UTEG

UNIVERSIDAD TECNOLOGICA EMPRESARIAL DE GUAYAQUIL

TESIS

En opción al Título de:

Ingeniería en Gestión Empresarial con Mención Gestión en Informática

Título de la Tesis:

Estudio de Factibilidad y Diseño de la Infraestructura de Red Informática en el Nuevo Campus de la Universidad Tecnológica Empresarial de Guayaquil (U.T.E.G.)

AUTORES:

Andrea Estefanía Pages Camacho

Gustavo Andrés Montalvo Espinosa

TUTOR:

Ing. Edison Toala

GUAYAQUIL - ECUADOR

Octubre del 2007

DEDICATORIA

A mis padres que con amor y sacrificio, supieron motivarme moral y materialmente para culminar mis estudios superiores obteniendo un titulo mas y así asegurarme una vida digna y clara en el futuro.

A mis queridos profesores quienes con amor y sabiduría, depositaron en mi todo su apostolado lo cual recibí las mejores enseñanzas.

A mis hermanas y hermano, que aportaron con la paciencia, el amor y esos detalles que los llevare dentro de mi corazón.

A mi compañero de tesis por el apoyo en estos 5 años de estudios, en los cuales nos hemos apoyado mutuamente.

Y a todos en general que de una u otra manera me han dado ese aliento para que no desmaye y siga adelante en esta ardua tarea.Mil gracias.

Andrea

A mi padre por su apoyo durante todos estos años de preparación en mis estudios.

A mí querida madre por su constante apoyo y presión para poder culminar mis estudios y ser la luz que me guía.

A mi hermano por su esfuerzo incondicional en apoyarme en los momentos difíciles.

A mi compañera de tesis por creer en mí y ser la persona que hizo posible terminar esta etapa de mi vida.

Y a todas aquellas personas que colaboraron con un granito de arena para ayudarme.

Gustavo Andrés

AGRADECIMIENTO

Ante todo a Dios por guiar nuestro camino y ayudarnos a culminar una etapa más en nuestras vidas.

A nuestros padres por depositar su confianza y constante apoyo.

Agradecemos al Ing. Cesar Arrieta de la empresa Transferdatos S.A., por su amistad sincera y desinteresada, por ser una gran persona, un buen ejemplo a seguir, por la dedicación y el tiempo que nos dio para que la realización y culminación de este proyecto se haya llevado a cabo.

Al Ing. Rubén Carrillo por su gran apoyo e interés en ayudarnos en el desarrollo final del proyecto.

A los miembros del jurado asignados para la evaluación de este proyecto (Ing. Xavier Mosquera, Ing. Gianpaolo Lauri e Ing. Jose Townsend), les estamos agradecidos por las recomendaciones y observaciones realizadas en la Predefensa para ser de este un mejor proyecto.

Agradecemos al Ing. Edison Toala por su desempeño como tutor en este proyecto.

Y por ultimo pero no menos importante a todas aquellas personas que colaboraron con su granito de arena en el transcurso del desarrollo del proyecto.

Muchas Gracias

RESUMEN EJECUTIVO

El tema propuesto se basa en el estudio de factibilidad para el diseño de la infraestructura de red informática en el nuevo campus de la universidad, en su análisis con la finalidad de disminuir costos en la implementación y en el crecimiento de la red.

El análisis empieza con los antecedentes de la universidad, su breve reseña histórica, misión, visión, sus principios institucionales, valores y metodología de enseñanza.

Una vez culminado los antecedentes de la universidad, se procede a realizar un estudio de las redes, sus características, tipos de redes, medios de transmisión ya sean alámbricas e inalámbricas y equipos de comunicación.

Se estudia y se hará referencia sobre las arquitecturas, los protocolos que se manejan en las redes con sus respectivas características, de la Internet como un medio informativo y de transmisión de datos.

En lo que respecta a seguridad informática tanto la seguridad física como la seguridad lógica serán revisadas e investigadas para generar las correspondientes recomendaciones para el diseño del proyecto.

A continuación se procederá a identificar los recursos informáticos con los que cuenta actualmente la universidad con el fin de conocer las necesidades actuales y así poder aplicarlas en la red del nuevo campus.

Una vez concluido con estos análisis se procederá a la identificación de los requerimientos de comunicación del nuevo campus donde se colocara en forma adecuada y en puntos estratégicos los equipos de comunicación para dar una mayor eficiencia y eficacia a la red.

A continuación se procederá con el diseño de las diversas redes que brindaran cobertura al nuevo campus universitario de la UTEG, incluyendo la tecnología más conveniente para brindar las mejores soluciones a los requerimientos identificados en las etapas previas.

El análisis de factibilidad es uno de los principales objetivos, se deberá analizar los costos por la inversión en los equipos tecnológicos que se van a utilizar para diseñar dicho proyecto y el tipo de pago que se va a realizar, ya sea de contado o financiado.

SUMMARY

The proposed subject is about the study of the faculty to the design of the network infrastructure at the new campus of the college, anything it with the objective to reduce costs in the introduction and in the growth of the network.

The analysis begins with the antecedents of the college, its brief historical outline, mission, vision, their institutional sources, their values and their teaching methodology.

Once that it has been finished the antecedents of the college, it proceeds to realize a study of the network, their characteristics, network types, media transmission being wire or wireless and communication equipments.

It will be studied and it will make reference to the architectures, the protocols which are managed and the network wife their own characteristics, about the internet like an info media and data transmission.

About the computer science security as physical as logical they will be reviewed and researched to make the corresponded recommendations to the project design.

To continue, the procedure will be to identify the computer science resources which actually the college has, with the proposal to know the actual needs and to apply them on the network at the new campus.

Once that these analysis are finished, the procedure will be to identify the communication request of the new campus where will be set on, onto a property way and onto strategic points, the communication media to give a mayor efficiency and efficacy on the network.

At next, it will proceed with the design of several networks which will offer a high covering to the new college campus of UTEG, including the most convenient technology to offer the best solutions to the identified stages.

The faculty analysis is one of the prime objectives, it will be analyzed the costs about the investment on the technological equipments which will be used to the mentioned project design and about the payment type that will be done, it can be cash or financed.

Objetivo General

Realizar el estudio de factibilidad y el diseño de la infraestructura de Red informática para el nuevo campus de la UTEG

Objetivos Específicos

- Proponer un diseño optimo de Red basado en Tecnología CISCO
- Determinar los costos de implementación de esta Red, incluido el crecimiento estimado.
- Realizar el análisis de factibilidad del Proyecto
- Diseñar un esquema de direccionamiento IP para red de voz y datos del nuevo campus de la UTEG
- Diseñar políticas de seguridad de VLANs y ACLs

Hipótesis

La realización de un correcto estudio de factibilidad y el análisis de los recursos tecnológicos para el diseño de una red informática nos permite la disminución de gastos innecesarios en su posterior implementación

Alcances

- El diseño de Red informática se realizara para su posterior implementación en el nuevo campus de la UTEG ubicado vía a la Costa
- El proyecto incluye diseño de Red y análisis de factibilidad, sin llegar a prototipos, implementación ni pruebas
- El diseño de red incluirá la Red administrativa y la Red de estudiantes

INDICE DE LOS CAPITULOS

CAPITULO 1: UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL (U.T.E.G.)

CAPITULO 2: ESTUDIO TÉCNICO DE LAS REDES

CAPITULO 3: ARQUITECTURA Y PROTOCOLOS DE REDES

CAPITULO 6: ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED INFORMÀTICA DE LA U.T.E.G.

CAPITULO 7: IDENTIFICACIÓN DE LOS REQUERIMIENTOS DE COMUNICACIÓN DEL NUEVO CAMPUS UNIVERSITARIO

CAPITULO 8: DISEÑO DE LA RED INFORMATICA DEL NUEVO CAMPUS DE LA U.T.E.G

CAPITULO 9: ANÁLISIS ECONOMICO

CAPITULO 10: EVALUACIÓN INTEGRAL DEL PROYECTO

INDICE DE LOS GRAFICOS

INDICE DE LAS TABLAS

CAPITULO 1: UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL (U.T.E.G.)

1.1. Antecedentes

1.1.1. Reseña Histórica

La Universidad Tecnológica Empresarial de Guayaquil UTEG fue creada, por iniciativa de la Cámara de Comercio de Guayaquil, mediante la ley 2000 - 50 la misma que fue aprobada por el H. Congreso Nacional, sancionada por el Presidente Constitucional de la República, Dr. Gustavo Noboa Bejarano, y publicada en el Registro Oficial el 31 de enero del 2000, con la finalidad de ofrecer estudios en carreras superiores de tercer nivel. La idea y los esfuerzos para lograrlo fueron impulsados por el señor Joaquín Zevallos Macchiavello presidente de la Cámara de Comercio de Guayaquil. Su primera Rectora fue la doctora Genoveva Zavala de Mayer y su actual Rector es el abogado Marcelo Santos Vera.

La Cámara de Comercio de Guayaquil había iniciado su actividad educativa en 1984 con el Instituto de Desarrollo Profesional (IDEPRO), financiado por la AID .El éxito alcanzado ha permitido que dicha institución continúe hasta la fecha con seminarios y cursos de capacitación dictados a un promedio de cuatro mil personas al año.

El 6 de marzo de 1995 se fundó el Instituto Tecnológico de Comercio (INTESCO) con la finalidad de formar técnicos titulados en administración, capaces de incorporarse al siglo XXI según las exigencias de nueva economía globalizada.

Importante puntal de crecimiento del INTESCO fue el convenio con la Cámara de Comercio de la ciudad de Sherbrooke, Québec, Canadá, por medio del cual se ofrecía adiestramiento técnico a los profesores de la institución, al mismo tiempo que permitía establecer contactos comerciales entre empresas canadienses y ecuatorianas.

En 1997, se graduó la primera promoción de técnicos superiores en las especializaciones de finanzas, marketing y comercio exterior. En 1998 egresó la primera promoción de tecnólogos.

Desde enero del año 2000 la UTEG ha crecido en número de alumnos y niveles académicos, y ha conquistado la confianza y el respeto de la comunidad, proyectándose al futuro con optimismo y liderazgo.

1.2. Misión

La Universidad Tecnológica Empresarial de Guayaquil UTEG es una universidad privada, abierta a todas las corrientes de pensamiento, cuya función social es la formación de profesionales, la investigación científica y la innovación tecnológica, a partir de un modelo de gestión universitaria que potencia el aprendizaje por problemas, la realización de proyectos de creación y una constante vinculación entre la teoría y la práctica, sustentando valores éticos y morales, con un fuerte compromiso hacia la comunidad, la realidad del entorno, la defensa de los derechos humanos, la democracia y la paz.

1.3. Visión

La Universidad Tecnológica Empresarial de Guayaquil UTEG, tiene como objetivo ser la universidad líder en la formación profesional de los empresarios del globalizado mundo de hoy, a base del ejercicio simultáneo de la docencia, la investigación y la práctica laboral en escenarios reales, contribuyendo al desarrollo socioeconómico del país, presente y futuro.

1.4. Principios Institucionales

Formar profesionales con mentalidad proactiva, que confirmen los valores e ideales de nacionalidad, justicia social, democracia, paz, solidaridad y defensa de los derechos humanos.
Estudiar, analizar y comparar la realidad regional, del país y del mundo, identificando los problemas para encontrar soluciones desde una perspectiva científica y humana.
Promover la interacción entre la universidad y el sector externo, a través de la asistencia y el apoyo a las iniciativas estudiantiles, empresariales y culturales.

1.5. Valores Institucionales

- Importancia de la Nacionalidad
- Justicia Social
- Fomento de la Paz
- Defensa de la Democracia
- Defensa de los Derechos Humanos.
- Honestidad
- Orden

1.6. Metodología de enseñanza

El método de enseñanza utilizado por la UTEG está diseñado en un 40% por instrucción teórica y un 60% por ejecución práctica. La malla curricular de cada carrera hace énfasis en la investigación, planificación y desarrollo de proyectos y casos, para proponer soluciones y mejoras a problemas reales y actuales. Esto familiariza al estudiante con su campo de acción profesional y lo prepara para el mundo laboral y para la vida.

CAPITULO 2: ESTUDIO TÉCNICO DE LAS REDES

En este capitulo se va a analizar el estudio técnico de la redes, sus objetivos, su clasificación, sus características y sus principales beneficios en el mundo actual.

2.1. Concepto de Red.

Una red en general es un conjunto de dispositivos de red (pc, impresoras, etc.) interconectados físicamente, ya sea vía alámbrica o vía inalámbrica que comparten recursos y que se comunican entre sí a través de reglas o protocolos de comunicación.

2.2. Objetivos y beneficios

Sus objetivos y beneficios son muy evidentes y se hacen prevalentes hoy en día a través de "fenómeno" de la Internet, debido a los beneficios que esta da, el poder tener acceso a variada información en todo el mundo, amplia el campo por explorar a altos niveles de aprendizaje, teniendo a la mano en minutos información variada e importante para el investigador en si.

Se puede afirmar de forma categórica, que el mundo se detiene cuando las Redes se detienen sea esto por fallas propias, ataques de seguridad, congestionamiento de tráfico, etc.

Sus beneficios incluyen ahorro en costos de producción, distribución y ventas de bienes y servicios, principalmente en las siguientes actividades:

- INDUSTRIA:
  - Líneas de producción automáticas
  - Sistemas automáticos de abastecimiento de insumos

- COMERCIO:
  - Comercio Electrónico
  - Reducción del costo de inventarios

- FINANZAS Y BANCA:
  - Sistemas por VPN
  - Sistemas bancarios virtuales, banca en línea.

- AHORRO EN COMUNICACIONES

  - INTERNA:
    - E – Mail, GroupWare, etc.
    - Tecnología CTI (Computer Telephony Integration)
    - Intranets

  - EXTERNA:
    - Uso de Internet como medio de transmisión de Datos.
    - Telefonía IP y Telefonía a través de Internet.
    - Extranets

- AHORROS EN TODOS LOS ASPECTOS ADMINISTRATIVOS DE LA EMPRESA

  - ADMINISTRACIÓN: Facilidades para la recopilación y acceso a información actualizada sobre el estado de la empresa.

  - ATENCIÓN AL CLIENTE: A través de tecnologías como Workflow, se mejora en forma espectacular el nivel de servicios dado a clientes.

  - CAPACITACION INTERNA: Intranets, Videoconferencias, etc...

2.3. Características de las Redes

Sus características varían de acuerdo a los siguientes factores:

- NUMERO DE DISPOSITIVOS ENLAZADOS:
  - Caso más simple : 2 computadoras interconectados
  - Caso más complejo: La Internet

- ALCANCE GEOGRÁFICO:
  - Red de área local (LAN)
  - Red de área metropolitanas (MAN)
  - Red de área extensa (WAN y redes globales)

- MEDIOS FISICOS DE TRANSMISIÓN DE REDES:
  - Alámbricos (Cobre, Fibra óptica, etc.)
  - Inalámbricos (Radio, Satélite, etc.)

- ACCESIBILIDAD DE LA RED:
  - Redes Privadas: Pertenecen a una sola empresa o grupo
  - Redes Públicas: Libre acceso a todo quien pueda pagar la tarifa de uso (Ej.: Redes Frame Relay, la Internet, etc.)

2.3.1. Según el alcance geográfico

De acuerdo con la distribución geográfica:

- Red de área local (LAN)

  Una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo un edificio.

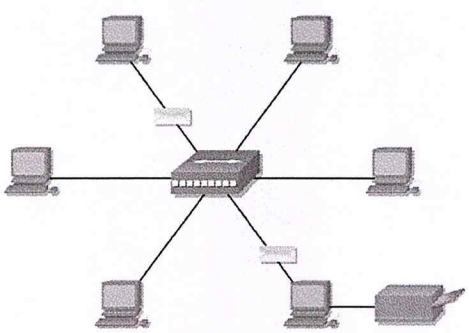


Figura 2.1. Red LAN

- Red de área metropolitanas (MAN)

  Una red MAN es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

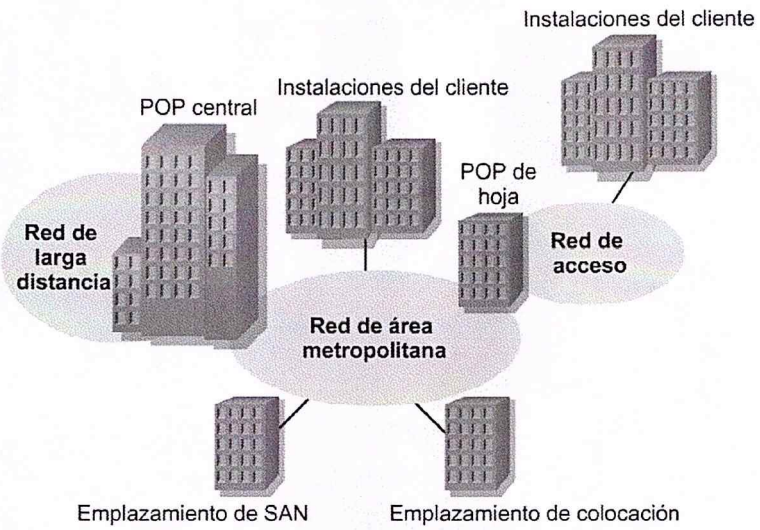


Figura 2.2. Red MAN

- Red de área extensa (WAN y redes globales)

  Las WAN y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites.

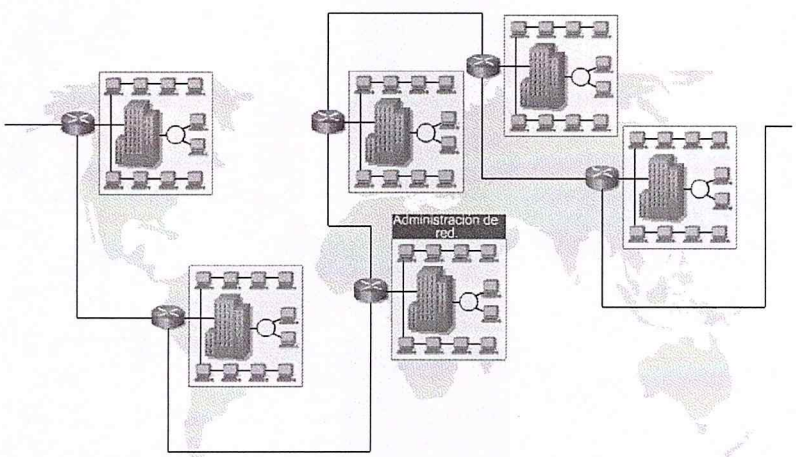


Figura 2.3. Red WAN

2.4. Topologías de Red

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada. Existen tres topologías comunes:

- **Anillo**

El anillo, como su propio nombre indica, consiste en conectar linealmente entre sí todos los ordenadores, en un bucle cerrado. La información se transfiere en un solo sentido a través del anillo, mediante un paquete especial de datos, llamado **testigo**, que se transmite de un nodo a otro, hasta alcanzar el nodo destino.

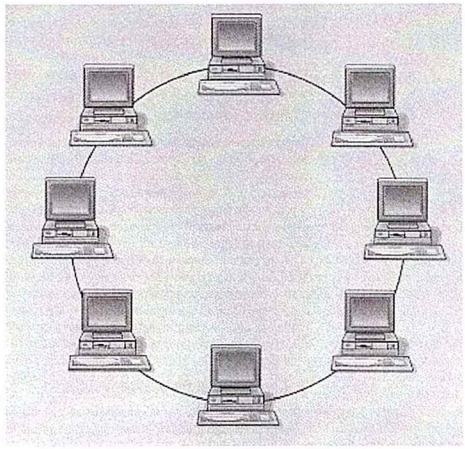


Figura 2.4 Anillo

El cableado de la red en anillo es el más complejo de los tres enumerados, debido por una parte al mayor coste del cable, así como a la necesidad de emplear unos dispositivos denominados Unidades de Acceso Multiestación (MAU) para implementar físicamente el anillo.

A la hora de tratar con fallos y averías, la red en anillo presenta la ventaja de poder derivar partes de la red mediante los MAU's, aislando dichas partes defectuosas del resto de la red mientras se determina el problema. Un fallo, pues, en una parte del cableado de una red en anillo, no debe detener toda la red. La adición de nuevas estaciones no supone una complicación excesiva, puesto que una vez más los MAU's aíslan las partes a añadir hasta que se hallan listas, no siendo necesario detener toda la red para añadir nuevas estaciones.
Dos buenos ejemplos de red en anillo serían Token-Ring y FDDI (fibra óptica)

- **Estrella**

Esta topología se caracteriza por existir en ella un punto central, o más propiamente nodo central, al cual se conectan todos los equipos, de un modo muy similar a los radios de una rueda.

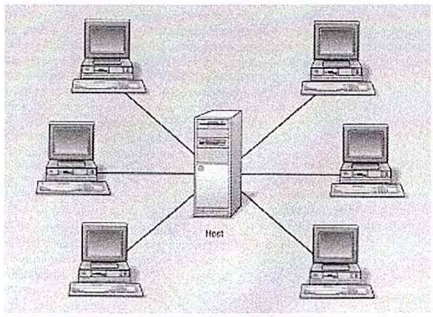


Figura 2.5 Estrella

De esta disposición se deduce el inconveniente de esta topología, y es que la máxima vulnerabilidad se encuentra precisamente en el nodo central, ya que si este falla, toda la red fallaría. Este posible fallo en el nodo central, aunque posible, es bastante improbable, debido a la gran seguridad que suele poseer dicho nodo. Sin embargo presenta como principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.

Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.

La topología en estrella es empleada en redes Ethernet y ArcNet.

- **Bus**

En la topología en bus, al contrario que en la topología de Estrella, no existe un nodo central, si no que todos los nodos que componen la red quedan unidos entre sí linealmente, uno a continuación del otro.

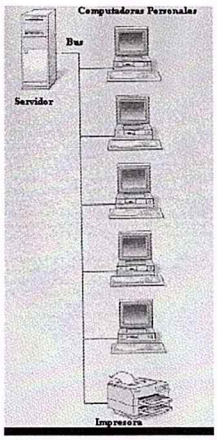


Figura 2.6. Bus

El cableado en bus presenta menos problemas logísticos, puesto que no se acumulan montones de cables en torno al nodo central, como ocurriría en una disposición en estrella. Pero, por contra, tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Es además muy difícil encontrar y diagnosticar las averías que se producen en esta topología.

Debido a que en el bus la información recorre todo el bus bidireccionalmente hasta hallar su destino, la posibilidad de interceptar la información por usuarios no autorizados es superior a la existente en una Red en estrella debido a la modularidad que ésta posee.

La red en bus posee un retardo en la propagación de la información mínimo, debido que los nodos de la red no deben amplificar la señal, siendo su función pasiva respecto al tráfico de la red. Esta pasividad de los nodos es debida más bien al método de acceso empleado que a la propia disposición geográfica de los puestos de red. La Red en Bus necesita incluir en ambos extremos del bus, unos dispositivos llamados terminadores, los cuales evitan los posibles rebotes de la señal, introduciendo una impedancia característica (50 Ohm.)

Añadir nuevos puesto a una red en bus, supone detener al menos por tramos, la actividad de la red. Sin embargo es un proceso rápido y sencillo. Es la topología tradicionalmente usada en redes Ethernet.

- **Híbridas**

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

- Anillo en estrella

  Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

- "Bus en estrella"

  El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

- Estrella Jerárquica

  Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.

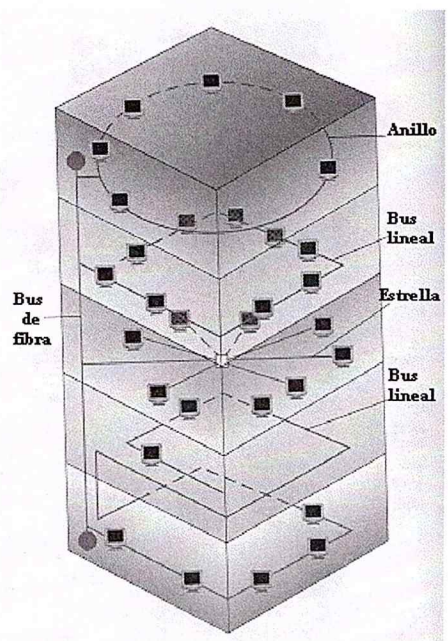


Figura 2.7. Hibridas

2.5. Estudio técnico de las redes Alámbricas

2.5.1. Medios de transmisión

Los medios de transmisión de las redes alambricas se da mediante la unión de cableado, esto depende de según su velocidad y tasa de transferencia.

2.5.1.1. Par Trenzado

Cable Par trenzado blindado (Cable STP)

El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico. Los dos pares de hilos están envueltos juntos en una trenza o papel metálico. Generalmente es un cable de 150 ohmios. Según se especifica para el uso en instalaciones de redes Token Ring, el STP reduce el ruido eléctrico dentro del cable como, por ejemplo, el acoplamiento de par a par y la diafonía. El STP también reduce el ruido electrónico desde el exterior del cable, como, por ejemplo, la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y de instalación más difícil que el UTP.

Un nuevo híbrido de UTP con STP tradicional se denomina UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El ScTP consiste, básicamente, en cable UTP envuelto en un blindaje de papel metálico. ScTP, como UTP, es también un cable de 100 Ohms. Muchos fabricantes e instaladores de cables pueden usar el término STP para describir el cable ScTP. Es importante entender que la mayoría de las referencias hechas a STP hoy en día se refieren en realidad a un cable de cuatro pares apantallado. Es muy improbable que un verdadero cable STP sea usado durante un trabajo de instalación de cable.

Los materiales metálicos de blindaje utilizados en STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están adecuadamente conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el STP y el ScTP se pueden volver susceptibles a graves problemas de ruido.

Son susceptibles porque permiten que el blindaje actúe como una antena que recoge las señales no deseadas. Sin embargo, este efecto funciona en ambos sentidos. El blindaje no sólo evita que ondas electromagnéticas externas produzcan ruido en los cables de datos sino que también minimiza la irradiación de las ondas electromagnéticas internas. Estas ondas podrían producir ruido en otros dispositivos.

Los cables STP y ScTP no pueden tenderse sobre distancias tan largas como las de otros medios de networking (tales como el cable coaxial y la fibra óptica) sin que se repita la señal. El uso de aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable. Además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra. Sin embargo, el STP y el ScTP todavía desempeñan un papel importante, especialmente en Europa o en instalaciones donde exista mucha EMI y RFI cerca de los cables.

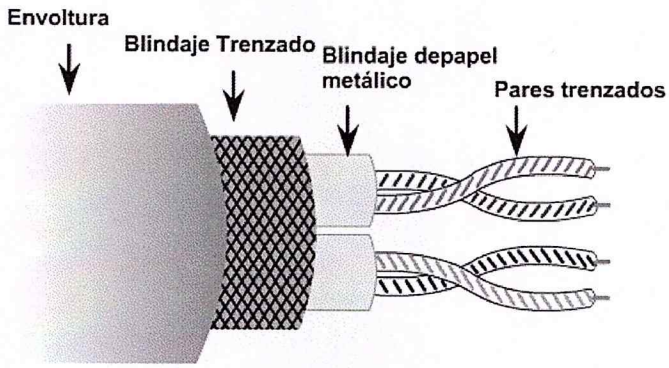


Figura 2.8. Cable STP

Cable de Par trenzado blindado
Velocidad y tasa de transferencia: 0 – 100 Mbps
Costo: Moderado
Tamaño de los medios y del conector: Mediano a grande
Longitud máxima del cable: 100 m

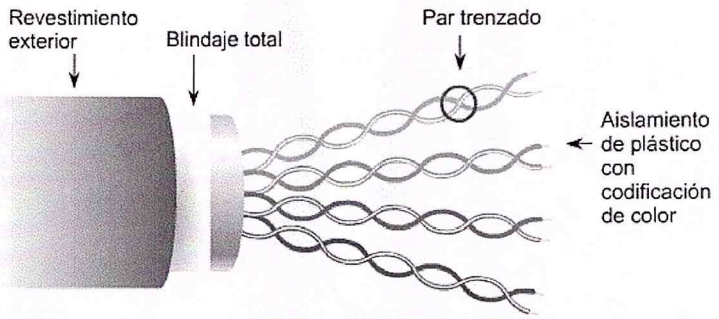


Figura 2.9. Cable ScTP

Sctp (Cable de Par trenzado apantallado)
Velocidad y tasa de transferencia: 0 – 100 Mbps
Costo promedio por punto: Moderado Caro
Tamaño de los medios y del conector: Mediano a grande
Longitud máxima del cable: 100 m

Cable Par trenzado no blindado (Cable UTP)

El cable de par trenzado no blindado (UTP) es un medio de cuatro pares de hilos que se utiliza en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislante. Además, cada par de hilos está trenzado. Este tipo de cable cuenta sólo con el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.

El estándar TIA/EIA-568-B.2 especifica los componentes de cableado, transmisión, modelos de sistemas, y los procedimientos de medición necesarios para verificar los cables de par trenzado balanceado. Exige el tendido de dos cables, uno para voz y otro para datos en cada toma. De los dos cables, el cable de voz debe ser UTP de cuatro pares. El cable Categoría 5 es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones. Sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5 en instalaciones de red. El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la Categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios para networking. De hecho, el UTP cuesta menos por metro que cualquier otro tipo de cableado para LAN. Sin embargo, la ventaja real es su tamaño. Debido a que su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Esto puede ser un factor sumamente importante a tener en cuenta, en especial si se está instalando una red en un edificio antiguo.

Además, si se está instalando el cable UTP con un conector RJ-45, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad. El cableado de par trenzado presenta ciertas desventajas. El cable UTP es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios para networking y la distancia que puede abarcar la señal sin el uso de repetidores es menor para UTP que para los cables coaxiales y de fibra óptica.

En una época, el cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable de par trenzado es el más rápido entre los medios basados en cobre.

Para que sea posible la comunicación, la señal transmitida por la fuente debe ser entendida por el destino. Esto es cierto tanto desde una perspectiva física como en el software. La señal transmitida necesita ser correctamente recibida por la conexión del circuito que está diseñada para recibir las señales. El pin de transmisión de la fuente debe conectarse en fin al pin receptor del destino. A continuación se presentan los tipos de conexiones de cable utilizadas entre dispositivos de internetwork.

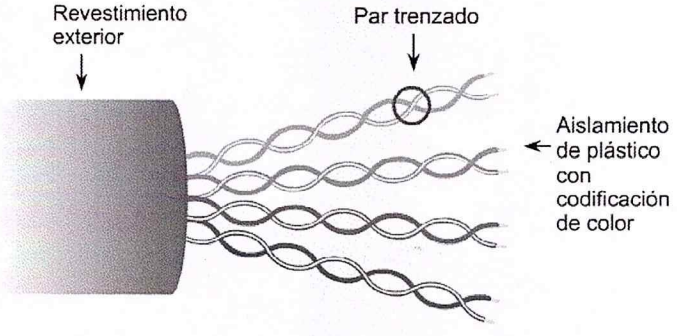


Figura 2.10. Cable UTP

Cable de Par trenzado no blindado

Velocidad y tasa de transferencia: 10 – 100 - 1000 Mbps (Según la calidad/categoría del cable)

Costo promedio por nodo: El menos Caro

Tamaño de los medios y del conector: Pequeño

Longitud máxima del cable: 100 m

2.5.1.2. Cable coaxial

El cable coaxial consiste de un conductor de cobre rodeado de una capa de aislante flexible. El conductor central también puede ser hecho de un cable de aluminio cubierto de estaño que permite que el cable sea fabricado de forma económica. Sobre este material aislante existe una malla de cobre tejida u hoja metálica que actúa como el segundo hilo del circuito y como un blindaje para el conductor interno. Esta segunda capa, o blindaje, también reduce la cantidad de interferencia electromagnética externa. Cubriendo la pantalla está la chaqueta del cable.

Para las LAN, el cable coaxial ofrece varias ventajas. Puede tenderse a mayores distancias que el cable de par trenzado blindado STP, y que el cable de par trenzado no blindado, UTP, sin necesidad de repetidores. Los repetidores regeneran las señales de la red de modo que puedan abarcar mayores distancias. El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos, incluida la televisión por cable.

Al trabajar con cables, es importante tener en cuenta su tamaño. A medida que aumenta el grosor, o diámetro, del cable, resulta más difícil trabajar con él. Recuerde que el cable debe pasar por conductos y cajas existentes cuyo tamaño es limitado. Se puede conseguir cable coaxial de varios tamaños. El cable de mayor diámetro es de uso específico como cable de backbone de Ethernet porque tiene mejores características de longitud de transmisión y de limitación del ruido. Este tipo de cable coaxial frecuentemente se denomina thicknet o red gruesa. Como su apodo lo indica, este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. Generalmente, cuanto más difícil es instalar los medios de red, más costosa resulta la instalación. El cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet casi nunca se usa, salvo en instalaciones especiales.

En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm (a veces denominado thinnet o red fina) se usaba para las redes Ethernet. Era particularmente útil para las instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación de thinnet era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet (red barata). El trenzado externo metálico o de cobre del cable coaxial abarca la mitad del circuito eléctrico. Se debe tener especial cuidado de asegurar una sólida conexión eléctrica en ambos extremos, brindando así una correcta conexión a tierra. La incorrecta conexión del material de blindaje constituye uno de los problemas principales relacionados con la instalación del cable coaxial. Los problemas de conexión resultan en un ruido eléctrico que interfiere con la transmisión de señales sobre los medios de networking. Por esta razón, thinnet ya no se usa con frecuencia ni está respaldado por los estándares más recientes (100 Mbps y superiores) para redes Ethernet.

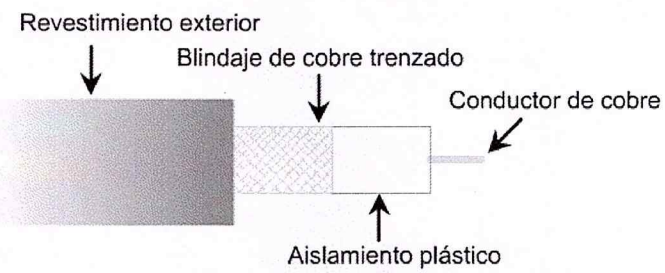


Figura 2.11. Cable Coaxial

Cables coaxiales
Velocidad y tasa de transferencia: 10 – 100 Mbps
Costo: Económico
Tamaño de los medios y del corrector: Medio
Longitud máxima del cable: 500 m

2.5.1.3. Fibra óptica

Los circuitos de fibra óptica son filamentos de vidrio (compuestos de cristales naturales) o plástico (cristales artificiales), del espesor de un pelo (entre 10 y 300 micrones). Llevan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción.

Las fibras ópticas pueden ahora usarse como los alambres de cobre convencionales, tanto en pequeños ambientes autónomos (tales como sistemas de procesamiento de datos de aviones), como en grandes redes geográficas (como los sistemas de largas líneas urbanas mantenidos por compañías telefónicas).

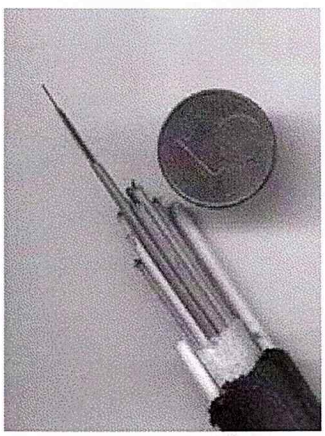


Figura 2.12. Sección de fibra óptica.

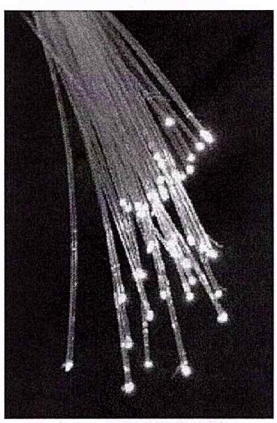


Figura 2.13. Fibra óptica brillando Cuando transmite luz.

En un sistema de transmisión por fibra óptica existe un transmisor que se encarga de transformar las ondas electromagnéticas en energía óptica o en luminosa, por ello se le considera el componente activo de este proceso. Una vez que es transmitida la señal luminosa por las minúsculas fibras, en otro extremo del circuito se encuentra un tercer componente al que se le denomina detector óptico o receptor, cuya misión consiste en transformar la señal luminosa en energía electromagnética, similar a la señal original. El sistema básico de transmisión se compone en este orden, de señal de entrada, amplificador, fuente de luz, corrector óptico, línea de fibra óptica (primer tramo), empalme, línea de fibra óptica (segundo tramo), corrector óptico, receptor, amplificador y señal de salida.

En resumen, se puede decir que este proceso de comunicación, la fibra óptica funciona como medio de transportación de la señal luminosa, generado por el transmisor de LED'S (diodos emisores de luz) y láser.

Los diodos emisores de luz y los diodos láser son fuentes adecuadas para la transmisión mediante fibra óptica, debido a que su salida se puede controlar rápidamente por medio de una corriente de polarización. Además su pequeño tamaño, su luminosidad, longitud de onda y el bajo voltaje necesario para manejarlos son características atractivas.

Los Componentes de una fibra Óptica son:

El Núcleo: En sílice, cuarzo fundido o plástico - en el cual se propagan las ondas ópticas. Diámetro: 50 o 62,5 um para la fibra multimodo y 9um para la fibra monomodo.
La Funda Óptica: Generalmente de los mismos materiales que el núcleo pero con aditivos que confinan las ondas ópticas en el núcleo.
El revestimiento de protección: por lo general esta fabricado en plástico y asegura la protección mecánica de la fibra.

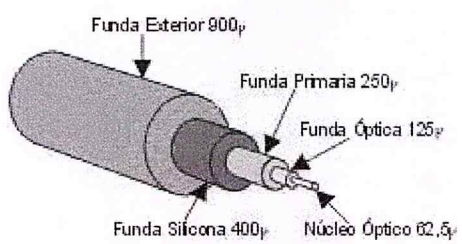


Figura 2.14. Componentes de una fibra Óptica

2.5.1.3.1. Tipos de Fibras óptica

Los tipos de Fibra Óptica son:

Fibra Monomodo:

Potencialmente, esta es la fibra que ofrece la mayor capacidad de transporte de información. Tiene una banda de paso del orden de los 100 GHz/km. Los mayores flujos se consiguen con esta fibra, pero también es la más compleja de implantar.

El dibujo muestra que sólo pueden ser transmitidos los rayos que tienen una trayectoria que sigue el eje de la fibra, por lo que se ha ganado el nombre de "monomodo" (modo de propagación, o camino del haz luminoso, único). Son fibras que tienen el diámetro del núcleo en el mismo orden de magnitud que la longitud de onda de las señales ópticas que transmiten, es decir, de unos 5 a 8 m m. Si el núcleo está constituido de un material cuyo índice de refracción es muy diferente al de la cubierta, entonces se habla de fibras monomodo de índice escalonado. Los elevados flujos que se pueden alcanzar constituyen la principal ventaja de las fibras monomodo, ya que sus pequeñas dimensiones implican un manejo delicado y entrañan dificultades de conexión que aún se dominan mal.

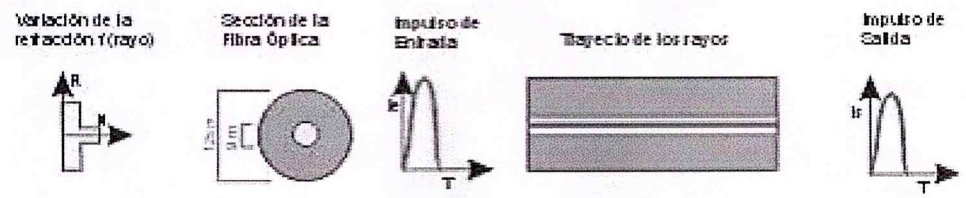


Figura 2.15. Fibra Monomodo

Fibra Multimodo de Índice Gradiante Gradual:

Las fibras multimodo de índice de gradiente gradual tienen una banda de paso que llega hasta los 500MHz por kilómetro. Su principio se basa en que el índice de refracción en el interior del núcleo no es único y decrece cuando se desplaza del núcleo hacia la cubierta. Los rayos luminosos se encuentran enfocados hacia el eje de la fibra, como se puede ver en el dibujo. Estas fibras permiten reducir la dispersión entre los diferentes modos de propagación a través del núcleo de la fibra.

La fibra multimodo de índice de gradiente gradual de tamaño 62,5/125 m (diámetro del núcleo/diámetro de la cubierta) está normalizado, pero se pueden encontrar otros tipos de fibras:- Multimodo de índice escalonado 100/140 mm.

- Multimodo de índice de gradiente gradual 50/125 mm.

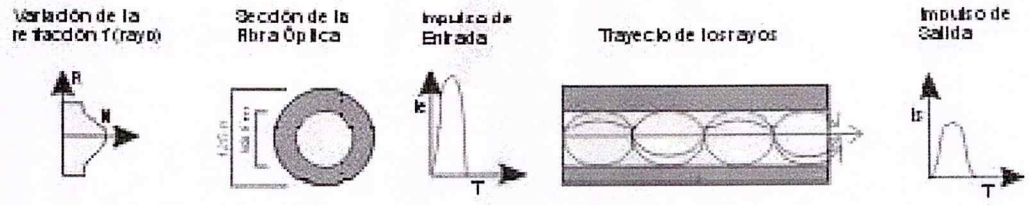


Figura 2.16. Fibra Multimodo de índice Gradiante Gradual

Fibra Multimodo de índice escalonado:

Las fibras multimodo de índice escalonado están fabricadas a base de vidrio, con una atenuación de 30 dB/km, o plástico, con una atenuación de 100 dB/km. Tienen una banda de paso que llega hasta los 40 MHz por kilómetro. En estas fibras, el núcleo está constituido por un material uniforme cuyo índice de refracción es claramente superior al de la cubierta que lo rodea. El paso desde el núcleo hasta la cubierta conlleva por tanto una variación brutal del índice, de ahí su nombre de índice escalonado.

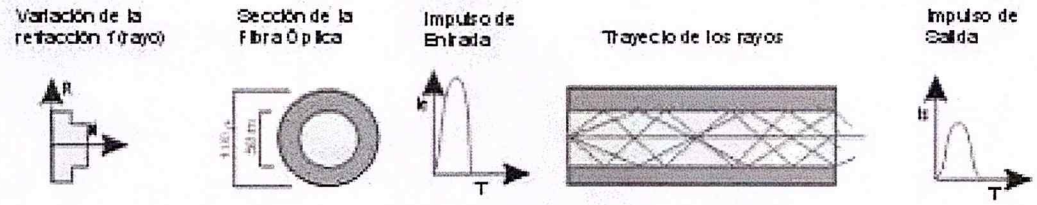


Figura 2.17. Fibra Multimodo de índice escalonado

Con la Fibra Óptica se puede usar Acopladores y Conectores:

Acopladores:

Un acoplador es básicamente la transición mecánica necesaria para poder dar continuidad al paso de luz del extremo conectorizado de un cable de fibra óptica a otro. Pueden ser provistos también acopladores de tipo "Híbridos", que permiten acoplar dos diseños distintos de conector, uno de cada lado, condicionado a la coincidencia del perfil del pulido.

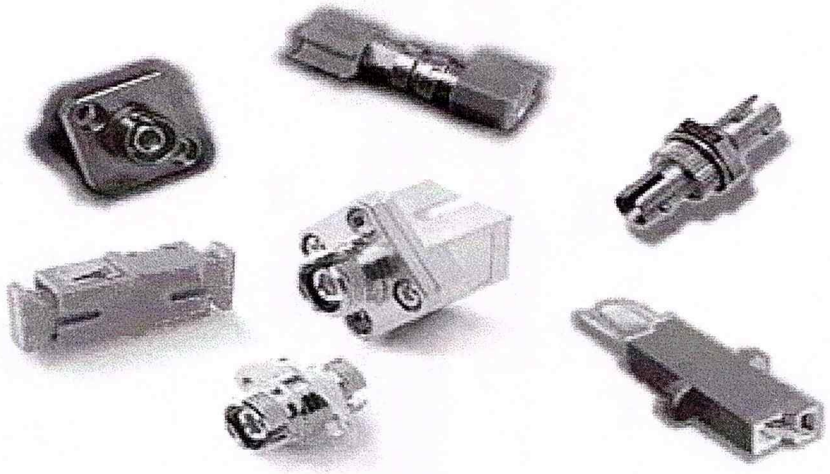


Figura 2.18. Acopladores

Conectores:

1.- Se recomienda el conector 568SC pues este mantiene la polaridad. La posición correspondiente a los dos conectores del 568SC en su adaptador, se denominan como A y B. Esto ayuda a mantener la polaridad correcta en el sistema de cableado y permite al adaptador a implementar polaridad inversa acertada de pares entre los conectores

2.- Sistemas con conectores BFOC/2.5 y adaptadores (Tipo ST) instalados pueden seguir siendo utilizados en plataformas actuales y futuras.

Identificación: Conectores y adaptadores Multimodo se representan por el color marfil Conectores y adaptadores Monomodo se representan por el color azul.

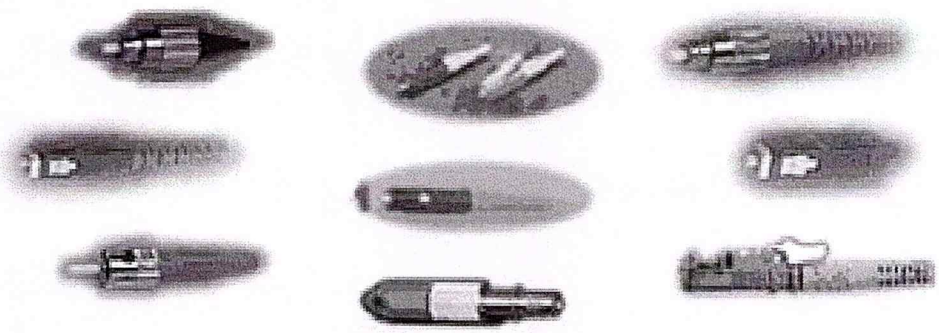


Figura 2.19. Conectores

Para la terminación de una fibra óptica es necesario utilizar conectores o empalmar Pigtails (cables armados con conector) por medio de fusión. Para el caso de conectorización se encuentran distintos tipos de conectores dependiendo el uso y la normativa mundial usada y sus Características.

ST conector de Fibra para Monomodo o Multimodo con uso habitual en Redes de Datos y equipos de Networking locales en forma Multimodo.-

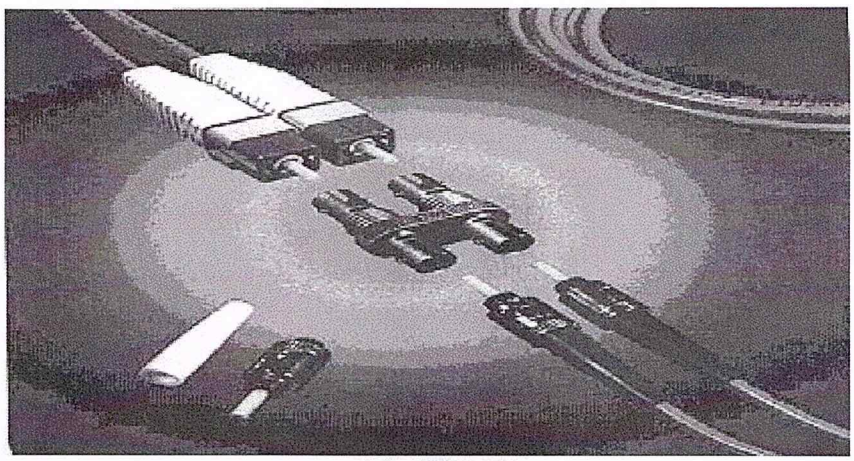


Figura 2.20 ST conector de Fibra

FC conector de Fibra Óptica para Monomodo o Multimodo con uso habitual en telefonía y CATV en formato Monomodo y Monomodo Angular.

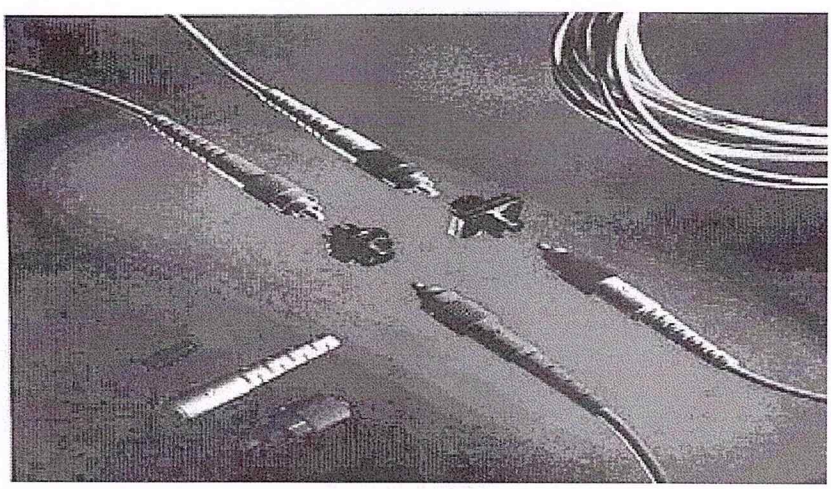


Figura 2.21. FC conector de Fibra

SC conector de Fibra óptica para Monomodo y Multimodo con uso habitual en telefonía en formato Monomodo.

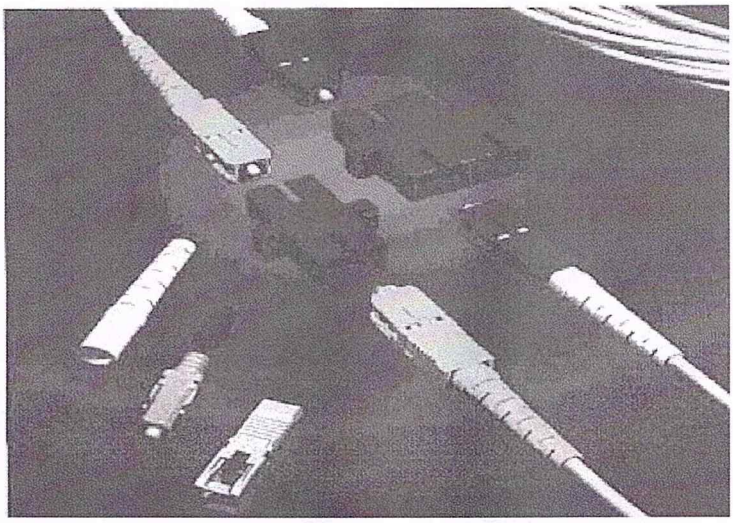


Figura 2.22. SC conector de Fibra

2.5.1.3.2. Ventajas y Desventajas de la Fibra Óptica

Ventajas

- La fibra óptica hace posible navegar por Internet a una velocidad de dos millones de bps.
- Acceso ilimitado y continuo las 24 horas del día, sin congestiones.
- Video y sonido en tiempo real.
- Es inmune al ruido y las interferencias
- Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.
- Carencia de señales eléctricas en la fibra.
- Presenta dimensiones más reducidas que los medios pre-existentes.
- El peso del cable de fibras ópticas es muy inferior al de los cables metálicos.
- La materia prima para fabricarla es abundante en la naturaleza.
- Compatibilidad con la tecnología digital.

Desventajas

- Sólo pueden suscribirse las personas que viven en las zonas de la ciudad por las cuales ya esté instalada la red de fibra óptica.
- El coste es alto en la conexión de fibra óptica, las empresas no cobran por tiempo de utilización sino por cantidad de información transferida al computador, que se mide en megabytes.
- El coste de instalación es elevado.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.
- Nuevas Características de la Fibra Óptica.

Coberturas más resistentes:

La cubierta especial es extruida a alta presión directamente sobre el mismo núcleo del cable, resultando en que la superficie interna de la cubierta del cable tenga arista helicoidales que se aseguran con los subcables.

La cubierta contiene 25% más material que las cubiertas convencionales.

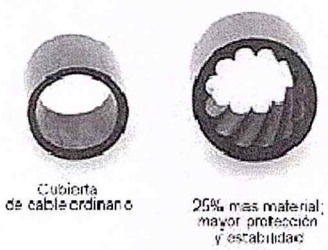


Figura 2.23. Coberturas

Uso Dual (interior y exterior):

La resistencia al agua, hongos y emisiones ultra violeta; la cubierta resistente; buffer de 900 μm; fibras ópticas probadas bajo 100 kpsi; y funcionamiento ambiental extendida; contribuyen a una mayor confiabilidad durante el tiempo de vida.

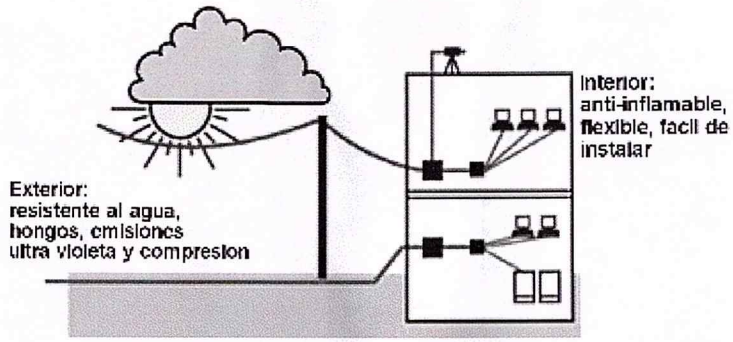


Figura 2.24. Uso Dual

Mayor protección en lugares húmedos:

En cables de tubo holgado rellenos de gel, el gel dentro de la cubierta se asienta dejando canales que permitan que el agua migre hacia los puntos de terminación. El agua puede acumularse en pequeñas piscinas en los vacíos, y cuando la delicada fibra óptica es expuesta, la vida útil es recortada por los efectos dañinos del agua en contacto. combaten la intrusión de humedad con múltiples capas de protección alrededor de la fibra óptica. El resultado es una mayor vida útil, mayor confiabilidad especialmente ambientes húmedos.

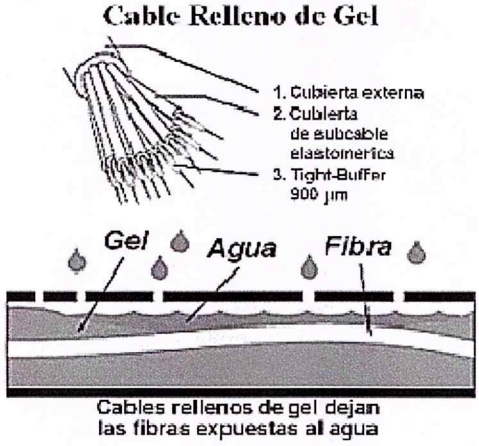


Figura 2.25. Cable Relleno de Gel

Empaquetado de alta densidad:

Con el máximo número de fibras en el menor diámetro posible se consigue una más rápida y más fácil instalación, donde el cable debe enfrentar dobleces agudos y espacios estrechos. Se ha llegado a conseguir un cable con 72 fibras de construcción súper densa cuyo diámetro es un 50% menor al de los cables convencionales.

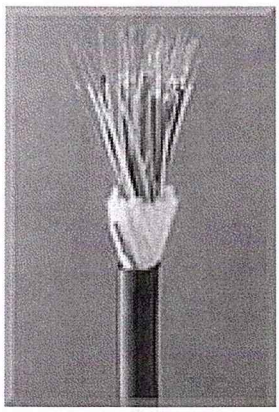


Figura 2.26. Empaquetado

2.6. Cableado estructurado y sus componentes

Las partes de un Cableado estructurado son:

1. **Área de trabajo:** Es el lugar donde se encuentra el personal trabajando con las computadoras, impresoras, etc. En este lugar se instalan los servicios (nodos de datos, telefonía, energía eléctrica, etc.) Closet de comunicaciones – Es el punto donde se concentran todas las conexiones que se necesitan en el área de trabajo.

2. **Cableado Horizontal:** es aquel que viaja desde el área de trabajo hasta el closet de comunicaciones.

3. **Closet de Equipo** – En este cuarto se concentran los servidores de la red, el conmutador telefónico, etc. Este puede ser el mismo espacio físico que el del closet de comunicaciones y de igual forma debe ser de acceso restringido.

4. Instalaciones de **Entrada (Acometida)** – Es el punto donde entran los servicios al edificio y se les realiza una adaptación para unirlos al edificio y hacerlos llegar a los diferentes lugares del edificio en su parte interior. (no necesariamente tienen que ser datos pueden ser las líneas telefónicas, o Back Bone que venga de otro edificio, etc.)

5. **Cableado Vertebral (Back Bone)** – Es el medio físico que une 2 redes entre si.

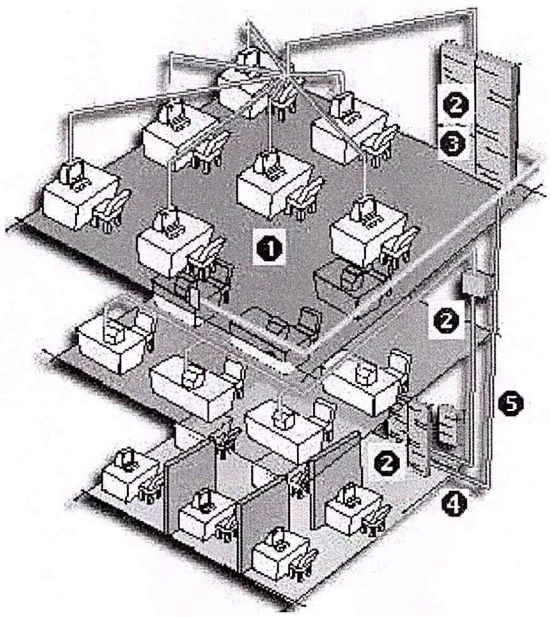


Figura 2.27. Backbone

- En la siguiente imagen se detalla un edificio con 3 pisos, se trata de simular un edificio corporativo donde existe un considerable numero de nodos o servicios en cada piso, por tanto el cableado se divide en un closet de comunicaciones principal en el piso superior y sub closets en los demás pisos y estos closets se unen con un back bone que corre entre los pisos.

- El cableado horizontal (los puntos 1 y 2) forzosamente tienen que estar considerados en cualquier cableado estructurado por mas pequeño que sea. Estos puntos son los mínimos necesarios.

- El closet de equipo puede ser tan grande o pequeño como se requiera, puede ser desde un pequeño servidor hasta varios servidores unidos entre si.

- Los puntos 4 y 5, La Acometida y El Cableado Vertebral dependen del tamaño de cableado.

La acometida puede no ser necesaria si no requerimos de servicios que viene de la calle para ser incorporados a al red, o esta puede ser tan pequeña como un simple hoyo en la pared para que pase una línea telefónica.

El BackBone no es necesario al menos de que se deseen unir closets de comunicaciones.

Para detallar mejor en lo consiste el cableado horizontal se tiene la siguiente gráfica:

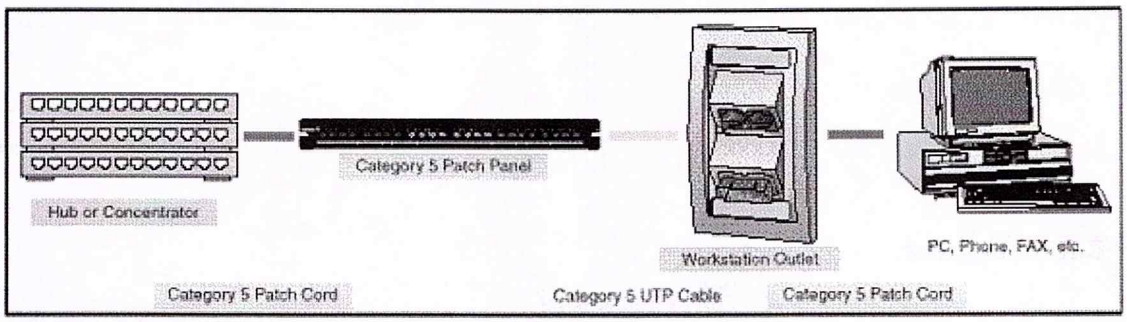


Figura 2.28. Cableado Horizontal

Esta es la trayectoria que lleva el cableado horizontal, observese de derecha a izquierda

- Se tiene el dispositivo que se quiere conectar a la red, este puede ser un teléfono, una computadora, o cualquier otro.

- Patch Cord – Se debe de contar con un cable que une este dispositivo a la placa que se encuentra en la pared (en el área de trabajo), este es un cable de alta resistencia ya que esta considerado para ser conectado y desconectado cuantas veces lo requiera el usuario.

- Placa con servicios – Esta placa contiene los conectores donde puede ser conectado el dispositivo, pensando en una red de datos, se tiene un conector RJ45 donde puede ser insertado el plug del cable, y pensando en un teléfono, pues se obtiene un conector RJ11 para insertar ahí el conector telefónico. La misma placa puede combinar servicios (voz, datos, video, etc.).

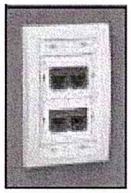
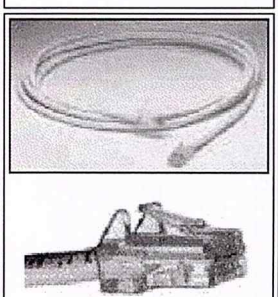
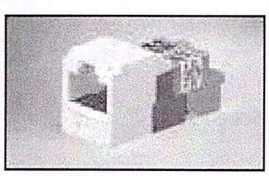
Placa con Servicios	Patch Cord	Conector Instalado en la placa
		

Figura 2.29. Dispositivos de Red

- Cableado Oculto – Es la parte del cableado que nunca debe ser movida una vez instalada, es el cable que viaja desde el área de trabajo, hasta el closet de comunicaciones donde se concentran todos los puntos que vienen de las áreas de trabajo. Este puede viajar entubado, en canaletas, escalerillas, o similares.

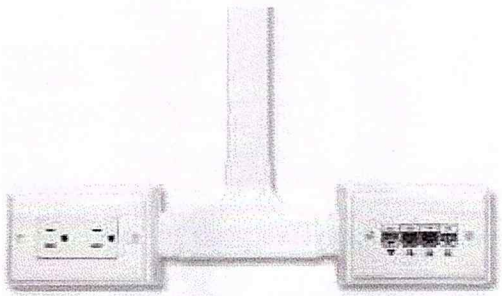


Figura 2.30. Cableado Oculto

- Panel de Parcheo – Todos los cables que vienen de las áreas de trabajo al llegar al closet de comunicaciones se terminan de alguna manera en la que se puedan administrar. Esta imagen muestra una regleta que tiene 24 conectores idénticos a los que se tienen instalados en las placas de los servicios que se encuentran en el área de trabajo, esta regleta va fijada en un rack y aquí es donde termina el cableado oculto, de esta manera se garantiza que el cableado que viaja oculto nunca se mueva y no sufra alteraciones.

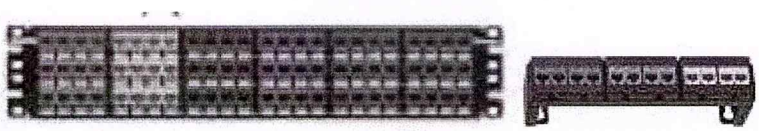


Figura 2.31. Paneles de Parcheo instalados dentro de los clósets

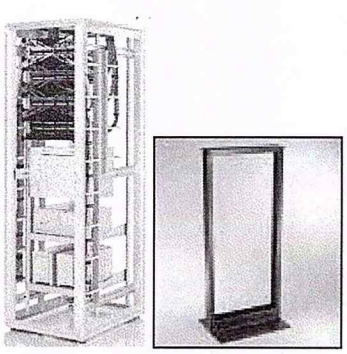


Figura 2.32. Gabinete o Rack

- Patch Cord – Nuevamente viene un Patch Cord, pero este une al servicio que viene del área de trabajo con el equipo activo.

Una vez que el cableado es terminado en ambos extremos, es probado con herramientas altamente confiables que certifican el buen funcionamiento del cableado. Una vez que se pasan todas las pruebas, Si se pasan las pruebas se cierran.

2.6.1. Identificadores para los elementos de las Redes de cableado Estructurado

2.6.1.1. Cables

Cable principal de Campus.		
Identificador:	CPC XXX –[Tipo]-YYY[Tipo 2]	
Estructura:	CPC	= Cable principal de Campus
	XXX	= Número consecutivo
	[Tipo]	= SCREBH, SCREB, ASP, ASPB, FO, etc.
	YYY	= Capacidad en pares o conductores
	[Tipo2]	= P: pares, C: conductores ópticos

Tabla 2.1. Cable Principal de Campus

Cable principal de edificio.		
Identificador:	CPE XXX –[Tipo 1]-YYY[Tipo 2]	
Estructura:	CPE	= Cable principal de edificio
	XXX	= Número consecutivo
	[Tipo 1]	= SCREBH, SCREB, ASP, ASPB, FO, etc.
	YYY	= Capacidad en pares o conductores
	[Tipo 2]	= P: pares, C: conductores ópticos

Tabla 2.2. Cable Principal de Edificio

Cable horizontal.		
Identificador:	CHX –STYYY-[Tipo1]-ZZZ[Tipo 2]	
Estructura:	CH	= Cable horizontal.
	X	= Número de segmento en el enlace. No aplica cuando se efectúa el cableado directo entre DCP y ST.
	ST	= Salida de telecomunicaciones.
	YYY	= Número de la salida de telecomunicaciones a la que se interconecta
	[Tipo 1]	= UTP, FTP, FO, ARMANEL, etc.
	ZZZ	= Capacidad en pares o conductores.
	[Tipo 2]	= P: pares, C: conductores ópticos.

Tabla 2.3. Cable Horizontal

Cable de entrada.		
Identificador:	CENT XXX -[Tipo1]-YYY[Tipo2]	
Estructura:	CENT	= Cable de entrada.
	XXX	= Número consecutivo.
	[Tipo 1]	= SCREBH, SCREB, ASP, ASPB, FO, etc.
	YYY	= Capacidad en pares o conductores.
	[Tipo 2]	= P: pares, C: conductores ópticos.

Tabla 2.4. Cable de entrada

Nota: Para la identificación física de los cables principales de Campus, cables principales de edificio y cables de entrada, también se deben incluir en la etiqueta los campos de origen y destino del cable.

Empalme de cables.		
Identificador:	EXXX	
Estructura:	E	= Empalme de cables
	XXX	= Número consecutivo

Tabla 2.5. Empalme de cables

Par de cable principal de cobre o fibra óptica.		
Identificador:	[Cable]-PXXX	
Estructura:	[Cable]	= Identificador del cable principal de Campus/Edificio o de entrada
	P	= Par
	XXX	= Número de par

Tabla 2.6. Par de cable principal de cobre o fibra óptica

Conductor de cable principal de fibra óptica.		
Identificador:	[Cable]-CXXX	
Estructura	[Cable]	= Identificador del cable principal de Campus/Edificio o de entrada
	C	= Conductor.
	XXX	= Número de conductor.

Tabla 2.7. Conductor de cable principal de fibra óptica

2.6.1.2. Espacios de Telecomunicaciones

Cuarto de equipos.		
Identificador:	CEXX	
Estructura:	CE XX	= Cuarto de equipos = Número consecutivo

Tabla 2.8. Cuarto de Equipos

Cuarto de telecomunicaciones.		
Identificador:	CTXXX	
Estructura:	CT XXX	= Cuarto de telecomunicaciones = Número consecutivo

Tabla 2.9. Cuarto de Telecomunicaciones

2.6.1.3. Distribuidores y Gabinetes

Distribuidores de cableado.		
Identificador:	DC[Tipo]XXX	
Estructura:	DC [Tipo] XXX	= Distribuidor de cableado = C: Campus; E: Edificio; P: Piso; = Número consecutivo

Tabla 2.10. Distribuidores de Cableado

Nota: Cuando un distribuidor tenga las funciones de DCC, DCE y/o DCP al mismo tiempo, se debe utilizar el identificador del distribuidor de mayor jerarquía.

Gabinetes.		
Identificador:	[Distribuidor]-GABXXX	
Estructura	[Distribuidor GAB XXX	= Identificador del distribuidor al que que pertenece el gabinete = Gabinete. = Número consecutivo.

Tabla 2.11. Gabinetes

Administrador horizontal de cables.		
Identificador:	AHC-XXX	
Estructura:	AHC XXX	= Administrador horizontal de cables = Número consecutivo

Tabla 2.12. Administrador horizontal de cables

2.6.1.4. Accesorios de Conexión

Accesorio de conexión.		
Identificador:	[Gabinete]-CXX-RYY-[Tecnología]-ZZ	
Estructura	[Gabinete] C XX R YY [Tecnología] ZZ	= Identificador del gabinete al que pertenece el accesorio de conexión = Columna. = No. de columna en la que se ubica el accesorio de conexión. = Renglón. = No. de renglón dentro de la columna donde se ubica el accesorio de conexión. = PPO: Panel de Parcheo óptico. PPC: Panel de Parcheo de cobre. IDC: Contacto por desplazamiento de aislamiento. = Número de puertos del accesorio de conexión.

Tabla 2.13. Accesorio de Conexión

Posición de terminación para accesorios de conexión.		
Identificador:	[Gabinete]-CXX-RYY-PZZ -[Tecnología]-AA	
Estructura	[Gabinete] C XX R YY P ZZ [Tecnologia] AA	= Identificador del gabinete al que pertenece el accesorio de conexión = Columna. = No. de columna en la que se ubica el accesorio de conexión. = Renglón. = No. de renglón dentro de la columna donde se ubica el accesorio de conexión. = Posición de terminación. = Número de la posición dentro del accesorio de conexión. = PPO: Panel de parcheo óptico. PPC: Panel de parcheo de cobre. IDC: Contacto por desplazamiento de aislamiento. = Número de puertos del accesorio de conexión.

Tabla 2.14. Posición de terminación para accesorios de conexión

Salida/Conector de telecomunicaciones.		
Identificador:	STXXX	
Estructura:	ST	= Salida/conector de telecomunicaciones
	XXX	= Consecutivo

Tabla 2.15. Salida/Conector de telecomunicaciones

Nota: Cuando se requiera identificar el tipo de servicio, y sólo para instalaciones de cableado existentes, se permite utilizar la siguiente nomenclatura: V-XXX para servicios de voz, D-XXX para servicios de datos y VCXXX para servicios de video.

Toma de telecomunicaciones.		
Identificador:	TT-STXXX/STYYY	
Estructura	TT	= TT = Toma de telecomunicaciones.
	STXXX	= Identificador de la salida/conector de telecomunicaciones con el número menor de los contenidos en la toma de telecomunicaciones.
	STYYY	= Identificador de la salida/conector de telecomunicaciones con el número mayor de los contenidos en la toma de telecomunicaciones.

Tabla 2.16. Toma de telecomunicaciones

Nota: Cuando en una toma de telecomunicaciones existan más de dos conectores, la toma se debe identificar únicamente utilizando el identificador de la salida/conector de telecomunicaciones menor y el identificador de la salida/conector de telecomunicaciones mayor. Ejemplo: Para una TT que tiene cuatro conectores con los siguientes identificadores: ST001, ST002, ST003 y ST004, su identificador es: TT ST001-ST004. Si los identificadores contenidos en una TT no son consecutivos, el identificador de la TT debe contener todos los identificadores de los conectores/salida de telecomunicaciones separados con el signo "/".

Punto de consolidación.		
Identificador:	PCO- STXXX / STYYY	
Estructura	PCO	= PCO = Punto de consolidación.
	STXXX	= Identificación de la primera posición de terminación del PCO, que corresponde al identificador de la salida/conector de telecomunicaciones con la cual se interconecta.
	STYYY	= Identificación de la última posición de terminación del PCO, que corresponde al identificador de la salida/conector de telecomunicaciones con la cual se interconecta o se interconectará .

Tabla 2.17. Punto de Consolidación

Nota: En el proceso de diseño de las redes de cableado, se debe considerar que las salidas/conectores de telecomunicaciones que sean alimentadas por un punto de consolidación deben ser consecutivos.

Salida multiusuario de telecomunicaciones.		
Identificador:	SMT-STXXX / STYYY	
Estructura	SMT	= Salida multiusuario de telecomunicaciones
	STXXX	= Identificador de la salida/conector de telecomunicaciones con el número menor de los contenidos en la toma de telecomunicaciones.
	STYYY	= Identificador de la salida/conector de telecomunicaciones con el número mayor de los contenidos en la toma de telecomunicaciones.

Tabla 2.18. Salida multiusuario de telecomunicaciones

Nota: En el proceso de diseño de las redes de cableado, se debe considerar que las salidas/conector de telecomunicaciones contenidas en una salida multiusuarios deben ser consecutivos.

2.6.1.5. Canalizaciones Horizontales

Tubería horizontal.		
Identificador:	TH XXX –[Material]ZZ-YYY	
Estructura	TH	= Tubo horizontal.
	XXX	= Número consecutivo.
	Material	= AG: Acero galvanizado, AL: Aluminio.
	AGCP	= Acero galvanizado con cubierta de PVC.
	ALCP	= Aluminio con cubierta de PVC.
	ZZ	= Cédula del tubo (20 o 40).
	YYY	= Diámetro del tubo en mm.

Tabla 2.19. Tubería Horizontal

Bajante con canaleta.		
Identificador:	BCC XXX –[Material]	
Estructura	BCC	= Bajante con canaleta
	XXX	= Número consecutivo
	[Material]	= AL: Aluminio, PVC: Plástico, AG: Acero galvanizado.

Tabla 2.20. Bajante con canaleta

2.6.1.6. Canalizaciones principales de Edificio.

Tubería.		
Identificador:	CAPE-T[Tipo] XXX -[Material]ZZ-YYY	
Estructura	CAPE	= Canalización principal de edificio.
	T	= Tubo.
	[Tipo]	= H: Horizontal, V:Vertical.
	XXX	= Número consecutivo.
	[Material]	= AG: Acero galvanizado, AL : Aluminio. AGCP: Acero galvanizado con cubierta de PVC. ALCP: Aluminio con cubierta de PVC.
	ZZ	= Cédula del tubo (20 o 40).
	YYY	= Diámetro del tubo en mm.

Tabla 2.21. Tubería

2.6.1.7. Canalizaciones principales de Campus.

Tubería exterior.		
Identificador:	CAPC-TEXXX -[Material]ZZ-YYY	
Estructura	CAPC	= Canalización principal de Campus.
	TE	= Tubo exterior.
	XXX	= Número consecutivo.
	[Material]	= AG: Acero galvanizado, AL : Aluminio, AGCP: Acero galvanizado con cubierta de PVC, ALCP: Aluminio con cubierta de PVC.
	ZZ	= Cédula del tubo (20 o 40)
	YYY	= Diámetro del tubo en mm.

Tabla 2.22. Tubería Exterior

Canalización de entrada al Campus.		
Identificador:	CAPC-CAE XXX -[Material]ZZ-YYY	
Estructura	CAPC	= Canalización Principal de Campus.
	CAE	= Canalización de entrada.
	XXX	= Número consecutivo.
	[Material]	= AG: Acero galvanizado, AL : aluminio, AGCP: Acero galvanizado con cubierta de PVC, ALCP: Aluminio con cubierta de PVC, PVCP: PVC pesado.
	ZZ	= Cédula del tubo (20 o 40).
	YYY	= Diámetro de tubo en mm.

Tabla 2.23. Canalización de entrada al Campus

2.6.1.8. Identificadores para equipos terminales.

Aparato telefónico UTEG	
Identificador:	[Clave]XXXXX
Estructura:	[Clave] = Clave larga distancia de la red de la UTEG XXXXX = Número telefónico de la red de la UTEG (5 dígitos)

Tabla 2.24. Aparato telefónico UTEG

Aparato telefónico externo.	
Identificador:	[Clave]XXXXXXX
Estructura	[Clave] = Clave larga distancia de la red pública del proveedor externo. XXXXXXX = Número telefónico de la red pública del proveedor externo.

Tabla 2.25. Aparato telefónico Externo

Computadoras.	
Identificador:	PC-[Dirección]
Estructura:	PC = Computadora [Direccion] = Dirección IP asignada a la computadora

Tabla 2.26. Computadoras

Tablero eléctrico (Centro de carga).	
Identificador:	CECAXXX
Estructura:	CECA = Centro de carga XXX = Consecutivo

Tabla 2.27. Tablero Eléctrico

Cables eléctricos para alimentación de equipos.	
Identificador:	CELECTXXX
Estructura:	CELECT = Cable eléctrico XXX = Consecutivo del cable

Tabla 2.28. Cables eléctricos par alimentación de equipos

Contacto eléctrico múltiple.	
Identificador:	CEMULXXX
Estructura:	CEMUL = Contacto eléctrico múltiple XXX = Consecutivo del contacto

Tabla 2.29 Contacto eléctrico Múltiple

Interruptor de tablero eléctrico.	
Identificador:	[Tablero eléctrico]-I-XXX
Estructura	[Tablero electrico] = Identificador del centro de carga donde se encuentra instalado el interruptor. I = Interruptor. XXX = Número del interruptor.

Tabla 2.30. Interruptor de tablero eléctrico

2.6.1.9. Ejemplos de Etiquetado

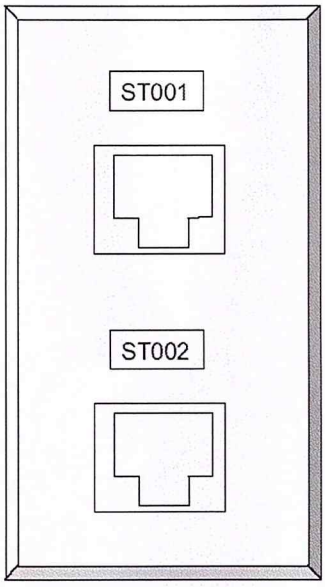


Figura 2.33. Ejemplo de etiquetado para una toma de telecomunicaciones doble

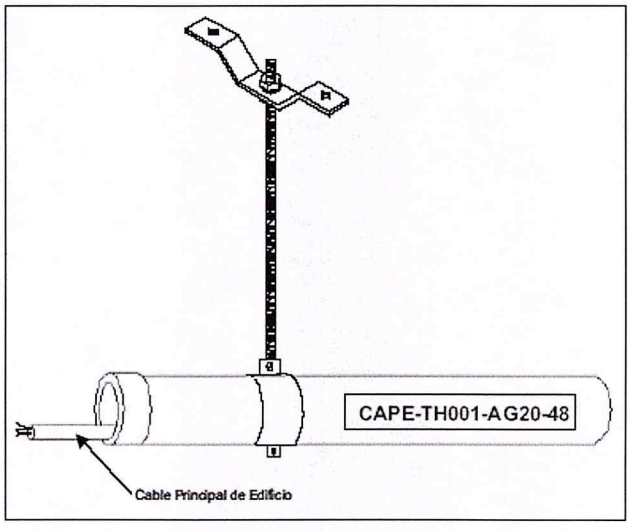


Figura 2.34. Ejemplo de etiquetado de tubería

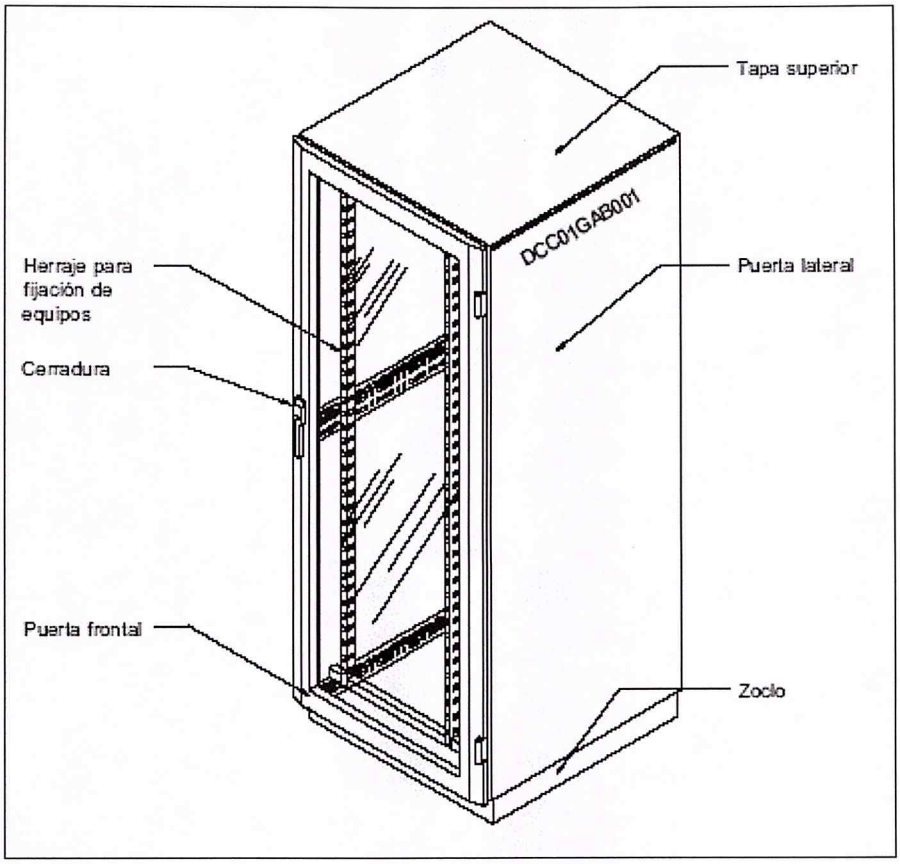


Figura 2.35. Ejemplo de etiquetado de un gabinete

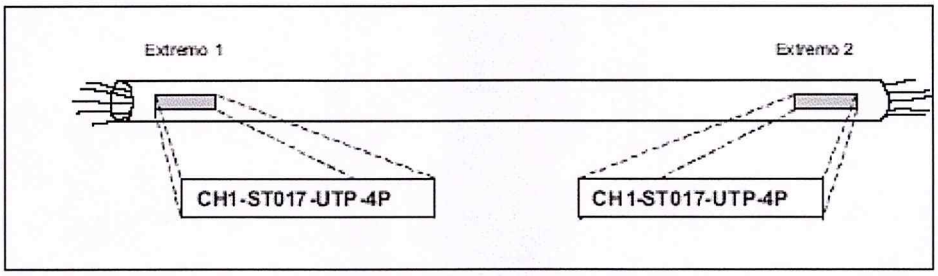


Figura 2.36. Ejemplo de etiquetado de cable horizontal

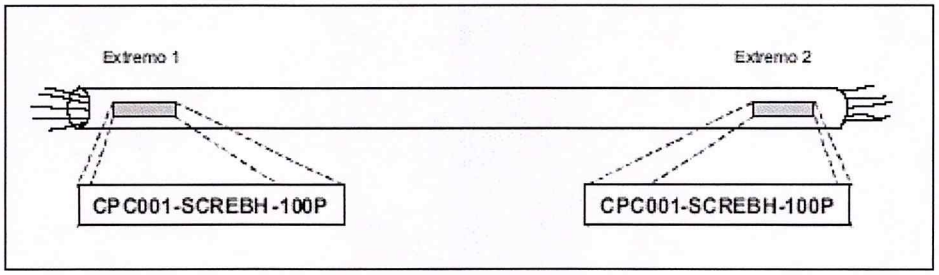


Figura 2.37. Ejemplo de etiquetado de cable principal

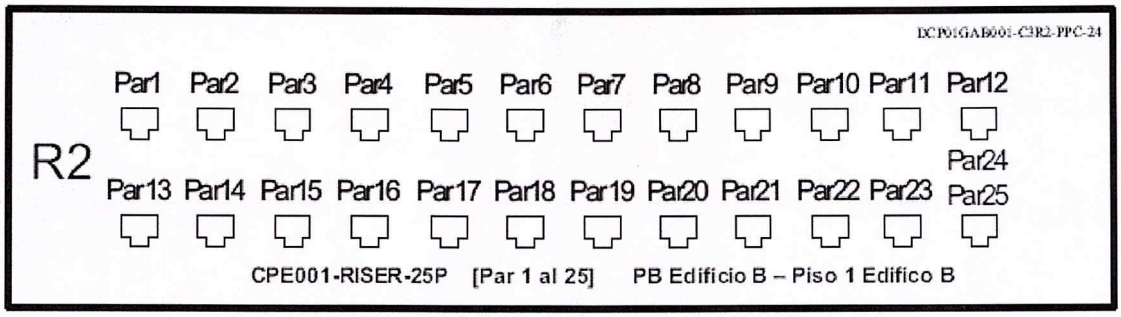


Figura 2.38. Ejemplo de etiquetado en panel de parcheo de cobre para terminación de cableado principal

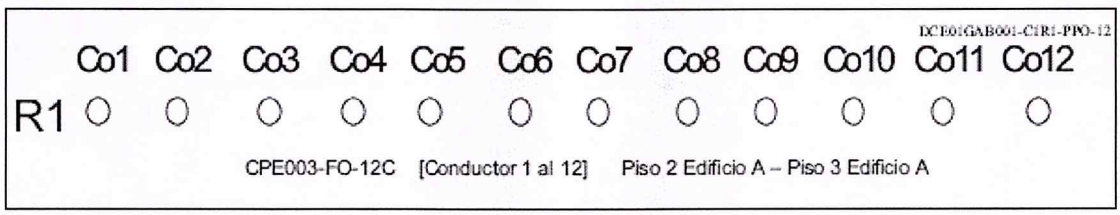


Figura 2.39. Ejemplo de etiquetado en panel de parcheo óptico con adaptadores simples para terminación de cableado principal

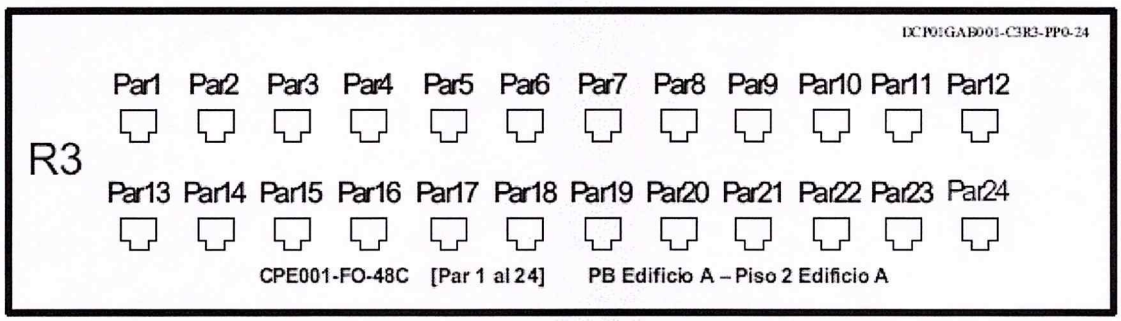


Figura 2.40. Ejemplo de etiquetado en panel de parcheo óptico con adaptadores dúplex para terminación de cableado principal

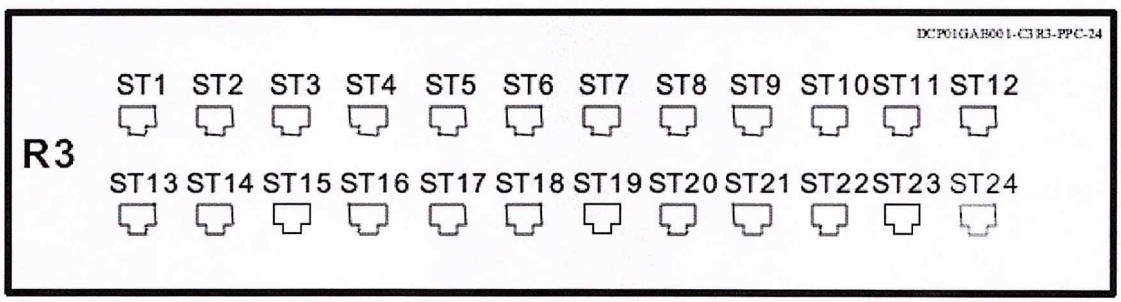


Figura 2.41. Ejemplo de etiquetado en panel de parcheo para terminación de cableado horizontal

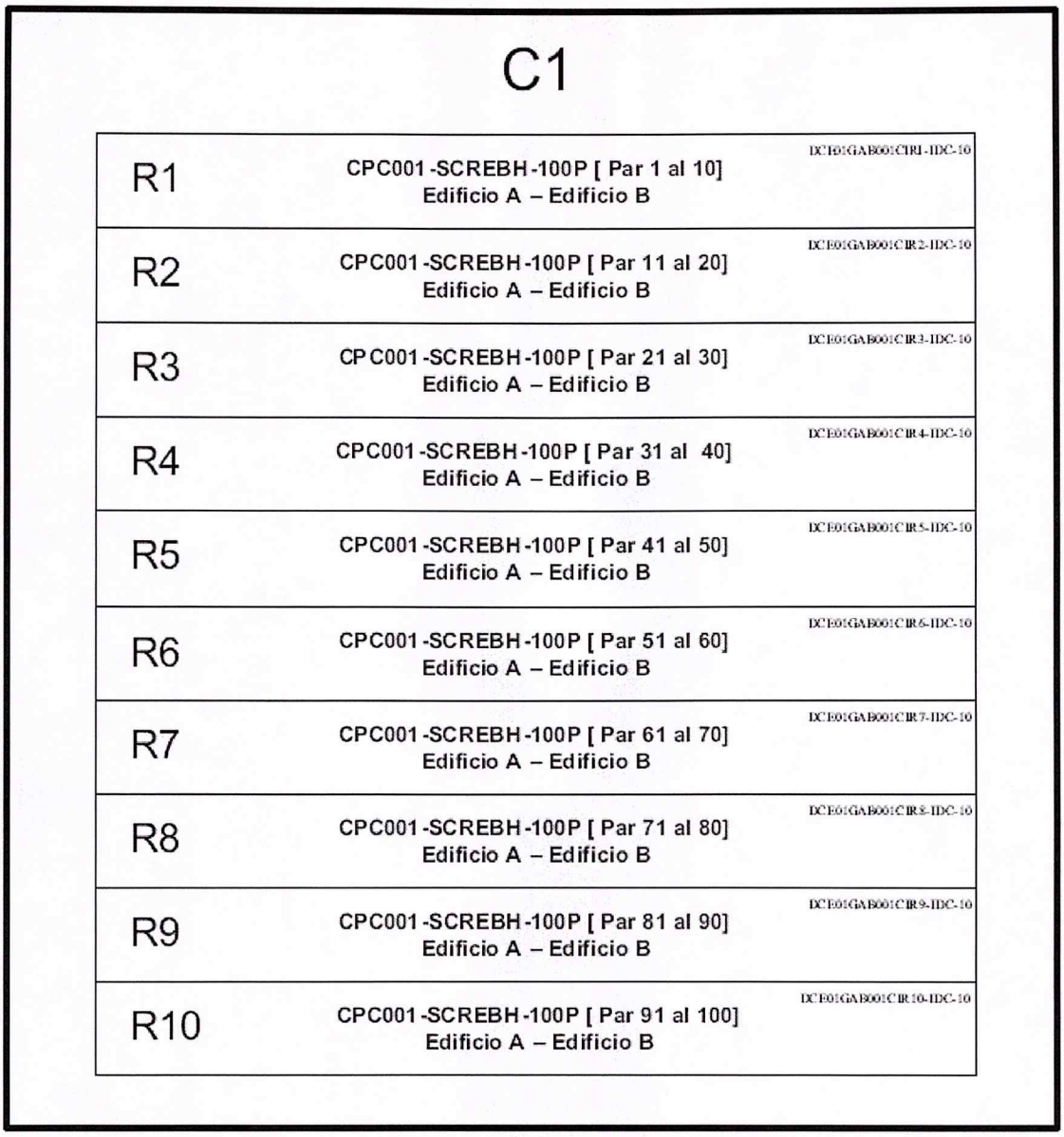


Figura 2.42. Ejemplo de etiquetado en bloque de conexión IDC para cableado principal (alternativa1)

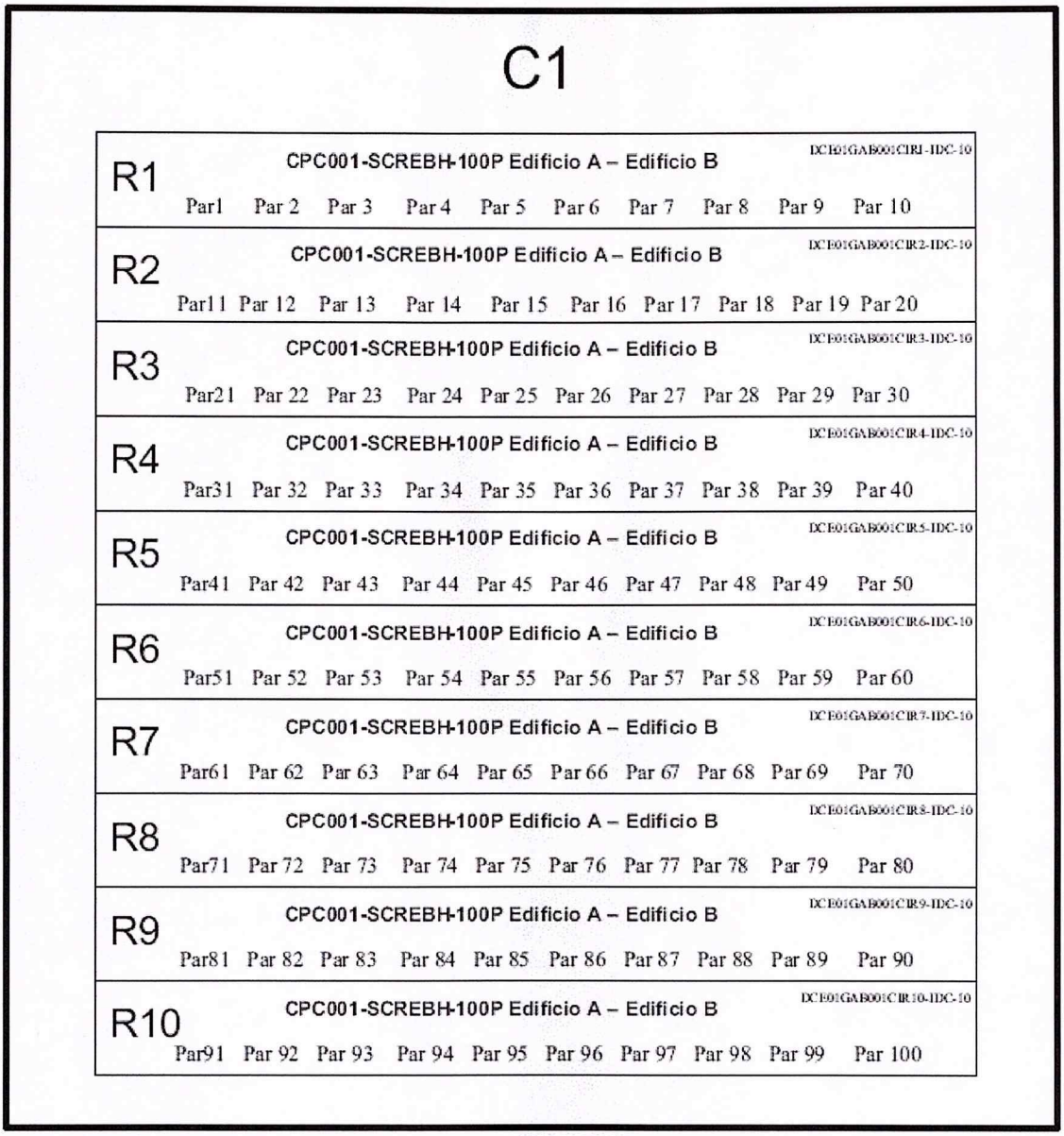


Figura 2.43. Ejemplo de etiquetado en bloque de conexión IDC para cableado principal (Alternativa2)

2.7. Estudio técnico de las Redes Inalámbricas

2.7.1. Medios de Transmisión

Los medios de transmisión de las redes inalámbricas se da mediante el enlace por medio de señales de frecuencias de ondas , esto depende de según su velocidad y tasa de transferencia.

2.7.1.1. Radio

De 10 KHz – 100 MHz. Las ondas de radio son fáciles de generar, puede cruzar distancias largas, y entrar fácilmente en los edificios. Son omnidireccionales, lo cual implica que los transmisores y recibidores no tienen que ser alineados.

- Las ondas de frecuencias bajas pasan por los obstáculos, pero el poder disminuye con la distancia.
- Las ondas de frecuencias más altas van en líneas rectas. Rebotan en los obstáculos y la lluvia las absorbe.

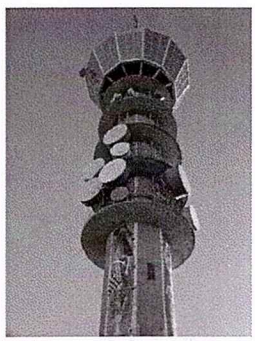


Figura 2.44. Antenas de Radio

2.7.1.2. Microondas

Con el término microondas se identifica a las ondas electromagnéticas en el espectro de frecuencias comprendido entre 300 MHz y 300 GHz. El periodo de una señal de microondas está en el rango de 3 ns a 3 ps, y la correspondiente longitud de onda en el rango de 1 m a 1 mm. Algunos autores proponen que el espectro electromagnético que comprenden es de 1

GHz a 30 GHz, es decir, a longitudes de onda entre 30 cm a 1 cm. A las señales con longitud de onda en el orden de los milímetros se les llama ondas milimétricas.

Las microondas tienen longitudes de onda aproximadamente en el rango entre 30 cm (frecuencia=1 GHz) a 1 mm (300 GHz). La existencia de ondas electromagnéticas, de las cuales las microondas forman parte del espectro de alta frecuencia, fueron predichas por Maxwell en 1864, a partir de sus famosas Ecuaciones de Maxwell.

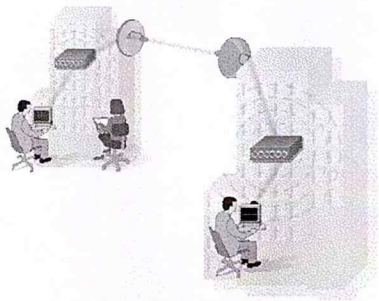


Figura 2.45. Vía Microondas

En 1888, Heinrich Rudolf Hertz fue el primero en demostrar la existencia de ondas electromagnéticas mediante la construcción de un aparato para producir ondas de radio.
El rango de las microondas incluye las bandas de radiofrecuencia de UHF (ultra-high frequency, frecuencia ultra alta en español) (0.3-3 GHz), SHF (super-high frequency, super alta frecuencia) (3-30 GHz) y EHF (extremely high frequency, extremadamente alta frecuencia) (30-300 GHz).

El espectro de microondas es usualmente definido como energía electromagnética en el rango entre 1 GHz y 1000 GHz. Las aplicaciones más comunes de las microondas están en el rango de 1 y 40 GHz.

Bandas de frecuencia de microondas	
Designación	**Rango de frecuencias**
Banda L	1 a 2 GHz
Banda S	2 a 4 GHz
Banda C	4 a 8 GHz
Banda X	8 a 12 GHz
Ku band	12 a 18 GHz
BandaK	18 a 26 GHz
Ka band	26 a 40 GHz
Banda Q	30 a 50 GHz
BandaU	40 a 60 GHz
Banda V	50 a 75 GHz
Banda E	60 a 90 GHz
Banda W	75 a 110 GHz
Banda F	90 a 140 GHz
Banda D	110 a 170 GHz

Tabla 2.31. Rangos de Frecuencia

2.7.1.3. Satélite

Las señales llegan al satélite desde la estación en tierra por el "haz ascendente" y se envían a la tierra desde el satélite por el "haz descendente". Para evitar interferencias entre los dos haces, las frecuencias de ambos son distintas. Las frecuencias del haz ascendente son mayores que las del haz descendente, debido a que cuanto mayor sea la frecuencia se produce mayor atenuación en el recorrido de la señal, y por tanto es preferible transmitir con más potencia desde la tierra, donde la disponibilidad energética es mayor.

Para evitar que los canales próximos del haz descendente interfieran entre sí, se utilizan polarizaciones distintas. En el interior del satélite existen unos bloques denominados transpondedores, que tienen como misión recibir, cambiar y transmitir las frecuencias del satélite, a fin de que la información que se envía desde la base llegue a las antenas receptoras.

Cuando se trata de satélites de comunicaciones, la porción del espectro radioeléctrico que utilizarán lo determina prácticamente todo: la capacidad del sistema, la potencia y el precio. Las longitudes de onda diferentes poseen propiedades diferentes. Las longitudes de onda largas pueden recorrer grandes distancias y atravesar obstáculos. Las grandes longitudes de onda pueden rodear edificios o atravesar montañas, pero cuanto mayor sea la frecuencia (y por tanto, menor la longitud de onda), más fácilmente pueden detenerse las ondas.

Cuando las frecuencias son lo suficientemente altas (hablamos de decenas de gigahertz), las ondas pueden ser detenidas por objetos como las hojas o las gotas de lluvia, provocando el fenómeno denominado "rain fade". Para superar este fenómeno se necesita bastante más potencia, lo que implica transmisores más potentes o antenas más enfocadas, que provocan que el precio del satélite aumente.

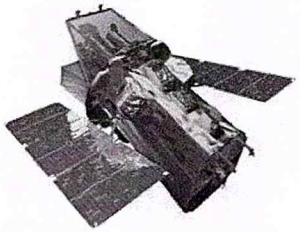


Figura 2.46. Satélite

La ventaja de las frecuencias elevadas (las bandas Ku y Ka) es que permiten a los transmisores enviar más información por segundo. Esto es debido a que la información se deposita generalmente en cierta parte de la onda: la cresta, el valle, el principio o el fin. El compromiso de las altas frecuencias es que pueden transportar más información, pero necesitan más potencia para evitar los bloqueos, mayores antenas y equipos más caros. Concretamente, las bandas más utilizadas en los sistemas de satélites son:

Banda	Velocidad MHz
Banda P	200-400 MHz
Banda L	1530-2700 MHz
Banda S	2700-3500 MHz
Banda C	3700-4200 MHz
	4400-4700 MHz
	5725-6425 MHz
Banda X	7900-8400 MHz
Banda Ku1	10,7-11,75 GHz (Banda PSS)
Banda Ku2	11,75-12,5 GHz (Banda DBS)
Banda Ku3	12,5-12,75 GHz (Banda Telecom)
Banda Ka	17,7-21,2 GHz
Banda K	27,5-31 GHz

Tabla 2.32 Velocidad Mhz

1 MHz= 1.000.000 Hz

1 GHz= 1.000 MHz = 1.000.000.000 Hz

- Banda L:

  Rango de frecuencias: 1,53-2,7 GHz.

  Ventajas: grandes longitudes de onda pueden penetrar a través de las estructuras terrestres; precisan transmisores de menor potencia. Inconvenientes: poca capacidad de transmisión de datos.

- Banda Ku:

  Rango de frecuencias: en recepción 11,7-12,7 GHz, y en transmisión 14-17,8 GHz. Ventajas: longitudes de onda medianas que traspasan la mayoría de los obstáculos y transportan una gran cantidad de datos. Inconvenientes: la mayoría de las ubicaciones están adjudicadas.

2.7.1.4. Wi-fi

Wi-Fi (inglés Wireless Fidelity) es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Creado para ser utilizado en redes locales inalámbricas, es frecuente que en la actualidad también se utilice para acceder a Internet.

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.

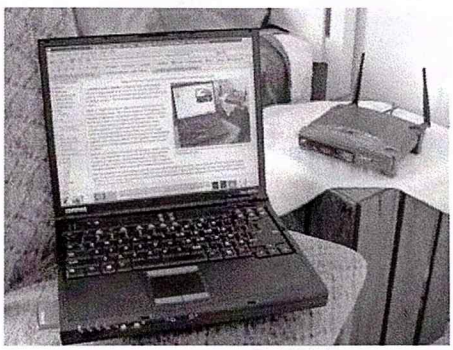


Figura 2.47. Laptop conectada por Wi-fi

Hay tres tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado. Un cuarto estándar, el 802.11n, está siendo elaborado y se espera su aprobación final para la segunda mitad del año 2007. Los estándares IEEE 802.11b e IEEE 802.11g disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. Existe también un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz a una velocidad de 108 Mbps.

Aunque estas velocidades de 108 Mbps son capaces de alcanzarse ya con el estándar 802.11g gracias a técnicas de aceleramiento que consiguen duplicar la transferencia teórica. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N, sin embargo, no se sabe si serán compatibles ya que el estándar no está completamente revisado y aprobado.

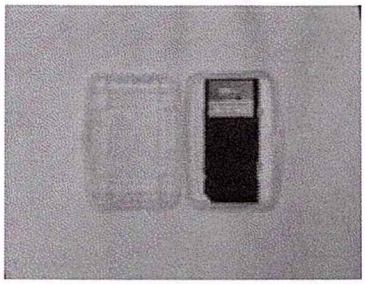


Figura 2.48. Tarjeta Wi-Fi para PalmOne.

En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además no existen otras tecnologías (Bluetooth, micro-ondas, etc) que la estén utilizando, por lo tanto hay muy pocas interferencias.

La tecnología inalámbrica Bluetooth también funciona a una frecuencia de 2.4 GHz por lo que puede presentar interferencias con Wi-Fi, sin embargo, en la versión 1.2 y mayores del estándar Bluetooth se ha actualizado su especificación para que no haya interferencias en la utilización simultánea de ambas tecnologías.

2.8. Equipos de comunicación para redes

HUB's (Concentradores)

Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.

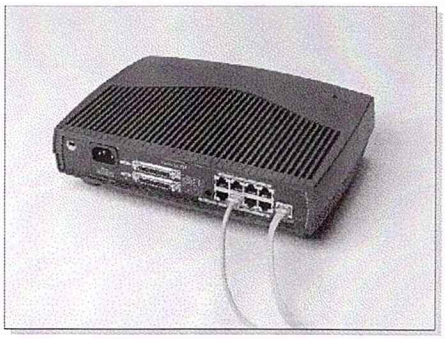


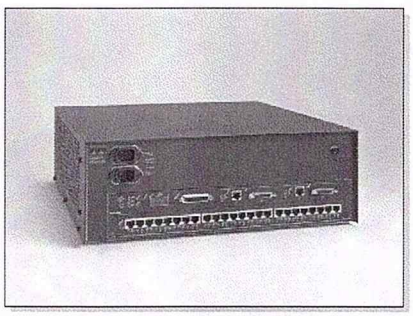
Figura 2.49. Hub

SWITCH's (Conmutadores)

Un Switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El Switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El Switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.



Cisco Catalyst 2926G

Figura 2.50. Switch

ROUTER's (Encaminadores)

Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar de brodcast y proporcionar seguridad, control y redundancia entre dominios individuales de brodcast, también puede dar servicio de firewall y un acceso económico a una WAN.

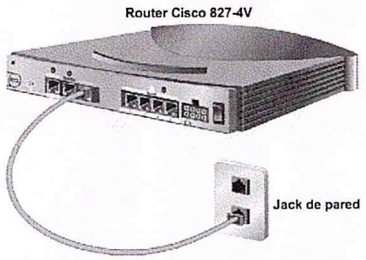


Figura 2.51. Router

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una desición más inteligente que al Switch, al momento de reenviar los paquetes.

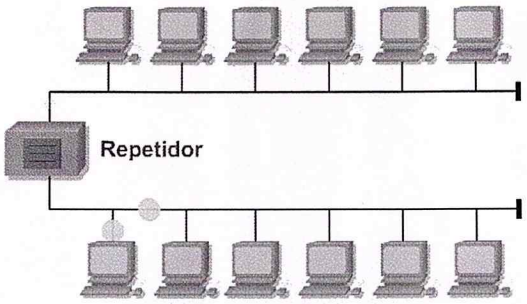
El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

REPETIDORES

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.



El propósito de un repetidor es el de regenerar y sincronizar los bits que conforman las señales en un red.

Figura 2.52. Esquema de un Repetidor

BRIDGE's (Puentes)

Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

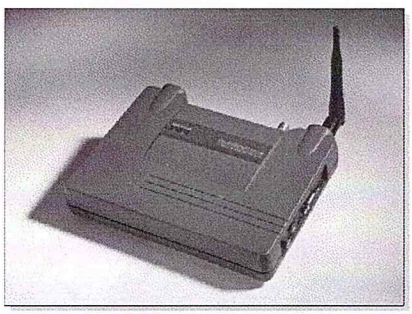


Figura 2.53. Puente

GATEWAY's

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

SERVIDORES

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos

compartidos. Así un Terminal conectado a uno de estos dispositivos puede establecer sesiones contra varios ordenadores multiusuario disponibles en la red. Igualmente, cualquier sistema de la red puede imprimir en las impresoras conectadas a un servidor.

MODEM's

Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; son los encargados de la modulación y demodulación de señales electrónicas para que puedan ser procesadas por las computadoras. Los módems pueden ser externos (un dispositivo de comunicación) o interno (dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora).

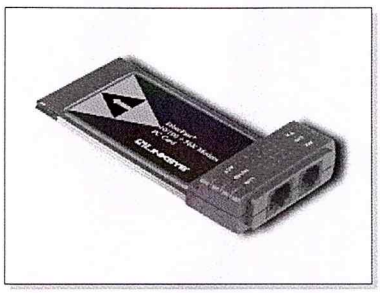


Figura 2.54. Modem

ACCESS POINT's (Punto de acceso de Ethernet inalámbrico)

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) 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. Este o su antena son normalmente colocados 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 inalámbrica.

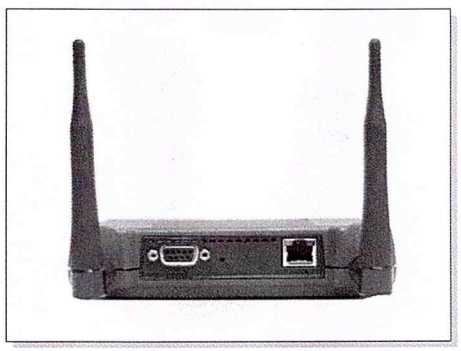


Figura 2.55. Access Point

CAPITULO 3: PROTOCOLOS Y ARQUITECTURA DE REDES

En este capitulo se va a hacer un análisis sobre los protocolos y las arquitecturas de las Redes

3.1. Protocolo

Los protocolos son un conjunto de Reglas para el cumplimiento de una tarea específica dentro del proceso de comunicación informática. Dentro de las funciones básicas de los protocolos tenemos:

- Conexión física (interfases) de los equipos a los Medios de Transmisión
- Manejo de Errores (de la conexión Física)
- Manejo de Congestión (Control de flujo)
- Determinar la Ruta más adecuada (optimización).
- Asegurar la interoperabilidad de las Aplicaciones

Aunque ciertos aspectos de los Protocolos tienen que ver con el Hardware, en general son implementados por medios de Software, salvo en el caso de los protocolos para la conexión Física.

- Ciertos Protocolos cumplen funciones similares pero otros cumplen funciones complementarias.

    - El usuario puede escoger entre uno u otro
    - Se debe emplear un "conjunto" de Protocolos para cumplir el proceso de comunicación.
    - El "conjunto" o "familia" de protocolos es denominado Arquitectura.

3.2 Arquitectura de Redes

La arquitectura de redes, se refiere básicamente al conjunto de varios protocolos que permiten solucionar todos los problemas de transmisión de información entre dos o más nodos. Si bien

el término "Arquitectura" podría ser entendido desde el punto de vista físico, generalmente se refiere a la estructura de protocolos.

Debe existir una coordinación entre todos los Protocolos utilizados en el proceso de comunicación. Es decir, los Protocolos deben ser "diseñados" en base a un "patrón común". Los protocolos de una arquitectura operan en forma jerárquica (secuencial). La arquitectura define los niveles jerárquicos, conocidos como "capas" o "Protocol Layers", cada capa esta compuesta de uno o más Protocolos afines (funciones similares).

3.2.1. Diseño de una Arquitectura Elemental

Diseñar una arquitectura requiere "agrupar" funciones comunes. Las funciones más relevantes de una arquitectura son:

- Interfase con la Aplicación
- Interfases con el medio físico
- Otras funciones

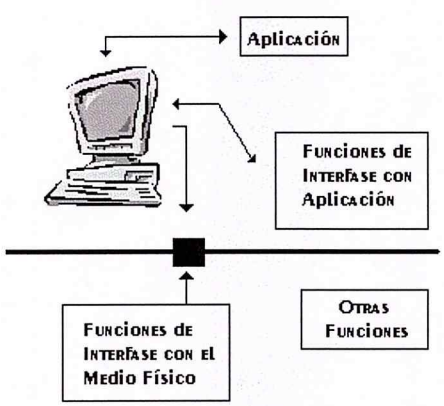


Figura 3.1. Arquitectura Elemental

En general existen muchas formas de agrupar las funciones del software de Redes. Al principio esto dio origen a la proliferación de Arquitecturas. Inicialmente (años 60's y 70's) habían muchas arquitecturas: DECnet, XNS (Xerox Network System), SNA (System Network Architecture), etc.

3.2.2. Arquitecturas comúnmente Usadas

En la actualidad la Arquitectura mas usada es la TCP/IP (Transmisión Control Protocol / Internet Protocol). Otras arquitecturas de hoy son:

- SNA / APPN : Sisytemas IBM
- IPX / SPX: Redes Novell
- Apple Talk: Computadoras Apple/ Macintosh

A fin de garantizar la interoperabilidad entre las diversas Arquitecturas, se hizo necesario crear un modelo de referencia llamado OSI : Open System Interconnection, ideada por la ISO a fines de los 70's.

3.3. Arquitectura Referencial OSI

3.3.1. Características Generales

Es un modelo Conceptual que define un patrón general a ser seguido por otras Arquitecturas de Redes, en busca de interoperabilidad entre ellas. El modelo agrupa las funciones y Protocolos en siete grupos o capas.

El modelo OSI es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final, este modelo es el más conocido y el mas usado para describir los entornos de red.

3.3.2. Capas OSI

Figura 3.2. Capas OSI

3.3.3. Características de cada capa

CAPA 1: FÍSICA

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (p.e. tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es uni o bidireccional (símplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos, dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.
Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

CAPA 2: DE ENLACE DE DATOS

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

CAPA 3: RED

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés routers y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande). La PDU de la capa 3 es paquetes.

CAPA 4: TRANSPORTE

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra

característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.

Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío.

Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación.

Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Para finalizar, podemos definir a la capa de transporte como:
Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmentos.

CAPA 5: SESION

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:
1 Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
2 Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
3 Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de

verificación en lugar de repetirla desde el principio. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén trasmitiendo archivos.

CAPA 6: PRESENTACIÓN

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.
Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor

CAPA 7: APLICACIÓN

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (HyperText Transfer Protocol) el protocolo bajo la www
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros
- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de tcp/ip) envío y distribución de correo electrónico
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name System)

3.4. Introducción a la arquitectura TCP/IP

El TCP/IP surgió con el objeto de ser utilizado en Internet.

Es la arquitectura de redes de computadoras de mayor popularidad en la actualidad, no es necesariamente la mejor arquitectura, adolece de varias limitaciones, aun así ha sido implementada para casi toda plataforma de Hardware y Software.

No se ciñe estrictamente al modelo OSI, pero en forma general incluye todas las funciones estipuladas en OSI.

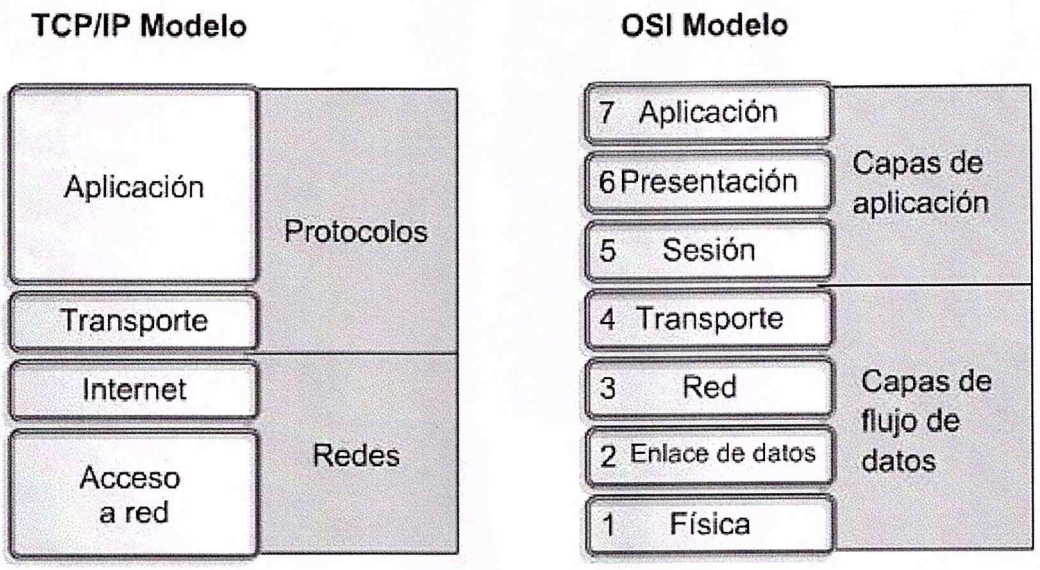


Figura 3.3. TCP/IP vs OSI

Es independiente de las Capas Físicas y de Enlace de Datos, opera sobre cualquier tipo de enlace físico, ya sea dedicados o compartidos. No define ningún Protocolo para dichas Capas, pero esto no significa que no requiera de dichas Capas, ya que son indispensables en toda arquitectura.

La capa de aplicación determinada como un programa de uso común, intercambia información con otros similares. En el caso de los programas para navegar en la Internet, se requieren varios Protocolos en la capa de aplicación a continuación se detallan algunos protocolos:

- URL (SEÑALA DONDE ENCONTRAR LA INFORMACION)
- HTTP (INDICA COMO TRANSFERIR LA INFORMACION)
- HTML (DETERMINA COMO MOSTRAR LA INFORMACION)

  Es un lenguaje de hipertexto que es interpretado por el browser, permite hacer referencias a ciertas palabras (texto) del documento, permite incluir gráficos y otros objetos.

Las aplicaciones de TCP/IP son:

- Correo electrónico (mail)
- Existen diversos programas disponibles como el Netscape, Outlook, etc.
- Login remoto (Telnet)
- Transferencia de archivos (ftp)
- Servidores Gopher (motor de bus)
- Herramientas de búsqueda: Archie, Verónica
- Servidores httpd
- Browsers gráficos y de texto
- Servidores y clientes de noticias
- Servidores y clientes Chat

Los Protocolos a nivel de aplicación TCP/IP son:

- **Protocolo de transferencia de archivos (FTP):** es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.

- **Protocolo trivial de transferencia de archivos (TFTP):** es un servicio no orientado a conexión que utiliza el Protocolo de datagrama de usuario (UDP). Los Routers utilizan el TFTP para transferir los archivos de configuración e imágenes IOS de Cisco y para transferir archivos entre los sistemas que admiten TFTP. Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.

- **Sistema de archivos de red (NFS):** es un conjunto de protocolos para un sistema de archivos distribuido, desarrollado por Sun Microsystems que permite acceso a los archivos de un dispositivo de almacenamiento remoto, por ejemplo, un disco rígido a través de una red.

- **Protocolo simple de transferencia de correo (SMTP):** administra la transmisión de correo electrónico a través de las redes informáticas. No admite la transmisión de datos que no sea en forma de texto simple.

- **Emulación de terminal (Telnet):** Telnet tiene la capacidad de acceder de forma remota a otro computador. Permite que el usuario se conecte a un host de Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.

- **Protocolo simple de administración de red (SNMP):** es un protocolo que provee una manera de monitorear y controlar los dispositivos de red y de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.

- **Sistema de denominación de dominio (DNS):** es un sistema que se utiliza en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP.

3.4.1. Comparación entre el modelo OSI y el TCP/IP

La siguiente es una comparación de los modelos OSI y TCP/IP comparando sus similitudes y diferencias:

Similitudes entre los modelos OSI y TCP/IP:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación por paquetes y no de conmutación por circuito.
- Los profesionales de networking deben conocer ambos modelos.

Diferencias entre los modelos OSI y TCP/IP:

- TCP/IP combina las capas de presentación y de sessión en una capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.

La Internet se desarrolla de acuerdo con los estándares de los protocolos TCP/IP. El modelo TCP/IP gana credibilidad gracias a sus protocolos. A diferencia, en general, las redes no se construyen a base del protocolo OSI. El modelo OSI se utiliza como guía para comprender el proceso de comunicación.

3.5. Direcciones IP

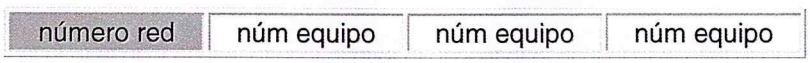
El Protocolo Internet (IP) es la implementación más conocida de un esquema de direccionamiento de red jerárquico: IP es el protocolo de red que usa Internet. A medida que la información fluye por las distintas capas del modelo OSI, los datos se encapsulan en cada capa. En la capa de red, los datos se encapsulan en paquetes (también denominados datagramas). IP determina la forma del encabezado del paquete IP (que incluye información de direccionamiento y otra información de control) pero no se ocupa de los datos en sí (acepta cualquier información que recibe desde las capas superiores). Es decir, se preocupa de llevar el contenido al destino gracias a su direccionamiento y los routers, pero no contiene datos en si.

El número de red de una dirección IP identifica la red a la cual se encuentra conectado un dispositivo. La porción host de una dirección IP identifica el dispositivo específico de esta red. Como las direcciones IP están formadas por cuatro bytes separados por puntos, se pueden utilizar uno, dos o tres de estos bytes para identificar el número de red. De modo similar, se pueden utilizar hasta tres de estos bytes para identificar la parte de host de una dirección IP.

Hay tres clases de direcciones IP que una organización puede recibir de parte del proveedor de Internet: Clase A, B ó C que dependen del tamaño de la red, así las A soportan mas equipos que la B y C. En la actualidad, se reservan las direcciones Clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como Hewlett Packard) y las direcciones Clase B para las medianas empresas. Se otorgan direcciones Clase C para todos los demás solicitantes

- **Clase A**

Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección Clase A siempre es 0. Un ejemplo de una dirección IP Clase A es 124.95.44.15. El primer byte, 124, identifica el número de red. Los administradores internos de la red asignan los restantes valores. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase A es verificar el primer byte de su dirección IP, cuyo valor debe estar entre 0 y 126.



Todas las direcciones IP Clase A utilizan solamente los primeros 8 bits para identificar la parte de red de la dirección. Los tres bytes restantes son para los equipos de la red. A cada una de las redes que utilizan una dirección IP Clase A se les pueden asignar hasta 2 elevado a la 24 potencia (2^24), o 16.777.214 direcciones IP posibles para los dispositivos que están conectados. Está claro que son organismos muy grandes para poder gestionar mas de 16 millones de ordenadores.

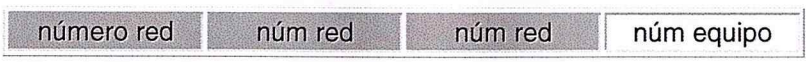
- **Clase B**

Los primeros 2 bits de una dirección Clase B siempre son 10 (uno y cero). Un ejemplo de una dirección IP Clase B es 151.10.13.28. Los dos primeros bytes identifican el número de red. Los otros dos bytes son para numerar los equipos de la red. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase B es verificar el primer byte de su dirección IP. Las direcciones IP Clase B siempre tienen valores que van del 128 al 191 en su primer byte.

Todas las direcciones IP Clase B utilizan los primeros 16 bits para identificar la parte de red de la dirección. Los dos bytes restantes de la dirección IP se encuentran reservados para la porción del host de la dirección. Cada red que usa un esquema de direccionamiento IP Clase B puede tener asignadas hasta 2 a la 16ta potencia (2^16) ó 65.534 direcciones IP posibles a dispositivos conectados a su red.

- **Clase C**

Los 3 primeros bits de una dirección Clase C siempre son 110 (uno, uno y cero). Un ejemplo de dirección IP Clase C es 201.110.213.28. Los tres primeros bytes identifican el número de red. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase C es verificar el primer bytes de su dirección IP. Las direcciones IP Clase C siempre tienen valores que van del 192 al 223 en su primer bytes.



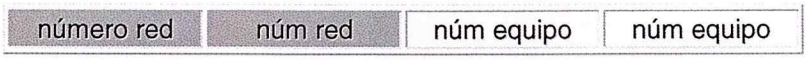
Todas las direcciones IP Clase C utilizan los primeros 24 bits para identificar la porción de red de la dirección. Sólo se puede utilizar el último byte de una dirección IP Clase C para la parte de la dirección que corresponde al equipo. A cada una de las redes que utilizan una dirección IP Clase C se les pueden asignar hasta 28 (menos 2), o 254, direcciones IP posibles para los dispositivos que están conectados a la red

Clases de direcciones IP				
	1 byte 8 bits	1 byte 8 bits	1 byte 8 bits	1 byte 8 bits
Clase A	número red	núm equipo	núm equipo	núm equipo
Clase B	número red	núm red	núm equipo	núm equipo
Clase C	número red	núm red	núm red	núm equipo

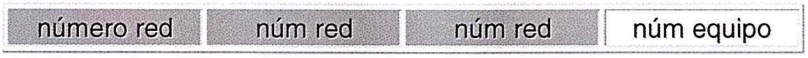
Tabla 3.1. Clases de direcciones IP

Así que para facilitar la administración los que diseñaron esto de las direcciones IP dividieron éstas en tres tipos. Unas pocas de clase A para los organismos mas importantes y grandes empresas, su formato es "número de red.numero de equipo.número de equipo.número de equipo". Sólo reserva un byte para definir el número de red lo que da sólo 254 redes de este tamaño. Eso si, como los otros tres bytes son para definir el equipo podemos definir 2^24 equipos--> que son mas de 16 millones de equipos.

Las clases B se usan para redes medianas:



Reserva 2^16 para definir el número de red y el resto para definir el número de equipo. Tenemos en total posibilidad de "direccionar" hasta 65.000 equipos.
Finalmente la de clase C:



Que define muchas mas pequeñas redes: hasta 2^24. Finalmente dedica hasta 2^8 valores, que son 254 para numerar los equipos. Suficiente para pequeñas empresas.

Clases	Direcciones Privadas	Direcciones Publicas		
	Intervalos	Intervalos	Direcciónes de Red Posibles	Direcciónes de Host Posibles
A	10.0.0.0 hasta 10.255.255.255	1.xxx.xxx.xxx hasta 126.xxx.xxx.xxx	126	16'777,216
B	172.16.0.0 hasta 172.31.255.255	128.0.xxx.xxx hasta 191.255.xxx.xxx	16,384	65,536
C	192.168.0.0 hasta 192.168.255.255	192.0.0.xxx hasta 223.255.255.xxx	2'097,152	254

Tabla 3.2. Direcciones IPs Privadas y Públicas

El diseño de TCP/IP es ideal para la gran red que es Internet. Muchos de los protocolos utilizados hoy en día se diseñaron utilizando el modelo TCP/IP de cuatro capas.

Todos los dispositivos conectados a Internet que deseen comunicarse con otros dispositivos en línea deben tener un identificador exclusivo. El identificador se denomina dirección IP debido a que los Routers utilizan un protocolo de la capa tres, el protocolo IP, para encontrar la mejor ruta hacia dicho dispositivo. IPv4, la versión actual de IP, se diseñó antes de que se produjera una gran demanda de direcciones. El crecimiento explosivo de Internet ha amenazado con agotar el suministro de direcciones IP. La división en subredes, la Traducción de direcciones en red (NAT) y el direccionamiento privado se utilizan para extender el direccionamiento IP sin agotar el suministro. Otra versión de IP conocida como IPv6 mejora la versión actual proporcionando un espacio de direccionamiento mucho mayor, integrando o eliminando los métodos utilizados para trabajar con los puntos débiles del IPv4.

IPv4	
VENTAJAS	**DESVENTAJAS**
Inicio fines de los 70´s	Direcciones IP se estan agotando
Diseño poderoso y flexible	No tienen mecanismo de reserva de ancho de banda para transmisión de audio real
Soporta el crecimiento de Procesadores	
Crecimiento de Memorias	Ataques de Hackers en la red (No posee autenticación del dispositivo de origen)
Incremento de Ancho de banda en backbone de Internet	
Aumento de Usuarios	
Nueva Tecnología LAN	

Tabla 3.3. Ventajas y Desventajas de las direcciones IPv4

IPv6
CARACTERISTICAS
Direcciones mas largas: velocidad de 128 bits
Flexibilidad en el formato del header: Utiliza un conjunto de headers opcionales
Reserva de recursos: reserva recursos como retardo y ancho de banda
Posee mecanismos para extender el protocolo:Se puede adaptar a cambios o nuevas tecnologías

Tabla 3.4 Características de las direcciones IPv6

3.6. Voz sobre IP

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VozIP, VoIP, o Telefonía IP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla en forma de circuitos como una compañía telefónica convencional o PSTN.

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. Pueden ser vistos como implementaciones comerciales de la Red experimental de Protocolo de Voz (1973), inventadas por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local (LAN).

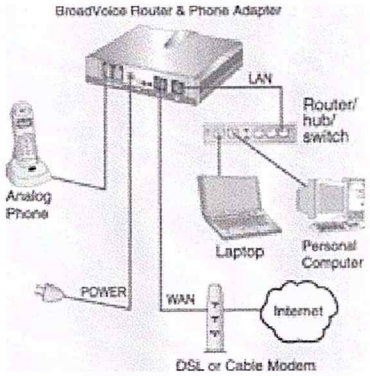


Figura 3.4. Unas soluciones típicas basadas en VoIP.

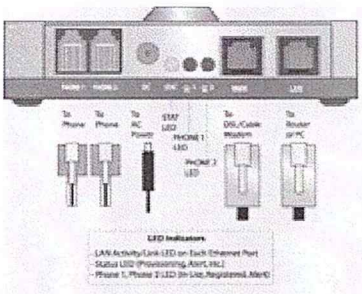


Figura 3.5. Un adaptador para un teléfono analógico corriente para conectar un teléfono común a una red VoIP.

3.6.1. Ventajas

La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada (PSTN)). Algunos ahorros en el costo son debidos a utilizar una misma red para llevar voz y datos, especialmente cuando los usuarios tienen sin utilizar toda la capacidad de una red ya existente en la cual pueden usar para VoIP sin un costo adicional. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis, en contraste con las llamadas de VoIP a PSTN que generalmente cuestan al usuario de VoIP.

Hay dos tipos de servicio de PSTN a VoIP: Llamadas Locales Directas (Direct Inward Dialling: DID) y Números de acceso. DID conecta a quien hace la llamada directamente al

usuario VoIP mientras que los Números de Acceso requieren que este introduzca el número de extensión del usuario de VoIP. Los Números de acceso son usualmente cobrados como una llamada local para quien hizo la llamada desde la PSTN y gratis para el usuario de VoIP.

3.6.1.1. Funcionalidad

VozIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas comunes:

Las llamadas telefónicas locales pueden ser automáticamente enrutadas a tu teléfono VoIP, sin importar en donde estés conectado a la red. Lleva contigo tu teléfono VoIP en un viaje, y donde quiera que estés conectado a Internet, podrás recibir llamadas.

Números telefónicos gratuitos para usar con VoIP están disponibles en Estados Unidos de América, Reino Unido y otros países de organizaciones como Usuario VoIP.

Los agentes de Call center usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a Internet lo suficientemente rápida.

Algunos paquetes de VoIP incluyen los servicios extra por los que PSTN (Red Telefónica Conmutada) normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos países, como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamadas.

3.6.1.2. Movil

Los usuarios de VoIP pueden viajar a cualquier lugar en el mundo y seguir haciendo y recibiendo llamadas de la siguiente forma:

Los subscriptores de los servicios de las líneas telefónicas pueden hacer y recibir llamadas locales fuera de su localidad. Por ejemplo, si un usuario tiene un número telefónico en la ciudad de Nueva York y está viajando por Europa y alguien llama a su número telefónico, esta se recibirá en Europa. Además si una llamada es hecha de Europa a Nueva York, esta será cobrada como llamada local, por supuesto el usuario de viaje por Europa debe tener una conexión a Internet disponible.

Los usuarios de Mensajería Instantánea basada en servicios de VoIP pueden también viajar a cualquier lugar del mundo y hacer y recibir llamadas telefónicas.

Los teléfonos VoIP pueden integrarse con otros servicios disponibles en Internet, incluyendo videoconferencias, intercambio de datos y mensajes con otros servicios en paralelo con la conversación, audio conferencias, administración de libros de direcciones e intercambio de información con otros (amigos, compañeros, etc).

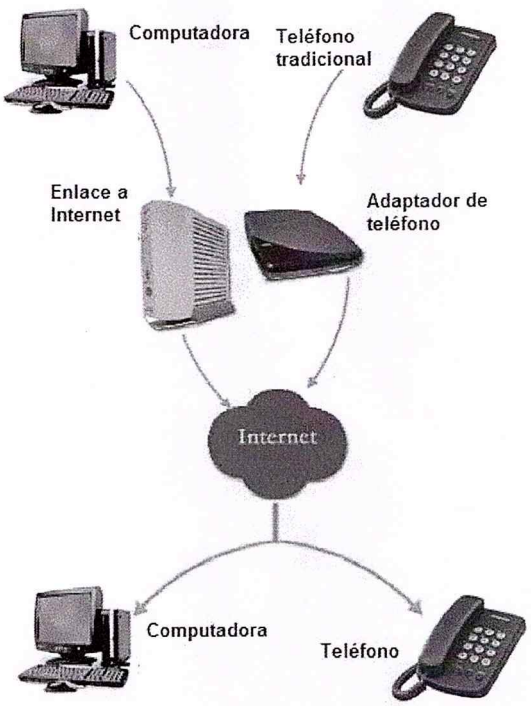


Figura 3.6. VoIP

3.6.2. Estándar VoIP (H323)

Definido en 1996 por la UIT (Unión Internacional de Telecomunicaciones) proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto.

3.6.2.1. Características Principales

Por su estructura el estándar proporciona las siguientes ventajas:

Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento. Las redes soportadas en IP presentan las siguientes ventajas adicionales:

Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.

Es independiente del hardware utilizado.

Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.
Permite la integración de Video y TPV

3.6.2.2. IP como tecnología

En muchos países del mundo, IP ha generado múltiples discordias, entre lo territorial y lo legal sobre esta tecnología, está claro y debe quedar claro que la tecnología de VoIP no es un servicio como tal, sino una tecnología que usa el Protocolo de Internet (IP) a través de la cual se comprimen y descomprimen de manera altamente eficiente paquetes de datos o datagramas, para permitir la comunicación de dos o más clientes a través de una red como la red de Internet. Con esta tecnología pueden prestarse servicios de Telefonía o Videoconferencia, entre otros.

3.6.2.3. Arquitectura de Red

El propio estándar define tres elementos fundamentales en su estructura:

Terminales: Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

Gatekeepers: Son el centro de toda la organización VoIP, y serían el sustituto para las actuales centrales. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

Gateways: Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

Con estos tres elementos, la estructura de la red VoIP podría ser la conexión de dos delegaciones de una misma empresa. La ventaja es inmediata: todas las comunicaciones entre

las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva.

Protocolos: Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión.

Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

Por orden de antigüedad (de más antiguo a más nuevo):

- H.323 - Protocolo definido por la ITU-T
- SIP - Protocolo definido por la IETF
- Megaco (También conocido como H.248) y MGCP - Protocolos de control
- Skinny Client Control Protocol - Protocolo propiedad de Cisco
- MiNet - Protocolo propiedad de Mitel
- CorNet-IP - Protocolo propiedad de Siemens
- IAX - Protocolo original para la comunicación entre PBXs Asterisk (obsoleto)
- Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype
- IAX2 - Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX
- Jingle - Protocolo abierto utilizado en tecnología Jabber
- Telme- Protocolo propietario Woip2 utilizado en la aplicación DeskCall

Como hemos visto VoIP presenta una gran cantidad de ventajas, tanto para las empresas como para los usuarios comunes. La pregunta sería ¿por qué no se ha implantado aún esta tecnología?. A continuación analizaremos los aparentes motivos, por los que VoIP aún no se ha impuesto a las telefonías convencionales.

3.6.2.4. Parámetros de la VoIP

Este es el principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP. Garantizar la calidad de servicio sobre una red IP, por medio de retardos y ancho de banda, actualmente no es posible; por eso, se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

Códecs:

La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de Códecs que garanticen la codificación y compresión del audio o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.

Entre los códecs utilizados en VoIP encontramos los G.711, G.723.1 y el G.729 (especificados por la ITU-T)

Retardo o latencia:

Una vez establecidos los retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

Calidad del servicio:

La calidad de servicio se está logrando en base a los siguientes criterios:

La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.

Compresión de cabeceras aplicando los estándares RTP/RTCP.

CAPITULO 4: LA INTERNET COMO UN MEDIO DE TRANSMISIÓN DE DATOS

En este capitulo se analiza los servicios, las ventajas que hay a través del Internet en la transmisión de datos

4.1. Descripción del Internet

Internet es un conjunto de redes de computo comunicadas entre si que llega a millones de personas en todo el mundo, por medio de estas redes se puede transmitir información de un punto a otro, proporcionar a los investigadores acceso a los recursos caros de hardware, también puede ser utilizado como búsqueda de información para realizar investigaciones de cualquier tipo tanto legal, económica, etc.

4.2. Servicios del Internet

Los servicios que nos proporciona Internet son:

- Conectarse a servidores remotamente. Todos los servicios en la Internet operan bajo el principio cliente / servidor en el cual se requiere que el servidor este en conexión permanente.
- Consulta de correo electrónico. Se necesita tener una dirección E-mail para poder acceder al correo, este ofrece un servicio rápido y conveniente para transferir información, también se pueden enviar mensajes cortos o largos documentos, así como archivos binarios codificados.
- Tener acceso a información en otras partes del mundo
- Copiar archivos y programas remotamente
- Hacer compras electrónicas
- Acceso a servidores de noticias
- Establecer diálogos con personas en otras partes del mundo (Chat)
- Videoconferencias, etc.

El principio básico es el enrutamiento, Router o Switch (capa 3) capaces de manejar direcciones lógicas. Poseen algoritmos de enrutamiento para alcanzar una ruta optima y asegurar la entrega si no se puede por un lado existen otros.

4.3. Ventajas y desventajas de usar la Internet como medio de transmisión

La Internet como medio de transmisión de datos nos brinda servicios como:

- Servicios de información (WWW, ftp)
- Servicios de Comunicación (E- mails, news, IRC, InternetPhone)
- Servicios de Administración y control (Telnet, Ping, Rlogin, etc.)

Ventajas

Unas de las ventajas del uso de la Internet es que evita a la empresa tener que implementar toda una estructura de comunicaciones debido a que emplea la infraestructura del ISP.
Tiene comunicación a nivel local y a nivel mundial.

El costo es bajo debido a que así lo utilice al resto del país o del mundo el costo de su conexión es local y el bajo costo de los equipos debido a que solo requiere de un MODEM y un router de ser necesario.

Desventajas

Dependencia de la disponibilidad del ISP, la comunicación vía e-mail no es en tiempo real, no se puede saber cuando será recibido, aunque se puede conocer cuando ya lo fue.

La seguridad de la información podría ser tomada por otros, la conexión a Internet abre las puertas a posibles violaciones de seguridad, debido a esto se deben instalar Firewalls.

4.4. Uso de la Internet como medio de transmisión (VPN)

Las redes privadas virtuales (VPN) crean un túnel o conducto dedicado de un sitio a otro. Las VPNs son una alternativa a buen costo, para usar líneas alquiladas que conecten sucursales o

para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegiendo la información y el password.

La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un canal privado a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de una red local.

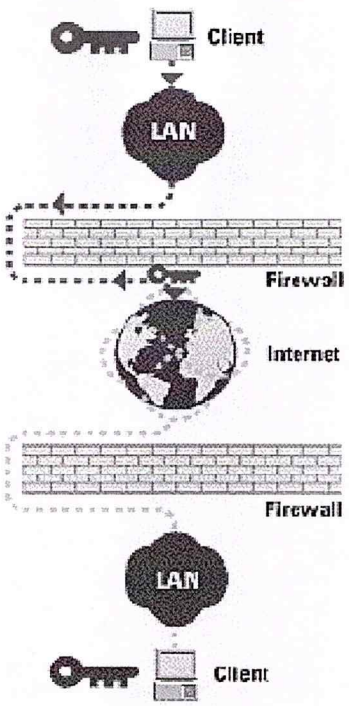


Figura 4.1. Internet como medio de transmisión de datos

Las redes privadas pueden ser relativamente nuevas, pero la tecnología de túneles está basada en standares preestablecidos. La tecnología de túneles – Tunneling – es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes, ya que los paquetes están encriptados de forma de los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

Los proveedores de varias firewall incluyen redes privadas virtuales como una característica segura en sus productos

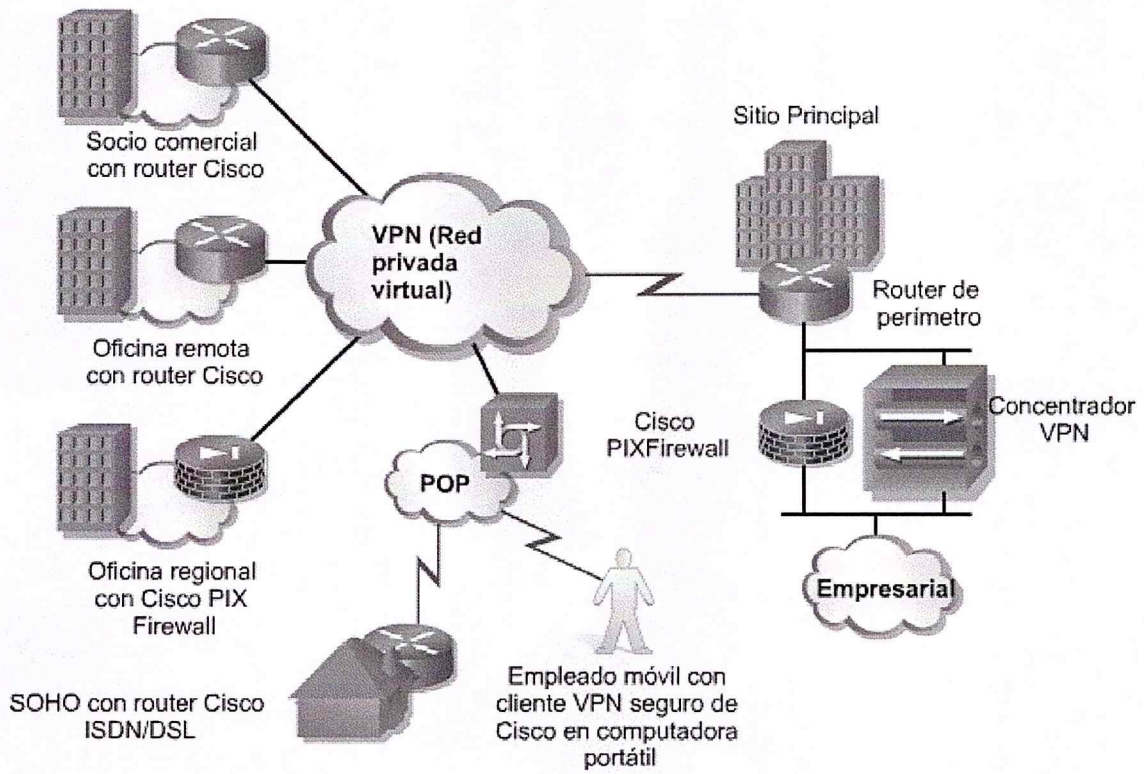


Figura 4.2. VPN

A continuación se describen los tres principales tipos de VPN:

VPN de acceso: Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.

Redes internas VPN: Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.

Redes externas VPN: Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

4.5. Consideraciones en el uso de la Internet como medio de Transmisión

Con los accesos remotos seguros, las conexiones vía MODEM telefónico pueden transferir seguro vía un proveedor de servicios Internet o una red corporativa. Los datos se encriptan en el cliente antes de que sean transmitidos y se desencriptan en la puerta de la firewall. El software proporcionado, habilita a los usuarios remotos a que se pueden conectar a la red corporativa como si ellos estuvieran detrás de la firewall.

La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulación, una VPN básica, crea un pasillo privado a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de una red local.

Como se ha indicado, una red privada virtual es una red donde todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia. Para lograr esta funcionalidad, se definió una tecnología de redes seguras, privadas y virtuales, las cuales deben completar tres tareas.

Primero, deben poder pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública.

Segundo, la solución debe agregar encripción, tal que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado.

Finalmente, la solución tiene que ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de manera que un adversario no pueda acceder a los recursos del sistema.

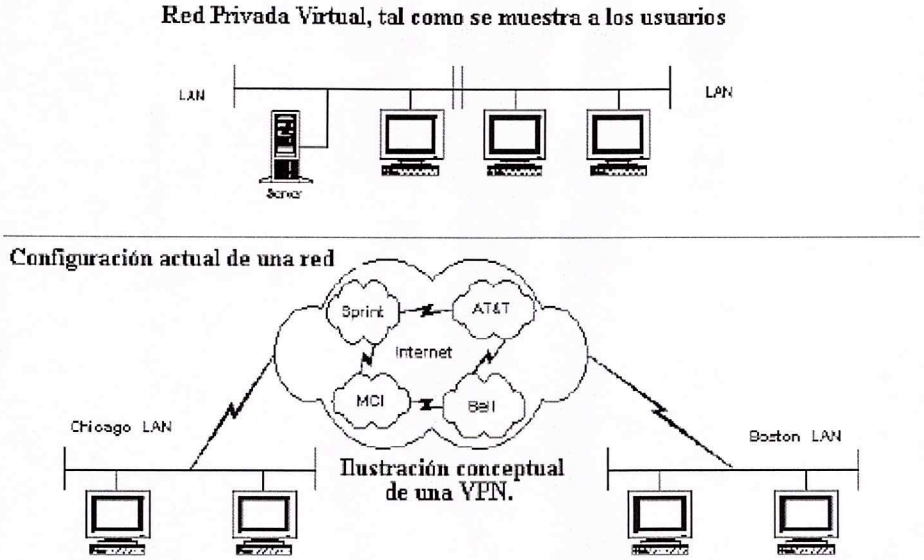


Figura 4.3. VPN

CAPITULO 5: SEGURIDADES

En este capitulo se analiza todo lo referente a las seguridades que se deben tomar al transmitir información.

5.1. Seguridad Informática

La seguridad de un sistema informático se define como el conjunto de normas y procedimientos que permiten garantizar la confidencialidad, la integridad y la disponibilidad de la información almacenada en medios electrónicos de cualquier especie.

Estas seguridades deben cumplir ciertas propiedades como son:

1. Confidencialidad
2. Autenticidad
3. Integridad
4. Control de Acceso
5. Disponibilidad

- **Confidencialidad.-** El modo seguro en el que viaja la información desde su transmisor hasta su receptor, de tal manera que no es manipulada por otro usuario.

- **Autenticidad.-** La información que se a enviando de un punto a otro no va a recibir modificaciones en el transcurso de su viaje.

- **Integridad.-** Los paquetes de información llegan completos a su lugar de destino.

- **Control de Acceso.-** Debería mantenerse ciertas normas de seguridad en el envío de la información, como en el caso de la encriptación de los archivos que se envían para evitar la adulteración de la información.

- **Disponibilidad.-** La información depende de las personas autorizadas, estará disponible dicha información solo alas personas que tengan la clave de acceso.

En una red de equipos, la seguridad consiste en definir una contraseña sobre un recurso, como un directorio, que es compartido en la red. Todos los usuarios de una red de Trabajo en Grupo define su propia seguridad, y puede haber recursos compartidos en cualquier equipo, en lugar de únicamente en un servidor centralizado; de este modo, es muy difícil mantener un control centralizado. Esta falta de control tiene un gran impacto en la seguridad de la red, ya que puede que algunos usuarios no implementen ninguna medida de seguridad. Si la seguridad es importante, puede que sea mejor usar una red basada en servidor.

En lo que respecta las políticas de seguridad a nivel de software se implementan en base a un análisis exhaustivo de las amenazas más comunes utilizadas por hackers, es por esto que se debe incluir lo siguiente:

- Seguridades de acceso a los servidores
  Se utiliza canales encriptados para autenticación

- Seguridades de MAC (capa 2)
  Controlamos acceso por MAC de clientes

- Seguridades IP (capa 3)
  El bloqueo de IPS y puertos (Firewalls)

5.2. Gestión de Seguridad

5.2.1. Políticas y procedimientos

Definición de una política de seguridad.-

1) Las políticas deben ser totalmente incluyentes y deben considerar la mayor parte de aspectos (Tiene una puerta de acero?. de nada sirve si la puerta de servicio queda abierta). Lo que quiere decir es que debemos ser cuidadosos con los detalles.

2) Las políticas deben ajustarse a nuestras necesidades y recursos, debemos valorar los costes en caso de un desastre y compararlos con los costes que implica tomar las medidas de seguridad.

Generalmente se siguen tres caminos cuando se diseña un conjunto de políticas de seguridad:

1) Evaluación de costos
2) Evaluación de riesgos
3) Estrategia de protección

5.2.1.1 Evaluación de costos.- EL costo de lo que se quiera proteger debe ser mayor al costo de protegerlo, de otra manera no tendría sentido querer protegerlo, visto de otra forma si atacar un sistema cuesta mas de lo que este sistema vale el atacante lo pensara dos veces antes de atacarlo.

De aquí que hay que considerar dos cosas muy puntuales, el valor intrínseco de lo que estamos protegiendo y los costes derivados de su perdida.

El costo intrínsico.- El costo intrínsico incluye los siguientes componentes:

1. Costo del hardware involucrado
2. Costo del software involucrado
3. Costo invertido en el sistema que se creo, incluyendo materiales involucrados.
4. Costo de la información personal contenida (Cuanto me costo obtenerla)

Costos derivados.- Para determinar de encontrar los costos derivados, se debe determinar los costos asociados con la información que se pierda. Se debe tratar de abarcar todas las posibilidades:

1. Costo de sustituir el hardware
2. Costo de sustituir el software
3. Costo de reingresar los datos de esos 10000 clientes (Tiempo).
4. Costo de la documentación perdida.
5. Valor de la información personal perdida

Los costos derivados son mucho mas difíciles de evaluar, considere por ejemplo que pierde la base de datos con información de sus clientes, y que esta información sea utilizada para suplantar las identidades de un grupo de delincuentes para cometer delitos, es obvio que esto tendría por tanto un costo mucho mas elevado que el aparente.

5.2.1.2 Evaluación de riesgos.- Para realizar la evaluación de riesgos, puede ser recomendable seguir las reglas del sentido común:

1. Sus políticas deben observar todas las posibles formas de ataque.
2. La máxima seguridad obtenible es aquella del elemento mas débil de la cadena (Principio de la puerta trasera)
3. Una política de seguridad constituye un sistema dentro de otro sistema.
4. Considere las interacciones de los distintos elementos involucrados.

5.2.1.3 Estrategias de protección.- Se deben identificar al menos tres dimensiones que sostienen una estrategia de protección:

1. Nivel Físico
2. Nivel Humano
3. Nivel Logístico

Una adecuada estrategia de seguridad debería contemplar estos cuatro niveles.

Nivel físico.- Es el nivel mas evidente y el que se debería considerar en un primer lugar, anteriormente se ha analizado varios tipos de intrusiones físicas, por tanto es evidente establecer un adecuado perímetro de seguridad que sea restrictivo en cuanto al acceso físico y que preste las suficientes garantías para el funcionamiento de equipos de computo. Es necesario establecer también, a este nivel normativas y procedimientos de contingencia, ejemplo: Que hacer en caso de robo del servidor donde estaba la base de datos? Observe detalles como evitar que alguien deje un vaso con acido justo encima de su servidor principal al que lo tenia abierto por que estaba instalándole 512Mbytes adicionales de memoria RAM.

Algunos aspectos claves del nivel físico son:

1. Condiciones medioambientales adecuadas (temperatura, humedad, polvo, entornos corrosivos, etc.)
2. Prevención de catástrofes (Incendios, inundaciones, fallos de energía eléctrica, etc.)
3. Limitación de acceso (Cuarto con llaves, racks cerrados, cámaras de vigilancia, guardias armados, etc.)
4. Sistemas de recuperación (Respaldos, redundancia de servidores, etc.)

Nivel humano.- Es valido hablar de un nivel humano en la definición de políticas de seguridad debido a que son seres humanos quienes a fin de cuentas van a estar interactuando con el sistema y lo van a afectar y serán afectados por este.

Aquí se puede considerar cuatro subniveles.

1. **El administrador del sistema.-** Debe existir una persona encargada del sistema, esta persona es la única que puede decidir sobre cada elemento de la operación y debe tener control absoluto. Esta debería ser la única persona que tiene acceso al centro de cómputo o los servidores. Debido a que poner todo el poder en una sola persona podría ser peligroso, generalmente hay un segundo al mando que podría reemplazar al administrador principal en caso de ausencia obligada de este.

   Es obvio que para poder poner toda la seguridad de un sistema informático en una persona, esta debería reunir requisitos de máxima confiabilidad, de igual manera debería ser una persona de trayectoria conocida, equilibrada emocionalmente y por supuesto de reconocida capacidad.

   Se debe cultivar en esta persona un máximo nivel de lealtad hacia la empresa, esto se logra con un trato adecuado y digno de sus superiores (no olvide el factor humano), adicionalmente debe promoverse un sistema de compensaciones en base a objetivos planteados, recuerde que bajos salarios lo harán susceptible al soborno o chantaje y penalizaciones excesivas lo pondrán al borde de la desesperación o a un nerviosismo que disminuya su capacidad.

2. **Los usuarios del sistema.-** Seria ideal que solo el administrador del sistema tuviese acceso al mismo, en la vida real esto no sucede y con frecuencia hay que dar permisos de acceso a otras personas para que utilicen el sistema, en estos casos lo mas recomendado es establecer con exactitud las zonas de acceso a las que deberá tener cada usuario y limitarlo solo a eso mediante adecuadas configuraciones de los servicios generalmente mediante la utilización de users y passwords, y cada uno será responsable de las actividades que el sistema registre para ese usuario.

   Es necesario que los usuarios sean conscientes de la responsabilidad que tienen y deben estar comprometidos con estas políticas. Nadie que no este de acuerdo con las políticas de seguridad o que no este dispuesto a aceptar la responsabilidad de sus actos debería tener acceso al sistema bajo ningún concepto. Hay casos en que las empresas contratan trabajadores eventuales y lo hacen sin hacer ningún tipo de investigación sobre los antecedentes o costumbres de estos nuevos trabajadores, esto es especialmente peligroso si se les asigna responsabilidades inmediatamente, en lo posible evite que trabajadores nuevos o eventuales tengan acceso a información que luego podría ser mal utilizada.

3. **Personas relacionadas que no son usuarios del sistema.-** Generalmente hay personas que no necesitan tener acceso al sistema o a la infraestructura, esto puede aplicarse a los altos ejecutivos o a los propietarios del negocio, pero estos usualmente, sin saberlo y por vanidad quieren mostrar a sus amigos el ultimo servidor o lo ultimo en tecnología que adquirieron, esto que en principio parece inofensivo es un agujero de seguridad enorme. Si para el administrador o responsable es imposible evitar este tipo de paseos por la oficina, al menos debería dejar sentado y por escrito las responsabilidades que esta asumiendo este ejecutivo. La mejor forma de manejar este tipo de inconvenientes es que el responsable de la seguridad posea un rango superior de manera que ningún ejecutivo pueda sobreseer sus funciones. También debería establecerse un protocolo de acceso y vigilancia al personal de rango medio.

4. **Personas ajenas al sistema.-** Estas personas deberían ser tratadas siempre como intrusos aunque esto no impide que sean tratadas con cortesía. Aunque debería evitarse mostrar las infraestructuras del sistema a alguien ajeno en ocasiones es necesario e inevitable, si este es el caso nunca debería autorizarse estas visitas sin el permiso y

consentimiento del encargado o responsable, y durante la visita el visitante debería ser sometido a una férrea pero discreta vigilancia.

En ocasiones puede establecerse una sala alterna ficticia con ordenadores viejos, si el visitante no es técnico esto a menudo bastara.

Nivel Logístico.- Como hemos podido observar, el tratar de implementar un sistema de protección es un tema relativamente complejo, a mas de los puntos que hemos considerado, debemos tener en cuenta la interacción de los diversos elementos y su debida coordinación. Se hace necesario establecer una logística de coordinación que tenga en cuenta los siguientes aspectos:

1. **El aspecto físico.-** No es lo mismo asegurar un sistema que conste de un solo servidor en una oficina aislada sin conexión al Internet que tratar de proteger una corporación con varias oficinas en el país que están interconectadas, en este caso es a veces imposible conocer a todo el personal involucrado que trabaja en las oficinas remotas, por lo que es necesario establecer directrices generales de seguridad, repartirlas y medir sus grados de cumplimiento.

2. **Dinámica laboral.-** Un ambiente de trabajo relajado puede beneficiar el cuidado de los detalles, aunque el tipo de ambiente como este no siempre es posible, es necesario un grupo de directrices que no dejen lugar a la duda cuando se trate de tomar decisiones.

3. **Dinámica de grupos.-** Define las vías de comunicación disponibles para la notificación de problemas al mando mas elevado. Un ambiente en el que no haya una dinámica laboral aceptable tarda mucho en reaccionar ante ataques y notificarlos.

5.3. VLANS

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico.

Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, sin importar la conexión física o la ubicación.

La configuración o reconfiguración de las VLAN se logra mediante el software. Por lo tanto, la configuración de las VLAN no requiere que los equipos de red se trasladen o conecten físicamente.

Una estación de trabajo en un grupo de VLAN se limita a comunicarse con los servidores de archivo en el mismo grupo de VLAN. Las VLAN segmentan de forma lógica la red en diferentes dominios de broadcast, de manera tal que los paquetes sólo se conmutan entre puertos y se asignan a la misma VLAN. Las VLAN se componen de hosts o equipos de red conectados mediante un único dominio de puenteo. El dominio de puenteo se admite en diferentes equipos de red. Los switches de LAN operan protocolos de puenteo con un grupo de puente separado para cada VLAN.

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LANs. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

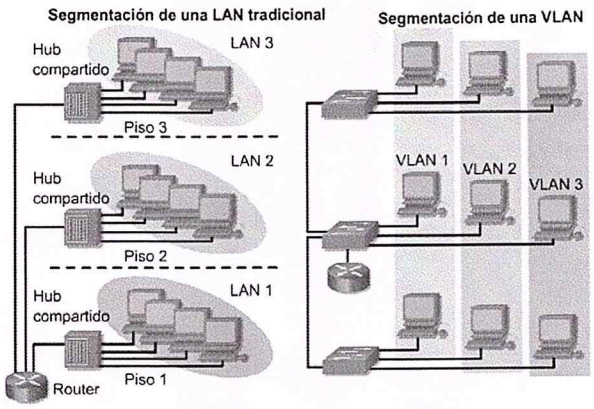


Figura 5.1. VLANs

Una característica importante de la conmutación de Ethernet es la capacidad para crear redes de área local virtuales (VLAN). Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red, las VLAN se pueden agrupar por función laboral o departamento sin importar la ubicación física de los usuarios.

El tráfico entre las VLAN está restringido, los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN.

Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica. Las empresas con frecuencia usan las VLAN como una manera de garantizar que un conjunto determinado de usuarios se agrupen lógicamente más allá de su ubicación física. Las organizaciones usan las VLAN para agrupar usuarios en el mismo departamento.

5.4. ACLs

Los administradores de redes deben ser capaces de denegar el acceso no deseado a la red a la vez que permiten el acceso si deseado. Aunque las herramientas de seguridad (Contraseñas o dispositivos físicos de seguridad) son útiles, a menudo carecen de la flexibilidad del filtrado básico de tráfico y de los controles específicos que prefieren la mayoría de los administradores. Los routers proporcionan capacidades básicas de filtrado del tráfico, como el bloqueo de tráfico de Internet, mediante las ACL´s (listas de control de acceso). Una ACL es una colección secuencial de sentencias de permiso o denegación que se aplica a las direcciones o los protocolos de la capa superior.

Las ACL´s filtran el tráfico de la red controlando si los paquetes enrutados se enviaron o bloquearon en las interfaces del router. Este examina cada paquete para determinar si debe enviarlo o descartarlo, en función de las condiciones especificadas en la ACL. Dichas condiciones pueden ser la dirección de origen del tráfico, la dirección de destino del tráfico, el protocolo de la capa superior, el puerto o las aplicaciones.

5.5. Criptografía

La palabra criptología proviene de las palabras griegas Krypto y Logos, y significa estudio de lo oculto. Una rama de de la criptología es la criptografía (Kryptos y Graphos que significa descripción), que se ocupa del cifrado de mensajes.
Esta se basa en que el emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio de un canal de comunicación establecido, llega al descifrador que apoyándose en diversos métodos, extrae el texto original.

Según explica Jorge Ramió Aguirre en su libro "Seguridad Informática" la criptografía es:

"Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de sistemas de cifra que permiten asegurar estos cuatro aspectos de la seguridad informática: la confidencialidad, la integridad, la disponibilidad y el no repudio de emisor y receptor."

Otra definición a tener en cuenta es el significado de criptoanálisis, el cual es el arte y la ciencia de transgredir las claves de acceso, es decir la que se encarga de descifrar los mensajes.

En la siguiente figura podemos observar un ejemplo de un criptosistema que nos muestra como sería el funcionamiento esquemático, sea cual sea el canal de transmisión, del cifrado y descifrado de un mensaje en su paso del transmisor al receptor.

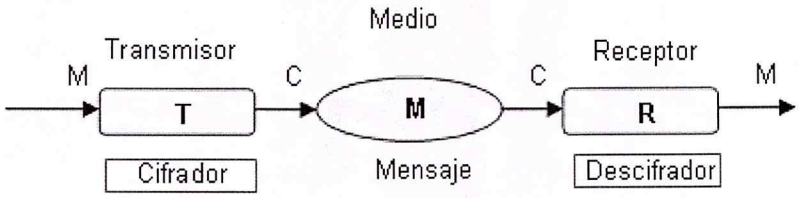


Figura 5.2. Criptografía

5.5.1. Sistema de cifrado Simétrico

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave. Es importante que dicha clave sea muy difícil de adivinar ya que hoy en día las computadoras pueden adivinar claves muy rápidamente.

Por ejemplo el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 72 mil billones de claves posibles. Actualmente ya existen ordenadores especializados que son capaces de probar todas ellas en cuestión de horas. Hoy por hoy se están utilizando ya claves de 128 bits que aumentan la cantidad de claves posibles (2 elevado a 128) de forma que aunque se uniesen todos los ordenadores existentes en estos momentos no lo conseguirían en miles de millones de años.

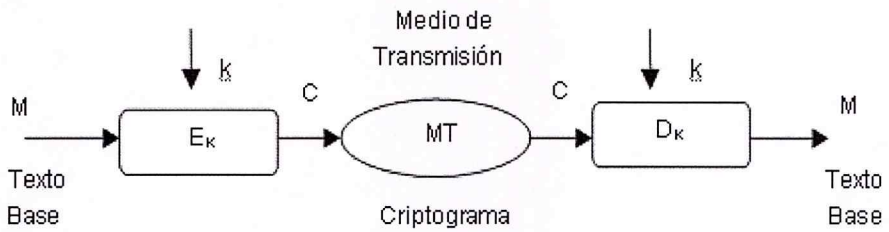


Figura 5.3. Sistema de Cifrado Simétrico

Con Ek ciframos el mensaje original aplicándole la clave k y con Dk lo desciframos, aplicándole de la misma forma la clave k. La confidencialidad y la integridad se lograrán si se protegen las claves en el cifrado y en el descifrado. Es decir, se obtienen simultáneamente si se protege la clave secreta.

5.5.2. Sistema de cifrado Asimétrico

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

Un sistema de cifrado de clave pública basado en la factorización de números primos se basa en que la clave pública contiene un número compuesto de dos números primos muy grandes. Para cifrar un mensaje, el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. Para descifrar el mensaje, el algoritmo de descifrado requiere conocer los factores primos, y la clave privada tiene uno de esos factores, con lo que puede fácilmente descifrar el mensaje.

Es fácil, con las computadoras de hoy en día, multiplicar dos números grandes para conseguir un número compuesto, pero es muy difícil la operación inversa, Dado ese numero compuesto, factorizarlo para conocer cada uno de los dos números. Mientras que 128 bits se considera suficiente en las claves de cifrado simétrico, y dado que la tecnología de hoy en día se encuentra muy avanzada, se recomienda en este caso que la clave pública tenga un mínimo de 1024 bits. Para un ataque de fuerza bruta, por ejemplo, sobre una clave publica de 512 bits, se debe factorizar un numero compuesto de hasta 155 cifras decimales.

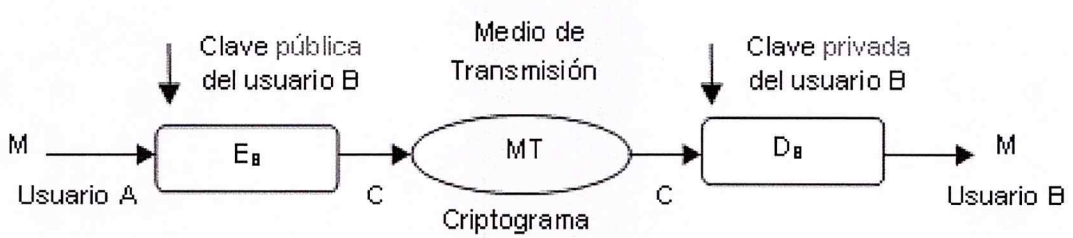


Figura 5.4. Sistema de Cifrado Asimétrico A

Hay que tener en cuenta que Eb y Db son inversas dentro de un cuerpo, además se debe de tener en cuenta que se cifra con la clave pública del destinatario, de forma que conseguimos que solo él, al tener su clave privada pueda acceder al mensaje original.

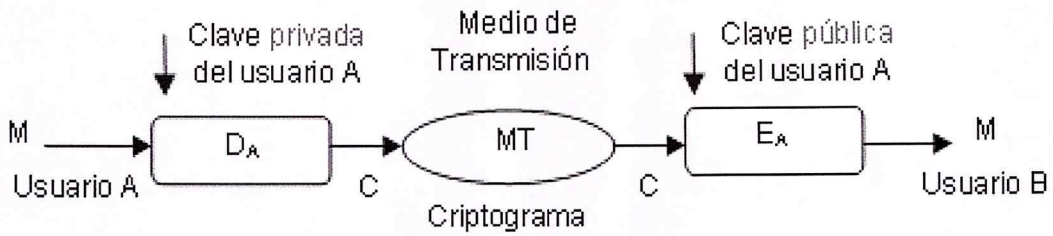


Figura 5.5. Sistema de Cifrado Asimétrico B

En este segundo caso podemos observar como esta basado en el cifrado con la clave privada del emisor y al igual que antes hay que tener en cuenta que Ea y Da son inversas dentro de un cuerpo.

5.5.3. Sistemas de cifrado híbridos

Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico.

En cada mensaje, la clave simétrica utilizada es diferente por lo que si un atacante pudiera descubrir la clave simétrica, solo le valdría para ese mensaje y no para los restantes. La clave simétrica es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave simétrica y acto seguido usa la clave simétrica para descifrar el mensaje

5.6. Seguridades Físicas

Las seguridades físicas son tomadas para poder evitar pérdida de información, clonación de información y para tener autenticidad y credibilidad en la información que se encuentra almacenada en dicho equipo.

En lo que respecta a los racks (almacena servidores) para tener seguridades tiene que ser cerrado; así también tenemos otro tipo de seguridades por medio de cámaras que graben quien tiene acceso a dicho lugar y detecte cualquier tipo de movimiento (cámara inteligente) conectada a sensores de movimientos.

Debemos tener en cuenta las fuentes de amenaza que son: 55% por error humano, el 10% de empleados resentidos, el 10% empleados deshonestos, 10% personal outsourcing y el 15% Hackers.

En el centro de monitoreo debemos tener personal 7x24 (7 días, 24 horas) si es que el caso lo amerita; es donde se deben tener controles en lo que respecta el flujo de red, procesadores, medio ambiente, los UPS, niveles de software, control del uso del ancho de banda, el monitoreo de alarmas y el control de los intentos de ataques.

Las cámaras de circuito cerrado, sirven para la vigilancia de las instalaciones con registro en cintas esto es llevar almacenamiento de las grabaciones, en las salas de vigilancia tener múltiples monitores y el personal debe ser especializado.

Para el sistema de control de acceso se debe tener tarjetas para control de acceso del personal autorizado.

Para la detección de incendios se debe tener un sistema de detección de humo, llamas y gases, también se debe contar con extinguidotes para la operación manual en las áreas adecuadas.

5.7. Ataques

Los métodos de ataque más extendidas y conocidos en el mundo de la informática incluyen pero no se limitan a:

1. Ataques que involucran ingeniería social
2. Ataques Físicos
3. Ataques desde la red (Internet)

Los métodos de ataque más extendidos y conocidos en el mundo de la informática incluyen pero no se limitan a:

5.7.1 Ataques que involucran ingeniería social.- Se conoce como ingeniería social a cualquier forma de manipulación o engaño que se utilice para persuadir a las personas para que entreguen información sensible de su sistema informático (passwords, números de cuenta, etc.). Se conocen algunas técnicas o métodos que aunque sencillos y simples son muy

efectivos especialmente cuando son dirigidos a personal no técnico que por algún motivo manipula o utiliza este tipo de información. A continuación se describen algunas de estas técnicas.

1. **Suplantación.-** Se da la suplantación cuando el individuo que quiere vulnerar nuestro sistema intenta convencer a la victima de que es alguien autorizado para pedir información sensible, es decir trata de convencernos de que es quien dice ser a pesar de no serlo. Generalmente se hace vía telefónica o con algún correo electrónico.

2. **Ataque al ego.-** Este tipo de engaño tiene que ver mucho con la psicología y autoestima de la victima, en ocasiones el atacante busca ganar la confianza de su victima atacando directamente su autoestima principalmente mediante elogios, de manera que esta deposite su confianza en el atacante, luego de lo cual este empieza a pedir información a la victima de una manera muy sutil.

3. **Profesiones poco sospechosas.-** No en pocas ocasiones los atacantes intentan acceder a zonas reservadas haciéndose pasar por personal de servicio de la compañía de gas o teléfonos por ejemplo, normalmente la gente tiende a descuidarse de estas personas, de aquí que los atacantes aprovechan esta ventaja para pasar desapercibidos y buscar información sensible como passwords, direcciones de red, etc.

5.7.2 Ataques (Intrusiones) Físicos.- Cuando el atacante tiene acceso físico al área de trabajo o al área de servidores o cuarto de racks hay muchas posibilidades de que encuentre información sensible acerca de nuestra red o sistema informático, es por esto que se hace necesario establecer un perímetro de seguridad mínimo al que el acceso sea restringido, a continuación algunas de las variantes de intrusiones físicas que pueden afectarnos.

1. **Intrusión al área de trabajo.-** Talvez el área mas vulnerable es nuestra área de trabajo u oficina donde por lo general establecemos mínimas medidas de seguridad, los posibles objetivos de un atacante serian información a las vista, tales como documentos, una nota adherida al monitor conteniendo una password, o el numero de una tarjeta de crédito. Incluso información en CD-ROM o disqueteras son bienvenidas.

Entre la información mas apetecida se encuentran listados telefónicos, diagramas de la empresa, documentación sobre políticas de seguridad, calendarios de actividades, etc. A veces la mejor forma de protección contra este tipo de ataque es mantener un escritorio ordenado en un área cerrada si esto no fuese posible trate de mantener la menor cantidad de información posible a la vista de la gente. Evite escribir información como números de tarjeta o contraseñas en papeles o agendas, memorícelas o guárdelas en archivos de computadora cifrados.

2. **Rebuscar el contenedor de basura.-** Aunque le parezca mentira los atacantes encuentran esta actividad muy provechosa. Buscando en los tachos de basura de la gente se puede encontrar información confidencial muy útil como los passwords escritos en pequeños papeles que una vez que los memorizamos echamos al tacho de basura. Tenga en cuenta que en muchos países la búsqueda en recipientes de basura se considera una actividad legal. El peligro se multiplica si echamos a nuestro tacho de desperdicios CD-ROMS, disquetes incluso la agenda del año pasado. Toda empresa debería tener políticas de tratamiento de información sensible que detallen normas y procedimientos que indiquen como se puede manejar (almacenar, transmitir o destruir) esta información y esta debe publicarse y distribuirse a todos los empleados de la oficina. Utilice picadores de papel cruzado, o destruya CDROM's, y ubique los contenedores de basura de ser posible protegidos por puerta con llave.

3. **Ataques contra los secretos de la red.-** El acceso a los cuartos de servidores o racks hace posible que los atacantes obtengan fácilmente información sobre los sistemas que se posee y sus configuraciones. A veces los administradores de red utilizan etiquetas o notas adhesivas a sus equipos, estas notas por lo general revelan información como números ip o nombres de computadoras, tipo de sistema operativo o incluso esquemas enteros de la red, esto facilita la vida del atacante por que le da un mapa de los puntos mas vulnerables de manera que ya sabe donde poner un analizador de trafico o sistemas de escucha telefónica. Lo mejor que se puede hacer ante esto es evitar poner este tipo de información visible, esto en ocasiones dificulta el trabajo del administrador de red, de manera que si es inevitable lo mejor que puede hacerse es restringir el acceso al área de oficina e instalaciones de equipos de cómputo.

4. **Acceso a la consola.-** Este es uno de los mas antiguos agujeros de seguridad en informática y uno de los mas peligrosos, quien no ha salido alguna vez de su puesto de

trabajo ya sea para ir al baño o para ir a la tienda de la esquina, el tiempo en que nuestra consola esta descuidada bien podría ser usado por un atacante para acceder a el e instalar algún programa malicioso como un troyano. En ocasiones incluso dejamos abiertas sesiones de trabajo por varios días si cerrar en servidores a los cuales de esta manera es muy fácil acceder. A veces la forma más efectiva de evitar este tipo de acceso a consolas es utilizar protectores de pantalla protegidos por contraseñas que saltan luego de tiempos razonables.

5. **Acceso físico al arranque de los servidores.-** Estos talvez sean los casos mas dañinos de acceso, cuando el atacante ingresa a tu cuarto de servidores puede reiniciar tu servidor y obligarlo a que inicie sin necesidad de pedir contraseña. Incluso el atacante puede intentar reiniciar el servidor utilizando un CDROM de inicio que también puede caber en un disquete. La forma mas adecuada de protegerse contra esto es configurando nuestro sistema para que solo bootee con contraseña, en el segundo caso es mejor deshabilitar en la BIOS el inicio o arranque desde disquetes o unidades de CDROM.

5.7.3 Ataques desde la red (Internet)

Sin duda los ataques más difíciles de detectar y contrarrestar son los ataques que vienen desde la red pública o Internet, pues es muy fácil iniciar un ataque sin ser descubierto.

Hay un sinnúmero de técnicas y herramientas conocidas por los posibles atacantes y lo peor de todo es que están disponibles en la Internet, a continuación haremos un repaso de las mas conocidas.

1. **Guerra Telefónica.-** Este tipo de ataques son muy usuales y se dan cuando los usuarios dejan sus módems conectados a las líneas telefónicas, el principio es sencillo, el atacante posee un software de marcado automático programable y empieza a marcar aleatoriamente los números de un listado telefónico, cuando encuentra que el numero que esta marcando corresponde a un MODEM y no a un teléfono convencional, espera una secuencia de inicio de sesión que le pida un usuario y un password, de aquí en adelante empieza a tratar de adivinar por medio de diccionarios esta información. La manera mas efectiva de resguardarse de este ataque es desconectar nuestro MODEM

mientras no lo usamos, y poner passwords lo suficientemente fuertes para disminuir las posibilidades de éxito al atacante.

2. **Contraseñas predeterminadas.-** Un agujero de seguridad muy común es el hecho de que ciertos programas traen configuración de passwords por defecto, esto es especialmente cierto en nuevos equipos. Por lo tanto tenga en cuenta cambiar los passwords que los programas traen por defecto consultando el manual. Incluso cuando se adquiere hardware nuevo como routers o switches estos vienen con passwords que todo el mundo conoce, si alguien consigue entrar a uno de estos equipos tendrá ya puesto un pie dentro de su sistema.

3. **Analizadores de paquetes (Sniffers).-** Los sniffers son sofisticadas herramientas utilizadas por los atacantes para recolectar información vital acerca de las redes, en esencia los sniffers son programas que ponen las interfaces de red en modo promiscuo, es decir que escuchan o capturan todos los paquetes de la red aunque no estén dirigidos a ellos, una vez capturados los paquetes este software puede clasificarlos por protocolo y presentar las tramas de información en texto claro.

   Es por esto que no es recomendable utilizar programas que envíen información sensible en texto claro como contraseñas o números de tarjetas de crédito. Los sniffers más populares son Tcpdump, Ethereal, Hunt.

4. **Escaneado de puertos.-** Esta herramienta es ampliamente utilizada por los atacantes para conocer cuales son los servicios que presta tu servidor, con esta información queda claro que si utiliza un servidor de correos entonces estará abierto el puerto 25 TCP luego ejecutara algo como telnet tu dirección ip 25 si tu servidor de correo no esta correctamente configurado responderá con información como la versión y el tipo de servidor, incluso el sistema operativo, con esto ya puede buscar alguna vulnerabilidad conocida y ejecutar un ataque orientado a explotar esta vulnerabilidad. Las herramientas más populares para escaneo de puertos son nmap, netcat, strobe. Una medida de seguridad muy útil y cerrar todos los puertos que no se necesiten y desactivar todos los programas que no estén siendo usados, por que cada uno de ellos es una puerta susceptible a ser abierta.

5. **Ataques de denegación de servicio (DoS).-** Se conoce como ataques de denegación de servicios todos aquellos ataques que hagan nuestro sistema o nuestra red inutilizable por algún lapso de tiempo, en esta categoría podemos ubicar a las inundaciones, en el que el atacante empieza a enviar gran cantidad de paquetes (protocolo ICMP) hacia nuestro sistema de manera que consume los recursos de memoria del mismo lo que lo vuelve inutilizable, en esta misma categoría caen los ataques DDoS que son lo mismo que los anteriores pero son llevados a cabo desde varios puntos de la red simultáneamente. Normalmente se deshabilita la opción que perite a los servidores responder a peticiones ICMP.

5.8. Firewall PIX

PIX es una de las soluciones de seguridad ofrecidas por Cisco Systems; se trata de un firewall completamente hardware: a diferencia de otros sistemas cortafuegos, PIX no se ejecuta en una máquina Unix, sino que incluye un sistema operativo empotrado denominado Finesse que desde espacio de usuario se asemeja más a un router que a un sistema Unix clásico.

El cortafuegos PIX utiliza un algoritmo de protección denominado Adaptive Security Algorithm (ASA): a cualquier paquete inbound (generalmente, los provenientes de redes externas que tienen como origen una red protegida) se le aplica este algoritmo antes de dejarles atravesar el firewall, aparte de realizar comprobaciones contra la información de estado de la conexión (PIX es stateful) en memoria; para ello, a cada interfaz del firewall se le asigna un nivel de seguridad comprendido entre 0 (el interfaz menos seguro, externo) y 100 (el más seguro, interno). La filosofía de funcionamiento del Adaptive Security Algorithm se basa en estas reglas:

- Ningún paquete puede atravesar el cortafuego sin tener conexión y estado.
- Cualquier conexión cuyo origen tiene un nivel de seguridad mayor que el destino (outbound) es permitida si no se prohíbe explícitamente mediante listas de acceso.
- Cualquier conexión que tiene como origen una interfaz o red de menor seguridad que su destino (inbound) es denegada, si no se permite explícitamente mediante listas de acceso.
- Los paquetes ICMP son detenidos a no ser que se habilite su tráfico explícitamente.
- Cualquier intento de violación de las reglas anteriores es detenido, y un mensaje de alerta es enviado a syslog.

- Cuando a un interfaz del cortafuegos llega un paquete proveniente de una red con menor nivel de seguridad que su destino, el firewall le aplica el adaptive security algorithm para verificar que se trata de una trama válida, y en caso de que lo sea comprobar si del host origen se ha establecido una conexión con anterioridad; si no había una conexión previa, el firewall PIX crea una nueva entrada en su tabla de estados en la que se incluyen los datos necesarios para identificar a la conexión.

El cortafuegos PIX puede resultar muy complejo de gestionar, especialmente a los que provienen del mundo Unix, ya que como hemos dicho se asemeja más a un router que a un servidor con cualquier flavour de Unix.

5.8.1. Introducción a la detección de intrusos:

El IDS de Cisco Secure es una opción exclusiva para IP que ofrece al administrador del PIX la flexibilidad necesaria para personalizar el tipo de tráfico que requiere ser auditado, registrado y eliminado.

Las opciones IDS de Cisco Secure ofrecen lo siguiente:

- Auditoria del tráfico: Las firmas de nivel de aplicación solo se auditan como parte de una sesión activa. La auditoria deberá estar asignada a una interfaz.
- Soporte para las distintas normas de auditoria. El trafico que coincida con una firma desencadena una serie de acciones configurables.
- Posibilidad de desactivar la auditoria de la firma.
- Posibilidad de activar el IDS y desactivar selectivamente las acciones de una clase de firma (informativa, de ataque).

La auditoria se lleva a cabo examinando los paquetes IP a la medida que llegan a una interfaz de entrada. Si un paquete desencadena una firma y la acción configurada no elimina el paquete, ese mismo paquete podrá desencadenar otras firmas.

El firewall PIX soporta la auditoria en la entrada de todas las interfaces. Es posible configurar individualmente las interfaces con distintas firmas, así como las acciones predeterminadas que se tomaran al coincidir una firma configurada.

5.8.2. Niveles de Seguridad ASA

El algoritmo de seguridad adaptable utiliza el concepto de niveles de seguridad.

Los niveles de seguridad van de 0 a 100 y las reglas más específicas para estos niveles de seguridad son las siguientes:

- **Nivel de Seguridad 100.-** Es el nivel de seguridad mas alto en una interfaz. Se usa para la interfaz interna del firewall PIX. Es la configuración predeterminada del firewall PIX y no puede ser cambiada. Dado que 100 es el nivel de seguridad de interfaz más fiable, la red de la universidad deberá estar configurada detrás de esa interfaz. De este modo, nadie podrá acceder a la red universitaria a menos que s ele dé un permiso. Ese permiso deberá estar configurado en el PIX. Una vez configurado, todos los dispositivos que estén en esta interfaz podrán tener acceso fuera de la red de la universidad.

- **Nivel de Seguridad 0.-** es el nivel de Seguridad más bajo. Este nivel de seguridad se usa para la interfaz externa del firewall PIX. Es la configuración predeterminada del firewall PIX y no puede ser modificada. Dado que 0 es el nivel de seguridad de interfaz menos fiable, la red menos fiable deberá estar detrás de esta interfaz. A los dispositivos del exterior se le spermite acceder a través del PIX sólo si este está configurado para ello. Esta interfaz sirve para conectarse a Internet.

- **Nivel de Seguridad 1-99.-** Estos niveles de seguridad pueden ser asignados a las interfaces de Perímetro que están conectadas con el firewall PIX. Es muy habitual conectar una de estas interfaces de perímetro a una red que actúe como zona desmilitarizada (DMZ). Una DMZ es un dispositivo o red a los que pueden acceder los usuarios desde el entorno no fiable. La DMZ es un área aislada, separada del entorno interno y fiable.

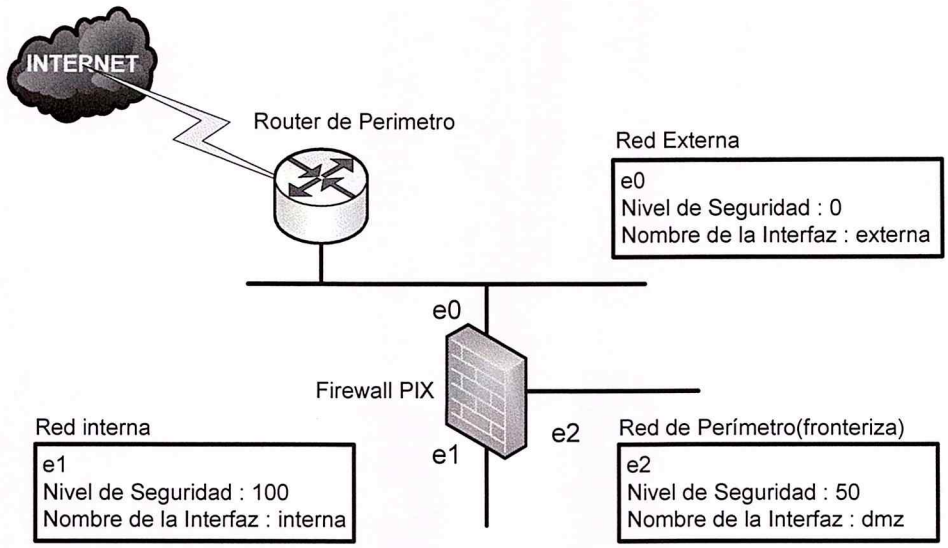


Figura 5.6. Niveles de Seguridad ASA

5.9. Firewall ASA

El dispositivo de seguridad adaptable de la serie Cisco® ASA 5500 es una plataforma que proporciona servicios de seguridad y VPN de próxima generación para entornos que van desde oficinas pequeñas/hogareñas y empresas medianas hasta grandes empresas. La serie Cisco ASA 5500 ofrece a las empresas un portafolio completo de servicios que se personalizan mediante ediciones de productos adaptados para firewall, prevención de intrusiones (IPS), anti-X y VPN.

Estas ediciones permiten una protección superior al proporcionar los servicios adecuados para cada ubicación. Cada edición combina un conjunto centrado de servicios Cisco ASA para satisfacer las necesidades de entornos específicos dentro de la red empresarial. Al satisfacer las necesidades de seguridad de cada ubicación, se eleva la posición de seguridad de toda la red.

Figura 5.7. Ediciones Serie Cisco ASA 5500

La serie Cisco ASA 5500 permite la estandarización en una sola plataforma para reducir el costo operativo general de la seguridad. Un entorno común de configuración simplifica la administración y reduce los costos de capacitación de personal, mientras que la plataforma de hardware común de la serie reduce los costos de repuestos.

Cada edición aborda las necesidades de entornos empresariales específicos:

- **Edición de Firewall:** permite a las empresas implementar en forma segura y confiable aplicaciones y redes cruciales. Su exclusivo diseño modular ofrece una protección de la inversión significativa y reduce los costos operativos.

- **Edición IPS:** protege los servidores y la infraestructura cruciales de la empresa contra gusanos, piratas informáticos y otras amenazas mediante una combinación de servicios de firewall, seguridad de aplicaciones y prevención de intrusiones.

- **Edición Anti-X:** protege a usuarios en sitios pequeños o remotos mediante un completo paquete de servicios de seguridad. Los servicios de firewall y VPN de calidad empresarial proporcionan una conectividad segura con el sistema principal de la empresa. Los servicios anti-X líderes de la industria de Trend Micro protegen al sistema cliente contra sitios Web maliciosos y amenazas basadas en el contenido tales como virus, spyware y phishing.

- **Edición VPN SSL/IPsec:** permite a los usuarios remotos acceder en forma segura a sistemas y servicios de la red interna, y admite la agrupación de redes VPN para implementaciones empresariales de mayor envergadura. Las tecnologías de acceso remoto Secure Sockets Layer (SSL) y VPN con seguridad IP (IPsec) se combinan con tecnologías de mitigación contra amenazas tales como Cisco Secure Desktop, y con servicios de firewall y prevención de intrusiones para asegurar que el tráfico VPN no introduzca amenazas a la empresa

Cinco razones principales para comprar dispositivos adaptables de seguridad de la serie Cisco ASA 5500

1. Firewall confiable y tecnología VPN protegida contra amenazas

Basada en la comprobada tecnología de dispositivos de seguridad Cisco PIX® y concentradores de la serie Cisco VPN 3000. La serie Cisco ASA 5500 es la primera solución que ofrece servicios de VPN SSL e IPsec protegidos por la tecnología de firewall líder del mercado.

2. Servicios Anti-X líderes de la industria

Combina la experiencia de Trend Micro en la protección contra amenazas y el control de contenidos de Internet con las comprobadas soluciones Cisco para proporcionar completas funciones antivirus, antispyware, bloqueo de archivos, antispam, antiphishing, bloqueo y filtrado de URL y filtrado de contenidos.

3. Servicios avanzados de prevención de intrusiones

Proporciona completos servicios anticipatorios de prevención de intrusiones para detener una amplia gama de amenazas, como gusanos, ataques a la capa de aplicaciones, ataques al nivel del sistema operativo, rootkits, spyware, intercambio de archivos entre pares y mensajería instantánea.

4. Completos servicios de administración y supervisión

Proporciona servicios intuitivos de administración y supervisión de dispositivos únicos a través del Cisco Adaptive Security Device Manager (ASDM), y servicios de administración de varios dispositivos de calidad empresarial mediante Cisco Security Management Suite.

5. Menores costos de instalación y operación

Al proporcionar un diseño y una interfaz compatibles con las soluciones de seguridad existentes de Cisco, la serie Cisco ASA 5500 permite que el costo de propiedad sea significativamente inferior tanto con respecto a la implementación de seguridad inicial como a la administración cotidiana.

CAPITULO 6: ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED INFORMÀTICA DE LA U.T.E.G.

En este capitulo se analiza la situación actual de la red informática, sus antecedentes

6.1. Antecedentes

En la actualidad la UTEG cuenta con lo detallado a continuación:

6.1.1. Parte Física

En lo que respecta a la parte física cuenta con cableado UTP categoría 5e debido a que es el más adecuado para las necesidades de la universidad en la actualidad, se utilizo este tipo de cable principalmente por costos y porque la infraestructura en donde se encuentra la universidad no es propia. Esta se la tiene que devolver en las mismas condiciones entregadas al inicio del contrato de arrendamiento. Solo posee una red de fibra entre la red del edificio 399 y el edificio 520 para poder enlazar las redes LAN.

En cuanto a las maquinas (computadoras) que posee actualmente la UTEG se las detalla a continuación por laboratorios y edificios:

UTEG		
Edificios	**PCs**	**Total de Pcs**
Edificio 610		**4**
Biblioteca	4	
Edificio 399		**12**
Edificio 520		**34**
Administrativa	3	
Laboratorio 1	13	
Laboratorio 2	12	
Laboratorio 3	6	
Edificio 402		**2**
Total		**52**

Tabla 6.1. Distribución actual de PCs

En la parte Administrativa hay máximo 2 usuarios por maquina y todos tienen su propio usuario de dominio, en los Laboratorios y Biblioteca hay 1 solo usuario.

Los sistemas operativos utilizados actualmente son Windows 2000 Server y Linux (Fedora) los mismos que se encuentran instalados en los servidores de la red, el tipo de back up utilizado es Tape Backup, con un software de administración que automatiza los respaldos.

La UTEG posee 3 Redes LAN, dos Redes que usan cableado y una Red Wireless, se utiliza cableado de tipo horizontal con topología de estrella. El tipo de redes con el que trabajan es en una topología de estrella en la parte física y son del tipo Ethernet 10/100, bajo protocolo TCP/IP. Los equipos que se utilizan son Routers y Switchs, y en algunos nodos aún usan Hubs. Los racks se encuentran en cada edificio, existe un RACK en donde se concentra el cableado. Uno de los rack es de pared el mismo que se encuentra en el área de servidores en el edificio 399. El equipo que se utiliza para la Wireless es Access Point marca DLink

La velocidad utilizada para la Red de Área Local es de 10/100 Mbps y para el enlace a Internet 256/512 Kbps. El proveedor de Internet actual es SatNet.

El software que maneja actualmente la UTEG para medir el ancho de banda es el MRTG:

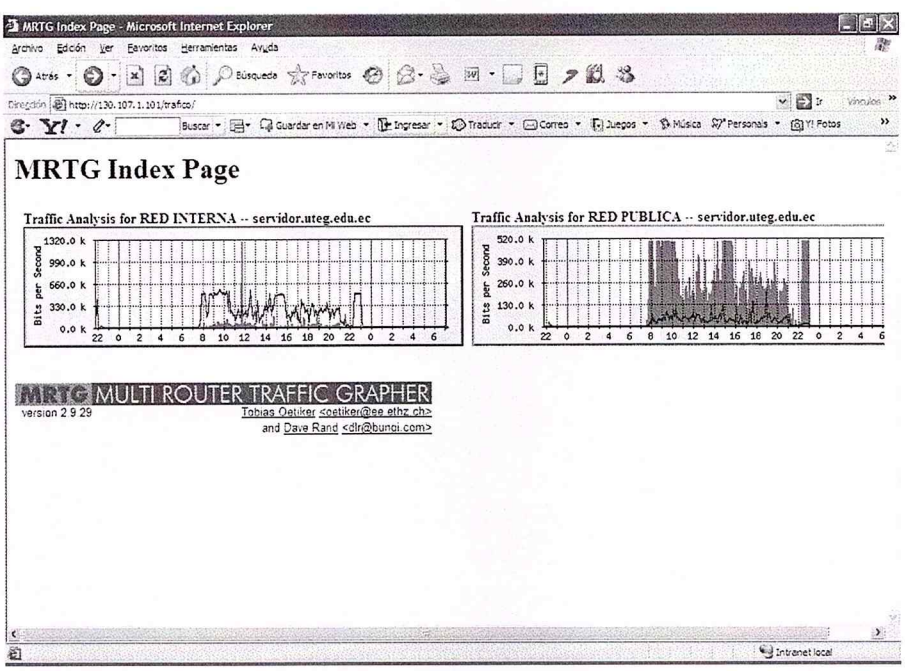


Figura 6.1. MRTG

El tipo de equipos con el que se conectan en la red LAN son Switch y Hub, éstos últimos son pocos. Las seguridades existentes en la Universidad para los equipos son puertas, acceso restringido esto es solo para personal autorizado en el área de servidores.

6.1.2. Diagrama de red

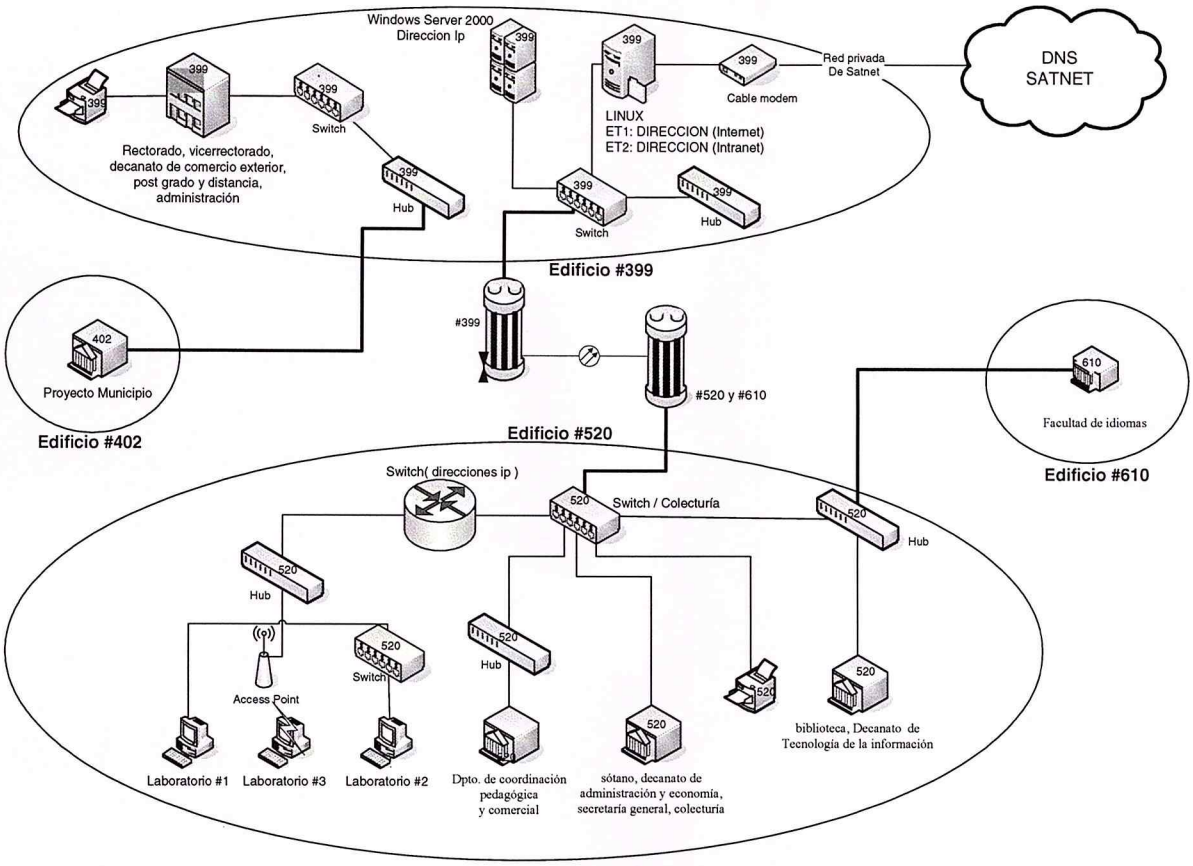


Figura 6.2. Diagrama de Red Actual de la Universidad

La universidad está comprendida por 4 edificios: el edificio # 399, el edificio # 520, el edificio # 610 y el edificio # 402. El cuarto de servidores del edificio # 399 consta de un SWITCH el mismo que tiene un convertidor para conectar el cable de fibra óptica al utp en donde se hallan conectados los servidores de la universidad, el servidor de Linux que es el da la salida al intranet y al Internet lo que permite la conexión a la red privada de tvcable.

El servidor de Windows Server 2000 que es el que se encarga de las direcciones ip, a su vez de el SWITCH del edifico # 399 se conecta un HUB que abarca la red LAN del edificio # 402 en donde está ejecutándose el proyecto con el municipio; del mismo HUB que abarca este proyecto tiene salida a un SWITCH en donde esta la red LAN del edificio # 399 que comprende el rectorado, vicerrectorado, decanato de comercio exterior, de post grado y distancia, parte administrativa y las impresoras de red.

El edifico #399 se enlaza con los edificios #520 y #610 por medio de fibra óptica, que a su vez llega hasta un convertidor que esta a lado del SWITCH que está en colecturía. Este switch

abarca la red LAN mas amplia en donde constan el sótano, decanato de administración y economía, secretaría general, colecturía. Este es el punto principal de conexión de las demás áreas LAN, se encarga de la configuración de los usuarios del e_mail, de las impresoras que constan en la red, de la dirección IP SMTP, del correo POP3 (uteg.edu.ec), de la submask dirección, de la gateway dirección, de las direcciones de los nombres de dominios del sistema (dns).

El SWITCH que se encuentra ubicado en colecturía da salida para formar varias redes LAN. Una de ellas la que consta en le edificio #520 que por medio de un HUB conecta al departamento de coordinación pedagógica y comercial, la otra red LAN que se mantiene conectada por un HUB es la biblioteca, decanato de Tecnología de la información y el edificio #610 donde se encuentra la facultad de idiomas. El Switch principal del edificio #520 se conecta otro SWITCH que se encarga de dar direcciones ip dinámicas en los laboratorios; este SWITCH se conecta a un HUB que es el que da conexión a todos los laboratorio, el laboratorio 1 se mantiene en red mediante la misma conexión directa al HUB, el laboratorio 2 esta en red por medio de un SWITCH y el laboratorio 3 lo hace mediante un Access point (HUB Wireless).

6.1.3. Parte Lógica

El tipo de servidores que posee la UTEG son Windows 2000 y Linux bajo Fedora 4.
En lo que respecta a seguridades tienen claves de acceso, firewall, antivirus. Como seguridades lógicas tienen el ACL y el Firewall, que son configurados en el Servidor Linux. El Antivirus que se utiliza es Symantec en los servidores y estaciones Windows, y Vexira mail en el servidor Linux. Tiene continuos ataques al servidor Linux. Se recibe continuamente correo SPAM.
Los Controladores de dominio=>Windows 2000 Server
Los programas que poseen en el servidor son:
LINUX =>se actualiza cada 5 minutos (replica) con la base de Miami.
PROXY=> squid
Denegador de servicio=>Dans guardian
Regla de ruteo a través de mail (antivirus) =>Vexira

No Tiene cerrados todos los puertos de acceso debido a que el proveedor de correo electrónico es palo santo y debe tener acceso al servidor de Miami, el mismo que cada 5 min. Se actualiza con la base de datos de dicho servidor.

La marca de los switch son D-Link (los switch son 100/100).Pero se navega en 10/100 porque el ancho de banda baja por los hubs.

La universidad tiene para red inalámbrica un Access point de la categoría "Indoor", con una radio de 50 metros.

SISTEMA ADMINISTRATIVO:

Los usuarios:

1. Colecturía
2. Contabilidad
3. Cobros / pagaduría
4. Secretarias de facultad

SISTEMA ACADEMICO:

Los usuarios:

1. Decanos
2. Alumnos
3. Profesores
4. Coordinadores
5. Administrador

CAPITULO 7: IDENTIFICACIÓN DE LOS REQUERIMIENTOS DE COMUNICACIÓN DEL NUEVO CAMPUS UNIVERSITARIO

7.1. Identificación de Requerimientos de la UTEG

El objetivo de la Universidad es llegar a tener una red con los mejores equipos tecnológicos que están en funcionamiento actualmente en el mercado, equipos evaluados que certifiquen el correcto funcionamiento de las redes. Se debe saber en que se van a regir para implementar de una mejor manera la red debido a la magnitud de la misma, para que este acorde a las necesidades de los usuarios; también se debe tener en cuenta el porcentaje de crecimiento de la red en el futuro y analizar todas las seguridades necesarias para evitar la perdida de información y la visita de Hackers que puedan ocasionar problemas en la red.

7.2. Identificación del área de cobertura

El área de cobertura de la red abarca todos los edificios, estos son:

1. Área de Administración
2. Desarrollo Regional
3. Auditorio
4. Biblioteca
5. Cafetería y la Asociación de estudiantes
6. Facultad de Tecnología de la Información
7. Facultad de Administración
8. Facultad de Economía
9. Facultad de Comercio Exterior
10. Facultad de Postgrado
11. Educación a distancia
12. Seguridad
13. Preparatoria
14. Colegio y Escuela

7.3. Requerimientos de Conectividad

Como identificamos en el área de cobertura son 14 los edificios que se van a enlazar en el nuevo campus, sin embargo en lo que respecta al área de cableado estructurado solo podemos estudiar 12 ya que solo de estos nos proporcionaron los planos arquitectónicos. A continuación el cuadro de distribución de puntos de voz y datos de cada edificio.

DISTRIBUCION DE PUNTOS DE VOZ Y DATOS												
EDIFICIOS		SOTANO		PLANTA BAJA		PLANTA PRIMERO ALTO		PLANTA SEGUNDO ALTO		TOTAL DE PUNTOS		Total de Puntos
		Puntos de Voz	Puntos de Datos	Puntos de Voz	Puntos de Datos	Puntos de Voz	Puntos de Datos	Puntos de Voz	Puntos de Datos	VOZ	DATOS	
1	AREA ADMINISTRATIVA			27	36	5	9			32	45	77
2	AUDITORIO	0	1	0	2	1	3			1	6	7
3	BIBLIOTECA			2	14	1	8			3	22	25
4	CAFETERIA			1	1	2	17			3	18	21
5	CENTRO DESARROLLO REGIONAL			2	21	3	6			5	27	32
6	COLEGIO Y ESCUELA			14	97	6	67	4	120	24	284	308
7	FACULTAD ADMINISTRACION			3	53	0	48	0	48	3	149	152
8	FACULTAD COMERCIO EXTERIOR			3	53	0	48	0	48	3	149	152
9	FACULTAD ECONOMIA			3	53	0	48	0	48	3	149	152
10	FACULTAD POSTGRADO			5	86	0	5	0	0	5	91	96
11	FACULTAD TECN.DE LA INFORMACION			3	49	0	48	0	48	3	145	148
12	PREPARATORIA			4	4	0	0	0	0	4	4	8
TOTAL										89	1089	

Tabla 7.1. Distribución de puntos de voz y datos

Adicional identificamos los lugares de conexión inalámbrica estos son lugares estratégicos como valor agregado a los estudiantes y profesores que necesiten navegar en su computador personal.

ACCESS POINT					
EDIFICIOS	SOTANO - ACCESS POINT	PLANTA BAJA - ACCESS POINT	PLANTA PRIMERO ALTO - ACCESS POINT	PLANTA SEGUNDO ALTO - ACCES POINT	TOTAL
AUDITORIO			1		1
BIBLIOTECA		1	1		2
CAFETERIA		1	1		2
FACULTAD DE TECNOLOGIA DE LA INFORMACION		2			2
TOTAL					7

Tabla 7.2. Access Point

Ya que se han identificado los puntos de voz y datos, se procede a utilizar una Matriz de facilidades con la finalidad de saber los requerimientos en cuanto a la conectividad de la Red, resumida en la siguiente tabla.

MATRIZ DE FACILIDADES														
		DIRECCIONAMIENTO		PUNTO		WIRELESS		VLAN					ACCESO	
	EDIFICIOS	ESTATICA	DINAMICA	DATOS	VOZ	WEP	LIBRE	ADMINISTRATIVA	LABORATORIOS	ESTUDIANTES	PEDAGOGIA	RRHH	INTRANET	INTERNET
1	AREA ADMINISTRATIVA	45		45	32			36			5	4	X	X
2	AUDITORIO	6		6	1	1		6						
3	BIBLIOTECA	8	14	22	3	2		15	7				X	X
4	CAFETERIA	17	1	18	3	2		2	4	12			X	X
5	CENTRO DESARROLLO REGIONAL	10	17	27	5			6	3	18			X	X
6	COLEGIO Y ESCUELA	55	229	284	24			39	204	41			X	X
7	FACULTAD ADMINISTRACION	15	134	149	3			9	123	17			X	X
8	FACULTAD COMERCIO EXTERIOR	15	134	149	3			9	123	17			X	X
9	FACULTAD ECONOMIA	15	134	149	3			9	123	17			X	X
10	FACULTAD POSTGRADO	6	85	91	5			6	80	5			X	X
11	FACULTAD TECN.DE LA INFORMACION	11	134	145	3	2		5	123	17			X	X
12	PREPARATORIA	3	1	4	4			3	1					
	TOTAL	206	883	1089	89	7								

Tabla 7.3. Matriz de Facilidades

Se puede apreciar en cantidades el direccionamiento de acuerdo a sus direcciones como van a estar, ya sea estática o dinámica, la cantidad de puntos de voz y datos que hay por cada edificio, el tipo de acceso Wireless que hay en el campus y en que edificios se va a emplear, las cantidad de puntos de acuerdo a las VLANs, y el acceso hacia la Intranet e Internet.

Adicional se recurre a utilizar direcciones IP, dinámicas y estáticas con la finalidad de manejar de una mejor forma los recursos. Además se manejaran VLANs por la seguridad y el control de acceso a la red.

La Matriz de Facilidades fue sacada de los planos arquitectónicos del nuevo Campus de estos se procedió a hacer el conteo de puntos de voz y datos por edifico, en este caso separando por piso la cantidad de puntos de acuerdo a las necesidades de cada usuario. Cabe recalcar que

solo se pudo tomar información de 12 edificios, ya que solo nos proporcionaron los planos arquitectónicos de los mismos. (VER ANEXOS DEL 1 AL 12 SOPORTE DE LOS CUADROS).

7.4. Identificación de Requerimientos para el Backbone de Fibra Óptica

De acuerdo a lo planteado anteriormente tenemos en nuestra cobertura 14 edificios que son los que vamos a enlazar, podemos realizar esta unión de algunas maneras, de acuerdo a las diferentes topologías que hemos conocido en el transcurso de este proyecto, sin embargo decidimos enlazarlas por medio de un anillo. Por lo tanto vamos a identificar las necesidades de los 14 edificios:

- Ancho de banda para 1096 puntos que van a estar enlazados en este anillo a diseñar.
- Salida a Internet
- Seguridad en la parte lógica y física

7.5. Identificación de Requerimientos para la Central Telefónica

Según el análisis realizado los puntos de voz a implementarse serán 89, por lo tanto es el número de extensiones que tendremos en el nuevo campus de la Universidad.

La tecnología a usarse es Voz sobre IP con la finalidad de que toda el área administrativa se encuentre comunicada y reducir costos de llamadas telefónicas convencionales.

CAPITULO 8: DISEÑO DE LA RED INFORMATICA DEL NUEVO CAMPUS DE LA U.T.E.G.

En base de los requerimientos del capitulo anterior se ha determinado dividir el diseño a los siguientes temas:

8.1. Modelo Jerárquico.
8.2. Diseño de Red para cada Edificio.
8.3. Diseño del Backbone de fibra para el Campus.
8.4. Identificación de requerimientos de Switch por Puntos de Voz y Datos
8.5. Diseño de la Red Wi-fi para zonas concurrentes
8.6. Direccionamiento IP
8.7. Diseño de Seguridad y Acceso a Internet.
8.8. Resumen de Equipamiento a utilizar.
8.9. Certificaciones y Pruebas

8.1. Modelo Jerárquico

Con el fin de simplificar el diseño, implementación y administración de las redes, se baso en un modelo jerárquico para describir la red informática. Es muy importante comprender el modelo para poder determinar el equipo y características que se van a necesitar en la red.

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

El modelo Jerárquico se va a distribuir de la siguiente manera:

- Capa de Acceso
- Capa de distribución
- Capa del núcleo Principal

Capa de Acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. A esta capa se la denomina capa de puesto de trabajo. Los usuarios y todos los recursos a los que se necesitan acceder con más frecuencia están disponibles a nivel local. En la capa de acceso se pueden encontrar múltiples de grupos de usuarios con sus correspondientes recursos.

Capa de Distribución

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. A esta capa se la denomina capa de grupo de trabajo. La función principal de esta capa es realizar funciones como enrutamiento, filtrado y acceso a WAN. La capa de distribución abarca una gran diversidad de funciones, tales como:

- Servir como punto de acumulación para acceder a los dispositivos de capa.
- Enrutar el tráfico para proporcionar a los departamentos o grupos de trabajos.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token ring y Ethenet.
- Proporcionar servicios de seguridades y filtrado.

Capa de núcleo Principal

La capa del núcleo principal se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. A esta capa se la conoce como capa Backbone. Generalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Como ejemplos de estos servicios se puede hacer referencia al correo electrónico, al acceso a Internet o una videoconferencia.

Cuando un usuario necesite acceder a un servicio corporativo, la petición se procesa a nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado al núcleo.

8.2. Diseño de la Red de cada edificio

Para el diseño de la red de cada edificio tenemos dos opciones; la primera, hacer una red alambrica y la segunda opción es hacer una red inalámbrica.

Se escogió la opción de red alambrica debido a que esta ofrece mejores beneficios a cualquier tipo de red, proporciona mayor y mejor seguridad de conexión en la actualidad. En base de las investigaciones y de la practica, la red inalámbrica aun no esta plenamente desarrollada para poderse implementar del todo en una red compleja, en vista de que existe una variedad de estándares de comunicación entre Access Point y las tarjetas inalámbricas de las PC'S; también se debe tomar en cuenta donde se van a colocar los equipos los parámetros de configuración de los mismos, el grosor de las paredes.

Entre los estándares que se a consideran en el desarrollo del proyecto son:

- Estándar 802.11b: se conoce como Wi-fi o fidelity inalámbrica, comprobación de la interoperabilidad entre los productos de distintos fabricantes. Trabaja con una frecuencia de 2.4 Ghz y con una velocidad de datos de 11 Mbps.

- Estándar 802.11g: Desarrolla un estándar de velocidad alta con una frecuencia portadora de la onda idéntica a la 802.11b pero que utiliza OFDM como técnica de propagación y la integración de QAM como una de las técnicas de modulación permitida. Trabaja con una frecuencia de 2.4 Ghz y con velocidad de datos de 36 o 54 Mbps.

- Estándar 802.11a: es un complemento de los estándares 802.11b y 802.11g. Trabaja con una frecuencia de 5.7 GHz y con una velocidad de datos de 54 Mbps.

Para realizar un correcto cableado estructurado dentro de los edificios se va a necesitar los siguientes elementos:

- Cable UTP 4 pares cat6 marca Quest metros
- Conectores RJ-45 marca Quest (funda 100 und)
- Cajas sobrepuestas 40mm marca Dexson
- Face plate 2p con i.d. marca Quest

- Jack cat6 marca Quest
- Patch cord 3ft cat6 marca Quest
- Patch cord 7ft cat6 Marca Quest
- Patch panel 24p solido cat6 marca Quest
- Organizador horizontal 60x40 1ur marca Beaucoup
- Organizador vertical 84" 80x80mm marca Beaucoup
- Rack de piso 72" (36ur) tuerca remachada marca Beaucoup
- Gabinete de Piso 72" 180x604x754 MM marca Beaucoup
- Canaleta 40x25 marca Dexson
- Accesorios para canaleta 20x12 marca Dexson

Adicional utilizaremos Switch 3COM Baseline 2824 en capa 2, (MAS DETALLES TECNICOS EN EL ANEXO 13) de acuerdo a la cantidad de puntos de voz y datos que se necesite para cada planta.

Diseño de cada estación de trabajo por cada piso de edificio.

En cada estación de trabajo se va a tener una tarjeta NIC, la cual va a permitir la conexión por medio del Patchcord al Jack, el mismo que va a estar conectado mediante el cableado estructurado al Patch Panel; a su vez se va a enlazar mediante un Patchcord al Switch 3COM.

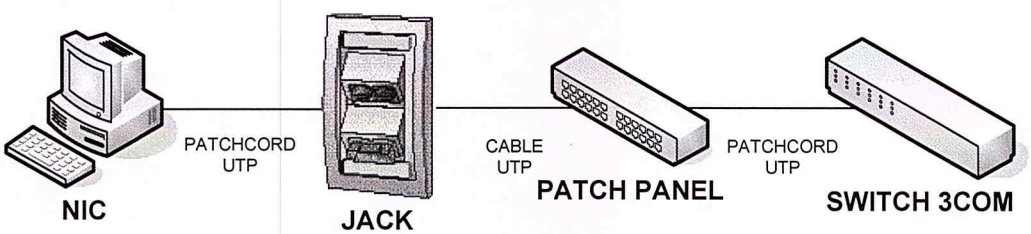


Figura 8.1. Cableado Horizontal

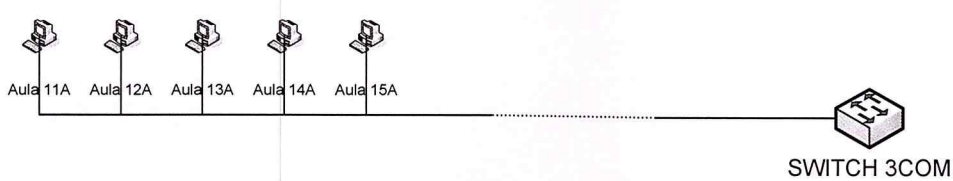


Figura 8.2. Diseño de Red por piso de edificio

El diseño del cableado vertical se forma mediante el enlace directo de cada uno de los Switch 3COM Baseline 2824 por planta hasta el Switch de Backbone.

El grafico del cableado vertical hacia el Switch del Backbone de cada edificio quedaría de la siguiente manera

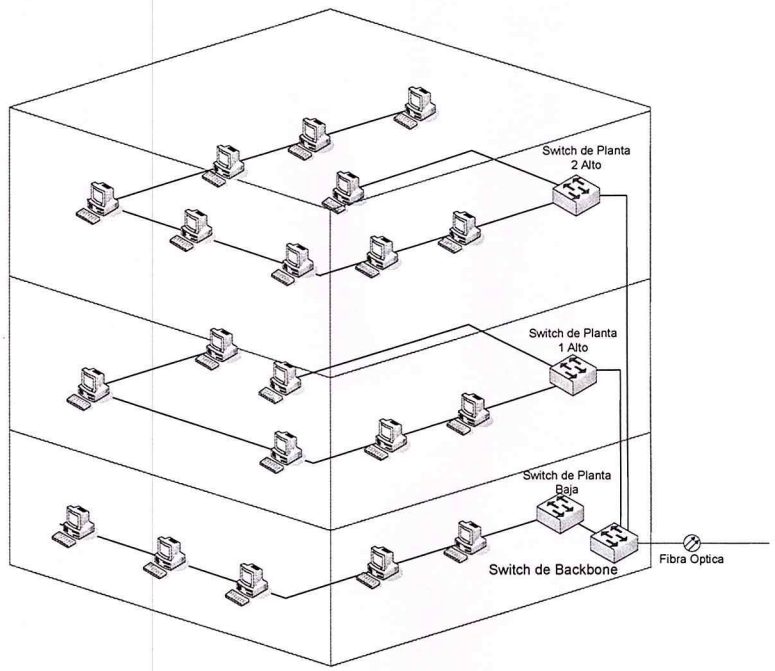


Figura 8.3. Cableado Vertical

8.3. Diseño de Backbone de fibra para el campus

Se decidió analizar 2 escenarios de Backbone de fibra Optica para la conexión de los 14 edificios, el tipo de fibra a utilizar será Fibra Multimodo de índice escalonado debido a que la distancia entre edificios es corta y el costo del equipo final es accesible.

Para el diseño de Backbone de fibra óptica para el nuevo campus se va a utilizar un Switch Cisco Catalyst 3560G-24PS (MAS DETALES TECNICOS EN EL ANEXO 14).

En cada piso hay un Switch 3COM de acceso que se conectan al Switch de fibra Cisco Catalyst 3560G-24PS que se encuentra en la planta baja de cada uno de los edificios. La conexión entre edificio se da mediante la fusión de la fibra óptica con el pigtail de fibra en la bandeja de empalme del ODF que se encuentra dentro del Patch Panel para fibra óptica, con esto se va a fusionar los 6 hilos de fibra de entrada de un extremo con los 6 hilos de pigtail. Una vez que suceda esto, el pigtail se unirá por medio de un conector macho a la placa

adaptable mediante un conector hembra. Se debe tomar en cuenta que en el ODF se puede adaptar 3 placas, en donde solo utilizaremos 2 espacios para las placas adaptadoras, por tal motivo se va a utilizar una placa ciega para tapar el espacio que no se va a utilizar. Luego estas 2 placas adaptadoras van a estar conectadas por medio un Patchcord al Switch del Backbone. Se debe tomar en cuenta que se realicen las respectivas mediciones con el OTDR que es la certificación del buen funcionamiento de la fusión de los hilos de fibra con el pigtail.

El proceso de la fusión se la hace al otro edificio para la unión del backbone de fibra óptica, de tal manera que se termina fusionando 12 hilos de fibra óptica por cada edificio.

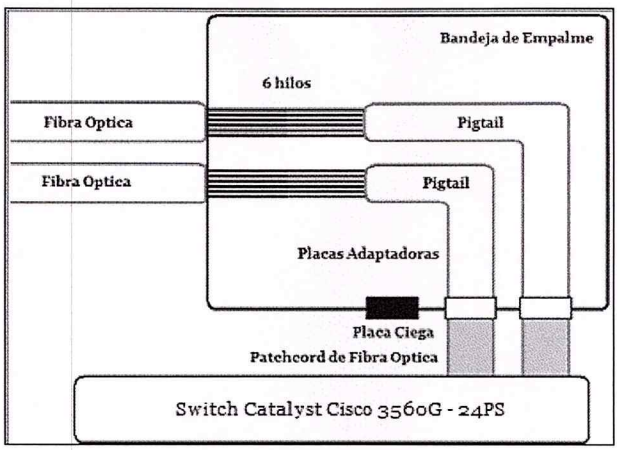


Figura 8.4. Grafico del ODF

El Backbone de fibra le dará a la universidad un ancho de banda mayor al que tienen en la actualidad, a su vez podrán utilizar el cableado interno estructurado categoría 6 para enlazar conjuntamente la información que va a los puntos de voz y datos mediante un mismo cable con un equipo de voz IP, esto abarataría mas costos en lo que respecta a la comunicación internacional y si se requiere tener una conferencia o una clase on line lo podrán realizar si ponen los equipos adecuados debido a que el cableado que se oferta para implementar es una excelente opción y se acopla a las necesidades de la Universidad según los planos arquitectónicos.

Hay tres razones por las que el uso de fibra óptica constituye una manera efectiva de mover el tráfico de Backbone:

- Las fibras ópticas son impermeables al ruido eléctrico.
- La fibra no conduce corrientes que puedan causar bucles en la conexión a tierra.

- Los sistemas de fibra óptica tienen un ancho de banda elevado y pueden funcionar a altas velocidades.

8.3.1. Escenario 1: Topología Anillo

Se decidió hacer un anillo de Fibra Optica para la conexión de los 14 edificios, de manera que si se da un corte de fibra en un edificio, la comunicación llegue a los otros sin ningún inconveniente y no será interrumpida. Aunque si se da el corte se tiene ya establecido un análisis de costos sobre un backup del cableado de fibra optica que se utiliza en el Backbone, para evitar en el peor de los casos dos cortes en el anillo de fibra optica.

Para poder llevar a cabo el anillo de fibra óptica que va a generar un enlace entre cada uno de los edificios se necesitan los siguientes elementos:

- Patch panel para Fibra Óptica, Siemon (ODF) de 12 puertos
- Placa adaptadora de 6 puertos SC
- Placa ciega para Patch panel de Fibra Optica.
- Pigtails SC, Multimodo 62.5/125 um
- Patch cord de F.O.Multimodo 62.5/125 um SC/SC, 3 m.
- Fusiones de hilos de fibra óptica (mano de obra)
- Mediciones OTDR
- Fibra Optica Multimodo 62.5/125 um, de 6 hilos, Tipo ducto
- Switch de fibra Cisco Catalyst 3560G-24PS
- Switch 3COM Baseline 2824 de acceso

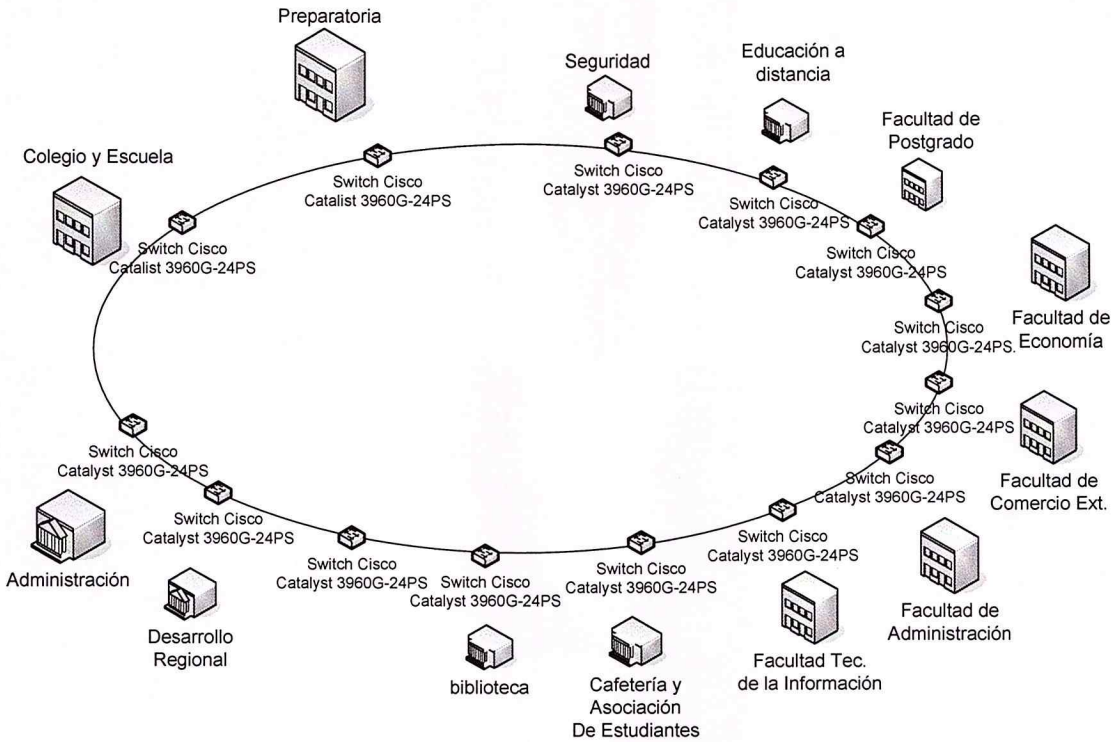


Figura 8.5. Diseño del Anillo de Fibra Optica

8.3.2. Escenario 2: Topología Estrella

Se decidió hacer una estrella de Fibra Optica para la conexión de los 14 edificios, de manera que si se da un corte de fibra en un edificio, la comunicación llegue a los otros sin ningún inconveniente ya que no alteraría en nada debido al tramo que hay de cada edificio al edificio principal. Aunque si se da el corte se tiene ya establecido un análisis de costos sobre un backup del cableado de fibra optica que se utiliza en el Backbone, para evitar en el peor de los casos dos cortes en el anillo de fibra optica.

Para poder llevar a cabo la estrella de fibra óptica que va a generar un enlace entre cada uno de los edificios se necesitan los siguientes elementos:

- Patch panel para Fibra Óptica, Siemon (ODF) de 12 puertos
- Placa adaptadora de 6 puertos SC
- Placa ciega para Patch panel de Fibra Optica.
- Pigtails SC, Multimodo 62.5/125 um
- Patch cord de F.O.Multimodo 62.5/125 um SC/SC, 3 m.
- Fusiones de hilos de fibra óptica (mano de obra)
- Mediciones OTDR

- Conectores SC Multimodo
- Conectorizaciones de Fibra Optica
- Patch cord 7FT Cat6 Marca Quest
- Convertidor Gigabit 1000 Base-T to SX (SC Type)
- Fibra Optica Multimodo 62.5/125 um, de 6 hilos, Tipo ducto
- Switch de fibra Cisco Catalyst 3560G-24PS
- Switch 3COM Baseline 2824 de acceso

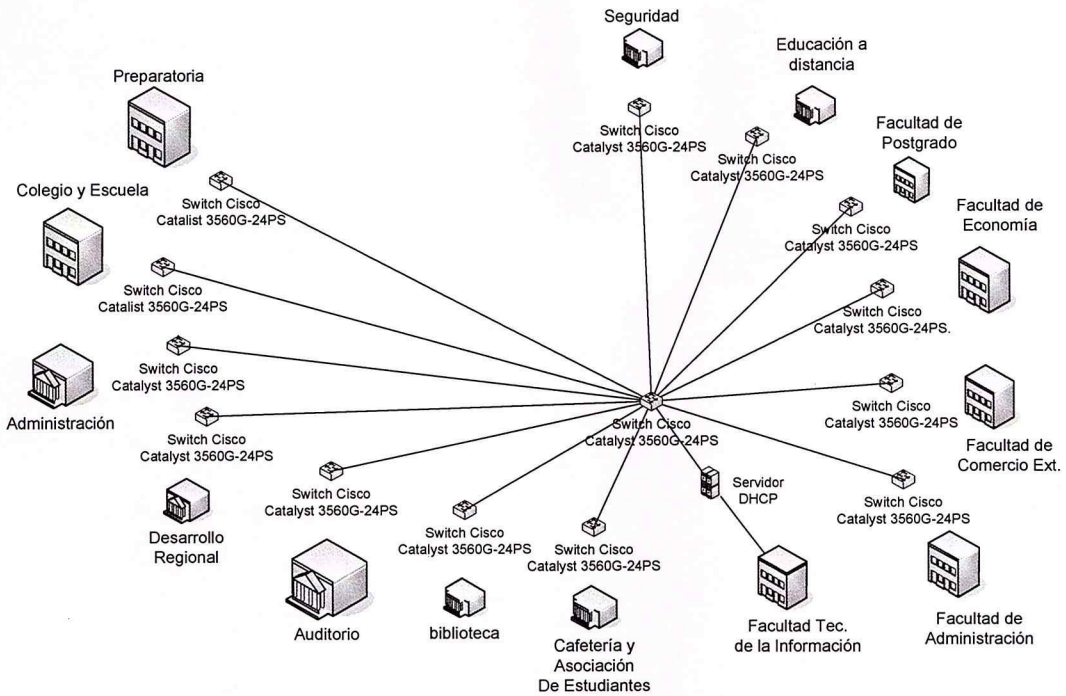


Figura 8.6. Diseño de la Estrella de Fibra Optica

El Backbone de fibra óptica tanto en Anillo como en estrella también puede actualizarse y ofrecer un mayor rendimiento cuando se cuenta con un equipo de Terminal mas avanzado.

8.4. Identificación de requerimientos de Switch por Puntos de Voz y Datos

Para ver cuantos Switch se van a utilizar, se debe tener la cantidad correcta de distribución de los puntos de voz y de datos esto incluye los puntos de los Access point por piso de cada edificio. Se va a proceder a instalar un Switch Principal en el Backbone de cada edificio por medio del cual se van a enlazar los edificios del campus.

En el Switch Principal se procede a reservar una cantidad establecida de puertos para las conexiones entre los edificios, en los puertos restantes se procede a conectar a usuarios del mismo piso; se coloca un Switch de Acceso para los puntos que falten por enlazar.

En los siguientes pisos se proceden a colocar de acuerdo a los puertos contabilizados la cantidad de Switch, teniendo en cuenta de que cada Switch de Acceso va a tener 24 puertos, no obstante si se ocupa todo los puertos del Switch y queda un porcentaje mínimo de puntos libres por unir, se utilizara el Switch de otro piso del mismo edificio.

Inventario de Equipos												
EDIFICIOS	AREA ADMINISTRATTVA	AUDITORIO	BIBLIOTECA	CAFETERIA	CENTRO DE DESARROLLO REGIONAL	COLEGIO Y ESCUELA	FACULTAD ADMINISTRACION	FACULTAD COMERCIO EXTERIOR	FACULTAD ECONOMIA	FACULTAD POSTGRADO	FACULTAD TECNOLOGIA DE LA INFORMACION	PREPARATORIA
wifi		1	2	2							2	
Sotano												
Puntos de Voz		0										
Puntos de Datos		1										
Planta Baja												
Switch Cisco Catalyst3560G	1	1	1	1	1	1	1	1	1	1	1	1
puertos disponibles sw de backbone	16	16	16	16	16	16	16	16	16	16	10	16
puertos por atender en sw 3com de acceso	47	-14	0	-14	7	95	40	40	40	75	42	-8
cantidad de sw 3com	2	0	0	0	0	4	2	2	2	3	2	0
Puntos de Voz	27	0	2	1	2	14	3	3	3	5	3	4
Puntos de Datos	36	2	14	1	21	97	53	53	53	86	49	4
total	63	2	16	2	23	111	56	56	56	91	52	8
Planta 1° Alto												
cantidad de sw 3com	1	0	1	1	1	3	2	2	2	1	2	0
Puntos de Voz	5	1	1	2	3	6	0	0	0	0	0	0
Puntos de Datos	9	3	8	17	6	67	48	48	48	5	48	0
total	14	4	9	19	9	73	48	48	48	5	48	0
Planta 2° Alto												
cantidad de sw 3com						5	2	2	2	0	2	0
Puntos de Voz						4	0	0	0		0	0
Puntos de Datos						120	48	48	48		48	0
total	0	0	0	0	0	124	48	48	48	0	48	0
Total Puntos de Voz	32	1	3	3	5	24	3	3	3	5	3	4
Total Puntos de Datos	45	7	24	20	27	284	149	149	149	91	147	4
cantidad de sw 3com	3	0	1	1	1	12	6	6	6	4	6	0
total	45											

Tabla 8.1. Inventario de Equipos

8.5. Diseño de la red Wifi para zonas concurrentes

Se incluyen en el proyecto 7 bases de Access Point AT-WA7400 Allied Telesis (VER ANEXO 15) para red inalámbrica como valor agregado para ciertos sectores concurrentes de la universidad, el cual le da a los alumnos y profesores la opción de navegar con su

computador portátil (Laptop) por medio de los centros de acceso de tal manera que los estudiantes registraran su User y Password y estos se validaran al Servidor donde se controla el acceso a Internet.

Este control permitirá al estudiante navegar en páginas que le sirvan para su preparación académica, se mantendrá un control estricto sobre el acceso a páginas que no entren en el plano de desarrollo o investigativo.

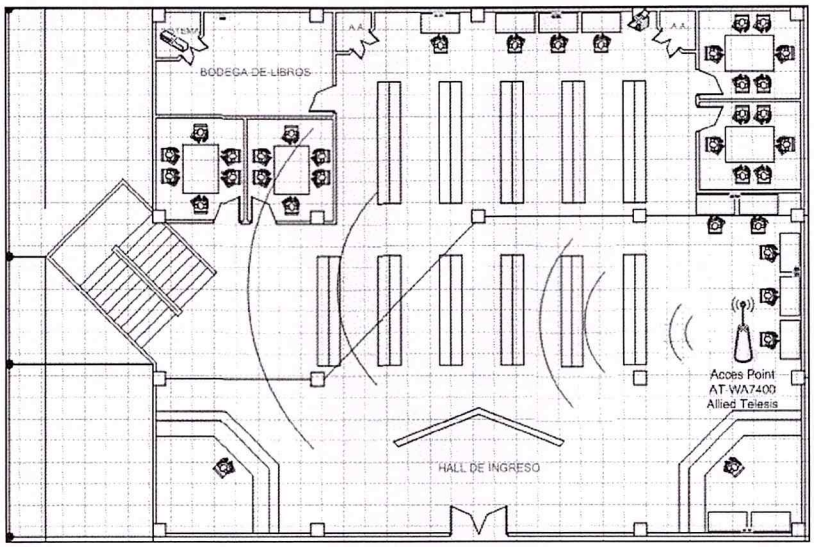


Figura 8.7. Wi-fi en la Biblioteca/Planta Baja

8.6. Direccionamiento IP

Se va a utilizar Direcciones IP de Clase B Privadas, debido a la cantidad de puntos de voz y datos, según el siguiente cuadro:

DIRECCIONAMIENTO IP								
EDIFICIOS	NUMERO DE DIRECCIONES IP'S		MASCARA DE RED	DIRECCION IP				
	USADAS	DISPONIBLES		RED	GATEWAY	BROADCAST	INICIO	FIN
AREA ADMINISTRATIVA	45	209	255.255.255.0	172.16.1.0	172.16.1.1	172.16.1.255	172.16.1.2	172.16.1.47
AUDITORIO	6	247	255.255.255.0	172.16.2.0	172.16.2.1	172.16.2.255	172.16.2.2	172.16.2.8
BIBLIOTECA	22	232	255.255.255.0	172.16.3.0	172.16.3.1	172.16.3.255	172.16.3.2	172.16.3.24
CAFETERIA	18	236	255.255.255.0	172.16.4.0	172.16.4.1	172.16.4.255	172.16.4.2	172.16.4.20
CENTRO DESARROLLO REGIONAL	27	227	255.255.255.0	172.16.5.0	172.16.5.1	172.16.5.255	172.16.5.2	172.16.5.28
COLEGIO Y ESCUELA	284	224	255.255.252.0	172.16.6.0	172.16.6.1	172.16.7.255	172.16.6.2	172.16.7.31
FACULTAD ADMINISTRACION	149	105	255.255.255.0	172.16.8.0	172.16.8.1	172.16.8.255	172.16.8.2	172.16.8.151
FACULTAD COMERCIO EXTERIOR	149	105	255.255.255.0	172.16.9.0	172.16.9.1	172.16.9.255	172.16.9.2	172.16.9.151
FACULTAD ECONOMIA	149	105	255.255.255.0	172.16.10.0	172.16.10.1	172.16.10.255	172.16.10.2	172.16.10.151
FACULTAD POSTGRADO	91	163	255.255.255.0	172.16.11.0	172.16.11.1	172.16.11.255	172.16.11.2	172.16.11.93
FACULTAD TECN.DE LA INFORMACION	145	109	255.255.255.0	172.16.12.0	172.16.12.1	172.16.12.255	172.16.12.2	172.16.12.147
PREPARATORIA	4	250	255.255.255.0	172.16.13.0	172.16.13.1	172.16.13.255	172.16.13.2	172.16.13.6

Tabla 8.2. Direccionamiento IP

Se puede observar todas las IPs, las cantidades que se van a usar en cada edificio y las que se encuentran disponibles para nuevos usuarios, la mascara de red, la dirección de Red de cada edifico, en si todo el direccionamiento IP que se va a manejar en la Universidad en cada uno de los edificios.

8.6.1. VoIP aplicada al Campus Universitario.

Como se menciono anteriormente se tomo en consideración los planos arquitectónicos para determinar de los puntos de voz de acuerdo a los usuarios que van a tener extensión telefónica.

En lo que respecta a la transmisión de Voz se tomo la tecnología de VoIP, está pasara por el mismo cableado estructurado de datos de cada uno de los edificios del nuevo Campus.

Diseño de cada estación de trabajo por cada piso de edificio.

En cada estación de trabajo que se necesite la transmisión de Voz se va a tener un teléfono Linksys - Sipura SPA-841 SIP VoIP Phone (VER ANEXO 16), la cual va a permitir la transmisión por medio del Patchcord al Jack, el mismo que va a estar conectado mediante el cableado estructurado al Patch Panel; a su vez se va a enlazar mediante un Patchcord al Switch 3COM.

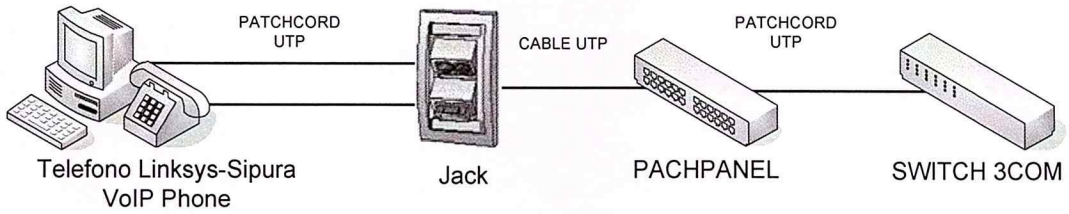


Figura 8.8. Cableado Horizontal (VoIP)

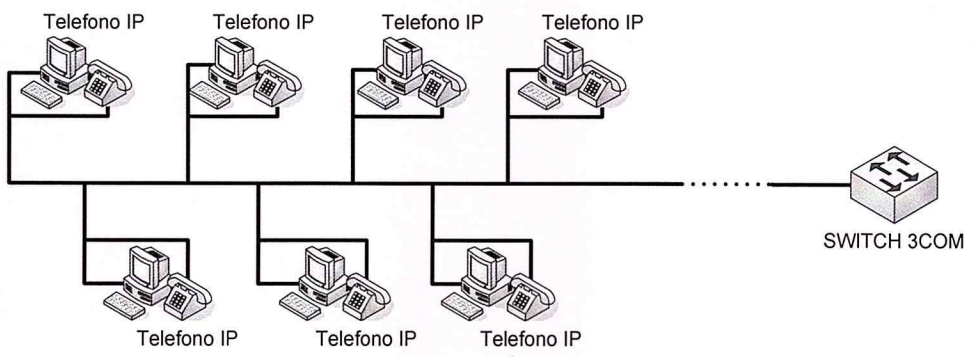


Figura 8.9. Diseño de Transmisión de VoIP por Piso

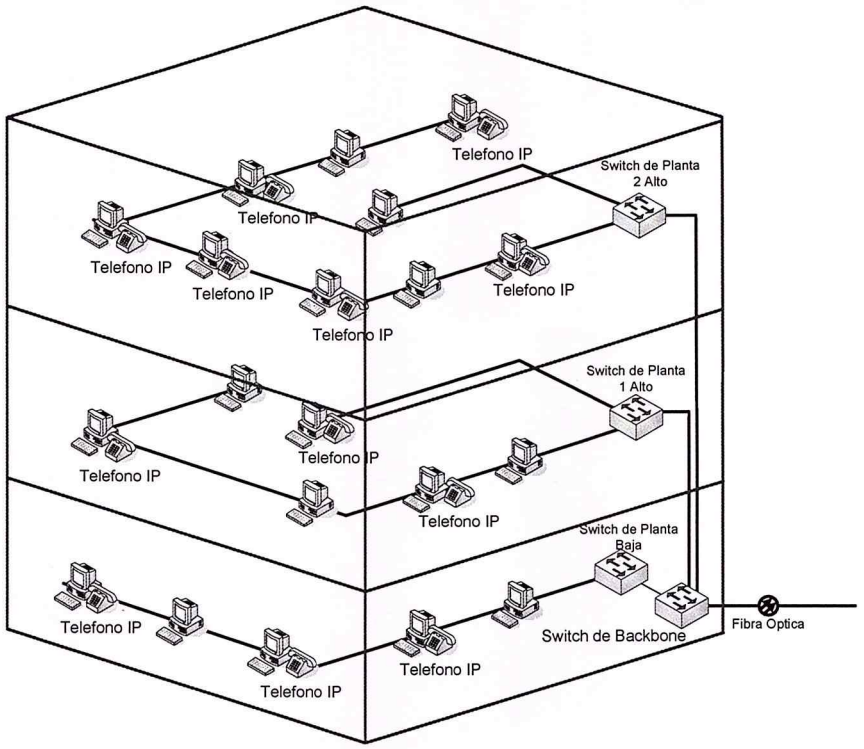


Figura 8.10. Cableado Vertical (VoIP)

En el Edificio Principal que es el edificio de Tecnología de la Información va a estar el equipo de VoIP de 16 FXO con una WAN Publica y una LAN la que va a estar conectada al IPPBX Server que es el Servidor Asterisk, el mismo que esta conectado al Switch Principal de Backbone, se hace esto debido a que si hay muchas extensiones se debe conectar en Cascada, en este caso tenemos 89 Puntos de Voz.

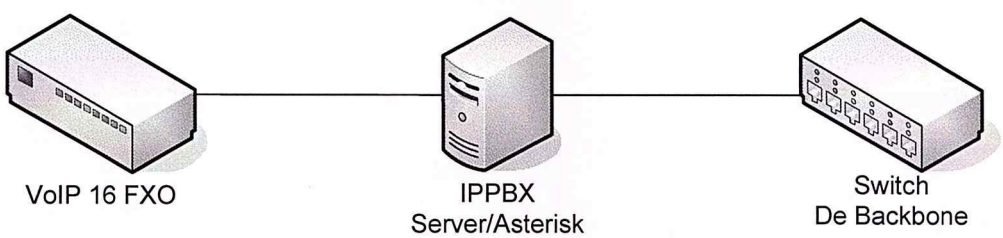


Figura 8.11. Estación VoIP en el Edificio Principal

8.7. Diseño de seguridad y acceso a Internet.

El proyecto se desarrolla en IPV4 debido a que se esta utilizando actualmente en el mercado global de redes, se manejan equipos de ultima tecnología para llevar estas configuraciones de direcciones.

Los equipos que se están utilizando en un futuro pueden crecer en su red e implementar el direccionamiento de la misma con la tecnología IPV6, que se esta utilizando en otros países como lo ultimo en avances tecnológicos. En el cual las direcciones de esta tecnología abarcan más redes para el crecimiento de red.

Además de la dirección física MAC, cada computador necesita de una dirección IP exclusiva o dirección lógica, para formar parte de la Internet. Varios son los métodos para la asignación de una dirección IP a un dispositivo. Algunos dispositivos siempre cuentan con una dirección estática, mientras que otros cuentan con una dirección variable que se les asigna cada vez que se conectan a la red. Cada vez que se necesita una dirección IP asignada dinámicamente, el dispositivo puede obtenerla de varias formas.

Las direcciones IP repetidas pueden detener el eficiente enrutamiento de los datos. Para la salida al mundo del Internet se va a utilizar un Router Cisco 1841 (MAS DETALLES TECNICOS EN ANEXO 21)

8.7.1. Firewall

Estas entidades han proliferado debido a Internet. Limitan la exposición de la red privada con el mundo exterior restringiendo accesos. Pueden monitorear toda la actividad hacia la llamada red de redes de forma efectiva, además de ayudar a mantener las políticas de seguridad, ya que son puntos centrales. Cabe destacar que no protege contra malas intenciones de personas dentro de la red privada, ni resguarda conexiones que no sean controladas por él y tampoco contra virus.

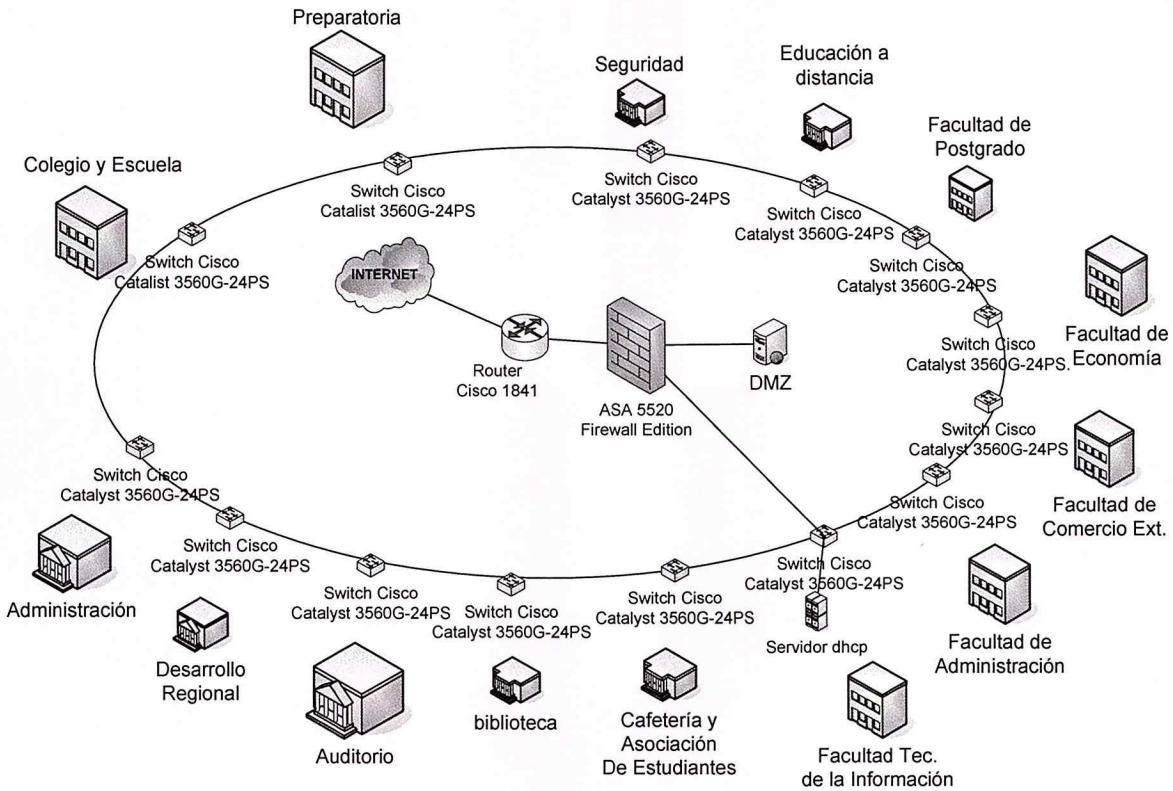


Figura 8.12. Anillo de Fibra con Acceso a Internet

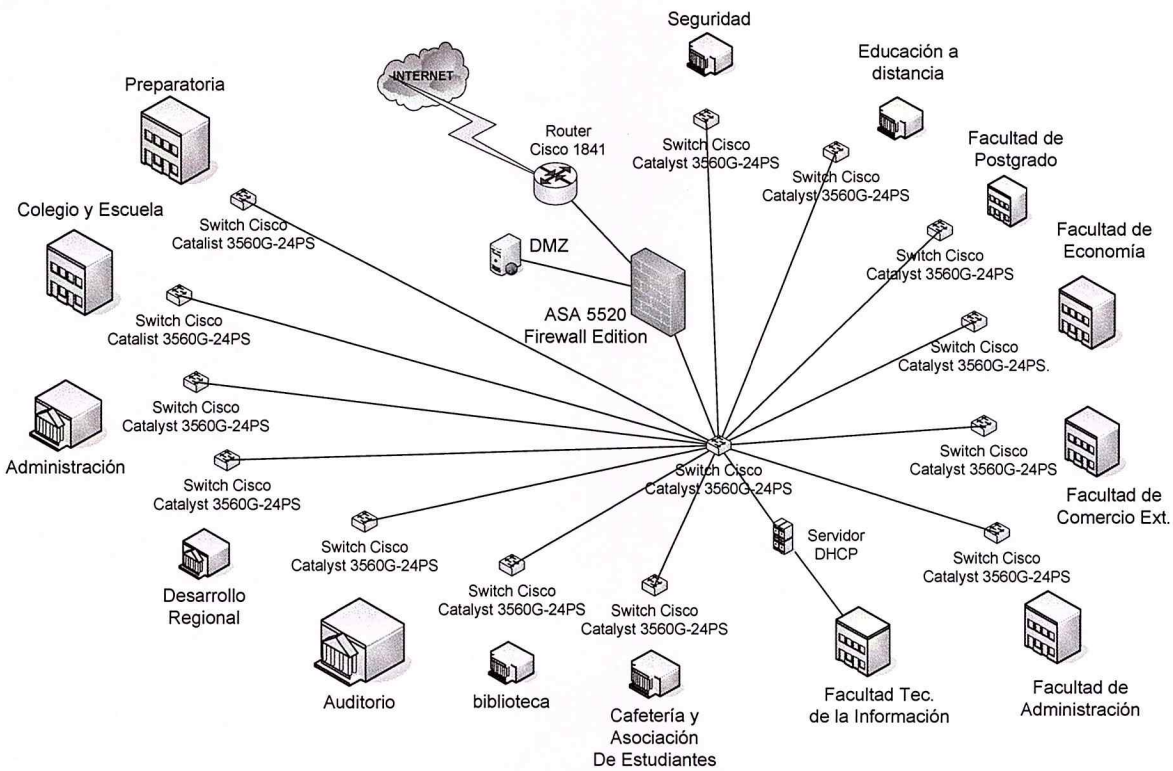


Figura 8.13. Estrella de Fibra con Acceso a Internet

El cometido básico de tener un firewall consiste en llevar a cabo las siguientes funciones:

- No permitir acceso desde el exterior hasta el interior.
- Permitir un acceso limitado desde el exterior hasta la DMZ.
- Permitir todo el acceso desde el interior hasta el exterior.
- Permitir un acceso limitado desde el interior hasta la DMZ.

8.7.1.1. Firewall PIX

Un dispositivo Cisco PIX es un firewall de hardware totalmente dedicado a este tipo de funciones de seguridad.

Todas las versiones de Cisco PIX tienen un número de modelo 5xx. Uno de sus modelos más populares es el PIX 501, diseñado para oficinas hogareñas y pequeñas redes. Otro de los muy conocidos es el PIX 515, para redes de tamaño medio.

El sistema operativo de estos dispositivos es el PIX Operating System (PIX OS), el cual si bien es similar a Cisco IOS, es lo suficientemente diferente como para frustrar a todo operador que no esté interiorizado en su línea de comando. Para facilitar la tarea de configuración y administración, el PIX ofrece una interface gráfica denominada PIX Device Manager (PDM). Esta interfaz es una aplicación desarrollada en Java que se ejecuta desde un navegador.

Típicamente un PIX posee una interfaz de salida que se suele conectar a la interfaz de entrada del router de acceso a Internet; y una interfaz de entrada que se suele conectar al switch LAN para enlazar con la red privada interna.

El firewall PIX que se va analizar en el proyecto es el Cisco PIX 515E (MAS DETALLES TECNICOS EN EL ANEXO 17), el diseño versátil de la unidad apoya hasta seis interfaces rápidos de 10/100 Ethernet, haciendo esta una buena opción aplicable, resistente de la seguridad con la ayuda de DMZ.

8.7.1.2. Firewall ASA

La línea Cisco ASA es una nueva línea de dispositivos de Cisco Systems que conjuga un firewall de hardware con una implementación anti-malware.

En el caso de Cisco ASA los modelos existentes corresponden a la serie 55xx. Hay cuatro versiones enterprise: Firewall, IPS, Anti-x y VPNs; y una versión business para empresas medianas y pequeñas. Un total de 5 modelos.

Todos los ASA operan con el software ASA versión 7.2.2 con una interfaz más cercana al Cisco IOS que PIX OS.

Estos dispositivos incluyen servicios de prevención de intrusiones (IPS) y concentrado de VPNs. Es por esto que Cisco Systems indica que un ASA realiza por sí solo las tareas que hasta ahora requerían 3 dispositivos separados: un firewall PIX, un VPN Concentrator (como el VPN 3000) y un IPS como el Cisco IPS 4000.

El firewall ASA que se va analizar en el proyecto es el Cisco ASA 5520 Firewall Edition (MAS DETALLES TECNICOS EN EL ANEXO 18), este diseño se basa en la tecnología confiable del dispositivo de seguridad Cisco PIX y del concentrador de la serie Cisco VPN 3000. Aporta una amplia gama de servicios de seguridad, con alta disponibilidad Activo/Activo y conectividad Gigabit Ethernet para empresas medianas.

8.7.1.3. Firewall PIX vs Firewall ASA

En los puntos anteriores se realiza un análisis sobre los detalles técnicos de cada uno de los Firewall, con la finalidad de seleccionar el equipo de seguridad de mejores especificaciones para proteger la red de la UTEG. Los 2 firewall son buenos pero se analiza el caso sobre las características de cada uno de ellos y se procede a hacer comparaciones entre los 2 para escoger el mejor y aplicar su funcionamiento en la protección de la red del nuevo Campus universitario.

Cisco PIX es y ha sido un excelente firewall, pero en los últimos años los requerimientos de prestaciones de seguridad de las redes ha variado sensiblemente.

Ya no resulta suficiente proteger a la red con un firewall en capacidad de realizar un filtrado de paquetes stateful. Han aparecido nuevos riesgos que incluyen virus, gusanos, phishing, ataques de capa de aplicación, la ejecución de aplicaciones no deseadas como mensajería instantánea, programas P2P, juegos, etc. El dispositivo que protege de este tipo o variedad de riesgos de seguridad es lo que denomina un Anti-X, o sea un dispositivo que brinda protección contra múltiples riesgos.

Un PIX no puede brindar este nivel de protección. Sin embargo muchas organizaciones buscan concentrar su implementación de seguridad en un único dispositivo, o lo que se suele denominar un dispositivo UTM (Unified Threat Management). O sea un dispositivo que brinde los servicios "todo en uno".

Cisco ASA es una respuesta a esta necesidad ya que ofrece protección a estos diferentes tipos de ataques. Los ASA soportan la posibilidad de inclusión de un módulo CSC-SSM (Content Security and Control Security Service Module). Este módulo es el que realiza las tareas de Anti-X constituyendo a los ASA en verdaderos dispositivos UTM. Sin el módulo CSC-SSM un ASA es muy semejante en sus capacidades a un PIX, aunque siempre con mayor performance.

CISCO PIX 515E	CISCO ASA 5520
Soporta 250 o mas usuarios	Numero ilimitado de usuarios
3 Puertos 10/100	4 Gigabit Ethernet ports and 1 Fast Ethernet port
Proporciona servicios avanzados de la seguridad y del establecimiento de una red para las redes del negocio, en una aplicación modular, purpose-built. Su diseño versátil de la unidad del uno-estante (1RU) apoya hasta seis interfaces rápidos de 10/100 Ethernet, siendo una opción excelente para los negocios que requieren una solución rentable, resistente de la seguridad con la ayuda de DMZ.	Proporciona completos servicios anticipatorios de prevención de intrusiones para detener una amplia gama de amenazas, como gusanos, ataques a la capa de aplicaciones, ataques al nivel del sistema operativo, rootkits, spyware, intercambio de archivos entre pares y mensajería instantánea.
Soporta IPV4 y IPV6,cambiar configuracion	Soporta IPV4 y IPV6,cambiar configuracion
Provee Direcciones Estaticas y dinamicas basadas en NAT y PAT Service	
25 es la cantidad maxima de VLANS	100 es la cantidad maxima de VLANS
Se maneja con el Servidor DHCP para distribuir las direcciones dinamicas	
Supports multiple virtual interfaces on a single physical interface through VLAN trunking, with support for multiple VLAN trunks per Cisco PIX Security Appliance	Cisco ASA Advanced Inspection and Prevention Security Services Module ASA-SSM-20
La aplicación de la seguridad de Cisco PIX 515E proporciona a usuario robusto y aplicación de la política del uso, protección del ataque del multi-vector, y los servicios seguros de la conectividad a través de una amplia gama de los servicios ricos de la seguridad y del establecimiento de una red, incluyendo: Mercado-Que conduce Voz-Sobre-IP y seguridad de las multimedias, Sitio-a-Sitio robusto y conectividad de IPSec VPN del acceso alejado	Puede extender su capacidad IPSec (IP Security) y SSL (Secure Sockets Layer) VPN para soportar mayor número de teletrabajadores y conexiones remotas. Puede duplicar la capacidad VPN sólo con instalar un upgrade de licencia VPN. Las aplicaciones del ASA 5520 pueden extenderse utilizando el Módulo de Servicios de Seguridad (SSM).
	Protegidos con la tecnología de firewall líder en el mercado

Tabla 8.3. Cuadro Comparativo PIX vs ASA

8.7.2. VLANS

En este proyecto se va hacer el diagrama de red mediante la división de áreas por VLANS, el objetivo de generar grupos de trabajos es que manejen la misma información entre si, y a su vez no sea mal utilizada o adulterada por alguna persona que no conste en la misma red.

Diseño de las VLANS en cada edificio:

Las VLANS que va a tener la universidad son:

- Administrador de la Red
- Administración
- Laboratorios
- Aulas
- Pedagogía
- RRHH

EDIFICIOS	AREA ADMINISTRATIVA	AUDITORIO	BIBLIOTECA	CAFETERIA	CENTRO DE DESARROLLO REGIONAL	COLEGIO Y ESCUELA	FACULTAD ADMINISTRACION	FACULTAD COMERCIO EXTERIOR	FACULTAD ECONOMIA	FACULTAD POSTGRADO	FACULTAD TECNOLOGIA DE LA INFORMACION	PREPARATORIA
VLANS	Administrador dela Red											
	Administracion		Administración									
			Laboratorios									
		Aulas				Aulas						
	Pedagogia											
	RRHH											

Tabla 8.4. VLANS en el nuevo Campus de la Universidad

NOTA: Las VLANS son independientes por cada edificio. Cada edifico esta compuesto de VLANS sin embargo solo se podrán ver los usuarios que estén dentro de la VLAN del mismo edificio.

8.7.3. ACLs

La configuración de las listas de acceso se ha basado en el tipo de tráfico y el uso de la red, se han creado listas flexibles que permitan trabajar sin muchas restricciones a los miembros de la red de la UTEG pero a la vez prohibida a lo que ser refiere a tráfico de hosts extraños. La necesidad de trabajar en equipo hace necesario que cada uno de los usuarios pueda compartir tráficos de datos con cualquier otro usuario, por lo tanto, se permite el libre tráfico entre ellos salvo en lo que respecta a los accesos al servidor de archivos de localidad.

- **ACL 1.- Negar el acceso a las redes que no sean de la UTEG**

  Negar el tráfico a diferentes direcciones IP de red que no pertenezcan al direccionamiento de la UTEG. Dicha condición a sido asignada para todas las interfaces usadas del Router Cisco 1841 para el tráfico entrante y saliente.

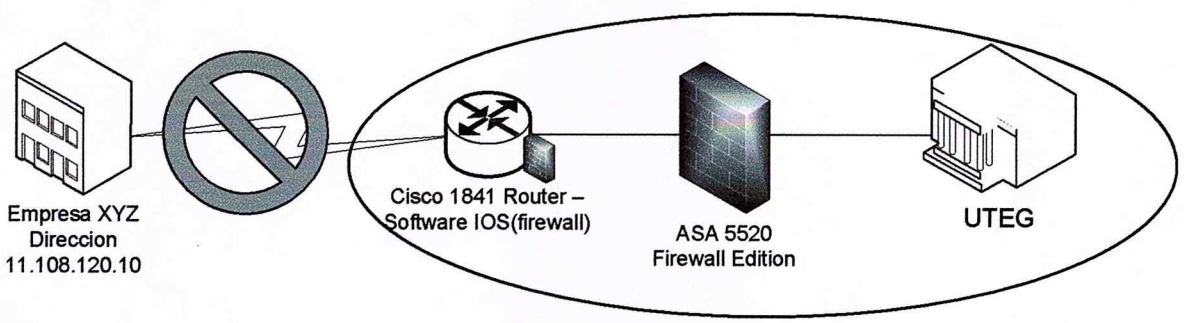


Figura 8.14. ACL 1

- **ACL 2.- Permitir el tráfico de la Internet**

  Permitir el tráfico hacia y desde la Internet a toda la red de la UTEG. Dicha condición se asigno a todas las interfaces del Router Cisco 1841.

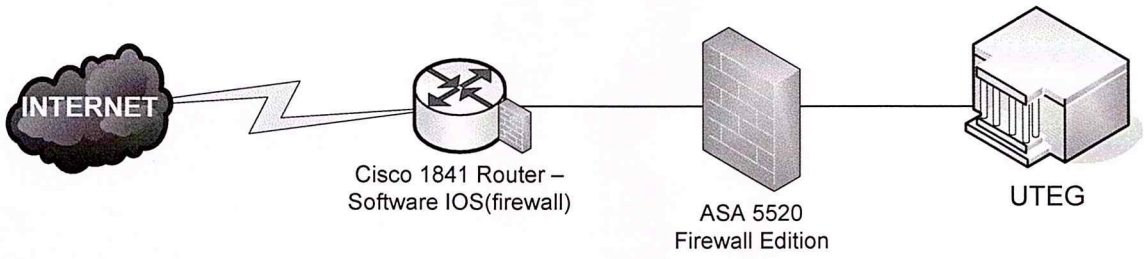


Figura 8.15. ACL 2

8.7.4. DMZ

La zona desmilitarizada es utilizada solo para servicios externos, esto son los servicios públicos:

- SMTP
- HTTP
- HTTP1

Se recomienda diseñar una DMZ para la protección del servidor Web y el acceso al servidor de correo electrónico ya que la Universidad se maneja con el proveedor que es Palo Santo. Esta zona es creada para los servicios que son accesibles desde afuera de la Universidad.

El objetivo de crear esta zona es para que las conexiones desde la red interna y la externa por medio de la DMZ este permitida, de esta manera los equipos que están en la DMZ pueden dar servicio a la red externa y a la vez se protege la red interna en caso de que intrusos quieran violar la seguridad de los equipos situados en esta zona.

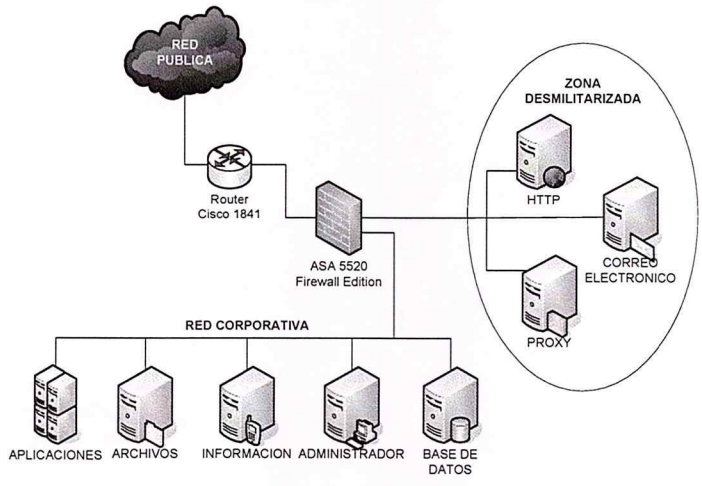


Figura 8.16. DMZ

8.7.5. Servidor DHCP

Se recomienda configurar DHCP (Protocolo de configuración dinámica de host) dentro del diseño de la red del nuevo campus de la UTEG para la asignación de direcciones dinámicas a los host de cada subred. Funciona en el modo cliente/servidor, permite que los clientes DHCP de una red IP obtengan sus configuraciones y así elimina una carga de trabajo al administrador de Red.

En cada subred el Router con el de Servidor DHCP y administra la asignación de las direcciones y responde a las peticiones de configuración de los clientes. Los clientes alquilan la información del servidor por un periodo definido administrativamente. Cuando el periodo de alquiler se termina, el cliente debe pedir otra dirección, aunque en general, se le reasigne la misma dirección.

Se recomienda a los administradores de la red, que ofrezcan servicios DHCP porque estas soluciones facilitan el crecimiento y la administración de la Red.

8.8. Resumen de Equipamiento a utilizar

Tenemos equipos que soporta IPV6, los mismos que con tan solo cambiar la configuración soportan dicha tecnología, en lo que respecta a aplicaciones, las videoconferencias pueden realizarse por el canal de backbone debido a que tanto los equipos como el cableado soportan hasta 1 Giga de velocidad

Para los siguientes escenarios se deberán utilizar los siguientes equipos de comunicación:

8.8.1. Escenario 1: Topología Anillo

- 45 Switch 3COM Baseline 2824: el cual dará acceso a los usuarios para poder enlazarse con el Switch de Backbone.
- 14 Switch Cisco Catalyst 3560g: el que estará colocado en cada edificio para poder enlazar los 14 edificios, este switch va a ser el principal de cada edificio.

- 1 Router Cisco 1841: el switch de Backbone del edificio de informática dará salida al router que es el que va a permitir la salida al internet.

- 1 Cisco ASA 5520 Firewall Edition: es el que protege la red interna y la zona desmilitarizada de los intrusos y de los hackers.
- 9 Servidores: vamos a tener en la granja de servidores una división, para la zona desmilitarizada de los servidores de aplicación de la red.

8.8.2. Escenario 2: Topología Estrella

- 46 Switch 3COM Baseline 2824
- 14 Switch Cisco Catalyst 3560g
- 1 Router Cisco 1841
- 1 Cisco ASA 5520 Firewall Edition
- 9 Servidores
- 13 Convertidor Gigabit 1000 Base-T to SX (SC Type): Es el equipo que va a permitir la conexión de la información del cable del Backbone de Fibra optica al Switch de Backbone Principal de salida ethernet.

Y sin olvidarnos de los agregados para los 2 escenarios:

- 13 Rack: Se utilizaran 13 Racks 1 por cada edificio.
- 1 Gabinete: 1 en la facultad de informática el que va a ser el cuarto central de toda la red.

Los equipos que vamos a necesitar para la VoIP serán:

- 1 Equipo FXO de 1WAN, LAN, 16 FXO: Sirve para la entrada de las líneas telefónicas a la central.
- 89 Linksys Sipura 841, 1LAN, 2 Users SIP, LCD: teléfonos para los puntos de voz.
- 1 IPPBX Server: Servidor de VoIP

Las especificaciones técnicas de todos los equipos mencionados se encuentran en los anexos.

8.9. Certificaciones y pruebas

Las certificaciones del cableado tanto de cobre como de fibra se lo debe realizar cuando este implementado, para que dichas certificaciones sean validas nos regimos a los estándares establecidos para realizar un correcto cableado estructurado y un anillo de fibra que este bajo las normas establecidas.

De esta manera podremos sacar el respectivo informe de los antecedentes para la instalación de un cable de fibra óptica multimodo de 6 hilos del cuarto de telecomunicaciones de un edificio a otro de tal manera que quede formado un anillo de fibra entre los 14 edificios del nuevo campus de la Universidad.

En dicho informe constaran los trabajos realizados, esto es el tendido y cable de fibra óptica multimodo de 6 hilos indicando el punto de partida y el punto de llegada a los respectivos cuartos de telecomunicaciones.

El tipo de instalación del ODF que se realizo de cuantos puertos y el tipo si es SC (distribuidores de fibra) en ambos racks.

Las fusiones de los pigtails deben ser multimodo de tipos SC en los ODF de acuerdo al tipo de instalación del ODF.

De tal manera queda constancia que el proyecto del enlace de fibra óptica para el nuevo Campus de la Universidad incluye el suministro, montaje y certificación del enlace de fibra óptica entre los 14 edificios, trabajos que se han realizado cumpliendo con todas las normas y los estándares internacionales que para cableado de Telecomunicaciones que existen de acuerdo con las regulaciones y controles de la EIA/TIA, involucrados en este tipo de proyectos.

Los equipos pasivos instalados en el rack de Telecomunicaciones corresponden a:

- Gabinete ODF de 12 puertos tipo SC
- Etiquetamiento y Certificación
- Plano

8.9.1. Estándares para la red alámbrica

Las normas y estándares cubiertos son:
ANSI/EIA/TIA 568-A: Estándar para el cableado horizontal y vertical de Telecomunicaciones para edificios comerciales.

ANSI/EIA/TIA 569-A: Estándar para las rutas, espacios e instalación de ductos.

Luego se procede a hacer las lecturas con el OTDR de un punto hacia otro de tal manera que el cableado de fibra óptica quede certificado de su buen funcionamiento en el momento de transmitir la información.

8.9.2. Estándares para la red inalámbrica

Hacia 1993, los fundamentos para une estándar estaban establecidos, y en Junio de 1997, el estándar 802.11 del IEEE, que tenia mas de seis años en el proceso de creación, fue ratificado. Este primer estándar 802.11 proporcionaba velocidades de datos de 1 y 2 megabits por segundo (Mbps), esto marco el comienzo de una nueva era y estableció los fundamentos para el siguiente estándar, 802.11b, que fue ratificado en 1999 y ofrece una velocidad de datos de 11 Mbps, aproximadamente la misma velocidad que el estándar Ethernet.

Comparación de las especificaciones 802.11b, 802.11g y 802.11a			
Características	**802.11b**	**802.11g**	**802.11a**
Frecuencia	2.4 GHz	2.4 GHz	5.7 GHz
Velocidad de datos	11 Mbps	54 Mbps	54 Mbps

Tabla 8.5. Estándares red Inalámbrica

8.9.3. Cableado Estructurado

Para el cableado estructurado se decidió utilizar cable utp cat 6 debido a que tiene más ventajas en la actualidad que el cat 5e. El cable utp cat 6 tiene una cruceta para la separación de los pares y las trenzas entre cables son mas continuas esto es que la información va a llegar a su destino de tal manera que no este distorsionada o que allá perdida de información el cable de cat 5e tiene un 100% de inducción magnética en cambio por la cruceta del cat 6 se elimina un 50 % de inducción magnética.

Actualmente existe una gran cantidad de proveedores que ofrecen productos acordes con la Categoría 6, pero hasta ahora, dicha categoría no había sido oficialmente aprobada como estándar internacional.

Con este anuncio se da un gran paso hacia grandes mejoras en el desempeño de la información.

Diferencias con la Categoría 5

Bajo el código de TIA/EIA-568-B.2-1, la nueva categoría aprobada permitirá duplicar el ancho de banda existente con la categoría anterior (5e) y alcanzar rangos de transmisión de información de 250 MGz, lo que se traduce en mayor velocidad en las comunicaciones y la posibilidad de optimizar el manejo de voz, datos y video.

Para la aprobación la TIA, máximo estamento de estándares de tecnología para Telecomunicaciones, estudio detalladamente las posibilidades e implicaciones de la Categoría 6 y después de más de 5 años de investigación decidió hacer el anunció por considerarlo un hecho memorable en la historia comercial del cableado, según lo afirmó Bob Jensen Director del comité de estándares de la TIA.

La nueva categoría traerá:

- **Mayor velocidad**
  Al duplicar el ancho de banda existente actualmente, la nueva categoría permitirá mejorar los tiempos de transmisión a velocidades nunca antes vistas.

- **Ampliación de posibilidades**
  Las empresas podrán enfrentarse a mayores posibilidades de transmisión de información y de esta forma estar más acordes a los nuevos estándares de trabajo que requieren mayor riqueza en imágenes y video.

- **Compatibilidad**
  Los usuarios de categorías anteriores como la 3,5 o la 5e no tendrán que cambiar completamente su infraestructura ya que la Categoría 6 permite soportar completamente tecnologías anteriores. Sin embargo, para lograr un resultado final acople con las ventajas de la categoría 6 se recomienda que todos los componentes trabajen bajo esta misma categoría.

- **Durabilidad**
  La Categoría 6 fue diseñada en principio para que sus componentes soporten los requerimientos tecnológicos de los próximos años. Se espera que su tiempo de vida útil supere los 15 años.

Acerca de BICSI (Buildings industries Consulting Services, Internacional)

Con más de 20.000 miembros alrededor del mundo, BICSI es la asociación profesional de ingenieros, diseñadores e instaladores de distribución de telecomunicaciones más ampliamente reconocida. Actuando en 85 países, BICSI ayuda los profesionales en el avance de sus carreras proporcionándoles entrenamiento sin vínculos con proveedores, publicaciones y calificaciones en el diseño de tecnologías para voz, datos y video. Fundada en 1974, BICSI es una asociación sin fines de lucro. Su sede central está en los estados Unidos y cuenta, actualmente, con filiales en el Reino Unido, Australia, Brasil y Japón.

8.9.4. Fibra (OTDR) Principales reportes que ofrece técnicamente

El OTDR permite certificar que los hilos de la fibra pueden transmitir la información de un punto a otro de tal manera que no van a existir perdida de paquetes ni intromisión de personas que quieran sabotear la conexión.
Hay cuatro fases en la prueba del cable de fibra óptica:

1) Inspección visual para detectar daños durante el envío
2) Prueba de preinstalación, que ocurre inmediatamente después de la entrega de los cables
3) Prueba de instalación, que ocurre después de colocar el cable y en cada punto de empalme.
4) Prueba de aceptación final, que ocurre inmediatamente antes de la activación.

Prueba de preinstalación

La prueba de preinstalación por lo general consiste de una prueba de Reflectómetro óptico en el dominio de tiempo (OTDR) realizada a 1550 nanometros. Todos los cables de fibra óptica pasan por la prueba OTDR antes de su envío y el informe de la prueba se adjunta. Una prueba de preinstalación verificará las características del cable y comprobará si hay daños de envío.

El operador del sistema y el grupo de construcción pueden llevar a cabo las pruebas al mismo tiempo para anticipar dificultades futuras si un cable se dañara durante la construcción.

Prueba de instalación

El cable debería probarse después de haberse colocado en la planta y antes del empalme para asegurarse que no se hayan producido daños de instalación. La prueba de instalación por lo general se hace con un reflectómetro óptico en el dominio tiempo (OTDR).

La prueba de empalme se lleva a cabo después de cada empalme para asegurarse de haber hecho una conexión nítida y de baja pérdida.

En el OTDR, la detección de inyección local y la alineación de configuración se pueden usar solas o en combinación para la prueba de empalme.

Postinstalación - Prueba de aceptación final

El método de prueba de postinstalación normal es realizar una prueba de reflectómetro (OTDR) de punta a punta. Los resultados deberían compararse con la prueba de preinstalación. Se recomienda seriamente establecer un programa de prueba continua después de haberse activado el sistema.

Prueba de atenuación con un OTDR

La prueba de atenuación con un Reflectómetro óptico en el dominio tiempo (OTDR) debería realizarse como parte de cualquier régimen de prueba de preinstalación. Todas las fibras en un cable deben probarse y deben registrarse y documentarse los resultados.

La atenuación se define como la pérdida en potencia óptica a medida que viaja a través del cable de fibra óptica y normalmente se expresa en decibeles por 1,000 metros (dB/km). Otras pruebas generales de atenuación incluyen la aceptación de cables, verificación de pérdida de empalme y mediciones finales de punta a punta. Deben realizarse trazados de firma de todas las fibras después del empalme y la conectorización para mostrar la ruta completa del cable.

Estos trazados serán invaluables en caso de ocurrir problemas en la planta de cables pasiva. Los OTDR tienen varias ventajas considerables en comparación con otros métodos de prueba, son instrumentos extremadamente versátiles que pueden ser operados por un solo técnico. A través de comparaciones periódicas con los trazados de firma iniciales, los OTDR pueden

enviar advertencias tempranas de una falla catastrófica potencial al indicar puntos de estrés en el cable.

El OTDR opera mediante la transmisión de un pulso óptico a través de la fibra.

La pérdida de señal se mide al graficar las reflexiones de un pulso de luz a medida que se retrodispersa por la estructura de vidrio o se refleja más definidamente debido a una falla o rotura en la fibra o en el extremo del cable mismo. La distancia a la falla se mide por el tiempo transcurrido entre el momento de originarse el pulso y la llegada de la luz retroreflejada en el OTDR.

El resultado (un trazado lineal de la fibra indicado como la distancia desde el origen [eje horizontal] comparado con la potencia relativa [eje vertical]) se visualiza en una pantalla o se imprime.

La documentación es esencial en la planta de fibra óptica. Mientras que una instalación coaxial se encarga de un solo conductor a lo largo de una distancia, una instalación de cables de fibra óptica tiene que ver con fibras múltiples en un cable que puede ser considerablemente más largo.

Si un cable se daña durante la instalación y esto no se detecta mediante una prueba de campo continua, los costos de reemplazo pueden ser extremadamente altos.

CAPITULO 9: ANÁLISIS ECONOMICO

Una vez observado en el capitulo anterior las características al detalle de los componentes de la red y los equipos que se van a utilizar, se procede a revisar las cotizaciones de lo que se necesita para evaluar los costos y que tan factible resultara este tipo de red en el nuevo campus. Sin embargo se tomo en cuenta un segundo escenario para poder realizar de una mejor manera la explicación de la elección de la topología que se tomo para este proyecto.

9.1. Costo promedio por punto de Datos para escenarios

El edificio de la facultad de Tecnología de la Información es el que se va a utilizar como edificio principal, es donde van a estar los equipos de conexión y los servidores principales.
Se toma en consideración de las cotizaciones de los proveedores; los precios unitarios de los equipos y accesorios de comunicación que se van a utilizar para cada punto de datos.

COTIZACION POR PUNTO DE DATOS

ITEMS	ACCESORIOS	PRECIO UNITARIO	COTIZACION TIPO POR PUNTO	UNIDADES DE MEDIDA	TOTAL DOLARES
1	CABLE UTP 4 PARES CAT6 MARCA QUEST METROS	$ 0.84	30	METROS	$ 25.20
2	CONECTORES RJ-45 MARCA QUEST (FUNDA 100 UND)	$ 30.00	2/100	UNIDAD	$ 0.60
3	CAJAS SOBREPUESTAS 40MM MARCA DEXSON	$ 1.47	1	UNIDAD	$ 1.47
4	FACE PLATE 2P CON I.D. MARCA QUEST	$ 1.44	1/2	UNIDAD	$ 0.72
5	JACK CAT6 MARCA QUEST	$ 5.75	1	UNIDAD	$ 5.75
6	PATCH CORD 3FT CAT6 MARCA QUEST	$ 4.41	1	UNIDAD	$ 4.41
7	PATCH CORD 7FT CAT6 MARCA QUEST	$ 6.60	1	UNIDAD	$ 6.60
8	PATCH PANEL 24P SOLIDO CAT6 MARCA QUEST	$ 177.00	1/24	UNIDAD	$ 7.38
9	ORGANIZADOR HORIZONTAL 60X40 1UR MARCA BEAUCOUP	$ 10.14	1/24	UNIDAD	$ 0.42
10	ORGANIZADOR VERTICAL 84" 80X80MM MARCA BEAUOCUP	$ 39.56	1/76	UNIDAD	$ 0.52
11	CANALETA 40X25 MARCA DEXSON	$ 4.55	3	UNIDADES	$ 13.65
12	ACCESORIOS PARA CANALETA 20X12 MARCA DEXSON	$ 0.28	1	UNIDAD	$ 0.28
13	ETIQUETADO	$ 0.05	1	UNIDAD	$ 0.05
			VALOR TOTAL		$ 67.05

PROMEDIO PUNTO	$ 80.46
MANO DE OBRA	$ 15.00
VALOR TOTAL POR PUNTO DE DATOS	$ 95.46
TOTAL DE PUNTOS	1,096
TOTAL CABLEADO	$104,621.56

Tabla 9.1. Cotización por Punto

Nota: Cotización de Referencia de Punto de Red (VER ANEXO 19)

Para poder asignar cada punto para voz y datos se analizaron las necesidades de los usuarios, de acuerdo a la amplitud de cada espacio según las medidas en los planos arquitectónicos de la Universidad.

De esta manera se determino para poder seguir con el análisis del cableado estructurado que son 1096 puntos de datos que se podrían colocar en la infraestructura, se tiene un estimado de $ 95.46 dólares por punto, lo cual en todo el cableado estructurado incluyendo los accesorios y canaletas da un costo de $ 104,621.56 dólares entre los 12 edificios, cabe recalcar que los edificios que hemos estudiado son 12 debido a que **no** nos proporcionaron los planos del edificio de seguridad y educación a distancia, sin embargo son 14 los edificios que se encuentran en el plano arquitectónico general del nuevo campus.

9.2. Costo de la Central Telefónica para la Red de Voz

Para la central telefónica vamos a poner 16 entradas de líneas telefónicas debido a la cantidad de usuarios estos están estimados en 89, las mismas que estarán diseccionadas al numero principal del PBX. Dicha central tendrá un Software Asterisk a continuación se detallan los costos:

CENTRAL TELEFONICA				
Items	**Cantidad**	**Descripcion**	**Precio Un.**	**Total**
1	1	1 WAN, 1 LAN, 16 FXO	$ 1,471.00	$ 1,471.00
2	89	1LAN, 2 USERS IP, LCD (Linksys Sipura 841)	$ 100.00	$ 8,900.00
3	1	IP PBX Server	$ 2,500.00	$ 2,500.00
4	1	Instalación de Central Telefónica	$ 1,000.00	$ 1,000.00
TOTAL				$ 13,871.00

Tabla 9.2. Central Telefónica

Nota: Cotización referente para la central telefónica (VER ANEXO 16)

9.3. Costo de los Racks para los equipos de telecomunicación

Este Activo es donde estarán almacenados los equipos de telecomunicaciones del campus, se han elegido 13 racks de piso abiertos ya que cada nodo tiene un cuarto y el mismo debe estar cerrado, por su tamaño ese escogió este tipo de rack, sin embargo para el de la Facultad de Informática ya que es donde va a estar la central de equipos y debe estar mas protegido se pondrá un Gabinete el mismo que tiene una cerradura.

RACKS				
Items	**Cantidad**	**Descripcion**	**Precio Un.**	**Total**
3	13	Rack d Piso 72" (36 UR) Tuerca Remachada marca BEAUCOUP	$ 163.00	$ 2,119.00
4	1	Gabinete de Piso 72" 180x604x754 MM marca BEAUCOUP	$ 649.00	$ 649.00
TOTAL				$ 2,768.00

Tabla 9.3. Racks

9.4. Costo de los UPS

Para cada Switch de Backbone que conecta el anillo vamos a utilizar UPS como una medida de seguridad para evitar perdida de información en el anillo de Fibra cuando se este transmitiendo la información. Va a haber un UPS de capacidad mayor para el edificio Principal en donde va a haber los enlaces para la salida a la Red WAN y 13 UPS con menos capacidad de voltaje que el primero para el resto de Switch de Backbone por cada edificio.

UPS				
Items	**Cantidad**	**Descripcion**	**Precio Un.**	**Total**
1	1	UPS POWERWARE modelo 9120 capacidad 3KVA tecnología ON LINE	$ 1,345.00	$ 1,345.00
2	1	Configuracion para 3 horas de Respaldo con Gabinete	$ 2,278.13	$ 2,278.13
3	13	UPS POWERWARE modelo 9120 capacidad 700 va tecnología ON LINE	$ 525.00	$ 6,825.00
4	13	Configurado con 1 hora de Respaldo con Gabinete	$ 550.53	$ 7,156.89
TOTAL				$ 17,605.02

Tabla 9.4. UPS

Nota: Cotizaciones referentes para UPS (VER ANEXO 22)

9.5. Escenario 1: Topología Anillo para backbone de Fibra Optica

9.5.1. Costo por enlace entre edificios para la topología Anillo

Los costos para realizar el enlace son:

ENLACE POR CADA EDIFICIO EN TOPOLOGIA ANILLO					
Items	**Cantidad**	**Unidades**	**Descripción**	**Precio Unitario**	**Precio total**
1	1	u	Patch panel para Fibra Óptica, Siemon (ODF) de 12 puertos	$ 130.00	$ 130.00
2	2	u	Placa adaptadora de 6 puertos SC	$ 45.00	$ 90.00
3	1	u	Placa ciega para patch panel de F.O.	$ 15.00	$ 15.00
4	12	u	Pigtails SC, Multimodo 62.5/125 um	$ 20.00	$ 240.00
5	4	u	Patch cord de F.O.Multimodo 62.5/125 um SC/SC, 3 m.	$ 40.00	$ 160.00
6	12	u	Fusiones de hilos de fibra óptica (mano de obra)	$ 25.00	$ 300.00
7	12	u	mediciones OTDR	$ 20.00	$ 240.00
TOTAL					$ 1,175.00

Tabla 9.5. Enlace en Topología Anillo por cada Edificio

Nota: No incluye obra civil, todos los edificios tienen tubería subterránea para unirse. Cotización referente para enlace de Fibra Óptica (VER ANEXO 20)

9.5.2. Costo del anillo de fibra óptica sin equipos

Para enlazar los edificios del campus se decidió hacerlo por medio de un anillo de fibra óptica en el primer escenario, se tiene 1081,60 metros para el anillo de fibra sin embargo se va a considerar un 20% de margen de error por si se presenta algún inconveniente por algún daño en el cable, entonces se va a trabajar con 1300 metros de fibra óptica multimodo de 62.5 mm. de diámetro de núcleo y 125 mm. de cubierta de 6 hilos de índice escalonado, tipo ducto debido a que el cableado va a ser subterráneo ya que la Universidad aun no esta construida y se puede incluir en la obra civil los ductos.

Los 1300 metros de fibra óptica multimodo con el tendido del cable de fibra y el costo de terminación de la fibra por edificio nos da el costo del anillo sin los equipos como podemos observar en el siguiente cuadro:

COSTO DEL ANILLO DE FIBRA OPTICA SIN EQUIPOS					
Items	**Cantidad**	**Unidad**	**Descripción**	**Precio Un.**	**Precio total**
1	1300	m	Metros de F.O. Multimodo 62.5/125 um, de 6 hilos, Tipo ducto	$ 3.65	$ 4,745.00
2	1300	m	Tendido de Fibra	$ 0.60	$ 780.00
3	14	u	Costo de terminacion de fibra por edificio	$ 1,175.00	$ 16,450.00
total					$ 21,975.00

Tabla 9.6. Costo Anillo de Fibra Óptica

Se tomo en consideración el backup del anillo de Fibra en caso extremo que se de mas de un corte de enlace en la comunicación, de tal manera que lo único que se tendría que hacer es cambiar el cable del anillo principal con el anillo backup. Se efectuó el costo del anillo backup tomando en consideración las mediciones del OTDR para que el backup tenga un correcto funcionamiento como se puede observar en el siguiente cuadro:

BACKUP COSTO DEL ANILLO DE FIBRA OPTICA SIN EQUIPOS					
Items	**Cantidad**	**Unidad**	**Descripción**	**Precio Un.**	**Precio total**
1	1300	m	Metros de F.O. Multimodo 62.5/125 um, de 6 hilos, Tipo ducto	$ 3.65	$ 4,745.00
2	1300	m	Tendido de Fibra	$ 0.60	$ 780.00
3	14	u	mediciones OTDR	$ 20.00	$ 280.00
total					$ 5,805.00

Tabla 9.7. Costo Backup Anillo de Fibra Óptica

Nota: Cotización referente para enlace de Fibra Óptica (VER ANEXO 20).

9.5.3 Costo de los equipos de telecomunicación a utilizar en el nuevo campus en la topología Anillo.

En el cuadro a continuación se puede observar el valor total en equipos para el anillo de fibra:

EQUIPOS EN TOPOLOGIA ANILLO DE FIBRA OPTICA				
Items	**Cantidad**	**Descripcion**	**Precio Un.**	**Total**
1	14	Switch de fibra Cisco Catalist 3560g-24PS puertos	$ 4,372.50	$ 61,215.00
2	45	Switch 3COM de acceso	$ 450.00	$ 20,250.00
3	1	Router de Servicios Integrados Cisco 1841	$ 1,547.00	$ 1,547.00
4	2	Tarjeta HWIC- 4 ESW	$ 472.00	$ 944.00
5	7	Acces Point AT-WA7400 Allied Telesis	$ 349.00	$ 2,443.00
6	1	Cisco ASA 5520 Firewall Edition	$ 6,441.36	$ 6,441.36
7	1	Servidor DHCP Linux	$ 1,000.00	$ 1,000.00
TOTAL				$ 93,840.36

Tabla 9.8. Equipos en Topología Anillo

Nota: Cotización referente para los equipos (VER ANEXOS)

9.5.4. Costo total del proyecto en topología Anillo

Con todos los datos indicados anteriormente con esta topología el proyecto esta costeado alrededor de $ 260,485.94; en el que esta incluido el anillo de fibra con sus respectivos equipos, la central telefónica de VoIP y el cableado estructurado con sus respectivos accesorios, canaletas y equipos de enlace.

COSTO TOTAL DEL PROYECTO EN TOPOLOGIA ANILLO DE FIBRA OPTICA		
Items	**Equipos**	**Valor**
1	Backbone de fibra	$ 21,975.00
2	Equipos de Comunicación	$ 93,840.36
3	Cableado Estructurado	$ 104,621.56
4	Racks	$ 2,768.00
5	Central Telefonica	$ 13,871.00
6	UPS	$ 17,605.02
7	Backup de Backbone	$ 5,805.00
TOTAL		$ 260,485.94

Tabla 9.9. Costo Total del Proyecto Topología Anillo

9.6. Escenario 2: Topología Estrella para Backbone de Fibra Optica

9.6.1. Costo por enlace entre edificios en topología Estrella

Los costos para realizar el enlace de fibra en topología estrella son:

ENLACE POR CADA EDIFICIO EN TOPOLOGIA ESTRELLA					
Items	**Cantidad**	**Unidades**	**Descripción**	**Precio Unitario**	**Precio total**
1	1	u	Patch panel para Fibra Óptica, Siemon (ODF) de 12 puertos	$ 130.00	$ 130.00
2	2	u	Placa adaptadora de 6 puertos SC	$ 45.00	$ 90.00
3	1	u	Placa ciega para patch panel de F.O.	$ 15.00	$ 15.00
4	12	u	Pigtails SC, Multimodo 62.5/125 um	$ 20.00	$ 240.00
5	4	u	Patch cord de F.O.Multimodo 62.5/125 um SC/SC, 3 m.	$ 40.00	$ 160.00
6	12	u	Fusiones de hilos de fibra óptica (mano de obra)	$ 25.00	$ 300.00
7	12	u	mediciones OTDR	$ 20.00	$ 240.00
8	12	u	Conectores SC Multimodo	$ 6.00	$ 72.00
9	12	u	Conectorizaciones de hilos de fibra óptica	$ 25.00	$ 300.00
10	1	u	Patch Cord 7FT CAT6 Marca QUEST	$ 5.28	$ 5.28
TOTAL					$ 1,552.28

Tabla 9.10. Enlace en Topología Estrella por cada Edificio

Nota: No incluye obra civil, todos los edificios tienen tubería subterránea para unirse. Cotización referente para enlace de Fibra Óptica (VER ANEXO 20)

9.6.2. Costo de la estrella de fibra óptica sin equipos

Para enlazar los edificios del campus se decidió hacerlo por medio de una topología estrella de fibra óptica, se tiene 1366,88 metros para el anillo de fibra sin embargo se va a considerar un 20% de margen de error por si se presenta algún inconveniente por algún daño en el cable, entonces se va a trabajar con 1700 metros de fibra óptica multimodo de 62.5 mm. de diámetro de núcleo y 125 mm. de cubierta de 6 hilos de índice escalonado, tipo ducto debido a que el cableado va a ser subterráneo ya que la Universidad aun no esta construida y se puede incluir en la obra civil los ductos.

Los 1700 metros de fibra óptica multimodo con el tendido del cable de fibra y el costo de terminación de la fibra por edificio nos da el costo de la estrella sin los equipos como podemos observar en el siguiente cuadro:

COSTO DE LA ESTRELLA DE FIBRA OPTICA SIN EQUIPOS					
Items	**Cantidad**	**Unidad**	**Descripción**	**Precio Un.**	**Precio total**
1	1700	m	Metros de F.O. Multimodo 62.5/125 um, de 6 hilos, Tipo ducto	$ 3.65	$ 6,205.00
2	1700	m	Tendido de Fibra	$ 0.60	$ 1,020.00
3	14	u	Costo de terminacion de fibra por edificio	$ 1,552.28	$ 21,731.92
total					$ 28,956.92

Tabla 9.11. Costo Estrella de Fibra Óptica

Se tomo en consideración el backup de estrella de Fibra en caso extremo que se de mas de un corte de enlace en la comunicación, de tal manera que lo único que se tendría que hacer es cambiar el cable de al estrella principal con la estrella backup. Se efectuó el costo de la estrella backup tomando en consideración las mediciones del OTDR para que el backup tenga un correcto funcionamiento como se puede observar en el siguiente cuadro:

BACKUP COSTO DE ESTRELLA DE FIBRA OPTICA SIN EQUIPOS					
Items	**Cantidad**	**Unidad**	**Descripción**	**Precio Un.**	**Precio total**
1	1700	m	Metros de F.O. Multimodo 62.5/125 um, de 6 hilos, Tipo ducto	$ 3.65	$ 6,205.00
2	1700	m	Tendido de Fibra	$ 0.60	$ 1,020.00
3	14	u	mediciones OTDR	$ 20.00	$ 280.00
total					$ 7,505.00

Tabla 9.12. Costo Backup Estrella de Fibra Óptica

Nota: Cotización referente para enlace de Fibra Óptica (VER ANEXO 20).

9.6.3. Costo de los equipos de telecomunicación a utilizar en el nuevo campus con topología Estrella.

En el cuadro a continuación se puede observar el valor total en equipos para la estrella de fibra:

EQUIPOS EN TOPOLOGIA ESTRELLA DE FIBRA OPTICA				
Items	**Cantidad**	**Descripcion**	**Precio Un.**	**Total**
1	14	Switch de fibra Cisco Catalist 3560g-24PS puertos	$ 4,372.50	$ 61,215.00
2	46	Switch 3COM de acceso	$ 450.00	$ 20,700.00
3	1	Router de Servicios Integrados Cisco 1841	$ 1,547.00	$ 1,547.00
4	2	Tarjeta HWIC- 4 ESW	$ 472.00	$ 944.00
5	7	Acces Point AT-WA7400 Allied Telesis	$ 349.00	$ 2,443.00
6	1	Cisco ASA 5520 Firewall Edition	$ 6,441.36	$ 6,441.36
7	1	Servidor DHCP Linux	$ 1,000.00	$ 1,000.00
8	13	Convertidor Gigabit 1000 Base-T to SX (SC Type)	$ 250.00	$ 3,250.00
TOTAL				$ 97,540.36

Tabla 9.13. Equipos en Topología Estrella

Nota: Cotización referente para los equipos (VER ANEXOS)

9.6.4. Costo total del proyecto en Topología Estrella

Con todos los datos indicados anteriormente el proyecto en topología estrella esta costeado alrededor de $ 272,867.86; en el que esta incluido la estrella de fibra con sus respectivos equipos, la central telefónica de VoIP y el cableado estructurado con sus respectivos accesorios, canaletas y equipos de enlace.

COSTO TOTAL DEL PROYECTO EN TOPOLOGIA ESTRELLA DE FIBRA OPTICA		
Items	**Equipos**	**Valor**
1	Backbone de fibra	$ 28,956.92
2	Equipos de Comunicación	$ 97,540.36
3	Cableado Estructurado	$ 104,621.56
4	Racks	$ 2,768.00
5	Central Telefonica	$ 13,871.00
6	UPS	$ 17,605.02
7	Backup de Backbone	$ 7,505.00
TOTAL		$ 272,867.86

Tabla 9.14. Costo Total del Proyecto en Topología Estrella

9.7. Topología Anillo Vs. Topología Estrella

Una vez culminado los 2 escenarios con sus respectivos Costos se puede apreciar la diferencia en cuanto al Costo total del anillo de fibra Optica contra el Costo Total de la estrella de fibra Optica, para un mejor entendimiento se va a realizar una comparación de los 2 escenarios propuestos.

	TOPOLOGIA ANILLO	TOPOLOGIA ESTRELLA	DIFERENCIA
COSTO TOTAL DE LOS EQUIPOS	$88,599.00	$92,299.00	Mas costo debido a los 13 Convertidores Gigabit 1000 Base-T to SX (SC Type)
COSTO TOTAL DEL ENLACE	$1,175.00	$1,552.28	Mas costo debido a los 13 Conectores SC Multimodo y las 13 Conectorizaciones de hilos de fibra optica
BACKBONE DE FIBRA OPTICA	$21,975.00	$28,956.92	Mas costo debido a los 400 Metros mas de F.O. Multimodo 62.5/125 um, de 6 hilos, Tipo ducto y en el tendido de Fibra en comparacion a la Topologia Anillo
COSTO TOTAL	$255,244.58	$267,626.50	$12,381.92

Tabla 9.15. Inversiones de Activos Fijos

El proyecto es una inversión en Activo Fijo, si es a más de un año plazo, será una inversión en Activo Fijo a largo plazo

El Rendimiento no es palpable monetariamente pero es medible en cuanto a la eficiencia y productividad. En este caso se busca el beneficio que se tiene con la implementación de esta red en el aspecto académico.

Cuando se genera una inversión de este tipo se necesita saber que tipo de mantenimiento en sus equipos y accesorios para la red informática se va dar.
Hay dos tipos de mantenimiento:

1. Preventivo
2. Correctivo

El mantenimiento preventivo es el que le da el departamento de Sistemas de la Universidad.

El mantenimiento Correctivo que se encarga la empresa que garantizo la mano de obra. Este mantenimiento se basa en los siguientes estándares:

- Garantía de materiales por un año
- Garantía de mano de obra por 3 años

En este proyecto no hay costos por mantenimiento porque se va a manejar bajo estos parámetros porque están las garantías.

CAPITULO 10: EVALUACIÓN INTEGRAL DEL PROYECTO

La evaluación del financiamiento del proyecto, se hará de acuerdo a las necesidades de inversión del mismo, si la universidad tuviera el capital para levantar dicha red se tendrá una inversión de contado, de lo contrario se solicitaría un préstamo a una institución financiera y se obtendría una inversión con financiamiento, o se podría plantear hacer un aumento de capital a los accionistas de la Universidad.

10.1. Evaluación de contado

La evaluación de contado se da presentando un informe de los costos de los equipos y suministros a utilizar en el proyecto, de tal modo que sea evaluado por el departamento financiero de la Universidad y el mismo pueda determinar si se debe invertir el costo total del proyecto en un solo desembolso de dinero (de contado).

10.2. Evaluación con financiamiento

La evaluación con financiamiento se plantea al momento de que no se cuente con el capital necesario para levantar el proyecto, la persona encargada de la parte económica acudirá a una o varias entidades financieras, para solicitar un préstamo para analizar la capacidad de poder adquisitivo y que propuesta le conviene mas a la Universidad si esta en capacidad de cubrir la deuda.

10.2.1. Tabla de Amortización

Se tomo de la página del banco central del Ecuador, las tasas de interés del mercado en la actualidad de acuerdo al tipo de préstamo.

En los Anexos 23 y 24 respectivamente, se detalla por entidad las tasas nominales promedio ponderadas, por plazos y por línea de negocio (comercial, consumo, microcrédito y vivienda) de los principales sistemas controlados.

MONTO	275,000.00
PLAZO AÑOS	4.00
PAGOS	12.00
TASA	15%
PAGOS	-$7,653.46

DIVIDENDOS	CAPITAL	INTERES	PAGO	SLDO. CAPITAL
0				275,000.00
1	-$4,215.96	-$3,437.50	-$7,653.46	$270,784.04
2	-$4,268.66	-$3,384.80	-$7,653.46	$266,515.39
3	-$4,322.01	-$3,331.44	-$7,653.46	$262,193.38
	-$12,806.62	-$10,153.74	-$22,960.37	
4	-$4,376.04	-$3,277.42	-$7,653.46	$257,817.34
5	-$4,430.74	-$3,222.72	-$7,653.46	$253,386.60
6	-$4,486.12	-$3,167.33	-$7,653.46	$248,900.47
	-$13,292.90	-$9,667.47	-$22,960.37	
7	-$4,542.20	-$3,111.26	-$7,653.46	$244,358.27
8	-$4,598.98	-$3,054.48	-$7,653.46	$239,759.30
9	-$4,656.46	-$2,996.99	-$7,653.46	$235,102.83
	-$13,797.64	-$9,162.73	-$22,960.37	
10	-$4,714.67	-$2,938.79	-$7,653.46	$230,388.16
11	-$4,773.60	-$2,879.85	-$7,653.46	$225,614.56
12	-$4,833.27	-$2,820.18	-$7,653.46	$220,781.29
	-$14,321.55	-$8,638.82	-$22,960.37	
	-$54,218.71	-$37,622.75	-$91,841.47	
13	-$4,893.69	-$2,759.77	-$7,653.46	$215,887.60
14	-$4,954.86	-$2,698.59	-$7,653.46	$210,932.73
15	-$5,016.80	-$2,636.66	-$7,653.46	$205,915.94
16	-$5,079.51	-$2,573.95	-$7,653.46	$200,836.43
17	-$5,143.00	-$2,510.46	-$7,653.46	$195,693.43
18	-$5,207.29	-$2,446.17	-$7,653.46	$190,486.14
19	-$5,272.38	-$2,381.08	-$7,653.46	$185,213.76
20	-$5,338.28	-$2,315.17	-$7,653.46	$179,875.48
21	-$5,405.01	-$2,248.44	-$7,653.46	$174,470.47
22	-$5,472.57	-$2,180.88	-$7,653.46	$168,997.89
23	-$5,540.98	-$2,112.47	-$7,653.46	$163,456.91
24	-$5,610.24	-$2,043.21	-$7,653.46	$157,846.67
	-$62,934.62	-$28,906.85	-$91,841.47	
25	-$5,680.37	-$1,973.08	-$7,653.46	$152,166.29
26	-$5,751.38	-$1,902.08	-$7,653.46	$146,414.92
27	-$5,823.27	-$1,830.19	-$7,653.46	$140,591.65
28	-$5,896.06	-$1,757.40	-$7,653.46	$134,695.59
29	-$5,969.76	-$1,683.69	-$7,653.46	$128,725.83
30	-$6,044.38	-$1,609.07	-$7,653.46	$122,681.44
31	-$6,119.94	-$1,533.52	-$7,653.46	$116,561.51
32	-$6,196.44	-$1,457.02	-$7,653.46	$110,365.07
33	-$6,273.89	-$1,379.56	-$7,653.46	$104,091.18
34	-$6,352.32	-$1,301.14	-$7,653.46	$97,738.86
35	-$6,431.72	-$1,221.74	-$7,653.46	$91,307.14
36	-$6,512.12	-$1,141.34	-$7,653.46	$84,795.02
	-$73,051.64	-$18,789.83	-$91,841.47	
37	-$6,593.52	-$1,059.94	-$7,653.46	$78,201.51
38	-$6,675.94	-$977.52	-$7,653.46	$71,525.57
39	-$6,759.39	-$894.07	-$7,653.46	$64,766.18
40	-$6,843.88	-$809.58	-$7,653.46	$57,922.30
41	-$6,929.43	-$724.03	-$7,653.46	$50,992.88
42	-$7,016.04	-$637.41	-$7,653.46	$43,976.83
43	-$7,103.75	-$549.71	-$7,653.46	$36,873.09
44	-$7,192.54	-$460.91	-$7,653.46	$29,680.55
45	-$7,282.45	-$371.01	-$7,653.46	$22,398.10
46	-$7,373.48	-$279.98	-$7,653.46	$15,024.62
47	-$7,465.65	-$187.81	-$7,653.46	$7,558.97
48	-$7,558.97	-$94.49	-$7,653.46	-$0.00
	-$84,795.02	-$7,046.45	-$91,841.47	

Tabla 10.1 Tabla de Amortización

De acuerdo a las tasas del mercado actual y acuerdo al tipo de préstamo, se asume que debido a que el costo del proyecto es elevado se tomo la opción de que los pagos se los realice a mas de 360 días por lo tanto el porcentaje de interés del préstamo que se haría se lo tomo con el 15 % ya que la tasa mas alta del mercado para préstamo de este tipo no asciende de dicho porcentaje.

Entonces el pago que realizaría seria en un periodo de 10 años según la tabla de amortización que se presento anteriormente.

RECOMENDACIONES

- De acuerdo al estudio se recomienda la implementación del diseño de la UTEG basado en el anillo de fibra Óptico propuesto.

- Se recomienda la implementación de las direcciones IPs basados en un servidor DHCP para facilitar la administración del direccionamiento de las IPs.

- Prever mantenimiento periódico Preventivo y Correctivo de los equipos de Comunicación y de los enlaces.

CONCLUSIONES

- Se presento un diseño de la infraestructura de la red informática para el nuevo campus de la Universidad, incluida la red de voz y datos.

- Se determinaron los costos de implementación del diseño de red y del escenario propuesto con el respectivo análisis de crecimiento.

- Se realizó un estudio de factibilidad y el respectivo análisis de los recursos tecnológicos para el diseño de la red informática para la disminución de gastos innecesarios en su posterior implementación.

- De acuerdo al análisis realizado se concluyo que la elaboración del proyecto es factible.

- El proyecto da a la Universidad un valor agregado a los Alumnos y profesores de tal forma que la recuperación de lo invertido seria solventado de manera rápida, por medio de las pensiones de los estudiantes.

- En lo que respecta a la factibilidad del proyecto hemos demostrado que si se puede implementar el mismo; los costos de equipos y cableado están dentro del presupuesto considerando un 20% como margen de error o de crecimiento.

- Se realizo el diseño de la red informática tomando en consideración un modelo Jerárquico basado en tres capas.

- Se realiza el diseño de la red informática de voz y datos, por cada facultad, desde el cableado estructurado a través de las VLANS hasta la forma del enlace entre edificios por medio del backbone de fibra óptica.

- Como beneficio al diseño de esta red, se puede tomar en cuenta los puntos de datos que hay en cada aula para ejercer una materia más dinámica e interactiva.

GLOSARIO

Ancho de banda: Existen dos usos comunes para el termino ancho de banda: uno se refiere a las señales analógicas y el otro, a las señales digitales.

Ancho de banda digital.- El ancho de banda es la medición de la cantidad de información que puede fluir desde un lugar hacia otro en un periodo de tiempo determinado.

Ancho de banda analógico.- Es la diferencia entre la frecuencia mas alta y mas baja por la cual viaja una señal.

Bucles.- Un bucle en programación es una sentencia que se realiza repetidas veces

Caché.- Forma de replicación en la que la información que se adquiere durante una transacción previa se usa para procesar transacciones posteriores.

Conector RJ.- Abreviación de del conector de contacto registrado. Conectores estándar que originalmente se usaban para conectar líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para 10BaseT y otros tipos de conexiones de red. RJ-11, RJ-12 r RJ-45 son tipos muy usados de conectores RJ

Demodulación.- Operación inversa de la modulación, que consiste en separar la señal de modulación de la onda portadora.

Ethernet.- Especificación para una LAN de banda base que inventó la compañía Seros Corporation y que fue desarrollada en conjunto por Seros, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y funcionan a través de una variedad de tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares 802.3 del IEEE.

FXO: Interfaz de central externa, es el puerto que recibe la línea analógica. Es un enchufe del teléfono o aparato de fax, o el enchufe de su centralita telefónica analógica. Envía una indicación de colgado/descolgado (cierre de bucle). Como el puerto FXO está adjunto a un dispositivo, tal como un fax o teléfono, el dispositivo a menudo se denomina "dispositivo FXO".

Gbps.- Abreviación para gigabits por segundo.

GHz.- Abreviación para mil millones de ciclos por segundo.

IDC.- Contacto por desplazamiento del aislamiento(Insulation Displacement Contact)

IEEE.- Acrónimo del instituto de Ingenieros Eléctricos y Electrónicos.

Mbps.- Abreviación de megabits por segundo.

Modulación.- El Proceso mediante el cual las características de las señales eléctricas se transforman para representar información.

NIC (Network interface card).- Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

PIX .- es el acrónimo de Private Internet Exchange.
Esta sigla es utilizada por el fabricante tecnológico Cisco, para referirse a sus modelos de equipos Cortafuegos (FireWalls) completamente hardware: a diferencia de otros sistemas cortafuegos, PIX no se ejecuta en una máquina Unix, sino que incluye un sistema operativo empotrado denominado Finesse que desde espacio de usuario se asemeja más a un router que a un sistema Unix clásico.

Topología.- Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

ODF.- Bandeja de Fibra Óptica.

OFDM.- (Orthogonal Frequency Division Multiplexing), Multiplexion de división ortogonal de frecuencia

QAM.- Acrónimo de la modulación de amplitud de cuadratura. Método de modulación de señales digitales en una señal de portadora de frecuencia de radio que se relaciona con la amplitud y el código de fase. QAM es un esquema de modulación que se usa principalmente

en la dirección de flujo descendente (QAM-64, QAM-256). QAM-16 normalmente se usa más en la dirección de flujo ascendente. Los números indican la cantidad de puntos de código por símbolo. La tasa QAM o el número de puntos en la constelación QAM se puede calcular por 2 elevado a la potencia de <numero de bits/símbolo>

SNA.- Acrónimo de Arquitectura de Sistema de Red. Las arquitecturas de redes grandes, complejas y con muchas características, fueron desarrolladas en la década de los 70 por IBM. Es similar en algunos aspectos al modelo de referencia OSI, pero tienen varias diferencias. SNA esta esencialmente compuesto por 7 capas que son: Capa de Control de flujo de Datos, Capa de control de enlace de Datos, Capa de control de Trayectoria, Capa de control física, Capa de Servicios de Presentación, Capa de Servicios de Transacción y Capa de control de Transmisión.

VLAN.- (Virtual Local Area Network) Acrónimo de área de red local virtual. Un grupo de clientes que están ubicados en distintos lugares pero que se comunican entre ellos como si pertenecieran al mismo segmento LAN.

WECA. - Wíreles Ethernet Compatibility Alliance

BIBLIOGRAFÍA

- Banco Central del Ecuador, series de las tasas activas nominales promedio ponderadas, por entidad: http://www.superban.gov.ec

- Bellovin, S.M. y Cheswick, W.R., Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley, 1994.

- Cisco Secure Intrusion Detection System: Technical Tips. http://www.cisco.com/warp/public/707/#cs_ids

- Comer, D.E., Internetworking with TCP/IP, volumen 1, cuarta edicion, Prentice Hall, 2000

- Comunicaciones IP de Cisco www.cisco.com/go/ipc

- Firewall http://www.infospyware.com/Firewall/Cortafuegos.htm

- Fox Andy y David W. Chapman Jr.: Firewalls PIX de Cisco Secure reduzca el riesgo de ataques a las redes con el libro official CSPFA, Nuñez de Balboa, 120 28006 Madrid, Cisco Press, primera edición, Pearson Educación S.A., Felix Fuentes y Eva Maria Lopez, 2002, Ruth Vázquez Llorente.

- Guía de Productos de Cisco para pequeñas y medianas empresas

- Halabi B. y McPherson, D., Arquitecturas de enrutamiento en Internet, segunda edicion, Cisco Press, 2001.

- Halsall, F., Data Communications, Computer Networks, and Open Systems, cuarta edicion, Addison-Wesley, 1996

- Murdick/Munson.: Sistemas de Información y Administrativa. Editorial Prentice Hall Segunda Edición, 1998.

- Nerwork Security Policy: Best Practices White Paper: hhtp://www.cisco.com/warp/public/126/secpol.html

- Perlman, R., Interconnections: Bridges, Routers, Switches and Internetworking Protocols, segunda edicion, Addison-Wesley, 1999.

- Peterson, L., y Davie B.S., Computer Networks: A Systems Approach, segunda edicion, Morgan Kaufmann Publishers, 1999

- Pinsky Bruce y Leindwand Allan: Configuración de Routers Cisco Una introducción practica a la configuración del software Cisco IOS, Núñez de Balboa, 120 28006 Madrid, Cisco Press, segunda edición, Pearson Educación S.A.,Alejandro Domínguez, Félix Fuentes y Eva Maria Lopez, 2001, José Arroyo Pérez

- Productos para redes inalámbricas de Cisco www.cisco.com/go/wireless

- Reid Neil y Seide Ron.: 802.11 (Wi-Fi) Manual de Redes Inalámbricas. McGraw-Hill Interamericana, primera edición en español, Delegación Iztapalapa C.P.09810 México D.F., Fernando Castellanos Rodríguez, McGraw-Hill Interamericana Editores, S.A. de C.V., Septiembre 2003, 345.

- Routers de Cisco www.cisco.com/go/routers

- Soluciones de Seguridad de Cisco www.cisco.com/go/security

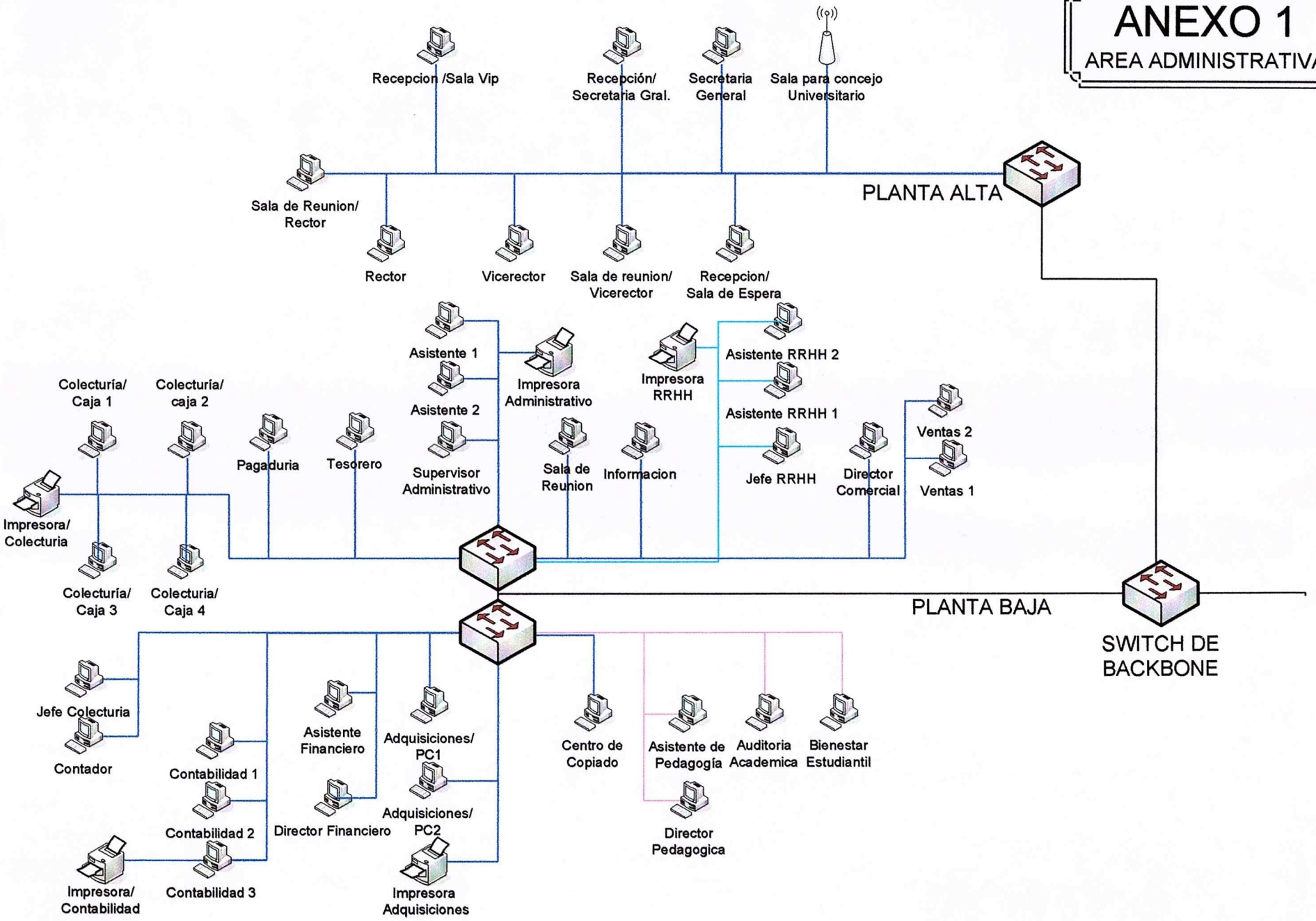
- Switches de la serie Cisco Catalyst www.cisco.com/go/switching

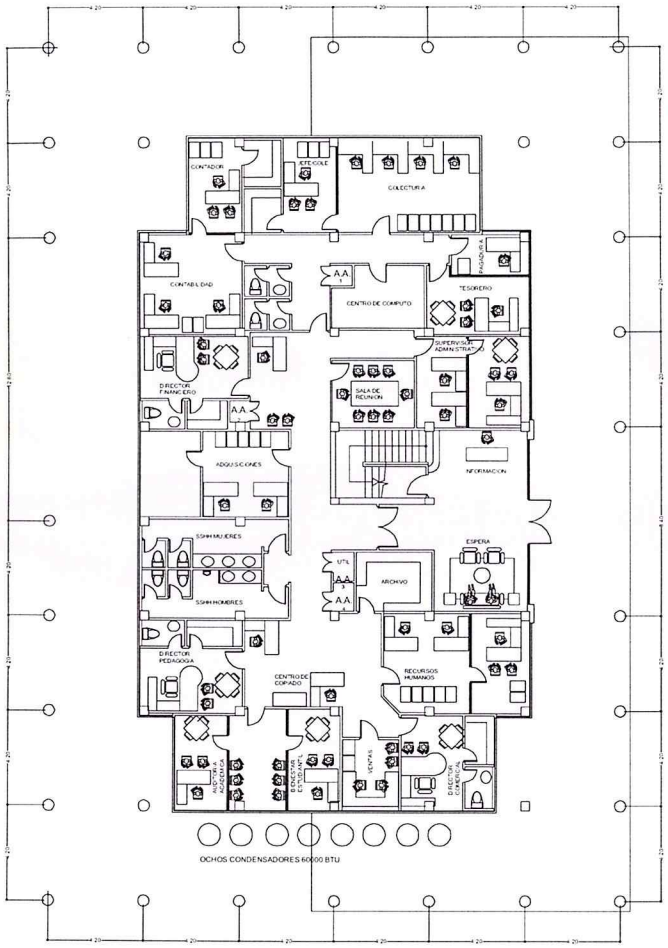
- Tipos de Redes http://es.wikipedia.org/wiki/Red_de_computadoras#Tipos_de_redes

- Zwicky, E.D., et al., Building Internet Firewalls, segunda edicion, O'Reilly & Associates, 2000.

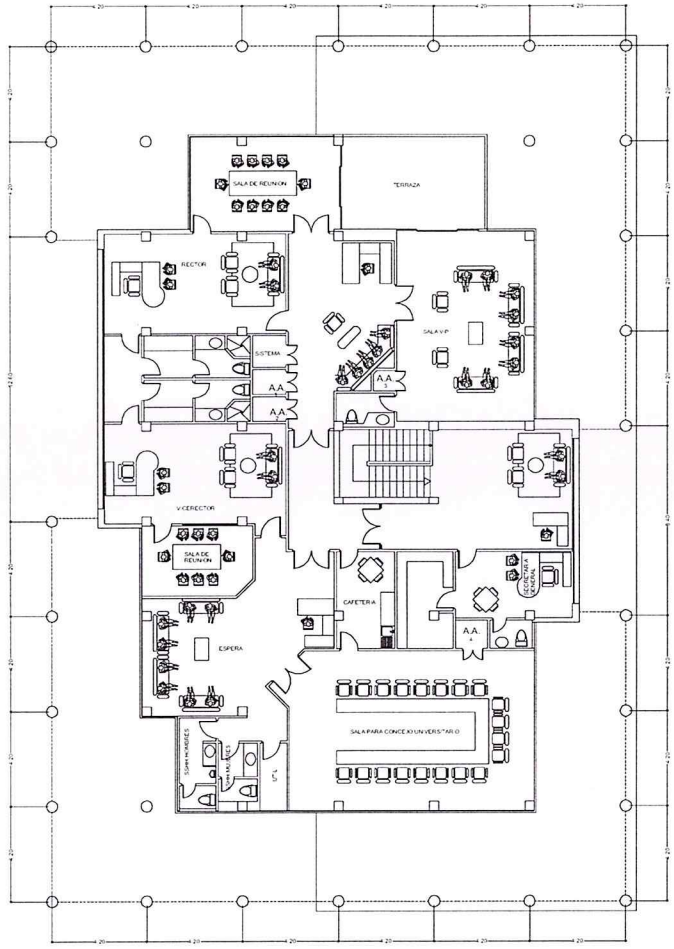
ANEXO 1

ANEXO 1
AREA ADMINISTRATIVA





Planta Baja



Planta Alta

Obra
Universidad Tecnologica Empresarial Guayaquil
area adminstrativa

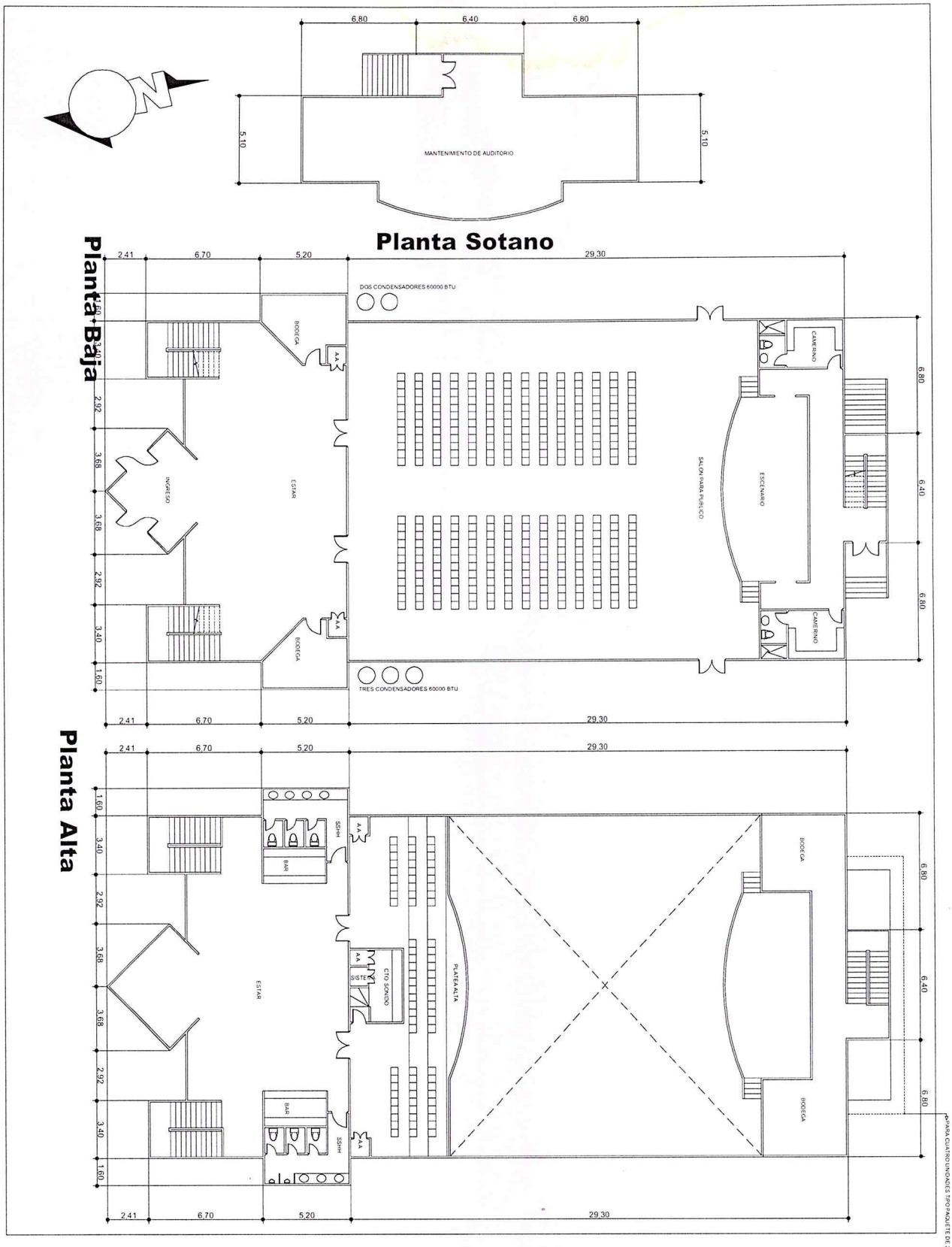
Contiene

Obra: Universidad Tecnologica Empresarial Guayaquil	
Proyecto: Arq. Luis Valera S. R.P.G. 1808	Resp. Tecnico: Arq. Luis Valera S. R.P.G. 1808
Propietario:	Escala: 1:100
	Fecha: AGOST/05
Colaborador: Arq. Victor Beuhing R.	Lamina: 2

Sellos Municipales

Contiene:
AREA ADMINISTRATIVA

ANEXO 2



LOSA DE CUBIERTA DE 15X3.10 MTS
APARA CUATRO UNIDADES TIPO PAQUETE DE 240000 BTU CU

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
auditorio

Propietario
Universidad Tecnologica Empresarial Guayaquil

Proyectó
Arq. Victor Ramirez R.

Propietario

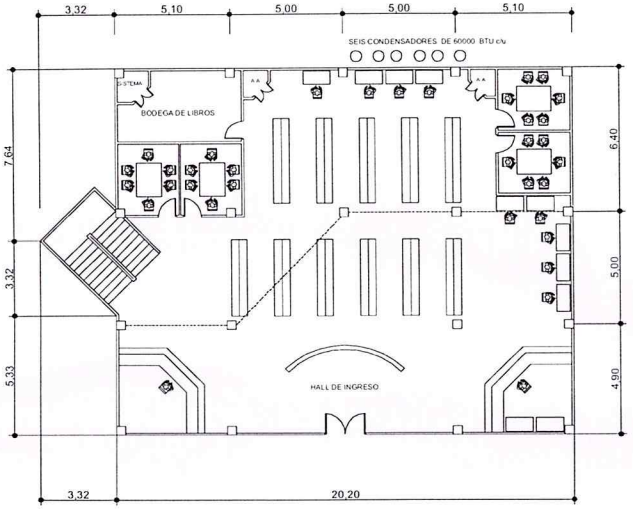
Escala
1:__100

Fecha
AGOSTO/05

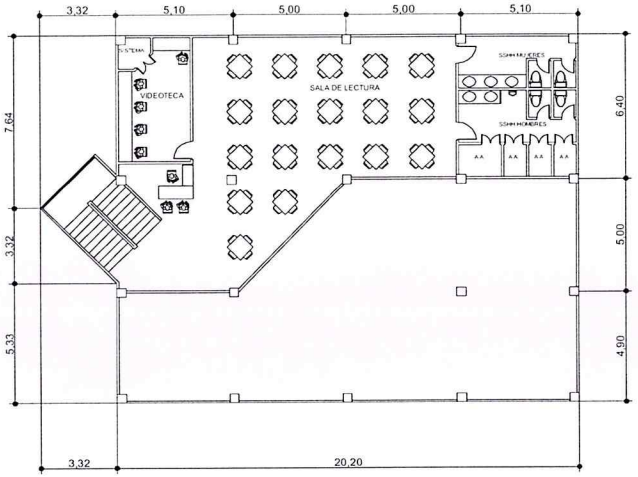
Lámina
13

Contiene
AUDITORIO

ANEXO 3



Planta Baja



Planta Alta

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
biblioteca

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto
Arq. Luis Velarde B.
R.P.G. 1808

Resp. Técnico
Arq. Luis Velarde B.
R.P.G. 1808

Propietario

Escala
1 : 100

Fecha
AGOST/05

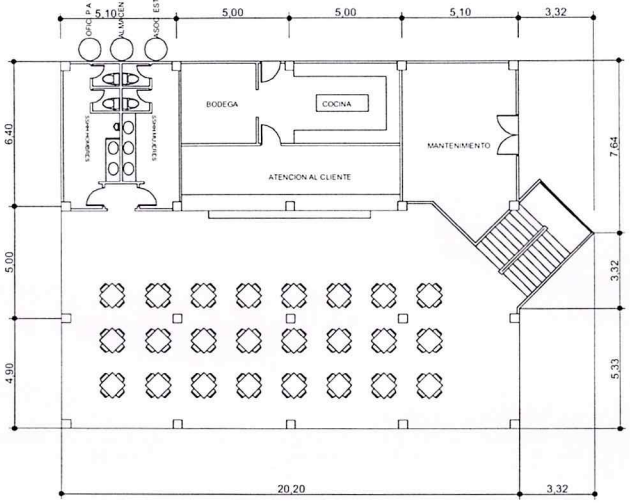
Colaborador
Arq. Victor Sauhing R.

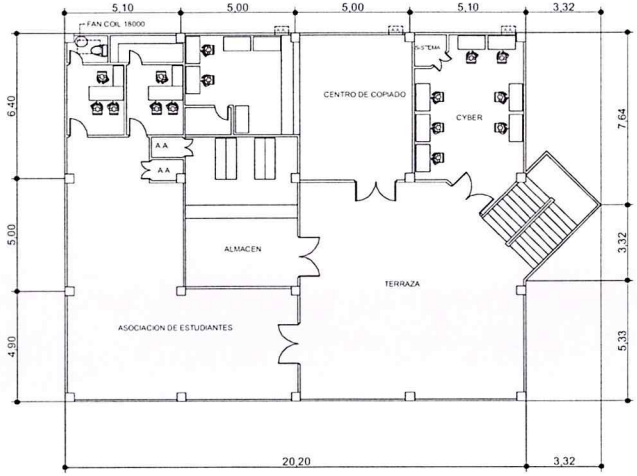
Lamina
12

Sellos Municipales

Contiene
BIBLIOTECA

ANEXO 4





A A. 3 AIRES DE VENTANA DE 24000 BTU c/u

Planta Baja

Planta Alta

Universidad Tecnologica Empresarial Guayaquil

cafeteria

Obra: Universidad Tecnologica Empresarial Guayaquil

Proyecto: Arq. Luis Vivero S. R.P.G. 1808

Resp. Tecnico: Arq. Luis Vivero S. R.P.G. 1808

Propietario:

Escala: 1 100

Fecha: AGOST/05

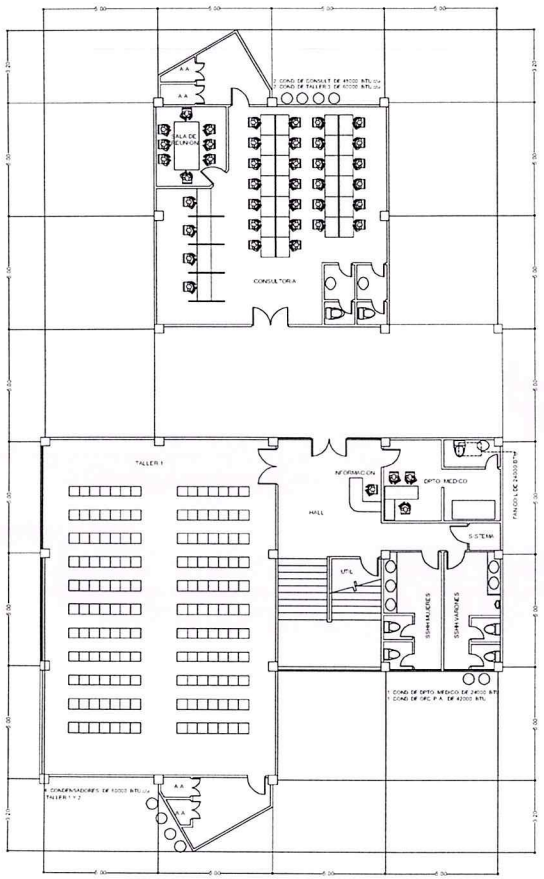
Colaborador: Arq. Victor Seuhing R.

Lamina: 12

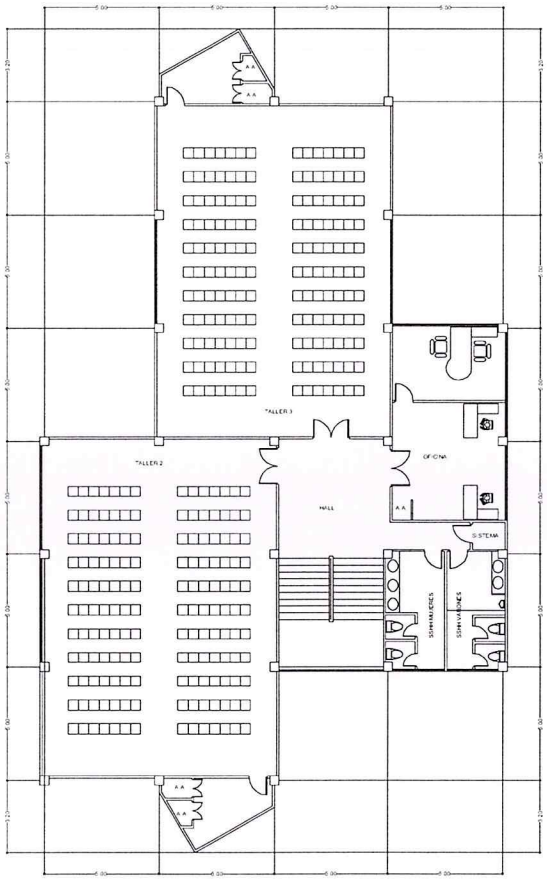
Sellos Municipales:

Contiene: CAFETERIA

ANEXO 5



Planta Baja



Planta Alta

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
centro de desarrollo regional

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto
Arq. Luis Velasco R.
R.P.G. 1808

Resp. Técnico
Arq. Luis Velasco R.
R.P.G. 1808

Propietario

Escala
1:100

Fecha
JUNIO/05

Colaborador
Arq. Victor Sevilla R.

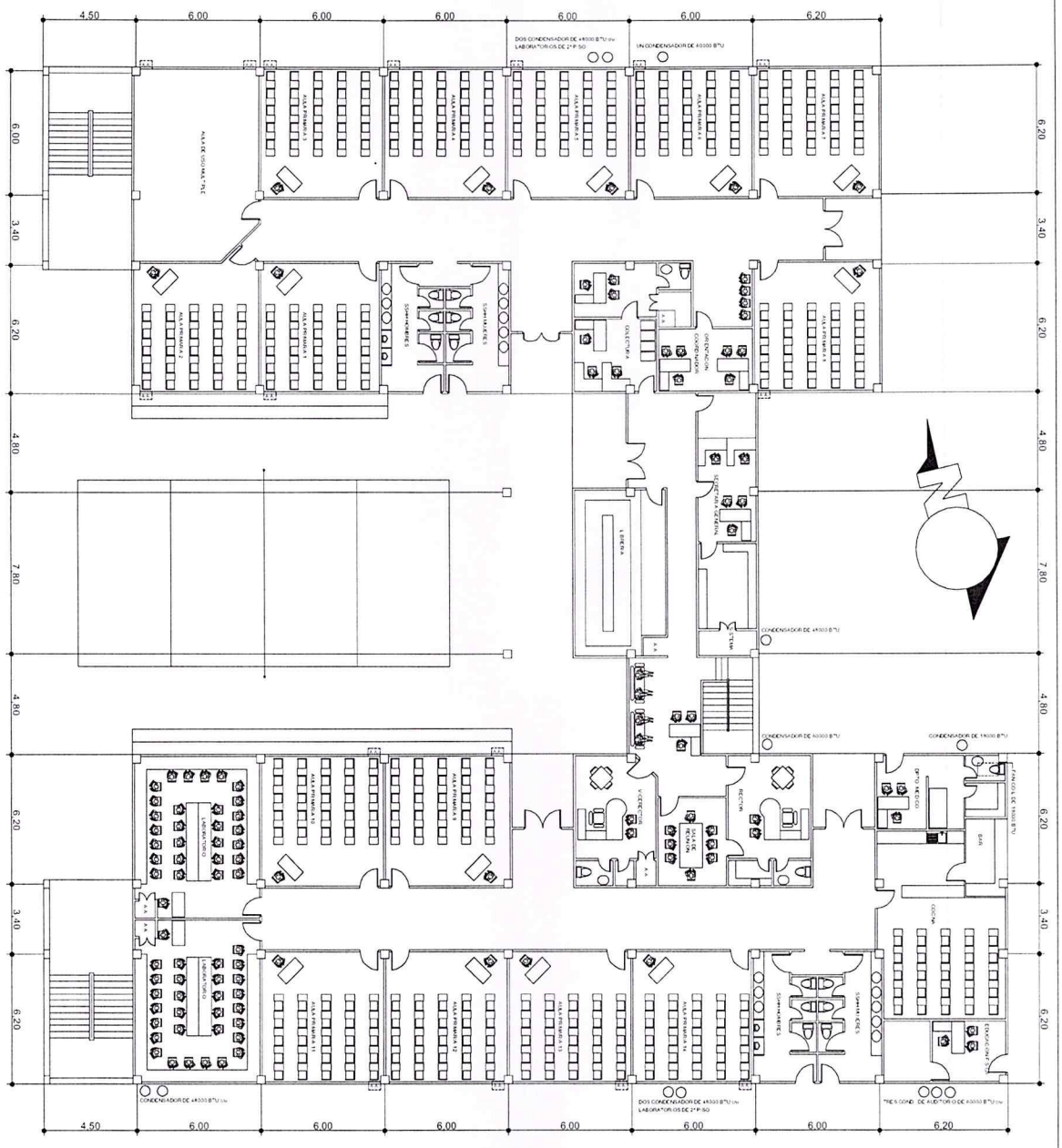
Lamina
3

Sellos Municipales

Contiene
CENTRO DE DESARROLLO REGIONAL

ANEXO 6

Planta Baja



Obra

Universidad Tecnologica Empresarial Guayaquil

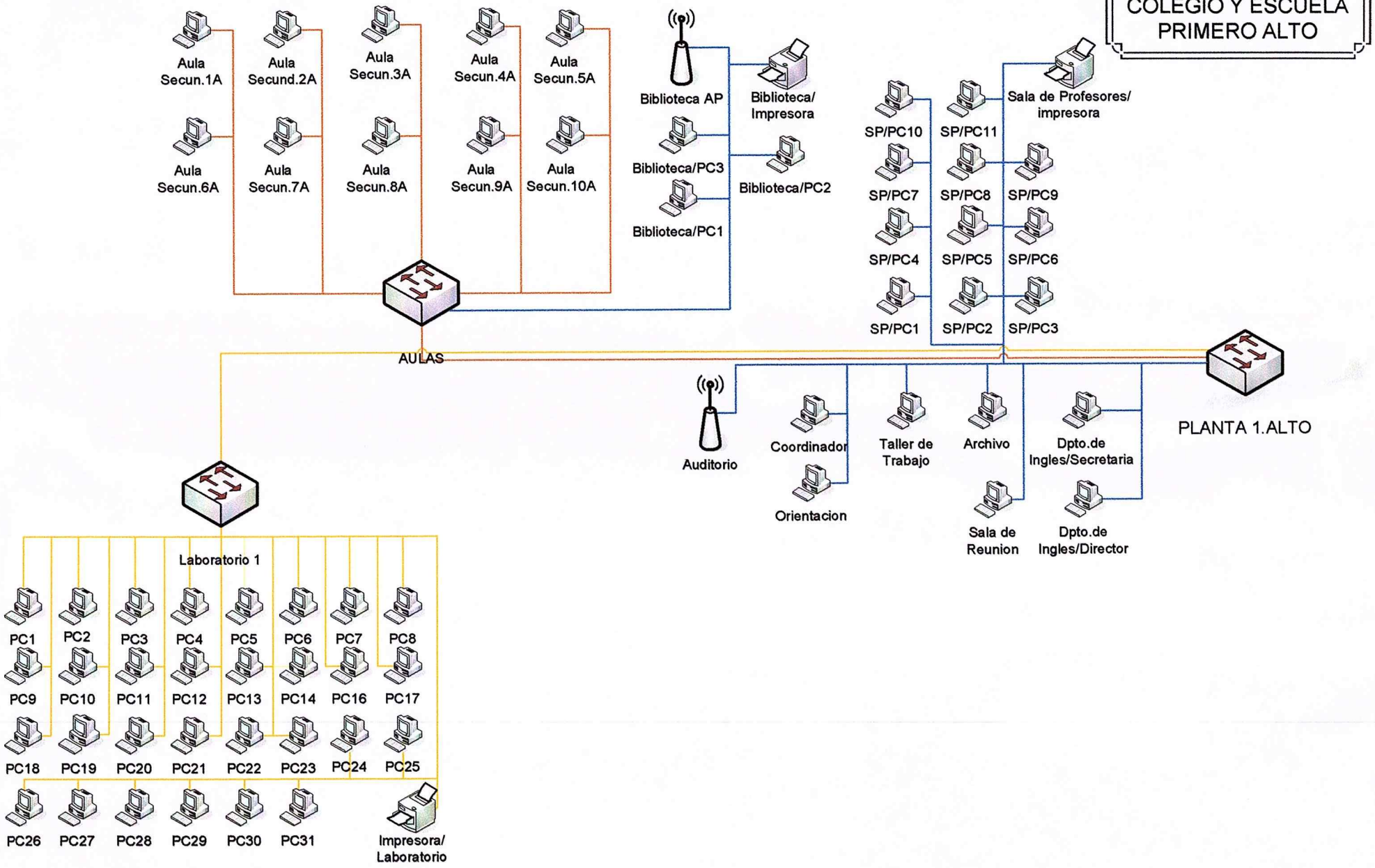
Contiene

colegio y escuela planta baja

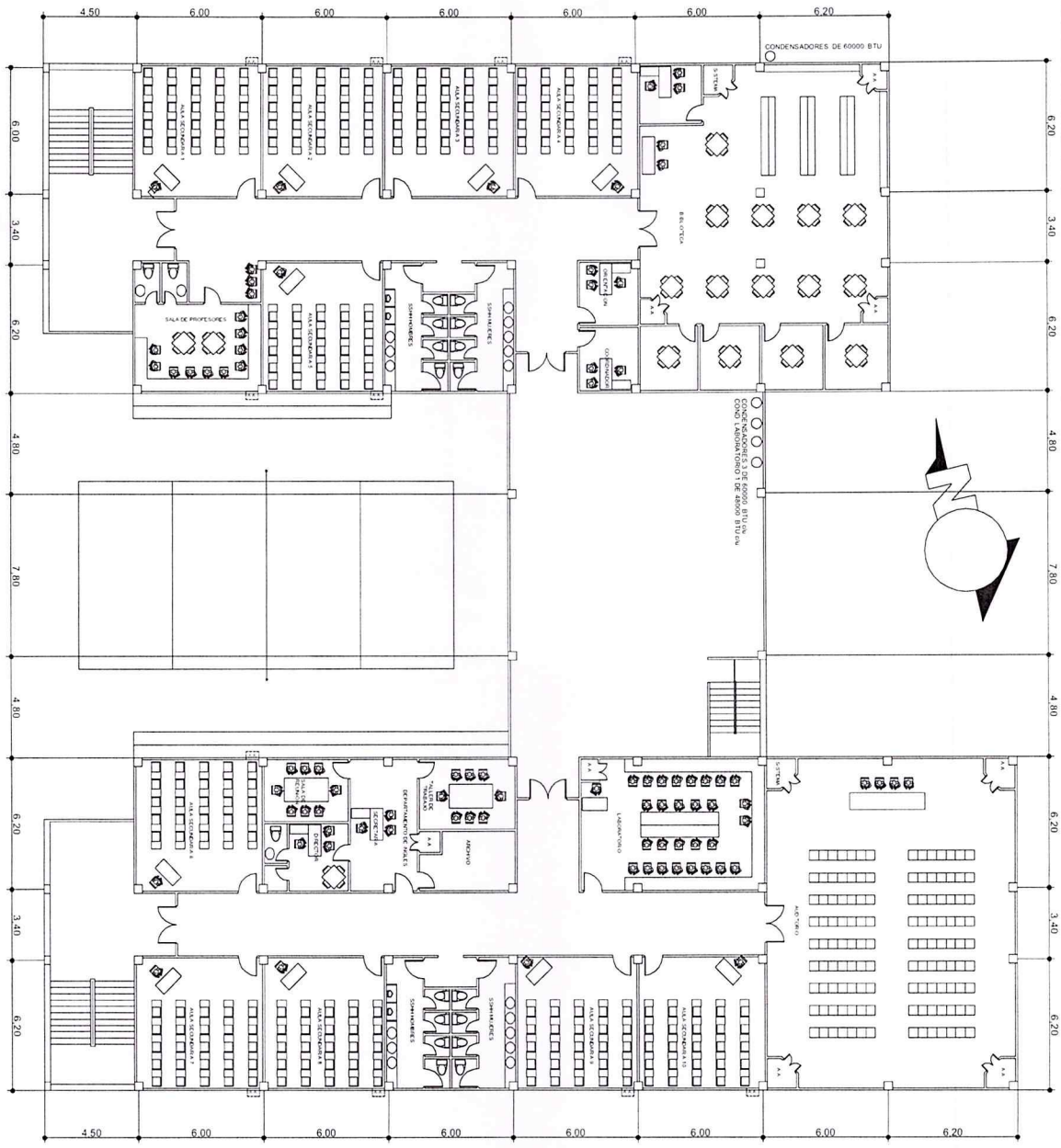
Obra	Universidad Tecnologica Empresarial (Guayaquil
Propietario	
Arq. Victor Sachna R.	
Contiene	COLEGIO Y ESCUELA PLANTA BAJA
Fecha	AGOSTO/05
Escala	1:100
Lamina	9

ANEXO 6

COLEGIO Y ESCUELA
PRIMERO ALTO



Planta Primer Alto



Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
COLEGIO Y ESCUELA
PLANTA PRIMER ALTO

Propietario

Arq. Víctor Andrade R.

Fecha
AGOSTO/08

Escala
1 : 100

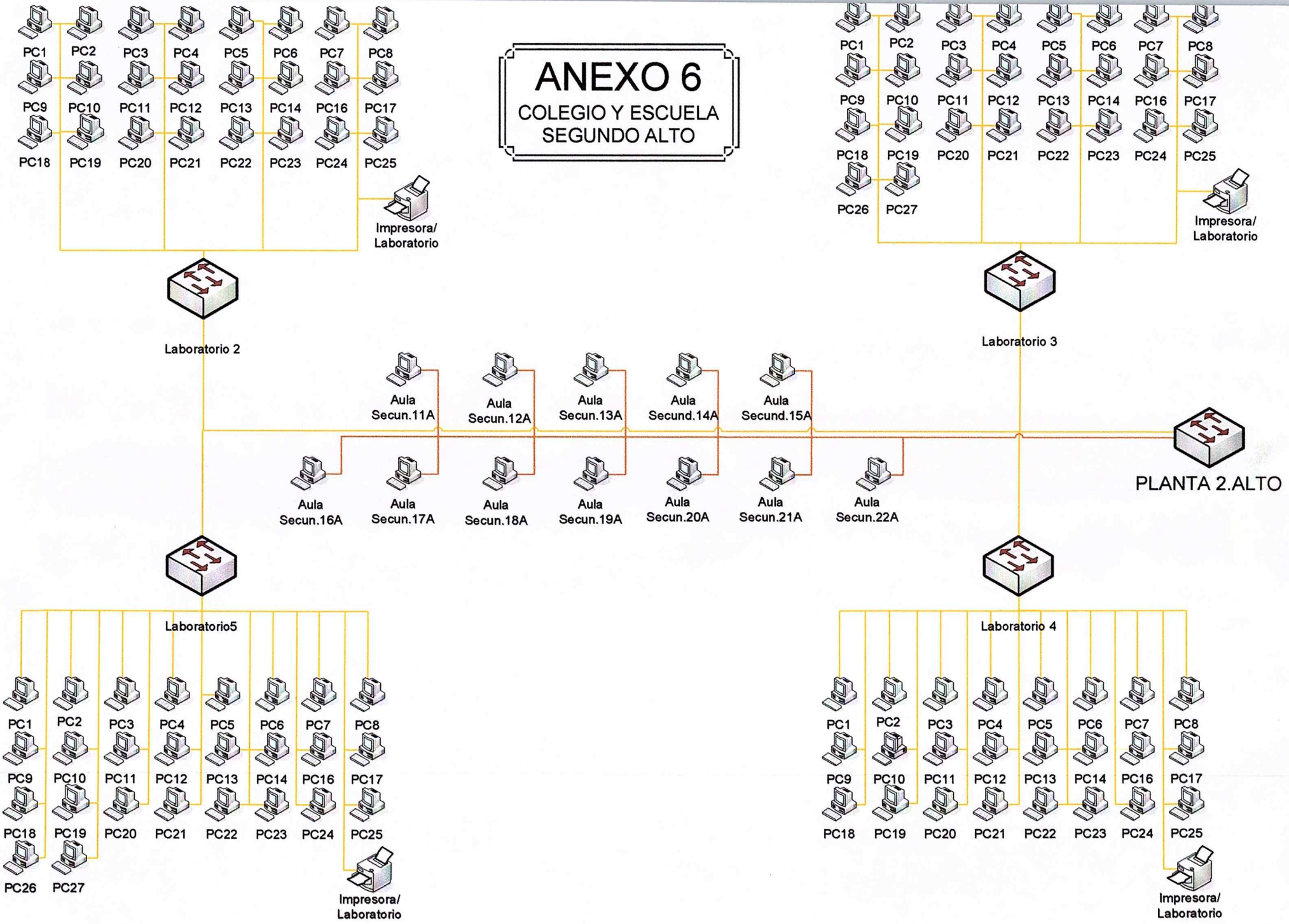
Hoja
9

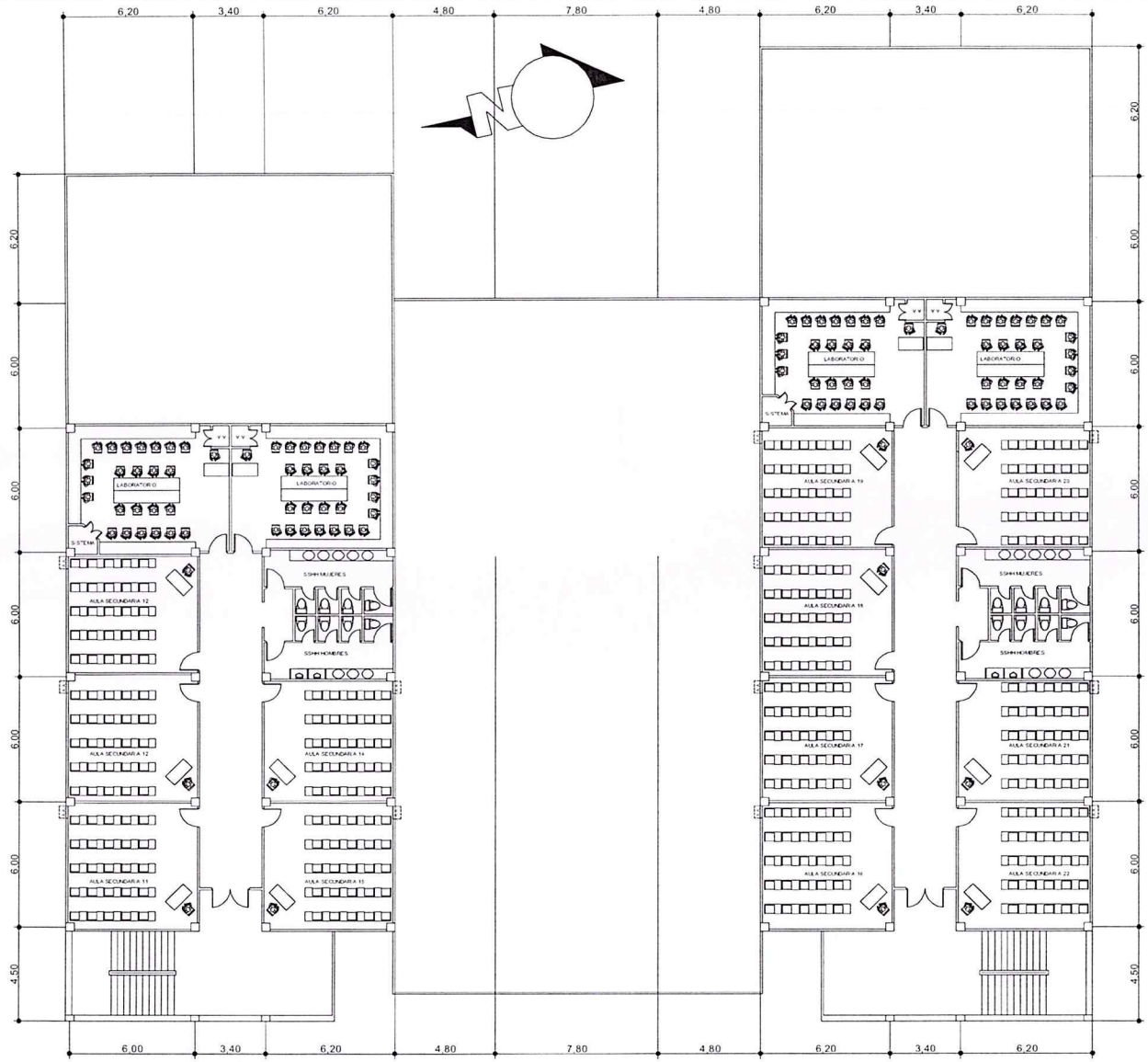
Universidad Tecnologica Empresarial Guayaquil

colegio y escuela planta 1er. alto

ANEXO 6

COLEGIO Y ESCUELA
SEGUNDO ALTO





Planta Segundo Alto

A A. 12 AIRES DE VENTANA DE 24000 BTU c/u

Obra
Universidad Tecnologica Empresarial Guayaquil
colegio y escuela planta 2do. alto

Contiene

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyectó
Arq. Luis Velero S. R.P.G. 1808

Resp. Técnico
Arq. Luis Velero S. R.P.G. 1808

Presupuesto

Escala
1:100

Fecha
AGOST/05

Colaborador
Arq. Victor Beuhing R.

Lamina
9

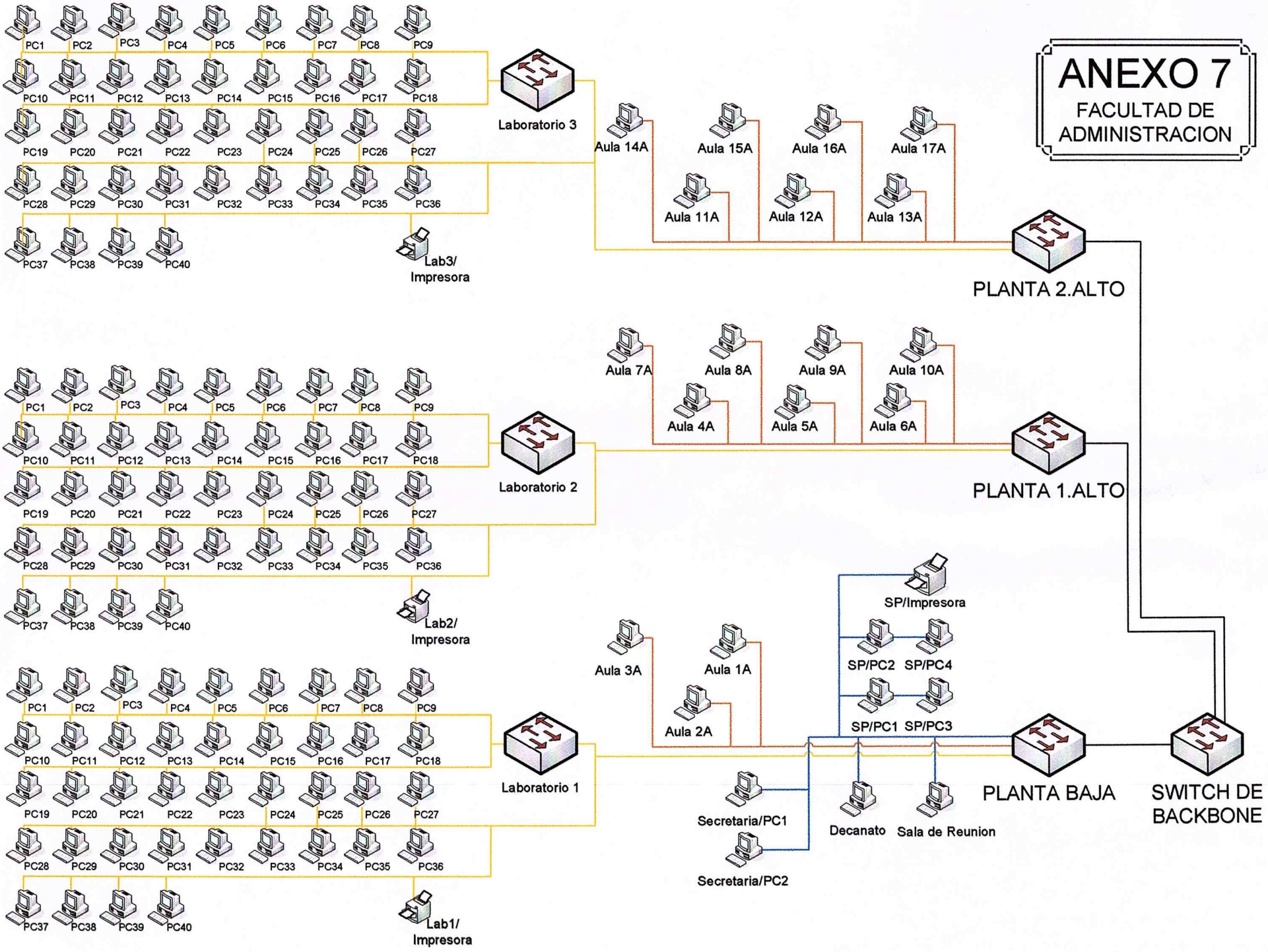
Sellos Municipales

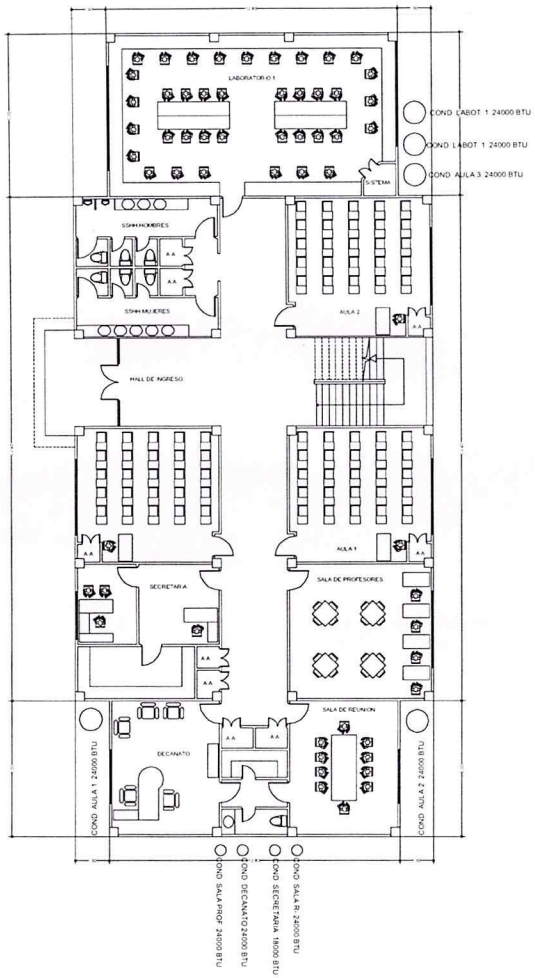
Contiene
COLEGIO Y ESCUELA PLANTA SEGUNDO ALTO

ANEXO 7

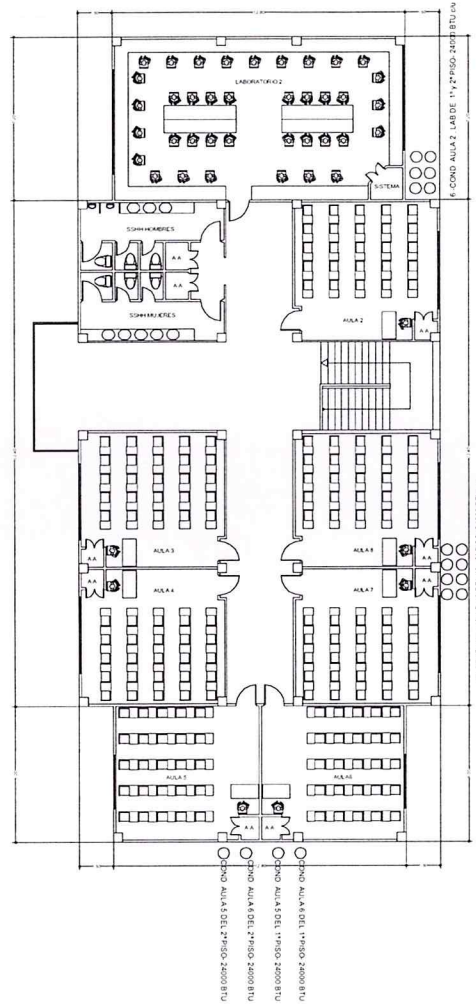
ANEXO 7

FACULTAD DE ADMINISTRACION





Planta Baja



Planta 1ro. y 2do. Alto

Universidad Tecnologica Empresarial Guayaquil

facultad administracion

Obra: Universidad Tecnologica Empresarial Guayaquil

Proyecto: Arq. Luis Vidoza S. R.P.G. 1808

Resp. Tecnico: Arq. Luis Vidoza S. R.P.G. 1808

Propietario:

Escala: 1:100

Fecha: AGOST/05

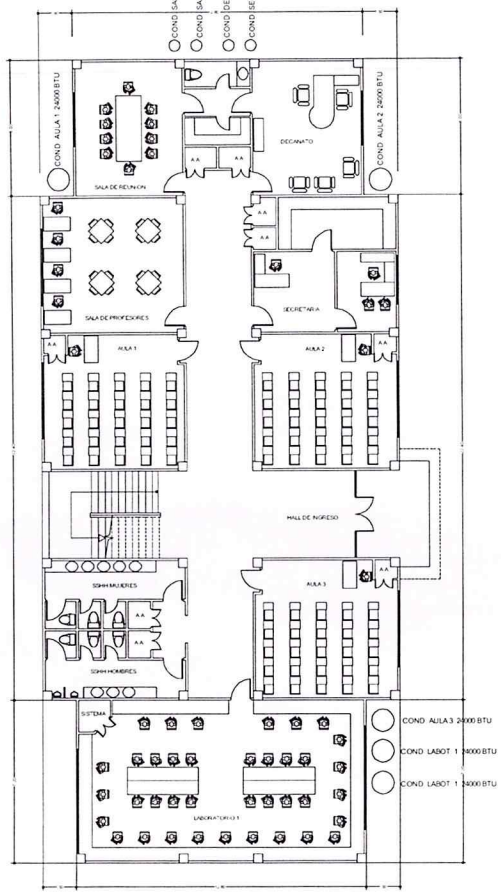
Colaborador: Ars. Victor Bautista R.

Lamina: 4

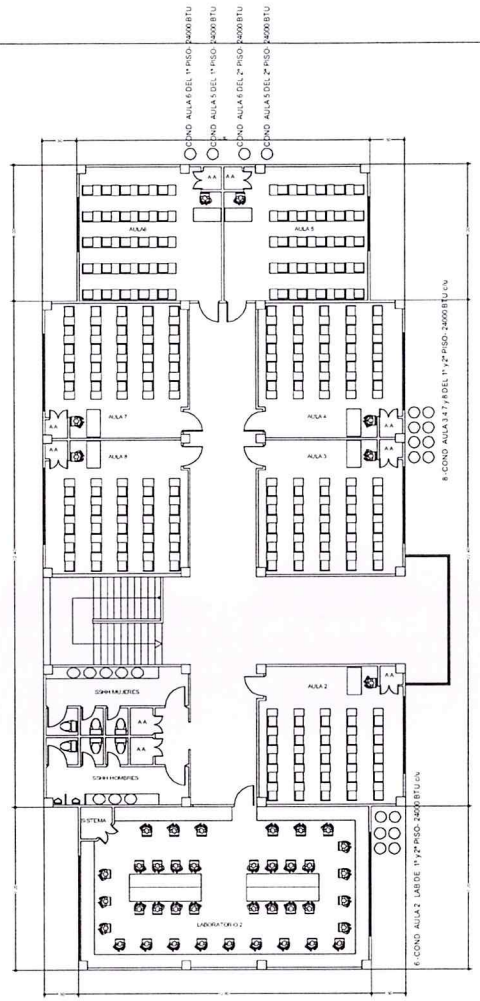
Sellos Municipales:

Contiene: FACULTAD DE ADMINISTRACION

ANEXO 8



Planta Baja



Planta 1ro. y 2do. Alto

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
facultad comercio exterior

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto
Arq. Luis Vidarte R. R.P.G. 1808

Resp. Tecnico
Arq. Luis Vidarte R. R.P.G. 1808

Propietario

Escala
1:100

Fecha
AGOST/05

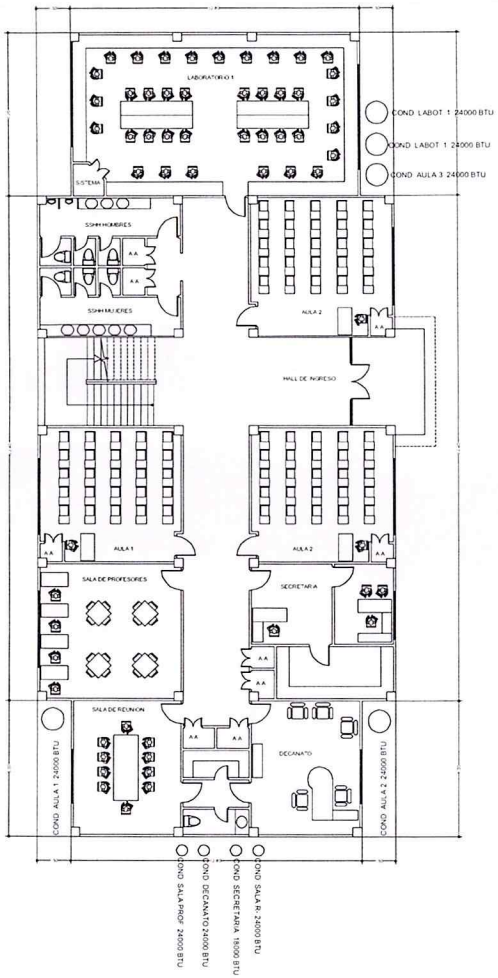
Colaborador
Arq. Victor Beuhing R.

Lamina
4

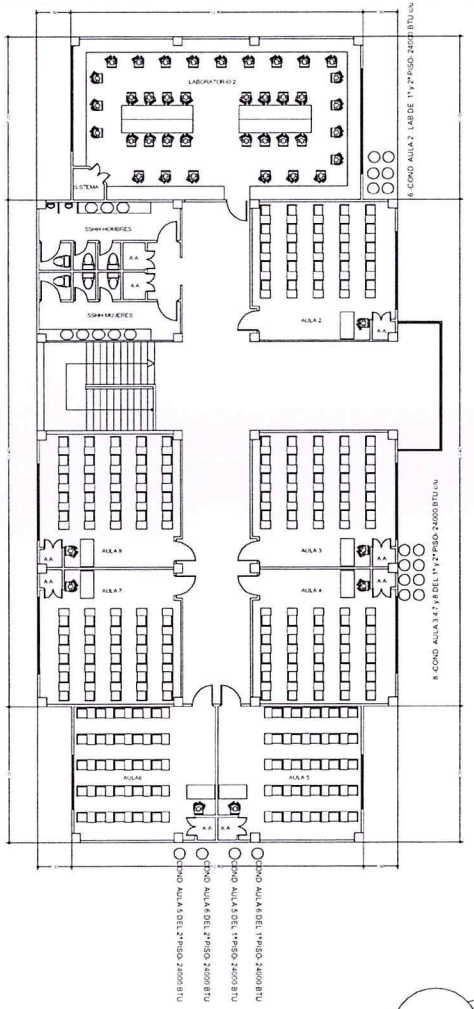
Datos Municipales

Contiene
FACULTAD DE COMERCIO EXTERIOR

ANEXO 9



Planta Baja



Planta 1ro. y 2do. Alto

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
facultad economia

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto
Arq. Luis Velasco R. R.P.G. 1808

Resp. Técnico
Arq. Luis Velasco R. R.P.G. 1808

Propietario

Escala
1 : 100

Fecha
AGOST/05

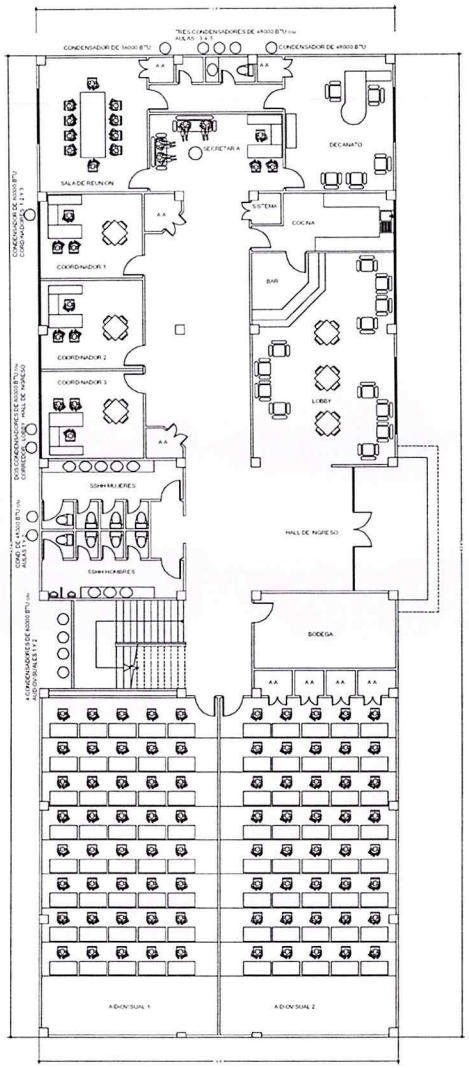
Colaborador
Arq. Victor Bejring R.

Lamina
4

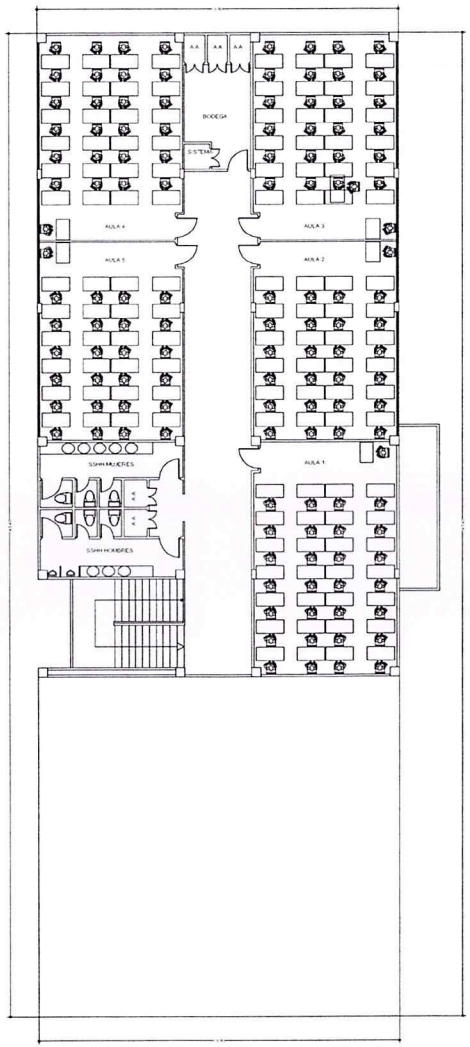
Sellos Municipales

Contiene
FACULTAD DE ECONOMIA

ANEXO 10



Planta Baja



Planta 1ro. y 2do. Alto

Obra
Universidad Tecnologica Empresarial Guayaquil
Contiene
facultad postgrado

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto
Arq. Luis Vizuete R. R.P.A. 1808

Resp. Tecnico
Arq. Luis Vizuete R. R.P.A. 1808

Propietario

Escala
1 100

Fecha
AGOST/05

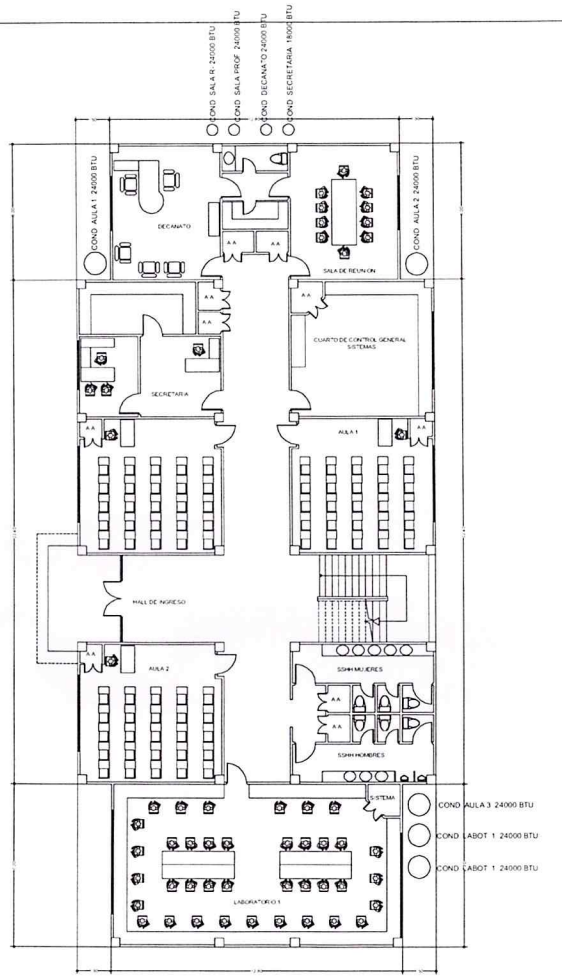
Colaborador
Arq. Victor Sieuhing R.

Lamina
4

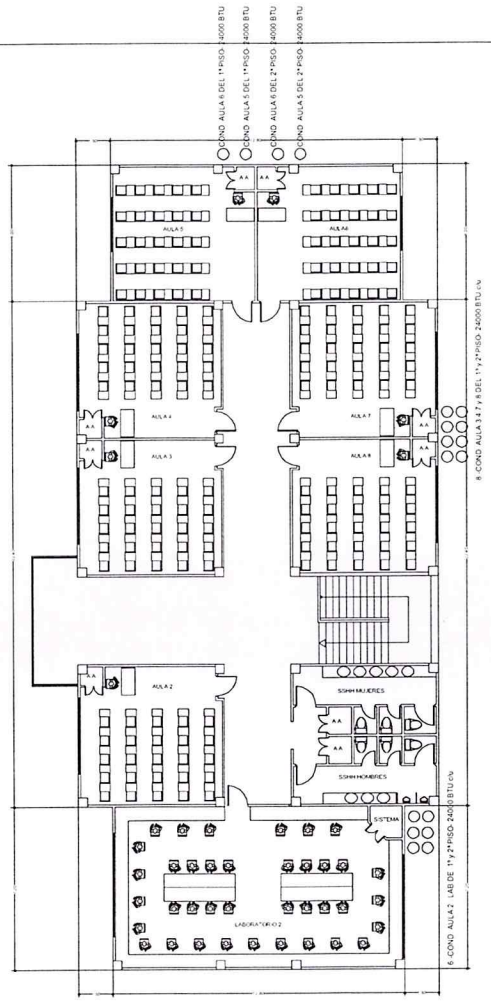
Sellos Municipales

Contiene
FACULTAD DE POSTGRADO

ANEXO 11



Planta Baja



Planta 1ro. y 2do. Alto

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
facultad tecnologia y comunicacion

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto

Resp. Tecnico
Arq. Luis Velarde R.
R.P.G. 1606

Propietario

Escala
1 100

Fecha
AGOST/05

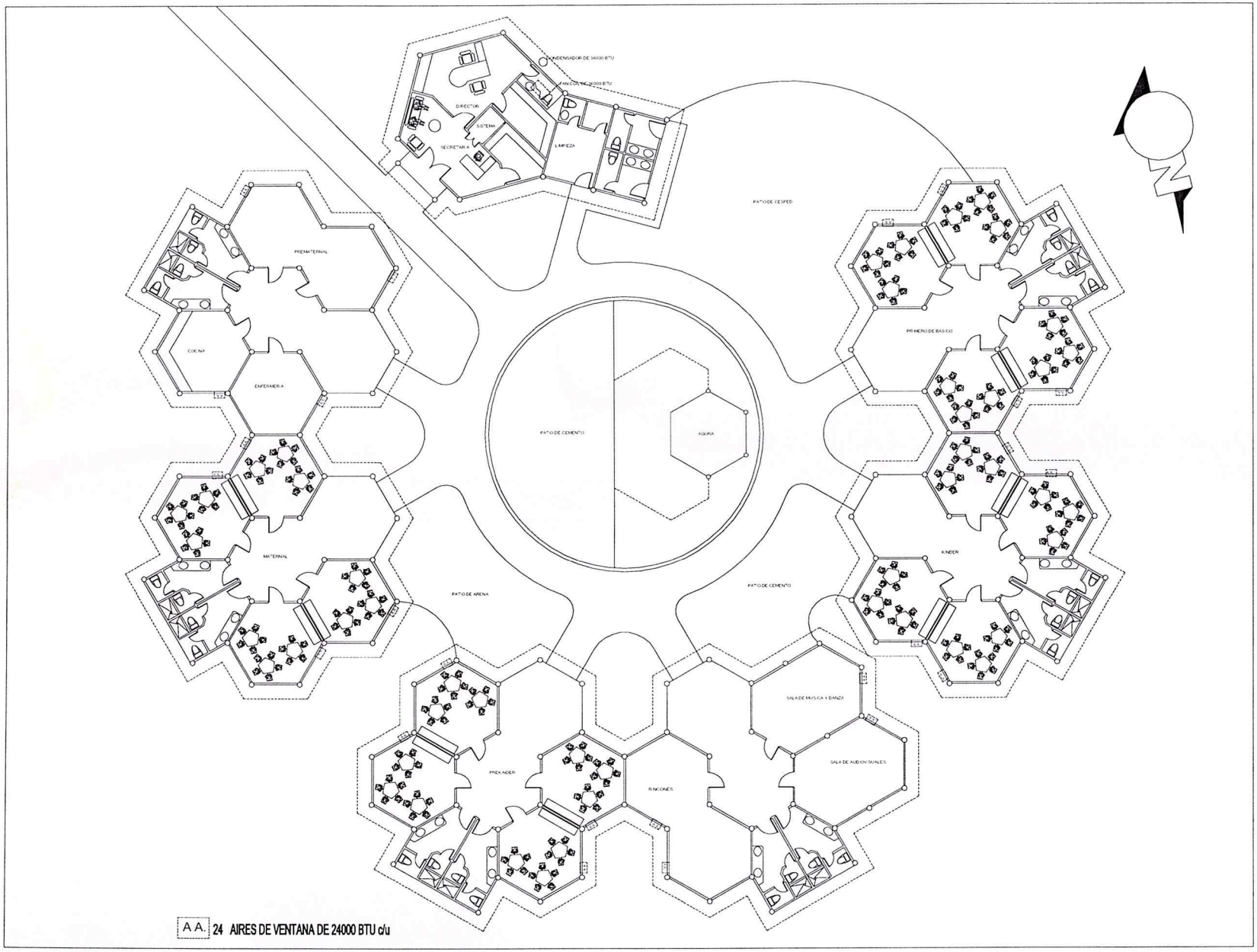
Colaborador
Arq. Victor Beuhing R.

Lamina
4

Sellos Municipales

Contiene
FACULTAD DE TECNOLOGIA Y COMUNICACION

ANEXO 12



A.A. 24 AIRES DE VENTANA DE 24000 BTU c/u

Obra
Universidad Tecnologica Empresarial Guayaquil

Contiene
preparatoria

Obra
Universidad Tecnologica Empresarial Guayaquil

Proyecto
Arq. Luis Velero S. R.P.G. 1808

Resp. Tecnico
Arq. Luis Velero S. R.P.G. 1808

Propietario

Escala
1 : 100

Fecha
JUNIO/05

Colaborador
Arq. Victor Seuhing R.

Lamina
8

Sellos Municipales

Contiene
PREPARATORIA

ANEXO 13

ANEXO 13

3Com® Baseline Switch 2824

Switching Gigabit de Alto Rendimiento para Pequeñas Empresas

El 3Com® Switch 2824 es un switch Gigabit muy asequible, de alto rendimiento y sin administración, ideal en contextos dinámicos y creativos de pequeñas empresas. Con velocidades Gigabit de 1000 Mbps y una capacidad de switching de 32 Gbps, cumple con las necesidades de rendimiento incluso de las aplicaciones que más requieren un gran ancho de banda. Las características avanzadas de switching tales como priorización de tráfico 802.1p y Clase de Servicio (CoS) garantizan que aplicaciones en tiempo real como las de vídeo y audio tengan prioridad, de forma que puedan funcionar con efectividad, y permiten a los switches operar en contextos de redes de mayor tamaño.

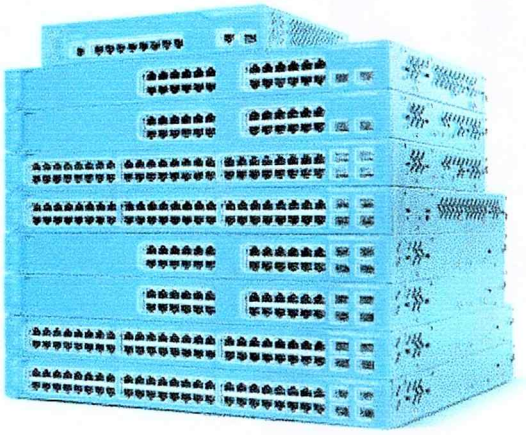
Los switches 3Com para pequeñas empresas se sitúan reiteradamente entre los productos más fiables de la industria.' 3Com ofrece también un importante paquete de soporte con garantía limitada de por vida para el hardware, noventa días de asistencia técnica telefónica gratuita y soporte Web ilimitado, para garantizar así una total tranquilidad incluso mucho tiempo después del despliegue.

- Switch Gigabit de alta fiabilidad que ofrece un valor excepcional, al proporcionar un destacado rendimiento a un bajo precio
- El switch viene preconfigurado de fábrica, de forma que resulta fácil instalarlo nada más desembalarlo'
- El rendimiento sin bloqueo mejora el acceso a los recursos de red
- La auto-negociación permite acomodar LANs con diversos anchos de banda
- La priorización IEEE 802.1p proporciona compatibilidad con redes que funcionan con aplicaciones en tiempo real
- MDI/MDIX automático en todos los puertos simplifica la instalación
- El factor de forma de una unidad de rack (1RU) optimiza el espacio en rack
- Garantía limitada de por vida para el hardware, noventa días de asistencia técnica telefónica gratuita y soporte Web ilimitado que garantizan una total tranquilidad

Cisco Catalyst 3560 Series Switches

Foundation for Innovation-Powered by Cisco

Figure 1. Catalyst 3560 Series Switches



The Cisco® Catalyst® 3560 Series (Figure 1) is a line of fixed-configuration, enterprise-class switches that includes IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE) capability in Fast Ethernet and Gigabit Ethernet configurations. The Cisco Catalyst 3560 is an ideal access-layer switch for small enterprise LAN access or branch-office environments, combining both 10/100/1000 and PoE configurations for maximum productivity and investment protection while facilitating the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks. Customers can deploy networkwide intelligent services-such as advanced quality of service (QoS), rate limiting, access control lists (ACLs), multicast management, and high-performance IP routing-while maintaining the simplicity of traditional LAN switching.

PRODUCT BENEFITS

IEEE 802.3af and Cisco Prestandard Power over Ethernet

The Cisco Catalyst 3560 Series can provide a lower total cost of ownership (TCO) for deployments that incorporate Cisco IP phones, Cisco Aironet® wireless LAN (WLAN) access points, or any IEEE 802.3af-compliant end device. PoE removes the need for wall power to each PoE-enabled device and eliminates the cost for additional electrical cabling that would otherwise be necessary in IP phone and WLAN deployments.

The Cisco Catalyst 3560 24-port PoE configurations can support 24 simultaneous full-powered PoE ports at 15.4 watts (W) for maximum powered-device support. Taking advantage of Cisco Catalyst Intelligent Power Management, the 48-port PoE configurations can deliver the necessary power to support 24 ports at 15.4W, 48 ports at 7.7W, or any combination in between through the sophisticated power-management features in Cisco IOS® Software.

Maximum power availability for a converged voice and data network is attainable when a Cisco Catalyst 3560 Series switch is combined with the Cisco RPS 675 Redundant Power System for transparent protection against internal power supply failures and an uninterruptible power supply (UPS) system to safeguard against power outages.

Gigabit Ethernet

At speeds of 1000 Mbps, Gigabit Ethernet provides the bandwidth to meet new and evolving network demands, alleviate bottlenecks, and boost performance while increasing the return on existing and new infrastructure investments. Today's workers are placing higher demands on networks, running multiple, concurrent applications. For example, a worker joins a team conference call through an IP videoconference, sends a 10-MB spreadsheet to meeting participants, broadcasts the latest marketing video for the team to evaluate, and queries the customer relationship management (CRM) database for the latest real-time feedback. Meanwhile, a multiple-gigabyte system backup starts in the background, taking advantage of simple and affordable network attached storage (NAS) to comply with regulatory record keeping requirements such as Sarbanes-Oxley.

The Cisco Catalyst 3560 Series can scale the access network to 1 Gbps over existing Category 5 copper cabling and make the most of the desktops and notebooks that are now shipping with Gigabit Ethernet network interface cards (NICs) and higher PC bus speeds for full bandwidth utilization. In addition to being easy to deploy, Gigabit Ethernet networks are simpler to maintain with the new Cisco Time Domain Reflectometry (TDR) that helps verify existing cabling.

The Gigabit Ethernet models of the Cisco Catalyst 3560 Series also facilitate high-performance Grid and distributed computing in addition to preparing your network to deploy software applications such as Microsoft Exchange, as well as Microsoft Vista's remote imaging, data synchronization, and computer-to-computer search capabilities.

Enhanced Security

With the wide range of security features that the Cisco Catalyst 3560 Series offers, businesses can protect important information, keep unauthorized people off the network, guard privacy, and maintain uninterrupted operation. The Cisco Catalyst 3560 Series supports a comprehensive set of security features for connectivity and access control, including network admission control (NAC), ACLs, Dynamic ARP Inspection, IP Source Guard, VPN Routing/Forwarding Lite (VRF Lite), port-level security, and identity-based network services with 802.1x and extensions. These features increase LAN security; protect passwords and configuration information; offer options for network security based on users, ports, or MAC addresses; and help quicken responses to intruder and hacker detection. NAC helps organizations to limit damage from viruses and worms by enforcing security-policy compliance on endpoint devices.

Availability and Scalability

The Cisco Catalyst 3560 Series is equipped with a robust set of features that allow for network scalability and higher availability through IP routing as well as a complete suite of Spanning Tree Protocol enhancements aimed to maximize availability in a Layer 2 network. Enhancements to the standard Spanning Tree Protocol, such as Per-VLAN Spanning Tree Plus (PVST+), Uplink Fast, and Port Fast, as well as innovations such as Flex Links, maximize network uptime. PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. Uplink Fast, Port Fast, and Backbone Fast all greatly reduce the standard 30- to 60-second Spanning Tree Protocol convergence time.

The Cisco Catalyst 3560 Series also delivers high-performance, hardware-based IP routing for either unicast or multicast traffic. The Cisco Express Forwarding-based routing architecture allows for very high-speed lookups while delivering the stability, performance, and scalability necessary to meet the needs of future requirements. Implementing routed uplinks to the core will improve network availability by enabling faster failover protection and simplifying the Spanning Tree Protocol algorithm by terminating all Spanning Tree Protocol instances at the aggregator switch. Additionally, routed uplinks allow better bandwidth utilization by implementing equal cost routing (ECR) on the uplinks to perform load balancing. Routed uplinks optimize the utility of uplinks out of the wiring closet by eliminating unnecessary broadcast data flows into the network backbone. Private VLANs improve scalability and provide IP address management benefits and Layer 2 security by partitioning a regular VLAN domain into subdomains. Support for the IPv6 industry standard in the Cisco Catalyst 3560 Series also alleviates address space problems.

Advanced Quality of Service

The Cisco Catalyst 3560 Series provides intelligent services to keep everything flowing smoothly. Industry-leading mechanisms for marking, classifying, and scheduling deliver best-in-class performance for data, voice, and video traffic-all at wire speed. Important features include Shaped Round Robin scheduling and policing/rate limiting as well as innovations like Scavenger Traffic Queuing functions. The IP Services license (formerly called the Enhanced Multilayer Image, or EMI) provides a richer set of enterprise-class features, including advanced hardware-based IP Unicast and IP Multicast routing as well as policy-based routing (PBR). The Advanced IP Services license, although not available as a pre-installed option, upgrades Cisco Catalyst 3560 Series switches to include IPv6 routing and IPv6 ACL support. Upgrade licenses are available to upgrade a switch from the IP Base license to the IP Services license or Advanced IP Services license as well as from the IP Services license to the Advanced IP Service license.

Enhanced Security

The Cisco Catalyst 3560 Series uses the following capabilities to protect sensitive data and network resources from internal and external threats:

- The Cisco Catalyst 3560 Series supports Network Admission Control (NAC), an industry initiative sponsored by Cisco Systems® that uses the network infrastructure to enforce security-policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms. Using NAC, organizations can provide network access to endpoint devices such as PCs, personal digital assistants (PDAs), and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.
- Dynamic ARP Inspection and IP Source Guard are security features in the Cisco Catalyst 3560 Series that protect the network from certain man-in-the-middle attacks. Dynamic ARP Inspection validates Address Resolution Protocol (ARP) packets in a network and ensures that only valid ARP requests and responses are relayed. IP Source Guard restricts IP traffic from untrusted sources.
- VPN Routing/Forwarding Lite (VRF Lite) in the Cisco Catalyst 3560 Series helps enable unique VPNs without additional equipment at the customer site.
- The IEEE 802.1x standard supported by the Cisco Catalyst 3560 Series prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated.

- Cisco Identity Based Networking Services (IBNS) in the Catalyst 3560 Series prevents unauthorized access and helps ensure that users receive only their designated privileges. It provides the ability to dynamically administer granular levels of network access.
- Secure Shell Protocol Version 2 (SSHv2) and Simple Network Management Protocol Version 3 (SNMPv3) provide network security by encrypting administrator traffic-preventing unauthorized users from accessing passwords or configuration information.
- Access control lists (ACLs) can be used to restrict access to sensitive portions of the network by denying packets based on source and destination MAC addresses, IP addresses, or TCP/UDP ports. ACLs can be used to guard against denial-of-service (DoS) and other attacks, and because ACL processing is done in hardware, forwarding performance of the switch is not compromised when implementing ACL-based security.
- Private VLAN edge provides security and isolation between ports on a switch, helping ensure that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port.
- Port security can be used to limit access on an Ethernet port based on the MAC address of the device that is connected to it. It also can be used to limit the total number of devices plugged into a switch port, thereby reducing the risks of rogue wireless access points or hubs.
- MAC Address Notification can be used to monitor the network and track users by sending an alert to a management station so that network administrators know when and where users entered the network. The Dynamic Host Configuration Protocol (DHCP) Interface Tracker (Option 82) feature tracks where a user is physically connected on a network by providing both switch and port ID to a DHCP server. Additionally, the DHCP Snooping Option 82 feature enables granular control over IP address assignment by a DHCP server by augmenting a host IP address request so that the DHCP server can make a more sophisticated address assignment.
- TACACS+ or RADIUS authentication facilitates centralized access control of switches and restricts unauthorized users from altering the configurations. Alternatively, a local username and password database can be configured on the switch itself. Fifteen levels of authorization on the switch console and two levels on the Web-based management interface provide the ability to give different levels of configuration capabilities to different administrators.

Redundancy

The Cisco Catalyst 3560 Series supports the following capabilities to optimize network availability, so that users can access data at all times, locally and remotely:

- Per VLAN Rapid Spanning Tree Plus (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances.
- Flex Links are a pair of Layer 2 interfaces (switch ports or port channels), where one interface is configured to act as a backup to the other. This feature provides an alternative solution to the Spanning Tree Protocol, allowing users to turn off Spanning Tree Protocol and still provide basic link redundancy.
- 802.1s Multiple Spanning Tree Protocol facilitates load balancing and improves network fault tolerance by providing multiple forwarding paths for data traffic. 802.1w Rapid Spanning Tree Protocol provides rapid recovery of uplink connectivity following failure.

- Cisco Hot Standby Router Protocol (HSRP) is supported to create redundant, failsafe routing topologies.
- Equal cost routing (ECR) provides load balancing and redundancy. Basic IP Unicast routing protocols (static, RIPv1, and RIPv2) are supported for small-network routing applications. Advanced IP Unicast routing protocols (OSPF, Interior Gateway Routing Protocol [IGRP], Enhanced IGRP [EIGRP], and Border Gateway Protocol Version 4 [BGPv4]) are supported for load balancing and constructing scalable LANs. IP Services or Advanced IP Services is required.
- Switch port auto-recovery (errdisable) automatically attempts to re-enable a link that is disabled because of a network error.
- The optional Cisco RPS 675 Redundant Power System protects against internal power supply failures.

Management

The Cisco Catalyst 3560 Series supports the following management capabilities:

- IEEE 802.3af and Cisco prestandard PoE support come with automatic discovery to detect a Cisco prestandard or IEEE 802.3af endpoint, negotiate the power to be budgeted for that device, and provide the necessary power-all done by the Cisco Catalyst 3560 Series switch without any user configuration.
- Cisco Smartport macros offer a set of verified feature templates per connection type in an easy-to-apply manner. With these templates, users can consistently and reliably configure essential security, IP telephony, availability, QoS, and manageability features with minimal effort and expertise. Smartport macros simplify the configuration of critical features for Ethernet networks.
- All Cisco Catalyst 3560 Series switches can be managed by the CiscoWorks LAN Management Solution (LMS) applications such as Resource Manager Essentials, Campus Manager, Device Fault Manager, and CiscoView. CiscoWorks LMS is a suite of powerful management tools that simplify the configuration, administration, monitoring, and troubleshooting of large Cisco networks. It integrates these capabilities into a world-class solution for improving the accuracy and efficiency of operations staff, increasing the overall availability of networks through proactive planning, and maximizing network security.
- Cisco Network Assistant software can manage a small network consisting of a diverse array of network devices, such as Cisco routers and Cisco Aironet wireless access points. A few mouse clicks enable the security, availability, and QoS features recommended by Cisco, without the need to consult a detailed design guide. The Security wizard automatically restricts unauthorized access to servers with sensitive data. Cisco Smartports and wizards save hours of time for network administrators, reduce human errors, and help ensure that the configuration of the switch is optimized for these applications. Available at no cost, Cisco Network Assistant can be downloaded from http://www.cisco.com/go/cna.
- The Cisco Express Setup feature simplifies initial configuration, eliminating the need for more complex terminal emulation programs and knowledge of CLI. This reduces the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.
- The DHCP Server feature enables a convenient deployment option for the assignment of IP addresses in networks that do not have a dedicated DHCP server.

Bandwidth Optimization

- Voice VLAN allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony, simplifying phone installations and providing easier network traffic administration and troubleshooting.
- Cisco Fast EtherChannel® and Gigabit EtherChannel technology allows for aggregating ports for up to 2 Gbps full duplex on network or server connections. Use Port Aggregation Protocol (PAgP) for automatic configuration. Similarly, Link Aggregation Group Protocol (LACP) allows creation of Ethernet channeling with devices that conform to IEEE 802.3ad standard.
- Internet Group Management Protocol (IGMP) facilitates monitoring and management of multicast applications (such as e-learning and videoconferencing) while minimizing the performance impact of managing group membership information.

IPv6

- The Cisco Catalyst 3560 Series supports the IPv6 standard, which increases Internet global address space to accommodate the rapidly increasing number of users and applications that require unique global IP addresses.
- In addition to the larger address space, the Cisco Catalyst 3560 Series switches also make the most of other IPv6 features such as address autoconfiguration, embedded IP Security (IPSec), routing optimized for mobile devices, and Duplicate Address Detection.

Advanced Quality of Service

Cisco Catalyst intelligent switches offer industry-leading QoS features to prioritize critical traffic and applications thereby avoid bottlenecks. These features bring new levels of control, predictability, and adaptability to networks of all sizes:

- The Cisco Catalyst 3560 Series can identify traffic flows or traffic groups, and classify or reclassify these groups using Differentiated Services Code Point (DSCP) in the IP packet and the 802.1p class of service (CoS) field in the Ethernet packet.
- Users can mitigate DoS attacks by assigning a minimal bandwidth queue to "scavenger traffic" or unimportant traffic used for peer-to-peer media sharing, gaming, or any entertainment video applications. This reduces scavenger traffic during periods of congestion, but allows it to be available if bandwidth is not being used for business purposes, for example during off-peak hours.
- Rate limiting gives control over the amount of bandwidth across any configured interface, for appropriate distribution of available bandwidth.
- Four egress queues help network administrators to be more discriminating and specific in assigning priorities for the various applications on the LAN. Scheduling is performed in egress to assign the appropriate queues to the outgoing packets.
- Shaped Round Robin (SRR) scheduling helps ensure differential prioritization of packet flows by intelligently servicing the ingress queues and egress queues.
- Weighted Tail Drop (WTD) provides congestion avoidance at the ingress and egress queues before a disruption occurs.
- 64 policers per 10/100 or Gigabit Ethernet port used to allocate bandwidth based on source/destination (IP address, MAC address) or TCP/UDP port numbers.

CISCO CATALYST 3560 SERIES SWITCHES

Each model is available with the IP Base or the IP Services software loaded on it. All models can later be updated to the IP Advanced Services software.

Table 1 lists the switches currently available in the Cisco Catalyst 3560 Series.

Table 1. Cisco Catalyst 3560 Series Switches

Product	Port Speed	Number of Ports	Uplinks	When to Buy
Cisco Catalyst 3560-8PC	10/100 with IEEE 802.3af and Cisco prestandard PoE	8	1 dual-purpose 10/100/1000 and Small Form-Factor Pluggable (SFP) port	For deployments outside the wiring closet requiring low-density access with PoE
Cisco Catalyst 3560-24TS	10/100	24	2 SFP-based ports	For networks requiring low-density access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560-48TS	10/100	48	4 SFP-based ports	For networks requiring medium-density access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560-24PS	10/100 with IEEE 802.3af and Cisco prestandard PoE	24	2 SFP-based ports	For networks requiring low-density access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560-48PS	10/100 with IEEE 802.3af and Cisco pre-standard PoE	48	4 SFP-based ports	For networks requiring medium-density access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560G-24TS	10/100/1000	24	4 SFP-based ports	For networks requiring low-density 10/100/1000 access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560G-24PS	10/100/1000 with IEEE 802.3af and Cisco prestandard PoE	24	4 SFP-based ports	For networks requiring low-density 10/100/1000 access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560G-48TS	10/100/1000	48	4 SFP-based ports	For networks requiring medium-density 10/100/1000 access, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks
Cisco Catalyst 3560G-48PS	10/100/1000 with IEEE 802.3af and Cisco prestandard PoE	48	4 SFP-based ports	For networks requiring medium-density 10/100/1000 access, PoE, Layer 2+ features with optional advanced IP routing, and one or more fiber uplinks

FOR MORE INFORMATION

For more information, please visit http://www.cisco.com/go/catalyst3560 .

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C02-379065-00 11/06

ANEXO 15

ANEXO 15

NEWNETWORKS S.A.

INFORMATICA Y TELECOMUNICIONES

Urbanización Albán Borja, Condominio La Tienda 3 Local L, 2do Piso ✆ 2200-894/2200-895

Guayaquil, 29 de Junio del 2007

Srta.
Andrea Pages
TRANS-TELCO
Ciudad

De mis consideraciones:

Por medio de la presente pongo a su consideración la siguiente oferta, según lo conversado:

Artículo	Cantidad	Precio Unitario	Valor Total
Access Point AT-WA7400 Allied Telesis	1	USD 349	USD 349

Condiciones Comerciales:

Tiempo de entrega: 7 días contados a partir de la recepción de la orden de compra

Forma de Pago: 70% como anticipo
30% contra entrega

Impuestos: No incluidos

Esperando contar con vuestra aprobación para participar en proyectos conjuntos en los que pondremos a su servicio nuestras habilidades.

Muy Atentamente,

Rogelio Armijos

ANEXO 15

AT-WA7400
Enterprise wireless access point

AT-WA7400
Enterprise wireless access point

Features

- Secure information transmission with 40-128 bit
- Wired Equivalent Privacy (WEP) data encryption
- In excess of 153 metres transmission distances
- IP tunnelling
- Wireless bridging
- Telnet and SNMP web GUI management
- Long range antennas available
- Dual speed access point
- Dual radio slot
- IEEE 802.11a, 802.11b, 802.11g
- and 802.11i standard support
- IP54 enclosure (AT-WA7501 only)
- WiFi and WPA certified
- Power over Ethernet capable
- Multiple SSID and Virtual LAN (VLAN) on each radio
- Secure Fast Roaming on patented Wireless Spanning
- Tree Technology

ANEXO 16

ANEXO 16

Guayaquil, 21 de Agosto de 2007

Señores
UTEG
Att. Andrea Pagés
Presente

De mis consideraciones

A continuación el costo de lo solicitado.

Ítem	Cantidad	Descripción	Precio Unitario	Total
1	1	1 WAN, 1 LAN, 16 FXO	1471	$ 1.471,00
2	89	1 LAN, 2 Users SIP, LCD (Linksys Sipura 841)	100	$ 8.900,00
3	1	IPPBX SERVER	2500	$ 2.500,00
4	1	Instalación Central Telefónica	1000	$ 1.000,00

Subtotal	$ 13.871,00
IVA	$ 1.664,52
TOTAL	$ 15.535,52

Por la atención a la presente, anticipo mis agradecimientos

Atentamente

Ing. Martin Correa
Gerente General

Ceibos Norte Los Corales # 3 Guayaquil – Ecuador
Telefax 5934 6001999 www.telered.ec

ANEXO 16

Caracteristicas

Linksys - Sipura SPA-841 SIP VoIP Phone

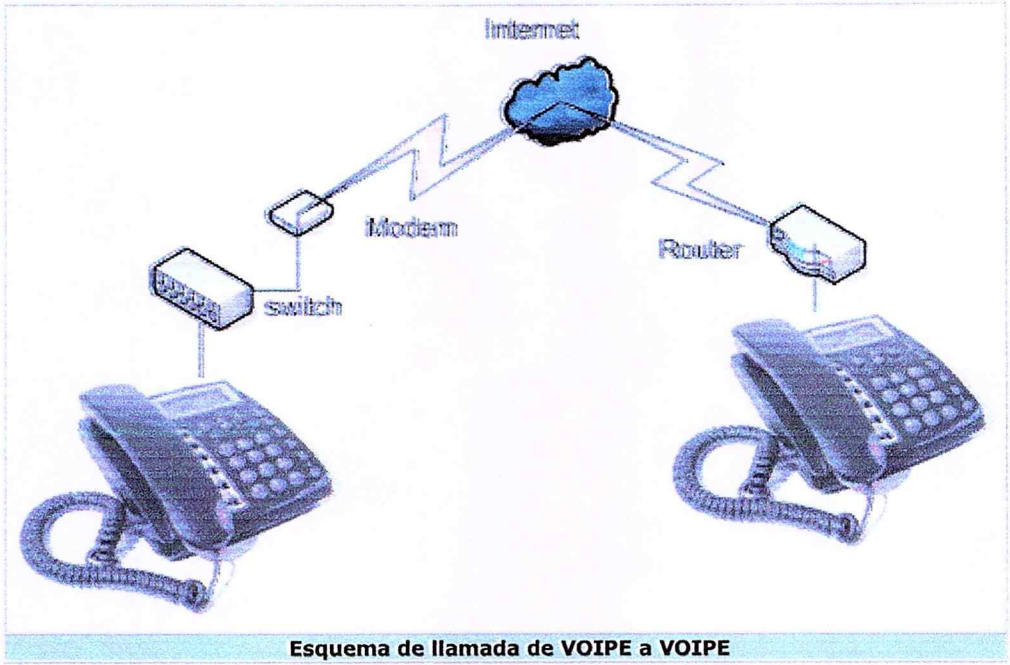
Una de las mejores opciones que tienes para comunicarte hacia cualquier parte del mundo es por medio del nuevo teléfono Sipura de Voipe. Tan solo conéctalo al switch, MODEM o router y podrás hablar todo el tiempo que quieras e ilimitadamente. El teléfono Sipura SPA-841 IP puede ser configurado con 2 líneas o con 4 si tiene un upgrade vía software. Puede ser usado en residencias, empresas y negocios grandes incluyendo servicios como PBX y CENTREX IP. Este modelo es uno de los favoritos en el mercado por su tecnología de fabricación y eficiencia en su calidad de voz.

Beneficios

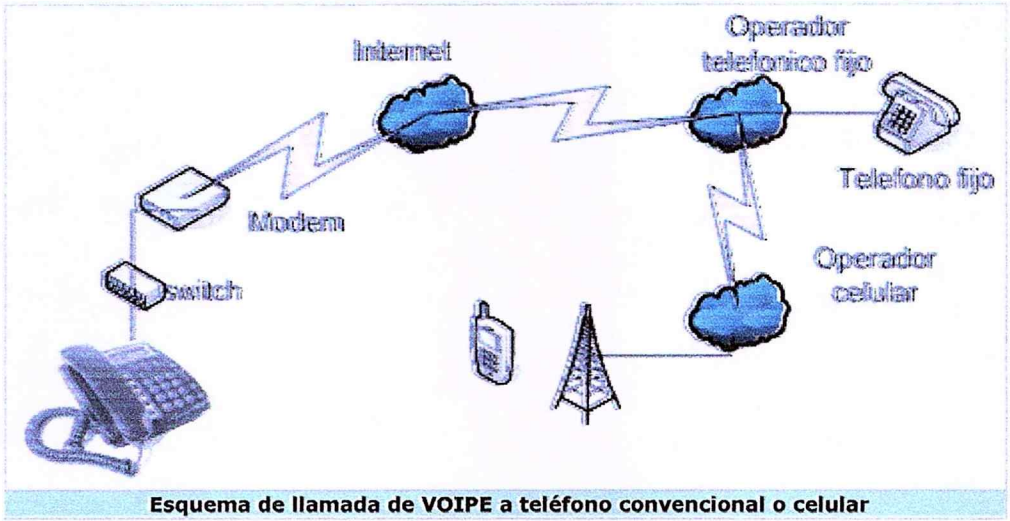
- Puedes comunicarte con quien quieras desde cualquier parte del mundo completamente gratis con el teléfono Linksys Sipura IP de Voipe, comunicándote a través de Internet hacia otro teléfono IP.
- Si deseas realizar llamadas internacionales a cualquier teléfono convencional o celular desde cualquier parte del mundo lo puedes hacer activando tu Linksys Sipura IP con los nuevos planes telefónicos internacionales de Voipe.
- Soporta las siguientes especificaciones de tecnología telefónica: Identificador de llamadas, muestra u oculta, llamada en espera, espera y transferencia de llamada.
- Posee hasta 8 líneas virtuales para recibir esa cantidad de llamadas simultáneas, como que si fuera una PBX con su respectivo display donde podrás apreciar y realizar todas las configuraciones y programaciones que desees, para cambio de tono o coger llamadas en espera, ver el tiempo que duro una llamada, etc.

Ceibos Norte Los Corales # 3 Guayaquil – Ecuador
Telefax 5934 6001999 www.telered.ec

- Puedes realizar conferencias entre 3 personas al mismo tiempo por el mismo equipo.
- Una vez realizada la configuración inicial, el equipo se vuelve "conéctalo y úsalo" , es decir lo puedes llevar a cualquier parte, lo conectas donde exista acceso a Internet y puedes realizar llamadas con tu mismo número telefónico.



Esquema de llamada de VOIPE a VOIPE



Esquema de llamada de VOIPE a teléfono convencional o celular

El teléfono Sipura SPA-841 IP puede ser configurado con 2 líneas o con 4 si tiene un upgrade vía software. Puede ser usado en residencias, empresas y negocios grandes

incluyendo servicios como PBX y CENTREX IP. Este modelo es uno de los favoritos en el mercado por su tecnología de fabricación y eficiencia en su calidad de voz.

Características técnicas

- Soporta los protocolos SARP/RARP, ICMP, DNS, DHCP, NTP, TFTP
- Soporta doble línea, por tanto doble registro a los servidores de VOIPE.
- Soporta NAT traversal con redireccionamento a un outbound Proxy de VOIPE.
- Posee interoperabilidad con casi todos los teléfonos IP del mercado, y con los registros del Proxy/sip de la empresa VOIPE
- Posee un avanzado proceso de señalización digital para asegurar la alta fidelidad de sonido.
- Avanzado en el control de perdida de paquetes y retrazo de la señal.
- Soporta los codecs G.723.1 (5.3K/6.3K), G.729A/B, G.711 (a-law and u-law), G.726, G.728, and wide-band G.722 (Model 102D). Puede negociar el codec dinámicamente.
- Soporta las siguientes especificaciones de tecnología telefónica: Caller ID Display or Block, Call Waiting, Hold, TransfForward, FLASH, in-band and out-of-band DTMF (RFC2833), Dial Plans, off-hook auto dial, configurable emergency dialing (e.g., 911), early dial, click-to-dial
- Soporta comunicación full-duplex, cancelación de eco acústico, control de volumen, correo de voz con indicador, descargas de tonos, redial y call log.
- Soporta suppression de silencio, VAD (Voice Activity Detection), CNG (Comfort Noise Generation), Line Echo Cancellation (G.168), and AGC (Automatic Gain Control).
- Soporta autenticación DIGEST y encriptación usando MD5.
- Provee una facil configuración vía web, a través del protocolo http.
- Soporta 802.1Q VLAN, 802.1p y QoS (ToS, DiffServ, MPLS).
- Soporta fail-over SIP server and DNS server.
- Posee la capacidad de registrarse por un proxy de salida exterior a los servidores de VOIPE.

DATA SHEET

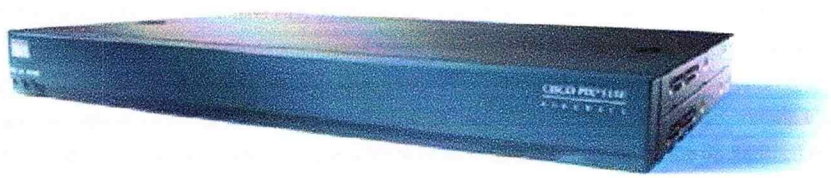
CISCO PIX 515E SECURITY APPLIANCE

The Cisco® PIX® 515E Security Appliance delivers a wealth of advanced security and networking services for small-to-medium business and enterprise networks, in a modular, purpose-built appliance. Its versatile one-rack unit (1RU) design supports up to six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with DMZ support.

Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 515E Security Appliance provides robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of rich security and networking services, including:

- **Advanced Application-Aware Firewall Services**
- **Market-Leading Voice-Over-IP and Multimedia Security**
- **Robust Site-to-Site and Remote Access IPSec VPN Connectivity**
- **Award-Winning Resiliency**
- **Intelligent Networking Services**
- **Flexible Management Solutions**

Figure 1. Cisco PIX 515E Security Appliance



ADVANCED FIREWALL SERVICES DELIVER STRONG BUSINESS PROTECTION AND RICH APPLICATION CONTROL

Robust Stateful Inspection and Application Layer Security

Cisco PIX Security Appliances integrate a broad range of advanced firewall services to protect businesses from the constant barrage of threats on the Internet and in many business network environments. As a secure foundation, Cisco PIX Security Appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access. Building upon those services, Cisco PIX Security Appliances deliver strong application layer security through 30 intelligent, application-aware inspection engines that examine network flows at Layers 4–7. To defend networks from application layer attacks and to give businesses more control over applications and protocols used in their environment, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL deobfuscation. These inspection engines also give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and protect network bandwidth for legitimate business applications.

INTELLIGENT NETWORKING SERVICES ENABLE SIMPLIFIED DEPLOYMENT AND SEAMLESS NETWORK INTEGRATION

Cisco PIX Security Appliances leverage over 20 years of Cisco Systems networking leadership and innovation to deliver a wide-range of intelligent networking services for seamless integration into today's diverse network environments. Administrators can easily integrate Cisco PIX Security Appliances into switched network environments by taking advantage of native 802.1q-based VLAN support. Cisco IP phone deployments can benefit from the "zero-touch provisioning" services provided by Cisco PIX Security Appliances, which help the phones automatically register with the appropriate Cisco CallManager and download any additional configuration information and software images. Businesses can improve their overall network resiliency by taking advantage of the robust Open Shortest Path First (OSPF) dynamic routing services provided by Cisco PIX Security Appliances, which can detect network outages within seconds and route around them. Mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services can be securely delivered using the comprehensive PIM-Sparse Mode v2 and Bidirectional-PIM routing support provided by Cisco PIX Security Appliances. Businesses can secure deployments of next-generation IPv6 networks using the advanced IPv6 security services provided by Cisco PIX Security Appliances, while simultaneously securing existing IPv4 environments with the same appliance during the transition period towards an IPv6 infrastructure.

FLEXIBLE MANAGEMENT SOLUTIONS LOWER OPERATIONAL COSTS

The Cisco PIX 515E Security Appliance delivers a wealth of configuration, monitoring, and troubleshooting methods, giving businesses flexibility to use the methods that best meet their needs. Management solutions range from centralized, policy-based management tools to integrated, Web-based management, to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Security Appliances additionally provide up to 16 levels of customizable administrative roles, so that businesses can grant administrators and operations personnel the appropriate level of access to each appliance, for example: monitoring only access, read-only access to the configuration, network configuration only, firewall configuration only, and so on.

Next-Generation Centralized Management Solutions

Administrators can easily manage large numbers of Cisco PIX Security Appliances using CiscoWorks VPN/Security Management Solution (VMS). This suite consists of several integrated software modules including Management Center for Firewalls, Auto Update Server Software, and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- Intelligent discovery and optimization of security policies and object groups
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Attack Mitigation and Event Monitoring Solutions

Network-based attacks can be easily and accurately identified, managed, and eliminated within commercial or enterprise environments using the Cisco Security Monitoring, Analysis, and Response System (CS-MARS) product family. CS-MARS appliances analyze and correlate security events, syslog, and NetFlow data from numerous desktop, server, and network security solutions to determine actual attack paths and provide mitigation options, simplifying security incident management for environments where dedicated security analysts may not be available.

Additionally, Cisco offers the CiscoWorks Security Information Management Solution (CWSIMS), which is well suited for large enterprises and managed security services providers with dedicated security analysts who require in-depth data collection, forensic analysis, audit and compliance, and reporting for complex, multi-vendor networks.

World-Class Device Management Solutions

The integrated Cisco Adaptive Security Device Manager (ASDM) provides a world-class Web-based management interface that greatly simplifies the deployment, on-going configuration, and monitoring of a single Cisco PIX Security Appliance—without requiring any software (other than a standard Web browser and Java Plug-In) to be installed on an administrator's computer. Intelligent setup and VPN wizards provide easy integration into any network environment, while informative monitoring features, including a dashboard and real-time syslog viewer, provide vital device/network health status and event monitoring at a glance.

Alternatively, administrators can remotely configure, monitor, and troubleshoot their Cisco PIX Security Appliances using a command-line interface (CLI). Secure CLI access is available using several methods, including Secure Shell (SSHv2) Protocol, Telnet over IPSec, and out of band through a console port.

Table 1. Product Features and Benefits

Features	Benefit
Reliable and Expandable Security Appliance	
Purpose-Built Security Appliance	• Uses a proprietary, hardened operating system that eliminates the security risks associated with general-purpose operating systems • Combines Cisco product quality with no moving parts to provide a highly reliable security platform
Fast Ethernet Expansion Options	• Supports easy installation of additional network interfaces two PCI expansion slots • Supports expansion cards including single-port Fast Ethernet and four-port Fast Ethernet cards
Hardware VPN Acceleration	• Delivers high speed VPN services through the addition of either a VPN Accelerator Card (VAC) or a VPN Accelerator Card+ (VAC+)—Unrestricted (UR), Failover (FO) and Failover-Active/Active (FO-AA) models have integrated hardware VPN acceleration services
Integration with Leading Third-Party Solutions	• Supports the broad range of Cisco Technology Developer partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Industry Certifications and Evaluations	• Earned numerous leading industry certifications and evaluations, including: – Common Criteria Evaluated Assurance Level 4 (EAL4) – ICSA Labs Firewall 4.0 Certification, Corporate RSSP Category – Network Equipment Building Standards (NEBS) Level-3 Compliant
Advanced Firewall Services	
Stateful Inspection Firewall	• Provides wide-range of perimeter network security services to prevent unauthorized network access • Delivers robust stateful inspection firewall services which track the state of all network communications • Provides flexible access-control capabilities for more than 100 predefined applications, services, and protocols, with the ability to define custom applications and services • Supports inbound/outbound ACLs for interfaces, time-based ACLs, and per-user/per-group policies for improved control over network and application usage • Simplifies management of security policies by giving administrators the ability to create re-usable network and service object groups that can be referenced by multiple security policies, simplifying initial policy definition and ongoing policy maintenance

Features	Benefit
Advanced Application and Protocol Inspection	• Integrates 30 specialized inspection engines that provide rich application control and security services for protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Extended Simple Mail Transfer Protocol (ESMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), Internet Control Message Protocol (ICMP), SQL*Net, Network File System (NFS), H.323 Versions 1-4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), GPRS Tunneling Protocol (GTP), Internet Locator Service (ILS), Sun Remote Procedure Call (RPC), and many more
Modular Policy Framework	• Provides a powerful, highly flexible framework for defining flow- or class-based policies, enabling administrators to identify a network flow or class based on a variety of conditions, and then apply a set of customizable services to each flow/class • Improves control over applications by introducing ability to have flow- or class-specific firewall/inspection policies, QoS policies, connection limits, connection timers, and more
Security Contexts	• Enables creation of multiple security contexts (virtual firewalls) within a single Cisco PIX Security Appliance, with each context having its own set of security policies, logical interfaces, and administrative domain • Supports one licensed level of security contexts: 5 (maximum number of security contexts supported based on model of Cisco PIX Security Appliance) • Provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance or failover pair, yet retaining the ability to manage each of these virtual instances separately • Enables service providers to deliver resilient multi-tenant firewall services with a pair of redundant appliances
Layer 2 Transparent Firewall	• Supports deployment of a Cisco PIX Security Appliance in a secure Layer 2 bridging mode, providing rich Layer 2—7 firewall security services for the protected network while remaining "invisible" to devices on each side of it • Simplifies Cisco PIX Security Appliance deployments in existing network environments by not requiring businesses to re-address the protected networks • Supports creation of Layer 2 security perimeters by enforcing administrator defined Ethertype-based access control policies for Layer 2 network traffic
Multi-Vector Attack Protection	• Provides wealth of advanced attack protection services to defend businesses from many popular forms of attacks, including denial-of-service (DoS) attacks, fragmented attacks, replay attacks, and malformed packet attacks • Delivers advanced TCP stream reassembly and traffic normalization services to assist in detecting hidden application and protocol layer attacks • Integrates with Cisco Network Intrusion Prevention System (IPS) solutions to identify and dynamically block or shun hostile network nodes
Authentication, Authorization, and Accounting (AAA) Support	• Integrates with popular AAA services via TACACS+ and RADIUS, with support for redundant servers for increased AAA services resiliency • Provides highly flexible user and administrator authentication services, dynamic per-user/per-group policies, and administrator privilege control through tight integration with Cisco Secure Access Control Server (ACS)

Features	Benefit
Robust IPSec VPN Services	
Cisco Easy VPN Server	• Delivers feature-rich remote access VPN concentrator services for up to 2000 remote software- or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions (such as the Cisco VPN Client) upon connection, helping to ensure that the latest corporate VPN security policies are used • Performs VPN client security posture checks when a VPN connection attempt is received, including enforcing usage of authorized host-based security products (such as the Cisco Security Agent) and verifying its version number and status prior to letting the remote user access the corporate network • Provides administrators precise control over what different types of VPN clients (software client, router, VPN 3002, and PIX) are allowed to connect based on type of client, operating system installed, and version of VPN client software • Supports automatic software updates of Cisco VPN Clients and Cisco 3002 Hardware VPN Clients, with the ability to trigger updates when VPN connections are established, or on-demand for currently connected VPN clients • Extends VPN reach into environments using NAT or Port Address Translation (PAT), via support of a variety of TCP and UDP-based NAT traversal methods including the Internet Engineering Task Force (IETF) draft standard
Cisco VPN Client	• Includes a free unlimited license for the highly acclaimed, industry-leading Cisco VPN Client • Available on wide-range of platforms including Microsoft Windows 98, ME, NT, 2000, XP; Sun Solaris; Intel-based Linux distributions; and Apple Macintosh OS X • Provides many innovative features including dynamic security policy downloading from Cisco Easy VPN Server-enabled products, automatic failover to backup Easy VPN Servers, administrator customizable distributions, and more • Integrates with the award-winning Cisco Security Agent (CSA) for comprehensive endpoint security
Site-to-Site VPN	• Supports IKE and IPSec VPN standards • Extends networks securely over the Internet by helping to ensure data privacy, data integrity, and strong authentication with remote networks and remote users • Improves network reliability and performance through support of OSPF dynamic routing and reverse-route injection over site-to-site VPN tunnels • Supports 56-bit DES, 168-bit 3DES, and up to 256-bit AES data encryption
Native Integration with Popular User Authentication Services	• Provides convenient method for authenticating VPN users through native integration with popular authentication services including Microsoft Active Directory, Microsoft Windows Domains, Kerberos, LDAP, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server to act as an intermediary)
X.509 Certificate and CRL Support	• Supports Simple Certificate Enrollment Protocol (SCEP)-based enrollment and manual enrollment with leading X.509 solutions from Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign • Interoperates with large-scale Public Key Infrastructure (PKI) deployments through n-tiered certificate hierarchy support

Features	Benefit
Resilient Architecture	
Active/Active and Active/Standby Stateful Failover	• Ensures resilient network protection for businesses through the award-winning high availability services provided by certain models of Cisco PIX 515E Security Appliances • Supports Active/Standby failover services as a cost-effective high availability solution, where one failover pair member operates in hot-standby mode acting as a complete redundant system that maintains current session state information for the active unit • Delivers advanced Active/Active failover services where both Cisco PIX Security Appliances in a failover pair actively pass network traffic simultaneously and share state information bi-directionally, enabling support for asymmetric routing environments and effectively doubling the throughput of the failover pair for bursty network traffic conditions • Supports long-distance failover enabling geographic separation of failover pair members, providing another layer of protection
VPN Stateful Failover	• Maximizes VPN connection uptime with new Active/Standby stateful failover for VPN connections • Synchronizes all security association (SA) state information and session key material between failover pair members, providing a highly resilient VPN solution **Note:** This feature is available on Unrestricted (UR), Failover (FO), and Failover-Active/Active (FO-AA) models only.
Zero-Downtime Software Upgrades	• Enables businesses to perform software maintenance release upgrades on Cisco PIX Security Appliance failover pairs without impacting network uptime or connections through the support of state-sharing between mixed Cisco PIX Security Appliance Software versions (running version 7.0(1) or higher)
Intelligent Networking Services	
VLAN-Based Virtual Interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking, with support for multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 25 total VLANs on Cisco PIX 515E Security Appliances
QoS Services	• Delivers per-flow, policy-based QoS services, with support for LLQ and traffic policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications • Enables businesses to have end-to-end QoS policies for their extended network

Features	Benefit
OSPF Dynamic Routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
PIM Multicast Routing	• Streamlines the delivery of multimedia traffic in video-conferencing, collaborative computing, and mission critical real-time enterprise applications through full PIM-Sparse Mode v2 and Bidirectional-PIM routing support (based on world-class Cisco IOS multicast technology)
IPv6 Networking	• Provides access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4/IPv6 network environments through dual-stack support • Delivers IPv6-enabled inspection services for HTTP, FTP, SMTP, ICMP, TCP, and UDP-based applications • Supports SSHv2, telnet, HTTP/HTTPS, and ICMP-based management over IPv6
Dynamic Host Control Protocol (DHCP) Client and Server	• Obtains IP address for outside interface of appliance automatically from service provider • Provides DHCP server services on one or more interfaces, allowing devices to obtain IP addresses dynamically • Includes extensions for automated provisioning of Cisco IP phones and Cisco SoftPhone IP telephony solutions
DHCP Relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking and maintenance of IP addresses
NAT/PAT Support	• Provides rich dynamic, static, and policy-based NAT, and PAT services
Flexible Management Solutions	
CiscoWorks VPN/Security Management Solution (VMS)	• Provides a comprehensive management suite for large scale Cisco security product deployments • Integrates policy management, software maintenance and security monitoring in a single management console
Cisco Adaptive Security Device Manager (ASDM)	• World-class Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides a wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events

Features	Benefit
Auto Update	• Provides "touchless" secure remote management of Cisco PIX Security Appliance configuration and software images via a unique "push/pull" management model • Next-generation secure Extensible Markup Language (XML) over HTTPS management interface can be used by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment and monitoring • Integrates with CiscoWorks Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)
Cisco PIX Command Line Interface (CLI)	• Allows customers to use existing Cisco IOS Software CLI knowledge for easy installation and management without additional training • Supports improved ease-of-use with services such as command completion, context-sensitive help, and command aliasing • Accessible through variety of methods including console port, Telnet, and SSHv2
Command-Level Authorization	• Gives businesses the ability to create up to 16 customizable administrative roles/profiles for managing a Cisco PIX Security Appliance (monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, etc.) • Uses either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and Syslog Support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications • Supports Cisco IPSec Flow Monitoring SNMP MIB, providing a wealth of VPN flow statistics including tunnel uptime, bytes/packets transferred, and more

LICENSE OPTIONS

The Cisco PIX 515E Security Appliance is available in four primary models that provide different levels of interface density, failover capabilities, and VPN throughput. Optional licenses support enabling features including security contexts, GTP inspection, and various strengths of encryption technology.

Platform Licenses

Restricted Software License

The Cisco PIX 515E Restricted (PIX 515E-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with minimal interface density and VPN throughput requirements. It includes 64 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for one additional 10/100 Fast Ethernet interface.

Unrestricted Software License

The PIX 515E Unrestricted (PIX 515E-UR) model extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 128 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to four additional 10/100 Fast Ethernet interfaces. The Cisco PIX 515E-UR also adds the ability to share state information with a secondary Cisco PIX Security Appliance (either in an Active/Active or Active/Standby deployment model) for resilient network protection.

Failover Active/Standby Software License

The Cisco PIX 515E "Failover" (PIX 515E-FO) model is designed for use in conjunction with a PIX 515E-UR, providing a cost-effective, Active/Standby high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 515E-UR, it delivers the ultimate in high availability for a fraction of the price.

Failover Active/Active Software License

The Cisco PIX 515E Failover Active/Active (PIX 515E-FO-AA) model is designed for use in conjunction with a PIX 515E-UR, providing a scalable Active/Active high-availability solution. Advanced network topologies, such as those with asymmetric routing, are supported through the Active/Active architecture where both Cisco PIX Security Appliances pass network traffic and exchange bi-directional state sharing updates with one another. This license is supported by Cisco PIX Security Appliance Software v7.0 and higher. License upgrades are available for existing PIX 515E-FO units to convert from Active/Standby to Active/Active failover.

Feature Licenses

Security Context Licenses

The Cisco PIX 515E Security Appliance can support up to 5 security contexts, with each context having its own separate security policies and administrative domain. One tier of security context licensing is available for Cisco PIX 515E Security Appliances—5 security contexts. This license is supported by Cisco PIX Security Appliance Software v7.0 and higher, and requires an Unrestricted (UR), Failover (FO), or Failover Active/Active (FO-AA) license—security contexts are not supported on Restricted (R) models.

GTP Inspection License

The Cisco PIX 515E Security Appliance can provide advanced security services for GTP/GPRS 3G Mobile Wireless environments upon installation of the GTP Inspection License. This license is supported by Cisco PIX Security Appliance Software v7.0 and higher, and requires either an Unrestricted (UR), Failover (FO), or Failover Active/Active (FO-AA) license—GTP inspection is not supported on Restricted (R) models.

Encryption License

3DES/AES and DES Encryption Licenses

The Cisco PIX 515E Security Appliance has two optional encryption licenses—one license (PIX-VPN-3DES) enables 168-bit 3DES and up to 256-bit AES encryption, the other license (PIX-VPN-DES) enables 56-bit DES encryption. Both are available either at the time of ordering the Cisco PIX 515E Security Appliance, or can be obtained subsequently through Cisco.com. Note that an encryption license must be installed to activate encryption services which are required before using certain features including VPN and secure remote management.

PERFORMANCE SUMMARY

- Cleartext throughput: Up to 190 Mbps
- Concurrent connections: 130,000
- 168-bit 3DES IPSec VPN throughput: Up to 135 Mbps with VAC+ or 63 Mbps with VAC
- 128-bit AES IPSec VPN throughput: Up to 130 Mbps with VAC+
- 256-bit AES IPSec VPN throughput: Up to 130 Mbps with VAC+
- Simultaneous VPN tunnels: 2000

TECHNICAL SPECIFICATIONS

- Processor: 433-MHz Intel Celeron Processor
- Random access memory: 64 MB or 128 MB of SDRAM
- Flash memory: 16 MB

- Cache: 128 KB level 2 at 433 MHz
- System bus: Single 32-bit, 33-MHz PCI

ENVIRONMENTAL OPERATING RANGES

Operating

- Temperature: -25° to 131°F (-5° to 55°C)
- Relative Humidity: 5% to 95% noncondensing
- Altitude: 0 to 9843 ft (3000 m)
- Shock: 1.14 m/sec (45 in./sec) 1/2 sine input
- Vibration: 0.41 Grms2 (3-500 Hz) random input
- Acoustic Noise: 45 dBa maximum

Nonoperating

- Temperature: -13° to 158°F (-25° to 70°C)
- Relative Humidity: 5% to 95% noncondensing
- Altitude: 0 to 15,000 ft (4570 m)
- Shock: 30 G
- Vibration: 0.41 Grms2 (3-500 Hz) random input

POWER

Input (Per Power Supply)

- Range Line Voltage: 100V to 240V AC or 48V DC
- Nominal Line Voltage: 100V to 240V AC or 48V DC
- Current: 1.5 Amps
- Frequency: 50 to 60 Hz, single phase

Output

- Steady State: 50W
- Maximum Peak: 65W
- Maximum Heat Dissipation: 410 BTU/hr, full power usage (65W)

PHYSICAL SPECIFICATIONS

Dimensions and Weight Specifications

- Form factor: 1 RU, standard 19-in. rack mountable
- Dimensions (H x W x D): 1.72 x 16.82 x 11.8 in (4.37 x 42.72 x 29.97 cm)
- Weight (one power supply): 11 lb (4.11 kg)

Expansion

- Two 32-bit/33-MHz PCI slots
- Two 168-pin DIMM RAM slots, supporting up to 64 MB memory maximum

Interfaces

- Console Port: RS-232, 9600 bps, RJ45
- Failover Port: RS-232, 115 Kbps, DB-15 (special PIX failover cable required)
- Two integrated 10/100 Fast Ethernet interfaces, auto-negotiate (half/full duplex), RJ45

REGULATORY AND STANDARDS COMPLIANCE

Safety

UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR1040

Electro Magnetic Compatibility (EMC)

FCC Part 15 (CFR 47) Class A, ICES-003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

PRODUCT ORDERING INFORMATION

Table 2 lists ordering information for the Cisco PIX 515E Security Appliances and related products.

Table 2. Ordering Information

PIX-515E	PIX 515E Chassis (chassis, software, 2 10/100 interfaces)
PIX-515E-DC	PIX 515E DC Chassis (chassis, software, 2 10/100 interfaces)
PIX-515E-R-BUN	PIX 515E Restricted Bundle (chassis, restricted license, software, 2 10/100 interfaces, 64 MB RAM)
PIX-515E-R-DMZ-BUN	PIX 515E DMZ Bundle (chassis, restricted license, software, 3 10/100 interfaces, 64 MB RAM)
PIX-515E-UR-BUN	PIX 515E Unrestricted Bundle (chassis, unrestricted license, software, 2 10/100 ports, 128 MB RAM, VAC or VAC+)
PIX-515E-UR-FE-BUN	PIX 515E Unrestricted 6-port Fast Ethernet Bundle (chassis, unrestricted license, software, 6 10/100 ports, 128 MB RAM, VAC or VAC+)
PIX-515E-FO-BUN	PIX 515E Active/Standby Failover Bundle (chassis, Active/Standby failover license, software, 2 10/100 interfaces, 128 MB RAM, VAC or VAC+)
PIX-515E-FO-FE-BUN	PIX 515E Active/Standby Failover 6-port Fast Ethernet Bundle (chassis, Active/Standby failover license, software, 6 10/100 interfaces, 128 MB RAM, VAC or VAC+)
PIX-515E-AA-FE-BUN	PIX 515E Active/Active Failover 6-port Fast Ethernet Bundle (chassis, Active/Active failover license, software, 6 10/100 interfaces, VAC or VAC+)
PIX-515E-DC-R-BUN	PIX 515E DC Restricted Bundle (chassis, restricted license, software, 2 10/100 interfaces, 64 MB RAM)
PIX-515E-DC-UR-BUN	PIX 515E DC Unrestricted Bundle (chassis, unrestricted license, software, 2 10/100 interfaces, 128 MB RAM, VAC or VAC+)
PIX-515E-DC-FO-BUN	PIX 515E DC Active/Standby Failover Bundle (chassis, Active/Standby failover license, software, 2 10/100 interfaces, 128 MB RAM, VAC or VAC+)
PIX-515E-HW=	PIX 515E rack mount kit, console cable, failover cable
PIX-FO=	PIX failover cable

PIX-4FE-66	PIX 64-bit/66-MHz 4-port 10/100 Fast Ethernet interface card, RJ45
PIX-1FE	PIX single-port 10/100 Fast Ethernet interface card
PIX-VPN-ACCEL	PIX DES/3DES VPN Accelerator Card (VAC)
PIX-VAC-PLUS	PIX DES/3DES/AES VPN Accelerator Card+ (VAC+)
PIX-SW-SC-5	Cisco PIX 5 security contexts license
PIX-SW-GTP	Cisco PIX GTP/GPRS inspection license
PIX-515-VPN-3DES	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-DES	56-bit DES encryption software license

SUPPORT SERVICES

Support services are available from Cisco and Cisco partners. Cisco SMARTnet® service augments customer support resources, and provides anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

SUPPORT ORDERING INFORMATION

Table 3 lists ordering information for Cisco SMARTnet support services.

Table 3. Cisco SMARTnet Ordering Information

CON-SNT-PIX515E	Cisco SMARTnet 8x5xNBD service for PIX 515E chassis only
CON-SNT-PIX515ER	Cisco SMARTnet 8x5xNBD service for PIX 515E-R bundle
CON-SNT-PIX515EUR	Cisco SMARTnet 8x5xNBD service for PIX 515E-UR bundle
CON-SNT-PIX515EFE	Cisco SMARTnet 8x5xNBD service for PIX 515E-UR-FE bundle
CON-SNT-PIX515EFO	Cisco SMARTnet 8x5xNBD service for PIX 515E-FO bundle
CON-SNT-PIX515EFF	Cisco SMARTnet 8x5xNBD service for PIX 515E-FO-FE bundle
CON-SNT-PIX515EAA	Cisco SMARTnet 8x5xNBD service for PIX 515E-FO-AA bundle
CON-SNTE-PIX515E	Cisco SMARTnet 8x5x4 service for PIX 515E chassis only
CON-SNTE-PIX515ER	Cisco SMARTnet 8x5x4 service for PIX 515E-R bundle
CON-SNTE-PIX515EUR	Cisco SMARTnet 8x5x4 service for PIX 515E-UR bundle
CON-SNTE-PIX515EFE	Cisco SMARTnet 8x5x4 service for PIX 515E-UR-FE bundle
CON-SNTE-PIX515EFO	Cisco SMARTnet 8x5x4 service for PIX 515E-FO bundle
CON-SNTE-PIX515EFF	Cisco SMARTnet 8x5x4 service for PIX 515E-FO-FE bundle

CON-SNTE-PIX515EAA	Cisco SMARTnet 8x5x4 service for PIX 515E-FO-AA bundle
CON-SNTP-PIX515E	Cisco SMARTnet 24x7x4 service for PIX 515E chassis only
CON-SNTP-PIX515ER	Cisco SMARTnet 24x7x4 service for PIX 515E-R bundle
CON-SNTP-PIX515EUR	Cisco SMARTnet 24x7x4 service for PIX 515E-UR bundle
CON-SNTP-PIX515EFE	Cisco SMARTnet 24x7x4 service for PIX 515E-UR-FE bundle
CON-SNTP-PIX515EFO	Cisco SMARTnet 24x7x4 service for PIX 515E-FO bundle
CON-SNTP-PIX515EFF	Cisco SMARTnet 24x7x4 service for PIX 515E-FO-FE bundle
CON-SNTP-PIX515EAA	Cisco SMARTnet 24x7x4 service for PIX 515E-FO-AA bundle
CON-OS-PIX515E	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E chassis only
CON-OS-PIX515ER	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E-R bundle
CON-OS-PIX515EUR	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E-UR bundle
CON-OS-PIX515EFE	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E-UR-FE bundle
CON-OS-PIX515EFO	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E-FO bundle
CON-OS-PIX515EFF	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E-FO-FE bundle
CON-OS-PIX515EAA	Cisco SMARTnet On-Site 8x5xNBD service for PIX 515E-FO-AA bundle
CON-OSE-PIX515E	Cisco SMARTnet On-Site 8x5x4 service for PIX 515E chassis only
CON-OSE-PIX515ER	Cisco SMARTnet On-Site 8x5x4 service for PIX 515E-R bundle
CON-OSE-PIX515EUR	Cisco SMARTnet On-Site 8x5x4 service for PIX 515E-UR bundle
CON-OSE-PIX515EFO	Cisco SMARTnet On-Site 8x5x4 service for PIX 515E-FO bundle
CON-OSE-PIX515EAA	Cisco SMARTnet On-Site 8x5x4 service for PIX 515E-AA bundle
CON-OSP-PIX515E	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E chassis only
CON-OSP-PIX515ER	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E-R bundle
CON-OSP-PIX515EUR	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E-UR bundle
CON-OSP-PIX515EFE	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E-UR-FE bundle
CON-OSP-PIX515EFO	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E-FO bundle
CON-OSP-PIX515EFF	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E-FO –FE bundle
CON-OSP-PIX515EAA	Cisco SMARTnet On-Site 24x7x4 service for PIX 515E-AA bundle

ADDITIONAL INFORMATION

For more information, please visit the following links.

Cisco PIX Security Appliance Series: http://www.cisco.com/go/pix

Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm

Current list of Cisco product security certifications: http://www.cisco.com/go/securitycert

Cisco Secure ACS: http://www.cisco.com/go/acs

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software and Security Monitor: http://www.cisco.com/go/vms

CiscoWorks SIMS: http://www.cisco.com/go/sims

SAFE Blueprint from Cisco: http://www.cisco.com/go/safe

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

204177.c_ETMG_MH_1.05

Printed in the USA

Cisco ASA 5520 Firewall Edition

El Cisco ASA 5520 aporta una amplia gama de servicios de seguridad, con alta disponibilidad Activo/Activo y conectividad Gigabit Ethernet para empresas medianas.

Costo $6,441.36

General

MPN: ASA5520-BUN-K9
Tipo de dispositivo: Aparato de seguridad
Altura (unidades de bastidor): 1U
Cantidad de módulos instalados (máx.): 0 (1)
Anchura: 44.5 cm
Profundidad: 33.5 cm
Altura: 4.4 cm
Peso: 9.1 kg

Procesador / memoria / almacenamiento

RAM instalada (máx.): 512 MB
Memoria flash instalada (máx.): 64 MB Flash

Conexión de redes

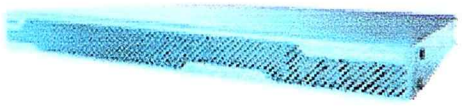
Factor de forma: Montable en bastidor
Tecnología de conectividad: Cableado
Protocolo de interconexión de datos: Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte: IPSec
Rendimiento:

- Capacidad del cortafuegos : 450 Mbps
- Capacidad de la VPN : 225 Mbps
- Tasa de conexiones : 9000 sesiones por segundo

Capacidad:

- Sesiones concurrentes : 280000
- Peers VPN IPSec : 750
- Peers VPN SSL : 2
- Interfaces virtuales (VLAN) : 100

Características: Protección firewall, VPN, equilibrio de carga, soporte VLAN
Algoritmo de cifrado: Triple DES, AES



Descripción del fabricante sobre el producto

El Cisco ASA 5520 aporta una amplia gama de servicios de seguridad, con alta disponibilidad Activo/Activo y conectividad Gigabit Ethernet para empresas medianas. Este modelo es capaz de ampliarse si el crecimiento de su negocio requiere ampliar la seguridad, facilitando así el regorno de la inversión. Suempresa puede extender su capacidad IPSec y SSL VPN para soportar mayor número de teletrabajadores y conexiones remotas. Puede duplicar la capacidad VPN sólo con instalar un upgrade de licencia VPN. Las aplicaciones del ASA 5520 pueden extenderse utilizando el Módulo de Servicios de Seguridad (SSM).

Expansión / conectividad

Total ranuras de expansión (libres):

- 1 (1) x Ranura de expansión
- 1 memoria

Interfaces:

- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x gestión - consola - RJ-45
- 2 x Hi-Speed USB - 4 PIN USB tipo A
- 1 x gestión - auxiliar - RJ-45
- 4 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45

Diverso

Cumplimiento de normas: CE, CISPR 22 Class A, EN 60950, EN 61000-3-2, UL 1950, VCCI Class A ITE, IEC 60950, EN 61000-3-3, CSA 22.2 No. 950, EN55022 Class A, AS/NZS 3260, AS/NZ 3548 Class A, FCC Part 15

Alimentación

Dispositivo de alimentación: Fuente de alimentación - interna
Voltaje necesario: CA 120/230 V (50/60 Hz)
Potencia suministrada: 190 vatios

Parámetros de entorno

Temperatura mínima de funcionamiento: 0 °C
Temperatura máxima de funcionamiento: 40 °C
Ámbito de humedad de funcionamiento: 5 - 95%

Ciao

Incluido en Ciao desde : 17/02/2006

ANEXO 19

HENTEL
YANEZ AVALOS CIA. LTDA.

COTIZACION Nro 6050

CLIENTE: *SRTA. ANDREA PAGES*
DIRECCION: *CDLA. LOS CEIBOS*
ATENCION:
TELEFONO: *2630335*

Fecha: *09-Mar-2007*
Validez: *8 dias*

Cantidad	Unidad	Producto	Precio Unitario	Desc%	Total Dólares
1	MTR	FIBRA OPTICA MM 4 HILOS 62,5/125 ARMADA LOOSE TOUBE MARCA NEWLINK	2.80	20%	2.24
305	MTR	CABLE UTP 4 PARES CAT6 MARCA QUEST	0.84	20%	204.96
1	UND	CONECTORES RJ-45 MARCA QUEST (FUNDA 100 UND)	30.00	20%	24.00
1	UND	CAJAS SOBREPUESTAS 40MM MARCA DEXSON	1.47	20%	1.18
1	UND	FACE PLATE 2P CON I.D. MARCA QUEST	1.44	20%	1.15
1	UND	JACK CAT6 MARCA QUEST	5.75	20%	4.60
1	UND	PATCH CORD 3FT CAT6 MARCA QUEST	4.41	20%	3.53
1	UND	PATCH CORD 7FT CAT6 MARCA QUEST	6.60	20%	5.28
1	UND	PATCH PANEL 24P SOLIDO CAT6 MARCA QUEST	177.00	20%	141.60
1	UND	MULTITOMA HORIZONTAL 4 TOMAS DOBLES MARCA BEAUOCUP	31.50	20%	25.20
1	UND	MULTITOMA VERTICAL 72" 8 TOMAS DOBLES MARCA BEAUOCUP	56.23	20%	44.98
1	UND	MULTITOMA VERTICAL 84" 12 TOMAS DOBLES MARCA BEAUOCUP	66.86	20%	53.49
1	UND	ORGANIZADOR HORIZONTAL 60X40 1UR MARCA BEAUCOUP	10.14	20%	8.11
1	UND	ORGANIZADOR HORIZONTAL 60X80 2UR MARCA BEAUCOUP	12.06	20%	9.65
1	UND	ORGANIZADOR VERTICAL 84" 80X80MM MARCA BEAUOCUP	39.56	20%	31.65
1	UND	BANDEJA ESTANDAR 19" MARCA BEAUCOUP	15.40	20%	12.32
1	UND	BANDEJA CORREDIZA PARA TECLADO MARCA BEAUCOUP	39.82	20%	31.86
1	UND	BANDEJA DE 4 PARANTES 450MM MARCA BEAUCOUP	28.49	20%	22.79
1	UND	BANDEJA TIPO FLEX GALVANIZADA 20X5X3	50.00	20%	40.00
1	UND	RACK DE PISO 72" (36UR) TUERCA REMACHADA MARCA BEAUCOUP	163.00	20%	130.40
1	UND	RACK DE PISO 84" (44UR) TUERCA REMACHADA MARCA BEAUCOUP	183.00	20%	146.40
1	UND	GABINETE DE PISO 72" 1804X604X754 MM MARCA BEAUCOUP	649.00	20%	519.20
1	UND	GABINETE DE PISO 72" 1804X804X1004 MM MARCA BEAUCOUP	814.00	20%	651.20
1	UND	GABINETE DE PISO 84" 2154X604X754 MM MARCA BEAUCOUP	726.00	20%	580.80
1	UND	GABINETE DE PISO 84" 2154X804X1004 MM MARCA BEAUCOUP	911.00	20%	728.80
1	UND	SOPORTE DE PARED DE 5UR MARCA BEAUCOUP	29.00	20%	23.20
1	UND	SOPORTE DE PARED DE 6UR MARCA BEAUCOUP	34.00	20%	27.20
1	UND	SOPORTE DE PARED DE 8UR MARCA BEAUCOUP	47.00	20%	37.60
1	UND	GABINETE DE PARED DE 6UR MARCA HIGHTECH	159.00	20%	127.20
1	UND	GABINETE DE PARED DE 10UR COMPACTO MARCA BEAUCOUP	179.00	20%	143.20
1	UND	GABINETE DE PARED DE 10UR ABATIBLE MARCA BEAUCOUP	239.00	20%	191.20
1	UND	CANALETA 20X12 MARCA DEXSON	1.22	20%	0.98
1	UND	CANALETA 32X12 MARCA DEXSON	1.96	20%	1.57
1	UND	CANALETA 40X25 MARCA DEXSON	4.55	20%	3.64
1	UND	ACCESORIOS PARA CANALETA 20X12 MARCA DEXSON	0.28	20%	0.22
1	UND	ACCESORIOS PARA CANALETA 32X12 MARCA DEXSON	0.39	20%	0.31
1	UND	ACCESORIOS PARA CANALETA 40X25 MARCA DEXSON	0.74	20%	0.59
1	UND	HERRAMIENTA UNIVERSAL 4,6,8 HILOS MARCA QUEST	50.00	20%	40.00
1	UND	HERRAMIENTA PONCHADORA TIPO 110 MARCA QUEST	45.00	20%	36.00
1	UND	LAN TESTER MARCA QUEST	81.36	20%	65.09
1	UND	ETIQUETADORA DE CABLES MARCA BRADY	176.00	20%	140.80
				Subtotal	4,261.94
				12% IVA	511.43
				TOTAL	**4,773.37**

NOTA: EL DESCUENTO PUEDE VARIAR DEPENDIENDO DEL MONTO DE LA COMPRA
FORMA DE PAGO: A CONVENIR

ATENTAMENTE

Glenda Alcivar M.
Gerente de Ventas Guayaquil
CIA HENTEL
Telf: 2295664-2295258

ANEXO 20

ANEXO 20

COTIZACIÓN PARA TÉSIS DE FIBRA ÓPTICA

Cantidad	*Características*	*P. Unitario*	*P. Total*
180	Metros de F.O. Multimodo 62.5/125 um, de 6 hilos	$ 3.65	$ 657.00
2	Patch panel para Fibra Óptica, Siemon (ODF)	$ 130.00	$ 260.00
2	Placa adaptadora de 6 puertos SC	$ 45.00	$ 90.00
4	Placa ciega para patch panel de F.O.	$ 15.00	$ 60.00
12	Pigtails SC, Multimodo 62.5/125 um	$ 20.00	$ 240.00
12	Fusiones de hilos de fibra óptica	$ 25.00	$ 300.00
2	MEDIA CONVERTER 2 Km, 10/100 Base - TX/FX 2 Km, SC	$ 180.00	$ 360.00
2	Patch cord de F.O.Multimodo 62.5/125 um SC/SC, 3 m.	$ 40.00	$ 80.00
2	Patch cord RJ-45 de 3 pies	$ 3.50	$ 7.00
1	Dirección Técnica: Incluye Mano de Obra, Tendido de Fibra Memorias Técnicas	$ 200.00	$ 200.00
		Sub - Total	$ 2,254.00
		IVA	$ 270.48
		Total	$ 2,524.48

NOTA.- Si si desea trabajar a 1000 Mbps, se deberá instalar convertidores de fibra óptica a 1000 o adquirir un switch que tenga slots para colocar módulos de fibra que hacen las veces de un convertidor de fibra óptica.

2	Con vertidor Gigabit 1000 Base-T to SX (SC Type)	$ 250.00	$ 500.00

2	Switch de 24 puertos RJ-45, con dos slots para fibra	$ 520.00	$ 1,040.00
2	Módulos de fibra LC a 1000 Mbps	$ 250.00	$ 500.00
2	Patch cord SC/LC de 3 metros	$ 70.00	$ 140.00

Si no desea realizar fusiones con los Pigtails, se podría hacer conectorizaciones para lo cual se deberán comprar conectores SC

12	Conectores SC Multimodo	$ 6.00	$ 72.00
12	Conectorizaciones de hilos de fibra óptica	$ 25.00	$ 300.00

ANEXO 20

COTIZACIÓN PARA TÉSIS DE FIBRA ÓPTICA

Cantidad	*Unidad*	*Descripción*	*Precio Un.*	*Precio total*
450	m	Fibra monomodo 12h aéreo	$ 2.40	$ 1,080.00
9	gb	Herrajes	$ 12.00	$ 108.00
2	u	Bandeja para FO tipo rack 24 puertos conector SC	$ 350.00	$ 700.00
24	u	Pigtail monomodo tipo SC	$ 15.00	$ 360.00
2	u	Patch cord 2m tipo SC monomodo duplex	$ 38.70	$ 77.40
450	m	Tendido de cable de FO	$ 0.60	$ 270.00
24	gb	Fusion de hilo de FO	$ 25.00	$ 600.00
24	gb	Mediciones con OTDR	$ 25.00	$ 600.00
			SUBTOTAL	$ 3,795.40






ANEXO 21

Guayaquil, 29 de Junio del 2007

Srta.
Andrea Pages
TRANS-TELCO
Ciudad

De mis consideraciones:

Por medio de la presente pongo a su consideración la siguiente cotizacion:

ITEM	DESCRIPCION	CANTIDAD	UNIDAD	VALOR	
1	FIBRA OPTICA MM 4 HILOS 62,5/125 ARMADA LOOSE TOUBE MARCA NEWLINK	1	M	2.80	
2	CABLE UTP CAT. 6 MARCA SIEMON	1	U	2.40	
3	PATCH PANEL DE 24 PUERTOS MODULAR	1	U	26.00	
4	JACK DE DATOA CAT. 5E	1	U	3.20	
5	CAJAS RECTANGULARES 40mm DEXON		U	1.40	
6	CABLE UTP CAT. 5E MARCA SIEMON	305	M	183.00	
7	CONECTORES RJ-45	1	U	0.35	
8	PATCH CORD 3M	1	U	3.00	
9	RACK 12UR	1	U	480.00	
10	ODF 6 PUERTOS	1	U	150.00	
11	FIBRA 6 HILOS MONOMODO	1	M	3.80	
12	PIGTAIL	1	U	30.00	
13	BANDEJA PORTAEMPALME	1	U	25.00	
14	FUSIÓN	1	U	20.00	
15	PROTECTORES DE FIBRA OPTICA	1	U	1.00	
16	TRANSCEIVER	1	U	180.00	
17	CISCO 831	1	U	290.00	
18	CISCO 1841 CON WIC 1T	1	U	1487	
19	CISCO 1601	1	U	200.00	
20	CATALYST 2960G 24 PUERTOS	1	U	1968.00	2662.00
21	MODULO DE FIBRA PARA SW	1	U	347.00	
22	SWITCH 3COM 24 PUERTOS	1	U	450.00	
23	PIX 501	1	U	382.00	
24	BANDEJAS PARA RACK	1	U	25.00	
	TOTAL			**6260.95**	

Muy Atentamente,

Paola Lizano
iseyco c.a.

Cisco 1800 Series Integrated Services Routers: Cisco 1841 Router (Modular)

Cisco Systems® is redefining best-in-class enterprise and small- to-medium-sized business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, and video services. Founded on 20 years of leadership and innovation, the modular Cisco® 1800 Series of integrated services routers (refer to Figure 1) intelligently embed data and security into a single, resilient system for fast, scalable delivery of mission-critical business applications. The best-in-class Cisco 1800 Series architecture has been specifically designed to meet requirements of small–to-medium-sized businesses, small enterprise branch offices, and service provider-managed services applications for delivery of concurrent services at wire-speed performance. The integrated secure systems architecture of the Cisco 1800 Series delivers maximum business agility and investment protection.

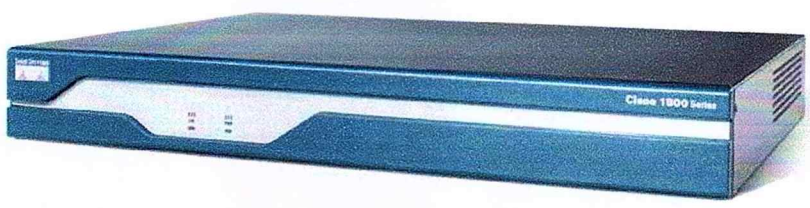
Product Overview

Cisco 1800 Series integrated services routers are the next evolution of the award-winning Cisco 1700 Series modular access routers. The Cisco 1841 router (Figure 1) is designed for secure data connectivity and provides significant additional value compared to prior generations of Cisco 1700 Series routers by offering more than a fivefold performance increase and integrated hardware-based encryption enabled by an optional Cisco IOS® Software security image. The Cisco 1841 dramatically increase interface card slot performance and density over the Cisco 1700 Series while maintaining support for more than 30 existing WAN interface cards (WICs) and multiflex trunk cards (voice/WICs [VWICs]—for data only on the Cisco 1841 router).

The Cisco 1841 router features secure, fast, and high-quality delivery of multiple, concurrent services for small-to-medium-sized businesses and small enterprise branch offices. The Cisco 1841 router offers embedded hardware-based encryption enabled by an optional Cisco IOS Software security image; further enhancement of VPN performance with an optional VPN acceleration module; an intrusion prevention system (IPS) and firewall functions; interfaces for a wide range of connectivity requirements, including support for optional integrated switch ports; plus sufficient performance and slot density for future network expansion and advanced applications as well as an integrated real-time clock.

Support of high-density WICs (HWICs) is optional.

Figure 1. Cisco 1800 Series Integrated Services Routers

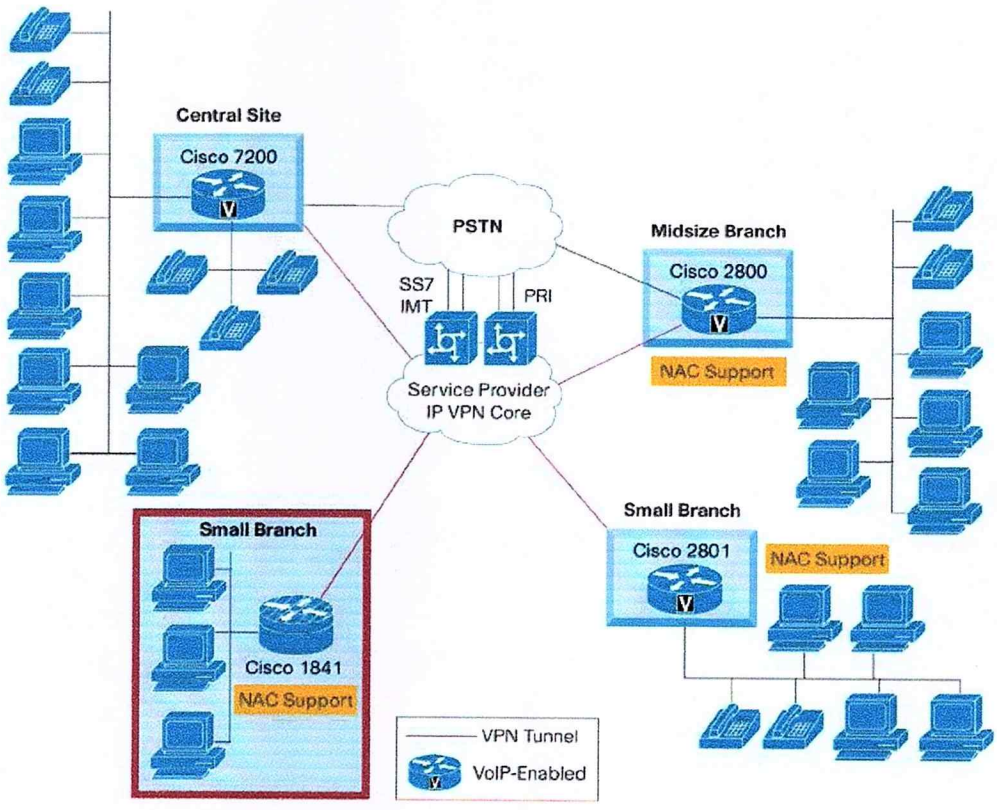


Applications

Secure Network Connectivity for Data

Security has become a fundamental building block of any network, and Cisco routers play an important role in embedding security at the customer's access edge. The Cisco IOS Software security feature sets for the Cisco 1841 router that enable the hardware-based encryption on the motherboard provide a robust array of features such as Cisco IOS Firewall, IPS support, IP Security (IPSec) VPNs (Digital Encryption Standard [DES], Triple DES [3DES], and Advanced Encryption Standard [AES]), SSL Web VPN, Dynamic Multipoint VPN (DMVPN), network admissions control (NAC) for antivirus defense, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMP) in one solution set. In addition, the Cisco 1841 router offers bundled network security solutions with IPSEC and SSL VPN encryption-acceleration modules, making it the industry's most robust and adaptable security solution available for small-to-medium-sized businesses and small enterprise branch offices. As Figure 2 demonstrates, the Cisco 1800 Series routers help enable customers to deliver high-performance, concurrent, mission-critical data applications with integrated, end-to-end security.

Figure 2. Secure Network Connectivity with Cisco 1841 Router



Integrated Services

The new, high-performance and secure integrated services architecture of the Cisco 1841 router (as shown in Figure 2) enables customers to deploy simultaneous services such as secured data communications with traditional IP routing at wire-speed performance. By offering a hardware-based encryption on the motherboard that can be enabled with an optional Cisco IOS Software security image and the flexibility to integrate a wide array of services, modules, and interface cards, the Cisco 1841 router helps enable businesses to incorporate the functions of a standalone secure data solution.

Primary Features and Benefits

Architecture Features and Benefits

The Cisco 1841 modular architecture has been specifically designed to meet requirements of small to medium-sized businesses and small enterprise branch offices as well as service provider-managed applications for concurrent services at wire-speed performance. The Cisco 1841 router, together with other Cisco integrated services routers such as the Cisco 2800 Series, provide the broadest range of secure connectivity options in the industry combined with availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite of transport protocols, quality of service (QoS), and security. Table 1 gives the architecture features and benefits of the Cisco 1841 router.

Table 1. Architecture Features and Benefits of Cisco 1841 Router

Feature	Benefit
High-performance processor	Supports concurrent deployment of high-performance, secure data services with headroom for future applications
Modular architecture	• Offers wide variety of LAN and WAN options; network interfaces are field-upgradable to accommodate future technologies • Provides many types of slots to add connectivity and services in the future on an "integrate-as-you-grow" basis • Supports more than 30 modules and interface cards, including existing WAN (WIC) and multiflex (VWIC) interface cards (for data support only on the Cisco 1841 router) and advanced integration modules (AIMs)
Integrated hardware-based encryption acceleration	• Offers cryptography accelerator as standard integrated hardware that can be enabled with an optional Cisco IOS Software for 3DES and AES encryption support • Provides enhanced feature set of security performance through support of optional VPN acceleration card for VPN 3DES or AES encryption
Ample default memory	Provides 32 MB of Flash and 128 MB of synchronous dynamic RAM (SDRAM) memory to support deployment of concurrent services
Integrated dual high-speed Ethernet LAN ports	• Helps enable connectivity speeds up to 100BASE-T Ethernet technology without the need for cards and modules • Allows segmentation of the LAN
Support for Cisco IOS 12.3T, 12.4, 12.4T feature sets and beyond	• Supports the Cisco 1841 router starting with Cisco IOS Software Release 12.3T • Helps enable end-to-end solutions with support for latest Cisco IOS Software-based QoS, bandwidth management, and security features
Integrated standard power supply	Provides for easier installation and management of the router platform

Modularity Features and Benefits

The Cisco 1841 router provides enhanced modular capabilities while protecting customer investments. The modular architecture has been designed to provide the increased bandwidth and performance required to support concurrent, secure applications. Most existing WICs, multi-flex trunk interface cards (for data only), and Advanced Integration Modules (AIMs) are supported in the Cisco 1841. Table 2 lists the modularity features and benefits of the Cisco 1841 router.

Table 2. Modularity Features and Benefits of Cisco 1841 Router

Feature	Benefit
HWIC slots	• The modular architecture on the Cisco 1841 router supports HWIC slots. The newly designed high-speed WAN interface slots significantly increase the data-throughput capability (up to 800-Mbps aggregate). Table 6 lists the High Speed WAN Interface cards supported on the Cisco 1841. • Both slots on the Cisco 1841 router are HWIC slots and provide compatibility with WICs and multiflex trunk (VWICs) interface cards (for data only).
AIM slots (internal)	• The Cisco 1841 router supports hardware-accelerated encryption through AIM modules (AIM-VPN/BPII-PLUS, AIM-VPN/SSL-1). • The Cisco 1841 router has one internal AIM slot.

Secure Networking Features and Benefits

The Cisco 1800 Series features a built-in hardware-accelerated encryption on the motherboard that can be enabled with an optional Cisco IOS Software security image. The onboard hardware-based encryption acceleration offloads the encryption processes to provide greater IPSec 3DES and AES throughput. With the integration of optional VPN AIMs, NAC for antivirus defense, and Cisco IOS Software-based firewall and IPS support, Cisco offers the industry's leading robust and adaptable security solution for small to medium-sized businesses and small enterprise branch offices. Table 3 outlines router-integrated security features and benefits.

Table 3. Features and Benefits of Secure Networking

Feature	Benefit
Hardware-based encryption on motherboard	Support for hardware-based encryption on the Cisco 1841 can be enabled through an optional Cisco IOS Software security image.
AIM-based VPN acceleration	Support for an optional dedicated VPN AIM can deliver two to three times the performance of embedded encryption capabilities.
SSL Web VPN	Allows businesses to securely and transparently extend their networks to any Internet-enabled location using SSL VPN; the Cisco IOS WebVPN supports clientless access to applications such as HTML-based intranet content, e-mail, network file shares, and Citrix and to the Cisco SSL VPN Client, enabling full network access remotely to virtually any application
AIM-based SSL VPN	An optional dedicated SSL VPN AIM module provides SSL VPN acceleration and supports two times the number of tunnels when compared to embedded IOS based SSL VPN capabilities. The SSL VPN AIM module also supports IPSEC VPN and IP Payload Compression Protocol in hardware.
NAC	NAC allows network access only to compliant and trusted endpoint devices for antivirus defense.
IPS support	• Flexible support is provided with Cisco IOS Software. • New intrusion-detection-system (IDS) signatures can be dynamically loaded independent of the Cisco IOS Software release.
Cisco Easy VPN remote and server support	This feature eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
Cisco IOS Firewall, including URL filtering	URL filtering support is available with optional Cisco IOS Security Software.
Real-time clock support	Real-time clock support keeps an accurate value of date and time for applications that require an accurate time stamp—such as logging, debugging, and digital certificates.
Cisco Router and Security Device Manager (SDM)	• An intuitive, easy-to-use, Web-based device management tool embedded within the Cisco IOS Software access routers can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features. • Cisco SDM helps resellers and customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of the Cisco IOS Software command-line interface.
USB port (1.1)	The integrated USB port is configurable with an optional USB token for secure configuration distribution and off-platform storage of VPN credentials.

Cisco 1800 Series	Cisco 1841
Dimensions (W x D)	13.5 x 10.8 in. (34.3 x 27.4 cm) Height without rubber feet: 1.73 in. (4.39 cm) Height with rubber feet: 1.87 in. (4.75 cm)
Weight	Maximum: 6.2 lb (2.8 kg); with interface cards and modules Minimum: 6.0 lb (2.7 kg) (no interface cards and modules)
Architecture	
DRAM	Synchronous dual in-line memory module (DIMM) DRAM
DRAM capacity	Default: 128 MB Maximum: 384 MB
Flash memory	External compact Flash
Flash memory capacity	Default: 32 MB Maximum: 128 MB
Modular slots—total	Two
Modular slots for WAN access	Two
Modular slots for HWICs	Two
Modular slots for voice support	None—The Cisco 1841 does not support voice
Analog and digital voice support	No
VoIP support	Voice-over-IP (VoIP) pass-through only
Onboard Ethernet ports	Two 10/100
Onboard USB ports	One (1.1)
Console port	One–up to 115.2 kbps
Auxiliary port	One–up to 115.2 kbps
Onboard AIM slots	One (internal)
Packet-voice-DSP-module (PVDM) slots on motherboard	None—The Cisco 1841 does not support voice
Integrated hardware-based encryption on motherboard	Yes
Encryption support in software and hardware by default	DES, 3DES, AES 128, AES 192, AES 256
Power Supply Specifications	
Internal power supply	Yes
Redundant power supply	No
DC power support	No
AC input voltage	100 to 240 VAC
Frequency	50 to 60 Hz
AC input current	1.5A maximum
Output power	50W (maximum)
System Power Dissipation	
	153 BTU/hr
Software Support	
First Cisco IOS Software release	12.3(8)T
Cisco IOS Software default image, release	IP BASE, 12.4(1)
Environmental	
Operating temperature	32 to 104°F (0 to 40°C)
Operating humidity	10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating
Nonoperating Temperature	-4 to 149°F (-25 to 65°C)
Operating altitude	10,000 feet (3000 meters) @ 77°F (25°C)

Cisco 1800 Series	Cisco 1841
Noise level	Normal operating temperature: <78° F/26°C: 34 dBA >78°F/26°C through <104°F/40°C: 37 dBA >104°F/40°C: 42 dBA
Regulatory Compliance	
Safety	UL60950-1 CAN/CSA 60950-1 AS 3260 EN60950-1
EMI	EN 55022, 1998, class A CISPR22, 1997, class A CFR47, Part 15, Subpart B, 1995, class A EN61000-3-2 Harmonic Current Emission (only for equipment >75W but <16A) EN61000-3-3 Voltage Fluctuation and Flicker (only for equipment ≤16A)
Immunity	CISPR24, 1997 ITE-Immunity characteristics, Limits and methods of measurement EN 55024,1998 ITE-Immunity characteristics, Limits and methods of measurement EN50082-1, 1997 Electromagnetic compatibility—Generic immunity standard, Part 1 EN 300 386, 1997 Telecommunications network equipment EMC requirements The requirements are covered by the following standards: IEC 61000-4-2:1995 Immunity to Electrostatic Discharges IEC 61000-4-3:1995 Immunity to Radio Frequency Electromagnetic Fields IEC 61000-4-4:1995 Immunity to Electrical Fast Transients IEC 61000-4-5:1995 Immunity to Power Line Transients (Surges) IEC 61000-4-6:1996 Immunity to Radio Frequency Induced Conducted Disturbances IEC 61000-4-11:1995 Immunity to Voltage Dips, Voltage Variations, and Short Voltage Interruptions
Network homologation	USA—TIA-968-A, T1.TRQ.6-2001 Canada—CS-03 European Union—RTTE Directive 5/99 Argentina—CTR 21 Australia—AS/ACIF S002, S003, S016 , S031, 3043 Brazil—225-540-788, CTR3, 225-100-717 Edition 3, NET 001/92 1990 China—ITU-G.992.1, ITU-G.992.1, ITU-G.991.2, CTR3, ITU I.431 1993 Hong Kong—HKTA 2033, HKTA 2033, HKTA 2014, HKTA 2017 Issue 3 2003, HKTA 2011 Issue 1, HKTA 2011 Issue 2, HKTA 2013 Issue 1 India—I_DCA_18_02_Jun_99-199, S/ISN-01/02 Issue 1999 S/ISN-02 1 1998, IR/PRI-01/02 Issue 1 1998, S/INT-2W/02 MAY 2001, S/INT-2W/02 MAY 2001 Israel—U.S. approval accepted Japan—Technical condition (DoC acceptance in process) Korea—U.S. approval accepted Mexico—U.S. approval accepted New Zealand—PTC 270/272, CTR 3, ACA 016 Revision 4 1997, PTC 200 Singapore—IDA TS ADSL1 Issue 1, IDA TS ADSL 2, IDA TS HDSL, IDA TS ISDN 1 Issue 1 1999, IDA TS ISDN 3 Issue 1 1999, IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4 South Africa—U.S. approval accepted Taiwan—U.S. approval accepted

Items	Description	Cisco 1841
WIC-2AM	2-port analog modem WIC	√
WIC-1AM-V2	1-port analog modem WIC (updated version)	√
WIC-2AM-V2	2-port analog modem WIC (updated version)	√
T1, E1, and G.703 VWICs		
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk—T1	√ (data only)
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk—T1	√ (data only)
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk—T1 with drop and insert	√ (data only)
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk—E1	√ (data only)
VWIC-1MFT-G703	1-port RJ-48 multiflex trunk—G.703	√ (data only)
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk—E1	√ (data only)
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk—E1 with drop and insert	√ (data only)
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk—G.703	√ (data only)
VWIC2-1MFT-T1/E1	1-port 2nd generation multiflex trunk—T1/E1	√ (data only)
VWIC2-2MFT-T1/E1	2-port 2nd generation multiflex trunk—T1/E1	√ (data only)
VWIC2-1MFT-G703	1-port 2nd generation multiflex trunk—G.703	√ (data only)
VWIC2-2MFT-G703	2-port 2nd generation multiflex trunk—G703	√ (data only)
AIMs		
AIM-VPN/BPII-PLUS	Enhanced-performance DES, 3DES, AES, and compression VPN encryption AIM	√
AIM-VPN/SSL-1	DES/3DES/AES/SSL VPN Encryption/Compression	√

Cisco 1841	List of Supported Images in 12.4(T)
c1841-adventerprisek9-mz	ADVANCED ENTERPRISE SERVICES
c1841-spservicesk9-mz	SP SERVICES

Service and Support

Leading-edge technology deserves leading-edge support. Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business.

Cisco SMARTnet® technical support for the Cisco 1800 integrated services routers is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation.

All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- Twenty-four-hour-a-day access to the industry's largest dedicated technical support staff

For more information about Cisco Services, refer to Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco 1800 Series Integrated Services Router, visit http://www.cisco.com/go/1800 or contact your local account representative.

For more information about Cisco products, contact:

- **United States and Canada:** 800 553-NETS (6387)
- **Europe:** 32 2 778 4242
- **Australia:** 612 9935 4107
- **Other:** 408 526-7209
- **Web:** http://www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C78-367648-01 11/06

CISCO ETHERSWITCH HWIC SUMMARY

Table 1 gives the product numbers for the 4- and 9-port Cisco EtherSwitch HWICs.

Table 1. Product Numbers for 4- and 9-Port Cisco EtherSwitch HWICs

Product Number	Description
HWIC-4ESW	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
HWIC-4ESW-POE*	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC with power daughter card
HWIC-D-9ESW	9-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
HWIC-D-9ESW-POE**	9-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC with power daughter card

* This part number (HWIC-4ESW-POE) should be ordered only if you require in-line power. You must also order the matching internal power unit to support in-line power on a Cisco 2800 or Cisco 3800 router.

** This part number (HWIC-D-9ESW) should be ordered only if you require in-line power. You must also order the matching internal power unit to support in-line power on a Cisco 2800 or Cisco 3800 router.

Table 2 gives the power supply options for the Cisco 2800 and Cisco 3800 series to support inline power on the 4- and 9-port HWICs.

Table 2. Power Supply Product Numbers

Product Number	Description
PWR-2801-AC-IP=	Cisco 2801 AC inline power supply
PWR-2811-AC-IP=	Cisco 2811 AC inline power supply
PWR-2821-51-AC-IP=	Cisco 2821 and Cisco 2851 AC inline power supply
PWR-3825-AC-IP=	Cisco 3825 AC-IP power supply
PWR-3845-AC-IP=	Cisco 3845 AC-IP power supply

PLATFORM SUPPORT

Table 3 lists the supported platforms for the 4- and 9-port Cisco EtherSwitch HWICs.

Table 3. Supported Platforms for 4- and 9-Port Cisco EtherSwitch HWICs

Chassis	4-Port Cisco EtherSwitch HWIC	9-Port Cisco EtherSwitch HWIC	Internal Inline Power Supply (optional)
Cisco 1841	Yes, 2 HWICs per router	No	No
Cisco 2801	Yes, 2 HWICs per router	Yes, 2 HWICs per router	Yes
Cisco 2811	Yes, 2 HWICs per router	Yes, 2 HWICs per router	Yes
Cisco 2821	Yes, 2 HWICs per router	Yes, 2 HWICs per router	Yes
Cisco 2851	Yes, 2 HWICs per router	Yes, 2 HWICs per router	Yes
Cisco 3825	Yes, 2 HWICs per router	Yes, 2 HWICs per router	Yes
Cisco 3845	Yes, 2 HWICs per router	Yes, 2 HWICs per router	Yes

Note: The Cisco 2800 and Cisco 3800 series also offer bundles that already come with the inline power supply. The part numbers are CISCO2801-AC-IP, CISCO2811-AC-IP, CISCO2821-AC-IP, CISCO2851-AC-IP, CISCO3825-AC-IP, and CISCO3845-AC-IP. These bundles offer the router chassis with the inline power supply included to support inline power on the 4- and 9-port HWICs.

Converged IP Communications in a Small-to-Large Enterprise Branch Office with Data Devices and IP Phones

The 4- or 9-port Cisco EtherSwitch HWICs when combined with analog or digital voice modules for the Cisco 2800 and Cisco 3800 series routers provide a small-to-large enterprise branch office infrastructure for IP telephony deployments. This solution can be combined with Cisco CallManager Express IP Telephony or the Cisco IOS Software Survivable Remote Site Telephony (SRST) solution. SRST runs on the local branch office router, allowing it to automatically detect a failure in the network, and initiates a process to intelligently autoconfigure the router to provide call-processing backup redundancy for the IP phones in that office. In the case of a Cisco CallManager Express deployment, call-processing features are offered on the branch router without a centralized call manager.

The Cisco EtherSwitch HWIC with the optional internal chassis provides IP phone power and phone discovery for IP phones. In addition, the Cisco EtherSwitch HWIC supports separate VLAN configuration for IP phones. The auxiliary VLAN feature allows network administrators to segment phones into separate logical networks, even though the data and voice infrastructures are physically the same. The phone discovery feature allows the Cisco 4- and 9-port EtherSwitch HWICs (product numbers HWIC-4ESW-POE or HWIC-D-9ESW-POE) to automatically detect the presence of an IP phone and supply inline power.

For more information about the voice features for the Cisco 2800 and Cisco 3800 series routers, visit:
Cisco 2800 Series: http://www.cisco.com/go/2800
Cisco 3800 Series: http://www.cisco.com/go/3800

FEATURES AND BENEFITS

Table 4 gives the architecture, features, and benefits of the Cisco 4- and 9-port HWICs.

Table 4. Architecture, Features, and Benefits of 4- and 9-Port Cisco EtherSwitch HWICs

Feature	Benefit
4 or 9 10BASE-T/100BASE-TX Ports	These ports deliver up to 200 Mbps of aggregate bandwidth (full duplex) for forwarding Layer 2 traffic on each port.
Autosensing, Autonegotiation, and Auto-MDIX (Automatic Media-Dependant Interface Crossed Over)	• The Autosensing feature allows the switch to detect the speed of the attached device and automatically configure the port for 10- or 100-Mbps operation. • The Autonegotiation feature allows the switch to automatically select half- or full-duplex transmission mode to optimize bandwidth on all the ports of the HWIC • The Auto-MDIX feature allows the switch to automatically detect cable type (straight through vs. crossover) between the attached Ethernet device and switch line pairs.
Integrated Switching	Integrated switching provides fewer points of management for remote and small branch offices.
802.1P QoS (Traffic Prioritization)	This feature provides support for QoS based on the IEEE class of service (CoS) and port-based prioritization, allowing the switch to change the CoS settings of tagged packets on a per-port basis.
802.1Q Trunking	This feature allows the setup of separate VLANs with tagged and untagged framing; trunking is used to save ports when creating a link between two devices implementing VLANs; VLANs allow segmentation of the LAN.
802.1D Spanning Tree Protocol	This Layer 2 link-management protocol provides path redundancy while preventing undesirable loops in the network; it simplifies network configuration and improves fault tolerance.
Voice VLAN (VVLAN)	VVLANs help enable Cisco IP phones to place voice and data in their own separate VLANs. The HWIC switch port is manually configured as a trunk port to support voice and data VLANs on the same port. The switch then uses Cisco Discovery to dynamically configure the Cisco IP phones.
802.1x Authentication	This client-server-based access control and authentication protocol restricts unauthorized devices from connecting to a LAN through publicly accessible ports.

Feature	Description
Supported Router Platforms	• Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series integrated services routers: • Cisco 1841 (supports HWIC-4ESW only; no PoE support) • Cisco 2801 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845
Form Factor	• HWIC-4ESW = Single-wide HWIC form factor • HWIC-D-9ESW = Double-wide HWIC form factor
Dimensions (W x D x H)	• HWIC-4ESW = 3.08 x 4.74 x 0.76 in. • HWIC-D-9ESW = 6.20 x 4.74 x 0.76 in.
Weight	• HWIC-4ESW = 79 grams (0.17 lb) • HWIC-4ESW-POE = 108 grams (0.24 lb) • HWIC-D-9ESW = 149 grams (0.33 lb) • HWIC-D-9ESW-POE = 196 grams (0.43 lb)
Standards	
IEEE Protocols	• Ethernet: IEEE 802.3, 10BASE-T • Fast Ethernet: IEEE 802.3u, 100BASE-TX • IEEE 802.1d Spanning Tree Protocol • IEEE 802.1p CoS for Traffic Prioritization • IEEE 802.1q VLAN • IEEE 802.1x Security • IEEE 802.3x Full Duplex and Flow Control • IEEE 802.3af Power over Ethernet Standard
RFC	RFC 2284, PPP Extensible Authentication Protocol (EAP)
MIBs	• RFC 1213 • IF MIB • RFC 2037 ENTITY MIB • CISCO-CDP-MIB • CISCO-IMAGE-MIB • CISCO-FLASH-MIB • OLD-CISCO-CHASSIS-MIB • CISCO-VTP-MIB • CISCO-HSRP-MIB • OLD-CISCO-TS-MIB • CISCO-ENTITY-ASSET-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • BRIDGE MIB (RFC 1493) • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VLAN-IFINDEX-RELATIONSHIP-MIB • RMON1-MIB • PIM-MIB • CISCO-STP-EXTENSIONS-MIB • OSPF MIB (RFC 1253) • IPMROUTE-MIB • CISCO-MEMORY-POOL-MIB • ETHER-LIKE-MIB (RFC 1643) • CISCO-ENTITY-FRU-CONTROL-MIB.my • CISCO-RTTMON-MIB • CISCO-PROCESS-MIB • CISCO-COPS-CLIENT-MIB To obtain lists of supported MIBs by platform and Cisco IOS Software release, and to download MIB modules, go to the Cisco MIB Website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

http://www.cisco.com/go/2800
http://www.cisco.com/go/3800

Table 6 provides ordering information for the 4- and 9-port Cisco EtherSwitch HWICs.

Table 6. Ordering Information for 4- and 9-Port Cisco EtherSwitch HWICs (part numbers HWIC- 4ESW and HWIC-D-9ESW)

Product Number	Product Description
Ethernet HWICs	
HWIC-4ESW	4-port 10/100 Ethernet switch
HWIC-4ESW=	4-port 10/100 Ethernet switch, spare
HWIC-4ESW-POE	4-port 10/100 Ethernet switch with 4-port inline power daughter card
HWIC-4ESW-POE=	4-port 10/100 Ethernet switch with 4-port inline power daughter card, spare
HWIC-D-9ESW	9-port 10/100 Ethernet switch
HWIC-D-9ESW=	9-port 10/100 Ethernet switch, spare
HWIC-D-9ESW-POE	9-port 10/100 Ethernet switch with 8-port inline power daughter card
HWIC-D-9ESW-POE=	9-port 10/100 Ethernet switch with 8-port inline power daughter card, spare
Daughter Card Modules for Inline Power Support	
ILPM-4=	4-port inline power module for PoE applications, spare
ILPM-8=	8-port Inline power module for PoE applications, spare
Cisco 2800 and Cisco 3800 Routers with Inline Power Supply	
CISCO2801-AC-IP	Cisco 2801 router with inline power, 2 Fast Ethernet ports, 4 slots, IP BASE, 64F/128D
CISCO2811-AC-IP	Cisco 2811 with AC+PoE, 2 Fast Ethernet ports , 4 HWICs, 2 packet voice DSP modules (PVDMs), 1 enhanced network module [(NME), 2 advanced integration modules (AIMs), IP BASE, 64F/256D
CISCO2821-AC-IP	Cisco 2821 with AC+PoE, 2 Gigabit Ethernet ports, 4 HWICs, 3 PVDMs, 1 NME-X, 2 AIMs, IP BASE, 64F/256D
CISCO2851-AC-IP	Cisco 2851 with AC+PoE, 2 Gigabit Ethernet ports, 4 HWICs, 3 PVDMs, 1 NME-XD, 2 AIMs, IP BASE, 64F/256D
CISCO3825-AC-IP	2 Gigabit Ethernet router with 1 Small Form-Factor Pluggable (SFP), 2 NME-XHDs, 4 HWICs, IP BASE, power supply
CISCO3845-AC-IP	2 Gigabit Ethernet router with 1 SFP, 4 NME-XHDs, 4 HWICs, IP BASE, power supply
Inline Power Supply	
PWR-2801-AC-IP	Cisco 2801 AC inline power supply
PWR-2801-AC-IP=	Cisco 2801 AC inline power supply, spare
PWR-2821-51-AC-IP=	Cisco 2821 and Cisco 2851 AC-IP power supply, spare
PWR-3825-AC-IP=	Cisco 3825 AC-IP power supply, spare
PWR-3845-AC-IP=	Cisco 3845 AC-IP power supply, spare

Also, check with your Cisco representative regarding the Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series bundle offerings for security, voice, DSL, and other solutions.

CISCO IOS SOFTWARE SUPPORT

The Cisco EtherSwitch HWICs are supported in all Cisco IOS Software feature sets. Table 7 lists the first Cisco IOS Software release the 4- and 9-port HWICs are supported on for the respective routing platforms.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205290.BB_ETMG_CC_6.05

Printed in the USA

ANEXO 22

FVG-**2624**-2007 Guayaquil, 10 de Septiembre del 2007

Señores :
TRANSTELCO
Fonos: 2630335 EXT. 201
Edificio WTC Galerías Milenium Local 52
Ciudad.-

ATT. **ING. ANDREA PAGES**

De mis consideraciones:

FIRMESA INDUSTRIAL CIA. LTDA. empresa líder en el mercado, pone a sus ordenes 34 años de experiencia en el campo del ACONDICIONAMIENTO DEL SUMINISTRO ELECTRICO. FIRMESA cuenta con una excelente infraestructura, personal técnico altamente calificado y entrenado por nuestro proveedor en los Estados Unidos, lo cual nos permite brindar a nuestros clientes, un eficiente servicio y asesoria basados en la excelencia a la calidad. Además contamos con un stock completo de repuestos para asegurarle un respaldo permanente.

Tenemos el agrado de proveer a ustedes la siguiente cotización por UNA FUENTE DE ENERGIA ININTERRUMPIBLE, UPS marca POWERWARE SISTEMA EN LINEA, modelo **POWERWARE 9120 DE 3Kva** de nuestra representada POWERWARE CORPORATION(EXIDE ELECTRONICS) de los Estados Unidos de Norteamérica USA.

1.- **DESCRIPCIÓN DEL EQUIPO:**

CANTIDAD	DESCRIPCIÓN	P. TOTAL
1	UPS POWERWARE modelo **9120 de 3Kva** Baterías Selladas libres de mantenimiento VOLTAJE DE ENTRADA: 120 VAC .MONOFÁSICA RANGO DE SALIDA, : +/-2% Exactitud ON LINE ININTERRUMPIBLE, TECNOLOGÍA MULTICONVERCION TIEMPO DE TRANSFERENCIA: 0 MILISEGUNDOS Panel de Señalización (indicadores para cualquier anomalía Dentro del UPS). BYPASS : ELECTRÓNICO TIEMPO DE RESPALDO 10 MIN. AL 100% DE CARGA.	**USD$ 1.345,00**

Cant.	Descripción	V. Total
01	UPS POWERWARE modelo 9120 capacidad 3KVA tecnología ON LINE	$ 1.345.00
	CONFIGURACIÓN PARA 3 HORAS DE RESPALDO CON GABINETE	$ 3.901.20
	TOTAL DE UPS + CONFIGURACION	$ 5.246.20

NOTA: EN ESTOS VALORES NO ESTA INCLUIDO EL 12% DEL IVA.
INCLUYE SOTWARE PARA MONITOREO totalmente GRATIS

CARACTERÍSTICAS TÉCNICAS:	Descritas en el catálogo adjunto.
FORMA DE PAGO:	CONTADO
TIEMPO DE ENTREGA:	UPS: Inmediata Configuración: 15 Días
VALIDEZ DE LA OFERTA:	10 Días

2.- **ADIESTRAMIENTO:**

Firmesa se compromete a instruir a dos personas que el cliente designe, sobre el correcto manejo y operación de las unidades UPS ofertadas.

Para caso de mantenimiento Preventivo y/o Correctivo de las unidades, Firmesa dispone de técnicos entrenados, para realizar estos trabajos, quienes operan desde nuestras Divisiones Comerciales de Quito y Guayaquil.

3.- **INTERCALACIÓN:**

Firmesa se compromete a enviar, sin costo para el cliente, a uno de sus técnicos para intercalar el UPS a la red eléctrica. Por lo tanto, el cliente deberá tener listas sus líneas de acometida y alimentación hacia el UPS y desde el UPS hacia los equipos que se van a proteger.

Para la región Insular de Galápagos, el costo de intercalación se facturará por separado.

4.- **SOPORTE:**

Firmesa realizará visitas técnicas, las mismas que obedecerán a llamadas que haga el cliente a través de nuestros LINEAS DE SERVICIO AL CLIENTE, así como nuestros teléfonos celulares que estarán a su disposición durante las 24 horas, los 365 dias del año, tanto en Quito como en Guayaquil.

Si en algún momento llegara a presentarse un problema técnico mayor que amerite que el UPS sea trasladado a nuestras instalaciones industriales para recibir servicio, FIRMESA se compromete a respaldar al cliente mediante el préstamo de un equipo de acondicionamiento o UPS, hasta que el UPS de su propiedad sea reparado.

5.- **GARANTIA:**

POWERWARE CORPORATION ofrece dos años de garantía para todos sus productos. FIRMESA INDUSTRIAL CIA. LTDA. en su calidad de REPRESENTANTE AUTORIZADO PARA VENTAS Y SERVICIO EN EL ECUADOR, hace efectiva esta garantía en forma LOCAL.

La garantía del UPS puede extenderse indefinidamente mediante la firma de CONTRATOS DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO que tendrá una duración de un año adicional, o el tiempo que el cliente crea conveniente.

Firmesa compromete a brindar servicio técnico, acesoria permanente y mantener un stock completo de partes y piezas de la unidad ofertada.

En caso de que surgiere cualquier consulta técnica o de otra índole, estaremos gustosos de atenderles.

Atentamente,
FIRMESA INDUSTRIAL CIA. LTDA.

CAROLINA GONZALEZ
SUBGERENTE DE VENTAS
DIV. COMERCIAL GQUIL.
CEL.: 097786434

MARIUXI ROMERO
ASESORA COMERCIAL
DIV. COMERCIAL GYE
CEL: 085044446

ANEXO 22

FVG-2624-2007 Guayaquil, 10 de Septiembre del 2007

Señores :
TRANSTELCO
Ciudad.-

ATT : **SRTA. ANDREA PAGES**

De mis consideraciones:

FIRMESA INDUSTRIAL CIA. LTDA. empresa líder en el mercado, pone a sus ordenes 34 años de experiencia en el campo del ACONDICIONAMIENTO DEL SUMINISTRO ELECTRICO. FIRMESA cuenta con una excelente infraestructura, personal técnico altamente calificado y entrenado por nuestro proveedor en los Estados Unidos, lo cual nos permite brindar a nuestros clientes, un eficiente servicio y asesoria basados en la excelencia a la calidad. Además contamos con un stock completo de repuestos para asegurarle un respaldo permanente.

Tenemos el agrado de proveer a ustedes la siguiente cotización por TRECE FUENTES DE ENERGIA ININTERRUMPIBLE, UPS marca POWERWARE SISTEMA EN LINEA, modelo POWERWARE 9120 DE 700 VA de nuestra representada POWERWARE CORPORATION de los Estados Unidos de Norteamérica USA.

1.- **DESCRIPCIÓN DEL EQUIPO:**

CANTIDAD	DESCRIPCIÓN	P. UNITARIO	P. TOTAL
13	**UPS POWERWARE modelo 9120 de 700 va** baterías Selladas libres de mantenimiento VOLTAJE DE ENTRADA: **120 VAC .MONOFÁSICA** **RANGO DE SALIDA, : +/-2% Exactitud** ON LINE ININTERRUMPIBLE, TECNOLOGÍA MULTICONVERCION TIEMPO DE TRANSFERENCIA: **0 MILISEGUNDOS** PANTALLA LCD Panel de Señalización (indicadores para cualquier anomalía Dentro del UPS). Bypass AUTOMATICO Y MANUAL ELECTRÓNICO **TIEMPO DE RESPALDO 7 MIN. AL 100% DE CARGA.**	**$ 525.00**	**$ 6.825,00**

Cant.	Descripción	V. Unitario	V. Total
13	UPS POWERWARE modelo 9120 capacidad 700 va tecnología ON LINE	$ 525.00	$ 6.825.00
	CONFIGURADO CON 1 HORA DE RESPALDO CON GABINETE	$ 691.34	$ 8.987.42
	TOTAL DEL UPS + CONFIGURACION	$ 1.216.34	$ 15.812.42

NOTA: **EN ESTOS VALORES NO ESTA INCLUIDO EL 12% DEL IVA.**
INCLUYE SOTWARE PARA MONITOREO totalmente GRATIS

CARACTERÍSTICAS TÉCNICAS:	Descritas en el catálogo adjunto.
FORMA DE PAGO:	Contado
TIEMPO DE ENTREGA:	UPS: Inmediata CONFIGURACIÓN: 15 Días
VALIDEZ DE LA OFERTA:	10 Días

2.- **ADIESTRAMIENTO:**

Firmesa se compromete a instruir a dos personas que el cliente designe, sobre el correcto manejo y operación de las unidades UPS ofertadas.

Para caso de mantenimiento Preventivo y/o Correctivo de las unidades, Firmesa dispone de técnicos entrenados, para realizar estos trabajos, quienes operan desde nuestras Divisiones Comerciales de Quito y Guayaquil.

3.- **INTERCALACIÓN:**

Firmesa se compromete a enviar, sin costo para el cliente, a uno de sus técnicos para intercalar el UPS a la red eléctrica. Por lo tanto, el cliente deberá tener listas sus líneas de acometida y alimentación hacia el UPS y desde el UPS hacia los equipos que se van a proteger.

Para la región Insular de Galápagos, el costo de intercalación se facturará por separado.

4.- **SOPORTE:**

Firmesa realizará visitas técnicas, las mismas que obedecerán a llamadas que haga el cliente a través de nuestros LINEAS DE SERVICIO AL CLIENTE, así como nuestros teléfonos celulares que estarán a su disposición durante las 24 horas, los 365 dias del año, tanto en Quito como en Guayaquil.

Si en algún momento llegara a presentarse un problema técnico mayor que amerite que el UPS sea trasladado a nuestras instalaciones industriales para recibir servicio, FIRMESA se compromete a respaldar al cliente mediante el préstamo de un equipo de acondicionamiento o UPS, hasta que el UPS de su propiedad sea reparado.

5.- **GARANTIA:**

POWERWARE CORPORATION ofrece dos años de garantía para todos sus productos. FIRMESA INDUSTRIAL CIA. LTDA. en su calidad de REPRESENTANTE AUTORIZADO PARA VENTAS Y SERVICIO EN EL ECUADOR, hace efectiva esta garantía en forma LOCAL.

La garantía del UPS puede extenderse indefinidamente mediante la firma de CONTRATOS DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO que tendrá una duración de un año adicional, o el tiempo que el cliente crea conveniente.

Firmesa compromete a brindar servicio técnico, acesoria permanente y mantener un stock completo de partes y piezas de la unidad ofertada.

En caso de que surgiere cualquier consulta técnica o de otra índole, estaremos gustosos de atenderles.

Atentamente,
FIRMESA INDUSTRIAL CIA. LTDA.

CAROLINA GONZALEZ
SUBGERENTE DE VENTAS
DIV. COMERCIAL GYE.
CEL: 097786434

MARIUXI ROMERO
ASESORA COMERCIAL
DIV. COMERCIAL GYE.
CEL: 085044446

ANEXO 23

TABLA DE AMORTIZACION

MONTO	260,000.00
PLAZO AÑOS	10.00
PAGOS	12.00
TASA	15%
PAGOS	-$4,194.71

DIVIDENDOS	CAPITAL	INTERES	PAGO	SLDO. CAPITAL
0				260,000.00
1	-$944.71	-$3,250.00	-$4,194.71	$259,055.29
2	-$956.52	-$3,238.19	-$4,194.71	$258,098.77
3	-$968.47	-$3,226.23	-$4,194.71	$257,130.30
	-$2,869.71	-$9,714.43	-$12,583.13	
4	-$980.58	-$3,214.13	-$4,194.71	$256,149.72
5	-$992.84	-$3,201.87	-$4,194.71	$255,156.88
6	-$1,005.25	-$3,189.46	-$4,194.71	$254,151.63
	-$2,978.67	-$9,605.46	-$12,583.13	
7	-$1,017.81	-$3,176.90	-$4,194.71	$253,133.82
8	-$1,030.54	-$3,164.17	-$4,194.71	$252,103.28
9	-$1,043.42	-$3,151.29	-$4,194.71	$251,059.87
	-$3,091.77	-$9,491.36	-$12,583.13	
10	-$1,056.46	-$3,138.25	-$4,194.71	$250,003.41
11	-$1,069.67	-$3,125.04	-$4,194.71	$248,933.74
12	-$1,083.04	-$3,111.67	-$4,194.71	$247,850.70
	-$3,209.16	-$9,374.96	-$12,584.13	
	-$12,149.30	-$38,187.21	-$50,336.51	
13	-$1,096.58	-$3,098.13	-$4,194.71	$246,754.13
14	-$1,110.28	-$3,084.43	-$4,194.71	$245,643.84
15	-$1,124.16	-$3,070.55	-$4,194.71	$244,519.68
16	-$1,138.21	-$3,056.50	-$4,194.71	$243,381.47
17	-$1,152.44	-$3,042.27	-$4,194.71	$242,229.03
18	-$1,166.85	-$3,027.86	-$4,194.71	$241,062.18
19	-$1,181.43	-$3,013.28	-$4,194.71	$239,880.75
20	-$1,196.20	-$2,998.51	-$4,194.71	$238,684.55
21	-$1,211.15	-$2,983.56	-$4,194.71	$237,473.40
22	-$1,226.29	-$2,968.42	-$4,194.71	$236,247.11
23	-$1,241.62	-$2,953.09	-$4,194.71	$235,005.49
24	-$1,257.14	-$2,937.57	-$4,194.71	$233,748.35
	-$14,102.35	-$36,234.15	-$50,336.51	
25	-$1,272.85	-$2,921.85	-$4,194.71	$232,475.50
26	-$1,288.77	-$2,905.94	-$4,194.71	$231,186.73
27	-$1,304.87	-$2,889.83	-$4,194.71	$229,881.86
28	-$1,321.19	-$2,873.52	-$4,194.71	$228,560.67
29	-$1,337.70	-$2,857.01	-$4,194.71	$227,222.97
30	-$1,354.42	-$2,840.29	-$4,194.71	$225,868.55
31	-$1,371.35	-$2,823.36	-$4,194.71	$224,497.20
32	-$1,388.49	-$2,806.21	-$4,194.71	$223,108.70
33	-$1,405.85	-$2,788.86	-$4,194.71	$221,702.85
34	-$1,423.42	-$2,771.29	-$4,194.71	$220,279.43
35	-$1,441.22	-$2,753.49	-$4,194.71	$218,838.21
36	-$1,459.23	-$2,735.48	-$4,194.71	$217,378.98
	-$16,369.37	-$33,967.14	-$50,336.51	
37	-$1,477.47	-$2,717.24	-$4,194.71	$215,901.51
38	-$1,495.94	-$2,698.77	-$4,194.71	$214,405.57
39	-$1,514.64	-$2,680.07	-$4,194.71	$212,890.93
40	-$1,533.57	-$2,661.14	-$4,194.71	$211,357.36
41	-$1,552.74	-$2,641.97	-$4,194.71	$209,804.62
42	-$1,572.15	-$2,622.56	-$4,194.71	$208,232.46
43	-$1,591.80	-$2,602.91	-$4,194.71	$206,640.66
44	-$1,611.70	-$2,583.01	-$4,194.71	$205,028.96
45	-$1,631.85	-$2,562.86	-$4,194.71	$203,397.11
46	-$1,652.24	-$2,542.46	-$4,194.71	$201,744.87
47	-$1,672.90	-$2,521.81	-$4,194.71	$200,071.97
48	-$1,693.81	-$2,500.90	-$4,194.71	$198,378.16
	-$19,000.82	-$31,335.69	-$50,336.51	
49	-$1,714.98	-$2,479.73	-$4,194.71	$196,663.18
50	-$1,736.42	-$2,458.29	-$4,194.71	$194,926.76
51	-$1,758.12	-$2,436.58	-$4,194.71	$193,168.64
52	-$1,780.10	-$2,414.61	-$4,194.71	$191,388.54
53	-$1,802.35	-$2,392.36	-$4,194.71	$189,586.18
54	-$1,824.88	-$2,369.83	-$4,194.71	$187,761.30
55	-$1,847.69	-$2,347.02	-$4,194.71	$185,913.61
56	-$1,870.79	-$2,323.92	-$4,194.71	$184,042.82
57	-$1,894.17	-$2,300.54	-$4,194.71	$182,148.65
58	-$1,917.85	-$2,276.86	-$4,194.71	$180,230.80
59	-$1,941.82	-$2,252.88	-$4,194.71	$178,288.97
60	-$1,966.10	-$2,228.61	-$4,194.71	$176,322.88
	-$22,055.29	-$28,281.22	-$50,336.51	
61	-$1,990.67	-$2,204.04	-$4,194.71	$174,332.20
62	-$2,015.56	-$2,179.15	-$4,194.71	$172,316.65
63	-$2,040.75	-$2,153.96	-$4,194.71	$170,275.90
64	-$2,066.26	-$2,128.45	-$4,194.71	$168,209.64
65	-$2,092.09	-$2,102.62	-$4,194.71	$166,117.55
66	-$2,118.24	-$2,076.47	-$4,194.71	$163,999.31
67	-$2,144.72	-$2,049.99	-$4,194.71	$161,854.59
68	-$2,171.53	-$2,023.18	-$4,194.71	$159,683.06
69	-$2,198.67	-$1,996.04	-$4,194.71	$157,484.39
70	-$2,226.15	-$1,968.55	-$4,194.71	$155,258.24
71	-$2,253.98	-$1,940.73	-$4,194.71	$153,004.26
72	-$2,282.16	-$1,912.55	-$4,194.71	$150,722.10
	-$25,600.77	-$24,735.73	-$50,336.51	

Anexo

DIVIDENDOS	CAPITAL	INTERES	PAGO	SLDO. CAPITAL
73	-$2,310.68	-$1,884.03	-$4,194.71	$148,411.42
74	-$2,339.57	-$1,855.14	-$4,194.71	$146,071.85
75	-$2,368.81	-$1,825.90	-$4,194.71	$143,703.04
76	-$2,398.42	-$1,796.29	-$4,194.71	$141,304.62
77	-$2,428.40	-$1,766.31	-$4,194.71	$138,876.22
78	-$2,458.76	-$1,735.95	-$4,194.71	$136,417.46
79	-$2,489.49	-$1,705.22	-$4,194.71	$133,927.97
80	-$2,520.61	-$1,674.10	-$4,194.71	$131,407.36
81	-$2,552.12	-$1,642.59	-$4,194.71	$128,855.25
82	-$2,584.02	-$1,610.69	-$4,194.71	$126,271.23
83	-$2,616.32	-$1,578.39	-$4,194.71	$123,654.91
84	-$2,649.02	-$1,545.69	-$4,194.71	$121,005.89
	-$29,716.21	-$20,620.29	-$50,336.51	
85	-$2,682.14	-$1,512.57	-$4,194.71	$118,323.75
86	-$2,715.66	-$1,479.05	-$4,194.71	$115,608.09
87	-$2,749.61	-$1,445.10	-$4,194.71	$112,858.48
88	-$2,783.98	-$1,410.73	-$4,194.71	$110,074.51
89	-$2,818.78	-$1,375.93	-$4,194.71	$107,255.73
90	-$2,854.01	-$1,340.70	-$4,194.71	$104,401.72
91	-$2,889.69	-$1,305.02	-$4,194.71	$101,512.03
92	-$2,925.81	-$1,268.90	-$4,194.71	$98,586.22
93	-$2,962.38	-$1,232.33	-$4,194.71	$95,623.84
94	-$2,999.41	-$1,195.30	-$4,194.71	$92,624.43
95	-$3,036.90	-$1,157.81	-$4,194.71	$89,587.52
96	-$3,074.86	-$1,119.84	-$4,194.71	$86,512.66
	-$34,493.23	-$15,843.28	-$50,336.51	
97	-$3,113.30	-$1,081.41	-$4,194.71	$83,399.36
98	-$3,152.22	-$1,042.49	-$4,194.71	$80,247.14
99	-$3,191.62	-$1,003.09	-$4,194.71	$77,055.52
100	-$3,231.51	-$963.19	-$4,194.71	$73,824.01
101	-$3,271.91	-$922.80	-$4,194.71	$70,552.10
102	-$3,312.81	-$881.90	-$4,194.71	$67,239.29
103	-$3,354.22	-$840.49	-$4,194.71	$63,885.07
104	-$3,396.15	-$798.56	-$4,194.71	$60,488.93
105	-$3,438.60	-$756.11	-$4,194.71	$57,050.33
106	-$3,481.58	-$713.13	-$4,194.71	$53,568.75
107	-$3,525.10	-$669.61	-$4,194.71	$50,043.65
108	-$3,569.16	-$625.55	-$4,194.71	$46,474.49
	-$40,038.17	-$10,298.34	-$50,336.51	
109	-$3,613.78	-$580.93	-$4,194.71	$42,860.71
110	-$3,658.95	-$535.76	-$4,194.71	$39,201.76
111	-$3,704.69	-$490.02	-$4,194.71	$35,497.07
112	-$3,751.00	-$443.71	-$4,194.71	$31,746.08
113	-$3,797.88	-$396.83	-$4,194.71	$27,948.20
114	-$3,845.36	-$349.35	-$4,194.71	$24,102.84
115	-$3,893.42	-$301.29	-$4,194.71	$20,209.42
116	-$3,942.09	-$252.62	-$4,194.71	$16,267.32
117	-$3,991.37	-$203.34	-$4,194.71	$12,275.96
118	-$4,041.26	-$153.45	-$4,194.71	$8,234.70
119	-$4,091.78	-$102.93	-$4,194.71	$4,142.92
120	-$4,142.92	-$51.79	-$4,194.71	-$0.00
Total	-$46,474.49	-$3,862.02	-$50,336.51	

Total General	-$260,000.00	-$243,365.07	-$503,365.07

Anexo

ANEXO 24

SISTEMA DE BANCOS PRIVADOS

SERIES DE LAS TASAS ACTIVAS NOMINALES PROMEDIO PONDERADAS, POR ENTIDAD

(en porcentales)

Recuerde seleccionar fecha, entidad y/o plazo para una mejor consulta de datos.

ESCOGER FECHA	ENTIDADES	PLAZOS	Comercial TNPP	Consumo TNPP	Microcredito TNPP	Vivienda TNPP
Jul-07	AMAZONAS	1) 1 a 30 días	12.49	13.78		
Jul-07	AUSTRO	1) 1 a 30 días	12.53	13.81		
Jul-07	CITIBANK	1) 1 a 30 días	12.31			
Jul-07	COFIEC	1) 1 a 30 días	12.31			
Jul-07	COMERCIAL DE MANABI	1) 1 a 30 días	12.49	13.78		
Jul-07	DE GUAYAQUIL	1) 1 a 30 días	12.50	13.83		
Jul-07	DE LA PRODUCCION	1) 1 a 30 días	12.24	13.72		
Jul-07	DE LOJA	1) 1 a 30 días	12.52		13.41	
Jul-07	DE MACHALA	1) 1 a 30 días	12.53	13.82	13.81	
Jul-07	DEL LITORAL	1) 1 a 30 días	12.53	13.82		
Jul-07	DEL PACIFICO	1) 1 a 30 días	12.54	13.67	14.61	
Jul-07	GENERAL RUMIÑAHUI	1) 1 a 30 días	12.48	13.51		
Jul-07	INTERNACIONAL	1) 1 a 30 días	12.47	13.51		
Jul-07	MM JARAMILLO ARTEAGA	1) 1 a 30 días	12.56	13.49		
Jul-07	PICHINCHA	1) 1 a 30 días	12.50	13.52		10.00
Jul-07	SOLIDARIO	1) 1 a 30 días	12.54	13.67		
Jul-07	SUDAMERICANO	1) 1 a 30 días	12.33	13.73		
Jul-07	BOLIVARIANO	1) 1 a 30 días	12.21			11.75
Jul-07	CAPITAL	1) 1 a 30 días		13.79		
Jul-07	DELBANK	1) 1 a 30 días		13.51		
Jul-07	LLOYDS TSB BANK	1) 1 a 30 días	12.33	13.78		
Jul-07	PROCREDIT	1) 1 a 30 días		13.77	13.36	
Jul-07	UNIBANCO	1) 1 a 30 días	12.53	13.81		
Jul-07	**TOTAL SISTEMA**	**1) 1 a 30 días**	**12.45**	**13.70**	**13.80**	**10.88**

SISTEMA DE COOPERATIVAS DE AHORRO Y CREDITO
SERIES DE LAS TASAS ACTIVAS NOMINALES PROMEDIO PONDERADAS, POR ENTIDAD
(en porcentales)

Recuerde seleccionar fecha, entidad y/o plazo para una mejor consulta de datos.

ESCOGER FECHA	ENTIDADES	PLAZOS	Comercial	Consumo	Microcredito	Vivienda
			TNPP	TNPP	TNPP	TNPP
Jul-07	ALIANZA DEL VALLE	1) 1 a 30 días		13.81		
Jul-07	CAMARA DE COMERCIO DE QUITO LTDA.	1) 1 a 30 días		13.77		
Jul-07	15 DE ABRIL	1) 1 a 30 días		13.77		
Jul-07	23 DE JULIO	1) 1 a 30 días		13.77	13.39	
Jul-07	29 DE OCTUBRE	1) 1 a 30 días		13.66		
Jul-07	ANDALUCIA	1) 1 a 30 días		13.77		
Jul-07	CACPECO	1) 1 a 30 días		13.78	13.67	
Jul-07	DE LA PEQUEÑA EMPRESA BIBLIA	1) 1 a 30 días		13.79		
Jul-07	GUARANDA	1) 1 a 30 días		13.78		
Jul-07	NACIONAL	1) 1 a 30 días		13.79	13.71	
Jul-07	PABLO MUÑOZ VEGA	1) 1 a 30 días		13.81	13.76	
Jul-07	PROGRESO	1) 1 a 30 días		13.77		
Jul-07	RIOBAMBA	1) 1 a 30 días		13.51	13.40	
Jul-07	SAN FRANCISCO	1) 1 a 30 días		13.77	13.39	
Jul-07	SANTA ROSA	1) 1 a 30 días		13.77		
Jul-07	TULCAN	1) 1 a 30 días		13.78		
Jul-07	COOPERATIVA PADRE JULIAN LORENTE LTDA.	1) 1 a 30 días		15.67		
Jul-07	COOPMEGO	1) 1 a 30 días		13.77		
Jul-07	JUVENTUD ECUATORIANA PROGRESISTA LTDA.	1) 1 a 30 días		13.77	13.36	
Jul-07	**TOTAL SISTEMA**	**1) 1 a 30 días**		**13.86**	**13.53**	

SISTEMA DE MUTUALISTAS

SERIES DE LAS TASAS ACTIVAS NOMINALES PROMEDIO PONDERADAS, POR ENTIDAD

(en porcentales)

Recuerde seleccionar fecha, entidad y/o plazo para una mejor consulta de

ESCOGER FECHA			Comercial	Consumo	Microcrédito	Vivienda
	ENTIDADES	PLAZOS	TNPP	TNPP	TNPP	TNPP
Jul-07	BENALCAZAR	3) 91 a 180 días		13.27		
Jul-07	BENALCAZAR	5) 361 días o mayor	10.16	13.2		11.23
Jul-07	AMBATO	5) 361 días o mayor		13.19		11.47
Jul-07	AZUAY	2) 31 a 90 días		13.6		
Jul-07	AZUAY	3) 91 a 180 días				10.59
Jul-07	AZUAY	4) 181 a 360 días		12.66		
Jul-07	AZUAY	5) 361 días o mayor	10.2	13.19		11.46
Jul-07	IMBABURA	2) 31 a 90 días	11.52			
Jul-07	IMBABURA	5) 361 días o mayor	10.2	13.19	12.94	11.47
Jul-07	PICHINCHA	1) 1 a 30 días	12.48	13.77		
Jul-07	PICHINCHA	2) 31 a 90 días	11.65	13.6		11.55
Jul-07	PICHINCHA	3) 91 a 180 días	10.9	13.25		
Jul-07	PICHINCHA	4) 181 a 360 días	11.15	12.66		
Jul-07	PICHINCHA	5) 361 días o mayor	10.2	13.2		11.45
Jul-07	Total Sistema	1) 1 a 30 días	12.48	13.77		
Jul-07	Total Sistema	2) 31 a 90 días	11.59	13.60		11.55
Jul-07	Total Sistema	3) 91 a 180 días	10.90	13.26		10.59
Jul-07	Total Sistema	4) 181 a 360 días	11.15	12.66		
Jul-07	Total Sistema	5) 361 días o mayor	10.19	13.19	12.94	11.42

SISTEMA DE SOCIEDADES FINANCIERAS

SERIES DE LAS TASAS ACTIVAS NOMINALES PROMEDIO PONDERADAS, POR ENTIDAD

(en porcentales)

Recuerde seleccionar fecha, entidad y/o plazo para una mejor consulta de

ESCOGER FECHA	ENTIDADES	PLAZOS	Comercial TNPP	Consumo TNPP	Microcredito TNPP	Vivienda TNPP
Jul-07	FINCA S.A.	5) 361 días o mayor			12.91	
Jul-07	PROINCO S.A.	5) 361 días o mayor	9.91	13.18		
Jul-07	CONSULCREDITO	5) 361 días o mayor	10.46	13.18	12.86	11.07
Jul-07	DINERS CLUB	5) 361 días o mayor	10.45	13.19		
Jul-07	FIDASA	5) 361 días o mayor		13.18	13.00	11.48
Jul-07	FIRESA	5) 361 días o mayor	10.12	13.20		
Jul-07	GLOBAL	5) 361 días o mayor	10.20	13.19		11.47
Jul-07	INTERAMERICANA	5) 361 días o mayor	10.20			11.44
Jul-07	LEASINGCORP	5) 361 días o mayor	10.32	13.02		
Jul-07	UNIFINSA	5) 361 días o mayor	10.16	13.20		11.22
Jul-07	VAZCORP S.A.	5) 361 días o mayor	10.24	13.19	13.02	
Jul-07	**Total Sistema**	**5) 361 días o mayor**	**10.23**	**13.17**	**12.95**	**11.34**