándares modernos. En 1977, la Apple Computer Company presentó el microcomputador, conocido también como computador personal. En 1981 IBM presentó su primer computador personal. El equipo Mac, de uso sencillo, el PC IBM de arquitectura abierta y la posterior microminiaturización de los circuitos integrados dio como resultado el uso difundido de los computadores personales en hogares y empresas.

A mediados de la década de 1980 los usuarios con computadores autónomos comenzaron a usar módems para conectarse con otros computadores y compartir archivos. Estas comunicaciones se denominaban comunicaciones

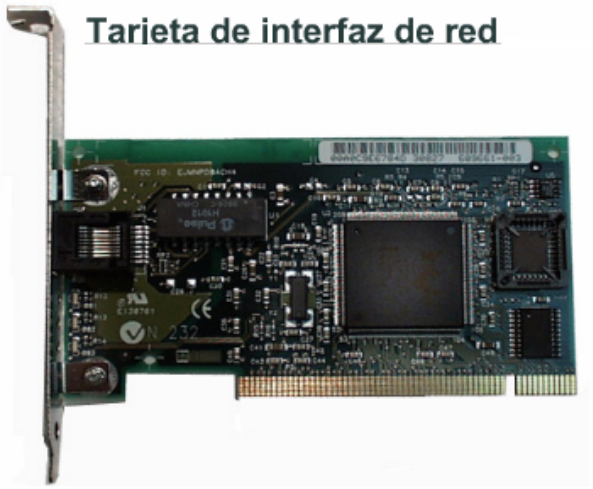
punto-a-punto o de acceso telefónico. El concepto se expandió a través del uso de computadores que funcionaban como punto central de comunicación en una conexión de acceso telefónico. Estos computadores se denominaron tableros de boletín. Los usuarios se conectaban a los tableros de boletín, donde depositaban y levantaban mensajes, además de cargar y descargar archivos. La desventaja de este tipo de sistema era que había poca comunicación directa, y únicamente con quienes conocían el tablero de boletín. Otra limitación era la necesidad de un módem por cada conexión al computador del tablero de boletín. Si cinco personas se conectaban simultáneamente, hacían falta cinco módems conectados a cinco líneas telefónicas diferentes. A medida que crecía el número de usuarios interesados, el sistema no pudo soportar la demanda. Imagine, por ejemplo, que 500 personas quisieran conectarse de forma simultánea. A partir de la década de 1960 y durante las décadas de 1970, 1980 y 1990, el Departamento de Defensa de Estados Unidos (DoD) desarrolló redes de área amplia (WAN) de gran extensión y alta confiabilidad, para uso militar y científico. Esta tecnología era diferente de la comunicación punto-a-punto usada por los tableros de boletín. Permitía la internetworking de varios computadores mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de un computador a otro. En lugar de poder comunicarse con un solo computador a la vez, se podía acceder a varios computadores mediante la misma conexión. La WAN del DoD finalmente se convirtió en la Internet

DISPOSITIVOS DE RED

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos. El primer grupo está compuesto por los dispositivos de usuario final. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario. El segundo grupo está formado por los dispositivos de red. Los dispositivos de red son todos

aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los hosts se ven sumamente limitadas. Los dispositivos host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos. Un NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard de un computador, o puede ser un dispositivo periférico. También se denomina adaptador de red. Las NIC para computadores portátiles o de mano por lo general tienen el tamaño de una tarjeta PCMCIA. Cada NIC individual tiene un código único, denominado dirección de control de acceso al medio (MAC). Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Tal como su nombre lo indica, la NIC controla el acceso del host al medio.



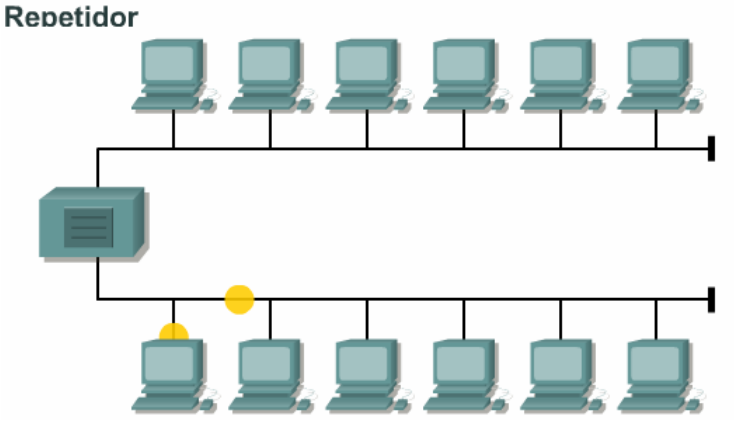
No existen símbolos estandarizados para los dispositivos de usuario final en la industria de networking. Son similares en apariencia a los dispositivos reales para permitir su fácil identificación.

Iconos de dispositivo del usuario final

Dispositivos del usuario final	
PC 	Impresora 
MAC 	Servidor de archivos 
Computadora portátil 	Mainframe IBM 

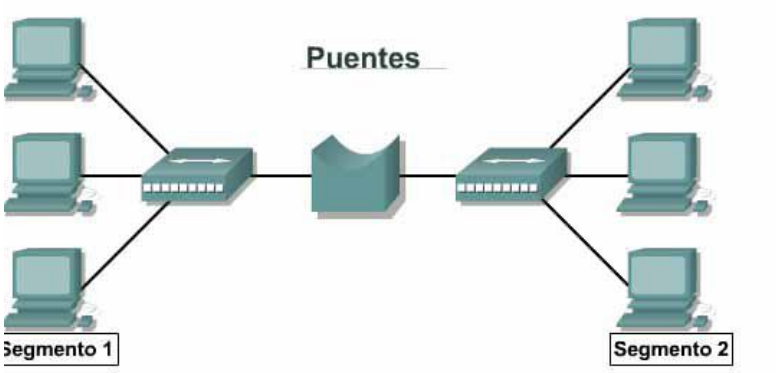
Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers. Por ahora se brinda una breve descripción general de los dispositivos de networking.

Un repetidor es un dispositivo de red que se utiliza para regenerar una señal. Los repetidores regeneran señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación. Un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un router o puente.

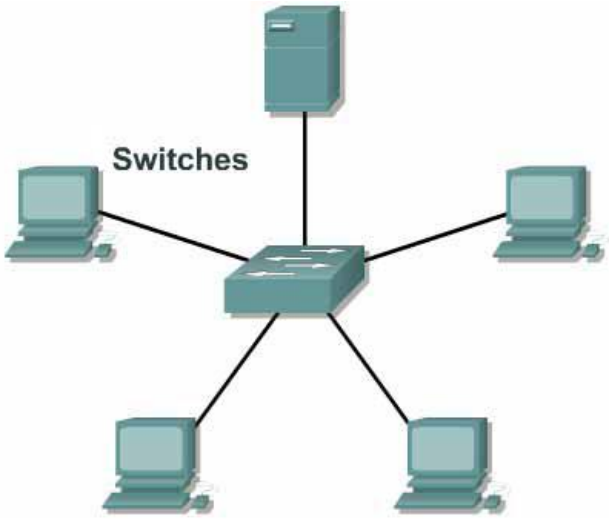


Los hubs concentran las conexiones. En otras palabras, permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs activos no sólo concentran hosts, sino que además regeneran señales.

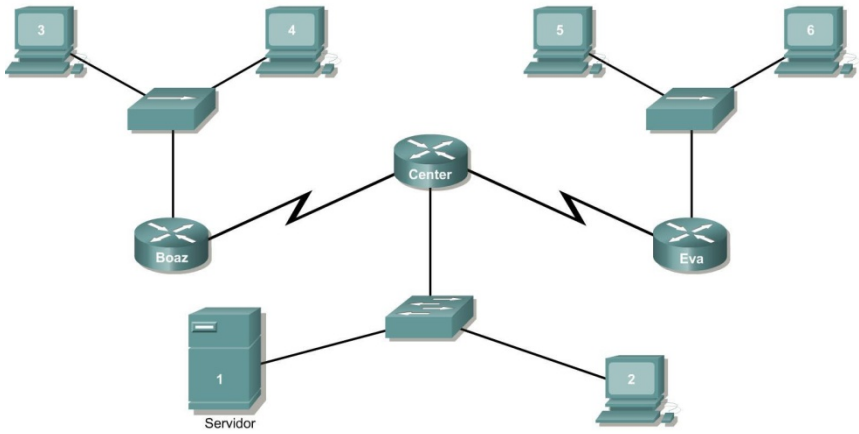
Los puentes convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.



Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.



Los routers poseen todas las capacidades indicadas arriba. Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.



PROTOCOLOS DE RED

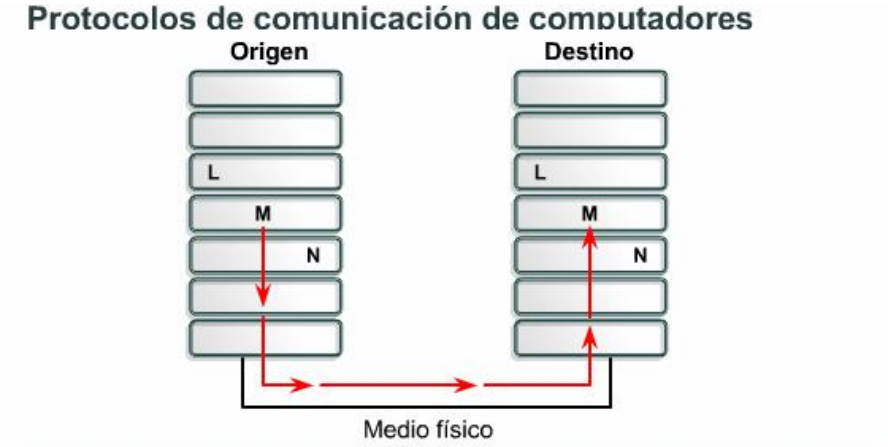
Los conjuntos de protocolos son colecciones de protocolos que posibilitan la comunicación de red desde un host, a través de la red, hacia otro host. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí. Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador.

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física
- Cómo los computadores se conectan a la red
- Cómo se formatean los datos para su transmisión
- Cómo se envían los datos
- Cómo se manejan los errores

Estas normas de red son creadas y administradas por una serie de diferentes organizaciones y comités. Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización

(ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT), antiguamente conocida como el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).



L, M, N	Capas en nuestro Modelo de Comunicación de Computadoras
Msource, Mdestination	Capas de pares
→	Comunicación entre pares
Protocolo de M capas	Las reglas mediante las cuales Msource se comunica con Mdestination

REDES DE AREA LOCAL LAN

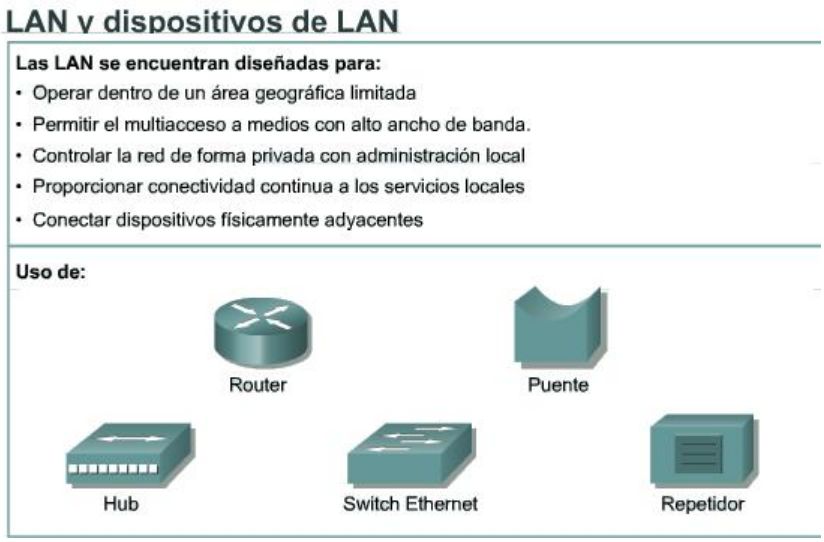
Las LAN constan de los siguientes componentes:

- Computadores
- Tarjetas de interfaz de red
- Dispositivos periféricos
- Medios de networking
- Dispositivos de networking

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo electrónico. Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

Algunas de las tecnologías comunes de LAN son:

- Ethernet
- Token Ring
- FDDI



REDES DE AREA AMPLIA WAN

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

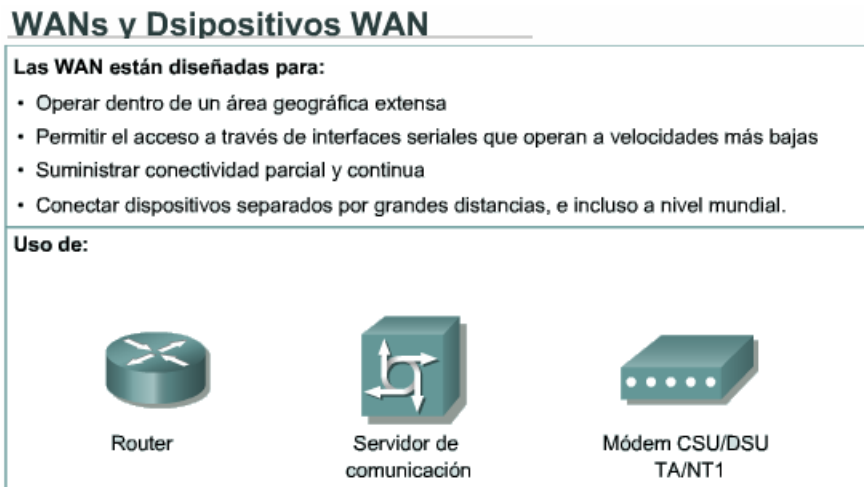
Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes

- Posibilitar capacidades de comunicación en tiempo real entre usuarios
- Brindar recursos remotos de tiempo completo, conectados a los servicios locales
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico

Algunas de las tecnologías comunes de WAN son:

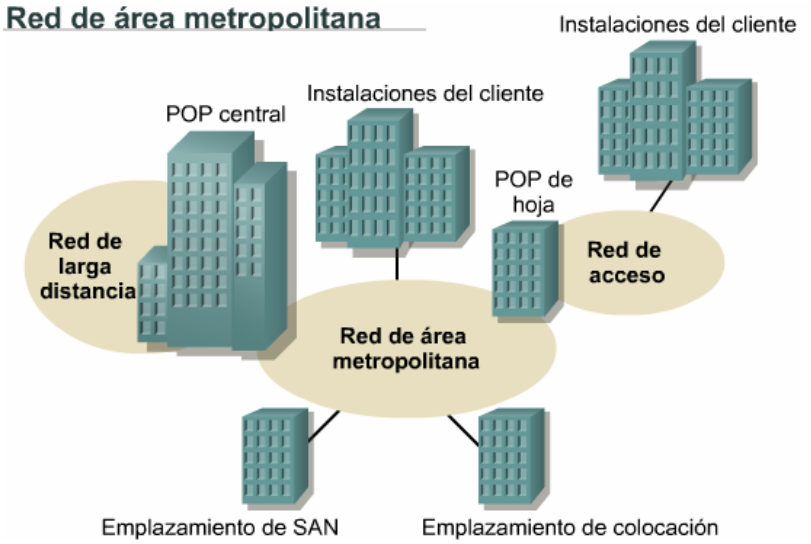
- Módems
- Red digital de servicios integrados (RDSI)
- Línea de suscripción digital (DSL – Digital Subscriber Line)
- Frame Relay
- Series de portadoras para EE.UU. (T) y Europa : T1, E1, T3, E3
- Red óptica síncrona (SONET)



REDES DE AREA METROPOLITANA MAN

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando

tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas



REDES DE AREA DE ALMACENAMIENTO SAN

Una SAN es una red dedicada, de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada, evita todo conflicto de tráfico entre clientes y servidores.

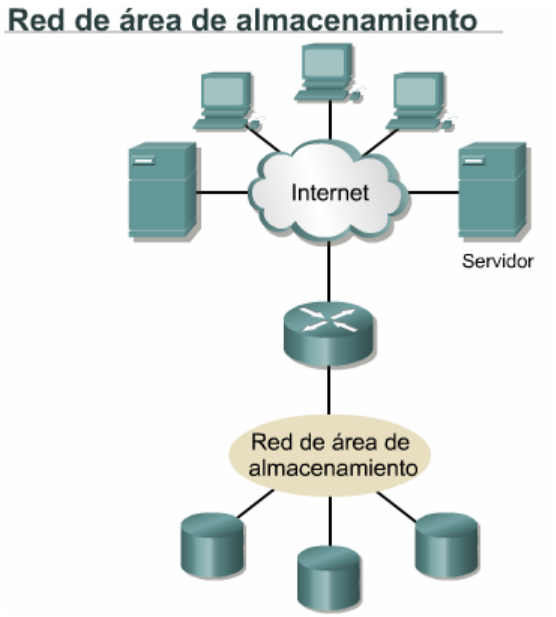
La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor. Este método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

Las SAN poseen las siguientes características:

- **Rendimiento:** Las SAN permiten el acceso concurrente de matrices de disco o cinta por dos o más servidores a alta velocidad, proporcionando un mejor rendimiento del sistema.

- **Disponibilidad:** Las SAN tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de10 kilómetros (km) o 6,2 millas.

- **Escalabilidad:** Al igual que una LAN/WAN, puede usar una amplia gama de tecnologías. Esto permite la fácil reubicación de datos de copia de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas



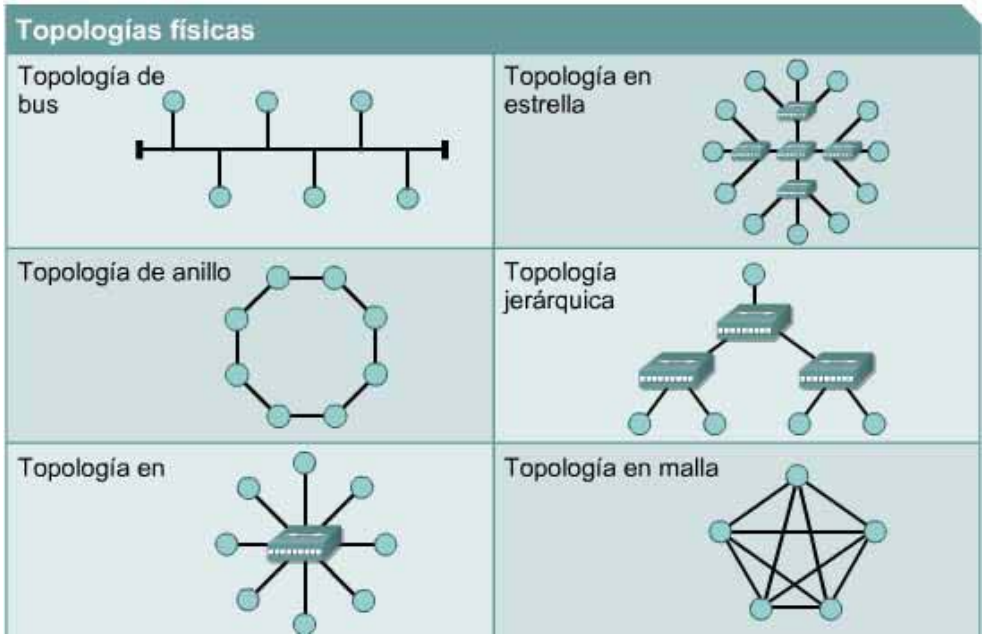
TOPOLOGIAS DE RED

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Las topologías físicas más comúnmente usadas son las siguientes: Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone. La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable. La topología en estrella conecta todos los cables con un punto central de concentración. Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red. Una topología jerárquica es similar a una estrella extendida. Pero en lugar de

conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de controlen red de una planta nuclear sería un ejemplo excelente. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa. La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens. La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada. La segunda topología lógica es la transmisión de tokens.

La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.



INTERNET

Internet, interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir, cada ordenador de la red puede conectarse a cualquier otro ordenador de la red. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados *intranets*, generalmente para el uso de una única organización, que obedecen a la misma filosofía de interconexión.

La tecnología de Internet es una precursora de la llamada “superautopista” de la información”, un objetivo teórico de las comunicaciones informáticas que permitiría proporcionar a colegios, bibliotecas, empresas y hogares acceso universal a una información de calidad que eduque, informe y entretenga. A finales de 1998 estaban conectados a Internet unos 148 millones de ordenadores, y la cifra sigue en aumento.

CÓMO FUNCIONA INTERNET

Internet es un conjunto de redes locales conectadas entre sí a través de una computadora especial por cada red, conocida como *60ateway* o puerta. Las interconexiones entre *gateways* se efectúan a través de diversas vías de comunicación, entre las que figuran líneas telefónicas, fibras ópticas y enlaces por radio. Pueden añadirse redes adicionales conectando nuevas puertas. La información que se debe enviar a una máquina remota se etiqueta con una dirección

Los distintos tipos de servicio proporcionados por Internet utilizan diferentes formatos de dirección. Uno de los formatos se conoce como decimal con puntos, por ejemplo 123.45.67.89. Otro formato describe el nombre del ordenador de destino y otras informaciones para el enrutamiento, por ejemplo "mayor.dia.fi.upm.es". Las redes situadas fuera de Estados Unidos utilizan sufijos que indican el país, por ejemplo (.es) para España o (.ar) para Argentina. Dentro de Estados Unidos, el sufijo anterior especifica el tipo de organización a que pertenece la red informática en cuestión, que por ejemplo puede ser una institución educativa (.edu), un centro militar (.mil), una oficina del Gobierno (.gov) o una organización sin ánimo de lucro (.org).

Una vez direccionada, la información sale de su red de origen a través de la puerta. De allí es encaminada de puerta en puerta hasta que llega a la red local que contiene la máquina de destino. Internet no tiene un control central, es decir, no existe ningún ordenador individual que dirija el flujo de información.

EL PROTOCOLO DE INTERNET

El Protocolo de Internet (IP) es el soporte lógico básico empleado para controlar este sistema de redes. Este protocolo especifica cómo las computadoras de puerta encaminan la información desde el ordenador emisor hasta el ordenador receptor. Otro protocolo denominado Protocolo de Control de Transmisión (TCP)

comprueba si la información ha llegado al ordenador de destino y, en caso contrario, hace que se vuelva a enviar. La utilización de protocolos TCP/IP es un elemento común en las redes Internet e *intranet*.

SERVICIOS DE INTERNET

Los sistemas de redes como Internet permiten intercambiar información entre computadoras, y ya se han creado numerosos servicios que aprovechan esta función. Entre ellos figuran los siguientes: conectarse a un ordenador desde otro lugar (telnet); transferir ficheros entre una computadora local y una computadora remota (protocolo de transferencia de ficheros, o FTP) y leer e interpretar ficheros de ordenadores remotos (gopher). El servicio de Internet más reciente e importante es el protocolo de transferencia de hipertexto (http), un descendiente del servicio de gopher. El http puede leer e interpretar ficheros de una máquina remota: no sólo texto sino imágenes, sonidos o secuencias de vídeo. El http es el protocolo de transferencia de información que forma la base de la colección de información distribuida denominada World Wide Web. Internet permite también intercambiar mensajes de correo electrónico (*e-mail*); acceso a grupos de noticias y foros de debate (*news*), y conversaciones en tiempo real (*chat*, *IRC*), entre otros servicios.

LA WORLD WIDE WEB

World Wide Web (también conocida como Web o WWW) es una colección de ficheros, que incluyen información en forma de textos, gráficos, sonidos y vídeos, además de vínculos con otros ficheros. Los ficheros son identificados por un localizador universal de recursos (URL, siglas en inglés) que específica el protocolo de transferencia, la dirección de Internet de la máquina y el nombre del fichero. Por ejemplo, un URL podría ser http://www.yahoo.com. Los programas informáticos denominados exploradores como Navigator, de Netscape, o Internet Explorer, de Microsoft utilizan el protocolo http para recuperar esos ficheros. Continuamente se desarrollan nuevos tipos de ficheros

para la WWW, que contienen por ejemplo animación o realidad virtual (VRML). Hasta hace poco había que programar especialmente los lectores para manejar cada nuevo tipo de archivo. Los nuevos lenguajes de programación (como JAVA, de Sun Microsystems) permiten que los exploradores puedan cargar programas de ayuda capaces de manipular esos nuevos tipos de información.

La gran cantidad de información vertida a la red ha dado lugar a la aparición de buscadores, páginas especializadas en hacer índices de los contenidos que facilitan localizaciones específicas. Algunos de los más populares son Yahoo, Google, Altavista o Lycos. También los hay específicos para páginas en español como Ozú u Olé.

DIRECCIONES IP Y MASCARA DE RED

Las direcciones binarias de 32 bits que se usan en Internet se denominan direcciones de Protocolo Internet (IP). En esta sección se describe la relación entre las direcciones IP y las máscaras de red.

Cuando se asignan direcciones IP a los computadores, algunos de los bits del lado izquierdo del número IP de 32 bits representan una red. La cantidad de bits designados depende de la clase de dirección. Los bits restantes en la dirección IP de 32 bits identifican un computador de la red en particular. El computador se denomina host. La dirección IP de un computador está formada por una parte de red y otra de host que representa a un computador en particular de una red en particular.

Para informarle al computador cómo se ha dividido la dirección IP de 32 bits, se usa un segundo número de 32 bits denominado máscara de subred. Esta máscara es una guía que indica cómo se debe interpretar la dirección IP al identificar cuántos de los bits se utilizan para identificar la red del computador. La máscara de subred completa los unos desde la parte izquierda de la máscara

de forma secuencial. Una máscara de subred siempre estará formada por unos hasta que se identifique la dirección de red y luego estará formada por ceros desde ese punto hasta el extremo derecho de la máscara. Los bits de la máscara de subred que son ceros identifican al computador o host en esa red. A continuación se suministran algunos ejemplos de máscaras de subred:

11111111000000000000000000000000 escrito en notación decimal separada por puntos es 255.0.0.0

O bien,

11111111111111110000000000000000 escrito en notación decimal separada por puntos es 255.255.0.0

En el primer ejemplo, los primeros ocho bits desde la izquierda representan la parte de red de la dirección y los últimos 24 bits representan la parte de host de la dirección. En el segundo ejemplo, los primeros 16 bits representan la parte de red de la dirección y los últimos 16 bits representan la parte de host de la dirección.

La conversión de la dirección IP 10.34.23.134 en números binarios daría como resultado lo siguiente:

00001010.00100010.00010111.10000110

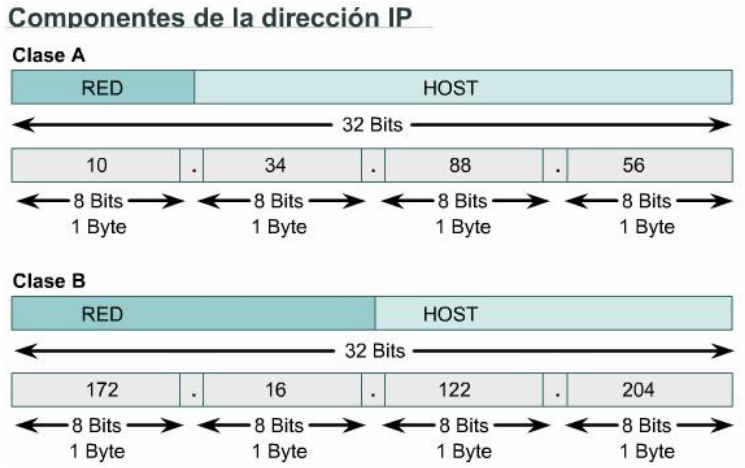
La ejecución de una operación AND booleana de la dirección IP 10.34.23.134 y la máscara de subred 255.0.0.0 da como resultado la dirección de red de este host:

00001010.00100010.00010111.10000110
11111111.00000000.00000000.00000000
00001010.00000000.00000000.00000000

00001010.00100010.00010111.10000110
11111111.11111111.00000000.00000000
00001010.00100010.00000000.00000000

Convirtiendo el resultado a una notación decimal separada por puntos, se obtiene 10.34.0.0 que es la parte de red de la dirección IP cuando se utiliza la máscara 255.255.0.0.

La siguiente es una ilustración breve del efecto que tiene la máscara de red sobre una dirección IP. La importancia de las máscaras se hará mucho más evidente a medida que se trabaje más con las direcciones IP. Por el momento, sólo hay que comprender el concepto de lo que es una máscara.



5.5 DISEÑO DE UNA RED LAN[1]

Objetivos del diseño de LAN

El primer paso en el diseño de una LAN es establecer y documentar los objetivos de diseño. Estos objetivos son específicos para cada organización o situación.

- **Funcionalidad:** La red debe funcionar. Es decir, debe permitir que los usuarios cumplan con sus requisitos laborales. La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.
- **Escalabilidad:** La red debe poder aumentar de tamaño. Es decir, el diseño original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.
- **Adaptabilidad:** La red debe diseñarse teniendo en cuenta futuras tecnologías. La red no debería incluir elementos que limiten la implementación de nuevas tecnologías a medida que éstas van apareciendo.
- **Facilidad de administración:** La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad de funcionamiento constante.

Consideraciones del diseño de una LAN

Muchas organizaciones han actualizado sus LAN en la actualidad o planean implementar nuevas LAN. Esta expansión en el diseño de la LAN se debe al desarrollo de tecnologías de alta velocidad como por ejemplo el Modo de Transferencia Asíncrona (ATM). Esta expansión también se debe a arquitecturas LAN complejas que utilizan conmutación de LAN y LAN virtuales (VLAN).

Para maximizar el ancho de banda y el rendimiento disponible de la LAN, deberán tenerse en cuenta las siguientes consideraciones de diseño de LAN:

[1] Ver Anexo 1

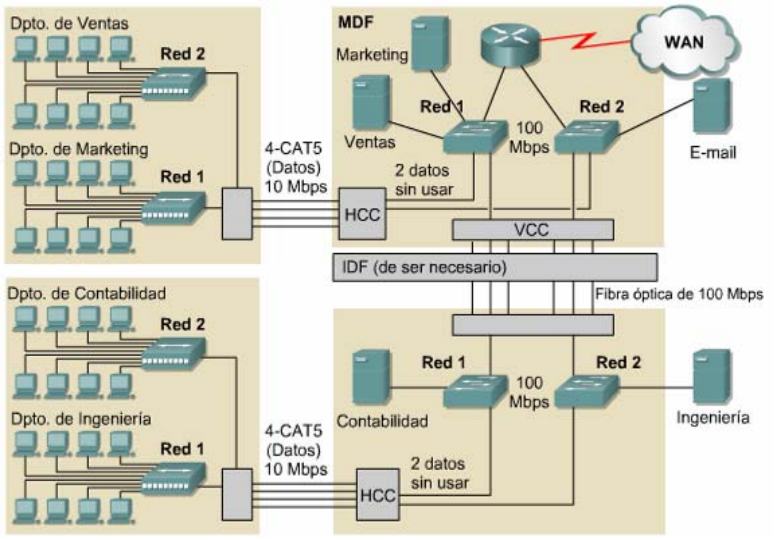
- Función y ubicación de los servidores
- Temas relacionados con los dominios de colisión[2]
- Temas de segmentación
- Temas relacionados con los dominios de broadcast[3]

Los servidores permiten que los usuarios de red se comuniquen y compartan archivos, impresoras y servicios de aplicación. Los servidores por lo general no operan como estaciones de trabajo. Los servidores ejecutan sistemas operativos especializados como por ejemplo NetWare, Windows NT, UNIX y Linux. Cada servidor por lo general está dedicado a una función, por ejemplo, correo electrónico o archivos compartidos.

Los servidores se pueden categorizar en servidores empresariales o servidores de grupo de trabajo. Un servidor empresarial soporta todos los usuarios en la red ofreciendo servicios tales como correo electrónico o Sistema de Nombres de Dominio (DNS). El correo electrónico o el DNS son servicios que cualquier persona de una organización necesita porque son funciones centralizadas. Un servidor de grupo de trabajo soporta un conjunto específico de usuarios y ofrece servicios como por ejemplo el procesamiento de texto y capacidades de archivos compartidos.

Como se ve en la figura, los servidores empresariales deben colocarse en el servicio de distribución principal (MDF).

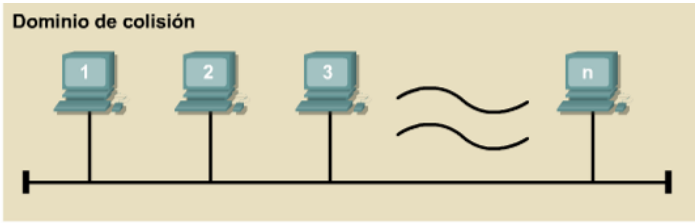
[2] Ver anexo 2
[3] Ver anexo 2



Siempre que sea posible, el tráfico hacia los servidores empresariales sólo tiene que viajar hacia el MDF y no transmitirse a través de otras redes. Sin embargo, algunas redes utilizan un núcleo enrutado o incluso pueden tener un servidor central para los servidores empresariales. En estos casos, el tráfico de red viaja a través de otras redes y por lo general no se puede evitar. Lo ideal es que los servidores de grupo de trabajo se coloquen en el servicio de distribución intermedia (IDF) más cercano a los usuarios que acceden a las aplicaciones en estos servidores. Esto permite al tráfico viajar por la infraestructura de red hacia un IDF y no afecta a los demás usuarios en ese segmento de red. Los switches LAN de Capa 2 ubicados en el MDF y los IDF deben tener 100 Mbps o más asignados para estos servidores.

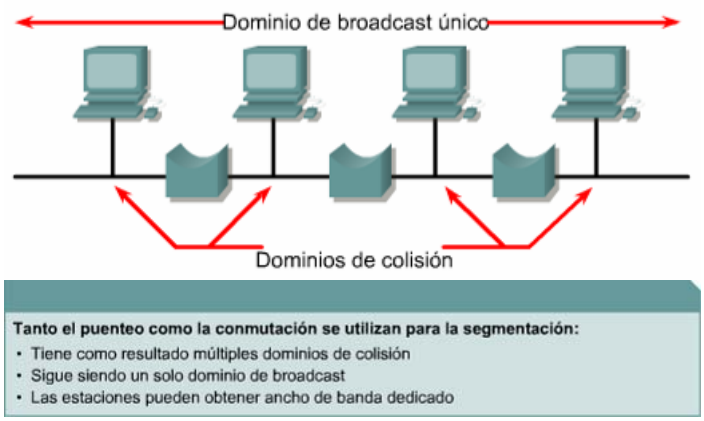
Los nodos Ethernet utilizan CSMA/CD. Cada nodo debe disputar con otros nodos para acceder al medio compartido o al dominio de colisión. Si dos nodos transmiten al mismo tiempo, se produce una colisión. Cuando se produce una colisión la trama transmitida se elimina y se envía una señal de embotellamiento a todos los nodos del segmento. Los nodos esperan un período de tiempo al azar y luego vuelven a enviar los datos. Las colisiones excesivas pueden reducir el

ancho de banda disponible de un segmento de red a treinta y cinco o cuarenta por ciento del ancho de banda disponible.



Dominio de colisión: Acceso compartido básico

La segmentación se realiza cuando un sólo dominio de colisión se divide en dominios de colisión más pequeños.

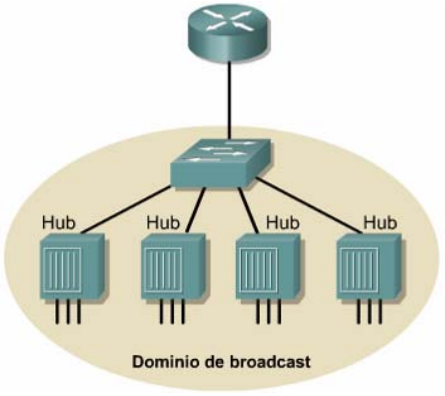


Tecnología Ethernet - Segmentación

Los dominios de colisión más pequeños reducen la cantidad de colisiones en un segmento LAN y permiten una mayor utilización del ancho de banda. Los dispositivos de la Capa 2 como por ejemplo puentes y switches se pueden utilizar para segmentar una LAN. Los routers pueden lograr esto a nivel de la Capa 3.

Se produce un broadcast cuando el control de acceso al medio destino (MAC) se configura en FF-FF-FF-FF-FF-FF. Un dominio de broadcast se refiere al conjunto de dispositivos que reciben una trama de datos de broadcast desde cualquier dispositivo dentro de este conjunto. Todos los hosts que reciben una trama de datos de broadcast deben procesarla. Este proceso consume los recursos y el ancho de banda disponible del host. Los dispositivos de Capa 2 como los puentes y switches reducen el tamaño de un dominio de colisión. Estos dispositivos no

reducen el tamaño del dominio de broadcast. Los routers reducen el tamaño del dominio de colisión y el tamaño del dominio de broadcast en la Capa 3.



Dominio de Broadcast

Metodología de diseño de una LAN

Para que una LAN sea efectiva y satisfaga las necesidades de los usuarios, se la debe diseñar e implementar de acuerdo con una serie planificada de pasos sistemáticos:

- Reunir requisitos y expectativas
- Analizar requisitos y datos
- Diseñar la estructura o topología de las Capas 1, 2 y 3 de la LAN
- Documentar la implementación física y lógica de la red

El proceso destinado a recabar información ayuda a aclarar e identificar cualquier problema de red actual. Esta información incluye el historial de la organización y su estado actual, el crecimiento proyectado, las políticas operativas y los procedimientos de administración, los sistemas y procedimientos de oficina y los puntos de vista de las personas que utilizarán las LAN.

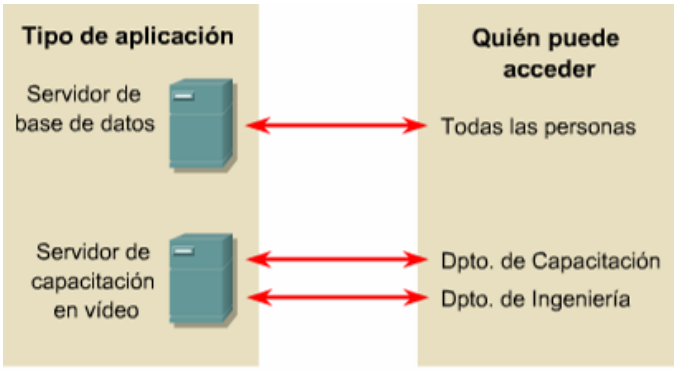
Reunir requisitos y expectativas

Deberán formularse las siguientes preguntas al reunir la información:

- ¿Quiénes son las personas que utilizarán la red?

- ¿Cuál es el nivel de capacitación de estas personas?
- ¿Cuáles son sus actitudes con respecto a las computadoras y las aplicaciones informáticas?
- ¿Cuál es el nivel de desarrollo de las políticas documentadas organizacionales?
- ¿Sólo se soportan determinados hosts de escritorio?
- ¿Quién es responsable de las direcciones, la denominación, el diseño de topología y la configuración de las LAN?
- ¿Cuáles son los recursos humanos organizacionales, de hardware y de software?
- ¿Cómo se vinculan y comparten estos recursos actualmente?
- ¿Cuáles son los recursos financieros de los que dispone la organización?

La documentación de los requisitos permite una estimación informada de los costos y líneas temporales para la implementación de diseño de LAN. Es importante comprender los problemas de rendimiento de cualquier red.



Análisis de requisitos y datos

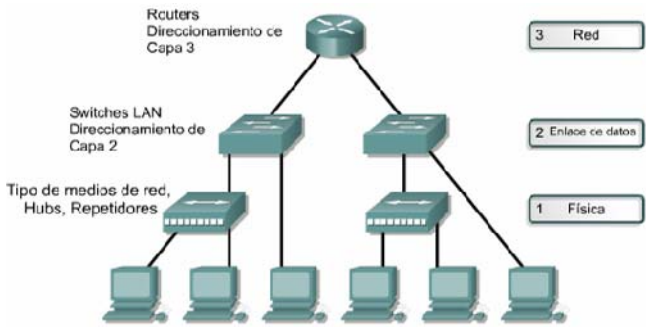
La disponibilidad mide la utilidad de la red. A continuación, presentamos algunas de las muchas cosas que afectan la disponibilidad:

- Tasa de transferencia
- Tiempo de respuesta
- Acceso a los recursos

El siguiente paso en el diseño de red es analizar los requisitos de la red y de sus usuarios. Las necesidades del usuario de la red cambian constantemente. A medida que se introducen más aplicaciones de red basadas en voz y vídeo, la presión por aumentar el ancho de banda de la red se torna también más intensa.

Una LAN que no puede suministrar información veloz y precisa a los usuarios no tiene ninguna utilidad. Se deben tomar medidas para asegurar que se cumplan los requisitos de información de la organización y de sus trabajadores.

El siguiente paso es decidir cuál será la topología LAN general que satisface los requisitos del usuario.



Desarrollo de una topología LAN

La topología en estrella y la topología en estrella extendida usan la tecnología CSMA/CD Ethernet 802.3. La topología en estrella CSMA/CD es la configuración dominante en la industria.

El diseño de topología LAN se puede dividir en las tres siguientes categorías únicas del modelo de referencia OSI:

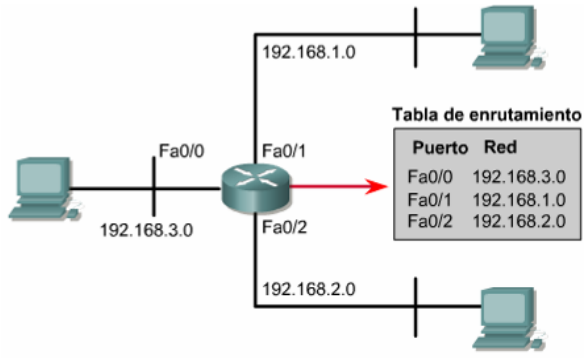
- Capa de red
- Capa de enlace de datos
- Capa física

El paso final en la metodología de diseño LAN es documentar la topología física y lógica de la red. La topología física de la red se refiere a la forma en que distintos

componentes de LAN se conectan entre sí. El diseño lógico de la red se refiere al flujo de datos que hay dentro de una red. También se refiere a los esquemas de nombre y dirección que se utilizan en la implementación de la solución de diseño LAN.

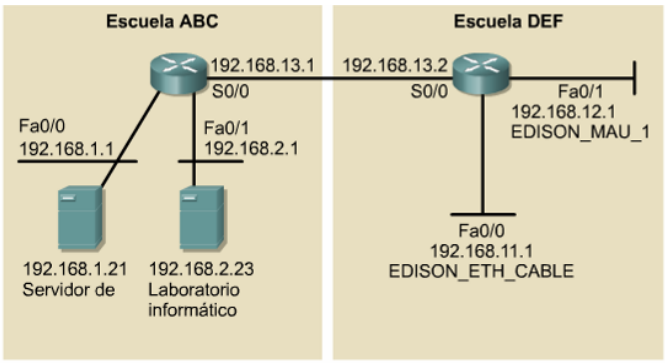
A continuación, presentamos documentación de diseño LAN importante:

- Mapa de topología de capa OSI
- Mapa lógico de LAN
- Mapa físico de la LAN
- Planes de distribución
- Mapa lógico de VLAN
- Mapa lógico de Capa 3



Se utilizan los routers para imponer una estructura lógica

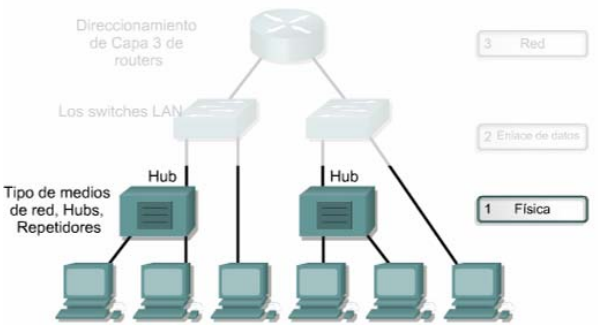
- Mapas de dirección



Asignaciones de direccionamiento

Diseño de Capa 1

Uno de los componentes más importantes a considerar en el diseño de red son los cables.



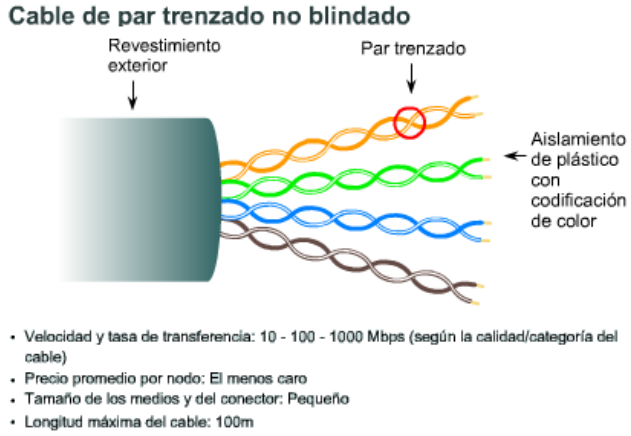
Desarrollo de topología LAN de Capa 1

En la actualidad, la mayor parte del cableado LAN se basa en la tecnología Fast Ethernet. Fast Ethernet es la tecnología Ethernet que se ha actualizado de 10 Mbps a 100 Mbps y tiene la capacidad de utilizar la funcionalidad full-duplex. Fast Ethernet utiliza la topología de bus lógica orientada a broadcast Ethernet estándar de 10BASE-T, y el método CSMA/CD para direcciones MAC.

Los temas de diseño en la Capa 1 incluyen el tipo de cableado que se debe utilizar (normalmente cable de cobre o fibra óptica) y la estructura general del cableado.

Esto también incluye el estándar TIA/EIA-568-A para la configuración y conexión de los esquemas de cableado. Los tipos de medios de la Capa 1 incluyen el par trenzado no blindado (UTP) o el par trenzado blindado (STP) Categoría 5, 5e o 6 10/100BASE-TX y el cable de fibra óptica 100BaseFX.

Deberá realizarse una evaluación minuciosa de los puntos fuertes y debilidades de las topologías. Una red tiene la misma efectividad que la de los cables que se utilizan.

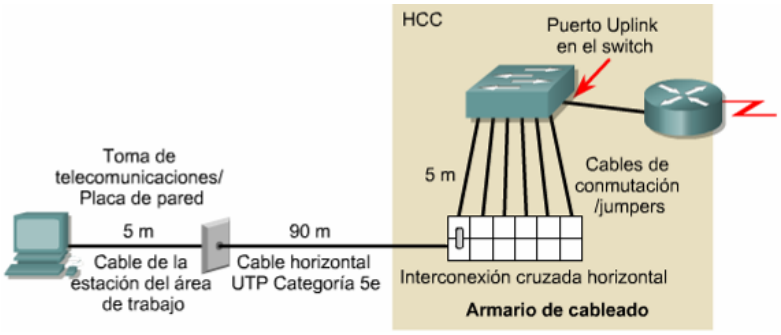


Los temas de Capa 1 provocan la mayoría de los problemas de red. Se deberá llevar a cabo una auditoria de cableado cuando se planee realizar cambios significativos en una red. Esto ayuda a identificar las áreas que requieren actualizaciones y nuevo cableado.

En todos los diseños de cable se debe utilizar cable de fibra óptica en el backbone y en los conductos verticales. El cable UTP Categoría 5e se deberá utilizar en los tendidos horizontales. La actualización de cable debe tener prioridad sobre cualquier otro cambio necesario. Las empresas también deberán asegurarse de que estos sistemas se implementen de conformidad con estándares de la industria bien definidos como por ejemplo las especificaciones TIA/EIA-568-A

El estándar TIA/EIA-568-A especifica que cada dispositivo conectado a la red debe estar conectado a una ubicación central a través de cableado horizontal. Esto se aplica si todos los hosts que necesitan acceso a la red se encuentran dentro de un límite de distancia de 100 metros (328 pies) para el UTP Ethernet Categoría 5e.

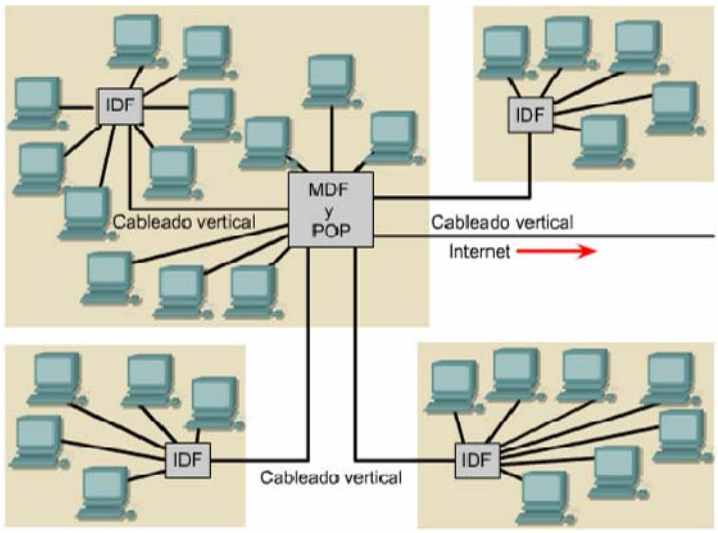
En una topología en estrella simple con un solo armario del cableado, el MDF incluye uno o más paneles de conexión cruzada horizontal (HCC).



MDF típica de la topología en estrella

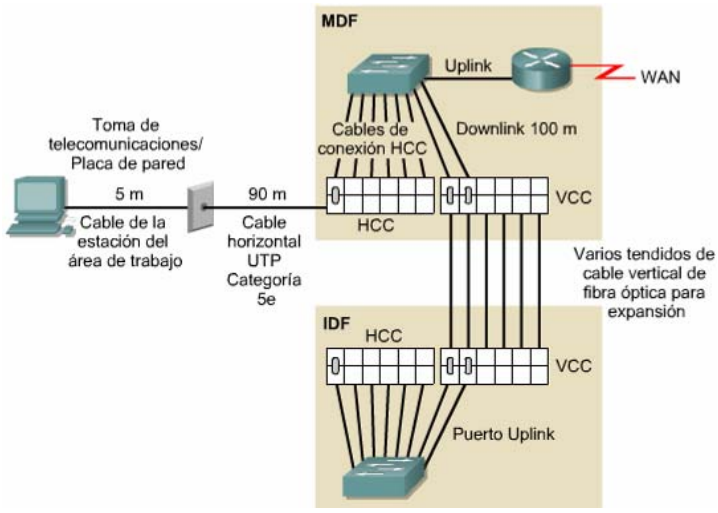
Los cables de conexión HCC se utilizan para conectar el cableado horizontal de Capa 1 con los puertos del switch LAN de Capa 2. El puerto uplink del switch LAN, basado en el modelo, está conectado al puerto Ethernet del router de Capa 3 con un cable de conexión. En este punto, el host final tiene una conexión física completa hacia el puerto del router.

Cuando los hosts de las redes de mayor tamaño están ubicados fuera del límite de 100 metros (328ft.) para el UTP Categoría 5e, se requiere más de un armario de cableado. La presencia de varios armarios de cableado implica la existencia de múltiples áreas de captación. Los armarios secundarios de cableado se denominan IDF.



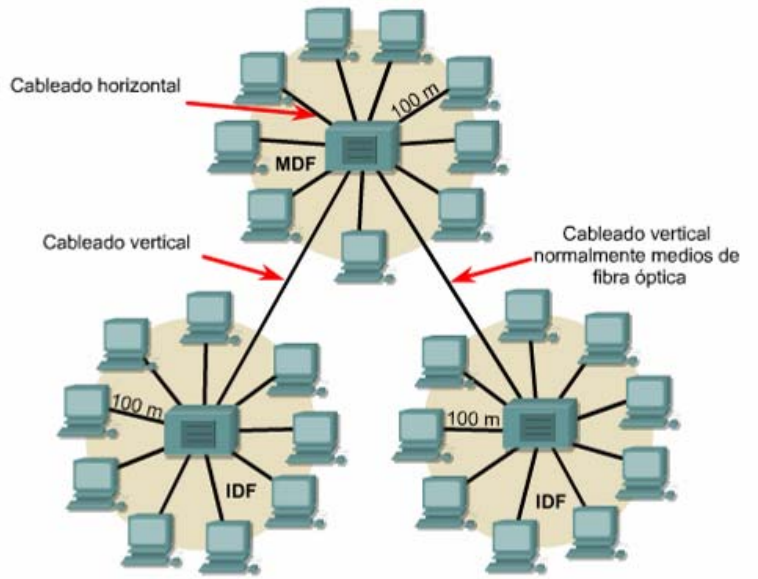
Campus con varios edificios

Los estándares TIA/EIA-568-A especifican que los IDF se deben conectar al MDF utilizando cableado vertical, también denominado cableado backbone.



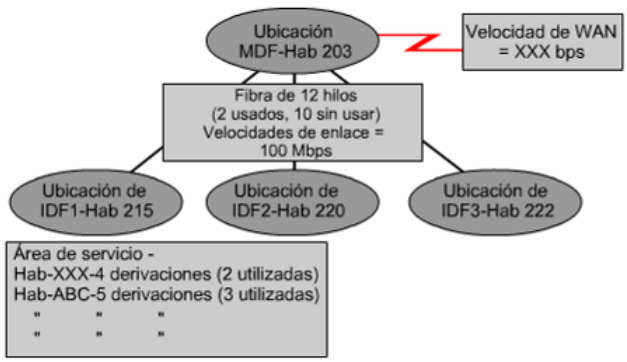
Topología en estrella extendida en un campus compuesto por varios edificios

Se utiliza un cable de conexión cruzada vertical (VCC) para interconectar los diversos IDF con el MDF central. Se utiliza normalmente el cable de fibra óptica debido a que las longitudes del cable vertical son generalmente más largas que el límite de 100metros (328 pies) del cable UTP Categoría 5e.



Topología en estrella extendida

El diagrama lógico es el modelo de topología de red sin todos los detalles de la instalación exacta del cableado



Documentación de la Capa 1 – Diagrama lógico

El diagrama lógico es el mapa de ruta básico de la LAN que incluye los siguientes elementos:

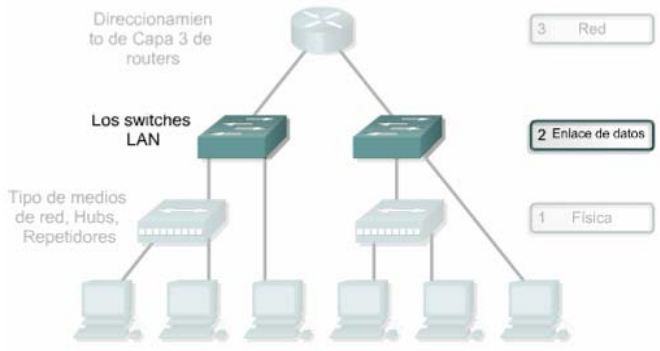
- Especificar las ubicaciones e identificaciones de los armarios de cableado MDF e IDF.
- Documentar el tipo y la cantidad de cables que se utilizan para interconectar los IDF con el MDF.
- Documentar la cantidad de cables de repuesto que están disponibles para aumentar el ancho de banda entre los armarios de cableado. Por ejemplo, si el cableado vertical entre el IDF 1 y el MDF se ejecuta a un 80% de su uso, se pueden utilizar dos pares adicionales para duplicar la capacidad.
- Proporcionar documentación detallada sobre todos los tendidos de cable, los números de identificación y en cuál de los puertos del HCC o VCC termina el tendido de cableado.

El diagrama lógico es esencial para diagnosticar los problemas de conectividad de la red. Si la habitación 203 pierde conectividad a la red, el plan de distribución muestra que la habitación tiene un tendido de cable 203-1, que se termina en el puerto 13 de HCC1. Se pueden utilizar analizadores de cables para determinar las fallas de la Capa 1. De haber alguna, uno de los dos tendidos se puede utilizar

para reestablecer la conectividad y ofrecer tiempo para diagnosticar las fallas del tendido 203-1.

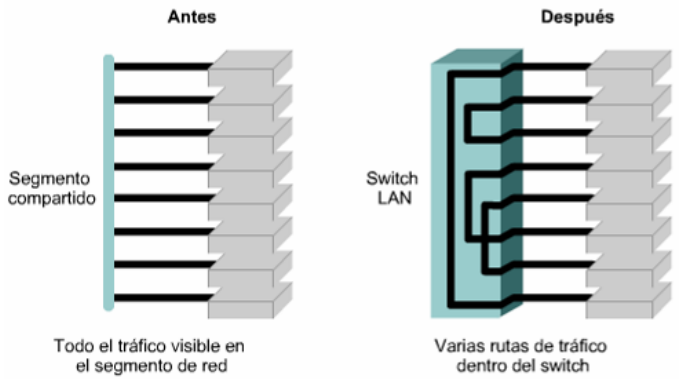
Diseño de Capa 2

El propósito de los dispositivos de la Capa 2 en la red es conmutar tramas basadas en sus direcciones MAC destino, ofrecer detección de errores y reducir la congestión en la red.



Los dos dispositivos de networking de Capa 2 más comunes son los puentes y switches LAN. Los dispositivos de la Capa 2 determinan el tamaño de los dominios de colisión.

Las colisiones y el tamaño de los dominios de colisión son dos factores que afectan de forma negativa el rendimiento de una red.

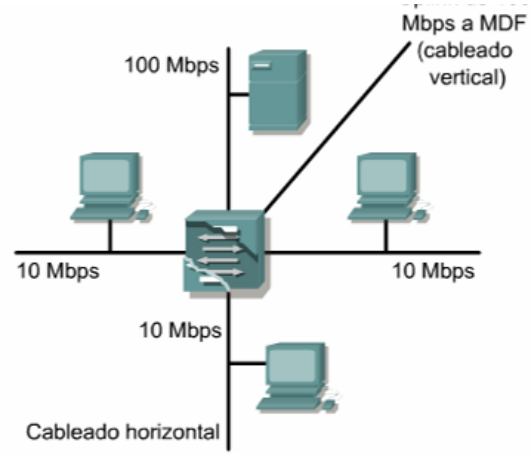


Microsegmentación de la red

La microsegmentación de la red reduce el tamaño de los dominios de colisión y reduce las colisiones. La microsegmentación se implementa a través del uso de puentes y switches. El objetivo es aumentar el rendimiento de un grupo de

trabajo o de un backbone. Los switches se pueden utilizar junto con hubs para suministrar el nivel de rendimiento adecuado para distintos usuarios y servidores.

Otra característica importante de un switch LAN es la forma en que puede asignar ancho de banda por puerto. Esto permite ofrecer más ancho de banda para el cableado vertical, los uplinks y los servidores.



Conmutación asimétrica

Este tipo de conmutación se conoce como conmutación asimétrica. La conmutación asimétrica proporciona conexiones de conmutación entre puertos con distinto ancho de banda por ejemplo, una combinación de puertos de 10 Mbps y de 100 Mbps. La conmutación simétrica ofrece conexiones conmutadas entre puertos de ancho de banda similar.

La capacidad deseada de un tendido de cable vertical es mayor que la de un tendido de cable horizontal. La instalación de un switch LAN en MDF e IDF, permite al tendido de cable vertical administrar el tráfico de datos que se transmiten desde el MDF hasta el IDF.

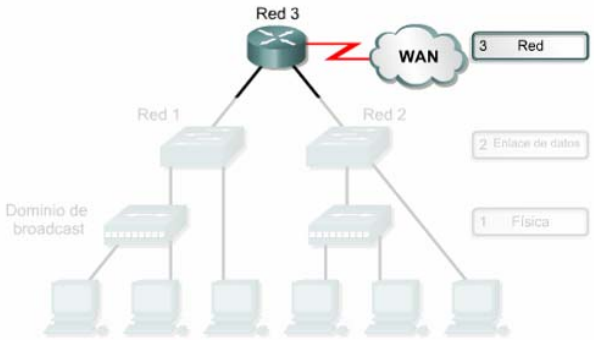
El tamaño de un dominio de colisión se determina por la cantidad de hosts que se conectan físicamente a cualquier puerto en el switch. Esto también afecta la cantidad de ancho de banda de la red que está disponible para cualquier host. En

una situación ideal, hay solamente un host conectado a un puerto de switch LAN. El dominio de colisión consistiría solamente en el host origen y el host destino. El tamaño del dominio de colisión sería de dos. Debido al pequeño tamaño de este dominio de colisión, prácticamente no se producen colisiones cuando alguno de los dos hosts se comunica con el otro.

Diseño de Capa 3

Un router es un dispositivo de Capa 3 que se considera como uno de los dispositivos más poderosos en la topología de red.

Los dispositivos de la Capa 3 se pueden utilizar para crear segmentos LAN únicos. Los dispositivos de Capa 3 permiten la comunicación entre los segmentos basados en las direcciones de Capa 3, como por ejemplo direcciones IP. La implementación de los dispositivos de Capa 3 permite la segmentación de la LAN en redes lógicas y físicas exclusivas. Los routers también permiten la conectividad a las WAN como, por ejemplo, Internet.



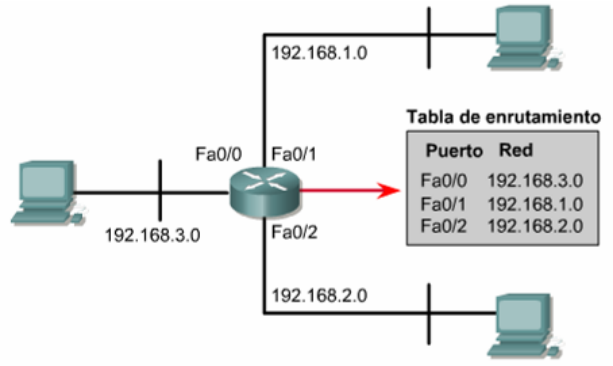
Los routers sirven como firewalls de broadcast.

Implementación del router de Capa 3

El enrutamiento de Capa 3 determina el flujo de tráfico entre los segmentos de red física exclusivos basados en direcciones de Capa 3. Un router envía paquetes de datos basados en direcciones destino. Un router no envía broadcasts basados en LAN, tales como las peticiones ARP. Por lo tanto, la interfaz del router se

considera como el punto de entrada y salida de un dominio de broadcast y evita que los broadcasts lleguen hasta los otros segmentos LAN.

Los routers ofrecen escalabilidad dado que sirven como cortafuegos para los broadcasts y pueden dividir las redes en subredes, basadas en direcciones de Capa 3.



Se utilizan routers para imponer una estructura lógica

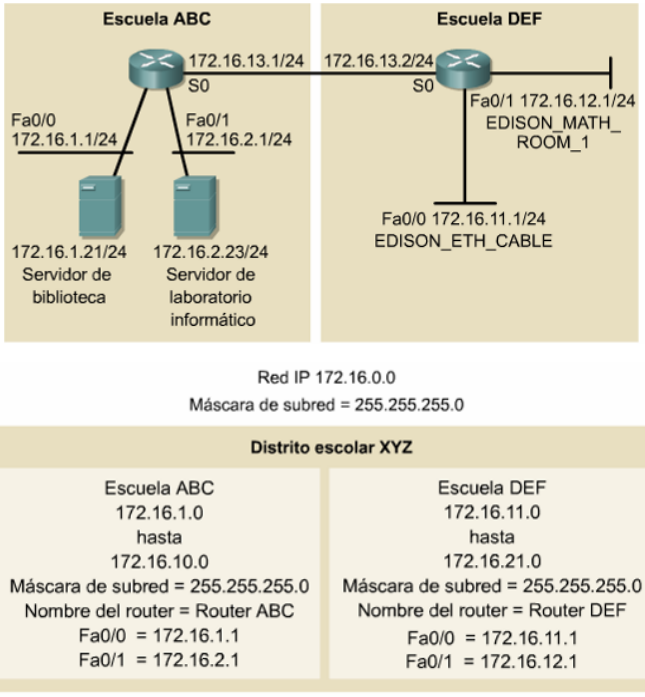
Para decidir si es conveniente utilizar routers o switches, es importante determinar el problema que necesita resolverse. Si el problema está relacionado con el protocolo en lugar de temas de contención, entonces, los routers son una solución apropiada. Los routers solucionan los problemas de broadcasts excesivos, protocolos que no son escalables, temas de seguridad y direccionamiento de la capa de red. Sin embargo, los routers son más caros y más difíciles de configurar que los switches.

Una vez que se desarrolla el esquema de direccionamiento IP para un cliente, éste se debe documentar con precisión. Se debe establecer una convención estándar para el direccionamiento de hosts importantes en la red.

Dirección lógica	Dispositivos de la red física
x.x.x.1-x.x.x.10	Router, puertos de LAN y WAN
x.x.x.11-x.x.x.20	Switches de LAN
x.x.x.21-x.x.x.30	Servidores empresariales
x.x.x.31-x.x.x.80	Servidores de grupo de trabajo
x.x.x.81-x.x.x.254	Hosts

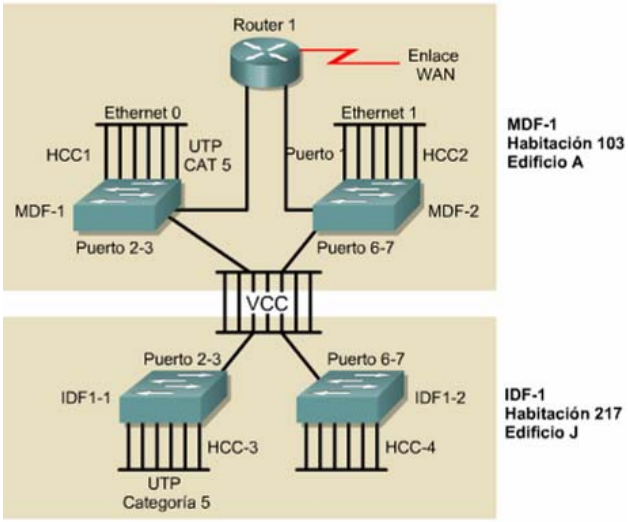
Router de Capa 3 para segmentación

Este esquema de direccionamiento debe ser uniforme en toda la red. Los mapas de direccionamiento ofrecen una instantánea de la red.



Asignaciones de direccionamiento

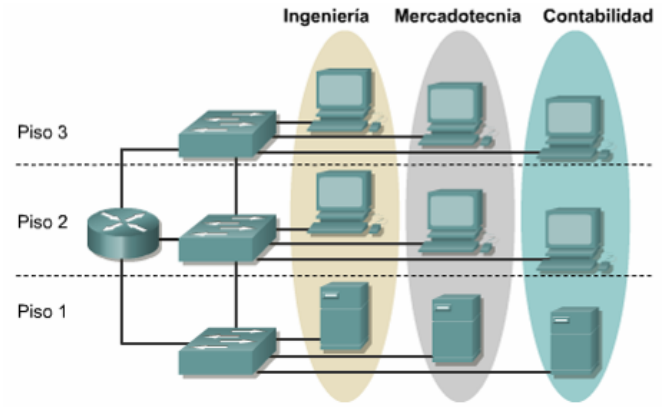
Los mapas físicos de la red ayudan a diagnosticar las fallas de la red.



Asignaciones de red lógica y asignaciones de direccionamiento

La implementación de las VLAN combina la conmutación de Capa 2 y las tecnologías de enrutamiento de Capa 3 para limitar tanto los dominios de

colisión como los dominios de broadcast. Las VLAN también ofrecen seguridad con la creación de grupos VLAN que se comunican con otras VLAN a través de routers.



5.6 DISEÑO DEL SISTEMA DE ALARMAS

Un sistema de alarma está basado en un circuito cerrado de sensores y detectores, conectado a una caja central que recibe cualquier incidencia o señal, y que hará sonar la sirena cuando sea necesario.

Cuenta con un método anti sabotaje que hace saltar la alarma si alguien corta algún cable, o intenta manipular la sirena o caja central.

Para el diseño se realizo los siguientes pasos

1. Análisis de las áreas criticas.
2. Identificación del área a colocar los pulsadores de pánico, que debe ser de fácil acceso para el personal,
3. Identificar el lugar a colocar la sirena de alerta, por lo regular en el exterior del edificio, con la finalidad de sea acuchada por el personal.
4. Identificar el área a colocar el panel de alarma. Esta área debe tener acceso a una toma de alimentación y no debe ser un área pública.
5. Identificados esta áreas se procede a realizar diagramas de conexión de los pulsadores de pánico que en este caso serán tres:
   - Incendios-Fuego.
   - Asalto-Robo.
   - Emergencias

   Siendo esta ultima de tipo silenciosa, para las dos primeras serán audibles, sirenas con el panel de alarma en los planos[4] del edificio
6. Con las especificaciones de Instalación del panel de alarmas se procederá a realizar un diagrama de cableado de asignación de ZONA para los pulsadores de pánico, y para la sirena.
7. Escoger el sistemas de monitoreo más adecuado teniendo en cuenta eficiencia y costos, conjuntamente con equipos que soporten esta tecnología, en este caso el monitoreo se lo realizara a través de internet.

[4] Ver anexo 4

5.7 Propuesta

ITEM	Descripción	Cantidad	V. Unitario	V. Total
1	Rollos de cable UTP CAT 5E de 305MTS	3	109,9	329,70
2	Protectores para conectores RJ-45	52	0,25	13,00
3	Conector RJ-45 macho	52	0,28	14,56
4	Central de monitoreo VisorAlarm + software de monitoreo	2	1153,32	2306,64
5	Módulos de comunicación IP mIP	17	194,5	3306,50
6	Switchs 3com 4400 24-port 10/100Mbps administrable	5	460	2300,00
7	Bridges 3Com® 54 Mbps Wireless LAN Building-to-Building Bridge	11	1176,7	12943,70
8	Router 3com 2950	1	1250	1250,00
9	Servidor IBM SYSTEM x3200	1	1118,88	1118,88
10	PC Intel Core 2 Duo 2,33GHz-E6550	1	1199	1199,00
11	Unidad DSC New Power 10Z Incluye: Caja, bacteria ,transformador	17	140	2380,00
12	Botoneras de emergencia	57	5	285,00
13	Sirena 30w blindada incluye: caja, tamper	17	40	680,00
14	Canaletas 13x7 de 2 metros	114	2	228,00
15	Torre de 9 metros STZ-35, Tramo de remate SCZ-35 G, base de torre, Base y bridas para torre SBZ-35 G	1	494	494,00
16	Torre de 6 metros STZ-35, Tramo de remate SCZ-35 G, base de torre, Base y bridas para torre SBZ-35 G	5	375	1875,00
17	Torre de 3 metros STZ-35, Tramo de remate SCZ-35 G, base de torre, Base y bridas para torre SBZ-35 G	5	256	1280,00
18	Antema omnidireccional de 12 dBi	1	209,3	209,30
			SUB-TOTAL	28354,98
			IVA	3402,60
			TOTAL	31757,58

CAPITULO VI

6.1 CONCLUSIONES

De acuerdo con los objetivos planteados se llegaron a las siguientes conclusiones

- La utilización de de la tecnología IP en monitoreo de Alarmas nos permite mantener una supervisión de las alarmas en tiempo real.
- El Protocolo TCP/IP garantiza la universalidad de uso de cualquier panel de alarmas a las conexiones físicas a la entrada de la interfaz del comunicador IP.
- Las transmisión de señales por línea telefónica tenía la mejor relación costo/ rendimiento, con tecnología IP la relación costo / rendimiento es infinitamente mejor**.**
- El "pishing" del bus de comunicaciones entre el panel y el teclado es una técnica que nos permite procesar datos en forma nativa, es muy veloz y simple que permite la configuración de las alarmas en forma remota vía internet.
- La implementación de un sistema de TCP/IP en una central de monitoreo de alarmas proporciona mayor seguridad para el cliente, seguridad en la comunicación.
- Para el mantenimiento del sistema de monitoreo de las alarmas se requieren conocimiento de RED mínimos.
- Una Red TCP/IP es sistema de Transmisión de datos flexible, adaptable y escalable a tecnologías de hoy.

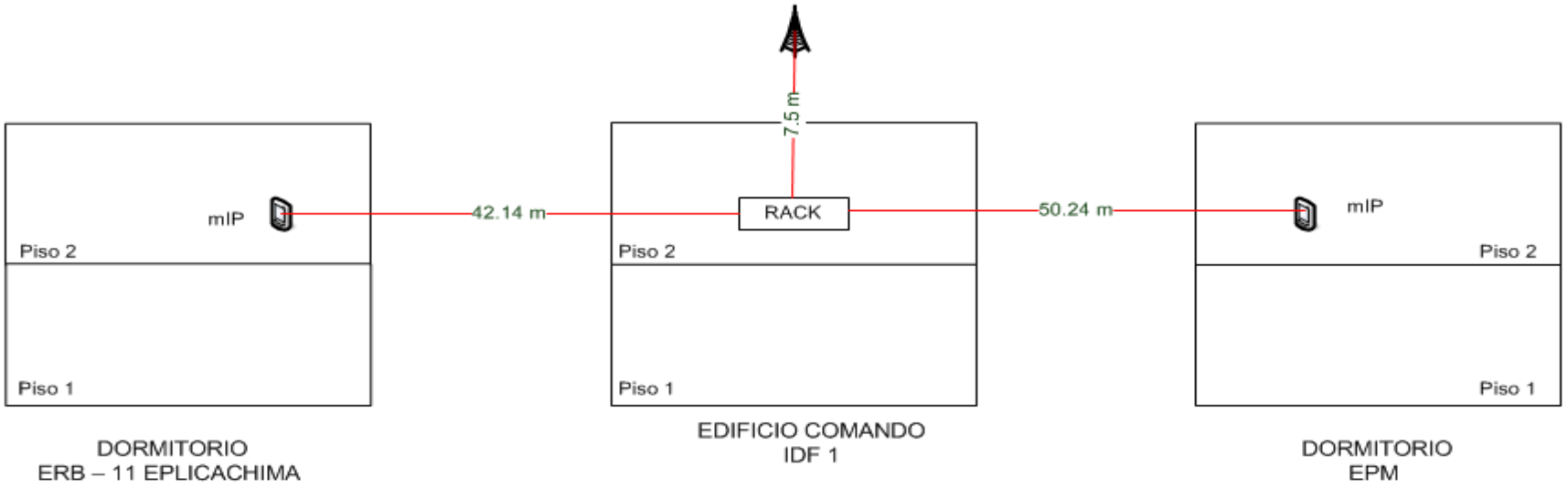
6.2 RECOMENDACIONES

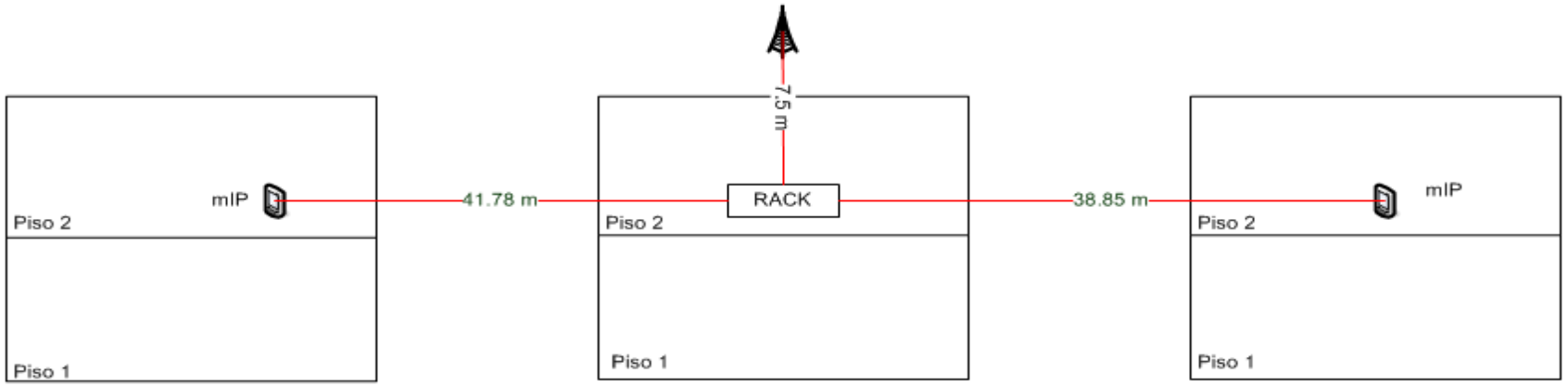
- ✍ Estudiar y planificar el diseño de un nuevo sistemas de alarmas al evolucionar a una nueva tecnología de monitoreo de Alarmas.
- ✍ Capacitar al personal que va ha estar encargado del monitoreo en los siguientes temas fundamentales: Administración y mantenimiento de redes y sistemas de alarmas.
- ✍ Utilizar paneles de alarmas que permitan protocolos como CONTACT-ID o similares.
- ✍ La programación de los paneles de alarmas se lo realizará de acuerdo a la hoja de programación y especificaciones técnicas.

ANEXOS

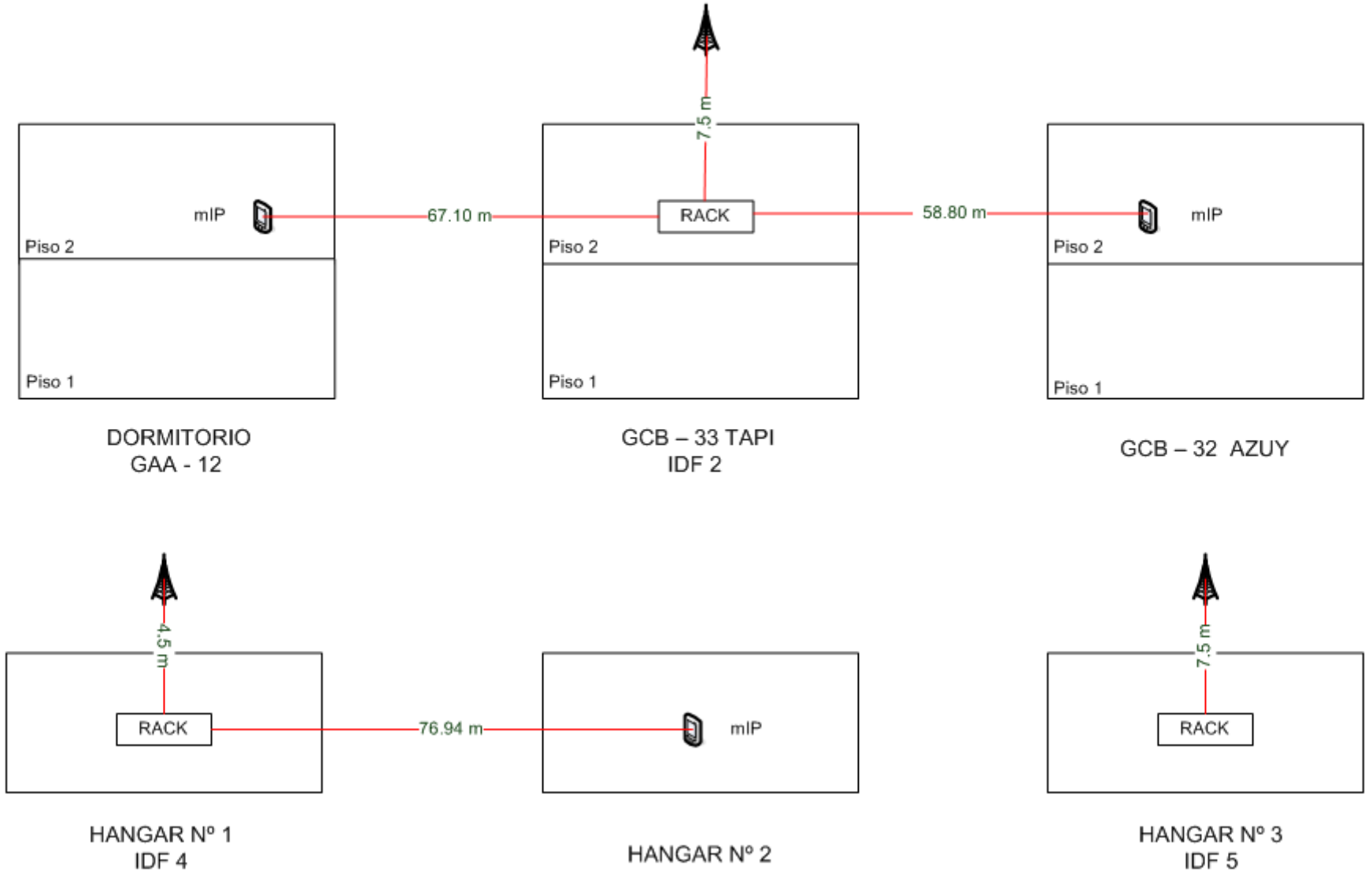
ANEXO 1

DIAGRA UNIFILAR DE RED

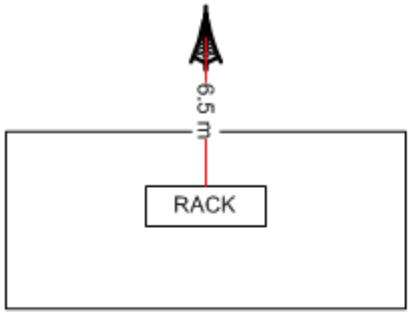




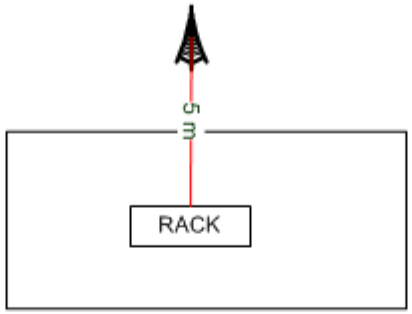
DIAGRA UNIFILAR DE RED



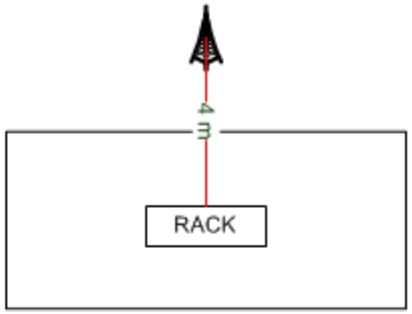
DIAGRA UNIFILAR DE RED



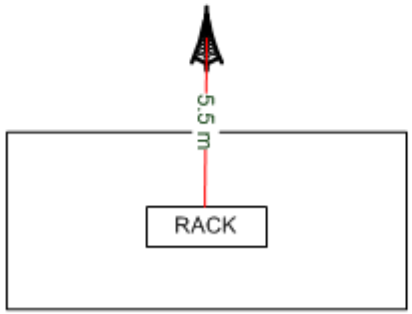
COMISARIATO
IDF 6



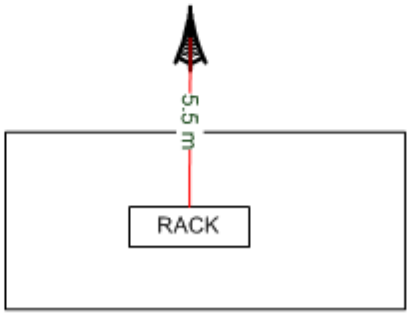
COCINAS
IDF 7



GARITA NORTE
IDF 8

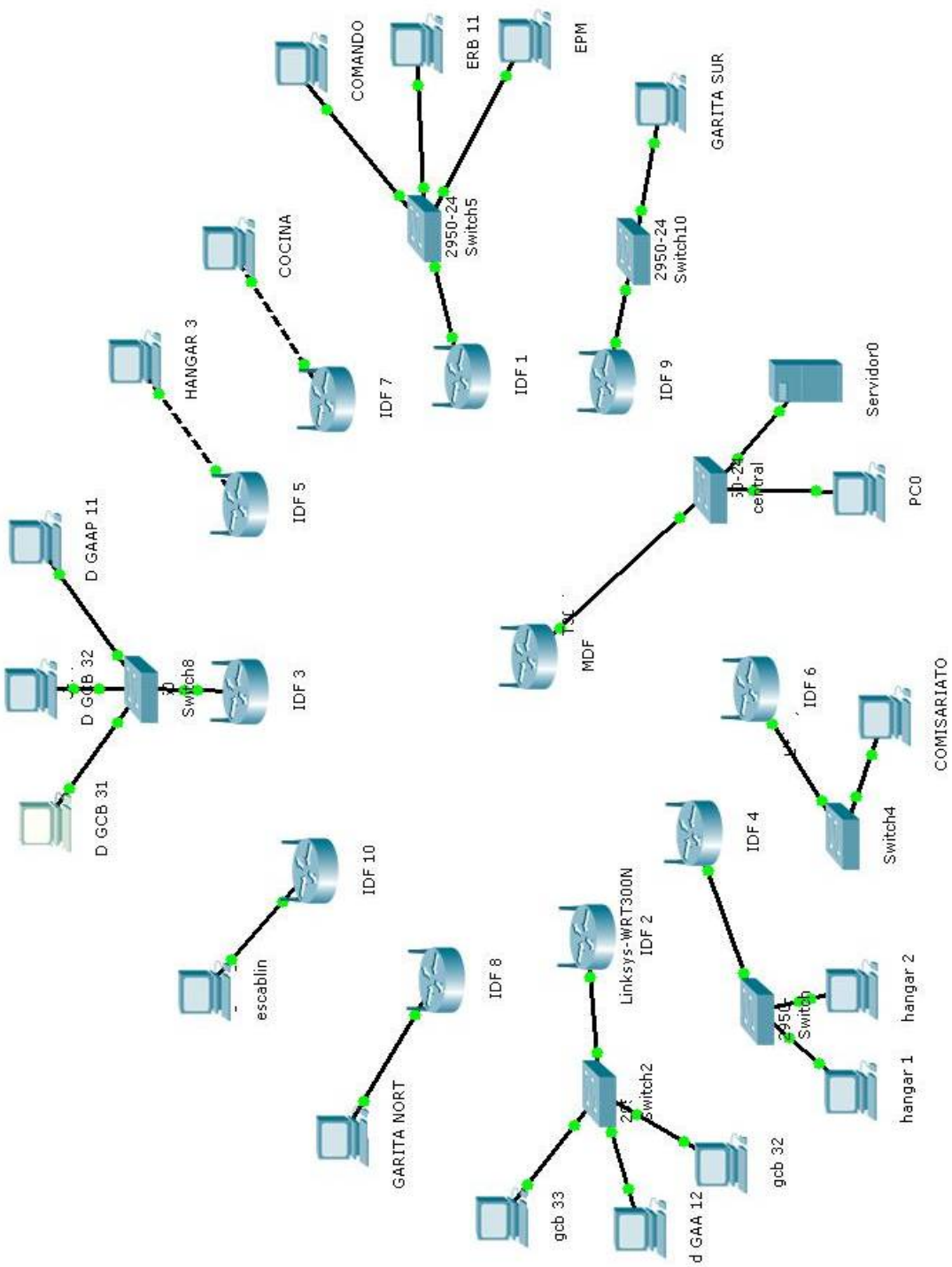


GARITA SUR
IDF 9



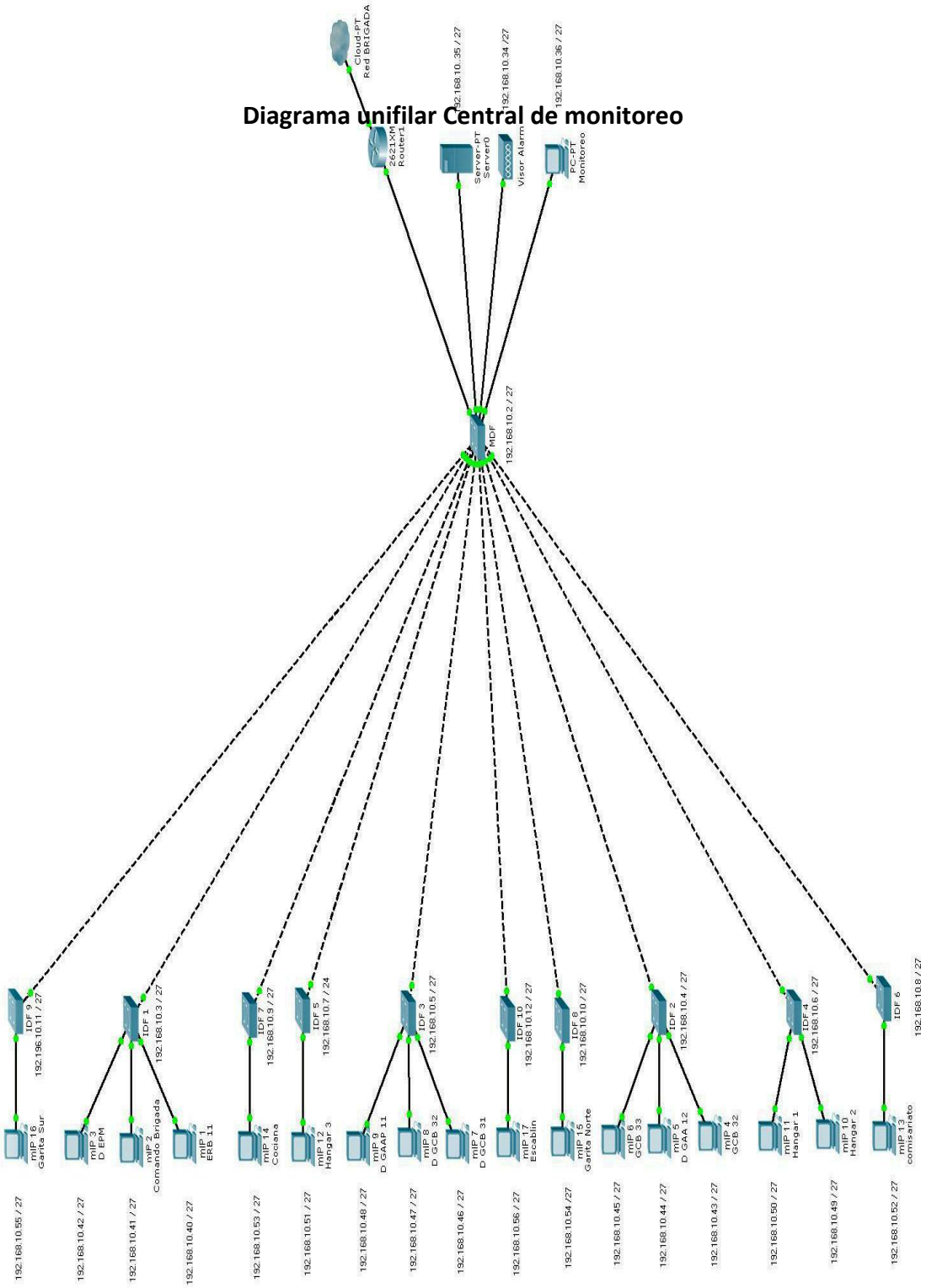
ESCABLIN
IDF 10

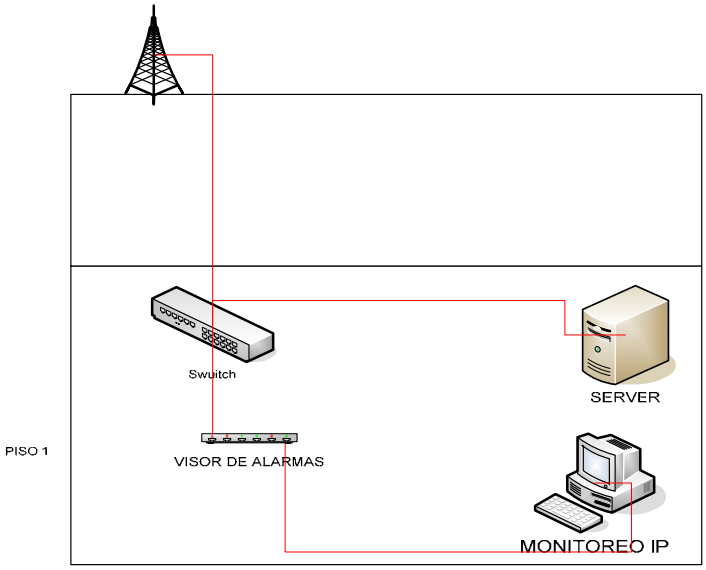
TOPOLOGÍA FÍSICA DE RED



TOPOLOGÍA LÓGICA DE RED

Diagrama unifilar Central de monitoreo





CALCULO DE DISTANCIA DE LOS ENLACES

DE RADIO FRECUENCIA (RF)

CENTAL - IDF 1	
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 1	2,793
Longuitud B	78,6481
Latitud B	1,656

$$D = \sqrt{(\Delta Long * 111.32)^2 + (\Delta Lat * 111.32)^2 + (\Delta h)^2}$$

D2=	0,11675406
D=	**0,34169293** Km

CENTRAL - IDF 2

Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 2	2,81
Longuitud B	78,6488
Latitud B	1,6474

$$D=\sqrt{(\Delta Long*111.32)^2+(\Delta Lat*111.32)^2+(\Delta h)^2}$$

D2= 0,403761

D= 0,63542191 Km

CENTRAL - IDF 3

Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 3	2,805
Longuitud B	78,6486
Latitud B	1,654

$$D=\sqrt{(\Delta Long*111.32)^2+(\Delta Lat*111.32)^2+(\Delta h)^2}$$

D2= 0,01313567

D= 0,11461095 Km

CENTRAL - IDF 4

Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 4	2,805
Longuitud A	78,6506
Latitud A	1,6509

$$D=\sqrt{(\Delta Long*111.32)^2+(\Delta Lat*111.32)^2+(\Delta h)^2}$$

D2= 0,08786029

D= 0,29641236 Km

	CENTRAL - IDF 5
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 5	2,793
Longuitud B	78,6484
Latitud B	1,6557

$$D = \sqrt{(\Delta Long * 111.32)^2 + (\Delta Lat * 111.32)^2 + (\Delta h)^2}$$

D2= 0,08998703
D= 0,300 Km

	CENTRAL - IDF 6
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 6	2,795
Longuitud B	78,6509
Latitud B	1,6529

$$D = \sqrt{(\Delta Long * 111.32)^2 + (\Delta Lat * 111.32)^2 + (\Delta h)^2}$$

D2= 0,04074623
D= 0,20185695 Km

	CENTRAL - IDF 7
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 7	2,7995
Longuitud B	78,6509
Latitud B	1,6529

$$D = \sqrt{(\Delta Long * 111.32)^2 + (\Delta Lat * 111.32)^2 + (\Delta h)^2}$$

D2= 0,04067648
D= 0,2016841 Km

CENTRAL - IDF 8	
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 8	2,82
Longuitud B	78,6488
Latitud B	1,6474

$$D=\sqrt{(\Delta Long*111.32)^2+(\Delta Lat*111.32)^2+(\Delta h)^2}$$

D2= 0,403961
D= 0,63557926 Km

CENTRAL - IDF 9	
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 9	2,799
Longuitud B	78,6476
Latitud B	1,6593

$$D=\sqrt{(\Delta Long*111.32)^2+(\Delta Lat*111.32)^2+(\Delta h)^2}$$

D2= 0,50427227
D= 0,71012131 Km

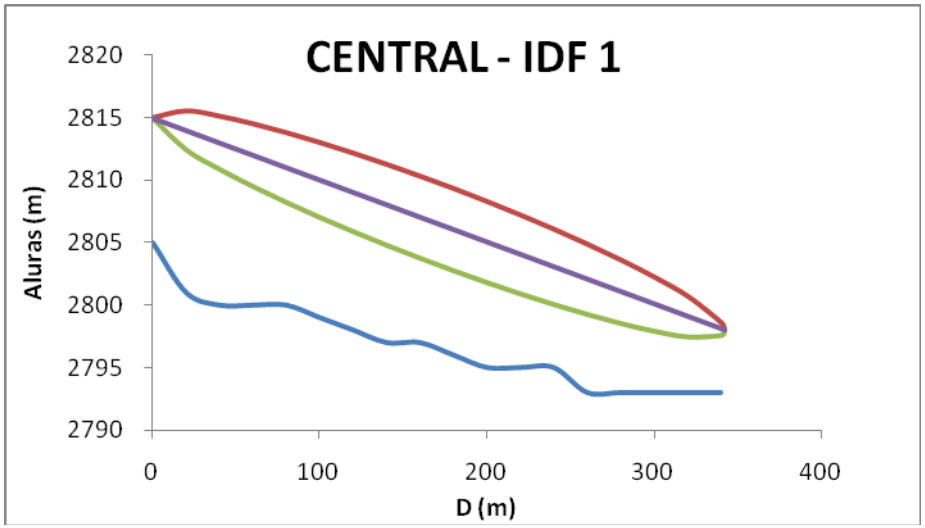
CENTRAL - IDF 10	
Central	2,805
Longuitud A	78,6491
Latitud A	1,6531
IDF 10	2,817
Longuitud B	78,649
Latitud B	1,6513

$$D=\sqrt{(\Delta Long*111.32)^2+(\Delta Lat*111.32)^2+(\Delta h)^2}$$

D2= 0,04041846
D= 0,20104344 Km

PRIMERA ZONA DE FRESNEL

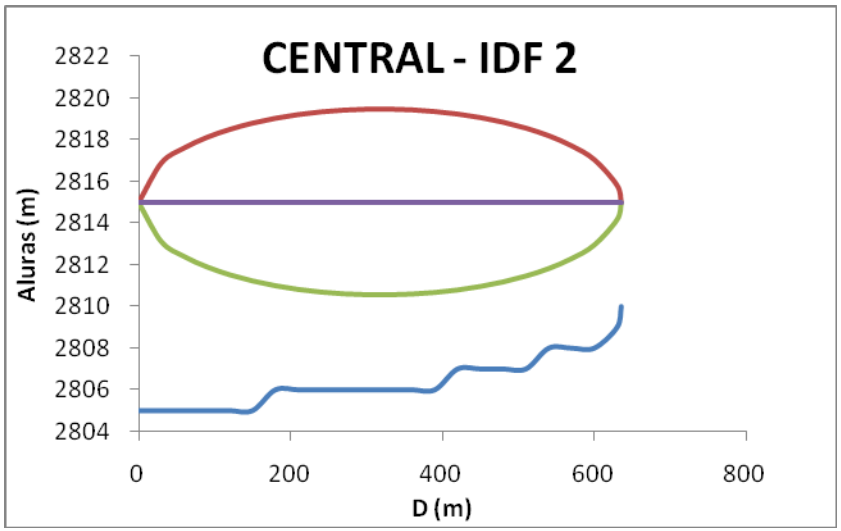
	ENLACE:		
DATOS DEL ENLACE	**Central - IDF 1**		
Estación	**A:**	**CENTRAL**	
	Longitud:	**78 38 56,8**	**W**
	Latitud:	**1 39 11,2**	**S**
	Altura:	**2805,00**	**m.**
	Torre:	**10,00**	**m.**
Estación	**B:**	**IDF 1**	
	Longitud:	**78 38 53,3**	**W**
	Latitud:	**1 39 25,1**	**S**
	Altura:	**2793,00**	**m.**
	Torre:	**5,00**	**m.**
DISTANCIA DEL ENLACE:		**341, 692**	**m.**
FRECUENCIA:		**2400**	**MHz.**
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	**m.**



DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	341,69	0,0	2805,00	2815,00	0,00	2815,00	2815,00
20	2801	321,69	0,4	2801,38	2814,00	1,53	2815,54	2812,47
40	2800	301,69	0,7	2800,71	2813,01	2,10	2815,11	2810,91
60	2800	281,69	1,0	2800,99	2812,01	2,49	2814,50	2809,53
80	2800	261,69	1,2	2801,23	2811,02	2,77	2813,79	2808,25
100	2799	241,69	1,4	2800,42	2810,02	2,97	2813,00	2807,05
120	2798	221,69	1,6	2799,56	2809,03	3,12	2812,15	2805,91
140	2797	201,69	1,7	2798,66	2808,03	3,21	2811,25	2804,82
160	2797	181,69	1,7	2798,71	2807,04	3,26	2810,30	2803,78
180	2796	161,69	1,7	2797,71	2806,04	3,26	2809,31	2802,78
200	2795	141,69	1,7	2796,67	2805,05	3,22	2808,27	2801,83
220	2795	121,69	1,6	2796,57	2804,05	3,13	2807,18	2800,92
240	2795	101,69	1,4	2796,44	2803,06	2,99	2806,05	2800,07
260	2793	81,69	1,2	2794,25	2802,06	2,79	2804,85	2799,28
280	2793	61,69	1,0	2794,02	2801,07	2,51	2803,58	2798,56
300	2793	41,69	0,7	2793,74	2800,07	2,14	2802,21	2797,94
320	2793	21,69	0,4	2793,41	2799,08	1,59	2800,67	2797,49
340	2793	1,69	0,0	2793,03	2798,08	0,46	2798,54	2797,63
341,69	2793	0	0,0	2793,00	2798,00	0,00	2798,00	2798,00

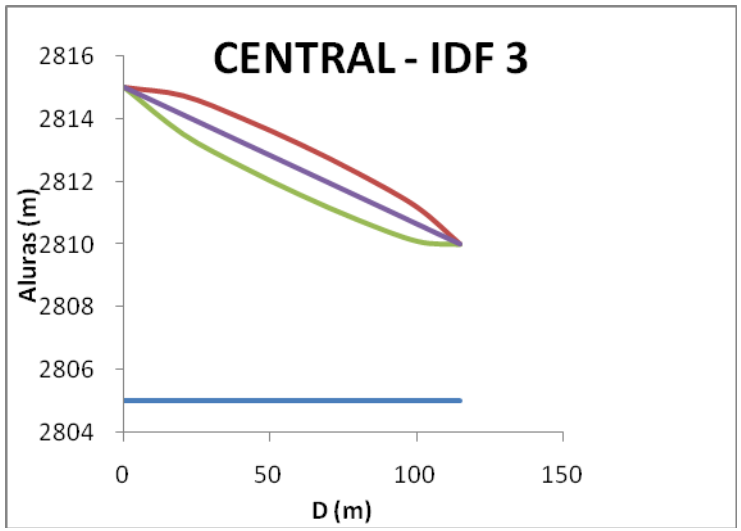
DATOS DEL ENLACE **ENLACE: Central - IDF 2**

Estación	**A:**	**CENTRAL**	
	Longitud:	**78 38 56,8**	**W**
	Latitud:	**1 39 11,2**	**S**
	Altura:	**2805,00**	**m.**
	Torre:	**10,00**	**m.**
Estación	**B:**	**IDF 1**	
	Longitud:	**78 39 4,1**	**W**
	Latitud:	**1 38 55,2**	**S**
	Altura:	**2810,00**	**m.**
	Torre:	**5,00**	**m.**
DISTANCIA DEL ENLACE:		**635,42**	**m.**
FRECUENCIA:		**2400**	**MHz.**
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	**m.**



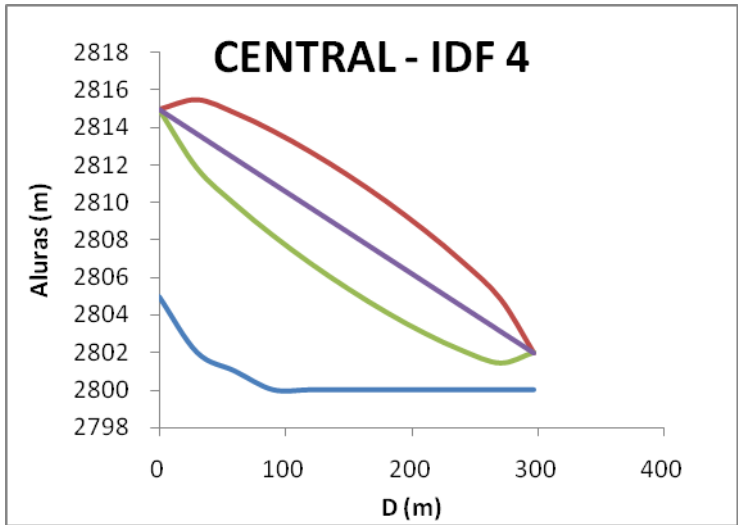
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	635,42	0,0	2805,00	2815,00	0,00	2815,00	2815,00
30	2805	605,42	1,1	2806,07	2815,00	1,89	2816,89	2813,11
60	2805	575,42	2,0	2807,03	2815,00	2,61	2817,61	2812,39
90	2805	545,42	2,9	2807,89	2815,00	3,11	2818,11	2811,89
120	2805	515,42	3,6	2808,64	2815,00	3,49	2818,49	2811,51
150	2805	485,42	4,3	2809,28	2815,00	3,78	2818,78	2811,22
180	2806	455,42	4,8	2810,82	2815,00	4,02	2819,02	2810,98
210	2806	425,42	5,3	2811,26	2815,00	4,19	2819,19	2810,81
240	2806	395,42	5,6	2811,58	2815,00	4,32	2819,32	2810,68
270	2806	365,42	5,8	2811,80	2815,00	4,41	2819,41	2810,59
300	2806	335,42	5,9	2811,92	2815,00	4,45	2819,45	2810,55
330	2806	305,42	5,9	2811,93	2815,00	4,45	2819,45	2810,55
360	2806	275,42	5,8	2811,83	2815,00	4,42	2819,42	2810,58
390	2806	245,42	5,6	2811,63	2815,00	4,34	2819,34	2810,66
420	2807	215,42	5,3	2812,32	2815,00	4,22	2819,22	2810,78
450	2807	185,42	4,9	2811,91	2815,00	4,05	2819,05	2810,95
480	2807	155,42	4,4	2811,39	2815,00	3,83	2818,83	2811,17
510	2807	125,42	3,8	2810,76	2815,00	3,55	2818,55	2811,45
540	2808	95,42	3,0	2811,03	2815,00	3,18	2818,18	2811,82
570	2808	65,42	2,2	2810,19	2815,00	2,71	2817,71	2812,29
600	2808	35,42	1,3	2809,25	2815,00	2,04	2817,04	2812,96
630	2809	5,42	0,2	2809,20	2815,00	0,82	2815,82	2814,18
635,42	2810	0	0,0	2810,00	2815,00	0,00	2815,00	2815,00

		ENLACE :		
DATOS DEL ENLACE		**Central - IDF 3**		
Estación	**A:**	**CENTRAL**		
	Longitud:	78 38 56,8	**W**	
	Latitud:	1 39 11,2	**S**	
	Altura:	2805,00	**m.**	
	Torre:	10,00	**m.**	
Estación	**B:**	**IDF 3**		
	Longitud:	78 38 55,3	**W**	
	Latitud:	1 39 15,3	**S**	
	Altura:	2805,00	**m.**	
	Torre:	5,00	**m.**	
DISTANCIA DEL ENLACE:		**114,61**	**m.**	
FRECUENCIA:		**2400**	**MHz.**	
FACTOR K		**1,33**		
ALTURA DE MALEZA		**0**	**m.**	



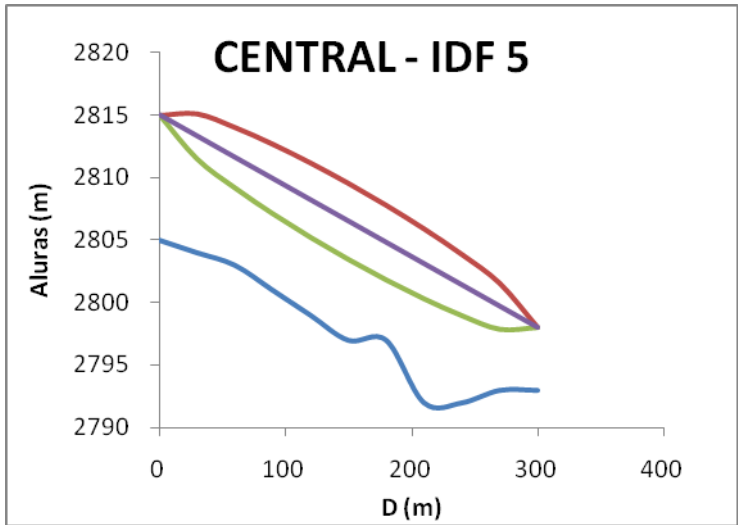
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	114,61	0,0	2805,00	2815,00	0,00	2815,00	2815,00
20	2805	94,61	0,1	2805,11	2814,13	0,61	2814,74	2813,52
40	2805	74,61	0,2	2805,18	2813,25	0,77	2814,02	2812,49
60	2805	54,61	0,2	2805,19	2812,38	0,80	2813,19	2811,58
80	2805	34,61	0,2	2805,16	2811,51	0,74	2812,25	2810,77
100	2805	14,61	0,1	2805,09	2810,64	0,54	2811,17	2810,10
114,61	2805	0	0,0	2805,00	2810,00	0,00	2810,00	2810,00

		ENLACE:		
DATOS DEL ENLACE		**Central - IDF 4**		
Estación	**A:**	**CENTRAL**		
	Longitud:	78 38 56,8	**W**	
	Latitud:	1 39 11,2	**S**	
	Altura:	2805,00	**m.**	
	Torre:	10,00	**m.**	
Estación	**B:**	**IDF 4**		
	Longitud:	78 39 2,2	**W**	
	Latitud:	1 39 34	**S**	
	Altura:	2800,00	**m.**	
	Torre:	2,00	**m.**	
DISTANCIA DEL ENLACE:		296,41	**m.**	
FRECUENCIA:		**2400**	**MHz.**	
FACTOR K		**1,33**		
ALTURA DE MALEZA		**0**	**m.**	



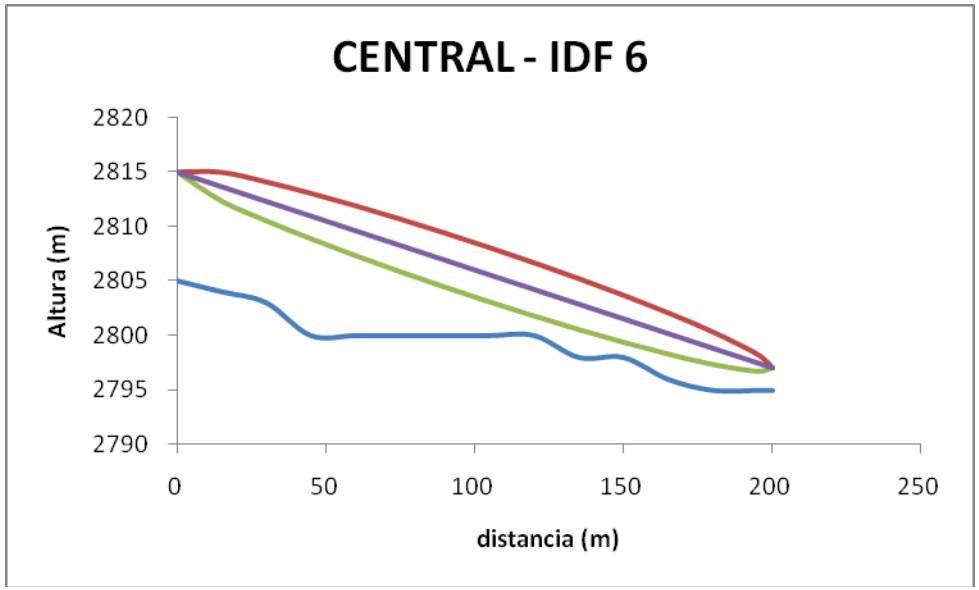
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	296,41	0,0	2805,00	2815,00	0,00	2815,00	2815,00
30	2802	266,41	0,5	2802,47	2813,68	1,84	2815,52	2811,85
60	2801	236,41	0,8	2801,83	2812,37	2,45	2814,81	2809,92
90	2800	206,41	1,1	2801,09	2811,05	2,80	2813,85	2808,25
120	2800	176,41	1,2	2801,25	2809,74	2,99	2812,72	2806,75
150	2800	146,41	1,3	2801,29	2808,42	3,04	2811,46	2805,38
180	2800	116,41	1,2	2801,23	2807,11	2,97	2810,08	2804,13
210	2800	86,41	1,1	2801,07	2805,79	2,77	2808,56	2803,02
240	2800	56,41	0,8	2800,80	2804,47	2,39	2806,86	2802,08
270	2800	26,41	0,4	2800,42	2803,16	1,73	2804,89	2801,42
296,41	2800	0	0,0	2800,00	2802,00	0,00	2802,00	2802,00

		ENLACE:		
DATOS DEL ENLACE		**Central - IDF 5**		
Estación	**A:**	**CENTRAL**		
	Longitud:	78 38 56,8	**W**	
	Latitud:	1 39 11,2	**S**	
	Altura:	2805,00	**m.**	
	Torre:	10,00	**m.**	
Estación	**B:**	**IDF 5**		
	Longitud:	78 38 54,3	**W**	
	Latitud:	1 39 20,6	**S**	
	Altura:	2793,00	**m.**	
	Torre:	5,00	**m.**	
DISTANCIA DEL ENLACE:		300	**m.**	
FRECUENCIA:		**2400**	**MHz.**	
FACTOR K		**1,33**		
ALTURA DE MALEZA		**0**	**m.**	



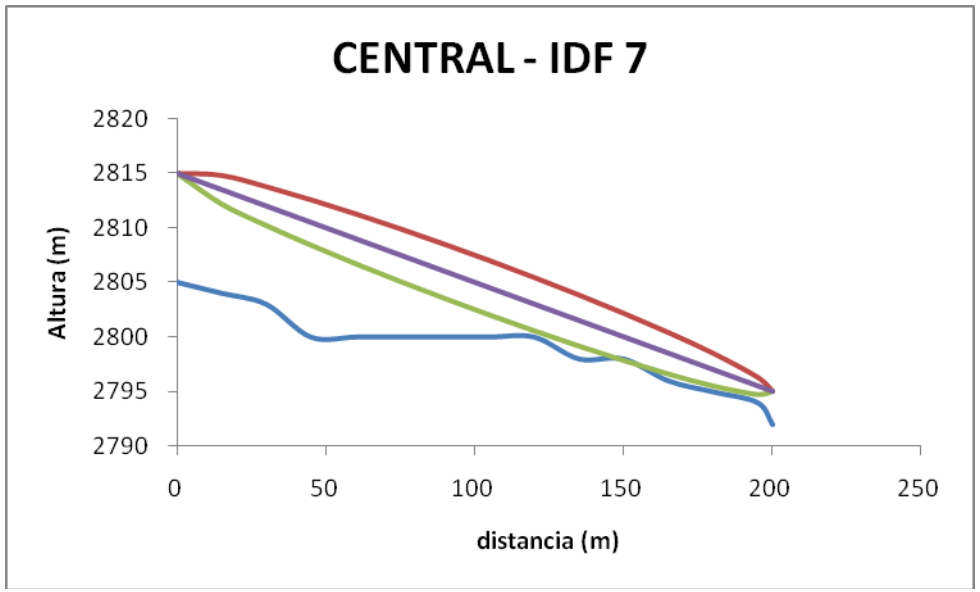
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	300	0,0	2805,00	2815,00	0,00	2815,00	2815,00
30	2804	270	0,5	2804,48	2813,30	1,84	2815,14	2811,46
60	2803	240	0,8	2803,85	2811,60	2,45	2814,05	2809,15
90	2801	210	1,1	2802,11	2809,90	2,81	2812,71	2807,09
120	2799	180	1,3	2800,27	2808,20	3,00	2811,20	2805,20
150	2797	150	1,3	2798,32	2806,50	3,06	2809,56	2803,44
180	2797	120	1,3	2798,27	2804,80	3,00	2807,80	2801,80
210	2792	90	1,1	2793,11	2803,10	2,81	2805,91	2800,29
240	2792	60	0,8	2792,85	2801,40	2,45	2803,85	2798,95
270	2793	30	0,5	2793,48	2799,70	1,84	2801,54	2797,86
300	2793	0	0,0	2793,00	2798,00	0,00	2798,00	2798,00

DATOS DEL ENLACE	ENLACE: Central - IDF 6		
Estación	A:	CENTRAL	
	Longitud:	78 38 56,8	W
	Latitud:	1 39 11,2	S
	Altura:	2805,00	m.
	Torre:	10,00	m.
Estación	B:	IDF 6	
	Longitud:	78 39 3,3	W
	Latitud:	1 39 10,6	S
	Altura:	2795,00	m.
	Torre:	2,00	m.
DISTANCIA DEL ENLACE:		200	m.
FRECUENCIA:		**2400**	MHz.
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	m.



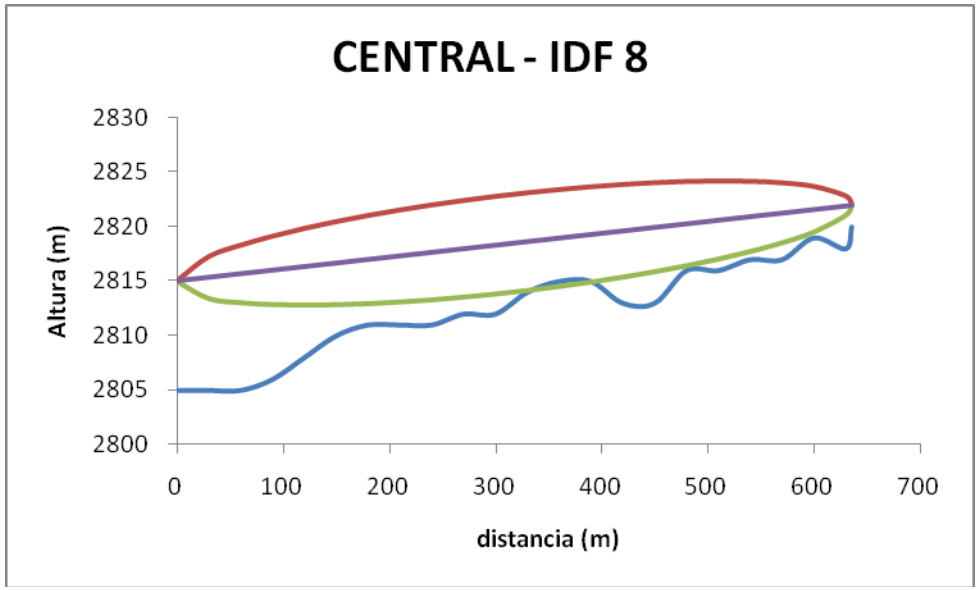
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	200	0,0	2805,00	2815,00	0,00	2815,00	2815,00
15	2804	185	0,2	2804,16	2813,65	1,32	2814,97	2812,33
30	2803	170	0,3	2803,30	2812,30	1,79	2814,09	2810,51
45	2800	155	0,4	2800,41	2810,95	2,09	2813,04	2808,86
60	2800	140	0,5	2800,49	2809,60	2,29	2811,89	2807,31
75	2800	125	0,6	2800,55	2808,25	2,42	2810,67	2805,83
90	2800	110	0,6	2800,58	2806,90	2,49	2809,39	2804,41
105	2800	95	0,6	2800,59	2805,55	2,50	2808,05	2803,05
120	2800	80	0,6	2800,56	2804,20	2,45	2806,65	2801,75
135	2798	65	0,5	2798,52	2802,85	2,34	2805,19	2800,51
150	2798	50	0,4	2798,44	2801,50	2,17	2803,67	2799,33
165	2796	35	0,3	2796,34	2800,15	1,90	2802,05	2798,25
180	2795	20	0,2	2795,21	2798,80	1,50	2800,30	2797,30
195	2795	5	0,1	2795,06	2797,45	0,78	2798,23	2796,67
200	2795	0	0,0	2795,00	2797,00	0,00	2797,00	2797,00

DATOS DEL ENLACE	ENLACE: Central - IDF 7		
Estación	A:	CENTRAL	
	Longitud:	78 38 56,8	W
	Latitud:	1 39 11,2	S
	Altura:	2805,00	m.
	Torre:	10,00	m.
Estación	B:	IDF 7	
	Longitud:	78 38 58,7	W
	Latitud:	1 39 21,2	S
	Altura:	2792,00	m.
	Torre:	3,00	m.
DISTANCIA DEL ENLACE:		200	m.
FRECUENCIA:		**2400**	MHz.
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	m.



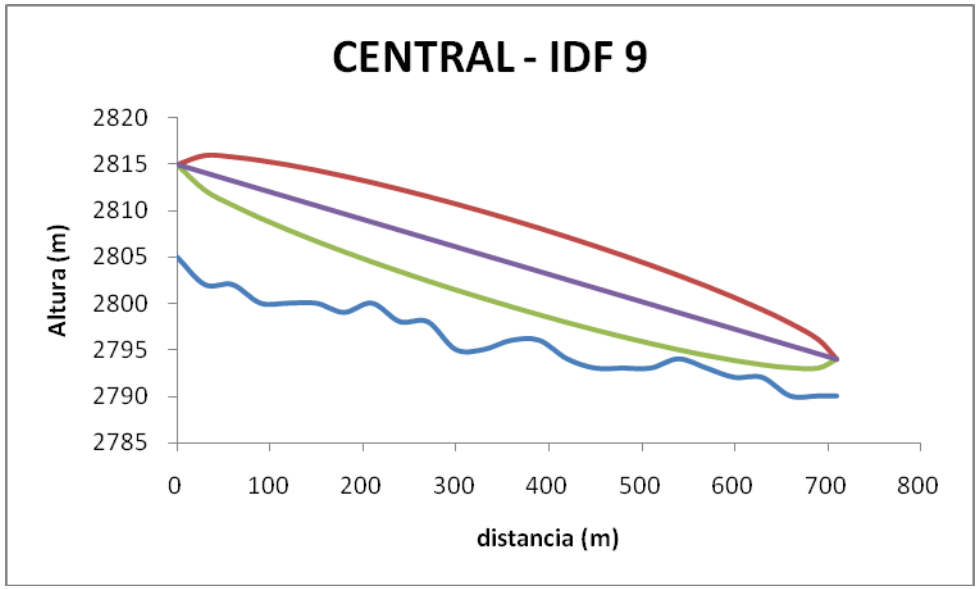
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	200	0,0	2805,00	2815,00	0,00	2815,00	2815,00
15	2804	185	0,2	2804,16	2813,50	1,32	2814,82	2812,18
30	2803	170	0,3	2803,30	2812,00	1,79	2813,79	2810,21
45	2800	155	0,4	2800,41	2810,50	2,09	2812,59	2808,41
60	2800	140	0,5	2800,49	2809,00	2,29	2811,29	2806,71
75	2800	125	0,6	2800,55	2807,50	2,42	2809,92	2805,08
90	2800	110	0,6	2800,58	2806,00	2,49	2808,49	2803,51
105	2800	95	0,6	2800,59	2804,50	2,50	2807,00	2802,00
120	2800	80	0,6	2800,56	2803,00	2,45	2805,45	2800,55
135	2798	65	0,5	2798,52	2801,50	2,34	2803,84	2799,16
150	2798	50	0,4	2798,44	2800,00	2,17	2802,17	2797,83
165	2796	35	0,3	2796,34	2798,50	1,90	2800,40	2796,60
180	2795	20	0,2	2795,21	2797,00	1,50	2798,50	2795,50
195	2794	5	0,1	2794,06	2795,50	0,78	2796,28	2794,72
200	2792	0	0,0	2792,00	2795,00	0,00	2795,00	2795,00

DATOS DEL ENLACE	ENLACE: Central - IDF 8		
Estación	A:	CENTRAL	
	Longitud:	78 38 56,8	W
	Latitud:	1 39 11,2	S
	Altura:	2805,00	m.
	Torre:	10,00	m.
Estación	B:	IDF 8	
	Longitud:	78 38 56	W
	Latitud:	1 38 50,7	S
	Altura:	2820,00	m.
	Torre:	2,00	m.
DISTANCIA DEL ENLACE:		635,57	m.
FRECUENCIA:		**2400**	MHz.
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	m.



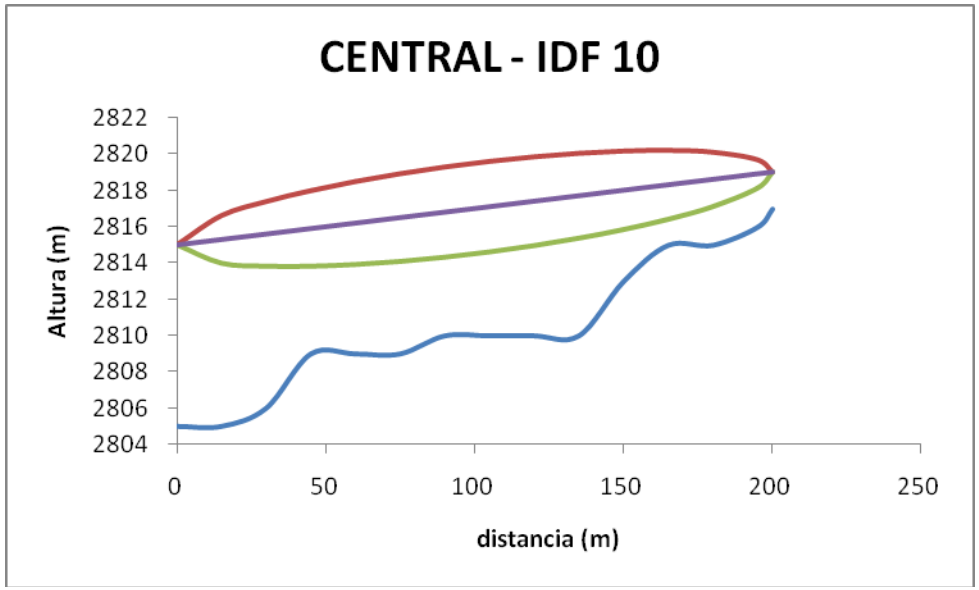
DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	635,57	0,0	2805,00	2815,00	0,00	2815,00	2815,00
30	2805	605,57	1,1	2806,07	2815,33	1,89	2817,22	2813,44
60	2805	575,57	2,0	2807,03	2815,66	2,61	2818,27	2813,05
90	2806	545,57	2,9	2808,89	2815,99	3,11	2819,10	2812,88
120	2808	515,57	3,6	2811,64	2816,32	3,49	2819,81	2812,83
150	2810	485,57	4,3	2814,28	2816,65	3,78	2820,44	2812,87
180	2811	455,57	4,8	2815,82	2816,98	4,02	2821,00	2812,97
210	2811	425,57	5,3	2816,26	2817,31	4,19	2821,51	2813,12
240	2811	395,57	5,6	2816,58	2817,64	4,32	2821,96	2813,32
270	2812	365,57	5,8	2817,81	2817,97	4,41	2822,38	2813,57
300	2812	335,57	5,9	2817,92	2818,30	4,45	2822,75	2813,85
330	2814	305,57	5,9	2819,93	2818,63	4,45	2823,09	2814,18
360	2815	275,57	5,8	2820,84	2818,96	4,42	2823,38	2814,55
390	2815	245,57	5,6	2820,63	2819,30	4,34	2823,64	2814,96
420	2813	215,57	5,3	2818,33	2819,63	4,22	2823,85	2815,41
450	2813	185,57	4,9	2817,91	2819,96	4,05	2824,01	2815,90
480	2816	155,57	4,4	2820,39	2820,29	3,83	2824,12	2816,45
510	2816	125,57	3,8	2819,77	2820,62	3,55	2824,17	2817,07
540	2817	95,57	3,0	2820,04	2820,95	3,19	2824,13	2817,76
570	2817	65,57	2,2	2819,20	2821,28	2,71	2823,99	2818,57
600	2819	35,57	1,3	2820,26	2821,61	2,05	2823,66	2819,56
630	2818	5,57	0,2	2818,21	2821,94	0,83	2822,77	2821,11
635,57	2820	0	0,0	2820,00	2822,00	0,00	2822,00	2822,00

DATOS DEL ENLACE	ENLACE: Central - IDF 9		
Estación	A:	CENTRAL	
	Longitud:	78 38 56,8	W
	Latitud:	1 39 11,2	S
	Altura:	2805,00	m.
	Torre:	10,00	m.
Estación	B:	IDF 9	
	Longitud:	78 38 51,5	W
	Latitud:	1 39 33,6	S
	Altura:	2790,00	m.
	Torre:	4,00	m.
DISTANCIA DEL ENLACE:		710,12	m.
FRECUENCIA:		**2400**	MHz.
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	m.



DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	710,12	0,0	2805,00	2815,00	0,00	2815,00	2815,00
30	2802	680,12	1,2	2803,20	2814,11	1,90	2816,01	2812,22
60	2802	650,12	2,3	2804,29	2813,23	2,62	2815,85	2810,61
90	2800	620,12	3,3	2803,28	2812,34	3,13	2815,47	2809,20
120	2800	590,12	4,2	2804,17	2811,45	3,53	2814,98	2807,92
150	2800	560,12	4,9	2804,94	2810,56	3,85	2814,41	2806,72
180	2799	530,12	5,6	2804,61	2809,68	4,10	2813,78	2805,58
210	2800	500,12	6,2	2806,18	2808,79	4,30	2813,09	2804,49
240	2798	470,12	6,6	2804,64	2807,90	4,46	2812,36	2803,45
270	2798	440,12	7,0	2804,99	2807,02	4,57	2811,59	2802,44
300	2795	410,12	7,2	2802,24	2806,13	4,65	2810,78	2801,47
330	2795	380,12	7,4	2802,38	2805,24	4,70	2809,94	2800,54
360	2796	350,12	7,4	2803,41	2804,35	4,71	2809,06	2799,64
390	2796	320,12	7,3	2803,34	2803,47	4,69	2808,15	2798,78
420	2794	290,12	7,2	2801,17	2802,58	4,63	2807,21	2797,95
450	2793	260,12	6,9	2799,89	2801,69	4,54	2806,23	2797,15
480	2793	230,12	6,5	2799,50	2800,81	4,41	2805,21	2796,40
510	2793	200,12	6,0	2799,00	2799,92	4,24	2804,16	2795,68
540	2794	170,12	5,4	2799,40	2799,03	4,02	2803,05	2795,01
570	2793	140,12	4,7	2797,70	2798,14	3,75	2801,89	2794,39
600	2792	110,12	3,9	2795,89	2797,26	3,41	2800,67	2793,85
630	2792	80,12	3,0	2794,97	2796,37	2,98	2799,35	2793,39
660	2790	50,12	1,9	2791,95	2795,48	2,41	2797,90	2793,07
690	2790	20,12	0,8	2790,82	2794,59	1,56	2796,16	2793,03
710,12	2790	0	0,0	2790,00	2794,00	0,00	2794,00	2794,00

DATOS DEL ENLACE	ENLACE: Central - IDF 10		
Estación	A:	CENTRAL	
	Longitud:	78 38 56,8	W
	Latitud:	1 39 11,2	S
	Altura:	2805,00	m.
	Torre:	10,00	m.
Estación	B:	IDF 10	
	Longitud:	78 38 56,4	W
	Latitud:	1 39 4,7	S
	Altura:	2817,00	m.
	Torre:	2,00	m.
DISTANCIA DEL ENLACE:		200	m.
FRECUENCIA:		**2400**	MHz.
FACTOR K		**1,33**	
ALTURA DE MALEZA		**0**	m.



DISTANCIA 1	ALTURA SOBRENIVEL DEL MAR	DISTANCIA 2	FACTOR DE CORRECCION DE ALURA	ALTURA CORREGIDA	ALTURA DEL RAYO	RADIO DE LA 1a. ZONA DE FRESNEL	ALTURA SUPERIOR DE FRESNEL	ALTURA INFERIOR DE FRESNEL
(metros)	(m)	(m)		(m)	(m)	(m)	(m)	(m)
0	2805	200	0,0	2805,00	2815,00	0,00	2815,00	2815,00
15	2805	185	0,2	2805,16	2815,30	1,32	2816,62	2813,98
30	2806	170	0,3	2806,30	2815,60	1,79	2817,39	2813,81
45	2809	155	0,4	2809,41	2815,90	2,09	2817,99	2813,81
60	2809	140	0,5	2809,49	2816,20	2,29	2818,49	2813,91
75	2809	125	0,6	2809,55	2816,50	2,42	2818,92	2814,08
90	2810	110	0,6	2810,58	2816,80	2,49	2819,29	2814,31
105	2810	95	0,6	2810,59	2817,10	2,50	2819,60	2814,60
120	2810	80	0,6	2810,56	2817,40	2,45	2819,85	2814,95
135	2810	65	0,5	2810,52	2817,70	2,34	2820,04	2815,36
150	2813	50	0,4	2813,44	2818,00	2,17	2820,17	2815,83
165	2815	35	0,3	2815,34	2818,30	1,90	2820,20	2816,40
180	2815	20	0,2	2815,21	2818,60	1,50	2820,10	2817,10
195	2816	5	0,1	2816,06	2818,90	0,78	2819,68	2818,12
200	2817	0	0,0	2817,00	2819,00	0,00	2819,00	2819,00

ANEXO 2

MODELO OSI

En sus inicios, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de networking, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controlan todo uso de la tecnología. Las tecnologías de networking que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI. Esto es en particular así cuando lo que buscan es enseñar a los usuarios a utilizar sus productos. Se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

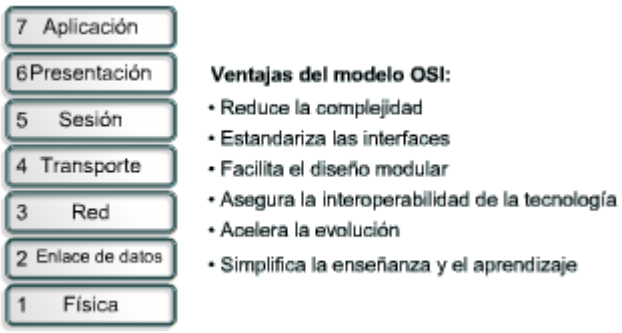
LAS CAPAS DEL MODELO OSI

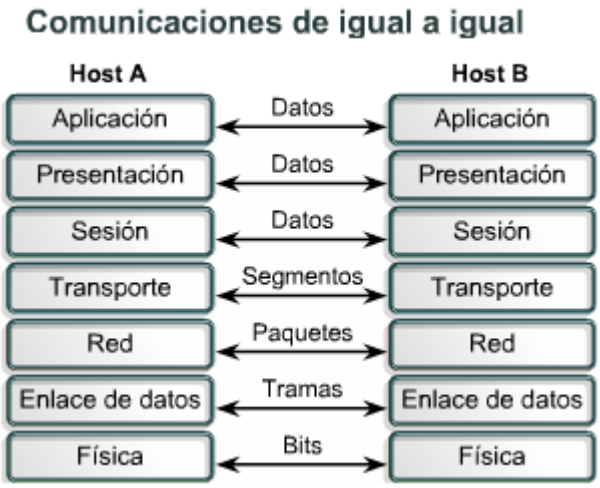
El modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. El modelo de referencia OSI explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. - La división de la red en siete capas permite obtener las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Evita que los cambios en una capa afecten las otras capas.

- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje





MODELO TCP/IP

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP.

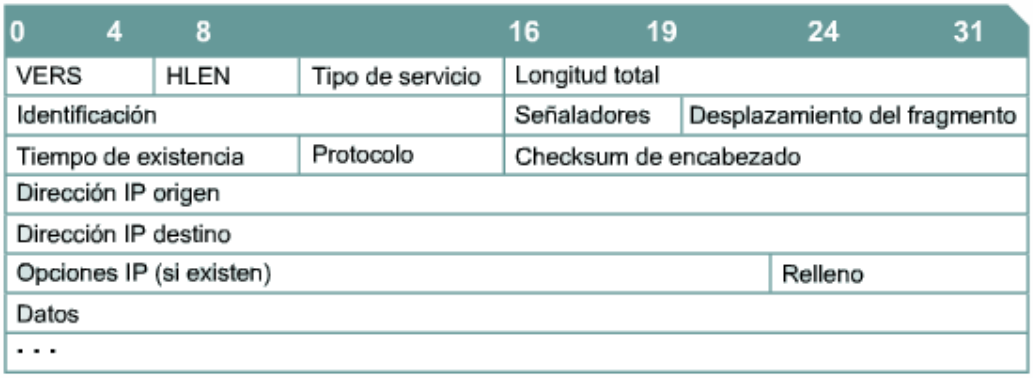
A diferencia de las tecnologías de networking propietarias mencionadas anteriormente, el TCP/IP se desarrolló como un estándar abierto. Esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar.

El modelo TCP/IP tiene las siguientes cuatro capas:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
- Capa de acceso a la red

ANATOMIA DEL UN PAQUETE IP

Los paquetes IP constan de los datos de las capas superiores más el encabezado IP. El encabezado IP está formado por lo siguiente:



0 4	8		16 19	24 31
VERS	HLEN	Tipo de servicio	Longitud total	
Identificación			Señaladores	Desplazamiento del fragmento
Tiempo de existencia		Protocolo	Checksum de encabezado	
Dirección IP origen				
Dirección IP destino				
Opciones IP (si existen)				Relleno
Datos				
. . .				

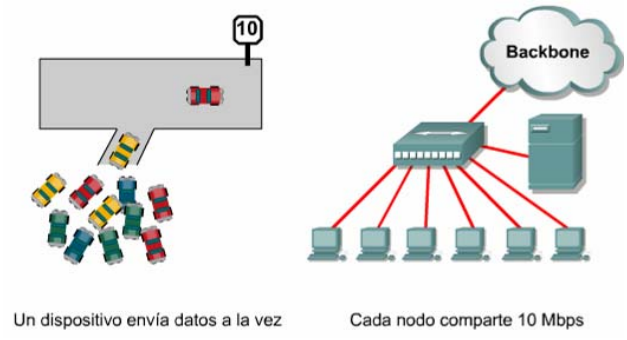
Aunque las direcciones de origen y destino IP son importantes, los otros campos del encabezado han hecho que IP sea muy flexible. Los campos del encabezado contienen las direcciones origen y destino del paquete y generalmente incluyen la longutid del mensaje. La información para enrutar el mensaje también está incluída en el encabezado de IP, el cual puede ser largo y complejo.

LAN Ethernet/802.3

Las tecnologías LAN más antiguas usaban infraestructuras de Ethernet de cable fino o grueso.

Ethernet es básicamente una tecnología compartida donde todos los usuarios en un segmento LAN dado compiten por el mismo ancho de banda disponible. A

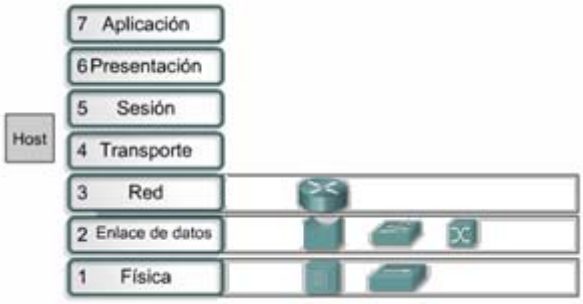
medida que se agregaban hubs a la red, más usuarios entraban a la competencia por el mismo ancho de banda.



Acceso a Ethernet por medio de hubs

Las colisiones son un producto secundario de las redes Ethernet. Si dos o más dispositivos intentan transmitir señales al mismo tiempo, se produce una colisión. La consecuencia del exceso de colisiones en una red son los tiempos de respuesta de red lentos. Esto indica que la red se encuentra demasiado congestionada o que demasiados usuarios necesitan acceder a la red al mismo tiempo.

Las LAN normalmente utilizan una combinación de dispositivos de Capa 1, Capa 2 y Capa 3. La implementación de estos dispositivos depende de las necesidades específicas de la organización.



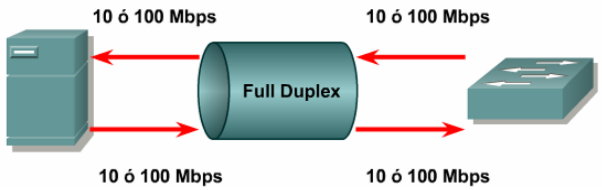
Transmisión full duplex

Ethernet full duplex permite la transmisión de un paquete y la recepción de un paquete distinto al mismo tiempo. Esta transmisión y recepción simultánea requiere del uso de dos pares de hilos dentro del cable y una conexión conmutada entre cada nodo. Esta conexión se considera de punto a punto y está libre de colisiones. Debido a que ambos nodos pueden transmitir y recibir al mismo tiempo, no existen negociaciones para el ancho de banda. Ethernet full duplex puede utilizar una infraestructura de cables ya implementada, siempre y cuando el medio cumpla con los estándares de Ethernet mínimos.

Para transmitir y recibir de forma simultánea, se necesita un puerto de switch dedicado para cada nodo. La conexiones full duplex pueden utilizar medios 10BASE-T, 100BASE-TX o 100BASE-FX para crear conexiones punto a punto. Las NIC en todos los dispositivos conectados deben tener capacidades full-duplex.

El switch Ethernet full-duplex aprovecha los dos pares de hilos en un cable y crea una conexión directa entre el transmisor (TX) en un extremo del circuito y el receptor (RX) en el otro extremo. Con las dos estaciones conectadas de esta manera, se crea un dominio libre de colisiones debido a que se produce la transmisión y la recepción de los datos en circuitos distintos no competitivos.

Ethernet generalmente puede usar únicamente 50%-60% del ancho de banda de 10 Mbps disponible debido a las colisiones y la latencia. Ethernet full duplex ofrece 100% del ancho de banda en ambas direcciones. Esto produce una tasa de transferencia potencial de 20 Mbps, lo que resulta de 10 Mbps TX y 10 Mbps RX.



Factores que afectan el rendimiento de la red

En la actualidad, las LAN están cada vez más congestionadas y sobrecargadas. Además de una gran cantidad de usuarios de red, algunos otros factores se han combinado para poner a prueba las capacidades de las LAN tradicionales:

- El entorno multitarea, presente en los sistemas operativos de escritorio actuales como Windows, Unix/Linux y MAC OS X, permite transacciones de red simultáneas. Esta capacidad aumentada ha dado como resultado una mayor demanda de recursos de red.
- El uso de las aplicaciones que hacen uso intensivo de la red, como la World Wide Web, ha aumentado. Las aplicaciones de cliente/servidor permiten que los administradores centralicen la información, facilitando así el mantenimiento y la protección de la información.
- Las aplicaciones de cliente/servidor no requieren que las estaciones de trabajo mantengan información ni proporcionen espacio del disco duro para almacenarla.

MEDIOS DE ETHERNET Y REQUISITOS DE CONECTOR

Las especificaciones de los cables y conectores usados para admitir las implementaciones de Ethernet derivan del cuerpo de estándares de la Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (EIA) Las categorías de cableado definidas para Ethernet derivan del Estándar de Recorridos y Espacios de Telecomunicaciones para Edificios Comerciales EIA/TIA-568 (SP-2840).

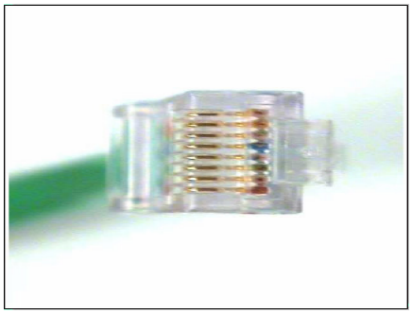
La Figura compara las especificaciones de los cables y conectores para las implementaciones de Ethernet más conocidas.

Medios de Ethernet y requisitos de conector

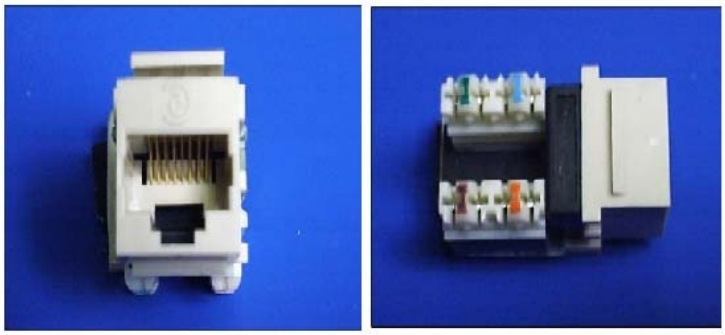
	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Medios	Cable coaxial de 50 ohmios (Thinnet)	Cable coaxial de 50 ohmios (Thicknet)	UTP Categoría 3, 4, 5 EIA/TIA, dos pares	UTP Categoría 5 EIA/TIA, dos pares	fibra multimodo 62.5/125	STP	UTP Categoría 5 EIA/TIA, cuatro pares	fibra micro multimodo 62.5/50	fibra micro multimodo 62.5/50; fibra monomodo de 9 micrones
Longitud de segmento máxima	185 m (606,94 pies)	500 m (1.640,4 pies)	100 m (328 pies)	100 m (328 pies)	400 m (1312,3 pies)	25 m (82 pies)	100 m (328 pies)	275 m (853 pies) para microfibra 62.5; 550 m (1804,5 pies) para microfibra 50	440 m (1443,6 pies) para microfibra 62.5; 550 m (1804,5 pies) para micro fibra 50; 3 a 10 km (1,86 a 6,2 millas) para fibra monomodo
Topología	Bus	Bus	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella
Conector	BNC	Interfaz de unidad de conexión (AUI)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		

EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. Las letras RJ significan "registered jack" (jack registrado), y el número 45 se refiere a una secuencia específica de cableado.

Conector RJ-45



Jack RJ – 45



Cableado UTP

Utilice cables directos (“ straight-through”) para conectar:

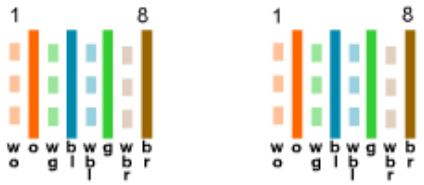
- Switch to router
- Switch to PC or server

Utilice cables cruzados (“ crossover”) para conectar:

- witch to switch
- Switch to hub
- Hub to hub
- Router to router
- PC to PC
- Router to PC

Implementación de UTP de Conexión directa

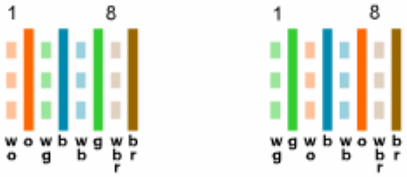
Pin	Rótulo
1	TD+
2	TD-
3	RD+
4	NC
5	NC
6	RD-
7	NC
8	NC



Los hilos en el extremo del cable están en el mismo orden.

Implementación de UTP de Conexión Cruzado

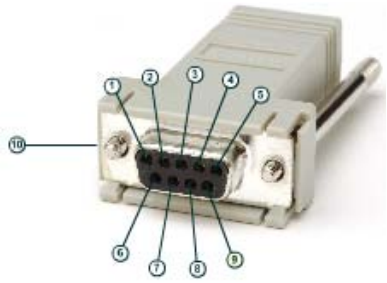
Pin	Rótulo	Pin	Rótulo
1	TD+	1	TD+
2	TD-	2	TD-
3	RD+	3	RD+
4	NC	4	NC
5	NC	5	NC
6	RD-	6	RD-
7	NC	7	NC
8	NC	8	NC



El par de hilos anaranjados y el par de hilos verdes cambian de lugar en un extremo del

Cable consola

RJ 45	DB9
1 RTS	8 CTS
2 DTR	6 DSR
3 TxD	2 RxD
4 GND	5 GND
5 GND	5 GND
6 RxD	3TXD
7 DSR	4 DTR
8 CTS	7 RTS



RTS= peticion para enviar

DTR= terminal de datos lista

TxD= transmitir datos

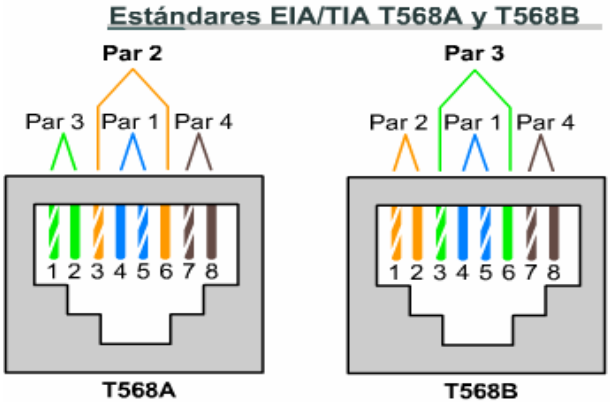
GND=tierra uno pata txd y uno para rxd

RxD= recibir datos

DSR= conjunto de datos listo

CTS= listo para enviar

NOTA: El RJ45 corresponde al estándar TIA/EIA 568-B



DOMINIOS DE COLISION

Los dominios de colisión son los segmentos de red física conectados, donde pueden ocurrir colisiones. Las colisiones causan que la red sea ineficiente. Cada vez que ocurre una colisión en la red, se detienen todas las transmisiones por un período de tiempo. La duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo de la red.
Los tipos de dispositivos que interconectan los segmentos de medios definen los dominios de colisión. Estos dispositivos se clasifican en dispositivos OSI de Capa 1, 2 ó 3. Los dispositivos de Capa 1 no dividen los dominios de colisión; los dispositivos de Capa 2 y 3 sí lo hacen. La división o aumento del número de dominios de colisión con los dispositivos de Capa 2 y 3 se conoce también como segmentación.

Los dispositivos de Capa 2 dividen o segmentan los dominios de colisión. El control de propagación de trama con la dirección MAC asignada a todos los dispositivos de Ethernet ejecuta esta función. Los dispositivos de Capa 2, los puentes y switches, hacen un seguimiento de las direcciones MAC y el segmento en el que se encuentran. Al hacer esto, estos dispositivos pueden controlar el flujo de tráfico en el nivel de Capa 2. Esta función hace que las redes sean más eficientes, al permitir que los datos se transmitan por diferentes segmentos de la LAN al mismo tiempo sin que las tramas colisionen. Al usar puentes y switches, el dominio de colisión se divide efectivamente en partes más pequeñas, que se transforman cada una a su vez en un dominio de colisión.

Estos dominios de colisión más pequeños tendrán menos hosts y menos tráfico que el dominio original. Cuanto menor sea la cantidad de hosts en un dominio de colisión, mayores son las probabilidades de que el medio se encuentre disponible.

BROADCAST DE CAPA 2

Para comunicarse con todos los dominios de colisión, los protocolos utilizan tramas de broadcast y multicast a nivel de Capa 2 en el modelo OSI. Cuando un nodo necesita comunicarse con todos los hosts de la red, envía una trama de broadcast con una dirección MAC destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual debe responder la tarjeta de interfaz de la red (Network Interface Card, NIC) de cada host.

Los dispositivos de Capa 2 deben inundar todo el tráfico de broadcast y multicast. La acumulación de tráfico de broadcast y multicast de cada dispositivo de la red se denomina radiación de broadcast. En algunos casos, la circulación de radiación de broadcast puede saturar la red, entonces no hay ancho de banda disponible para los datos de las aplicaciones. En este caso, no se pueden establecer las conexiones en la red, y las conexiones existentes pueden descartarse, algo que se conoce como tormenta de broadcast. La probabilidad de las tormentas de broadcast aumenta a medida que crece la red conmutada.

DOMINIOS DE BROADCAST

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host.

Pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast. En otras palabras, todos los

nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3. Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts. Los routers, en realidad, funcionan en las Capas 1, 2 y 3.

Protocolos Enrutables y Enrutados

Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes

Un protocolo describe lo siguiente:

- El formato el cual el mensaje se debe conformar
- La manera en que los computadores intercambian un mensaje dentro del contexto de una actividad en particular.

Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y un número de host.

- IPX, requieren sólode un número de red porque estos protocolos utilizan la dirección MAC del host como número de Host.
- IP, requieren una dirección completa que especifique la porción de red y la porción de Host. IP requiere una máscara de red para diferenciar estos dos números.

Protocolos de Enrutamiento

Determina el mejor camino que los protocolos ruteados utilizarán para alcanzar el destino.

- Proveen procesos para compartir información de enrutamiento.
- Permite a los Routers a comunicarse con otros Routers para actualizar y mantener las tablas de enrutamiento

Vector Distancia: RIP, IGRP

- Determina la dirección (vector) y la distancia a un enlace en la red. Esta cuenta repetitiva del # de saltos (# of hops) permite al router a encontrar el camino más corto en el árbol de rutas (shortest path spanning tree.)

Enrutamiento de Estado: OSPF

- Se recrea una topología exacta de toda la red

RIP es un protocolo de enrutamiento de vector-distancia que utiliza el número de saltos como métrica para determinar la dirección y la distancia a cualquier enlace en Internetworking. RIP no puede enrutar más alla de los 15 saltos. RIP Version 1 (RIPv1) necesita que todos los dispositivos de la red utilicen la misma máscara de subred, debido a que no incluye la información de la máscara en sus actualizaciones de enrutamiento (enrutamiento de clase).

RIP Versión 2 (RIPv2) ofrece un prefijo de enrutamiento y envía información de la máscara de subred en sus actualizaciones. Esto se conoce como enrutamiento sin clase. En los protocolos sin clase, las distintas subredes dentro de la misma red pueden tener varias máscaras de subred. El uso de diferentes máscaras de subred dentro de la misma red se denomina máscara de subred de longitud variable (VLSM).

IGRP es un protocolo de enrutamiento de vector-distancia desarrollado por CISCO. El IGRP se desarrollo específicamente para ocuparse de los problemas relacionados con el enrutamiento de grandes redes que no se podían administrar con protocolos como, por ejem: RIP, IGRP puede elegir la ruta disponible más rápida basándose en el retardo, el ancho de banda, la carga y la confiabilidad. IGRP también posee un limite máximo de número de saltos mucho mayor que RIP. Utiliza sólo enrutamiento con clase

OSPF es un protocolo de enrutamiento de estado de enlace desarrollado por la Fuerza de tareas de ingeniería de internet (IETF) en 1988. El OSPF se elaboro para cubrir las necesidades de las grandes internetworks escalables que RIP no podía cubrir.El sist intermed-sist intermed (IS-IS) es un protocolo de enrutamiento de

estado de enlace utilizado para protocolos enrutados distintos a IP. El IS-IS integrado es un sistema de implementación expandido de IS-IS que admite vario protocolos de enrutamiento, inclusive IP.

CISCO es propietario de **EIGRP** y también IGRP. EIGRP es una versión mejorada de IGRP. EIGRP suministra una eficiencia de operación superior tal como una convergencia rápida y un bajo gasto del ancho de banda. EIGRP es un protocolo mejorado de vector-distancia que también utiliza alguna de las funciones del protocolo de estado de enlace. El EIGRP a veces viene incluido como un protocolo híbrido.

El protocolo Gateway Fronterizo (BGP) es un ejemplo de protocolo de Gateway exterior (EGP). BGP intercambia información de enrutamiento entre sistemas autónomos a la vez que garantiza una elección de ruta libre de loops. BGP es el protocolo principal de publicación de rutas utilizado por las compañías más importantes e ISP en la Internet. BGP 4 es la primera versión BGP que admite enrutamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de Gateway internos (IGP), como RIP OSPF, y EIGRP, BGP no usa métricas como número de saltos, ancho de banda, o retardo. En cambio, BGP toma decisiones de enrutamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

ANEXO 3

3COM® SUPERSTACK® 3 SWITCH 4400

3com

DATA SHEET

3Com® SuperStack® 3 Switch 4400 Family

Key Benefits

Advanced, affordable 10/100 networking solutions

Standard Features

Affordability
High performance switches with advanced stackability at an affordable price.

Performance
Forwarding rates up to 6.6 million pps (24-port), or 10.1 million pps (48-port).

Easy Management
3Com® Network Supervisor application is included with discovery, mapping, monitoring, and alerting for easy network administration.

Scalable
Simple stacking architecture increases workgroup capacity when needed and allows high-speed trunks between the workgroup and other network resources.

Easy Management
Stack up to 192 10/100 ports and manage as a single entity with one IP address.

Flexibility
Install up to two optional modules for stacking or to provide extra high-bandwidth ports.

Resilient and Fault Tolerant
For non-stop network operation, the 3Com® SuperStack® 3 Switch 4400 family allows resilient and hot-swappable stacking and resilient network connections.

Limited Lifetime Warranty
Ensures peace of mind. Lifetime warranty includes fan and power supply.

Enhanced Features

Prioritize Business Critical Traffic
Advanced Class of Service support including multilayer packet classification capabilities to allow prioritization of critical traffic.

Greater Bandwidth
Suppress unwanted protocols and applications from the network.

Transparent Webcache Redirection
Web traffic can be redirected automatically to a 3Com SuperStack 3 Webcache device, improving web performance and easing network administration.

The 3Com SuperStack 3 Switch 4400 family delivers high-performance 10/100 Ethernet switching in a simple, affordable platform.

Two models come with standard and advanced features ready for today's most demanding 10/100 Ethernet switching applications. Choose the SuperStack 3 Switch 4400 24-Port or Switch 4400 48-Port.

The SuperStack 3 Switch 4400 SE comes with the standard Switch 4400 family capabilities, and is upgradeable* to the enhanced feature set.

* Affordable 3Com SuperStack 3 Switch 4400 Enhanced Software Upgrade (3C17207) available 2nd half 2002

Specifications

Connectors

24 or 48 auto-negotiating 10BASE-T/100BASE-TX ports configured as Auto MDIX

2 module slots accommodating media modules or stacking modules

All fiber module connectors are MT-RJ

Advanced Redundant Power System Type 2A connector

RS232 console port

Stacking

Up to 192 10/100 front panel ports

Mix and match Switch 4400 24-port (3C17203) and Switch 4400 48-port (3C17204)

Stack Switch 4400 SE (3C17206) only with other like units

Traffic Management

Four priority queues per port
IEEE 802.1p CoS
DiffServ*
Application/protocol blocking*
Transparent Webcache redirection*

Performance

*24-port**
8.8 Gbps switching capacity
6.6 million packets per second
8,000 MAC addresses supported

48-port
17.6 Gbps switching capacity
10.1 million packets per second
8,000 MAC addresses supported

Reliability

24-port: MTBF @ 40°C:
326,000 hours

48-port: MTBF @ 40°C:
176,294 hours

Dimensions

Height: 43.6 mm (1.7 in or 1U)
Width: 440 mm (17.3 in)
Depth: 274 mm (10.8 in)
Weight: *24-port:* 2.8 kg (6.2 lb)
Weight: *48-port:* 3.2 kg (7.1 lb)

Environmental Requirements

Operating temperature:
0° to 40°C (32° to 104°F)

Storage Temperature:
-40° to +70°C (-40° to +158°F)

Operating Humidity:
10% to 90% relative humidity noncondensing

Standards: EN60068 (IEC68)

Safety Agency Certifications

24-port: UL1950, EN60950, CSA22.2 No. 950, IEC 60950

48-port: UL60950, EN60950, CSA22.2 No. 60950, IEC 60950

Emissions

EN55022 Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, AS/NZS 3548 Class A, CNS 13438 Class A

Immunity: EN55024

Heat Dissipation:
24-port: 75 W maximum (255 BTU/hr maximum)
48-port: 120 W maximum (410 BTU/hr maximum)

Power Supply

AC Line Frequency 50/60 Hz

Input Voltage 90-240 VAC

Current Rating:
24-port: 2.3A maximum
48-port: 2.8A maximum

SNMP Standards

SNMP Protocol (RFC 1157)

MIB-II (RFC 1213)

Bridge MIB (RFC 1493)

RMON MIB II (RFC2021)

Remote Monitoring MIB (RFC 1757)

Interface MIB (2233)

MAU MIB (RFC 2668)

Warranty and Non-Warranty Services

Limited Lifetime Warranty, for as long as the original customer owns the product, or five years after product discontinuance, whichever occurs first. Includes fan and power supply.

After registering the product online, other free support services such as telephone support, fast hardware replacement, and software updates may also be available, depending on regional availability and retailer participation.

Management

3Com Network Supervisor provided free of charge on accompanying CD

Web interface management

Command line interface management

SNMP compatibility

*Switch 4400 SE requires Enhanced Software Upgrade, 3C17207, to perform these functions.
* 24-port specifications refer to both Switch 4400 24-Port (3C17203) and Switch 4400 SE 24-Port (3C17206)

Ordering Information

3Com SuperStack 3 Switch 4400 24-port	3C17203
3Com SuperStack 3 Switch 4400 48-port	3C17204
3Com SuperStack 3 Switch 4400 SE 24-port	3C17206

Optional Modules and Accessories

3Com SuperStack 3 Switch 4400 Enhanced Software Upgrade*	3C17207
3Com SuperStack 3 Switch 4400 1000BASE-T Module	3C17220
3Com SuperStack 3 Switch 4400 1000BASE-SX Module	3C17221
3Com SuperStack 3 Switch 4400 100BASE-FX Module	3C17222
3Com SuperStack 3 Switch 4400 1000BASE-LX Module	3C17223
3Com SuperStack 3 Switch 4400 Stacking Kit (Two stacking modules and cable to stack two Switch 4400s—see stacking specifications above for restrictions)	3C17227
3Com SuperStack 3 Switch 4400 Stack Extender Kit (One stacking module, one cascade module and one cable for adding more Switch 4400s to an existing Switch 4400 stack—see stacking specifications above for restrictions)	3C17228
3Com SuperStack 3 Advanced Redundant Power System	3C16071B
3Com SuperStack 3 Advanced RPS Type 2A module	3C16074A

* Affordable 3Com SuperStack 3 Switch 4400 Enhanced Software Upgrade (3C17207) available 2nd half 2002

3Com Corporation, Corporate Headquarters, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

400679-005 04/02

3COM 11A 54 MBPS WIRELESS LAN

General

Tipo de dispositivo :	Puente inalámbrico
Diseño resistente :	Exteriores
Dispositivos integrados :	Punto de acceso inalámbrico
Anchura :	19 cm
Profundidad :	19.5 cm
Altura :	7.4 cm
Peso :	5.3 kg

Conexión de redes

»Factor de forma :	Externo
»Tecnología de conectividad :	Inalámbrico
»Velocidad de transferencia de datos :	108 Mbps
»Formato código de línea :	CCK, 64 QAM, BPSK, QPSK, 16 QAM, OFDM
»Protocolo de interconexión de datos :	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, 802.11 Super G
»Método de espectro expandido :	OFDM, DSSS
»Red / Protocolo de transporte :	TCP/IP, IPX/SPX, UDP/IP, NetBEUI/NetBIOS
»Protocolo de gestión remota :	SNMP 1, Telnet, SNMP 3, HTTP, HTTPS
»Alcance máximo al aire libre :	15.5 km
»Capacidad :	Conexión / cantidad de usuarios : 128
»Indicadores de estado :	Actividad de enlace, alimentación, tinta OK
»Características :	Soporte de DHCP, soporte VLAN, montable en pared, soporte Wi-Fi Multimedia (WMM), soporte de Access Control List (ACL)
»Algoritmo de cifrado :	AES, WEP de 128 bits, ncriptación de 64 bits WEP, WEP

	de 152 bits, SSL, TKIP, WPA, WPA2
»Método de autentificación :	Secure Shell (SSH), RADIUS
»Cumplimiento de normas :	IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, Wi-Fi CERTIFIED

Antena

»Antena :	Interna integrada
»Cantidad de antenas :	1
»Directividad :	Direccional
»Nivel de ganancia :	17 dBi

Expansión / Conectividad

»Interfaces :	1 x red - Radio-Ethernet - conector N-series x 2 1 x red / energía - Ethernet 10Base-T/100Base-TX 1 x red - Radio-Ethernet

Diverso

»Cables incluidos :	1 x cable de red - 30 m 1 x cable serie - 30 m
»Kit de montaje :	Incluido
»Cumplimiento de normas :	Certificado FCC Clase B , ETSI, EN 60950, EN 61000-3-2, IEC 60950, EN 61000-3-3, EN55022 Class A, UL 60950 Third Edition, ICES-003 Class B, EN 300.328, AS/NZS 3260, RSS-102, FCC Part 15, UL 2043, FCC CFR47 Part 15, CSA C22.2 No. 60950 Third Edition

Alimentación

»Alimentación por Ethernet (PoE) :	Sí
»Dispositivo de alimentación :	Inyector de corriente - externa

Software / Requisitos del sistema

»Software incluido :	Controladores y utilidades

Garantía del fabricante

»Servicio y mantenimiento :	1 año de garantía
»Detalles de Servicio y Mantenimiento :	Garantía limitada - 1 año

Parámetros de entorno

»Temperatura mínima de funcionamiento :	-40 °C
»Temperatura máxima de funcionamiento :	65 °C

Torres Syscom

STZ-35. Tramo de torre para zonas de fuertes vientos. Muy resistente a la corrosión del salitre y humedad. Altura máxima de 45 Mts. Requiere retenidas cada 9 Mts. Cada tramo pesa 20.6 Kgs. y mide 3 Mts. de largo más 10 cms. del niple. La torre está formada por tubo industrial de 1 1/4" amarrado con semiflecha de 5/16" en zig zag rígida con un ancho de 35 cms. dándole una alta resistencia.

TRAMOS DE REMATE / COPETE

Todos los tramos están hechos en formadores de alta precisión, por lo cual su torre quedará perfectamente recta y vertical sin necesidad de ajustes. Se recomienda el uso del remate para proteger su torre del agua de la lluvia en el interior. Indispensable para protección.

SCZ-35 G. Tramo de remate galvanizada por inmersión en caliente.

ANTENA OMNIDIRECCIONAL DE 12 DBI PARA 2.4 GHZ

2.4 GHz Omnidirectional Antena

Los sistemas de antenas omnidireccionales ofrecidas por Netkrom están hechos a base de Fibra de Vidrio resistentes a las radiaciones UV y con todos sus brackets hechos de acero inoxidable. La antena viene con conectores estándar tipo N-Hembra impermeables con tuercas resistentes para un montaje opcional aislador. La antena de 12dBi tiene un Electrical Downtilt estándar de 3º. Este también tiene conectores pigtail N-Hembra o N-Macho de 24" para conexión directa a Access Points Outdoor. La antena de 9dBi está disponible con un Electrical Downtilt de 0 º y 7 º la cual es perfecta para sistemas inalámbricos cercanos tales como complejos de apartamentos. Debido a su insuperable diseño de alto rendimiento el cual elimina nulls, pueden ser usados en una gran variedad de sistemas inalámbricos.

Características:

- Ganancia de Antena de 9 y 12 dB
- 12dB tiene 3 º de Electrical Downtilt Estándar
- 9dBi tiene Electrical Downtilt de 0 º o 7 º
- Robusto, ligero e impermeable

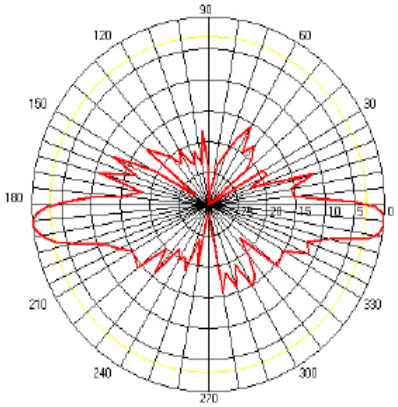
Aplicaciones:

- 2.4 GHz Aplicaciones en la Banda ISM (802.11b/g)
- Antenas para estaciones base
- Sistemas Punto a Multipunto
- Sistemas Inalámbricos de Banda Ancha
- Access Points WiFi

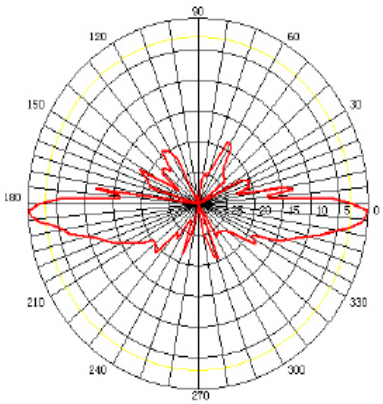
Especificaciones:

Código del Producto	W24-9O	W24-12O
Eléctricas		
Ganancia	9 dBi	12 dBi
Rango de Frecuencia	2400 – 2483 MHz	2400 – 2483 MHz
Pérdida de Retorno Input(S11)	-14 dB	-14 dB
WSWR	1.5:1	1.5:1
Impedancia	50 OHM	50 OHM
Amplitud de Rayo Vertical	14º	7º
Potencia de Entrada	100 W	100 W
Front to Back	20 dB	30 dB
Diámetro de Pole (OD)	1" (25) a 2" (50) Pulg. (mm)	1" (25) a 2" (50) Pulg. (mm)
Electrical Downtilt	0 º o 7 º	3 º
Mecánicas		
Dimensiones (L +/-1.0")	27" (69cm)	48" (122cm)
Peso	1.1 Lbs (0.5Kg)	1.4 Lbs (0.6Kg)
Temperatura de Operación	-40 a +70 º C	-40 a +70 º C
Resistencia al Viento	125mph (56 M/sec)	125mph (56 M/sec)

Patrón de Antenas a 2.4GHz



9dB Patrón de Antena Vertical 7 º Elec Downtilt – Plano E



12dB Patrón de Antena Vertical 3 º Elec Downtilt – Plano E

Información para Pedidos:

- **W24-9O** 2.4GHz 9dBi Omnidireccional Antena VPOL (Conector N Hembra Pigtail)
- **W24-12O** 2.4GHz 12dBi Omnidireccional Antena VPOL (Conector N Hembra Pigtail)

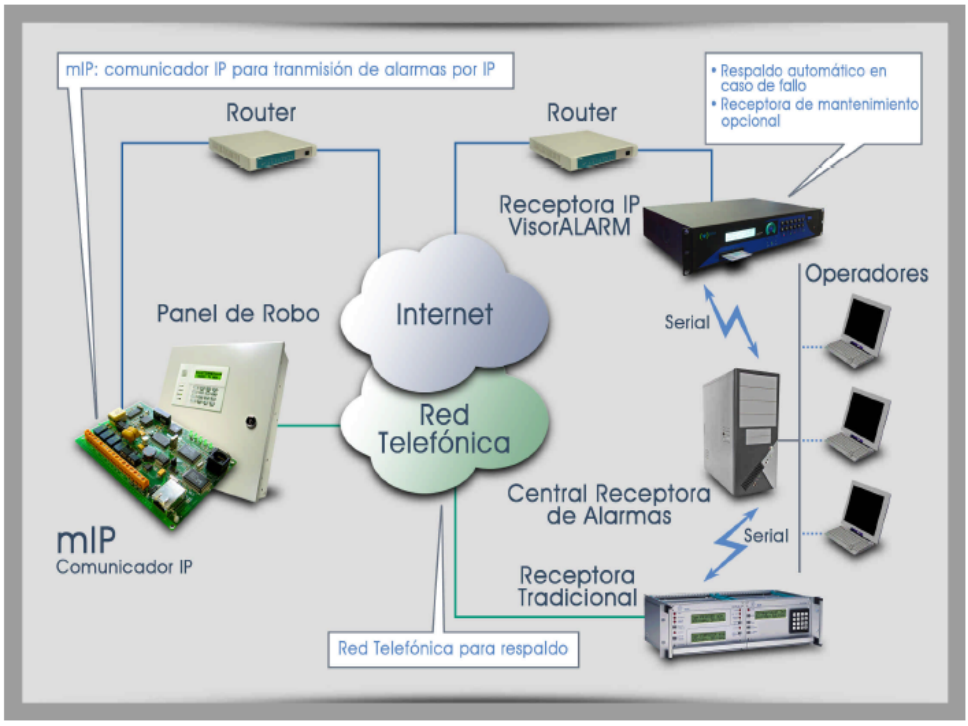
Modulo de comunicación IP mIP

REQUISITOS DE INSTALACIÓN

- Panel de robo compatible con el formato Contact-ID.
- Al menos 250mA de corriente disponibles para alimentar el mIP.
- Conexión ethernet 10/100 Mbps.
- Servidor DHCP disponible en la red o una dirección IP libre en la red para ser asignada al mIP.
- Puerto UDP de salida disponible para poder establecer la comunicación con la central receptora (por defecto puerto 80/udp).
- Dirección IP pública de la receptora IP con la que el mIP establecerá la conexión.
- Identificador de cuenta.
- Password de instalador (proporcionado por la central receptora de alarmas para poder realizar el registro con la receptora IP).

ARQUITECTURA DEL SISTEMA

- El mIP se conecta a un router de Internet.
- La línea telefónica, en lugar de conectarse directamente al panel de alarmas, se conecta al mIP y desde éste se proporciona línea telefónica al panel de alarmas.
- El mIP monitoriza el estado de la conexión de internet con la receptora IP y decide qué red utilizar para la transmisión de alarmas generadas por el panel.
- En la central receptora de alarmas, se podrá seguir utilizando una receptora tradicional para recibir las alarmas transmitidas por red telefónica. Si la conexión IP está disponible las alarmas y la supervisión se realizarán por IP como opción prioritaria.
- El mIP está en comunicación constante con el panel de alarmas proporcionando un mecanismo de supervisión en tiempo real.



ESPECIFICACIONES TÉCNICAS DEL mIP

ALIMENTACIÓN

- *Tensión nominal*: 10 VDC a 24 VDC
- *Corriente máxima:*

	Reposo	Alarma	Transitorio
A12Vdc	190mA	240mA	500mA
A24Vdc	100mA	120mA	300mA

DIMENSIONES Y PESO

- *Largo x Ancho x Alto*: 140x92x29 mm
- *Peso*: 150 gr

ESPECIFICACIONES AMBIENTALES

- *Temperatura ambiente:* 0º a 49º C (32º a 120º F)
- *Humedad relativa:* Máximo 95%

PUERTO LAN

- *Conector:* RJ45 hembra
- *Velocidad:* 10 Mbps
- *Protocolos:* UDP, IP, ARP, DHCP, AES, TELNET, ETHERNET BLUEBOK

ENTRADAS Y SALIDAS

- *Salida:* 2A Máx. Si V ≤ 30 VDC para cargas resistivas. Contacto seco N.A o N.C
- *Entrada:* 1AMax.

CONSOLA

- *Asíncrona:* 9600 bps, 8 bits, sin paridad, 1 bit stop. Protegida por contraseña
- *Telefónica:* Conexión por TO-AP con teléfono tonos**#contraseña
- *IP [TELNET]:* Protegida por contraseña

Telsec

Tedat Security S.L.
Parque Tecnológico de Madrid
28760 – Tres Cantos
MADRID - ESPAÑA
TEL.: +34.918076565
FAX.: +34.918076566
www.teldat.es

TeldatCorp
1111 Brickell Avenue - Suite 1100
MIAMI, FLORIDA 33131 - EE.UU.
TEL.: +1.305.3723480
TEL.: +1.866.4TELDAT
FAX : +1.305.5135209
www.teldatsecurity.com

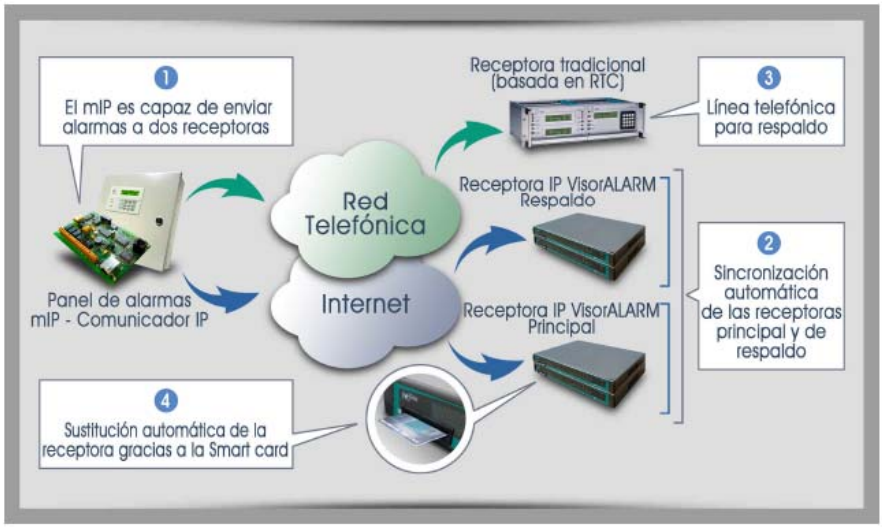
Central receptora de alarmas

RESPALDO

➔ El VisorALARM incorpora funcionalidades avanzadas de respaldo que permiten que los equipos remotos instalados envíen alarmas y sondeos de forma transparente a una receptora principal y otra de respaldo en caso de caída de la primera. Adicionalmente, ambas receptoras informan con alarmas técnicas del paso a respaldo y de la vuelta del mismo. Ambas receptoras sincronizan sus configuraciones e información de cuentas permitiendo así que en caso de paso a respaldo o vuelta del mismo no se produzca ninguna inconsistencia respecto al parque de equipos instalados.
Por último, existen mecanismos para incorporar una tercera receptora en el sistema, denominada de mantenimiento, sobre la que se pueden observar todas las alarmas que los equipos remotos envían bien a la receptora principal o bien a la receptora de respaldo.

SUPERVISIÓN DE LÍNEA

➔ La receptora VisorALARM recibe mensajes constantes de supervisión de los equipos remotos. Estos mensajes de supervisión suponen sondeos a la receptora que son contestados con paquetes de asentimiento. El estado de todos los equipos remotos es comprobado periódicamente y en caso de pérdida de conectividad de uno de los equipos se genera un evento Contact-ID 350 Communication Trouble. En caso de pérdida de conectividad en central y para evitar que la receptora VisorALARM genere múltiples eventos de fallo de comunicaciones por cada equipo, la receptora es capaz de monitorizar la línea de central y generar un solo evento Contact-ID 356 Loss of Central Polling en el caso de pérdida de la conectividad central.



Especificaciones técnicas VisorALARM

ARQUITECTURA HARDWARE

- *Procesadores*: Motorola MPC860, a 50, 66 u 80 MHz, según versiones
- *Memoria:* 32, 64, 128 ó 256 Mbytes de SDRAM, según versiones
- *Unidad de almacenamiento:* Memoria FLASH, 4, 8 ó 16 Mbytes según versiones EEPROM 2 Kbytes, NVRAM 128 Kbytes

INTERFAZ DE CONFIGURACIÓN

- *Terminal local :* V.24 9.600-8-N-1-sin control de flujo
- *Conector:* DB-9 hembra

INTERFACES WAN

- *Protocolos:* FRAME RELAY, X.25, PPP, SDLC, X.28
- *Interfaces:* Drivers insertables V.24 / V.35 / X.21 DTE/DCE
- *Nº Puertos:* 3
- *Velocidad:* 200 a 2048 Kbps
- *Conector:* DB-25 hembra

INTERFAZ LAN

- *Protocolos:* Ethernet (802.3) / Ethernet blue book
- *Velocidad:* 10 Mbps (10BaseT)/100 Mbps (100BaseT)
- *Conector:* RJ45 hembra

ALIMENTACIÓN AC

- *Tensión de entrada:* 100 – 240 V ~
- *Corriente de entrada:* 0.5- 1.0 A
- *Frecuencia de entrada:* 47-63 Hz

ALIMENTACIÓN DC

- *Tensión de entrada:* – 48 V
- *Corriente de entrada:* 1 A

DIMENSIONES Y PESO

- *Tipo:* Caja de sobremesa
- *Largo x Ancho x Alto:* 31.0 x 41.5 x 43.0 cm
- *Peso:* 3.5Kg

ESPECIFICACIONES AMBIENTALES

- *Temperatura ambiente:* Encendido: 5ºC a 55º C. Apagado: -20º C a 60º C
- *Humedad relativa:* Encendido: 8% a 85%. Apagado: 5% a 90%

CERTIFICACIONES

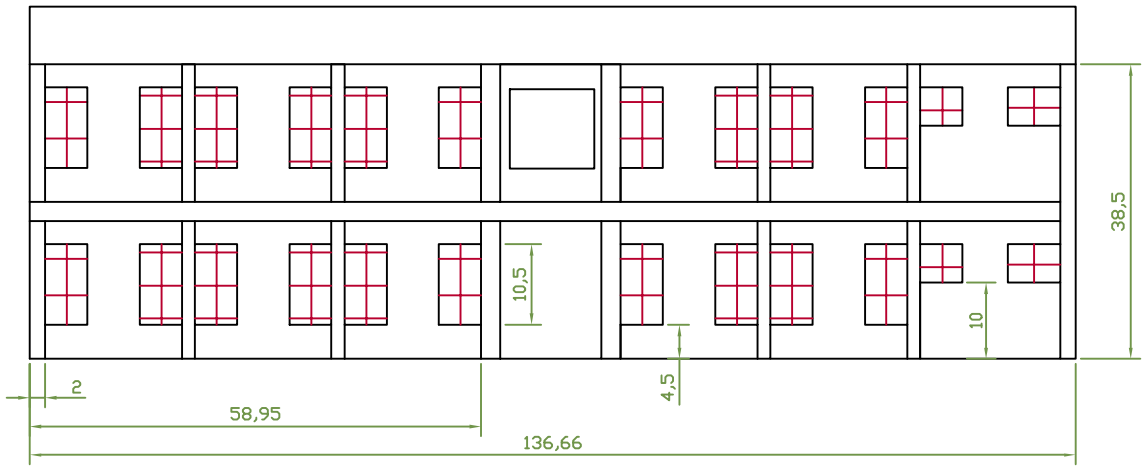
- *CE*

Telsec

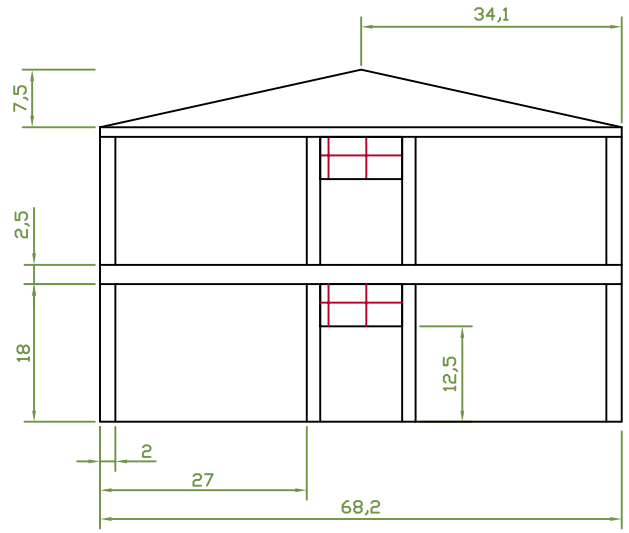
Tedat Security S.L.
Parque Tecnológico de Madrid
28760 – Tres Cantos
MADRID - ESPAÑA
TEL.: +34.918076565
FAX.: +34.918076566
www.teldat.es

Teldat Corp
1111 Brickell Avenue - Suite 1100
MIAMI, FLORIDA 33131 - EE.UU
TEL.: +1.305.3723480
TEL.: +1.866.4TELDAT
FAX : +1.305.5135209
www.teldatsecurity.com

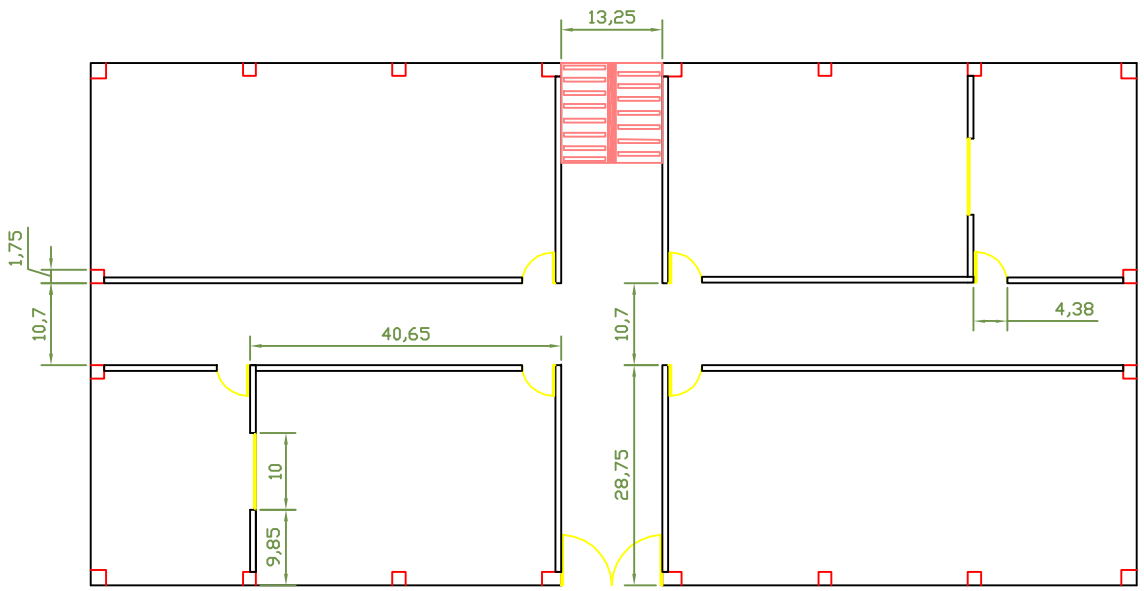
ANEXO 4



Vista Frontal

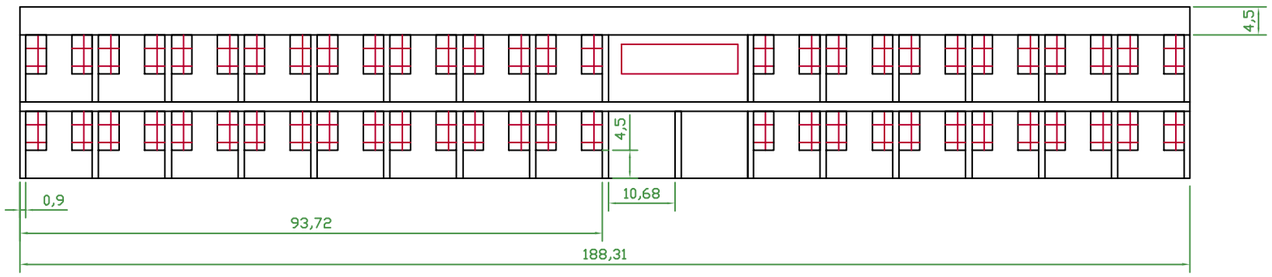


Vista Lateral

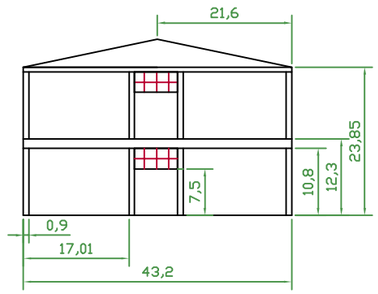


Vista Superior

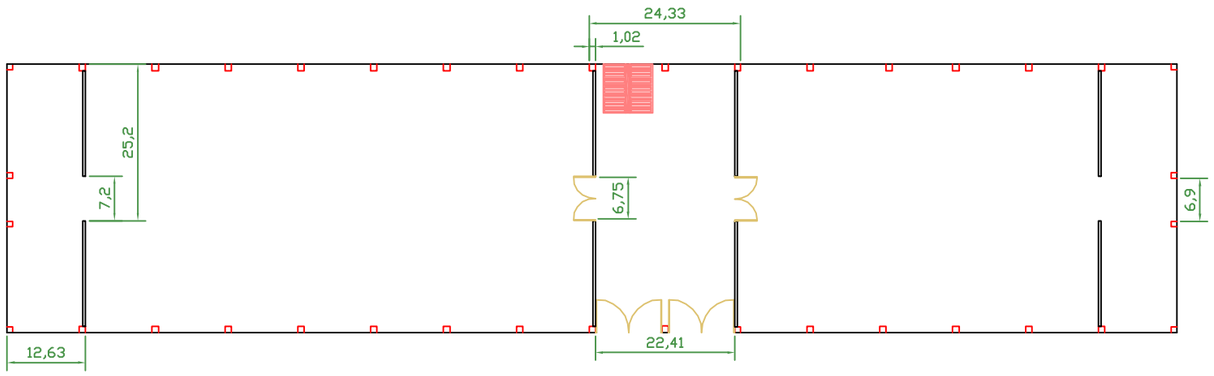
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Unidades: metros
COTAS COMANDO DE BRIGADA, GCB -32 Y GCB-33	Escala: 5 : 1
	N°Lámina: 01 / N° Hoja: 144



Vista Frontal

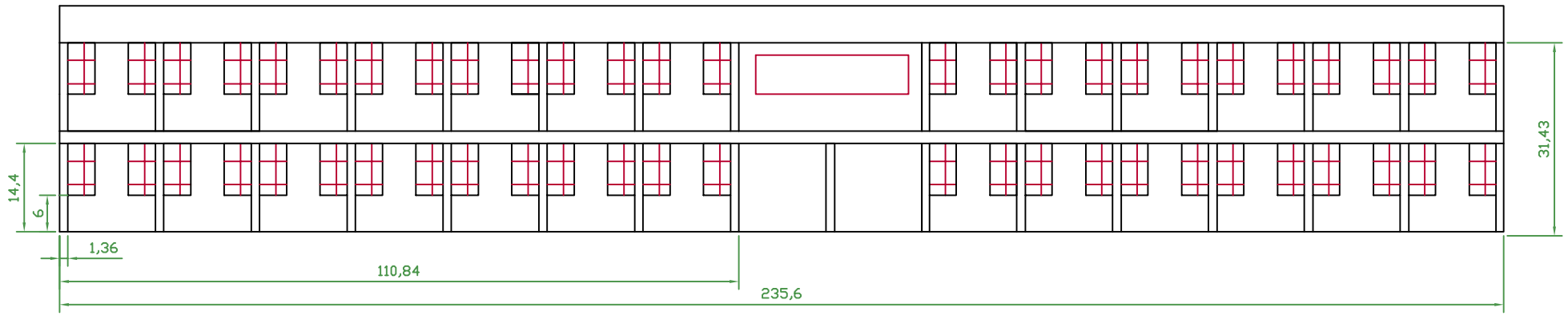


Vista Lateral

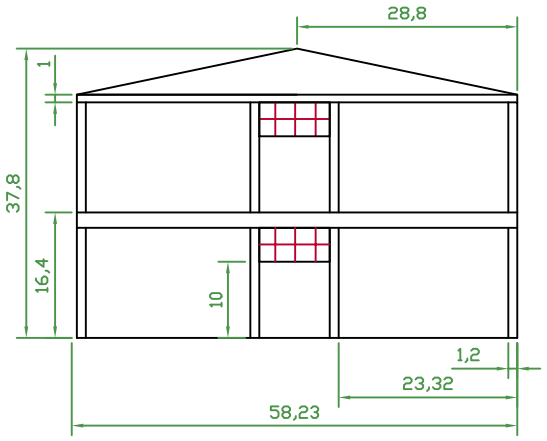


Vista Superior

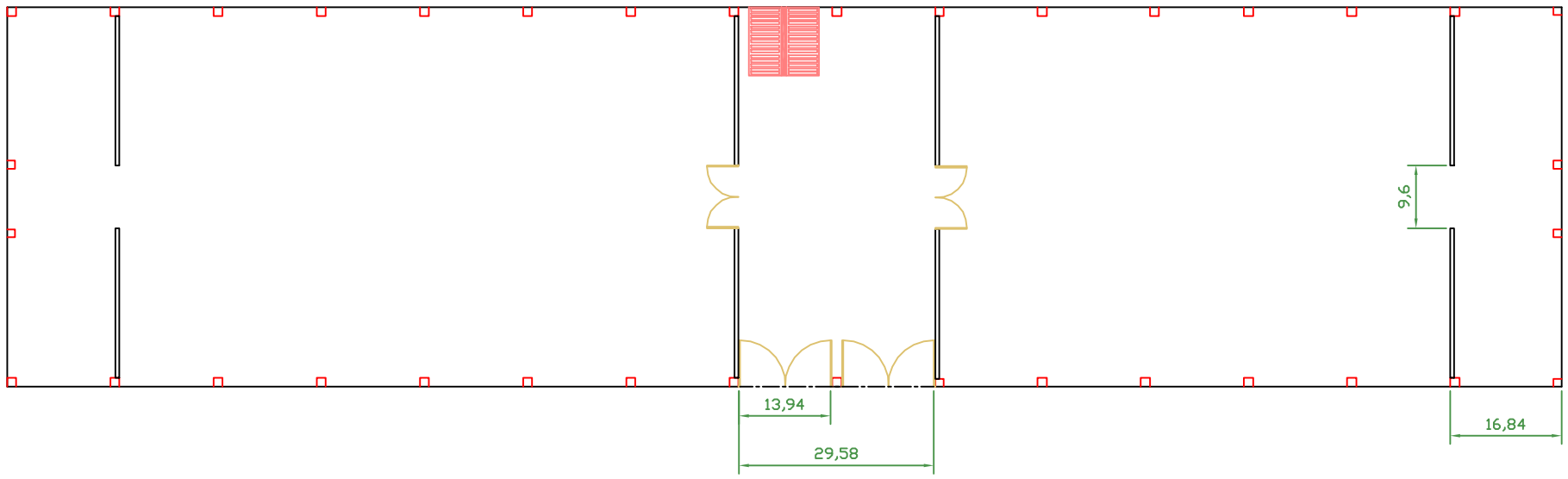
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Unidades : metros
COTAS DORMITORIOS **EPM** Y **GAA 12**	Escala: 3 : 1
	N° Lámina: 02 / N° Hoia: 145



Vista Frontal

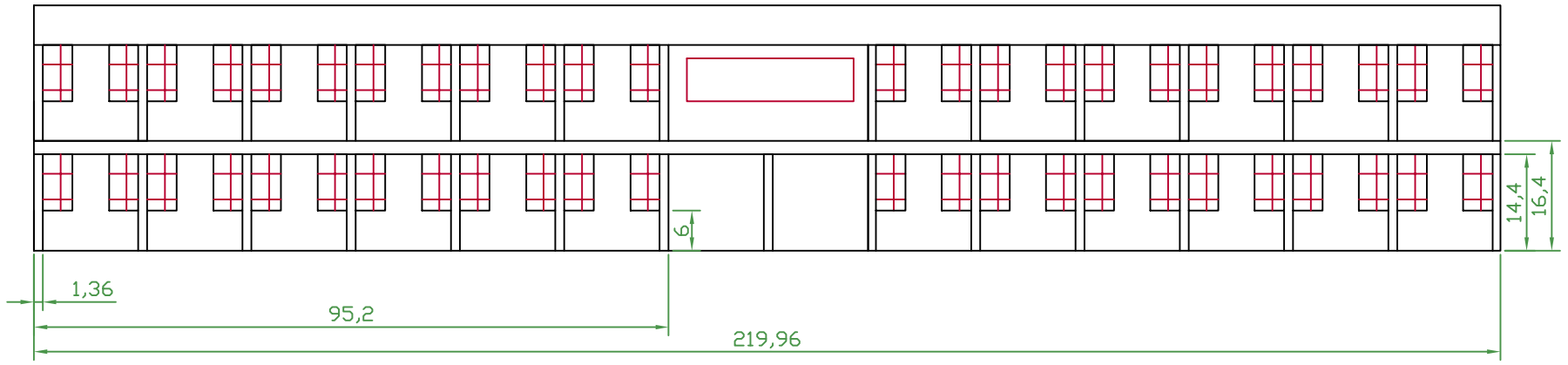


Vista Lateral

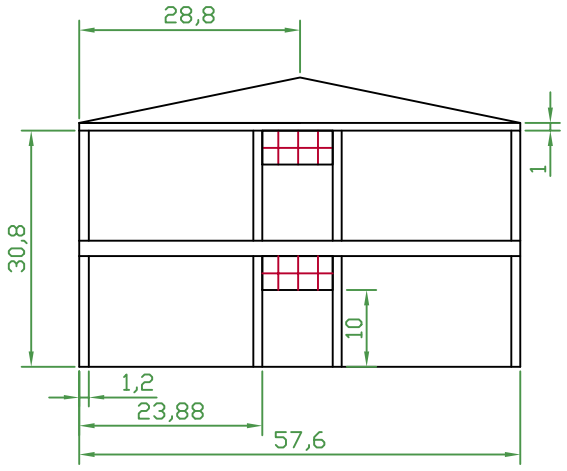


Vista Superior

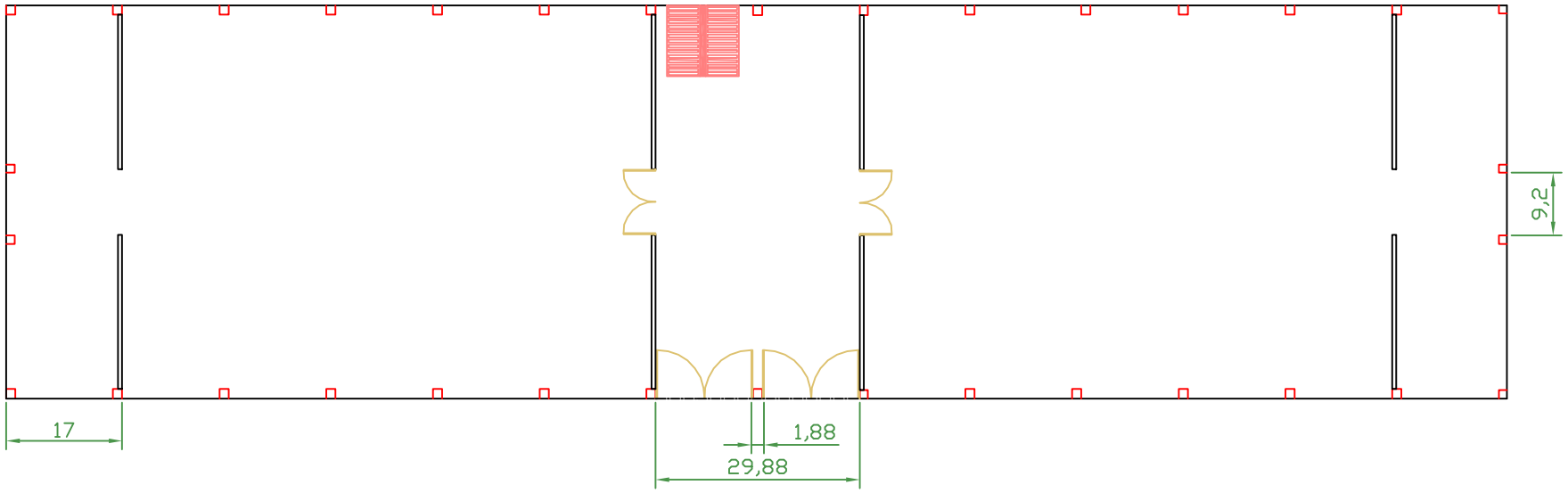
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Unidades : Metros
COTAS DORMITORIO ERB-11 EPLICACHIMA	Escala: 4 : 1
	N°Lámina: 03 / N°Hoja: 146



Vista Frontal

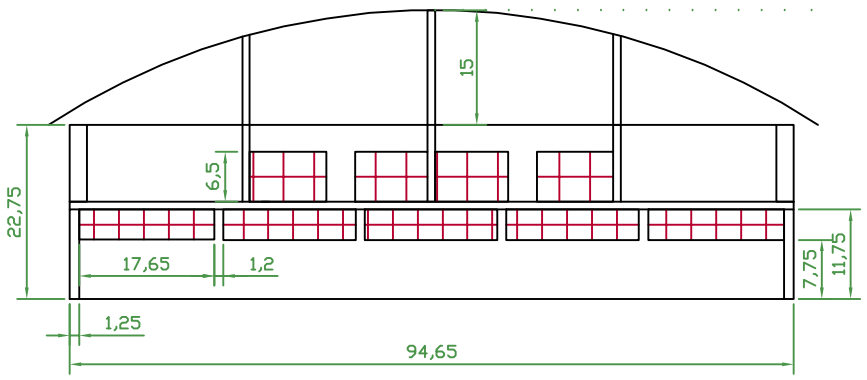


Vista Lateral

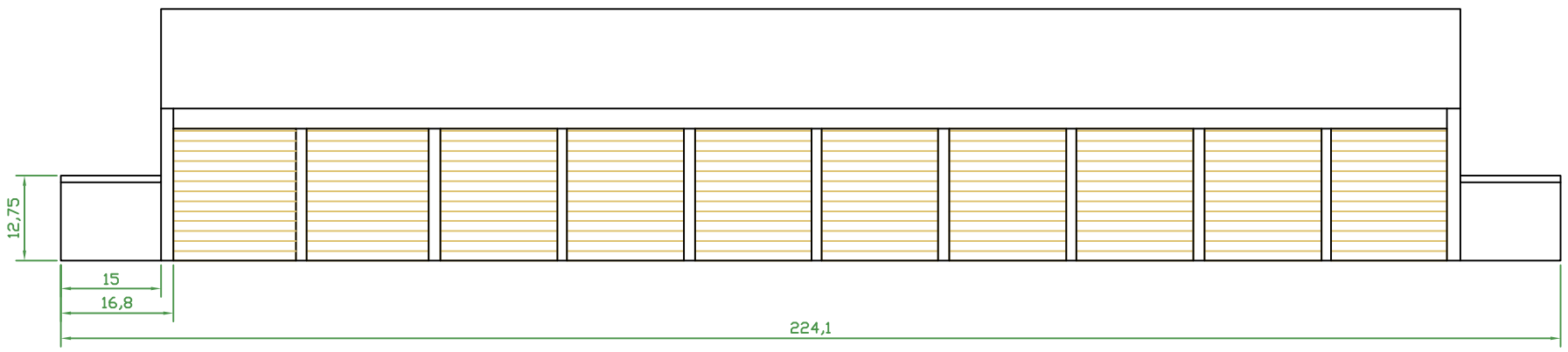


Vista Superior

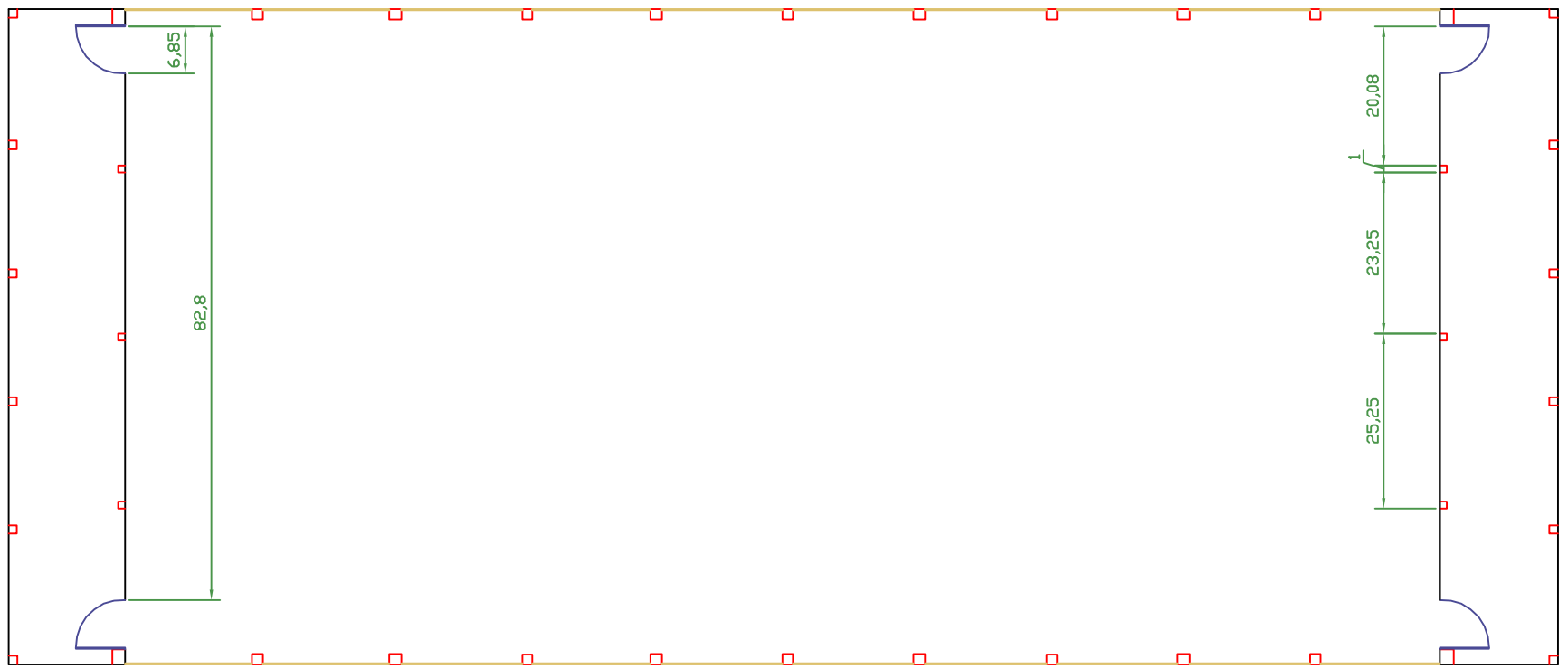
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Unidades: Metros
COTAS DORMITORIO GA-AP - 11 GCB - 31 GCB -32	Escala: 4 : 1
	N° Lámina: 04 / N° Hoja: 147



Vista Frontal

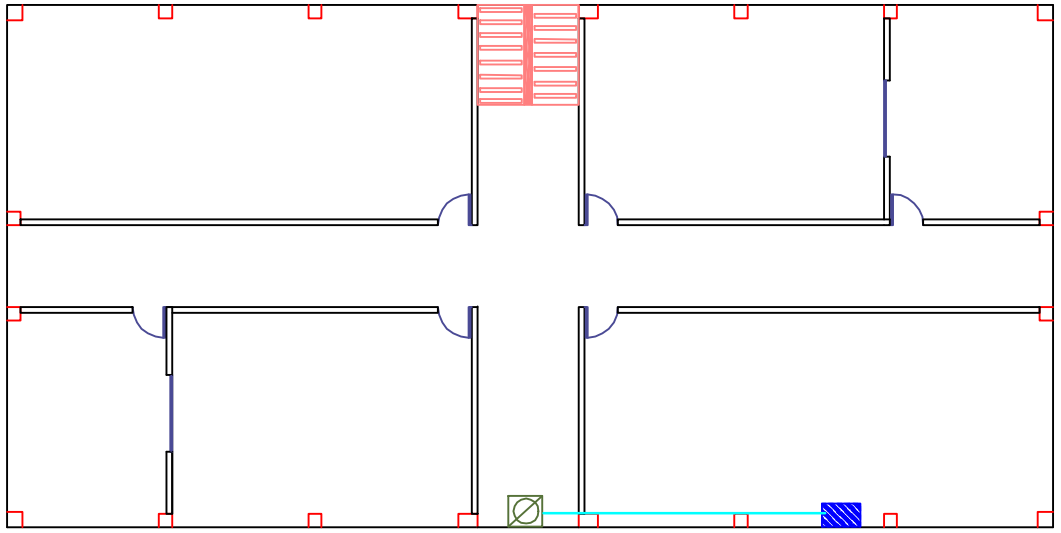


Vista Lateral

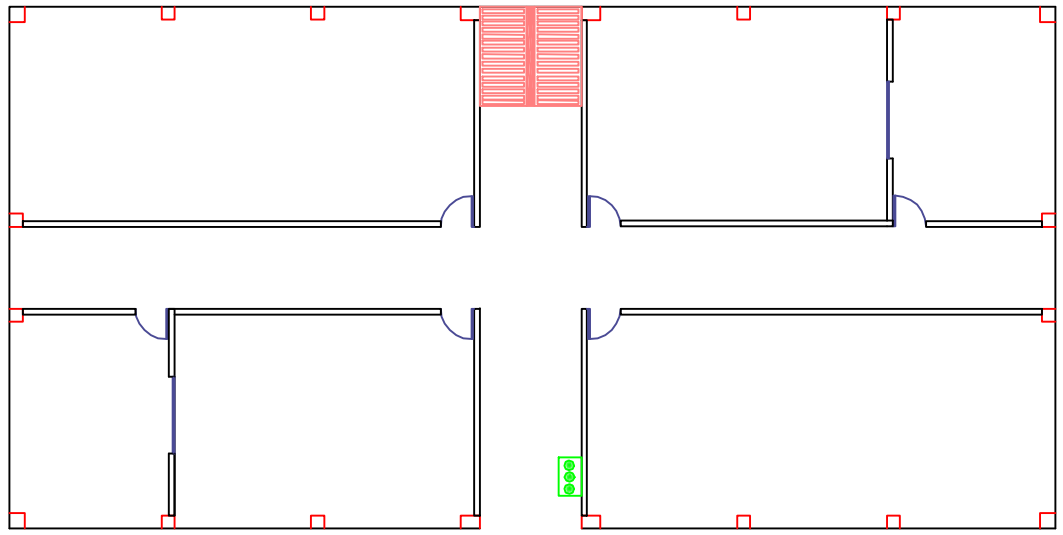


Vista Superior

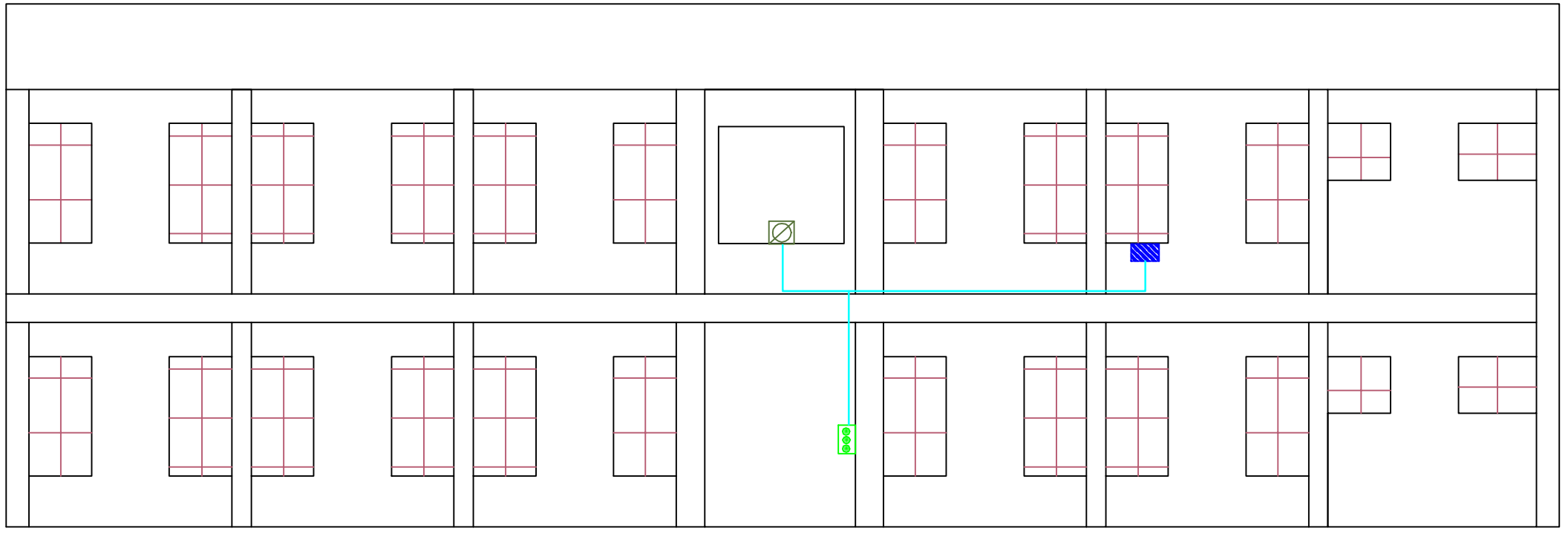
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	11 BCB "GALAPAGOS"
	Unidades : metros
COTAS HANGAR	Escala: 5 : 1
	N° Lámina: 05 / N° Hoja: 148



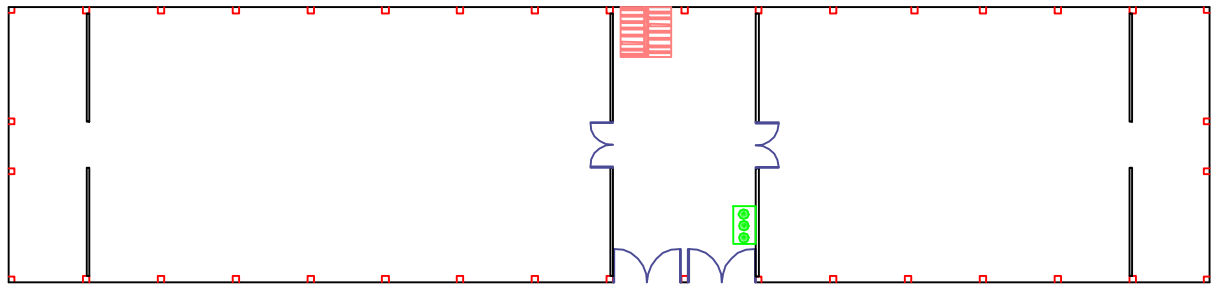
PRIMER PISO



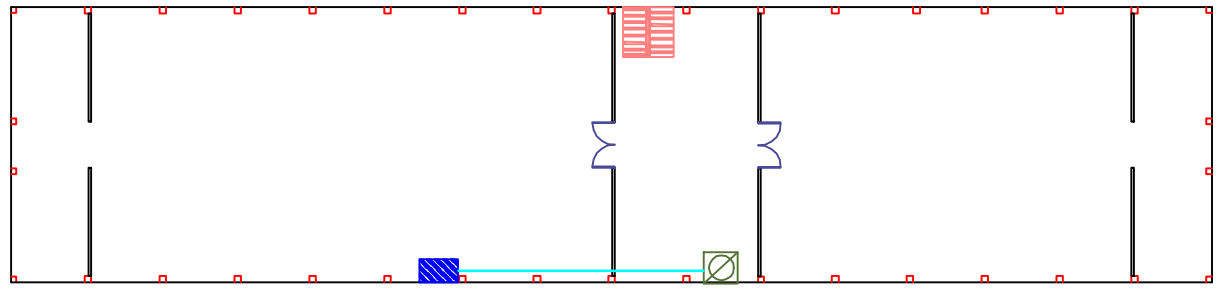
PLANTA BAJA



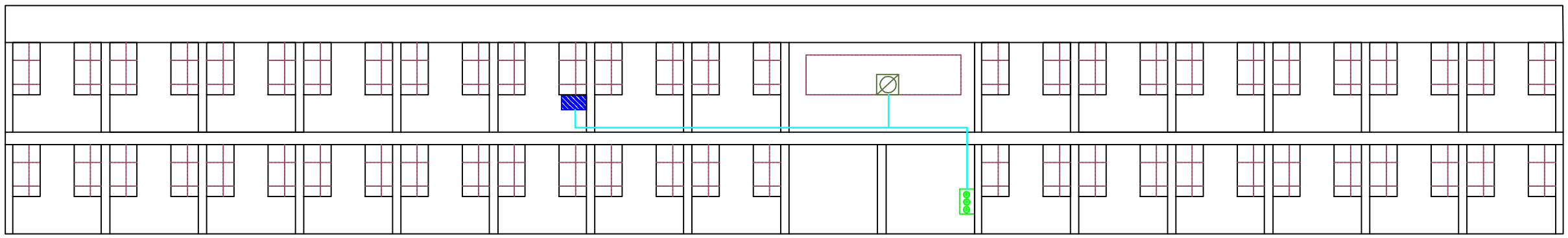
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
PANEL DE ALARMA COMANDO DE BRIGADA, GCB -32 Y GCB-33	Escala: 5 : 1
	N°Lámina: 06 / N° Hoja: 149



PLANTA BAJA

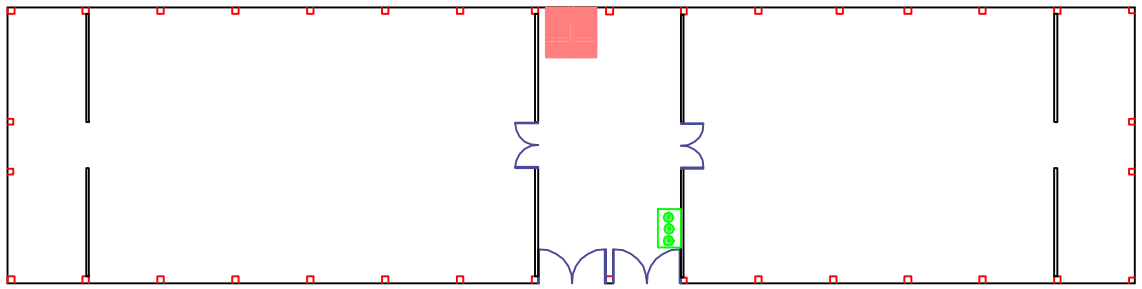


PRIMER PISO

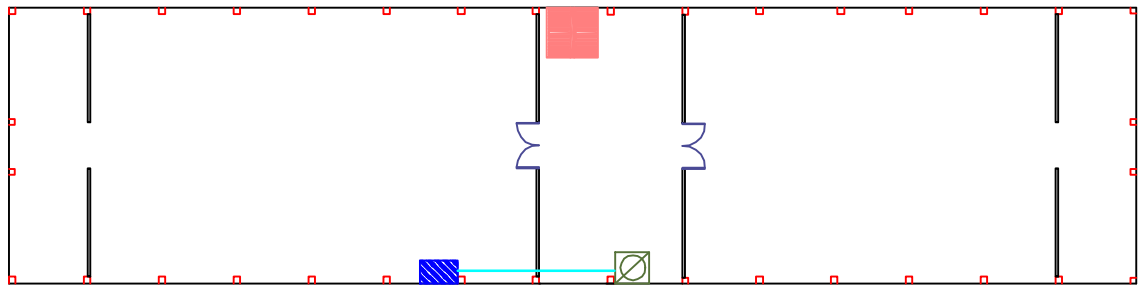


VISTA FRONTAL

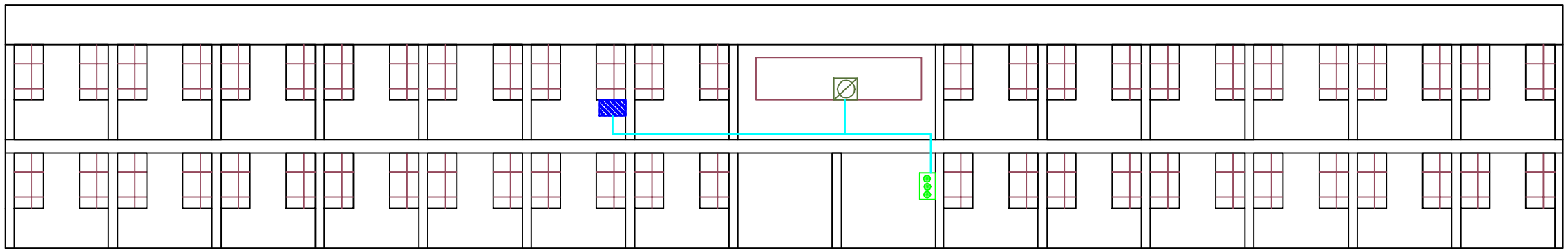
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
PANEL DE ALARMA DORMITORIOS **EPM** Y **GAA 12**	Escala: 2,5 : 1 5 : 1
	N° Lámina: 07 / N° Hoja: 150



PLANTA BAJA

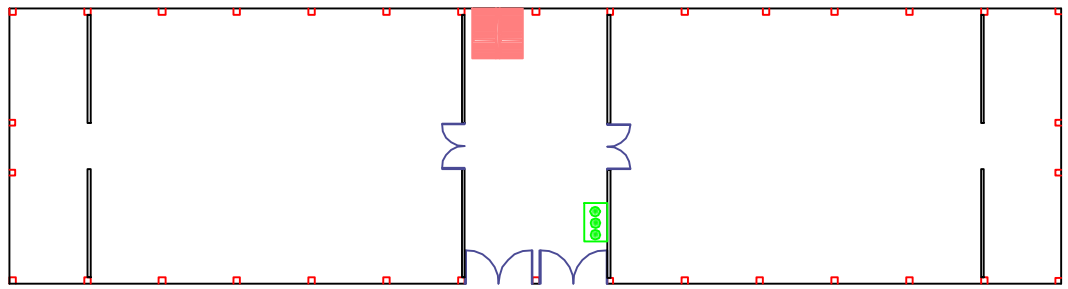


PRIMER PISO

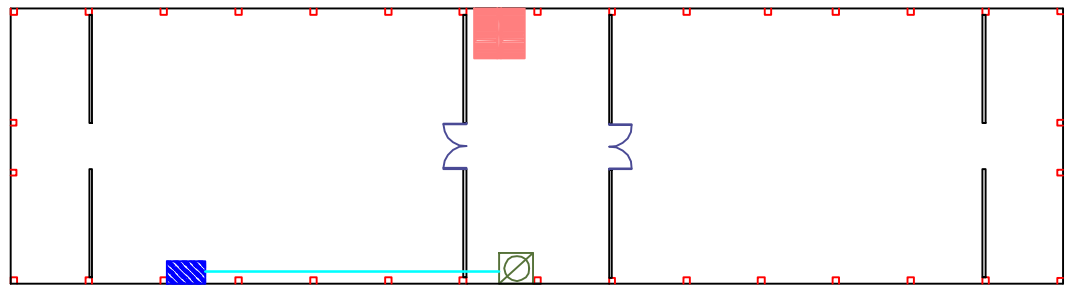


VISTA FRONTAL

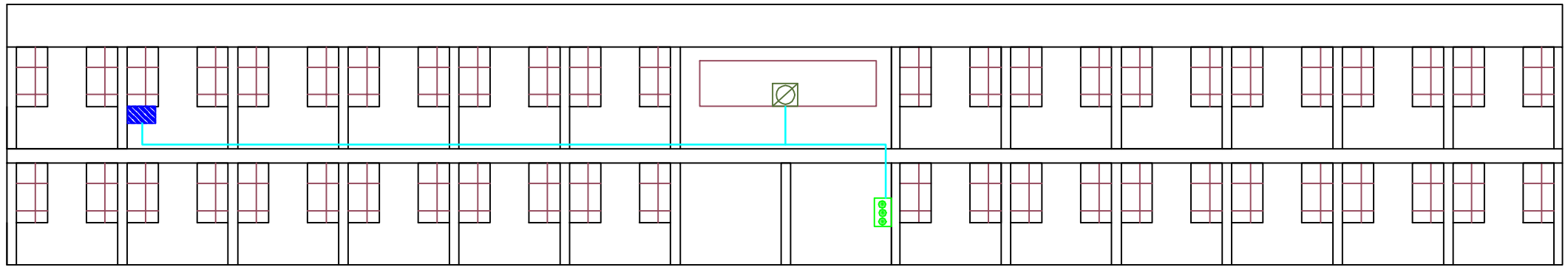
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
PANEL DE ALARMA DORMITORIO ERB-11 EPLICACHIMA	Escala: 5 : 1 2,5 . 1
	N° Lámina: 08 / N° Hoja: 151



PLANTA BAJA

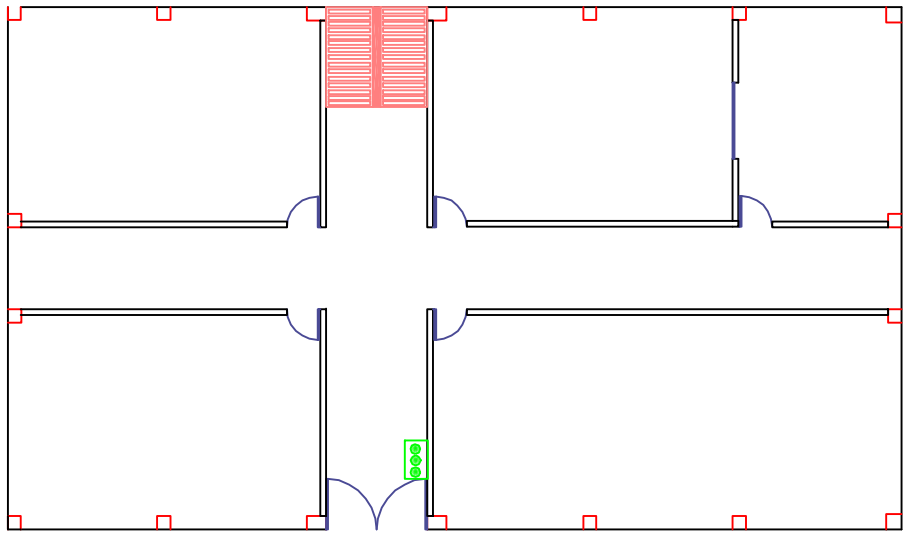


PRIMER PISO

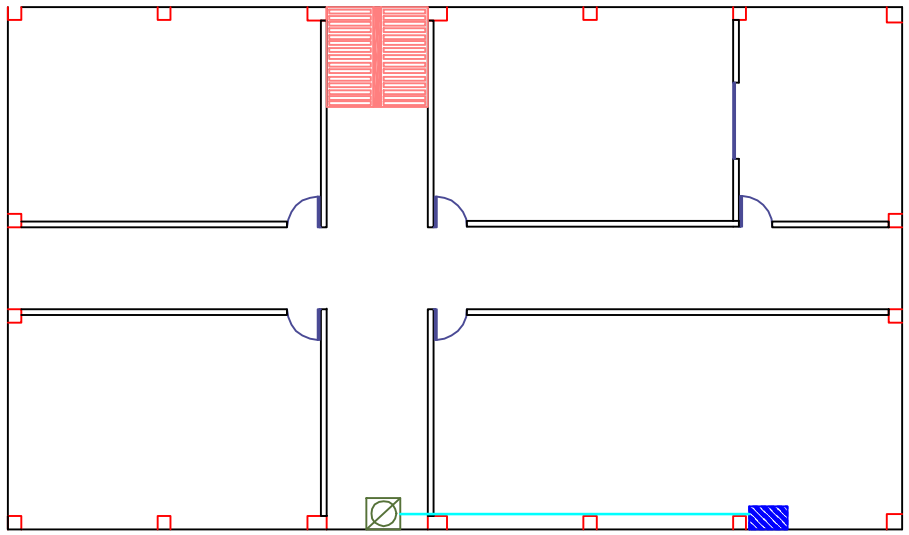


VISTA FRONTAL

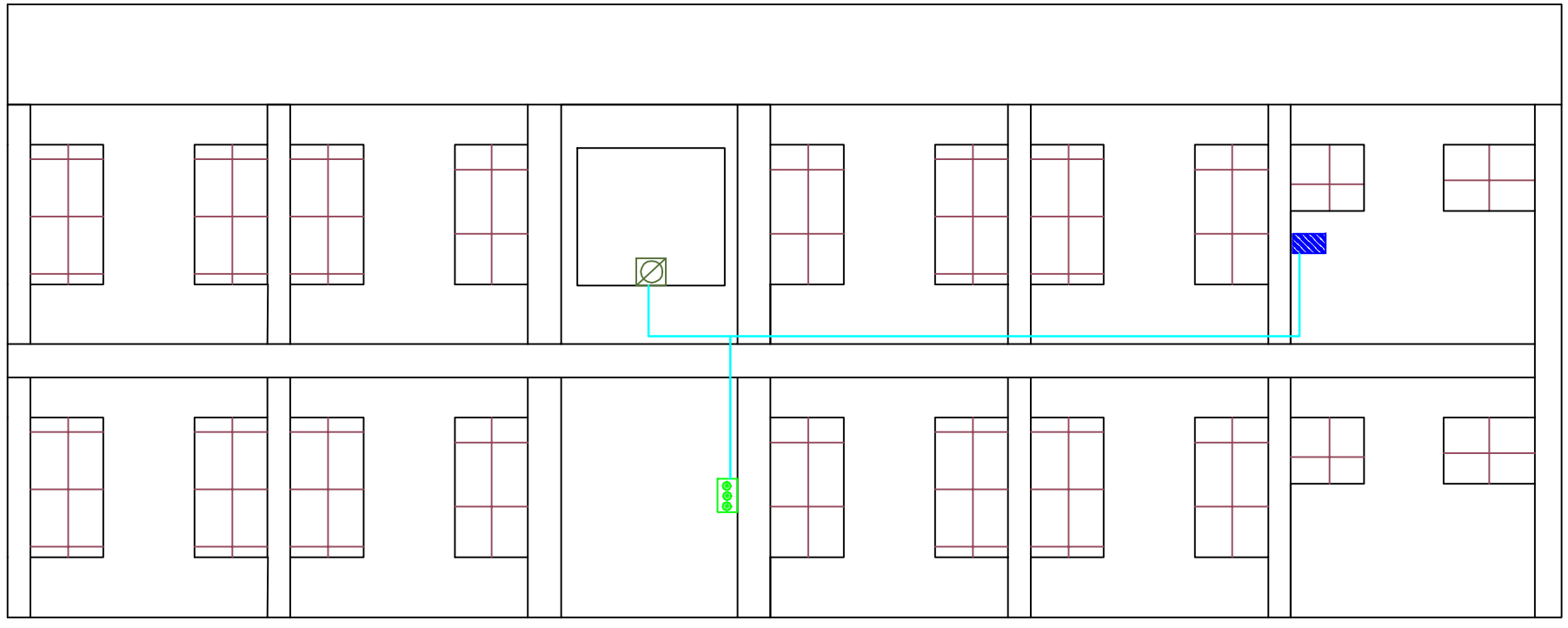
U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
PANEL DE ALARMA DORMITORIO GCB - 31, GCB - 32 y GAAP - 11	Escala: 5 : 1 2,5 . 1
	N° Lámina: 09 / N° Hoja: 152



PLANTA BAJA

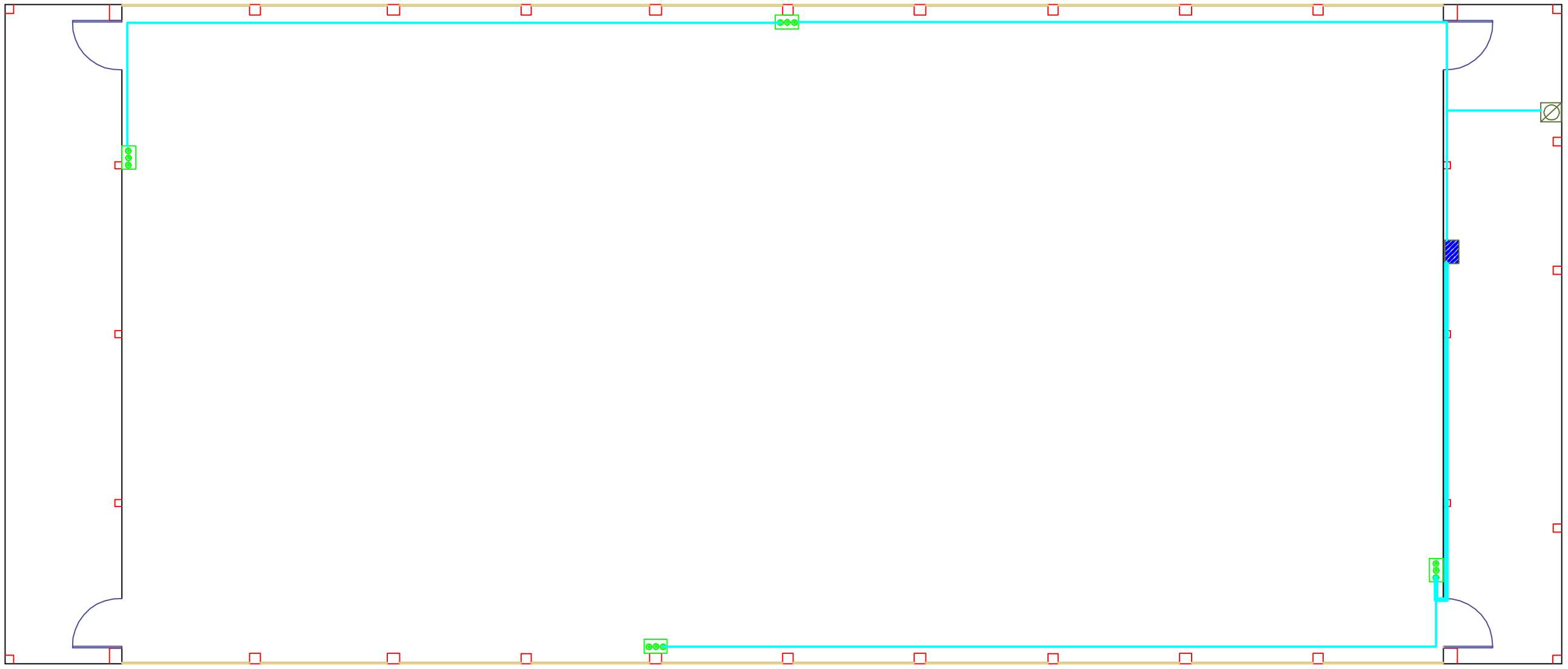


PRIMER PISO



VISTA FRONTAL

U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
PANEL DE ALARMA ESCABLIN	Escala: 5 : 1 10 : 1
	N° Lámina: 10 / N° Hoja: 153



U.T.A.
INGENIERIA ELECTRONICA Y COMUNICACIONES

PANEL DE ALARMA
HANGARES 1 y 3

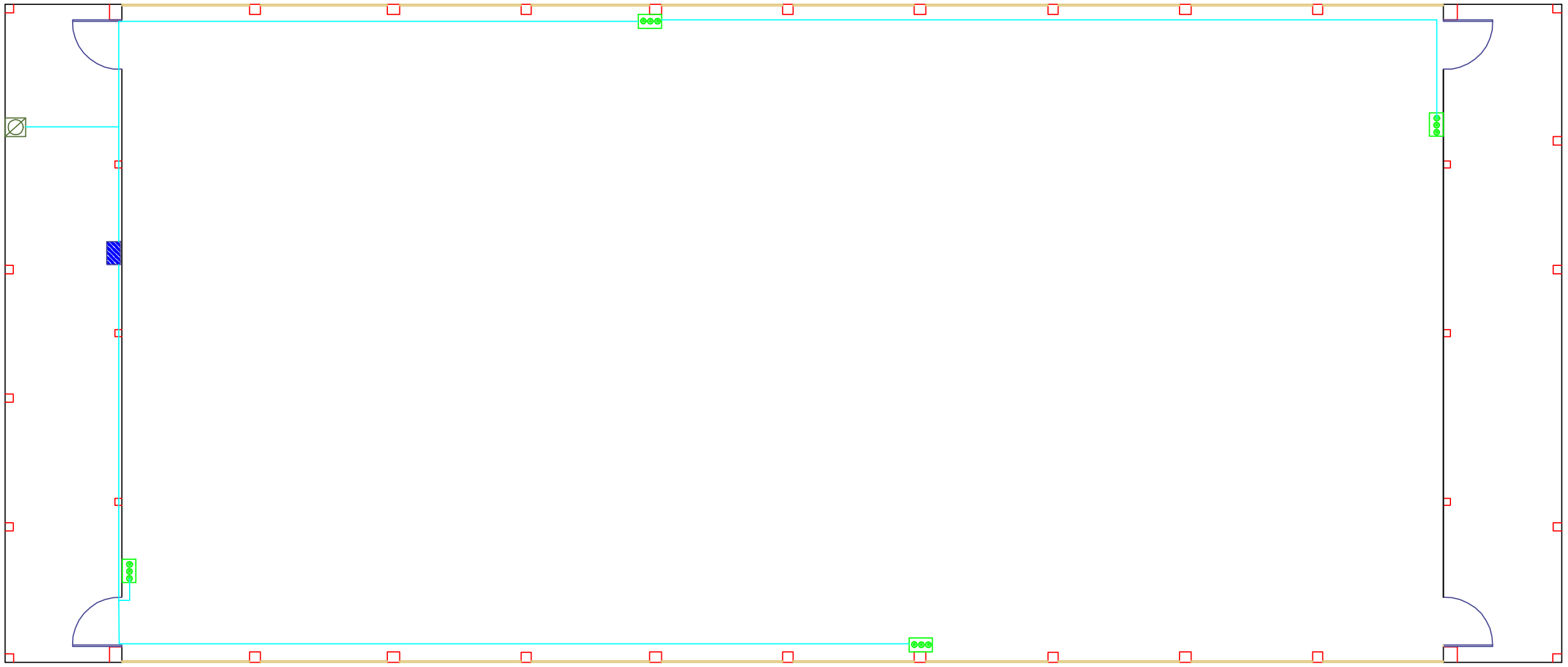
11 BCB "GALAPAGOS"

Fernando Lasluisa

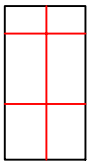
Escala: 10 : 1

N° Lámina: 11

N° Hoja: 154



U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
BOTONERAS Y PANEL DE ALARMA HANGAR 2	Escala: 10 : 1
	N° Lámina: 12 | N°Hoja: 155

	Ventana con malla de protección
	Gradas tipo tijeras
	Puerta de madera
	Puerta corredisa de crisal
	Puerta doble de cristal
	Puerta Lanfort
	Panel de alarma
	Sirena
	Pulsadores de pánico
	Canaleta
	Columna

U.T.A. INGENIERIA ELECTRONICA Y COMUNICACIONES	**11 BCB "GALAPAGOS"**
	Fernando Lasluisa
SIMBOLOGÍA	Escala:
	N° Lámina: 13 / N° Hoja: 156

BIBLIOGRAFÍA

- ✓ **ALTA VELOCIDAD Y CALIDAD DE SERVICIOS EN REDES IP.** GARCIA T. Jesús; RAYA J. Luis; RAYA V. Rodrigo.
- ✓ **TCP / IP.** RAY JOHN
- ✓ **REDES Y SERVICIOS DE BANDA ANCHA.** HUIDROVO M. Josi; ROLAND David.

Webgrafía

- ✓ http://www.energuia.com/es/productos4.aspx?ID=2465
- ✓ http://casadomo.com/noticiasDetalle.aspx?id=6808&c=1
- ✓ http://nt.paginasamarillas.es/scripts/mundo/mundo.noticia.asp?seccion=D_SE&id=706
- ✓ http://www.hogaryconstruccion.com.ar/index.php?newid=101717
- ✓ www.jungiberica.es/download/JUNG_CENTRAL_ALARMAS.pdf http://softdemonitoreo.com/info/files/Monitoreo_Ip_1.pdf
- ✓ http://www.jandei.com/sistemas-anti-robo-titania-960-tcp-ip/5-49-6-49.htm
- ✓ www.ethernetalliance.org/technology/white_papers/A_Bit_of_History.p-
- ✓ http://www.intel.com/standards/case/case_ethernet.htm
- ✓ http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/easyip2.pdf
- ✓ http://www.teldatsecurity.com/Pages/Product_Pages/Communication_modules/Spanish/Prod%20bottom%20frame%20MIP%20esp.htm
- ✓ http://www.teldatsecurity.com/Pages/Product_Pages/Communication_modules/Spanish/Prod%20bottom%20frame%20VisorALARM%20esp.htm